

CA Enterprise Log Manager

管理ガイド

r12.5

このドキュメント(組み込みヘルプ システムおよび電子的に配布される資料を含む、以下「本ドキュメント」)は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社(以下「CA」)により随時、変更または撤回されることがあります。

CA の事前の書面による承諾を受けずに本ドキュメントの全部または一部を複製、譲渡、開示、変更、複本することはできません。本ドキュメントは、CA が知的財産権を有する機密情報です。ユーザは本ドキュメントを開示したり、(i) 本ドキュメントが関係する CA ソフトウェアの使用について CA とユーザとの間で別途締結される契約または (ii) CA とユーザとの間で別途締結される機密保持契約により許可された目的以外に、本ドキュメントを使用することはできません。

上記にかかわらず、本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負います。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害(直接損害か間接損害かを問いません)が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本ドキュメントの制作者は CA です。

「制限された権利」のもとでの提供: アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1) 及び (2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2010 CA. All rights reserved. 本書に記載された全ての製品名、サービス名、商号およびロゴは各社のそれぞれの商標またはサービスマークです。

CA 製品リファレンス

このマニュアルが参照している CA の製品は以下のとおりです。

- 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®

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの **Web** サイト (<http://www.ca.com/jp/support/>) をご覧ください。

マニュアルの変更点

このドキュメントの最終リリース以降、サービスと CA アダプタ、サブスクリプション、フィルタとプロファイル、クエリとレポート、イベント相関とインシデント管理、およびログストレージに関する説明が更新されました。

関連するトピックは以下のとおりです。

- サービスおよび CA アダプタ
 - サービスの設定 -- 相関サービス、インシデント サービス、およびその他の新しいサービスに関するトピックが追加されました。
- サブスクリプション
 - サブスクリプションの拡張に関するトピック -- サブスクリプション ダウンロード ダッシュボードおよびその他の新機能または変更された機能に関するトピックが追加および更新されました。
 - オンデマンド更新 -- このトピックが更新され、オンデマンド更新処理の変更が反映されました。
- フィルタおよびプロファイル
 - グローバルおよびローカル フィルタ -- この既存のトピックおよびその他のトピックが更新され、イベント データベースまたはインシデント データベースのいずれかに対してフィルタを設定できる新機能が反映されました。
- クエリおよびレポート
 - クエリの作成方法 -- この既存のトピックおよび関連トピックが変更され、イベント データベースまたはインシデント データベースのいずれかに対してクエリを実行できる新機能が反映されました。
 - キー設定済みリストを管理する方法 -- この既存のトピックおよび関連トピックが変更され、キー設定済みリストを設定するインターフェースの変更が反映されました。
- イベント相関およびインシデント管理 -- この新しい章では、イベント相関ルール、それらのルールによってインシデントが作成される仕組み、およびインシデントの管理方法について説明します
 - 相関ルール タスク -- この新しいトピックおよび関連トピックでは、相関ルール、インシデント通知の設計と適用、および定義済み相関ルールの使用方法について説明します。

- インシデント管理タスク -- この新しいトピックおよび関連トピックでは、イベント相関によって作成されるインシデントに関する情報（インシデントの詳細の表示など）を提供します。

■ ログ ストレージ

- データ整合性検証 -- この新しいトピックおよび関連トピックでは、CA Enterprise Log Manager データの整合性システムについて説明します。これには、自動検証をスケジュールする方法、オンデマンドで検証を行う方法、およびデータベース シグネチャ キーの使用方法が含まれています。

詳細情報:

[サービス タスク](#) (P. 148)

[グローバル設定の編集](#) (P. 149)

[サービスの設定](#) (P. 154)

[グローバル サブスクリプション ステータスの表示](#) (P. 223)

[オンデマンド更新について](#) (P. 231)

[グローバル フィルタおよびローカル フィルタ](#) (P. 247)

[グローバル フィルタの作成](#) (P. 258)

[ローカル フィルタの作成](#) (P. 262)

[クエリおよびレポートについて](#) (P. 266)

[クエリの作成方法](#) (P. 295)

[キー設定済みリストを管理する方法](#) (P. 337)

目次

第 1 章: 概要	21
本書の内容	21
第 2 章: ユーザ アカウント	25
自己管理タスク	25
ユーザ アカウントのアンロック	26
ユーザ パスワードの変更	27
ルールに関連付けられたタスク	27
監査者タスク	28
アナリスト タスク	30
管理者タスク	31
既定の設定でアカウントを作成する方法	39
グローバル グループの作成	40
グローバル ユーザの作成	41
グローバル ユーザへのロールの割り当て	43
参照されたユーザ アカウントを管理する方法	44
ユーザの有効化のガイドライン	45
ユーザ アカウントの編集	46
ユーザ パスワードのリセット	49
ユーザ アカウントの削除	50
第 3 章: ポリシー	51
ポリシーの概要	52
事前定義されたアクセス ポリシー	52
全ユーザのポリシーの確認	53
Auditor 用のポリシーの確認	57
Analyst 用のポリシーの確認	59
Administrator のポリシーの確認	62
登録済み製品用のアクセス ポリシー	64
すべてのアクセス ポリシーのバックアップ	65
アクセス ポリシーの復元	70

