CA Enterprise Log Manager

Guía de referencia de la gramática de eventos comunes

r12.5



Esta documentación, que incluye sistemas incrustados de ayuda y materiales distribuidos por medios electrónicos (en adelante, referidos como la "Documentación") se proporciona con el único propósito de informar al usuario final, pudiendo CA proceder a su modificación o retirada en cualquier momento.

Queda prohibida la copia, transferencia, reproducción, divulgación, modificación o duplicado de la totalidad o parte de esta Documentación sin el consentimiento previo y por escrito de CA. Esta Documentación es información confidencial, propiedad de CA, y no puede ser divulgada por Vd. ni puede ser utilizada para ningún otro propósito distinto, a menos que haya sido autorizado en virtud de (i) un acuerdo suscrito aparte entre Vd. y CA que rija su uso del software de CA al que se refiere la Documentación; o (ii) un acuerdo de confidencialidad suscrito aparte entre Vd. y CA.

No obstante lo anterior, si dispone de licencias de los productos informáticos a los que se hace referencia en la Documentación, Vd. puede imprimir, o procurar de alguna otra forma, un número razonable de copias de la Documentación, que serán exclusivamente para uso interno de Vd. y de sus empleados, y cuyo uso deberá guardar relación con dichos productos. En cualquier caso, en dichas copias deberán figurar los avisos e inscripciones relativas a los derechos de autor de CA.

Este derecho a realizar copias de la Documentación sólo tendrá validez durante el período en que la licencia aplicable para el software en cuestión esté en vigor. En caso de terminarse la licencia por cualquier razón, Vd. es el responsable de certificar por escrito a CA que todas las copias, totales o parciales, de la Documentación, han sido devueltas a CA o, en su caso, destruidas.

EN LA MEDIDA EN QUE LA LEY APLICABLE LO PERMITA, CA PROPORCIONA ESTA DOCUMENTACIÓN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO INCLUIDAS, ENTRE OTRAS PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN FIN CONCRETO Y NO INCUMPLIMIENTO. CA NO RESPONDERÁ EN NINGÚN CASO, ANTE VD. NI ANTE TERCEROS, EN LOS SUPUESTOS DE DEMANDAS POR PÉRDIDAS O DAÑOS, DIRECTOS O INDIRECTOS, QUE SE DERIVEN DEL USO DE ESTA DOCUMENTACIÓN INCLUYENDO A TÍTULO ENUNCIATIVO PERO SIN LIMITARSE A ELLO, LA PÉRDIDA DE BENEFICIOS Y DE INVERSIONES, LA INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL, LA PÉRDIDA DEL FONDO DE COMERCIO O LA PÉRDIDA DE DATOS, INCLUSO CUANDO CA HUBIERA PODIDO SER ADVERTIDA CON ANTELACIÓN Y EXPRESAMENTE DE LA POSIBILIDAD DE DICHAS PÉRDIDAS O DAÑOS.

El uso de cualquier producto informático al que se haga referencia en la Documentación se regirá por el acuerdo de licencia aplicable. Los términos de este aviso no modifican, en modo alguno, dicho acuerdo de licencia.

CA es el fabricante de esta Documentación.

Esta Documentación presenta "Derechos Restringidos". El uso, la duplicación o la divulgación por parte del gobierno de los Estados Unidos está sujeta a las restricciones establecidas en las secciones 12.212, 52.227-14 y 52.227-19(c)(1) - (2) de FAR y en la sección 252.227-7014(b)(3) de DFARS, según corresponda, o en posteriores.

Copyright © 2010 CA. Todos los derechos reservados. Todas las marcas registradas y nombres comerciales, logotipos y marcas de servicios a los que se hace referencia en este documento pertenecen a sus respectivas compañías.

Referencias a productos de CA Technologies

En este documento se hace referencia a los siguientes productos de CA Technologies:

- CA Access Control
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Log Manager
- CA Identity Manager
- CA IT Process Automation Manager (CA IT PAM)
- CA NSM
- Centro de comandos de seguridad de CA (CA SCC)
- CA Service Desk
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

Información de contacto del servicio de Asistencia técnica

Para obtener asistencia técnica en línea, una lista completa de direcciones y el horario de servicio principal, acceda a la sección de Asistencia técnica en la dirección http://www.ca.com/worldwide.

Contenido

Capítulo 1: ¿Qué es la Gramática de eventos comunes? 39

Siete áreas de un evento 40
- Actor - Origen 40
- Actor - Destino 42
- Origen de evento 43
- Observador - Agente 43
- Repositorio de eventos 44
- Evento específico 45
- Especificación de resultado 46

Tipos de eventos 47
- Tipo 1: evento local 48
- Tipo 2: evento remoto 48
- Tipo 3: evento observado 49
- Tipo 4: evento observado distribuido 49

Identificación del tipo de evento 50

Capítulo 2: Normalización y categorización de eventos 51

Modelos ideales 52
- Lista de modelos ideales 52

Categorías de eventos 54
- Lista de categorías de eventos 54

Clases de eventos 57
- Lista de clases de eventos 57

Acciones de eventos 65
- Lista de acciones de eventos 66

Resultado del evento 70
- Ejemplo de asignación de resultado de eventos 70
- Severidad del evento 71

Valores de severidad de eventos 72

Capítulo 3: Categoría de gestión de configuraciones 75

Clase de gestión de configuraciones 75
- Acción de modificación de configuración 75

Acción de error de configuración 76
Acción de configuración de Vaciar todo 77
Acción de configuración de Vaciar territorios de autenticación 78
Acción de configuración de Vaciar caché de usuario 79
Acción de alerta de configuración 81
Acción de notificación de configuración 82
Acción de lectura de configuración 83
Acción de inicio de lectura de configuración 84
Acción de estado de configuración 85
Acción de advertencia de configuración 86
Acción de modificación de hora del sistema 87
Acción de creación de tareas 88
Acción de supresión de tareas 89
Acción de modificación de tareas 90
Acción de informes de tareas 91
Clase de gestión de políticas 92
Acción de configuración de políticas de contraseñas 92
Acción de activación de políticas 93
Acción de aplicación de políticas 94
Acción de creación de políticas 95
Acción de desactivación de políticas 96
Acción de supresión de políticas 97
Acción de error de política 98
Acción de lista de políticas 99
Acción de modificación de políticas 100
Acción de notificación de políticas 101
Acción de sustitución de política 102
Acción de advertencia de política 103
Acción de estado de reglas o políticas 104
Clase de gestión de copia de seguridad 106
Acción de copia de seguridad de configuración de dispositivo de red 106
Acción de restauración de configuración de dispositivo de red 107
Clase de gestión de perfiles 108
Acción de alerta de perfil 108
Acción de creación de perfiles 109
Acción de supresión de perfiles 110
Acción de error de perfil 111
Acción de lista de perfiles 112

Acción de modificación de perfiles . . . 113
Acción de notificación de perfil . . . 114
Acción de estado de perfil . . . 115
Acción de advertencia de perfil . . . 116

Capítulo 4: Categoría de seguridad de contenido 119

Clase de prevención de pérdida de datos . . . 119
Acción de inspección de contenido . . . 119
Acción de infracción de políticas . . . 120
Clase de inspección de correo electrónico . . . 121
Acción de análisis de archivo adjunto . . . 121
Acción de pérdida de información confidencial . . . 122
Acción de inspección de correo electrónico . . . 123
Acción de detección de lenguaje irreverente . . . 124
Acción de detección de spam . . . 126
Clase de inspección de mensaje . . . 127
Acción de revisión de mensaje . . . 127
Acción de rechazo de mensaje . . . 128
Clase de acceso de URL . . . 129
Acción de filtrado de URL . . . 129
Acción de redireccionamiento de URL . . . 130
Acción de filtrado de HTTP . . . 131
Acción de filtrado de FTP . . . 132
Acción de inspección de contenido . . . 133

Capítulo 5: Categoría de acceso de datos 135

Clase de gestión de aplicaciones . . . 135
Acción de operación de enlace . . . 135
Acción de creación de contexto . . . 136
Acción de supresión de contexto . . . 137
Acción de creación de funciones . . . 138
Acción de supresión de funciones . . . 139
Acción de modificación de funciones . . . 140
Acción de análisis de índices . . . 141
Acción de vaciado de índices . . . 142
Acción de creación de biblioteca . . . 143
Acción de creación de operadores . . . 144
Acción de supresión de operadores . . . 145

Acción de modificación de operadores 146
Acción de creación de cuerpo del paquete 147
Acción de supresión del cuerpo del paquete 149
Acción de modificación del cuerpo del paquete 150
Acción de creación de paquetes 151
Acción de supresión de paquetes 152
Acción de modificación de paquetes 153
Acción de creación de procedimientos 154
Acción de supresión de procedimientos 155
Acción de modificación de procedimientos 156
Acción de análisis de tabla 157
Acción de truncamiento de tabla 158
Acción de creación de iniciador 159
Acción de supresión de iniciador 160
Acción de desactivación de iniciador 161
Acción de activación de iniciador 162
Acción de modificación del iniciador 163
Acción de creación de cuerpo del tipo 164
Acción de supresión del cuerpo del tipo 165
Acción de modificación del cuerpo del tipo 166
Acción de creación del tipo 167
Acción de supresión del tipo 168
Acción de ejecución del tipo 169
Acción de modificación del tipo 170
Acción de operación de eliminación de enlace 171
Clase de eventos de auditoría 172
Acción de auditoría predeterminada 172
Acción de auditoría no predeterminada 173
Acción de auditoría de objetos 174
Acción de desactivación de auditoría de objetos 175
Acción de grabación de sesión 176
Acción de auditoría del sistema 177
Acción de desactivación de auditoría del sistema 178
Clase de acceso de datos 179
Acción de copia masiva 179
Acción de confirmación 180
Acción de supresión 181
Acción de inserción 182

Acción de ejecución de consulta 183
Acción de reversión 184
Acción de punto de retorno 185
Acción de selección 186
Acción de configuración de transacciones 187
Acción de truncamiento 188
Acción de actualización 189
Clase de gestión de objetos 190
Acción de creación de conjunto 190
Acción de interrupción de conjunto 191
Acción de modificación de conjunto 192
Acción de creación de archivo de control 193
Acción de creación de dimensiones 194
Acción de supresión de dimensiones 195
Acción de modificación de dimensiones 196
Acción de creación de directorios 197
Acción de supresión de directorio 198
Acción de creación de edición 200
Acción de interrupción de edición 201
Acción de modificación de edición 202
Acción de actualización de todos los índices 203
Acción de creación de índices 204
Acción de supresión de índices 205
Acción de modificación de índices 206
Acción de validación de índices 207
Acción de creación de tipo de índice 208
Acción de supresión de tipo de índice 209
Acción de creación de objeto Java 210
Acción de supresión de objeto Java 211
Acción de modificación de objeto Java 212
Acción de bloqueo 213
Acción de creación de vista materializada 214
Acción de supresión de vista materializada 215
Acción de modificación de vista materializada 216
Acción de creación de registro de vista materializada 217
Acción de supresión de registro de vista materializada 218
Acción de modificación de registro de vista materializada 219
Acción de falta de funcionamiento 220

Acción de restauración de objetos 221
Acción de creación de esquema 222
Acción de supresión de esquema 223
Acción de modificación de esquema 224
Acción de creación de sinónimo público 225
Acción de supresión de sinónimo público 226
Acción de modificación de nombre 227
Acción de modificación de costes de recursos 228
Acción de creación de reglas 229
Acción de modificación de regla 230
Acción de supresión de reglas 231
Acción de creación de esquema 232
Acción de creación de secuencias 233
Acción de supresión de secuencias 234
Acción de modificación de secuencias 235
Acción de asociación de estadísticas 236
Acción de desasociación de estadísticas 237
Acción de modificación de resumen 238
Acción de creación de sinónimo 239
Acción de supresión de sinónimo 240
Acción de comprobación de tabla 241
Acción de creación de tabla 242
Acción de supresión de tabla 243
Acción de vaciado de tabla 244
Acción de modificación de tabla 245
Acción de optimización de tabla 246
Acción de purga de tabla 247
Acción de modificación de nombre de tabla 248
Acción de reparación de tabla 249
Acción de desbloqueo de tabla 250
Acción de creación de vista 251
Acción de modificación de vista 252
Acción de supresión de vista 253
Clase de gestión del mismo nivel 254
Acción de creación de vínculo de base de datos 254
Acción de supresión de vínculo de base de datos 255
Clase de gestión de privilegios 256
Acción de supresión de biblioteca 256

Acción de denegación de objeto . . . 257
Acción de concesión de objeto . . . 258
Acción de revocación de objeto . . . 259
Acción de creación de perfiles . . . 260
Acción de supresión de perfiles . . . 261
Acción de modificación de perfiles . . . 262
Acción de revocación de funciones . . . 263
Acción de denegación de instrucciones . . . 264
Acción de concesión de instrucciones . . . 265
Acción de revocación de instrucciones . . . 266
Clase de utilización de aplicaciones y servicios . . . 267
Acción de ejecución de método . . . 267
Acción de ejecución de procedimiento . . . 268
Acción de ejecución de iniciador . . . 269
Clase de actividad del sistema . . . 270
Acción de alerta de base de datos . . . 270
Acción de notificación de base de datos . . . 271
Acción de operación de base de datos . . . 272
Acción de estado de base de datos . . . 273
Acción de advertencia de base de datos . . . 274
Clase de gestión del sistema . . . 275
Acción de análisis de clúster . . . 275
Acción de copia de seguridad de base de datos . . . 276
Acción de alerta de copia de seguridad de base de datos . . . 277
Acción de error de copia de seguridad de base de datos . . . 278
Acción de notificación de copia de seguridad de base de datos . . . 279
Acción de estado de copia de seguridad de base de datos . . . 280
Acción de advertencia de copia de seguridad de base de datos . . . 281
Acción de comprobación de base de datos . . . 282
Acción de creación de clúster . . . 283
Acción de supresión de clúster . . . 284
Acción de desactivación de base de datos . . . 285
Acción de activación de base de datos . . . 286
Acción de modificación de clúster . . . 287
Acción de inicio de duplicación de base de datos . . . 288
Acción de detención de duplicación de base de datos . . . 289
Acción de montaje de base de datos . . . 290
Acción de creación de base de datos . . . 291

Acción de supresión de base de datos . . . 292
Acción Flashback de base de datos . . . 293
Acción de modificación de base de datos . . . 294
Acción de conciliación de base de datos . . . 295
Acción de liberación de base de datos . . . 296
Acción de restauración de base de datos . . . 297
Nuevo tema (19) . . . 298
Acción de suspensión de base de datos . . . 299
Acción de replicación de base de datos . . . 300
Acción de truncamiento de clúster . . . 301
Acción de desmontaje de base de datos . . . 302
Acción de explicación . . . 303
Acción Flashback . . . 304
Acción de creación de archivos Flashback . . . 305
Acción de interrupción de archivos Flashback . . . 306
Acción de modificación de archivos Flashback . . . 307
Acción de purga de la papelera de reciclaje . . . 308
Acción de creación del segmento de reversión . . . 309
Acción de supresión del segmento de reversión . . . 310
Acción de modificación del segmento de reversión . . . 311
Acción de concesión del sistema . . . 312
Acción de modificación del sistema . . . 313
Acción de revocación del sistema . . . 314
Acción de actualización de tablas del sistema . . . 315
Acción Flashback de tabla . . . 316
Acción de creación de espacio de tabla . . . 317
Acción de supresión de espacio de tabla . . . 318
Acción de modificación de espacio de tabla . . . 319
Acción de purga de espacio de tabla . . . 320
Acción de copia de seguridad del registro de transacción . . . 321
Acción de desactivación de todos los iniciadores . . . 322
Acción de activación de todos los iniciadores . . . 323
Acción de ejecución de instrucción de transacción . . . 324

Capítulo 6: Categoría de seguridad de host 325

Clase de actividad de antivirus . . . 325
Acción del estado del antivirus . . . 325
Acción de bloqueo de archivo . . . 326

Acción de exclusión de archivo 327
Acción de supresión de archivos 328
Acción de supresión de archivos 329
Acción de modificación de nombre de archivo 330
Acción de alerta de exploración 331
Acción de omisión de exploración 332
Acción de error de análisis 333
Acción de notificación de exploración 334
Acción de operación de exploración 335
Acción de informe de análisis 336
Acción de estado de exploración 337
Acción de advertencia de exploración 338
Acción de eliminación de virus 339
Acción de virus detectado 340
Acción de actualización de motor de virus 341
Acción de alerta de motor de virus 342
Acción de error de motor de virus 343
Acción de notificación de motor de virus 345
Acción de operación de motor de virus 346
Acción de reversión de motor de virus 347
Acción de estado de motor de virus 348
Acción de advertencia de motor de virus 349
Acción de cuarentena de virus 350
Acción de exploración de virus iniciada 351
Acción de detención de exploración de virus 352
Acción de exploración de virus completada 353
Acción de exploración de virus pausada 354
Acción de exploración de virus reanudada 355
Acción de actualización de firmas de virus 356
Acción de instalación de antivirus 357
Acción de cliente de antivirus eliminado 358
Acción de desinstalación de antivirus 359
Acción de denegación del servicio 361
Acción de ataque de desbordamiento del búfer 361
Acción de ataque de denegación del servicio 362
Clase de seguridad de aplicaciones 363
Acción de ataque de desbordamiento del búfer 363
Acción de ataque de cadena de formato 364

Acción de pérdida de memoria 365
Acción de ataque de XML 366
Clase de actividad de cifrado 367
Acción alerta de cifrado 367
Acción de error de cifrado 368
Acción de notificación de cifrado 369
Acción de operación de cifrado 370
Acción de estado del cifrado 371
Acción de advertencia de cifrado 372
Acción de operación de descifrado 373
Acción de estado del descifrado 374
Acción de alerta de cifrado 375
Acción de error de cifrado 376
Acción de notificación de cifrado 377
Acción de operación de cifrado 378
Acción de inicio de cifrado 379
Acción de advertencia de cifrado 380
Acción de estado de cifrado 381
Acción de adición de clave 382
Acción de alerta de clave 383
Acción de supresión de clave 384
Acción de error de clave 385
Acción de generación de clave 386
Acción de modificación de clave 387
Acción de notificación de clave 388
Acción de operación de clave 389
Acción de uso compartido de clave 390
Acción de estado de clave 391
Acción de advertencia de clave 392
Clase de actividad de infracción de firmas 393
Acción de vulnerabilidad de seguridad de kernel 393
Acción de infracción de firmas 394
Acción de modificación de registro de Windows 395
Acción de actividad de daemon/servicio sospechosa 396
Kernel y actividad del sistema operativo 397
Acción de error de volcado del núcleo 397
Acción de inicio de volcado de memoria 398
Acción de modificación del kernel 399

Acción de notificación de kernel 400
Acción de operación de kernel 401
Acción de estado del kernel 402
Acción de advertencia de kernel 403
Acción de vulnerabilidad de seguridad de Linux 404
Acción de acceso a la memoria 405
Acción de adjudicación de memoria 406
Acción de error de paridad de la memoria 407
Acción de alerta de llamada de sistema 408
Acción de error de llamada de sistema 409
Acción de ejecución de llamada de sistema 410
Acción de notificación de llamada de sistema 412
Acción de operación de llamada de sistema 413
Acción de estado de llamada de sistema 414
Acción de advertencia de llamada de sistema 415
Gestión de notificaciones 417
Difusión de mensajes 417
Clase de actividad de red 418
Paquete de red entrante 418
Paquete de red saliente 419
Acción de alerta de puerto 420
Acción de cierre de puerto 421
Acción de error de puerto 422
Acción de establecimiento de puerto 423
Acción de enumeración de puertos 424
Acción de notificación de puerto 425
Acción de estado de puerto 426
Acción de advertencia de puerto 427
Clase de actividad sospechosa 428
Acción de inserción de código 428
Acción de modificación de código 429
Acción de captura de pulsación 430
Acción alerta de memoria 431
Acción de daño en la memoria 432
Acción de modificación de memoria 433
Acción de pérdida de contraseña 434
Acción de vulnerabilidad de seguridad del servidor 435

Capítulo 7: Categoría de gestión de identidades 437

Clase de gestión de cuentas . . . 437
Acción de creación de cuentas . . . 437
Acción de supresión de cuentas . . . 438
Acción de desactivación de cuentas . . . 439
Acción de activación de cuenta . . . 440
Acción de importación de cuentas . . . 441
Acción de enumeración de cuentas . . . 442
Acción de bloqueo de cuenta . . . 443
Acción de alerta de gestión de cuentas . . . 444
Acción de error de gestión de cuentas . . . 445
Acción de notificación de gestión de cuentas . . . 446
Acción de advertencia de gestión de cuentas . . . 447
Acción de modificación de cuenta . . . 448
Acción de modificación de contraseña de cuenta . . . 449
Acción de restablecimiento de contraseña de cuenta . . . 451
Acción de estado de cuenta . . . 452
Acción de suspensión de cuenta . . . 453
Acción de desbloqueo de cuenta . . . 454
Acción de lista de grupos . . . 455
Acción de infracción de atributos de cuenta de usuario . . . 456
Acción de solicitud de creación de cuenta de usuario . . . 457
Acción de solicitud de modificación de cuenta de usuario . . . 458
Acción de solicitud de validación de cuenta de usuario . . . 459
Clase de actividad de atestación . . . 460
Acción de atestación iniciada . . . 460
Acción de fin de certificación . . . 461
Acción de notificación de certificación . . . 462
Acción de inicio de certificación . . . 463
Acción Certificar usuario . . . 464
Acción de solicitud aprobada . . . 465
Acción de solicitud archivada . . . 466
Acción de solicitud delegada . . . 467
Acción de solicitud transferida . . . 468
Acción de solicitud reasignada . . . 469
Acción de solicitud recibida . . . 470
Acción de solicitud rechazada . . . 471
Acción de solicitud revocada . . . 472

Acción de estado de solicitud 473
Gestión de grupos 475
Acción de habilitación de grupo 475
Acción de creación de grupos 476
Acción de deshabilitación de grupo 477
Acción de supresión de grupos 478
Acción de alerta de gestión de grupos 479
Acción de error de gestión de grupos 480
Acción de notificación de gestión de grupos 481
Acción de advertencia de gestión de grupos 482
Acción de adición de pertenencia a grupo 483
Acción de supresión de pertenencia a grupo 484
Acción de modificación de pertenencia a grupo 485
Acción de modificación de grupos 486
Clase de gestión de identidades 488
Acción de correlación de identidades 488
Acción de creación de identidades 489
Acción de supresión de identidades 490
Acción de desactivación de identidades 491
Acción de activación de identidades 492
Acción de modificación de identidad 493
Acción de modificación de contraseña de identidad 494
Acción de sincronización de identidades 495
Clase de gestión de derechos de usuario 496
Acción de actualización de cuenta 496
Acción de enlace doble de funciones detectado 497
Acción de número excesivo de permisos detectado 498
Acción de número mínimo de permisos detectado 499
Acción de infracción de segregación de tareas 500
Acción de permiso de usuario sospechoso detectado 501
Acción de asignación de derechos de administración de usuario 502
Acción de supresión de derechos de administración de usuario 503
Acción de asignación de permisos de usuario 504
Acción de error de coincidencia de permisos de usuario 505
Acción de solicitud de modificación de permiso de usuario 506
Acción de superposición de permisos de usuario 507
Acción de supresión de permisos de usuario 508
Acción de solicitud de validación de permiso de usuario 510

Acción de infracción de permiso de usuario 511
Acción de asignación de derechos de usuario 512
Acción de creación de derechos de usuario 513
Acción de supresión de derechos de usuario 514
Acción de enumeración de derechos de usuario 515
Acción de modificación de derechos de usuario 516
Acción de notificación de derecho de usuario 517
Acción de superposición de funciones de usuario 518
Clase de gestión de función de usuario 519
Acción de enlace doble de permisos detectado 519
Acción de número excesivo de funciones detectado 520
Acción de jerarquía excesiva de funciones detectada 521
Acción de pertenencia a función excesiva detectada 522
Acción de jerarquía mínima de funciones detectada 523
Acción de pertenencia a función mínima detectada 524
Acción de número mínimo de funciones detectado 525
Acción de solicitud de modificación de función 526
Acción de validación de rol 527
Acción de solicitud de validación de función 528
Acción de infracción de función 529
Acción de infracción de segregación de tareas 530
Acción de asignación de función sospechosa detectada 531
Acción de función sospechosa detectada 532
Acción de permiso de usuario sospechoso detectado 533
Acción de asignación de funciones de administración de usuario 534
Acción de supresión de función de administrador de usuarios 535
Acción de modificación de función de administrador de usuario 536
Acción de supresión de función de administrador de usuarios 537
Acción de asignación de función de usuario 538
Acción de creación de función de usuario 539
Acción de supresión de función de usuario 540
Acción de modificación de función de usuario 541
Acción de superposición de funciones de usuario 542
Acción de supresión de función de usuario 543
Clase de gestión de flujo de trabajo 544
Acción de aprobación de tareas 544

Capítulo 8: Categoría de mensajería 547

Clase de actividad de correo . . . 547
Acción de transferencia de red troncal . . . 547
Acción de transferencia de puerta de enlace . . . 548
Acción de supresión de mensaje . . . 549
Acción de entrega de mensaje . . . 550
Acción de envío de mensajes . . . 551
Acción de redirigimiento de mensajes . . . 552
Acción de liberación de mensaje . . . 553
Acción de desvío de mensaje . . . 554
Acción de transferencia de mensajes . . . 555
Acción de sondeo . . . 556
Acción de supresión de informe . . . 557
Acción de recepción de informe . . . 558
Acción de entrega de SMTP . . . 559
Acción de error de SMTP . . . 560
Acción de notificación de SMTP . . . 561
Acción de SMTP en cola . . . 562
Acción de transferencia de SMTP . . . 563
Acción de advertencia de SMTP . . . 564
Clase de sistema de mensajería . . . 565
Acción de advertencia de mensaje . . . 565

Capítulo 9: Categoría de seguridad de red 567

Clase de control de acceso . . . 567
Acción de bloqueo del puerto . . . 567
Acción de desbloqueo del puerto . . . 568
Acción de infracción de la seguridad del puerto . . . 569
Acción de alerta del límite de la frecuencia . . . 570
Acción de error del límite de la frecuencia . . . 571
Acción de operación de límite de la frecuencia . . . 572
Acción de estado del límite de la frecuencia . . . 573
Acción de advertencia del límite de la frecuencia . . . 574
Acción de bloqueo de conexión . . . 575
Acción de desbloqueo de conexión . . . 576
Acción de bloqueo de host . . . 577
Acción de desbloqueo de host . . . 578
Acción de notificación de acceso a red . . . 579

Acción de bloqueo de red 580
Acción de desbloqueo de red 581
Acción de activación de tasa límite 582
Acción de desactivación de tasa límite 583
Clase de actividad de antivirus 584
Acción de revocación de confianza 584
Clase de seguridad de aplicaciones 585
Acción de ataque de flujo excesivo del búfer 585
Vulnerabilidad de seguridad del servidor de correo 586
Acción de ataque de divulgación de orígenes 587
Acción de explotación de correo electrónico 588
Acción de explotación remota 589
Acción de ejecución de comando especial 590
Acción de explotación de software 591
Acción de actividad de aplicación Web 592
Acción de ataque de aplicación Web 593
Acción de explotación del explorador Web 594
Clase de actividad de certificado 595
Acción de alerta de certificado 595
Acción de exportación de certificado 596
Acción de caducidad de certificado 597
Acción de error de certificado 598
Acción de generación de certificado 599
Acción de operación de certificado 600
Acción de importación de certificado 601
Acción de inicialización de certificado 602
Acción de notificación de certificado 603
Acción de revocación de certificado 604
Acción de alerta de lista de revocación de certificados 605
Acción de error de lista de revocación de certificados 606
Acción de caducidad de lista de revocaciones de certificados 607
Acción de importación de lista de revocaciones de certificados 608
Acción de notificación de lista de revocación de certificados 609
Acción de operación de lista de revocación de certificados 610
Acción de renovación de lista de revocaciones de certificados 611
Acción de estado de lista de revocación de certificados 612
Acción de validación de lista de revocaciones de certificados 613
Acción de advertencia de lista de revocación de certificados 614

Acción de renovación de certificado 615
Acción de solicitud de certificado 616
Acción de revocación de certificado 617
Acción de estado de certificado 618
Acción de suspensión de certificado 619
Acción de cancelación de revocación de certificado 620
Acción de validación de certificado 621
Acción de advertencia de certificado 622
Acción de establecimiento de confianza 623
Clase de actividad de conexión 624
Acción de supresión de certificado 624
Notificación de conexión 625
Acción de fase 1 de la negociación para el intercambio de claves 626
Acción de operación de túnel 627
Acción de alerta de certificado 628
Acción de intento de conexión 629
Acción de restablecimiento de conexión 630
Acción de solicitud de conexión 631
Acción de estado de conexión 632
Acción de finalización de conexión 633
Acción de advertencia de conexión 634
Acción de inicio de fase 1 de intercambio de claves 635
Acción de alerta de protocolo 636
Acción de bloqueo de puerto 637
Acción de error de protocolo 638
Acción de reenvío de puerto 639
Acción de operación de protocolo 640
Acción de estado de protocolo 641
Acción de advertencia de protocolo 642
Acción de notificación de protocolo 643
Acción de caducidad de asociación de seguridad 644
Acción de solicitud de asociación de seguridad 645
Acción de exploración de virus 646
Clase de infracción de política corporativa 648
Acción de sustitución de contenido 648
Acción de contenido ilegal 649
Software sospechoso detectado 650
Uso de acción de programas de chat 651

Uso de acción de cliente P2P 652
Uso de acción de tecnologías multimedia de transmisión 653
Denegación de clase de servicio 654
Acción de explotación de aplicaciones 654
Acción de ataque de agotamiento de ancho de banda 655
Acción de flujo excesivo del búfer 656
Acción de explotación de base de datos 657
Acción de ataque distribuido 658
Acción de explotación de firmware 659
Acción de ataque de fragmentación 660
Acción de ataque de paquete mal formado 661
Acción de ataque de conectividad de red 662
Acción de explotación del SO 663
Acción de explotación de protocolo 664
Acción de ataque de agotamiento de recursos 665
Acción de explotación de software 666
Acción de explotación de servidor Web 668
Acción de ataque en dispositivos inalámbricos 669
Clase de actividad de cifrado 670
Acción alerta de cifrado 670
Acción de error de cifrado 671
Acción de notificación de cifrado 672
Acción de operación de cifrado 673
Acción de estado del cifrado 674
Acción de advertencia de cifrado 675
Acción de operación de descifrado 676
Acción de estado del descifrado 677
Generación de claves 678
Acción de creación de firma digital 679
Acción de alerta de cifrado 680
Acción de error de cifrado 681
Acción de notificación de cifrado 682
Acción de operación de cifrado 683
Acción de estado de cifrado 684
Acción de advertencia de cifrado 685
Clase de pérdida de información 686
Descodificación de una acción de consulta de RPC 686
Acción de ataque de inserción de SQL 687

Acción de uso incorrecto de acceso legítimo 688
Acción de actividad de reconocimiento 689
Acción de actividad de programas de puerta trasera y troyanos 690
Acción de análisis de vulnerabilidades 691
Clase de actividad de software maligno 692
Acción de actividad de programas de puerta trasera y troyanos 692
Acción de software espía detectado 693
Acción de gusano detectado 694
Acción de actividad de programas de puerta trasera y troyanos 695
Acción de clase de gestión de direcciones de red 696
Acción de creación de grupo de multidifusión 696
Acción de supresión de grupo de multidifusión 697
Acción de modificación de grupo de multidifusión 697
Clase de escalación de privilegios 699
Acción de obtención de privilegios de administrador 699
Acción de actividad de omisión de control 700
Acción de obtención de privilegios de usuario 701
Acción de clase de la actividad de enrutamiento 702
Acción de configuración del enrutamiento 702
Clase de infracción de firmas 703
Acción de infracción de firmas 703
Clase de actividad sospechosa 704
Detección de una acción de protocolo no estándar 704
Detección de una acción de puerto inusual 705
Acción detectada de código ejecutable 706
Acción de ataques varios 707
Acción de ataque del servicio de nombres 708
Acción de enumeración de red 709
Acción de vulnerabilidad de seguridad de la red 710
Acción de ataque de puerto 711
Acción de vulnerabilidad de la seguridad de las URL 712
Acción de ataque de VoIP 713
Acción de exploración de ping 715
Acción de exploración de puertos 716
Actividad de posible ataque de fuerza bruta 717
Acción de explotación de protocolo 718
Acción de comando sospechoso detectado 719
Acción detectada de nombre de archivo sospechoso 720

Acción de cadena sospechosa detectada 721
Acción de inicio de sesión sospechoso detectado 722
Acción de tráfico de túnel detectado 723
Acción de tráfico no solicitado 724
Acción de explotación de servidor Web 725
Clase de gestión de servicios Web 726
Acción de procesamiento de filtro del mensaje 726
Acción de procesamiento de filtro del mensaje 727
Acción de modificación de mensaje SOAP 728
Acción de descifrado XML 729
Acción de cifrado XML 730
Acción de validación de esquema XML 731

Capítulo 10: Categoría de seguridad operacional 733

Clase de gestión de aplicaciones 733
Acción de cierre de la aplicación 733
Acción de error de aplicaciones 734
Clase de gestión del rendimiento de la aplicación 735
Acción de métrica de la conexión 735
Acción de métrica de la agrupación de conexiones 736
Acción de métrica del componente 737
Acción de métrica de la CPU 738
Acción de métrica del rendimiento de datos 739
Acción de métrica del evento 740
Acción de métrica de la memoria 741
Acción de métrica de la mensajería 742
Acción de métrica del método 743
Acción de métrica del programa 744
Acción de métrica del socket 745
Acción de métrica del grupo de subprocesos 746
Clase de gestión de copia de seguridad 747
Acción de creación de registro de auditoría 747
Acción de alerta de copia de seguridad 748
Acción de finalización de copia de seguridad 749
Acción de configuración de copia de seguridad 750
Acción de inicio de copia de seguridad 751
Acción de instantánea de datos 752
Acción de copia de seguridad de archivo 753

Acción de restauración de archivo 754
Acción de copia de seguridad de imagen 755
Acción de restauración de imagen 756
Acción de error de proceso 757
Acción de inicio de restauración 758
Acción de completado de restauración 759
Acción de operación de reversión 760
Clase de gestión del dominio 761
Acción de alerta del controlador de dominio 761
Acción de error del controlador de dominio 762
Acción de notificación del controlador de dominio 763
Acción de operación del controlador de dominio 764
Acción de estado del controlador de dominio 765
Acción de advertencia del controlador de dominio 766
Acción de modificación de la confianza 767
Clase de actividad de proceso 768
Acción de error de copia de seguridad 768
Acción de notificación de copia de seguridad 769
Acción de advertencia de copia de seguridad 770
Acción de simulación de política 771
Acción de operación de impresión 772
Acción de creación de proceso 773
Acción de supresión de proceso 774
Acción de modificación de proceso 775
Acción de notificación de proceso 776
Acción de operación de proceso 777
Acción de restauración de proceso 778
Acción de inicio de proceso 779
Acción de detención del proceso 780
Acción de suspensión de proceso 781
Acción de advertencia de proceso 782
Acción de advertencia de sistema 783
Clase de actividad de conexión 784
Acción de notificación de registro de seguridad 784
Acción de bloqueo de terminal 785
Acción de desbloqueo de terminal 786
Clase de actividad de puerto y dispositivo 787
Acción de alerta de dispositivo 787

Acción de conexión de dispositivo 788
Acción de creación de dispositivo 789
Acción de eliminación de dispositivo 790
Acción de modificación de dispositivo 791
Acción de notificación de dispositivo 792
Acción de operación de dispositivo 794
Acción de advertencia de dispositivo 795
Acción de desconexión de dispositivo 796
Acción de error de dispositivo 797
Acción de montaje de dispositivo 798
Acción de pausa de dispositivo 799
Acción de restablecimiento del dispositivo 800
Acción de reanudación de dispositivo 801
Acción de cambio del estado del dispositivo 802
Acción de desmontaje de dispositivo 804
Acción de estado de dispositivo 805
Acción de conexión de HID (dispositivo de interfaz humana) 806
Acción de desconexión de HID (dispositivo de interfaz humana) 807
Acción de error de dirección MAC 808
Acción de inicialización de proceso 809
Acción de conexión de dispositivo de almacenamiento 810
Acción de desconexión de dispositivo de almacenamiento 811
Acción de advertencia de sistema 812
Clase de gestión de infraestructuras 814
Acción de advertencia de agente 814
Acción de conflicto de direcciones 815
Acción de métrica del agente 816
Acción de restablecimiento del agente 817
Acción de métrica del gestor 818
Acción de alerta de denominación 819
Acción de notificación de denominación 820
Acción de advertencia de denominación 821
Acción de alerta de agente 823
Acción de desactivación de agente 824
Acción de activación de agente 825
Acción de error de agente 826
Acción de modificación de agente 827
Acción de notificación de agente 829

Acción de operación de agente 830
Acción de inicio de agente 831
Acción de detención de agente 832
Acción de finalización de agente 833
Acción de asignación de alarma 834
Acción de creación de alarma 835
Acción de supresión de alarma 837
Acción de retractación de alarma 838
Acción de estado de alarma 839
Acción de actualización de alarma 840
Acción de alerta de API 841
Acción de error de API 843
Acción de notificación de API 844
Acción de operación de API 845
Acción de estado de API 846
Acción de advertencia de API 847
Acción de alerta de aplicación 849
Acción de inicialización de aplicación 850
Acción de operación de aplicación 851
Acción de estado de aplicación 852
Acción de carga masiva de datos 853
Acción de notificación de cola de registro 854
Acción de advertencia de cola de registro 855
Acción de estado de modelo 857
Acción de cambio de estado de objeto 858
Acción de estado crítico de objeto 859
Acción de estado normal de objeto 860
Acción de estado de objeto sin conexión 861
Acción de advertencia de estado de objeto 862
Acción de error de coincidencia del software 863
Acción de adición de sistema 864
Acción de detección de sistema 865
Acción de umbral excedido 866
Clase de gestión de redes 867
Acción de alerta de red 867
Acción de creación de red 868
Acción de supresión de red 869
Acción de error de red 870

Acción de modificación de red 871
Acción de notificación de red 872
Acción de estado de red 873
Acción de advertencia de red 875
Acción de alerta de SNMP 876
Acción de error de SNMP 877
Acción de notificación de SNMP 878
Acción de operación de SNMP 879
Acción de estado de SNMP 880
Acción de advertencia de SNMP 882
Acción de creación de VLAN 883
Acción de supresión de VLAN 884
Acción de modificación de VLAN 885
Clase de actividad de proceso 886
Acción de alerta de proceso 886
Acción de proceso desactivado 887
Acción de reanudación de proceso 888
Acción de estado de proceso 889
Acción de iniciación de tarea 890
Clase de actividad de registro de seguridad 892
Acción de configuración de registro 892
Acción de ejecución de política 893
Acción de acceso al registro de seguridad 894
Acción de alerta de registro de seguridad 895
Acción de supresión de registro de seguridad 896
Acción de error de registro de seguridad 897
Acción de supresión de registro de seguridad 898
Acción de advertencia de registro de seguridad 899
Acción de configuración de auditoría del sistema 900
Acción de desactivación de auditoría del sistema 901
Acción de activación de auditoría del sistema 902
Acción de ejecución de tarea 903
Clase de gestión del nivel de servicio 904
Acción de degradación moderada del servicio 904
Acción de alerta de servicio 905
Acción de servicio desactivado 906
Acción de error de servicio 907
Acción de notificación de servicio 908

Acción de operación de servicio 909
Acción de estado de servicio 910
Acción de servicio no disponible. 912
Acción de advertencia de servicio 913
Acción de degradación grave del servicio 914
Acción de alerta de SLA 915
Acción de error de SLA 916
Acción de notificación de SLA 917
Acción de operación de SLA 918
Acción de estado de SLA 919
Acción de advertencia de SLA 921
Acción de degradación ligera del servicio 922
Clase de actividad del sistema 923
Acción de alerta de firmware 923
Acción de error de firmware 924
Acción de notificación de firmware 925
Acción de estado de firmware 926
Acción de advertencia de firmware 927
Acción de alerta de hardware 928
Acción de notificación de hardware 929
Acción de operación de hardware 931
Acción de estado de hardware 932
Acción de advertencia de hardware 933
Acción de actividad de registro 934
Acción de alerta de registro 935
Acción de supresión de registros 936
Acción de error de registro 937
Acción de notificación de registro 938
Acción de inicio de registro 939
Acción de detención de registro 940
Acción de advertencia de registro 941
Acción de supresión de inconvenientes. 942
Acción de servicio no disponible 943
Acción de alerta de sistema 944
Acción de alerta de entorno de sistema 945
Acción de error del sistema 946
Acción de inicialización de sistema 947
Acción de conmutación de sistema 948

Acción de notificación del sistema 949
Acción de pausa del sistema 950
Acción de restablecimiento de sistema 951
Acción de alerta de recurso de sistema 952
Acción de error de recurso de sistema 953
Acción de advertencia de recurso de sistema 954
Acción de reinicio del sistema 955
Acción de reanudación del sistema 956
Acción de guardado de sistema 957
Acción de cierre del sistema 958
Acción de inicio del sistema 959
Acción de estado del sistema 960
Acción de sistema no disponible 961
Acción de advertencia de sistema 962
Acción de alerta de confianza 963
Acción de error de confianza 964
Acción de notificación de confianza 965
Acción de operación de confianza 966
Acción de estado de confianza 967
Acción de advertencia de confianza 968
Clase de gestión del sistema 969
Acción de error de licencia 969
Acción de caducidad de licencia 970
Acción de notificación de licencia 971
Acción de operación de licencia 972
Acción de infracción de licencia 973
Acción de advertencia de licencia 974
Acción de instalación de servicio 975
Acción de desinstalación del servicio 976
Acción de instalación de software 977
Acción de falta de software 978
Acción de actualización de software 979
Acción de desinstalación de software 981
Clase de actividad de virtualización 982
Acción de alerta de dispositivo 982
Acción de creación de dispositivo 983
Acción de eliminación de dispositivo 984
Acción de error de dispositivo 985

Acción de importación de dispositivo 987
Acción de notificación de dispositivo 988
Acción de operación de dispositivo 989
Acción de estado de dispositivo 990
Acción de advertencia de dispositivo 991
Acción de alerta de hipervisor 993
Acción de error de hipervisor 994
Acción de notificación de hipervisor 995
Acción de operación de hipervisor 996
Acción de inicio de hipervisor 997
Acción de estado de hipervisor 998
Acción de advertencia de hipervisor 999
Acción de alerta de imagen 1001
Acción de clonación de imagen 1002
Acción de error de imagen 1003
Acción de exportación de imagen 1004
Acción de modificación de imagen 1005
Acción de notificación de imagen 1007
Acción de migración de imagen 1008
Acción de apertura de imagen 1009
Acción de operación de imagen 1010
Acción de restauración de imagen 1011
Acción de estado de imagen 1013
Acción de advertencia de imagen 1014
Acción de escritura de imagen 1015
Acción de creación de puerto 1016
Acción de eliminación de puerto 1017
Acción de creación de agrupación de recursos 1018
Acción de supresión de agrupación de recursos 1019
Acción de modificación de agrupación de recursos 1020
Acción de alerta de instantánea 1022
Acción de error de instantánea 1023
Acción de advertencia de instantánea 1024
Acción de creación de sistema 1025
Acción de eliminación de sistema 1026
Acción de exportación de sistema 1027
Acción de importación de sistema 1028
Acción de instantánea de sistema 1029

Clase de gestión de virtualización 1030
Acción de creación de aplicación 1030
Acción de modificación de aplicación 1032
Acción de notificación de aplicación 1033
Acción de supresión de aplicación 1034
Acción de creación de componente 1035
Acción de supresión de componente 1036
Acción de modificación de componente 1037
Acción de notificación de componente 1038
Acción de activación de sistema 1039
Acción de adición de sistema 1040
Acción de conexión de sistema 1041
Acción de desconexión de sistema 1042
Acción de detección de sistema 1043
Acción de modificación del sistema 1045
Acción de eliminación de sistema 1046

Capítulo 11: Categoría de acceso físico 1047

Clase de actividad de acceso físico 1047
Acción de análisis de identificador 1047
Acción de desactivación de cámara 1048
Acción de activación de cámara 1049
Acción de falta de disponibilidad de la cámara 1050
Acción de cierre de puerta 1051
Acción de apertura de puerta 1052
Acción de cierre de ventana 1053
Acción de apertura de ventana 1054

Capítulo 12: Categoría de acceso a recursos 1057

Clase de actividad de aplicación 1057
Acción de acceso a aplicación 1057
Acción de acceso a objeto 1058
Clase de actividad de directorio 1059
Acción de alerta de directorio 1059
Acción de error de directorio 1061
Acción de notificación de directorio 1062
Acción de operación de directorio 1063
Acción de estado de directorio 1064

Acción de advertencia de directorio 1066
Clase de actividad de recursos 1067
Acción de acceso a recursos 1067
Acción de alerta de recurso 1068
Acción de ubicación de recursos 1069
Acción de cierre de recurso 1070
Acción de copia de recurso 1071
Acción de creación de recurso 1072
Acción de supresión de recurso 1073
Acción de error de recurso 1074
Acción de ejecución de recurso 1075
Acción de retención de recurso 1076
Acción de importación de recursos 1077
Acción de enumeración de recursos 1078
Acción de recurso marcado 1079
Acción de modificación de recurso 1080
Acción de movimiento de recurso 1081
Acción de apertura de recurso 1082
Acción de actualización de recurso 1083
Acción de replicación de recurso 1084
Acción de búsqueda de recursos 1085
Acción de estado de recurso 1087
Acción de advertencia de recurso 1088
Acción de definición de ACL 1089
Acción de configuración de criterios de búsqueda 1090
Clase de control de versión 1091
Acción de protección de recurso 1091
Acción de desprotección de recurso 1092
Acción de creación de recurso 1093
Acción de modificación de etiqueta de recurso 1094
Acción de combinación de recursos 1095
Acción de búsqueda de recursos 1096
Acción de cancelación de desprotección de recurso 1097
Acción de actualización de recurso 1098
Acción de estado de versión 1099

