CA Enterprise Log Manager

ELM-Schemadefinition – Referenzhandbuch

r12.5

CA-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von 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
- CA Security Command Center (CA SCC)
- CA Service Desk
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Inhalt

Kapitel 7: Kategorie "Identitätsverwaltung" 435

Kapitel 16: Kategorie "Schwachstellenverwaltung" 1167

Kapitel 1: Was ist die CEG?

Die CA ELM-Schemadefinition (Common Event Grammar = CEG) ist eine Grammatik, die verwendet wird, um Ereignisinformationen nach deren Erfassung auszugeben. Sie bietet ein Mittel, die Rohereignisdaten, die von den Protokollquellen gesammelt wurden, zu normalisieren, und sie zur einfachen Anzeige und zum leichten Verständnis in einem allgemeinen Format anzugeben. Jedes Datenfeld in einem Protokollereignis wird in eine bestimmte Datendarstellung konvertiert und einheitlich kategorisiert. Die CEG verwendet einen Standardsatz von Feldern, um Ereignisinformationen anzugeben. Die Liste der Felder ist in sieben Bereiche aufgeteilt, die beschreibende Informationen über die Entitäten in dem Ereignis liefern.

Dieses Kapitel enthält folgende Themen:

Sieben Bereiche eines Ereignisses

Wenn ein Ereignis auftritt, gibt es unterschiedliche Arten von Informationen, die als Teil des Ereignisses angegeben werden. Diese Informationen können eine Entität oder das Ereignis selbst beschreiben.

Akteur - Quelle

Identifiziert die Entität, die die vom Ereignis verursachte Aktion initiiert.

Akteur - Ziel

Identifiziert die Entität, die das Ziel der vom Ereignis verursachten Aktion darstellt.

Ereignisquelle

Identifiziert die Entität, die das ursprüngliche Ereignis aufgezeichnet hat.

Observer (SIM-Agent)

Zeichnet das Ereignis auf und wählt eine Kopie des ursprünglichen Ereignisses aus der Ereignisquelle aus.

Ereignis-Repository

Identifiziert die temporäre Speicherung für das Ereignis, bis es von dem Agenten aufgezeichnet wird.

Ereignisspezifisch

Enthält die Daten, wie z. B. Ereignis-ID, Idealmodell, Ereigniskategorie usw.

Ergebnisspezifisch

Enthält die Daten, wie z. B. das Ergebnis und den Schweregrad des Ereignisses.

Akteur – Quelle

Feldname	Beschreibung
source_username	Benutzername oder die Identität, der/die die in den Ereignisinformationen angegebene Aktion initiiert hat
source_domainname	Authentifizierungsdomäne des Benutzernamens bzw. der im Feld "source_username" angegebenen Identität

Feldname	Beschreibung
source_groupname	Name der in den Ereignisinformationen angegebenen Gruppe
source_uid	Identifikationsnummer des Benutzernamens bzw. der im Feld "source_username" angegebenen Identität
source_gid	Identifikationsnummer der im Feld "source_groupname" angegebenen Gruppe
source_hostname	Name (FQDN oder Kurzname) des Hosts, von dem die in den Ereignisinformationen angegebene Aktion initiiert wurde; wenn "Source_hostname" leer ist, wird dieser Wert in den DM- und XMP-Dateien in das Feld "Source_address" übernommen.
source_hostdomainname	Domänenname des im Feld "source_hostname" angegebenen Hosts
source_address	IP-Adresse (oder sonstige Protokolladresse) des im Feld "source_hostname" angegebenen Hosts
source_mac_address	MAC-Adresse des im Feld "source_hostname" angegebenen Hosts.
source_port	Kommunikationsanschluss zur Initialisierung der in den Ereignisinformationen angegebenen Aktion
source_processname	Name des Prozesses bzw. der laufenden Anwendung, die die in den Ereignisinformationen angegebene Aktion initiiert hat
source_objectname	Name des Objekts, das an der in den Ereignisinformationen angegebenen Aktion beteiligt ist
source_objectattr	Name des Attributs des in den Ereignisinformationen angegebenen Objekts
source_objectid	Identifikationsnummer des im Feld "source_objectname" angegebenen Objekts
source_objectclass	Klasse des im Feld "source_objectname" angegebenen Objekts
source_objectvalue	Wert des im Feld "source_objectname" angegebenen Objekts

Akteur – Ziel

Feldname	Beschreibung
dest_username	Benutzername oder die Identität, der/die die in den Ereignisinformationen angegebene Aktion initiiert hat
dest_domainname	Authentifizierungsdomäne des Benutzernamens bzw. der im Feld "dest_username" angegebenen Identität
dest_groupname	Name der in den Ereignisinformationen angegebenen Gruppe
dest_uid	Identifikationsnummer des Benutzernamens bzw. der im Feld "dest_username" angegebenen Identität
dest_gid	Identifikationsnummer der im Feld "dest_groupname" angegebenen Gruppe
dest_hostname	Name (FQDN oder Kurzname) des Hosts, für den die in den Ereignisinformationen angegebene Aktion bestimmt war; wenn "Dest _hostname" leer ist, wird dieser Wert in den DM- und XMP-Dateien in das Feld "Dest _address" übernommen.
dest_hostdomainname	Domänenname des im Feld "dest_hostname" angegebenen Hosts
dest_address	IP-Adresse (oder sonstige Protokolladresse) des im Feld "dest_hostname" angegebenen Hosts
dest_mac_address	MAC-Adresse des im Feld "dest_hostname" angegebenen Hosts.
dest_port	Kommunikationsanschluss zur Initialisierung der in den Ereignisinformationen angegebenen Aktion
dest_processname	Name des Prozesses bzw. der laufenden Anwendung, die die in den Ereignisinformationen angegebene Aktion initiiert hat
dest_objectname	Name des Objekts, das an der in den Ereignisinformationen angegebenen Aktion beteiligt ist

Feldname	Beschreibung
dest_objectattr	Name des Attributs des in den Ereignisinformationen angegebenen Objekts
dest_objectid	Identifikationsnummer des im Feld "dest_objectname" angegebenen Objekts
dest_objectclass	Klasse des im Feld "dest_objectname" angegebenen Objekts
dest_objectvalue	Wert des im Feld "dest_objectname" angegebenen Objekts

Ereignisquelle

Feldname	Beschreibung
event_source_hostname	Der Name (FQDN oder Kurzname) des Hosts, auf dem die Ereignisinformationen ursprünglich angegeben wurden Wenn "event_source_hostname" leer ist, dann wird dieser Wert in den DM- und XMP-Dateien auf "Event_source_address" gesetzt.
event_source_hostdomainname	Domänenname des im Feld "event_source_hostname" angegebenen Hosts
event_source_address	Die IP-Adresse (oder sonstige Protokolladresse) des im Feld "event_source_hostname" angegebenen Hosts
event_source_processname	Der Name des Prozesses, der die Ereignisinformationen ursprünglich angegeben hat

Observer - Agent

Feldname	Beschreibung
agent_name	Der Name des SIM-Agenten, der die Ereignisinformationen aufzeichnet

Feldname	Beschreibung
agent_address	Die IP-Adresse (oder sonstige Protokolladresse) des im Feld "event_source_hostname" angegebenen Hosts
agent_hostname	Der Name (FQDN oder Kurzname) des Hosts, auf dem der im Feld "agent_name" angegebene Agent ausgeführt wird Wenn "Agent_hostname" leer ist, dann wird dieser Wert in den DM- und XMP-Dateien auf "Agent_address" gesetzt.
agent_hostdomainname	Domänenname des im Feld "agent_hostname" angegebenen Hosts
agent_version	Die Version des im Feld "agent_name" angegebenen Agenten
agent_id	Die Identifikationsnummer des im Feld "agent_name" angegebenen Agenten
agent_group	Der Gruppenname des Agenten, der dieses Ereignis erfasst hat
agent_connector_name	Der Name des Connectors des Agenten, der dieses Ereignis erfasst hat

Ereignis-Repository

Feldname	Beschreibung
receiver_name	Name des Empfängermoduls, das die Ereignisinformationen empfangen hat
receiver_hostname	Name (FQDN oder Kurzname) des Hosts, auf dem die Ereignisinformationen empfangen wurden
receiver_hostaddress	IP-Adresse (oder sonstige Protokolladresse) des im Feld "receiver_hostname" angegebenen Hosts
receiver_hostaddress	IP-Adresse (oder sonstige Protokolladresse) des im Feld "receiver_hostname" angegebenen Hosts
receiver_hostdomainname	Domänenname des im Feld "receiver_hostname" angegebenen Hosts
receiver_por	Kommunikationsanschluss für den im Feld "receiver_name" angegebenen Empfänger

Feldname	Beschreibung
receiver_time_gmt	Zeit (GMT), zu der das Ereignis empfangen wurde
receiver_timezone	Zeitzone des im Feld "receiver_hostname" angegebenen Hosts
receiver_version	Version des im Feld "receiver_name" angegebenen Empfängers

Ereignisspezifisch

Feldname	Beschreibung
event_protocol	Der Name bzw. die ID des in den Ereignisinformationen angegebenen Protokolls
event_logname	Der Name des in den Ereignisinformationen angegebenen Protokolls
event_euuid	Der eindeutige Bezeichner für diese Instanz der in den Ereignisinformationen angegebenen Aktion
event_count	Die Häufigkeit (als Ganzzahl), mit der dieses Ereignis innerhalb des im Feld "event_duration" angegebenen Zeitraums eingetreten ist
event_summarized	Ein Flag (W/F), das angibt, ob die vermittelten Ereignisinformationen zusammengefasst wurden
event_duration	Die seit dem im Feld "event_time_gmt" angegebenen Wert vergangene Zeit
event_time_gmt	Datum und Zeit, die in den Ereignisinformationen angegeben werden Für zusammengefasste Ereignisse enthält dieses Feld die in den Ereignisinformationen angegebene "Startzeit". Diese sollte als GMT-Zeit angegeben werden.
event_timezone	Die Zeitzone der in dem Ereignis angegebenen Informationen
event_sequence	Der Name der initiierten Sequenz, die die im Feld "event_action" angegebene Aktion ausgelöst hat Dies ist die zweite in der CEG verfügbare Gruppierungsebene.

Feldname	Beschreibung
event_trend	Die Daten, die in zukünftigen oder derzeit verwendeten Diagrammen berechnet werden
event_action	Der Name der in den Ereignisinformationen angegebenen Aktion Dies ist die vierte in der CEG verfügbare Normalisierungsebene.
event_id	Die systemeigene Identifikationsnummer für die angegebenen Ereignisinformationen Dieses Feld wird normalerweise vom Anbieter zur Verfügung gestellt.
event_category	Der Name der in den Ereignisinformationen angegebenen Ereigniskategorie Dies ist die zweite in der CEG verfügbare Normalisierungsebene.
event_class	Der Name der in den Ereignisinformationen angegebenen Ereignisklasse Welche Optionen für die Ereignisklasseninformationen verfügbar sind, hängt von der Kategorie des angegebenen Ereignisses ab. Dies ist die dritte in der CEG verfügbare Normalisierungsebene.
ideal_model	Der Name der Technologieklasse, der die Ereignisinformationen angegeben hat Dies ist die erste in der CEG verfügbare Normalisierungsebene.
event_severity	Eine ganze Zahl, die den von CA standardisierten Schweregrad für das Ereignis angibt

Ergebnisspezifisch

Feldname	Beschreibung
event_result	Der Rückgabewert der angegebenen Ereignisinformationen. Dieser Wert ist normalerweise "S" für Success (Erfolg) oder "F" für Failure (Fehler). In einigen Fällen kann dieses Feld auch andere Werte annehmen ("A" für Accepted (Akzeptiert), "D" für Dropped (Verworfen) und "R" für Rejected (Zurückgewiesen).

Feldname	Beschreibung
result_string	Deskriptive Zeichenfolge, die beschreibt, welche Aktion in diesem Ereignis angegeben wird. Gelegentlich wird dieses Feld vom Lieferanten bereitgestellt.
result_signature	Die Signatur ist der Name des Virus oder der Name der IDS-Signatur, für die eine Übereinstimmung gefunden wurde. Für andere Ereignistypen, die keine signaturbasierte Übereinstimmungssuche verwenden, bleibt dieses Feld leer.
result_code	Der in den Ereignisinformationen angegebene Rückgabecode Dieses Feld wird normalerweise für fehlgeschlagene Ereignisse ausgefüllt.
result_version	Die Version der im Feld "result_signature" angegebenen Signatur
result_priority	Die Priorität der angegebenen Ereignisinformationen
result_scope	Der Gültigkeitsbereich der angegebenen Ereignisinformationen
result_severity	Der Schweregrad der angegebenen Ereignisinformationen

Ereignistypen

Der Ereignistyp legt fest, wie die Informationsabschnitte ausgefüllt werden. Vier Ereignistypen werden von CEG berücksichtigt. Jeder Ereignistyp stellt eine Perspektive der im Ereignis angegebenen Aktion dar. Die Ereignisquelle zeichnet normalerweise ein Ereignis in Übereinstimmung mit einer der in diesem Abschnitt beschriebenen Perspektiven auf.

Typ 1: Lokales Ereignis

Der erste Ereignistyp ist das lokale Ereignis. Dieser Ereignistyp besitzt eine lokale Perspektive, die eine einzelne Entität involviert. Diese Entität stellt die Quelle, das Ziel, die Ereignisquelle und den im Ereignis angegebenen Agenten dar. Ereignisse des Typs 1 enthalten normalerweise sehr wenige Informationen, die im Ereignis angegeben sind. Die bereitgestellten Informationen müssen dupliziert werden, damit sie im CEG-Format korrekt angegeben werden.

Ein Beispiel für dieses Ereignis ist die Anmeldung über die Konsole, die auf demselben Host mit lokal installiertem Agenten aufgezeichnet wird.

Quelle	Ziel	Ereignisquelle	Agent
Host A	Host A	Host A	Host A

Typ 2: Remote-Ereignis

Der zweite Ereignistyp ist das Remote-Ereignis. Dieser Ereignistyp involviert zwei Entitäten, wobei eine der Entitäten entweder die Quelle oder das Ziel der im Ereignis angegebenen Aktion ist. Das bedeutet, dass die Agenten- und Ereignisquelle dieselbe Entität sind, da entweder die Quelle oder das Ziel der Aktion im Ereignis angegeben ist.

Ein Beispiel für diesen Ereignistyp ist ein Anmeldeereignis, das eine Verbindung zu einer Netzwerkfreigabe von einer Workstation ausdrückt. Der Agent ist auf dem Server installiert, der die Netzwerkfreigabe hostet.

Quelle	Ziel	Ereignisquelle	Agent
Host A	Host B	Host A	Host A
Host A	Host B	Host B	Host B

Typ 3: Überwachtes Ereignis

Der dritte Ereignistyp ist das überwachte Ereignis. Dieser Ereignistyp involviert drei Entitäten, wobei die Agent- und die Ereignisquelle dieselbe Entität besitzen. Diese Entität ist jedoch nicht die Quelle oder das Ziel des Ereignisses.

Ein Beispiel für diesen Ereignistyp ist eine Netzwerk-IDS oder Firewall, die eine Verbindung zwischen zwei Netzwerkentitäten überwacht.

Quelle	Ziel	Ereignisquelle	Agent
Host A	Host B	Host C	Host C

Typ 4: Verteiltes überwachtes Ereignis

Der vierte Ereignistyp ist das verteilte überwachte Ereignis. Dieser Ereignistyp involviert vier Entitäten, wobei der Agent von der Ereignisquelle ferninstalliert ist. Bei einer zweiten Konfiguration würde der Agent das Ereignis aus einer fünften Entität auswählen, das so genannte Ereignis-Repository, bei dem die Ereignisquelle das Ereignis zu diesem Repository führt und der Agent die Ereignisse aus dem Repository auswählt.

Ein Beispiel dieses Ereignistyps ist ein Netzwerk-IDS, der verteilte Sensoren und eine zentrale Management-Konsole (ISS) verwendet. Die Remote-Sensoren überwachen die Interaktionen zwischen den Netzwerkentitäten und leiten die Ereignisse an die zentrale Management-Konsole weiter. Ein auf dem fünften Host installierter Agent wählt diese Ereignisse aus und verarbeitet sie mit Hilfe der ODBC- oder OPSEC-Protokolle.

Quelle	Ziel	Ereignisquelle	Agent
Host A	Host B	Host C	Host D

Ermittlung des Ereignistyps

Dieser Abschnitt liefert Informationen darüber, wie der Typ des Ereignisses, das angegeben wurde, ermittelt wird. Das hauptsächliche Unterscheidungsmerkmal zwischen den Ereignistypen ist die Anzahl der Hosts (Netzwerkelemente), die in den Ereignisinformationen angegeben wird. Verwenden Sie diese Tabelle als Richtlinie, um den Ereignistyp für das Beispiel, mit dem Sie derzeit arbeiten, festzulegen.

Anzahl der Hosts	Ereignistyp
1	Typ 1
2	Typ 2
3	Typ 3
4+	Typ 4

Kapitel 2: Normalisierung und Kategorisierung von Ereignissen

Der nächste Schritt ist die Normalisierung und Kategorisierung der Ereignisse. CEG bietet verschiedene Felder, mit denen unterschiedliche Aspekte des Ereignisses normalisiert werden können. Der erste Aspekt, der normalisiert werden muss, ist die Technologieklasse, die das Ereignis angegeben hat. Als nächstes müssen die Kategorie, Klasse und Aktion, die von dem Ereignis angegeben werden, festgelegt werden.

Dieses Kapitel enthält folgende Themen:

Idealmodelle

Der erste Schritt für die Normalisierung der Ereignisinformationen in dem CEG ist die Bereitstellung eines Feldes zur Normalisierung der Technologie, die das Ereignis angibt. Diese Normalisierung der Technologieklasse ermöglicht eine schnelle und problemlose Referenz aller Ereignisse, die unabhängig vom Anwendungslieferanten von einer bestimmten Technologieklasse angegeben wurden Das CEG-Feld für die Normalisierung der Technologieklasse ist das Feld "ideal_model". Dieses Feld beschreibt die Technologieklasse, die das Ereignis angegeben hat. Beispiele für "ideal_model":

- Antivirus
- DBMS
- Firewall
- Host-IDS/IPS
- Netzwerk-IDS/IPS
- Netzwerkgerät
- Betriebssystem
- Webserver
- Schwachstellenverwaltung

Check Point, Cisco und Netscreen/Juniper z. B. stellen spezielle Produkte her, die mit einem Wert der Firewall im Feld "ideal_model" normalisiert werden.

Liste der Idealmodelle

Nachfolgend ist die aktuelle Liste von "ideal_models" aufgeführt:

Name	Beschreibung
Antivirus	Das Antivirus-Modell umfasst die Ereignisse, die von Antivirus-Produkten stammen. Beispiele: CA eTrust Antivirus, ITM, McAfee VirusScan, Symantec Antivirus Corporate Edition, TrendMicro OfficeScan.
Authentifizierungsdienst	CA SiteMinder Policy Server, Cisco Secure ACS
Content Management	CA SCM, SurfControl E-Mail-Filter
E-Mail-Server des Unternehmens	Microsoft Exchange

Name	Beschreibung
DBMS	Das DBMS-Modell umfasst Produkte wie MS-SQL, MySQL, DB2 oder Oracle.
Firewall	Eine Firewall ist eine Perimeter-Sicherheitseinrichtung, die üblicherweise verwendet wird, um Netzwerkelemente vor anderen Netzwerkelementen zu schützen. Dazu gehören Netzwerk-Firewalls und Personal Firewalls. BorderWare Firewall Server, CheckPoint, Cisco PIX, Netscreen/Juniper.
Host-IDS/IPS	Das Host-IDS-Modell umfasst Produkte wie Access Control, Cisco ACS oder McAfee Host Intrusion Prevention. eTrust Access Control - UNIX
Identitäts- und Kontobereitstellung	Das Modell Identitäts- und Kontobereitstellung umfasst Ereignisse, die von Bereitstellungsprodukten, wie z. B. CA Identity Manager, stammen.
Netzwerkgerät	Cisco IOS-basierte Geräte (Switches, Router) und andere Lieferanten.
Netzwerk-IDS/IPS	CA eTrust ID, Enterasys Dragon, SNORT, ISS usw.
Netzwerkverwaltung	CA Unicenter NSM Event Management, HP OpenView usw.
Betriebssystem	Windows, Unix, Top-Secret, ACF2, Top-Secret usw.
Proxyserver	WebSphere Edge Caching Proxy Server
Security Management System	CiscoWorks LMS, CiscoWorks VPN/Security Manager, CiscoWorks ACL Manager, Microsoft MOM, ISS RealSecurie Site Protector, Symantec Enterprise Security Manager, TrendMicro Control Manager
VPN Gateway	Nortel Connectivity
Schwachstellenverwaltung	Nessus Client, ISS Internet Scanner, Foundstone Foundscan, Nessus Server
Webserver	Microsoft IIS, Sun Sun One, Apache

Ereigniskategorien

Der zweite Schritt zur Normalisierung von Ereignisinformationen in der CEG besteht darin, die Kategorie zu bestimmen, in die die angegebenen Ereignisinformationen am besten passen. Mit dem bereitgestellten Feld zur Kategorisierung der angegebenen Ereignisinformationen unterstützt die CEG ein produktübergreifendes Reporting für umfassende Ereigniskategorien. Das in diesem Normalisierungsschritt verwendete CEG-Feld lautet "event_category". Es dient auch als bequeme Referenz zur Einrichtung von Filtern, mit dem Ziel, spezielle Informationen für das Konformitäts-Reporting anzuzeigen.

Beispiele für event_category:

- Identitätsverwaltung
- Netzwerksicherheit
- Hostsicherheit
- Betriebssicherheit

Zu Beispiel werden alle fehlgeschlagenen und erfolgreichen Anmeldungen mit demselben Wert – Systemzugriff – im Feld "event_category" aufgezeichnet.

Ereigniskategorienliste

Die nachstehende Liste enthält aktuelle Ereigniskategorien:

Name	Beschreibung
Identitätsverwaltung	Identitätsverwaltung umfasst Kontenverwaltung, Gruppenverwaltung, Identitätsverwaltung und Benutzerrechteverwaltung. Hierzu zählen folgende Ereignisse: Konto erstellt, Konto geändert, Hinzufügungen von Gruppenmitgliedern, Gruppenerstellungen oder -Löschungen usw.
Konfigurationsverwaltung	Konfigurations- und Richtlinienverwaltung umfasst Informationen aus Richtlinienänderungen oder Konfigurationsänderungen. Dies betrifft alle Einrichtungen, z. B. Firewalls, Hosts, Server oder Audit/SCC-Richtlinien. Hierzu zählen Ereignisse wie Richtlinienänderung, Richtlinienerstellung oder Konfigurationsänderungsereignisse.

Name	Beschreibung
Inhaltssicherheit	Inhaltssicherheit umfasst Informationen aus folgenden Quellen: Inhaltsprüfungstools zur Überwachung von Inhalten in Internet-Kommunikationskanälen wie E-Mail, WebMail, Instant Messaging, FTP und Online-Kollaborationstools (z. B. Blogs und Wikis).
Datenzugriff	Datenzugriff umfasst Informationen aus einem Datenbank-Management-System oder aus Datenbanküberwachungstools. Hierzu zählen Ereignisse wie Abfrage ausgeführt, Tabelle erstellt, Index geändert usw.
Hostsicherheit	Hostsicherheit und Integrität umfassen Informationen über die Sicherheit eines einzelnen Hosts (normalerweise Desktop-Systeme). Hierzu zählen Ereignisse wie Virus erkannt, Virus bereinigt etc.
Netzwerksicherheit	Netzwerksicherheit umfasst Informationen zum Schutz von Netzwerkentitäten vor dem Zugriff durch andere Netzwerkentitäten. Hierzu zählen Ereignisse wie Firewall-Unterbrechungsprotokolle oder IDS/IPS-Verstoßmeldungen.
Betriebssicherheit	Betriebssicherheit umfasst Informationen über die Fähigkeit, den Normalbetrieb aufrechtzuerhalten. Hierzu zählen Ereignisse wie Servicebeendigung, Servicestart, Herunterfahren des Systems oder Starten des Systems. Außerdem zählen hierzu gelöschte Sicherheitsprotokolle.
Physischer Zugriff	Physischer Zugriff umfasst Informationen über Versuche, physische Sicherheitsschranken zu überwinden. Hierzu zählen zum Beispiel Ereignisse wie Ausweis gescannt oder Kamera deaktiviert.
Ressourcenzugriff	Ressourcenzugriff umfasst Informationen über Versuche, auf Ressourcen zuzugreifen. Letztere beinhalten Dateizugriffressourcen, Registrierungsressourcen oder URI-Ressourcen. Bei Ressourcen steht "Host" für den Host, der das Ereignis aufgezeichnet hat. "Benutzer" steht für den Benutzer oder die Identität, der/die versucht, auf die Ressource zuzugreifen.

Name	Beschreibung
Systemzugriff	Systemzugriff umfasst Informationen über Versuche, auf verschiedene Systeme zuzugreifen. Hierzu zählen Ereignisse wie Anmeldungen, Versuche zur Festlegung des Benutzers und Netzwerkauthentifizierungsversuche (VPNs, NAP, 802.11x). In Bezug auf den Systemzugriff ist eine Ressource definiert als Anwendung, die den Anmeldeprozess vereinfacht. Ressourcen wären in diesem Zusammenhang zum Beispiel "ftpd" und "sshd".
Unbekannte Kategorie	Ereignisse, die keiner speziellen Kategorie zugeordnet sind, fallen unter die Kategorie "Unbekannt". Beispiel Datenzuordnungsdateien: Wenn keine der Zuordnungsbedingungen erlaubt, ein spezielles Ereignis zuzuordnen, wird das Ereignis mit dieser Kategorie gekennzeichnet. Datenzuordnungsdateien sollten aktualisiert werden, um die Anzahl der Ereignisse der Kategorie "Unbekannt" zu verringern.
Schwachstellenverwaltung	Schwachstellenverwaltung umfasst Informationen aus Tools für Sicherheitsbewertung und -Management. Hierzu zählen Ereignisse wie “Schwachstelle gefunden” oder “Patch erforderlich”.
SIM-Vorgänge	SIM-Vorgänge umfassen operative Berichte über den Zustand von Operationen für SIM. Diese Informationen sind unabhängig von den durch SIM erfassten und verarbeiteten Informationen.

Ereignisklassen

Der dritte Schritt zur Normalisierung von Ereignisinformationen in der CEG besteht darin, die Klasse der angegebenen Ereignisinformationen zu bestimmen. Mit dem Feld "event_class" werden Ereignisse einer speziellen Ereigniskategorie weiter aufgegliedert. Mit Hilfe einer weiteren Klassifizierungsebene können Sicherheitsereignisse weiter gruppiert werden, um spezielle Interessens- und Technologiebereiche abzudecken.

Das Feld "event_class" dient als Platzhalter für die Klassifizierung von Ereignissen innerhalb einer speziellen Kategorie. Es gehört sowohl zu einer Ereigniskategorie als auch zu einer Ereignisklasse. Beispielsweise gehört die Aktion "Kontoerstellung" zur Kategorie "Identitätsverwaltung" und zur Klasse "Kontenverwaltung".

Beispiele für Ereignisklassen innerhalb der Ereigniskategorie "Identitätsverwaltung":

- Kontenverwaltung
- Gruppenverwaltung
- Benutzerrollenverwaltung
- Benutzerrechteverwaltung

Ereignisklassenliste

Nachfolgend wird die aktuelle Liste mit Ereignisklassen erläutert.

Identitätsverwaltung

Name	Beschreibung
Kontenverwaltung	Die Klasse der Kontenverwaltung umfasst Aktionen, die Kontenaktivitäten, wie z. B. Kontenerstellung, Kontenlöschung, Kontendeaktivierung und Kontenänderung, betreffen.
Gruppenverwaltung	Die Klasse der Gruppenverwaltung umfasst Aktionen, die Gruppenaktionen, wie z. B. Gruppenerstellung, Änderung der Gruppenmitgliedschaft, Gruppenlöschung und Gruppenänderung, betreffen.

Name	Beschreibung
Identitätsverwaltung	Die Klasse der Identitätsverwaltung umfasst Aktionen, die Identitätsaktivitäten, wie z. B. Identitätserstellung, Identitätslöschung und Identitätsänderung, betreffen. Diese Ereignisklasse ist in der Regel auf Bereitstellungsprodukte, wie z. B. Identity Manager, beschränkt.
Benutzerrechteverwaltung	Die Klasse der Benutzerrechteverwaltung umfasst Aktionen, die die Erstellung, Löschung und Zuweisung von Benutzerrechten betreffen.
Benutzerrollenverwaltung	Die Klasse der Benutzerrollenverwaltung umfasst Aktionen, die Benutzerrollenaktivitäten, wie z. B. Benutzerrollenzuweisung, Zuweisung der Benutzerrolle "Admin" und andere, betreffen.

Konfigurationsverwaltung

Name	Beschreibung
Konfigurationsverwaltung	Die Konfigurationsverwaltungsklasse deckt Aktionen ab, die sich mit Konfigurationsaktivitäten wie Konfigurationsänderung, Konfigurationslöschung usw. befassen.
Richtlinienverwaltung	Die Richtlinienverwaltungsklasse deckt Aktionen ab, die sich mit Richtlinienaktivitäten befassen wie etwa Richtlinienerstellung, Richtlinienaktivierung, Richtlinienanwendung, Richtliniendeaktivierung und Richtlinienlöschung.
Sicherungsverwaltung	Die Sicherungsverwaltungsklasse deckt Aktionen ab, die sich mit der Sicherung von Konfigurationsdaten und realen Daten befassen. Diese Klasse wird bei Sicherungsaktionen im Zusammenhang mit Konfigurationsdaten der Konfigurationsverwaltungskategorie zugeordnet. Diese Klasse wird bei Sicherungsaktionen im Zusammenhang mit realen Daten der Betriebssicherheitskategorie zugeordnet.

Name	Beschreibung
Profilverwaltung	Die Profilverwaltungsklasse deckt Aktionen ab, die sich mit Profilaktivitäten befassen wie Profilerstellung, Profillöschung und Profiländerung. Ein Profil wird definiert, um basierend auf speziellen Bedingungen Geräte, Komponenten, Aktionen, Prozesse etc. zu gruppieren. Richtlinien bzw. Regeln werden anschließend auf der Grundlage von Profilen statt einzelnen Komponenten angewandt.

Inhaltsprüfung

Name	Beschreibung
E-Mail-Prüfung	
URL-Zugriff	

Datenzugriff

Name	Beschreibung
Anwendungsverwaltung	Die Anwendungsverwaltungsklasse deckt Aktionen ab, die sich mit Anwendungsverwaltungsaktivitäten wie Indexanalyse, Trigger-Erstellung usw. befassen.
Audit-Ereignisse	Die Audit-Ereignisklasse deckt Aktionen ab, die sich mit der Verwaltung von Audit-Services befassen, z. B. Audit-Aktionen, Audit-Berechtigungen und Änderung der Audit-Richtlinie.
Datenzugriff	Die Datenzugriffsklasse deckt Aktionen ab, die sich mit der Zuordnung von Datenelementen oder -Ressourcen zu Inhalten und Services befassen. Zum Beispiel: In Tabelle einfügen, Aus Anzeige auswählen, Aus Tabelle löschen, Tabelle trunkieren, Tabelle aktualisieren.

Name	Beschreibung
Objektverwaltung	Die Objektverwaltungsklasse deckt Aktionen ab, die sich mit Objektverwaltungsaktivitäten befassen wie Tabellenerstellung, Indexerstellung, Tabellenlöschung usw.
Peer-Verwaltung	Die Peer-Verwaltungsklasse deckt Aktionen ab, die sich mit Peer-Verwaltungsaktivitäten befassen wie Datenverknüpfungserstellung, Datenverknüpfungslöschung usw.
Berechtigungsverwaltung	Die Berechtigungsverwaltungsklasse deckt Aktionen ab, die sich mit der Verwaltung von Berechtigungen befassen, z. B. Rolle erstellen, Berechtigung gewähren, Rolle ändern, Rolle unterbrechen, Objekt gewähren, Rolle gewähren, Rolle widerrufen und Objekt widerrufen.
Service- und Anwendungsauslastung	Die Klasse für Service- und Anwendungsauslastung deckt Aktionen ab, die sich mit der Verwaltung und Verwendung von Services und Anwendungen befassen, z. B. Prozedurausführung, Methodenausführung usw.
Systemverwaltung	Die Systemverwaltungsklasse deckt Aktionen ab, die sich mit der Verwaltung von Systemaktivitäten wie Papierkorb löschen, Tabellenbereich ändern usw. befassen.

Hostsicherheit

Name	Beschreibung
Antivirusaktivität	Die Klasse für Antivirusaktivität umfasst Aktionen wie "Virus gefunden", "Virusaktualisierung angewandt" und andere.
IDS-/IPS-Aktivität	Die Klasse für IDS-/IPS-Aktivität umfasst Aktionen wie Richtlinienverletzung und andere.

Netzwerksicherheit

Name	Beschreibung
Verbindungsaktivität	Die Klasse der Verbindungsaktivität umfasst Aktionen, die die Verbindungsaktivität, wie z. B. Verbindungsversuche und andere, betreffen.
Aktivität bei Signaturverletzung	Die Klasse der Aktivität bei Signaturverletzung umfasst Aktionen, die die Signaturübereinstimmung, wie z. B. Signaturverletzung und andere, betreffen.
Anwendungssicherheit	Die von Netzwerkgeräten, wie IDS, IPS und Gateways, gemeldete Anwendungsaktivität
Verletzung der Unternehmensrichtlinien	Jede Netzwerkaktivität, die die Unternehmensrichtlinie verletzt
Informationsverlust	Netzwerkaktivität, die den versuchten oder erfolgreichen Datendiebstahl und die nicht autorisierte Datenübertragung betrifft
Berechtigungseskalation	Versuche, Benutzerberechtigungen zu eskalieren
DoS	Aktivität, die den Versuch betrifft, eine Computerressource für vorgesehene Benutzer unzugänglich zu machen
Verdächtige Aktivität	Jede Art einer gemeldeten verdächtigen Aktion, die nicht in andere Klassen in der Kategorie “Netzwerksicherheit” klassifiziert werden kann

Betriebssicherheit

Name	Beschreibung
Prozessaktivität	Die Klasse der Prozessaktivität umfasst Aktionen, die die Prozessaktivität, wie z. B. Prozessstart, Prozessstopp und andere, betreffen.
Systemaktivität	Die Klasse der Systemaktivität umfasst Aktionen, die die Systemaktivität, wie z. B. Systemstart, Systemstopp und andere, betreffen.

Name	Beschreibung
Sicherheitsprotokollaktivität	Die Klasse der Sicherheitsprotokollaktivität umfasst Aktionen, wie z. B. Löschen des Sicherheitsprotokolls, Sicherheitsprotokoll-Rollover und andere.
Sitzungsaktivität	Die Sitzungsaktivität umfasst Aktionen, wie z. B. Sitzungsstart, Sitzungsstopp und andere.
Sicherungsverwaltung	Die Sicherungsverwaltungsklasse deckt Aktionen ab, die sich mit der Sicherung von Konfigurationsdaten und realen Daten befassen. Diese Klasse wird bei Sicherungsaktionen im Zusammenhang mit Konfigurationsdaten der Konfigurationsverwaltungskategorie zugeordnet. Diese Klasse wird bei Sicherungsaktionen im Zusammenhang mit realen Daten der Betriebssicherheitskategorie zugeordnet.

Physischer Zugriff

Name	Beschreibung
Physische Zugriffsaktivität	Die Klasse des physischen Zugriffs umfasst Aktionen, bei denen der Versuch unternommen wird, über physische Sicherheitseinrichtungen zuzugreifen.

Ressourcenzugriff

Name	Beschreibung
Ressourcenaktivität	Die Klasse der Ressourcenaktivität umfasst Aktionen, die die Ressourcenaktivität, wie z. B. Ressource öffnen, Ressource schließen und andere, betreffen.

Systemzugriff

Name	Beschreibung
Authentifizierungsaktivität	Die Klasse der Authentifizierungsaktivität umfasst Aktionen, die die Authentifizierung von Anmeldeinformationen, wie z. B. Authentifizierungsversuche und anderes, betreffen.
Autorisierungsaktivität	Die Klasse der Autorisierungsaktivität umfasst Aktionen, die die Autorisierung von Anmeldeinformationen, wie z. B. Autorisierungsversuche und anderes, betreffen.
Anmeldeaktivität	Die Klasse der Anmeldeaktivität umfasst Aktionen, die die Anmeldeaktivität, wie z. B. Anmeldeversuche und anderes, betreffen.
Abmeldeaktivität	Die Klasse der Abmeldeaktivität umfasst Aktionen, die die Abmeldeaktivität, wie z. B. Abmeldung und anderes, betreffen.
Berechtigungserlangung	Die Klasse der Berechtigungserlangung umfasst Aktionen, wie z. B. Berechtigungserlangung und anderes.
Berechtigungsverwendung	Die Klasse der Berechtigungsverwendung umfasst Aktionen, wie z. B. Berechtigungsverwendung und anderes.
Sitzungsaktivität	Die Klasse der Sitzungsaktivität umfasst Aktionen, die die Sitzungsaktivität, wie z. B. Sitzungsstart, Sitzungstrennung und anderes, betreffen.
Aktivität zur Festlegung des Benutzers	Die Klasse der Festlegung des Benutzers umfasst Aktionen, wie z. B. Festlegung des Benutzers und anderes.

Unbekannte Kategorie

Name	Beschreibung
Unbekannte Klasse	Ereignisse, die keiner speziellen Klasse zugeordnet sind, werden der "Unbekannten Klasse" zugeordnet. Datenzuordnungsdateien sollten aktualisiert werden, um die Ereignisse mit "Unbekannter Klasse" zu reduzieren.

Schwachstellenverwaltung

Name	Beschreibung
Schwachstellenbewertung	Die Klasse der Schwachstellenbewertung umfasst Aktionen, die die Schwachstellenbewertung, wie z. B. Schwachstellenbewertung starten, Schwachstellenbewertung abgeschlossen und anderes, betreffen.
Schwachstellenverwaltung	Die Klasse der Schwachstellenverwaltung umfasst Aktionen, die die Verwaltung von Schwachstellen betreffen, wie beispielsweise "Schwachstelle gefunden", "Patch erforderlich" und andere.

SIM-Vorgänge

Name	Beschreibung
Alarmverwaltung	Die Klasse der Alarmverwaltung umfasst Aktionen, die die Verwaltung von Alarmen, wie z. B. Alarmerstellung, Alarmlöschung, Alarmeskalation, Alarmzuweisung und anderes, betreffen.
Baseline-Verwaltung	Die Klasse der Baseline-Verwaltung umfasst Aktionen, die die Verwaltung von Baseline-Tests, wie z. B. Baseline-Erstellung, Baseline-Löschung, Baseline-Aktivierung, Baseline-Einrichtung und anderes, betreffen.

Name	Beschreibung
Ereignisquellenverwaltung	Die Klasse der Ereignisquellenverwaltung umfasst Aktionen, die die Verwaltung von Ereignisquellen, wie z. B. Erkennung von Ereignisquellen, Bereitstellung von Ereignisquellen, Autorisierung von Ereignisquellen und anderes, betreffen.
Vorfallverwaltung	Die Klasse der Vorfallverwaltung umfasst Aktionen, die die Verwaltung von Vorfällen, wie z. B. Vorfallerstellung, Vorfalländerung, Vorfallauflösung und andere, betreffen.
Untersuchungsverwaltung	Die Klasse der Untersuchungsverwaltung umfasst Aktionen, die die Verwaltung von Untersuchungen, wie z. B. Untersuchung öffnen, Untersuchung löschen, Untersuchung schließen und andere, betreffen.
Benachrichtigungsverwaltung	Die Klasse der Benachrichtigungsverwaltung umfasst Aktionen, die die Verwaltung von Benachrichtigungen, wie z. B. Benachrichtungserstellung, Benachrichtigungsübermittlung und anderes, betreffen.
Anforderungsverwaltung	Die Klasse der Anforderungsverwaltung umfasst Aktionen, die die Verwaltung von Anforderungen, wie z. B. Anforderungserstellung, Anforderungsänderung, Anforderungsübermittlung und anderes, betreffen.

Ereignisaktionen

Der vierte Schritt zur Normalisierung von Ereignisinformationen in der CEG besteht darin, die normalisierte Aktion zu bestimmen, die in den Ereignisinformationen angegeben ist. Das Feld "event_action" bietet einen Platzhalter, in dem allgemeine Aktionen, die aufgetreten sind, mit einem allgemeinen Namen normalisiert werden können.

Es beschreibt kurz und genau, was stattgefunden hat. Kontoerstellung ist zum Beispiel eine Aktion, die voraussetzt, dass jemand ein Konto oder eine Reihe von Konten auf einem bestimmten Host erstellt hat.

Das Feld "event_action" gehört zu einer Ereigniskategorie und einer Ereignisklasse. Beispielsweise gehört die Aktion "Kontoerstellung" (event_action) zur Kategorie "Identitätsverwaltung" (event_category) und zur Klasse "Kontenverwaltung" (event_class).

Jede Ereignisaktion kann eine oder mehrere der folgenden Ergebniswerte aufweisen: Success (Erfolg), Failure (Fehler), Accept (Akzeptiert), Reject (Zurückgewiesen), Drop (Verworfen) und Unknown (Unbekannt).

Alle fehlgeschlagenen Anmeldungen werden zum Beispiel mit dem Aktionswert "Anmeldeversuch" im Feld "event_action" normalisiert. Wenn der Anmeldeversuch fehlgeschlagen ist, wird im Feld "event_result" als Wert "Fehler" angezeigt. Bei erfolgreicher Anmeldung zeigt das Feld "event_result" als Wert "Erfolg" an.

Ereignisaktionenliste

Die CEG gliedert sich in sechs Abschnitte. Jeder dieser sechs Abschnitte ist wie folgt weiter unterteilt. Zur erfolgreichen Zuordnung müssen aus jedem der angegebenen Unterabschnitte einige Informationen gemäß der obigen Bezeichnung zur Verfügung gestellt werden. Alle **fett** formatierten Felder sind erforderlich, damit die einzelnen Abschnitte das Ergebnis GENEHMIGT erhalten, sofern der jeweilige Abschnitt als primär eingestuft ist. Felder im **Fett-/Kursiv**-Format sind alternative Felder. Es ist nur eines der alternativen Felder erforderlich, um für einen Abschnitt das Ergebnis GENEHMIGT zu erhalten, sofern der jeweilige Abschnitt als primär eingestuft ist.

Informationen	Feldinformationen
Quelle – Benutzerinformationen	source_domainname, source_username, source_uid

Informationen	Feldinformationen
Quelle – Host-Informationen	*source_hostname*, *source_address*, source_mac_address, source_hostdomainname, source_port
Quelle – Objektinformationen	source_objectname, source_objectid, source_objectattr, source_objectclass, source_objectvalue
Quelle – Prozessinformationen	source_processname
Quelle – Gruppeninformationen	source_groupname, source_gid
Ziel – Benutzerinformationen	dest_domainname, dest_username, dest_uid
Ziel – Host-Informationen	*dest_hostname*, *dest_address*, dest_mac_address, dest_hostdomainname, dest_port
Ziel – Objektinformationen	dest_objectname, dest_objectid, dest_objectattr, dest_objectclass, dest_objectvalue
Ziel – Prozessinformationen	dest_processname
Ziel – Gruppeninformationen	dest_groupname, dest_gid
Agent – Informationen	agent_name, agent_version, agent_id, agent_group, agent_connector_name
Agent – Host-Informationen	*agent_hostname*, *agent_address*, agent_hostdomainname
Ereignisquelle – Host-Informationen	*event_source_hostname*, *event_source_address*, event_source_hostdomainname
Ereignisquelle – Informationen	*event_source_processname*
Ereignis – Informationen	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
Ergebnis – Informationen	event_result, result_string, result_signature, result_code, result_version, result_priority, result_scope, result_severity

Die beiden letzten Abschnitte der CEG sind für alle Aktionen erforderlich.

Bei jeder Aktion werden die CEG-Informationen nach folgenden Eigenschaften unterschieden: primär, sekundär oder tertiär. Primäre Informationen sind zu den meisten Ereignisquellen vorhanden und erforderlich, damit das Ereignis als zugeordnet gilt. Sekundäre Informationen sind zu einigen Ereignisquellen vorhanden und erwünscht, damit das Ereignis als zugeordnet gilt. Tertiäre Informationen schließlich sind möglicherweise zu einigen Ereignisquellen vorhanden. Falls vorhanden, sollte das Ereignis zugeordnet werden.

Bei der Kontoerstellungsaktion, zum Beispiel, stellt sich folgende Frage: Wer hat welches Konto auf welchem Host erstellt, und auf welchem Host wurden diese Ereignisinformationen angegeben? Die Antwort auf diese Frage könnte wie folgt lauten: Der Administrator erstellte BenutzerA auf HostA, und das Ereignis wurde auf HostA angegeben. Diese Informationen enthalten Werte für "Quelle – Benutzerinformationen", "Ziel – Host-Informationen" und "Ziel – Benutzerinformationen". Darüber hinaus sollte jede CEG-Ereignisinformation Angaben darüber enthalten, welcher Agent das Ereignis aufgezeichnet hat und auf welchem Host es angegeben wurde. Nachfolgend sind diese Informationen als Tabelle dargestellt:

Informationen	**Ebene**
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	sekundär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär

Informationen	Ebene
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Zu jeder Aktion in dieser Tabelle gibt es entsprechend formulierte Informationen. Bei Informationen in Ereignissen sind folgende Hinweise zu beachten:

Ereignisse des Typs 1:

- Der Host, auf dem die Informationen angegeben wurden, entspricht dem Host, auf dem das Konto erstellt wurde.
- Möglicherweise gibt es Informationen zu "Quelle – Host-Informationen". Wenn das der Fall ist, sind diese Informationen mit dem Host identisch, auf dem die Aktion erfolgte.
- Bei diesen Ereignissen sollte nur ein Set mit Host-Informationen vorkommen.

Ereignisse des Typs 2:

- In diesen Ereignissen sollten zwei Sets mit Host-Informationen vorkommen.
- Das erste Set mit Host-Informationen bezieht sich auf den Abschnitt "Quelle – Host-Informationen". Diese Host-Informationen sollten sich von dem Host, auf dem die Aktion erfolgte, unterscheiden.
- Möglicherweise gibt es Informationen zu dem Host, auf dem der SIM-Agent installiert ist. Diese Informationen sollten aber mit dem Host identisch sein, auf dem die Aktion erfolgte und dem Host, auf dem die Ereignisinformationen angegeben wurden.

Ereignisse des Typs 3:

- In diesen Ereignissen gibt es drei Sets mit Host-Informationen.
- Das erste Set mit Informationen enthält "Quelle – Host-Informationen".
- Das zweite Set mit Informationen enthält "Ziel – Host-Informationen" in Bezug auf den Host, auf dem die Aktion erfolgte.
- Das dritte Set mit Informationen enthält "Ereignisquelle – Host-Informationen" in Bezug auf den Host, auf dem das Ereignis angegeben wurde und der SIM-Agent installiert ist.

Ereignisse des Typs 4:

- In diesen Ereignissen gibt es vier Sets mit Host-Informationen.
- Das erste Set mit Informationen enthält "Quelle – Host-Informationen".
- Das zweite Set mit Informationen enthält "Ziel – Host-Informationen" in Bezug auf den Host, auf dem die Aktion erfolgte.

- Das dritte Set mit Informationen enthält "Ereignisquelle – Host-Informationen" in Bezug auf den Host, auf dem das Ereignis angegeben wurde.
- Das vierte Set mit Informationen enthält "Agent – Host-Informationen" in Bezug auf den Host, auf dem der SIM-Agent installiert ist.

Ereignisergebnis

Jedes Ereignis wird mit Hilfe von 16 Abschnitten beschrieben. Jeder Abschnitt definiert eine Reihe von Feldern.

Jeder Abschnitt wird als primär, sekundär oder tertiär eingestuft.

Ein Ereignis gilt als zugeordnet, wenn mindestens eines der erforderlichen Felder in jedem primären Abschnitt vorhanden ist.

Klassifizierung	Informationen verfügbar	Bedingung
primär	zu den meisten Ereignisquellen	erforderlich
sekundär	zu einigen Ereignisquellen	erwünscht
tertiär	zu einigen Ereignisquellen	Optional

Beispiel für die Zuordnung von Ereignisergebnissen

Betrachten Sie das folgende Beispiel: Wer erstellte welches Konto auf welchem Host, und auf welchem Host wurde dieses Konto für die Ereignisaktion "Kontoerstellung" angegeben. Die Informationen sind als primär, sekundär oder tertiär eingestuft.

Überprüfen Sie zunächst die Tabelle der Kontoerstellungsaktion in der Kontenverwaltungsklasse der Identitätsverwaltungskategorie.

Informationen	Ebene
Quelle – Benutzerinformationen	primär *(von wem erstellt)*
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär

Informationen	Ebene
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär *(welches Konto)*
Ziel – Host-Informationen	primär *(welcher Host)*
Ziel – Objektinformationen	sekundär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär *(Auf welchem Host ausgegeben?)*
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Schweregrad des Ereignisses

Schweregrad des Ereignisses ist das letzte für die Standardisierung verwendete CEG-Feld. Schweregrad des Ereignisses ist die Interpretation der Bedeutung eines Ereignisses, die für alle Typen von Ereignissen gültig ist. Das Feld "event_severity" enthält einen Schweregradwert zwischen 0 und 7 mit klar definierten Beschreibungen.