第 4 章: カスタム ロールおよびカスタム ポリシー 73

ポリシー作成時のガイドライン	73
CALM アクセス ポリシーのタイプ	77
リソースとアクション	80
CALM リソースと EEM フォルダ	83
グローバル リソースと CA EEM の機能	86
ユーザ ロールの計画	87
カスタム ユーザ ロールおよびアクセス ポリシーの設定	88
アプリケーション ユーザ グループ (ロール) の作成	92
カスタム ロールによる CA Enterprise Log Manager へのアクセスの許可	93
既存ポリシーへの ID の追加	95
CALM アクセス ポリシーの作成	96
スコープ ポリシーの作成	99
既存のポリシーをベースにしたポリシーの作成	103
新しいポリシーのテスト	105
動的ユーザ グループ ポリシーの作成	106
アクセスフィルタの作成	108
ユーザ アカウントとアクセス ポリシーの保守	110
カレンダーの作成	110
ポリシーへのカレンダーの追加	111
例: 営業日へのアクセス制限	112
アクセス ポリシーのエクスポート	114
カスタム ポリシーの削除	115
アクセスフィルタおよび責任ポリシーの削除	115
例: 管理者以外のユーザへのアーカイブ管理の許可	116
ユーザ: Win-Admin のデータ アクセスを制限するシナリオ	120
手順 1: Win-Admin ユーザの作成	122
手順 2: CALM アプリケーション アクセス ポリシーへの Win-Admin の追加	123
手順 3: Win-Admin システム アクセス ポリシーの作成	124
手順 4: Win-Admin データ アクセス フィルタの作成	128
手順 5: Win-Admin ユーザとしてのログオン	131
手順 6: 許可されたアクションの拡張	132
ロールのアクセス制限: PCI-Analyst シナリオ	134
手順 1: 作成するロールとポリシーの計画	135
手順 2: PCI-Analyst ロールの作成	136
手順 3: CALM アプリケーション アクセス ポリシーへの PCI-Analyst の追加	137

手順 4: 既存ポリシーへの PCI-Analyst の追加	137
手順 5: 分析担当者用レポート表示/編集ポリシーをベースにしたポリシーの作成	138
手順 6: PCI-Analyst ロールへのユーザの割り当て	139
手順 7: PCI-Analyst としてのログインとアクセス権の評価	139
カスタム統合のポリシーの例	141
抑制ルールおよび集約ルール用のポリシーの例	143

第 5 章: サービスおよび CA アダプタ 147

サービス タスク	148
サービス ホストの削除	149
グローバル設定の編集	149
グローバル サービス設定の編集	152
ローカル サービスの設定の編集	153
サービスの設定	154
アラート サービスに関する注意事項	154
関連サービスに関する注意事項	157
イベントログストアに関する注意事項	158
インシデント サービスに関する注意事項	163
ODBC サーバの注意事項	164
レポートサーバに関する注意事項	165
ルールのテスト サービスに関する注意事項	166
サブスクリプションに関する注意事項	166
システム ステータス サービス	171
CA アダプタ環境設定タスク	171
グローバル アダプタ設定の編集	172
ローカル アダプタ設定の編集	173
アダプタの自己監視イベントの表示	174
アダプタ ステータスの表示	175
SAPI サービスに関する注意事項	176
iTechnology イベント サービスに関する注意事項	178
システム ステータス タスク	178
サポート診断ファイルの作成	179
ホスト サーバの再起動	180
ELM サービスの再起動	180
サービスのステータスおよびバージョンの確認	181
システム ステータスの自己監視イベントの確認	181

第 6 章: ログ ストレージ 183

ログ ストレージについて	184
イベントログ データベースの状態	186
バックアップおよび復元の自動化	189
データ整合性検証	190
自動整合性検証の有効化	190
データ整合性検証のスケジュール	191
データ整合性のオンデマンド検証	191
検疫されたデータベースのシグネチャの再生成	192
キーの循環	192
キーのインポート	193
キーのエクスポート	193
復元用の非対話型認証の設定	194
例: リモートストレージから復元ポイントへの認証の設定	195
例: ストレージ サーバからレポート サーバへの認証の設定	197
アーカイブ カタログのクエリ	200
自動アーカイブ済みファイルの復元	202
アーカイブ済みデータベースを復元するための復元スクリプト	203
手動によるアーカイブ済みデータベースのバックアップ	205
バックアップされていないデータベースの特定	206
バックアップの実行	207
バックアップの記録	208
手動による元のイベントログ ストアへのアーカイブの復元	209
アーカイブ済みデータベースの復元の準備	210
アーカイブ済みデータベースのアーカイブ ディレクトリへの移動	212
手動によるアーカイブ済みファイルの復元	213
復元の検証	214
手動による新規イベントログ ストアへのアーカイブの復元	215
復元されたアーカイブの最大アーカイブ日数の設定	217
復元されたデータベースのカatalogへの追加	218
LMArchive によるバックアップ/復元の追跡	219