Capítulo 13: Categoría de operaciones SIM 1101

Clase de gestión de alerta 1101

Acción de confirmación de alerta 1101
Acción de anotación de alerta 1102
Acción de creación de alerta 1103
Acción de supresión de alerta 1104
Acción de entrega de alerta 1105
Acción de escalación de alerta 1106
Acción de modificación de tarea de alerta 1107
Acción de supresión de tarea de alerta 1108
Acción de configuración de tarea de alerta 1109
Acción de modificación de alerta 1110
Clase de gestión de línea de base 1111
Acción de aceptación de línea de base 1111
Acción de activación de línea de base 1112
Acción de creación de línea de base 1113
Acción de desactivación de línea de base 1114
Acción de establecimiento de línea de base 1115
Acción de modificación de línea de base 1116
Clase de gestión de origen de evento 1117
Acción de autorización de origen de evento 1117
Acción de configuración de origen de evento 1118
Acción de descubrimiento de origen de evento 1119
Acción de provisión de origen de evento 1120
Acción de tendencia de evento 1121
Acción de entrada de datos externos 1123
Acción de salida de datos externos 1124
Clase de gestión de incidente 1125
Acción de cierre de incidente 1125
Acción de creación de incidente 1126
Acción de supresión de incidente 1127
Acción de modificación de incidente 1128
Acción de resolución de incidente 1129
Clase de gestión de investigación 1130
Acción de anotación de investigación 1130
Acción de cierre de investigación 1131
Acción de supresión de investigación 1132
Acción de modificación de investigación 1133
Acción de apertura de investigación 1134
Acción de pausa de investigación 1135

Acción de resolución de investigación . . . 1136
Acción de reanudación de investigación . . . 1137
Clase de gestión de notificaciones . . . 1138
Acción de creación de notificación . . . 1138
Acción de entrega de notificación . . . 1139
Clase de gestión de solicitud . . . 1140
Acción de confirmación de solicitud . . . 1140
Acción de anotación de solicitud . . . 1141
Acción de cierre de solicitud . . . 1142
Acción de creación de solicitud . . . 1143
Acción de entrega de solicitud . . . 1144
Acción de modificación de solicitud . . . 1145

Capítulo 14: Categoría de acceso al sistema 1147

Clase de gestión de accesos . . . 1147
Acción de creación de dominio de seguridad . . . 1147
Acción de supresión de dominio de seguridad . . . 1148
Acción de modificación de dominio de seguridad . . . 1150
Acción de modificación de etiqueta de seguridad . . . 1151
Clase de actividad de autenticación . . . 1152
Acción de autenticación . . . 1152
Acción de desactivación de autenticación . . . 1153
Acción de activación de autenticación . . . 1154
Acción de error de autenticación . . . 1155
Acción de retroceso de autenticación . . . 1156
Acción de notificación de autenticación . . . 1157
Acción de carga de paquete de autenticación . . . 1158
Acción de inicio de autenticación . . . 1159
Acción de advertencia de autenticación . . . 1160
Acción de autorización . . . 1161
Acción de creación de territorio de seguridad . . . 1163
Acción de supresión de territorio de seguridad . . . 1164
Acción de definición de propiedad de grupo . . . 1165
Acción de alerta de territorio de confianza . . . 1166
Acción de error de territorio de confianza . . . 1167
Acción de advertencia de territorio de confianza . . . 1168
Clase de actividad de autorización . . . 1169
Acción de alerta de autorización . . . 1169

Acción de error de autorización 1170
Acción de notificación de autorización 1171
Acción de estado de autorización 1172
Acción de advertencia de autorización 1174
Acción de finalización de autorización 1175
Acción de caducidad de token de autorización 1176
Acción de alerta de permiso 1177
Acción de error de permiso 1178
Acción de advertencia de permiso 1179
Clase de actividad de inicio de sesión 1180
Acción de intento de inicio de sesión 1180
Clase de actividad de cierre de sesión 1182
Acción de cierre de sesión 1182
Clase de obtención de privilegios 1183
Acción de obtención de privilegios 1183
Clase de uso de privilegios 1184
Acción de utilización de privilegios 1184
Clase de actividad de sesión 1185
Acción alerta de sesión 1185
Acción de creación de sesión 1186
Acción de desconexión de sesión 1187
Acción de error de sesión 1188
Acción de modificación de sesión 1189
Acción de notificación de sesión 1190
Acción de operación de sesión 1191
Actividad de reconexión de la sesión 1193
Acción de estado de sesión 1194
Acción de advertencia de sesión 1195
Acción de validación de sesión 1196
Clase de actividad de configuración de usuario 1197
Acción de alerta de autenticación 1197
Acción de configuración de usuario 1198
Clase de actividad del sistema 1199
Acción de activación de sistema 1199

Capítulo 15: Categoría desconocida 1201

Clase desconocida 1201
Acción de acción desconocida 1201

Capítulo 16: Categoría de gestión de vulnerabilidades 1203

Clase de evaluación de vulnerabilidades 1203
Acción de recopilación de información 1203
Acción de detección de servicios 1204
Acción de descubrimiento de grupo y usuario 1205
Acción de análisis de vulnerabilidades iniciado 1206
Acción de análisis de vulnerabilidades completado 1207
Clase de descubrimiento de vulnerabilidades 1208
Acción de vulnerabilidad de punto de acceso 1208
Acción de vulnerabilidad de cuenta 1209
Acción de vulnerabilidad de antivirus 1211
Acción de vulnerabilidad de protocolo de aplicación 1212
Acción de vulnerabilidad de aplicación 1213
Acción de vulnerabilidad de programas de puerta trasera 1214
Acción de vulnerabilidad del búfer 1215
Acción de vulnerabilidad de interfaz CGI 1216
Acción de vulnerabilidad de CISCO 1217
Acción de vulnerabilidad de ejecución de comando 1218
Acción de vulnerabilidad de conformidad 1219
Acción de vulnerabilidad de configuración 1220
Acción de vulnerabilidad de credencial 1221
Acción de vulnerabilidad de cifrado 1222
Acción de vulnerabilidad de base de datos 1223
Acción de vulnerabilidad de denegación de servicio 1224
Acción de vulnerabilidad de archivo compartido 1225
Acción de vulnerabilidad de cortafuegos 1226
Acción de vulnerabilidad de pérdida de información 1227
Acción de vulnerabilidad de cliente de correo 1228
Acción de vulnerabilidad de servidor de correo 1229
Acción de vulnerabilidad de Microsoft 1230
Acción de vulnerabilidad de protocolo de red 1231
Acción de vulnerabilidad de OS 1232
Acción de vulnerabilidad del explorador de puerto 1233
Acción de vulnerabilidad de extensión de privilegios 1234
Acción de vulnerabilidad de explotación remota 1235
Acción de vulnerabilidad de SCADA 1236
Acción de vulnerabilidad de servicio/daemon 1237
Acción de vulnerabilidad de SMTP 1238

Acción de vulnerabilidad de software 1239
Acción de vulnerabilidad de inyección de código SQL 1240
Acción de vulnerabilidad de UNIX 1241
Acción de vulnerabilidad de enumeración de usuario 1242
Acción de vulnerabilidad de explorador Web 1243
Acción de vulnerabilidad de servidor Web 1245
Acción de vulnerabilidad de Windows 1246
Acción de vulnerabilidad de filtro XSS 1247
Clase de gestión de vulnerabilidades 1248
Acción de vulnerabilidad encontrada 1248

Capítulo 17: Preguntas frecuentes (FAQ) 1251

Diferencia entre las acciones Desactivación de cuentas, Suspensión de cuentas y Bloqueo de cuentas 1252
Diferencia entre los términos Cuenta, Identidad y Usuario 1253

Apéndice A: Asignación de nivel de seguridad 1255

Tabla de asignación de nivel de seguridad 1255

Capítulo 1: ¿Qué es la Gramática de eventos comunes?

La Gramática de eventos comunes de CA es una gramática utilizada para expresar la información del evento después de que se recopile. Proporciona los medios para normalizar los datos de eventos sin formato recopilados de orígenes de registro y los expresa en un formato común para conseguir una compresión y visualización sencillas. Los campos de datos en un evento de registro se convierten en una representación de datos independiente y se categorizan de forma coherente. La Gramática de eventos comunes utiliza un conjunto estándar de campos para expresar la información del evento. La lista de campos se divide en siete áreas que proporcionan información descriptiva acerca de las entidades en el evento.

Esta sección contiene los siguientes temas:

Siete áreas de un evento (en la página 40)
Tipos de eventos (en la página 47)
Identificación del tipo de evento (en la página 50)

Siete áreas de un evento

Cuando se produce un evento hay varios tipos de información expresada como parte del evento. Esta información puede describir una entidad o el evento en sí mismo.

Actor - Origen

Identifica la entidad que inicia la acción que provoca el evento.

Actor - Destino

Identifica la entidad que es el destino de la acción que provoca el evento.

Origen de evento

Identifica la entidad que ha registrado el evento original.

Observador (Agente SIM)

Registra el evento y recoge una copia del evento original del origen de evento.

Repositorio de eventos

Identifica el almacenamiento temporal del evento hasta que el agente lo registra.

Evento específico

Contiene datos como el ID de evento, el modelo ideal, la categoría de eventos, etc.

Resultado específico

Contiene los datos como el resultado y la severidad del evento.

Actor - Origen

Nombre de campo	Descripción
source_username	El nombre de usuario o identidad que inició la acción que se expresa en la información del evento.
source_domainname	El dominio de autenticación del nombre de usuario o identidad que se expresa en el campo source_username.
source_groupname	El nombre del grupo que se expresa en la información del evento.

Nombre de campo	Descripción
source_uid	El número de identificación del nombre de usuario o identidad que se expresa en el campo source_username.
source_gid	El número de identificación del grupo que se expresa en el campo source_groupname.
source_hostname	El nombre (FQDN o nombre corto) del host desde el que se ha iniciado la acción que se expresa en la información del evento. Si Source_hostname está vacío, este valor se establecerá en Source_address en los archivos DM y XMP.
source_hostdomainname	El nombre de dominio del host que se expresa en el campo source_hostname.
source_address	La dirección IP (u otro protocolo) del host que se expresa en el campo source_hostname.
source_mac_address	La dirección de MAC del host que se expresa en el campo source_hostname.
source_port	El puerto de comunicación utilizado para iniciar la acción que se expresa en la información del evento.
source_processname	El nombre del proceso o archivo ejecutable que inició la acción que se expresa en la información del evento.
source_objectname	El nombre del objeto implicado en la acción que se expresa en la información del evento.
source_objectattr	El nombre del atributo del objeto que se expresa en la información del evento.
source_objectid	El número de identificación del objeto que se expresa en el campo source_objectname.
source_objectclass	La clase del objeto que se expresa en el campo source_objectname.
source_objectvalue	El valor del objeto que se expresa en el campo source_objectname.

Actor - Destino

Nombre de campo	Descripción
dest_username	El nombre de usuario o identidad que inició la acción que se expresa en la información del evento.
dest_domainname	El dominio de autenticación del nombre de usuario o identidad expresado en el campo des_username.
dest_groupname	El nombre del grupo que se expresa en la información del evento.
dest_uid	El número de identificación del nombre de usuario o identidad expresado en el campo dest_username.
dest_gid	El número de identificación del grupo expresado en el campo dest_groupname.
dest_hostname	El nombre (FQDN o nombre corto) del host en el que se ha destinado la acción expresada en la información del evento. Si Dest_hostname está vacío, este valor se establecerá en Dest_address en los archivos DM y XMP.
dest_hostdomainname	El nombre de dominio del host expresado en el campo dest_hostname.
dest_address	La dirección IP (u otro protocolo) del host expresado en el campo dest_hostname.
dest_mac_address	La dirección de MAC del host expresada en el campo dest_hostname.
dest_port	El puerto de comunicación utilizado para iniciar la acción que se expresa en la información del evento.
dest_processname	El nombre del proceso o archivo ejecutable que inició la acción que se expresa en la información del evento.
dest_objectname	El nombre del objeto implicado en la acción que se expresa en la información del evento.

Nombre de campo	Descripción
dest_objectattr	El nombre del atributo del objeto que se expresa en la información del evento.
dest_objectid	El número de identificación del objeto expresado en el campo dest_objectname.
dest_objectclass	La clase del objeto expresada en el campo dest_objectname.
dest_objectvalue	El valor del objeto expresado en el campo dest_objectname.

Origen de evento

Nombre de campo	Descripción
event_source_hostname	El nombre (FQDN o nombre corto) del host en el que se ha expresado originalmente la información del evento. Si event_source_hostname está vacío, este valor se establecerá en Event_source_address en los archivos DM y XMP.
event_source_hostdomainname	El nombre de dominio del host expresado en el campo event_source_hostname.
event_source_address	La dirección IP (u otro protocolo) del host expresado en el campo event_source_hostname.
event_source_processname	El nombre del proceso que expresó originalmente la información del evento.

Observador - Agente

Nombre de campo	Descripción
agent_name	El nombre del agente SIM que registra la información del evento.
agent_address	La dirección IP (u otro protocolo) del host expresado en el campo agent_hostname.

Nombre de campo	Descripción
agent_hostname	El nombre (FQDN o nombre corto) del host en el que se está ejecutando el agente expresado en el campo agent_name. Si Agent _hostname está vacío, este valor se establecerá en Agent _address en los archivos DM y XMP.
agent_hostdomainname	El nombre de dominio del host expresado en el campo agent_hostname.
agent_version	La versión del agente expresada en el campo agent_name.
agent_id	El número de identificación del agente expresado en el campo agent_name.
agent_group	El nombre de grupo del agente que ha recopilado este evento.
agent_connector_name	El nombre del conector en el agente que ha recopilado este evento.

Repositorio de eventos

Nombre de campo	Descripción
receiver_name	El nombre del módulo del receptor que ha recibido la información del evento.
receiver_hostname	El nombre (FQDN o nombre corto) del host en el que se ha recibido la información del evento.
receiver_hostaddress	La dirección IP (u otro protocolo) del host expresado en el campo receiver_hostname.
receiver_hostaddress	La dirección IP (u otro protocolo) del host expresado en el campo receiver_hostname.
receiver_hostdomainname	El nombre de dominio del host expresado en el campo receiver_hostname.
receiver_por	El puerto de comunicación para el receptor expresado en el campo receiver_name.
receiver_time_gmt	La hora (en GMT) en la que se ha recibido el evento.

Nombre de campo	Descripción
receiver_timezone	La zona horaria del host expresada en el campo receiver_hostname.
receiver_version	La versión del receptor expresada en el campo receiver_name.

Evento específico

Nombre de campo	Descripción
event_protocol	El nombre del protocolo o ID del protocolo expresado en la información del evento.
event_logname	El nombre del registro expresado en la información del evento.
event_euuid	El identificador único para esta instancia de la acción expresada en la información del evento.
event_count	El recuento (entero) de veces que se ha producido este evento durante el tiempo expresado en el campo event_duration.
event_summarized	Un indicador (T/F) que especifica si se ha resumido la información del evento expresada.
event_duration	La duración del tiempo transcurrido desde el valor expresado en el campo event_time_gmt.
event_time_gmt	La fecha y hora expresadas en la información del evento. Para los eventos resumidos, este campo contiene la hora de inicio expresada en la información del evento. El campo se debe expresar en hora GMT.
event_timezone	La zona horaria de la información expresada en el evento.
event_sequence	El nombre de la secuencia iniciada que provocó la acción expresada en el campo event_action. Es el segundo nivel de agrupación disponible en la Gramática de eventos comunes.
event_trend	Los datos a los que se tenderá más adelante o gráficos usados actualmente.

Nombre de campo	Descripción
event_action	El nombre de la acción expresada en la información del evento. Es el cuarto nivel de normalización disponible en la Gramática de eventos comunes.
event_id	El número de identificación nativa para la información expresada del evento. Este campo normalmente lo proporciona el proveedor.
event_category	El nombre de la categoría de eventos que se expresa en la información del evento. Es el segundo nivel de normalización disponible en la Gramática de eventos comunes.
event_class	El nombre de la clase de evento expresada en la información del evento. Las posibilidades disponibles para la información acerca de la clase de evento se determinan mediante la categoría del evento expresada. Es el tercer nivel de normalización disponible en la Gramática de eventos comunes.
ideal_model	El nombre de la clase de tecnología expresada en la información del evento. Es el primer nivel de normalización disponible en la Gramática de eventos comunes.
event_severity	Un entero que representa una severidad para el evento tal y como está normalizado por CA.

Especificación de resultado

Nombre de campo	Descripción
event_result	El valor de resultado de la información del evento expresada. Normalmente se configura como “S” (del inglés success, correcto) cuando es correcto o como “F” (del inglés failure, incorrecto) cuando es erróneo. En algunas instancias hay otras opciones que se proporcionan (aceptado, interrumpido, rechazado) para este campo.

Nombre de campo	Descripción
result_string	Una cadena descriptiva que describe qué acción se expresa en este evento. Este campo a veces lo proporciona el proveedor.
result_signature	La firma es el nombre del virus o nombre de la firma de IDS coincidente. Para otros tipos de eventos que no utilizan coincidencias basadas en firma, este campo puede dejarse en blanco.
result_code	El código de retorno expresado en la información del evento. Este campo se rellena normalmente en los eventos erróneos.
result_version	La versión de la firma expresada en el campo result_signature.
result_priority	La prioridad de la información del evento expresada.
result_scope	El alcance de la información del evento expresada.
result_severity	La severidad de la información expresada del evento.

Tipos de eventos

El tipo de evento determina cómo se rellenan las secciones de información. Existen cuatro tipos de eventos que considera la Gramática de elementos comunes. Cada tipo de evento representa una perspectiva de la acción expresada en el evento. Un origen de evento normalmente registrará un evento de acuerdo a una de las perspectivas descritas en esta sección.

Tipo 1: evento local

El primer tipo de evento es el evento local. Este tipo de evento cuenta con una perspectiva local que afecta a una única entidad. Esta entidad representa el origen, destino, origen de evento y agente expresado en el evento. Los eventos de tipo 1 contienen normalmente información expresada en el evento y la información proporcionada debe duplicarse para expresarla correctamente en el formato de la Gramática de eventos comunes.

Un ejemplo de este evento es un inicio de sesión a través de la consola registrado en el mismo host con un agente instalado localmente.

Origen	Destino	Origen de evento	Agente
Host A	Host A	Host A	Host A

Tipo 2: evento remoto

El segundo tipo de evento es el evento remoto. Este tipo de evento afecta a dos entidades en la que una de ellas es el origen o el destino de la acción expresada en el evento. Esto significa que el agente y el origen de evento son la misma entidad que el origen o el destino de la acción expresada en el evento.

Un ejemplo d este tipo de evento es un evento de inicio de sesión que expresa una conexión a un recurso compartido de red de una estación de trabajo. El agente se instala en el servidor y aloja al recurso compartido de red.

Origen	Destino	Origen de evento	Agente
Host A	Host B	Host A	Host A
Host A	Host B	Host B	Host B

Tipo 3: evento observado

El tercer tipo de evento es el evento observado. Este tipo de evento afecta a tres entidades en las que el agente y el origen de evento son la misma entidad. Sin embargo, esta entidad no ese el origen o destino del evento.

Un ejemplo de este tipo de evento es un cortafuegos o IDS de red que examina una conexión entre dos entidades de red.

Origen	Destino	Origen de evento	Agente
Host A	Host B	Host C	Host C

Tipo 4: evento observado distribuido

El cuarto tipo de evento es el evento observado distribuido. Este tipo de evento afecta a cuatro entidades en las que el agente se instala de forma remota desde el origen de evento. Una segunda configuración haría que el agente recogiera el evento de una quinta entidad denominada acción de repositorio de eventos en donde el origen de evento manda el evento al repositorio y el agente recoge los eventos del repositorio.

Un ejemplo de este tipo de evento es un IDS de red que usa sensores distribuidos y una consola de gestión central (ISS). Los sensores remotos observan interacciones entre entidades de red y eventos de transferencia a la consola de gestión central. Un agente instalado en un cuarto host recogerá estos eventos y los procesará con los protocolos de ODBC y OPSEC.

Origen	Destino	Origen de evento	Agente
Host A	Host B	Host C	Host D

Identificación del tipo de evento

Esta sección proporciona información sobre cómo identificar el tipo de evento que se ha expresado. La característica de distinción principal entre los tipos de eventos son el número de host (entidades de red) expresado en la información del evento. Utilice esta tabla para guiar la determinación del tipo de evento para el ejemplo con el que esté trabajando.

Número de host	Tipo de evento
1	Tipo 1
2	Tipo 2
3	Tipo 3
4+	Tipo 4

Capítulo 2: Normalización y categorización de eventos

El siguiente paso es normalizar y categorizar los eventos. La Gramática de eventos comunes proporciona varios campos que se utilizan para normalizar varios aspectos del evento. El primer aspecto que debe normalizarse es la clase de tecnología que está expresando el evento. Después debe determinarse la categoría, clase y acción expresada por el evento.

Esta sección contiene los siguientes temas:

Modelos ideales (en la página 52)
Categorías de eventos (en la página 54)
Clases de eventos (en la página 57)
Acciones de eventos (en la página 65)
Resultado del evento (en la página 70)
Valores de severidad de eventos (en la página 72)

Modelos ideales

El primer paso para la normalización de información del evento en la Gramática de eventos comunes es proporcionar un campo para la normalización de la tecnología que expresa el evento. Esta normalización de la clase de tecnología permite una referencia rápida y sencilla a todos los eventos que haya expresado una clase específica de tecnología independientemente del proveedor de aplicaciones. El campo de la Gramática de eventos comunes que se utiliza para la normalización de la clase de tecnología es el campo ideal_model. Este campo describe la clase de tecnología que expresó el evento. Algunos ejemplos de ideal_model incluyen:

- Antivirus
- DBMS
- Cortafuegos
- IDS/IPS de host
- IDS/IPS de red
- Dispositivo de red
- Sistema operativo
- Servidor Web
- Gestión de vulnerabilidades

Por ejemplo, Check Point, Cisco y Netscreen/Juniper producen productos específicos que están normalizados con un valor de cortafuegos en el campo ideal_model.

Lista de modelos ideales

A continuación se encuentra la lista actual de ideal_models:

Nombre	Descripción
Antivirus	El modelo de antivirus incluye los eventos que vienen de productos de antivirus. Los ejemplos incluyen: CA eTrust Antivirus, ITM, McAfee VirusScan, Symantec Antivirus Corporate Edition, TrendMicro OfficeScan.
Servicio de autenticación	CA SiteMinder Policy Server, Cisco Secure ACS

Nombre	Descripción
Gestión de contenido	CA SCM, SurfControl E-mail Filter
Corporate Mail Server	Microsoft Exchange
DBMS	El modelo DBMS incluye productos como MS-SQL, MySQL, DB2 u Oracle.
Cortafuegos	Un cortafuegos es un dispositivo de seguridad de perímetro utilizado normalmente para proteger entidades de red de otras entidades de red. Esto incluye cortafuegos de red y cortafuegos personales. BorderWare Firewall Server, CheckPoint, Cisco PIX, Netscreen/Juniper.
IDS/IPS de host	El modelo IDS de host incluye productos como Access Control, Cisco ACS o McAfee Host Intrusion Prevention. CA eTrust Access Control.
Aprovisionamiento de cuenta e identidad	El modelo de aprovisionamiento de cuenta e identidad incluye los eventos que vienen con productos de aprovisionamiento como CA Identity Manager.
Dispositivo de red	Dispositivos basados en Cisco IOS (conmutadores, enrutadores) y también otros proveedores.
IDS/IPS de red	CA eTrust ID, Enterasys Dragon, SNORT, ISS, etc.
Gestión de red	CA Unicenter NSM Event Management, HP OpenView, etc.
Sistema operativo	Windows, Unix, Top-Secret, ACF2, Top-Secret, etc.
Proxy Server	WebSphere Edge Caching Proxy Server
Sistema de gestión de seguridad	CiscoWorks LMS, CiscoWorks VPN/Security Manager, CiscoWorks ACL Manager, Microsoft MOM, ISS RealSecurie Site Protector, Symantec Enterprise Security Manager, TrendMicro Control Manager
Puerta de enlace de VPN	Nortel Contivity
Gestión de vulnerabilidades	Nessus Client, ISS Internet Scanner, Foundstone Foundscan, Nessus Server
Servidor Web	Microsoft IIS, Sun Sun One, Apache

Categorías de eventos

El segundo paso para normalizar la información del evento en la Gramática de eventos comunes es determinar la categoría a la que mejor se ajuste la información del evento expresada. Si proporciona un campo para categorizar la información del evento expresada, la Gramática de eventos comunes es compatible con informes de productos cruzados para una amplia categoría de eventos. El campo de Gramática de eventos comunes para este paso de normalización es el campo event_category. También proporciona un punto de referencia sencillo para establecer filtros con el fin de mostrar información específica para la generación de informes de conformidad.

Algunos ejemplos de event_category son:

- Gestión de identidades
- Seguridad de red
- Seguridad de host
- Seguridad operacional

Por ejemplo, todos los inicios de sesión correctos e incorrectos se registran con el mismo valor, acceso de sistema, en el campo event_category.

Lista de categorías de eventos

A continuación se muestra la lista actual de categorías de eventos:

Nombre	Descripción
Gestión de identidades	Gestión de identidades consta de gestión de cuentas, gestión de grupos, gestión de identidades y gestión de derechos de usuario. Esto incluye eventos como la cuenta creada, la cuenta modificada, las adiciones de pertenencia a grupo, supresiones y creaciones de grupo y otros.

Nombre	Descripción
Gestión de configuraciones	Gestión de políticas y configuraciones está compuesta de información recopilada a partir de modificaciones de políticas o cambios de configuraciones. Esto se aplica a todos los dispositivos como cortafuegos, host, servidores o políticas de SCC/auditoría. Esto incluye eventos como eventos de modificación de configuraciones, creación de políticas y modificación de políticas.
Seguridad del contenido	Seguridad del contenido consta de información que proporcionan las herramientas de inspección de contenido que supervisan el contenido en los canales de comunicación de Internet, incluidas las herramientas de colaboración el línea (como blogs y wikis), FTP, MI y WebMail.
Acceso a datos	Acceso a datos consta de información proporcionada por un DBMS o herramientas de control de base de datos. Esto incluye eventos como una consulta ejecutada, tabla creada, índice modificado, etc.
Seguridad de host	Integridad y seguridad de host consta de información acerca de la seguridad de un único host (normalmente sistemas de escritorio). Esto incluye eventos como "Virus detectado", "Virus eliminado", etc.
Seguridad de red	Seguridad de red consta de información relativa a la protección de las entidades de red contra el acceso de otras entidades de red. Esto incluye eventos como registros de interrupción de cortafuegos o alertas de infracción de IDS/IPS.
Seguridad operacional	Seguridad operacional consta de información relativa a la capacidad de mantener operaciones normales. Esto incluye eventos como la detención de servicios, inicio de servicios, apagado del sistema o arranque del sistema. Esto también incluye eventos como "registro de seguridad eliminado".

Nombre	Descripción
Acceso físico	Acceso físico consta de información recopilada sobre los intentos de entrada a través de dispositivos de seguridad físicos. Esto incluye eventos como "identificador analizado" o "cámara desconectada".
Acceso a recursos	Acceso a recursos consta de información recopilada sobre los intentos de acceder a recursos. Esto incluye acceso a recursos de archivo, recursos de registro y recursos URI. En los recursos, el host es el host que ha registrado el evento y el usuario es el usuario o identidad que intenta acceder al recurso.
Acceso al sistema	Acceso a sistema consta de información recopilada de los intentos de acceso a distintos sistemas. Esto incluye eventos como intentos de establecimiento de usuario o inicios de sesión, así como intentos de autenticación de red (VPN, NAP, 802.11x). Para el acceso al sistema, un recurso es una aplicación que facilita el proceso de inicio de sesión. Por ejemplo, ftpd o sshd se considerarían recursos para el área de acceso del sistema.
Categoría desconocida	Los eventos que no se categorizan en una categoría específica se categorizan en la categoría "Desconocido". En los archivos de asignación de datos, si hay un error en todas las condiciones de asignación para la coincidencia de un evento específico, el evento se etiqueta en esta categoría. Los archivos de asignación de datos deben actualizarse para reducir los eventos con la categoría "Desconocido".
Gestión de vulnerabilidades	Gestión de vulnerabilidades consta de información recopilada de herramientas de gestión y evaluación de seguridad. Esto incluye eventos como “vulnerabilidad encontrada” o “parche necesario”.
Operaciones SIM	Operaciones SIM consta de informes operativos sobre la vida de las operaciones para SIM. Esta información es independiente de la información que procesa y recopila SIM.

Clases de eventos

El tercer paso para normalizar la información del evento en la Gramática de eventos comunes es determinar la clase de la información del evento expresada. El campo event_class representa una interrupción mayor de eventos para una categoría de eventos específica. Si se proporciona otra capa de clasificación, los eventos de seguridad pueden agruparse más para representar las áreas de tecnología e interés específicas.

El campo event_class proporciona un marcador para una clasificación de eventos en una categoría específica. Asocia una categoría de evento y una clase de evento. Por ejemplo, Creación de cuentas está asociada a la categoría gestión de identidades y la clase de gestión de cuentas.

Los ejemplos de clase de eventos en la categoría de eventos de gestión de identidades son:

- Gestión de cuentas
- Gestión de grupos
- Gestión de función de usuario
- Gestión de derechos de usuario

Lista de clases de eventos

Los siguientes temas describen la lista actual de clases de eventos.

Gestión de identidades

Nombre	Descripción
Gestión de cuentas	La clase de gestión de cuentas incluye acciones que tratan las actividades de cuentas como la creación de cuentas, supresión de cuentas, desactivación de cuentas y modificación de cuentas.
Gestión de grupos	La clase de gestión de grupos incluye acciones que tratan las actividades de grupo como la creación de grupos, modificación de pertenencia a grupo, supresión de grupos y modificación de grupos.

Nombre	Descripción
Gestión de identidades	La clase de gestión de identidades incluye acciones que tratan las actividades de identidad como la creación de identidades, supresión de identidades y modificación de identidades. Esta clase de eventos están normalmente restringidos a los productos de aprovisionamiento como Identity Manager.
Gestión de derechos de usuario	La clase de gestión de derechos de usuario incluye acciones que tratan la creación, supresión y asignación de derechos de usuario
Gestión de función de usuario	La clase de gestión de funciones de usuario incluye acciones que tratan las actividades de funciones de usuario como la asignación de funciones de usuario, asignación de funciones de administrador de usuarios.

Gestión de configuraciones

Nombre	Descripción
Gestión de configuraciones	La clase de gestión de configuraciones incluye las acciones relacionadas con la actividad de configuración como la modificación de configuración, eliminación de configuración y otras.
Gestión de políticas	La clase de gestión de políticas incluye las acciones relacionadas con la creación de políticas, activación de políticas, aplicación de políticas, desactivación de políticas y supresión de políticas.
Gestión de copia de seguridad	La clase de gestión de copia de seguridad incluye acciones relacionadas con la creación de copias de seguridad de los datos de configuración y datos reales. Esta clase se asignará en la categoría de gestión de configuraciones para las acciones de copia de seguridad relacionadas con datos de configuración. Esta clase se asignará en la categoría de seguridad de operaciones para las acciones de copia de seguridad relacionadas con datos reales.

Nombre	Descripción
Gestión de perfiles	La clase de gestión de perfiles incluye acciones relacionadas con actividades de perfiles como creación de perfiles, supresión de perfiles y modificación de perfiles. Se define un perfil para procesos/acciones/componentes/dispositivos de grupo, etc. basados en condiciones específicas y, a continuación, las políticas/reglas se aplican según el perfil en lugar de en componentes individuales.

Inspección de contenido

Nombre	Descripción
Inspección de correo electrónico	
Acceso a URL	

Acceso a datos

Nombre	Descripción
Gestión de aplicaciones	La clase de gestión de aplicaciones incluye acciones que tratan las actividades de gestión de aplicaciones como el análisis de índices, la creación de iniciaciones y otras.
Eventos de auditoría	La clase de eventos de auditoría incluye acciones que tratan la gestión de servicios de auditoría, como las acciones de auditoría, privilegios de auditoría y modificación de política de auditoría.
Acceso a datos	La clase de acceso de datos incluye acciones que tratan la asociación de elementos de datos o recursos con contenidos o servicios. Por ejemplo, insertar en tabla, seleccionar de vista, eliminar de tabla, truncar tabla, actualizar tabla.
Gestión de objetos	La clase de gestión de objetos incluye acciones que tratan la actividad de gestión de objetos como la creación de tablas, creación de índices, supresión de tablas y otras.

Nombre	Descripción
Gestión del mismo nivel	La clase de gestión del mismo nivel incluye acciones que tratan la actividad de gestión del mismo nivel como la creación de vínculos de datos, supresión de vínculos de datos y otras.
Gestión de privilegios	La clase de gestión de privilegios incluye acciones que tratan la gestión de privilegios como crear función, conceder privilegio, modificar función, interrumpir función, conceder objeto, conceder función, revocar función y revocar objeto.
Utilización de aplicaciones y servicios	La clase de utilización de aplicaciones y servicios que incluye las acciones que tratan de la utilización y gestión de servicios y aplicaciones como la ejecución de procedimientos, ejecución de métodos y otras.
Gestión del sistema	La clase de gestión del sistema incluye las acciones relacionadas con la gestión de actividades del sistema como el vaciado de la papelera de reciclaje, la modificación del espacio de tablas y otras.

Seguridad de host

Nombre	Descripción
Actividad del antivirus	La clase de actividad del antivirus incluye las acciones como virus encontrado, actualización de virus aplicada y otras.
Actividad de IDS/IPS	La clase de actividad de IDS/IPS incluye acciones como política infringida.

Seguridad de red

Nombre	Descripción
Actividad de conexión	La clase de actividad de conexión incluye acciones relacionadas con la actividad de conexión como el intento de conexión y otras.

Nombre	Descripción
Actividad de infracción de firmas	La clase de actividad de infracción de firmas incluye acciones relacionadas con las acciones de coincidencia de firmas como la violación de firmas y otras.
Seguridad de aplicación	La actividad de aplicación de la que informan los dispositivos de red como IDS, IPS y puertas de enlace.
Infracción de políticas corporativas	Cualquier actividad de red que infrinja la política corporativa.
Pérdida de información	Actividad de red relacionada con el intento o robo consumado de datos y transferencia no autorizada de datos.
Escalación de privilegios	Intentos de escalación de privilegios de usuario.
Denegación de servicio	Actividad relacionada con intentos para hacer que los recursos del equipo no estén disponibles para usuarios determinados.
Actividad sospechosa	Cualquier tipo de actividad sospechosa de la que se haya informado que no pueda clasificarse en otras clases en la categoría "Seguridad de red".

Seguridad operacional

Nombre	Descripción
Actividad de proceso	La clase de actividad de proceso incluye acciones que tratan la actividad de proceso como el inicio del proceso, la detención del proceso y otras.
Actividad del sistema	La clase de actividad del sistema incluye acciones que tratan la actividad del sistema como el inicio o cierre del sistema y otras.
Actividad de registro de seguridad	La clase de actividad de registro de seguridad incluye acciones como la activación y supresión de registro de seguridad y otras.
Actividad de sesión	La clase de activación de sesión incluye acciones como el inicio y detención de sesión y otras.

Nombre	Descripción
Gestión de copia de seguridad	La clase de gestión de copia de seguridad incluye acciones relacionadas con la creación de copias de seguridad de los datos de configuración y datos reales. Esta clase se asignará en la categoría de gestión de configuraciones para las acciones de copia de seguridad relacionadas con datos de configuración. Esta clase se asignará en la categoría de seguridad de operaciones para las acciones de copia de seguridad relacionadas con datos reales.

Acceso físico

Nombre	Descripción
Actividad de acceso físico	La clase de actividad de acceso físico incluye acciones que tratan los intentos de acceso a través de dispositivos de seguridad físicos.

Acceso a recursos

Nombre	Descripción
Actividad de recursos	La clase de actividad de recursos incluye acciones que tratan la actividad de recursos como la apertura y cierre de recurso y otras.

Acceso al sistema

Nombre	Descripción
Actividad de autenticación	La clase de actividad de autenticación incluye acciones que tratan la autenticación de credenciales como el intento de autenticación y otras.
Actividad de autorización	La clase de actividad de autorización incluye acciones que tratan la autenticación de credenciales como el intento de autorización y otras.

Nombre	Descripción
Actividad de inicio de sesión	La clase de actividad de inicio de sesión incluye acciones que tratan la actividad de inicio de sesión como el intento de inicio de sesión y otros.
Actividad de cierre de sesión	La clase de actividad de cierre de sesión incluye acciones que tratan la actividad de desconexión como el cierre de sesión y otras.
Obtención de privilegios	La clase de obtención de privilegios incluye acciones que tratan la actividad de obtención de privilegios como la obtención de privilegios y otras.
Uso de privilegios	La clase de uso de privilegios incluye acciones que tratan la actividad de uso de privilegios como el uso de privilegios y otras.
Actividad de sesión	La clase de actividad de sesión incluye acciones que tratan la actividad de sesión como el inicio de sesión, la desconexión de sesión y otras.
Actividad de configuración de usuario	La clase de actividad de configuración de usuario que trata la actividad de configuración de usuario como el establecimiento de usuario y otras.

Categoría desconocida

Nombre	Descripción
Clase desconocida	Los eventos que no se asignan a una clase específica se asignan en "Clase desconocida". Los archivos de asignación de datos deben actualizarse para reducir los eventos con la "Clase desconocida".

Gestión de vulnerabilidades

Nombre	Descripción
Evaluación de vulnerabilidades	La clase de evaluación de vulnerabilidades incluye acciones que tratan la actividad de la evaluación de vulnerabilidad como el inicio de la evaluación de vulnerabilidad, la evaluación de vulnerabilidad completada y otras.
Gestión de vulnerabilidades	La clase de gestión de vulnerabilidades incluye acciones que tratan la gestión de vulnerabilidades como la vulnerabilidad encontrada, el parche necesario y otras.

Operaciones SIM

Nombre	Descripción
Gestión de alertas	La clase de gestión de alertas incluye acciones que tratan la gestión de alertas como la creación, supresión, escalación, asignación de alertas y otras.
Gestión de línea de base	La clase de gestión de línea de base incluye acciones que tratan la gestión de prueba de línea de base como la creación, supresión, activación, establecimiento de línea de base y otras.
Gestión de origen de evento	La clase de gestión de origen de evento incluye acciones que tratan la gestión de orígenes de eventos como el descubrimiento, provisión y autorización de origen de evento y otras.
Gestión de incidentes	La clase de gestión de incidentes incluye acciones que tratan la gestión de incidentes como la creación, modificación y resolución de incidentes y otras.
Gestión de investigaciones	La clase de gestión de investigación incluye acciones que tratan la gestión de investigaciones como la apertura, supresión y cierre de investigaciones, entre otras.

Nombre	Descripción
Gestión de notificaciones	La clase de gestión de notificaciones incluye acciones que tratan la gestión de notificaciones como la creación o entrega de notificaciones y otras.
Gestión de solicitudes	La clase de gestión de solicitudes incluye acciones que tratan la gestión de solicitudes como la creación, modificación y entrega de solicitudes y otras.

Acciones de eventos

El cuarto paso para normalizar la información del evento en la Gramática de eventos comunes es determinar la acción normalizada que expresa la información del evento. El campo event_action proporciona un marcador de posición en el que las acciones comunes que se han producido pueden normalizarse con un nombre común.

Describe exactamente qué ocurre en una frase corta sin detalles. Por ejemplo, la creación de cuentas es una acción que implica que alguien ha creado una cuenta o un número de cuentas en un host específico.

El campo event_action se asocia a una categoría de eventos y una clase de eventos. Por ejemplo, la creación de cuentas event_action está asociada a la gestión de identidades event_category y la gestión de cuentas event_class.

Cada acción de eventos puede tener uno o más de los siguientes valores de resultados: correcto, incorrecto, aceptado, rechazado, interrumpido, desconocido.

Por ejemplo, todos los inicios de sesión erróneos se normalizan con un valor de acción de intentos de inicio de sesión en el campo event_action. Si se ha producido un error en el intento de inicio de sesión, aparece un valor de error en el campo event_result y si es correcto, aparece un valor de correcto en el campo event_result.

Lista de acciones de eventos

La Gramática de eventos comunes está dividida en seis secciones y cada una de ella está dividida a su vez de la siguiente manera. Para un ejercicio de asignación correcto, es necesario que se proporcione parte de la información de cada subsección especificada según la designación en la parte superior. Los campos designados en **negrita** son obligatorios para cada sección para recibir la puntuación PASS si se designan como principales. Los campos designados en **negrita y cursiva** son campos alternativos. Sólo uno de los campos alternativos es necesario para la sección para recibir la puntuación PASS si se designa como principal.

Información	**Información de campo**
Origen - Información de usuario	source_domainname, source_username, source_uid
Origen - Información de host	*source_hostname*, *source_address*, source_mac_address, source_hostdomainname, source_port
Origen - Información de objeto	source_objectname, source_objectid, source_objectattr, source_objectclass, source_objectvalue
Origen - Información de proceso	source_processname
Origen - Información de grupo	source_groupname, source_gid
Destino - Información de usuario	dest_domainname, dest_username, dest_uid
Destino - Información de host	*dest_hostname*, *dest_address*, dest_mac_address, dest_hostdomainname, dest_port
Destino - Información de objeto	dest_objectname, dest_objectid, dest_objectattr, dest_objectclass, dest_objectvalue
Destino - Información de proceso	dest_processname
Destino - Información de grupo	dest_groupname, dest_gid
Agente - Información	agent_name, agent_version, agent_id, agent_group, agent_connector_name
Agente - Información de host	*agent_hostname*, *agent_address*, agent_hostdomainname
Origen de evento - Información de host	*event_source_hostname*, *event_source_address*, event_source_hostdomainname

Información	Información de campo
Origen de evento - Información	*event_source_processname*
Evento - Información	event_protocol, event_logname, event_euuid, event_count, event_summarized, event_duration, event_time_gmt, event_timezone, event_sequence, event_action, event_id, event_category, event_class, ideal_model, event_severity
Resultado - Información	event_result, result_string, result_signature, result_code, result_version, result_priority, result_scope, result_severity

Las últimas dos secciones de la Gramática de eventos comunes son secciones obligatorias para todas las acciones.

Para cada acción, la información de la Gramática de eventos comunes se describe como principal, secundaria o terciaria. La información principal está disponible a partir de la mayor parte de los orígenes de eventos y es obligatorio que este evento se considere asignado. La información secundaria está disponible a partir de algunos de los orígenes de eventos y es deseable que este evento se considere asignado. Finalmente, la información terciaria debe estar disponible a partir de algunas fuentes de eventos y, si estuviera disponible, debe asignarse.

Por ejemplo, la acción de creación de cuentas busca la respuesta a quién ha creado qué cuenta en qué host y en qué host se ha expresado esta información del evento. La respuesta puede tener la siguiente forma: El Administrador ha creado UsuarioA en el HostA y el HostA ha expresado el evento. Esta información contiene valores para Origen - Información de usuario, Destino - Información de host, Destino - Información de usuario. Además, cada información de evento de la Gramática de eventos comunes debe contener información sobre qué agente ha registrado el evento y a partir de qué host se ha expresado el evento. Si pone esta información en una tabla debe aparecer lo siguiente:

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Para cada acción se proporciona esta tabla con la información descrita como corresponde. Deben seguirse las siguientes instrucciones cuando se observe la información en eventos.

Para eventos de tipo 1:

- El host que ha expresado la información es el mismo que el host en el que se ha creado la cuenta.
- Puede que haya información relativa a Origen - Información de host y si la hay, esta información es idéntica a la del host en el que se ha producido la acción.
- Debe haber sólo un conjunto de información de host en estos eventos.

Para eventos de tipo 2:

- Debe haber dos conjuntos de información de host en estos eventos.
- El primer conjunto de información de host hace referencia a la sección Origen - Información de host y esta información de host debe ser distinta de la del host en el que se produjo la acción.
- Debe haber información relativa al host en el que se ha instalado el agente SIM pero esta información debe ser la misma que la del host donde se ha producido la acción y el host que ha expresado la información del evento.

Para eventos de tipo 3:

- Existen tres conjuntos de información de host en estos eventos.
- El primer conjunto de información describe la información source-host.
- El segundo conjunto de información describe la información destino-host en la que se ha producido la acción.
- El tercer conjunto de información describe Origen de evento - Información de host en donde se ha expresado el evento y se ha instalado el agente SIM.

Para eventos de tipo 4:

- Existen cuatro conjuntos de información de host en estos eventos.
- El primer conjunto de información describe la información source-host.
- El segundo conjunto de información describe la información destino-host en la que se ha producido la acción.
- El tercer conjunto de información describe Origen de evento - Información de host en donde se ha expresado el evento.

- El cuarto conjunto de información describe la información agente-host en donde se ha instalado el agente SIM.

Resultado del evento

Cada evento se describe con 16 secciones. Cada sección define un conjunto de campos.

Cada sección se clasifica como principal, secundaria o terciaria.

Un evento se considera asignado si al menos se proporciona uno de los campos necesarios en cada sección principal.

Clasificación	Disponibilidad de información	Condición
Primario	De la mayor parte de orígenes de eventos	Requerido
Secundario	De algunos orígenes de eventos	Deseado
Terciario	De algunos orígenes de eventos	Opcional

Ejemplo de asignación de resultado de eventos

Tenga en cuenta el siguiente ejemplo: quién creó qué cuenta en qué host y en qué host se ha expresado esta cuenta para la acción de eventos de creación de cuentas; la información se clasifica como principal, secundaria o terciaria.

Para comenzar, revise la tabla de la acción de creación de cuentas en la clase de gestión de cuentas en la categoría de gestión de identidades:

Información	Nivel
Origen - Información de usuario	Principal *(quién ha creado)*
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Principal *(qué cuenta)*

Información	Nivel
Destino - Información de host	Principal *(qué host)*
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Principal *(qué host expresado)*
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Severidad del evento

Severidad del evento es el último campo de la Gramática de elementos comunes utilizado para la normalización. Severidad del evento es la interpretación de la seriedad de un evento que se aplica a todos los tipos de eventos. El campo event_severity consta de una valor de nivel de severidad que va de 0 a 7 con descripciones claramente definidas.

La severidad de eventos proporciona un punto de referencia para comparar la relatividad interna de un evento de seguridad en términos de amenaza e implicación a la integridad, disponibilidad, estabilidad y seguridad del sistema. Como campo, event_severity no siempre está asignado a result_severity pero transmite un mensaje parecido.

Cuando se aplica a la Gramática de eventos comunes, el propósito de los campos event_severity es asignar el valor del campo result_severity asignado por distintos proveedores en los registros de seguridad a un denominador común.

Valores de severidad de eventos

La asignación se basa en los procedimientos recomendados y principios de seguridad general. Por ejemplo, una acción errónea se considera normalmente más grave que una correcta desde un punto de vista de implicación de seguridad. La siguiente tabla muestra el valor, nombre y explicación de los ocho niveles de severidad. En el apéndice A se encuentra una lista detallada de asignación de nivel de seguridad.