Der Schweregrad des Ereignisses liefert einen Bezugspunkt für den Vergleich der internen Relativität eines Sicherheitsereignisses in Bezug auf dessen Gefahren und Implikationen auf die Sicherheit, Stabilität, Verfügbarkeit und Integrität des Systems. Als Feld ist "event_severity" nicht immer "result_severity" zugeordnet, überträgt jedoch ähnliche Meldungen.

Der Zweck der Felder "event_severity" im Fall von CEG ist es, den Wert des Feldes "result_severity", der von unterschiedlichen Herstellern in deren Sicherheitsprotokollen zugewiesen wurde, einem gemeinsamen Nenner zuzuordnen.

Werte für Schweregrad des Ereignisses

Die Zuweisung basiert auf allgemeinen Sicherheitsprinzipien und Best Practices. Vom Standpunkt der Sicherheitsimplikation aus betrachtet ist z. B. eine fehlgeschlagene Aktion schwerwiegender zu bewerten als eine erfolgreiche Aktion. In der folgenden Tabelle werden für alle acht Schweregrade Wert, Name sowie eine Beschreibung angegeben. Eine detaillierte Liste mit Zuweisungen des Schweregrads ist in Anhang A enthalten.

Wert	Name	Beschreibung
0	Unbekannt	Unbekannte Ereignisse Nicht CEG zugeordnete Ereignisse Nicht klassifiziert
1	Debug	Meldung, die nur beim Debugging erscheint Ereignisse in produktionsloser Umgebung
2	Informationen	Informationen zur allgemeinen Systemoperation Allgemeine Informationen zur Sicherheit Hinweis
3	Warning (Warnung)	Ungewöhnliche Änderungen für System/Funktion/Sicherheit Normaler, aber bedeutsamer Zustand Fehlerhafte Operationen Verminderte Leistung
4	Minor_Impact	Geringfügige Auswirkung auf System/Funktion Geringfügige Auswirkung auf Sicherheit
5	Major_Impact	Schwerwiegende Auswirkung auf System/Funktion Schwerwiegende Auswirkung auf Sicherheit
6	Critical (Kritisch)	Unmittelbare Reaktion erforderlich Wahrscheinliche Sicherheitslücke

Wert	Name	Beschreibung
7	Fatal (Schwerwiegend)	System nicht anwendbar/nicht verfügbar Hohe Wahrscheinlichkeit einer Sicherheitslücke Nicht zu behebende Probleme

Schweregrad 0 und 1 sind derzeit keiner bestehenden CEG-Ereignisaktion zugewiesen und für zukünftige Zwecke reserviert. Für restliche Schweregrade gelten folgende Richtlinien:

Schweregrad 2:

- Zuweisung zu normaler Systemoperation
- Sicherheitsrelevante Ereignisse mit einem Erfolgsergebnis

Schweregrad 3:

- Zuweisung zu normaler Systemoperation oder sicherheitsrelevanten Ereignisaktionen mit einem Fehlerergebnis
- Zuweisung zu ungewöhnlicher/seltener Systemoperation oder sicherheitsrelevanten Ereignissen mit einem Erfolgsergebnis

Schweregrad 4:

- Hauptsächlich Anwendungs- und Systemverwaltungsaktionen, die sich auf andere Systeme oder mehrfache Funktionen auswirken
- Ereignisse, die eine höhere Aufmerksamkeitsstufe als Warnstufe gewähren
- Geringfügige Fehlerbedingung

Schweregrad 5:

- Verhältnismäßig weniger kritische Ereignisse
- Schwerwiegende Fehlerbedingung

Schweregrad 6:

- Zuweisung zu Bereichen und Problemen mit hohen Sicherheitsimplikationen, für die sofortige Aufmerksamkeit oder Behebung erforderlich sind, wie z. B. Antivirusaktivitäten, Aktivitätsprotokolle und physikalische Sicherheit

Schweregrad 7:

- Zuweisung zu Ereignissen zum Herunterfahren des Systems

Kapitel 3: Konfigurationsverwaltungskategorie

Dieses Kapitel enthält folgende Themen:

Konfigurationsverwaltungsklasse

Konfigurationsänderungsaktion

Die Konfigurationsänderungsaktion erfolgt, wenn die Konfiguration eines bestimmten Systems oder einer bestimmten Anwendung geändert wird.

Informationen	Ebene
Quelle – Benutzerinformationen	Primär*
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	Primär*
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär

Informationen	Ebene
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welcher Benutzer oder welcher Prozess die Konfiguration von welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

* Diese Aktion erfordert entweder "Quelle – Benutzerinformationen" oder "Quelle – Prozessinformationen".

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Konfigurationsfehleraktion

Die Konfigurationsfehleraktion erfolgt, wenn die Benachrichtigung gesendet wird, dass ein Host auf einen Fehler in den Konfigurationsinformationen für diesen Host gestoßen ist. Wenn diese Aktion fehlschlägt, kann kein Fehler berichtet werden, und es erfolgt keine Aktion.

Informationen	Ebene
Quelle – Benutzerinformationen	tertiär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär

Informationen	Ebene
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welcher Host zu welchen Konfigurationsinformationen einen Konfigurationsfehler berichtet. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	6

Aktion "Konfiguration -Alles leeren"

Die Aktion "Konfiguration - Alles leeren" erfolgt, wenn entsprechende Ereignisinformationen zum Leeren aller Konfigurations-Cache-Informationen auf einem bestimmten Host oder System gesendet werden. Es gibt zwei mögliche Ergebnisse für diese Aktion: S für Success (Erfolg) und F für Failure (Fehler).

Informationen	Ebene
Quelle – Benutzerinformationen	tertiär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär

Informationen	Ebene
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welcher Host die Konfigurations-Cache-Informationen leert. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Aktion "Konfiguration für 'Authentifizierungsbereiche' leeren"

Die Aktion "Konfiguration für 'Authentifizierungsbereiche' leeren" erfolgt, wenn entsprechende Ereignisinformationen zum Leeren aller Konfigurations-Cache-Informationen in Bezug auf Authentifizierungsbereiche oder Authentifizierungsdomänen auf einem bestimmten Host oder System gesendet werden. Es gibt zwei mögliche Ergebnisse für diese Aktion: S für Success (Erfolg) und F für Failure (Fehler).

Informationen	Ebene
Quelle – Benutzerinformationen	tertiär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär

Informationen	Ebene
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welcher Host die Konfigurations-Cache-Informationen in Bezug auf Authentifizierungsbereiche leert. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Aktion "Konfiguration für 'Benutzer-Cache' leeren"

Die Aktion "Konfiguration für 'Benutzer-Cache' leeren" erfolgt bei Vorliegen von Ereignisinformationen zum Leeren aller Konfigurations-Cache-Informationen in Bezug auf Benutzerobjekte auf einem bestimmten Host oder System. Es gibt zwei mögliche Ergebnisse für diese Aktion: S für Success (Erfolg) und F für Failure (Fehler).

Informationen	Ebene
Quelle – Benutzerinformationen	tertiär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welcher Host die Konfigurations-Cache-Informationen in Bezug auf Benutzerobjekte leert. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Ergebnis	event_result	event_severity
Failure (Fehler)	F	3

Konfigurationsalarm – Aktion

Beim Konfigurationsalarm werden Informationen zu Alarmbedingungen, die während Konfigurationsänderungen auftreten, ausgegeben oder zu Alarmfehlern im Zusammenhang mit einer Konfigurationseinstellung.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	7

Konfigurationsbenachrichtigung – Aktion

Bei der Konfigurationsbenachrichtigung werden generische Konfigurationsinformationen ausgegeben. Es gibt zwei mögliche Ergebnisse für diese Aktion: S für Success (Erfolg) und F für Failure (Fehler).

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Bei dieser Aktion ist es wichtig zu wissen, welcher Host die Konfigurations-Cache-Informationen in Bezug auf Benutzerobjekte leert. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Lesen von Konfigurationen – Aktion

Beim Lesen von Konfigurationen geht es um Informationen zum Lesen oder Laden einer Konfiguration, zum Beispiel von einer Konfigurationsdatei aus.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Konfigurations-Lesestart"

Die Aktion "Konfigurations-Lesestart" erfolgt, wenn die Benachrichtigung gesendet wird, dass ein Host mit dem Lesen der Konfigurationsinformationen begonnen hat. Wenn diese Aktion fehlschlägt, ist keine Aktion aufgetreten.

Informationen	Ebene
Quelle – Benutzerinformationen	tertiär
Quelle – Host-Informationen	primär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welcher Host welche Konfiguration von welchen Host abruft. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Konfigurationsstatus – Aktion

Beim Konfigurationsstatus geht es um Informationen zum Status einer Konfigurationseinstellung.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Konfigurationswarnaktion

Die Konfigurationswarnaktion erfolgt, wenn die Benachrichtigung gesendet wird, dass ein Host auf eine Warnung in den Konfigurationsinformationen für diesen Host gestoßen ist. Wenn diese Aktion fehlschlägt, kann kein Fehler berichtet werden, und es erfolgt keine Aktion.

Informationen	Ebene
Quelle – Benutzerinformationen	tertiär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welcher Host zu welchen Konfigurationsinformationen eine Konfigurationswarnung ausgibt. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Success (Erfolg)	S	3

Systemzeitänderung

Die Systemzeitänderung erfolgt beim Ändern der Systemzeit auf einem bestimmten System.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär*
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär*
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer oder welcher Prozess die Systemzeit auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

* Diese Aktion erfordert entweder "Quelle – Benutzerinformationen" oder "Quelle – Prozessinformationen".

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Ergebnis	event_result	event_severity
Fehler	F	4

Aufgabenerstellung

Die Aufgabenerstellung erfolgt beim Erstellen einer Instanz einer Aufgabe auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer die Aufgabe auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aufgabenlöschung

Die Aufgabenlöschung erfolgt beim Löschen eines geplanten Jobs oder Workflows. Gültig für Planer auf Betriebssystemebene unter Windows oder UNIX oder einer anderen Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Aufgabe auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aufgabenänderung

Die Aufgabenänderung erfolgt beim Ändern einer Instanz einer Aufgabe auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Aufgabe auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aufgabenbericht

Der Aufgabenbericht erfolgt bei der Berichterstellung eines geplanten Jobs oder Workflows. Gültig für Planer auf Betriebssystemebene unter Windows oder UNIX oder einer anderen Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle - Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Aufgabe auf welchem Host berichtet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse der Richtlinienverwaltung

Aktion zur Einrichtung einer Kennwortrichtlinie

Mit der Aktion zur Einrichtung einer Kennwortrichtlinie werden Informationen zur Einrichtung von Kennwortrichtlinien zum Beispiel zur Steuerung der Kennwortqualität oder der Kennwortdauer ausgedrückt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Richtlinienaktivierung

Die Richtlinienaktivierung erfolgt beim Aktivieren einer speziellen Richtlinie auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär*
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär*
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer oder welcher Prozess welche Richtlinie auf welchem Host aktiviert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

* Diese Aktion erfordert entweder "Quelle – Benutzerinformationen" oder "Quelle – Prozessinformationen".

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Richtlinienanwendung

Die Richtlinienanwendung erfolgt beim Anwenden einer speziellen Richtlinie auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär*
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär*
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer oder welcher Prozess welche Richtlinie auf welchem Host angewendet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

* Diese Aktion erfordert entweder "Quelle – Benutzerinformationen" oder "Quelle – Prozessinformationen".

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Richtlinienerstellung

Die Richtlinienerstellung erfolgt beim Erstellen einer Richtlinie auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär*
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär*
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer oder welcher Prozess welche Richtlinie auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

* Diese Aktion erfordert entweder "Quelle – Benutzerinformationen" oder "Quelle – Prozessinformationen".

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Richtliniendeaktivierung

Die Richtliniendeaktivierung erfolgt beim Deaktivieren einer speziellen Richtlinie auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär*
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär*
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer oder welcher Prozess welche Richtlinie auf welchem Host deaktiviert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

* Diese Aktion erfordert entweder "Quelle – Benutzerinformationen" oder "Quelle – Prozessinformationen".

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Richtlinienlöschung

Die Richtlinienlöschung erfolgt beim Löschen einer Richtlinie auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär*
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär*
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer oder welcher Prozess welche Richtlinie auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

* Diese Aktion erfordert entweder "Quelle – Benutzerinformationen" oder "Quelle – Prozessinformationen".

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Richtlinienfehler – Aktion

Ein Richtlinienfehler bezieht sich auf Ereignisinformationen zu Richtlinien-Management-Fehlern.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär

Informationen	Ebene
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Bei dieser Aktion ist es von Bedeutung, welcher Benutzer oder Prozess welchen Fehler auf welchem Host verursacht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

* Diese Aktion erfordert entweder "Quelle – Benutzerinformationen" oder "Quelle – Prozessinformationen".

Ergebnis	event_result	event_severity
Erfolgreich	S	5

Richtlinienauflistung – Aktion

Die Richtlinienauflistung erfolgt beim Auflisten einer Richtlinie auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär

Informationen	Ebene
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Bei dieser Aktion ist es von Bedeutung, welcher Benutzer oder Prozess welche Richtlinie auf welchem Host aufgelistet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	2

Richtlinienänderung

Die Richtlinienänderung erfolgt beim Ändern einer Richtlinie auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär*
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär

Informationen	Ebene
Quelle - Prozessinformationen	Primär*
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer oder welcher Prozess welche Richtlinie auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

* Diese Aktion erfordert entweder "Quelle – Benutzerinformationen" oder "Quelle – Prozessinformationen".

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Richtlinienbenachrichtigung – Aktion

Bei der Richtlinienbenachrichtigung werden Informationen zu Benachrichtigungen aus der Richtlinien-Engine oder zu Benachrichtigungen im Zusammenhang mit der Richtlinienverwaltung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Richtlinienersetzung – Aktion

Bei der Richtlinienersetzung werden Informationen zur Ersetzung einer bestehenden Richtlinie durch eine neue Richtlinie ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Richtlinienwarnung – Aktion

Eine Richtlinienwarnung enthält Informationen zu Richtlinien-Management-Warnungen.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär
Ergebnis - Informationen	Primär

Bei dieser Aktion ist es von Bedeutung, welcher Benutzer oder Prozess auf welchem Host eine Warnung ausgegeben hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	5

Richtlinien- oder Regelstatus

Der Richtlinien- oder Regelstatus behandelt die Angabe von Informationen über das Ereignis, das für jeden Windows Filtering Platform Provider protokolliert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Sicherungsverwaltungsklasse

Sicherung der Netzwerkgerätkonfiguration

Die Sicherung der Netzwerkgerätkonfiguration erfolgt bei der Sicherung der Konfigurationsinformationen, die auf Geräten wie Router, Switches, Firewalls, drahtlosen Geräten, Lastenausgleichern usw. gespeichert sind.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Prozess welche Konfiguration auf welchem Gerät gesichert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Wiederherstellung der Netzwerkgerätkonfiguration

Die Wiederherstellung der Netzwerkgerätkonfiguration erfolgt bei der Wiederherstellung der Konfigurationsinformationen vom Sicherungsserver auf Geräten wie Router, Switches, Firewalls, drahtlosen Geräten, Lastenausgleichern usw.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Prozess welche Konfiguration auf welchem Gerät wiederhergestellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse der Profilverwaltung

Profilalarm – Aktion

Beim Profilalarm werden Informationen zu profilbezogenen Alarmen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Profilerstellung

Die Profilerstellung erfolgt beim Erstellen von Profilen auf Gruppensystemen, Geräten, Anwendungen, Netzwerken usw. für die Verwaltung von Richtlinien auf Grundlage des Profils/der Profile.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle - Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welches Profil auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Profillöschung

Die Profillöschung erfolgt beim Löschen von Profilen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle - Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welches Profil auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Profilfehler – Aktion

Bei der Aktion "Profilfehler" werden Informationen zu profilbezogenen Fehlern ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Profilauflistung – Aktion

Die Profillöschung erfolgt, wenn Profile auf einem bestimmten Host aufgelistet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Bei dieser Aktion ist es von Bedeutung, von welchem Konto welches Profil auf welchem Host aufgelistet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Profiländerung

Die Profiländerung erfolgt beim Ändern oder Aktualisieren von Profilen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle - Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welches Profil auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Profilbenachrichtigung – Aktion

Bei der Profilbenachrichtigung werden Informationen zu Profilbenachrichtigungen und systemgenerierten Meldungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Profilstatus – Aktion

Bei der Aktion "Profilstatus" werden Informationen zum Profilstatus ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Profilwarnung

Bei der Profilwarnung werden Informationen über Warnungen im Zusammenhang mit Profilen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	**Ebene**	
Ergebnis - Informationen	Primär	
Ergebnis	**event_result**	**event_severity**
Fehler	F	4

Kapitel 4: Inhaltssicherheitskategorie

Dieses Kapitel enthält folgende Themen:

Verhinderung von Datenverlusten – Klasse

Inhaltsprüfungsaktion

Bei der Inhaltsprüfungsaktion werden Informationen zum Prüfen von Inhalten zur Verhinderung von Datenverlusten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Sekundär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Richtlinienverletzung – Aktion

Bei der Richtlinienverletzung werden Informationen zu Richtlinienverletzungen im Zusammenhang mit Steuerelementen und Richtlinien zur Verhinderung von Datenverlusten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär

Informationen	Ebene	
Ergebnis - Informationen	Primär	
Ergebnis	**event_result**	**event_severity**
Fehler	F	5

E-Mail-Prüfung – Klasse

Anhang-Scan-Aktion

Die Anhang-Scan-Aktion erfolgt, wenn entsprechende Ereignisinformationen zum Scannen von Anhängen in E-Mails gesendet werden. Das Ereignis wird ausgelöst, wenn ein bestimmter Host den Transport einer E-Mail zwischen zwei Netzwerkentitäten aufzeichnet. Diese Ereignisse werden generiert, wenn der E-Mail-Server die E-Mail mit Anhang verarbeitet.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	primär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	tertiär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	sekundär
Ereignis – Informationen	primär

Informationen	Ebene
Ergebnis – Informationen	primär

Für diese Aktion ist die Information von Bedeutung, welcher Host auf welchen anderen Host zuzugreifen versucht. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Aktion "Vertraulichkeitsverlust"

Die Aktion "Vertraulichkeitsverlust" erfolgt, wenn entsprechende Ereignisinformationen zum Scannen von E-Mails nach vertraulichen Informationen gesendet werden. Das Ereignis wird ausgelöst, wenn ein definierter Host den Transport einer E-Mail zwischen zwei Netzwerkentitäten aufzeichnet. Diese Ereignisse werden generiert, wenn die Content-Management-Software die E-Mail und Prüfungen auf vertrauliche Angelegenheiten verarbeitet.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	primär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär

Informationen	Ebene
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	sekundär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welcher Benutzer (Absender) versucht, an welchen Benutzer (Empfänger) eine E-Mail mit vertraulichen Informationen zu senden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

E-Mail-Prüfungsaktion

Die E-Mail-Prüfungsaktion erfolgt, wenn Ereignisinformationen zum Scannen von E-Mails gesendet werden.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	primär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär

Informationen	Ebene
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	sekundär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Profanity-Erkennung

Die Profanity-Erkennung erfolgt, wenn Ereignisinformationen über das Scannen von E-Mails mit ungültigen Wörtern auf zwei Netzwerkelementen, die von einem bestimmten Host aufgezeichnet wurden, gesendet werden. Diese Ereignisse werden erzeugt, wenn die Content Management Software die E-Mail verarbeitet und der Profanity-Detektor diese intern prüft.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär

Informationen	Ebene
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer (Sender) versucht, eine E-Mail mit Profanität an welchen Benutzer (Empfänger) zu senden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Spam-Erkennung

Die Spam-Erkennung erfolgt, wenn Ereignisinformationen über die Erkennung von Spam zwischen zwei Netzwerkelementen, die von einem bestimmten Host aufgezeichnet wurden, gesendet werden. Diese Ereignisse können erzeugt werden, wenn Sie versuchen, auf eine Website zuzugreifen und der Inhalt der Website als Spam kategorisiert ist.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär

Informationen	Ebene
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Primär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Host auf welchen anderen Host zuzugreifen versucht. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Nachrichtenüberprüfung – Klasse

Nachrichtenüberprüfung – Aktion

Die Nachrichtenüberprüfung erfolgt, wenn eine Nachricht von einer Kontrollentität, z. B. Compliance-Scan, überprüft wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär

Informationen	Ebene
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Nachrichtenablehnung – Aktion

Die Nachrichtenablehnung erfolgt, wenn eine Nachricht von einer Kontrollentität, z. B. Compliance-Scan, abgelehnt wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär

Informationen	Ebene
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse des URL-Zugriffs

URL-Filterung

Die URL-Filterung erfolgt, wenn Ereignisinformationen über den Zugriff auf URLs zwischen zwei Netzwerkelementen gesendet werden, die von einem bestimmten Host aufgezeichnet wurden. Die Ereignisse können erzeugt werden, wenn auf eine URL zugegriffen wird, und diese gegen die für die SPA-URL-Filterung eingerichtete Content Management Software-Richtlinie validiert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle - Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär

Informationen	Ebene
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Host auf welches Objekt (URL) versucht zuzugreifen. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

URL-Umleitung – Aktion

Die URL-Umleitung findet statt, wenn Ereignisinformationen zu einem Client an eine andere URL umgeleitet werden, beispielsweise zur Authentifizierung.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär

Informationen	Ebene
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Host an welches Objekt (URL) umleitet. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

HTTP-Filteraktion

Die HTTP-Filteraktion erfolgt, wenn Ereignisinformationen über den Zugriff auf HTTP-Protokoll/HTTP-Downloads zwischen zwei Netzwerkelementen, die auf einem bestimmten Host aufgezeichnet wurden, gesendet werden. Diese Ereignisse können erzeugt werden, wenn über das HTTP-Protokoll auf eine URL zugegriffen wird, und diese gegen die für den HTTP-Zugriff eingerichtete Content Management Software-Richtlinie validiert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär

Informationen	Ebene
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Host auf welches Objekt (URL) versucht zuzugreifen. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

FTP-Filtereraktion

Die FTP-Filteraktion erfolgt, wenn Ereignisinformationen über den Zugriff auf FTP-Protokoll/FTP-Downloads zwischen zwei Netzwerkelementen, die von einem bestimmten Host aufgezeichnet wurden, gesendet werden. Diese Ereignisse können erzeugt werden, wenn über das FTP-Protokoll auf eine URL zugegriffen wird, und diese gegen die für den FTP-Zugriff eingerichtete Content Management Software-Richtlinie validiert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Host auf welches Objekt (URL) versucht zuzugreifen. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Ergebnis	event_result	event_severity
Fehler	F	3

Inhaltsprüfungsaktion

Die Inhaltsprüfungsaktion erfolgt, wenn Ereignisinformationen zum Scannen von HTTP-Datenverkehr gesendet werden.

Informationen	Ebene
Quelle – Benutzerinformationen	tertiär
Quelle – Host-Informationen	primär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	sekundär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehlschlag	F	3

Kapitel 5: Datenzugriffskategorie

Dieses Kapitel enthält folgende Themen:

Anwendungsverwaltungsklasse

Bindungsoperation – Aktion

Bei der Bindungsoperation werden Informationen zum Binden oder Erstellen von Verknüpfungen zwischen Datenbankobjekten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Kontexterstellungsaktion

Die Kontexterstellungsaktion erfolgt, wenn Kontext erstellt wird.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär

Informationen	Ebene
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welches Konto welchen Kontext auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Kontextlöschungsaktion

Die Kontextlöschungsaktion erfolgt, wenn Kontext gelöscht wird.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär

Informationen	Ebene
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welches Konto welchen Kontext auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Failure (Fehler)	F	3

Funktionserstellung

Die Funktionserstellung erfolgt, wenn eine Funktion von einem Quell-Host von einem Anwender der Datenbank erstellt wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und welchem Betriebssystembenutzer auf welchem Host und in welcher Datenbank die Funktion zu welcher Zeit erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Funktionslöschung

Die Funktionslöschung erfolgt, wenn eine Funktion von einem Quell-Host von einem Anwender der Datenbank gelöscht wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und welchem Betriebssystembenutzer auf welchem Host und in welcher Datenbank die Funktion zu welcher Zeit gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Funktionsänderung

Die Funktionsänderung erfolgt, wenn eine Funktion von einem Quell-Host von einem Anwender der Datenbank geändert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär

Informationen	Ebene
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und welchem Betriebssystembenutzer auf welchem Host und in welcher Datenbank die Funktion zu welcher Zeit geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Indexanalyse

Die Indexanalyse erfolgt beim Initialisieren der Analyse eines Indexes auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär

Informationen	Ebene
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto eine Analyse des Indexes/der Indizes auf welchem Host initiiert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Index leeren

Beim Leeren des Indexes wird ein Index aus dem Papierkorb entfernt und der gesamte Speicherplatz, der dem Index zugeordnet ist, freigegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär

Informationen	Ebene
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Index auf welchem Host geleert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Aktion "Bibliothekerstellung"

Die Bibliothekerstellung erfolgt beim Erstellen einer Bibliothek auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär

Informationen	Ebene
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Bibliothek auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Operatorerstellung

Die Operatorerstellung erfolgt beim Erstellen eines Operators und Definieren von dessen Bindungen auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär

Informationen	Ebene
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Operator auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Löschen des Operators

Das Löschen des Operators erfolgt beim Löschen eines Operators auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär

Informationen	Ebene
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Operator auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Änderung des Operators

Das Ändern des Operators erfolgt beim Ändern eines Operators auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär

Informationen	Ebene
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Operator auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Erstellung des Paketkörpers

Das Erstellen des Paketkörpers erfolgt beim Erstellen eines Paketkörpers auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Paketkörper auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Löschung des Paketkörpers

Das Löschen des Paketkörpers erfolgt beim Löschen eines Paketkörpers auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Paketkörper auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Änderung des Paketkörpers

Das Ändern des Paketkörpers erfolgt beim Ändern eines Paketkörpers auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Paketkörper auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Paketerstellung

Die Paketerstellung erfolgt beim Erstellen eines Pakets auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welches Paket auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Paketlöschung

Die Paketlöschung erfolgt beim Löschen eines Pakets auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welches Paket auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Paketänderung

Die Paketänderung erfolgt beim Ändern eines Pakets auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welches Paket auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Prozedurerstellung

Die Prozedurerstellung erfolgt beim Erstellen einer Prozedur auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto eine Prozedur auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Prozedurlöschung

Die Prozedurlöschung erfolgt beim Löschen einer Prozedur auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto eine Prozedur auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Prozeduränderung

Die Prozeduränderung erfolgt beim Ändern einer Prozedur auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto eine Prozedur auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Tabellenanalyse

Die Tabellenanalyse erfolgt beim Initiieren einer Analyse einer Tabelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto die Analyse in welcher Tabelle auf welchem Host initiiert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Tabellenkürzung

Die Tabellenkürzung erfolgt beim Kürzen einer Tabelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Tabelle auf welchem Host gekürzt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Trigger-Erstellung

Die Trigger-Erstellung erfolgt beim Erstellen eines Triggers auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Trigger auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Trigger-Löschung

Die Trigger-Löschung erfolgt beim Löschen eines Triggers auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Trigger auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Trigger-Deaktivierung

Die Trigger-Deaktivierung erfolgt beim Deaktivieren eines Triggers auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Trigger auf welchem Host deaktiviert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Trigger-Aktivierung

Die Trigger-Aktivierung erfolgt beim Aktivieren eines Triggers auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Trigger auf welchem Host aktiviert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Trigger-Änderung

Die Trigger-Änderung erfolgt beim Ändern eines Triggers auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Trigger auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Erstellung des Typkörpers

Die Erstellung des Typkörpers erfolgt beim Erstellen eines Typkörpers durch einen Quell-Hostanwender der Datenbank.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und von welchem Betriebssystembenutzer auf welchem Host und in welcher Datenbank der Typkörper erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Löschung des Typkörpers

Die Löschung des Typkörpers erfolgt beim Löschen eines Typkörpers durch einen Quell-Hostanwender der Datenbank.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und von welchem Betriebssystembenutzer auf welchem Host und in welcher Datenbank der Typkörper gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Änderung des Typkörpers

Die Änderung des Typkörpers erfolgt beim Ändern eines Typkörpers durch einen Quell-Hostanwender der Datenbank.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und von welchem Betriebssystembenutzer auf welchem Host und in welcher Datenbank der Typkörper geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Typerstellung

Die Typerstellung erfolgt beim Erstellen eines Typs durch einen Quell-Hostanwender der Datenbank.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und von welchem Betriebssystembenutzer auf welchem Host und in welcher Datenbank der Typ erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Typlöschung

Die Typlöschung erfolgt beim Löschen eines Typs durch einen Quell-Hostanwender der Datenbank.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und von welchem Betriebssystembenutzer auf welchem Host und in welcher Datenbank der Typ gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Typausführung

Die Typausführung erfolgt beim Ausführen eines Typs durch einen Quell-Hostanwender der Datenbank.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und von welchem OS-Benutzer auf welchem Host und in welcher Datenbank der Typ ausgeführt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Typänderung

Die Typänderung erfolgt beim Ändern eines Typs durch einen Quell-Hostanwender der Datenbank.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und von welchem Betriebssystembenutzer auf welchem Host und in welcher Datenbank der Typ geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Operation zur Aufhebung von Bindungen – Aktion

Bei der Operation zur Aufhebung von Bindungen werden Informationen zum Aufheben von Bindungen oder Entfernen von Verknüpfungen zwischen Datenbankobjekten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Auditereignisklasse

Auditstandardaktion

Die Auditstandardaktion erfolgt, wenn die Auditierungsoption so eingestellt wird, dass Operationen auf einer kompletten Datenbank auf einem bestimmten Host verfolgt werden.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	primär
Quelle – Prozessinformationen	sekundär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	tertiär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welcher Benutzer den Auditstandard auf welchen Host und welcher Datenbank festgelegt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Kein Audit-Standard

Die Aktion "Kein Audit-Standard" verhindert, dass weitere Objekte standardmäßig geprüft werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer "Kein Audit-Standard" auf welchem Host und in welcher Datenbank eingestellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Objekt-Audit

Das Objekt-Audit erfolgt beim Einstellen der Audit-Option, um Operationen eines speziellen Schemaobjekts auf einem bestimmten Host zu verfolgen.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer "Objekt-Audit" auf welchem Host und in welcher Datenbank eingestellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Kein Objekt-Audit

Die Aktion "Kein Objekt-Audit" erfolgt beim Deaktivieren der Überwachung, die zuvor für ein spezielles Schemaobjekt auf einem bestimmten Host aktiviert wurde.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer "Kein Objekt-Audit" auf welchem Host und in welcher Datenbank eingestellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Sitzungsaufzeichnung

Die Sitzungsaufzeichnung erfolgt beim Aufzeichnen einer Sitzung von einem beliebigen Benutzer der Datenbank in der Überwachungsliste auf einem Quellhost.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Benutzeraktivität zur Überwachungsliste auf welchem Host und in welche Datenbank hinzugefügt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

System-Audit

Das System-Audit erfolgt beim Einstellen der Audit-Option von einem Quellhost durch einen beliebigen Benutzer der Datenbank.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und von welchem Betriebssystembenutzer auf welchem Host und in welcher Datenbank die Audit-Option eingestellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Kein System-Audit

Das Kein System-Audit erfolgt beim Deaktivieren des System-Auditing von einem Quellhost durch einen beliebigen Benutzer der Datenbank.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und von welchem Betriebssystembenutzer auf welchem Host und in welcher Datenbank die System-Audit-Option deaktiviert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenzugriffsklasse

Massenkopieren – Aktion

Beim Massenkopieren werden Informationen zum Übertragen von Daten in Blöcken statt in Form von einzelnen Datensätzen zwischen verschiedenen Datenspeichern ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Commit-Aktion

Die Commit-Aktion erfolgt, wenn bei Beendigung einer Transaktion alle während der Transaktion durchgeführten Änderungen dauerhaft übernommen werden.

Informationen	Ebene
Quelle – Benutzerinformationen	tertiär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	primär
Quelle – Prozessinformationen	sekundär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär

Informationen	Ebene
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welche Transaktion auf welcher Datenbank und welchem Host per "Commit" übergeben wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Löschaktion

Die Löschaktion erfolgt, wenn Daten aus einer Tabelle einer Datenbank eines Terminals (Hosts) von einem beliebigen Benutzer gelöscht werden.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	primär
Quelle – Prozessinformationen	sekundär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär

Informationen	Ebene
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welche Tabelle aus welcher Datenbank auf welchem Host von welchem Benutzer zu welcher Zeit gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Failure (Fehler)	F	3

Einfügen der Aktion

Das Einfügen der Aktion erfolgt beim Initiieren einer INSERT-Anweisung in einer Tabelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto eine INSERT-Anweisung in einer Tabelle auf welchem Host initiiert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Abfrageausführung – Aktion

Bei der Abfrageausführung werden Informationen zu Datenbankabfragen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Abfrage in welcher Datenbank auf welchem Host festgelegt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Rollback

Die Rollback-Aktion erfolgt beim Initiieren eines Rollbacks, um eine Aufgabe, die in der aktuellen Transaktion ausgeführt wurde, rückgängig zu machen, oder eine Aufgabe, die von einer zweifelhaften verteilten Transaktion ausgeführt wurde, manuell rückgängig zu machen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Transaktion in welcher Datenbank auf welchem Host zurückgesetzt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Sicherungspunkt

Der Sicherungspunkt identifiziert einen Punkt in einer Transaktion, auf den zu einem späteren Zeitpunkt zurückgesetzt werden kann.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär

Informationen	Ebene
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Sicherungspunkt in welcher Datenbank auf welchem Host identifiziert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Auswahl

Die Auswahl erfolgt beim Initiieren einer SELECT-Anweisung in einer Tabelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto eine SELECT-Anweisung in einer Tabelle auf welchem Host initiiert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Festlegung der Transaktion

Die Festlegung der Transaktion richtet die aktuelle Transaktion als Transaktion mit Leseberechtigung oder Lese-/Schreibberechtigung ein, richtet eine Isolationsebene ein oder weist die Transaktion einem speziellen Rollback-Segment zu.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär

Informationen	Ebene
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Transaktion in welcher Datenbank auf welchem Host eingestellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verkürzen – Aktion

Beim Verkürzen werden Informationen zur Verkürzung von Daten in Tabellen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär

Informationen	Ebene
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktualisierung

Die Aktualisierung erfolgt beim Initiieren einer UPDATE-Anweisung in einer Tabelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär

Informationen	Ebene
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto eine UPDATE-Anweisung in einer Tabelle auf welchem Host initiiert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse der Objektverwaltung

Assembly-Erstellung

Die Assembly-Erstellung behandelt die Ablage eines Assembly. Verwaltete Datenbankobjekte, wie z. B. gespeicherte Prozeduren oder Trigger, werden kompiliert und dann in Einheiten, den so genannten Assemblies, angewandt. Der verwendete Befehl lautet CREATE ASSEMBLY.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Assembly-Ablage

Die Assembly-Ablage behandelt die Ablage eines Assembly. Verwaltete Datenbankobjekte, wie z. B. gespeicherte Prozeduren oder Trigger, werden kompiliert und dann in Einheiten, den so genannten Assemblies, angewandt. Der verwendete Befehl lautet DROP ASSEMBLY.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Assembly-Änderung

Die Assembly-Änderung behandelt die Ablage eines Assembly. Verwaltete Datenbankobjekte, wie z. B. gespeicherte Prozeduren oder Trigger, werden kompiliert und dann in Einheiten, den so genannten Assemblies, angewandt. Der verwendete Befehl lautet MODIFY ASSEMBLY.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Steuerungsdateierstellungs-Aktion

Die Steuerungsdateierstellungs-Aktion erfolgt, wenn auf einem bestimmten Host eine Steuerungsdatei erstellt wird.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	primär
Quelle – Prozessinformationen	sekundär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	tertiär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welcher Benutzer die Steuerungsdatei auf welchen Host und welcher Datenbank erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	6

Dimensionserstellungsaktion

Die Dimensionserstellungsaktion stellt mittels Über- und Unterordnung eine Beziehung zwischen Spaltensetpaaren her.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welches Konto welche Dimension auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Dimensionslöschungsaktion

Die Dimensionslöschungsaktion befasst sich mit der Löschung einer Dimension auf einem bestimmten Host.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welches Konto welche Dimension auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Dimensionsänderungsaktion

Die Dimensionsänderungsaktion erfolgt, wenn eine Dimension auf einem bestimmten Host geändert wird.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, welches Konto welche Dimension auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Verzeichniserstellungsaktion

Die Verzeichniserstellungsaktion erfolgt, wenn durch einen beliebigen Datenbankbenutzer zu einer bestimmten Zeit ein Verzeichnis erstellt wird, das Datenbankobjekte aus einem Terminal (Host) enthält.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	primär
Quelle – Prozessinformationen	sekundär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, von welchem Benutzer bzw. Betriebssystembenutzer der Verzeichnisname mit Pfad auf welchem Host und welcher Datenbank zu welcher Zeit erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Verzeichnislöschungsaktion

Die Verzeichnislöschungsaktion erfolgt, wenn ein Verzeichnisobjekt durch einen beliebigen Benutzer der Datenbank vom Quellhost gelöscht wird.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	sekundär
Quelle – Prozessinformationen	sekundär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	primär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, von welchem Benutzer bzw. Betriebssystembenutzer der Verzeichnisname auf welchem Host und welcher Datenbank zu welcher Zeit gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Failure (Fehler)	F	3

Editionserstellung

Die Editionserstellung behandelt die Erstellung von Editionen. In Oracle, wird Edition Object verwendet, um mehrere Versionen von Trigger, Ansichten, Synonymen usw. in der Datenbank zu speichern. Der in Oracle verwendete Befehl lautet CREATE EDITION.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Editionsunterbrechung

Die Editionsunterbrechung behandelt die Erstellung von Editionen. In Oracle, wird Edition Object verwendet, um mehrere Versionen von Trigger, Ansichten, Synonymen usw. in der Datenbank zu speichern. Der in Oracle verwendete Befehl lautet ALTER EDITION.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Editionsänderung

Die Editionsänderung behandelt die Erstellung von Editionen. In Oracle, wird Edition Object verwendet, um mehrere Versionen von Trigger, Ansichten, Synonymen usw. in der Datenbank zu speichern. Der in Oracle verwendete Befehl lautet ALTER EDITION.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Kompletten Index aktualisieren

Die Aktion "Kompletten Index aktualisieren" aktualisiert den kompletten Index, der einer Tabelle oder Ansicht auf einem bestimmten Host zugeordnet ist.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Index in welcher Datenbank auf welchem Host aktualisiert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Indexerstellung

Die Indexerstellung erfolgt beim Erstellen eines Indexes auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto ein Index auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Indexlöschung

Die Indexlöschung erfolgt beim Löschen eines Indexes auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto ein Index auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Indexänderung

Die Indexänderung erfolgt beim Ändern eines Indexes auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto ein Index auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Indexvalidierung

Die Indexvalidierung erfolgt beim Validieren eines Indexes auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto eine Validierung des Indexes/der Indizes auf welchem Host initiiert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Erstellung des Indextyps

Die Erstellung des Indextyps erfolgt beim Erstellen eines Indextyps auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Indextyp auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Löschen des Indextyps

Das Löschen des Indextyps erfolgt beim Löschen eines Indextyps auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Indextyp auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Java-Erstellung

Die Java-Erstellung erfolgt beim Erstellen eines Schemaobjekts, das eine Java-Quelle, -Klasse oder -Ressource enthält.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welches Schemaobjekt auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Java-Löschung

Die Java-Löschung erfolgt beim Löschen eines Schemaobjekts, das eine Java-Quelle, -Klasse oder -Ressource enthält.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welches Schemaobjekt auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Java-Änderung

Die Java-Änderung erfolgt beim Ändern eines Schemaobjekts, das eine Java-Quelle, -Klasse oder -Ressource enthält.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welches Schemaobjekt auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Sperren

Das Sperren erfolgt beim Initiieren einer LOCK-Anweisung für ein Objekt auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto eine LOCK-Anweisung für welches Objekt auf welchem Host initiiert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Erstellung der materialisierten Ansicht

Die Erstellung der materialisierten Ansicht erfolgt beim Erstellen einer materialisierten Ansicht auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche materialisierte Ansicht auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Löschen der materialisierten Ansicht

Das Löschen der materialisierten Ansicht erfolgt beim Löschen einer materialisierten Ansicht auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche materialisierte Ansicht auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Änderung der materialisierten Ansicht

Die Änderung der materialisierten Ansicht erfolgt beim Ändern einer materialisierten Ansicht auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto die materialisierte Ansicht auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Erstellung eines Protokolls für die materialisierte Ansicht

Die Erstellung eines Protokolls für die materialisierte Ansicht erfolgt beim Erstellen eines Protokolls für die materialisierte Ansicht auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welches Protokoll für die materialisierte Ansicht auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Löschen des Protokolls für die materialisierte Ansicht

Das Löschen eines Protokolls für die materialisierte Ansicht erfolgt beim Löschen eines Protokolls für die materialisierte Ansicht auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welches Protokoll für die materialisierte Ansicht auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Änderung eines Protokolls für die materialisierte Ansicht

Die Änderung eines Protokolls für die materialisierte Ansicht erfolgt beim Ändern eines Protokolls für die materialisierte Ansicht auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welches Protokoll für die materialisierte Ansicht auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Kein Vorgang

Die Aktion "Kein Vorgang" erfolgt, wenn Klauseln und Verfahren ausgeführt werden, die keine Auswirkungen haben, aber hierfür keine Fehler ausgegeben werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Klausel oder welches Verfahren auf welchem Host ausgeführt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Wiederherstellung eines gelöschten Objekts

Die Wiederherstellung eines gelöschten Objekts erfolgt beim Widerherstellen eines gelöschten Objekts, das auf einem bestimmten Host zum Löschen gekennzeichnet wurde.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welches gelöschte Objekt auf welchem Host wiederhergestellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Umrisserstellung

Die Umrisserstellung erfolgt, wenn ein Umriss von einem Quell-Hostanwender der Datenbank erstellt wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer welchen Umriss auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Umrisslöschung

Die Umrisslöschung erfolgt, wenn ein Umriss von einem Quell-Hostanwender der Datenbank gelöscht wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer welchen Umriss auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Umrissänderung

Die Umrissänderung erfolgt, wenn ein Umriss von einem Quell-Hostanwender der Datenbank geändert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer welchen Umriss auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Erstellung eines öffentlichen Synonyms

Die Erstellung eines öffentlichen Synonyms erfolgt beim Erstellen eines öffentlichen Synonyms auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto ein öffentliches Synonym auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Löschung eines öffentlichen Synonyms

Die Löschung eines öffentlichen Synonyms erfolgt beim Löschen eines öffentlichen Synonyms auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto ein öffentliches Synonym auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	3
Fehler	F	3

Umbenennung

Die Umbenennung erfolgt beim Umbenennen eines Objekts auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welches Objekt auf welchem Host umbenannt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

"source_objectname" ist der ursprüngliche Name des Objekts und "dest_objectname" ist der neue Name des Objekts.

Ergebnis	event_result	event_severity
Erfolgreich	E	3

Ergebnis	event_result	event_severity
Fehler	F	3

Ändern der Ressourcenkosten

Das Ändern der Ressourcenkosten erfolgt beim Definieren der Ressourcenkosten für die Profilerstellung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto Ressourcenkosten auf welchem Host geändert wurden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	3
Fehler	F	3

Regelerstellung – Aktion

Bei der Regelerstellung werden Informationen zur Erstellung von Regeln ausgegeben, die auf Datenbankobjekte angewendet werden können.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene	
Ergebnis - Informationen	Primär	
Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Regeländerung – Aktion

Bei der Regeländerung werden Informationen zur Änderung von Regeln ausgegeben, die auf Datenbankobjekte angewendet werden können.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Regellöschung – Aktion

Bei der Regellöschung werden Informationen zur Löschung von Regeln ausgegeben, die auf Datenbankobjekte angewendet werden können.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Schemaerstellung

Die Schemaerstellung erfolgt beim Erstellen mehrerer Tabellen und Ansichten sowie beim Erteilen mehrerer Berechtigungen in einer einzigen Transaktion auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welches Schema auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Sequenzerstellung

Die Sequenzerstellung erfolgt beim Erstellen einer Sequenz auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto eine Sequenz auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Sequenzlöschung

Die Sequenzlöschung erfolgt beim Löschen einer Sequenz auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto eine Sequenz auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	3
Fehler	F	3

Sequenzänderung

Die Sequenzänderung erfolgt beim Ändern einer Sequenz auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto eine Sequenz auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	3
Fehler	F	3

Statistikzuordnung

Bei der Statistikzuordnung wird ein Statistiktyp, der relevante Funktionen für die Erfassung von Statistiken, die Selektivität oder die Kosten enthält, einer oder mehreren Spalten, eigenständigen Funktionen, Paketen, Typen, Domänenindizes oder Indextypen zugewiesen.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Statistiktyp auf welchem Host zugewiesen wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Statistikzuordnung aufheben

Beim Aufheben der Statistikzuordnung wird die Zuordnung eines Statistiktyps zu einer oder mehreren Spalten, eigenständigen Funktionen, Paketen, Typen, Domänenindizes oder Indextypen aufgehoben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto die Zuweisung welches Statistiktyps auf welchem Host aufgehoben wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Übersichtsänderung

Die Übersichtsänderung erfolgt beim Ändern einer Übersicht auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto auf welchem Host eine Übersicht geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Synonymerstellung

Die Synonymerstellung erfolgt beim Erstellen eines Synonyms auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto auf welchem Host ein Synonym erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Synonymlöschung

Die Synonymlöschung erfolgt beim Löschen eines Synonyms auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto auf welchem Host ein Synonym gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Tabellenüberprüfung – Aktion

Bei der Tabellenüberprüfung werden Informationen zur Fehlerüberprüfung einer oder mehrerer Tabellen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Tabellenerstellung

Die Tabellenerstellung erfolgt beim Erstellen einer Tabelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Tabelle auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Tabellenlöschung

Die Tabellenlöschung erfolgt beim Löschen einer Tabelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Tabelle auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Tabellenleerung – Aktion

Bei der Tabellenleerung werden Informationen zum Entfernen aller Abfrageergebnisse aus dem Abfragen-Cache ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Tabellenänderung

Die Tabellenänderung erfolgt beim Ändern einer Tabelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Tabelle auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Tabellenoptimierung – Aktion

Bei der Tabellenoptimierung werden Informationen zum Entfernen aller Abfrageergebnisse aus dem Abfragen-Cache ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Entfernung einer Tabelle

Bei der Entfernung einer Tabelle wird diese aus dem Papierkorb entfernt und sämtlicher ihr zugewiesene Speicher freigegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Tabelle auf welchem Host entfernt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Tabellenumbenennung

Die Tabellenumbenennung erfolgt beim Umbenennen einer Tabelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Tabelle auf welchem Host umbenannt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

"source_objectname" ist der ursprüngliche Name der Tabelle und "dest_objectname" ist der neue Name der Tabelle.

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Ergebnis	event_result	event_severity
Fehler	F	3

Tabellenreparatur – Aktion

Die Tabellenreparatur erfolgt, wenn eine Tabelle auf einem bestimmten Host repariert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Tabelle auf welchem Host repariert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Ergebnis	event_result	event_severity
Fehler	F	3

Tabellenentsperrung – Aktion

Bei der Tabellenentsperrung werden Informationen zum Entsperren eines zuvor gesperrten, in einer Transaktion verwendeten Objekts ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ansichterstellung

Die Ansichterstellung erfolgt beim Erstellen einer Ansicht auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Ansicht auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ansichtänderung

Die Ansichtänderung erfolgt beim Ändern einer Ansicht auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Ansicht auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ansichtlöschung

Die Ansichtlöschung erfolgt beim Löschen einer Ansicht auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Ansicht auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Peer-Verwaltungsklasse

Erstellung der Datenbankverbindung

Die Erstellung der Datenbankverbindung erfolgt beim Erstellen einer Datenbankverbindung zwischen zwei Datenbanken.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto eine Verbindung von welcher Datenbank zu welcher anderen Datenbank auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Löschung der Datenbankverbindung

Die Löschung der Datenbankverbindung erfolgt beim Löschen einer Datenbankverbindung zwischen zwei Datenbanken.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto eine Verbindung von welcher Datenbank zu welcher anderen Datenbank auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Berechtigungsverwaltungsklasse

Löschen der Bibliothek

Das Löschen der Bibliothek erfolgt beim Löschen einer Bibliothek auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Bibliothek auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Objektverweigerung

Die Objektverweigerung erfolgt beim Verweigern des Zugriffs auf ein Objekt auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Erteilung von Objektberechtigungen

Die Erteilung von Objektberechtigungen erfolgt beim Erteilen von Berechtigungen für ein Objekt auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Kontenberechtigungen für welches Objekt auf welchem Host gewährt wurden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Widerrufen eines Objekts

Das Widerrufen eines Objekts erfolgt beim Widerrufen von Rechten für ein Objekt auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Kontenberechtigungen für welches Objekt auf welchem Host widerrufen wurden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Profilerstellung

Die Profilerstellung erfolgt beim Erstellen eines Profils auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto ein Profil auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Profillöschung

Die Profillöschung erfolgt beim Löschen eines Profils auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto ein Profil auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	4
Fehler	F	3

Profiländerung

Die Profiländerung erfolgt beim Ändern eines Profils auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto ein Profil auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	4
Fehler	F	3

Widerrufen einer Rolle

Das Widerrufen einer Rolle erfolgt beim Widerrufen einer Rolle.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Anweisungsverweigerung

Bei der Anweisungsverweigerung geht es um die Verweigerung einer Anweisung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Anweisungserteilung

Bei der Anweisungserteilung wird eine Anweisung erteilt.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Widerrufen einer Anweisung

Beim Widerrufen einer Anweisung geht es um die Zurücknahme einer Anweisung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse für Service- und Anwendungsauslastung

Methodenausführung

Die Methodenausführung erfolgt beim Ausführen einer speziellen Methode auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Methode auf welchem Host ausgeführt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Prozedurausführung

Die Prozedurausführung erfolgt, wenn eine bestimmte Prozedur auf einem bestimmten System oder in einer bestimmten Anwendung ausgeführt wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Prozedur auf welchem Host ausgeführt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Trigger-Ausführung – Aktion

Bei der Trigger-Ausführung werden Informationen zur Ausführung eines für eine Tabelle oder Spalte definierten Triggers ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse für Systemaktivität

Datenbankalarm – Aktion

Die Aktion "Datenbankalarm" erfolgt, wenn Datenbank- oder DBMS-Alarme gesendet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene	
Ergebnis - Informationen	Primär	
Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	6

Datenbankbenachrichtigung – Aktion

Die Datenbankbenachrichtigung erfolgt, wenn Datenbank- oder DBMS-Benachrichtigungen gesendet werden.