第 7 章: サブスクリプション 221

サブスクリプションによる CA Enterprise Log Manager バージョン 12.5 へのアップグレード	221
グローバル サブスクリプション ステータスの表示	223

サーバのサブスクリプション ステータスの表示	224
グローバル サブスクリプション設定の編集	226
サーバのローカル サブスクリプション設定の編集	227
オフライン サブスクリプション用のモジュールのダウンロードと選択	229
オンデマンド更新について	231
オンデマンド更新の開始	233
更新用の空きディスク領域	235
サブスクリプション公開鍵について	236
サブスクリプションの自己監視イベント	236
サブスクリプション イベントの監視	237
サブスクリプション イベントの詳細の表示	240
エージェントおよびコネクタへのサブスクリプション更新の適用	242

第 8 章: フィルタおよびプロファイル 245

第 9 章: グローバル フィルタおよびローカル フィルタ 247

単純フィルタについて	248
単純フィルタの設定	249
プロファイル フィルタについて	250
プロファイルの作成方法	251
プロファイル ウィザードを開きます。	252
プロファイルの詳細の追加	252
データフィルタの作成	253
タグ フィルタの作成	254
プロファイルのインポート	255
プロファイルのエクスポート	256
プロファイルの設定	257
グローバル フィルタの作成	258
グローバル クエリに関する値の設定	260
グローバル フィルタの編集	261
グローバル フィルタの削除	261
ローカル フィルタの作成	262
ローカル フィルタの編集	263
ローカル フィルタの削除	263

第 10 章: クエリおよびレポート	265
クエリおよびレポートについて	266
タグ タスク	270
クエリの表示	270
レポートの表示	272
選択されたレポートの表示の無効化	273
例: PCI レポートの実行	274
PCI タグが付いたレポートのリストの表示	274
特定の PCI DSS 規制のレポートの検索	275
単一の PCI レポートの操作	277
プロンプト	278
コネクタ プロンプトの使用	279
ホスト プロンプトの使用	282
IP プロンプトの使用	285
ログ名プロンプトの使用	288
ポートプロンプトの使用	290
ユーザ プロンプトの使用	292
クエリの作成方法	295
クエリの実設計ウィザードの表示	296
クエリの詳細の追加	297
クエリ列の追加	298
クエリフィルタの設定	301
結果の条件の設定方法	306
クエリ表示の視覚化の作成	311
ドリルダウンレポートの追加	312
クエリの編集	313
カスタム クエリの削除	313
選択されたクエリの表示の無効化	314
クエリ定義のエクスポートとインポート	314
クエリ定義のエクスポート	315
クエリ定義のインポート	316
レポートの作成方法	317
レポート デザイン ウィザードの表示	317
レポートの詳細の追加	318
レポートレイアウトの設計	319
例: 既存のクエリによるレポートの作成	320

例: 連携および連携されたレポートの設定	323
レポートの編集	328
カスタムレポートの削除	328
例: 30 日以上経過した日単位レポートの削除	329
レポート定義のエクスポート	330
レポート定義のインポート	331
キー設定済みリストのあるレポートの使用準備	332
動的値のインポートの有効化	333
キー設定済みリストを管理する方法	337
事前定義済みレポート用のキー設定済み値の作成	345
キー設定済みリストを使用したレポートの表示	349

第 11 章: アクション アラート 351

アクション アラートについて	352
アクション アラートとしてタグが付いたクエリの使用	353
アラートで使用するその他のクエリの指定	355
アクション アラートのクエリのカスタマイズ	356
重大なイベント用の単純フィルタの指定	357
重大なイベントだけを取得するクエリの作成	359
重大なイベントだけを取得するためのクエリのカスタマイズ	361
アクション アラートに関する注意事項	367
CA IT PAM イベント/アラート出力プロセスの使用	370
CA IT PAM イベント/アラート出力プロセスについて	371
サンプルのイベント/アラート出力プロセスのインポート	379
イベント/アラート出力プロセスを作成するためのガイドライン	387
CA IT PAM 統合の詳細の収集	390
例: 選択したクエリ結果を使用したイベント/アラート出力プロセスの実行	394
イベント/アラート出力プロセスに送信するイベントのクエリの実装	398
例: 行ごとに IT PAM プロセスを実行するアラートの送信	400
例: クエリごとに IT PAM プロセスを実行するアラートの送信	405
SNMP トラップの操作	408
SNMP トラップについて	408
トラップとして送信するアラート用の単純なフィルタの例	409
MIB ファイルについて	410
SNMP トラップを使用する手順	427
SNMP トラップの宛先との統合の設定	428