Valor	Nombre	Descripción
0	Desconocido	Eventos desconocidos Eventos no asignados a la Gramática de eventos comunes Sin clasificar
1	Depurar	Mensaje que aparece sólo durante el proceso de depuración Eventos en el entorno que no es de producción
2	Información	Informe de funcionamiento del sistema general Información relacionada con la seguridad general Aviso
3	Advertencia	Cambios poco corrientes en el sistema/función/seguridad Condición normal pero significativa Operaciones erróneas Rendimiento reducido
4	Minor_Impact	Impacto de importancia baja en el sistema/función Impacto de importancia baja en la seguridad
5	Major_Impact	Impacto de importancia alta en el sistema/función Impacto de importancia alta en la seguridad
6	Crítico	Acción inmediata necesaria Probable infracción de seguridad
7	Grave	Sistema inservible/apagado Alta probabilidad de infracción de seguridad Problemas no recuperables

Los niveles de severidad 0 y 1 se encuentran actualmente sin asignar a una acción de eventos de la Gramática de eventos comunes existente y se reserva para uso futuro. Para el resto de niveles de seguridad, se siguen las siguientes directrices:

Nivel de severidad 2:

- Asignación a funcionamiento normal del sistema.
- Seguridad relacionada con eventos con un resultado correcto.

Nivel de severidad 3:

- Asignación a acciones de eventos relacionadas con la seguridad o funcionamiento del sistema normal con un resultado incorrecto.
- Asignación a eventos relacionados con la seguridad o funcionamiento del sistema poco frecuente/inusual con resultado correcto.

Nivel de severidad 4:

- Principalmente, acciones de gestión de sistemas y aplicaciones que afectan a otros sistemas o varias funciones.
- Eventos que garantizan un nivel más alto de atención que una advertencia.
- Condición de error de importancia baja

Nivel de severidad 5:

- Eventos comparativamente menos graves.
- Condición de error de importancia alta

Nivel de severidad 6:

- Asignación de áreas de implicación de seguridad y problemas de importancia alta que necesitan una solución o que se preste atención inmediatamente, como actividades de antivirus, registro de actividades y seguridad física.

Nivel de severidad 7:

- Asignación a eventos de apagado del sistema.

Capítulo 3: Categoría de gestión de configuraciones

Esta sección contiene los siguientes temas:

Clase de gestión de configuraciones (en la página 75)
Clase de gestión de políticas (en la página 92)
Clase de gestión de copia de seguridad (en la página 106)
Clase de gestión de perfiles (en la página 108)

Clase de gestión de configuraciones

Acción de modificación de configuración

La acción de modificación de configuración se produce cuando se cambia la configuración de una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario*
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario*
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario o qué proceso ha modificado la configuración de qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

* - o el origen - Información de usuario u Origen - Información de proceso son necesarios para esta acción.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de error de configuración

La acción de error de configuración se produce cuando se envía una notificación de que el host ha encontrado un error en la información de configuración para ese host. Si no se puede realizar esta acción, no habrá ningún error del que informar y no se llevará a cabo la acción.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué host está informando de un error de configuración en qué información de configuración. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6

Acción de configuración de Vaciar todo

La acción de configuración de Vaciar todo se produce cuando se envía información del evento relativa a la eliminación de toda la información de la caché de la configuración de un host o sistema determinados. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host está vaciando la información de la caché de configuración. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de configuración de Vaciar territorios de autenticación

La acción de configuración de Vaciar territorios de autenticación se produce cuando se envía la información del evento relativa a la eliminación de toda la información de la caché de configuración relacionada con los territorios de autenticación o dominios de autenticación en un host o sistema determinados. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host está borrando la información de la caché de configuración relacionada con los territorios de autenticación. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de configuración de Vaciar caché de usuario

La acción de configuración de Vaciar caché de usuario se ocupa de la expresión de la información del evento relativa a la eliminación de toda la información de la caché de configuración relacionada con los objetos de usuario en un sistema o host determinados. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Terciario

Información	Nivel
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host está borrando la información de la caché de configuración relacionada con los objetos de usuario. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de alerta de configuración

La acción de alerta de configuración trata la expresión de información relativa a las condiciones de alerta generadas durante los cambios de configuración o los errores de alerta relacionados con un valor de configuración.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	7

Acción de notificación de configuración

La acción de notificación de configuración se encarga de proporcionar información genérica relativa a la configuración. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host está borrando la información de la caché de configuración relacionada con los objetos de usuario. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de lectura de configuración

La acción de lectura de configuración proporciona información relativa a la lectura o la carga de una configuración, por ejemplo, a partir un archivo de configuración.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de inicio de lectura de configuración

La acción de inicio de lectura de configuración se produce cuando se envía la notificación de que un host ha comenzado a leer la información de comunicación. Si se produce un error en esta acción, no se lleva a cabo.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host está recuperando qué configuración de qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2

Acción de estado de configuración

La acción de estado de configuración proporciona información relativa al estado de un parámetro de configuración.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de configuración

La acción de advertencia de configuración se produce cuando se envía una notificación de que un host ha encontrado una advertencia en la información de configuración para ese host. Si no se puede realizar esta acción, no habrá ningún error del que informar y no se llevará a cabo la acción.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué host está informando de una advertencia de configuración en qué información de configuración. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3

Acción de modificación de hora del sistema

La acción de modificación de hora del sistema se produce cuando se cambia la hora del sistema en un sistema determinado.

Información	Nivel
Origen - Información de usuario	Primario*
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario*
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario o qué proceso ha modificado la hora del sistema en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

* - o el origen - Información de usuario o el origen - La información de proceso es necesaria para esta acción.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	4

Acción de creación de tareas

La acción de creación de tareas se produce cuando se crea una instancia de una tarea en un sistema determinado o aplicación.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha creado la tarea en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de tareas

La acción de supresión de tareas se produce cuando se suprime una tarea programada o flujo de trabajo. Debe ser válida para el programador de nivel del SO en Windows o UNIX u otra aplicación.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha suprimido qué tarea en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de tareas

La acción de modificación de tareas se produce cuando se modifica una instancia de una tarea en un sistema determinado o aplicación.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha modificado qué tarea en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de informes de tareas

La acción de informes de tareas se produce cuando se informa de una tarea programada o flujos de trabajo. Debe ser válida para el programador de nivel del SO en Windows o UNIX u otra aplicación.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha informado de qué tarea en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión de políticas

Acción de configuración de políticas de contraseñas

La acción de configuración de políticas de contraseñas refleja información sobre la definición de políticas de contraseñas, como las que controlan la calidad o la duración de las contraseñas.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de activación de políticas

La acción de activación de políticas se produce cuando se activa una política específica en un sistema o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Primario*
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario*
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario o qué proceso ha activado qué política en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

* - o el origen - Información de usuario o el origen - La información de proceso es necesaria para esta acción.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de aplicación de políticas

La acción de aplicación de políticas se produce cuando se aplica una política específica en un sistema determinado o aplicación.

Información	Nivel
Origen - Información de usuario	Primario*
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario*
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

La información importante para esta acción es qué usuario o qué proceso ha aplicado qué política en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

* - o el origen - Información de usuario o el origen - La información de proceso es necesaria para esta acción.

Resultado	event_result	event_severity
Correcto	S	2

Acción de creación de políticas

La acción de creación de políticas se produce cuando se crea una política en un sistema determinado o aplicación.

Información	Nivel
Origen - Información de usuario	Primario*
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario*
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario o qué proceso ha creado qué política en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

* - o el origen - Información de usuario o el origen - La información de proceso es necesaria para esta acción.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desactivación de políticas

La acción de desactivación de políticas se produce cuando se desactiva una política específica en un sistema determinado o aplicación.

Información	Nivel
Origen - Información de usuario	Primario*
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario*
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario o qué proceso ha desactivado qué política en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

* - o el origen - Información de usuario o el origen - La información de proceso es necesaria para esta acción.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de políticas

La acción de supresión de políticas se produce cuando se suprime una política en un sistema determinado o aplicación.

Información	Nivel
Origen - Información de usuario	Primario*
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario*
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario o qué proceso ha suprimido qué política en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

* - o el origen - Información de usuario o el origen - La información de proceso es necesaria para esta acción.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de error de política

La acción de error de política proporciona información sobre los eventos de error relacionados con la gestión de cualquier política.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario o qué proceso ha causado qué error en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

* - o el origen - Información de usuario o el origen - La información de proceso es necesaria para esta acción.

Resultado	event_result	event_severity
Correcto	S	5

Acción de lista de políticas

La acción de lista de políticas se produce cuando se enumera una política en un sistema o una aplicación determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario o qué proceso ha enumerado qué política en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	2

Acción de modificación de políticas

La acción de modificación de políticas se produce cuando se modifica una política existente en un sistema o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Primario*
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario*
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario o qué proceso ha modificado qué política en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

* - o el origen - Información de usuario o el origen - La información de proceso es necesaria para esta acción.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de notificación de políticas

La acción de notificación de políticas proporciona información relativa a las notificaciones del motor de políticas o las notificaciones relacionadas con la gestión de políticas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de sustitución de política

La acción de sustitución de política proporciona información relativa a la sustitución de una política existente por una política nueva.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de política

La acción de advertencia de política contiene información sobre advertencias relacionadas con la gestión de cualquier política.

Información	Nivel
Origen - Información de usuario	Primario

Información	Nivel
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario o qué proceso ha emitido una advertencia en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5

Acción de estado de reglas o políticas

La acción de estado de reglas o políticas trata la expresión de la información relativa al evento registrado para cada proveedor de la Plataforma de filtrado de Windows presente.

Información	Nivel
Origen - Información de usuario	Primario

Información	Nivel
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión de copia de seguridad

Acción de copia de seguridad de configuración de dispositivo de red

La acción de copia de seguridad de configuración de dispositivo de red se produce cuando se realiza la copia de seguridad de información de comunicación almacenada en dispositivos como enrutadores, conmutadores, cortafuegos, dispositivos inalámbricos, equilibradores de carga, etc.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué proceso ha realizado la copia de seguridad de qué configuración en qué dispositivo. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de restauración de configuración de dispositivo de red

La acción de restauración de configuración de dispositivos de red se produce cuando se restaura la información de configuración del servidor de copia de seguridad en dispositivos como enrutadores, conmutadores, cortafuegos, dispositivos inalámbricos, equilibradores de carga, etc.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué proceso ha restaurado qué configuración en qué dispositivo. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión de perfiles

Acción de alerta de perfil

La acción de alerta de perfil proporciona información sobre alertas relativas a perfiles.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	6

Acción de creación de perfiles

La acción de creación de perfiles se produce cuando se crean perfiles para agrupar sistemas, dispositivos, aplicaciones, redes, etc. y gestionar políticas basadas en los perfiles.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué perfil en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de perfiles

La acción de supresión de perfiles se produce cuando se eliminan perfiles.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué perfil en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de error de perfil

La acción de error de perfil proporciona información sobre errores relativos a perfiles.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de lista de perfiles

La acción de lista de perfiles se produce cuando se enumera un perfil en un host determinado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha enumerado qué perfil en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de perfiles

La acción de modificación de perfiles se produce cuando se modifican o actualizan perfiles.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué perfil en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de notificación de perfil

La acción de notificación de perfil proporciona información sobre las notificaciones y los mensajes relacionados con perfiles que se generan en un sistema.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de perfil

La acción de estado de perfil proporciona información acerca del estado de los perfiles.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de perfil

La acción de advertencia de perfil proporciona información sobre las advertencias relativas a los perfiles.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Capítulo 4: Categoría de seguridad de contenido

Esta sección contiene los siguientes temas:

Clase de prevención de pérdida de datos (en la página 119)
Clase de inspección de correo electrónico (en la página 121)
Clase de inspección de mensaje (en la página 127)
Clase de acceso de URL (en la página 129)

Clase de prevención de pérdida de datos

Acción de inspección de contenido

La inspección de contenido expresa información acerca de la inspección del contenido para prevenir la pérdida de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Secundario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de infracción de políticas

Esta acción expresa información sobre las infracciones de políticas relacionadas con los controles y las políticas de prevención de pérdida de datos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	5

Clase de inspección de correo electrónico

Acción de análisis de archivo adjunto

La acción de análisis de archivo adjunto se produce cuando se envía la información del evento relativa al análisis de archivo adjunto en el correo entre dos entidades de red según lo que registra un host determinado. Estos eventos pueden generarse cuando el servidor de correo procesa el correo electrónico con un archivo adjunto.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host está intentando acceder a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de pérdida de información confidencial

La acción de pérdida de información confidencial se produce cuando se envía información del evento relativa al análisis de correo electrónico de información confidencial en dos entidades de red según lo que registra un host determinado. Estos eventos pueden generarse cuando el software de gestión de contenido procesa el correo electrónico y comprueba la información confidencial en el correo.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario (remitente) está intentando enviar un correo con información confidencial a qué usuario (destinatario). La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de inspección de correo electrónico

La acción de inspección de correo electrónico se produce cuando se envía la información del evento relativa al análisis de correo electrónico.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de detección de lenguaje irreverente

La acción de detección de lenguaje irreverente se produce cuando se envía información del evento relativa al análisis de palabras soeces en el correo electrónico en las dos entidades de red según lo que registra un host determinado. Estos eventos pueden generarse cuando el software de gestión de contenido procesa el correo electrónico y el programa de detección de lenguaje irreverente realiza la comprobación del correo de forma interna.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario (remitente) está intentando enviar un correo con lenguaje irreverente a qué usuario (destinatario). La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de detección de spam

La acción de detección de spam se produce cuando se envía información del evento relativa a la detección de spam entre dos entidades según lo que registra un host determinado. Estos eventos pueden generarse cuando intente acceder a algún sitio Web y el contenido del sitio Web se categoriza como spam.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Primario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host está intentando acceder a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3

Clase de inspección de mensaje

Acción de revisión de mensaje

La acción de revisión de mensaje tiene lugar cuando se revisa un mensaje en una entidad de control como el revisor de cumplimiento.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de rechazo de mensaje

La acción de rechazo de mensaje tiene lugar cuando se rechaza un mensaje desde una entidad de control como el revisor de cumplimiento.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de acceso de URL

Acción de filtrado de URL

El filtrado de URL se produce cuando se envía la información del evento relativa al acceso a las URL entre dos entidades de red según lo que registra un host determinado. Estos eventos pueden generase cuando se accede a una URL y se valida con la política de software de gestión de contenidos establecida para el filtrado de URL de SPAM.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host está intentando acceder a qué objeto (URL). La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de redireccionamiento de URL

Esta acción se produce cuando la información de evento relativa a un cliente se redirige a otra dirección URL, por ejemplo, para fines de autenticación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host está realizando la redirección a qué objeto (URL). La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de filtrado de HTTP

La acción de filtrado de HTTP se produce cuando se envía la información del evento relativa al acceso a descargas de HTTP/protocolo de HTTP entre dos entidades de red según lo que registra un host determinado. Estos eventos pueden generase cuando se accede a una URL a través de un protocolo HTTP y se valida con la política de software de gestión de contenidos establecida para el acceso de HTTP.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

La información importante para esta acción es qué host está intentando acceder a qué objeto (URL). La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de filtrado de FTP

La acción de filtrado de FTP se produce cuando se envía la información del evento relativa al acceso a descargas de FTP/protocolo de FTP entre dos entidades de red según lo que registra un host determinado. Estos eventos pueden generase cuando se accede a una URL a través de un protocolo FTP y se valida con la política de software de gestión de contenidos establecida para el acceso de FTP.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host está intentando acceder a qué objeto (URL). La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de inspección de contenido

La acción de inspección de contenido se produce cuando se envía la información del evento relativa al análisis del tráfico HTTP.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Capítulo 5: Categoría de acceso de datos

Esta sección contiene los siguientes temas:

Clase de gestión de aplicaciones (en la página 135)
Clase de eventos de auditoría (en la página 172)
Clase de acceso de datos (en la página 179)
Clase de gestión de objetos (en la página 190)
Clase de gestión del mismo nivel (en la página 254)
Clase de gestión de privilegios (en la página 256)
Clase de utilización de aplicaciones y servicios (en la página 267)
Clase de actividad del sistema (en la página 270)
Clase de gestión del sistema (en la página 275)

Clase de gestión de aplicaciones

Acción de operación de enlace

Esta acción expresa información sobre el enlace o la creación de vínculos entre los objetos de la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de creación de contexto

La acción de creación de contexto se produce cuando se crea un contexto.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué contexto en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de contexto

La acción de supresión de contexto se produce cuando se elimina un contexto.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué contexto en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de creación de funciones

La acción de creación de funciones se produce cuando un usuario de la base de datos crea una función a partir de un host de origen.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la función creada por qué usuario y qué usuario del SO en qué host y qué base de datos en un momento determinado. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de funciones

La acción de supresión de funciones se produce cuando un usuario de la base de datos suprime una función a partir de un host de origen.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la función suprimida por qué usuario y qué usuario del SO en qué host y qué base de datos en un momento determinado. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de modificación de funciones

La acción de modificación de funciones se produce cuando un usuario de la base de datos modifica una función a partir de un host de origen.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la función modificada por qué usuario y qué usuario del SO en qué host y qué base de datos en un momento determinado. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de análisis de índices

La acción de análisis de índices se produce cuando se inicia el análisis de un índice en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha iniciado un análisis de los índices en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de vaciado de índices

La acción de vaciado de índices elimina los índices de la papelera de reciclaje y libera todo el espacio asociado al índice.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha vaciado qué índice en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de creación de biblioteca

La acción de creación de biblioteca se produce cuando se crea una biblioteca en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué biblioteca en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de operadores

La acción de creación de operadores se produce cuando se crea un operador y definen los enlaces en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué operador en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de operadores

La acción de supresión de operadores se produce cuando se suprime un operador en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué operador en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de modificación de operadores

La acción de modificación de operadores se produce cuando se modifica un operador en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué operador en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de cuerpo del paquete

La acción de creación de cuerpo del paquete se produce cuando se crea un cuerpo del paquete en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario

Información	Nivel
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué cuerpo del paquete en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión del cuerpo del paquete

La supresión del cuerpo del paquete se produce cuando se elimina un cuerpo del paquete en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué cuerpo del paquete en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de modificación del cuerpo del paquete

La acción de modificación del cuerpo del paquete se produce cuando se modifica un cuerpo del paquete en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué cuerpo del paquete en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de paquetes

La acción de creación de paquetes se produce cuando se crea un paquete en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué paquete en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de paquetes

La acción de supresión de paquetes se produce cuando se elimina un paquete en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué paquete en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de modificación de paquetes

La acción de modificación de paquetes se produce cuando se modifica un paquete en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué paquete en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de procedimientos

La creación de procedimientos se produce cuando se crea un procedimiento en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado un procedimiento en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de procedimientos

La acción de supresión de procedimientos se produce cuando se elimina un procedimiento en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido un procedimiento en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de modificación de procedimientos

La acción de modificación de procedimientos se produce cuando se modifica un procedimiento en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado un procedimiento en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de análisis de tabla

La acción de análisis de tabla se produce cuando se inicia un análisis de una tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha iniciado el análisis de qué tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de truncamiento de tabla

La acción de truncamiento de tabla se produce cuando se trunca una tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha truncado qué tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de creación de iniciador

La acción de creación de iniciador se produce cuando se crea un iniciador en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué iniciador en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de iniciador

La acción de supresión de iniciador se produce cuando se elimina un iniciador en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué iniciador en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de desactivación de iniciador

La acción de desactivación de iniciador se produce cuando se desactiva un iniciador en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha desactivado qué iniciador en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de activación de iniciador

La acción de activación de iniciador se produce cuando se activa un iniciador en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha activado qué iniciador en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación del iniciador

La acción de modificación del iniciador se produce cuando se cambia un iniciador en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué iniciador en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de cuerpo del tipo

La acción de creación de cuerpo del tipo se produce cuando un usuario de host de origen de la base de datos crea un cuerpo del tipo.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la creación del cuerpo del tipo por qué usuario y por qué usuario del SO en qué host y en qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión del cuerpo del tipo

La acción de supresión del cuerpo del tipo se produce cuando un usuario de host de origen de la base de datos crea un cuerpo del tipo.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la supresión del cuerpo del tipo por qué usuario y por qué usuario del SO en qué host y en qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de modificación del cuerpo del tipo

La acción de modificación del cuerpo del tipo se produce cuando un usuario de host de la base de datos cambia un cuerpo del tipo.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la modificación del cuerpo del tipo por qué usuario y por qué usuario del SO en qué host y en qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación del tipo

La acción de creación del tipo se produce cuando un usuario de host de origen de la base de datos crea un tipo.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la creación del tipo por qué usuario y por qué usuario del SO en qué host y en qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión del tipo

La acción de supresión del tipo se produce cuando un usuario de host de origen de la base de datos elimina un tipo.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la supresión del tipo por qué usuario y por qué usuario del SO en qué host y en qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de ejecución del tipo

La acción de ejecución del tipo se produce cuando un usuario de host de origen de la base de datos ejecuta un tipo.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la ejecución del tipo por qué usuario y por qué usuario del SO en qué host y en qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación del tipo

La acción de modificación del tipo se produce cuando un usuario de host de origen de la base de datos cambia un tipo.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la modificación del tipo por qué usuario y por qué usuario del SO en qué host y en qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de eliminación de enlace

Esta acción expresa información sobre la eliminación del enlace o los vínculos entre los objetos de la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Clase de eventos de auditoría

Acción de auditoría predeterminada

La acción de auditoría predeterminada se produce cuando se establece la opción de auditoría para realizar el seguimiento de operaciones en una base de datos completa en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es el valor predeterminado de la auditoría establecido por qué usuario en qué host y qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de auditoría no predeterminada

La acción de auditoría no predeterminada evita que más objetos se auditen de forma predeterminada.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la acción de auditoría no predeterminada establecida por qué usuario en qué host y qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de auditoría de objetos

La acción de auditoría de objetos se produce cuando se configura la opción de auditoría para realizar el seguimiento de las operaciones en un objeto de esquema específico en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la auditoría de objetos establecida por qué usuario en qué host y qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desactivación de auditoría de objetos

La acción de desactivación de auditoría de objetos se produce cuando se desactiva la auditoría que se ha activado anteriormente en un objeto de esquema específico en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la desactivación de auditoría de objetos establecida por qué usuario en qué host y qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de grabación de sesión

La acción de grabación de sesión se produce cuando un usuario de la base de datos registra la actividad de la sesión en los datos de seguimiento de auditoría en un host de origen.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué actividad de usuario se ha agregado al seguimiento de auditoría en qué host y qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de auditoría del sistema

La acción de auditoría del sistema se produce cuando un usuario de la base de datos establece la opción de auditoría del host de origen.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la opción de auditoría establecida por qué usuario y por qué usuario del SO en qué host y en qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desactivación de auditoría del sistema

La acción de desactivación de auditoría del sistema se produce cuando un usuario de la base de datos desactiva la auditoría del sistema de un host de origen.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la configuración de la opción de desactivación de la auditoría del sistema por qué usuario y por qué usuario del SO en qué host y en qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de acceso de datos

Acción de copia masiva

Esta acción expresa información sobre la transferencia de datos en bloques en lugar de como registros individuales de diferentes almacenes de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de confirmación

La acción de confirmación se produce cuando finaliza una transacción y se hacen permanentes todos los cambios realizados en la transacción.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué transacción se ha realizado en qué base de datos en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión

La acción de supresión se produce cuando un usuario elimina datos de una tabla en una base de datos de un terminal (host).

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué tabla se ha visto afectada por qué usuario y base de datos en qué host en qué momento. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de inserción

La acción de inserción se produce cuando se inicia una instrucción INSERT en una tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha iniciado una instrucción INSERT en una tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de ejecución de consulta

La acción de ejecución de consulta proporciona información relativa a las consultas de la base de datos.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué consulta se ha establecido en qué base de datos de qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de reversión

La acción de reversión se produce cuando se inicia una reversión para deshacer el trabajo realizado en la transacción actual o deshacer manualmente el trabajo realizado por una transacción dudosa distribuida.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué transacción se ha revertido en qué base de datos en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de punto de retorno

La acción de punto de retorno identifica un punto en una transacción al que se puede revertir más adelante.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué punto de retorno se ha identificado en qué base de datos en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de selección

La acción de selección se produce cuando se inicia una instrucción SELECT en una tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué cuenta ha iniciado una instrucción SELECT en una tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de configuración de transacciones

La acción de configuración de transacciones establece la transacción actual como sólo lectura o sólo escritura, establece su nivel de aislamiento o la asigna a un segmento de reversión específico.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué transacción se ha establecido en qué base de datos en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de truncamiento

Esta acción expresa información sobre el truncamiento de datos en una tabla.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de actualización

La acción de actualización se produce cuando se inicia una instrucción UPDATE en una tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha iniciado una instrucción UPDATE en una tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión de objetos

Acción de creación de conjunto

La acción de creación de conjunto trata la interrupción de un conjunto. Los objetos de base de datos gestionados, como las iniciaciones o procedimientos almacenados, se compilan y, a continuación, se implementan en unidades denominadas conjunto. El comando utilizado es CREATE ASSEMBLY.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de interrupción de conjunto

La acción de interrupción de conjunto trata la interrupción de un conjunto. Los objetos de base de datos gestionados, como las iniciaciones o procedimientos almacenados, se compilan y, a continuación, se implementan en unidades denominadas conjunto. El comando utilizado es DROP ASSEMBLY.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de modificación de conjunto

La acción de modificación de conjunto trata la interrupción de un conjunto. Los objetos de base de datos gestionados, como las iniciaciones o procedimientos almacenados, se compilan y, a continuación, se implementan en unidades denominadas conjunto. El comando utilizado es MODIFY ASSEMBLY.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de archivo de control

La acción de creación de archivo de control se produce cuando crea un archivo de control en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es el archivo de control creado por qué usuario en qué host y en qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	6

Acción de creación de dimensiones

La acción de creación de dimensiones establece una relación primario-secundario entre pares de conjuntos de columnas.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué dimensión en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de dimensiones

La acción de supresión de dimensiones trata la supresión de dimensiones en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué dimensión en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de dimensiones

La acción de modificación de dimensiones se produce cuando se modifica una dimensión en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué dimensión en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de directorios

La acción de creación de directorios se produce cuando cualquier usuario de la base de datos crea un directorio para mantener un objeto de base de datos en una terminal (host) en un momento determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario

Información	Nivel
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es el nombre de directorio con la ruta creada por qué usuario y por qué usuario del SO en qué host y qué base de datos en un momento determinado. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de directorio

La acción de supresión de directorio se produce cuando un usuario determinado de la base de datos suprime un objeto de directorio de un host de origen.

Información	Nivel
Origen - Información de usuario	Primario

Información	Nivel
Origen - Información de host	Secundario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es el nombre de directorio suprimido por qué usuario y qué usuario del SO en qué host y qué base de datos en un momento determinado. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de creación de edición

La acción de creación de edición trata la creación de ediciones. En Oracle, Edition Object se utiliza para almacenar varias versiones de inicio, vistas, sinónimos, etc. en la base de datos. El comando utilizado en Oracle es CREATE EDITION.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de interrupción de edición

La acción de interrupción de edición trata la creación de ediciones. En Oracle, Edition Object se utiliza para almacenar varias versiones de inicio, vistas, sinónimos, etc. en la base de datos. El comando utilizado en Oracle es ALTER EDITION.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de modificación de edición

La acción de modificación de edición trata la creación de ediciones. En Oracle, Edition Object se utiliza para almacenar varias versiones de inicio, vistas, sinónimos, etc. en la base de datos. El comando utilizado en Oracle es ALTER EDITION.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de actualización de todos los índices

La acción de actualización de todos los índices actualiza todos los índices asociados a una tabla o vista en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha actualizado los índices en qué base de datos en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de índices

La acción de creación de índices se produce cuando se crea un índice en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado un índice en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de índices

La acción de supresión de índices se produce cuando se suprime un índice en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido un índice en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de modificación de índices

La acción de modificación de índices se produce cuando se modifica un índice en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado un índice en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de validación de índices

La acción de validación de índices se produce cuando se valida un índice en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha iniciado una validación de los índices en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de tipo de índice

La creación de tipo de índice se produce cuando se crea un tipo de índice en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué tipo de índice en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de tipo de índice

La acción de supresión de tipo de índice se produce cuando se suprime un tipo de índice en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué tipo de índice en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de creación de objeto Java

La acción de creación de objeto Java se produce cuando se crea un objeto de esquema que contiene un recurso, clase u origen Java.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué objeto de esquema en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de objeto Java

La acción de supresión de objeto Java se produce cuando se elimina un objeto de esquema que contiene un recurso, clase u origen Java.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué objeto de esquema en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de modificación de objeto Java

La acción de modificación de Java se produce cuando se modifica un objeto de esquema que contiene un recurso, clase u origen Java.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué objeto de esquema en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de bloqueo

La acción de bloqueo se produce cuando se inicia una instrucción LOCK en un objeto en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué cuenta ha iniciado una instrucción LOCK en qué objeto en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de vista materializada

La acción de creación de vista materializada se produce cuando se crea una vista materializada en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué vista materializada en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de vista materializada

La acción de supresión de vista materializada se produce cuando se suprime una vista materializada en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué vista materializada en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de modificación de vista materializada

La acción de modificación de vista materializada se produce cuando se modifica una vista materializada en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué vista materializada en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de creación de registro de vista materializada

La acción de creación de registro de vista materializada se produce cuando se crea un registro de vista materializada en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué registro de vista materializada en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de registro de vista materializada

La acción de supresión de registro de vista materializada se produce cuando se suprime un registro de vista materializada en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué registro de vista materializada en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de modificación de registro de vista materializada

La acción de modificación de registro de vista materializada se produce cuando se modifica un registro de vista materializada en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué registro de vista materializada en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de falta de funcionamiento

La acción de falta de funcionamiento se produce cuando las cláusulas y procedimientos se ejecutan sin que se produzca ningún error pero no surten efecto.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cláusula o procedimiento se ha ejecutado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de restauración de objetos

La acción de restauración de objetos restablece un objeto que se ha marcado para la supresión en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha restablecido qué objeto en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de esquema

La acción de creación de esquema se produce cuando un usuario de host de origen de la base de datos crea un esquema.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario ha creado qué esquema en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de esquema

La acción de creación de esquema se produce cuando un usuario de host de origen suprime un esquema de la base de datos.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario ha suprimido qué esquema en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de esquema

La acción de modificación de esquema se produce cuando un usuario de host de origen modifica un esquema de la base de datos.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario ha modificado qué esquema en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de sinónimo público

La acción de creación de sinónimo público se produce cuando se crea un sinónimo público en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado un sinónimo público en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de sinónimo público

La acción de supresión de sinónimo público se produce cuando se suprime un sinónimo público en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido un sinónimo público en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de modificación de nombre

La acción de modificación de nombre se produce cuando se cambia el nombre de un objeto en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado el nombre de qué objeto en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Source_objectname es el nombre original del objeto y dest_objectname es el nuevo nombre del objeto.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de modificación de costes de recursos

La acción de modificación de costes de recursos se produce cuando se definen costes de recursos que usa el comando de creación de perfiles.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado un coste de recurso en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de creación de reglas

Esta acción expresa información acerca de la creación de reglas que se pueden aplicar a los objetos de la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de modificación de regla

Esta acción expresa información acerca de la modificación de reglas que se pueden aplicar a los objetos de la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de supresión de reglas

Esta acción expresa información acerca de la supresión de reglas que se pueden aplicar a los objetos de la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de creación de esquema

La acción de creación de esquema se produce cuando se crean varias tablas y vistas y se realizan varias concesiones en una única transacción en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué esquema en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de secuencias

La acción de creación de secuencias se produce cuando se crea una secuencia en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado una secuencia en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de secuencias

La acción de supresión de secuencias se produce cuando se elimina una secuencia en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido una secuencia en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de modificación de secuencias

La acción de modificación de secuencias se produce cuando se modifica una secuencia en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué secuencia en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de asociación de estadísticas

La acción de asociación de estadísticas vincula un tipo de estadística que contiene funciones relativas al coste, selectividad y recopilación de estadísticas con una o más columnas, funciones independientes, paquetes, tipos, índices de dominio o tipos de índice.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha asociado qué tipo de estadísticas en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desasociación de estadísticas

La acción de desasociación de estadísticas cancela la asociación un tipo de estadísticas de una o más columnas, funciones independientes, paquetes, tipos, índices de dominio o tipos de índices.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha cancelado la asociación de qué tipo de estadísticas en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de resumen

La acción de modificación de resumen se produce cuando se modifica un resumen en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado un resumen en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de sinónimo

La acción de creación de sinónimo público se produce cuando se crea un sinónimo en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado un sinónimo en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de supresión de sinónimo

La acción de supresión de sinónimo se produce cuando se suprime un sinónimo en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido un sinónimo en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de comprobación de tabla

La acción de comprobación de tabla proporciona información relativa a la comprobación de una o varias tablas con el objetivo de identificar posibles errores.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de tabla

La acción de creación de tabla se produce cuando se crea una tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de tabla

La acción de creación de tabla se produce cuando se elimina una tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de vaciado de tabla

La acción de vaciado de tabla proporciona información relativa a la eliminación de todos los resultados de consultas de la memoria caché de consultas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de tabla

La acción de creación de tabla se produce cuando se modifica una tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de optimización de tabla

La acción de optimización de tabla proporciona información relativa a la eliminación de todos los resultados de consultas de la memoria caché de consultas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de purga de tabla

La acción de purga de tabla elimina una tabla de la papelera de reciclaje y libera todo el espacio asociado a la tabla.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha purgado qué tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de modificación de nombre de tabla

La acción de modificación de nombre de tabla se produce cuando se modifica el nombre de una tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado el nombre de qué tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Source_objectname es el nombre original de la tabla y dest_objectname es el nuevo nombre de la tabla.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de reparación de tabla

La acción de reparación de tabla se produce cuando se repara una tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha reparado qué tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desbloqueo de tabla

La acción de desbloqueo de tabla proporciona información relativa al desbloqueo de un objeto bloqueado con anterioridad como parte de una transacción.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de vista

La acción de creación de vista se produce cuando se crea una vista en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué vista en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de vista

La acción de modificación de vista se produce cuando se modifica una vista en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué vista en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de vista

La acción de supresión de vista se produce cuando se suprime una vista en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué vista en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Clase de gestión del mismo nivel

Acción de creación de vínculo de base de datos

La acción de creación de vínculo de base de datos se produce cuando se crea un vínculo de base de datos entre dos bases de datos.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado un vínculo de qué base de datos a qué base de datos en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2

Resultado	event_result	event_severity
Incorrecto	F	3

Acción de supresión de vínculo de base de datos

La acción de supresión de vínculo de base de datos se produce cuando se suprime un vínculo de base de datos entre dos bases de datos.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido un vínculo de qué base de datos a qué base de datos en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Clase de gestión de privilegios

Acción de supresión de biblioteca

La acción de supresión de biblioteca se produce cuando se suprime una biblioteca en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué biblioteca en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de denegación de objeto

La acción de denegación de objeto se produce cuando se deniega el acceso a un objeto en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de concesión de objeto

La acción de concesión de objeto se produce cuando se conceden derechos a un objeto en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha concedido qué derechos de cuenta a qué objeto en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de revocación de objeto

La acción de revocación de objeto se produce cuando se revocan derechos en un objeto en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha revocado qué derechos de cuenta a qué objeto en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de perfiles

La acción de creación de perfil se produce cuando se crea un perfil en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado un perfil en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de perfiles

La acción de supresión de perfiles se produce cuando se elimina un perfil en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué perfil se ha suprimido en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de modificación de perfiles

La acción de modificación de perfiles se produce cuando se modifica un perfil en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado un perfil en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de revocación de funciones

La acción de revocación de funciones se produce cuando se revoca una función.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de denegación de instrucciones

La acción de denegación de instrucciones trata la denegación de instrucciones.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de concesión de instrucciones

La acción de concesión de instrucciones trata la concesión de instrucciones.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de revocación de instrucciones

La acción de revocación de instrucciones trata la revocación de instrucciones.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de utilización de aplicaciones y servicios

Acción de ejecución de método

La ejecución de método se produce cuando se ejecuta un método en un sistema o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha ejecutado qué método en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de ejecución de procedimiento

La acción de ejecución de procedimiento se produce cuando se ejecuta un procedimiento en un sistema o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha ejecutado qué procedimiento en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de ejecución de iniciador

La acción de ejecución de iniciador expresa información acerca de la ejecución de un activador que se define para una tabla o una columna.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Clase de actividad del sistema

Acción de alerta de base de datos

La acción de alerta de base de datos se produce cuando se envían alertas relativas a la base de datos o a DBMS.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6

Acción de notificación de base de datos

La acción de notificación de base de datos se produce cuando se envían notificaciones relativas a la base de datos o a DBMS.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de base de datos

La acción de operación de base de datos proporciona información acerca de las operaciones generales relativas a la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de base de datos

La acción de estado de base de datos proporciona información sobre el estado general de las bases de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de base de datos

La acción de advertencia de base de datos se produce cuando se envían advertencias de la base de datos. Esta acción tiene un carácter menos grave que la acción de error de base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué advertencia se ha producido en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4

Clase de gestión del sistema

Acción de análisis de clúster

La acción de análisis de clúster se produce cuando se analiza un clúster.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha analizado qué clúster en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de copia de seguridad de base de datos

La acción de copia de seguridad de base de datos se produce cuando se realiza una copia de seguridad de una base de datos en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha realizado la copia de seguridad de qué base de datos en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de alerta de copia de seguridad de base de datos

La acción de alerta de copia de seguridad de base de datos proporciona información relativa a las condiciones de alerta generadas durante la realización de la copia de seguridad de la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	6

Acción de error de copia de seguridad de base de datos

La acción de error de copia de seguridad de base de datos proporciona información relativa a las condiciones de error generadas durante la realización de la copia de seguridad de la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de notificación de copia de seguridad de base de datos

La acción de notificación de copia de seguridad de base de datos proporciona información relativa a las notificaciones y los mensajes generados durante la realización de la copia de seguridad de la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de copia de seguridad de base de datos

La acción de estado de copia de seguridad de base de datos proporciona información relativa al estado de la copia de seguridad de la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de copia de seguridad de base de datos

La acción de advertencia de copia de seguridad de base de datos proporciona información relativa a las advertencias generadas durante la realización de la copia de seguridad de la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de comprobación de base de datos

Esta acción expresa información acerca de la comprobación de una base de datos para asegurarse de la integridad lógica y física de todos los objetos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de creación de clúster

La acción de creación de clúster se produce cuando se crea un clúster.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué clúster en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de clúster

La acción de supresión de clúster se produce cuando se suprime un clúster.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué clúster en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desactivación de base de datos

Esta acción expresa información acerca de la desactivación de una base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de activación de base de datos

Esta acción expresa información acerca de la activación de una base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de modificación de clúster

La acción de modificación de clúster se produce cuando se modifica el clúster.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué clúster en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de inicio de duplicación de base de datos

La acción de inicio de duplicación de base de datos expresa información acerca del inicio de la duplicación de la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de detención de duplicación de base de datos

La acción de detención de duplicación de base de datos expresa información acerca de la detención de la duplicación de la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de montaje de base de datos

Esta acción expresa información acerca del montaje de una base de datos a partir de un conjunto de archivos de dispositivos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de creación de base de datos

La acción de creación de base de datos se produce cuando se crea una base de datos en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado una base de datos en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de base de datos

La acción de supresión de base de datos se produce cuando se suprime una base de datos en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido una base de datos en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción Flashback de base de datos

La acción Flashback de base de datos se produce cuando se recupera el estado de una base de datos a un punto anterior.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha recuperado una base de datos en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de modificación de base de datos

La acción de modificación de base de datos se produce cuando se modifica una base de datos en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado una base de datos en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de conciliación de base de datos

La acción de conciliación de base de datos proporciona información relativa a la conciliación de los datos incluidos en las bases de datos con los datos procedentes de componentes externos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de liberación de base de datos

Esta acción expresa información acerca de la liberación de una base de datos una vez que se han suspendido sus operaciones.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de restauración de base de datos

La acción de restauración de base de datos se produce cuando se restaura una base de datos en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha restaurado una base de datos en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Nuevo tema (19)

La acción de instantánea de base de datos se produce cuando se toma una instantánea en un host determinado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha tomado una instantánea en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de suspensión de base de datos

Esta acción expresa información acerca de las operaciones de suspensión que realizan en una base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de replicación de base de datos

La acción de replicación de base de datos proporciona información relativa a la replicación de bases de datos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de truncamiento de clúster

La acción de truncamiento de clúster se produce cuando se trunca un clúster.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha truncado qué clúster en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desmontaje de base de datos

Esta acción expresa información acerca del desmontaje de una base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de explicación

La acción de explicación se produce cuando se describe cada paso de un plan de ejecución.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha ejecutado la explicación en qué objeto en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción Flashback

La acción Flashback se produce cuando se recupera un estado anterior de un objeto.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha recuperado qué objeto en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de archivos Flashback

La acción de creación de archivos Flashback trata la creación de archivos Flashback. Un archivo de datos Flashback proporciona la capacidad de realizar el seguimiento y almacenar todos los cambios transaccionales en una tabla durante su duración. El comando utilizado es CREATE FLASHBACK ARCHIVE.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de interrupción de archivos Flashback

La acción de interrupción de archivos Flashback trata la creación de archivos Flashback. Un archivo de datos Flashback proporciona la capacidad de realizar el seguimiento y almacenar todos los cambios transaccionales en una tabla durante su duración. El comando utilizado es DROP FLASHBACK ARCHIVE.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de archivos Flashback

La acción de modificación de archivos Flashback trata la creación de archivos Flashback. Un archivo de datos Flashback proporciona la capacidad de realizar el seguimiento y almacenar todos los cambios transaccionales en una tabla durante su duración. El comando utilizado es MODIFY FLASHBACK ARCHIVE.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de purga de la papelera de reciclaje

La acción de purga de la papelera de reciclaje se produce cuando se eliminan los datos de la papelera de reciclaje de un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha purgado la papelera de reciclaje en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación del segmento de reversión

La creación del segmento de reversión se produce cuando se crea un segmento de reversión en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué segmento de reversión en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión del segmento de reversión

La acción de supresión del segmento de reversión se produce cuando se suprime un segmento de reversión en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué segmento de reversión en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación del segmento de reversión

La acción de modificación del segmento de reversión se produce cuando se modifica un segmento de reversión en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué segmento de reversión en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de concesión del sistema

La acción de concesión del sistema se produce con el problema de la opción de concesión de nivel del sistema de un host de origen realizada por un usuario de la base de datos.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la concesión de sistema establecida por qué usuario y por qué usuario del SO en qué host y qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación del sistema

La acción de modificación del sistema se produce con el problema de instrucción ALTER SYSTEM de un host de origen realizada por un usuario de la base de datos.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la modificación del sistema por qué usuario y por qué usuario del SO en qué host y en qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de revocación del sistema

La acción de revocación del sistema se produce cuando se revocan privilegios del sistema como DBA, Crear sesión, etc. por un usuario de host de la base de datos.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la revocación del privilegio del sistema por qué usuario y por qué usuario del SO en qué host y en qué base de datos. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de actualización de tablas del sistema

Esta acción expresa información acerca de la actualización de la tabla del sistema cuando se modifican los metadatos o la infraestructura del sistema de la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción Flashback de tabla

La acción Flashback de tabla se produce cuando se recupera una tabla a un punto anterior.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha recuperado qué tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de espacio de tabla

La creación de espacio de tabla se produce cuando se crea un espacio de tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado un espacio de tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de espacio de tabla

La acción de supresión de espacio de tabla se produce cuando se elimina un espacio de tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido un espacio de tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de modificación de espacio de tabla

La acción de modificación de espacio de tabla se produce cuando se modifica un espacio de tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado un espacio de tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de purga de espacio de tabla

La acción de purga de espacio de tabla se produce cuando un espacio de tabla elimina objetos de la papelera de reciclaje.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha purgado qué objetos de espacio de tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de copia de seguridad del registro de transacción

La acción de copia de seguridad del registro de transacción expresa información acerca de la copia de seguridad de un registro de transacción de la base de datos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de desactivación de todos los iniciadores

La acción de desactivación de todos los iniciadores se produce cuando se desactivan todos los iniciadores en una tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha desactivado todos los iniciadores en qué tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de activación de todos los iniciadores

La acción de activación de todos los iniciadores se produce cuando se activan todos los iniciadores en una tabla en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha activado todos los iniciadores en qué tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de ejecución de instrucción de transacción

La acción de ejecución de instrucción de transacción se produce cuando se ejecuta una instrucción de transacción.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha purgado qué objetos de espacio de tabla en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Capítulo 6: Categoría de seguridad de host

Esta sección contiene los siguientes temas:

Clase de actividad de antivirus (en la página 325)
Acción de denegación del servicio (en la página 361)
Clase de seguridad de aplicaciones (en la página 363)
Clase de actividad de cifrado (en la página 367)
Clase de actividad de infracción de firmas (en la página 393)
Kernel y actividad del sistema operativo (en la página 397)
Gestión de notificaciones (en la página 417)
Clase de actividad de red (en la página 418)
Clase de actividad sospechosa (en la página 428)

Clase de actividad de antivirus

Acción del estado del antivirus

La acción del estado del antivirus gestiona la expresión de la información del evento relativa al estado del sistema de antivirus o del software de un sistema.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de bloqueo de archivo

La acción de bloqueo de archivo se produce cuando se detecta un archivo bloqueado por un antivirus en un host determinado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

La información importante para esta acción es qué archivo se ha bloqueado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2

Acción de exclusión de archivo

La acción de exclusión de archivo se produce cuando se excluye un archivo del proceso de análisis en un host determinado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

La información importante de esta acción es qué archivo se ha excluido del análisis en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de archivos

La acción de supresión de archivos se produce cuando se elimina un archivo infectado en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de archivos

La acción de supresión de archivos sirve para eliminar archivos con virus o software maligno.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de nombre de archivo

La acción de modificación de nombre de archivo se produce cuando se cambia el nombre de un archivo infectado en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado el nombre de qué archivo en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Source_objectname es el nombre original del objeto y dest_objectname es el nuevo nombre del objeto.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de alerta de exploración

La acción de alerta de exploración proporciona información relativa a condiciones de alerta relacionadas con la exploración.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	7

Acción de omisión de exploración

La acción de omisión de exploración proporciona información relativa a la omisión de una exploración.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de error de análisis

La acción de error de análisis se produce cuando se detecta un error del que se informa durante un análisis del antivirus en un host determinado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué antivirus ha informado del error en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6

Acción de notificación de exploración

La acción de notificación de exploración proporciona información relativa a las notificaciones y los mensajes generados en una exploración.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de exploración

La acción de operación de exploración proporciona información general acerca de las operaciones relativas a la exploración.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de informe de análisis

La acción de informe de análisis se produce cuando se detecta información de resumen que proporciona el análisis del antivirus en un host determinado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué antivirus proporciona la información de resumen de análisis en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2

Acción de estado de exploración

La acción de estado de exploración proporciona información general acerca del estado de las exploraciones.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de exploración

Se puede asignar a la acción de advertencia de exploración cualquier tipo de advertencia relativa a una exploración. Los eventos más graves deberán asignarse a la acción de error de exploración.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de eliminación de virus

La acción de eliminación de virus trata la resolución de acción de supresión en relación con la identificación de un virus en un host determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	*Primario*

Información	Nivel
Destino - Información de proceso	*Primario*
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué proceso o archivo ha intentado eliminar el virus en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

El nombre del virus debe almacenarse en el campo result_signature de la Gramática de eventos comunes.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	6

Acción de virus detectado

La acción de virus detectado se produce cuando se detecta un virus conocido en un host determinado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es en qué proceso o archivo se ha detectado el virus en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

El nombre del virus debe almacenarse en el campo result_signature de la Gramática de eventos comunes.