Informationen	Ebene	
Quelle - Benutzerinformationen	Sekundär	
Quelle – Host-Informationen	Tertiär	
Quelle - Objektinformationen	Tertiär	
Quelle - Prozessinformationen	Tertiär	
Quelle - Gruppeninformationen	Tertiär	
Ziel - Benutzerinformationen	Tertiär	
Ziel - Host-Informationen	Primär	
Ziel - Objektinformationen	Primär	
Ziel - Gruppeninformationen	Tertiär	
Agent - Informationen	Primär	
Agent - Host-Informationen	Primär	
Ereignisquelle – Host-Informationen	Primär	
Ereignisquelle - Informationen	Tertiär	
Ereignis - Informationen	Primär	
Ergebnis - Informationen	Primär	
Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2

Informationen	Ebene	
Fehler	F	3

Datenbankoperation – Aktion

Bei der Datenbankoperation werden Informationen zu allgemeinen Datenbankoperationen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbankstatus – Aktion

Beim Datenbankstatus werden Informationen zum allgemeinen Status von Datenbanken ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbankwarnung – Aktion

Die Datenbankwarnung erfolgt, wenn Datenbankwarnungen gesendet werden. Diese Aktion ist weniger streng als die Datenbankfehleraktion.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Warnung auf welchem Host ausgelöst wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Systemverwaltungsklasse

Cluster-Analyse

Die Cluster-Analyse erfolgt beim Analysieren eines Clusters.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welchen Cluster auf welchem Host analysiert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbanksicherung

Die Datenbanksicherung erfolgt bei der Sicherung einer Datenbank auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Datenbank auf welchem Host gesichert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbanksicherungsalarm – Aktion

Beim Datenbanksicherungsalarm geht es um Informationen zu Alarmbedingungen, die während einer Datenbanksicherung auftreten.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Datenbanksicherungsfehler – Aktion

Bei der Aktion "Datenbanksicherungsfehler" geht es um Informationen über Fehlerbedingungen, die während einer Datenbanksicherung auftreten.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Datenbank-Sicherungsbenachrichtigung – Aktion

Bei der Datenbank-Sicherungsbenachrichtigung geht es um Informationen über Benachrichtigungen und Meldungen, die von der Datenbanksicherung erzeugt werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbanksicherungsstatus – Aktion

Bei der Aktion "Datenbanksicherungsstatus" geht es um Informationen über den Status einer Datenbanksicherung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbanksicherungswarnung – Aktion

Bei der Datenbanksicherungswarnung geht es um Warnungen, die während einer Datenbanksicherung generiert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Datenbankprüfung – Aktion

Bei der Datenbankprüfung werden Informationen zur Prüfung einer Datenbank ausgegeben, die stattfindet, um die logische und physische Integrität aller Objekte sicherzustellen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Cluster-Erstellung

Die Cluster-Erstellung erfolgt beim Erstellen eines Clusters.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welchen Cluster auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Cluster-Löschung

Die Cluster-Löschung erfolgt beim Löschen eines Clusters.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welchen Cluster auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbankdeaktivierung – Aktion

Bei der Datenbankdeaktivierung werden Informationen zum Deaktivieren einer Datenbank ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbankaktivierung – Aktion

Bei der Datenbankaktivierung werden Informationen zum Aktivieren einer Datenbank ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Cluster-Änderung

Die Cluster-Änderung erfolgt beim Ändern eines Clusters.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welchen Cluster auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbankspiegelungs-Start – Aktion

Beim Datenbankspiegelungs-Start werden Informationen zum Starten einer Datenbankspiegelung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbankspiegelungs-Beendigung – Aktion

Bei der Datenbankspiegelungs-Beendigung werden Informationen zur Beendigung einer Datenbankspiegelung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbankbereitstellung – Aktion

Bei der Datenbankbereitstellung werden Informationen zum Bereitstellen einer Datenbank aus einem Set von Gerätedateien ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbankerstellung

Die Datenbankerstellung erfolgt bei der Erstellung einer Datenbank auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto eine Datenbank auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbanklöschung

Die Datenbanklöschung erfolgt beim Löschen einer Datenbank auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto eine Datenbank auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Datenbank-Flashback

Datenbank-Flashback erfolgt beim Wiederherstellen einer Datenbank auf deren früheren Status.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto eine Datenbank auf welchem Host wiederhergestellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Datenbankänderung

Die Datenbankänderung erfolgt beim Ändern einer Datenbank auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto eine Datenbank auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Datenbankabgleich – Aktion

Bei der Aktion "Datenbankabgleich" werden Informationen zum Abgleich von Daten in Datenbanken mit Daten aus externen Komponenten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbankfreigabe – Aktion

Bei der Datenbankfreigabe werden Informationen zum Freigeben einer Datenbank im Anschluss an eine Unterbrechung der darin stattfindenden Operationen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbankwiederherstellung

Die Datenbankwiederherstellung erfolgt beim Wiederherstellen einer Datenbank auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto eine Datenbank auf welchem Host wiederhergestellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Neues Thema (19)

Der Datenbank-Snapshot erfolgt beim Erstellen eines Snapshots auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto auf welchem Host ein Snapshot erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbankunterbrechung – Aktion

Bei der Datenbankunterbrechung werden Informationen zu unterbrochenen Operationen in einer Datenbank ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Datenbankreplikation – Aktion

Bei der Datenbankreplikation werden Informationen zur Replikation von Datenbanken ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Cluster-Kürzung

Die Cluster-Kürzung erfolgt beim Kürzen eines Clusters.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welchen Cluster auf welchem Host gekürzt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aufhebung der Datenbankbereitstellung – Aktion

Bei der Aufhebung der Datenbankbereitstellung werden Informationen zum Aufheben einer Datenbankbereitstellung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Erklärung

Die Aktion "Erklärung" erfolgt beim Beschreiben der Schritte eines Ausführungsplans.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto die Aktion "Erklärung" für welches Objekt auf welchem Host ausgeführt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Flashback-Aktion

Die Flashback-Aktion erfolgt beim Wiederherstellen eines Objekts auf dessen früheren Status.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welches Objekt auf welchem Host wiederhergestellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Flashback-Archiv-Erstellung

Bei der Flashback-Archiv-Erstellung geht es um das Erstellen von Flashback-Archiven. Ein Flashback-Datenarchiv bietet die Möglichkeit, sämtliche Transaktionsänderungen an einer Tabelle über ihre Lebensdauer nachzuverfolgen und zu speichern. Der verwendete Befehl lautet CREATE FLASHBACK ARCHIVE.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Flashback-Archiv-Bereinigung

Die Flashback-Archiv-Bereinigung betrifft das Erstellen von Flashback-Archiven. Ein Flashback-Datenarchiv bietet die Möglichkeit, sämtliche Transaktionsänderungen an einer Tabelle über ihre Lebensdauer nachzuverfolgen und zu speichern. Der verwendete Befehl lautet DROP FLASHBACK ARCHIVE.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Flashback-Archiv-Änderung

Bei der Flashback-Archiv-Änderung geht es um das Ändern von Flashback-Archiven. Ein Flashback-Datenarchiv bietet die Möglichkeit, sämtliche Transaktionsänderungen an einer Tabelle über ihre Lebensdauer nachzuverfolgen und zu speichern. Der verwendete Befehl lautet MODIFY FLASHBACK ARCHIVE.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Leeren des Papierkorbs

Die Leeren des Papierkorbs erfolgt beim Löschen von Daten aus dem Papierkorb auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto der Papierkorb auf welchem Host geleert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Erstellen eines Rollback-Segments

Das Erstellen eines Rollback-Segments erfolgt beim Erstellen eines Rollback-Segments auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welches Rollback-Segment auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Löschen eines Rollback-Segments

Das Löschen eines Rollback-Segments erfolgt beim Löschen eines Rollback-Segments auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welches Rollback-Segment auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Ändern eines Rollback-Segments

Das Ändern eines Rollback-Segments erfolgt beim Ändern eines Rollback-Segments auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welches Rollback-Segment auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Erteilung von Systemberechtigungen

Die Erteilung von Systemberechtigungen erfolgt bei Festlegung einer Option für Systemberechtigungen von einem Quellhost durch einen Benutzer der Datenbank.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und welchem BS-Benutzer auf welchem Host und in welcher Datenbank Systemberechtigungen erteilt wurden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Systemänderung

Die Systemänderung erfolgt bei Festlegung einer ALTER SYSTEM-Anweisung von einem Quellhost durch einen Benutzer der Datenbank.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und welchem BS-Benutzer auf welchem Host und in welcher Datenbank Systemänderungen durchgeführt wurden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Systemsperrung

Eine Systemsperrung erfolgt, wenn Systemberechtigungen wie "DBA", "Sitzung erstellen" usw. von einem Quellhostbenutzer der Datenbank widerrufen werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Benutzer und welchem BS-Benutzer auf welchem Host und in welcher Datenbank Systemberechtigungen widerrufen wurden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Systemtabellenaktualisierung – Aktion

Bei der Systemtabellenaktualisierung werden Informationen zur Aktualisierung von Systemtabellen ausgegeben, die stattfindet, wenn die Systeminfrastruktur der Datenbank oder Metadaten geändert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Tabellen-Flashback

Ein Tabellen-Flashback erfolgt beim Wiederherstellen einer Tabelle auf einen Status zu einem früheren Zeitpunkt.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Tabelle auf welchem Host wiederhergestellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Tablespace-Erstellung

Die Tablespace-Erstellung erfolgt beim Erstellen eines Tablespace auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto auf welchem Host ein Tablespace erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Tablespace-Löschung

Die Tablespace-Löschung erfolgt beim Löschen eines Tablespace auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto auf welchem Host ein Tablespace gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Tablespace-Änderung

Die Tablespace-Änderung erfolgt beim Ändern eines Tablespace auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto auf welchem Host ein Tablespace geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Entfernung eines Tablespace

Die Entfernung eines Tablespace erfolgt beim Entfernen von Objekten bestimmter Tablespaces aus dem Papierkorb.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Tablespace-Objekte auf welchem Host entfernt wurden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Transaktionsprotokollsicherung – Aktion

Bei der Transaktionsprotokollsicherung werden Informationen zum Sichern eines Datenbank-Transaktionsprotokolls ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Deaktivierung aller Trigger

Die Deaktivierung aller Trigger erfolgt beim Deaktivieren aller Trigger für eine Tabelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto für welche Tabelle alle Trigger auf welchem Host deaktiviert wurden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Aktivierung aller Trigger

Die Aktivierung aller Trigger erfolgt beim Aktivieren aller Trigger für eine Tabelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto für welche Tabelle alle Trigger auf welchem Host aktiviert wurden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Ausführung einer Transact-Anweisung

Die Ausführung einer Transact-Anweisung erfolgt, wenn eine Transact-Anweisung ausgeführt wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Tablespace-Objekte auf welchem Host entfernt wurden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Kapitel 6: Kategorie "Host-Sicherheit"

Dieses Kapitel enthält folgende Themen:

Klasse der Antivirusaktivität

Aktion "Antivirus-Status"

Mit dem Antivirus-Status werden Ereignisinformationen zum Status von Antivirussystemen oder -Software auf einem System beschrieben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Dateiblockierung

Die Dateiblockierung erfolgt beim Erkennen einer Datei, die von einem Antivirus-Produkt auf einem bestimmten Host blockiert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Datei auf welchem Host blockiert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Dateiausschluss

Der Dateiausschluss erfolgt beim Ausschließen einer Datei von einem Scanvorgang auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Datei auf welchem Host von dem Scanvorgang ausgeschlossen wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Löschen einer Datei

Das Löschen einer Datei erfolgt, wenn eine infizierte Datei auf einem bestimmten Host gelöscht wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Dateilöschung

Eine Dateilöschung betrifft das Löschen von Malware oder von Dateien, die Viren enthalten.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Dateiumbenennung

Die Dateiumbenennung erfolgt beim Umbenennen einer infizierten Datei auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Datei auf welchem Host umbenannt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

"source_objectname" ist der ursprüngliche Name des Objekts und "dest_objectname" ist der neue Name des Objekts.

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Scan-Alarm – Aktion

Beim Scan-Alarm werden Informationen zu scanbezogenen Alarmbedingungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	7

Scan-Umgehung – Aktion

Bei der Scan-Umgehung werden Informationen zum Umgehen eines Scans ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Scan-Fehler

Ein Scan-Fehler erfolgt, wenn während einer Antivirenprüfung auf einem bestimmten Host ein Fehler gemeldet wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Antivirus-Produkt der Fehler auf welchem Host gemeldet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	6

Scan-Benachrichtigung – Aktion

Bei der Scan-Benachrichtigung werden Informationen zu Benachrichtigungen und Meldungen ausgegeben, die mittels Scan generiert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Scan-Vorgang – Aktion

Bei der Aktion "Scan-Vorgang" werden allgemeine Informationen zu Scan-Vorgängen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Scan-Bericht

Ein Scan-Bericht erfolgt, wenn Zusammenfassungsinformationen von einem Virenscan auf einem bestimmten Host erkannt werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Bei dieser Aktion ist die Information von Bedeutung, welcher Bericht mit Scan-Zusammenfassungsinformationen eines Antivirus-Produkts auf welchem Host erkannt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2

Scan-Status – Aktion

Bei der Aktion "Scan-Status" werden allgemeine Informationen zum Scan-Status ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Scan-Warnung – Aktion

Jeder Typ von Warnung vor einem Scan kann der Aktion "Scan-Warnung" zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Scan-Fehler" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Virenbereinigung

Die Virenbereinigung betrifft die Durchführung einer Bereinigung bei Identifizierung eines Virus auf einem bestimmten Host. Für diese Aktion gibt es zwei mögliche Ergebnisse: "S" für "Success" (Erfolgreich) und "F" für "Failure" (Fehler).

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	*Primär*
Ziel - Prozessinformationen	*Primär*
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, bei welchem Prozess oder welcher Datei auf welchem Host versucht wurde, den Virus zu bereinigen. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Der Virusname sollte im Feld "result_signature" in der CEG gespeichert sein.

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Ergebnis	event_result	event_severity
Fehler	F	6

Virenerkennung

Die Virenerkennung erfolgt bei Erkennung eines bekannten Virus auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, bei welchem Prozess oder welcher Datei auf welchem Host der Virus erkannt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Der Virusname sollte im Feld "result_signature" in der CEG gespeichert sein.

Ergebnis	event_result	event_severity
Erfolgreich	S	6

Viren-Engine-Aktualisierung

Die Viren-Engine-Aktualisierung erfolgt beim Aktualisieren einer Viren-Engine auf einem bestimmten Host. Für diese Aktion gibt es zwei mögliche Ergebnisse: "S" für "Success" (Erfolgreich) und "F" für "Failure" (Fehler).

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Engine auf welchem Host aktualisiert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	5

Viren-Engine-Alarm – Aktion

Beim Viren-Engine-Alarm werden Informationen zu Alarmbedingungen im Zusammenhang mit der Viren-Engine ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene	
Ergebnis - Informationen	Primär	
Ergebnis	**event_result**	**event_severity**
Fehler	F	6

Viren-Engine-Fehler – Aktion

Bei der Aktion "Viren-Engine-Fehler" werden Informationen zu Fehlerbedingungen im Zusammenhang mit der Viren-Engine ausgegeben.

Informationen	Ebene	
Quelle - Benutzerinformationen	Tertiär	
Quelle – Host-Informationen	Tertiär	
Quelle - Objektinformationen	Tertiär	
Quelle - Prozessinformationen	Tertiär	
Quelle - Gruppeninformationen	Tertiär	
Ziel - Benutzerinformationen	Tertiär	
Ziel - Host-Informationen	Primär	
Ziel - Objektinformationen	Primär	
Ziel - Gruppeninformationen	Tertiär	
Agent - Informationen	Primär	
Agent - Host-Informationen	Primär	
Ereignisquelle – Host-Informationen	Primär	
Ereignisquelle - Informationen	Tertiär	
Ereignis - Informationen	Primär	
Ergebnis - Informationen	Primär	
Ergebnis	**event_result**	**event_severity**
Fehler	F	5

Viren-Engine-Benachrichtigung – Aktion

Bei der Aktion "Virus-Engine-Fehler" wird jeder Typ von Benachrichtigung angezeigt, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "Viren-Engine-Status", wenn das Ereignis den Status der Viren-Engine beschreibt.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Viren-Engine-Operation – Aktion

Bei der Aktion "Viren-Engine-Fehler" kann jedes Ereignis angezeigt werden, das im Rahmen der normalen Funktion oder Operation der Viren-Engine aufgezeichnet wird. Lässt sich ein Ereignis nicht präziser einer bestimmten CEG-Aktion zuordnen, kann es dieser Aktion zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Viren-Engine-Rollback – Aktion

Beim Viren-Engine-Rollback werden Informationen über das Zurücksetzen der Viren-Engine auf eine frühere Version ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Viren-Engine-Status – Aktion

Bei der Aktion "Viren-Engine-Status" werden Informationen zum Status der Viren-Engine ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Viren-Engine-Warnung – Aktion

Bei der Aktion "Viren-Engine-Warnung" werden Informationen zu Warnungen im Zusammenhang mit der Viren-Engine ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Virenquarantäne

Die Virenquarantäne betrifft die Quarantäne bei Identifizierung eines Virus auf einem bestimmten Host. Für diese Aktion gibt es zwei mögliche Ergebnisse: "S" für "Success" (Erfolgreich) und "F" für "Failure" (Fehler).

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	*Primär*
Ziel - Prozessinformationen	*Primär*
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Prozess oder welche Datei aufgrund welches Virus auf welchem Host unter Quarantäne gestellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Der Virusname sollte im Feld "result_signature" in der CEG gespeichert sein.

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Ergebnis	event_result	event_severity
Fehler	F	6

Start des Virenscans

Der Start des Virenscans erfolgt, wenn ein Virenscan auf einem bestimmten Host gestartet wird. Für diese Aktion gibt es zwei mögliche Ergebnisse: "S" für "Success" (Erfolgreich) und "F" für "Failure" (Fehler).

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Virenscan auf welchem Host initiiert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Virenscan-Abbruch – Aktion

Beim Virenscan-Abbruch werden Informationen zum Abbruch eines auf einem bestimmten Host erfolgten Virenscans ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene	
Ergebnis - Informationen	Primär	
Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Abschluss des Virenscans

Der Abschluss des Virenscans erfolgt, wenn ein Virenscan auf einem bestimmten Host abgeschlossen wird. Für diese Aktion gibt es zwei mögliche Ergebnisse: "S" für "Success" (Erfolgreich) und "F" für "Failure" (Fehler).

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Virenscan auf welchem Host abgeschlossen wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Anhalten des Virenscans

Das Anhalten des Virenscans erfolgt, wenn ein Virenscan auf einem bestimmten Host angehalten wird. Für diese Aktion gibt es zwei mögliche Ergebnisse: "S" für "Success" (Erfolgreich) und "F" für "Failure" (Fehler).

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Virenscan auf welchem Host angehalten wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Fortsetzung des Virenscans

Die Fortsetzung des Virenscans erfolgt, wenn ein Virenscan auf einem bestimmten Host fortgesetzt wird. Für diese Aktion gibt es zwei mögliche Ergebnisse: "S" für "Success" (Erfolgreich) und "F" für "Failure" (Fehler).

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Virenscan auf welchem Host fortgesetzt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktualisierung der Virensignaturen

Die Aktualisierung der Virensignaturen erfolgt, wenn die Virensignaturen auf einem bestimmten Host aktualisiert werden. Für diese Aktion gibt es zwei mögliche Ergebnisse: "S" für "Success" (Erfolgreich) und "F" für "Failure" (Fehler).

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Virensignaturdatenbank auf welchem Host aktualisiert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	4

Antivirus-Installation

Die Antivirus-Installation erfolgt beim Installieren einer Antivirus-Anwendung auf einem bestimmten Host. Für diese Aktion gibt es zwei mögliche Ergebnisse: S für "Erfolgreich", F für "Fehler".

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto die Antivirus-Anwendung auf welchem Host installiert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Antivirus-Client entfernt

Die Aktion "Antivirus-Client entfernt" erfolgt beim Entfernen der Client-Software einer Antivirus-Anwendung auf einem bestimmten Host. Für diese Aktion gibt es zwei mögliche Ergebnisse: S für "Erfolgreich", F für "Fehler".

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto der Antivirus-Client auf welchem Host entfernt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	4

Antivirus-Deinstallation

Die Antivirus-Deinstallation erfolgt beim Deinstallieren einer Antivirus-Anwendung auf einem bestimmten Host. Für diese Aktion gibt es zwei mögliche Ergebnisse: S für "Erfolgreich", F für "Fehler".

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto die Antivirus-Anwendung auf welchem Host deinstalliert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	4

Aktion "DoS"

Aktion "Pufferüberlaufangriff"

Beim Pufferüberlaufangriff werden Ereignisinformationen zur Erfassung eines Pufferüberlaufangriffs auf einen Host angezeigt.

Wenn der Angriff *nicht* zu DoS führt, dann führen Sie eine Zuordnung zur gleichen Aktion in der Kategorie "Hostsicherheit" und in der Klasse der Anwendungssicherheit durch. Wenn das Ereignis im Zusammenhang mit einer Netzwerkumgebung steht, dann führen Sie eine Zuordnung zur gleichen Aktion in der Kategorie "Netzwerksicherheit" durch.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär

Informationen	Ebene
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Aktion "DoS-Angriff"

Die Aktion "DoS-Angriff" befasst sich mit Ereignisinformationen zu allgemeinen Exploits, die zu DoS führen.

Führen Sie eine Zuordnung zu entsprechenden Aktionen in der DoS-Klasse durch, wenn die Ursache des DoS-Angriffs bekannt ist.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär

Informationen	Ebene
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Klasse der Anwendungssicherheit

Aktion "Pufferüberlaufangriff"

Die Aktion "Pufferüberlaufangriff" gibt Informationen zur Erkennung eines Pufferüberlaufangriffs auf ein Hostsystem.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär

Informationen	Ebene
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Aktion "Formatstring-Angriff"

Die Aktion "Formatstring-Angriff" beschreibt Ereignisinformationen zu Exploits von ungefilterten Anwendereingaben als Formatstringparameter in bestimmten Formatierungsfunktionen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär

Informationen	Ebene
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	5
Fehler	F	4

Aktion "Speicherverlust"

Die Aktion "Speicherverlust" beschreibt Ereignisinformationen zu Anwendungen oder Systemen, die zugewiesenen Speicher nicht frei setzen und damit verfügbaren Speicher aufbrauchen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Aktion "XML-Angriff"

Die Aktion "XML-Angriff" beschreibt Ereignisinformationen zu Angriffen, die Schwachstellen in der XML-Technologie ausnutzen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Klasse für Verschlüsselungsaktivität

Aktion "Kryptografischer Alarm"

Die Aktion "Kryptografischer Alarm" beschreibt Informationen zu Alarmbedingungen im Zusammenhang mit kryptografischen Vorgängen oder Kryptosystemen in einer bestimmten Hostumgebung.

Jeder Typ von Alarm in Bezug auf kryptografische Vorgänge oder Kryptosysteme kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Kryptografischer Fehler" zugeordnet. Wenn sich die Aktion auf Netzwerkumgebungen bezieht, wird sie demselben Ereignis unter der Kategorie "Netzwerksicherheit" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	6

Aktion "Kryptografischer Fehler"

Die Aktion "Kryptografischer Fehler" beschreibt Informationen zu Fehlerbedingungen im Zusammenhang mit kryptografischen Vorgängen oder Kryptosystemen in einer bestimmten Hostumgebung.

Jeder Fehlertyp in Bezug auf kryptografische Vorgänge oder Kryptosysteme kann dieser Aktion zugeordnet werden. Weniger kritische Ereignisse sollten den Aktionen "Kryptografischer Vorgang" oder "Kryptosystem-Warnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "Kryptografischer Alarm" zugeordnet werden. Wenn sich die Aktion auf Netzwerkumgebungen bezieht, wird sie demselben Ereignis unter der Kategorie "Netzwerksicherheit" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär

Informationen	Ebene
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	5

Aktion "Kryptografische Benachrichtigung"

Die Aktion "Kryptografische Benachrichtigung" enthält Informationen zu Benachrichtigungen und Meldungen, die mithilfe von kryptografischen Vorgängen oder Kryptosystemen in einer bestimmten Hostumgebung generiert wurden.

Jeder Typ von Benachrichtigung zu kryptografischen Vorgängen oder Kryptosystemen kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "Kryptografischer Status", wenn das Ereignis den Status von kryptografischen Vorgängen oder Kryptosystemen beschreibt. Wenn sich die Aktion auf Netzwerkumgebungen bezieht, wird sie demselben Ereignis unter der Kategorie "Netzwerksicherheit" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär

Informationen	Ebene
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Kryptografischer Vorgang"

Die Aktion "Kryptografischer Vorgang" beschreibt Informationen zu allgemeinen Vorgängen der Funktionsweise von Kryptosystemen in einer bestimmten Hostumgebung.

Wenn ein Ereignis als Teil des kryptografischen Vorgangs oder der normalen Funktionen des Kryptosystems aufgezeichnet ist oder das Ereignis keiner spezifischeren CEG-Aktion zugeordnet werden kann, können Sie es dieser Aktion zuordnen. Wenn sich die Aktion auf Netzwerkumgebungen bezieht, wird sie demselben Ereignis unter der Kategorie "Netzwerksicherheit" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär

Informationen	Ebene
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Kryptografischer Status"

Die Aktion "Kryptographischer Status" beschreibt Informationen im Zusammenhang mit dem Status von kryptographischen Vorgängen oder Kryptosystemen in einer bestimmten Hostumgebung.

Wenn ein Ereignis als Teil der normalen Funktionen in kryptografischen Vorgängen oder Kryptosystemen aufgezeichnet wird, oder wenn sich ein Ereignis nicht präziser einer bestimmten CEG-Aktion zuordnen lässt, kann es dieser Aktion zugeordnet werden. Wenn sich die Aktion auf Netzwerkumgebungen bezieht, wird sie demselben Ereignis unter der Kategorie "Netzwerksicherheit" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Kryptografische Warnung"

Die Aktion "Kryptografische Warnung" beschreibt Informationen zu Warnungen im Zusammenhang mit kryptografischen Vorgängen oder Kryptosystemen in einer bestimmten Hostumgebung.

Jeder Warnungstyp in Bezug auf kryptografische Vorgänge oder Kryptosysteme kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Kryptografischer Fehler" zugeordnet werden. Wenn sich die Aktion auf Netzwerkumgebungen bezieht, wird sie demselben Ereignis unter der Kategorie "Netzwerksicherheit" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	4

Aktion "Entschlüsselungsvorgang"

Die Aktion "Entschlüsselungsvorgang" beschreibt Informationen im Zusammenhang mit allgemeinen Entschlüsselungsvorgängen auf einem Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Entschlüsselungsstatus"

Die Aktion "Entschlüsselungsstatus" beschreibt Informationen zum Entschlüsselungsstatus auf einem Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Verschlüsselungsalarm – Aktion

Die Aktion "Verschlüsselungsalarm" enthält Informationen zu verschlüsselungsbezogenen Alarmbedingungen auf einem Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Verschlüsselungsfehler

Die Aktion "Verschlüsselungsfehler" enthält Informationen zu verschlüsselungsbezogenen Fehlerbedingungen auf einem Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Verschlüsselungsbenachrichtigung – Aktion

Die Aktion "Verschlüsselungsbenachrichtigung" enthält Informationen zu Benachrichtigungen, die von einer Verschlüsselungs-Engine auf einem Host generiert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verschlüsselungsoperation – Aktion

Die Aktion "Verschlüsselungsoperation" enthält Informationen zu allgemeinen verschlüsselungsbezogenen Aktivitäten auf einem Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verschlüsselungsstart – Aktion

Die Aktion "Verschlüsselungsstart" enthält Informationen zum Start einer Verschlüsselungsoperation.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verschlüsselungswarnung – Aktion

Die Aktion "Verschlüsselungswarnung" enthält Informationen zu Benachrichtigungen und Meldungen von der Verschlüsselungs-Engine auf einem Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	3

Verschlüsselungsstatus – Aktion

Die Aktion "Verschlüsselungsstatus" enthält Informationen zum Status von Verschlüsselungsaktivitäten auf einem Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Schlüsselhinzufügung

Schlüsselhinzufügung in Zusammenhang mit der Hostauthentifizierung und Verschlüsselung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Authentifizierungsschlüssel auf welchem Host hinzugefügt wird. Auf welchem Host werden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host werden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Schlüsselalarm – Aktion

Die Aktion "Schlüsselalarm" enthält Informationen zu Alarmbedingungen in Bezug auf Verschlüsselungsschlüssel.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Schlüssellöschung – Aktion

Bei der Schlüssellöschung werden Informationen zum Löschen eines Verschlüsselungsschlüssels ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Schlüsselfehler – Aktion

Die Aktion "Schlüsselfehler" enthält Informationen zu Fehlerbedingungen in Bezug auf Verschlüsselungsschlüssel.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Schlüsselerstellung

Schlüsselerstellungsaktivitäten in Zusammenhang mit der Hostauthentifizierung und Verschlüsselung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Authentifizierungsschlüssel auf welchem Host generiert wird. Auf welchem Host werden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host werden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Schlüsseländerung – Aktion

Bei der Schlüsseländerung werden Informationen zum Ändern eines Verschlüsselungsschlüssels ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Schlüsselbenachrichtigung – Aktion

Die Aktion "Schlüsselbenachrichtigung" enthält Informationen zu Meldungen und Benachrichtigungen, die von einem Verschlüsselungsmechanismus generiert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Schlüsseloperation – Aktion

Die Aktion "Schlüsseloperation" enthält allgemeine Informationen zu Verschlüsselungsschlüsseln.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Schlüsselfreigabe – Aktion

Die Schlüsselfreigabe enthält Informationen zur Freigabe oder Synchronisation von Schlüsseln zwischen Systemen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Schlüssel auf welchem Host freigegeben werden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Schlüsselstatus – Aktion

Die Aktion "Schlüsselstatus" enthält Informationen zum Status von Verschlüsselungsschlüsseln.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Schlüsselwarnung – Aktion

Die Aktion "Schlüsselwarnung" enthält Informationen zu Warnungen in Bezug auf Verschlüsselungsschlüssel.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	3

Klasse für Signaturverletzungsaktivität

Aktion "Kernel-Exploit"

Die Aktion "Kernel-Exploit" gibt Informationen zur Erkennung eines Exploits, das einen Kernel beeinträchtigt oder beeinflusst.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	5
Fehler	F	4

Signaturverletzung

Bei der Signaturverletzung werden Ereignisinformationen zur Erkennung einer Verletzung durch ein signaturbasiertes Erkennungsmodul auf einem bestimmten Host angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2

Änderung der Windows-Registrierung

Bei einer Änderung der Windows-Registrierung werden Ereignisinformationen zur Änderung der Windows-Registrierung ausgegeben. Änderungen betreffen das Hinzufügen, Löschen und Ändern von Schlüsseln und Werten.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Verdächtige Service-/Daemon-Aktivität

Bei verdächtiger Service-/Daemon-Aktivität werden Ereignisinformationen in Zusammenhang mit der Erkennung verdächtiger Daemon- oder Serviceaktivitäten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Kernel und BS-Aktivität

Aktion "Kernspeicherauszugsfehler"

Die Aktion "Kernspeicherauszugsfehler" beschreibt Ereignisinformationen zu Fehlern im Zusammenhang mit Kernspeicherauszugsaktivitäten.

Wenn der Angriff *nicht* zu DoS führt, dann führen Sie eine Zuordnung zur gleichen Aktion in der Kategorie "Hostsicherheit" und in der Klasse der Anwendungssicherheit durch. Wenn das Ereignis im Zusammenhang mit einer Netzwerkumgebung steht, dann führen Sie eine Zuordnung zur gleichen Aktion in der Kategorie "Netzwerksicherheit" durch.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	5

Aktion "Start des Absturzabbilds"

Die Aktion "Start des Absturzabbilds" beschreibt Ereignisinformationen zum Start des Absturzabbildungsprozesses.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Kernel-Änderung"

Die Aktion "Kernel-Änderung" gibt Informationen zur Änderung eines Systemkernels.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Kernel-Benachrichtigung"

Die Aktion "Kernel-Benachrichtigung" gibt Informationen zu Benachrichtigungen und Meldungen eines Systemkernels. Sie können dieser Aktion jeden beliebigen Kernel-Benachrichtigungstyp zuordnen, wenn das Ereignis keiner spezifischeren Aktion zugeordnet werden kann. Verwenden Sie die Aktion "Kernel-Status", wenn das Ereignis den Status eines Kernels beschreibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Kernel-Vorgang"

Die Aktion "Kernel-Vorgang" gibt allgemeine Informationen zu Systemkernel-Vorgängen. Wenn Sie normale Kernel-Funktionen aufzeichnen wollen oder das Ereignis keiner spezifischeren CEG-Aktion zuordnen können, ziehen Sie in Betracht, das Ereignis dieser Aktion zuzuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Kernel-Status"

Die Aktion "Kernel-Status" gibt allgemeine Informationen zu Systemkernel-Status.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Kernel-Warnung"

Die Aktion "Kernel-Warnung" gibt Informationen zu mit Systemkernel in Verbindung stehenden Warnungen. Sie können dieser Aktion jeden beliebigen Warnungstyp über den Kernel zuordnen. Schwerwiegendere Ereignisse sollten der Aktion "Kernel-Fehler" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Aktion "Linux-Exploit"

Die Aktion "Linux-Exploit" beschreibt Ereignisinformationen zu Exploits oder Angriffen unter dem Betriebssystem Linux.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Aktion "Arbeitsspeicherzugriff"

Die Aktion "Arbeitsspeicherzugriff" gibt Informationen zum Arbeitsspeicherzugriff durch einen Prozess.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Arbeitsspeicherzuordnung"

Die Aktion "Arbeitsspeicherzuordnung" beschreibt Ereignisinformationen zur Arbeitsspeicherzuordnung für Prozesse auf einem System.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Arbeitsspeicher-Paritätsfehler"

Die Aktion "Arbeitsspeicher-Paritätsfehler" beschreibt Ereignisinformationen zu Paritätsfehlern im Speicher.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	5

Aktion "Systemaufruf-Alert"

Die Aktion "Systemaufruf-Alert" gibt Informationen zu mit Systemaufrufen in Verbindung stehenden Alerts. Ein Systemaufruf ist eine von einem beliebigen Programm gestellte Anfrage an das Betriebssystem nach der Ausführung von Aufgaben. Systemaufrufe sorgen für die Schnittstelle zwischen einem Prozess und dem Betriebssystem. Sie können dieser Aktion jeden beliebigen Warnungstyp zu Systemaufrufen zuordnen. Sie können eine Fehlerbedingung, die keiner sofortigen Beachtung bedarf, der Aktion "Systemaufruf-Fehler" zuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Aktion "Systemaufruf-Fehler"

Die Aktion "Systemaufruf-Fehler" gibt Informationen zu mit Systemaufrufen in Verbindung stehenden Fehlern. Ein Systemaufruf ist eine von einem beliebigen Programm gestellte Anfrage an das Betriebssystem nach der Ausführung von Aufgaben. Systemaufrufe sorgen für die Schnittstelle zwischen einem Prozess und dem Betriebssystem. Sie können dieser Aktion jeden beliebigen Systemaufruf-Fehlertyp zuordnen. Weniger schwerwiegende Ereignisse sollten der Aktion "Systemaufruf-Warnung" zugeordnet werden. Sie können schwerwiegendere Ereignisse, die sofortiger Beachtung bedürfen, der Aktion "Systemaufruf-Alert" zuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Aktion "Systemaufruf-Ausführung"

Die Aktion "Systemaufruf-Ausführung" gibt Informationen über die Ausführung eines Systemaufrufs. Ein Systemaufruf ist eine von einem beliebigen Programm gestellte Anfrage an das Betriebssystem nach der Ausführung von Aufgaben. Systemaufrufe sorgen für die Schnittstelle zwischen einem Prozess und dem Betriebssystem.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Systemaufruf-Benachrichtigung"

Die Aktion "Systemaufruf-Benachrichtigung" gibt Informationen zu Benachrichtigungen und Meldungen, die von einem Systemaufruf generiert wurden. Ein Systemaufruf ist eine von einem beliebigen Programm gestellte Anfrage an das Betriebssystem nach der Ausführung von Aufgaben. Systemaufrufe sorgen für die Schnittstelle zwischen einem Prozess und dem Betriebssystem. Sie können dieser Aktion jede beliebige Systemaufruf-Benachrichtigung zuordnen, wenn das Ereignis keiner spezifischeren Aktion zugeordnet werden kann. Verwenden Sie die Aktion "Systemaufruf-Status", wenn das Ereignis den Status eines Systemaufrufs beschreibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2

Informationen	Ebene	
Fehler	F	3

Aktion "Systemaufruf-Vorgang"

Die Aktion "Systemaufruf-Vorgang" gibt Informationen zu Systemaufrufvorgängen. Ein Systemaufruf ist eine von einem beliebigen Programm gestellte Anfrage an das Betriebssystem nach der Ausführung von Aufgaben. Systemaufrufe sorgen für die Schnittstelle zwischen einem Prozess und dem Betriebssystem. Wenn ein Ereignis als Teil von normalen Systemaufruffunktionen aufgezeichnet ist oder das Ereignis nicht einer spezifischeren CEG-Aktion zugeordnet werden kann, können Sie es dieser Aktion zuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Systemaufruf-Status"

Die Aktion "Systemaufruf-Status" gibt Informationen zum Status der Systemaufrufe. Ein Systemaufruf ist eine von einem beliebigen Programm gestellte Anfrage an das Betriebssystem nach der Ausführung von Aufgaben. Systemaufrufe sorgen für die Schnittstelle zwischen einem Prozess und dem Betriebssystem. Sie können dieser Aktion jede beliebige Systemaufruf-Statusmeldung zuordnen, wenn das Ereignis keiner spezifischeren Aktion zugeordnet werden kann.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Systemaufruf-Warnung"

Die Aktion "Systemaufruf-Warnung" gibt Informationen zu mit Systemaufrufen in Verbindung stehenden Warnungen. Ein Systemaufruf ist eine von einem beliebigen Programm gestellte Anfrage an das Betriebssystem nach der Ausführung von Aufgaben. Systemaufrufe sorgen für die Schnittstelle zwischen einem Prozess und dem Betriebssystem. Sie können dieser Aktion jeden beliebigen Systemaufruf-Warnungstyp zuordnen. Schwerwiegendere Ereignisse sollten der Aktion "Systemaufruf-Fehler" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Benachrichtigungsverwaltung

Meldungs-Broadcast

Jede Art von Broadcast-Meldung (von einem Benutzer an mehrere Systeme, zwischen Netzwerkgeräten).

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse für Netzwerkaktivität

Eingehendes Netzwerkpaket

Ein beliebiges eingehendes Netzwerkpaket (generisch)

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ausgehendes Netzwerkpaket

Ein beliebiges ausgehendes Netzwerkpaket (generisch)

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Port-Alarm – Aktion

Alarmbedingungen im Zusammenhang mit einem Port.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Port-Schließung

Aktivität in Zusammenhang mit dem Schließen eines Ports.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Port-Fehler – Aktion

Fehlerbedingungen im Zusammenhang mit einem Port. Weniger schwerwiegende Ereignisse sollten der Aktion "Port-Warnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "Port-Alarm" zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Fehler	F	5

Port-Einrichtung

Aktivität in Zusammenhang mit der Einrichtung eines Ports.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Port-Abhörung

Aktivität in Zusammenhang mit dem Abhören eines Ports.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Port-Benachrichtigung – Aktion

Jeder Typ von Benachrichtigung über den Port kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Port-Fehler" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Port-Status – Aktion

Jede Port-bezogene Statusmeldung kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Port-Warnung – Aktion

Jeder Typ von Warnung in Bezug auf den Port kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Port-Fehler" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Klasse für verdächtige Aktivität

Aktion "Code-Einfügung"

Die Aktion "Code-Einfügung" gibt Informationen zur Einfügung externer Codes in ein Programm.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Aktion "Code-Änderung"

Die Aktion "Code-Änderung" gibt Informationen zur Änderung von Codes.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Aktion "Tastenkombinationserfassung"

Die Aktion "Tastenkombinationserfassung" gibt Informationen über die Erfassung von Tastenkombinationen auf einem System.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	3
Fehler	F	3

Aktion "Arbeitsspeicher-Alert"

Die Aktion "Arbeitsspeicher-Alert" gibt Informationen zu mit dem Arbeitsspeicher in Verbindung stehenden Alerts.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Aktion "Speicherbeschädigung"

Mit der Aktion "Speicherbeschädigung" werden Ereignisinformationen zur Erkennung von Speicherbeschädigungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	5
Fehler	F	4

Aktion "Arbeitsspeicheränderung"

Die Aktion "Arbeitsspeicheränderung" gibt Informationen zur Änderung des Arbeitsspeichers durch einen Prozess.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Kennwortverlust"

Die Aktion "Kennwortverlust" gibt Informationen zu Versuchen, Kennwörter offenzulegen, aufzulisten, zu extrahieren oder preiszugeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	3
Fehler	F	3

Aktion "Server-Exploit"

Mit der Aktion "Server-Exploit" werden Ereignisinformationen zur Erkennung von Angriffsaktivitäten angezeigt, durch die Schwachstellen in der Server-Software ausgenutzt werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Kapitel 7: Kategorie "Identitätsverwaltung"

Dieses Kapitel enthält folgende Themen:

Kontenverwaltungsklasse

Kontoerstellungsaktion

Die Kontoerstellungaktion erfolgt, wenn auf einem bestimmten System oder für eine bestimmte Anwendung neue Konten erstellt werden.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	sekundär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär

Informationen	Ebene
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, wer welches Konto auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Kontolöschungsaktion

Die Kontolöschungsaktion erfolgt, wenn auf einem bestimmten System oder für eine bestimmte Anwendung Konten gelöscht werden.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	sekundär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär

Informationen	Ebene
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, wer welches Konto auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Kontodeaktivierungsaktion

Die Kontodeaktivierungsaktion erfolgt, wenn auf einem bestimmten System oder für eine bestimmte Anwendung Konten deaktiviert werden.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	sekundär
Ziel – Prozessinformationen	tertiär

Informationen	Ebene
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, wer welches Konto auf welchem Host deaktiviert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Kontoaktivierungsaktion

Die Kontoaktivierungsaktion erfolgt, wenn auf einem bestimmten System oder für eine bestimmte Anwendung Konten aktiviert werden.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	sekundär

Informationen	Ebene
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, wer welches Konto auf welchem Host aktiviert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Kontenimport – Aktion

Bei der Aktion "Kontenimport" werden Informationen zum Importieren von Konten ausgegeben. Dieser Vorgang erfolgt in der Regel über die Stapelverarbeitung.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär

Informationen	Ebene
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Kontoauflistungsaktion

Die Kontoauflistungsaktion erfolgt, wenn auf einem bestimmten System oder für eine bestimmte Anwendung Konten aufgelistet werden.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	sekundär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	sekundär

Informationen	Ebene
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, wer welche Konten auf welchem Host aufgelistet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Kontosperrungsaktion

Die Kontosperrungsaktion erfolgt, wenn auf einem bestimmten System oder für eine bestimmte Anwendung Konten gesperrt werden.

Informationen	Ebene
Quelle – Benutzerinformationen	sekundär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	sekundär

Informationen	Ebene
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, wer welches Konto auf welchem Host gesperrt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Kontenverwaltungsalarm – Aktion

Beim Kontenverwaltungsalarm werden Informationen zu Alarmbedingungen ausgegeben, die die Kontenverwaltung betreffen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Kontenverwaltungsfehler – Aktion

Beim Kontenverwaltungsfehler werden Informationen zu Fehlerbedingungen ausgegeben, die die Kontenverwaltung betreffen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Kontenverwaltungsbenachrichtigung – Aktion

Bei der Kontenverwaltungsbenachrichtigung werden Informationen zu kontenverwaltungsbezogenen Benachrichtigungen und Meldungen ausgegeben, die von Identitätsmanagementsystemen generiert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Kontenverwaltungswarnung – Aktion

Bei der Kontenverwaltungswarnung werden Informationen zu Warnungen ausgegeben, die die Kontenverwaltung betreffen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene	
Ergebnis - Informationen	Primär	
Ergebnis	**event_result**	**event_severity**
Fehler	F	3

Kontoänderungsaktion

Die Kontoänderungsaktion erfolgt, wenn auf einem bestimmten System oder für eine bestimmte Anwendung Kontoinformationen geändert werden.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	sekundär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, wer welches Konto auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Aktion "Änderung von Kontokennwörtern"

Die Aktion "Änderung von Kontokennwörtern" erfolgt, wenn auf einem bestimmten System oder für eine bestimmte Anwendung Kontokennwörter geändert werden.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	sekundär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, wer das Kennwort für welches Konto auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Aktion zur Zurücksetzung von Kontokennwörtern

Die Aktion zur Zurücksetzung von Kontokennwörtern erfolgt, wenn Konten auf einem bestimmten System zurückgesetzt werden. Diese Aktion gehört zu einer übergeordneten Ebene und darf nicht für alle Ereignisquellen angegeben werden.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	sekundär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär

Informationen	Ebene
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, wer das Kennwort für welches Konto auf welchem Host zurückgesetzt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Aktion "Kontenstatus"

Die Aktion "Kontenstatus" gibt Informationen zum Status von Benutzer- oder Systemkonten auf einem System.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Kontosuspendierungsaktion

Die Kontosuspendierungsaktion erfolgt, wenn Konten auf einem bestimmten System oder für eine bestimmte Anwendung suspendiert werden.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	sekundär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, wer das Kennwort für welches Konto auf welchem Host suspendiert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Kontoentsperrungsaktion

Die Kontoentsperrungsaktion erfolgt, wenn Konten auf einem bestimmten System oder für eine bestimmte Anwendung entsperrt werden.