アラートから SNMP トラップを受信するための CA Spectrum の準備	429
例: CA Spectrum への設定変更のアラート通知	434
アラートから SNMP トラップを受信するための CA NSM の準備	439
例: CA NSM に対する設定変更のアラート	444
アクション アラートを作成する方法	453
アクション アラートのスケジュール ウィザードの表示	454
アラート クエリの選択	455
アラート ジョブ スケジュール用パラメータの設定	456
通知の宛先の設定	457
アラート ジョブ クエリの宛先の定義	462
例: ディスク空き容量低下用のアクション アラートの作成	463
例: 自己監視イベント用のアラートの作成	467
例: イベントフローの停止時に管理者に電子メールを送信	470
アクション アラート保持の設定	473
例: Business_Critical_Sources 用のアラートの作成	474
アクション アラートの編集	477
アクション アラートの無効化または有効化	478
アクション アラートの削除	479

第 12 章: スケジュール済みレポート 481

作成済みレポートの表示	481
フィルタレポート	482
作成済みレポートの表示	483
レポートジョブをスケジュールする方法	484
レポートのスケジュール ウィザードの表示	485
レポートの選択	486
詳細フィルタの使用	487
結果の条件の設定方法	489
スケジュール用パラメータの設定	493
フォーマットと通知の設定の選択	494
レポート クエリ ターゲットの選択	495
例: 共通のタグを持つレポートのスケジュール	495
例: 日単位 PCI レポートを PDF として電子メールで送信する	499
スケジュール済みレポートジョブの編集	500
スケジュールされたレポートジョブの有効化および無効化	501
スケジュールされたレポートジョブの削除	502

自己監視イベント	502
自己監視イベントの表示	503

第 13 章: 抑制ルールおよび集約ルール 505

イベント精製コンポーネントのバージョン	505
抑制ルールおよび集約ルール タスク	506
抑制ルールによる影響	507
抑制ルールを作成する方法	508
集約ルールを作成する方法	513
抑制ルールまたは集約ルールの適用	520
エージェント コンポーネントに抑制と集約を適用する方法	520
抑制ルールまたは集約ルールのコピー	524
抑制ルールまたは集約ルールの編集	525
抑制ルールまたは集約ルールの削除	526
抑制ルールまたは集約ルールのインポート	527
抑制ルールまたは集約ルールのエクスポート	528
Windows イベント 560 の抑制ルールの作成	529

第 14 章: マッピングおよび解析 531

イベント状態	532
マッピングおよび解析ルール タスク	534
メッセージ解析ファイルを作成する方法	534
解析ファイル ウィザードの表示	536
ファイル詳細の定義	536
サンプル イベントのロード	538
グローバル フィールドの追加	539
事前一致フィルタの作成	540
解析フィルタの作成	542
XMP ファイルの分析	552
データ マッピング ファイルを作成する方法	553
マッピング ファイル ウィザードの表示	555
ファイル詳細の指定	556
サンプル イベントの利用	556
直接マッピングの設定	558
関数マッピングの設定	559

concat 関数マッピングの設定	561
条件付きマッピングの設定	562
ブロック マッピングの設定	564
マッピング分析の実行	566
イベント転送ルール タスク	566
イベント転送ルールを作成する方法	567
転送された syslog イベントについて	574
転送ルールの編集	575
転送ルールの削除	575
転送するルールのインポート	576
転送するルールのエクスポート	577

第 15 章: 統合およびコネクタ 579

統合とコネクタのタスク	579
統合の作成方法	581
統合ウィザードの表示	582
統合コンポーネントの追加	583
抑制ルールと集約ルールの適用	584
デフォルト設定の定義	585
ファイル ログ設定の設定	586
syslog リスナの作成方法	589
リスナ ウィザードの表示	590
リスナ コンポーネントの追加	591
抑制ルールおよび集約ルールの適用	592
デフォルト設定の定義	593
syslog タイム ゾーンの追加	595
新しい統合バージョンの作成	596
統合の削除	597
統合定義のエクスポートおよびインポート	597
統合定義のインポート	598
統合定義のエクスポート	598
コネクタの作成方法	599
コネクタウィザードの表示	599
コネクタの詳細の追加	600
抑制ルールおよび集約ルールの適用	601
コネクタ設定の設定	601

コネクタの表示	602
コネクタ ガイドの表示	603
コネクタの編集	604
保存済み設定について	604
保存済み設定の作成	605
コネクタを一括して設定する方法	606
収集ソースの設定ウィザードの表示	606
ソースの詳細の選択	608
抑制ルール適用	609
集約ルール適用	609
コネクタの設定	610
エージェントの選択およびソースのマッピング	611
複数コネクタの設定の更新	612
第 16 章: イベント関連およびインシデント管理	613
第 17 章: 関連ルール タスク	615
関連ルールについて	616
定義済み関連ルールの使用	617
関連ルールとキー設定済みリストの使用	621
例: テスト用の CSV ファイルの作成	622
インシデント通知について	622
インシデント通知を設計および適用する方法	623
第 18 章: インシデント管理タスク	627
インシデント詳細の表示	628
第 19 章: エージェント	629
エージェント インストールの計画	629
エージェント設定の計画	632
直接ログ収集の計画	633
エージェントレス ログ収集の計画	635
エージェント ベースのログ収集の計画	635
設定するレベルの選択	636
エージェント管理タスク	637