Resultado	event_result	event_severity
Correcto	S	6

Acción de actualización de motor de virus

La acción de actualización de motor de virus se produce cuando se actualiza un motor de virus en un host determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué motor se ha actualizado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	5

Acción de alerta de motor de virus

La acción de alerta de motor de virus proporciona información sobre las condiciones de alerta relacionadas con el motor de virus.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	6

Acción de error de motor de virus

La acción de error de motor de virus proporciona información acerca de las condiciones de error relacionadas con el motor de virus.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de notificación de motor de virus

En caso de que no sea posible asignar el evento a una acción más específica, la acción de error de motor de virus podrá mostrar cualquier tipo de notificación. Utilice la acción de estado de motor de virus si el evento describe el estado del motor de virus.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de motor de virus

La acción de operación de motor de virus puede mostrar cualquier evento registrado como parte de las funciones u operaciones normales del motor de virus. Cuando no sea posible asignar un evento a una acción más específica de la gramática de eventos comunes, se recomienda asignar el evento a esta acción.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de reversión de motor de virus

La acción de reversión de motor de virus proporciona información sobre la recuperación de una versión anterior del motor de virus.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de estado de motor de virus

La acción de estado de motor de virus proporciona información relativa al estado del motor de virus.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de motor de virus

La acción de advertencia de motor de virus proporciona información sobre las advertencias relacionadas con el motor de virus.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de cuarentena de virus

La acción de cuarentena de virus trata la resolución de acción de cuarentena en relación con la identificación de un virus en un host determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	**Nivel**
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	*Primario*
Destino - Información de proceso	*Primario*
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué proceso o archivo se encuentra en cuarentena debido a la detección de qué virus en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

El nombre del virus debe almacenarse en el campo result_signature de la Gramática de eventos comunes.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	6

Acción de exploración de virus iniciada

La acción de exploración de virus iniciada se produce cuando se inicia el análisis de virus en un host determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué análisis de virus se ha iniciado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de detención de exploración de virus

La acción de detención de exploración de virus proporciona información relativa a la detención de una exploración de virus en un host determinado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de exploración de virus completada

La acción de exploración de virus completada se produce cuando se completa el análisis de virus en un host determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué análisis de virus se ha completado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de exploración de virus pausada

La acción de exploración de virus pausada se produce cuando se pausa el análisis de virus en un host determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué análisis de virus se ha pausado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de exploración de virus reanudada

La acción de exploración de virus reanudada se produce cuando se reanuda el análisis de virus en un host determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Secundario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué análisis de virus se ha reanudado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de actualización de firmas de virus

La actualización de firmas de virus se produce cuando se actualizan las firmas de virus en un host determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué base de datos de firmas de virus se ha actualizado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	4

Acción de instalación de antivirus

La acción de instalación de antivirus se produce cuando se instala una aplicación de antivirus en un host determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué aplicación de antivirus está instalada en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de cliente de antivirus eliminado

La acción de cliente de antivirus eliminado se produce cuando se elimina un software de cliente de aplicación de antivirus en un host determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido un cliente de antivirus en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	4

Acción de desinstalación de antivirus

La acción de desinstalación de antivirus se produce cuando se desinstala una aplicación de antivirus en un host determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha desinstalado una aplicación de antivirus en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	4

Acción de denegación del servicio

Acción de ataque de desbordamiento del búfer

La acción de ataque de desbordamiento del búfer gestiona la información del evento relativa a la detección del ataque de desbordamiento del búfer.

Si el ataque *no* conduce a una denegación del servicio, se asigna a la misma acción en la categoría de host de seguridad y de clase de seguridad de la aplicación. Si el evento se encuentra en el contexto de un entorno de red, se asigna a la misma acción en la categoría de seguridad de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Acción de ataque de denegación del servicio

La acción de ataque de denegación del servicio gestiona la expresión de la información del evento relativa a las vulnerabilidades de seguridad genéricas que dan lugar a la denegación del servicio.

El usuario puede asignarlo a una acción correspondiente específica en la clase de denegación del servicio si conoce la causa raíz del ataque de denegación del servicio.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Clase de seguridad de aplicaciones

Acción de ataque de desbordamiento del búfer

La acción de ataque de desbordamiento del búfer informa acerca de la detección de ataques de desbordamiento del búfer en el sistema host.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6

Información	Nivel	
Error	F	5

Acción de ataque de cadena de formato

La acción de ataque de cadena de formato gestiona la expresión de la información del evento relativa a la vulneración de la seguridad de entradas de usuario sin filtrar, como el parámetro de cadena de formato en ciertas funciones de formato.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5
Error	F	4

Acción de pérdida de memoria

La acción de pérdida de memoria gestiona la expresión de la información del evento relativa a una aplicación o sistema que no publica memoria adjudicada, por lo que se reduce la memoria disponible.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Acción de ataque de XML

La acción de ataque de XML gestiona la expresión de la información del evento relativa a cualquier acción de ataque que vulnere la seguridad en la tecnología XML.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Clase de actividad de cifrado

Acción alerta de cifrado

La acción de alerta de cifrado gestiona la expresión de la información acerca de las condiciones de alerta relacionadas con las operaciones o los sistemas de cifrado en un entorno de host específico.

A esta acción, se le puede asignar cualquier tipo de alerta relativa a las operaciones o sistemas de cifrado. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de cifrado. Si la acción está relacionada con el entorno de red, deberá asignarse al mismo evento bajo la categoría de seguridad de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D

Resultado	event_result	event_severity
Error	F	6

Acción de error de cifrado

La acción de error de cifrado gestiona la expresión de la información acerca de las condiciones de error relacionadas con las operaciones o los sistemas de cifrado en un entorno de host específico.

A esta acción, se le puede asignar cualquier tipo de error relativo a las operaciones o sistemas de cifrado. Los eventos de menor severidad deben asignarse a las operaciones de cifrado o las acciones de advertencia de los sistemas de cifrado. Los eventos de mayor severidad que requieran atención inmediata deberán asignarse a la acción de alerta de cifrado. Si la acción está relacionada con el entorno de red, deberá asignarse al mismo evento bajo la categoría de seguridad de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	5

Acción de notificación de cifrado

La acción de notificación de cifrado gestiona la expresión de la información relativa a las notificaciones y mensajes generados de operaciones o sistemas de cifrado en un entorno de host específico.

En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar cualquier tipo de notificación de operaciones o sistemas de cifrado. Si el evento describe el estado de las operaciones o los sistemas de cifrado, deberá utilizarse la acción de estado del cifrado. Si la acción está relacionada con el entorno de red, deberá asignarse al mismo evento bajo la categoría de seguridad de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de operación de cifrado

La acción de operación de cifrado gestiona la expresión de la información relativa a las operaciones generales referidas al funcionamiento de los sistemas de cifrado en un entorno de host específico.

Cuando un evento se registra como parte de la función normal de las operaciones o de los sistemas de cifrado, o si el evento no se puede asignar a una acción de la gramática de eventos comunes más específica, se recomienda asignar el evento a esta acción. Si la acción está relacionada con el entorno de red, deberá asignarse al mismo evento bajo la categoría de seguridad de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de estado del cifrado

La acción de estado del cifrado gestiona la expresión de la información relativa al estado de las operaciones o los sistemas de cifrado en un entorno de host específico.

Cuando un evento se registra como parte de la función normal de las operaciones o de los sistemas de cifrado, o si el evento no se puede asignar a una acción de la gramática de eventos comunes más específica, se recomienda asignar el evento a esta acción. Si la acción está relacionada con el entorno de red, deberá asignarse al mismo evento bajo la categoría de seguridad de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de advertencia de cifrado

La acción de alerta de cifrado gestiona la expresión de la información relativa a las advertencias relacionadas con las operaciones o los sistemas de cifrado en un entorno de host específico.

A esta acción, se le puede asignar cualquier tipo de advertencia relativa a las operaciones o a los sistemas de cifrado. Los eventos de mayor severidad deberán asignarse a la acción de error de cifrado. Si la acción está relacionada con el entorno de red, deberá asignarse al mismo evento bajo la categoría de seguridad de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	4

Acción de operación de descifrado

La acción de operación de descifrado gestiona la expresión de la información relativa a las operaciones generales relacionadas con el descifrado en un host.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de estado del descifrado

La acción de estado del descifrado gestiona la expresión de la información relativa al estado de la actividad de descifrado en un host.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de alerta de cifrado

La acción de alerta de cifrado contiene información acerca de las condiciones de alerta relativas al cifrado de un host.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de error de cifrado

La acción de error de cifrado contiene información sobre las condiciones de error relativas al cifrado de un host.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de notificación de cifrado

La acción de notificación de cifrado contiene información relativa a las notificaciones generadas por un motor de cifrado de un host.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de cifrado

La acción de operación de cifrado contiene información relativa a las actividades generales relacionadas con el cifrado de un host.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de inicio de cifrado

La acción de inicio de cifrado contiene información relativa al inicio de una operación de cifrado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de cifrado

La acción de advertencia de cifrado contiene información relativa a las notificaciones y los mensajes procedentes del motor de cifrado de un host.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	3

Acción de estado de cifrado

La acción de estado de cifrado contiene información relativa al estado de las actividades de cifrado de un host.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de adición de clave

Actividad de adición de clave relacionada con el cifrado y autenticación del host.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué clave de autenticación se agrega en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de alerta de clave

La acción de alerta de clave contiene información sobre las condiciones de alerta de cifrado relativas a la clave.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de supresión de clave

Esta acción expresa información acerca de la supresión de una clave cifrada.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de error de clave

La acción de error de clave contiene información acerca de las condiciones de error de cifrado relativas a la clave.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de generación de clave

Actividad de generación de clave relacionada con el cifrado y autenticación del host.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué clave de autenticación se genera en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de clave

Esta acción expresa información acerca de la modificación de una clave cifrada.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de notificación de clave

La acción de notificación de clave contiene información relativa a los mensajes o las notificaciones generados por el mecanismo de creación de claves de cifrado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de clave

La acción de operación de clave contiene información general relativa a las claves de cifrado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de uso compartido de clave

La acción de uso compartido de clave contiene información relativa al uso compartido o la sincronización de claves entre sistemas.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué claves se comparten en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de clave

La acción de estado de clave contiene información relativa al estado de las claves de cifrado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de clave

La acción de advertencia de clave contiene información acerca de las advertencias de cifrado relativas a la clave.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	3

Clase de actividad de infracción de firmas

Acción de vulnerabilidad de seguridad de kernel

La acción de vulnerabilidad de seguridad de kernel proporciona información acerca de la detección de una vulnerabilidad de seguridad que ponga en peligro o afecte un kernel.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5
Error	F	4

Acción de infracción de firmas

La acción de infracción de firmas trata la expresión de información del evento relativa a la detección de una infracción de un motor de detección basado en firmas en un host determinado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2

Acción de modificación de registro de Windows

La acción de modificación de registro de Windows trata la expresión de información del evento relativa a la modificación del registro de Windows. Las modificaciones incluyen la adición, supresión y modificación de claves y valores.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de actividad de daemon/servicio sospechosa

Las acciones de actividad de daemon/servicio sospechosas son información del evento relacionada con la detección de actividad de servicio o daemon sospechosa.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Kernel y actividad del sistema operativo

Acción de error de volcado del núcleo

La acción de error de volcado del núcleo gestiona la expresión de la información relativa a los errores relacionados con la actividad de volcado del núcleo.

Si el ataque *no* conduce a una denegación del servicio, se asigna a la misma acción en la categoría de host de seguridad y de clase de seguridad de la aplicación. Si el evento se encuentra en el contexto de un entorno de red, se asigna a la misma acción en la categoría de seguridad de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	5

Acción de inicio de volcado de memoria

La acción de inicio de volcado de memoria gestiona la expresión de la información del evento relativa al inicio del proceso de volcado de memoria.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de modificación del kernel

La acción de modificación del kernel informa acerca de la modificación de un kernel de sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de notificación de kernel

La acción de notificación de kernel proporciona información acerca de las notificaciones y mensajes desde un kernel del sistema. En el caso de que no se pueda asignar el evento a una acción más específica, el usuario podrá asignar cualquier tipo de notificación de kernel a esta acción. Utilice la acción de estado del kernel si el evento describe el estado de un directorio.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Información	Nivel	
Error	F	3

Acción de operación de kernel

La acción de operación de Kernel proporciona información general sobre operaciones de kernel del sistema. Cuando se desee registrar las funciones normales de kernel, o cuando no se pueda asignar el evento a una acción más específica de la gramática de eventos comunes, se recomienda asignar el evento a esta acción.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de estado del kernel

La acción estado del kernel proporciona información general sobre los estados del kernel del sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de advertencia de kernel

La acción de advertencia de kernel proporciona información acerca de las advertencias relacionadas con el kernel del sistema. El usuario puede asignar cualquier tipo de advertencia sobre el kernel a esta acción. Los eventos más graves deberán asignarse a la acción de error del kernel.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	5

Acción de vulnerabilidad de seguridad de Linux

La acción de vulnerabilidad de seguridad de Linux gestiona la expresión de la información del evento relativa a las vulnerabilidades de seguridad o ataques en el sistema operativo Linux.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Acción de acceso a la memoria

La acción de acceso a la memoria proporciona información acerca del acceso a la memoria a través de un proceso.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de adjudicación de memoria

La acción de adjudicación de memoria gestiona la expresión de la información del evento relativa a la adjudicación de memoria a un proceso de un sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de error de paridad de la memoria

La acción de error de paridad de la memoria gestiona la expresión de la información del evento relativa a los errores de paridad en la memoria.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	5

Acción de alerta de llamada de sistema

La acción de alerta de llamada de sistema informa acerca de las alertas relacionadas con las llamadas de sistema. Una llamada de sistema es una solicitud realizada por cualquier programa al sistema operativo que lleva a cabo las tareas. Las llamadas de sistema proporcionan la interfaz entre un proceso y el sistema operativo. El usuario puede asignar cualquier tipo de alerta sobre las llamadas del sistema a esta acción. Se puede asignar una condición de error que no garantiza la atención inmediata a la acción de de error de llamada de sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	6

Acción de error de llamada de sistema

La acción de error de llamada de sistema informa acerca de los errores relacionados con las llamadas de sistema. Una llamada de sistema es una solicitud realizada por cualquier programa al sistema operativo que lleva a cabo las tareas. Las llamadas de sistema proporcionan la interfaz entre un proceso y el sistema operativo. El usuario puede asignar cualquier tipo de error de llamada de sistema a esta acción. Los eventos menos graves deberán asignarse a la acción de advertencia de llamada de sistema. Se pueden asignar eventos más severos que garanticen la acción inmediata para la acción de alerta de llamada de sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	5

Acción de ejecución de llamada de sistema

La acción de ejecución de llamada de sistema informa acerca de la ejecución de una llamada de sistema. Una llamada de sistema es una solicitud realizada por cualquier programa al sistema operativo que lleva a cabo las tareas. Las llamadas de sistema proporcionan la interfaz entre un proceso y el sistema operativo.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de notificación de llamada de sistema

La acción de notificación de llamada de sistema proporciona información sobre las notificaciones y los mensajes generados por una llamada de sistema. Una llamada de sistema es una solicitud realizada por cualquier programa al sistema operativo que lleva a cabo las tareas. Las llamadas de sistema proporcionan la interfaz entre un proceso y el sistema operativo. En el caso de que no se pueda asignar el evento a una acción más específica, el usuario podrá asignar cualquier tipo de notificación llamada de sistema a esta acción. Utilice la acción de estado de llamada de sistema si el evento describe el estado de una llamada de sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de operación de llamada de sistema

La acción de operación de llamada de sistema informa acerca de las operaciones de llamada del sistema. Una llamada de sistema es una solicitud realizada por cualquier programa al sistema operativo que lleva a cabo las tareas. Las llamadas de sistema proporcionan la interfaz entre un proceso y el sistema operativo. Cuando se registra un evento como parte de las funciones normales de una llamada de sistema o cuando no se puede asignar el evento a una acción más específica de la gramática de eventos comunes, se recomienda asignar el evento a esta acción.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de estado de llamada de sistema

La acción de estado de llamada de sistema proporciona información acerca del estado de las llamadas de sistema. Una llamada de sistema es una solicitud realizada por cualquier programa al sistema operativo que lleva a cabo las tareas. Las llamadas de sistema proporcionan la interfaz entre un proceso y el sistema operativo. En el caso de que no se pueda asignar el evento a una acción más específica, el usuario podrá asignar cualquier tipo de mensaje sobre el estado de la llamada de sistema a esta acción.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de advertencia de llamada de sistema

La acción de advertencia de llamada de sistema informa acerca de las advertencias relacionadas con la llamada de sistema. Una llamada de sistema es una solicitud realizada por cualquier programa al sistema operativo que lleva a cabo las tareas. Las llamadas de sistema proporcionan la interfaz entre un proceso y el sistema operativo. El usuario puede asignar cualquier tipo de advertencia de llamada de sistema a esta acción. Los eventos más graves deberán asignarse a la acción de error de llamada de sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	4

Gestión de notificaciones

Difusión de mensajes

Cualquier tipo de difusión del mensaje (de un usuario a varios sistemas; entre dispositivos de red).

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de actividad de red

Paquete de red entrante

Un paquete de red entrante genérico.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Paquete de red saliente

Un paquete de red saliente genérico.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de alerta de puerto

Condiciones de alerta relativas a un puerto.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	6

Acción de cierre de puerto

Actividad relacionada con el cierre del puerto.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de error de puerto

Condiciones de error relativas a un puerto. Los eventos menos graves deberán asignarse a la acción de advertencia de puerto. Los eventos más graves que necesiten atención inmediata deberán asignarse a la acción de alerta de puerto.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de establecimiento de puerto

Actividad relacionada con el establecimiento de puerto.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de enumeración de puertos

Actividad relacionada con la enumeración de puertos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de notificación de puerto

Se puede asignar a esta acción cualquier tipo de notificación relativa a un puerto. Los eventos más graves deberán asignarse a la acción de error de puerto.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de puerto

En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de mensaje de estado relativo al puerto.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de puerto

Se puede asignar a esta acción cualquier tipo de advertencia relativa al puerto. Los eventos más graves deberán asignarse a la acción de error de puerto.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Clase de actividad sospechosa

Acción de inserción de código

La acción de inserción de código informa sobre la inserción de códigos externos al programa.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6

Información	Nivel	
Error	F	5

Acción de modificación de código

La acción de modificación de código proporciona información sobre la modificación de códigos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Acción de captura de pulsación

La acción de captura de pulsación informa acerca de la captura de pulsaciones en el sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Error	F	3

Acción alerta de memoria

La acción de alerta de memoria proporciona información sobre alertas relativas a la memoria.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	6

Acción de daño en la memoria

La acción de daño en la memoria gestiona la expresión de la información del evento relativa a la detección de los daños en la memoria.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5
Error	F	4

Acción de modificación de memoria

La acción de modificación de memoria proporciona información acerca de las modificaciones en la memoria llevadas a cabo por un proceso.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de pérdida de contraseña

La acción de pérdida de contraseña proporciona información acerca de los intentos de revelado, listado, extracción o pérdida de contraseñas.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Error	F	3

Acción de vulnerabilidad de seguridad del servidor

La acción de vulnerabilidad de seguridad del servidor gestiona la expresión de la información del evento relativa a la detección de actividad de ataques que intenta vulnerar la seguridad del software del servidor.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Capítulo 7: Categoría de gestión de identidades

Esta sección contiene los siguientes temas:

Clase de gestión de cuentas (en la página 437)
Clase de actividad de atestación (en la página 460)
Gestión de grupos (en la página 475)
Clase de gestión de identidades (en la página 488)
Clase de gestión de derechos de usuario (en la página 496)
Clase de gestión de función de usuario (en la página 519)
Clase de gestión de flujo de trabajo (en la página 544)

Clase de gestión de cuentas

Acción de creación de cuentas

La acción de creación de cuentas se produce cuando se crean nuevas cuentas en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha creado qué cuenta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de cuentas

La acción de supresión de cuentas se produce cuando se eliminan cuentas en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha suprimido qué cuenta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desactivación de cuentas

La acción de desactivación de cuentas se produce cuando se desactivan cuentas en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha desactivado qué cuenta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de activación de cuenta

La acción de activación de cuenta se produce cuando se activan cuentas en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario

Información	Nivel
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha activado qué cuenta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de importación de cuentas

La acción de importación de cuentas proporciona información relativa a la importación de cuentas, generalmente mediante una operación por lotes.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de enumeración de cuentas

La acción de enumeración de cuentas a se produce cuando se enumeran cuentas en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha enumerado qué cuenta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2

Acción de bloqueo de cuenta

La acción de bloqueo de cuenta se produce cuando se bloquean cuentas en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha bloqueado qué cuenta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2

Acción de alerta de gestión de cuentas

La acción de alerta de gestión de cuentas proporciona información relativa a condiciones de alerta relacionadas con la gestión de cuentas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de error de gestión de cuentas

La acción de error de gestión de cuentas proporciona información acerca de las condiciones de error relacionadas con la gestión de cuentas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de notificación de gestión de cuentas

La acción de notificación de gestión de cuentas proporciona información acerca de las notificaciones relacionadas con la gestión de cuentas y los mensajes generados mediante sistemas de gestión de identidades.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de gestión de cuentas

La acción de advertencia de gestión de cuentas proporciona información acerca de las advertencias relacionadas con la gestión de cuentas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	3

Acción de modificación de cuenta

La acción de modificación de cuenta se produce cuando se modifica la información de cuenta en un sistema o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha modificado qué cuenta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de contraseña de cuenta

La acción de modificación de contraseña de cuenta se produce cuando se cambian contraseñas de cuenta en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario

Información	Nivel
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha modificado la contraseña de qué cuenta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de restablecimiento de contraseña de cuenta

La acción de restablecimiento de contraseña de cuenta se produce cuando se restablecen cuentas en una aplicación o sistema determinados. Esta acción es una acción de nivel más alto y no debe realizarse en todos los orígenes de eventos.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es quién restablece la contraseña en qué cuenta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de cuenta

Las acción de estado de cuenta proporciona información acerca del estado de las cuentas del sistema o del usuario en el sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de suspensión de cuenta

La acción de suspensión de cuenta se produce cuando se suspenden cuentas en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es quién suspende la contraseña en qué cuenta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desbloqueo de cuenta

La acción de desbloqueo de cuenta se produce cuando se desbloquean cuentas en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha desbloqueado qué cuenta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de lista de grupos

La acción de lista de grupos refleja el listado de la información de grupos en una aplicación o un sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué grupos se enumeran en qué sistema. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de infracción de atributos de cuenta de usuario

La acción de infracción de atributos de cuenta de usuario contiene información acerca de la detección de una infracción relacionada con los atributos de una cuenta de usuario.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de solicitud de creación de cuenta de usuario

La acción de solicitud de creación de cuenta de usuario contiene información relativa a las solicitudes de creación de cuentas nuevas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de solicitud de modificación de cuenta de usuario

La acción de solicitud de modificación de cuenta de usuario contiene información relativa a las solicitudes realizadas para modificar una cuenta existente.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de solicitud de validación de cuenta de usuario

La acción de solicitud de validación de cuenta de usuario contiene información relativa a las solicitudes de validación de cuentas existentes.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de actividad de atestación

Acción de atestación iniciada

La acción de atestación iniciada contiene información acerca de las actividades de inicio de la atestación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Información	Nivel	
Incorrecto	F	3

Acción de fin de certificación

La acción de fin de certificación contiene información relativa a la finalización de procesos de certificación, tales como los certificados de derechos como parte de la gestión de identidades.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de notificación de certificación

La acción de notificación de certificación contiene información acerca de las notificaciones de procesos de certificación, tales como los certificados de derechos como parte de la gestión de identidades.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de inicio de certificación

La acción de inicio de certificación contiene información relativa al inicio de procesos de certificación, tales como los certificados de derechos como parte de la gestión de identidades.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción Certificar usuario

La acción Certificar usuario contiene información acerca de la certificación de cuentas de usuario como parte del proceso formal de certificación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de solicitud aprobada

La acción de solicitud aprobada contiene información relativa a la aprobación de una solicitud de atestación como parte de un proceso de atestación periódico.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de solicitud archivada

La acción de solicitud archivada contiene información relativa al archivado de una solicitud de atestación como parte de un proceso de atestación periódico.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de solicitud delegada

La acción de solicitud delegada contiene información relativa a la delegación de una solicitud de atestación como parte de un proceso de atestación periódico.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de solicitud transferida

La acción de solicitud transferida contiene información relativa a la transferencia de una solicitud de atestación como parte de un proceso de atestación periódico.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de solicitud reasignada

La acción de solicitud reasignada contiene información relativa a la reasignación de una solicitud de atestación como parte de un proceso de atestación periódico.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de solicitud recibida

La acción de solicitud recibida contiene información relativa al recibo de una solicitud de confirmación como parte del proceso de confirmación periódico.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de solicitud rechazada

La acción de solicitud rechazada contiene información relativa al rechazo de una solicitud de atestación como parte de un proceso de atestación periódico.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de solicitud revocada

La acción de solicitud revocada contiene información relativa a la revocación de una solicitud de atestación como parte de un proceso de atestación periódico.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de solicitud

La acción de estado de solicitud contiene información relativa al estado de una solicitud de atestación como parte de un proceso de atestación periódico.

Información	Nivel
Origen - Información de usuario	Terciario

Información	Nivel
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Gestión de grupos

Acción de habilitación de grupo

La acción de habilitación de grupo proporciona información relativa a la habilitación de un grupo en un sistema o una aplicación determinados.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Información	Nivel	
Incorrecto	F	3

Acción de creación de grupos

La creación de grupos se produce cuando se crean grupos en un sistema de aplicaciones determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha creado qué grupo en qué host. La información del evento que se ha expresado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de deshabilitación de grupo

La acción de deshabilitación de grupo proporciona información relativa a la deshabilitación de un grupo en un sistema o una aplicación determinados.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de grupos

La acción de supresión de grupos se produce cuando se eliminan grupos en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha suprimido qué grupo en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de alerta de gestión de grupos

La acción de alerta de gestión de grupos proporciona información sobre las condiciones de alerta relacionadas con la gestión de grupos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Primario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de error de gestión de grupos

La acción de error de gestión de grupos proporciona información acerca de las condiciones de error relacionadas con la gestión de grupos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de notificación de gestión de grupos

La acción de notificación de gestión de grupos proporciona información sobre las notificaciones y los mensajes relacionados con la gestión de grupos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de gestión de grupos

La acción de advertencia de gestión de grupos proporciona información acerca de las advertencias relacionadas con la gestión de grupos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	3

Acción de adición de pertenencia a grupo

La acción de adición de pertenencia a grupo se produce cuando se agrega información de pertenencia a grupo en un sistema de aplicaciones determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Primario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha agregado la pertenencia a qué grupo en qué host y a qué usuarios afectan estos cambios. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de pertenencia a grupo

La acción de supresión de pertenencia a grupo se produce cuando se suprime información de pertenencia a grupo en un sistema de aplicaciones determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha suprimido la pertenencia a qué grupo en qué host y a qué usuarios afectan estos cambios. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de pertenencia a grupo

La acción de modificación de pertenencia a grupo se produce cuando se modifica información de pertenencia a grupo en un sistema de aplicaciones determinado. Esto incluye la supresión y adición de información de pertenencia.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha modificado la pertenencia a qué grupo en qué host y a qué usuarios afectan estos cambios. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de grupos

La acción de modificación de grupos se produce cuando se modifica la información de grupo en un sistema o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha modificado qué grupo en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión de identidades

Acción de correlación de identidades

La acción de correlación de identidades contiene información relativa a procesos en los que se concilia y valida de forma adecuada la propiedad de distintas cuentas de usuario en los sistemas y aplicaciones de toda la empresa. Estos ID pueden vincular de forma permanente la propiedad de los ID de inicio de sesión de cuenta de usuario a individuos concretos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de identidades

La acción de creación de identidades se produce cuando se crean identidades en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha creado qué identidad en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de identidades

La acción de supresión de identidades se produce cuando se eliminan identidades en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha suprimido qué identidad en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desactivación de identidades

La acción de desactivación de identidades se produce cuando se desactivan identidades en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha desactivado qué identidad en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de activación de identidades

La acción de activación de identidades se produce cuando se activan identidades en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha activado qué identidad en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de identidad

La acción de modificación de identidad se produce cuando se modifica la información de identidad en un sistema o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha modificado qué identidad en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de contraseña de identidad

La acción de modificación de contraseña de identidad se produce cuando se cambia una contraseña de identidad en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es quién ha modificado la contraseña en qué identidad en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de sincronización de identidades

La acción de sincronización de identidades proporciona información relativa a procesos en los que se enlazan o sincronizan los usuarios o las identidades entre distintos almacenes de usuarios.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión de derechos de usuario

Acción de actualización de cuenta

La acción de actualización de cuenta se produce cuando se actualiza la información de una cuenta en una aplicación o un sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta se actualiza en qué sistema. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de enlace doble de funciones detectado

La acción de enlace doble de funciones detectado proporciona información relativa a la detección de dos enlaces de permisos entre la función y el recurso.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Secundario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de número excesivo de permisos detectado

La acción de número excesivo de permisos detectado contiene información relativa a la detección de un número excesivo de enlaces de permisos directos entre el usuario y varios recursos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Secundario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de número mínimo de permisos detectado

La acción de número mínimo de permisos detectado contiene información relativa a la detección de un número reducido de enlaces de permisos entre el usuario y los recursos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Acción de infracción de segregación de tareas

La acción de infracción de segregación de tareas contiene información relativa a la detección de infracciones del principio de segregación de tareas en relación con los derechos del usuario.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de permiso de usuario sospechoso detectado

La acción de permiso de usuario sospechoso detectado contiene información relativa a la detección de permisos sobre recursos pertenecientes a usuarios sospechosos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de asignación de derechos de administración de usuario

La acción de asignación de derechos de administración de usuario tiene lugar cuando se asignan derechos de usuario en una aplicación o un sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es a qué usuarios se asignan derechos en qué sistema. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de derechos de administración de usuario

La acción de supresión de derechos de administración de usuario se produce cuando se eliminan los derechos de usuario en una aplicación o un sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué derechos de usuario se eliminan en qué sistema. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de asignación de permisos de usuario

La acción de asignación de permisos de usuario se produce cuando se asigna un permiso de usuario existente en una aplicación o sistema determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha asignado qué permiso de usuario para qué usuario en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de error de coincidencia de permisos de usuario

La acción de error de coincidencia de permisos de usuario contiene información relativa a la detección de un error de coincidencia entre los permisos de usuario y los permisos de funciones.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de solicitud de modificación de permiso de usuario

La acción de solicitud de modificación de permiso de usuario contiene información relativa a las solicitudes realizadas con el fin de modificar los permisos de usuario.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de superposición de permisos de usuario

La acción de superposición de permisos de usuario contiene información relativa a la detección de permisos superpuestos para cuentas de usuario.

Información	Nivel
Origen - Información de usuario	Terciario

Información	Nivel
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de supresión de permisos de usuario

La acción de supresión de permisos de usuario se produce cuando se elimina un permiso de usuario existente en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario

Información	Nivel
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha suprimido qué permiso de usuario para qué usuario en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de solicitud de validación de permiso de usuario

La acción de solicitud de validación de permiso de usuario contiene información relativa a las solicitudes realizadas para validar permisos de usuario.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de infracción de permiso de usuario

La acción de infracción de permiso de usuario contiene información relativa a la detección de infracciones de permisos de usuario.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de asignación de derechos de usuario

La acción de asignación de derechos de usuario se produce cuando se asigna un derecho de usuario existente en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha asignado qué derecho de usuario para qué usuario en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de derechos de usuario

La acción de creación de derechos de usuario se produce cuando se crea un derecho de usuario en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha creado qué derecho usuario en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de derechos de usuario

La acción de supresión de derechos de usuario se produce cuando se elimina un derecho de usuario en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha suprimido qué derecho usuario en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de enumeración de derechos de usuario

La acción de enumeración de derechos de usuario se produce cuando recopilan los derechos de un usuario en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha enumerado los derechos de qué usuario en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de derechos de usuario

La acción de modificación de derechos de usuario se produce cuando se modifica un derecho de usuario en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha modificado qué derecho usuario en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de notificación de derecho de usuario

La acción de notificación de derecho de usuario informa acerca de notificaciones de derechos genéricos del usuario.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de superposición de funciones de usuario

La acción de superposición de funciones de usuario proporciona información relativa a la detección de funciones superpuestas de cuentas de usuario.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Clase de gestión de función de usuario

Acción de enlace doble de permisos detectado

La acción de enlace doble de permisos detectado contiene información relativa a la detección de dos enlaces de permisos entre el usuario y el recurso.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Secundario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de número excesivo de funciones detectado

La acción de número excesivo de funciones detectado proporciona información relativa a la detección de un recurso utilizado por numerosas funciones.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Secundario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de jerarquía excesiva de funciones detectada

La acción de jerarquía excesiva de funciones detectada proporciona información relativa a la detección de funciones con un número elevado de subfunciones.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de pertenencia a función excesiva detectada

La acción de pertenencia a función excesiva detectada proporciona información relativa a la detección de funciones con un número excesivo de usuarios directos, indirectos y dobles.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de jerarquía mínima de funciones detectada

La acción de jerarquía mínima de funciones detectada proporciona información relativa a la detección de una función con un número reducido de subfunciones.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Acción de pertenencia a función mínima detectada

La acción de pertenencia a función mínima detectada proporciona información relativa a la detección de una función con un número reducido de recursos totales.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Acción de número mínimo de funciones detectado

La acción de número mínimo de funciones detectado proporciona información relativa a la detección de un recurso utilizado por un número reducido de funciones.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Acción de solicitud de modificación de función

La acción de solicitud de modificación de función proporciona información relativa a las solicitudes de modificación de las funciones existentes.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de validación de rol

Esta acción expresa información acerca de la validación de un rol de usuario.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de solicitud de validación de función

La acción de solicitud de validación de función proporciona información relativa a las solicitudes realizadas con el fin de validar las funciones existentes.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de infracción de función

La acción de infracción de función proporciona información relativa a las infracciones de funciones.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de infracción de segregación de tareas

La acción de infracción de segregación de tareas proporciona información relativa a las infracciones de los principios de segregación de tareas en relación con las funciones de usuario.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de asignación de función sospechosa detectada

La acción de asignación de función sospechosa detectada proporciona información relativa a situaciones en las que existen usuarios o privilegios de función sospechosos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de función sospechosa detectada

La acción de función sospechosa detectada proporciona información relativa a situaciones en las que existe una función sospechosa.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de permiso de usuario sospechoso detectado

La acción de permiso de usuario sospechoso detectado proporciona información relativa a la detección de permisos sobre funciones pertenecientes a usuarios sospechosos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de asignación de funciones de administración de usuario

La acción de asignación de función de administrador de usuarios se produce cuando se asigna la función de usuario privilegiado o administrador en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha asignado la función de usuario privilegiado o administrador para qué usuario en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de supresión de función de administrador de usuarios

La acción de supresión de función de administrador de usuarios se produce cuando se suprime la función de usuario privilegiado o administrador en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha suprimido la función de usuario privilegiado o administrador para qué usuario en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de modificación de función de administrador de usuario

La acción de modificación de función de administrador de usuarios se produce cuando se modifica la función de usuario privilegiado o administrador en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha modificado la función de usuario privilegiado o administrador para qué usuario en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de supresión de función de administrador de usuarios

La acción de supresión de función de administrador de usuarios se produce cuando se suprime la función de usuario privilegiado o administrador en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha suprimido la función de usuario privilegiado o administrador para qué usuario en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de asignación de función de usuario

La acción de asignación de función de usuario se produce cuando se asigna una función de usuario en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es quién ha asignado qué función a qué usuario en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2

Acción de creación de función de usuario

La acción de creación de función de usuario se produce cuando se crea una función de usuario en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha creado qué función en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de función de usuario

La acción de supresión de función de usuario se produce cuando se suprime una función de usuario en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha suprimido qué función en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de función de usuario

La acción de modificación de función de usuario cuando se modifica una función de usuario en un sistema determinado o aplicación

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha modificado qué función en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de superposición de funciones de usuario

La acción de superposición de funciones de usuario proporciona información relativa a la detección de funciones superpuestas de cuentas de usuario.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3

Acción de supresión de función de usuario

La acción de supresión de función de usuario se produce cuando se suprime una función de usuario en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha suprimido qué función para qué usuario en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión de flujo de trabajo

Acción de aprobación de tareas

La acción de aprobación de tareas contiene información relativa a la aprobación de tareas enviadas o añadidas a un proceso o motor de flujo de trabajo.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Información	Nivel	
Incorrecto	F	3

Capítulo 8: Categoría de mensajería

Esta sección contiene los siguientes temas:

Clase de actividad de correo (en la página 547)
Clase de sistema de mensajería (en la página 565)

Clase de actividad de correo

Acción de transferencia de red troncal

La acción de transferencia de red troncal trata la expresión de información relativa al envío o recepción de correo desde/a otro sistema MAPI en un conector o una puerta de enlace.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de transferencia de puerta de enlace

La acción de transferencia de puerta de enlace trata la expresión de información relativa al envío o recepción de coreo a través de una puerta de enlace.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de mensaje

La acción de supresión de mensaje trata la expresión de información relativa a la eliminación de mensajes.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Resultado	event_result	event_severity
Incorrecto	F	3

Acción de entrega de mensaje

La acción de entrega de mensaje trata la expresión de información relativa a la entrega de un mensaje a la bandeja de correo o carpeta pública.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de envío de mensajes

La acción de envío de mensajes trata la expresión de información relativa al envío de un mensaje por el cliente.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de redirigimiento de mensajes

La acción de redirigimiento de mensajes trata la expresión de información relativa al envío de mensajes a bandejas de correo distintas a las bandejas de correo de los destinatarios.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de liberación de mensaje

La acción de liberación de mensaje se produce cuando se realiza la liberación de mensajes de la cuarentena a un almacén de usuarios como la bandeja de entrada de mensajes.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desvío de mensaje

La acción de desvío de mensaje trata la expresión de información relativa al desvío de mensajes a una ruta alternativa.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de transferencia de mensajes

La acción de transferencia de mensajes trata la expresión de información relativa a las transferencias de mensajes entre un cliente y un servidor, conector o puerta de enlace.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de sondeo

La acción de sondeo trata la expresión de información relativa a actividades de sondeo (por ejemplo: transferencia de sondeo X.400, X.400 [envío de sondeo].

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de informe

La acción de supresión de informe trata la expresión de información relativa a la eliminación, asimilación o descarte de una confirmación de entrega o informe de entrega no realizada.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de recepción de informe

La acción de recepción de informe trata la expresión de información relativa a la generación, transferencia, envío, generación de confirmación de entrega o informe de entrega no realizada.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de entrega de SMTP

La acción de entrega de SMTP trata la expresión de información relativa a la entrega de mensajes a una entidad como una puerta de enlace, agente de transferencia de correo (MTA), almacén local, unidad de almacenamiento, etc.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de error de SMTP

La acción de error de SMTP contiene información relativa a los errores generados durante la transferencia de correo electrónico a un servicio de correo por Internet o desde éste.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5

Acción de notificación de SMTP

La acción de notificación de SMTP contiene información relativa a las notificaciones generadas durante la transferencia de correo electrónico a un servicio de correo por Internet o desde éste.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de SMTP en cola

La acción de SMTP en cola trata la expresión de información relativa a la puesta en cola de correo saliente para el envío mediante el servicio de correo por Internet.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de transferencia de SMTP

La acción de transferencia de SMTP trata la expresión de información relativa a la transferencia de correo electrónico del servicio de correo por Internet o al servicio de correo por Internet.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de SMTP

La acción de advertencia de SMTP contiene información relativa a las advertencias generadas durante la transferencia de correo electrónico a un servicio de correo por Internet o desde éste.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Clase de sistema de mensajería

Acción de advertencia de mensaje

La acción de advertencia de mensaje proporciona información sobre advertencias relacionadas con el sistema de mensajes.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Capítulo 9: Categoría de seguridad de red

Esta sección contiene los siguientes temas:

Clase de control de acceso (en la página 567)
Clase de actividad de antivirus (en la página 584)
Clase de seguridad de aplicaciones (en la página 585)
Clase de actividad de certificado (en la página 595)
Clase de actividad de conexión (en la página 624)
Clase de infracción de política corporativa (en la página 648)
Denegación de clase de servicio (en la página 654)
Clase de actividad de cifrado (en la página 670)
Clase de pérdida de información (en la página 686)
Clase de actividad de software maligno (en la página 692)
Acción de clase de gestión de direcciones de red (en la página 696)
Clase de escalación de privilegios (en la página 699)
Acción de clase de la actividad de enrutamiento (en la página 702)
Clase de infracción de firmas (en la página 703)
Clase de actividad sospechosa (en la página 704)
Clase de gestión de servicios Web (en la página 726)

Clase de control de acceso

Acción de bloqueo del puerto

La acción de bloqueo del puerto gestiona la expresión de la información del evento relativa al bloqueo de un puerto por medio de un proceso manual o automatizado para limitar o controlar el tráfico de un puerto específico.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de desbloqueo del puerto

La acción de desbloqueo del puerto gestiona la expresión de la información del evento relativa al desbloqueo de un puerto por medio de un proceso manual o automatizado para eliminar el límite de un puerto específico.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de infracción de la seguridad del puerto

La acción de infracción de la seguridad del puerto gestiona la expresión de la información del evento relativa a la detección de infracciones relacionadas con los puertos de un conmutador o dispositivo similar.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	3

Acción de alerta del límite de la frecuencia

La acción de alerta del límite de la frecuencia gestiona la expresión de la información relativa a las condiciones de alerta relacionadas con los valores de configuración del límite de la frecuencia o de la formación de la frecuencia del tráfico de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	6

Acción de error del límite de la frecuencia

La acción de error del límite de la frecuencia gestiona la expresión de la información relativa a las condiciones de error relacionadas con los valores de configuración del límite de la frecuencia o de la formación de la frecuencia del tráfico de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	5

Acción de operación de límite de la frecuencia

La acción de operación de límite de la frecuencia gestiona la expresión de la información relativa a las operaciones generales relacionadas con el modo de uso de los valores de configuración del límite de la frecuencia o de la formación de la frecuencia del tráfico de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de estado del límite de la frecuencia

La acción de estado del límite de la frecuencia gestiona la expresión de la información relativa al estado de los valores de configuración del límite de la frecuencia o de la formación de la frecuencia del tráfico de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de advertencia del límite de la frecuencia

La acción de advertencia del límite de la frecuencia gestiona la expresión de la información relativa a las advertencias relacionadas con los valores de configuración del límite de la frecuencia o de la formación de la frecuencia del tráfico de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	4

Acción de bloqueo de conexión

Esta acción expresa información acerca del bloqueo de una conexión.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de desbloqueo de conexión

Esta acción expresa información acerca del desbloqueo de una conexión bloqueada.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de bloqueo de host

Esta acción expresa información acerca del desbloqueo de un host.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de desbloqueo de host

Esta acción expresa información acerca del desbloqueo de un host bloqueado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de notificación de acceso a red

La acción de notificación de acceso a red proporciona información acerca de las notificaciones generales de acceso a la red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de bloqueo de red

Esta acción expresa información acerca del bloqueo de una red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de desbloqueo de red

Esta acción expresa información acerca del desbloqueo de una red bloqueada.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de activación de tasa límite

Esta acción expresa información acerca de la activación de tasas límite con relación al tráfico de la red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de desactivación de tasa límite

Esta acción expresa información acerca de la desactivación de tasas límite con relación al tráfico de la red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Clase de actividad de antivirus

Acción de revocación de confianza

La acción de revocación de confianza proporciona información relativa a la eliminación de relaciones de confianza entre los sistemas o componentes de TI.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Clase de seguridad de aplicaciones

Acción de ataque de flujo excesivo del búfer

La acción de ataque de flujo excesivo del búfer trata la expresión de la información del evento relativa a la detección del ataque de flujo excesivo del búfer.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6

Resultado	event_result	event_severity
Incorrecto	F	5
Intento	A	5

Vulnerabilidad de seguridad del servidor de correo

La acción de vulnerabilidad de seguridad del servidor de correo gestiona la expresión de la información del evento relativa a cualquier acción de ataque que vulnera la seguridad en servidores de correo.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Acción de ataque de divulgación de orígenes

La acción de ataque de divulgación de orígenes gestiona la expresión de la información del evento relativa a los ataques dirigidos contra servidores Web que procesan páginas dinámicas. Los ataques intentan acceder al código fuente que puede incluir información de la instalación, como los ID y las contraseñas de usuario de acceso a las bases de datos. Esta forma de ataque se puede llevar a cabo mediante la emisión de URL especiales que el servidor procesa de manera incorrecta, o que hacen que el servidor ejecute algunos componentes del software que pueden contener errores o problemas.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Acción de explotación de correo electrónico

La acción de explotación de correo electrónico incluye información del evento relativa a la detección de explotaciones en un sistema de correo electrónico.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de explotación remota

La acción de explotación remota trata la expresión de información del evento relativa a la detección de una explotación a través de una conexión de red sin ningún acceso previo al sistema vulnerable.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6
Incorrecto	F	5
Intento	A	5

Acción de ejecución de comando especial

La acción de ejecución de comando especial trata la expresión de información del evento relativa a la ejecución de llamadas del sistema o comandos especiales.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	4
Intento	A	4

Acción de explotación de software

Acción existente - Se etiquetará con las clases de Gramática de eventos Denegación de servicio o Seguridad de aplicación según el contexto.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Incorrecto	F	5

Acción de actividad de aplicación Web

La acción de actividad de aplicación Web trata la expresión de información del evento relativa al acceso a una aplicación Web potencialmente vulnerable.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5

Acción de ataque de aplicación Web

La acción de ataque de aplicación Web trata la expresión de información del evento relativa a la detección de un ataque que afecta a las aplicaciones Web (por ejemplo: intento transversal de directorio).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6
Incorrecto	F	5
Intento	A	5

Acción de explotación del explorador Web

La acción de explotación del explorador Web trata cualquier actividad que esté intentando explotar vulnerabilidades en los exploradores Web.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Incorrecto	F	5

Clase de actividad de certificado

Acción de alerta de certificado

La acción de alerta de certificado proporciona información sobre las condiciones de alerta generadas durante la actividad de certificados o relativas a certificados digitales.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	6

Acción de exportación de certificado

la acción de exportación de certificado trata la exportación de un certificado a un archivo.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de caducidad de certificado

La acción de caducidad de certificado trata la caducidad de un certificado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de error de certificado

La acción de error de certificado trata la actividad de certificado genérico relacionada con errores como recibir un certificado vacío o en blanco.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de generación de certificado

La acción de generación de certificado trata la generación de un nuevo certificado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de certificado

La acción de operación de certificado proporciona información general sobre los certificados y la actividad de certificados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de importación de certificado

La acción de importación de certificado trata la importación de un certificado de un archivo.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de inicialización de certificado

La acción de inicialización de certificado trata la inicialización del certificado adquirido.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de notificación de certificado

La acción de notificación de certificado proporciona información relativa a las notificaciones y los mensajes generados a partir de una actividad de certificados o mediante una infraestructura de certificados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de revocación de certificado

La acción de publicación de lista de revocación de certificados trata la publicación que realiza una autoridad de certificados (CA) de una lista de revocación de certificados (CRL).