Informationen	Ebene
Quelle – Benutzerinformationen	primär
Quelle – Host-Informationen	sekundär
Quelle – Objektinformationen	tertiär
Quelle – Prozessinformationen	tertiär
Quelle – Gruppeninformationen	tertiär
Ziel – Benutzerinformationen	primär
Ziel – Host-Informationen	primär
Ziel – Objektinformationen	sekundär
Ziel – Prozessinformationen	tertiär
Ziel – Gruppeninformationen	tertiär
Agent – Informationen	primär
Agent – Host-Informationen	primär
Ereignisquelle – Host-Informationen	primär
Ereignisquelle – Informationen	tertiär
Ereignis – Informationen	primär
Ergebnis – Informationen	primär

Bei dieser Aktion ist es wichtig zu wissen, wer welches Konto auf welchem Host entsperrt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Failure (Fehler)	F	3

Gruppenauflistung – Aktion

Die Gruppenauflistung enthält Informationen zur Auflistung von Gruppeninformationen in einer bestimmten Anwendung oder auf einem bestimmten System.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Gruppen auf welchem System aufgelistet sind. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Benutzerkontoattribut-Verletzung – Aktion

Die Aktion "Benutzerkontoattribut-Verletzung" enthält Informationen über die Erkennung einer Verletzung im Zusammenhang mit Benutzerkontoattributen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene	
Ergebnis - Informationen	Primär	
Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Benutzerkonto-Erstellungsanfrage – Aktion

Die Aktion "Benutzerkonto-Erstellungsanfrage" enthält Informationen über Anfragen zur Erstellung eines neuen Kontos.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Benutzerkonto-Änderungsanfrage – Aktion

Die Aktion "Benutzerkonto-Änderung" enthält Informationen über erfolgte Anfragen zur Änderung eines bestehenden Kontos.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Benutzerkonto-Validierungsanfrage – Aktion

Die Aktion "Benutzerkonto-Validierungsanfrage" enthält Informationen über Anfragen zur Validierung bestehender Konten.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Bestätigungsaktivität – Klasse

Bestätigung gestartet – Aktion

Die Aktion "Bestätigung gestartet" enthält Informationen zu Startaktivitäten im Rahmen der Bestätigungsprozesses.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifizierung beenden – Aktion

Die Aktion "Zertifizierung beenden" enthält Informationen zum Abschluss oder zur Beendigung eines Zertifizierungsprozesses, zum Beispiel Zertifizierungen von Benutzerberechtigungen als Bestandteil des Identitätsmanagements.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifizierungsbenachrichtigung – Aktion

Die Aktion "Zertifizierungsbenachrichtigung" enthält Informationen zu Benachrichtigungen eines Zertifizierungsprozesses, zum Beispiel Zertifizierungen von Benutzerberechtigungen im Rahmen des Identitätsmanagements.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifizierungsstart – Aktion

Die Aktion "Zertifizierungsstart" enthält Informationen zum Start eines Zertifizierungsprozesses, zum Beispiel Zertifizierungen von Benutzerberechtigungen im Rahmen des Identitätsmanagements.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Benutzer zertifizieren – Aktion

Die Aktion "Benutzer zertifizieren" enthält Informationen zur Zertifizierung eines Benutzerkontos als Bestandteil eines formalen Zertifizierungsprozesses.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Anfrage genehmigt – Aktion

Die Aktion "Anfrage genehmigt" enthält Informationen zur Genehmigung der Bestätigungsanfrage im Rahmen eines regelmäßigen Bestätigungsprozesses.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Anfrage archiviert – Aktion

Die Aktion "Anfrage archiviert" enthält Informationen zur Archivierung einer Bestätigungsanfrage im Rahmen eines regelmäßigen Bestätigungsprozesses.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Anfrage delegiert – Aktion

Die Aktion "Anfrage delegiert" enthält Informationen zur Delegierung einer Bestätigungsanfrage im Rahmen eines regelmäßigen Bestätigungsprozesses.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Anfrage eskaliert – Aktion

Die Aktion "Anfrage eskaliert" enthält Informationen zur Eskalierung einer Bestätigungsanfrage im Rahmen eines regelmäßigen Bestätigungsprozesses.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Anfrage neu zugewiesen – Aktion

Die Aktion "Anfrage neu zugewiesen" enthält Informationen zur Neuzuweisung einer Bestätigungsanfrage im Rahmen eines regelmäßigen Bestätigungsprozesses.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Anfrage erhalten"

Die Aktion "Anfrage erhalten" enthält Informationen zum Erhalt einer Bescheinigungsanfrage im Rahmen eines regelmäßigen Bescheinigungsprozesses.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Anfrage abgelehnt – Aktion

Die Aktion "Anfrage abgelehnt" enthält Informationen zur Ablehnung einer Bestätigungsanfrage im Rahmen eines regelmäßigen Bestätigungsprozesses.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Anfrage widerrufen – Aktion

Die Aktion "Anfrage widerrufen" enthält Informationen zum Widerruf einer Bestätigungsanfrage im Rahmen eines regelmäßigen Bestätigungsprozesses.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Anfragestatus – Aktion

Die Aktion "Anfragestatus" enthält Informationen zum Status einer Bestätigungsanfrage im Rahmen eines regelmäßigen Bestätigungsprozesses.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Gruppenverwaltung

Gruppenaktivierung – Aktion

Bei der Aktion "Gruppenaktivierung" werden Informationen zur Aktivierung einer Gruppe auf einem bestimmten System oder in einer bestimmten Anwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Gruppenerstellung

Die Gruppenerstellung erfolgt beim Erstellen von Gruppen auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Gruppe auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben? Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Gruppendeaktivierung – Aktion

Bei der Aktion "Gruppendeaktivierung" werden Informationen zur Deaktivierung einer Gruppe auf einem bestimmten System oder in einer bestimmten Anwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Gruppenlöschung

Die Gruppenlöschung erfolgt beim Löschen von Gruppen auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Gruppe auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Gruppenverwaltungsalarm – Aktion

Bei der Aktion "Gruppenverwaltungsalarm" werden Informationen zu Alarmbedingungen ausgegeben, die die Gruppenverwaltung betreffen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Gruppenverwaltungsfehler – Aktion

Beim Gruppenverwaltungsfehler werden Informationen zu Fehlerbedingungen ausgegeben, die die Gruppenverwaltung betreffen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Gruppenverwaltungsbenachrichtigung – Aktion

Bei der Gruppenverwaltungsbenachrichtigung werden Informationen zu Benachrichtigungen und Meldungen ausgegeben, die die Gruppenverwaltung betreffen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Gruppenverwaltungswarnung – Aktion

Bei der Gruppenverwaltungswarnung werden Informationen zu Warnungen ausgegeben, die die Gruppenverwaltung betreffen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	3

Hinzufügen einer Gruppenmitgliedschaft

Das Hinzufügen einer Gruppenmitgliedschaft erfolgt, wenn Informationen über eine Gruppenmitgliedschaft auf einem bestimmten System oder einer bestimmten Anwendung hinzugefügt werden. Für diese Aktion gibt es zwei mögliche Ergebnisse: S für "Erfolgreich", F für "Fehler".

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer die Mitgliedschaft welcher Gruppe auf welchem Host hinzugefügt hat, und welche Benutzer von diesen Änderungen betroffen waren. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Ergebnis	event_result	event_severity
Fehler	F	3

Entfernen einer Gruppenmitgliedschaft

Das Entfernen einer Gruppenmitgliedschaft erfolgt, wenn Informationen über eine Gruppenmitgliedschaft auf einem bestimmten System oder einer bestimmten Anwendung entfernt werden. Für diese Aktion gibt es zwei mögliche Ergebnisse: S für "Erfolgreich", F für "Fehler".

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer die Mitgliedschaft welcher Gruppe auf welchem Host entfernt hat, und welche Benutzer von diesen Änderungen betroffen waren. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Änderung der Gruppenmitgliedschaft

Die Änderung einer Gruppenmitgliedschaft erfolgt, wenn Informationen über eine Gruppenmitgliedschaft auf einem bestimmten System oder einer bestimmten Anwendung geändert werden. Dazu gehören das Entfernen und Hinzufügen von Mitgliederinformationen.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer die Mitgliedschaft welcher Gruppe auf welchem Host geändert hat, und welche Benutzer von diesen Änderungen betroffen waren. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Gruppenänderung

Die Gruppenänderung erfolgt, wenn Gruppeninformationen auf einem bestimmten System oder einer bestimmten Anwendung geändert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Gruppe auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse der Identitätsverwaltung

Identitätskorrelation – Aktion

Die Aktion "Identitätskorrelation" enthält Informationen zu einem Prozess, mit dem die ordnungsgemäße Inhaberschaft verschiedener Benutzerkonten über sämtliche Systeme und Anwendungen eines Unternehmens hinweg abgeglichen und validiert wird. Mit diesen IDs kann die Inhaberschaft der Benutzerkonto-Login-IDs stets einzelnen Personen zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Identitätserstellung

Die Identitätserstellung erfolgt beim Erstellen von Identitäten auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Identität auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Identitätslöschung

Die Identitätslöschung erfolgt beim Löschen von Identitäten auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Identität auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Identitätsdeaktivierung

Die Identitätsdeaktivierung erfolgt beim Deaktivieren von Identitäten auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär

Informationen	Ebene
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Identität auf welchem Host deaktiviert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Identitätsaktivierung

Die Identitätsaktivierung erfolgt beim Aktivieren von Identitäten auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Identität auf welchem Host aktiviert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Identitätsänderung

Die Identitätsänderung erfolgt beim Ändern von Identitätsinformationen auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär

Informationen	Ebene
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Identität auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Änderung des Identitätskennworts

Die Änderung des Identitätskennworts erfolgt beim Ändern eines Identitätskennworts auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär

Informationen	Ebene
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer das Kennwort für welche Identität auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Identitätssynchronisierung – Aktion

Bei der Identitätssynchronisierung werden Informationen zu sämtlichen Prozessen ausgegeben, mit denen Benutzer oder Identitäten zwischen verschiedenen Benutzerspeichern verknüpft oder synchronisiert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär

Informationen	Ebene
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Benutzerrechteverwaltung

Kontoaktualisierung – Aktion

Die Kontoaktualisierung erfolgt, wenn in einer bestimmten Anwendung oder auf einem bestimmten System Kontoinformationen aktualisiert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär

Informationen	Ebene
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto auf welchem System aktualisiert wird. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Doppelte Rollenverknüpfung erkannt – Aktion

Bei der Aktion "Doppelte Rollenverknüpfung erkannt" werden Informationen über die Erkennung zweier Berechtigungsverknüpfungen zwischen Rolle und Ressource ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Übermäßige Berechtigungen erkannt – Aktion

Die Aktion "Übermäßige Berechtigungsverknüpfungen erkannt" enthält Informationen über die Erkennung übermäßig vieler direkter Berechtigungsverknüpfungen zwischen einem Benutzer und vielen Ressourcen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Minimale Berechtigungen erkannt – Aktion

Die Aktion "Minimale Berechtigungsverknüpfung erkannt" enthält Informationen über die Erkennung weniger Berechtigungsverknüpfungen zwischen Benutzer und Ressourcen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Verletzung der Trennung von Pflichten – Aktion

Die Aktion "Verletzung der Trennung von Pflichten" enthält Informationen über die Erkennung von Verletzungen des Prinzips der Trennung von Pflichten im Zusammenhang mit Benutzerrechten.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Verdächtige Benutzerberechtigung erkannt – Aktion

Die Aktion "Verdächtige Benutzerberechtigung erkannt" enthält Informationen über die Erkennung von Ressourcenberechtigungen für verdächtige Benutzer.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Zuweisung des Benutzerrechts "Admin"

Die Zuweisung des Benutzerrechts "Admin" erfolgt, wenn Benutzerrechte für eine bestimmte Anwendung oder auf einem bestimmten System zugewiesen werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Bei dieser Aktion ist es von Bedeutung, welchen Benutzern auf welchem System Rechte zugewiesen werden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Löschung des Benutzerrechts "Admin"

Die Löschung des Benutzerrechts "Admin" erfolgt, wenn Benutzerrechte für eine bestimmte Anwendung oder auf einem bestimmten System gelöscht werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Bei dieser Aktion ist es von Bedeutung, welche Benutzerrechte auf welchem System gelöscht werden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zuweisung von Benutzerberechtigungen

Die Zuweisung von Benutzerberechtigungen erfolgt beim Zuweisen einer bestehenden Benutzerberechtigung auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Benutzerberechtigung für welchen Benutzer auf welchem Host zugewiesen hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Benutzerberechtigungskonflikt –Aktion

Die Aktion "Benutzerberechtigungskonflikt" enthält Informationen über die Erkennung eines Konflikts zwischen Benutzer- und Rollenberechtigungen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Änderungsanfrage zur Benutzerberechtigung – Aktion

Die Aktion "Änderungsanfrage zur Benutzerberechtigung" enthält Informationen über erfolgte Anfragen zur Änderung von Benutzerberechtigungen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Benutzerberechtigungsüberschneidung –Aktion

Die Aktion "Benutzerberechtigungsüberschneidung" enthält Informationen über die Erkennung von Berechtigungsüberschneidungen für Benutzerkonten.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Entfernen von Benutzerberechtigungen

Das Entfernen von Benutzerberechtigungen erfolgt beim Entfernen einer bestehenden Benutzerberechtigung auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Benutzerberechtigung für welchen Benutzer auf welchem Host entfernt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Validierungsanfrage zur Benutzerberechtigung – Aktion

Die Aktion "Validierungsanfrage zur Benutzerberechtigung" enthält Informationen über erfolgte Anfragen zur Validierung von Benutzerberechtigungen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Benutzerberechtigungsverletzung –Aktion

Die Aktion "Benutzerberechtigungsverletzung" enthält Informationen über die Erkennung von Benutzerberechtigungsverletzungen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Zuweisung von Benutzerrechten

Die Zuweisung von Benutzerrechten erfolgt beim Zuweisen eines bestehenden Benutzerrechts auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Benutzerrechte für welchen Benutzer auf welchem Host zugewiesen hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Erstellung von Benutzerrechten

Die Erstellung von Benutzerrechten erfolgt beim Erstellen eines Benutzerrechts auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welches Benutzerrecht auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Löschung von Benutzerrechten

Das Löschen von Benutzerrechten erfolgt beim Löschen eines Benutzerrechts auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welches Benutzerrecht auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Auflistung von Benutzerrechten

Die Auflistung von Benutzerrechten erfolgt beim Auflisten von Benutzerrechten auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer die Rechte von welchem Benutzer auf welchem Host aufgelistet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Änderung von Benutzerrechten

Die Änderung von Benutzerrechten erfolgt beim Ändern eines Benutzerrechts auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welches Benutzerrecht auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Benutzerrechtsbenachrichtigung"

Die Aktion "Benutzerrechtsbenachrichtigung" gibt Informationen zu generischen Benutzerrechtsbenachrichtigungen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Benutzerrollenüberschneidung – Aktion

Bei der Aktion "Benutzerrollenüberschneidung" werden Informationen über die Erkennung von Rollenüberschneidungen bei Benutzerkonten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Klasse der Benutzerrollenverwaltung

Doppelte Berechtigungsverknüpfung erkannt – Aktion

Die Aktion "Doppelte Berechtigungsverknüpfung erkannt" enthält Informationen über zwei erkannte Berechtigungsverknüpfungen zwischen Benutzer und Ressource.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Übermäßige Rollen erkannt – Aktion

Bei der Aktion "Übermäßige Rollen erkannt" werden Informationen über die Erkennung einer Ressource ausgegeben, die von vielen Rollen verwendet wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Übermäßige Rollenhierarchie erkannt – Aktion

Bei der Aktion "Übermäßige Rollenhierarchie erkannt" werden Informationen über die Erkennung von Rollen mit vielen vorhandenen Unterrollen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Übermäßige Rollenmitgliedschaft erkannt – Aktion

Bei der Aktion "Übermäßige Rollenmitgliedschaft erkannt" werden Informationen über die Erkennung von Rollen ausgegeben, denen zu viele direkte, indirekte und doppelte Benutzer zugewiesen sind.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Minimale Rollenhierarchie erkannt – Aktion

Bei der Aktion "Minimale Rollenhierarchie erkannt" werden Informationen über die Erkennung einer Rolle ausgegeben, der nur wenige Unterrollen aufweist.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Minimale Rollenmitgliedschaft erkannt – Aktion

Bei der Aktion "Minimale Rollenmitgliedschaft erkannt" werden Informationen über die Erkennung einer Rolle mit einer geringen Gesamtanzahl von Ressourcen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Minimale Rollen erkannt – Aktion

Bei der Aktion "Minimale Rollen erkannt" werden Informationen über die Erkennung einer Ressource ausgegeben, die von wenigen Rollen verwendet wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Rollenänderungsanfrage – Aktion

Bei der Aktion "Rollenänderungsanfrage" werden Informationen über Anfragen zur Änderung vorhandener Rollen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Rollenvalidierung – Aktion

Bei der Rollenvalidierung werden Informationen zum Validieren einer Benutzerrolle ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Rollenvalidierungsanfrage – Aktion

Bei der Aktion "Rollenvalidierungsanfrage" werden Informationen über Anfragen zur Validierung vorhandener Rollen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Rollenverletzung – Aktion

Bei der Aktion "Rollenverletzung" werden Informationen über Rollenverletzungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Verletzung der Trennung von Pflichten – Aktion

Bei der Aktion "Verletzung der Trennung von Pflichten" werden Informationen zu Verletzungen des Prinzips der Trennung von Pflichten ausgegeben, die in Verbindung mit Benutzerrollen auftreten.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Verdächtige Rollenzuweisung erkannt – Aktion

Bei der Aktion "Verdächtige Rollenzuweisung erkannt" werden Informationen über Situationen ausgegeben, in denen Benutzer- oder Rollenberechtigungen verdächtig sind.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Verdächtige Rolle erkannt – Aktion

Bei der Aktion "Verdächtige Rolle erkannt" werden Informationen über Situationen ausgegeben, in denen eine Rolle verdächtig ist.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Verdächtige Benutzerberechtigung erkannt – Aktion

Bei der Aktion "Verdächtige Benutzerberechtigung erkannt" werden Informationen über die Erkennung von Rollenberechtigungen für verdächtige Benutzer ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Zuweisung der Benutzerrolle "Admin"

Die Zuweisung der Benutzerrolle "Admin" erfolgt beim Zuweisen der Benutzerrolle "Admin" oder "Berechtigter Benutzer" auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer die Benutzerrolle "Admin" oder "Berechtigter Benutzer" welchem Benutzer auf welchem Host zugewiesen hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Löschung der Benutzerrolle "Admin"

Die Löschung der Benutzerrolle "Admin" erfolgt beim Löschen der Benutzerrolle "Admin" oder "Berechtigter Benutzer" auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer die Benutzerrolle "Admin" oder "Berechtigter Benutzer" für welchen Benutzer auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Änderung der Benutzerrolle "Admin"

Die Änderung der Benutzerrolle "Admin" erfolgt beim Ändern der Benutzerrolle "Admin" oder "Berechtigter Benutzer" auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer die Benutzerrolle "Admin" oder "Berechtigter Benutzer" für welchen Benutzer auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Entfernen der Benutzerrolle "Admin"

Das Entfernen der Benutzerrolle "Admin" erfolgt beim Entfernen der Benutzerrolle "Admin" oder "Berechtigter Benutzer" auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer die Benutzerrolle "Admin" oder "Berechtigter Benutzer" für welchen Benutzer auf welchem Host entfernt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Zuweisung von Benutzerrollen

Die Zuweisung von Benutzerrollen erfolgt beim Zuweisen einer Benutzerrolle auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Rolle für welchen Benutzer auf welchem Host zugewiesen hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Erstellung von Benutzerrollen

Die Erstellung von Benutzerrollen erfolgt beim Erstellen einer Benutzerrolle auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Rolle auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Löschung von Benutzerrollen

Das Löschen von Benutzerrollen erfolgt beim Löschen einer Benutzerrolle auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Rolle auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Änderung von Benutzerrollen

Die Änderung von Benutzerrollen erfolgt beim Ändern einer Benutzerrolle auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Rolle auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Benutzerrollenüberschneidung – Aktion

Bei der Aktion "Benutzerrollenüberschneidung" werden Informationen über die Erkennung von Rollenüberschneidungen bei Benutzerkonten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3

Entfernen von Benutzerrollen

Das Entfernen von Benutzerrollen erfolgt beim Entfernen einer Benutzerrolle auf einem bestimmten System oder einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle - Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle - Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Rolle für welchen Benutzer auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Workflow-Management – Klasse

Aufgabengenehmigung – Aktion

Die Aktion "Aufgabengenehmigung" enthält Informationen zur Genehmigung von Aufgaben, die an einen Workflow-Prozess oder an eine Workflow-Engine übermittelt bzw. hinzugefügt werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Kapitel 8: Kategorie "Messaging"

Dieses Kapitel enthält folgende Themen:

Klasse für E-Mail-Aktivität

Backbone-Übertragung

Bei der Backbone-Übertragung werden Informationen zur Übermittlung und zum Empfang von E-Mails an ein anderes bzw. von einem anderen MAPI-System über einen Connector oder ein Gateway ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Gateway-Übertragung

Bei der Gateway-Übertragung werden Informationen zur Übermittlung und zum Empfang von E-Mails über ein Gateway ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Meldungslöschung

Bei der Meldungslöschung werden Informationen zur Löschung von Meldungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Ergebnis	event_result	event_severity
Fehler	F	3

Meldungszustellung

Bei der Meldungszustellung werden Informationen zur Zustellung von Meldungen an ein Postfach oder einen öffentlichen Ordner ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Meldungsübermittlung

Bei der Meldungsübermittlung werden Informationen zur Meldungsübermittlung durch den Client ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Meldungsumleitung

Bei der Meldungsumleitung werden Informationen zur Übermittlung von Meldungen an andere Postfächer als die der Empfänger ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Nachrichtenfreigabe – Aktion

Die Nachrichtenfreigabe erfolgt, wenn Nachrichten aus der Quarantäne für einen Benutzerspeicher, z. B. Posteingang, freigegeben werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Pfadumleitung von Meldungen

Bei der Pfadumleitung von Meldungen werden Informationen zur Umleitung von Meldungen an einen alternativen Pfad ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Meldungsübertragung

Bei der Meldungsübertragung werden Informationen zur Übertragung von Meldungen zwischen einem Client und einem Server, Connector oder Gateway ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Test

Beim Test werden Informationen zu Testaktivitäten ausgegeben (z. B.: X.400-Testübertragung, X.400-Testübermittlung).

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Berichtslöschung

Bei der Berichtslöschung werden Informationen zum Löschen, Annehmen oder Verwerfen einer Übermittlungsbestätigung oder eines Unzustellbarkeitsberichts (NDR, Non-Delivery Report) ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Berichtsempfang

Beim Berichtsempfang werden Informationen zum Erstellen, Übertragen, Übermitteln oder Generieren einer Übermittlungsbestätigung bzw. eines Unzustellbarkeitsberichts (NDR, Non-Delivery Report) ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

SMTP-Übermittlung

Bei der SMTP-Übermittlung werden Informationen zur Übermittlung von Meldungen an eine Entität wie ein Gateway, einen MTA (Mail Transfer Agent), einen lokalen Speicher, einen Speichertreiber usw. ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

SMTP-Fehler – Aktion

Der SMTP-Fehler enthält Informationen zu Fehlern, die während der Übertragung von E-Mails an einen bzw. von einem Internet Mail-Dienst verursacht werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	5

SMTP-Benachrichtigung – Aktion

Die SMTP-Benachrichtigung enthält Informationen zu Warnungen, die während der Übertragung von E-Mails an einen bzw. von einem Internet Mail-Dienst verursacht werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

SMTP-Warteschlange

Für die SMTP-Warteschlange werden Informationen zur Warteschlange für ausgehende E-Mails ausgegeben, die auf die Übermittlung durch den Internet-E-Mail-Dienst warten.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

SMTP-Übertragung

Bei der SMTP-Übertragung werden Informationen zur Übertragung von E-Mails an einen oder von einem Internet-E-Mail-Dienst ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

SMTP-Warnung – Aktion

Die SMTP-Warnung enthält Informationen zu Warnungen, die während der Übertragung von E-Mails an einen bzw. von einem Internet Mail-Dienst verursacht werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Messaging-System – Klasse

Meldungswarnung – Aktion

Die Aktion "Meldungswarnung" enthält Informationen zu Warnungen in Bezug auf das Meldungssystem.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Kapitel 9: Kategorie "Netzwerksicherheit"

Dieses Kapitel enthält folgende Themen:

Zugriffssteuerung – Klasse

Aktion "Port-Blockierung"

Mit der Aktion "Port-Blockierung" werden Ereignisinformationen zur Blockierung von Ports angezeigt, die durch manuelle oder automatische Vorgänge zur Einschränkung oder Steuerung des Datenverkehrs eines bestimmten Ports dienen soll.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär

Informationen	Ebene
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Port-Blockierung aufheben"

Mit der Aktion "Port-Blockierung aufheben" werden Ereignisinformationen zur Aufhebung der Port-Blockierung angezeigt, die durch manuelle oder automatische Vorgänge zur Entfernung von Einschränkungen eines bestimmten Ports dienen soll.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Portsicherheitsverletzung"

Mit der Aktion "Portsicherheitsverletzung" werden Ereignisinformationen zur Erkennung von Portsicherheitsverletzungen auf einem Switch oder ähnlichen Geräten angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	3

Aktion "Alarm zur Ratenbegrenzung"

Mit der Aktion "Alarm zur Ratenbegrenzung" werden Informationen zu Alarmbedingungen der Ratenbegrenzungseinstellungen oder der Ratengestaltung im Netzwerkverkehr angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	6

Aktion "Ratenbegrenzungsfehler"

Mit der Aktion "Ratenbegrenzungsfehler" werden Informationen zu Fehlerbedingungen der Ratenbegrenzungseinstellungen oder der Ratengestaltung im Netzwerkverkehr angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	5

Aktion "Vorgang der Ratenbegrenzung"

Mit der Aktion "Vorgang der Ratenbegrenzung" werden Informationen zu allgemeinen Vorgängen im Zusammenhang mit der Ausführung von Ratenbegrenzungseinstellungen oder der Ratengestaltung im Netzwerkverkehr angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Status der Ratenbegrenzung"

Mit der Aktion "Status der Ratenbegrenzung" werden Informationen zum Status der Ratenbegrenzungseinstellungen oder der Ratengestaltung im Netzwerkverkehr angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Warnung zur Ratenbegrenzung"

Mit der Aktion "Warnung zur Ratenbegrenzung" werden Informationen zu Warnungsbedingungen der Ratenbegrenzungseinstellungen oder der Ratengestaltung im Netzwerkverkehr angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	4

Verbindungsblockierung – Aktion

Bei der Verbindungsblockierung werden Informationen zum Blockieren einer Verbindung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aufheben von Verbindungsblockierungen – Aktion

Beim Aufheben von Verbindungsblockierungen werden Informationen zum Aufheben der Blockierung einer Verbindung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Host-Blockierung – Aktion

Bei der Host-Blockierung werden Informationen zum Blockieren eines Hosts ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aufheben von Host-Blockierungen – Aktion

Beim Aufheben von Host-Blockierungen werden Informationen zum Aufheben der Blockierung eines Hosts ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Netzwerkzugriffsbenachrichtigung"

Die Aktion "Netzwerkzugriffsbenachrichtigung" gibt Informationen zu generischen Netzwerkzugriffsbenachrichtigungen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Netzwerkblockierung – Aktion

Bei der Netzwerkblockierung werden Informationen zum Blockieren eines Netzwerks ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aufheben von Netzwerkblockierungen – Aktion

Beim Aufheben von Netzwerkblockierungen werden Informationen zum Aufheben der Blockierung eines Netzwerks ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktivieren der Geschwindigkeitsbegrenzung – Aktion

Beim Aktivieren der Geschwindigkeitsbegrenzung werden Informationen zur Aktivierung von Geschwindigkeitsbegrenzungen für den Netzwerkverkehr ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Deaktivieren der Geschwindigkeitsbegrenzung – Aktion

Beim Deaktivieren der Geschwindigkeitsbegrenzung werden Informationen zur Deaktivierung von Geschwindigkeitsbegrenzungen für den Netzwerkverkehr ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse der Antivirusaktivität

Vertrauensbeziehung widerrufen – Aktion

Bei der Aktion "Vertrauensbeziehung widerrufen" werden Informationen zum Entfernen von vertrauenswürdigen Beziehungen zwischen IT-Komponenten oder Systemen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Klasse der Anwendungssicherheit

Pufferüberlaufangriff

Beim Pufferüberlaufangriff werden Ereignisinformationen zur Erfassung eines Pufferüberlaufangriffs angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	6

Ergebnis	event_result	event_severity
Fehler	F	5
Versuch	A	5

E-Mail-Server-Exploit

Mit der Aktion "E-Mail-Server-Exploit" werden Ereignisinformationen zu Angriffen, die Schwachstellen in E-Mail-Servern ausnutzen, angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Aktion "Angriff über Quellcodezugriff"

Mit der Aktion "Angriff über Quellcodezugriff" werden Ereignisinformationen zu Angriffen auf Webserver, die dynamische Seiten verarbeiten, angezeigt. Mit dem Angriff wird versucht, auf Quellcode zuzugreifen, um u. a. Installationsinformationen, wie Benutzer-IDs und Kennwörter zu erhalten, und somit auf Datenbanken zugreifen zu können. Diese Art von Angriff kann durch das Ausgeben einer bestimmten URL durchgeführt werden, die der Server nicht korrekt verarbeiten kann oder den Server einige Software-Komponenten ausführen lässt, die Fehler enthalten können.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

E-Mail-Exploit

Beim E-Mail-Exploit werden Ereignisinformationen in Zusammenhang mit der Erkennung von Exploits in einem E-Mail-System ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Remote-Exploit

Beim Remote-Exploit werden Ereignisinformationen zur Erkennung eines Angriffs über eine Netzwerkverbindung ohne vorherigen Zugriff auf das anfällige System angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	6
Fehler	F	5

Ergebnis	event_result	event_severity
Versuch	V	5

Ausführung von Spezialbefehl

Ausführung von Spezialbefehl drückt Ereignisinformationen zur Ausführung von Systemaufrufen oder Spezialbefehlen aus.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	4
Fehler	F	4
Versuch	V	4

Software-Exploit

Vorhandene Aktion: Sie wird je nach Kontext den CEG-Klassen für Denial of Service (DoS) oder Anwendungssicherheit zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Fehler	F	5

Webanwendungsaktivität

Bei Webanwendungsaktivitäten werden Ereignisinformationen in Zusammenhang mit Zugriffen auf eine potenziell anfällige Webanwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	5

Webanwendungsangriff

Bei einem Webanwendungsangriff werden Ereignisinformationen zur Erkennung eines Angriffs auf Webanwendungen ausgegeben. (Z. B. bei einem Directory-Traversal-Versuch)

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Fehler	F	5
Versuch	A	5

Web-Exploit

Der Webbrowser-Exploit betrifft alle Aktivitäten, bei denen versucht wird, Browserschwachstellen auszunutzen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Fehler	F	5

Klasse für Zertifikatsaktivität

Zertifikatalarm – Aktion

Beim Zertifikatalarm werden Informationen über Alarmbedingungen ausgegeben, die während einer Zertifikataktivität oder im Zusammenhang mit digitalen Zertifikaten auftreten.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Zertifikatexport

Beim Zertifikatexport wird ein Zertifikat in eine Datei exportiert.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Ergebnis	event_result	event_severity
Fehler	F	3

Zertifikatsablauf

Der Zertifikatsablauf betrifft den Ablauf eines Zertifikats.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatfehler

Zertifikatfehler betreffen Fehler in Zusammenhang mit allgemeinen Zertifizierungsaktivitäten wie z. B. dem Empfang eines leeren Zertifikats.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatserstellung

Bei der Zertifikatserstellung wird ein neues Zertifikat erstellt.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatoperation – Aktion

Bei der Zertifikatoperation werden allgemeine Informationen zu Zertifikaten und zur Zertifikataktivität ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatimport

Beim Zertifikatimport wird ein Zertifikat aus einer Datei importiert.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatsinitialisierung

Bei der Zertifikatsinitialisierung werden erworbene Zertifikate initialisiert.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatbenachrichtigung – Aktion

Bei der Zertifikatbenachrichtigung werden Informationen zu Benachrichtigungen und Meldungen ausgegeben, die anhand der Zertifikataktivität oder durch die Zertifikatinfrastruktur generiert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatssperrung

Die Festlegung der Zertifikatssperrliste betrifft die regelmäßige Ausstellung einer Zertifikatssperrliste (Certificate Revocation List, CRL) durch die Zertifizierungsstelle (Certificate Authority, CA).

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatssperrlistenalarm – Aktion

Beim Zertifikatssperrlistenalarm werden Informationen zu Alarmen in Verbindung mit Zertifikatssperrlisten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Zertifikatssperrlistenfehler – Aktion

Bei der Aktion "Zertifikatssperrlistenfehler" werden Informationen zu Fehlern in Verbindung mit Zertifikatssperrlisten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Zertifikatssperrlistenablauf

Der Zertifikatssperrlistenablauf betrifft Aktivitäten in Zusammenhang mit dem Ablauf einer Zertifikatssperrliste (Certificate Revocation List, CRL). Beispielsweise läuft eine CRL ab, wenn der Zertifizierungsstellenschlüssel geändert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Tertiär
Ereignisquelle - Informationen	Primär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche CRL-Aktivitäten auf welchem Host stattfinden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatssperrlistenimport

Beim Zertifikatssperrlistenimport wird eine Zertifikatssperrliste (Certificate Revocation List, CRL) für ein Gerät oder eine Anwendung importiert. Beispiel: Import einer CRL in eine Internetbrowser-Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	4

Zertifikatssperrlistenbenachrichtigung – Aktion

Bei der Zertifikatssperrlistenbenachrichtigung werden allgemeine Informationen zu Benachrichtigungen in Verbindung mit Zertifikatssperrlisten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatssperrlistenoperation – Aktion

Bei der Zertifikatssperrlistenoperation werden allgemeine Informationen zu Zertifikatssperrlistenoperation ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatssperrlistenerneuerung

Bei einer Zertifikatssperrlistenerneuerung wird eine Zertifikatssperrliste (Certificate Revocation List, CRL) durch die Zertifizierungsstelle (Certificate Authority, CA) erneuert.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatssperrlistenstatus – Aktion

Beim Zertifikatssperrlistenstatus werden Informationen zum Status von Zertifikatssperrlisten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatssperrlistenvalidierung

Die Zertifikatssperrlistenvalidierung betrifft alle Aktivitäten, die mit der Validierung einer Zertifikatssperrliste (Certificate Revocation List, CRL) in Zusammenhang stehen. Beispielsweise bei einer CRL mit einem ungültigen Zeitstempel.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	4

Zertifikatssperrlistenwarnung – Aktion

Bei der Zertifikatssperrlistenwarnung werden Informationen zu Warnungen im Zusammenhang mit Zertifikatlisten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Zertifikatserneuerung

Bei der Zertifikatserneuerung erfolgt die Erneuerung von Zertifikaten nach Ablauf des Gültigkeitszeitraums unter Verwendung eines neuen oder vorhandenen Schlüsselpaares.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatsanforderung

Bei der Zertifikatsanforderung (auch als Zertifikatsignieranforderung bezeichnet) wird eine Meldung an eine Zertifizierungsstelle (Certificate Authority, CA) gesendet, um ein digitales Identitätszertifikat zu beantragen. Dieser Vorgang kann manuell oder automatisch erfolgen.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Sperren eines Zertifikats

Beim Sperren eines Zertifikats geht es um die Zertifikatssperrung. Zertifikate können von der Zertifizierungsstelle (Certificate Authority, CA) gesperrt werden, beispielsweise bei unsicheren Zertifikaten, verlorenen Token, die private Schlüssel enthalten, usw.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	4

Zertifikatstatus – Aktion

Bei der Aktion "Zertifikatstatus" werden Informationen zum Zertifikatstatus ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatssuspendierung

Bei der Zertifikatssuspendierung wird ein Zertifikat suspendiert. Eine Suspendierung ist nur mit OCSP möglich, wobei die Validierung in Echtzeit erfolgt. Eine CRL (Zertifikatssperrliste) wird nur für gesperrte Zertifikate verwendet.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatsperrung aufheben – Aktion

Bei der Aktion "Zertifikatsperrung aufheben" werden Informationen zur Rückgängigmachung einer Zertifikatsperrung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatsvalidierung

Bei der Zertifikatsvalidierung wird ein Zertifikat anhand der Zertifikatssperrliste (Certificate Revocation List, CRL) oder des Online Certificate Status-Protokolls (OCSP) validiert.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Zertifikatwarnung – Aktion

Bei der Zertifikatwarnung werden Informationen zu Warnungen ausgegeben, die von einer Zertifikataktivität oder -Infrastruktur generiert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Vertrauensbeziehung herstellen – Aktion

Bei der Aktion "Vertrauensbeziehung herstellen" werden Informationen zur Herstellung vertrauenswürdiger Beziehungen zwischen IT-Komponenten oder Systemen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse der Verbindungsaktivität

Zertifikat-Rollover – Aktion

Beim Zertifikat-Rollover wird ein Rollover eines Zertifikats durchgeführt, indem ein neues Zertifikat erstellt wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Bei dieser Aktion ist es von Bedeutung, für welchen Host das Zertifikat-Rollover durchgeführt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verbindungsbenachrichtigung

Mit der Aktion "Verbindungsbenachrichtigung" werden Informationen zu Benachrichtigungen und Meldungen, die von einer bereits vorhandenen Verbindung zwischen zwei Netzwerkentitäten erstellt wurden, angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Schlüsselaustauschphase 1 – Verhandlung"

Mit der Aktion "Schlüsselaustauschphase 1 – Verhandlung" werden Ereignisinformationen über Verhandlungen in der Phase 1 für die Einrichtung von SAs (Sicherheitszuordnungen) angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Tunnelvorgang"

Mit der Aktion "Tunnelvorgang" werden Informationen zu Vorgängen im Zusammenhang mit Netzwerkverbindungstunneln angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Zertifikat-Alert"

Die Aktion "Zertifikat-Alert" gibt Informationen zu Alert-Bedingungen in Verbindung mit Netzwerkverbindungen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Verbindungsversuch

Beim Verbindungsversuch werden Ereignisinformationen zum Verbindungsversuch zwischen zwei Netzwerkentitäten angezeigt, die auf einem bestimmten Host aufgezeichnet werden. Für diese Aktion gibt es drei mögliche Ergebnisse: A für "Akzeptieren" der Verbindung, D für stilles "Unterbrechen" der Verbindung und R für "Ablehnen" (oder Verweigern) des Verbindungsversuchs.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Host mit welchem Host versucht zu verbinden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Akzeptieren	A	2

Ergebnis	event_result	event_severity
Unterbrechen	D	3
Ablehnen	-r	3

Verbindungswiederherstellung

Beim Verbindungsversuch werden Ereignisinformationen zur Wiederherstellung einer Verbindung zwischen zwei Netzwerkentitäten angezeigt, die auf einem bestimmten Host aufgezeichnet werden. Für diese Aktion gibt es zwei mögliche Ergebnisse: S für "Erfolgreich" und F für "Fehler" (fehlerhafte Wiederherstellung). Die Wiederherstellung einer Verbindung tritt häufig auf, wenn sich Teile der Host-Informationen, wie z. B. NAT-Szenario, ändern.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Host beim Wiederherstellen der Verbindung versucht, eine Verbindung mit welchem Host herzustellen. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verbindungsanforderung

Bei der Verbindungsanforderung werden Ereignisinformationen zur Anforderung einer Verbindung zwischen zwei Netzwerkentitäten, die auf einem bestimmten Host aufgezeichnet werden, angezeigt. Die Anforderung einer Verbindung ist ein sehr detailliertes Teil der Debug-Informationen und wird in der Regel nicht benötigt, wenn der Verbindungsversuch für dieselbe Verbindung aufgezeichnet wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Host beim Wiederherstellen der Verbindung versucht, eine Verbindung mit welchem Host herzustellen. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Verbindungsstatus

Beim Verbindungsstatus werden Ereignisinformationen zum Status einer Verbindung zwischen zwei Netzwerkentitäten, die auf einem bestimmten Host aufgezeichnet werden, angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Host eine Verbindung mit welchem anderen Host hergestellt wurde, und von welchem Host die Informationen aufgezeichnet wurden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Verbindungsbeendigung

Bei der Verbindungsbeendigung werden Ereignisinformationen zur Beendigung einer zuvor aufgebauten Verbindung zwischen zwei Netzwerkentitäten angezeigt, die auf einem bestimmten Host aufgezeichnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, zwischen welchen beiden Hosts die Verbindung beendet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Verbindungswarnung – Aktion

Bei einer Verbindungswarnung werden Informationen im Zusammenhang mit der Erkennung allgemeiner Fehler bei einer Verbindung zwischen zwei Netzwerkentitäten auf einem bestimmten Host angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Fehler auf welchen Verbindungen gefunden werden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Starten der Schlüsselaustauschphase 1

Beim Starten der Schlüsselaustauschphase 1 werden Ereignisinformationen zum Starten einer IKE-Verhandlung für eine IPSEC-Verbindung zwischen zwei Netzwerkentitäten auf einem bestimmten Host angezeigt. Für diese Aktion gibt es zwei mögliche Ergebnisse: S für "Erfolgreich" und F für "Fehler".

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Host eine IKE-Verhandlung mit welchem Host versucht zu starten. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Protokollalarm – Aktion

Bei der Aktion "Protokollalarm" werden Informationen zu sämtlichen Typen von Protokollalarmen ausgegeben. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Protokollfehler" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär

Informationen	Ebene
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Port-Blockierung – Aktion

Bei der Aktion "Port-Blockierung" werden Informationen ausgegeben, die die Blockierung von Netzwerk- oder Kommunikationsports zur Filterung des Datenverkehrs betreffen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Protokollfehler – Aktion

Bei der Aktion "Protokollfehler" werden Informationen zu protokollbezogenen Fehlerbedingungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Port-Weiterleitung – Aktion

Bei der Port-Weiterleitung werden Ereignisinformationen zur Weiterleitung von Ports ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Bei dieser Aktion ist es von Bedeutung, welcher Port weitergeleitet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Protokolloperation – Aktion

Bei der Aktion "Protokolloperation" werden allgemeine Informationen zu Protokolloperationen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Protokollstatus – Aktion

Bei der Aktion "Protokollstatus" werden Informationen zum Status von Protokolloperationen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Protokollwarnung – Aktion

Bei der Aktion "Protokollwarnung" werden Fehlerinformationen zu Protokolloperationen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Protokollbenachrichtigung

Bei Protokollbenachrichtigungen werden Informationen zu Benachrichtigungen, Meldungen sowie Statusaktualisierungen von einem beliebigen Netzwerkprotokoll ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Ergebnis	event_result	event_severity
Fehler	F	3

Ablauf der Sicherheitszuordnung

Beim Ablauf der Sicherheitszuordnung werden Ereignisinformationen im Zusammenhang mit dem Ablauf einer Sicherheitszuordnung angezeigt, die eine IPSEC-Verbindung zwischen zwei Netzwerkelementen auf einem bestimmten Host definiert. Für diese Aktion gibt es zwei mögliche Ergebnisse: E für "Erfolgreich" und F für "Fehler".

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, vom Ablauf welcher Sicherheitszuordnung die Verbindung zwischen welchen beiden Hosts betroffen ist. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Anfordern einer Sicherheitszuordnung

Beim Anfordern einer Sicherheitszuordnung werden Ereignisinformationen im Zusammenhang mit der Herstellung einer Sicherheitszuordnung angezeigt, die eine IPSEC-Verbindung zwischen zwei Netzwerkelementen auf einem bestimmten Host definiert. Für diese Aktion gibt es zwei mögliche Ergebnisse: E für "Erfolgreich" und F für "Fehler".

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Sicherheitszuordnung für die Verbindung zwischen welchen beiden Hosts angefordert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Viren-Scan – Aktion

Beim Viren-Scan werden Informationen zum Scannen oder erneuten Scannen eines Objekts ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Bei dieser Aktion ist es von Bedeutung, welches Objekt gescannt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse der Verletzung der Unternehmensrichtlinien

Inhaltsaustausch

Beim Inhaltsaustausch werden Ereignisinformationen zur Erfassung eines Inhaltsaustauschs angezeigt. (Beispiel: Hochladen von Dateien mit Hilfe von IM)

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	5
Fehler	F	4
Versuch	A	4

Unzulässiger Inhalt

Beim unzulässigen Inhalt werden Ereignisinformationen zur Erkennung von unzulässigen Daten angezeigt. (Beispiel: Dateien mit anstößigen Bildern)

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Erkennung verdächtiger Software

Bei der Erkennung verdächtiger Software geht es um das Erkennen verdächtiger Software.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	5

Verwendung von Chatprogrammen

Bei Verwendung von Chatprogrammen werden Ereignisinformationen zur Verwendung von Chatprotokollen und -programmen (z. B. AIM, ICQ und IRC) ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär

Informationen	Ebene
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4

P2P-Client-Verwendung

Bei der P2P-Client-Verwendung werden Ereignisinformationen zur Verwendung von P2P-Clients ausgegeben. (Z. B. die Verwendung von P2P-Clients wie Napster oder Skype)

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Verwendung von Streaming Multimedia-Technologien

Bei der Verwendung von Streaming Multimedia-Technologien werden Ereignisinformationen zur Verwendung dieser Technologien ausgegeben. (Z. B. bei der Nutzung von RealPlayer, YouTube usw. durch Mitarbeiter)

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär

Informationen	Ebene
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4

DoS-Klasse

Anwendungs-Exploit

Beim Anwendungs-Exploit werden Ereignisinformationen zur Erkennung von Angriffsaktivitäten angezeigt, durch die Schwachstellen bei der Implementierung von Enterprise-Anwendungen ausgenutzt werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär

Informationen	Ebene
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	5
Versuch	A	4

Bandbreiten-Erschöpfungsangriff

Beim Bandbreiten-Erschöpfungsangriff werden Ereignisinformationen zur Erfassung von Angriffen angezeigt, die verschiedene Flooding-Techniken zum Überhäufen eines Netzwerks zur DOS-Erstellung einsetzen. (Beispiel: Smurf, Überladen der Datenleitung)

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Versuch	A	6

Pufferüberlauf

Vorhandene Aktion: Sie wird je nach Kontext den CEG-Klassen für Denial of Service (DoS) oder Anwendungssicherheit zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Fehler	F	5

Datenbank-Exploit

Beim Datenbank-Exploit werden Ereignisinformationen zur Erkennung von Angriffsaktivitäten angezeigt, durch die Schwachstellen in Datenbankservern ausgenutzt werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	5
Versuch	A	4

Verteilte Angriffsaktion

Bei der verteilten Angriffsaktion werden Ereignisinformationen zur Erkennung von verteilten Angriffsaktivitäten angezeigt (z. B. Ddos mit Hilfe von Bots).

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Versuch	A	6

Firmware-Exploit

Der Firmware-Exploit betrifft alle Signaturaktivitäten, bei denen versucht wird, Firmwareschwachstellen auszunutzen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Fehler	F	5

Fragmentierungsangriff

Beim Fragmentierungsangriff werden Ereignisinformationen zur Erkennung einer Angriffsaktivität, bei der die Paketfragmentierung involviert ist (Beispiel: IP-Fragmentierungsangriffe, Tear-Drop-Angriff), angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Versuch	A	6

Fehlerhafter Paketangriff

Beim fehlerhaften Paketangriff werden Ereignisinformationen zur Erfassung von fehlerhaften Netzwerkdatenpaketen, wie z. B. IP und TCP, angezeigt. (Beispiel: Land-Angriff, Christbaum-Angriff)

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Versuch	A	6

Angriff auf Netzwerkverbindungen

Beim Angriff auf Netzwerkverbindungen werden Ereignisinformationen zur Erkennung von Angriffsaktivitäten angezeigt, durch die Schwachstellen in den Netzwerkverbindungen ausgenutzt werden. (Beispiel: SYN Flood)

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	5
Versuch	A	4

Betriebssystem-Exploit

Beim Betriebssystem-Exploit werden Ereignisinformationen zur Erkennung von Angriffsaktivitäten angezeigt, durch die Schwachstellen in der Betriebssystem-Software ausgenutzt werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	6
Versuch	V	5

Protokoll-Exploit

Beim Protokoll-Exploit werden Ereignisinformationen zur Erkennung von Angriffsaktivitäten angezeigt, durch die die Schwachstellen eines bestimmten Protokolls wie "ssh", "ftp" oder "telnet" ausgenutzt werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	5
Versuch	V	4

Ressourcenerschöpfungsangriff

Ressourcenerschöpfungsangriff drückt Ereignisinformationen zur Erkennung von Angriffsaktivitäten aus, mit denen die Ressourcen auf einem Gerät oder Host erschöpft werden sollen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	5
Versuch	V	4

Software-Exploit

Beim Software-Exploit werden Ereignisinformationen zur Erkennung von Angriffsaktivitäten angezeigt, durch die Schwachstellen in Anwendungssoftware ausgenutzt werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	5
Versuch	V	4

Webserver-Exploit

Bei einem verteilten Angriff werden Ereignisinformationen zur Erkennung von Angriffsaktivitäten angezeigt, durch die Schwachstellen von Webserver-Software ausgenutzt werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Versuch	A	5

Drahtlosverbindungsangriff

Bei einem Drahtlosverbindungsangriff werden Ereignisinformationen zur Erkennung von Angriffsaktivitäten angezeigt, durch die Schwachstellen von Drahtloshardware sowie -software ausgenutzt werden. (Z. B. Deauth-Angriff, Rogue-WAP)

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	5
Versuch	A	4

Klasse für Verschlüsselungsaktivität

Aktion "Kryptografischer Alarm"

Die Aktion "Kryptografischer Alarm" beschreibt Informationen zu Alarmbedingungen im Zusammenhang mit kryptografischen Vorgängen oder Kryptosystemen in einer bestimmten Hostumgebung.

Jeder Typ von Alarm in Bezug auf kryptografische Vorgänge oder Kryptosysteme kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Kryptografischer Fehler" zugeordnet. Wenn sich die Aktion auf Netzwerkumgebungen bezieht, wird sie demselben Ereignis unter der Kategorie "Netzwerksicherheit" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V

Ergebnis	event_result	event_severity
Fehler	F	6

Aktion "Kryptografischer Fehler"

Die Aktion "Kryptografischer Fehler" beschreibt Informationen zu Fehlerbedingungen im Zusammenhang mit kryptografischen Vorgängen oder Kryptosystemen in einer bestimmten Hostumgebung.

Jeder Fehlertyp in Bezug auf kryptografische Vorgänge oder Kryptosysteme kann dieser Aktion zugeordnet werden. Weniger kritische Ereignisse sollten den Aktionen "Kryptografischer Vorgang" oder "Kryptosystem-Warnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "Kryptografischer Alarm" zugeordnet werden. Wenn sich die Aktion auf Netzwerkumgebungen bezieht, wird sie demselben Ereignis unter der Kategorie "Netzwerksicherheit" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	5

Aktion "Kryptografische Benachrichtigung"

Die Aktion "Kryptografische Benachrichtigung" enthält Informationen zu Benachrichtigungen und Meldungen, die mithilfe von kryptografischen Vorgängen oder Kryptosystemen in einer bestimmten Hostumgebung generiert wurden.

Jeder Typ von Benachrichtigung zu kryptografischen Vorgängen oder Kryptosystemen kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "Kryptografischer Status", wenn das Ereignis den Status von kryptografischen Vorgängen oder Kryptosystemen beschreibt. Wenn sich die Aktion auf Netzwerkumgebungen bezieht, wird sie demselben Ereignis unter der Kategorie "Netzwerksicherheit" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Kryptografischer Vorgang"

Die Aktion "Kryptografischer Vorgang" beschreibt Informationen zu allgemeinen Vorgängen der Funktionsweise von Kryptosystemen in einer bestimmten Hostumgebung.

Wenn ein Ereignis als Teil des kryptografischen Vorgangs oder der normalen Funktionen des Kryptosystems aufgezeichnet ist oder das Ereignis keiner spezifischeren CEG-Aktion zugeordnet werden kann, können Sie es dieser Aktion zuordnen. Wenn sich die Aktion auf Netzwerkumgebungen bezieht, wird sie demselben Ereignis unter der Kategorie "Netzwerksicherheit" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Kryptografischer Status"

Die Aktion "Kryptographischer Status" beschreibt Informationen im Zusammenhang mit dem Status von kryptographischen Vorgängen oder Kryptosystemen in einer bestimmten Hostumgebung.