エージェント認証キーの更新	638
エージェント バイナリのダウンロード	639
エージェントの設定	640
変更された設定ファイルの処理	642
エージェント ダッシュボードの表示	643
エージェントまたはコネクタのステータスの表示と管理	645
エージェントグループを作成する方法	647
エージェントグループ ウィザードの表示	647
エージェントグループの詳細の追加	648
エージェントグループへのエージェントの追加	649
エージェント管理の設定方法	650
Log Manager サーバの割り当てウィザードの表示	651
ターゲット エージェントの選択	652
ログ マネージャの選択	653
サーバ IP アドレスの変更の影響からエージェントを保護する方法	654
動的 IP アドレスを持つサーバの可用性の確保	655
静的 IP アドレスを再割り当てする際のサーバの可用性の確保	655
サブスクリプション更新を適用する方法	657
更新リスト ウィザードの表示	658
更新するエージェントまたはコネクタの選択	659
エージェントまたはコネクタ統合のバージョンの更新	660

第 20 章: カスタム証明書 661

カスタム証明書の実装	661
管理 CA Enterprise Log Manager サーバへの信頼されたルート証明書の追加	662
その他のすべての CA Enterprise Log Manager サーバへの信頼されたルート証明書の追加	664
アクセス ポリシーへの証明書共通名の追加	665
新しい証明書の展開	666

付録 A: アクセシビリティ機能 669

アクセシビリティ モード	669
アクセシビリティ コントロール	669
CA Enterprise Log Manager 言語表示設定	670
手動による CA Enterprise Log Manager のローカライゼーション	671

付録 B: ODBC と JDBC を使用した収集済みイベントへのアクセス	673
CA Enterprise Log Manager での ODBC/JDBC アクセスについて	673
CA Enterprise Log Manager で使用する ODBC および JDBC クエリの作成	674
SQL サポートの制限事項	674
サポートされている SQL 機能	675
クエリの処理方法	676
結果列の別名	677
結果の制限	677
CA Enterprise Log Manager 固有のエラー コード	678
例: アクセスフィルタを使用して、ODBC の結果を制限する	678
例: Crystal Reports と共に ODBC および JDBC クライアントを使用する準備	680
ODBC や JDBC へのアクセス用の CA Enterprise Log Manager ユーザの作成	681
ODBC サービス設定の設定	682
「ELM」ODBC データソースの作成	682
Crystal Reports 設定ファイルの編集	685
ODBC の例のためのイベントの作成	687
ODBC を利用した Crystal Reports からイベント ログ ストアへのアクセス	688
JDBC を使用した Crystal Reports からイベントへのアクセス	689
JDBC ドライバ JAR ファイルのコピー	689
JDBC を利用した Crystal Reports からイベント ログ ストアへのアクセス	690
Windows システム上の ODBC クライアントの削除	691
JDBC クライアントの削除	691
 用語集	 693
 索引	 725

第 1 章：概要

このセクションには、以下のトピックが含まれています。

[本書の内容](#) (P. 21)

本書の内容

この「CA Enterprise Log Manager 管理ガイド」は、管理者が CA Enterprise Log Manager をインストールし、初期サーバ設定を実行した後に実行するタスクについて説明します。これらのタスクには、システムの非標準的な変更に対応するタスクのほか、定期的に行うルーチンタスクや、継続的な監視タスクなどがあります。

このマニュアルは、以下を初めとするすべてのユーザを対象としています。

- 本製品の設定の管理、およびログ ストレージとサブスクリプション更新の管理を担当する管理者
- レポートを使用した環境の監視、カスタムレポートの作成、およびアラート生成のスケジュールを担当する分析担当者
- レポートのスケジュール、クエリとレポートを使用した規制へのコンプライアンスの確認、およびレポートへの注釈の追加を担当する監査担当者

このマニュアルには、用語集と目次が含まれています。次に、各セクションの概要を示します。

セクション	説明内容
ユーザ アカウント	事前定義済みロールを使用したユーザ アカウントの設定と、ユーザ アカウントの自己管理
ポリシー	事前定義済みロールおよびポリシーを活用した、カスタム ロール および関連ポリシーの計画
カスタム ロールおよびカスタム ポリシー	カスタム ロール、カスタム ポリシーおよびアクセス フィルタを使用したユーザ アクセスの制限
サービスおよび CA アダプタ	イベント ログ ストア、レポート サーバ、サブスクリプション サービス、および特定のイベント アダプタの設定