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de alerta de lista de revocación de certificados

La acción de alerta de lista de revocación de certificados proporciona información sobre las alertas relacionadas con las listas de revocación de certificados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	6

Acción de error de lista de revocación de certificados

La acción de error de lista de revocación de certificados proporciona información sobre los errores relacionados con las listas de revocación de certificados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de caducidad de lista de revocaciones de certificados

La caducidad de la lista de revocaciones de certificados trata la actividad relacionada con la caducidad de la lista de revocaciones de certificados (CRL). Por ejemplo, caduca la lista de revocaciones de certificado (CRL) de la autoridad de certificados (CA) cuando cambia la clave de la autoridad de certificados (CA).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Terciario
Origen de evento - Información	Primario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué actividad de la lista de revocaciones de certificados (CRL) se produce en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de importación de lista de revocaciones de certificados

Las acciones de importación de lista de revocaciones de certificados hacen referencia a la importación de una lista de revocaciones de certificados (CRL) a un dispositivo o aplicación. Por ejemplo, la importación de una lista de revocaciones de certificados (CRL) en una aplicación de explorador Web.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	4

Acción de notificación de lista de revocación de certificados

La acción de notificación de lista de revocación de certificados proporciona información general sobre las notificaciones relativas a las listas de revocación de certificados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de lista de revocación de certificados

La acción de operación de lista de revocación de certificados proporciona información general sobre las operaciones relativas a las listas de revocación de certificados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de renovación de lista de revocaciones de certificados

Las acciones de renovación de lista de revocaciones de certificados tienen relación con la renovación por parte de las autoridades de certificados (CA) de la lista de revocaciones de certificados (CRL).

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de lista de revocación de certificados

La acción de estado de lista de revocación de certificados proporciona información acerca del estado de las listas de revocación de certificados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de validación de lista de revocaciones de certificados

Las acciones de validación de lista de revocaciones de certificados hacen referencia a cualquier actividad relacionada con la validación de una lista de revocaciones de certificados (CRL). Por ejemplo, una lista de revocaciones de certificados con una marca de hora errónea.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	4

Acción de advertencia de lista de revocación de certificados

La acción de advertencia de lista de revocación de certificados proporciona información sobre las advertencias relativas a las listas de certificados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de renovación de certificado

La acción de renovación de certificado trata la renovación de certificados después de que finalice el período de validez por un par de claves nuevo o existente.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de solicitud de certificado

La acción de solicitud de certificado (también denominada solicitud de firma de certificado (CSR)) trata el envío de un mensaje a una autoridad de certificados (CA) para solicitar un certificado de identidad digital. Esta acción puede ser manual o automática.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de revocación de certificado

La acción de revocación de certificado trata la revocación de certificados. Una autoridad de certificados (CA) puede revocar certificados por motivos como los de certificados en peligro, tokens perdidos que contengan claves privadas, etc.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	4

Acción de estado de certificado

La acción de estado de certificado proporciona información relativa al estado de los certificados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de suspensión de certificado

La acción de suspensión de certificado trata la suspensión de un certificado. La suspensión sólo funciona con el protocolo de estado de certificado en línea (OCSP), que es una validación en tiempo real. El protocolo de estado de certificado en línea (OCSP) sólo se utiliza para certificados revocados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de cancelación de revocación de certificado

La acción de cancelación de revocación de certificado proporciona información relativa a la cancelación de la revocación de un certificado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de validación de certificado

La acción de validación de certificado trata la verificación de la validación del certificado con la lista de revocación de certificados (CRL) en el protocolo de estado de certificado en línea (OCSP).

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de certificado

La acción de advertencia de certificado proporciona información relativa a las advertencias generadas mediante una actividad o infraestructura de certificados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de establecimiento de confianza

La acción de establecimiento de confianza proporciona información relativa al establecimiento de relaciones de confianza entre los sistemas o componentes de TI.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de actividad de conexión

Acción de supresión de certificado

La acción de supresión de certificado proporciona información relativa a la supresión de un certificado mediante la generación de un nuevo certificado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es el certificado de qué host se ha suprimido. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Notificación de conexión

La acción de notificación de conexión gestiona la expresión de la información relativa a las notificaciones y mensajes generados de una conexión establecida entre dos entidades de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de fase 1 de la negociación para el intercambio de claves

La acción de fase 1 de la negociación para el intercambio de claves gestiona la expresión de la información del evento relativa a la fase 1 de las negociaciones para el establecimiento de las asociaciones de seguridad (SA).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de operación de túnel

La acción de operación de túnel gestiona la expresión de la información relativa a las operaciones relacionadas con un túnel de conexión de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de alerta de certificado

La acción de alerta de certificado informa acerca de las condiciones de la alerta relacionadas con las conexiones de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	6

Acción de intento de conexión

La acción de intento de conexión trata la expresión de la información del evento relativa al intento de conexión entre dos entidades de red según lo que registra un host determinado. Existen tres resultados posibles para esta acción: A para aceptar la conexión, D para la anular silenciosamente la conexión y R para rechazar (o anular) el intento de conexión.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host está intentando conectar con qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Aceptar	A	2
Anular	D	3

Resultado	event_result	event_severity
Rechazar	R	3

Acción de restablecimiento de conexión

La acción de restablecimiento de conexión trata la expresión de la información del evento relativa al restablecimiento de una conexión entre dos entidades de red según lo que registra un host determinado. Hay dos resultados posibles para esta acción: S (del inglés successsful, correcto) para el restablecimiento correcto y F (del inglés failed, incorrecto) para el restablecimiento incorrecto. A veces se produce el restablecimiento de la conexión cuando cambian partes de la información como un escenario NAT.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host está intentando conectar con qué host cuando se restablece la conexión. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de solicitud de conexión

La acción de solicitud de conexión trata la expresión de la información del evento relativa a la solicitud de una conexión entre dos entidades de red según lo que registra un host determinado. La solicitud de una conexión es una parte muy detallada de información de depuración y no es necesaria normalmente si se registra el intento de conexión para a misma conexión.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

La información importante para esta acción es qué host está intentando conectar con qué host cuando se restablece la conexión. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2

Acción de estado de conexión

La acción de estado de conexión trata la expresión de la información del evento relativa al estado de una conexión entre dos entidades de red según lo que registra un host determinado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host dispone de una conexión establecida con qué host y qué host ha registrado la información. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2

Acción de finalización de conexión

La acción de finalización de conexión trata la expresión de la información del evento relativa a la finalización de una conexión establecida anteriormente entre dos entidades de red según lo que registra un host determinado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es la conexión que ha finalizado de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2

Acción de advertencia de conexión

La acción de advertencia de conexión proporciona información relativa a la detección de errores genéricos en una conexión entre dos entidades de red según el registro de un host determinado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué errores se han detectado en qué conexiones. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4

Acción de inicio de fase 1 de intercambio de claves

La acción de inicio de fase 1 de intercambio de claves con la expresión de información del evento relativa al inicio de una negociación IKE para la conexión IPSEC entre dos entidades de red según lo que registra un host determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host está intentando iniciar una negociación IKE en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de alerta de protocolo

La acción de alerta de protocolo proporciona información relativa a cualquier tipo de alerta de protocolo. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de protocolo.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	6

Acción de bloqueo de puerto

La acción de bloqueo de puerto proporciona información relativa al bloqueo de los puertos de red o comunicación con el objetivo de filtrar el tráfico.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de error de protocolo

La acción de error de protocolo proporciona información acerca de las condiciones de error relativas a un protocolo.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de reenvío de puerto

La acción de reenvío de puerto se encarga de proporcionar información sobre los eventos relacionados con el reenvío de puertos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué puerto se ha reenviado. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de protocolo

La acción de operación de protocolo proporciona información general sobre las operaciones de protocolo.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de protocolo

La acción de estado de protocolo proporciona información relativa al estado de las operaciones de protocolo.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de protocolo

La acción de advertencia de protocolo proporciona información sobre las condiciones de error relacionadas con operaciones de protocolo.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de notificación de protocolo

Las acciones de notificación de protocolo expresan información sobre notificaciones, mensajes y actualizaciones de estado de cualquier protocolo de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de caducidad de asociación de seguridad

La acción de caducidad de asociación de seguridad trata la expresión de información del evento relativa a la caducidad de una asociación de seguridad que define una conexión IPSEC entre dos entidades de red según lo que registra un host determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué asociación de seguridad ha caducado y está afectando a la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de solicitud de asociación de seguridad

La acción de solicitud de asociación de seguridad trata la expresión de información del evento relativa a la solicitud para establecer una asociación de seguridad que define una conexión IPSEC entre dos entidades de red según lo que registra un host determinado. Hay dos resultados posibles para esta acción: S (del inglés sucessful, correcto) y F (del inglés failure, incorrecto).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué asociación de seguridad se ha solicitado para la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de exploración de virus

La acción de exploración de virus proporciona información relativa a la exploración o la exploración repetida de un objeto.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué objeto se ha explorado. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de infracción de política corporativa

Acción de sustitución de contenido

La acción de sustitución de contenido trata la expresión de información del evento relativa a la detección de una activada de sustitución de contenido (por ejemplo: la carga de archivos mediante MI)

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5

Resultado	event_result	event_severity
Incorrecto	F	4
Intento	A	4

Acción de contenido ilegal

La acción de contenido ilegal trata la expresión de información del evento relativa a la detección de los datos censurables (por ejemplo: archivos con imágenes ofensivas).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4

Software sospechoso detectado

La acción de software sospechoso detectado trata la detección de software sospechoso.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5

Uso de acción de programas de chat

El uso de la acción de programas de chat trata la expresión de información del evento relativa al uso de los programas y protocolos de chat (por ejemplo, el uso de AIM, ICQ e IRC)

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4

Uso de acción de cliente P2P

El uso de acción de cliente P2P trata la expresión de información del evento relativa al uso del cliente P2P (por ejemplo, el uso de clientes P2P como Napster o Skype).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4

Uso de acción de tecnologías multimedia de transmisión

El uso de acción de tecnologías multimedia de transmisión trata la expresión de información del evento relativa al uso de tecnologías multimedia de transmisión (por ejemplo: el uso de RealPlayer, You Tube etc. por parte de los empleados).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4

Denegación de clase de servicio

Acción de explotación de aplicaciones

La acción de explotación de aplicaciones trata la expresión de información del evento relativa a la detección de actividad de ataques que intenta explotar las vulnerabilidades en la implementación de las aplicaciones Enterprise.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5
Intento	A	4

Acción de ataque de agotamiento de ancho de banda

La acción de ataque de agotamiento de ancho de banda trata la expresión de información del evento relativa a la detección de actividad de ataque que utiliza varias técnicas de desbordamiento para inundar una red para crear DOS (por ejemplo: Smurf, sobrecarga de tubería de datos).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6
Intento	A	6

Acción de flujo excesivo del búfer

Acción existente - Se etiquetará con las clases de Gramática de eventos Denegación de servicio o Seguridad de aplicación según el contexto.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6
Incorrecto	F	5

Acción de explotación de base de datos

La acción de explotación de base de datos trata la expresión de información del evento relativa a la detección de actividad de ataques que intenta explotar las vulnerabilidades en los servidores de base de datos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5
Intento	A	4

Acción de ataque distribuido

La acción de ataque distribuido trata la expresión de información del evento relativa a la detección de actividad de ataque distribuido (por ejemplo: Ddos que usa bots).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6
Intento	A	6

Acción de explotación de firmware

La acción de explotación de firmware trata cualquier actividad de firmas que esté intentando explotar infracciones en el firmware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6
Incorrecto	F	5

Acción de ataque de fragmentación

La acción de ataque de fragmentación trata la expresión de información del evento relativa a la detección de actividad de ataque que implica la fragmentación de paquetes (por ejemplo: ataques de fragmentación de IP, ataque Teardrop).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6
Intento	A	6

Acción de ataque de paquete mal formado

La acción de ataque de paquete mal formado trata la expresión de información del evento relativa a la detección de paquetes de datos de red mal formados como IP o TCP (por ejemplo: ataque de tipo Land, ataque tipo Christmas tree).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6
Intento	A	6

Acción de ataque de conectividad de red

La acción de ataque de conectividad de red trata la expresión de información del evento relativa a la detección de actividad de ataques que intenta explotar las vulnerabilidades en las conexiones de red (por ejemplo: SYN Flood).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5
Intento	A	4

Acción de explotación del SO

La acción de explotación del SO trata la expresión de información del evento relativa a la detección de actividad de ataques que intenta explotar las vulnerabilidades en el software del SO.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6
Intento	A	5

Acción de explotación de protocolo

La acción de explotación de protocolo trata la expresión de información del evento relativa a la detección de actividad de ataques que intenta explotar las vulnerabilidades en un protocolo específico como ssh, ftp o telnet.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5
Intento	A	4

Acción de ataque de agotamiento de recursos

La acción de ataque de agotamiento de recursos trata la expresión de información del evento relacionada con la supresión de actividad de ataque que intenta agotar los recursos en un dispositivo o host.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario

Información	Nivel
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5
Intento	A	4

Acción de explotación de software

La acción de explotación de software trata la expresión de información del evento relativa a la detección de actividad de ataques que intenta explotar las vulnerabilidades en el software de aplicaciones.

Información	Nivel
Origen - Información de usuario	Terciario

Información	Nivel
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5
Intento	A	4

Acción de explotación de servidor Web

La acción de ataque distribuido trata la expresión de información del evento relativa a la detección de actividad de ataques que intenta explotar las vulnerabilidades en el software del servidor Web.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6
Intento	A	5

Acción de ataque en dispositivos inalámbricos

La acción de ataque en dispositivos inalámbricos trata la expresión de información del evento relativa a la actividad de detección de ataque que intenta explotar las vulnerabilidades en las comunicaciones de radio y software y hardware inalámbrico (ejemplo: ataque Deauth, Rogue WAP).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5
Intento	A	4

Clase de actividad de cifrado

Acción alerta de cifrado

La acción de alerta de cifrado gestiona la expresión de la información acerca de las condiciones de alerta relacionadas con las operaciones o los sistemas de cifrado en un entorno de host específico.

A esta acción, se le puede asignar cualquier tipo de alerta relativa a las operaciones o sistemas de cifrado. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de cifrado. Si la acción está relacionada con el entorno de red, deberá asignarse al mismo evento bajo la categoría de seguridad de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D

Resultado	event_result	event_severity
Error	F	6

Acción de error de cifrado

La acción de error de cifrado gestiona la expresión de la información acerca de las condiciones de error relacionadas con las operaciones o los sistemas de cifrado en un entorno de host específico.

A esta acción, se le puede asignar cualquier tipo de error relativo a las operaciones o sistemas de cifrado. Los eventos de menor severidad deben asignarse a las operaciones de cifrado o las acciones de advertencia de los sistemas de cifrado. Los eventos de mayor severidad que requieran atención inmediata deberán asignarse a la acción de alerta de cifrado. Si la acción está relacionada con el entorno de red, deberá asignarse al mismo evento bajo la categoría de seguridad de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	5

Acción de notificación de cifrado

La acción de notificación de cifrado gestiona la expresión de la información relativa a las notificaciones y mensajes generados de operaciones o sistemas de cifrado en un entorno de host específico.

En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar cualquier tipo de notificación de operaciones o sistemas de cifrado. Si el evento describe el estado de las operaciones o los sistemas de cifrado, deberá utilizarse la acción de estado del cifrado. Si la acción está relacionada con el entorno de red, deberá asignarse al mismo evento bajo la categoría de seguridad de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de operación de cifrado

La acción de operación de cifrado gestiona la expresión de la información relativa a las operaciones generales referidas al funcionamiento de los sistemas de cifrado en un entorno de host específico.

Cuando un evento se registra como parte de la función normal de las operaciones o de los sistemas de cifrado, o si el evento no se puede asignar a una acción de la gramática de eventos comunes más específica, se recomienda asignar el evento a esta acción. Si la acción está relacionada con el entorno de red, deberá asignarse al mismo evento bajo la categoría de seguridad de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de estado del cifrado

La acción de estado del cifrado gestiona la expresión de la información relativa al estado de las operaciones o los sistemas de cifrado en un entorno de host específico.

Cuando un evento se registra como parte de la función normal de las operaciones o de los sistemas de cifrado, o si el evento no se puede asignar a una acción de la gramática de eventos comunes más específica, se recomienda asignar el evento a esta acción. Si la acción está relacionada con el entorno de red, deberá asignarse al mismo evento bajo la categoría de seguridad de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de advertencia de cifrado

La acción de alerta de cifrado gestiona la expresión de la información relativa a las advertencias relacionadas con las operaciones o los sistemas de cifrado en un entorno de host específico.

A esta acción, se le puede asignar cualquier tipo de advertencia relativa a las operaciones o a los sistemas de cifrado. Los eventos de mayor severidad deberán asignarse a la acción de error de cifrado. Si la acción está relacionada con el entorno de red, deberá asignarse al mismo evento bajo la categoría de seguridad de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	4

Acción de operación de descifrado

La acción de operación de descifrado gestiona la expresión de la información relativa a las operaciones generales relacionadas con el descifrado en un host.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de estado del descifrado

La acción de estado del descifrado gestiona la expresión de la información relativa al estado de la actividad de descifrado en un host.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Generación de claves

La acción de generación de claves gestiona la expresión de la información relativa a la creación de claves de cifrado o pares de claves para la autenticación de red o cifrado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de creación de firma digital

La acción de creación de firma digital incluye mensajes de firma digital para la integridad y autenticación.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de alerta de cifrado

La acción de alerta de cifrado proporciona información relativa a las alertas de cifrado relacionadas con el nivel de red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de error de cifrado

La acción de error de cifrado incluye información sobre los errores de cifrado genéricos incluidos los errores en la acción de transporte y gestión de claves.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de notificación de cifrado

La acción de notificación de cifrado proporciona información relativa a las notificaciones y los mensajes generados por un motor de cifrado de un dispositivo o una red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de cifrado

La acción de operación de cifrado proporciona información general acerca de las operaciones de cifrado de una red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de cifrado

La acción de estado de cifrado proporciona información relativa al estado de las actividades de cifrado de una red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de cifrado

La acción de advertencia de cifrado proporciona información relativa a las advertencias de cifrado relacionadas con el nivel de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	3

Clase de pérdida de información

Descodificación de una acción de consulta de RPC

La descodificación de una acción de consulta de RPC trata la expresión de información del evento relativa a la detección de la solicitud de asignación de puertos de RPC.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4

Resultado	event_result	event_severity
Incorrecto	F	4
Intento	A	4

Acción de ataque de inserción de SQL

La acción de ataque de inserción de SQL gestiona la supresión de una zona de seguridad para la gestión de un grupo de activos con una política de seguridad unificada.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Acción de uso incorrecto de acceso legítimo

La acción de uso incorrecto de acceso legítimo trata la expresión de información del evento relativa a la detección del uso incorrecto de privilegios de acceso (por ejemplo: descarga de información financiera en el escritorio).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5
Incorrecto	F	4
Intento	A	4

Acción de actividad de reconocimiento

La acción de actividad de reconocimiento trata la actividad relacionada con el reconocimiento de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6
Incorrecto	F	5

Acción de actividad de programas de puerta trasera y troyanos

La acción de actividad de programas de puerta trasera y troyanos trata la expresión de información del evento relativa a la detección de actividad de programas de puerta trasera y troyanos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6

Acción de análisis de vulnerabilidades

La acción de análisis de vulnerabilidades trata la expresión de información del evento relativa a la actividad de detección de análisis.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5
Incorrecto	F	4
Intento	A	4

Clase de actividad de software maligno

Acción de actividad de programas de puerta trasera y troyanos

La acción de adware detectado trata las actividades relacionadas con la detección de actividad de adware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6

Acción de software espía detectado

La acción de software espía detectado trata las actividades relacionadas con la detección de actividad de spyware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6

Acción de gusano detectado

La acción de gusano detectado trata las actividades relacionadas con la detección de actividad de gusanos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6

Acción de actividad de programas de puerta trasera y troyanos

Acción existente - Se etiquetará con las clases de Gramática de eventos Actividad de software maligno o Pérdida de información según el contexto.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6

Acción de clase de gestión de direcciones de red

Acción de creación de grupo de multidifusión

La acción de creación de grupo de multidifusión gestiona la expresión de la información del evento relativa a la creación de un grupo de multidifusión.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de supresión de grupo de multidifusión

La acción de supresión de grupo de multidifusión gestiona la expresión de la información del evento relativa a la supresión de un grupo de multidifusión.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de modificación de grupo de multidifusión

La acción de modificación de grupo de multidifusión gestiona la expresión de la información del evento relativa a la modificación de un grupo de multidifusión, incluyendo los cambios en la pertenencia al grupo.

Información	Nivel
Origen - Información de usuario	Secundario

Información	Nivel
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Clase de escalación de privilegios

Acción de obtención de privilegios de administrador

La acción de obtención de privilegios de administrador trata la expresión de información del evento relativa a la detección de actividad relacionada con la obtención de privilegios de la cuenta de administrador (por ejemplo: ataque de fuerza bruta en una cuenta de administrador).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6
Incorrecto	F	5
Intento	A	5

Acción de actividad de omisión de control

La acción de actividad de omisión de control trata la actividad de firmas que está intentando omitir las restricciones de control mediante la manipulación de privilegios u otros medios.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Incorrecto	F	5

Acción de obtención de privilegios de usuario

La acción de obtención de privilegios de usuario trata la expresión de información del evento relativa a la detección de actividad relacionada con la obtención de privilegios de la cuenta de usuario (por ejemplo: ataque por fuerza bruta en una cuenta SQL con mayores privilegios).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3
Intento	A	3

Acción de clase de la actividad de enrutamiento

Acción de configuración del enrutamiento

La acción de configuración del enrutamiento gestiona la expresión de la información del evento relativa a las rutas de instalación por medio de un proceso manual o automatizado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Clase de infracción de firmas

Acción de infracción de firmas

La acción de infracción de firmas trata la expresión de la información del evento relativa a la detección de una conexión con infracciones entre dos entidades de red según lo que registra un host determinado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6

Clase de actividad sospechosa

Detección de una acción de protocolo no estándar

La detección de una acción de protocolo no estándar trata la expresión de información del evento relativa a la detección de un protocolo no estándar.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4

Detección de una acción de puerto inusual

La detección de una acción de puerto inusual trata la expresión de información del evento relativa a la detección de un puerto inusual.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4

Acción detectada de código ejecutable

La acción detectada de código ejecutable trata la expresión de la información de evento relativa a la detección de código ejecutable en el tráfico de red (por ejemplo: un atacante que ejecuta un código arbitrario).

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5

Acción de ataques varios

La acción de ataques varios trata la expresión de información del evento relativa a la detección de actividad sospechosa que no puede asignarse a una acción de IDS existente que se defina en la Gramática de eventos comunes.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	5
Intento	A	4

Acción de ataque del servicio de nombres

La acción de ataque del servicio de nombres gestiona la expresión de la información del evento relativa a los componentes de ataque del servicio de nombres.

Los ataques de DNS, incluyendo el envenenamiento DNS, y el redireccionamiento pueden asignarse a esta acción.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Acción de enumeración de red

La acción de enumeración de red gestiona la detección de host y dispositivos en una red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Acción de vulnerabilidad de seguridad de la red

La acción de vulnerabilidad de seguridad de la red gestiona la expresión de la información del evento relativa a la vulneración de la seguridad presente en el sistema de red, proceso o marco.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Acción de ataque de puerto

La acción de ataque de puerto gestiona la expresión de la información del evento relativa a la vulnerabilidad de la seguridad de los puertos abiertos.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Acción de vulnerabilidad de la seguridad de las URL

La acción de vulnerabilidad de la seguridad de las URL gestiona la expresión de la información del evento relativa a la vulneración de la seguridad de las URL.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5
Error	F	4

Acción de ataque de VoIP

La acción de ataque de VoIP gestiona la expresión de la información del evento relativa a la vulneración de la seguridad de VoIP.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Error	F	5

Acción de exploración de ping

La acción de exploración de ping proporciona información sobre la exploración de host en la red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Error	F	3

Acción de exploración de puertos

Esta acción expresa información acerca del sondeo de puertos abiertos en el host de la red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Error	F	4

Actividad de posible ataque de fuerza bruta

La acción de actividad de posible ataque de fuerza bruta trata las actividades que indican una posibilidad de ataque de fuerza bruta.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5
Incorrecto	F	5

Acción de explotación de protocolo

Acción existente - Se etiquetará con las clases de Gramática de eventos Denegación de servicio o Actividad sospechosa según el contexto.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Incorrecto	F	5

Acción de comando sospechoso detectado

La acción de comando sospechoso detectado trata las infracciones de firmas de IDS relacionadas con la detección de comandos sospechosos en el tráfico de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5

Acción detectada de nombre de archivo sospechoso

La acción detectada de nombre de archivo sospechoso trata la expresión de información del evento relativa a la detección de nombre de archivo sospechoso.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es qué firma coincide con la conexión de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4

Acción de cadena sospechosa detectada

La acción de cadena sospechosa detectada trata las infracciones de firmas de IDS relacionadas con la detección de cadenas sospechosas en el tráfico de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5

Acción de inicio de sesión sospechoso detectado

La acción de inicio de sesión sospechoso detectado trata las infracciones de firmas de IDS relacionadas con la detección de inicios de sesión sospechosos en el tráfico de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5

Acción de tráfico de túnel detectado

La acción de tráfico de túnel detectado trata la detección de tráfico de túnel.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5

Acción de tráfico no solicitado

La acción de tráfico no solicitado proporciona información acerca de la supresión de tráfico entrante no solicitado a la red.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Error	F	3

Acción de explotación de servidor Web

Acción existente - Se etiquetará con las clases de Gramática de eventos Denegación de servicio o Actividad sospechosa según el contexto.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Incorrecto	F	5

Clase de gestión de servicios Web

Acción de procesamiento de filtro del mensaje

Las acciones de la acción de procesamiento de filtro de mensaje expresan información sobre la validación del mensaje XML. Por ejemplo, información de validación de definición de tipo de documento (DTD).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de procesamiento de filtro del mensaje

Las acciones de la acción de procesamiento de filtro del mensaje expresan información sobre la configuración de filtros para procesar mensajes XML.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de mensaje SOAP

Las acciones de modificación de mensaje SOAP expresan información sobre la alteración de mensajes SOAP.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de descifrado XML

La acción de descifrado XML incluye información sobre el descifrado de datos y representación de los resultados en XML. Los datos pueden resultar arbitrarios (incluido un documento XML), un elemento XML o contenido de elemento XML.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de cifrado XML

La acción de cifrado XML incluye información sobre el cifrado de datos y representación de los resultados en XML. Los datos pueden resultar arbitrarios (incluido un documento XML), un elemento XML o contenido de elemento XML.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de validación de esquema XML

La acción de validación de esquema XML incluye información sobre la validación de datos XML o documentos en el esquema XML.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Capítulo 10: Categoría de seguridad operacional

Esta sección contiene los siguientes temas:

Clase de gestión de aplicaciones (en la página 733)
Clase de gestión del rendimiento de la aplicación (en la página 735)
Clase de gestión de copia de seguridad (en la página 747)
Clase de gestión del dominio (en la página 761)
Clase de actividad de proceso (en la página 768)
Clase de actividad de conexión (en la página 784)
Clase de actividad de puerto y dispositivo (en la página 787)
Clase de gestión de infraestructuras (en la página 814)
Clase de gestión de redes (en la página 867)
Clase de actividad de proceso (en la página 886)
Clase de actividad de registro de seguridad (en la página 892)
Clase de gestión del nivel de servicio (en la página 904)
Clase de actividad del sistema (en la página 923)
Clase de gestión del sistema (en la página 969)
Clase de actividad de virtualización (en la página 982)
Clase de gestión de virtualización (en la página 1030)

Clase de gestión de aplicaciones

Acción de cierre de la aplicación

La acción de cierre de la aplicación gestiona la expresión de la información del evento relativa al cierre de una aplicación de manera interactiva.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de error de aplicaciones

La acción de error de aplicaciones trata los eventos de excepciones o errores que se generan cuando se ejecuta una aplicación. Estos errores pueden deberse a varias condiciones como que falte un archivo, una excepción de tiempo de ejecución o un archivo dañado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión del rendimiento de la aplicación

Acción de métrica de la conexión

La acción de métrica de la conexión gestiona la expresión de la información del evento relativa al seguimiento o control de la métrica y la tendencia del rendimiento o de las operaciones de gestión de la conexión por aplicación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de métrica de la agrupación de conexiones

La acción de métrica de la agrupación de conexiones gestiona la expresión de la información del evento relativa al seguimiento o control de la métrica y la tendencia del rendimiento o de las operaciones de gestión de la agrupación de conexiones por aplicación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de métrica del componente

La acción de métrica del componente gestiona la expresión de la información del evento relativa al seguimiento o control de la métrica y la tendencia del rendimiento o de las operaciones de la actividad del componente dentro de un contexto de aplicación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de métrica de la CPU

La acción de métrica de la CPU gestiona la expresión de la información del evento relativa al seguimiento o control de la métrica y la tendencia del rendimiento o de las operaciones de la utilización de la CPU por aplicación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de métrica del rendimiento de datos

La acción de métrica del rendimiento de datos gestiona la expresión de la información del evento relativa al seguimiento o control de la métrica y la tendencia del rendimiento o de las operaciones del rendimiento de datos por aplicación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de métrica del evento

La acción de métrica del evento gestiona la expresión de la información del evento relativa al seguimiento o control de la métrica y la tendencia del rendimiento o de las operaciones de la generación del evento por aplicación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de métrica de la memoria

La acción de métrica de la memoria gestiona la expresión de la información del evento relativa al seguimiento o control de la métrica y la tendencia del rendimiento o de las operaciones de la utilización de la memoria por una aplicación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de métrica de la mensajería

La acción de métrica de la mensajería gestiona la expresión de la información del evento relativa al seguimiento o control de la métrica del rendimiento o de las operaciones y a la tendencia de la actividad de mensajería de una aplicación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de métrica del método

La acción de métrica del método gestiona la expresión de la información del evento relativa al seguimiento o control de la métrica del rendimiento o de las operaciones y a la tendencia de la ejecución del método de una aplicación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de métrica del programa

La acción de métrica del programa gestiona la expresión de la información del evento relativa al seguimiento o control de la métrica del rendimiento o de las operaciones y a la tendencia de un programa específico que forma parte de una aplicación global.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de métrica del socket

La acción de métrica del socket gestiona la expresión de la información del evento relativa al seguimiento o control de la métrica del rendimiento o de las operaciones y a la tendencia de la actividad de mensajería de una aplicación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de métrica del grupo de subprocesos

La acción de métrica del grupo de subprocesos gestiona la expresión de la información del evento relativa al seguimiento o control de la métrica del rendimiento o de las operaciones y a la tendencia de la gestión del grupo de subprocesos de una aplicación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Clase de gestión de copia de seguridad

Acción de creación de registro de auditoría

La acción de creación de registro de auditoría proporciona información relativa a la creación de registros de auditoría en un sistema o una aplicación determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Secundario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado un registro de auditoría en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de alerta de copia de seguridad

La acción de alerta de copia de seguridad proporciona información sobre las condiciones de alerta relacionadas con las operaciones de copia de seguridad. El usuario puede asignar cualquier tipo de alerta sobre las operaciones de copia de seguridad a esta acción. Si se trata de una condición de error que no garantiza atención inmediata, se deberá asignar la alerta a la acción de error de copia se seguridad.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	6

Acción de finalización de copia de seguridad

La acción de finalización de copia de seguridad trata el evento de finalización de cualquier tarea de operación de copia de seguridad genérica.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha completado la tarea de copia de seguridad en qué objeto en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de configuración de copia de seguridad

La acción de configuración de copia de seguridad proporciona información relativa a la configuración de los trabajos y tareas de copia de seguridad. Se puede asignar a esta acción cualquier tipo de acción en la que se defina la configuración de las operaciones de copia de seguridad.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de inicio de copia de seguridad

La acción de inicio de copia de seguridad trata el evento de inicio de cualquier tarea de operación de copia de seguridad genérica.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha iniciado la tarea de copia de seguridad en qué objeto en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de instantánea de datos

La acción de instantánea de datos proporciona información relativa a la realización de copias de un conjunto de datos, archivos y directorios tal y como estaban en un punto concreto del pasado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de copia de seguridad de archivo

La acción de copia de seguridad de archivo trata los eventos relacionados con la realización de copias de seguridad de recursos de archivo.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha iniciado la tarea de copia de seguridad de archivos iniciada en qué objeto de archivo en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de restauración de archivo

La acción de restauración de archivo trata los eventos relacionados con la restauración de un recurso de archivo.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha iniciado la tarea de restauración de archivo en qué objeto de archivo en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de copia de seguridad de imagen

La acción de copia de seguridad de imagen trata los eventos relacionados con la realización de copias de seguridad de una imagen completa del sistema.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha iniciado la tarea de copia de seguridad en qué imagen en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	4

Acción de restauración de imagen

La acción de restauración de imagen trata los eventos relacionados con la restauración de imágenes completas del sistema.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha iniciado la tarea de restauración en qué imagen en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	4

Acción de error de proceso

La acción de error de proceso proporciona información sobre las condiciones de error relativas a un proceso o servicio en un sistema o una aplicación determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Secundario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha generado un error en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de inicio de restauración

La acción de inicio de restauración trata el evento de inicio de cualquier tarea de operación de restauración genérica.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha iniciado la tarea de restauración en qué objeto en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de completado de restauración

La acción de completado de restauración trata el evento de finalización de cualquier tarea de operación de restauración genérica.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha completado la tarea de restauración en qué objeto en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de reversión

La acción de operación de reversión proporciona información relativa a las operaciones de reversión.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión del dominio

Acción de alerta del controlador de dominio

La acción alerta del controlador de dominio gestiona la expresión de la información relativa a las condiciones de la alerta de un controlador de dominio.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	6

Acción de error del controlador de dominio

La acción de error del controlador de dominio gestiona la expresión de la información relativa a las condiciones de error de un controlador de dominio.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	5

Acción de notificación del controlador de dominio

La acción notificación del controlador de dominio gestiona la expresión de la información relativa a las notificaciones o mensajes generados por un controlador de dominio.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de operación del controlador de dominio

La acción de operación del controlador de dominio gestiona la expresión de la información relativa a las operaciones generales del controlador de dominio.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de estado del controlador de dominio

La acción de estado del controlador de dominio gestiona la expresión de la información relativa a las operaciones generales del controlador de dominio.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de advertencia del controlador de dominio

La acción de advertencia del controlador de dominio gestiona la expresión de la información relativa a las advertencias relacionadas con los controladores de dominio.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	4

Acción de modificación de la confianza

La acción de modificación de la confianza gestiona la expresión de la información relativa a la modificación de una relación de confianza existente entre dos dominios.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Clase de actividad de proceso

Acción de error de copia de seguridad

La acción de error de copia de seguridad proporciona información sobre las condiciones de error relativas a procesos de copia de seguridad.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5

Acción de notificación de copia de seguridad

La acción de notificación de copia de seguridad proporciona información general sobre las notificaciones de copia de seguridad.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de copia de seguridad

La acción de advertencia de copia de seguridad proporciona información sobre las advertencias relativas a procesos generales de copia de seguridad. Los eventos más graves se asignan a la acción de error de copia de seguridad.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de simulación de política

La acción de simulación de política trata la expresión de información del evento generada por una simulación de política.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de impresión

La acción trata la impresión.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de proceso

La acción de creación de proceso trata la expresión de información relativa a la creación de un proceso de servicio en un sistema o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario ha creado qué proceso en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de proceso

Eliminación de un vínculo de servicio de niveles de ejecución.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de proceso

Establezca la prioridad inicial de un comando de proceso como "nice" y "renice" en Unix. Modifique la prioridad inicial de un comando de proceso como "renice".

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5
Incorrecto	F	4

Acción de notificación de proceso

La acción de notificación de proceso trata la expresión de información relativa a la notificación de un proceso o servicio en un host determinado en una aplicación o host secundario.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué notificación se ha enviado de qué host a qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de proceso

Las acciones de operación de proceso expresan información sobre la operación de un proceso o servicio en un host determinado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de restauración de proceso

La acción de restauración de proceso trata la expresión de información relativa a la restauración de un proceso o servicio en un sistema o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario ha restaurado qué proceso en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de inicio de proceso

La acción de inicio de proceso trata la expresión de información relativa al inicio de un proceso o servicio en un sistema determinado o aplicación.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario ha iniciado qué proceso en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de detención del proceso

La acción de detención de proceso trata la expresión de información relativa a la detención de un proceso o servicio en un sistema o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario ha detenido qué proceso en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de suspensión de proceso

La acción de suspensión de proceso trata la expresión de información relativa a la suspensión o pausa de un proceso o servicio en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué usuario ha suspendido qué proceso en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de proceso

La acción de advertencia de proceso proporciona información relativa a las advertencias generadas por un proceso o servicio en un sistema o una aplicación determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Secundario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de advertencia de sistema

La acción de advertencia de sistema proporciona información sobre los mensajes de advertencia de un sistema relativos a las funciones principales del sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Clase de actividad de conexión

Acción de notificación de registro de seguridad

La acción de notificación de registro de seguridad proporciona información sobre los mensajes genéricos relacionados con el registro de seguridad, como la carga y descarga de registros.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué mensaje se ha enviado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de bloqueo de terminal

La acción de bloqueo de terminal proporciona información relativa al bloqueo de un terminal en un sistema determinado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué terminal se ha bloqueado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desbloqueo de terminal

La acción de desbloqueo de terminal proporciona información relativa al desbloqueo de un terminal en un sistema determinado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué terminal se ha desbloqueado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de actividad de puerto y dispositivo

Acción de alerta de dispositivo

La acción de alerta de dispositivo proporciona información acerca de las condiciones de alerta relacionadas con un dispositivo. El dispositivo puede ser un componente de hardware como un dispositivo de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem). Se puede asignar a esta acción cualquier tipo de alerta relativa al dispositivo. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de dispositivo.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel	
Resultado - Información	Primario	
Resultado	**event_result**	**event_severity**
Correcto	n/d	n/d
Incorrecto	F	6

Acción de conexión de dispositivo

Actividad de conexión relacionada con dispositivos genéricos (distintos a un HID y dispositivo de almacenamiento).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	4

Acción de creación de dispositivo

La acción de creación de dispositivo proporciona información relativa a la creación de un dispositivo de software o la instalación de un dispositivo de hardware. El dispositivo puede ser un componente de hardware como un dispositivo de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de eliminación de dispositivo

La acción de eliminación de dispositivo proporciona información acerca de la eliminación de dispositivos virtuales en un entorno virtualizado. Los dispositivos virtuales simulan la funcionalidad de componentes de hardware físicos como dispositivos de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de dispositivo

Esta acción expresa información acerca de la modificación de un dispositivo. Un dispositivo puede ser un componente de hardware como un dispositivo de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de notificación de dispositivo

La acción de notificación de dispositivo proporciona información relativa a las notificaciones y los mensajes generados en el dispositivo. El dispositivo puede ser un componente de hardware como un dispositivo de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem). En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de notificación relativa al dispositivo. Utilice la acción de estado de dispositivo si el evento describe el estado de un dispositivo.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de dispositivo

La acción de operación de dispositivo proporciona información acerca de las operaciones generales relacionadas con el funcionamiento de un dispositivo. El dispositivo puede ser un componente de hardware como un dispositivo de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem). Cuando no sea posible asignar un evento registrado como parte de las funciones u operaciones normales de un dispositivo a una acción más específica de la gramática de eventos comunes, se recomienda asignar el evento a esta acción.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de dispositivo

La acción de advertencia de dispositivo proporciona información acerca de las advertencias relacionadas con el dispositivo. El dispositivo puede ser un componente de hardware como un dispositivo de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem). Se puede asignar a esta acción cualquier tipo de advertencia relativa al dispositivo. Los eventos más graves deberán asignarse a la acción de advertencias de dispositivos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de desconexión de dispositivo

Actividad de desconexión relacionada con dispositivos genéricos (distintos a un HID y dispositivo de almacenamiento).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	4

Acción de error de dispositivo

Cualquier error de dispositivo genérico.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	4

Acción de montaje de dispositivo

Montaje de un dispositivo o sistema de archivos (por ejemplo: montaje de NFS, dispositivos de hardware).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario

Información	Nivel
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	4

Acción de pausa de dispositivo

La acción de pausa de dispositivo proporciona información acerca de la pausa temporal de un dispositivo.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de restablecimiento del dispositivo

La acción de restablecimiento del dispositivo gestiona la expresión de la información relativa al restablecimiento de un dispositivo a los valores de configuración originales.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de reanudación de dispositivo

La acción de reanudación de dispositivo proporciona información acerca de la reanudación de las operaciones de un dispositivo tras una pausa temporal.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de cambio del estado del dispositivo

La acción de cambio del estado del dispositivo gestiona la expresión de la información en los cambios realizados al estado de un dispositivo.

Información	Nivel
Origen - Información de usuario	Secundario

Información	Nivel
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de desmontaje de dispositivo

Desmontaje de un dispositivo o sistema de archivos (por ejemplo: montaje de NFS, dispositivos de hardware).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Información	Nivel	
Incorrecto	F	4

Acción de estado de dispositivo

Cualquier mensaje de estado de dispositivo genérico.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de conexión de HID (dispositivo de interfaz humana)

Actividad de conexión relacionada con dispositivos de interfaz humana (HID) como el ratón o el teclado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desconexión de HID (dispositivo de interfaz humana)

Actividad de desconexión relacionada con dispositivos de interfaz humana (HID) como el ratón o el teclado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de error de dirección MAC

La acción de error de dirección MAC proporciona información acerca de los errores relacionados con direcciones MAC.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	5

Acción de inicialización de proceso

La acción de inicialización de proceso proporciona información relativa a la inicialización de un proceso o servicio en un sistema o una aplicación determinados. Estos eventos se generan antes de que se inicie el proceso.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de conexión de dispositivo de almacenamiento

Actividad de conexión relacionada con dispositivos de almacenamiento conectados al sistema (por ejemplo: unidades de disco duro externas o unidades ópticas externas como unidades de CD-ROM, cámaras, escáneres, dispositivos de memoria Flash, PDA).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	4

Acción de desconexión de dispositivo de almacenamiento

Actividad de desconexión relacionada con dispositivos de almacenamiento conectados al sistema (por ejemplo; unidades de disco duro externas o unidades ópticas externas como unidades de CD-ROM, cámaras, escáneres, dispositivos de memoria Flash, PDA).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario

Información	Nivel
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	4

Acción de advertencia de sistema

La acción de advertencia de sistema proporciona información sobre las advertencias de un sistema en relación con las funciones principales del sistema.