Wenn ein Ereignis als Teil der normalen Funktionen in kryptografischen Vorgängen oder Kryptosystemen aufgezeichnet wird, oder wenn sich ein Ereignis nicht präziser einer bestimmten CEG-Aktion zuordnen lässt, kann es dieser Aktion zugeordnet werden. Wenn sich die Aktion auf Netzwerkumgebungen bezieht, wird sie demselben Ereignis unter der Kategorie "Netzwerksicherheit" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Kryptografische Warnung"

Die Aktion "Kryptografische Warnung" beschreibt Informationen zu Warnungen im Zusammenhang mit kryptografischen Vorgängen oder Kryptosystemen in einer bestimmten Hostumgebung.

Jeder Warnungstyp in Bezug auf kryptografische Vorgänge oder Kryptosysteme kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Kryptografischer Fehler" zugeordnet werden. Wenn sich die Aktion auf Netzwerkumgebungen bezieht, wird sie demselben Ereignis unter der Kategorie "Netzwerksicherheit" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	4

Aktion "Entschlüsselungsvorgang"

Die Aktion "Entschlüsselungsvorgang" beschreibt Informationen im Zusammenhang mit allgemeinen Entschlüsselungsvorgängen auf einem Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Entschlüsselungsstatus"

Die Aktion "Entschlüsselungsstatus" beschreibt Informationen zum Entschlüsselungsstatus auf einem Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Schlüsselerstellung

Mit der Aktion "Schlüsselerstellung" werden Informationen zur Erstellung von Verschlüsselungscodes oder Schlüsselpaaren für die Netzwerkauthentifizierung oder Verschlüsselung angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Erstellung digitaler Signaturen

Die Erstellung digitaler Signaturen betrifft die digitale Signatur von Meldungen für die Sicherstellung der Integrität und Authentifizierung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verschlüsselungsalarm – Aktion

Beim Verschlüsselungsalarm werden Informationen zu Verschlüsselungsalarmen ausgegeben, die die Netzwerkebene betreffen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Verschlüsselungsfehler

Verschlüsselungsfehler betreffen Informationen in Zusammenhang mit allgemeinen Verschlüsselungsfehlern, einschließlich Fehlern bei der Schlüsselverwaltung und beim Transport.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verschlüsselungsbenachrichtigung – Aktion

Bei der Verschlüsselungsbenachrichtigung werden Informationen zu Benachrichtigungen und Meldungen ausgegeben, die von einer Verschlüsselungs-Engine auf einem Gerät oder in einem Netzwerk generiert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verschlüsselungsoperation – Aktion

Bei der Aktion "Verschlüsselungsoperation" werden allgemeine Informationen zu Verschlüsselungsoperationen in einem Netzwerk ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verschlüsselungsstatus – Aktion

Bei der Aktion "Verschlüsselungsstatus" werden Informationen zum Status von Verschlüsselungsaktivitäten in einem Netzwerk ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verschlüsselungswarnung – Aktion

Bei der Verschlüsselungswarnung werden Informationen zu Verschlüsselungswarnungen ausgegeben, die die Netzwerkebene betreffen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	3

Klasse des Informationsverlusts

Dekodieren einer RPC-Abfrage

Beim Dekodieren einer RPC-Abfrage werden Ereignisinformationen zur Erkennung einer RPC-Portmap-Abfrage angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Ergebnis	event_result	event_severity
Fehler	F	4
Versuch	A	4

Aktion "Angriff durch Einschleusung von SQL-Befehlen"

Mit der Aktion "Angriff durch Einschleusung von SQL-Befehlen" wird das Löschen von Sicherheitsbereichen zur Verwaltung einer Asset-Gruppe mit einer vereinheitlichten Sicherheitsrichtlinie aufgezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Missbrauch von berechtigtem Zugriff

Beim Missbrauch von berechtigtem Zugriff werden Ereignisinformationen zur Erkennung von Missbrauch der Zugriffsberechtigungen angezeigt. (Beispiel: Herunterladen von Finanzdaten auf dem Desktop).

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	5
Fehler	F	4
Versuch	A	4

Reconnaissance-Aktivität

Reconnaissance-Aktivitäten betreffen alle Aktivitäten, die mit der Netzwerk-Reconnaissance (Netzwerk-Aufklärung) in Zusammenhang stehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Fehler	F	5

Aktivität von Trojanern und Backdoor-Programmen

Bei Aktivität von Trojanern und Backdoor-Programmen werden Ereignisinformationen zur Aktivität von Trojanern und Backdoor-Programmen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	6

Schwachstellenscan

Beim Schwachstellenscan werden Ereignisinformationen zur Erkennung von Scanaktivitäten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	5
Fehler	F	4
Versuch	A	4

Klasse für Malware-Aktivität

Trojaner- und Backdoor-Programmaktivität

Die Adware-Erkennung betrifft Aktivitäten, die mit der Erkennung von Adware in Zusammenhang stehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	6

Spyware-Erkennung

Die Spyware-Erkennung betrifft Aktivitäten, die mit der Erkennung von Spyware in Zusammenhang stehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	6

Wurmerkennung

Die Wurmerkennung betrifft Aktivitäten, die mit der Erkennung von Wurmaktivitäten in Zusammenhang stehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	6

Trojaner- und Backdoor-Programmaktivität

Vorhandene Aktion: Sie wird je nach Kontext den CEG-Klassen für Malware-Aktivität oder Informationsverlust zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	6

Aktion "Klasse der Netzadressverwaltung"

Aktion "Erstellen von Multicast-Gruppen"

Mit der Aktion "Erstellen von Multicast-Gruppen" werden Ereignisinformationen zur Erstellung einer Multicast-Gruppe angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2

Ergebnis	event_result	event_severity
Fehler	F	3

Aktion "Löschen von Multicast-Gruppen"

Mit der Aktion "Löschen von Multicast-Gruppen" werden Ereignisinformationen zur Löschung einer Multicast-Gruppe angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Ändern von Multicast-Gruppen"

Mit der Aktion "Ändern von Multicast-Gruppen" werden Ereignisinformationen zur Änderung einer Multicast-Gruppe inklusive Änderungen der Mitgliedschaft angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Klasse für Berechtigungseskalation

Administratorberechtigungserlangung

Die Administratorberechtigungserlangung behandelt den Ausdruck von Ereignisinformationen, die zu der Erfassung von Aktivitäten für die Berechtigungserlangung des Administratorkontos gehören. (Beispiel: Brute-Force-Angriff auf ein Administratorkonto)

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Fehler	F	5
Versuch	A	5

Zugriffssteuerungsumgehung

Die Zugriffssteuerungsumgehung betrifft alle Signaturaktivitäten, bei denen versucht wird, Zugriffsbeschränkungen durch die Veränderung von Berechtigungen oder mit Hilfe anderer Maßnahmen zu umgehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Fehler	F	5

Benutzerberechtigungserlangung

Bei der Benutzerberechtigungserlangung werden Ereignisinformationen zur Erkennung von Aktivitäten angezeigt, die mit der Erlangung von Berechtigungen für ein anderes Benutzerkonto in Zusammenhang stehen. (Z. B. Brute-Force-Angriff auf ein SQL-Konto mit umfassenderen Berechtigungen)

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3
Versuch	A	3

Aktion "Routing-Aktivitätsklasse"

Aktion "Routing-Setup"

Mit der Aktion "Routing-Setup" werden Ereignisinformationen zum Einrichten von Routen durch manuelle oder automatische Vorgänge angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Klasse für Signaturverletzungen

Signaturverletzung

Bei der Signaturverletzung werden Ereignisinformationen zur Entdeckung einer verletzenden Verbindung zwischen zwei Netzwerkelementen auf einem bestimmten Host angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	6

Klasse für verdächtige Aktivität

Erkennung eines nicht standardisierten Protokolls

Bei der Erkennung eines nicht standardisierten Protokolls werden Ereignisinformationen zur Erkennung eines nicht standardisierten Protokolls angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Erkennung eine ungewöhnlichen Ports

Bei der Erkennung eines ungewöhnlichen werden Ereignisinformationen zur Erkennung eines ungewöhnlichen Ports angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Erkennung von ausführbaren Codes

Bei der Erkennung von ausführbaren Codes werden Ereignisinformationen zur Erkennung von ausführbaren Codes im Netzwerkdatenverkehr angezeigt. (Beispiel: Angreifer, die einen beliebigen Code ausführen)

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	5

Sonstige Angriffe

Bei der Aktion "Sonstige Angriffe" werden Ereignisinformationen zur Erkennung einer verdächtigen Aktivität angezeigt, die keiner bestehenden in CEG definierten IDS-Aktion zugeordnet werden können.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	5
Versuch	A	4

Aktion "Angriff über Namensdienst"

Mit der Aktion "Angriff über Namensdienst" werden Ereignisinformationen zu den Namensdienstkomponenten des Angriffs angezeigt.

DNS-Angriffe sowie Missbrauch ihres DNS und Weiterleitungen können dieser Aktion zugewiesen werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Aktion "Netzwerkaufzählung"

Die Aktion "Netzwerkaufzählung" gibt erkannte Hosts und Geräte in einem Netzwerk an.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Aktion "Netzwerk-Exploit"

Mit der Aktion "Netzwerk-Exploit" werden Ereignisinformationen zu ausgenutzten Schwachstellen in Netzwerken, Prozessen oder Frameworks angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Aktion "Portangriff"

Mit der Aktion "Portangriff" werden Ereignisinformationen zur Nutzung von offenen Ports angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Aktion "URL-Exploit"

Mit der Aktion "URL-Exploit" werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit URLs angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär

Informationen	Ebene
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	5
Fehler	F	4

Aktion "VOIP-Angriff"

Mit der Aktion "VOIP-Angriff" werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit VOIP angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär

Informationen	Ebene
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	6
Fehler	F	5

Aktion "Ping-Scan"

Die Aktion "Ping-Scan" gibt Informationen zum Scannen der Hosts auf dem Netzwerk.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	3
Fehler	F	3

Port-Scan – Aktion

Beim Port-Scan werden Informationen zur Prüfung des Netzwerkhosts auf offene Ports ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	4

Möglicher Brute-Force-Angriff

Bei einem möglichen Brute-Force-Angriff handelt es sich um Aktivitäten, die auf die Möglichkeit eines Brute-Force-Angriffs hinweisen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	5
Fehler	F	5

Protokoll-Exploit

Vorhandene Aktion: Sie wird je nach Kontext den CEG-Klassen für Denial of Service (DoS) oder verdächtige Aktivität zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Fehler	F	5

Erkennung verdächtiger Befehle

Die Erkennung verdächtiger Befehle betrifft IDS-Signaturverletzungen in Zusammenhang mit der Erkennung verdächtiger Befehle im Netzwerkdatenverkehr.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	5

Erkennung verdächtiger Dateinamen

Bei der Erkennung verdächtiger Dateinamen werden Ereignisinformationen zur Erkennung verdächtiger Dateinamen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Signatur für die Verbindung zwischen welchen beiden Hosts zugeordnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Erkennung verdächtiger Zeichenfolgen

Die Erkennung verdächtiger Zeichenfolgen betrifft IDS-Signaturverletzungen in Zusammenhang mit der Erkennung verdächtiger Zeichenfolgen im Netzwerkdatenverkehr.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	5

Erkennung verdächtiger Anmeldungen

Die Erkennung verdächtiger Anmeldungen betrifft IDS-Signaturverletzungen in Zusammenhang mit der Erkennung verdächtiger Anmeldungen im Netzwerkdatenverkehr.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	5

Tunnel-Datenverkehr-Erkennung

Die Tunnel-Datenverkehr-Erkennung betrifft die Erkennung von Tunnel-Datenverkehr (Tunnel Traffic).

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	5

Aktion "Unaufgeforderter Datenverkehr"

Die Aktion "Unaufgeforderter Datenverkehr" gibt Informationen zur Erkennung von unaufgefordert eingehendem Datenverkehr auf dem Netzwerk.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	3
Fehler	F	3

Webserver-Exploit

Vorhandene Aktion: Sie wird je nach Kontext den CEG-Klassen für Denial of Service (DoS) oder verdächtige Aktivität zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Fehler	F	5

Klasse für Webservices-Verwaltung

Meldungsfilterverarbeitung

Bei der Meldungsfilterverarbeitung werden Informationen zur Validierung von XML-Meldungen ausgegeben. Hierzu gehören beispielsweise DTD-Validierungsinformationen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Meldungsfilterverarbeitung

Bei der Meldungsfilterverarbeitung werden Informationen zur Einrichtung von Filtern für die Verarbeitung von XML-Meldungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Änderung von SOAP-Meldungen

Bei der Änderung von SOAP-Meldungen werden Informationen zu SOAP-Meldungsänderungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

XML-Entschlüsselung

Die XML-Entschlüsselung betrifft die Ausgabe von Informationen zur Datenentschlüsselung und Darstellung der Ergebnisse in XML. Bei den Daten kann es sich um beliebige Daten (z. B. ein XML-Dokument), ein XML-Element oder XML-Elementinhalte handeln.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

XML-Verschlüsselung

Die XML-Verschlüsselung betrifft die Ausgabe von Informationen zur Datenverschlüsselung und Darstellung der Ergebnisse in XML. Bei den Daten kann es sich um beliebige Daten (z. B. ein XML-Dokument), ein XML-Element oder XML-Elementinhalte handeln.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

XML-Schemavalidierung

Bei der XML-Schemavalidierung werden Informationen zur Validierung von XML-Daten und -Dokumenten für ein XML-Schema ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Kapitel 10: Kategorie "Betriebssicherheit"

Dieses Kapitel enthält folgende Themen:

Anwendungsverwaltungsklasse

Aktion "Schließen von Anwendungen"

Mit der Aktion "Schließen von Anwendungen" werden Ereignisinformationen zum interaktiven Schließen von Anwendungen angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Anwendungsfehler

Anwendungsfehler betreffen Fehler- oder Ausnahmeereignisse, die während der Ausführung einer Anwendung generiert wurden. Diese Fehler können aufgrund unterschiedlicher Bedingungen auftreten, wie z. B. einer fehlenden oder beschädigten Datei oder einer Laufzeitausnahme.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse der Anwendungsleistungsverwaltung

Aktion "Verbindungsmetrik"

Mit der Aktion "Verbindungsmetrik" werden Ereignisinformationen zur Verfolgung und Überwachung der Leistung oder der Betriebsmetrik sowie der Trends zur Verbindungsverwaltung einer Anwendung angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Verbindungspoolmetrik"

Mit der Aktion "Verbindungspoolmetrik" werden Ereignisinformationen zur Verfolgung und Überwachung der Leistung oder der Betriebsmetrik sowie der Trends zur Verwaltung des Verbindungspools einer Anwendung angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Komponentenmetrik"

Mit der Aktion "Komponentenmetrik" werden Ereignisinformationen zur Verfolgung und Überwachung der Leistung oder der Betriebsmetrik sowie der Trends zur Komponentenaktivität einer Anwendung angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "CPU-Metrik"

Mit der Aktion "CPU-Metrik" werden Ereignisinformationen zur Verfolgung und Überwachung der Leistung oder der Betriebsmetrik sowie der Trends zur CPU-Auslastung einer Anwendung angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Datendurchsatzmetrik"

Mit der Aktion "Datendurchsatzmetrik" werden Ereignisinformationen zur Verfolgung und Überwachung der Leistung oder der Betriebsmetrik sowie der Trends zum Datendurchsatz einer Anwendung angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Ereignismetrik"

Mit der Aktion "Ereignismetrik" werden Ereignisinformationen zur Verfolgung und Überwachung der Leistung oder der Betriebsmetrik sowie der Trends zur Ereigniserstellung einer Anwendung angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Speichermetrik"

Mit der Aktion "Speichermetrik" werden Ereignisinformationen zur Verfolgung und Überwachung der Leistung oder der Betriebsmetrik sowie der Trends zur Speicherauslastung einer Anwendung angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Messaging-Metrik"

Mit der Aktion "Messaging-Metrik" werden Ereignisinformationen zur Verfolgung und Überwachung der Leistung oder der Betriebsmetrik sowie der Trends der Messaging-Aktivität einer Anwendung angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Methodenmetrik"

Mit der Aktion "Methodenmetrik" werden Ereignisinformationen zur Verfolgung und Überwachung der Leistung oder der Betriebsmetrik sowie der Trends zur Methodenausführung einer Anwendung angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Programmmetrik"

Mit der Aktion "Programmmetrik" werden Ereignisinformationen zur Verfolgung und Überwachung der Leistung oder der Betriebsmetrik sowie der Trends bestimmter Programme, die Teil einer übergreifenden Anwendung sind, angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Socket-Metrik"

Mit der Aktion "Socket-Metrik" werden Ereignisinformationen zur Verfolgung und Überwachung der Leistung oder der Betriebsmetrik sowie der Trends der Socket-Aktivitäten einer Anwendung angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Threadpool-Metrik"

Mit der Aktion "Threadpool-Metrik" werden Ereignisinformationen zur Verfolgung und Überwachung der Leistung oder der Betriebsmetrik sowie der Trends zur Verwaltung des Threadpools einer Anwendung angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Sicherungsverwaltungsklasse

Audit-Datensatzerstellung – Aktion

Bei der Audit-Datensatzerstellung werden Informationen zum Erstellen von Audit-Protokolldatensätzen auf einem bestimmten System oder in einer bestimmten Anwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Sekundär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto auf welchem Host ein Protokolldatensatz erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Ergebnis	event_result	event_severity
Fehler	F	3

Aktion "Sicherungs-Alert"

Die Aktion "Sicherungs-Alert" gibt Informationen zu mit Sicherungsvorgängen in Verbindung stehenden Alert-Bedingungen. Sie können dieser Aktion jeden beliebigen Alert-Typ bezüglich Sicherungsvorgängen zuordnen. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, können Sie sie der Aktion "Sicherungsfehler" zuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Abschluss der Sicherung

Der Abschluss der Sicherung betrifft das Beendigungsereignis eines generischen Sicherungsjobs.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto einen Sicherungsjob für welches Objekt auf welchem Host beendet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Sicherungskonfiguration – Aktion

Bei der Sicherungskonfiguration werden Informationen über die Einrichtung von Sicherungsjobs und -Aufgaben ausgegeben. Jeder Typ von Aktion, der Einstellungen für Sicherungsvorgänge festlegt, kann dieser Aktion zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Sicherungsstart

Der Sicherungsstart betrifft das Startereignis eines generischen Sicherungsjobs.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto einen Sicherungsjob für welches Objekt auf welchem Host gestartet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Daten-Snapshot – Aktion

Beim Daten-Snapshot werden Informationen zum Kopieren einer Reihe von Daten, Dateien und Verzeichnissen ausgegeben, deren Stand auf einem bestimmten Zeitpunkt in der Vergangenheit beruht.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Dateisicherung

Die Dateisicherung behandelt Ereignisse, die sich auf die Sicherung einer Dateiressource beziehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto einen Dateisicherungsjob für welches Dateiobjekt auf welchem Host gestartet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Dateiwiederherstellung

Die Dateiwiederherstellung behandelt Ereignisse, die sich auf die Wiederherstellung einer Dateiressource beziehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto einen Dateiwiederherstellungsjob für welches Dateiobjekt auf welchem Host gestartet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Image-Sicherung

Die Image-Sicherung behandelt Ereignisse, die sich auf die Sicherung eines kompletten System-Image beziehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto einen Sicherungsjob für welches Image auf welchem Host gestartet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	4

Image-Wiederherstellung

Die Image-Wiederherstellung behandelt Ereignisse, die sich auf die Wiederherstellung eines kompletten System-Image beziehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto einen Wiederherstellungsjob für welches Image auf welchem Host gestartet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	4

Prozessfehler – Aktion

Bei einem Prozessfehler werden Informationen zu einem Prozess- oder Dienstfehler auf einem bestimmten System oder in einer bestimmten Anwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Sekundär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto auf welchem Host ein Fehler ausgelöst wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Starten der Wiederherstellung

Das Starten der Wiederherstellung betrifft das Startereignis für einen generischen Wiederherstellungs-Job.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto einen Wiederherstellungs-Job für welches Objekt auf welchem Host gestartet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Abschluss der Wiederherstellung

Der Abschluss der Wiederherstellung betrifft das Beendigungsereignis für einen generischen Wiederherstellungs-Job.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto einen Wiederherstellungs-Job für welches Objekt auf welchem Host beendet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Rollback-Operation – Aktion

Bei der Rollback-Operation werden Informationen zu Rollback-Operationen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Domänenverwaltungsklasse

Aktion "Alarm des Domänen-Controllers"

Mit der Aktion "Alarm des Domänen-Controllers" werden Informationen zu Alarmbedingungen im Zusammenhang mit Domänen-Controller angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	6

Aktion "Fehler des Domänen-Controllers"

Mit der Aktion "Fehler des Domänen-Controllers" werden Informationen zu Fehlerbedingungen im Zusammenhang mit Domänen-Controller angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	5

Aktion "Benachrichtigung des Domänen-Controllers"

Mit der Aktion "Benachrichtigung des Domänen-Controllers" werden Informationen zu Benachrichtigungen oder Meldungen angezeigt, die von einem Domänen-Controller generierten wurden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Vorgang des Domänen-Controllers"

Mit der Aktion "Vorgang des Domänen-Controllers" werden Informationen zu allgemeinen Vorgängen des Domänen-Controllers angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Status des Domänen-Controllers"

Mit der Aktion "Status des Domänen-Controllers" werden Informationen zum Status des Domänen-Controllers angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Warnung des Domänen-Controllers"

Mit der Aktion "Warnung des Domänen-Controllers" werden Informationen zu Warnungen im Zusammenhang mit Domänen-Controller angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	4

Aktion "Vertrauensänderung"

Mit der Aktion "Vertrauensänderung" werden Informationen zu Änderungen vorhandener Vertrauensstellungen zwischen zwei Domänen angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Klasse für Prozessaktivität

Sicherungsfehler – Aktion

Bei der Aktion "Sicherungsfehler" werden Informationen zu Sicherungsvorgangsfehlern ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	5

Sicherungsbenachrichtigung – Aktion

Bei der Sicherungsbenachrichtigung geht es um allgemeine Informationen der Sicherungsbenachrichtigung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Sicherungswarnung – Aktion

Bei der Sicherungswarnung werden Informationen zu allgemeinen Sicherungsvorgangswarnungen ausgegeben. Schwerwiegendere Ereignisse werden der Aktion "Sicherungsfehler" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Richtliniensimulation – Aktion

Bei der Richtliniensimulation werden Ereignisinformationen ausgegeben, die von einer Richtliniensimulation generiert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Druckvorgang

Diese Aktion betrifft das Drucken.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Prozesserstellung

Bei der Prozesserstellung werden Informationen zur Erstellung eines Prozesses oder Services auf einem bestimmten System oder in einer bestimmten Anwendung angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer welchen Prozess auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Prozesslöschung

Löschen einer Service-Verknüpfung von der Ausführungsebene.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Prozessänderung

Festlegen der Anfangspriorität eines Prozessbefehls wie "nice" und "renice" unter Unix. Ändern der Anfangspriorität eines Prozessbefehls wie "renice".

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	5
Fehler	F	4

Prozessbenachrichtigung

Bei der Prozessbenachrichtigung werden Informationen zur Benachrichtigung von einem Prozess oder Service auf einem bestimmten Host an einen zweiten Host oder eine zweite Anwendung angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Benachrichtigung von welchem Host an welchen anderen Host gesendet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Verarbeitungsvorgang

Bei Verarbeitungsvorgängen werden Informationen zur Verarbeitung eines Prozesses oder Services auf einem bestimmten Host ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Prozessneustart

Beim Prozessneustart werden Informationen zum Neustart eines Prozesses oder Services auf einem bestimmten System oder in einer bestimmten Anwendung angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer welchen Prozess auf welchem Host neu gestartet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Prozessstart

Beim Prozessstart werden Informationen zum Start eines Prozesses oder Services auf einem bestimmten System oder in einer bestimmten Anwendung angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer welchen Prozess auf welchem Host gestartet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Prozessbeendigung

Bei der Prozessbeendigung werden Informationen zur Beendigung eines Prozesses oder Services auf einem bestimmten System oder in einer bestimmten Anwendung angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer welchen Prozess auf welchem Host beendet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Prozessunterbrechung

Bei der Prozessunterbrechung werden Informationen zur Unterbrechung eines Prozesses oder Services auf einem bestimmten System oder in einer bestimmten Anwendung angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Benutzer welchen Prozess auf welchem Host angehalten hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Prozesswarnung – Aktion

Bei einer Prozesswarnung werden Informationen zu Warnungen ausgegeben, die von einem Prozess oder Dienst auf einem bestimmten System oder in einer bestimmten Anwendung generiert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Systemwarnung – Aktion

Bei der Systemwarnung werden Informationen über Warnmeldungen eines Systems ausgegeben, welche sich auf die Kernfunktionen des Systems beziehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Klasse der Verbindungsaktivität

Sicherheitsprotokoll-Benachrichtigung – Aktion

Bei der Sicherheitsprotokoll-Benachrichtigung werden Informationen zu allgemeinen Sicherheitsprotokoll-bezogenen Meldungen wie Upload- und Download-Protokolle ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Nachricht auf welchem Host gesendet wird. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Ergebnis	event_result	event_severity
Fehler	F	3

Terminalsperrung – Aktion

Bei einer Terminalsperrung werden Informationen zum Sperren eines Terminals auf einem bestimmten System ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Terminal auf welchem Host gesperrt wird. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Ergebnis	event_result	event_severity
Fehler	F	3

Terminalentsperrung – Aktion

Bei einer Terminalentsperrung werden Informationen zum Entsperren eines Terminals auf einem bestimmten System ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Terminal auf welchem Host entsperrt wird. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Ergebnis	event_result	event_severity
Fehler	F	3

Klasse für Geräte- und Portaktivität

Gerätealarm – Aktion

Beim Gerätealarm werden Informationen über Alarmbedingungen im Zusammenhang mit einem Gerät ausgegeben. Bei einem Gerät kann es sich um eine Hardwarekomponente handeln, z. B. ein Netzwerkgerät (Router, Switch, Netzwerkkarte oder Modem). Jeder Typ von Alarm in Bezug auf das Gerät kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Gerätefehler" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	6

Verbindung von Geräten

Aktivitäten in Zusammenhang mit dem Verbinden allgemeiner Geräte (mit Ausnahme von Speichergeräten sowie Eingabegeräten).

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	4

Geräteerstellung – Aktion

Bei der Geräteerstellung werden Informationen über die Erstellung eines Softwaregeräts oder die Installierung eines Hardwaregeräts ausgegeben. Bei einem Gerät kann es sich um eine Hardwarekomponente handeln, z. B. ein Netzwerkgerät (Router, Switch, Netzwerkkarte oder Modem).

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Informationen	Ebene	
Fehler	F	3

Gerätelöschung – Aktion

Bei der Gerätelöschung werden Informationen über die Löschung eines virtuellen Geräts in einer virtualisierten Umgebung ausgegeben. Ein virtuelles Gerät simuliert eine physische Hardwarekomponente, z. B. ein Netzwerkgerät (Router, Switch, Netzwerkkarte oder Modem).

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Geräteänderung – Aktion

Bei der Geräteänderung werden Informationen zur Änderung eines Geräts ausgegeben. Bei einem Gerät kann es sich um eine Hardwarekomponente handeln, z. B. um ein Netzwerkgerät, einen Router, einen Switch, eine Netzwerkkarte oder ein Modem.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Gerätebenachrichtigung – Aktion

Bei der Gerätebenachrichtigung werden Informationen über Benachrichtigungen und Meldungen ausgegeben, die von einem Gerät generiert werden. Bei einem Gerät kann es sich um eine Hardwarekomponente handeln, z. B. ein Netzwerkgerät (Router, Switch, Netzwerkkarte oder Modem). Jeder Typ von Benachrichtigung vom Gerät kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "Gerätestatus", wenn das Ereignis den Status eines Geräts beschreibt.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Geräteoperation – Aktion

Bei der Geräteoperation werden Informationen über allgemeine Operationen im Zusammenhang mit der Funktionsweise eines Geräts ausgegeben. Bei einem Gerät kann es sich um eine Hardwarekomponente handeln, z. B. ein Netzwerkgerät (Router, Switch, Netzwerkkarte oder Modem). Wenn sich ein Ereignis, das im Rahmen einer normalen Gerätefunktion oder -Operation aufgezeichnet wird, nicht präziser einer bestimmten CEG-Aktion zuordnen lässt, kann es dieser Aktion zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Gerätewarnung – Aktion

Bei der Gerätewarnung werden Informationen über Warnungen im Zusammenhang mit einem Gerät ausgegeben. Bei einem Gerät kann es sich um eine Hardwarekomponente handeln, z. B. ein Netzwerkgerät (Router, Switch, Netzwerkkarte oder Modem). Jeder Typ von Warnung in Bezug auf das Gerät kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Gerätewarnung" zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	4

Trennung von Geräten

Aktivitäten in Zusammenhang mit dem Trennen allgemeiner Geräte (mit Ausnahme von Speichergeräten sowie Eingabegeräten).

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	4

Gerätefehler

Alle allgemeinen Gerätefehler.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	4

Gerätebereitstellung

Bereitstellung eines Geräts oder Dateisystems (z. B. NFS-Bereitstellung, Hardwaregeräte)

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	4

Aktion "Gerät anhalten"

Die Aktion "Gerät anhalten" gibt Informationen über temporäres Anhalten eines Geräts.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Gerätezurücksetzung"

Mit der Aktion "Gerätezurücksetzung" werden Informationen zur Zurücksetzung von Geräten auf die ursprüngliche Einstellung oder Konfiguration angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Gerätvorgänge fortsetzen"

Die Aktion "Gerätvorgänge fortsetzen" gibt Informationen über das Fortsetzen der Vorgänge eines Geräts nach temporärer Pause.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Änderung am Gerätestatus"

Mit der Aktion "Änderung am Gerätestatus" werden Informationen zur Änderung des Gerätestatus angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aufhebung der Gerätebereitstellung

Aufhebung der Bereitstellung eines Geräts oder Dateisystems (z. B. NFS-Bereitstellung, Hardwaregeräte)

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	4

Gerätestatus

Alle generischen Meldungen zum Gerätestatus.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verbindung von Eingabegeräten

Aktivitäten in Zusammenhang mit dem Verbinden von Eingabegeräten, wie Maus, Tastatur usw.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Trennung von Eingabegeräten

Aktivitäten in Zusammenhang mit dem Trennen von Eingabegeräten, wie Maus, Tastatur usw.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

MAC-Adressfehler – Aktion

Beim der Aktion "MAC-Adressfehler" werden Informationen über Fehler im Zusammenhang mit MAC-Adressen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	5

Prozessinitialisierung – Aktion

Bei einer Prozessinitialisierung werden Informationen zur Initialisierung eines Prozesses oder Dienstes auf einem bestimmten System oder in einer bestimmten Anwendung ausgegeben. Diese Ereignisse werden generiert, bevor der Prozess gestartet wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verbindung von Speichergeräten

Aktivitäten in Zusammenhang mit dem Verbinden von Speichergeräten, die an das System angeschlossen sind (z. B. externe Festplatten, externe optische Laufwerke wie CD-ROM-Laufwerke, Kameras, Scanner, Flash-Speichergeräte, PDAs).

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	4

Trennung von Speichergeräten

Aktivitäten in Zusammenhang mit dem Trennen von Speichergeräten, die an das System angeschlossen sind (z. B. externe Festplatten, externe optische Laufwerke wie CD-ROM-Laufwerke, Kameras, Scanner, Flash-Speichergeräte, PDAs).

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	4

Systemwarnung – Aktion

Bei der Systemwarnung werden Informationen über Warnungen eines Systems ausgegeben, welche sich auf die Kernfunktionen des Systems beziehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Infrastrukturmanagement – Klasse

Agentenwarnung – Aktion

Bei der Aktion "Agentenwarnung" werden Informationen über Warnbedingungen im Zusammenhang mit einem Agenten ausgegeben. "Agent" bezieht sich auf sämtliche Software- oder Hardwarekomponenten, die von einer Manager-Komponente verwaltet werden. Jeder Typ von Warnung in Bezug auf den Agenten kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Agentenfehler" zugeordnet werden. Verwenden Sie für die Zuordnung keine CEG-Felder, die mit "agent_" beginnen, da sich diese Felder auf CA Enterprise Log Manager-Agenten beziehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	4

Aktion "Adresskonflikt"

Mit der Aktion "Adresskonflikt" werden Ereignisinformationen zu Konflikten im Adressbereich der Enterprise angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	3
Fehler	F	N/V

Aktion "Agentenmetrik"

Mit der Aktion "Agentenmetrik" werden Ereignisinformationen zur Verfolgung und Überwachung der Leistung oder der Betriebsmetrik sowie der Trends von Agenten einer Anwendung angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Agentenzurücksetzung"

Mit der Aktion "Agentenzurücksetzung" werden Ereignisinformationen zur Zurücksetzung von Agenten oder Clients angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Managermetrik"

Mit der Aktion "Managermetrik" werden Ereignisinformationen zur Verfolgung und Überwachung der Leistung oder der Betriebsmetrik sowie der Trends von Managern einer Anwendung angegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Alarm zur Namensgebung"

Mit der Aktion "Alarm zur Namensgebung" werden Informationen zu Alarmen angezeigt, die im Zusammenhang mit der Namensgebung von Assets stehen, wie Namenskonflikte, Probleme mit Namensrichtlinien oder andere allgemeine Verletzungen der Namensgebung.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	N/V
Fehler	F	5

Aktion "Benachrichtigungen zur Namensgebung"

Mit der Aktion "Benachrichtigungen zur Namensgebung" werden Informationen zu Benachrichtigungen angezeigt, die im Zusammenhang mit der Namensgebung von Assets stehen, wie Namenskonflikte, Probleme mit Namensrichtlinien oder andere allgemeine Verletzungen der Namensgebung.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Warnung zur Namensgebung"

Mit der Aktion "Warnung zur Namensgebung" werden Informationen zu Warnungen angezeigt, die im Zusammenhang mit der Namensgebung von Assets stehen, wie Namenskonflikte, Probleme mit Namensrichtlinien oder andere allgemeine Verletzungen der Namensgebung.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolg	S	N/V
Fehler	F	3

Agentenalarm – Aktion

Beim Agentenalarm werden Informationen über Alarmbedingungen bezüglich eines Agenten ausgegeben, der einem Infrastrukturmanager oder einer ähnlichen zentralisierten Systemkomponente unterstellt ist. "Agent" bezieht sich auf sämtliche Software- oder Hardwarekomponenten, die von einer Manager-Komponente verwaltet werden. Jeder Typ von Alarm in Bezug auf den Agenten kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Agentenfehler" zugeordnet. Verwenden Sie für die Zuordnung keine CEG-Felder, die mit "agent_" beginnen, da sich diese Felder auf CA Enterprise Log Manager-Agenten beziehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.

Informationen	Ebene	
Fehler	F	6

Aktion "Agent deaktivieren"

Die Aktion "Agent deaktivieren" gibt Informationen zum Deaktivieren eines Agenten auf einem System. "Agent" bezieht sich auf sämtliche Software- oder Hardwarekomponenten, die von einer Manager-Komponente verwaltet werden. Wenn ein Agent deaktiviert wird, kann die Manager-Komponente das System, auf dem der Agent ausgeführt wird, nicht kontrollieren oder keine Informationen davon erhalten.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Agent aktivieren"

Die Aktion "Agent aktivieren" gibt Informationen zum Aktivieren eines Agenten auf einem System. "Agent" bezieht sich auf sämtliche Software- oder Hardwarekomponenten, die von einer Manager-Komponente verwaltet werden. Wenn ein Agent deaktiviert wird, kann die Manager-Komponente das System, auf dem der Agent ausgeführt wird, nicht kontrollieren oder keine Informationen davon erhalten.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Agentenfehler – Aktion

Beim Agentenfehler werden Informationen über Fehlerbedingungen bezüglich eines Agenten ausgegeben, der einem Infrastrukturmanager oder einer ähnlichen zentralisierten Systemkomponente unterstellt ist. "Agent" bezieht sich auf sämtliche Software- oder Hardwarekomponenten, die von einer Manager-Komponente verwaltet werden. Jeder Typ von Fehler in Bezug auf den Agenten kann dieser Aktion zugeordnet werden. Weniger schwerwiegende Ereignisse sollten der Aktion "Agentenwarnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "Agentenalarm" zugeordnet werden. Verwenden Sie für die Zuordnung keine CEG-Felder, die mit "agent_" beginnen, da sich diese Felder auf CA Enterprise Log Manager-Agenten beziehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	5

Aktion "Agent ändern"

Die Aktion "Agent ändern" gibt Informationen zu Änderungen an jeder beliebigen Agentenkomponente.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Agentenbenachrichtigung – Aktion

Bei der Agentenbenachrichtigung werden Informationen ausgegeben, die allgemeine Benachrichtigungen von einem Agenten betreffen. "Agent" bezieht sich auf sämtliche Software- oder Hardwarekomponenten, die von einer Manager-Komponente verwaltet werden. Jeder Typ von Benachrichtigung vom Agenten kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "Agentenstatus", wenn das Ereignis den Status eines Agenten beschreibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Agentenoperation – Aktion

Bei der Agentenoperation werden Informationen über allgemeine Operationen im Zusammenhang mit der Funktionsweise eines Agenten ausgegeben. "Agent" bezieht sich auf sämtliche Software- oder Hardwarekomponenten, die von einer Manager-Komponente verwaltet werden. Lässt sich ein Ereignis, das im Rahmen einer normalen Funktion oder Operation eines Agenten aufgezeichnet wird, nicht präziser einer bestimmten CEG-Aktion zuordnen, kann es der Aktion "Agentenoperation" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Agentenstart – Aktion

Beim Agentenstart werden Informationen zum Starten eines Agenten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Agentenbeendigung – Aktion

Bei der Agentenbeendigung werden Informationen zur Beendigung eines Agenten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Agent beenden"

Die Aktion "Agent beenden" gibt Informationen zum Beenden eines Agenten. Einen Agenten zu beenden ist eine abruptere Aktion, als einen Agenten zu deaktivieren.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	3
Fehler	F	3

Alarmzuweisung – Aktion

Bei der Alarmzuweisung werden Informationen über die Zuweisung von Alarmen an Problemlöser, Support-Mitarbeiter oder Support-Systeme ausgegeben. Ein Alarm ist ein Objekt, welches anzeigt, dass es in der verwalteten Umgebung benutzerinduzierte Unregelmäßigkeiten gibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Sekundär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Informationen	Ebene	
Fehler	F	3

Alarmerstellung – Aktion

Bei der Alarmerstellung werden Informationen über die Erstellung eines Alarms durch ein Überwachungssystem ausgegeben. Ein Alarm ist ein Objekt, welches anzeigt, dass es in der verwalteten Umgebung benutzerinduzierte Unregelmäßigkeiten gibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Alarmlöschung – Aktion

Bei der Alarmlöschung werden Informationen über die Löschung eines Alarms ausgegeben. Die Löschung erfolgt entweder durch ein Überwachungssystem oder manuell durch einen Endbenutzer oder Administrator. Ein Alarm ist ein Objekt, welches anzeigt, dass es in der verwalteten Umgebung benutzerinduzierte Unregelmäßigkeiten gibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Alarm deaktiviert – Aktion

Bei der Aktion "Alarm deaktiviert" werden Informationen über die Deaktivierung eines Alarms ausgegeben. Die Deaktivierung erfolgt entweder durch ein Überwachungssystem oder manuell durch einen Endbenutzer oder Administrator. Ein Alarm ist ein Objekt, welches anzeigt, dass es in der verwalteten Umgebung benutzerinduzierte Unregelmäßigkeiten gibt. Einen Alarm zu deaktivieren bedeutet, eine hergestellte Verknüpfung zwischen einem Alarm und einem Gerät bzw. einem Model aufzuheben.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Alarmstatus – Aktion

Bei der Aktion "Alarmstatus" werden Informationen über Statusbedingungen eines Alarms durch ein Überwachungssystem ausgegeben. Ein Alarm ist ein Objekt, welches anzeigt, dass es in der verwalteten Umgebung benutzerinduzierte Unregelmäßigkeiten gibt. Der Status eines Alarms kann so geändert werden, dass die erfolgten Arbeitsschritte zur Behandlung von Alarmproblemen angezeigt werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Alarmaktualisierung – Aktion

Bei der Aktion "Alarmaktualisierung" werden Informationen über die Aktualisierung oder Änderung eines Alarms ausgegeben. Dies erfolgt entweder durch ein Überwachungssystem oder manuell durch einen Endbenutzer oder Administrator. Ein Alarm ist ein Objekt, welches anzeigt, dass es in der verwalteten Umgebung benutzerinduzierte Unregelmäßigkeiten gibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

API-Alarm – Aktion

Beim API-Alarm werden Informationen über Alarmbedingungen im Zusammenhang mit einer API ausgegeben. Eine Application Programming Interface (API) ist eine Schnittstelle, über die verschiedene Möglichkeiten definiert werden, wie ein Anwendungsprogramm mit externen Bibliotheken und/oder Betriebssystemen interagiert. Jeder Typ von Fehler in Bezug auf die API kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "API-Fehler" zugeordnet.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	6

API-Fehler – Aktion

Beim API-Fehler werden Informationen über Fehlerbedingungen im Zusammenhang mit einer API ausgegeben. Eine Application Programming Interface (API) ist eine Schnittstelle, über die verschiedene Möglichkeiten definiert werden, wie ein Anwendungsprogramm mit externen Bibliotheken und/oder Betriebssystemen interagiert. Jeder Typ von Fehler in Bezug auf die API kann dieser Aktion zugeordnet werden. Weniger schwerwiegende Ereignisse sollten der Aktion "API-Warnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf müssen der Aktion "API-Alarm" zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	5

API-Benachrichtigung – Aktion

Bei der API-Benachrichtigung werden Informationen über Benachrichtigungen und Meldungen ausgegeben, die aus bzw. von API-Modulen generiert werden. Eine Application Programming Interface (API) ist eine Schnittstelle, über die verschiedene Möglichkeiten definiert werden, wie ein Anwendungsprogramm mit externen Bibliotheken und/oder Betriebssystemen interagiert. Jeder Typ von Benachrichtigung von der API kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "API-Status", wenn das Ereignis den Status eines API-Moduls beschreibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

API-Operation – Aktion

Bei der API-Operation werden Informationen über allgemeine Operationen im Zusammenhang mit der Funktionsweise einer API ausgegeben. Eine Application Programming Interface (API) ist eine Schnittstelle, über die verschiedene Möglichkeiten definiert werden, wie ein Anwendungsprogramm mit externen Bibliotheken und/oder Betriebssystemen interagiert. Lässt sich ein Ereignis, das im Rahmen einer normalen Funktion oder Operation einer API aufgezeichnet wird, nicht präziser einer bestimmten CEG-Aktion zuordnen, kann es der Aktion "API-Operation" zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

API-Status – Aktion

Bei der Aktion "API-Status" werden Informationen über den Status von API-Modulen ausgegeben. Eine Application Programming Interface (API) ist eine Schnittstelle, über die verschiedene Möglichkeiten definiert werden, wie ein Anwendungsprogramm mit externen Bibliotheken und/oder Betriebssystemen interagiert. Jeder Ereignistyp, der den Status von API-Modulen beschreibt, kann dieser Aktion zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

API-Warnung – Aktion

Bei der API-Warnung werden Informationen über Warnbedingungen im Zusammenhang mit einer API ausgegeben. Eine Application Programming Interface (API) ist eine Schnittstelle, über die verschiedene Möglichkeiten definiert werden, wie ein Anwendungsprogramm mit externen Bibliotheken und/oder Betriebssystemen interagiert. Jeder Typ von Warnung in Bezug auf die API kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "API-Fehler" zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	4

Anwendungsalarm – Aktion

Beim Anwendungsalarm werden Informationen über Alarmbedingungen im Zusammenhang mit der Funktionsweise einer Anwendung ausgegeben. Jeder Typ von Alarm in Bezug auf die Anwendung kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Anwendungsfehler" zugeordnet. Ordnen Sie Alarme in Bezug auf Hintergrundprozesse wie Services oder Daemons der Aktion "Prozessalarm" zu.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	6

Anwendungsinitialisierung – Aktion

Bei der Anwendungsinitialisierung werden Informationen über Initialisierungsoperationen im Zusammenhang mit dem Start einer Anwendung ausgegeben. Beim Start einer Anwendung können eine Reihe von Ereignissen und Meldungen von Audit-Protokollen aufgezeichnet werden, bevor Startereignisse aufgezeichnet werden. Ordnen Sie Ereignisse in Verbindung mit diesem Szenario der Aktion "Anwendungsinitialisierung" zu. Ordnen Sie Initialisierungsereignisse in Bezug auf Hintergrundprozesse wie Services oder Daemons der Aktion "Prozessinitialisierung" zu.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Anwendungsoperation – Aktion

Bei der Anwendungsoperation werden Informationen über allgemeine Operationen im Zusammenhang mit der Funktionsweise einer Anwendung ausgegeben. Lässt sich ein Ereignis, das im Rahmen einer normalen Funktion oder Operation einer Anwendung aufgezeichnet wird, nicht präziser einer bestimmten CEG-Aktion zuordnen, kann es dieser Aktion zugeordnet werden. Ordnen Sie Funktionsereignisse in Bezug auf Hintergrundprozesse wie Services oder Daemons der Aktion "Prozessoperation" zu.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Anwendungsstatus – Aktion

Bei der Aktion "Anwendungsstatus" werden Informationen über den Status einer Anwendung ausgegeben. Jeder Typ von Statusmeldung in Verbindung mit einer Anwendung kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Ordnen Sie Statusereignisse in Bezug auf Hintergrundprozesse wie Services oder Daemons der Aktion "Prozessstatus" zu.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Massenladung von Daten – Aktion

Bei der Massenladung von Daten werden Informationen zum Laden oder Importieren von externen Daten oder Objekten ausgegeben, die in Blöcken oder Massen in eine Anwendung oder ein System integriert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Protokollwarteschlangen-Benachrichtigung – Aktion

Bei der Protokollwarteschlangen-Benachrichtigung werden Informationen über Benachrichtigungen im Zusammenhang mit Protokollwarteschlangen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Protokollwarteschlangen-Warnung – Aktion

Bei der Protokollwarteschlangen-Warnung werden Informationen über Warnungen im Zusammenhang mit Protokollwarteschlangen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	4

Modellstatus – Aktion

Bei der Aktion "Modellstatus" werden Informationen über den Status eines Modells ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Objektstatusänderung"

Die Aktion "Objektstatusänderung" gibt Informationen zur Änderung des Status eines überwachten Objekts.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Kritischer Objektstatus – Aktion

Bei kritischem Objektstatus werden Informationen zu einem Objekt in kritischem Zustand ausgegeben. Bei einem Objekt kann es sich um ein System, ein Gerät, eine Anwendung oder ein beliebiges physisches oder logisches Konfigurationselement handeln.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Fehler	F	4

Normaler Objektstatus – Aktion

Bei normalem Objektstatus werden Informationen zu einem Objekt in normalem Zustand ausgegeben. Bei einem Objekt kann es sich um ein System, ein Gerät, eine Anwendung oder ein beliebiges physisches oder logisches Konfigurationselement handeln.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Offline-Objektstatus – Aktion

Beim Offline-Objektstatus werden Informationen zu einem Offline-Objekt ausgegeben. Bei einem Objekt kann es sich um ein System, ein Gerät, eine Anwendung oder ein beliebiges physisches oder logisches Konfigurationselement handeln.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Fehler	F	3

Objektstatuswarnung – Aktion

Bei der Objektstatuswarnung werden Informationen zu einem Objekt in einem Warnzustand ausgegeben. Bei einem Objekt kann es sich um ein System, ein Gerät, eine Anwendung oder ein beliebiges physisches oder logisches Konfigurationselement handeln.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Fehler	F	3

Software-Konflikt – Aktion

Bei der Aktion "Software-Konflikt" werden Informationen über die Erkennung von inkompatibler oder ungeeigneter Software auf einem System ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	entf.	entf.