セクション	説明内容
ログ ストレージ	自動アーカイブの設定、およびアーカイブ済みデータベースの復元
サブスクリプション	サブスクリプション設定の管理、更新の適用、およびサブスクリプション バックアップの復元
フィルタおよびプロファイル	フィルタを使用した、1 つのレポートまたはクエリ、あるいはすべてのレポートとクエリに表示するデータの制限 プロファイルを使用した、タグリスト、クエリリスト、およびレポートリストの制限
クエリおよびレポート	現在のイベント ログおよび最近のイベント ログを表示するためのクエリとレポートの作成、編集、およびインポート/エクスポート
アクション アラート	指定したイベントの発生時に、ユーザまたは SNMP トラップの宛先への通知あるいは IT PAM プロセスを実行するアクション アラートの作成
スケジュール済みレポート	レポート ジョブのスケジュールと管理、作成済みレポートの表示、および注釈の追加
抑制ルールおよび集約ルール	サーバの負荷を軽減し、不要なイベントの収集や処理を防ぐための抑制ルールおよび集約ルールの作成と使用
マッピングおよび解析	各種の形式でフォーマットされている元のイベントを標準的な CEG 互換の値に再設定するためのマッピング ルールと解析ルールの作成と使用、およびイベント転送ルールの作成
統合およびコネクタ	コネクタとして導入することで、単一のイベントソースから CA Enterprise Log Manager サーバへのイベントの精製と送信が可能になる、製品統合の作成
エージェント	エージェントの使用計画、エージェント インストールの準備、エージェントおよびエージェントグループの設定、およびエージェントへのサブスクリプション更新の適用
カスタム証明書	事前定義済み証明書を置き換えるためのカスタム証明書の実装
アクセシビリティ機能	アクセシビリティ コントロールの使用
ODBC/JDBC による収集されたイベントへのアクセス	サード パーティのレポート ユーティリティを使用したカスタムレポートの設定、またはサード パーティ製品を使用した特定のログ情報の取得

注: サポートするオペレーティング システムやシステム要件の詳細については、「リリース ノート」を参照してください。単一システムの運用を開始し、収集された **syslog** および **Windows** イベントに関するクエリ結果を表示するためのチュートリアルについては、「概要ガイド」を参照してください。**CA Enterprise Log Manager** のインストールおよび初期設定の実行に関する詳細な手順については、「実装ガイド」を参照してください。エージェントのインストールの詳細については、「エージェント インストール ガイド」を参照してください。**CA Enterprise Log Manager** ページの使用方法については、オンライン ヘルプを参照してください。

第 2 章: ユーザ アカウント

このセクションには、以下のトピックが含まれています。

- [自己管理タスク \(P. 25\)](#)
- [ロールに関連付けられたタスク \(P. 27\)](#)
- [既定の設定でアカウントを作成する方法 \(P. 39\)](#)
- [グローバル グループの作成 \(P. 40\)](#)
- [グローバル ユーザの作成 \(P. 41\)](#)
- [グローバル ユーザへのロールの割り当て \(P. 43\)](#)
- [参照されたユーザ アカウントを管理する方法 \(P. 44\)](#)
- [ユーザの有効化のガイドライン \(P. 45\)](#)
- [ユーザ アカウントの編集 \(P. 46\)](#)
- [ユーザ パスワードのリセット \(P. 49\)](#)
- [ユーザ アカウントの削除 \(P. 50\)](#)

自己管理タスク

CA Enterprise Log Manager へのアクセス権を持つユーザは、設定されたユーザ ストアがデフォルトの CA Enterprise Log Manager ユーザ ストアであれば、自分のパスワードを変更し、ロックされたユーザ アカウントをアンロックできます。

管理者が新規ユーザ アカウントを作成すると、新しいパスワードが割り当てられます。ユーザは、最初のログイン セッション中に、そのパスワードをパスワード ポリシーに準拠する新しいパスワードに変更します。パスワード ポリシーでは、ユーザ名と同じパスワードを許可するかどうか、最小文字数と最大文字数、最大繰り返し文字数、および数字の最小数が定義されます。パスワードの変更禁止期間と最長有効期間に関するパスワード ポリシーに基づいて、一定の頻度でパスワードを変更することはユーザの責任です。

個人ユーザは、以下の方法で自分のアカウントを管理します。

- パスワード ポリシーに準拠する方法でパスワードを変更する
- 関連するパスワード ポリシーによって許可されていれば、ロックされているユーザ アカウントをアンロックする

ユーザ アカウントのアンロック

パスワード ポリシーによって許可されていれば、ルールにかかわらずロックされたユーザ アカウントをアンロックできます。アカウントがロックされると、ルールに付与された権限にアクセスするには、別のユーザがそのロックを解除する必要があります。

ロックおよびアンロックは、以下の 2 つのパスワード ポリシーによって制御されます。

- <n> 回ログインに失敗したら、ユーザ アカウントをロックする
- ユーザにパスワードのアンロックを許可する

ある回数ログインに失敗した場合や、指定されたしきい値を超える回数、無効な認証情報でログインしようとした場合にユーザ アカウントをロックするようパスワード ポリシーを設定すれば、ユーザ アカウントをロックできます。