Información	Nivel
Origen - Información de usuario	Secundario

Información	Nivel
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Clase de gestión de infraestructuras

Acción de advertencia de agente

La acción de advertencia de agente proporciona información acerca de las condiciones de advertencia relacionadas con un agente. Se entiende por agente cualquier componente de software o hardware controlado por un componente del gestor. Se puede asignar a esta acción cualquier tipo de advertencia relativa al agente. Los eventos más graves deberán asignarse a la acción de error de agente. No se deberá asignar la alerta a aquellos campos de la gramática de eventos comunes que empiecen por agent_, ya que dichos campos están relacionados con los agentes de CA Enterprise Log Manager.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de conflicto de direcciones

La acción de conflicto de direcciones gestiona la expresión de la información del evento relativa a los conflictos en el espacio de las direcciones de la empresa.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Error	F	N/D

Acción de métrica del agente

La acción de métrica del agente gestiona la expresión de la información del evento relativa al seguimiento o control de la métrica del rendimiento o de las operaciones y a la tendencia de un agente.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de restablecimiento del agente

La acción de restablecimiento del agente gestiona la expresión de la información del evento relativa al restablecimiento de un agente o cliente.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de métrica del gestor

La acción de métrica del gestor gestiona la expresión de la información del evento relativa al seguimiento o control de la métrica del rendimiento o de las operaciones y a la tendencia de un gestor.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de alerta de denominación

La acción de alerta de denominación gestiona la expresión de la información relativa a las alertas relacionadas con la denominación de activos como los conflictos de denominación, las incidencias de la política de denominación y otras infracciones de denominación genéricas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	5

Acción de notificación de denominación

La acción de notificación de denominación gestiona la expresión de la información relativa a las notificaciones relacionadas con la denominación de activos como los conflictos de denominación, las incidencias de la política de denominación y otras infracciones de denominación genéricas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de advertencia de denominación

La acción de advertencia de denominación gestiona la expresión de la información relativa a las advertencias relacionadas con la denominación de activos como los conflictos de denominación, las incidencias de la política de denominación y otras infracciones de denominación genéricas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	N/D
Error	F	3

Acción de alerta de agente

La acción de alerta de agente proporciona información acerca de las condiciones de alerta relacionadas con un agente que envía informes a un gestor de infraestructuras o un componente de sistema centralizado de características similares. Se entiende por agente cualquier componente de software o hardware controlado por un componente del gestor. Se puede asignar a esta acción cualquier tipo de alerta relativa al agente. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de agente. No se deberá asignar la alerta a aquellos campos de la gramática de eventos comunes que empiecen por agent_, ya que dichos campos están relacionados con los agentes de CA Enterprise Log Manager.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	6

Acción de desactivación de agente

La acción de desactivación de agente proporciona información acerca de la desactivación de un agente en un sistema. Se entiende por agente cualquier componente de software o hardware controlado por un componente del gestor. Cuando se desactiva un agente, el componente del gestor no puede controlar el sistema que ejecuta el agente o no puede obtener información del sistema que ejecuta el agente.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de activación de agente

La acción de activación de agente proporciona información acerca de la activación de un agente en un sistema. Se entiende por agente cualquier componente de software o hardware controlado por un componente del gestor. Cuando se desactiva un agente, el componente del gestor no puede controlar el sistema que ejecuta el agente o no puede obtener información del sistema que ejecuta el agente.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de error de agente

La acción de error de agente proporciona información acerca de las condiciones de error relacionadas con un agente que envía informes a un gestor de infraestructuras o un componente de sistema centralizado de características similares. Se entiende por agente cualquier componente de software o hardware controlado por un componente del gestor. Se puede asignar a esta acción cualquier tipo de error relativo al agente. Los eventos menos graves deberán asignarse a la acción de advertencia de agente. Los eventos más graves que necesiten atención inmediata deberán asignarse a la acción de alerta de agente. No se deberá asignar la alerta a aquellos campos de la gramática de eventos comunes que empiecen por agent_, ya que dichos campos están relacionados con los agentes de CA Enterprise Log Manager.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	5

Acción de modificación de agente

La acción de modificación de agente proporciona información acerca de las modificaciones en cualquier componente del agente.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de notificación de agente

La acción de notificación de agente proporciona información relativa a notificaciones genéricas de agentes. Se entiende por agente cualquier componente de software o hardware controlado por un componente del gestor. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de notificación relativa al agente. Utilice la acción de estado de agente si el evento describe el estado de un agente.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de agente

La acción de operación de agente proporciona información acerca de las operaciones generales relacionadas con el funcionamiento de un agente. Se entiende por agente cualquier componente de software o hardware controlado por un componente del gestor. Cuando no sea posible asignar un evento registrado como parte de las funciones u operaciones normales de un agente a una acción más específica de la gramática de eventos comunes, se recomienda asignar el evento a la acción de operación de agente.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de inicio de agente

La acción de inicio de agente proporciona información relativa al inicio de un agente.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de detención de agente

La acción de detención de agente proporciona información relativa a la detención de un agente.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de finalización de agente

La acción de finalización de agente proporciona información relativa a la finalización de un agente. La finalización de un agente es una acción más abrupta que la desactivación un agente.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Error	F	3

Acción de asignación de alarma

La acción de asignación de alarma proporciona información relativa a la asignación de alarmas a solucionadores de problemas, miembros del personal de asistencia técnica o el sistema de soporte. Una alarma es un objeto que indica la existencia de una condición anómala procesable por el usuario en el entorno gestionado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Primario
Destino - Información de host	Secundario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de alarma

La acción de creación de alarma proporciona información sobre la creación de alarmas en un sistema de supervisión. Una alarma es un objeto que indica la existencia de una condición anómala procesable por el usuario en el entorno gestionado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de alarma

La acción de supresión de alarma proporciona información relativa a la supresión de alarmas de forma automática desde un sistema de supervisión o de forma manual como resultado de la acción de un usuario final o administrador. Una alarma es un objeto que indica la existencia de una condición anómala procesable por el usuario en el entorno gestionado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Información	Nivel	
Incorrecto	F	3

Acción de retractación de alarma

La acción de retractación de alarma proporciona información relativa a la retractación de alarmas de forma automática desde un sistema de supervisión o de forma manual como resultado de la acción de un usuario final o administrador. Una alarma es un objeto que indica la existencia de una condición anómala procesable por el usuario en el entorno gestionado. Por "retractación de alarmas" se entiende la anulación de la correlación de un enlace afirmado entre una alarma y un dispositivo o modelo.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de alarma

La acción de estado de alarma proporciona información relativa a las condiciones de estado de alarmas notificadas por un sistema de supervisión. Una alarma es un objeto que indica la existencia de una condición anómala procesable por el usuario en el entorno gestionado. Es posible modificar el estado de una alarma a fin de indicar el trabajo realizado para solucionar los problemas relacionados con la alarma.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de actualización de alarma

La acción de actualización de alarma proporciona información relativa a la actualización o modificación de una alarma de forma automática desde un sistema de supervisión o de forma manual como resultado de la acción de un usuario final o administrador. Una alarma es un objeto que indica la existencia de una condición anómala procesable por el usuario en el entorno gestionado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de alerta de API

La acción de alerta de API proporciona información acerca de las condiciones de alerta relacionadas con una API. Una API (Interfaz de programación de aplicaciones) es una interfaz que define las distintas formas en las que un programa de aplicación puede interactuar con bibliotecas externas y/o sistemas operativos. Se puede asignar a esta acción cualquier tipo de error relativo a la API. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de API.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	6

Acción de error de API

La acción de error de API proporciona información acerca de las condiciones de error relacionadas con una API. Una API (Interfaz de programación de aplicaciones) es una interfaz que define las distintas formas en las que un programa de aplicación puede interactuar con bibliotecas externas y/o sistemas operativos. Se puede asignar a esta acción cualquier tipo de error relativo a la API. Los eventos menos graves deberán asignarse a la acción de advertencia de API. Los eventos más graves que necesiten atención inmediata deberán asignarse a la acción de alerta de API.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	5

Acción de notificación de API

La acción de notificación de API proporciona información relativa a las notificaciones y mensajes generados en los módulos API. Una API (Interfaz de programación de aplicaciones) es una interfaz que define las distintas formas en las que un programa de aplicación puede interactuar con bibliotecas externas y/o sistemas operativos. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de notificación relativa a la API. Utilice la acción de estado de API si el evento describe el estado de un módulo API.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de API

La acción de operación de API proporciona información acerca de las operaciones generales relacionadas con el funcionamiento de una API. Una API (Interfaz de programación de aplicaciones) es una interfaz que define las distintas formas en las que un programa de aplicación puede interactuar con bibliotecas externas y/o sistemas operativos. Cuando no sea posible asignar un evento registrado como parte de las funciones u operaciones normales de una API a una acción más específica de la gramática de eventos comunes, se recomienda asignar el evento a la acción de operación de API.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de API

La acción de estado de API proporciona información relativa al estado de los módulos API. Una API (Interfaz de programación de aplicaciones) es una interfaz que define las distintas formas en las que un programa de aplicación puede interactuar con bibliotecas externas y/o sistemas operativos. Se puede asignar a esta acción cualquier tipo de evento que describa el estado de los módulos API.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de API

La acción de advertencia de API proporciona información acerca de las condiciones de advertencia relacionadas con una API. Una API (Interfaz de programación de aplicaciones) es una interfaz que define las distintas formas en las que un programa de aplicación puede interactuar con bibliotecas externas y/o sistemas operativos. Se puede asignar a esta acción cualquier tipo de advertencia relativa a la API. Los eventos más graves deberán asignarse a la acción de error de API.

Información	Nivel
Origen - Información de usuario	Terciario

Información	Nivel
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de alerta de aplicación

La acción de alerta de aplicación proporciona información sobre las condiciones de alerta relativas al funcionamiento de una aplicación. Se puede asignar a esta acción cualquier tipo de alerta relativa a la aplicación. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de aplicación. Las alertas relacionadas con procesos en segundo plano como servicios o demonios deberán asignarse a la acción de alerta de proceso.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	6

Acción de inicialización de aplicación

La acción de inicialización de aplicación proporciona información acerca de las operaciones de inicialización relacionadas con el inicio de una aplicación. Al iniciar una aplicación, es posible registrar diversos eventos y mensajes en los registros de auditoría antes de que se registren los eventos de inicio. Los eventos propios de este caso deberán asignarse a la acción de inicialización de aplicación. Los eventos de inicialización relacionados con procesos en segundo plano como servicios o demonios deberán asignarse a la acción de inicialización de proceso.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de aplicación

La acción de operación de aplicación proporciona información acerca de las operaciones generales relacionadas con el funcionamiento de una aplicación. Cuando no sea posible asignar un evento registrado como parte de las funciones u operaciones normales de una aplicación a una acción más específica de la gramática de eventos comunes, se recomienda asignar el evento a esta acción. Los eventos de operaciones relacionados con procesos en segundo plano como servicios o demonios deberán asignarse a la acción de operaciones del proceso.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de aplicación

La acción de estado de aplicación proporciona información relativa al estado de una aplicación. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de mensaje de estado relativo a una aplicación. Los eventos de estado relacionados con procesos en segundo plano como servicios o demonios deberán asignarse a la acción de estado de proceso.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de carga masiva de datos

La acción de carga masiva de datos proporciona información relativa a la carga o la importación de datos u objetos externos en bloques o de forma masiva en una aplicación o un sistema.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de notificación de cola de registro

La acción de notificación de cola de registro proporciona información acerca de las notificaciones relacionadas con las colas de registros.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de cola de registro

La acción de advertencia de cola de registro proporciona información acerca de las advertencias relacionadas con las colas de registros.

Información	Nivel
Origen - Información de usuario	Terciario

Información	Nivel
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de estado de modelo

La acción de estado de modelo proporciona información acerca del estado de un modelo.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de cambio de estado de objeto

La acción de cambio de estado de objeto proporciona información relativa a la modificación del estado de un objeto controlado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de estado crítico de objeto

Esta acción expresa información acerca de un objeto en condición crítica. Un objeto puede ser un sistema, un dispositivo, una aplicación o cualquier elemento lógico o físico de la configuración.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	4

Acción de estado normal de objeto

Esta acción expresa información acerca de un objeto que se encuentra en condición normal. Un objeto puede ser un sistema, un dispositivo, una aplicación o cualquier elemento lógico o físico de la configuración.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de estado de objeto sin conexión

Esta acción expresa información acerca de un objeto sin conexión. Un objeto puede ser un sistema, un dispositivo, una aplicación o cualquier elemento lógico o físico de la configuración.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	3

Acción de advertencia de estado de objeto

Esta acción expresa información acerca de un objeto que se encuentra en condición de advertencia. Un objeto puede ser un sistema, un dispositivo, una aplicación o cualquier elemento lógico o físico de la configuración.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	3

Acción de error de coincidencia del software

La acción de error de coincidencia del software proporciona información relativa a la detección de versiones de software incompatibles o no coincidentes en un sistema.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	n/d	n/d

Acción de adición de sistema

La acción de adición de sistema informa acerca del registro o la adición de un sistema a una plataforma de gestión de infraestructuras para control y gestión. Si el usuario desea registrar la adición de plataformas de gestión virtuales como VMware vCenter, deberá asignarse el evento a la acción de adición de sistema ubicada en la clase de gestión de virtualización.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Información	Nivel	
Error	F	3

Acción de detección de sistema

La acción de detección de sistema proporciona información relativa a la detección de un sistema de gestión o control.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de umbral excedido

La acción de umbral excedido proporciona información relativa a la detección de una condición en la que se exceden los umbrales establecidos en la configuración del sistema.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Clase de gestión de redes

Acción de alerta de red

La acción de alerta de red proporciona información acerca de las condiciones de alerta relacionadas con las redes. Se puede asignar a esta acción cualquier tipo de alerta relativa a la red. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	6

Acción de creación de red

La acción de creación de red proporciona información acerca de la creación de una red en un sistema de redes físico o virtual.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de supresión de red

La acción de supresión de red proporciona información acerca de la creación de una red en un sistema de redes físico o virtual.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de error de red

La acción de error de red proporciona información acerca de las condiciones de error relacionadas con las redes. Se puede asignar a esta acción cualquier tipo de error relativo a la red. Los eventos menos graves deberán asignarse a la acción de advertencia de red. Los eventos más graves que necesiten atención inmediata deberán asignarse a la acción de alerta de red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	5

Acción de modificación de red

La acción de modificación de red proporciona información acerca de la modificación o actualización de una red en un sistema de redes físico o virtual.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de notificación de red

La acción de notificación de red proporciona información relativa a las notificaciones y los mensajes generados en las redes. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de notificación relativa a la red. Utilice la acción de estado de red si el evento describe el estado de una red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de red

La acción de estado de red proporciona información relativa al estado de las redes. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de mensaje de estado relativo a la red.

Información	Nivel
Origen - Información de usuario	Terciario

Información	Nivel
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de red

La acción de advertencia de red proporciona información acerca de las advertencias relacionadas con una red.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de alerta de SNMP

La acción de alerta de SNMP proporciona información acerca de las condiciones de alerta relacionadas con el SNMP. El Protocolo simple de administración de redes (SNMP) se utiliza en sistemas de gestión de redes para controlar los dispositivos conectados a una red con el objetivo de detectar la existencia de condiciones que requieran atención inmediata. Se puede asignar a esta acción cualquier tipo de alerta relacionada con el SNMP. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de SNMP.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	6

Acción de error de SNMP

La acción de error de SNMP proporciona información acerca de las condiciones de error relacionadas con el SNMP. El Protocolo simple de administración de redes (SNMP) se utiliza en sistemas de gestión de redes para controlar los dispositivos conectados a una red con el objetivo de detectar la existencia de condiciones que requieran atención inmediata. Se puede asignar a esta acción cualquier tipo de error relacionado con el SNMP. Los eventos menos graves deberán asignarse a la acción de advertencia de SNMP. Los eventos más graves que necesiten atención inmediata deberán asignarse a la acción de alerta de SNMP.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	5

Acción de notificación de SNMP

La acción de notificación de SNMP proporciona información relativa a las notificaciones y los mensajes generados a partir del SNMP. El Protocolo simple de administración de redes (SNMP) se utiliza en sistemas de gestión de redes para controlar los dispositivos conectados a una red con el objetivo de detectar la existencia de condiciones que requieran atención inmediata. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de notificación relativa al SNMP. Utilice la acción de estado de SNMP si el evento describe el estado de un SNMP.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de SNMP

La acción de operación de SNMP proporciona información acerca de las operaciones generales relativas al funcionamiento del SNMP. Cuando no sea posible asignar un evento registrado como parte de las funciones normales del SNMP o una operación a una acción más específica de la gramática de eventos comunes, se recomienda asignar el evento a esta acción.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de SNMP

La acción de estado de SNMP proporciona información relativa al estado del SNMP. El Protocolo simple de administración de redes (SNMP) se utiliza en sistemas de gestión de redes para controlar los dispositivos conectados a una red con el objetivo de detectar la existencia de condiciones que requieran atención inmediata. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de mensaje de estado relativo al SNMP.

Información	Nivel
Origen - Información de usuario	Terciario

Información	Nivel
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de SNMP

La acción de advertencia de SNMP proporciona información acerca de las condiciones de advertencia relacionadas con el SNMP. El Protocolo simple de administración de redes (SNMP) se utiliza en sistemas de gestión de redes para controlar los dispositivos conectados a una red con el objetivo de detectar la existencia de condiciones que requieran atención inmediata. Se puede asignar a esta acción cualquier tipo de advertencia relacionada con el SNMP. Los eventos más graves deberán asignarse a la acción de error de SNMP.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de creación de VLAN

La acción de creación de VLAN proporciona información acerca de la creación de un VLAN en un sistema de redes físico o virtual.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de supresión de VLAN

La acción de supresión de VLAN proporciona información acerca de la supresión de un VLAN en un sistema de redes físico o virtual.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de modificación de VLAN

La acción de modificación de VLAN proporciona información acerca de la modificación o actualización de un VLAN en un sistema de redes físico o virtual.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Clase de actividad de proceso

Acción de alerta de proceso

La acción de alerta de proceso proporciona información relativa a las alertas generadas mediante un proceso o servicio en un sistema o una aplicación determinados. Un proceso es un programa que se ejecuta en segundo plano, como un demonio de UNIX o un servicio de Windows. Se puede asignar a esta acción cualquier tipo de condición de alerta relacionada con el proceso. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de proceso.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	6

Acción de proceso desactivado

La acción de proceso desactivado proporciona información acerca del estado de un proceso detenido. El usuario puede asignar eventos a la acción de detención de proceso para registrar la acción de detención. Si el evento simplemente indica que el estado está desactivado, se deberá asignar a la acción de proceso desactivado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	4

Acción de reanudación de proceso

La acción de reanudación de proceso proporciona información acerca de la reanudación de un proceso o servicio en un sistema o una aplicación determinados. Un proceso es un programa que se ejecuta en segundo plano, como un demonio de UNIX o un servicio de Windows.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de proceso

La acción de estado de proceso proporciona información relativa al estado de un proceso o servicio en un sistema o una aplicación determinados. Un proceso es un programa que se ejecuta en segundo plano, como un demonio de UNIX o un servicio de Windows. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de mensaje de estado relativo a un proceso.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de iniciación de tarea

La acción de iniciación de tarea proporciona información relativa al inicio de una tarea ya programada.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Clase de actividad de registro de seguridad

Acción de configuración de registro

La acción de configuración de registro proporciona información acerca de la configuración de registros con ajustes como la adición de filtros a los registros o la omisión de determinadas acciones.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	n/d	n/d

Acción de ejecución de política

La acción de ejecución de política proporciona información relativa a la ejecución de políticas.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de acceso al registro de seguridad

Esta acción expresa información acerca del acceso a los registros de seguridad.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de alerta de registro de seguridad

La acción de alerta de registro de seguridad proporciona información acerca de las condiciones de alerta relacionadas con el registro de seguridad. El usuario puede asignar cualquier tipo de alerta de registro de seguridad a esta acción. Si una condición de error no garantiza la atención inmediata, se deberá asignar a la acción de error de registro de seguridad.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	6

Acción de supresión de registro de seguridad

La acción de supresión de registro de seguridad trata la expresión de información relativa al inicio de un proceso o servicio en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha suprimido el registro de seguridad en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	6
Incorrecto	F	6

Acción de error de registro de seguridad

La acción de error de registro de seguridad proporciona información acerca de las condiciones de error relacionadas con el registro de seguridad. El usuario puede asignar cualquier tipo de error de registro de seguridad a esta acción. Se pueden asignar eventos menos severos a la acción de advertencia de registro de seguridad. Se pueden asignar eventos más severos que garanticen la acción inmediata para la acción de alerta de registro de seguridad.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	5

Acción de supresión de registro de seguridad

La acción de supresión de registro de seguridad trata la expresión de información relativa al ciclo de archivos de registro en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host ha suprimido los registros de seguridad. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de registro de seguridad

La acción de advertencia de registro de seguridad proporciona información acerca de las advertencias relacionadas con el registro de seguridad. El usuario puede asignar cualquier tipo de advertencia de registro de seguridad a esta acción. Se pueden asignar eventos más severos a la acción de error de registro de seguridad.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	4

Acción de configuración de auditoría del sistema

Esta acción expresa información acerca de la modificación de la configuración de auditoría del sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Error	F	3

Acción de desactivación de auditoría del sistema

Esta acción expresa información acerca de la desactivación de una auditoría de nivel del sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Error	F	3

Acción de activación de auditoría del sistema

Esta acción expresa información acerca de la activación de una auditoría de nivel del sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de ejecución de tarea

La acción de ejecución de tarea proporciona información relativa a la ejecución de tareas.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión del nivel de servicio

Acción de degradación moderada del servicio

Esta acción expresa información acerca de una degradación del servicio de nivel moderado.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	4

Acción de alerta de servicio

La acción de alerta de servicio proporciona información sobre las condiciones de alerta relacionadas con el servicio. El usuario puede asignar cualquier tipo de alerta relacionada con el servicio a esta acción. Los eventos más graves deberán asignarse a la acción de error del servicio.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	6

Acción de servicio desactivado

La acción de servicio desactivado proporciona información acerca del cierre total del servicio.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	6

Acción de error de servicio

La acción de error de servicio proporciona información sobre las condiciones de error relacionadas con el servicio.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	5

Acción de notificación de servicio

La acción de notificación de servicio proporciona información sobre los mensajes y notificaciones generadas por un servicio. Cuando un evento forma parte de las funciones normales del servicio, o cuando no se puede asignar el evento a una acción más específica de la gramática de eventos comunes, se recomienda asignar el evento a esta acción.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de operación de servicio

La acción de operación de servicio proporciona información general sobre las operaciones de servicio. En el caso de que no se pueda asignar el evento a una acción más específica, el usuario podrá asignar cualquier tipo de mensaje sobre el estado del servicio a esta acción.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de estado de servicio

La acción de estado de servicio proporciona información general acerca del estado del servicio.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de servicio no disponible.

La acción de servicio no disponible proporciona información acerca de en un servicio no disponible.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	5

Acción de advertencia de servicio

La acción de advertencia de servicio proporciona información acerca de advertencias relacionadas con el servicio. En el caso de que no se pueda asignar el evento a una acción más específica, el usuario podrá asignar cualquier tipo de mensaje de estado relacionado con el servicio a esta acción.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	4

Acción de degradación grave del servicio

Esta acción expresa información acerca de una degradación del servicio de nivel grave.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	5

Acción de alerta de SLA

La acción de alerta de SLA proporciona información acerca de las condiciones de alerta relacionadas con un SLA. Un contrato de nivel de servicio (SLA) es la parte de un contrato de servicio en la que se define oficialmente el nivel de servicio. Se puede asignar a esta acción cualquier tipo de alerta relacionada con el SLA. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de SLA.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	6

Acción de error de SLA

La acción de error de SLA proporciona información acerca de las condiciones de error relacionadas con un SLA. Un contrato de nivel de servicio (SLA) es la parte de un contrato de servicio en la que se define oficialmente el nivel de servicio. Se puede asignar a esta acción cualquier tipo de error relacionado con un SLA. Los eventos menos graves deberán asignarse a la acción de advertencia de SLA. Los eventos más graves que necesiten atención inmediata deberán asignarse a la acción de alerta de SLA.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	5

Acción de notificación de SLA

La acción de notificación de SLA proporciona información acerca de las notificaciones y los mensajes generados en relación con la actividad del SLA. Un contrato de nivel de servicio (SLA) es la parte de un contrato de servicio en la que se define oficialmente el nivel de servicio. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de notificación relativa a la actividad del SLA. Utilice la acción de estado de SLA si el evento describe el estado de un SLA.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de SLA

La acción de operación de SLA proporciona información acerca de las operaciones generales relativas a un SLA. Cuando no sea posible asignar un evento registrado como parte de la gestión de SLA a una acción más específica de la gramática de eventos comunes, se recomienda asignar el evento a esta acción.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de SLA

La acción de estado de SLA proporciona información relativa al estado de un SLA. Un contrato de nivel de servicio (SLA) es la parte de un contrato de servicio en la que se define oficialmente el nivel de servicio. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de mensaje de estado relativo a un SLA.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de SLA

La acción de advertencia de SLA proporciona información acerca de las condiciones de advertencia relacionadas con un SLA. Un contrato de nivel de servicio (SLA) es la parte de un contrato de servicio en la que se define oficialmente el nivel de servicio. Se puede asignar a esta acción cualquier tipo de advertencia relacionada con un SLA. Los eventos más graves deberán asignarse a la acción de error de SLA.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de degradación ligera del servicio

Esta acción expresa información acerca de una degradación del servicio de nivel menor.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	3

Clase de actividad del sistema

Acción de alerta de firmware

La acción de alerta de firmware proporciona información acerca de las condiciones de alerta relacionadas con el firmware. Se puede asignar a esta acción cualquier tipo de alerta relativa al firmware. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de firmware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	6

Acción de error de firmware

La acción de error de firmware proporciona información acerca de las condiciones de error relacionadas con el firmware. Se puede asignar a esta acción cualquier tipo de error relativo al firmware. Los eventos menos graves deberán asignarse a la acción de advertencia de firmware. Los eventos más graves que necesiten atención inmediata deberán asignarse a la acción de alerta de firmware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	5

Acción de notificación de firmware

La acción de notificación de firmware proporciona información relativa a las notificaciones y los mensajes generados en el firmware. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de notificación relativa al firmware. Utilice la acción de estado de firmware si el evento describe el estado del firmware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de firmware

La acción de estado de firmware proporciona información relativa al estado del firmware. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de mensaje de estado relativo al firmware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de firmware

La acción de advertencia de firmware proporciona información acerca de las advertencias relacionadas con el firmware. Se puede asignar a esta acción cualquier tipo de advertencia relativa al firmware. Los eventos más graves deberán asignarse a la acción de error de firmware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de alerta de hardware

La acción de alerta de hardware proporciona información sobre las condiciones de alerta relacionadas con el hardware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	6

Acción de notificación de hardware

La acción de notificación de hardware proporciona información sobre las notificaciones y los mensajes generados por el hardware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de hardware

La acción de operación de hardware proporciona información general sobre las funciones del hardware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de hardware

La acción de estado de hardware proporciona información sobre el estado del hardware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de hardware

La acción de advertencia de hardware proporciona información sobre las advertencias relacionadas con el hardware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de actividad de registro

Actividad de registro genérico como la generación de informes de registros recopilados, análisis de registros, etc.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Primario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de alerta de registro

La acción de alerta de registro proporciona información acerca de las condiciones de alerta relacionadas con el registro. El usuario puede asignar cualquier tipo de alerta relacionada con el registro a esta acción. Los eventos más graves deberán asignarse a la acción de error del registro.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	6

Acción de supresión de registros

Esta acción expresa información acerca de la supresión de los archivos de registro.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Error	F	3

Acción de error de registro

La acción de error de registro proporciona información acerca de las condiciones de error relacionadas con los registros y la infraestructura de auditoría.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	5

Acción de notificación de registro

La acción de notificación de registro proporciona información acerca de las notificaciones y los mensajes generados en un sistema de registro.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de inicio de registro

Esta acción expresa información acerca del inicio de las operaciones de registro.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de detención de registro

Esta acción expresa información acerca de la detención de las operaciones de registro.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	3
Error	F	3

Acción de advertencia de registro

La acción de advertencia de registro proporciona información acerca de las advertencias relacionadas con el sistema de registro.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de supresión de inconvenientes.

Una acción genérica que puede aplicarse a cualquier producto de terceros como un antivirus que elimina macros, archivos ejecutables, etc.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Primario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de servicio no disponible

La acción de servicio no disponible proporciona información acerca de la falta de disponibilidad de un servidor.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	n/d	n/d

Acción de alerta de sistema

La acción de alerta de sistema informa acerca de las alertas relacionadas con un sistema. El usuario puede asignar cualquier tipo de alerta o alarma sobre el sistema a esta acción. Si una condición de error no garantiza la atención inmediata, se deberá asignar a la acción de error de sistema.

Información	**Nivel**
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	**event_result**	**event_severity**
Error	F	6

Acción de alerta de entorno de sistema

La acción de alerta de entorno de sistema proporciona información acerca de las alertas relacionadas con componentes del entorno como voltaje, potencia, calor, o humedad.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	6

Acción de error del sistema

Las acciones de error del sistema expresan información sobre las funciones principales del sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5

Acción de inicialización de sistema

La acción de inicialización de sistema proporciona información relativa a la inicialización de un sistema.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de conmutación de sistema

La acción de conmutación de sistema proporciona información relativa a las actividades de conmutación en entornos de alta disponibilidad.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de notificación del sistema

Las acciones de notificación del sistema expresan información de notificación sobre las funciones principales del sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de pausa del sistema

La acción de pausa del sistema trata la expresión de la información relativa a la pausa del sistema o aplicación.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha pausado qué sistema en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	3

Acción de restablecimiento de sistema

La acción de restablecimiento de sistema proporciona información acerca de restablecimientos inesperados del sistema debido a condiciones graves.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Error	F	5

Acción de alerta de recurso de sistema

La acción de alerta de recurso de sistema informa acerca de las alertas relacionadas con los recursos del sistema. El usuario puede asignar cualquier tipo de alerta o alarma sobre los recursos del sistema a esta acción. Si una condición de error no garantiza la atención inmediata, se deberá asignarla a la acción de error de recurso.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	6

Acción de error de recurso de sistema

La acción de error de recurso de sistema proporciona información relativa a las condiciones de error generadas durante la asignación o la creación de recursos de sistemas como el espacio de intercambio de memoria en un sistema o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d

Información	Nivel	
Incorrecto	F	5

Acción de advertencia de recurso de sistema

La acción de advertencia de recurso de sistema proporciona información relativa a las advertencias generadas durante la asignación o la creación de recursos de sistemas como el espacio de intercambio de memoria en un sistema o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de reinicio del sistema

La acción de reinicio del sistema trata la expresión de información relativa al reinicio del sistema.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Secundario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	6
Incorrecto	F	7

Acción de reanudación del sistema

La acción de reanudación del sistema trata la expresión de la información relativa a la reanudación del sistema o aplicación.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha reanudado qué sistema en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de guardado de sistema

La acción de guardado de sistema proporciona información relativa al guardado del estado de un sistema.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de cierre del sistema

La acción de cierre del sistema trata la expresión de información relativa al cierre de un proceso o servicio en un sistema determinado o aplicación.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

La información importante para esta acción es quién ha apagado qué sistema en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	7
Incorrecto	F	7

Acción de inicio del sistema

La acción de inicio del sistema trata la expresión de información relativa al inicio de un proceso o servicio en un sistema determinado o aplicación.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha iniciado qué sistema en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	6

Acción de estado del sistema

La acción de estado del sistema trata la expresión de información relativa al inicio de un proceso o servicio en un sistema determinado o aplicación.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué estado se ha informado para qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de sistema no disponible

La acción de sistema no disponible proporciona información acerca de la detección de una condición en la que un sistema no está disponible para procesar solicitudes o funciones.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5
Incorrecto	n/d	n/d

Acción de advertencia de sistema

La acción de advertencia de sistema proporciona información sobre las advertencias relacionadas con componentes de software.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de alerta de confianza

La acción de alerta de confianza proporciona información sobre las condiciones de alerta relacionadas con el establecimiento, la gestión y el control de la confianza entre dos sistemas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de error de confianza

La acción de error de confianza proporciona información sobre las condiciones de error relacionadas con el establecimiento, la gestión y el control de la confianza entre dos sistemas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de notificación de confianza

La acción de notificación de confianza proporciona información sobre las notificaciones y los mensajes relacionados con el establecimiento, la gestión y el control de la confianza entre dos sistemas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de confianza

La acción de operación de confianza proporciona información general sobre las operaciones relacionadas con el establecimiento, la gestión y el control de la confianza entre dos sistemas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de confianza

La acción de estado de confianza proporciona información relativa al estado de la confianza entre dos sistemas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de confianza

La acción de advertencia de confianza proporciona información sobre las advertencias relacionadas con el establecimiento, la gestión y el control de la confianza entre dos sistemas.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	3

Clase de gestión del sistema

Acción de error de licencia

La acción de alerta de licencia proporciona información acerca de las condiciones de alerta relacionadas con la licencia. El usuario puede asignar cualquier tipo de alerta de licencia a esta acción. Si una condición de error no garantiza la atención inmediata, se deberá asignarla a la acción de error de licencia.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de caducidad de licencia

La acción de caducidad de licencia trata la expresión de información del evento acerca de la caducidad de las claves o licencia de productos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de notificación de licencia

La acción de notificación de licencia proporciona información sobre las notificaciones relacionadas con las licencias de software o hardware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de licencia

Todas las actividades relacionadas con las operaciones de licencia como la adición de información de licencia.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de infracción de licencia

La acción de infracción de licencia proporciona información relativa a las infracciones de licencias de software o hardware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de licencia

La acción de advertencia de licencia proporciona información sobre las advertencias relativas a las licencias de software o hardware.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de instalación de servicio

La acción de instalación de servicio trata la expresión de información relativa al nuevo servicio que va a instalar el usuario indicado en el asunto como el sistema local.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Primario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Terciario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	4

Acción de desinstalación del servicio

Esta acción expresa información acerca de un servicio que está eliminando el usuario indicado en el asunto.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de instalación de software

Todas las actividades relacionadas con la instalación de software (se realizará un seguimiento del software relacionado con la seguridad en acciones distintas).

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	5

Acción de falta de software

La acción de falta de software proporciona información relativa a la falta del software necesario para una funcionalidad específica.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario

Información	Nivel
Origen - Información de objeto	Secundario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de actualización de software

La acción de actualización de software proporciona información relativa a las actualizaciones de software.

Información	Nivel
Origen - Información de usuario	Terciario

Información	Nivel
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desinstalación de software

Todas las actividades relacionadas con la desinstalación de software (se realizará un seguimiento del software relacionado con la seguridad en acciones distintas).

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Información	Nivel	
Incorrecto	F	5

Clase de actividad de virtualización

Acción de alerta de dispositivo

La acción de alerta de dispositivo proporciona información acerca de las condiciones de alerta relacionadas con un dispositivo virtual. Los dispositivos virtuales simulan la funcionalidad de componentes de hardware físicos como dispositivos de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem). Se puede asignar a esta acción cualquier tipo de alerta relacionada con el dispositivo virtual. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de dispositivo.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	6

Acción de creación de dispositivo

La acción de creación de dispositivo proporciona información relativa a la creación de dispositivos virtuales en un entorno virtualizado. Los dispositivos virtuales simulan la funcionalidad de componentes de hardware físicos como dispositivos de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de eliminación de dispositivo

La acción de eliminación de dispositivo proporciona información relativa a la eliminación de dispositivos virtuales en un entorno virtualizado. La acción de eliminación de dispositivo se encarga de proporcionar información relativa a la eliminación de dispositivos virtuales en un entorno virtualizado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de error de dispositivo

La acción de error de dispositivo proporciona información acerca de las condiciones de error relacionadas con un dispositivo virtual. Los dispositivos virtuales simulan la funcionalidad de componentes de hardware físicos como dispositivos de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem). Se puede asignar a esta acción cualquier tipo de error relacionado con el dispositivo virtual. Los eventos menos graves deberán asignarse a la acción de advertencia de dispositivo. Los eventos más graves que necesiten atención inmediata deberán asignarse a la acción de alerta de dispositivo.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	5

Acción de importación de dispositivo

La acción de importación de dispositivo proporciona información relativa a la importación de dispositivos virtuales en máquinas, sistemas o entornos virtuales. Los dispositivos virtuales simulan la funcionalidad de componentes de hardware físicos como dispositivos de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Información	Nivel	
Incorrecto	F	3

Acción de notificación de dispositivo

La acción de notificación de dispositivo proporciona información relativa a las notificaciones y los mensajes generados por un dispositivo virtual. Los dispositivos virtuales simulan la funcionalidad de componentes de hardware físicos como dispositivos de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem). En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de notificación del dispositivo virtual. Utilice la acción de estado de dispositivo si el evento describe el estado de un dispositivo virtual.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de operación de dispositivo

La acción de operación de dispositivo proporciona información acerca de las operaciones generales relacionadas con el funcionamiento de un dispositivo virtual. Los dispositivos virtuales simulan la funcionalidad de componentes de hardware físicos como dispositivos de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem). Cuando no sea posible asignar un evento registrado como parte de las funciones u operaciones normales de un dispositivo virtual a una acción más específica de la gramática de eventos comunes, se recomienda asignar el evento a esta acción.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de dispositivo

La acción de estado de dispositivo proporciona información relativa al estado de dispositivos virtuales. Los dispositivos virtuales simulan la funcionalidad de componentes de hardware físicos como dispositivos de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem). En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de mensaje de estado relativo a un dispositivo virtual.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de dispositivo

La acción de advertencia de dispositivo proporciona información acerca de las advertencias relacionadas con dispositivos virtuales. Los dispositivos virtuales simulan la funcionalidad de componentes de hardware físicos como dispositivos de red (por ejemplo, un enrutador, un conmutador, una tarjeta de red o un módem). Se puede asignar a esta acción cualquier tipo de advertencia relacionada con el dispositivo virtual. Los eventos más graves deberán asignarse a la acción de advertencia de dispositivo.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de alerta de hipervisor

La acción de alerta de hipervisor proporciona información acerca de las condiciones de alerta relativas a un hipervisor. Se puede asignar a esta acción cualquier tipo de alerta relacionada con el hipervisor. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de hipervisor.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d

Información	Nivel	
Incorrecto	F	3

6

Acción de error de hipervisor

La acción de error de hipervisor proporciona información acerca de las condiciones de error relativas a un hipervisor. Se puede asignar a esta acción cualquier tipo de error relativo al hipervisor. Los eventos menos graves deberán asignarse a la acción de advertencia de hipervisor. Los eventos más graves que necesiten atención inmediata deberán asignarse a la acción de alerta de hipervisor.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	5

Acción de notificación de hipervisor

La acción de notificación de hipervisor proporciona información relativa a las notificaciones y los mensajes generados en un hipervisor. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de notificación relativa al hipervisor. Utilice la acción de estado de hipervisor si el evento describe el estado de un hipervisor.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de hipervisor

La acción de operación de hipervisor proporciona información acerca de las operaciones generales relativas al funcionamiento del hipervisor. Cuando no sea posible asignar un evento registrado como parte de las funciones u operaciones normales de un hipervisor a una acción más específica de la gramática de eventos comunes, se recomienda asignar el evento a esta acción.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de inicio de hipervisor

La acción de inicio de hipervisor proporciona información relativa al inicio de un hipervisor.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de hipervisor

La acción de estado de hipervisor proporciona información acerca del estado de un hipervisor. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de mensaje de estado relativo al hipervisor.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de hipervisor

La acción de advertencia de hipervisor proporciona información acerca de las advertencias relativas a un hipervisor. Se puede asignar a esta acción cualquier tipo de advertencia relacionada con el hipervisor. Los eventos más graves deberán asignarse a la acción de error de hipervisor.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de alerta de imagen

La acción de alerta de imagen proporciona información acerca de las condiciones de alerta relacionadas con la imagen. Una imagen es un paquete de software precompilado, como un disco duro virtual (archivo .vhd) o un disco DVD virtual (archivo .iso), que puede utilizarse para crear o inicializar una máquina virtual. El usuario puede asignar cualquier tipo de alerta de imagen a esta acción. Si se trata de una condición de error que no garantiza atención inmediata, se deberá asignar la alerta a la acción de error de imagen.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	6

Acción de clonación de imagen

La acción de clonación de imagen informa acerca de la clonación de imágenes. Una imagen es un paquete de software precompilado, como un disco duro virtual (archivo .vhd) o un disco DVD virtual (archivo .iso), que puede utilizarse para crear o inicializar una máquina virtual.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de error de imagen

La acción de error de imagen proporciona información acerca de las condiciones de error relacionadas con una imagen de un entorno de virtualización. Una imagen es un paquete de software prefabricado, como un disco duro virtual (archivo .vhd) o un disco DVD virtual (archivo .iso), que puede utilizarse para generar una máquina virtual o crear una instancia de la misma. Se puede asignar a esta acción cualquier tipo de error relacionado con la imagen. Los eventos menos graves deberán asignarse a la acción de advertencia de imagen. Los eventos más graves que necesiten atención inmediata deberán asignarse a la acción de alerta de imagen.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	5

Acción de exportación de imagen

La acción de exportación de imagen proporciona información relativa a la exportación de una imagen de disco o una máquina virtual en un entorno de virtualización. Una imagen es un paquete de software prefabricado, como un disco duro virtual (archivo .vhd) o un disco DVD virtual (archivo .iso), que puede utilizarse para generar una máquina virtual o crear una instancia de la misma.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de imagen

La acción de modificación de imagen proporciona información relativa a las modificaciones realizadas en una imagen de disco o una máquina virtual en un entorno de virtualización. Una imagen es un paquete de software prefabricado, como un disco duro virtual (archivo .vhd) o un disco DVD virtual (archivo .iso), que puede utilizarse para generar una máquina virtual o crear una instancia de la misma.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de notificación de imagen

La acción de notificación de imagen proporciona información relativa a las notificaciones y los mensajes generados a partir de una imagen en un entorno de virtualización. Una imagen es un paquete de software prefabricado, como un disco duro virtual (archivo .vhd) o un disco DVD virtual (archivo .iso), que puede utilizarse para generar una máquina virtual o crear una instancia de la misma. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de notificación relativa a la imagen. Utilice la acción de estado de imagen si el evento describe el estado de una imagen.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel	
Resultado - Información	Primario	
Resultado	**event_result**	**event_severity**
Correcto	S	2
Incorrecto	F	3

Acción de migración de imagen

La acción de migración de imagen proporciona información sobre la migración de imágenes virtuales a través de host. Una imagen es un paquete de software precompilado, como un disco duro virtual (archivo .vhd) o un disco DVD virtual (archivo .iso), que puede utilizarse para crear o inicializar una máquina virtual.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de apertura de imagen

La acción de apertura de imagen proporciona información relativa a la apertura de una imagen de disco o una máquina virtual en un entorno de virtualización. Una imagen es un paquete de software prefabricado, como un disco duro virtual (archivo .vhd) o un disco DVD virtual (archivo .iso), que puede utilizarse para generar una máquina virtual o crear una instancia de la misma.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de imagen

La acción de operación de imagen proporciona información acerca de las operaciones generales relacionadas con el funcionamiento de una imagen en un entorno de virtualización. Una imagen es un paquete de software prefabricado, como un disco duro virtual (archivo .vhd) o un disco DVD virtual (archivo .iso), que puede utilizarse para generar una máquina virtual o crear una instancia de la misma. Cuando no sea posible asignar un evento registrado como parte de las funciones u operaciones normales de una imagen a una acción más específica de la gramática de eventos comunes, se recomienda asignar el evento a esta acción.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de restauración de imagen

La acción de restauración de imagen proporciona información relativa a la restauración de una imagen o la recuperación de una instantánea previa en un entorno de virtualización. Una imagen es un paquete de software prefabricado, como un disco duro virtual (archivo .vhd) o un disco DVD virtual (archivo .iso), que puede utilizarse para generar una máquina virtual o crear una instancia de la misma.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de imagen

La acción de estado de imagen proporciona información relativa al estado de una imagen en un entorno de virtualización. Una imagen es un paquete de software prefabricado, como un disco duro virtual (archivo .vhd) o un disco DVD virtual (archivo .iso), que puede utilizarse para generar una máquina virtual o crear una instancia de la misma. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de mensaje de estado relativo a una imagen.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de imagen

La acción de advertencia de imagen proporciona información acerca de las advertencias relativas a una imagen en un entorno de virtualización. Una imagen es un paquete de software prefabricado, como un disco duro virtual (archivo .vhd) o un disco DVD virtual (archivo .iso), que puede utilizarse para generar una máquina virtual o crear una instancia de la misma. Se puede asignar a esta acción cualquier tipo de advertencia relativa a la imagen. Los eventos más graves deberán asignarse a la acción de error de imagen.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de escritura de imagen

La acción de escritura de imagen proporciona información relativa a la escritura de un archivo de imagen en un entorno de virtualización. Una imagen es un paquete de software prefabricado, como un disco duro virtual (archivo .vhd) o un disco DVD virtual (archivo .iso), que puede utilizarse para generar una máquina virtual o crear una instancia de la misma.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de puerto

La acción de creación de puerto proporciona información relativa a la creación de un puerto virtual.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de eliminación de puerto

La acción de eliminación de puerto proporciona información relativa a la eliminación de un puerto virtual.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de agrupación de recursos

La acción de creación de agrupación de recursos proporciona información sobre la creación de una agrupación de recursos en un host proporcionado. Una agrupación de recursos es una agrupación de CPU, memoria y otros recursos del sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de supresión de agrupación de recursos

La acción de supresión de agrupación de recursos proporciona información sobre la supresión de una agrupación de recursos en un host proporcionado. Una agrupación de recursos es una agrupación de CPU, memoria y otros recursos del sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de modificación de agrupación de recursos

La acción de modificación de agrupación de recursos proporciona información sobre la modificación de una agrupación de recursos en un host proporcionado. Una agrupación de recursos es una agrupación de CPU, memoria y otros recursos del sistema.

Información	Nivel
Origen - Información de usuario	Secundario

Información	Nivel
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de alerta de instantánea

La acción de alerta de instantánea proporciona información acerca de las condiciones de alerta relacionadas con una instantánea. Se puede asignar a esta acción cualquier tipo de alerta relativa a la instantánea. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de instantánea.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d

Información	Nivel	
Incorrecto	F	6

Acción de error de instantánea

La acción de error de instantánea proporciona información acerca de las condiciones de error relativas a instantáneas. Se puede asignar a esta acción cualquier tipo de error relacionado con una instantánea. Los eventos menos graves deberán asignarse a la acción de advertencia de instantánea. Los eventos más graves que necesiten atención inmediata deberán asignarse a la acción de alerta de instantánea.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	5

Acción de advertencia de instantánea

La acción de advertencia de instantánea proporciona información acerca de las condiciones de advertencia relacionadas con instantáneas. Se puede asignar a esta acción cualquier tipo de advertencia relativa a una instantánea. Los eventos más graves deberán asignarse a la acción de error de instantánea.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de creación de sistema

La acción de creación de sistema proporciona información relativa a la creación de un sistema. Este evento se asigna en un entorno virtual.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de eliminación de sistema

La acción de eliminación de sistema proporciona información relativa a la cancelación del aprovisionamiento o la eliminación de un sistema. Este evento se asigna en un entorno virtual.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	n/d	n/d

Acción de exportación de sistema

La acción de exportación de sistema proporciona información relativa a la exportación de un sistema. Este evento se asigna en un entorno virtual.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de importación de sistema

La acción de importación de sistema proporciona información relativa a la importación de un sistema. Este evento se asigna en un entorno virtual.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de instantánea de sistema

La acción de instantánea de sistema proporciona información relativa a la toma de instantáneas en una máquina o una imagen virtuales.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión de virtualización

Acción de creación de aplicación

La acción de creación de aplicación proporciona información acerca de la creación de una aplicación en un entorno de virtualización.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de modificación de aplicación

La acción de modificación de aplicación proporciona información acerca de la modificación de una aplicación en un entorno de virtualización.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de notificación de aplicación

La acción de notificación de aplicación proporciona información relativa a la notificaciones sobre aplicaciones virtualizadas en un entorno de virtualización.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de supresión de aplicación

La acción de supresión de aplicación proporciona información acerca de la supresión de una aplicación en un entorno de virtualización.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de creación de componente

La acción de creación de componente proporciona información acerca de la creación de cualquier tipo de componente en un entorno de virtualización. En este contexto, el componente se refiere a objetos específicos del distribuidor que se crean en un entorno virtual. El usuario puede utilizar el campo dest_objectclass para asignar la clase del componente.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Información	Nivel	
Error	F	3

Acción de supresión de componente

La acción de supresión de componente proporciona información acerca de la supresión de cualquier tipo de componente en un entorno de virtualización. En este contexto, el componente se refiere a objetos específicos del distribuidor que se crean en un entorno virtual. El usuario puede utilizar el campo dest_objectclass para asignar la clase del componente.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de modificación de componente

La acción de modificación de componente proporciona información acerca de la modificación de cualquier tipo de componente en un entorno de virtualización. En este contexto, el componente se refiere a objetos específicos del distribuidor que se crean en un entorno virtual. El usuario puede utilizar el campo dest_objectclass para asignar la clase del componente.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de notificación de componente

La acción de notificación de componente proporciona información relativa a la notificaciones sobre cualquier componente en un entorno de virtualización. En este contexto, el componente se refiere a objetos específicos del distribuidor que se crean en un entorno virtual. El usuario puede utilizar el campo dest_objectclass para asignar la clase del componente.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de activación de sistema

La acción de activación de sistema proporciona información sobre la activación de un sistema en un entorno virtualizado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de adición de sistema

La acción de adición de sistema informa acerca del registro o la adición de un sistema a una plataforma de gestión virtual para control y gestión.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de conexión de sistema

La acción de conexión de sistema proporciona información sobre el establecimiento de una conexión correcta desde una plataforma de gestión virtual a un sistema para control y gestión.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de desconexión de sistema

La acción de desconexión de sistema informa sobre la desconexión de un sistema desde una plataforma de gestión virtual.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de detección de sistema

La acción de detección de sistema proporciona información relativa al descubrimiento de un sistema por una plataforma de gestión virtual.