Aktion "Systemhinzufügung"

Die Aktion "Systemhinzufügung" gibt Informationen über die Registrierung oder Hinzufügung eines Systems bei bzw. zu einer Infrastrukturverwaltungsplattform zwecks Überwachung und Verwaltung. Wenn Sie das Hinzufügen von virtuellen Verwaltungsplattformen wie VMWare vCenter aufzeichnen möchten, ordnen Sie das Ereignis der Aktion "Systemhinzufügung" unter der Klasse "Virtualisierungsverwaltung" zu.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Systementdeckung"

Die Aktion "Systementdeckung" gibt Informationen zur Entdeckung eines Verwaltungs- oder Überwachungssystems.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Schwellenwert überschritten – Aktion

Bei der Aktion "Schwellenwert überschritten" werden Informationen über die Erkennung eines Zustands ausgegeben, bei dem die Schwellenwerte für Systemeinstellungen überschritten sind.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Netzwerkmanagement – Klasse

Netzwerkalarm – Aktion

Beim Netzwerkalarm werden Informationen über Alarmbedingungen im Zusammenhang mit Netzwerken ausgegeben. Jeder Typ von Alarm in Bezug auf das Netzwerk kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Netzwerkfehler" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	6

Aktion "Netzwerkerstellung"

Die Aktion "Netzwerkerstellung" gibt Informationen zur Erstellung eines Netzwerks auf einem physischen oder virtuellen Netzwerksystem.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Netzwerklöschung"

Die Aktion "Netzwerklöschung" gibt Informationen zur Löschung eines Netzwerks auf einem physischen oder virtuellen Netzwerksystem.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Netzwerkfehler – Aktion

Beim Netzwerkfehler werden Informationen über Fehlerbedingungen im Zusammenhang mit einem Netzwerk ausgegeben. Jeder Typ von Fehler in Bezug auf das Netzwerk kann dieser Aktion zugeordnet werden. Weniger schwerwiegende Ereignisse sollten der Aktion "Netzwerkwarnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "Netzwerkalarm" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	5

Aktion "Netzwerk ändern"

Die Aktion "Netzwerk ändern" gibt Informationen zur Änderung oder Aktualisierung eines Netzwerks auf einem physischen oder virtuellen Netzwerksystem.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Netzwerkbenachrichtigung – Aktion

Bei der Netzwerkbenachrichtigung werden Informationen über Benachrichtigungen und Meldungen ausgegeben, die von Netzwerken generiert werden. Jeder Typ von Benachrichtigung vom Netzwerk kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "Netzwerkstatus", wenn das Ereignis den Status eines Netzwerks beschreibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Netzwerkstatus – Aktion

Bei der Aktion "Netzwerkstatus" werden Informationen über den Status eines Netzwerks ausgegeben. Jeder Typ von Statusmeldung in Verbindung mit einem Netzwerk kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Netzwerkwarnung – Aktion

Bei der Netzwerkwarnung werden Informationen über Warnungen im Zusammenhang mit einem Netzwerk ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	4

SNMP-Alarm – Aktion

Beim SNMP-Alarm werden Informationen über Alarmbedingungen im Zusammenhang mit SNMP ausgegeben. Das SNMP-Protokoll (Simple Network Management Protocol) wird in Netzwerk-Managementsystemen verwendet, um am Netzwerk angeschlossene Geräte im Hinblick auf Bedingungen zu überwachen, die für die Administration von Bedeutung sind. Jeder Typ von Alarm in Bezug auf SNMP kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "SNMP-Fehler" zugeordnet.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	6

SNMP-Fehler – Aktion

Beim SNMP-Fehler werden Informationen über Fehlerbedingungen im Zusammenhang mit einem SNMP ausgegeben. Das SNMP-Protokoll (Simple Network Management Protocol) wird in Netzwerk-Managementsystemen verwendet, um am Netzwerk angeschlossene Geräte im Hinblick auf Bedingungen zu überwachen, die für die Administration von Bedeutung sind. Jeder Typ von Fehler in Bezug auf das SNMP kann dieser Aktion zugeordnet werden. Weniger schwerwiegende Ereignisse sollten der Aktion "SNMP-Warnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "SNMP-Alarm" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	5

SNMP-Benachrichtigung – Aktion

Bei der SNMP-Benachrichtigung werden Informationen über Benachrichtigungen und Meldungen ausgegeben, die von einem SNMP generiert werden. Das SNMP-Protokoll (Simple Network Management Protocol) wird in Netzwerk-Managementsystemen verwendet, um am Netzwerk angeschlossene Geräte im Hinblick auf Bedingungen zu überwachen, die für die Administration von Bedeutung sind. Jeder Typ von Benachrichtigung vom SNMP kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "SNMP-Status", wenn das Ereignis den Status eines SNMP beschreibt.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

SNMP-Operation – Aktion

Bei der SNMP-Operation werden Informationen über allgemeine Operationen im Zusammenhang mit der Funktionsweise eines SNMP ausgegeben. Lässt sich ein Ereignis, das im Rahmen einer normalen Funktion oder Operation eines SNMP aufgezeichnet wird, nicht präziser einer bestimmten CEG-Aktion zuordnen, kann es dieser Aktion zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

SNMP-Status – Aktion

Bei der Aktion "SNMP-Status" werden Informationen über den Status eines SNMP ausgegeben. Das SNMP-Protokoll (Simple Network Management Protocol) wird in Netzwerk-Managementsystemen verwendet, um am Netzwerk angeschlossene Geräte im Hinblick auf Bedingungen zu überwachen, die für die Administration von Bedeutung sind. Jeder Typ von Statusmeldung in Verbindung mit einem SNMP kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

SNMP-Warnung – Aktion

Bei der SNMP-Warnung werden Informationen über Warnbedingungen im Zusammenhang mit einem SNMP ausgegeben. Das SNMP-Protokoll (Simple Network Management Protocol) wird in Netzwerk-Managementsystemen verwendet, um am Netzwerk angeschlossene Geräte im Hinblick auf Bedingungen zu überwachen, die für die Administration von Bedeutung sind. Jeder Typ von Warnung in Bezug auf das SNMP kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "SNMP-Fehler" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	4

Aktion "VLAN-Erstellung"

Die Aktion "VLAN-Erstellung" gibt Informationen zur Erstellung eines VLAN auf einem physischen oder virtuellen Netzwerksystem.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "VLAN-Löschung"

Die Aktion "VLAN-Löschung" gibt Informationen zur Löschung eines VLAN auf einem physischen oder virtuellen Netzwerksystem.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "VLAN ändern"

Die Aktion "VLAN ändern" gibt Informationen zur Änderung oder Aktualisierung eines VLAN auf einem physischen oder virtuellen Netzwerksystem.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Klasse für Prozessaktivität

Prozessalarm – Aktion

Beim Prozessalarm werden Informationen über Alarme ausgegeben, die von einem Prozess oder Dienst auf einem bestimmten System oder in einer bestimmten Anwendung generiert wurden. Ein Prozess ist ein im Hintergrund ablaufendes Programm, das mit UNIX Daemon oder dem Windows-Dienst vergleichbar ist. Jeder Typ von Alarmbedingung im Zusammenhang mit dem Prozess kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Prozess-Fehler" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	6

Aktion "Prozess gestoppt"

Die Aktion "Prozess gestoppt" gibt Informationen zum Status eines gestoppten Prozesses. Sie können Ereignisse zur Aktion "Prozess gestoppt" zuordnen, um die Stoppungsaktion aufzuzeichnen. Wenn das Ereignis nur anzeigt, dass der Prozess gestoppt wurde, ordnen Sie es der Aktion "Prozess gestoppt" zu.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Prozess fortsetzen – Aktion

Bei der Aktion "Prozess fortsetzen" werden Informationen ausgegeben, die die Fortsetzung eines Prozesses oder Dienstes auf einem bestimmten System oder in einer bestimmten Anwendung betreffen. Ein Prozess ist ein im Hintergrund ablaufendes Programm, das mit UNIX Daemon oder dem Windows-Dienst vergleichbar ist.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Informationen	Ebene	
Fehler	F	3

Prozess-Status – Aktion

Bei der Aktion "Prozess-Status" werden Informationen ausgegeben, die den Status eines Prozesses oder Dienstes auf einem bestimmten System oder in einer bestimmten Anwendung betreffen. Ein Prozess ist ein im Hintergrund ablaufendes Programm, das mit UNIX Daemon oder dem Windows-Dienst vergleichbar ist. Jeder Typ von Statusmeldung in Bezug auf einen Prozess kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Aufgabeninitiierung"

Die Aktion "Aufgabeninitiierung" gibt Informationen zur Initiierung einer bereits geplanten Aufgabe.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Klasse für Sicherheitsprotokollaktivität

Protokollkonfiguration – Aktion

Bei der Protokollkonfiguration werden Informationen über die Konfiguration von Protokollen ausgegeben, zum Beispiel Filter zu Protokollen hinzufügen oder bestimmte Aktionen ignorieren.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	entf.	entf.

Richtlinienausführung – Aktion

Bei der Richtlinienausführung werden Informationen zur Ausführung von Richtlinien ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Sicherheitsprotokoll-Zugriff – Aktion

Beim Sicherheitsprotokoll-Zugriff werden Informationen zum Zugriff auf Sicherheitsprotokolle ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Sicherheitsprotokoll-Alert"

Die Aktion "Sicherheitsprotokoll-Alert" gibt Informationen zu mit dem Sicherheitsprotokoll in Verbindung stehenden Alert-Bedingungen. Sie können dieser Aktion jede beliebige Art von Sicherheitsprotokoll-Alert zuordnen. Wenn eine Fehlerbedingung keiner sofortigen Beachtung bedarf, können Sie sie der Aktion "Sicherheitsprotokollfehler" zuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Aktion zum Löschen des Sicherheitsprotokolls

Mit der Aktion zum Löschen des Sicherheitsprotokolls werden Informationen zum Start eines Prozesses oder Services auf einem bestimmten System oder in einer bestimmten Anwendung angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer das Sicherheitsprotokoll auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	6
Fehler	F	6

Aktion "Sicherheitsprotokollfehler"

Die Aktion "Sicherheitsprotokollfehler" gibt Informationen zu mit dem Sicherheitsprotokoll in Verbindung stehenden Fehlerbedingungen. Sie können dieser Aktion jede beliebige Art von Sicherheitsprotokollfehler zuordnen. Sie können weniger schwerwiegende Ereignisse zur Aktion "Sicherheitsprotokollwarnung" zuordnen. Sie können schwerwiegendere Ereignisse, die sofortiger Beachtung bedürfen, der Aktion "Sicherheitsprotokoll-Alert" zuordnen.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Fehler	F	5

Aktion bei Sicherheitsprotokoll-Rollover

Beim Sicherheitsprotokoll-Rollover werden Informationen zum Durchlaufen von Protokolldateien auf einem bestimmten System oder in einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Host ein Rollover der Sicherheitsprotokolle durchgeführt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Aktion "Sicherheitsprotokollwarnung"

Die Aktion "Sicherheitsprotokollwarnung" gibt Informationen zu mit dem Sicherheitsprotokoll in Verbindung stehenden Warnungen. Sie können dieser Aktion jede beliebige Art von Sicherheitsprotokollwarnung zuordnen. Sie können schwerwiegendere Ereignisse zur Aktion "Sicherheitsprotokollfehler" zuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

System-Audit-Konfiguration – Aktion

Bei der System-Audit-Konfiguration werden Informationen zum Ändern von System-Audit-Einstellungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

System-Audit-Deaktivierung – Aktion

Bei der System-Audit-Deaktivierung werden Informationen zum Deaktivieren eines Audits auf Systemebene ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

System-Audit-Aktivierung – Aktion

Bei der System-Audit-Aktivierung werden Informationen zum Aktivieren eines Audits auf Systemebene ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aufgabenausführung – Aktion

Bei der Aufgabenausführung werden Informationen zur Ausführung von Aufgaben ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Service Level Management – Klasse

Mittlere Service-Beeinträchtigung – Aktion

Bei mittlerer Service-Beeinträchtigung werden Informationen zu einer mittleren Beeinträchtigung auf Service-Ebene ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Aktion "Service-Alert"

Die Aktion "Service-Alert" gibt Informationen zu mit Service in Verbindung stehenden Alert-Bedingungen. Sie können dieser Aktion jede beliebige Art von mit Service in Verbindung stehender Alert zuordnen. Schwerwiegendere Ereignisse sollten der Aktion "Service-Fehler" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Aktion "Service gestoppt"

Die Aktion "Service gestoppt" gibt Informationen zum vollständigen Herunterfahren eines Services.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Aktion "Service-Fehler"

Die Aktion "Service-Fehler" gibt Informationen zu mit Service in Verbindung stehenden Fehlerbedingungen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Aktion "Service-Benachrichtigung"

Die Aktion "Service-Benachrichtigung" gibt Informationen zu von einem Service generierten Meldungen und Benachrichtigungen. Wenn ein Ereignis Teil der normalen Funktion des Services ist, oder es sich keiner spezifischeren CEG-Aktion zuordnen lässt, kann es dieser Aktion zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Service-Vorgang"

Die Aktion "Service-Vorgang" gibt allgemeine Informationen zu Service-Vorgängen. Sie können dieser Aktion jede beliebige Art von mit Service in Verbindung stehenden Statusmeldungen zuordnen, wenn das Ereignis keiner spezifischeren Aktion zugeordnet werden kann.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Service-Status"

Die Aktion "Service-Status" gibt allgemeine Informationen zum Service-Status.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Service nicht verfügbar"

Die Aktion "Service nicht verfügbar" gibt Informationen zu einem nicht verfügbaren Service.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Aktion "Service-Warnung"

Die Aktion "Service-Warnung" gibt Informationen zu mit Service in Verbindung stehenden Warnungen. Sie können dieser Aktion jede beliebige Art von mit Service in Verbindung stehenden Statusmeldungen zuordnen, wenn das Ereignis keiner spezifischeren Aktion zugeordnet werden kann.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Schwere Service-Beeinträchtigung – Aktion

Bei schwerer Service-Beeinträchtigung werden Informationen zu einer erheblichen Beeinträchtigung auf Service-Ebene ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

SLA-Alarm – Aktion

Beim SLA-Alarm werden Informationen über Alarmbedingungen im Zusammenhang mit SLA ausgegeben. Ein Service Level Agreement (SLA) ist Bestandteil eines Servicevertrags, in dem der Servicegrad formal definiert ist. Jeder Typ von Alarm in Bezug auf SLA kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "SLA-Fehler" zugeordnet.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	6

SLA-Fehler – Aktion

Beim SLA-Fehler werden Informationen über Fehlerbedingungen im Zusammenhang mit einem SLA ausgegeben. Ein Service Level Agreement (SLA) ist Bestandteil eines Servicevertrags, in dem der Servicegrad formal definiert ist. Jeder Typ von Fehler in Bezug auf das SLA kann dieser Aktion zugeordnet werden. Weniger schwerwiegende Ereignisse sollten der Aktion "SLA-Warnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "SLA-Alarm" zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	5

SLA-Benachrichtigung – Aktion

Bei der SLA-Benachrichtigung werden Informationen zu Benachrichtigungen und Meldungen ausgegeben, die von der zugehörigen SLA-Aktivität generiert werden. Ein Service Level Agreement (SLA) ist Bestandteil eines Servicevertrags, in dem der Servicegrad formal definiert ist. Jeder Typ von Benachrichtigung von der SLA-Aktivität kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "SLA-Status", wenn das Ereignis den Status eines SLA beschreibt.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

SLA-Operation – Aktion

Bei der SLA-Operation werden Informationen über allgemeine Operationen im Zusammenhang mit einem SLA ausgegeben. Lässt sich ein Ereignis, das im Rahmen einer SLA-Verwaltung aufgezeichnet wird, nicht präziser einer bestimmten CEG-Aktion zuordnen, kann es dieser Aktion zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

SLA-Status – Aktion

Bei der Aktion "SLA-Status" werden Informationen über den Status eines SLA ausgegeben. Ein Service Level Agreement (SLA) ist Bestandteil eines Servicevertrags, in dem der Servicegrad formal definiert ist. Jeder Typ von Statusmeldung in Verbindung mit einem SLA kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

SLA-Warnung – Aktion

Bei der SLA-Warnung werden Informationen über Warnbedingungen im Zusammenhang mit einem SLA ausgegeben. Ein Service Level Agreement (SLA) ist Bestandteil eines Servicevertrags, in dem der Servicegrad formal definiert ist. Jeder Typ von Warnung in Bezug auf das SLA kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "SLA-Fehler" zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	4

Leichte Service-Beeinträchtigung – Aktion

Bei leichter Service-Beeinträchtigung werden Informationen zu einer geringfügigen Beeinträchtigung auf Service-Ebene ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	3

Klasse für Systemaktivität

Firmware-Alarm – Aktion

Beim Firmware-Alarm werden Informationen über Alarmbedingungen im Zusammenhang mit Firmware ausgegeben. Jeder Typ von Alarm in Bezug auf die Firmware kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Firmware-Fehler" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	6

Firmware-Fehler – Aktion

Beim Firmware-Fehler werden Informationen über Fehlerbedingungen im Zusammenhang mit Firmware ausgegeben. Jeder Typ von Fehler in Bezug auf die Firmware kann dieser Aktion zugeordnet werden. Weniger schwerwiegende Ereignisse sollten der Aktion "Firmware-Warnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "Firmware-Alarm" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	5

Firmware-Benachrichtigung – Aktion

Bei der Firmware-Benachrichtigung werden Informationen über Benachrichtigungen und Meldungen ausgegeben, die von der Firmware generiert werden. Jeder Typ von Benachrichtigung von der Firmware kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "Firmware-Status", wenn das Ereignis den Status einer Firmware beschreibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Firmware-Status – Aktion

Bei der Aktion "Firmware-Status" werden Informationen über den Status einer Firmware ausgegeben. Jeder Typ von Statusmeldung in Verbindung mit einer Firmware kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Firmware-Warnung – Aktion

Bei der Firmware-Warnung werden Informationen über Warnungen im Zusammenhang einer Firmware ausgegeben. Jeder Typ von Warnung in Bezug auf die Firmware kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Firmware-Fehler" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	4

Hardwarealarm – Aktion

Beim Hardwarealarm werden Informationen zu hardwarebezogenen Alarmbedingungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Hardwarebenachrichtigung – Aktion

Bei der Hardwarebenachrichtigung werden Informationen zu hardwaregenerierten Meldungen und Benachrichtigungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Hardwarefunktion – Aktion

Bei der Aktion "Hardwarefunktion" werden allgemeine Informationen zu Hardwarefunktionen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Hardwarestatus – Aktion

Bei der Aktion "Hardwarestatus" werden Informationen über den Status einer Hardware ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Hardwarewarnung – Aktion

Bei der Hardwarewarnung werden Informationen zu hardwarebezogenen Warnungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Protokollaktivität

Allgemeine Protokollaktivitäten wie die Generierung von Berichten anhand erfasster Protokolle, die Analyse von Protokollen usw.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Primär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Protokoll-Alert"

Die Aktion "Protokoll-Alert" gibt Informationen zu mit Protokollen in Verbindung stehenden Alert-Bedingungen. Sie können dieser Aktion jede beliebige Art von mit Protokollen in Verbindung stehender Alert zuordnen. Schwerwiegendere Ereignisse sollten der Aktion "Protokollfehler" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Protokolllöschung – Aktion

Bei der Protokolllöschung werden Informationen zur Löschung von Protokolldateien ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Protokollfehler – Aktion

Bei der Aktion "Protokollfehler" werden Informationen über Fehlerbedingungen im Zusammenhang mit Protokollen und Audit-Infrastrukturen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	5

Protokollbenachrichtigung – Aktion

Bei der Protokollbenachrichtigung werden Informationen über Benachrichtigungen und Meldungen ausgegeben, die von einem Protokollierungssystem generiert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Protokollstart – Aktion

Beim Protokollstart werden Informationen zum Starten von Protokollierungsoperationen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Protokollbeendigung – Aktion

Bei der Protokollbeendigung werden Informationen zur Beendigung von Protokollierungsoperationen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Protokollwarnung – Aktion

Bei der Protokollwarnung werden Informationen über Warnungen im Zusammenhang mit dem Protokollierungssystem ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	4

Verweigerung der Löschung

Eine allgemeine Aktion, die für jedes Drittanbieterprodukt möglich ist, z. B. beim Entfernen von Makros oder Anwendungen durch ein Antivirenprogramm.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Server nicht verfügbar – Aktion

Bei der Aktion "Server nicht verfügbar" werden Informationen über die Nichtverfügbarkeit eines Servers ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	entf.	entf.

Aktion "System-Alert"

Die Aktion "System-Alert" gibt Informationen zu mit einem System in Verbindung stehenden Alerts. Sie können dieser Aktion jede beliebige Art von Alert oder Alarm über das System zuordnen. Wenn eine Fehlerbedingung keiner sofortigen Beachtung bedarf, können Sie sie der Aktion "Systemfehler" zuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Aktion "Systemumgebungs-Alert"

Die Aktion "Systemumgebungs-Alert" gibt Informationen zu mit Umgebungskomponenten in Verbindung stehenden Alerts wie Spannung, Stromversorgung, Hitze oder Luftfeuchtigkeit.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	6

Systemfehler

Bei Systemfehlern werden Fehlerinformationen in Zusammenhang mit den Kernfunktionen eines Systems ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	5

Systeminitialisierung – Aktion

Bei der Systeminitialisierung werden Informationen über die Initialisierung eines Systems ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

System-Failover – Aktion

Beim System-Failover werden Informationen zu Failover-Aktivitäten in hochverfügbaren Umgebungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Systembenachrichtigung

Bei Systembenachrichtigungen werden Benachrichtigungsinformationen in Zusammenhang mit den Kernfunktionen eines Systems ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Anhalten des Systems

Beim Anhalten des Systems werden Informationen zum Anhalten eines Systems oder einer Anwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welches System auf welchem Host angehalten hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Aktion "System zurücksetzen"

Die Aktion "System zurücksetzen" gibt Informationen zu unerwarteten Systemzurücksetzungen aufgrund kritischer Bedingungen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	4
Fehler	F	5

Aktion "Systemressourcen-Alert"

Die Aktion "Systemressourcen-Alert" gibt Informationen zu mit Systemressourcen in Verbindung stehenden Alerts. Sie können dieser Aktion jede beliebige Art von Alert oder Alarm über Systemressourcen zuordnen. Wenn eine Fehlerbedingung keiner sofortigen Beachtung bedarf, können Sie sie der Aktion "Systemressourcen-Fehler" zuordnen.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Fehler	F	6

Systemressourcenfehler – Aktion

Bei der Aktion "Systemressourcenfehler" werden Informationen über Fehlerbedingungen ausgegeben, die während der Zuweisung von Systemressourcen wie Speicher und Auslagerungsbereich auf einem bestimmten System oder in einer bestimmten Anwendung auftreten.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	5

Systemressourcenwarnung – Aktion

Bei der Aktion "Systemressourcenwarnung" werden Informationen über Warnungen ausgegeben, die während der Zuweisung oder Erstellung von Systemressourcen wie Speicher und Auslagerungsbereich auf einem bestimmten System oder in einer bestimmten Anwendung auftreten.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	4

Systemneustart

Beim Systemneustart werden Informationen zum Neustart eines Systems ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Sekundär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	6
Fehler	F	7

Fortsetzen des Systems

Beim Fortsetzen des Systems werden Informationen zur Fortsetzung eines Systems oder einer Anwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welches System auf welchem Host fortgesetzt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Systemsicherung – Aktion

Bei der Systemsicherung werden Informationen über die Sicherung eines Systemzustands ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Herunterfahren des Systems

Beim Herunterfahren des Systems werden Informationen zum Herunterfahren eines Prozesses oder Diensts auf einem bestimmten System oder in einer bestimmten Anwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welches System auf welchem Host heruntergefahren hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	7
Fehler	F	7

Systemstart

Beim Systemstart werden Informationen zum Start eines Prozesses oder Diensts auf einem bestimmten System oder in einer bestimmten Anwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welches System auf welchem Host gestartet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	6

Systemstatus

Der Systemstatus liefert Informationen zum Start eines Prozesses oder Diensts auf einem bestimmten System oder in einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Status für welchen Host gemeldet wird. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

System nicht verfügbar – Aktion

Bei der Aktion "System nicht verfügbar" werden Informationen über die Erkennung eines Zustands ausgegeben, bei dem ein System nicht verfügbar ist, um eine Anfrage oder Funktion zu handhaben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	5
Fehler	entf.	entf.

Systemwarnung – Aktion

Bei der Systemwarnung werden Informationen zu Softwarekomponentenwarnungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Trust-Alarm – Aktion

Beim Trust-Alarm werden Informationen zu Alarmbedingungen ausgegeben, die sich mit der Herstellung, Verwaltung und Überwachung von vertrauenswürdigen Beziehungen zwischen zwei Systemen befassen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Trust-Fehler – Aktion

Beim Trust-Fehler werden Informationen zu Fehlerbedingungen ausgegeben, die sich mit der Herstellung, Verwaltung und Überwachung von vertrauenswürdigen Beziehungen zwischen zwei Systemen befassen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Trust-Benachrichtigung – Aktion

Bei der Trust-Benachrichtigung werden Informationen zu Meldungen und Benachrichtigungen ausgegeben, die sich mit der Herstellung, Verwaltung und Überwachung von vertrauenswürdigen Beziehungen zwischen zwei Systemen befassen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Trust-Operation – Aktion

Bei der Trust-Operation werden allgemeine Informationen zu Operationen ausgegeben, die sich mit der Herstellung, Verwaltung und Überwachung von vertrauenswürdigen Beziehungen zwischen zwei Systemen befassen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Vertrauensstatus – Aktion

Bei der Aktion "Vertrauensstatus" werden Informationen zum Vertrauensstatus zwischen zwei Systemen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Trust-Warnung – Aktion

Bei der Trust-Warnung werden Informationen zu Warnungen ausgegeben, die sich mit der Herstellung, Verwaltung und Überwachung von vertrauenswürdigen Beziehungen zwischen zwei Systemen befassen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	3

Systemverwaltungsklasse

Aktion "Lizenzfehler"

Die Aktion "Lizenzfehler" gibt Informationen zu mit Lizenzen in Verbindung stehenden Alert-Bedingungen. Sie können dieser Aktion jede beliebige Art von Lizenz-Alert zuordnen. Wenn eine Fehlerbedingung keiner sofortigen Beachtung bedarf, können Sie sie der Aktion "Lizenzfehler" zuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	4

Lizenzablauf

Beim Lizenzablauf werden Ereignisinformationen zum Ablauf von Produktlizenzen oder -schlüsseln ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Lizenzbenachrichtigung – Aktion

Bei der Lizenzbenachrichtigung werden Informationen zu Benachrichtigungen im Zusammenhang mit Software- oder Hardware-Lizenzen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Lizenzvorgang

Alle Aktivitäten in Zusammenhang mit Lizenzvorgängen wie z. B. dem Hinzufügen von Lizenzinformationen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Lizenzverletzung – Aktion

Bei der Lizenzverletzung werden Informationen im Zusammenhang mit Software- oder Hardware-Lizenzverletzungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Lizenzwarnung – Aktion

Bei der Lizenzwarnung werden Informationen zu Warnungen im Zusammenhang mit Software- oder Hardware-Lizenzen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Service-Installation

Bei einer Service-Installation werden Informationen zu dem neuen Service ausgegeben, der von dem angegebenen Benutzer z. B. auf dem lokalen System installiert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Primär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	4

Service-Deinstallation – Aktion

Bei der Service-Deinstallation werden Informationen zu einem Service ausgegeben, der von dem im Betreff angegebenen Benutzer entfernt wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Software-Installation

Alle Aktivitäten in Zusammenhang mit der Installation von Software. (Die Nachverfolgung sicherheitsrelevanter Software erfolgt mit separaten Aktionen.)

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	5

Software fehlt – Aktion

Bei der Aktion "Software fehlt" werden Informationen über eine fehlende Software ausgegeben, die für eine spezielle Funktion erforderlich ist.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Software-Update – Aktion

Bei der Software-Update-Aktion werden Informationen im Zusammenhang mit Software-Updates ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Software-Deinstallation

Alle Aktivitäten in Zusammenhang mit der Deinstallation von Software. (Die Nachverfolgung sicherheitsrelevanter Software erfolgt mit separaten Aktionen.)

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	5

Virtualisierungsaktivität – Klasse

Gerätealarm – Aktion

Beim Gerätealarm werden Informationen über Alarmbedingungen im Zusammenhang mit einem virtuellen Gerät ausgegeben. Ein virtuelles Gerät simuliert eine physische Hardwarekomponente, z. B. ein Netzwerkgerät (Router, Switch, Netzwerkkarte oder Modem). Jeder Typ von Alarm in Bezug auf das virtuelle Gerät kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Gerätefehler" zugeordnet.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.

Informationen	Ebene	
Fehler	F	6

Geräteerstellung – Aktion

Bei der Geräteerstellung werden Informationen über die Erstellung eines virtuellen Geräts in einer virtualisierten Umgebung ausgegeben. Ein virtuelles Gerät simuliert eine physische Hardwarekomponente, z. B. ein Netzwerkgerät (Router, Switch, Netzwerkkarte oder Modem).

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Gerätelöschung – Aktion

Bei der Gerätelöschung werden Informationen über die Löschung eines virtuellen Geräts in einer virtualisierten Umgebung ausgegeben. Bei der Aktion "Gerätelöschung" geht es um Informationen zur Löschung eines virtuellen Geräts in einer virtualisierten Umgebung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Gerätefehler

Beim Gerätefehler werden Informationen über Fehlerbedingungen im Zusammenhang mit einem virtuellen Gerät ausgegeben. Ein virtuelles Gerät simuliert eine physische Hardwarekomponente, z. B. ein Netzwerkgerät (Router, Switch, Netzwerkkarte oder Modem). Jeder Typ von Fehler in Bezug auf das virtuelle Gerät kann dieser Aktion zugeordnet werden. Weniger schwerwiegende Ereignisse sollten der Aktion "Gerätewarnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "Gerätealarm" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	5

Geräteimport – Aktion

Beim Geräteimport werden Informationen über den Import eines virtuellen Geräts in einen virtuellen Computer, ein virtuelles System oder eine virtuelle Umgebung ausgegeben. Ein virtuelles Gerät simuliert eine physische Hardwarekomponente, z. B. ein Netzwerkgerät (Router, Switch, Netzwerkkarte oder Modem).

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Gerätebenachrichtigung"

Die Aktion "Gerätebenachrichtigung" gibt Informationen über Benachrichtigungen und Meldungen, die von einem virtuellen Gerät generiert werden. Ein virtuelles Gerät simuliert eine physische Hardwarekomponente, z. B. ein Netzwerkgerät (Router, Switch, Netzwerkkarte oder Modem). Jeder Typ von Benachrichtigung vom virtuellen Gerät kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "Gerätestatus", wenn das Ereignis den Status eines virtuellen Geräts beschreibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Geräteoperation – Aktion

Bei der Geräteoperation werden Informationen über allgemeine Operationen im Zusammenhang mit der Funktionsweise eines virtuellen Geräts ausgegeben. Ein virtuelles Gerät simuliert eine physische Hardwarekomponente, z. B. ein Netzwerkgerät (Router, Switch, Netzwerkkarte oder Modem). Lässt sich ein Ereignis, das im Rahmen einer normalen Funktion oder Operation eines virtuellen Geräts aufgezeichnet wird, nicht präziser einer bestimmten CEG-Aktion zuordnen, kann es dieser Aktion zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Gerätestatus

Bei der Aktion "Gerätestatus" werden Informationen über den Status von virtuellen Geräten ausgegeben. Ein virtuelles Gerät simuliert eine physische Hardwarekomponente, z. B. ein Netzwerkgerät (Router, Switch, Netzwerkkarte oder Modem). Jeder Typ von Statusmeldung in Bezug auf ein virtuelles Gerät kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Gerätewarnung – Aktion

Bei der Gerätewarnung werden Informationen über Warnungen im Zusammenhang mit virtuellen Geräten ausgegeben. Ein virtuelles Gerät simuliert eine physische Hardwarekomponente, z. B. ein Netzwerkgerät (Router, Switch, Netzwerkkarte oder Modem). Jeder Typ von Warnung in Bezug auf das virtuelle Gerät kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Gerätewarnung" zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	4

Hypervisor-Alarm – Aktion

Beim Hypervisor-Alarm werden Informationen über Alarmbedingungen im Zusammenhang mit einem Hypervisor ausgegeben. Jeder Typ von Alarm in Bezug auf den Hypervisor kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Hypervisor-Fehler" zugeordnet.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	3

6

Hypervisor-Fehler – Aktion

Beim Hypervisor-Fehler werden Informationen über Fehlerbedingungen im Zusammenhang mit einem Hypervisor ausgegeben. Jeder Typ von Fehler in Bezug auf den Hypervisor kann dieser Aktion zugeordnet werden. Weniger schwerwiegende Ereignisse sollten der Aktion "Hypervisor-Warnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "Hypervisor-Alarm" zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	5

Hypervisor-Benachrichtigung – Aktion

Bei der Hypervisor-Benachrichtigung werden Informationen über Benachrichtigungen und Meldungen ausgegeben, die von einem Hypervisor generiert werden. Jeder Typ von Benachrichtigung vom Hypervisor kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "Hypervisor-Status", wenn das Ereignis den Status eines Hypervisors beschreibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Hypervisor-Operation – Aktion

Bei der Hypervisor-Operation werden Informationen über allgemeine Operationen im Zusammenhang mit der Funktionsweise eines Hypervisors ausgegeben. Lässt sich ein Ereignis, das im Rahmen einer normalen Funktion oder Operation eines Hypervisors aufgezeichnet wird, nicht präziser einer bestimmten CEG-Aktion zuordnen, kann es dieser Aktion zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Hypervisor-Start – Aktion

Beim Hypervisor-Start werden Informationen über den Start eines Hypervisors ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Hypervisor-Status – Aktion

Bei der Aktion "Hypervisor-Status" werden Informationen über den Status eines Hypervisors ausgegeben. Jeder Typ von Statusmeldung in Verbindung mit einem Hypervisor kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Hypervisor-Warnung – Aktion

Bei der Hypervisor-Warnung werden Informationen über Warnungen im Zusammenhang mit einem Hypervisor ausgegeben. Jeder Typ von Warnung in Bezug auf den Hypervisor kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Hypervisor-Fehler" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	4

Aktion "Image-Alert"

Die Aktion "Image-Alert" gibt Informationen zu mit virtuellen Images in Verbindung stehenden Alert-Bedingungen. Ein Image ist ein fertiges Softwarepaket, z. B. eine virtuelle Festplatte (VHD-Datei) oder eine virtuelle DVD-Disc (ISO-Datei), mit Hilfe derer ein virtueller Computer erstellt oder instanziiert werden kann. Sie können dieser Aktion jede beliebige Art von Image-Alert zuordnen. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, können Sie sie der Aktion "Image-Fehler" zuordnen.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Fehler	F	6

Aktion "Geklontes Image"

Die Aktion "Geklontes Image" gibt Informationen über das Klonen von Images. Ein Image ist ein fertiges Softwarepaket, z. B. eine virtuelle Festplatte (VHD-Datei) oder eine virtuelle DVD-Disc (ISO-Datei), mit Hilfe derer ein virtueller Computer erstellt oder instanziiert werden kann.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Image-Fehler – Aktion

Beim Image-Fehler werden Informationen über Fehlerbedingungen im Zusammenhang mit einem Image in einer Virtualisierungsumgebung ausgegeben. Ein Image ist ein fertiges Softwarepaket, z. B. eine virtuelle Festplatte (VHD-Datei) oder eine virtuelle DVD-Disc (ISO-Datei), mit Hilfe dessen ein virtueller Computer erstellt oder instanziiert wird. Jeder Typ von Fehler in Bezug auf das Image kann dieser Aktion zugeordnet werden. Weniger schwerwiegende Ereignisse sollten der Aktion "Image-Warnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "Image-Alarm" zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	5

Image-Export – Aktion

Beim Image-Export werden Information ausgegeben, die sich auf den Export eines Disk-Image oder eines virtuellen Computers in einer Virtualisierungsumgebung beziehen. Ein Image ist ein fertiges Softwarepaket, z. B. eine virtuelle Festplatte (VHD-Datei) oder eine virtuelle DVD-Disc (ISO-Datei), mit Hilfe dessen ein virtueller Computer erstellt oder instanziiert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Image ändern – Aktion

Bei der Aktion "Image ändern" werden Information über Änderungen an einem Disk-Image oder einem virtuellen Computer in einer Virtualisierungsumgebung ausgegeben. Ein Image ist ein fertiges Softwarepaket, z. B. eine virtuelle Festplatte (VHD-Datei) oder eine virtuelle DVD-Disc (ISO-Datei), mit Hilfe dessen ein virtueller Computer erstellt oder instanziiert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Image-Benachrichtigung – Aktion

Bei der Image-Benachrichtigung werden Informationen über Benachrichtigungen und Meldungen ausgegeben, die von einem Image in einer Virtualisierungsumgebung generiert werden. Ein Image ist ein fertiges Softwarepaket, z. B. eine virtuelle Festplatte (VHD-Datei) oder eine virtuelle DVD-Disc (ISO-Datei), mit Hilfe dessen ein virtueller Computer erstellt oder instanziiert wird. Jeder Typ von Benachrichtigung vom Image kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "Image-Status", wenn das Ereignis den Status eines Image beschreibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Image-Migration"

Die Aktion "Image-Migration" gibt Informationen über die Migration virtueller Images über verschiedene Hosts hinweg. Ein Image ist ein fertiges Softwarepaket, z. B. eine virtuelle Festplatte (VHD-Datei) oder eine virtuelle DVD-Disc (ISO-Datei), mit Hilfe derer ein virtueller Computer erstellt oder instanziiert werden kann.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Image öffnen – Aktion

Bei der Aktion "Image öffnen" werden Information zum Öffnen eines Disk-Image oder eines virtuellen Computers in einer Virtualisierungsumgebung ausgegeben. Ein Image ist ein fertiges Softwarepaket, z. B. eine virtuelle Festplatte (VHD-Datei) oder eine virtuelle DVD-Disc (ISO-Datei), mit Hilfe dessen ein virtueller Computer erstellt oder instanziiert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Image-Operation – Aktion

Bei der Image-Operation werden Informationen über allgemeine Operationen im Zusammenhang mit der Funktionsweise eines Image in einer Virtualisierungsumgebung ausgegeben. Ein Image ist ein fertiges Softwarepaket, z. B. eine virtuelle Festplatte (VHD-Datei) oder eine virtuelle DVD-Disc (ISO-Datei), mit Hilfe dessen ein virtueller Computer erstellt oder instanziiert wird. Lässt sich ein Ereignis, das im Rahmen einer normalen Funktion oder Operation eines Image aufgezeichnet wird, nicht präziser einer bestimmten CEG-Aktion zuordnen, kann es dieser Aktion zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Image-Wiederherstellung

Bei der Image-Wiederherstellung werden Informationen ausgegeben, die sich auf das Wiederherstellen eines Image oder das Zurückgreifen auf einen früheren Snapshot in einer Virtualisierungsumgebung beziehen. Ein Image ist ein fertiges Softwarepaket, z. B. eine virtuelle Festplatte (VHD-Datei) oder eine virtuelle DVD-Disc (ISO-Datei), mit Hilfe dessen ein virtueller Computer erstellt oder instanziiert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Image-Status – Aktion

Bei der Aktion "Image-Status" werden Informationen über den Status eines Image in einer Virtualisierungsumgebung ausgegeben. Ein Image ist ein fertiges Softwarepaket, z. B. eine virtuelle Festplatte (VHD-Datei) oder eine virtuelle DVD-Disc (ISO-Datei), mit Hilfe dessen ein virtueller Computer erstellt oder instanziiert wird. Jeder Typ von Statusmeldung in Verbindung mit einem Image kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Image-Warnung – Aktion

Bei der Image-Warnung werden Informationen über Warnungen im Zusammenhang mit einem Image in einer Virtualisierungsumgebung ausgegeben. Ein Image ist ein fertiges Softwarepaket, z. B. eine virtuelle Festplatte (VHD-Datei) oder eine virtuelle DVD-Disc (ISO-Datei), mit Hilfe dessen ein virtueller Computer erstellt oder instanziiert wird. Jeder Typ von Warnung in Bezug auf das Image kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Image-Fehler" zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	4

Image schreiben – Aktion

Bei der Aktion "Image schreiben" werden Informationen über das Schreiben in eine Image-Datei in einer Virtualisierungsumgebung ausgegeben. Ein Image ist ein fertiges Softwarepaket, z. B. eine virtuelle Festplatte (VHD-Datei) oder eine virtuelle DVD-Disc (ISO-Datei), mit Hilfe dessen ein virtueller Computer erstellt oder instanziiert wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Port erstellen – Aktion

Bei der Aktion "Port erstellen" werden Informationen über die Erstellung eines virtuellen Ports ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Port löschen – Aktion

Bei der Aktion "Port löschen" werden Informationen über die Löschung eines virtuellen Ports ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Ressourcen-Pool-Erstellung"

Die Aktion "Ressourcen-Pool-Erstellung" gibt Informationen zur Erstellung eines Ressourcen-Pools auf einem bestimmten Host. Ein Ressourcenpool ist ein Pool aus CPU, Speicher und anderen Systemressourcen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Ressourcen-Pool-Löschung"

Die Aktion "Ressourcen-Pool-Löschung" gibt Informationen zur Löschung eines Ressourcen-Pools auf einem bestimmten Host. Ein Ressourcenpool ist ein Pool aus CPU, Speicher und anderen Systemressourcen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Ressourcen-Pool ändern"

Die Aktion "Ressourcen-Pool ändern" gibt Informationen zur Änderung eines Ressourcen-Pools auf einem bestimmten Host. Ein Ressourcenpool ist ein Pool aus CPU, Speicher und anderen Systemressourcen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Snapshot-Alarm – Aktion

Beim Snapshot-Alarm werden Informationen über Alarmbedingungen im Zusammenhang mit einem Snapshot ausgegeben. Jeder Typ von Alarm in Bezug auf den Snapshot kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Snapshot-Fehler" zugeordnet.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	6

Snapshot-Fehler – Aktion

Beim Snapshot-Fehler werden Informationen über Fehlerbedingungen im Zusammenhang mit Snapshots ausgegeben. Jeder Typ von Fehler in Bezug auf den Snapshot kann dieser Aktion zugeordnet werden. Weniger schwerwiegende Ereignisse sollten der Aktion "Snapshot-Warnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "Snapshot-Alarm" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	5

Snapshot-Warnung – Aktion

Bei der Snapshot-Warnung werden Informationen über Warnbedingungen im Zusammenhang mit Snapshots ausgegeben. Jeder Typ von Warnung in Bezug auf den Snapshot kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Snapshot-Fehler" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	4

Systemerstellung – Aktion

Bei der Systemerstellung werden Informationen über die Erstellung eines Systems ausgegeben. Dieses Ereignis wird in einer virtuellen Umgebung zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Systemlöschung – Aktion

Bei der Systemlöschung werden Informationen über die Deprovisionierung bzw. Löschung eines Systems ausgegeben. Dieses Ereignis wird in einer virtuellen Umgebung zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	entf.	entf.

System-Export – Aktion

Beim System-Export werden Informationen über den Export eines Systems ausgegeben. Dieses Ereignis wird in einer virtuellen Umgebung zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

System-Import – Aktion

Beim System-Import werden Informationen über den Import eines Systems ausgegeben. Dieses Ereignis wird in einer virtuellen Umgebung zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

System-Snapshot – Aktion

Bei der Aktion "System-Snapshot" werden Informationen über die Erstellung eines Snapshot von einem virtuellen Computer oder virtuellen Image ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Virtualisierungsverwaltungsklasse

Aktion "Anwendungserstellung"

Die Aktion "Anwendungserstellung" gibt Informationen zur Erstellung einer Anwendung in einer Virtualisierungsumgebung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Anwendung ändern"

Die Aktion "Anwendung ändern" gibt Informationen zur Änderung einer Anwendung in einer Virtualisierungsumgebung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Anwendungsbenachrichtigung"

Die Aktion "Anwendungsbenachrichtigung" gibt Informationen zu Benachrichtigungen über virtualisierte Anwendungen in einer Virtualisierungsumgebung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Anwendungslöschung"

Die Aktion "Anwendungslöschung" gibt Informationen zur Löschung einer Anwendung in einer Virtualisierungsumgebung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Komponentenerstellung"

Die Aktion "Komponentenerstellung" gibt Informationen zur Erstellung einer beliebigen Art von Komponente in einer Virtualisierungsumgebung. In diesem Zusammenhang bezieht sich Komponente auf anbieterspezifische Objekte, die in einer virtuellen Umgebung erstellt werden. Sie können das Feld "dest_objectclass" verwenden, um die Klasse der Komponente zuzuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Komponentenlöschung"

Die Aktion "Komponentenlöschung" gibt Informationen zur Löschung einer beliebigen Art von Komponente in einer Virtualisierungsumgebung. In diesem Zusammenhang bezieht sich Komponente auf anbieterspezifische Objekte, die in einer virtuellen Umgebung erstellt werden. Sie können das Feld "dest_objectclass" verwenden, um die Klasse der Komponente zuzuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Komponente ändern"

Die Aktion "Komponente ändern" gibt Informationen zur Änderung einer beliebigen Art von Komponente in einer Virtualisierungsumgebung. In diesem Zusammenhang bezieht sich Komponente auf anbieterspezifische Objekte, die in einer virtuellen Umgebung erstellt werden. Sie können das Feld "dest_objectclass" verwenden, um die Klasse der Komponente zuzuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Komponentenbenachrichtigung"

Die Aktion "Komponentenbenachrichtigung" gibt Informationen zu Benachrichtigungen über jede beliebige Komponente in einer Virtualisierungsumgebung. In diesem Zusammenhang bezieht sich Komponente auf anbieterspezifische Objekte, die in einer virtuellen Umgebung erstellt werden. Sie können das Feld "dest_objectclass" verwenden, um die Klasse der Komponente zuzuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "System aktivieren"

Die Aktion "System aktivieren" gibt Informationen zur Aktivierung eines Systems in einer virtualisierten Umgebung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Systemhinzufügung"

Die Aktion "Systemhinzufügung" gibt Informationen über die Registrierung oder Hinzufügung eines Systems bei bzw. zu einer virtuellen Verwaltungsplattform zwecks Überwachung und Verwaltung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "System verbinden"

Die Aktion "System verbinden" gibt Informationen über die erfolgreiche Erstellung einer Verbindung zwischen einer virtuellen Verwaltungsplattform und einem System zwecks Überwachung und Verwaltung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Systemtrennung"

Die Aktion "Systemtrennung" gibt Informationen zur Trennung eines Systems von einer virtuellen Verwaltungsplattform.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Systemerkennung"

Die Aktion "Systemerkennung" gibt Informationen zur Erkennung eines Systems durch eine virtuelle Verwaltungsplattform.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Systemänderung"

Die Aktion "Systemänderung" gibt Informationen zur Änderung eines Systems in einer Virtualisierungsumgebung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Systementfernung"

Die Aktion "Systementfernung" gibt Informationen zur Entfernung eines Systems von einer virtuellen Verwaltungsplattform.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Kapitel 11: Kategorie "Physischer Zugriff"

Dieses Kapitel enthält folgende Themen:

Klasse für physische Zugriffsaktivität

Badge-Scan

Beim Badge-Scan werden Informationen über die physische Aktion eines Badges angezeigt, das von einem Badge-Scanner an einem physischen Zugriffspunkt gescannt wird.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Tertiär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto der Badge an welchem Ort gescannt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Kameradeaktivierung

Bei der Kameradeaktivierung werden Informationen zur physischen Aktion einer Kamera angezeigt, die in den deaktivierten Zustand wechselt.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Kamera auf welchem Host deaktiviert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Kameraaktivierung

Bei der Kameraaktivierung werden Informationen zur physischen Aktion einer Kamera angezeigt, die in den aktivierten Zustand wechselt.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Kamera auf welchem Host aktiviert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	4

Kamera nicht verfügbar

Bei der Aktion "Kamera nicht verfügbar" werden Informationen zur Verfügbarkeit einer Kamera angezeigt. Dies kann mit der Netzwerkverfügbarkeit, den Kabelanschlüsse usw. zusammenhängen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Kamera an welchem Standort nicht verfügbar ist. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	4

Schließen der Tür

Beim Schließen der Tür werden Informationen zur physischen Aktion beim Schließen einer Tür angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Tür an welchem Standort geschlossen wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	5

Öffnen einer Tür

Beim Öffnen der Tür werden Informationen zur physischen Aktion beim Öffnen einer Tür angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Tür an welchem Standort geöffnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	5

Schließen eines Fensters

Beim Schließen eines Fensters werden Informationen zum physischen Vorgang des Schließens eines Fensters ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Fenster an welchem Standort geschlossen wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	5

Öffnen eines Fensters

Beim Öffnen eines Fensters werden Informationen zum physischen Vorgang des Öffnens eines Fensters ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Fenster an welchem Standort geöffnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	4

Kapitel 12: Kategorie "Ressourcenzugriff"

Dieses Kapitel enthält folgende Themen:

Anwendungsaktivitätsklasse

Aktion "Anwendungszugriff"

Die Aktion "Anwendungszugriff" gibt Informationen über das Zugreifen auf eine Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Objektzugriff"

Die Aktion "Objektzugriff" gibt Informationen über das Zugreifen auf ein Objekt in einer Anwendung. In diesem Zusammenhang ist ein Objekt eine Unterkomponente einer Anwendung, zum Beispiel ein COM-Objekt, eine DLL oder ein Shared Object.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Klasse für Verzeichnisaktivität

Verzeichnisalarm – Aktion

Beim Verzeichnisalarm werden Informationen über Alarmbedingungen im Zusammenhang mit Verzeichnisaktivitäten ausgegeben. In diesem Kontext bezieht sich "Verzeichnis" auf universell einsetzbare, verteilte, hierarchische, objektorientierte Verzeichnistechnologien wie X.500 und LDAP Directory Services. Jeder Typ von Alarm in Bezug auf das Verzeichnis kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Verzeichnisfehler" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	6

Verzeichnisfehler – Aktion

Beim Verzeichnisfehler werden Informationen über Fehlerbedingungen im Zusammenhang mit Verzeichnisaktivitäten ausgegeben. In diesem Kontext bezieht sich "Verzeichnis" auf universell einsetzbare, verteilte, hierarchische, objektorientierte Verzeichnistechnologien wie X.500 und LDAP Directory Services. Jeder Typ von Fehler in Bezug das Verzeichnis kann dieser Aktion zugeordnet werden. Weniger schwerwiegende Ereignisse sollten der Aktion "Verzeichniswarnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "Verzeichnisalarm" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär

Informationen	Ebene
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	5

Verzeichnisbenachrichtigung – Aktion

Bei der Verzeichnisbenachrichtigung werden Informationen zu Benachrichtigungen und Meldungen ausgegeben, die von der Verzeichnisaktivität generiert werden. In diesem Kontext bezieht sich "Verzeichnis" auf universell einsetzbare, verteilte, hierarchische, objektorientierte Verzeichnistechnologien wie X.500 und LDAP Directory Services. Jeder Typ von Benachrichtigung aus dem Verzeichnis kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "Verzeichnisstatus", wenn das Ereignis den Status eines Verzeichnisses beschreibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär

Informationen	Ebene
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verzeichnisoperation – Aktion

Bei der Verzeichnisoperation werden Informationen über allgemeine Operationen im Zusammenhang mit der Arbeitsweise eines Verzeichnisses ausgegeben. In diesem Kontext bezieht sich "Verzeichnis" auf universell einsetzbare, verteilte, hierarchische, objektorientierte Verzeichnistechnologien wie X.500 und LDAP Directory Services. Lässt sich ein Ereignis, das im Rahmen einer normalen Funktion oder Operation eines Verzeichnisses aufgezeichnet wird, nicht präziser einer bestimmten CEG-Aktion zuordnen, kann es dieser Aktion zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär

Informationen	Ebene
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verzeichnisstatus – Aktion

Bei der Aktion "Verzeichnisstatus" werden Informationen über den Status eines Verzeichnisses ausgegeben. In diesem Kontext bezieht sich "Verzeichnis" auf universell einsetzbare, verteilte, hierarchische, objektorientierte Verzeichnistechnologien wie X.500 und LDAP Directory Services. Jeder Typ von Statusmeldung in Bezug auf ein Verzeichnis kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Verzeichniswarnung – Aktion

Bei der Verzeichniswarnung werden Informationen über Warnungen im Zusammenhang mit einem Verzeichnis ausgegeben. In diesem Kontext bezieht sich "Verzeichnis" auf universell einsetzbare, verteilte, hierarchische, objektorientierte Verzeichnistechnologien wie X.500 und LDAP Directory Services. Jeder Typ von Warnung in Bezug auf ein Verzeichnis kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Verzeichnisfehler" zugeordnet werden.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	entf.	entf.
Fehler	F	4

Klasse für Ressourcenaktivität

Ressourcenzugriff

Beim Ressourcenzugriff geht es um Zugriffsanforderungen für eine bestimmte Ressource auf einem bestimmten System oder in einer bestimmten Anwendung.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer auf welche Ressource auf welchem Host zugegriffen hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Ressourcenalarm – Aktion

Bei der Aktion "Ressourcenalarm" werden Informationen über Alarmbedingungen ausgegeben, die sich auf eine spezielle Ressource auf einem bestimmten System oder in einer bestimmten Anwendung beziehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Ressourcenzuweisung

Bei der Ressourcenzuweisung werden Ressourcen auf einem bestimmten System oder in einer bestimmten Anwendung zugewiesen.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Ressource auf welchem Host zugewiesen hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Schließen der Ressource

Beim Schließen der Ressource wird eine bestimmte Ressource auf einem bestimmten System oder in einer bestimmten Anwendung geschlossen.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Ressource auf welchem Host geschlossen hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Ressource kopieren – Aktion

Bei der Aktion "Ressource kopieren" werden Informationen zum Kopieren einer bestimmten Ressource von einem bestimmten System bzw. einer Anwendung auf ein anderes System ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ressourcenerstellung

Bei der Ressourcenerstellung wird eine bestimmte Ressource auf einem System oder in einer Anwendung erstellt.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Ressource auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Ressourcenlöschung

Bei der Ressourcenlöschung wird eine bestimmte Ressource auf einem System oder in einer Anwendung gelöscht.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Ressource auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Ressourcenfehler – Aktion

Bei der Aktion "Ressourcenfehler" werden Informationen ausgegeben, die sich auf Fehler im Zusammenhang mit einer Ressource auf einem bestimmten System oder in einer bestimmten Anwendung beziehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene	
Ergebnis - Informationen	Primär	
Ergebnis	**event_result**	**event_severity**
Fehler	F	4

Ressourcenausführung

Bei der Ressourcenausführung wird eine bestimmte Ressource auf einem System oder in einer Anwendung ausgeführt.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Ressource auf welchem Host ausgeführt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Ressource blockieren – Aktion

Bei der Aktion "Ressource blockieren" werden Informationen über das Blockieren einer Ressource zur Verhinderung von Vorgängen wie Löschen, Verschieben etc. ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Ressourcenimport"

Die Aktion "Ressourcenimport" gibt Informationen über das Importieren einer Ressource aus einer externen Ressource.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Ressourcenauflistung

Zum Beispiel "lsrset" mit verschiedenen Optionen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Sekundär
Quelle - Prozessinformationen	Sekundär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ressource markiert – Aktion

Bei der Aktion "Ressource markiert" werden Informationen ausgegeben, die sich auf das Kennzeichnen, Kommentieren und Markieren einer Ressource in einem System oder einer Anwendung beziehen. Dies erfolgt mit Hilfe von Metadaten und dient unter anderem der leichteren Referenz.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ressourcenänderung

Bei der Ressourcenänderung wird eine bestimmte Ressource auf einem System oder in einer Anwendung geändert.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Ressource auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Ressource verschieben – Aktion

Bei der Aktion "Ressource verschieben" werden Informationen zum Verschieben von Ressourcen zwischen Systemen und Anwendungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Öffnen einer Ressource

Beim Öffnen einer Ressource wird eine bestimmte Ressource auf einem System oder in einer Anwendung geöffnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welche Ressource auf welchem Host geöffnet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Ressourcenaktualisierung – Aktion

Bei der Ressourcenaktualisierung werden Informationen zur Aktualisierung einer bestimmten Ressource ausgegeben, beispielsweise im Cache befindliche Dateien auf einem bestimmten System bzw. in einer bestimmten Anwendung oder zwischengespeicherte Ressourcen auf einem Proxyserver.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Ressourcenreplikation – Aktion

Bei der Ressourcenreplikation werden Informationen zur Replikation einer Ressource in einem System oder einer Anwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ressourcensuche – Aktion

Bei der Ressourcensuche werden Informationen zur Suche nach einer Ressource in einem System oder einer Anwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ressourcenstatus – Aktion

Bei der Aktion "Ressourcenstatus" werden Informationen zum Status einer speziellen Ressource auf einem bestimmten System oder in einer bestimmten Anwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ressourcenwarnung – Aktion

Bei der Aktion "Ressourcenwarnung" werden Informationen über Warnungen ausgegeben, die sich auf eine spezielle Ressource auf einem bestimmten System oder in einer bestimmten Anwendung beziehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	3

ACL-Festlegung – Aktion

Bei der ACL-Festlegung werden Informationen zur Erstellung oder Änderung einer Zugriffssteuerungsliste (Access Control List) auf einem bestimmten Zielobjekt, z. B. Datei, Prozess, System oder Anwendung, ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Suchbedingung festlegen – Aktion

Bei der Aktion "Suchbedingung festlegen" werden Informationen ausgegeben, die sich auf die Festlegung von Suchkriterien oder Artefakten zur Extrahierung von Datensätzen und Informationen aus einem Dateisystem oder Repository beziehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Versionskontrolle – Klasse

Ressourcen-Checkin – Aktion

Beim Ressourcen-Checkin werden Informationen zum Einchecken einer versionskontrollierten Ressource nach standardmäßigen HTTP- und WebDAV-Methoden ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ressourcen-Checkout – Aktion

Beim Ressourcen-Checkout werden Informationen zum Auschecken einer versionskontrollierten Ressource ausgegeben. Durch den Checkout können die Inhalte oder veraltete Eigenschaften der Ressource geändert werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ressourcenerstellung

Bei der Ressourcenerstellung werden Informationen zur Erstellung von versionskontrollierten Ressourcen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ändern der Ressourcenbezeichnung – Aktion

Beim Ändern der Ressourcenbezeichnung werden Informationen über die Änderung eines Strings ausgegeben, mit dem innerhalb eines Versionsverlaufs Versionen voneinander unterschieden werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ressourcenzusammenführung – Aktion

Bei der Ressourcenzusammenführung werden Informationen über die Zusammenführung der versionskontrollierten Ressourcen eines Benutzers und der von einem anderen Benutzer erstellten Ressourcenversionen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ressourcensuche – Aktion

Bei der Ressourcensuche werden Informationen zur Suche von versionskontrollierten Ressourcen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ressourcen-Checkout annulieren – Aktion

Bei der Aktion "Ressourcen-Checkout annulieren" werden Informationen zu Anfragen ausgegeben, den Checkout-Status einer ausgecheckten versionskontrollierten Ressource rückgängig zu machen und den Ressourcenstatus vor dem Checkout wiederherzustellen.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	2
Fehler	F	3

Ressourcen-Update – Aktion

Beim Ressourcen-Update werden Informationen zur Versionsänderung ausgegeben, d. h. bei Änderung der aktuellen Version einer eingecheckten, versionskontrollierten Ressource in eine andere, historische Version.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Versionsstatus"

Die Aktion "Versionsstatus" gibt Informationen über den Status einer Version.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Kapitel 13: Kategorie "SIM-Vorgänge"

Dieses Kapitel enthält folgende Themen:

Klasse der Alarmverwaltung

Alarmbestätigung

Die Alarmbestätigung behandelt die Bestätigung eines Alarms auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welchen Alarm auf welchem Host bestätigt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Alarmanmerkung

Die Alarmanmerkung behandelt die Anmerkung eines Alarms auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welchen Alarm auf welchem Host mit Anmerkungen versehen hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Alarmerstellung

Die Alarmerstellung behandelt die Erstellung eines Alarms auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welchen Alarm auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Alarmlöschung

Die Alarmlöschung behandelt die Löschung eines Alarms auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welchen Alarm auf welchem Host gelöscht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Alarmübermittlung

Die Alarmübermittlung behandelt die Übermittlung eines Alarms von einem bestimmten Host an einen anderen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Alarm von welchem Host an welchen anderen Host übermittelt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Alarmeskalation

Die Alarmeskalation behandelt die Eskalation eines Alarms auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär

Informationen	Ebene
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welchen Alarm auf welchem Host eskaliert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Alarmjob-Änderung

Bei der Alarmjob-Änderung werden Informationen zum Ändern von für die Überprüfung von Alarmbedingungen geplanten Jobs ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Alarmjob-Entfernung

Bei der Alarmjob-Entfernung werden Informationen zum Löschen von für die Überprüfung von Alarmbedingungen geplanten Jobs ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Alarmjob-Einrichtung

Bei der Alarmjob-Einrichtung werden Informationen zur Planung von Jobs zur Überprüfung von Alarmbedingungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Alarmänderung

Die Alarmänderung behandelt die Änderung eines Alarms auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welchen Alarm auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse der Baseline-Verwaltung

Baseline-Akzeptanz

Die Baseline-Akzeptanz behandelt die Akzeptanz einer Baseline auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Baseline auf welchem Host akzeptiert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Baseline-Aktivierung

Die Baseline-Aktivierung behandelt die Aktivierung einer Baseline auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Baseline auf welchem Host aktiviert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Baseline-Erstellung

Die Baseline-Erstellung behandelt die Erstellung einer Baseline auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Baseline auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Baseline-Deaktivierung

Die Baseline-Deaktivierung behandelt die Deaktivierung einer Baseline auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Baseline auf welchem Host deaktiviert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Baseline-Definition

Die Baseline-Definition behandelt die Definition einer Baseline auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Baseline auf welchem Host definiert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Baseline-Änderung

Die Baseline-Änderung behandelt die Änderung einer Baseline auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Baseline auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Klasse der Ereignisquellenverwaltung

Ereignisquellenautorisierung

Die Ereignisquellenautorisierung behandelt die Autorisierung einer Ereignisquelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär

Informationen	Ebene
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Ereignisquelle auf welchem Host autorisiert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ereignisquellenkonfiguration

Die Ereignisquellenkonfiguration behandelt die Konfiguration einer Ereignisquelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär

Informationen	Ebene
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Ereignisquelle auf welchem Host konfiguriert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ereignisquellenentdeckung

Die Ereignisquellenentdeckung behandelt die Entdeckung einer Ereignisquelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär

Informationen	Ebene
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Host welche Ereignisquelle auf welchem Host entdeckt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ereignisquellenbereitstellung

Die Ereignisquellenbereitstellung behandelt die Bereitstellung einer Ereignisquelle auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär

Informationen	Ebene
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Ereignisquelle auf welchem Host bereitgestellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ereignistrend

Bei der Aktion Ereignistrend werden Informationen zu allen Daten, für die ein Trend erzeugt wurde, angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär

Informationen	Ebene
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Ereignisquelle auf welchem Host bereitgestellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Externer Daten-Input – Aktion

Bei der Aktion "Externer Daten-Input" werden Informationen zum Import externer Daten ausgegeben, welche aus anderen Quellen in SIM- und Protokollverwaltungstools wie CA Enterprise Log Manager für Event Correlation und kontextabhängige Berichterstellung übernommen werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Externer Daten-Output – Aktion

Bei der Aktion "Externer Daten-Output" werden Informationen zum Import interner Daten ausgegeben, welche aus SIM- und Protokollverwaltungstools wie CA Enterprise Log Manager zu Prozessautomatisierungs- und Alarmzwecken in externe Quellen übernommen werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse der Vorfallverwaltung

Schließen des Vorfalls

Das Schließen des Vorfalls behandelt das Schließen eines Vorfalls auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Vorfall auf welchem Host geschlossen wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2

Ergebnis	event_result	event_severity
Fehler	F	3

Vorfallerstellung

Die Vorfallerstellung behandelt das Erstellen eines Vorfalls auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Vorfall auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Vorfalllöschung

Die Vorfalllöschung behandelt das Löschen eines Vorfalls auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Vorfall auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Vorfalländerung

Die Vorfalländerung behandelt das Ändern eines Vorfalls auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Vorfall auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Vorfallauflösung

Die Vorfallauflösung behandelt das Auflösen eines Vorfalls auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Vorfall auf welchem Host aufgelöst wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse der Untersuchungsverwaltung

Untersuchung mit Anmerkungen versehen

Die Aktion "Untersuchung mit Anmerkungen versehen" behandelt die Anmerkungen einer Untersuchung auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Untersuchung auf welchem Host mit Anmerkungen versehen wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Schließen der Untersuchung

Das Schließen der Untersuchung behandelt das Schließen einer Untersuchung auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Untersuchung auf welchem Host geschlossen wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Löschen der Untersuchung

Das Löschen der Untersuchung behandelt das Löschen einer Untersuchung auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Untersuchung auf welchem Host gelöscht wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Andern der Untersuchung

Das Ändern der Untersuchung behandelt die Änderung einer Untersuchung auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Untersuchung auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Öffnen der Untersuchung

Das Öffnen der Untersuchung behandelt das Öffnen einer Untersuchung auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Untersuchung auf welchem Host geöffnet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Anhalten der Untersuchung

Das Anhalten der Untersuchung behandelt das Anhalten einer Untersuchung auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Untersuchung auf welchem Host angehalten wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Auflösen der Untersuchung

Das Auflösen der Untersuchung behandelt das Auflösen einer Untersuchung auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär

Informationen	Ebene
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Untersuchung auf welchem Host aufgelöst wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Fortsetzen der Untersuchung

Das Fortsetzen der Untersuchung behandelt das Fortsetzen einer angehaltenen Untersuchung auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Untersuchung auf welchem Host fortgesetzt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse der Benachrichtigungsverwaltung

Benachrichtigungserstellung

Die Benachrichtigungserstellung behandelt das Erstellen einer Benachrichtigung auf einem bestimmten Host.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär

Informationen	Ebene
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welche Benachrichtigung auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Benachrichtigungsübermittlung

Die Benachrichtigungsübermittlung behandelt die Übermittlung einer Benachrichtigung von einem bestimmten Host an einen anderen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär

Informationen	Ebene
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Benachrichtigung von welchem Host an welchen anderen Host übermittelt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse für Anforderungsverwaltung

Anforderungsbestätigung

Bei der Anforderungsbestätigung wird eine Anforderung auf einem bestimmten Host bestätigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Anforderung auf welchem Host bestätigt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2

Ergebnis	event_result	event_severity
Fehler	F	3

Anforderungsanmerkung

Bei der Anforderungsanmerkung wird eine Anforderung auf einem bestimmten Host mit Anmerkungen versehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Anforderung auf welchem Host mit Anmerkungen versehen hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Schließen der Anforderung

Beim Schließen der Anforderung wird eine Anforderung auf einem bestimmten Host geschlossen.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Anforderung auf welchem Host geschlossen hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Anforderungserstellung

Mit der Anforderungserstellung wird eine Anforderung auf einem bestimmten Host erstellt.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Anforderung auf welchem Host erstellt hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Anforderungsübermittlung

Bei der Anforderungsübermittlung wird eine Anforderung von einem bestimmten Host an einen anderen übermittelt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Primär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Anforderung von welchem Host an welchen anderen Host übermittelt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Anforderungsänderung

Bei der Anforderungsänderung wird eine Anforderung auf einem bestimmten Host geändert.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Anforderung auf welchem Host geändert hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Kapitel 14: Kategorie "Systemzugriff"

Dieses Kapitel enthält folgende Themen:

Zugriffsverwaltung – Klasse

Sicherheitsdomänenerstellung – Aktion

Bei der Sicherheitsdomänenerstellung werden Informationen über die Erstellung einer Sicherheitsdomäne ausgegeben. In einer Sicherheitsdomäne sind eine Reihe von Personen, Daten, Systeme oder Geräte zusammengefasst, die an eine Sicherheitsrichtlinie gebunden sind, z. B. Umfangsbeschreibung einer Sicherheitsrichtlinie.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Sicherheitsdomänenlöschung – Aktion

Bei der Sicherheitsdomänenlöschung werden Informationen über die Löschung einer Sicherheitsdomäne ausgegeben. In einer Sicherheitsdomäne sind eine Reihe von Personen, Daten, Systeme oder Geräte zusammengefasst, die an eine Sicherheitsrichtlinie gebunden sind, z. B. Umfangsbeschreibung einer Sicherheitsrichtlinie.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Sicherheitsdomänenänderung

Bei der Sicherheitsdomänenänderung werden Informationen über die Änderung einer Sicherheitsdomäne ausgegeben. In einer Sicherheitsdomäne sind eine Reihe von Personen, Daten, Systeme oder Geräte zusammengefasst, die an eine Sicherheitsrichtlinie gebunden sind, z. B. Umfangsbeschreibung einer Sicherheitsrichtlinie.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Änderung der Sicherheitsbezeichnung – Aktion

Bei der Änderung der Sicherheitsdomäne werden Informationen zur Änderung von Sicherheitsbezeichnungen wie den Bezeichnungen in einer MAC-Umgebung (Mandatory Access Control) ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse der Authentifizierung

Authentifizierung

Bei der Authentifizierung werden Ereignisinformationen zur Authentifizierung von Anmeldeinformationen angezeigt, die für eine Validierung bereitgestellt wurden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welches Konto auf welchem Host versucht hat zu authentifizieren. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Authentifizierung deaktivieren"

Die Aktion "Authentifizierung deaktivieren" gibt Informationen über das Deaktivieren des Authentifizierungsmoduls auf einem System.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär

Informationen	Ebene
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	5
Fehler	F	5

Aktion "Authentifizierung aktivieren"

Die Aktion "Authentifizierung aktivieren" gibt Informationen über das Aktivieren des Authentifizierungsmoduls auf einem System.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	5
Fehler	F	5

Authentifizierungsfehler – Aktion

Bei der Aktion "Authentifizierungsfehler" werden Informationen zu Fehlerbedingungen in einem Authentifizierungsmodul oder während des Authentifizierungsvorgangs ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Authentifizierungs-Fallback

Beim Authentifizierungs-Fallback werden Ereignisinformationen zum Authentifizierungs-Fallback für eine zweite Methode der Validierung von Anmeldeinformationen angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Host auf welche Authentifizierungsmethode zurückgegriffen hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	6

Authentifizierungsbenachrichtigung – Aktion

Bei der Authentifizierungsbenachrichtigung werden Informationen zu Benachrichtigungen in einem Authentifizierungsmodul oder während des Authentifizierungsvorgangs ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	3

Authentifizierungspaket geladen

Bei der Aktion "Authentifizierungspaket geladen" werden Ereignisinformationen zum Laden eines Authentifizierungspakets zur Validierung von Anmeldeinformationen auf einem bestimmten Host oder einer bestimmten Anwendung angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Host welches Authentifizierungspaket geladen hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	3
Fehler	F	3

Authentifizierungsstart

Beim Authentifizierungsstart werden Ereignisinformationen zum Starten eines Authentifizierungspakets auf einem bestimmten Host oder einer bestimmten Anwendung angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Host welches Authentifizierungspaket gestartet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	6

Authentifizierungswarnung – Aktion

Bei der Authentifizierungswarnung werden Informationen zu Warnmeldungen in einem Authentifizierungsmodul oder während des Authentifizierungsvorgangs ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Autorisierung

Bei der Autorisierung werden Ereignisinformationen zur Autorisierung von Anmeldeinformationen angezeigt, die für eine Validierung bereitgestellt wurden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, wer welches Konto auf welchem Host versucht hat zu autorisieren. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Sicherheitsbereichserstellung – Aktion

Bei der Sicherheitsbereichserstellung werden Informationen zur Erstellung eines Sicherheitsbereichs ausgegeben. Der Sicherheitsbereich steht für einen benannten Bestand an Benutzern, Gruppen oder Ressourcen, der in einer Zugriffssteuerungsrichtlinie referenziert ist.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär

Informationen	Ebene
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Sicherheitsbereichslöschung – Aktion

Bei der Sicherheitsbereichslöschung werden Informationen zum Löschen eines Sicherheitsbereichs ausgegeben. Der Sicherheitsbereich steht für einen benannten Bestand an Benutzern, Gruppen oder Ressourcen, der in einer Zugriffssteuerungsrichtlinie referenziert ist.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär

Informationen	Ebene
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Gruppenfestlegung – Aktion

Bei der Berechtigungsbeendigung werden Informationen zur Änderung realer Gruppen, effektiver Gruppen und des Gruppenbesitzes von Zielobjekten (Prozess, Datei, System) ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Vertrauensbereichsalarm – Aktion

Beim Vertrauensbereichsalarm werden Informationen über Alarmbedingungen im Zusammenhang mit vertrauenswürdigen Bereichen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Vertrauensbereichsfehler – Aktion

Beim Vertrauensbereichsfehler werden Informationen über Fehler im Zusammenhang mit vertrauenswürdigen Bereichen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Vertrauensbereichswarnung – Aktion

Bei der Vertrauensbereichswarnung werden Informationen über Warnungen im Zusammenhang mit vertrauenswürdigen Bereichen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	3

Autorisierungsaktivität – Klasse

Autorisierungsalarm – Aktion

Beim Autorisierungsalarm werden Informationen über Alarmbedingungen während einer Autorisierungsaktivität ausgegeben. Eine Autorisierungsaktivität umfasst das Einrichten von Berechtigungen in Bezug auf Objekte, Systeme und Anwendungen. Diese Berechtigungen gelten für Subjekte wie Benutzer- oder Systemkonten, Hosts usw. Jeder Typ von Alarm in Bezug auf die Autorisierung kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Autorisierungsfehler" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	6

Aktion "Autorisierungsfehler"

Die Aktion "Autorisierungsfehler" gibt Informationen über Fehlerbedingungen, die während einer Autorisierungsaktivität auftreten. Eine Autorisierungsaktivität umfasst das Einrichten von Berechtigungen in Bezug auf Objekte, Systeme und Anwendungen. Diese Berechtigungen gelten für Subjekte wie Benutzer- oder Systemkonten, Hosts usw. Jeder Typ von Fehler in Bezug auf die Autorisierung kann dieser Aktion zugeordnet werden. Weniger schwerwiegende Ereignisse sollten der Aktion "Autorisierungswarnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "Autorisierungsalarm" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	entf.	entf.
Fehler	F	5

Autorisierungsbenachrichtigung – Aktion

Bei der Autorisierungsbenachrichtigung werden Informationen über Benachrichtigungen angegeben, die während einer Autorisierungsaktivität vom System oder von der Autorisierungs-Engine ausgegeben werden. Eine Autorisierungsaktivität umfasst das Einrichten von Berechtigungen in Bezug auf Objekte, Systeme und Anwendungen. Diese Berechtigungen gelten für Subjekte wie Benutzer- oder Systemkonten, Hosts usw. Jeder Typ von Benachrichtigung von der Autorisierung kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt. Verwenden Sie die Aktion "Autorisierungsstatus", wenn das Ereignis den Status einer Autorisierungsaktivität beschreibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär

Informationen	Ebene
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Autorisierungsstatus – Aktion

Bei der Aktion "Autorisierungsstatus" werden Informationen zum Status einer Autorisierungsaktivität ausgegeben, die vom System oder der Autorisierungs-Engine aufgezeichnet wird. Eine Autorisierungsaktivität umfasst das Einrichten von Berechtigungen in Bezug auf Objekte, Systeme und Anwendungen. Diese Berechtigungen gelten für Subjekte wie Benutzer- oder Systemkonten, Hosts usw. Jeder Typ von Statusmeldung in Verbindung mit einer Autorisierung kann dieser Aktion zugeordnet werden, wenn sich das Ereignis nicht präziser einer bestimmten Aktion zuordnen lässt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär

Informationen	Ebene
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Autorisierungswarnung – Aktion

Bei der Aktion "Autorisierungswarnung" werden Informationen über Warnbedingungen ausgegeben, die während einer Autorisierungsaktivität ausgelöst werden. Eine Autorisierungsaktivität umfasst das Einrichten von Berechtigungen in Bezug auf Objekte, Systeme und Anwendungen. Diese Berechtigungen gelten für Subjekte wie Benutzer- oder Systemkonten, Hosts usw. Jeder Typ von Warnung in Bezug auf die Autorisierung kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Autorisierungsfehler" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär

Informationen	Ebene
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	4

Berechtigungsbeendigung – Aktion

Bei der Berechtigungsbeendigung werden Informationen zum Ablauf von Berechtigungsdaten wie bereitgestellte Anmeldeinformationen zu Validierungszwecken oder Informationen zur Auflösung von Berechtigungsumgebungen ausgegeben. Durch diese Aktion ist das Subjekt (Benutzer, Prozess oder System) gezwungen, dem Zielobjekt (System, Prozess) eine erneute Berechtigung zu erteilen.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär

Informationen	Ebene
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Ablauf des Autorisierungstoken – Aktion

Bei der Aktion "Ablauf des Autorisierungstoken" werden Informationen zum Ablauf eines Authentifizierungstoken ausgegeben, das zu Validierungszwecken während einer Authentifizierungssitzung bereitgestellt wurde.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär

Informationen	Ebene
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Berechtigungsalarm – Aktion

Beim Berechtigungsalarm werden Informationen über Alarmbedingungen im Zusammenhang mit Berechtigungen ausgegeben. Jeder Typ von Alarm in Bezug auf Berechtigungen kann dieser Aktion zugeordnet werden. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, wird sie der Aktion "Berechtigungsfehler" zugeordnet.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Tertiär

Informationen	Ebene
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	6

Berechtigungsfehler – Aktion

Bei der Aktion "Berechtigungsfehler" werden Informationen über Fehlerbedingungen im Zusammenhang mit Berechtigungen ausgegeben. Jeder Typ von Fehler in Bezug auf Berechtigungen kann dieser Aktion zugeordnet werden. Weniger schwerwiegende Ereignisse sollten der Aktion "Berechtigungswarnung" zugeordnet werden. Schwerwiegendere Ereignisse mit sofortigem Handlungsbedarf sollten der Aktion "Berechtigungsalarm" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär

Informationen	Ebene
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	5

Berechtigungswarnung – Aktion

Bei der Berechtigungswarnung werden Informationen über Warnungen im Zusammenhang mit Berechtigungsaktivitäten ausgegeben. Jeder Typ von Warnung in Bezug auf Berechtigungen kann dieser Aktion zugeordnet werden. Schwerwiegendere Ereignisse sollten der Aktion "Berechtigungsfehler" zugeordnet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär

Informationen	Ebene
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	entf.	entf.
Fehler	F	4

Klasse der Anmeldeaktivität

Anmeldeversuch

Beim Anmeldeversuch werden Ereignisinformationen zum Anmeldeversuch eines Kontos auf einem bestimmten Host oder einer bestimmten Anwendung angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär

Informationen	Ebene
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto sich auf welchem Host versucht anzumelden. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse der Abmeldeaktivität

Abmeldeaktion

Bei der Abmeldeaktion werden Ereignisinformationen zum Abmelden eines Kontos auf einem bestimmten Host oder einer bestimmten Anwendung angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto sich auf welchem Host abgemeldet hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse für Berechtigungserlangung

Berechtigungserlangung

Bei der Berechtigungserlangung werden Ereignisinformationen zum Versuch eines Kontos angezeigt, Berechtigungen für einen bestimmten Host oder eine bestimmte Anwendung zu erlangen.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Berechtigung auf welchem Host zu erlangen versucht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	3
Fehler	F	3

Klasse für Berechtigungsverwendung

Berechtigungsverwendung

Bei der Berechtigungsverwendung werden Ereignisinformationen zum Versuch eines Kontos angezeigt, Berechtigungen für einen bestimmten Host oder eine bestimmte Anwendung zu verwenden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär

Informationen	Ebene
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welches Konto welche Berechtigung auf welchem Host zu verwenden versucht hat. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	3
Fehler	F	3

Klasse für Sitzungsaktivität

Aktion "Sitzungs-Alert"

Die Aktion "Sitzungs-Alert" gibt Informationen zu mit Sitzungen in Verbindung stehenden Alert-Bedingungen. Sie können dieser Aktion jede beliebige Art von Sitzungs-Alert zuordnen. Wenn es sich um eine Fehlerbedingung handelt, die keiner sofortigen Beachtung bedarf, können Sie sie der Aktion "Sitzungsfehler" zuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär

Informationen	Ebene
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	7

Sitzungserstellung

Mit der Sitzungserstellung wird eine Sitzung auf einem bestimmten Host oder in einer bestimmten Anwendung erstellt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär

Informationen	Ebene
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Sitzung auf welchem Host erstellt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Sitzungstrennung

Bei der Sitzungstrennung werden Ereignisinformationen im Zusammenhang mit der Trennung einer Sitzung auf einem bestimmten Host oder in einer bestimmten Anwendung angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär

Informationen	Ebene
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Sitzung auf welchem Host getrennt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Aktion "Sitzungsfehler"

Die Aktion "Sitzungsfehler" gibt Informationen zu mit Sitzungen in Verbindung stehenden Fehlerbedingungen. Sie können dieser Aktion jede beliebige Art von Sitzungsfehler zuordnen. Weniger schwerwiegende Ereignisse sollten der Aktion "Sitzungswarnung" zugeordnet werden. Sie können schwerwiegendere Ereignisse, die sofortiger Beachtung bedürfen, der Aktion "Sitzungs-Alert" zuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	5

Sitzungsänderung

Mit der Sitzungsänderung wird eine Sitzung auf einem bestimmten Host oder in einer bestimmten Anwendung geändert.

Informationen	Ebene
Quelle - Benutzerinformationen	Tertiär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Sitzung auf welchem Host geändert wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	3
Fehler	F	3

Aktion "Sitzungsbenachrichtigung"

Die Aktion "Sitzungsbenachrichtigung" gibt Informationen zu sitzungsgenerierten Benachrichtigungen und Meldungen. Sie können dieser Aktion jede Art von Sitzungsbenachrichtigung zuordnen, wenn das Ereignis keiner spezifischeren Aktion zugeordnet werden kann. Verwenden Sie die Aktion "Sitzungsstatus", wenn das Ereignis den Status einer Sitzung beschreibt.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Sitzungsvorgang"

Die Aktion "Sitzungsvorgang" gibt allgemeine Informationen zu Sitzungsvorgängen. Sie können dieser Aktion ein Ereignis zuordnen, das als Teil normaler Sitzungsfunktionen aufgezeichnet ist, oder das keiner spezifischeren CEG-Aktion zugeordnet werden kann.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Wiederherstellung der Sitzungsverbindung

Beim Wiederherstellen einer Sitzungsverbindung werden Informationen ausgegeben, wenn ein Benutzer eine unterbrochene Verbindung mit einer Terminalserver- (bzw. Remote-Desktop)-Sitzung wiederherstellt, anstatt sich erneut anzumelden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Aktion "Sitzungsstatus"

Die Aktion "Sitzungsstatus" gibt Informationen über den Status einer Sitzung. Sie können dieser Aktion jede beliebige Sitzungsstatusmeldung zuordnen, wenn das Ereignis keiner spezifischeren Aktion zugeordnet werden kann.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Aktion "Sitzungswarnung"

Die Aktion "Sitzungswarnung" gibt Informationen zu sitzungsbezogenen Warnungen. Sie können dieser Aktion jede beliebige Art von Sitzungswarnungen zuordnen. Sie können schwerwiegendere Ereignisse zur Aktion "Sitzungsfehler" zuordnen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	4

Sitzungsvalidierung

Bei der Sitzungsvalidierung werden Informationen zur Einrichtung einer eingerichteten Sitzung auf einem bestimmten Host oder in einer bestimmten Anwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse für Festlegung des Benutzers

Authentifizierungsalarm – Aktion

Bei der Aktion "Authentifizierungsalarm" werden Informationen zu sämtlichen Alarmbedingungen in einem Authentifizierungsmodul oder während des Authentifizierungsvorgangs ausgegeben. Alarmbedingungen müssen sofort beachtet werden.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Sekundär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	6

Festlegung des Benutzers

Bei der Festlegung des Benutzers werden Ereignisinformationen zum Versuch eines Kontos angezeigt, Anmeldeinformationen auf einem bestimmten Host oder in einer bestimmten Anwendung zu ändern (also Kontoinformationen auszuführen).

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Primär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Tertiär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto versucht wurde, Anmeldeinformationen für welches Konto auf welchem Host festzulegen. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	E	2
Fehler	F	3

Klasse für Systemaktivität

Aktion "System aktivieren"

Die Aktion "System aktivieren" gibt Informationen zum Aktivieren eines Systems.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Tertiär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolg	S	2
Fehler	F	3

Kapitel 15: Unbekannte Kategorie

Dieses Kapitel enthält folgende Themen:

Unbekannte Klasse

Unbekannte Aktion

"Unbekannte Aktion" dient der Zuordnung aller Ereignisse, die in der CEG nicht als spezifische Aktion klassifiziert werden können.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Sekundär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Tertiär
Ergebnis - Informationen	Tertiär

Ergebnis	event_result	event_severity
Unbekannt	U	0

Kapitel 16: Kategorie "Schwachstellenverwaltung"

Dieses Kapitel enthält folgende Themen:

Klasse für Schwachstellenbewertung

Informationssammlung

Bei der Informationssammlung werden Ereignisinformationen zur Informationssammlung angezeigt.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Schwachstellenscan auf welchem Host gestartet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Service-Erkennung

Bei der Service-Erkennung werden Ereignisinformationen zur Erkennung von Services auf einem System ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	3
Erfolgreich	S	4

Benutzer- und Gruppenerkennung

Bei der Benutzer- und Gruppenerkennung werden Ereignisinformationen zur Erkennung von Benutzer- und Gruppenkonten auf einem System ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	3
Erfolgreich	S	2

Start eines Schwachstellenscans

Beim Start eines Schwachstellenscans werden Ereignisinformationen zur Initiierung eines Schwachstellenscans auf einem bestimmten Host oder in einer bestimmten Anwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Primär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, von welchem Konto welcher Schwachstellenscan auf welchem Host gestartet wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Abschluss eines Schwachstellenscans

Beim Abschluss eines Schwachstellenscans werden Ereignisinformationen zum Abschluss eines Schwachstellenscans auf einem bestimmten Host oder in einer bestimmten Anwendung ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welcher Schwachstellenscan auf welchem Host abgeschlossen wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	2
Fehler	F	3

Klasse für Schwachstellenentdeckung

Zugriffspunkt-Schwachstelle – Aktion

Bei der Aktion "Zugriffspunkt-Schwachstelle" werden Ereignisinformationen zur Erkennung von Schwachstellen im Zusammenhang mit einem drahtlosen Zugriffspunkt ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär

Informationen	Ebene
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Kontoschwachstelle

Bei Kontoschwachstellen werden Ereignisinformationen in Zusammenhang mit der Erkennung von Schwachstellen bei Benutzerkonten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär

Informationen	Ebene
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Antivirus-Schwachstelle – Aktion

Bei der Aktion "Antivirus-Schwachstelle" werden Ereignisinformationen zur Erkennung von Schwachstellen im Zusammenhang mit Antivirus-Software oder -Einrichtungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär

Informationen	Ebene
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Anwendungsprotokollschwachstelle

Bei Anwendungsprotokollschwachstellen werden Ereignisinformationen in Zusammenhang mit der Erkennung von Schwachstellen bei Anwendungsprotokollen wie HTTP, NFS und NIS ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär

Informationen	Ebene
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Anwendungsschwachstelle

Bei Anwendungsschwachstellen werden Ereignisinformationen in Zusammenhang mit der Erkennung von Schwachstellen bei Anwendungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär

Informationen	Ebene	
Ergebnis - Informationen	Primär	
Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	4

Backdoor-Schwachstelle

Bei Backdoor-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit Backdoor-Programmen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Pufferschwachstelle

Bei Pufferschwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit Pufferüberlaufbedingungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Primär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

CGI-Schwachstelle

Bei CGI-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit CGI ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

CISCO-Schwachstelle

Bei CISCO-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit CISCO-Produkten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Befehlsausführungsschwachstelle – Aktion

Bei der Aktion "Befehlsausführungsschwachstelle" werden Ereignisinformationen zur Erkennung von Schwachstellen im Zusammenhang mit Befehlsausführungen ausgegeben. Dies betrifft zum Beispiel die Ausführung von willkürlichen Befehlen, welche die Systemsteuerung umgehen.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Konformitätsschwachstelle

Bei Konformitätsschwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit der Konformität ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Konfigurationsschwachstelle

Bei Konfigurationsschwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit der Konfiguration ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Anmeldeinformationsschwachstelle

Bei Anmeldeinformationsschwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit Anmeldeinformationen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Kryptographieschwachstelle

Bei Kryptographieschwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit der Kryptographie ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Datenbankschwachstelle

Bei Datenbankschwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit Datenbanken und DBMS ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

DoS-Schwachstelle

Bei DoS-Schwachstellen werden Ereignisinformationen zur Erkennung von DoS-bezogenen Schwachstellen in Zusammenhang mit DoS-Aktivitäten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Dateifreigabeschwachstelle

Bei Dateifreigabeschwachstellen werden Ereignisinformationen in Zusammenhang mit der Erkennung von Schwachstellen aufgrund der Freigabeeinstellungen für Dateien (z. B. eine Freigabe mit Berechtigungen zum Öffnen) ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	3
Erfolgreich	S	4

Firewall-Schwachstelle

Bei Firewall-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit Firewall-Komponenten, -Richtlinien, -Einstellungen oder -Vorgängen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	3
Erfolgreich	S	4

Informationsverlust-Schwachstelle

Bei Informationsverlust-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit Informationsverlusten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Mailclient-Schwachstelle – Aktion

Bei der Aktion "Mailclient-Schwachstelle" werden Ereignisinformationen zur Erkennung von Schwachstellen im Zusammenhang mit Mailclients ausgegeben. Dies sind zum Beispiel in Microsoft Outlook entdecke Schwachstellen.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	4

Mailserver-Schwachstelle – Aktion

Bei der Aktion "Mailserver-Schwachstelle" werden Ereignisinformationen zur Erkennung von Schwachstellen im Zusammenhang mit Mailservern ausgegeben. Hier seien zum Beispiel Schwachstellen genannt, die in Microsoft Exchange oder Lotus Domino entdeckt wurden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Microsoft-Schwachstelle

Bei Microsoft-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit Microsoft-Produkten ausgegeben. Beispiele hierfür sind das Spoofing mit Internetinhalten in ISA Server 2000 und Proxyserver 2.0, Microsoft Office-Schwachstellen, Windows RAS-Überlauf usw.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Fehler	F	3
Erfolgreich	S	4

Netzwerkprotokollschwachstelle

Bei Netzwerkprotokollschwachstellen werden Ereignisinformationen in Zusammenhang mit der Erkennung von Schwachstellen bei Netzwerkprotokollen wie TCP, UDP, IP und ICMP ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Betriebssystem-Schwachstelle – Aktion

Bei der Aktion "Betriebssystem-Schwachstelle" werden Ereignisinformationen zur Erkennung von Schwachstellen im Zusammenhang mit Betriebssystemen ausgegeben. Verwenden Sie im Falle von UNIX oder Linux die Aktion "UNIX-Schwachstelle" für die Zuordnung. Im Falle von Windows ist die Aktion "Windows-Schwachstelle" für die Zuordnung zu verwenden. Verwenden Sie diese Aktion für alle anderen Betriebssysteme.

Informationen	**Ebene**
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	**event_result**	**event_severity**
Erfolgreich	S	4

Port Scanner-Schwachstelle

Bei Port Scanner-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit Port Scanner-Produkten ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Berechtigungseskalations-Schwachstelle – Aktion

Bei der Aktion "Berechtigungseskalations-Schwachstelle" werden Ereignisinformationen zur Erkennung von Schwachstellen im Zusammenhang mit der nicht autorisierten Eskalation von Berechtigungen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Remote-Exploit-Schwachstelle

Bei Remote-Exploit-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit Remote-Exploits ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

SCADA-Schwachstelle

Bei SCADA-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit SCADA-Systemen und anderen technischen Überwachungs- und Steuerungssystemen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Service-Daemon-Schwachstelle

Bei Service-Daemon-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit Services oder Daemons ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

SMTP-Schwachstelle – Aktion

Bei der Aktion "SMTP-Schwachstelle" werden Ereignisinformationen zur Erkennung von Schwachstellen im Zusammenhang mit SMTP ausgegeben. Bei einem offenen SMTP-Relay, zum Beispiel, kann im Internet jeder E-Mails über den Mailserver senden.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Software-Schwachstelle

Bei Software-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit Software ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

SQL-Injection-Schwachstelle

Bei SQL-Injection-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit der Einschleusung von SQL-Befehlen ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

UNIX-Schwachstelle

Bei UNIX-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit dem UNIX-Betriebssystem ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Benutzeraufzählungs-Schwachstelle – Aktion

Bei der Aktion "Benutzeraufzählungs-Schwachstelle" werden Ereignisinformationen zur Erkennung von Schwachstellen im Zusammenhang mit der nicht autorisierten Aufzählung von Benutzernamen oder Konten auf einem System ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Webbrowser-Schwachstelle

Bei Webbrowser-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit Webbrowsern ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Webserver-Schwachstelle

Bei Webserver-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit Webservern ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Windows-Schwachstelle

Bei Windows-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit dem Windows-Betriebssystem ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

XSS-Schwachstelle

Bei XSS-Schwachstellen werden Ereignisinformationen zur Erkennung von Schwachstellen in Zusammenhang mit siteübergreifenden Angriffen (Cross-Site-Scripting) ausgegeben.

Informationen	Ebene
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Ergebnis	event_result	event_severity
Erfolgreich	S	4

Klasse für Schwachstellenverwaltung

Schwachstellenerkennung

Bei der Schwachstellenerkennung werden Ereignisinformationen zur Erkennung einer Schwachstelle auf einem bestimmten Host oder in einer bestimmten Anwendung ausgegeben

Informationen	**Ebene**
Quelle - Benutzerinformationen	Sekundär
Quelle – Host-Informationen	Sekundär
Quelle - Objektinformationen	Tertiär
Quelle - Prozessinformationen	Tertiär
Quelle - Gruppeninformationen	Tertiär
Ziel - Benutzerinformationen	Tertiär
Ziel - Host-Informationen	Primär
Ziel - Objektinformationen	Primär
Ziel - Prozessinformationen	Tertiär
Ziel - Gruppeninformationen	Tertiär
Agent - Informationen	Primär
Agent - Host-Informationen	Primär
Ereignisquelle – Host-Informationen	Primär
Ereignisquelle - Informationen	Tertiär
Ereignis - Informationen	Primär
Ergebnis - Informationen	Primär

Für diese Aktion ist die Information von Bedeutung, welche Schwachstelle auf welchem Host erkannt wurde. Auf welchem Host wurden die Ereignisinformationen ausgegeben, und von welchem Agenten auf welchem Host wurden sie aufgezeichnet?

Ergebnis	event_result	event_severity
Erfolgreich	S	4
Fehler	F	3

Kapitel 17: Häufig gestellte Fragen (FAQ)

Die häufig gestellten Fragen bieten Antworten auf Fragen, anhand derer das Verhalten bestimmter Aspekte der CEG-Implementierung von CA geklärt wird. Jede Frage liefert gleichzeitig eine Antwort mit möglichst vielen Details.

Dieses Kapitel enthält folgende Themen:

Worin unterscheiden sich die Aktionen zur Kontodeaktivierung, Kontosuspendierung und Kontosperrung?

In allen drei Fällen ist eine Anmeldung des Kontos nicht mehr möglich, nachdem die Aktion erfolgt ist. Darüber hinaus kann das betreffende Konto bei allen drei Aktionen jederzeit von einem Konto mit Administratorberechtigungen aktiviert werden. Die folgenden Informationen sollen dazu beitragen, die Unterschiede zwischen diesen Aktionen zu verdeutlichen:

Kontosperrung

Das Konto wird möglicherweise aufgrund einer Richtlinie gesperrt, die einschränkt, wie viele Versuche für die Ausführung einer Aktion möglich sind, für die das Konto einer Beschränkung unterliegt. Die Richtlinie zur wiederholten Kennworteingabe in Windows ist ein gutes Beispiel dafür, wann die Kontosperrung wirksam wird. Dies ist beispielsweise der Fall, wenn der Benutzer versucht, sich mit ungültigen Anmeldeinformationen beim System anzumelden und die festgelegte Kennwortrichtlinie verletzt wird.

(Wenn der Benutzer z. B. 3 Mal ein falsches Kennwort eingibt, kann er sich nicht mehr anmelden, auch wenn er beim vierten Mal das richtige Kennwort verwendet.)

Kontodeaktivierung

Das Konto kann unter Umständen explizit aufgrund einer manuellen Aktion oder einer Kontoeinstellung deaktiviert werden, mit der die Nutzung des Kontos eingeschränkt wird. Dies wäre beispielsweise bei einem Konto möglich, das nur bis zu einem bestimmten Datum gültig ist. In diesem Fall wird das Konto deaktiviert, sobald das aktuelle Datum das in den Kontoinformationen festgelegte Datum überschritten hat.

(Wenn der Benutzer beispielsweise ein Konto erstellt, das **nur bis zu einem bestimmten Datum aktiv ist** (dem 19. Juli 2007), wird es nach diesem Tag automatisch deaktiviert.)

Kontosuspendierung

Das Konto könnte von einem Administrator vorübergehend suspendiert werden. Diese Suspendierung erfolgt aufgrund einer manuellen Aktion und nicht automatisch.

In diesem Fall ist das Konto **für einen bestimmten Zeitraum inaktiv** (z. B. vom 12.07.07 bis zum 20.07.07), woraufhin es deaktiviert wird.

Worin besteht der Unterschied zwischen den Begriffen "Konto", "Identität" und "Benutzer"?

Die Begriffe "Konto" und "Benutzer" sind in Bezug auf ihre Bedeutung Synonyme und werden langfristig unter dem Begriff "Konto" zusammengefasst. Alle Aktionen, die sich auf Benutzeraktionen beziehen, werden entsprechend in Kontoaktionen umbenannt.

Der Begriff "Identität" bezieht sich eher auf den eigentlichen Benutzer (die Person), der über mehrere Konten auf verschiedenen Systemen verfügt. Die Identitätsaktion kann für eine Rolle eingesetzt werden, um gemäß der für die Identität gewünschten Rolle mehrere Konten auf mehreren Systemen zu erstellen.