別のユーザによってパスワードをアンロックできるようにパスワード ポリシーを設定すれば、すべてのユーザが別のユーザのアカウントをアンロックできます。ユーザ アカウントをアンロックするには、そのユーザのパスワードが必要です。

ユーザ アカウントをアンロックする方法

1. [管理] タブをクリックし、[ユーザとアクセスの管理] サブタブをクリックします。
2. 左側ペインの[ユーザのアンロック]をクリックします。
3. ユーザ名とパスワードを入力し、[アンロック] ボタンをクリックします。
ユーザ アカウントがアンロックされます。

ユーザ パスワードの変更

ロールにかかわらず、自分のパスワードを変更できます。パスワードの最長有効期間に関するパスワード ポリシーが設定されている場合は、そのポリシーに一致する間隔でパスワードを変更する必要があります。

以下のケースに当てはまる場合は、できるだけ早くパスワードを変更してください。

- ユーザ アカウントをアンロックするために、自分のパスワードをだれかに教えた
- パスワードを忘れ、管理者にパスワードをリセットしてもらった

パスワードの変更方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. 左側ペインの[パスワードの変更]をクリックします。
3. 古いパスワードを入力します。
4. 新しいパスワードを 2 回入力します。
5. [OK]をクリックします。

ロールに関連付けられたタスク

管理者は、実行するタスクに基づいてユーザにロールを割り当てます。ユーザには、事前定義済みロール (Auditor、Analyst、および Administrator) を割り当てるか、作成したカスタム ロールを割り当てることができます。事前定義済みロールを使用する影響度を評価するために、各ロールに関連付けられたタスクを確認してください。

詳細情報:

[監査者タスク](#) (P. 28)

[アナリストタスク](#) (P. 30)

[管理者タスク](#) (P. 31)

監査者タスク

内部監査者は、以下のようなタスクを実行できます。

- クエリの検索と選択、およびクエリ結果の表示
- 選択したクエリ結果行について、CA IT PAM で設定したイベント/アラート出力プロセスを実行します。
- 最新のレポートの表示
- レポートのスケジュール
- スケジュール済みレポート ジョブ リストの表示
- 作成済みレポートリストの表示
- 作成済みレポートの表示および注釈の追加
- フィルタおよびプロファイルの設定

サードパーティ担当者のユーザ アカウントを作成する際には、権限レベルの低い **Auditor** ロールを割り当てることができます。たとえば、スケジュール済みアラートによりクエリレベルでイベント/アラート出力プロセスを実行する場合、アラートは、説明に URL を追加して **CA Enterprise Log Manager** に送信します。サードパーティ担当者が **CA Enterprise Log Manager** を参照できるようにするには、ユーザ アカウントが必要です。

注: アナリストと管理者は、各自のロール固有のタスクに加え、監査者のすべてのタスクを実行できます。

サイトの監査を行う間、一時的に **CA Enterprise Log Manager** へのアクセスを許可される外部監査者は、以下の内容について規制へのコンプライアンスを検証できます。

- ログが目的のソースから収集されているかどうかの検証
- データ損失の防止に対して手順が適切であるかどうかの検証。たとえば、データ損失を防ぐため、十分な頻度でデータのバックアップが実行されているかどうかを検証します。
- セキュリティ違反を検知するためにログが定期的に確認されているかどうかの検証
- ログが安全なアーカイブに正常に保存されているかどうかの検証
- アーカイブ済みデータの経過日数がログ保持の基準を満たしているかどうかの検証
- ログの内容に、保持が義務付けられた内容が含まれているかどうかの検証

詳細情報:

[レポートジョブをスケジュールする方法](#) (P. 484)

[作成済みレポートの表示](#) (P. 481)

[作成済みレポートの表示](#) (P. 483)

[クエリの表示](#) (P. 270)

[レポートの表示](#) (P. 272)

[例: 選択したクエリ結果を使用したイベント/アラート出力プロセスの実行](#) (P. 394)

[例: クエリごとに IT PAM プロセスを実行するアラートの送信](#) (P. 405)

アナリスト タスク

システム アナリストは、ログ収集ネットワークを監視して、レポート データの収集および配布を行います。

管理者は、以下のタスクを担当するユーザに **Analyst** ロールを割り当てます。

- カスタム レポートおよびカスタム クエリの作成と編集

レポートは、フィルタを備えた事前定義済みクエリやカスタム クエリの実行によって生成されるイベントログ データを、グラフィック形式や表形式で表示したものです。データの取得先には、選択したサーバや、必要な場合はその連携サーバの、イベントログ ストア内にあるホット データベース、ウォーム データベース、および解凍済みデータベースを指定できます。

- アクション アラートをスケジュールします。

アクション アラートは、スケジュール済みのクエリ ジョブです。ポリシー違反、使用状況、ログオン パターンなど、近い将来に注意が必要となりそうな情報を検出するために使用できます。アラート データは、UI または RSS フィードによって表示できます。スケジュールされたアラートを、電子メール受信者、SNMPトラップの宛先、または CA IT PAM イベント/アラートの出力プロセスに送信できます。プロセスは行ごとに 1 回、またはクエリごとに 1 回実行できます。