Información	Nivel
Origen - Información de usuario	Secundario

Información	Nivel
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de modificación del sistema

La acción de modificación de sistema proporciona información sobre la modificación de un sistema en un entorno virtualizado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de eliminación de sistema

La acción de eliminación de sistema informa sobre la eliminación de un sistema desde una plataforma de gestión virtual.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Capítulo 11: Categoría de acceso físico

Esta sección contiene los siguientes temas:

Clase de actividad de acceso físico (en la página 1047)

Clase de actividad de acceso físico

Acción de análisis de identificador

La acción de análisis de identificador trata la expresión de información relativa a la acción física de una identificación que se analiza mediante un explorador de identificaciones en un punto de acceso físico.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Terciario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha analizado el identificador en qué ubicación. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desactivación de cámara

La acción de desactivación de cámara trata la expresión de información relativa a la acción física del establecimiento del estado de desactivación de la cámara.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha desactivado qué cámara en qué ubicación. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de activación de cámara

La acción de activación de cámara trata la expresión de información relativa a la acción física del establecimiento del estado de activación de la cámara.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha activado qué cámara en qué ubicación. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	4

Acción de falta de disponibilidad de la cámara

La acción de falta de disponibilidad de la cámara trata la expresión de información relativa a la disponibilidad de la cámara. Esto puede deberse a la disponibilidad de red, conectividad por cables, etc.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cámara no se encuentra disponible en qué ubicación. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4
Incorrecto	F	4

Acción de cierre de puerta

La acción de cierre de puerta trata la expresión de información relativa a la acción física de cerrar la puerta.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué puerta se ha cerrado en qué ubicación. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	5

Acción de apertura de puerta

La acción de apertura de puerta trata la expresión de información relativa a la acción física de abrir la puerta.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué puerta se ha abierto en qué ubicación. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	5

Acción de cierre de ventana

La acción de cierre de ventana trata la expresión de información relativa a la acción física de cerrar la ventana.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué ventana se ha cerrado en qué ubicación. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	5

Acción de apertura de ventana

La acción de apertura de ventana trata la expresión de información relativa a la acción física de abrir la ventana.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué ventana se ha abierto en qué ubicación. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	4

Capítulo 12: Categoría de acceso a recursos

Esta sección contiene los siguientes temas:

Clase de actividad de aplicación (en la página 1057)
Clase de actividad de directorio (en la página 1059)
Clase de actividad de recursos (en la página 1067)
Clase de control de versión (en la página 1091)

Clase de actividad de aplicación

Acción de acceso a aplicación

La acción de acceso a aplicación proporciona información acerca del acceso a una aplicación.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de acceso a objeto

La acción de acceso a objeto proporciona información acerca del acceso a un objeto de una aplicación. En este contexto, un objeto es cualquier sub-componente de una aplicación, como por ejemplo un objeto COM, DLL, o un objeto compartido.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Clase de actividad de directorio

Acción de alerta de directorio

La acción de alerta de directorio proporciona información acerca de las condiciones de alerta relacionadas con la actividad de un directorio. En este contexto, se entiende por directorio un conjunto distribuido y jerárquico de tecnologías de directorios de propósito general orientadas al objeto, como X.500 y los servicios de directorios LDAP. Se puede asignar a esta acción cualquier tipo de alerta relativa al directorio. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de directorio.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	6

Acción de error de directorio

La acción de error de directorio proporciona información acerca de las condiciones de error relacionadas con la actividad de un directorio. En este contexto, se entiende por directorio un conjunto distribuido y jerárquico de tecnologías de directorios de propósito general orientadas al objeto, como X.500 y los servicios de directorios LDAP. Se puede asignar a esta acción cualquier tipo de error relativo al directorio. Los eventos menos graves deberán asignarse a la acción de advertencia de directorio. Los eventos más graves que necesiten atención inmediata deberán asignarse a la acción de alerta de directorio.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	5

Acción de notificación de directorio

La acción de notificación de directorio proporciona información relativa a las notificaciones y los mensajes generados a partir de la actividad del directorio. En este contexto, se entiende por directorio un conjunto distribuido y jerárquico de tecnologías de directorios de propósito general orientadas al objeto, como X.500 y los servicios de directorios LDAP. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de notificación relativa al directorio. Utilice la acción de estado de directorio si el evento describe el estado de un directorio.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de operación de directorio

La acción de operación de directorio proporciona información acerca de las operaciones generales relacionadas con el funcionamiento de un directorio. En este contexto, se entiende por directorio un conjunto distribuido y jerárquico de tecnologías de directorios de propósito general orientadas al objeto, como X.500 y los servicios de directorios LDAP. Cuando no sea posible asignar un evento registrado como parte de las funciones u operaciones normales de un directorio a una acción más específica de la gramática de eventos comunes, se recomienda asignar el evento a esta acción.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de directorio

La acción de estado de directorio proporciona información relativa al estado de un directorio. En este contexto, se entiende por directorio un conjunto distribuido y jerárquico de tecnologías de directorios de propósito general orientadas al objeto, como X.500 y los servicios de directorios LDAP. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de mensaje de estado relativo a un directorio.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de directorio

La acción de advertencia de directorio proporciona información acerca de las advertencias relacionadas con un directorio. En este contexto, se entiende por directorio un conjunto distribuido y jerárquico de tecnologías de directorios de propósito general orientadas al objeto, como X.500 y los servicios de directorios LDAP. Se puede asignar a esta acción cualquier tipo de advertencia relativa a un directorio. Los eventos más graves deberán asignarse a la acción de error de directorio.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Clase de actividad de recursos

Acción de acceso a recursos

La acción de acceso a recursos trata la solicitud de acceso para un recurso concreto en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha accedido a qué función en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de alerta de recurso

La acción de alerta de recurso proporciona información sobre las condiciones de alerta relacionadas con un recurso concreto de un sistema o una aplicación determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de ubicación de recursos

La acción de ubicación de recursos trata la ubicación de recursos en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha ubicado qué recurso en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de cierre de recurso

La acción de cierre de recurso trata el cierre de un recurso en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha cerrado a qué función en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de copia de recurso

La acción de copia de recurso proporciona información relativa a la copia de un recurso concreto de un sistema o una aplicación determinados en otro sistema.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de recurso

La acción de creación de recurso trata la creación de un recurso determinado en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

La información importante para esta acción es quién ha creado qué recurso en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de recurso

La acción de supresión de recurso trata la supresión de un recurso determinado en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha suprimido qué recurso en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de error de recurso

La acción de error de recurso proporciona información sobre los errores relacionados con un recurso concreto de un sistema o una aplicación determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de ejecución de recurso

La acción de ejecución de recurso trata la ejecución de un recurso determinado en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha ejecutado qué recurso en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de retención de recurso

La acción de retención de recurso proporciona información relativa a la retención de recursos con el objetivo de restringir su eliminación, movimiento, etc.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de importación de recursos

La acción de importación de recursos proporciona información relativa a la importación de un recurso desde un recurso externo.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de enumeración de recursos

Por ejemplo, “lsrset” con varias opciones.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Secundario
Origen - Información de proceso	Secundario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de recurso marcado

La acción de recurso marcado proporciona información sobre el etiquetado, comentario y marcado de recursos de un sistema o una aplicación con metadatos con el objetivo, entre otros, de facilitar la consulta.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de recurso

La acción de modificación de recurso trata la modificación de un recurso determinado en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha modificado qué recurso en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de movimiento de recurso

La acción de movimiento de recurso proporciona información relativa al movimiento de recursos en sistemas o aplicaciones.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de apertura de recurso

La acción de apertura de recurso trata la apertura de un recurso determinado en una aplicación o sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es quién ha abierto qué recurso en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de actualización de recurso

La acción de actualización de recurso proporciona información relativa a la actualización de un recurso concreto como, por ejemplo, archivos en caché en un sistema o una aplicación determinados o recursos en caché en un servidor proxy.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de replicación de recurso

La acción de replicación de recurso proporciona información relativa a la replicación de un recurso de un sistema o una aplicación.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de búsqueda de recursos

La acción de búsqueda de recursos proporciona información relativa a la búsqueda de los recursos de un sistema o una aplicación.

Información	Nivel
Origen - Información de usuario	Terciario

Información	Nivel
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de recurso

La acción de estado de recurso proporciona información relativa al estado de un recurso concreto en una aplicación o un sistema determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de recurso

La acción de advertencia de recurso proporciona información sobre las advertencias relacionadas con un recurso concreto de un sistema o una aplicación determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	3

Acción de definición de ACL

La acción de definición de ACL proporciona información relativa a la creación o la modificación de una lista de control de acceso en un objeto de destino determinado; por ejemplo, un archivo, un proceso, un sistema o una aplicación.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de configuración de criterios de búsqueda

La acción de configuración de criterios de búsqueda proporciona información relativa a los criterios de búsqueda o los artefactos utilizados para extraer los registros y la información de un sistema de archivos o repositorio.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de control de versión

Acción de protección de recurso

La acción de protección de recurso proporciona información relativa a la protección de un recurso con control de versiones mediante métodos HTTP y WebDAV de tipo estándar.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desprotección de recurso

La acción de desprotección de recurso proporciona información relativa a la desprotección de un recurso con control de versiones con el fin de permitir la modificación del contenido o las propiedades inactivas.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de recurso

La acción de creación de recurso proporciona información relativa a la creación de recursos con control de versiones.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de etiqueta de recurso

La acción de modificación de etiqueta de recurso proporciona información relativa a la modificación de una cadena que diferencia una versión incluida en el historial de versiones del resto de versiones de dicho historial.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de combinación de recursos

La acción de combinación de recursos proporciona información relativa a la combinación de los recursos con control de versiones de un usuario con las versiones de recursos creadas por otro usuario.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de búsqueda de recursos

La acción de búsqueda de recursos proporciona información relativa a la búsqueda de recursos con control de versiones.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de cancelación de desprotección de recurso

La acción de cancelación de desprotección de recurso proporciona información sobre las solicitudes aplicadas a un recurso desprotegido con control de versiones con el fin de cancelar la desprotección y restaurar el estado previo a la desprotección del recurso.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de actualización de recurso

La acción de actualización de recurso proporciona información relativa a la modificación de la versión de un recurso protegido con control de versiones, de una versión anterior a la versión actual.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de versión

La acción de estado de versión proporciona información relativa al estado de una versión.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Capítulo 13: Categoría de operaciones SIM

Esta sección contiene los siguientes temas:

Clase de gestión de alerta (en la página 1101)
Clase de gestión de línea de base (en la página 1111)
Clase de gestión de origen de evento (en la página 1117)
Clase de gestión de incidente (en la página 1125)
Clase de gestión de investigación (en la página 1130)
Clase de gestión de notificaciones (en la página 1138)
Clase de gestión de solicitud (en la página 1140)

Clase de gestión de alerta

Acción de confirmación de alerta

La acción de confirmación de alerta trata la confirmación de una alerta en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha confirmado qué alerta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de anotación de alerta

La acción de anotación de alerta trata la anotación de una alerta en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha anotado qué alerta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de alerta

La acción de creación de alerta trata la creación de una alerta en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué alerta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de alerta

La acción de supresión de alerta trata la eliminación de una alerta en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta suprimido qué alerta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de entrega de alerta

La acción de entrega de alerta trata la entrega de una alerta de un host determinado a un host determinado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué alerta se ha entregado a qué host desde qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de escalación de alerta

La acción de escalación de alerta trata la escalación de una alerta en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha escalado qué alerta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de tarea de alerta

Las acciones de modificación de tarea de alerta expresan información acerca de la modificación de tareas programadas para comprobar las condiciones de alerta.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de tarea de alerta

Las acciones de supresión de tarea de alerta expresan información acerca de la supresión de tareas programadas para comprobar las condiciones de alerta.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de configuración de tarea de alerta

Las acciones de configuración de tarea de alerta expresan información acerca de la programación de tareas para comprobar las condiciones de alerta.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de alerta

La acción de modificación de alerta trata la modificación de una alerta en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué alerta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión de línea de base

Acción de aceptación de línea de base

La acción de aceptación de línea de base trata la aceptación de una línea de base en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha aceptado qué línea de base en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de activación de línea de base

La acción de aceptación de línea de base trata la activación de una línea de base en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha activado qué línea de base en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de línea de base

La acción de creación de línea de base trata la creación de una línea de base en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué línea de base en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desactivación de línea de base

La acción de desactivación de línea de base trata la desactivación de una línea de base en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha desactivado qué línea de base en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de establecimiento de línea de base

La acción de establecimiento de línea de base trata la creación de un a línea de base en un host determinado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha establecido qué línea de base en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de línea de base

La acción de modificación de línea de base trata la modificación de una línea de base en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué línea de base en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Clase de gestión de origen de evento

Acción de autorización de origen de evento

La acción de autorización de origen de evento trata la autorización de un origen de evento en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha autorizado qué origen de evento en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de configuración de origen de evento

La acción de configuración de origen de evento trata la configuración de un origen de evento en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha configurado qué origen de evento en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de descubrimiento de origen de evento

La acción de descubrimiento de origen de evento trata el descubrimiento de un origen de evento en un host determinado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host ha descubierto qué origen de evento en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de provisión de origen de evento

La acción de provisión de origen de evento trata el aprovisionamiento de un origen de evento en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha aprovisionado qué origen de evento en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de tendencia de evento

La acción de tendencia de evento trata la expresión de información relativa a todos los datos a los que se tenderá.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha aprovisionado qué origen de evento en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de entrada de datos externos

La acción de entrada de datos externos proporciona información relativa a la importación de datos externos procedentes de otras fuentes en SIM y en herramientas de gestión de registros como CA Enterprise Log Manager para correlaciones de eventos y la creación de informes contextuales.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de salida de datos externos

La acción de salida de datos externos proporciona información relativa a la importación de datos internos desde SIM y herramientas de gestión de registros como CA Enterprise Log Manager a fuentes externas para la automatización de procesos, alertas, etc.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión de incidente

Acción de cierre de incidente

La acción de cierre de incidente trata el cierre de un incidente en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha cerrado qué incidente en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de incidente

La acción de creación de incidente trata la creación de un incidente en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué incidente en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de incidente

La acción de supresión de incidente trata la supresión de un incidente en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué incidente en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de modificación de incidente

La acción de modificación de incidente trata la modificación de un incidente en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué incidente en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de resolución de incidente

La acción de resolución de incidente trata la resolución de un incidente en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha resuelto qué incidente en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión de investigación

Acción de anotación de investigación

La acción de anotación de investigación trata la anotación de una investigación en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha anotado qué investigación en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de cierre de investigación

La acción de cierre de investigación trata el cierre de una investigación en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha cerrado qué investigación en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de investigación

La acción de supresión de investigación trata la supresión de una investigación en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha suprimido qué investigación en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de modificación de investigación

La acción de modificación de investigación trata la modificación de una investigación en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué investigación en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de apertura de investigación

La acción de apertura de investigación trata la apertura de una investigación en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha abierto qué investigación en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de pausa de investigación

La acción de pausa de investigación trata la pausa de una investigación en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha pausado qué investigación en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de resolución de investigación

La acción de resolución de investigación trata la resolución de una investigación en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha resuelto qué investigación en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de reanudación de investigación

La acción de reanudación de investigación trata la reanudación de una investigación pausada en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha reanudado qué investigación pausada en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión de notificaciones

Acción de creación de notificación

La acción de creación de notificación trata la creación de una notificación en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué notificación en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de entrega de notificación

La acción de entrega de notificación trata la entrega de una alerta de un host determinado a un host determinado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué notificación se ha entregado a qué host desde qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de gestión de solicitud

Acción de confirmación de solicitud

La acción de confirmación de solicitud trata la confirmación de una solicitud en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha confirmado qué solicitud en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de anotación de solicitud

La acción de anotación de solicitud trata la anotación de una solicitud en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha anotado qué solicitud en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de cierre de solicitud

La acción de cierre de solicitud trata el cierre de una solicitud en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha cerrado qué solicitud en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de solicitud

La acción de creación de solicitud trata la creación de una solicitud en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha creado qué solicitud en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de entrega de solicitud

La acción de entrega de solicitud trata la entrega de una solicitud de un host determinado a un host determinado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Primario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué solicitud se ha entregado a qué host desde qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de solicitud

La acción de modificación de solicitud trata la modificación de una solicitud en un host determinado.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha modificado qué solicitud en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Capítulo 14: Categoría de acceso al sistema

Esta sección contiene los siguientes temas:

Clase de gestión de accesos (en la página 1147)
Clase de actividad de autenticación (en la página 1152)
Clase de actividad de autorización (en la página 1169)
Clase de actividad de inicio de sesión (en la página 1180)
Clase de actividad de cierre de sesión (en la página 1182)
Clase de obtención de privilegios (en la página 1183)
Clase de uso de privilegios (en la página 1184)
Clase de actividad de sesión (en la página 1185)
Clase de actividad de configuración de usuario (en la página 1197)
Clase de actividad del sistema (en la página 1199)

Clase de gestión de accesos

Acción de creación de dominio de seguridad

La acción de creación de dominio de seguridad proporciona información relativa a la creación de un dominio de seguridad. Un dominio de seguridad es una agrupación de personas, datos, sistemas o dispositivos que debe cumplir una política de seguridad como, por ejemplo, la instrucción de ámbito de una política de seguridad.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de dominio de seguridad

La acción de supresión de dominio de seguridad proporciona información relativa a la supresión de un dominio de seguridad. Un dominio de seguridad es una agrupación de personas, datos, sistemas o dispositivos que debe cumplir una política de seguridad como, por ejemplo, la instrucción de ámbito de una política de seguridad.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de modificación de dominio de seguridad

La acción de modificación de dominio de seguridad proporciona información relativa a la modificación de un dominio de seguridad. Un dominio de seguridad es una agrupación de personas, datos, sistemas o dispositivos que debe cumplir una política de seguridad como, por ejemplo, la instrucción de ámbito de una política de seguridad.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Información	Nivel	
Incorrecto	F	3

Acción de modificación de etiqueta de seguridad

La acción de modificación del dominio de seguridad expresa información acerca de la modificación las etiquetas de seguridad como, por ejemplo, las etiquetas de un entorno de control de acceso obligatorio (MAC).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Clase de actividad de autenticación

Acción de autenticación

La acción de autenticación trata la expresión de información del evento relativa a la autenticación de credenciales ofrecidas para la validación.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es quién ha intentado autenticar como qué cuenta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desactivación de autenticación

La acción de desactivación de autenticación informa sobre la desactivación del módulo de autenticación en un sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5
Error	F	5

Acción de activación de autenticación

La acción de activación de autenticación informa sobre la activación del módulo de autenticación en un sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	5
Error	F	5

Acción de error de autenticación

La acción de error de autenticación proporciona información relativa a las condiciones de error generadas en un módulo de autenticación o durante el proceso de autenticación.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de retroceso de autenticación

La acción de retroceso de autenticación trata la expresión de información del evento relativa al retroceso de autenticación a un método secundario de validación de credenciales.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host ha retrasado qué método de autenticación. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	6

Acción de notificación de autenticación

La acción de notificación de autenticación proporciona información relativa a los mensajes de notificación generados en un módulo de autenticación o durante el proceso de autenticación.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	3

Acción de carga de paquete de autenticación

La acción de carga de paquete de autenticación trata la expresión de información del evento relativa a la carga de un paquete de autenticación para la validación de credenciales en un host o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host ha cargado qué paquete de autenticación. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de inicio de autenticación

La acción de inicio de autenticación trata la expresión de información del evento relativa al inicio de un paquete de autenticación en un host o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué host ha iniciado qué paquete de autenticación. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	6

Acción de advertencia de autenticación

La acción de advertencia de autenticación proporciona información relativa a los mensajes de advertencia generados en un módulo de autenticación o durante el proceso de autenticación.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de autorización

La acción de autorización trata la expresión de información del evento relativa a la autorización de credenciales ofrecidas para la validación.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante de esta acción es quién ha intentado autorizar el acceso como qué cuenta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de creación de territorio de seguridad

La acción de creación de territorio de seguridad proporciona información relativa a la creación de un territorio de seguridad. Un territorio de seguridad es un conjunto de usuarios, grupos o recursos con nombre al que se hace referencia en una política de control de acceso.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de supresión de territorio de seguridad

La acción de supresión de territorio de seguridad proporciona información relativa a la supresión de un territorio de seguridad. Un territorio de seguridad es un conjunto de usuarios, grupos o recursos con nombre al que se hace referencia en una política de control de acceso.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de definición de propiedad de grupo

La acción de definición de propiedad de grupo proporciona información relativa a la modificación de la propiedad de grupo, grupo real o grupo efectivo de los objetos de destino (proceso, archivo, sistema).

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de alerta de territorio de confianza

La acción de alerta de territorio de confianza proporciona información relativa a las condiciones de alerta relacionadas con los territorios de confianza.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	5

Acción de error de territorio de confianza

La acción de error de territorio de confianza proporciona información relativa a los errores relacionados con los territorios de confianza.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	4

Acción de advertencia de territorio de confianza

La acción de advertencia de territorio de confianza proporciona información relativa a las advertencias relacionadas con los territorios de confianza.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	3

Clase de actividad de autorización

Acción de alerta de autorización

La acción de alerta de autorización proporciona información relativa a las condiciones de alerta generadas durante actividades de autorización. Entre las actividades de autorización se incluyen la configuración de permisos sobre los objetos, sistemas o aplicaciones para sujetos como cuentas del sistema o del usuario, host, etc. Se puede asignar a esta acción cualquier tipo de alerta relativa a la autorización. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de autorización.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	6

Acción de error de autorización

La acción de error de autorización proporciona información relativa a las condiciones de error generadas durante las actividades de autorización. Entre las actividades de autorización se incluyen la configuración de permisos sobre los objetos, sistemas o aplicaciones para sujetos como cuentas del sistema o del usuario, host, etc. Se puede asignar a esta acción cualquier tipo de error relativo a la autorización. Los eventos menos graves deberán asignarse a la acción de advertencia de autorización. Los eventos más graves que necesiten atención inmediata deberán asignarse a la acción de alerta de autorización.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Error	F	5

Acción de notificación de autorización

La acción de notificación de autorización proporciona información relativa a las notificaciones emitidas por el sistema o el motor de autorización durante actividades de autorización. Entre las actividades de autorización se incluyen la configuración de permisos sobre los objetos, sistemas o aplicaciones para sujetos como cuentas del sistema o del usuario, host, etc. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de notificación relativa a la autorización. Utilice la acción de estado de autorización si el evento describe el estado de una actividad de autorización.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de autorización

La acción de estado de autorización proporciona información relativa al estado de una actividad de autorización tal como figura en el sistema o el motor de autorización. Entre las actividades de autorización se incluyen la configuración de permisos sobre los objetos, sistemas o aplicaciones para sujetos como cuentas del sistema o del usuario, host, etc. En caso de que no sea posible asignar el evento a una acción más específica, se puede asignar a esta acción cualquier tipo de mensaje de estado relativo una autorización.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de advertencia de autorización

La acción de advertencia de autorización proporciona información relativa a las condiciones de advertencia generadas durante actividades de autorización. Entre las actividades de autorización se incluyen la configuración de permisos sobre los objetos, sistemas o aplicaciones para sujetos como cuentas del sistema o del usuario, host, etc. Se puede asignar a esta acción cualquier tipo de advertencia relativa a la autorización. Los eventos más graves deberán asignarse a la acción de error de autorización.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Acción de finalización de autorización

La acción de finalización de autorización proporciona información relativa a la finalización de la información de autorización, como las credenciales proporcionadas para la validación o la finalización de la configuración del entorno de autorización. Esta acción obligará al sujeto (usuario, proceso o sistema) a repetir la autorización del objeto de destino (sistema, proceso).

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de caducidad de token de autorización

La acción de caducidad de token de autorización proporciona información relativa a la caducidad de un token de autorización proporcionado para la validación durante una sesión de autenticación.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de alerta de permiso

La acción de alerta de permiso proporciona información acerca de las condiciones de alerta relacionadas con los permisos. Se puede asignar a esta acción cualquier tipo de alerta relativa a los permisos. Si se trata de una condición de error que no necesita atención inmediata, la alerta deberá asignarse a la acción de error de permiso.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	6

Acción de error de permiso

La acción de error de permiso proporciona información acerca de las condiciones de error relacionadas con los permisos. Se puede asignar a esta acción cualquier tipo de error relativo a los permisos. Los eventos menos graves deberán asignarse a la acción de advertencia de permiso. Los eventos más graves que necesiten atención inmediata deberán asignarse a la acción de alerta de permiso.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	5

Acción de advertencia de permiso

La acción de advertencia de permiso proporciona información acerca de las advertencias relacionadas con actividades de permisos. Se puede asignar a esta acción cualquier tipo de advertencia relativa a los permisos. Los eventos más graves deberán asignarse a la acción de error de permiso.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	n/d	n/d
Incorrecto	F	4

Clase de actividad de inicio de sesión

Acción de intento de inicio de sesión

La acción de intento de inicio de sesión trata la expresión de información del evento relativa al intento de inicio de sesión de una cuenta en un host o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha intentado iniciar sesión en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de actividad de cierre de sesión

Acción de cierre de sesión

La acción de cierre de sesión trata la expresión de información del evento relativa al cierre de sesión de una cuenta en un host o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es en qué cuenta se ha cerrado la sesión de qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de obtención de privilegios

Acción de obtención de privilegios

La acción de obtención de privilegios trata la expresión de información del evento relativa al intento de la cuenta de obtener privilegios en un host o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha intentado obtener qué privilegio en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3

Resultado	event_result	event_severity
Incorrecto	F	3

Clase de uso de privilegios

Acción de utilización de privilegios

La acción de uso de privilegios trata la expresión de información del evento relativa al intento de la cuenta de usar privilegios en un host o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha intentado usar qué privilegio en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Clase de actividad de sesión

Acción alerta de sesión

La acción de alerta de sesión proporciona información acerca de las condiciones de alerta relacionadas con la sesión. El usuario puede asignar cualquier tipo de alerta de sesión a esta acción. Si se trata de una condición de error que no garantiza atención inmediata, se deberá asignar la alerta a la acción de error de sesión.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	7

Acción de creación de sesión

La acción de creación de sesión trata la creación de una sesión según lo que registra un host o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué sesión se ha creado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de desconexión de sesión

La acción de desconexión de sesión trata la expresión de información del evento relativa a la desconexión de la sesión según lo que registra un host o aplicaciones determinados.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué sesión se ha desconectado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de error de sesión

La acción de error de sesión proporciona información acerca de las condiciones de error relacionadas con la sesión. El usuario puede asignar cualquier tipo de error de sesión a esta acción. Los eventos menos graves deberán asignarse a la acción de advertencia de sesión. Se pueden asignar eventos más severos que garanticen la acción inmediata para la acción de alerta de sesión.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	5

Acción de modificación de sesión

La acción de modificación de sesión trata la modificación de una sesión según lo que registra un host o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Terciario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué sesión se ha modificado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	3
Incorrecto	F	3

Acción de notificación de sesión

La acción de notificación de sesión proporciona información acerca de notificaciones y mensajes generados por la sesión. En el caso de que no se pueda asignar el evento a una acción más específica, el usuario podrá asignar cualquier tipo de notificación de sesión a esta acción. Utilice la acción de estado de sesión si el evento describe el estado de una sesión.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Acción de operación de sesión

La acción de operación de sesión proporciona información general sobre las operaciones de sesión. El usuario puede asignar a esta acción un evento que se registra como parte de las funciones de sesión normales, o un evento que no se puede asignar a una acción de CEG más específica.

Información	Nivel
Origen - Información de usuario	Secundario

Información	Nivel
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Actividad de reconexión de la sesión

La acción "Reconexión de la sesión" trata la expresión de información relativa a cuándo un usuario se vuelve a conectar a una sesión del servidor de terminal desconectado (también denominado "escritorio remoto") en oposición a un inicio de sesión nuevo.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de estado de sesión

La acción de estado de sesión proporciona información relativa al estado de una sesión. En el caso de que no se pueda asignar el evento a una acción más específica, el usuario podrá asignar cualquier tipo de mensaje sobre el estado de la sesión a esta acción.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Información	Nivel	
Error	F	3

Acción de advertencia de sesión

La acción de advertencia de sesión proporciona información sobre las advertencias relacionadas con la sesión. El usuario puede asignar cualquier tipo de advertencia de sesión a esta acción. Se pueden asignar eventos más severos a la acción de error de sesión.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario

Información	Nivel
Resultado - Información	Primario

Resultado	event_result	event_severity
Error	F	4

Acción de validación de sesión

Las acciones de validación de sesión expresan información sobre la validación de una sesión establecida según lo que registra una aplicación o host determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2

Resultado	event_result	event_severity
Incorrecto	F	3

Clase de actividad de configuración de usuario

Acción de alerta de autenticación

La acción de alerta de autenticación proporciona información relativa a cualquier condición de alerta generada en un módulo de autenticación o durante el proceso de autenticación. Las condiciones de alerta requieren atención inmediata.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Secundario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	6

Acción de configuración de usuario

La acción de configuración de usuario trata la expresión de la información de evento relativa al intento de la cuenta de modificar las credenciales de autenticación (ejecución de información de cuenta) en una aplicación o host determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Primario
Destino - Información de host	Primario
Destino - Información de objeto	Terciario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha intentado establecer las credenciales de autenticación en qué cuenta en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de actividad del sistema

Acción de activación de sistema

La acción de activación de sistema expresa información acerca de la activación de un sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Terciario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario

Información	Nivel
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	2
Error	F	3

Capítulo 15: Categoría desconocida

Esta sección contiene los siguientes temas:

Clase desconocida (en la página 1201)

Clase desconocida

Acción de acción desconocida

La acción de acción desconocida se utiliza para asignar todos los eventos que no se pueden clasificar como acción específica en la Gramática de eventos comunes.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Secundario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Terciario
Resultado - Información	Terciario

Resultado	event_result	event_severity
Desconocido	U	0

Capítulo 16: Categoría de gestión de vulnerabilidades

Esta sección contiene los siguientes temas:

Clase de evaluación de vulnerabilidades (en la página 1203)
Clase de descubrimiento de vulnerabilidades (en la página 1208)
Clase de gestión de vulnerabilidades (en la página 1248)

Clase de evaluación de vulnerabilidades

Acción de recopilación de información

La acción de recopilación de información trata la expresión de información del evento relacionada con la recopilación de información.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha iniciado qué análisis de vulnerabilidad en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de detección de servicios

La acción de detección de servicios trata la expresión de información del evento relativa al descubrimiento de servicios en un sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	3
Correcto	S	4

Acción de descubrimiento de grupo y usuario

La acción de descubrimiento de grupo y usuario trata la expresión de información del evento relativa al descubrimiento de cuentas de grupo y usuario en un sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	3
Correcto	S	2

Acción de análisis de vulnerabilidades iniciado

La acción de análisis de vulnerabilidades iniciado trata la expresión de información del evento relativa a la iniciación de un análisis de vulnerabilidades en una aplicación o host determinados.

Información	Nivel
Origen - Información de usuario	Primario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué cuenta ha iniciado qué análisis de vulnerabilidad en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Acción de análisis de vulnerabilidades completado

La acción de análisis de vulnerabilidades completado trata la expresión de información del evento relativa a la finalización de un análisis de vulnerabilidades en una aplicación o un host determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué análisis de vulnerabilidades se ha completado en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	2
Incorrecto	F	3

Clase de descubrimiento de vulnerabilidades

Acción de vulnerabilidad de punto de acceso

La acción de vulnerabilidad de punto de acceso trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades relacionadas con un punto de acceso inalámbrico.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de cuenta

La acción de vulnerabilidad de cuenta trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con las cuentas de usuario.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de antivirus

Esta acción expresa de información del evento acerca del descubrimiento de vulnerabilidades en relación con software o dispositivos antivirus.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de protocolo de aplicación

La acción de vulnerabilidad de protocolo de aplicación trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con protocolos de aplicación como HTTP, NFS y NIS.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de aplicación

La acción de vulnerabilidad de aplicación trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con las aplicaciones.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de programas de puerta trasera

La acción de vulnerabilidad de programas de puerta trasera trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con los programas de puerta trasera.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad del búfer

La acción de vulnerabilidad del búfer trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con las condiciones de flujo excesivo del búfer.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Primario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de interfaz CGI

La acción de vulnerabilidad de interfaz CGI trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con la interfaz CGI.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de CISCO

La acción de vulnerabilidad de CISCO trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con los productos de CISCO.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de ejecución de comando

La acción de vulnerabilidad de ejecución de comando trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades relacionadas con la ejecución de comandos. Un ejemplo sería la ejecución de comandos arbitrarios que omiten los controles del sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de conformidad

La acción de vulnerabilidad de conformidad trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con la conformidad.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de configuración

La acción de vulnerabilidad de configuración trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con la configuración.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de credencial

La acción de vulnerabilidad de credencial trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con las credenciales.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de cifrado

La acción de vulnerabilidad de cifrado trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con el cifrado.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de base de datos

La acción de vulnerabilidad de base de datos trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con las bases de datos y sistemas de administración de base de datos (DBMS).

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de denegación de servicio

La acción de vulnerabilidad de denegación de servicio trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con la denegación de servicio.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de archivo compartido

La acción de vulnerabilidad de archivo compartido trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con la configuración de archivos compartidos, por ejemplo, un archivo compartido con permisos abiertos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	3
Correcto	S	4

Acción de vulnerabilidad de cortafuegos

La acción de vulnerabilidad de cortafuegos trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con las operaciones, configuración, políticas o componentes del cortafuegos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	3
Correcto	S	4

Acción de vulnerabilidad de pérdida de información

La acción de vulnerabilidad de pérdida de información trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con pérdidas de información.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de cliente de correo

La acción de vulnerabilidad de cliente de correo trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades relacionadas con el cliente de correo. Un ejemplo serían las vulnerabilidades detectadas en Microsoft Outlook.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de servidor de correo

La acción de vulnerabilidad de servidor de correo trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades relacionadas con los servidores de correo. Un ejemplo serían las vulnerabilidades detectadas en Microsoft Exchange o Lotus Domino.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de Microsoft

La acción de vulnerabilidad de Microsoft trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con los productos de Microsoft. Los ejemplos incluyen la suplantación de identidad IP de contenido de Internet de Proxy Server 2.0 e ISA Server 2000, vulnerabilidades de Microsoft Office, flujo excesivo de Windows RAS, etc.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Incorrecto	F	3

Información	Nivel	
Correcto	S	4

Acción de vulnerabilidad de protocolo de red

La acción de vulnerabilidad de protocolo de red trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con protocolos de red como TCP, UDP, IP e ICMP.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de OS

La acción de vulnerabilidad de OS trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con sistemas operativos. Para UNIX o Linux, utilice la acción de vulnerabilidad de UNIX a la hora de realizar asignaciones. Para Windows, utilice la acción de vulnerabilidad de Windows a la hora de realizar asignaciones. Utilice esta acción para el resto de sistemas operativos.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario

Información	Nivel
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad del explorador de puerto

La acción de vulnerabilidad del explorador de puerto trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con los productos del explorador de puerto.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario

Información	Nivel
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de extensión de privilegios

La acción de vulnerabilidad de extensión de privilegios trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con la extensión no autorizada de privilegios.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario

Información	Nivel
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de explotación remota

La acción de vulnerabilidad de explotación remota trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con explotaciones remotas.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario

Información	Nivel
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de SCADA

La acción de vulnerabilidad de SCADA trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con SCADA y otros sistemas de control industriales.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario

Información	Nivel
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de servicio/daemon

La acción de vulnerabilidad de servicio/daemon trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con los servicios o daemons.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario

Información	Nivel
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de SMTP

La acción de vulnerabilidad de SMTP trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con un SMTP. Un ejemplo sería una transmisión SMTP abierta que pueda permitir que cualquier usuario de Internet envíe correos electrónicos a través del servidor de correo.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario

Información	Nivel
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de software

La acción de vulnerabilidad de software trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con el software.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario

Información	Nivel
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de inyección de código SQL

La acción de vulnerabilidad de inyección de código SQL trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con la inyección de código SQL.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario

Información	Nivel
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de UNIX

La acción de vulnerabilidad de UNIX trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con el sistema operativo de UNIX.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario

Información	Nivel
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de enumeración de usuario

La acción de vulnerabilidad de enumeración de usuario trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades relacionadas con la enumeración no autorizada de nombres o cuentas de usuario en un sistema.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario

Información	Nivel
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de explorador Web

La acción de vulnerabilidad de explorador Web trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con los exploradores Web.

Información	Nivel
Origen - Información de usuario	Secundario

Información	Nivel
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de servidor Web

La acción de vulnerabilidad de servidor Web trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con los servidores Web.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de Windows

La acción de vulnerabilidad de Windows trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con el sistema operativo de Windows.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Acción de vulnerabilidad de filtro XSS

La acción de vulnerabilidad del filtro XSS trata la expresión de información del evento relativa al descubrimiento de vulnerabilidades en relación con el filtro de scripts de sitios.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

Resultado	event_result	event_severity
Correcto	S	4

Clase de gestión de vulnerabilidades

Acción de vulnerabilidad encontrada

La acción de vulnerabilidad encontrada trata la expresión de información del evento relativa al descubrimiento de una vulnerabilidad en un host o aplicación determinados.

Información	Nivel
Origen - Información de usuario	Secundario
Origen - Información de host	Secundario
Origen - Información de objeto	Terciario
Origen - Información de proceso	Terciario
Origen - Información de grupo	Terciario
Destino - Información de usuario	Terciario
Destino - Información de host	Primario
Destino - Información de objeto	Primario
Destino - Información de proceso	Terciario
Destino - Información de grupo	Terciario
Agente - Información	Primario
Agente - Información de host	Primario
Origen de evento - Información de host	Primario
Origen de evento - Información	Terciario
Evento - Información	Primario
Resultado - Información	Primario

La información importante para esta acción es qué vulnerabilidad se ha descubierto en qué host. La información del evento que se ha expresado en qué host y registrado por qué agente en qué host.

Resultado	event_result	event_severity
Correcto	S	4

Resultado	event_result	event_severity
Incorrecto	F	3

Capítulo 17: Preguntas frecuentes (FAQ)

La sección de preguntas frecuentes proporciona algunas respuestas a las preguntas que le ayudarán a aclarar la perspectiva de algunos aspectos de la implementación de la Gramática de eventos comunes de CA. Las preguntas se responden lo más detalladamente posible.

Esta sección contiene los siguientes temas:

Diferencia entre las acciones Desactivación de cuentas, Suspensión de cuentas y Bloqueo de cuentas (en la página 1252)
Diferencia entre los términos Cuenta, Identidad y Usuario (en la página 1253)

Diferencia entre las acciones Desactivación de cuentas, Suspensión de cuentas y Bloqueo de cuentas

En ninguno de los tres casos se permitirá iniciar sesión en la cuenta una vez que se ha producido la acción. Además, en las tres acciones, la cuenta puede activarse en cualquier momento por una cuenta con privilegios de administrador. La siguiente información debe servir de ayuda para aclarar las diferencias entres estas acciones:

Bloqueo de cuentas

Puede que la cuenta se haya bloqueado debido a una política que restringe el número de veces que la cuenta puede intentar una acción que no puede realizar. La política de recuperación de contraseña en Windows es un buen ejemplo de cuándo la acción de bloqueo de cuentas surte efecto. Por ejemplo, el usuario está intentando iniciar sesión en el sistema con las credenciales erróneas y ha infringido la política de contraseñas establecida

(por ejemplo: el usuario introduce la contraseña incorrectamente 3 veces, lo que no le permitirá iniciar sesión a pesar de que introduzca la contraseña correcta en el cuarto intento).

Desactivación de cuentas

La cuenta puede desactivarse de forma explícita debido a una configuración o acción manual en la cuenta que proporciona un efecto limitado en ésta. Por ejemplo, piense en una cuenta que se ha marcado sólo como válida hasta una fecha específica. En este caso, la cuenta se desactiva una vez que la fecha actual supera la fecha especificada en la información de cuenta

(por ejemplo: el usuario crea una cuenta que está **activa sólo hasta una fecha determinada** ,19 de julio de 2007. Después de esta fecha se desactiva de forma automática).

Suspensión de cuentas

Un administrador puede suspender temporalmente la cuenta. Esta suspensión se produce mediante una acción manual y no automáticamente.

En este caso la cuenta **no se encuentra activa durante un período específico** (por ejemplo del 12/07/07 al 20/07/07). Se activará después de esta fecha.

Diferencia entre los términos Cuenta, Identidad y Usuario

Los términos Cuenta y Usuario son sinónimos y se aunarán en Cuenta en el futuro. Se cambiará el nombre de todas las acciones relacionadas con la acción del usuario para referirse a la acción de cuenta.

El término Identidad hace referencia al usuario real (persona) que posee varias cuentas en varios sistemas. La acción de identidad puede aprovisionarse con una función para generar varias cuentas en varios sistemas según la función deseada para la identidad.