Anhang A: Zuweisung der Sicherheitsebene

Tabelle zur Zuweisung der Sicherheitsebene

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Identitätsverwaltung	Kontenmanagement	Kontoerstellung	Erfolg	2
Identitätsverwaltung	Kontenmanagement	Kontoerstellung	Fehler	3
Identitätsverwaltung	Kontenmanagement	Kontolöschung	Erfolg	2
Identitätsverwaltung	Kontenmanagement	Kontolöschung	Fehler	3
Identitätsverwaltung	Kontenmanagement	Kontodeaktivierung	Erfolg	2
Identitätsverwaltung	Kontenmanagement	Kontodeaktivierung	Fehler	3
Identitätsverwaltung	Kontenmanagement	Kontoaktivierung	Erfolg	2
Identitätsverwaltung	Kontenmanagement	Kontoaktivierung	Fehler	3
Identitätsverwaltung	Kontenmanagement	Kontoauflistung	Erfolg	2
Identitätsverwaltung	Kontenmanagement	Kontosperrung	Erfolg	2
Identitätsverwaltung	Kontenmanagement	Kontoänderung	Erfolg	2
Identitätsverwaltung	Kontenmanagement	Kontoänderung	Fehler	3
Identitätsverwaltung	Kontenmanagement	Kontokennwortänderung	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Identitätsverwaltung	Kontenmanagement	Kontokennwortänderung	Fehler	3
Identitätsverwaltung	Kontenmanagement	Kontokennwort zurücksetzen	Erfolg	2
Identitätsverwaltung	Kontenmanagement	Kontokennwort zurücksetzen	Fehler	3
Identitätsverwaltung	Kontenmanagement	Kontosuspendierung	Erfolg	2
Identitätsverwaltung	Kontenmanagement	Kontosuspendierung	Fehler	3
Identitätsverwaltung	Kontenmanagement	Konto entsperren	Erfolg	2
Identitätsverwaltung	Kontenmanagement	Konto entsperren	Fehler	3
Identitätsverwaltung	Gruppenverwaltung	Gruppenerstellung	Erfolg	2
Identitätsverwaltung	Gruppenverwaltung	Gruppenerstellung	Fehler	3
Identitätsverwaltung	Gruppenverwaltung	Gruppenlöschung	Erfolg	2
Identitätsverwaltung	Gruppenverwaltung	Gruppenlöschung	Fehler	3
Identitätsverwaltung	Gruppenverwaltung	Gruppenmitgliedschaft hinzufügen	Erfolg	2
Identitätsverwaltung	Gruppenverwaltung	Gruppenmitgliedschaft hinzufügen	Fehler	3
Identitätsverwaltung	Gruppenverwaltung	Gruppenmitgliedschaft entfernen	Erfolg	2
Identitätsverwaltung	Gruppenverwaltung	Gruppenmitgliedschaft entfernen	Fehler	3
Identitätsverwaltung	Gruppenverwaltung	Gruppenmitgliederänderung	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Identitätsverwaltung	Gruppenverwaltung	Gruppenmitgliederänderung	Fehler	3
Identitätsverwaltung	Gruppenverwaltung	Gruppenänderung	Erfolg	2
Identitätsverwaltung	Gruppenverwaltung	Gruppenänderung	Fehler	3
Identitätsverwaltung	Identitätsverwaltung	Identitätserstellung	Erfolg	2
Identitätsverwaltung	Identitätsverwaltung	Identitätserstellung	Fehler	3
Identitätsverwaltung	Identitätsverwaltung	Identitätslöschung	Erfolg	2
Identitätsverwaltung	Identitätsverwaltung	Identitätslöschung	Fehler	3
Identitätsverwaltung	Identitätsverwaltung	Identitätsdeaktivierung	Erfolg	2
Identitätsverwaltung	Identitätsverwaltung	Identitätsdeaktivierung	Fehler	3
Identitätsverwaltung	Identitätsverwaltung	Identitätsaktivierung\	Erfolg	2
Identitätsverwaltung	Identitätsverwaltung	Identitätsaktivierung\	Fehler	3
Identitätsverwaltung	Identitätsverwaltung	Identitätsänderung	Erfolg	2
Identitätsverwaltung	Identitätsverwaltung	Identitätsänderung	Fehler	3
Identitätsverwaltung	Identitätsverwaltung	Änderung des Identitätskennworts	Erfolg	2
Identitätsverwaltung	Identitätsverwaltung	Änderung des Identitätskennworts	Fehler	3
Identitätsverwaltung	Benutzerrechteverwaltung	Benutzerrechtezuweisung	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Identitätsverwaltung	Benutzerrechteverwaltung	Benutzerrechtezuweisung	Fehler	3
Identitätsverwaltung	Benutzerrechteverwaltung	Entfernung von Benutzerberechtigungen	Erfolg	2
Identitätsverwaltung	Benutzerrechteverwaltung	Entfernung von Benutzerberechtigungen	Fehler	3
Identitätsverwaltung	Benutzerrechteverwaltung	Benutzerrechtezuweisung	Erfolg	2
Identitätsverwaltung	Benutzerrechteverwaltung	Benutzerrechtezuweisung	Fehler	3
Identitätsverwaltung	Benutzerrechteverwaltung	Benutzerrechteerstellung	Erfolg	2
Identitätsverwaltung	Benutzerrechteverwaltung	Benutzerrechteerstellung	Fehler	3
Identitätsverwaltung	Benutzerrechteverwaltung	Benutzerrechtelöschung	Erfolg	2
Identitätsverwaltung	Benutzerrechteverwaltung	Benutzerrechtelöschung	Fehler	3
Identitätsverwaltung	Benutzerrechteverwaltung	Benutzerrechteauflistung	Erfolg	2
Identitätsverwaltung	Benutzerrechteverwaltung	Benutzerrechteauflistung	Fehler	3
Identitätsverwaltung	Benutzerrechteverwaltung	Benutzerrechteänderung	Erfolg	2
Identitätsverwaltung	Benutzerrechteverwaltung	Benutzerrechteänderung	Fehler	3
Identitätsverwaltung	Benutzerrollenverwaltung	User Admin Role-Zuweisung	Erfolg	3
Identitätsverwaltung	Benutzerrollenverwaltung	User Admin Role-Zuweisung	Fehler	3
Identitätsverwaltung	Benutzerrollenverwaltung	User Admin Role-Löschung	Erfolg	3

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Identitätsverwaltung	Benutzerrollenverwaltung	User Admin Role-Löschung	Fehler	3
Identitätsverwaltung	Benutzerrollenverwaltung	User Admin Role-Änderung	Erfolg	3
Identitätsverwaltung	Benutzerrollenverwaltung	User Admin Role-Änderung	Fehler	3
Identitätsverwaltung	Benutzerrollenverwaltung	Entfernung der Benutzerrolle "Admin"	Erfolg	3
Identitätsverwaltung	Benutzerrollenverwaltung	Entfernung der Benutzerrolle "Admin"	Fehler	3
Identitätsverwaltung	Benutzerrollenverwaltung	Zuweisung von Benutzerrollen	Erfolg	2
Identitätsverwaltung	Benutzerrollenverwaltung	Benutzerrollenerstellung	Erfolg	2
Identitätsverwaltung	Benutzerrollenverwaltung	Benutzerrollenerstellung	Fehler	3
Identitätsverwaltung	Benutzerrollenverwaltung	Benutzerrollenlöschung	Erfolg	2
Identitätsverwaltung	Benutzerrollenverwaltung	Benutzerrollenlöschung	Fehler	3
Identitätsverwaltung	Benutzerrollenverwaltung	Benutzerrollenänderung	Erfolg	2
Identitätsverwaltung	Benutzerrollenverwaltung	Benutzerrollenänderung	Fehler	3
Identitätsverwaltung	Benutzerrollenverwaltung	Entfernung von Benutzerrollen	Erfolg	2
Identitätsverwaltung	Benutzerrollenverwaltung	Entfernung von Benutzerrollen	Fehler	3
Konfigurationsverwaltung	Konfigurationsverwaltung	Konfigurationsänderung	Erfolg	2
Konfigurationsverwaltung	Konfigurationsverwaltung	Konfigurationsänderung	Fehler	3

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Konfigurationsverwaltung	Konfigurationsverwaltung	Konfigurationsfehler	Erfolg	6
Konfigurationsverwaltung	Konfigurationsverwaltung	Konfiguration "Alles leeren"	Erfolg	2
Konfigurationsverwaltung	Konfigurationsverwaltung	Konfiguration "Alles leeren"	Fehler	3
Konfigurationsverwaltung	Konfigurationsverwaltung	Konfiguration - Authentifizierungsbereiche leeren	Erfolg	2
Konfigurationsverwaltung	Konfigurationsverwaltung	Konfiguration - Authentifizierungsbereiche leeren	Fehler	3
Konfigurationsverwaltung	Konfigurationsverwaltung	Konfiguration - Benutzer-Cache leeren	Erfolg	2
Konfigurationsverwaltung	Konfigurationsverwaltung	Konfiguration - Benutzer-Cache leeren	Fehler	3
Konfigurationsverwaltung	Konfigurationsverwaltung	Start des Lesens von Konfigurationen	Erfolg	2
Konfigurationsverwaltung	Konfigurationsverwaltung	Konfigurationswarnung	Erfolg	3
Konfigurationsverwaltung	Konfigurationsverwaltung	Systemzeitänderung	Erfolg	4
Konfigurationsverwaltung	Konfigurationsverwaltung	Systemzeitänderung	Fehler	4
Konfigurationsverwaltung	Konfigurationsverwaltung	Aufgabenerstellung	Erfolg	2
Konfigurationsverwaltung	Konfigurationsverwaltung	Aufgabenerstellung	Fehler	3
Konfigurationsverwaltung	Konfigurationsverwaltung	Aufgabenänderung	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Konfigurationsverwaltung	Konfigurationsverwaltung	Aufgabenänderung	Fehler	3
Konfigurationsverwaltung	Richtlinienverwaltung	Richtlinienerstellung	Erfolg	2
Konfigurationsverwaltung	Richtlinienverwaltung	Richtlinienerstellung	Fehler	3
Konfigurationsverwaltung	Richtlinienverwaltung	Richtlinienlöschung	Erfolg	4
Konfigurationsverwaltung	Richtlinienverwaltung	Richtlinienlöschung	Fehler	3
Konfigurationsverwaltung	Richtlinienverwaltung	Richtlinienänderung	Erfolg	4
Konfigurationsverwaltung	Richtlinienverwaltung	Richtlinienänderung	Fehler	3
Konfigurationsverwaltung	Richtlinienverwaltung	Richtlinienaktivierung	Erfolg	2
Konfigurationsverwaltung	Richtlinienverwaltung	Richtlinienaktivierung	Fehler	3
Konfigurationsverwaltung	Richtlinienverwaltung	Richtliniendeaktivierung	Erfolg	2
Konfigurationsverwaltung	Richtlinienverwaltung	Richtliniendeaktivierung	Fehler	3
Konfigurationsverwaltung	Richtlinienverwaltung	Richtlinienanwendung	Erfolg	2
Inhaltssicherheit	E-Mail-Untersuchung	Spam-Erkennung	Erfolg	3
Inhaltssicherheit	E-Mail-Untersuchung	Anlagenscan	Erfolg	2
Inhaltssicherheit	E-Mail-Untersuchung	Anlagenscan	Fehler	3
Inhaltssicherheit	E-Mail-Untersuchung	Profanity-Erkennung	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Inhaltssicherheit	E-Mail-Untersuchung	Profanity-Erkennung	Fehler	3
Inhaltssicherheit	E-Mail-Untersuchung	Vertraulichkeitsverlust	Erfolg	2
Inhaltssicherheit	E-Mail-Untersuchung	Vertraulichkeitsverlust	Fehler	3
Inhaltssicherheit	E-Mail-Untersuchung	E-Mail-Untersuchung	Erfolg	2
Inhaltssicherheit	E-Mail-Untersuchung	E-Mail-Untersuchung	Fehler	3
Inhaltssicherheit	URL-Zugriff	URL-Filterung	Erfolg	2
Inhaltssicherheit	URL-Zugriff	URL-Filterung	Fehler	3
Inhaltssicherheit	URL-Zugriff	HTTP-Filterung	Erfolg	2
Inhaltssicherheit	URL-Zugriff	HTTP-Filterung	Fehler	3
Inhaltssicherheit	URL-Zugriff	FTP-Filterung	Erfolg	2
Inhaltssicherheit	URL-Zugriff	FTP-Filterung	Fehler	3
Inhaltssicherheit	URL-Zugriff	Inhaltsprüfung	Erfolg	2
Inhaltssicherheit	URL-Zugriff	Inhaltsprüfung	Fehler	3
Datenzugriff	Service- und Anwendungsauslastung	Methodenausführung	Erfolg	2
Datenzugriff	Service- und Anwendungsauslastung	Methodenausführung	Fehler	3
Datenzugriff	Service- und Anwendungsauslastung	Prozedurausführung	Erfolg	2
Datenzugriff	Service- und Anwendungsauslastung	Prozedurausführung	Fehler	3
Datenzugriff	Anwendungsverwaltung	Kontexterstellung	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Anwendungsverwaltung	Kontexterstellung	Fehler	3
Datenzugriff	Anwendungsverwaltung	Kontextlöschung	Erfolg	3
Datenzugriff	Anwendungsverwaltung	Kontextlöschung	Fehler	3
Datenzugriff	Anwendungsverwaltung	Funktionserstellung	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Funktionserstellung	Fehler	3
Datenzugriff	Anwendungsverwaltung	Funktionslöschung	Erfolg	4
Datenzugriff	Anwendungsverwaltung	Funktionslöschung	Fehler	3
Datenzugriff	Anwendungsverwaltung	Funktionsänderung	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Funktionsänderung	Fehler	3
Datenzugriff	Anwendungsverwaltung	Indexanalyse	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Indexanalyse	Fehler	3
Datenzugriff	Anwendungsverwaltung	Bibliothekserstellung	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Bibliothekserstellung	Fehler	3
Datenzugriff	Anwendungsverwaltung	Operator erstellen	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Operator erstellen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Operator löschen	Erfolg	4

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Anwendungsverwaltung	Operator löschen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Operator ändern	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Operator ändern	Fehler	3
Datenzugriff	Anwendungsverwaltung	Paketkörper erstellen	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Paketkörper erstellen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Paketkörper löschen	Erfolg	4
Datenzugriff	Anwendungsverwaltung	Paketkörper löschen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Paketkörper ändern	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Paketkörper ändern	Fehler	3
Datenzugriff	Anwendungsverwaltung	Paket erstellen	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Paket erstellen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Paket ändern	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Paket ändern	Fehler	3
Datenzugriff	Anwendungsverwaltung	Prozedur erstellen	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Prozedur erstellen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Paket löschen	Erfolg	4

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Anwendungsverwaltung	Paket löschen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Prozedur löschen	Erfolg	4
Datenzugriff	Anwendungsverwaltung	Prozedur löschen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Prozedur ändern	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Prozedur ändern	Fehler	3
Datenzugriff	Anwendungsverwaltung	Tabelle analysieren	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Tabelle analysieren	Fehler	3
Datenzugriff	Anwendungsverwaltung	Tabelle kürzen	Erfolg	3
Datenzugriff	Anwendungsverwaltung	Tabelle kürzen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Trigger erstellen	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Trigger erstellen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Trigger löschen	Erfolg	4
Datenzugriff	Anwendungsverwaltung	Trigger löschen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Trigger deaktivieren	Erfolg	4
Datenzugriff	Anwendungsverwaltung	Trigger deaktivieren	Fehler	3
Datenzugriff	Anwendungsverwaltung	Trigger aktivieren	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Anwendungsverwaltung	Trigger aktivieren	Fehler	3
Datenzugriff	Anwendungsverwaltung	Trigger ändern	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Trigger ändern	Fehler	3
Datenzugriff	Anwendungsverwaltung	Typkörper erstellen	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Typkörper erstellen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Typkörper löschen	Erfolg	3
Datenzugriff	Anwendungsverwaltung	Typkörper löschen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Typkörper ändern	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Typkörper ändern	Fehler	3
Datenzugriff	Anwendungsverwaltung	Typ erstellen	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Typ erstellen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Typ löschen	Erfolg	4
Datenzugriff	Anwendungsverwaltung	Typ löschen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Typ ausführen	Erfolg	2
Datenzugriff	Anwendungsverwaltung	Typ ausführen	Fehler	3
Datenzugriff	Anwendungsverwaltung	Typ ändern	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Anwendungsverwaltung	Typ ändern	Fehler	3
Datenzugriff	Peer-Verwaltung	Datenbankverbindung erstellen	Erfolg	2
Datenzugriff	Peer-Verwaltung	Datenbankverbindung erstellen	Fehler	3
Datenzugriff	Peer-Verwaltung	Datenbankverbindung löschen	Erfolg	4
Datenzugriff	Peer-Verwaltung	Datenbankverbindung löschen	Fehler	3
Datenzugriff	Systemverwaltung	Cluster analysieren	Erfolg	2
Datenzugriff	Systemverwaltung	Cluster analysieren	Fehler	3
Datenzugriff	Systemverwaltung	Cluster erstellen	Erfolg	2
Datenzugriff	Systemverwaltung	Cluster erstellen	Fehler	3
Datenzugriff	Systemverwaltung	Cluster löschen	Erfolg	2
Datenzugriff	Systemverwaltung	Cluster löschen	Fehler	3
Datenzugriff	Systemverwaltung	Cluster ändern	Erfolg	2
Datenzugriff	Systemverwaltung	Cluster ändern	Fehler	3
Datenzugriff	Systemverwaltung	Cluster kürzen	Erfolg	2
Datenzugriff	Systemverwaltung	Cluster kürzen	Fehler	3
Datenzugriff	Systemverwaltung	Datenbank erstellen	Erfolg	2
Datenzugriff	Systemverwaltung	Datenbank erstellen	Fehler	3
Datenzugriff	Systemverwaltung	Datenbank löschen	Erfolg	4
Datenzugriff	Systemverwaltung	Datenbank löschen	Fehler	3
Datenzugriff	Systemverwaltung	Datenbank-Flashback	Erfolg	3
Datenzugriff	Systemverwaltung	Datenbank-Flashback	Fehler	3

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Systemverwaltung	Datenbankänderung	Erfolg	3
Datenzugriff	Systemverwaltung	Datenbankänderung	Fehler	3
Datenzugriff	Systemverwaltung	Datenbanksicherung	Erfolg	2
Datenzugriff	Systemverwaltung	Datenbanksicherung	Fehler	3
Datenzugriff	Systemverwaltung	Datenbank wiederherstellen	Erfolg	3
Datenzugriff	Systemverwaltung	Datenbank wiederherstellen	Fehler	3
Datenzugriff	Systemverwaltung	Erklären	Erfolg	2
Datenzugriff	Systemverwaltung	Erklären	Fehler	3
Datenzugriff	Systemverwaltung	Flashback	Erfolg	2
Datenzugriff	Systemverwaltung	Flashback	Fehler	3
Datenzugriff	Systemverwaltung	Papierkorb leeren	Erfolg	2
Datenzugriff	Systemverwaltung	Papierkorb leeren	Fehler	3
Datenzugriff	Systemverwaltung	Rollback-Segment erstellen	Erfolg	2
Datenzugriff	Systemverwaltung	Rollback-Segment erstellen	Fehler	3
Datenzugriff	Systemverwaltung	Rollback-Segment löschen	Erfolg	2
Datenzugriff	Systemverwaltung	Rollback-Segment löschen	Fehler	3
Datenzugriff	Systemverwaltung	Rollback-Segment ändern	Erfolg	2
Datenzugriff	Systemverwaltung	Rollback-Segment ändern	Fehler	3
Datenzugriff	Systemverwaltung	Systemberechtigungen erteilen	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Systemverwaltung	Systemberechtigungen erteilen	Fehler	3
Datenzugriff	Systemverwaltung	System ändern	Erfolg	2
Datenzugriff	Systemverwaltung	System ändern	Fehler	3
Datenzugriff	Systemverwaltung	System widerrufen	Erfolg	2
Datenzugriff	Systemverwaltung	System widerrufen	Fehler	3
Datenzugriff	Systemverwaltung	Tabellen-Flashback	Erfolg	2
Datenzugriff	Systemverwaltung	Tabellen-Flashback	Fehler	3
Datenzugriff	Systemverwaltung	Tablespace erstellen	Erfolg	2
Datenzugriff	Systemverwaltung	Tablespace erstellen	Fehler	3
Datenzugriff	Systemverwaltung	Tablespace löschen	Erfolg	4
Datenzugriff	Systemverwaltung	Tablespace löschen	Fehler	3
Datenzugriff	Systemverwaltung	Tablespace ändern	Erfolg	3
Datenzugriff	Systemverwaltung	Tablespace ändern	Fehler	3
Datenzugriff	Systemverwaltung	Tablespace leeren	Erfolg	3
Datenzugriff	Systemverwaltung	Tablespace leeren	Fehler	3
Datenzugriff	Systemverwaltung	Transact-Anweisung ausführen	Erfolg	2
Datenzugriff	Systemverwaltung	Transact-Anweisung ausführen	Fehler	3
Datenzugriff	Systemverwaltung	Alle Trigger deaktivieren	Erfolg	4
Datenzugriff	Systemverwaltung	Alle Trigger deaktivieren	Fehler	3
Datenzugriff	Systemverwaltung	Alle Trigger aktivieren	Erfolg	3

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Systemverwaltung	Alle Trigger aktivieren	Fehler	3
Datenzugriff	Datenzugriff	Übernehmen	Erfolg	2
Datenzugriff	Datenzugriff	Übernehmen	Fehler	3
Datenzugriff	Datenzugriff	Löschen	Erfolg	3
Datenzugriff	Datenzugriff	Löschen	Fehler	3
Datenzugriff	Datenzugriff	Einfügen	Erfolg	2
Datenzugriff	Datenzugriff	Einfügen	Fehler	3
Datenzugriff	Datenzugriff	Rollback	Erfolg	2
Datenzugriff	Datenzugriff	Rollback	Fehler	3
Datenzugriff	Datenzugriff	Sicherungspunkt	Erfolg	2
Datenzugriff	Datenzugriff	Sicherungspunkt	Fehler	3
Datenzugriff	Datenzugriff	Auswählen	Erfolg	2
Datenzugriff	Datenzugriff	Auswählen	Fehler	3
Datenzugriff	Datenzugriff	Transaktion festlegen	Erfolg	2
Datenzugriff	Datenzugriff	Transaktion festlegen	Fehler	3
Datenzugriff	Datenzugriff	Aktualisieren	Erfolg	2
Datenzugriff	Datenzugriff	Aktualisieren	Fehler	3
Datenzugriff	Objektverwaltung	Zugriffsdatei erstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Zugriffsdatei erstellen	Fehler	6
Datenzugriff	Objektverwaltung	Dimension erstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Dimension erstellen	Fehler	3
Datenzugriff	Objektverwaltung	Dimension löschen	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Objektverwaltung	Dimension löschen	Fehler	3
Datenzugriff	Objektverwaltung	Dimension ändern	Erfolg	2
Datenzugriff	Objektverwaltung	Dimension ändern	Fehler	3
Datenzugriff	Objektverwaltung	Verzeichnis erstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Verzeichnis erstellen	Fehler	3
Datenzugriff	Objektverwaltung	Verzeichnis löschen	Erfolg	4
Datenzugriff	Objektverwaltung	Verzeichnis löschen	Fehler	3
Datenzugriff	Objektverwaltung	Kompletten Index aktualisieren	Erfolg	2
Datenzugriff	Objektverwaltung	Kompletten Index aktualisieren	Fehler	3
Datenzugriff	Objektverwaltung	Index erstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Index erstellen	Fehler	3
Datenzugriff	Objektverwaltung	Index löschen	Erfolg	3
Datenzugriff	Objektverwaltung	Index löschen	Fehler	3
Datenzugriff	Objektverwaltung	Index ändern	Erfolg	3
Datenzugriff	Objektverwaltung	Index ändern	Fehler	3
Datenzugriff	Objektverwaltung	Index leeren	Erfolg	3
Datenzugriff	Objektverwaltung	Index leeren	Fehler	3
Datenzugriff	Objektverwaltung	Indextyp erstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Indextyp erstellen	Fehler	3
Datenzugriff	Objektverwaltung	Indextyp löschen	Erfolg	3
Datenzugriff	Objektverwaltung	Indextyp löschen	Fehler	3
Datenzugriff	Objektverwaltung	Index validieren	Erfolg	2
Datenzugriff	Objektverwaltung	Index validieren	Fehler	3
Datenzugriff	Objektverwaltung	Java erstellen	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Objektverwaltung	Java erstellen	Fehler	3
Datenzugriff	Objektverwaltung	Java löschen	Erfolg	3
Datenzugriff	Objektverwaltung	Java löschen	Fehler	3
Datenzugriff	Objektverwaltung	Java ändern	Erfolg	3
Datenzugriff	Objektverwaltung	Java ändern	Fehler	3
Datenzugriff	Objektverwaltung	Sperren	Erfolg	2
Datenzugriff	Objektverwaltung	Sperren	Fehler	3
Datenzugriff	Objektverwaltung	Materialisierte Sicht erstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Materialisierte Sicht erstellen	Fehler	3
Datenzugriff	Objektverwaltung	Materialisierte Sicht löschen	Erfolg	3
Datenzugriff	Objektverwaltung	Materialisierte Sicht löschen	Fehler	3
Datenzugriff	Objektverwaltung	Materialisierte Sicht ändern	Erfolg	3
Datenzugriff	Objektverwaltung	Materialisierte Sicht ändern	Fehler	3
Datenzugriff	Objektverwaltung	Protokollbericht für materialisierte Sicht erstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Protokollbericht für materialisierte Sicht erstellen	Fehler	3
Datenzugriff	Objektverwaltung	Protokollbericht für materialisierte Sicht löschen	Erfolg	3
Datenzugriff	Objektverwaltung	Protokollbericht für materialisierte Sicht löschen	Fehler	3

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Objektverwaltung	Protokollbericht für materialisierte Sicht ändern	Erfolg	3
Datenzugriff	Objektverwaltung	Protokollbericht für materialisierte Sicht ändern	Fehler	3
Datenzugriff	Objektverwaltung	Kein Vorgang	Erfolg	2
Datenzugriff	Objektverwaltung	Kein Vorgang	Fehler	3
Datenzugriff	Objektverwaltung	Gelöschtes Objekt wiederherstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Gelöschtes Objekt wiederherstellen	Fehler	3
Datenzugriff	Objektverwaltung	Umriss erstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Umriss erstellen	Fehler	3
Datenzugriff	Objektverwaltung	Umriss löschen	Erfolg	2
Datenzugriff	Objektverwaltung	Umriss löschen	Fehler	3
Datenzugriff	Objektverwaltung	Umriss ändern	Erfolg	2
Datenzugriff	Objektverwaltung	Umriss ändern	Fehler	3
Datenzugriff	Objektverwaltung	Öffentliches Synonym erstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Öffentliches Synonym erstellen	Fehler	3
Datenzugriff	Objektverwaltung	Öffentliches Synonym löschen	Erfolg	3
Datenzugriff	Objektverwaltung	Öffentliches Synonym löschen	Fehler	3
Datenzugriff	Objektverwaltung	Ressourcenkosten ändern	Erfolg	3
Datenzugriff	Objektverwaltung	Ressourcenkosten ändern	Fehler	3
Datenzugriff	Objektverwaltung	Sequenz erstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Sequenz erstellen	Fehler	3

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Objektverwaltung	Sequenz löschen	Erfolg	3
Datenzugriff	Objektverwaltung	Sequenz löschen	Fehler	3
Datenzugriff	Objektverwaltung	Sequenz ändern	Erfolg	3
Datenzugriff	Objektverwaltung	Sequenz ändern	Fehler	3
Datenzugriff	Objektverwaltung	Statistik zuordnen	Erfolg	2
Datenzugriff	Objektverwaltung	Statistik zuordnen	Fehler	3
Datenzugriff	Objektverwaltung	Statistikzuordnung aufheben	Erfolg	2
Datenzugriff	Objektverwaltung	Statistikzuordnung aufheben	Fehler	3
Datenzugriff	Objektverwaltung	Übersicht ändern	Erfolg	2
Datenzugriff	Objektverwaltung	Übersicht ändern	Fehler	3
Datenzugriff	Objektverwaltung	Synonym erstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Synonym erstellen	Fehler	3
Datenzugriff	Objektverwaltung	Synonym löschen	Erfolg	3
Datenzugriff	Objektverwaltung	Synonym löschen	Fehler	3
Datenzugriff	Objektverwaltung	Umbenennen	Erfolg	3
Datenzugriff	Objektverwaltung	Umbenennen	Fehler	3
Datenzugriff	Objektverwaltung	Schema erstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Schema erstellen	Fehler	3
Datenzugriff	Objektverwaltung	Tabelle erstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Tabelle erstellen	Fehler	3
Datenzugriff	Objektverwaltung	Tabelle löschen	Erfolg	3
Datenzugriff	Objektverwaltung	Tabelle löschen	Fehler	3
Datenzugriff	Objektverwaltung	Tabelle ändern	Erfolg	3
Datenzugriff	Objektverwaltung	Tabelle ändern	Fehler	3
Datenzugriff	Objektverwaltung	Tabellenbereinigung	Erfolg	3

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Objektverwaltung	Tabellenbereinigung	Fehler	3
Datenzugriff	Objektverwaltung	Tabelle umbenennen	Erfolg	3
Datenzugriff	Objektverwaltung	Tabelle umbenennen	Fehler	3
Datenzugriff	Objektverwaltung	Sicht erstellen	Erfolg	2
Datenzugriff	Objektverwaltung	Sicht erstellen	Fehler	3
Datenzugriff	Objektverwaltung	Sicht löschen	Erfolg	3
Datenzugriff	Objektverwaltung	Sicht löschen	Fehler	3
Datenzugriff	Berechtigungsverwaltung	Bibliothek löschen	Erfolg	2
Datenzugriff	Berechtigungsverwaltung	Bibliothek löschen	Fehler	3
Datenzugriff	Berechtigungsverwaltung	Objektberechtigungen erteilen	Erfolg	2
Datenzugriff	Berechtigungsverwaltung	Objektberechtigungen erteilen	Fehler	3
Datenzugriff	Berechtigungsverwaltung	Objekt widerrufen	Erfolg	2
Datenzugriff	Berechtigungsverwaltung	Objekt widerrufen	Fehler	3
Datenzugriff	Berechtigungsverwaltung	Objekt verweigern	Erfolg	2
Datenzugriff	Berechtigungsverwaltung	Objekt verweigern	Fehler	3
Datenzugriff	Berechtigungsverwaltung	Profilerstellung	Erfolg	2
Datenzugriff	Berechtigungsverwaltung	Profilerstellung	Fehler	3
Datenzugriff	Berechtigungsverwaltung	Profillöschung	Erfolg	4

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Berechtigungsverwaltung	Profillöschung	Fehler	3
Datenzugriff	Berechtigungsverwaltung	Profiländerung	Erfolg	4
Datenzugriff	Berechtigungsverwaltung	Profiländerung	Fehler	3
Datenzugriff	Berechtigungsverwaltung	Rolle widerrufen	Erfolg	2
Datenzugriff	Berechtigungsverwaltung	Rolle widerrufen	Fehler	3
Datenzugriff	Berechtigungsverwaltung	Anweisung verweigern	Erfolg	2
Datenzugriff	Berechtigungsverwaltung	Anweisung verweigern	Fehler	3
Datenzugriff	Berechtigungsverwaltung	Anweisung widerrufen	Erfolg	2
Datenzugriff	Berechtigungsverwaltung	Anweisung widerrufen	Fehler	3
Datenzugriff	Berechtigungsverwaltung	Anweisung erteilen	Erfolg	2
Datenzugriff	Berechtigungsverwaltung	Anweisung erteilen	Fehler	3
Datenzugriff	Audit-Ereignisse	Audit-Standard	Erfolg	2
Datenzugriff	Audit-Ereignisse	Audit-Standard	Fehler	3
Datenzugriff	Audit-Ereignisse	Kein Audit-Standard	Erfolg	2
Datenzugriff	Audit-Ereignisse	Kein Audit-Standard	Fehler	3
Datenzugriff	Audit-Ereignisse	Objekt-Audit	Erfolg	2
Datenzugriff	Audit-Ereignisse	Objekt-Audit	Fehler	3
Datenzugriff	Audit-Ereignisse	Kein Objekt-Audit	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Datenzugriff	Audit-Ereignisse	Kein Objekt-Audit	Fehler	3
Datenzugriff	Audit-Ereignisse	Sitzung aufzeichnen	Erfolg	2
Datenzugriff	Audit-Ereignisse	Sitzung aufzeichnen	Fehler	3
Datenzugriff	Audit-Ereignisse	System-Audit	Erfolg	2
Datenzugriff	Audit-Ereignisse	System-Audit	Fehler	3
Datenzugriff	Audit-Ereignisse	Kein System-Audit	Erfolg	2
Datenzugriff	Audit-Ereignisse	Kein System-Audit	Fehler	3
Hostsicherheit	Antivirusaktivität	Dateiblock	Erfolg	2
Hostsicherheit	Antivirusaktivität	Datei ausschließen	Erfolg	2
Hostsicherheit	Antivirusaktivität	Datei ausschließen	Fehler	3
Hostsicherheit	Antivirusaktivität	Datei umbenennen	Erfolg	3
Hostsicherheit	Antivirusaktivität	Datei umbenennen	Fehler	3
Hostsicherheit	Antivirusaktivität	Scan-Fehler	Erfolg	6
Hostsicherheit	Antivirusaktivität	Scanbericht	Erfolg	2
Hostsicherheit	Antivirusaktivität	Virus bereinigen	Erfolg	2
Hostsicherheit	Antivirusaktivität	Virus bereinigen	Fehler	6
Hostsicherheit	Antivirusaktivität	Virus entdeckt	Erfolg	6
Hostsicherheit	Antivirusaktivität	Viren-Engine aktualisieren	Erfolg	2
Hostsicherheit	Antivirusaktivität	Viren-Engine aktualisieren	Fehler	5
Hostsicherheit	Antivirusaktivität	Virus in Quarantäne	Erfolg	2
Hostsicherheit	Antivirusaktivität	Virus in Quarantäne	Fehler	6
Hostsicherheit	Antivirusaktivität	Virenscan gestartet	Erfolg	2
Hostsicherheit	Antivirusaktivität	Virenscan gestartet	Fehler	3

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Hostsicherheit	Antivirusaktivität	Virenscan abgeschlossen	Erfolg	2
Hostsicherheit	Antivirusaktivität	Virenscan abgeschlossen	Fehler	3
Hostsicherheit	Antivirusaktivität	Virenscan angehalten	Erfolg	2
Hostsicherheit	Antivirusaktivität	Virenscan angehalten	Fehler	3
Hostsicherheit	Antivirusaktivität	Virenscan fortgesetzt	Erfolg	2
Hostsicherheit	Antivirusaktivität	Virenscan fortgesetzt	Fehler	3
Hostsicherheit	Antivirusaktivität	Virensignaturen aktualisieren	Erfolg	2
Hostsicherheit	Antivirusaktivität	Virensignaturen aktualisieren	Fehler	4
Hostsicherheit	Antivirusaktivität	Antivirusinstallation	Erfolg	2
Hostsicherheit	Antivirusaktivität	Antivirusinstallation	Fehler	3
Hostsicherheit	Antivirusaktivität	Antivirusdeinstallation	Erfolg	4
Hostsicherheit	Antivirusaktivität	Antivirusdeinstallation	Fehler	4
Hostsicherheit	Antivirusaktivität	Antiviren-Client entfernt	Erfolg	3
Hostsicherheit	Antivirusaktivität	Antiviren-Client entfernt	Fehler	4
Hostsicherheit	IDS-/IPS-Aktivität	Signaturverletzung	Erfolg	6
Netzwerksicherheit	Verbindungsaktivität	Verbindungsversuch	Accept	2
Netzwerksicherheit	Verbindungsaktivität	Verbindungsversuch	Unterbrechen	3

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Netzwerksicherheit	Verbindungsaktivität	Verbindungsversuch	Ablehnen	3
Netzwerksicherheit	Verbindungsaktivität	Verbindungsneuaufbau	Erfolg	2
Netzwerksicherheit	Verbindungsaktivität	Verbindungsneuaufbau	Fehler	3
Netzwerksicherheit	Verbindungsaktivität	Verbindungsanforderung	Erfolg	2
Netzwerksicherheit	Verbindungsaktivität	Verbindungsstatus	Erfolg	2
Netzwerksicherheit	Verbindungsaktivität	Verbindungsabbruch	Erfolg	2
Netzwerksicherheit	Verbindungsaktivität	Schlüsselaustausch Start Phase 1	Erfolg	2
Netzwerksicherheit	Verbindungsaktivität	Schlüsselaustausch Start Phase 1	Fehler	3
Netzwerksicherheit	Verbindungsaktivität	Ablauf der Sicherheitsverknüpfung	Erfolg	2
Netzwerksicherheit	Verbindungsaktivität	Ablauf der Sicherheitsverknüpfung	Fehler	3
Netzwerksicherheit	Verbindungsaktivität	Sicherheitszuordnung anfordern	Erfolg	2
Netzwerksicherheit	Verbindungsaktivität	Sicherheitszuordnung anfordern	Fehler	3
Netzwerksicherheit	Aktivität bei Signaturverletzung	Signaturverletzung	Erfolg	6
Betriebssicherheit	Prozessaktivität	Prozesserstellung	Erfolg	2
Betriebssicherheit	Prozessaktivität	Prozesserstellung	Fehler	3
Betriebssicherheit	Prozessaktivität	Prozessbenachrichtigung	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Betriebssicherheit	Prozessaktivität	Prozessbenachrichtigung	Fehler	3
Betriebssicherheit	Prozessaktivität	Prozessneustart	Erfolg	2
Betriebssicherheit	Prozessaktivität	Prozessneustart	Fehler	3
Betriebssicherheit	Prozessaktivität	Prozessstart	Erfolg	2
Betriebssicherheit	Prozessaktivität	Prozessstart	Fehler	3
Betriebssicherheit	Prozessaktivität	Prozess beenden	Erfolg	2
Betriebssicherheit	Prozessaktivität	Prozess beenden	Fehler	3
Betriebssicherheit	Prozessaktivität	Prozessaufschiebung	Erfolg	2
Betriebssicherheit	Prozessaktivität	Prozessaufschiebung	Fehler	3
Betriebssicherheit	Systemaktivität	System herunterfahren	Erfolg	7
Betriebssicherheit	Systemaktivität	System herunterfahren	Fehler	7
Betriebssicherheit	Systemaktivität	Systemstart	Erfolg	3
Betriebssicherheit	Systemaktivität	Systemstart	Fehler	6
Betriebssicherheit	Systemaktivität	Systemstatus	Erfolg	2
Betriebssicherheit	Systemaktivität	Systemstatus	Fehler	3
Betriebssicherheit	Systemaktivität	System angehalten	Erfolg	4
Betriebssicherheit	Systemaktivität	System angehalten	Fehler	3
Betriebssicherheit	Systemaktivität	System wiederaufnehmen	Erfolg	2
Betriebssicherheit	Systemaktivität	System wiederaufnehmen	Fehler	3

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Betriebssicherheit	Sicherheitsprotokollaktivität	Sicherheitsprotokoll löschen	Erfolg	6
Betriebssicherheit	Sicherheitsprotokollaktivität	Sicherheitsprotokoll löschen	Fehler	6
Betriebssicherheit	Sicherheitsprotokollaktivität	Sicherheitsprotokoll-Rollover	Erfolg	2
Betriebssicherheit	Sicherheitsprotokollaktivität	Sicherheitsprotokoll-Rollover	Fehler	3
Physischer Zugriff	Physische Zugriffsaktivität	Badge-Scan	Erfolg	2
Physischer Zugriff	Physische Zugriffsaktivität	Badge-Scan	Fehler	3
Physischer Zugriff	Physische Zugriffsaktivität	Kamera aktivieren	Erfolg	2
Physischer Zugriff	Physische Zugriffsaktivität	Kamera aktivieren	Fehler	4
Physischer Zugriff	Physische Zugriffsaktivität	Kamera deaktivieren	Erfolg	3
Physischer Zugriff	Physische Zugriffsaktivität	Kamera deaktivieren	Fehler	3
Physischer Zugriff	Physische Zugriffsaktivität	Kamera nicht verfügbar	Erfolg	4
Physischer Zugriff	Physische Zugriffsaktivität	Kamera nicht verfügbar	Fehler	4
Physischer Zugriff	Physische Zugriffsaktivität	Tür schließen	Erfolg	2
Physischer Zugriff	Physische Zugriffsaktivität	Tür schließen	Fehler	5
Physischer Zugriff	Physische Zugriffsaktivität	Tür öffnen	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Physischer Zugriff	Physische Zugriffsaktivität	Tür öffnen	Fehler	5
Physischer Zugriff	Physische Zugriffsaktivität	Fenster schließen	Erfolg	2
Physischer Zugriff	Physische Zugriffsaktivität	Fenster schließen	Fehler	5
Physischer Zugriff	Physische Zugriffsaktivität	Fenster öffnen.	Erfolg	2
Physischer Zugriff	Physische Zugriffsaktivität	Fenster öffnen.	Fehler	4
Ressourcenzugriff	Ressourcenaktivität	Ressourcenzugriff	Erfolg	2
Ressourcenzugriff	Ressourcenaktivität	Ressourcenzugriff	Fehler	3
Ressourcenzugriff	Ressourcenaktivität	Ressourcenzuordnung	Erfolg	2
Ressourcenzugriff	Ressourcenaktivität	Ressourcenzuordnung	Fehler	3
Ressourcenzugriff	Ressourcenaktivität	Ressourcenschließung	Erfolg	2
Ressourcenzugriff	Ressourcenaktivität	Ressourcenschließung	Fehler	3
Ressourcenzugriff	Ressourcenaktivität	Ressourcenerstellung	Erfolg	2
Ressourcenzugriff	Ressourcenaktivität	Ressourcenerstellung	Fehler	3
Ressourcenzugriff	Ressourcenaktivität	Ressourcenlöschung	Erfolg	2
Ressourcenzugriff	Ressourcenaktivität	Ressourcenlöschung	Fehler	3
Ressourcenzugriff	Ressourcenaktivität	Ressourcenausführung	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Ressourcenzugriff	Ressourcenaktivität	Ressourcenausführung	Fehler	3
Ressourcenzugriff	Ressourcenaktivität	Ressourcenänderung	Erfolg	2
Ressourcenzugriff	Ressourcenaktivität	Ressourcenänderung	Fehler	3
Ressourcenzugriff	Ressourcenaktivität	Ressourcenöffnung	Erfolg	2
Ressourcenzugriff	Ressourcenaktivität	Ressourcenöffnung	Fehler	3
Systemzugriff	Authentifizierungsaktivität	Authentifizierung	Erfolg	2
Systemzugriff	Authentifizierungsaktivität	Authentifizierung	Fehler	3
Systemzugriff	Authentifizierungsaktivität	Authentifizierungs-Fallback	Erfolg	2
Systemzugriff	Authentifizierungsaktivität	Authentifizierungs-Fallback	Fehler	6
Systemzugriff	Authentifizierungsaktivität	Authentifizierungspaket geladen	Erfolg	3
Systemzugriff	Authentifizierungsaktivität	Authentifizierungspaket geladen	Fehler	3
Systemzugriff	Authentifizierungsaktivität	Authentifizierungsstart	Erfolg	2
Systemzugriff	Authentifizierungsaktivität	Authentifizierungsstart	Fehler	6
Systemzugriff	Autorisierungsaktivität	Autorisierung	Erfolg	2
Systemzugriff	Autorisierungsaktivität	Autorisierung	Fehler	3
Systemzugriff	Abmeldeaktivität	Abmeldung	Erfolg	2
Systemzugriff	Abmeldeaktivität	Abmeldung	Fehler	3
Systemzugriff	Anmeldeaktivität	Anmeldeversuch	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Systemzugriff	Anmeldeaktivität	Anmeldeversuch	Fehler	3
Systemzugriff	Berechtigungszuwachs	Berechtigungszuwachs	Erfolg	3
Systemzugriff	Berechtigungszuwachs	Berechtigungszuwachs	Fehler	3
Systemzugriff	Berechtigungen verwenden	Berechtigungen verwenden	Erfolg	3
Systemzugriff	Berechtigungen verwenden	Berechtigungen verwenden	Fehler	3
Systemzugriff	Aktivität zur Festlegung des Benutzers	Benutzereinstellung	Erfolg	2
Systemzugriff	Aktivität zur Festlegung des Benutzers	Benutzereinstellung	Fehler	3
Systemzugriff	Sitzungsaktivität	Sitzungserstellung	Erfolg	2
Systemzugriff	Sitzungsaktivität	Sitzungserstellung	Fehler	3
Systemzugriff	Sitzungsaktivität	Sitzungstrennung	Erfolg	2
Systemzugriff	Sitzungsaktivität	Sitzungstrennung	Fehler	3
Systemzugriff	Sitzungsaktivität	Sitzungsänderung	Erfolg	3
Systemzugriff	Sitzungsaktivität	Sitzungsänderung	Fehler	3
Unbekannte Kategorie	Unbekannte Klasse	Unbekannte Aktion	Unbekannt	0
Schwachstellen-Management	Schwachstellenbewertung	Informationssammlung	Erfolg	2
Schwachstellen-Management	Schwachstellenbewertung	Informationssammlung	Fehler	3
Schwachstellen-Management	Schwachstellenbewertung	Schwachstellenscan gestartet	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
Schwachstellen-Management	Schwachstellenbewertung	Schwachstellenscan gestartet	Fehler	3
Schwachstellen-Management	Schwachstellenbewertung	Schwachstellenscan abgeschlossen	Erfolg	2
Schwachstellen-Management	Schwachstellenbewertung	Schwachstellenscan abgeschlossen	Fehler	3
Schwachstellen-Management	Schwachstellen-Management	Schwachstelle gefunden	Erfolg	4
Schwachstellen-Management	Schwachstellen-Management	Schwachstelle gefunden	Fehler	3
SIM-Vorgänge	Alarmverwaltung	Alarm bestätigen	Erfolg	2
SIM-Vorgänge	Alarmverwaltung	Alarm bestätigen	Fehler	3
SIM-Vorgänge	Alarmverwaltung	Alarm mit Anmerkungen versehen	Erfolg	2
SIM-Vorgänge	Alarmverwaltung	Alarm mit Anmerkungen versehen	Fehler	3
SIM-Vorgänge	Alarmverwaltung	Alarm erstellen	Erfolg	2
SIM-Vorgänge	Alarmverwaltung	Alarm erstellen	Fehler	3
SIM-Vorgänge	Alarmverwaltung	Alarmlöschung	Erfolg	3
SIM-Vorgänge	Alarmverwaltung	Alarmlöschung	Fehler	3
SIM-Vorgänge	Alarmverwaltung	Alarm eskalieren	Erfolg	2
SIM-Vorgänge	Alarmverwaltung	Alarm eskalieren	Fehler	3
SIM-Vorgänge	Alarmverwaltung	Alarmänderung	Erfolg	2
SIM-Vorgänge	Alarmverwaltung	Alarmänderung	Fehler	3
SIM-Vorgänge	Alarmverwaltung	Alarmübermittlung	Erfolg	2
SIM-Vorgänge	Alarmverwaltung	Alarmübermittlung	Fehler	3
SIM-Vorgänge	Baseline-Verwaltung	Baseline akzeptieren	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
SIM-Vorgänge	Baseline-Verwaltung	Baseline akzeptieren	Fehler	3
SIM-Vorgänge	Baseline-Verwaltung	Baseline aktivieren	Erfolg	2
SIM-Vorgänge	Baseline-Verwaltung	Baseline aktivieren	Fehler	3
SIM-Vorgänge	Baseline-Verwaltung	Baseline erstellen	Erfolg	2
SIM-Vorgänge	Baseline-Verwaltung	Baseline erstellen	Fehler	3
SIM-Vorgänge	Baseline-Verwaltung	Baseline deaktivieren	Erfolg	3
SIM-Vorgänge	Baseline-Verwaltung	Baseline deaktivieren	Fehler	3
SIM-Vorgänge	Baseline-Verwaltung	Baseline definieren	Erfolg	2
SIM-Vorgänge	Baseline-Verwaltung	Baseline definieren	Fehler	3
SIM-Vorgänge	Baseline-Verwaltung	Baseline ändern	Erfolg	3
SIM-Vorgänge	Baseline-Verwaltung	Baseline ändern	Fehler	3
SIM-Vorgänge	Ereignisquellenverwaltung	Ereignisquelle autorisieren	Erfolg	2
SIM-Vorgänge	Ereignisquellenverwaltung	Ereignisquelle autorisieren	Fehler	3
SIM-Vorgänge	Ereignisquellenverwaltung	Ereignisquellenkonfiguration	Erfolg	2
SIM-Vorgänge	Ereignisquellenverwaltung	Ereignisquellenkonfiguration	Fehler	3
SIM-Vorgänge	Ereignisquellenverwaltung	Ereignisquelle entdecken	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
SIM-Vorgänge	Ereignisquellenverwaltung	Ereignisquelle entdecken	Fehler	3
SIM-Vorgänge	Ereignisquellenverwaltung	Ereignisquelle bereitstellen	Erfolg	2
SIM-Vorgänge	Ereignisquellenverwaltung	Ereignisquelle bereitstellen	Fehler	3
SIM-Vorgänge	Incident-Verwaltung	Incident schließen	Erfolg	2
SIM-Vorgänge	Incident-Verwaltung	Incident schließen	Fehler	3
SIM-Vorgänge	Incident-Verwaltung	Incident erstellen	Erfolg	2
SIM-Vorgänge	Incident-Verwaltung	Incident erstellen	Fehler	3
SIM-Vorgänge	Incident-Verwaltung	Incident löschen	Erfolg	3
SIM-Vorgänge	Incident-Verwaltung	Incident löschen	Fehler	3
SIM-Vorgänge	Incident-Verwaltung	Incident ändern	Erfolg	2
SIM-Vorgänge	Incident-Verwaltung	Incident ändern	Fehler	3
SIM-Vorgänge	Incident-Verwaltung	Incident auflösen	Erfolg	2
SIM-Vorgänge	Incident-Verwaltung	Incident auflösen	Fehler	3
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung mit Anmerkungen versehen	Erfolg	2
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung mit Anmerkungen versehen	Fehler	3
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung schließen	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung schließen	Fehler	3
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung löschen	Erfolg	3
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung löschen	Fehler	3
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung ändern	Erfolg	2
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung ändern	Fehler	3
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung öffnen	Erfolg	2
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung öffnen	Fehler	3
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung anhalten	Erfolg	2
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung anhalten	Fehler	3
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung auflösen	Erfolg	2
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung auflösen	Fehler	3
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung fortsetzen	Erfolg	2
SIM-Vorgänge	Untersuchungsverwaltung	Untersuchung fortsetzen	Fehler	3
SIM-Vorgänge	Benachrichtigungsverwaltung	Benachrichtigung erstellen	Erfolg	2
SIM-Vorgänge	Benachrichtigungsverwaltung	Benachrichtigung erstellen	Fehler	3
SIM-Vorgänge	Benachrichtigungsverwaltung	Benachrichtigung übermitteln	Erfolg	2

KATEGORIE	KLASSE	AKTION	Ergebnis	Sicherheitsebene
SIM-Vorgänge	Benachrichtigungsverwaltung	Benachrichtigung übermitteln	Fehler	3
SIM-Vorgänge	Anforderungsverwaltung	Anforderung mit Anmerkungen versehen	Erfolg	2
SIM-Vorgänge	Anforderungsverwaltung	Anforderung mit Anmerkungen versehen	Fehler	3
SIM-Vorgänge	Anforderungsverwaltung	Anforderung schließen	Erfolg	2
SIM-Vorgänge	Anforderungsverwaltung	Anforderung schließen	Fehler	3
SIM-Vorgänge	Anforderungsverwaltung	Anforderungserstellung	Erfolg	2
SIM-Vorgänge	Anforderungsverwaltung	Anforderungserstellung	Fehler	3
SIM-Vorgänge	Anforderungsverwaltung	Anforderung ändern	Erfolg	2
SIM-Vorgänge	Anforderungsverwaltung	Anforderung ändern	Fehler	3
SIM-Vorgänge	Anforderungsverwaltung	Anforderung übermitteln	Erfolg	2
SIM-Vorgänge	Anforderungsverwaltung	Anforderung übermitteln	Fehler	3