Apéndice A: Asignación de nivel de seguridad

Tabla de asignación de nivel de seguridad

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Gestión de identidades	Gestión de cuentas	Creación de cuentas	Correcto	2
Gestión de identidades	Gestión de cuentas	Creación de cuentas	Error	3
Gestión de identidades	Gestión de cuentas	Supresión de cuentas	Correcto	2
Gestión de identidades	Gestión de cuentas	Supresión de cuentas	Error	3
Gestión de identidades	Gestión de cuentas	Desactivación de cuentas	Correcto	2
Gestión de identidades	Gestión de cuentas	Desactivación de cuentas	Error	3
Gestión de identidades	Gestión de cuentas	Activación de cuentas	Correcto	2
Gestión de identidades	Gestión de cuentas	Activación de cuentas	Error	3
Gestión de identidades	Gestión de cuentas	Enumeración de cuentas	Correcto	2
Gestión de identidades	Gestión de cuentas	Bloqueo de cuentas	Correcto	2
Gestión de identidades	Gestión de cuentas	Modificación de cuenta	Correcto	2
Gestión de identidades	Gestión de cuentas	Modificación de cuenta	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Gestión de identidades	Gestión de cuentas	Modificación de contraseña de cuenta	Correcto	2
Gestión de identidades	Gestión de cuentas	Modificación de contraseña de cuenta	Error	3
Gestión de identidades	Gestión de cuentas	Restablecimiento de contraseña de cuenta	Correcto	2
Gestión de identidades	Gestión de cuentas	Restablecimiento de contraseña de cuenta	Error	3
Gestión de identidades	Gestión de cuentas	Suspensión de cuentas	Correcto	2
Gestión de identidades	Gestión de cuentas	Suspensión de cuentas	Error	3
Gestión de identidades	Gestión de cuentas	Desbloqueo de cuentas	Correcto	2
Gestión de identidades	Gestión de cuentas	Desbloqueo de cuentas	Error	3
Gestión de identidades	Gestión de grupos	Creación de grupos	Correcto	2
Gestión de identidades	Gestión de grupos	Creación de grupos	Error	3
Gestión de identidades	Gestión de grupos	Supresión de grupos	Correcto	2
Gestión de identidades	Gestión de grupos	Supresión de grupos	Error	3
Gestión de identidades	Gestión de grupos	Adición de pertenencia a grupo	Correcto	2
Gestión de identidades	Gestión de grupos	Adición de pertenencia a grupo	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Gestión de identidades	Gestión de grupos	Supresión de pertenencia a grupo	Correcto	2
Gestión de identidades	Gestión de grupos	Supresión de pertenencia a grupo	Error	3
Gestión de identidades	Gestión de grupos	Modificación de pertenencia a grupo	Correcto	2
Gestión de identidades	Gestión de grupos	Modificación de pertenencia a grupo	Error	3
Gestión de identidades	Gestión de grupos	Modificación de grupos	Correcto	2
Gestión de identidades	Gestión de grupos	Modificación de grupos	Error	3
Gestión de identidades	Gestión de identidades	Creación de identidades	Correcto	2
Gestión de identidades	Gestión de identidades	Creación de identidades	Error	3
Gestión de identidades	Gestión de identidades	Supresión de identidades	Correcto	2
Gestión de identidades	Gestión de identidades	Supresión de identidades	Error	3
Gestión de identidades	Gestión de identidades	Desactivación de identidades	Correcto	2
Gestión de identidades	Gestión de identidades	Desactivación de identidades	Error	3
Gestión de identidades	Gestión de identidades	Activación de identidades	Correcto	2
Gestión de identidades	Gestión de identidades	Activación de identidades	Error	3
Gestión de identidades	Gestión de identidades	Modificación de identidades	Correcto	2

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Gestión de identidades	Gestión de identidades	Modificación de identidades	Error	3
Gestión de identidades	Gestión de identidades	Modificación de contraseña de identidad	Correcto	2
Gestión de identidades	Gestión de identidades	Modificación de contraseña de identidad	Error	3
Gestión de identidades	Gestión de derechos de usuario	Asignación de permisos de usuario	Correcto	2
Gestión de identidades	Gestión de derechos de usuario	Asignación de permisos de usuario	Error	3
Gestión de identidades	Gestión de derechos de usuario	Supresión de permisos de usuario	Correcto	2
Gestión de identidades	Gestión de derechos de usuario	Supresión de permisos de usuario	Error	3
Gestión de identidades	Gestión de derechos de usuario	Asignación de derechos de usuario	Correcto	2
Gestión de identidades	Gestión de derechos de usuario	Asignación de derechos de usuario	Error	3
Gestión de identidades	Gestión de derechos de usuario	Creación de derechos de usuario	Correcto	2
Gestión de identidades	Gestión de derechos de usuario	Creación de derechos de usuario	Error	3
Gestión de identidades	Gestión de derechos de usuario	Supresión de derechos de usuario	Correcto	2

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Gestión de identidades	Gestión de derechos de usuario	Supresión de derechos de usuario	Error	3
Gestión de identidades	Gestión de derechos de usuario	Enumeración de derechos de usuario	Correcto	2
Gestión de identidades	Gestión de derechos de usuario	Enumeración de derechos de usuario	Error	3
Gestión de identidades	Gestión de derechos de usuario	Modificación de derechos de usuario	Correcto	2
Gestión de identidades	Gestión de derechos de usuario	Modificación de derechos de usuario	Error	3
Gestión de identidades	Gestión de función de usuario	Asignación de función de administrador de usuarios	Correcto	3
Gestión de identidades	Gestión de función de usuario	Asignación de función de administrador de usuarios	Error	3
Gestión de identidades	Gestión de función de usuario	Supresión de función de administrador de usuarios	Correcto	3
Gestión de identidades	Gestión de función de usuario	Supresión de función de administrador de usuarios	Error	3
Gestión de identidades	Gestión de función de usuario	Modificación de función de administrador de usuarios	Correcto	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Gestión de identidades	Gestión de función de usuario	Modificación de función de administrador de usuarios	Error	3
Gestión de identidades	Gestión de función de usuario	Supresión de función de administrador de usuarios	Correcto	3
Gestión de identidades	Gestión de función de usuario	Supresión de función de administrador de usuarios	Error	3
Gestión de identidades	Gestión de función de usuario	Asignación de función de usuario	Correcto	2
Gestión de identidades	Gestión de función de usuario	Creación de función de usuario	Correcto	2
Gestión de identidades	Gestión de función de usuario	Creación de función de usuario	Error	3
Gestión de identidades	Gestión de función de usuario	Supresión de función de usuario	Correcto	2
Gestión de identidades	Gestión de función de usuario	Supresión de función de usuario	Error	3
Gestión de identidades	Gestión de función de usuario	Modificación de función de usuario	Correcto	2
Gestión de identidades	Gestión de función de usuario	Modificación de función de usuario	Error	3
Gestión de identidades	Gestión de función de usuario	Supresión de función de usuario	Correcto	2
Gestión de identidades	Gestión de función de usuario	Supresión de función de usuario	Error	3
Gestión de configuraciones	Gestión de configuraciones	Modificación de configuración	Correcto	2
Gestión de configuraciones	Gestión de configuraciones	Modificación de configuración	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Gestión de configuraciones	Gestión de configuraciones	Error de configuración	Correcto	6
Gestión de configuraciones	Gestión de configuraciones	Configuración de Vaciar todo	Correcto	2
Gestión de configuraciones	Gestión de configuraciones	Configuración de Vaciar todo	Error	3
Gestión de configuraciones	Gestión de configuraciones	Configuración de Vaciar territorios de autenticación	Correcto	2
Gestión de configuraciones	Gestión de configuraciones	Configuración de Vaciar territorios de autenticación	Error	3
Gestión de configuraciones	Gestión de configuraciones	Configuración de Vaciar caché de usuario	Correcto	2
Gestión de configuraciones	Gestión de configuraciones	Configuración de Vaciar caché de usuario	Error	3
Gestión de configuraciones	Gestión de configuraciones	Inicio de lectura de configuración	Correcto	2
Gestión de configuraciones	Gestión de configuraciones	Advertencia de configuración	Correcto	3
Gestión de configuraciones	Gestión de configuraciones	Modificación de hora del sistema	Correcto	4
Gestión de configuraciones	Gestión de configuraciones	Modificación de hora del sistema	Error	4
Gestión de configuraciones	Gestión de configuraciones	Creación de tareas	Correcto	2
Gestión de configuraciones	Gestión de configuraciones	Creación de tareas	Error	3
Gestión de configuraciones	Gestión de configuraciones	Modificación de tareas	Correcto	2
Gestión de configuraciones	Gestión de configuraciones	Modificación de tareas	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Gestión de configuraciones	Gestión de políticas	Creación de políticas	Correcto	2
Gestión de configuraciones	Gestión de políticas	Creación de políticas	Error	3
Gestión de configuraciones	Gestión de políticas	Supresión de políticas	Correcto	4
Gestión de configuraciones	Gestión de políticas	Supresión de políticas	Error	3
Gestión de configuraciones	Gestión de políticas	Modificación de políticas	Correcto	4
Gestión de configuraciones	Gestión de políticas	Modificación de políticas	Error	3
Gestión de configuraciones	Gestión de políticas	Activación de políticas	Correcto	2
Gestión de configuraciones	Gestión de políticas	Activación de políticas	Error	3
Gestión de configuraciones	Gestión de políticas	Desactivación de políticas	Correcto	2
Gestión de configuraciones	Gestión de políticas	Desactivación de políticas	Error	3
Gestión de configuraciones	Gestión de políticas	Aplicación de políticas	Correcto	2
Seguridad del contenido	Inspección de correo electrónico	Detección de spam	Correcto	3
Seguridad del contenido	Inspección de correo electrónico	Análisis de archivos adjuntos	Correcto	2
Seguridad del contenido	Inspección de correo electrónico	Análisis de archivos adjuntos	Error	3
Seguridad del contenido	Inspección de correo electrónico	Detección de lenguaje irreverente	Correcto	2
Seguridad del contenido	Inspección de correo electrónico	Detección de lenguaje irreverente	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Seguridad del contenido	Inspección de correo electrónico	Pérdida de información confidencial	Correcto	2
Seguridad del contenido	Inspección de correo electrónico	Pérdida de información confidencial	Error	3
Seguridad del contenido	Inspección de correo electrónico	Inspección de correo electrónico	Correcto	2
Seguridad del contenido	Inspección de correo electrónico	Inspección de correo electrónico	Error	3
Seguridad del contenido	Acceso a URL	Filtrado de URL	Correcto	2
Seguridad del contenido	Acceso a URL	Filtrado de URL	Error	3
Seguridad del contenido	Acceso a URL	Filtrado de HTTP	Correcto	2
Seguridad del contenido	Acceso a URL	Filtrado de HTTP	Error	3
Seguridad del contenido	Acceso a URL	Filtrado de FTP	Correcto	2
Seguridad del contenido	Acceso a URL	Filtrado de FTP	Error	3
Seguridad del contenido	Acceso a URL	Inspección de contenido	Correcto	2
Seguridad del contenido	Acceso a URL	Inspección de contenido	Error	3
Acceso a datos	Utilización de aplicaciones y servicios	Ejecución del método	Correcto	2
Acceso a datos	Utilización de aplicaciones y servicios	Ejecución del método	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Utilización de aplicaciones y servicios	Ejecución del procedimiento	Correcto	2
Acceso a datos	Utilización de aplicaciones y servicios	Ejecución del procedimiento	Error	3
Acceso a datos	Gestión de aplicaciones	Creación de contexto	Correcto	2
Acceso a datos	Gestión de aplicaciones	Creación de contexto	Error	3
Acceso a datos	Gestión de aplicaciones	Supresión de contexto	Correcto	3
Acceso a datos	Gestión de aplicaciones	Supresión de contexto	Error	3
Acceso a datos	Gestión de aplicaciones	Creación de funciones	Correcto	2
Acceso a datos	Gestión de aplicaciones	Creación de funciones	Error	3
Acceso a datos	Gestión de aplicaciones	Supresión de funciones	Correcto	4
Acceso a datos	Gestión de aplicaciones	Supresión de funciones	Error	3
Acceso a datos	Gestión de aplicaciones	Modificación de funciones	Correcto	2
Acceso a datos	Gestión de aplicaciones	Modificación de funciones	Error	3
Acceso a datos	Gestión de aplicaciones	Análisis de índices	Correcto	2
Acceso a datos	Gestión de aplicaciones	Análisis de índices	Error	3
Acceso a datos	Gestión de aplicaciones	Creación de bibliotecas	Correcto	2
Acceso a datos	Gestión de aplicaciones	Creación de bibliotecas	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión de aplicaciones	Creación de operadores	Correcto	2
Acceso a datos	Gestión de aplicaciones	Creación de operadores	Error	3
Acceso a datos	Gestión de aplicaciones	Supresión de operadores	Correcto	4
Acceso a datos	Gestión de aplicaciones	Supresión de operadores	Error	3
Acceso a datos	Gestión de aplicaciones	Modificación de operadores	Correcto	2
Acceso a datos	Gestión de aplicaciones	Modificación de operadores	Error	3
Acceso a datos	Gestión de aplicaciones	Creación del cuerpo del paquete	Correcto	2
Acceso a datos	Gestión de aplicaciones	Creación del cuerpo del paquete	Error	3
Acceso a datos	Gestión de aplicaciones	Supresión de cuerpo del paquete	Correcto	4
Acceso a datos	Gestión de aplicaciones	Supresión de cuerpo del paquete	Error	3
Acceso a datos	Gestión de aplicaciones	Modificación de cuerpo del paquete	Correcto	2
Acceso a datos	Gestión de aplicaciones	Modificación de cuerpo del paquete	Error	3
Acceso a datos	Gestión de aplicaciones	Creación de paquetes	Correcto	2
Acceso a datos	Gestión de aplicaciones	Creación de paquetes	Error	3
Acceso a datos	Gestión de aplicaciones	Modificación de paquetes	Correcto	2
Acceso a datos	Gestión de aplicaciones	Modificación de paquetes	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión de aplicaciones	Creación de procedimientos	Correcto	2
Acceso a datos	Gestión de aplicaciones	Creación de procedimientos	Error	3
Acceso a datos	Gestión de aplicaciones	Supresión de paquetes	Correcto	4
Acceso a datos	Gestión de aplicaciones	Supresión de paquetes	Error	3
Acceso a datos	Gestión de aplicaciones	Supresión de procedimientos	Correcto	4
Acceso a datos	Gestión de aplicaciones	Supresión de procedimientos	Error	3
Acceso a datos	Gestión de aplicaciones	Modificación de procedimientos	Correcto	2
Acceso a datos	Gestión de aplicaciones	Modificación de procedimientos	Error	3
Acceso a datos	Gestión de aplicaciones	Análisis de tabla	Correcto	2
Acceso a datos	Gestión de aplicaciones	Análisis de tabla	Error	3
Acceso a datos	Gestión de aplicaciones	Truncamiento de tabla	Correcto	3
Acceso a datos	Gestión de aplicaciones	Truncamiento de tabla	Error	3
Acceso a datos	Gestión de aplicaciones	Creación de iniciador	Correcto	2
Acceso a datos	Gestión de aplicaciones	Creación de iniciador	Error	3
Acceso a datos	Gestión de aplicaciones	Supresión de iniciador	Correcto	4
Acceso a datos	Gestión de aplicaciones	Supresión de iniciador	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión de aplicaciones	Desactivación de iniciador	Correcto	4
Acceso a datos	Gestión de aplicaciones	Desactivación de iniciador	Error	3
Acceso a datos	Gestión de aplicaciones	Activación de iniciador	Correcto	2
Acceso a datos	Gestión de aplicaciones	Activación de iniciador	Error	3
Acceso a datos	Gestión de aplicaciones	Modificación de iniciador	Correcto	2
Acceso a datos	Gestión de aplicaciones	Modificación de iniciador	Error	3
Acceso a datos	Gestión de aplicaciones	Creación de cuerpo del tipo	Correcto	2
Acceso a datos	Gestión de aplicaciones	Creación de cuerpo del tipo	Error	3
Acceso a datos	Gestión de aplicaciones	Supresión del cuerpo del tipo	Correcto	3
Acceso a datos	Gestión de aplicaciones	Supresión del cuerpo del tipo	Error	3
Acceso a datos	Gestión de aplicaciones	Modificación de cuerpo del tipo	Correcto	2
Acceso a datos	Gestión de aplicaciones	Modificación de cuerpo del tipo	Error	3
Acceso a datos	Gestión de aplicaciones	Creación del tipo	Correcto	2
Acceso a datos	Gestión de aplicaciones	Creación del tipo	Error	3
Acceso a datos	Gestión de aplicaciones	Supresión del tipo	Correcto	4
Acceso a datos	Gestión de aplicaciones	Supresión del tipo	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión de aplicaciones	Ejecución del tipo	Correcto	2
Acceso a datos	Gestión de aplicaciones	Ejecución del tipo	Error	3
Acceso a datos	Gestión de aplicaciones	Modificación del tipo	Correcto	2
Acceso a datos	Gestión de aplicaciones	Modificación del tipo	Error	3
Acceso a datos	Gestión del mismo nivel	Creación de vínculo de base de datos	Correcto	2
Acceso a datos	Gestión del mismo nivel	Creación de vínculo de base de datos	Error	3
Acceso a datos	Gestión del mismo nivel	Supresión de vínculo de base de datos	Correcto	4
Acceso a datos	Gestión del mismo nivel	Supresión de vínculo de base de datos	Error	3
Acceso a datos	Gestión del sistema	Análisis de clúster	Correcto	2
Acceso a datos	Gestión del sistema	Análisis de clúster	Error	3
Acceso a datos	Gestión del sistema	Creación de clúster	Correcto	2
Acceso a datos	Gestión del sistema	Creación de clúster	Error	3
Acceso a datos	Gestión del sistema	Supresión de clúster	Correcto	2
Acceso a datos	Gestión del sistema	Supresión de clúster	Error	3
Acceso a datos	Gestión del sistema	Modificación de clúster	Correcto	2
Acceso a datos	Gestión del sistema	Modificación de clúster	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión del sistema	Truncamiento de clúster	Correcto	2
Acceso a datos	Gestión del sistema	Truncamiento de clúster	Error	3
Acceso a datos	Gestión del sistema	Creación de base de datos	Correcto	2
Acceso a datos	Gestión del sistema	Creación de base de datos	Error	3
Acceso a datos	Gestión del sistema	Supresión de base de datos	Correcto	4
Acceso a datos	Gestión del sistema	Supresión de base de datos	Error	3
Acceso a datos	Gestión del sistema	Flashback de base de datos	Correcto	3
Acceso a datos	Gestión del sistema	Flashback de base de datos	Error	3
Acceso a datos	Gestión del sistema	Modificación de base de datos	Correcto	3
Acceso a datos	Gestión del sistema	Modificación de base de datos	Error	3
Acceso a datos	Gestión del sistema	Copia de seguridad de base de datos	Correcto	2
Acceso a datos	Gestión del sistema	Copia de seguridad de base de datos	Error	3
Acceso a datos	Gestión del sistema	Restauración de base de datos	Correcto	3
Acceso a datos	Gestión del sistema	Restauración de base de datos	Error	3
Acceso a datos	Gestión del sistema	Explicación	Correcto	2
Acceso a datos	Gestión del sistema	Explicación	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión del sistema	Flashback	Correcto	2
Acceso a datos	Gestión del sistema	Flashback	Error	3
Acceso a datos	Gestión del sistema	Purga de la papelera de reciclaje	Correcto	2
Acceso a datos	Gestión del sistema	Purga de la papelera de reciclaje	Error	3
Acceso a datos	Gestión del sistema	Creación de segmento de reversión	Correcto	2
Acceso a datos	Gestión del sistema	Creación de segmento de reversión	Error	3
Acceso a datos	Gestión del sistema	Supresión de segmento de reversión	Correcto	2
Acceso a datos	Gestión del sistema	Supresión de segmento de reversión	Error	3
Acceso a datos	Gestión del sistema	Modificación del segmento de reversión	Correcto	2
Acceso a datos	Gestión del sistema	Modificación del segmento de reversión	Error	3
Acceso a datos	Gestión del sistema	Concesión del sistema	Correcto	2
Acceso a datos	Gestión del sistema	Concesión del sistema	Error	3
Acceso a datos	Gestión del sistema	Modificación del sistema	Correcto	2

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión del sistema	Modificación del sistema	Error	3
Acceso a datos	Gestión del sistema	Revocación del sistema	Correcto	2
Acceso a datos	Gestión del sistema	Revocación del sistema	Error	3
Acceso a datos	Gestión del sistema	Flashback de tabla	Correcto	2
Acceso a datos	Gestión del sistema	Flashback de tabla	Error	3
Acceso a datos	Gestión del sistema	Creación de espacio de tabla	Correcto	2
Acceso a datos	Gestión del sistema	Creación de espacio de tabla	Error	3
Acceso a datos	Gestión del sistema	Supresión de espacio de tabla	Correcto	4
Acceso a datos	Gestión del sistema	Supresión de espacio de tabla	Error	3
Acceso a datos	Gestión del sistema	Modificación de espacio de tabla	Correcto	3
Acceso a datos	Gestión del sistema	Modificación de espacio de tabla	Error	3
Acceso a datos	Gestión del sistema	Purga de espacio de tabla	Correcto	3
Acceso a datos	Gestión del sistema	Purga de espacio de tabla	Error	3
Acceso a datos	Gestión del sistema	Ejecución de instrucción de transacción	Correcto	2
Acceso a datos	Gestión del sistema	Ejecución de instrucción de transacción	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión del sistema	Desactivación de todos los iniciadores	Correcto	4
Acceso a datos	Gestión del sistema	Desactivación de todos los iniciadores	Error	3
Acceso a datos	Gestión del sistema	Activación de todos los iniciadores	Correcto	3
Acceso a datos	Gestión del sistema	Activación de todos los iniciadores	Error	3
Acceso a datos	Acceso a datos	Confirmación	Correcto	2
Acceso a datos	Acceso a datos	Confirmación	Error	3
Acceso a datos	Acceso a datos	Suprimir	Correcto	3
Acceso a datos	Acceso a datos	Suprimir	Error	3
Acceso a datos	Acceso a datos	Insertar	Correcto	2
Acceso a datos	Acceso a datos	Insertar	Error	3
Acceso a datos	Acceso a datos	Reversión	Correcto	2
Acceso a datos	Acceso a datos	Reversión	Error	3
Acceso a datos	Acceso a datos	Punto de retorno	Correcto	2
Acceso a datos	Acceso a datos	Punto de retorno	Error	3
Acceso a datos	Acceso a datos	Seleccionar	Correcto	2
Acceso a datos	Acceso a datos	Seleccionar	Error	3
Acceso a datos	Acceso a datos	Configuración de transacciones	Correcto	2
Acceso a datos	Acceso a datos	Configuración de transacciones	Error	3
Acceso a datos	Acceso a datos	Actualizar	Correcto	2
Acceso a datos	Acceso a datos	Actualizar	Error	3
Acceso a datos	Gestión de objetos	Creación de archivo de control	Correcto	2

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión de objetos	Creación de archivo de control	Error	6
Acceso a datos	Gestión de objetos	Creación de dimensiones	Correcto	2
Acceso a datos	Gestión de objetos	Creación de dimensiones	Error	3
Acceso a datos	Gestión de objetos	Supresión de dimensiones	Correcto	2
Acceso a datos	Gestión de objetos	Supresión de dimensiones	Error	3
Acceso a datos	Gestión de objetos	Modificación de dimensiones	Correcto	2
Acceso a datos	Gestión de objetos	Modificación de dimensiones	Error	3
Acceso a datos	Gestión de objetos	Creación de directorios	Correcto	2
Acceso a datos	Gestión de objetos	Creación de directorios	Error	3
Acceso a datos	Gestión de objetos	Supresión de directorios	Correcto	4
Acceso a datos	Gestión de objetos	Supresión de directorios	Error	3
Acceso a datos	Gestión de objetos	Actualización de todos los índices	Correcto	2
Acceso a datos	Gestión de objetos	Actualización de todos los índices	Error	3
Acceso a datos	Gestión de objetos	Creación de índices	Correcto	2
Acceso a datos	Gestión de objetos	Creación de índices	Error	3
Acceso a datos	Gestión de objetos	Supresión de índices	Correcto	3
Acceso a datos	Gestión de objetos	Supresión de índices	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión de objetos	Modificación de índices	Correcto	3
Acceso a datos	Gestión de objetos	Modificación de índices	Error	3
Acceso a datos	Gestión de objetos	Vaciado de índices	Correcto	3
Acceso a datos	Gestión de objetos	Vaciado de índices	Error	3
Acceso a datos	Gestión de objetos	Creación de tipo de índice	Correcto	2
Acceso a datos	Gestión de objetos	Creación de tipo de índice	Error	3
Acceso a datos	Gestión de objetos	Supresión de tipo de índice	Correcto	3
Acceso a datos	Gestión de objetos	Supresión de tipo de índice	Error	3
Acceso a datos	Gestión de objetos	Validación de índice	Correcto	2
Acceso a datos	Gestión de objetos	Validación de índice	Error	3
Acceso a datos	Gestión de objetos	Creación de Java	Correcto	2
Acceso a datos	Gestión de objetos	Creación de Java	Error	3
Acceso a datos	Gestión de objetos	Supresión de objeto Java	Correcto	3
Acceso a datos	Gestión de objetos	Supresión de objeto Java	Error	3
Acceso a datos	Gestión de objetos	Modificación de objeto Java	Correcto	3
Acceso a datos	Gestión de objetos	Modificación de objeto Java	Error	3
Acceso a datos	Gestión de objetos	Bloqueo	Correcto	2
Acceso a datos	Gestión de objetos	Bloqueo	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión de objetos	Creación de vista materializada	Correcto	2
Acceso a datos	Gestión de objetos	Creación de vista materializada	Error	3
Acceso a datos	Gestión de objetos	Supresión de vista materializada	Correcto	3
Acceso a datos	Gestión de objetos	Supresión de vista materializada	Error	3
Acceso a datos	Gestión de objetos	Modificación de vista materializada	Correcto	3
Acceso a datos	Gestión de objetos	Modificación de vista materializada	Error	3
Acceso a datos	Gestión de objetos	Creación de registro de vista materializada	Correcto	2
Acceso a datos	Gestión de objetos	Creación de registro de vista materializada	Error	3
Acceso a datos	Gestión de objetos	Supresión de registro de vista materializada	Correcto	3
Acceso a datos	Gestión de objetos	Supresión de registro de vista materializada	Error	3
Acceso a datos	Gestión de objetos	Modificación de registro de vista materializada	Correcto	3
Acceso a datos	Gestión de objetos	Modificación de registro de vista materializada	Error	3
Acceso a datos	Gestión de objetos	Falta de funcionamiento	Correcto	2
Acceso a datos	Gestión de objetos	Falta de funcionamiento	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión de objetos	Restauración de objetos	Correcto	2
Acceso a datos	Gestión de objetos	Restauración de objetos	Error	3
Acceso a datos	Gestión de objetos	Creación de esquema	Correcto	2
Acceso a datos	Gestión de objetos	Creación de esquema	Error	3
Acceso a datos	Gestión de objetos	Supresión de esquema	Correcto	2
Acceso a datos	Gestión de objetos	Supresión de esquema	Error	3
Acceso a datos	Gestión de objetos	Modificación de esquema	Correcto	2
Acceso a datos	Gestión de objetos	Modificación de esquema	Error	3
Acceso a datos	Gestión de objetos	Creación de sinónimo público	Correcto	2
Acceso a datos	Gestión de objetos	Creación de sinónimo público	Error	3
Acceso a datos	Gestión de objetos	Supresión de sinónimo público	Correcto	3
Acceso a datos	Gestión de objetos	Supresión de sinónimo público	Error	3
Acceso a datos	Gestión de objetos	Modificación de costes de recursos	Correcto	3
Acceso a datos	Gestión de objetos	Modificación de costes de recursos	Error	3
Acceso a datos	Gestión de objetos	Creación de secuencias	Correcto	2
Acceso a datos	Gestión de objetos	Creación de secuencias	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión de objetos	Supresión de secuencias	Correcto	3
Acceso a datos	Gestión de objetos	Supresión de secuencias	Error	3
Acceso a datos	Gestión de objetos	Modificación de secuencias	Correcto	3
Acceso a datos	Gestión de objetos	Modificación de secuencias	Error	3
Acceso a datos	Gestión de objetos	Asociación de estadísticas	Correcto	2
Acceso a datos	Gestión de objetos	Asociación de estadísticas	Error	3
Acceso a datos	Gestión de objetos	Desasociación de estadísticas	Correcto	2
Acceso a datos	Gestión de objetos	Desasociación de estadísticas	Error	3
Acceso a datos	Gestión de objetos	Modificación de resumen	Correcto	2
Acceso a datos	Gestión de objetos	Modificación de resumen	Error	3
Acceso a datos	Gestión de objetos	Creación de sinónimo	Correcto	2
Acceso a datos	Gestión de objetos	Creación de sinónimo	Error	3
Acceso a datos	Gestión de objetos	Supresión de sinónimo	Correcto	3
Acceso a datos	Gestión de objetos	Supresión de sinónimo	Error	3
Acceso a datos	Gestión de objetos	Renombrar	Correcto	3
Acceso a datos	Gestión de objetos	Renombrar	Error	3
Acceso a datos	Gestión de objetos	Creación de esquema	Correcto	2

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión de objetos	Creación de esquema	Error	3
Acceso a datos	Gestión de objetos	Creación de tablas	Correcto	2
Acceso a datos	Gestión de objetos	Creación de tablas	Error	3
Acceso a datos	Gestión de objetos	Supresión de tablas	Correcto	3
Acceso a datos	Gestión de objetos	Supresión de tablas	Error	3
Acceso a datos	Gestión de objetos	Modificación de tablas	Correcto	3
Acceso a datos	Gestión de objetos	Modificación de tablas	Error	3
Acceso a datos	Gestión de objetos	Purga de tabla	Correcto	3
Acceso a datos	Gestión de objetos	Purga de tabla	Error	3
Acceso a datos	Gestión de objetos	Modificación de nombre de tablas	Correcto	3
Acceso a datos	Gestión de objetos	Modificación de nombre de tablas	Error	3
Acceso a datos	Gestión de objetos	Creación de vista	Correcto	2
Acceso a datos	Gestión de objetos	Creación de vista	Error	3
Acceso a datos	Gestión de objetos	Supresión de vista	Correcto	3
Acceso a datos	Gestión de objetos	Supresión de vista	Error	3
Acceso a datos	Gestión de privilegios	Supresión de biblioteca	Correcto	2
Acceso a datos	Gestión de privilegios	Supresión de biblioteca	Error	3
Acceso a datos	Gestión de privilegios	Concesión de objetos	Correcto	2
Acceso a datos	Gestión de privilegios	Concesión de objetos	Error	3
Acceso a datos	Gestión de privilegios	Revocación de objetos	Correcto	2

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión de privilegios	Revocación de objetos	Error	3
Acceso a datos	Gestión de privilegios	Denegación de objetos	Correcto	2
Acceso a datos	Gestión de privilegios	Denegación de objetos	Error	3
Acceso a datos	Gestión de privilegios	Creación de perfiles	Correcto	2
Acceso a datos	Gestión de privilegios	Creación de perfiles	Error	3
Acceso a datos	Gestión de privilegios	Supresión de perfiles	Correcto	4
Acceso a datos	Gestión de privilegios	Supresión de perfiles	Error	3
Acceso a datos	Gestión de privilegios	Modificación de perfiles	Correcto	4
Acceso a datos	Gestión de privilegios	Modificación de perfiles	Error	3
Acceso a datos	Gestión de privilegios	Revocación de funciones	Correcto	2
Acceso a datos	Gestión de privilegios	Revocación de funciones	Error	3
Acceso a datos	Gestión de privilegios	Denegación de instrucciones	Correcto	2
Acceso a datos	Gestión de privilegios	Denegación de instrucciones	Error	3
Acceso a datos	Gestión de privilegios	Revocación de instrucciones	Correcto	2
Acceso a datos	Gestión de privilegios	Revocación de instrucciones	Error	3
Acceso a datos	Gestión de privilegios	Concesión de instrucciones	Correcto	2

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a datos	Gestión de privilegios	Concesión de instrucciones	Error	3
Acceso a datos	Eventos de auditoría	Auditoría predeterminada	Correcto	2
Acceso a datos	Eventos de auditoría	Auditoría predeterminada	Error	3
Acceso a datos	Eventos de auditoría	Auditoría no predeterminada	Correcto	2
Acceso a datos	Eventos de auditoría	Auditoría no predeterminada	Error	3
Acceso a datos	Eventos de auditoría	Auditoría de objetos	Correcto	2
Acceso a datos	Eventos de auditoría	Auditoría de objetos	Error	3
Acceso a datos	Eventos de auditoría	Desactivación de auditoría de objetos	Correcto	2
Acceso a datos	Eventos de auditoría	Desactivación de auditoría de objetos	Error	3
Acceso a datos	Eventos de auditoría	Grabación de sesión	Correcto	2
Acceso a datos	Eventos de auditoría	Grabación de sesión	Error	3
Acceso a datos	Eventos de auditoría	Auditoría del sistema	Correcto	2
Acceso a datos	Eventos de auditoría	Auditoría del sistema	Error	3
Acceso a datos	Eventos de auditoría	Desactivación de auditoría del sistema	Correcto	2
Acceso a datos	Eventos de auditoría	Desactivación de auditoría del sistema	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Seguridad de host	Actividad del antivirus	Bloqueo de archivo	Correcto	2
Seguridad de host	Actividad del antivirus	Exclusión de archivo	Correcto	2
Seguridad de host	Actividad del antivirus	Exclusión de archivo	Error	3
Seguridad de host	Actividad del antivirus	Modificación de nombre de archivo	Correcto	3
Seguridad de host	Actividad del antivirus	Modificación de nombre de archivo	Error	3
Seguridad de host	Actividad del antivirus	Error de análisis	Correcto	6
Seguridad de host	Actividad del antivirus	Informe de análisis	Correcto	2
Seguridad de host	Actividad del antivirus	Eliminación de virus	Correcto	2
Seguridad de host	Actividad del antivirus	Eliminación de virus	Error	6
Seguridad de host	Actividad del antivirus	Detección de virus	Correcto	6
Seguridad de host	Actividad del antivirus	Actualización de motor de virus	Correcto	2
Seguridad de host	Actividad del antivirus	Actualización de motor de virus	Error	5
Seguridad de host	Actividad del antivirus	Cuarentena de virus	Correcto	2
Seguridad de host	Actividad del antivirus	Cuarentena de virus	Error	6
Seguridad de host	Actividad del antivirus	Inicio de la exploración de virus	Correcto	2
Seguridad de host	Actividad del antivirus	Inicio de la exploración de virus	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Seguridad de host	Actividad del antivirus	Exploración de virus completada	Correcto	2
Seguridad de host	Actividad del antivirus	Exploración de virus completada	Error	3
Seguridad de host	Actividad del antivirus	Pausa de la exploración de virus	Correcto	2
Seguridad de host	Actividad del antivirus	Pausa de la exploración de virus	Error	3
Seguridad de host	Actividad del antivirus	Reanudación de la exploración de virus	Correcto	2
Seguridad de host	Actividad del antivirus	Reanudación de la exploración de virus	Error	3
Seguridad de host	Actividad del antivirus	Actualización de firmas de virus	Correcto	2
Seguridad de host	Actividad del antivirus	Actualización de firmas de virus	Error	4
Seguridad de host	Actividad del antivirus	Instalación del antivirus	Correcto	2
Seguridad de host	Actividad del antivirus	Instalación del antivirus	Error	3
Seguridad de host	Actividad del antivirus	Desinstalación del antivirus	Correcto	4
Seguridad de host	Actividad del antivirus	Desinstalación del antivirus	Error	4
Seguridad de host	Actividad del antivirus	Cliente de antivirus eliminado	Correcto	3
Seguridad de host	Actividad del antivirus	Cliente de antivirus eliminado	Error	4
Seguridad de host	Actividad de IDS/IPS	Infracción de firmas	Correcto	6

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Seguridad de red	Actividad de conexión	Intento de conexión	Accept	2
Seguridad de red	Actividad de conexión	Intento de conexión	Anular	3
Seguridad de red	Actividad de conexión	Intento de conexión	Rechazar	3
Seguridad de red	Actividad de conexión	Restablecimiento de conexión	Correcto	2
Seguridad de red	Actividad de conexión	Restablecimiento de conexión	Error	3
Seguridad de red	Actividad de conexión	Solicitud de conexión	Correcto	2
Seguridad de red	Actividad de conexión	Estado de la conexión	Correcto	2
Seguridad de red	Actividad de conexión	Finalización de conexión	Correcto	2
Seguridad de red	Actividad de conexión	Inicio de fase 1 de intercambio de claves	Correcto	2
Seguridad de red	Actividad de conexión	Inicio de fase 1 de intercambio de claves	Error	3
Seguridad de red	Actividad de conexión	Caducidad de asociación de seguridad	Correcto	2
Seguridad de red	Actividad de conexión	Caducidad de asociación de seguridad	Error	3
Seguridad de red	Actividad de conexión	Solicitud de asociación de seguridad	Correcto	2
Seguridad de red	Actividad de conexión	Solicitud de asociación de seguridad	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Seguridad de red	Actividad de infracción de firmas	Infracción de firmas	Correcto	6
Seguridad operacional	Actividad de proceso	Creación de proceso	Correcto	2
Seguridad operacional	Actividad de proceso	Creación de proceso	Error	3
Seguridad operacional	Actividad de proceso	Notificación de proceso	Correcto	2
Seguridad operacional	Actividad de proceso	Notificación de proceso	Error	3
Seguridad operacional	Actividad de proceso	Restauración de proceso	Correcto	2
Seguridad operacional	Actividad de proceso	Restauración de proceso	Error	3
Seguridad operacional	Actividad de proceso	Inicio de proceso	Correcto	2
Seguridad operacional	Actividad de proceso	Inicio de proceso	Error	3
Seguridad operacional	Actividad de proceso	Detención de proceso	Correcto	2
Seguridad operacional	Actividad de proceso	Detención de proceso	Error	3
Seguridad operacional	Actividad de proceso	Suspensión de proceso	Correcto	2
Seguridad operacional	Actividad de proceso	Suspensión de proceso	Error	3
Seguridad operacional	Actividad del sistema	Cierre del sistema	Correcto	7
Seguridad operacional	Actividad del sistema	Cierre del sistema	Error	7
Seguridad operacional	Actividad del sistema	Inicio del sistema	Correcto	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Seguridad operacional	Actividad del sistema	Inicio del sistema	Error	6
Seguridad operacional	Actividad del sistema	Estado del sistema	Correcto	2
Seguridad operacional	Actividad del sistema	Estado del sistema	Error	3
Seguridad operacional	Actividad del sistema	Pausa del sistema	Correcto	4
Seguridad operacional	Actividad del sistema	Pausa del sistema	Error	3
Seguridad operacional	Actividad del sistema	Reanudación del sistema	Correcto	2
Seguridad operacional	Actividad del sistema	Reanudación del sistema	Error	3
Seguridad operacional	Actividad de registro de seguridad	Supresión de registro de seguridad	Correcto	6
Seguridad operacional	Actividad de registro de seguridad	Supresión de registro de seguridad	Error	6
Seguridad operacional	Actividad de registro de seguridad	Sustitución de registro de seguridad	Correcto	2
Seguridad operacional	Actividad de registro de seguridad	Sustitución de registro de seguridad	Error	3
Acceso físico	Actividad de acceso físico	Análisis de identificador	Correcto	2
Acceso físico	Actividad de acceso físico	Análisis de identificador	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso físico	Actividad de acceso físico	Activación de cámara	Correcto	2
Acceso físico	Actividad de acceso físico	Activación de cámara	Error	4
Acceso físico	Actividad de acceso físico	Desactivación de cámara	Correcto	3
Acceso físico	Actividad de acceso físico	Desactivación de cámara	Error	3
Acceso físico	Actividad de acceso físico	Cámara no disponible	Correcto	4
Acceso físico	Actividad de acceso físico	Cámara no disponible	Error	4
Acceso físico	Actividad de acceso físico	Cierre de puerta	Correcto	2
Acceso físico	Actividad de acceso físico	Cierre de puerta	Error	5
Acceso físico	Actividad de acceso físico	Apertura de puerta	Correcto	2
Acceso físico	Actividad de acceso físico	Apertura de puerta	Error	5
Acceso físico	Actividad de acceso físico	Cierre de ventana	Correcto	2
Acceso físico	Actividad de acceso físico	Cierre de ventana	Error	5
Acceso físico	Actividad de acceso físico	Apertura de ventana	Correcto	2
Acceso físico	Actividad de acceso físico	Apertura de ventana	Error	4
Acceso a recursos	Actividad de recursos	Acceso a recursos	Correcto	2
Acceso a recursos	Actividad de recursos	Acceso a recursos	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso a recursos	Actividad de recursos	Adjudicación del recurso	Correcto	2
Acceso a recursos	Actividad de recursos	Adjudicación del recurso	Error	3
Acceso a recursos	Actividad de recursos	Cierre del recurso	Correcto	2
Acceso a recursos	Actividad de recursos	Cierre del recurso	Error	3
Acceso a recursos	Actividad de recursos	Creación de recursos	Correcto	2
Acceso a recursos	Actividad de recursos	Creación de recursos	Error	3
Acceso a recursos	Actividad de recursos	Supresión de recursos	Correcto	2
Acceso a recursos	Actividad de recursos	Supresión de recursos	Error	3
Acceso a recursos	Actividad de recursos	Ejecución de recursos	Correcto	2
Acceso a recursos	Actividad de recursos	Ejecución de recursos	Error	3
Acceso a recursos	Actividad de recursos	Modificación del recurso	Correcto	2
Acceso a recursos	Actividad de recursos	Modificación del recurso	Error	3
Acceso a recursos	Actividad de recursos	Apertura de recursos	Correcto	2
Acceso a recursos	Actividad de recursos	Apertura de recursos	Error	3
Acceso al sistema	Actividad de autenticación	Autenticación	Correcto	2
Acceso al sistema	Actividad de autenticación	Autenticación	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso al sistema	Actividad de autenticación	Retroceso de autenticación	Correcto	2
Acceso al sistema	Actividad de autenticación	Retroceso de autenticación	Error	6
Acceso al sistema	Actividad de autenticación	Paquete de autenticación cargado	Correcto	3
Acceso al sistema	Actividad de autenticación	Paquete de autenticación cargado	Error	3
Acceso al sistema	Actividad de autenticación	Inicio de autenticación	Correcto	2
Acceso al sistema	Actividad de autenticación	Inicio de autenticación	Error	6
Acceso al sistema	Actividad de autorización	Autorización	Correcto	2
Acceso al sistema	Actividad de autorización	Autorización	Error	3
Acceso al sistema	Actividad de cierre de sesión	Cierre de sesión	Correcto	2
Acceso al sistema	Actividad de cierre de sesión	Cierre de sesión	Error	3
Acceso al sistema	Actividad de inicio de sesión	Intento de inicio de sesión	Correcto	2
Acceso al sistema	Actividad de inicio de sesión	Intento de inicio de sesión	Error	3
Acceso al sistema	Obtención de privilegios	Obtención de privilegios	Correcto	3
Acceso al sistema	Obtención de privilegios	Obtención de privilegios	Error	3
Acceso al sistema	Uso de privilegios	Uso de privilegios	Correcto	3
Acceso al sistema	Uso de privilegios	Uso de privilegios	Error	3

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Acceso al sistema	Actividad de configuración de usuario	Configuración de usuario	Correcto	2
Acceso al sistema	Actividad de configuración de usuario	Configuración de usuario	Error	3
Acceso al sistema	Actividad de sesión	Creación de sesión	Correcto	2
Acceso al sistema	Actividad de sesión	Creación de sesión	Error	3
Acceso al sistema	Actividad de sesión	Desconexión de sesión	Correcto	2
Acceso al sistema	Actividad de sesión	Desconexión de sesión	Error	3
Acceso al sistema	Actividad de sesión	Modificación de sesión	Correcto	3
Acceso al sistema	Actividad de sesión	Modificación de sesión	Error	3
Categoría desconocida	Clase desconocida	Acción desconocida	Desconocido	0
Gestión de vulnerabilidades	Evaluación de vulnerabilidades	Recopilación de información	Correcto	2
Gestión de vulnerabilidades	Evaluación de vulnerabilidades	Recopilación de información	Error	3
Gestión de vulnerabilidades	Evaluación de vulnerabilidades	Análisis de vulnerabilidades iniciado	Correcto	2
Gestión de vulnerabilidades	Evaluación de vulnerabilidades	Análisis de vulnerabilidades iniciado	Error	3
Gestión de vulnerabilidades	Evaluación de vulnerabilidades	Análisis de vulnerabilidades completado	Correcto	2

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Gestión de vulnerabilidades	Evaluación de vulnerabilidades	Análisis de vulnerabilidades completado	Error	3
Gestión de vulnerabilidades	Gestión de vulnerabilidades	Vulnerabilidad encontrada	Correcto	4
Gestión de vulnerabilidades	Gestión de vulnerabilidades	Vulnerabilidad encontrada	Error	3
Operaciones SIM	Gestión de alertas	Confirmación de alerta	Correcto	2
Operaciones SIM	Gestión de alertas	Confirmación de alerta	Error	3
Operaciones SIM	Gestión de alertas	Anotación de alerta	Correcto	2
Operaciones SIM	Gestión de alertas	Anotación de alerta	Error	3
Operaciones SIM	Gestión de alertas	Creación de alerta	Correcto	2
Operaciones SIM	Gestión de alertas	Creación de alerta	Error	3
Operaciones SIM	Gestión de alertas	Supresión de alerta	Correcto	3
Operaciones SIM	Gestión de alertas	Supresión de alerta	Error	3
Operaciones SIM	Gestión de alertas	Escalación de alerta	Correcto	2
Operaciones SIM	Gestión de alertas	Escalación de alerta	Error	3
Operaciones SIM	Gestión de alertas	Modificación de alerta	Correcto	2
Operaciones SIM	Gestión de alertas	Modificación de alerta	Error	3
Operaciones SIM	Gestión de alertas	Entrega de alerta	Correcto	2
Operaciones SIM	Gestión de alertas	Entrega de alerta	Error	3
Operaciones SIM	Gestión de línea de base	Aceptación de línea de base	Correcto	2

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Operaciones SIM	Gestión de línea de base	Aceptación de línea de base	Error	3
Operaciones SIM	Gestión de línea de base	Activación de línea de base	Correcto	2
Operaciones SIM	Gestión de línea de base	Activación de línea de base	Error	3
Operaciones SIM	Gestión de línea de base	Creación de línea de base	Correcto	2
Operaciones SIM	Gestión de línea de base	Creación de línea de base	Error	3
Operaciones SIM	Gestión de línea de base	Desactivación de línea de base	Correcto	3
Operaciones SIM	Gestión de línea de base	Desactivación de línea de base	Error	3
Operaciones SIM	Gestión de línea de base	Establecimiento de línea de base	Correcto	2
Operaciones SIM	Gestión de línea de base	Establecimiento de línea de base	Error	3
Operaciones SIM	Gestión de línea de base	Modificación de línea de base	Correcto	3
Operaciones SIM	Gestión de línea de base	Modificación de línea de base	Error	3
Operaciones SIM	Gestión de origen de evento	Autorización de origen de evento	Correcto	2
Operaciones SIM	Gestión de origen de evento	Autorización de origen de evento	Error	3
Operaciones SIM	Gestión de origen de evento	Configuración de origen de evento	Correcto	2
Operaciones SIM	Gestión de origen de evento	Configuración de origen de evento	Error	3
Operaciones SIM	Gestión de origen de evento	Descubrimiento de origen de evento	Correcto	2

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Operaciones SIM	Gestión de origen de evento	Descubrimiento de origen de evento	Error	3
Operaciones SIM	Gestión de origen de evento	Provisión de origen de evento	Correcto	2
Operaciones SIM	Gestión de origen de evento	Provisión de origen de evento	Error	3
Operaciones SIM	Gestión de incidentes	Cierre de incidente	Correcto	2
Operaciones SIM	Gestión de incidentes	Cierre de incidente	Error	3
Operaciones SIM	Gestión de incidentes	Creación de incidente	Correcto	2
Operaciones SIM	Gestión de incidentes	Creación de incidente	Error	3
Operaciones SIM	Gestión de incidentes	Supresión de incidente	Correcto	3
Operaciones SIM	Gestión de incidentes	Supresión de incidente	Error	3
Operaciones SIM	Gestión de incidentes	Modificación de incidente	Correcto	2
Operaciones SIM	Gestión de incidentes	Modificación de incidente	Error	3
Operaciones SIM	Gestión de incidentes	Resolución de incidente	Correcto	2
Operaciones SIM	Gestión de incidentes	Resolución de incidente	Error	3
Operaciones SIM	Gestión de investigaciones	Anotación de investigación	Correcto	2
Operaciones SIM	Gestión de investigaciones	Anotación de investigación	Error	3
Operaciones SIM	Gestión de investigaciones	Cierre de investigación	Correcto	2

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Operaciones SIM	Gestión de investigaciones	Cierre de investigación	Error	3
Operaciones SIM	Gestión de investigaciones	Supresión de investigación	Correcto	3
Operaciones SIM	Gestión de investigaciones	Supresión de investigación	Error	3
Operaciones SIM	Gestión de investigaciones	Modificación de investigación	Correcto	2
Operaciones SIM	Gestión de investigaciones	Modificación de investigación	Error	3
Operaciones SIM	Gestión de investigaciones	Apertura de investigación	Correcto	2
Operaciones SIM	Gestión de investigaciones	Apertura de investigación	Error	3
Operaciones SIM	Gestión de investigaciones	Pausa de investigación	Correcto	2
Operaciones SIM	Gestión de investigaciones	Pausa de investigación	Error	3
Operaciones SIM	Gestión de investigaciones	Resolución de investigación	Correcto	2
Operaciones SIM	Gestión de investigaciones	Resolución de investigación	Error	3
Operaciones SIM	Gestión de investigaciones	Reanudación de investigación	Correcto	2
Operaciones SIM	Gestión de investigaciones	Reanudación de investigación	Error	3
Operaciones SIM	Gestión de notificaciones	Creación de notificación	Correcto	2
Operaciones SIM	Gestión de notificaciones	Creación de notificación	Error	3
Operaciones SIM	Gestión de notificaciones	Entrega de notificación	Correcto	2

CATEGORÍA	CLASE	ACCIÓN	Resultado	Nivel de severidad
Operaciones SIM	Gestión de notificaciones	Entrega de notificación	Error	3
Operaciones SIM	Gestión de solicitudes	Anotación de solicitud	Correcto	2
Operaciones SIM	Gestión de solicitudes	Anotación de solicitud	Error	3
Operaciones SIM	Gestión de solicitudes	Cierre de solicitud	Correcto	2
Operaciones SIM	Gestión de solicitudes	Cierre de solicitud	Error	3
Operaciones SIM	Gestión de solicitudes	Creación de solicitud	Correcto	2
Operaciones SIM	Gestión de solicitudes	Creación de solicitud	Error	3
Operaciones SIM	Gestión de solicitudes	Modificación de solicitud	Correcto	2
Operaciones SIM	Gestión de solicitudes	Modificación de solicitud	Error	3
Operaciones SIM	Gestión de solicitudes	Entrega de solicitud	Correcto	2
Operaciones SIM	Gestión de solicitudes	Entrega de solicitud	Error	3