- タグの作成

タグは、同じカテゴリに属するクエリやレポートを識別するために使用する言葉またはキー フレーズです。特定のタグが付いたレポートを選択するよう設定したスケジュール済みジョブに新しいレポートを追加するには、この新しいレポートに共通のタグを追加するだけです。また、タグはクエリに関連付けられたキー フレーズでもあるため、タグを利用したクエリ内容の把握のほか、キー フレーズ ベースの分類や検索が可能です。

- RSS (Rich Site Summary) フィードの表示

RSS イベントは、サードパーティ製品やユーザにアクション アラートを送信するために CA Enterprise Log Manager によって生成されるイベントです。このイベントは、各アクション アラート結果のサマリであり、結果ファイルへのリンクでもあります。指定した RSS フィード項目の期間は設定可能です。

Analyst が CA Enterprise Log Manager の操作をよく理解すると、以下の作業を実行できます。

1. 使用可能な事前定義済みレポートの検証 (Auditor も実行可能)
2. カスタムレポートの作成、カスタムレポート用タグの作成、カスタムレポートのスケジュール、表示、および注釈の追加
3. 定期的な生成にとって重要なレポートのスケジュール (Auditor も実行可能)
4. 生成されたレポートの確認と注釈の入力 (Auditor も実行可能)
5. アラート送信基準、使用フォーマット、および受信者の特定と、基準が満たされた場合に生成されるアラートのスケジュール

管理者タスク

Administrator ロールを割り当てられたユーザには、すべての CA Enterprise Log Manager タブから使用できる機能に対して、無制限のアクセス権が与えられます。[管理]タブへのフルアクセス権を持っているのは、Administrator ロールを割り当てられたユーザだけです。管理者は、[管理]タブから、ログ収集のすべての設定、すべてのサービス、およびすべてのユーザアクセスを設定し、管理します。

詳細情報:

[ログ収集の設定とカスタマイズ](#) (P. 32)

[サービス設定および監視](#) (P. 34)

[ユーザとアクセスの管理](#) (P. 37)

ログ収集の設定とカスタマイズ

管理者ルールを割り当てられたユーザだけが、ログ収集に関する機能を設定し、管理することができます。管理者は、[管理]タブの[ログ収集]サブタブからのログ収集タスクを実行します。

管理者は、[ログ収集エクスペローラ]を使用して、エージェント上にコネクタを設定します。このコネクタは、ログ収集に必要となるものです。また、可能な場合には、エージェントにサブスクリプション更新を適用します。

イベント精製ライブラリの利用はオプションです。標準装備の機能は、定期的に更新され、多くのお客様のニーズを満たすように設計されています。

ログ収集に関する管理者タスクには、以下が含まれます。

- 収集専用の **CA Enterprise Log Manager** サーバから、インストール済みエージェントの設定と管理を実行
- **CA Enterprise Log Manager** レポートサーバ上のアーカイブ カタログにクエリを実行

アーカイブ カタログは、これまでに **CA Enterprise Log Manager** サーバ上に保存されたことがあるすべてのデータベースの記録です。アーカイブ カタログには、最近作成されたデータベース、バックアップされて移動されたデータベース、および、存在する場合はバックアップされる前に削除されたデータベースが含まれます。

- **CA Audit** が使用する **CA アダプタ** の設定
 - イベント精製ライブラリの管理
 - 事前定義済み統合の利用、および、ゼロからの、または事前定義済み統合のコピーを基にした、新規統合の作成

統合は、クエリおよびレポートに表示できるように、未分類のイベントを精製済みイベントに加工する手段です。

 - 事前定義済みリスナからの **syslog** リスナの作成
 - ゼロからの、または選択した事前定義済みファイルのコピーを基にした、新規解析ファイルの作成
- メッセージ解析ファイル (**XMP**) は、特定のイベントソースタイプに関連付けられており、元のイベントを名前/値ペアに分解する解析ルールを適用します。
- ゼロからの、または選択した事前定義済みファイルのコピーを基にした、新規マッピングファイルの作成

データ マッピング (DM) ファイルは XML ファイルです。CA 共通イベント文法 (CEG) を使用して、イベントをソース形式から、イベント ログ ストア内でのレポートや分析用として格納できる形式に変換します。

- ゼロからの、または選択した事前定義済みルールのコピーを基にした、集約ルールの作成

集約ルールは、一般的なタイプの特定のネイティブ イベントを 1 つの精製済みイベントに結合するルールです。

- ゼロからの、または選択した事前定義済みルールのコピーを基にした、抑制ルールの作成

抑制ルールは、精製済みの特定のイベントをレポートに表示されないようにします。

- イベント転送ルールの作成

イベント転送ルールによって、選択したイベントを、イベント ログ ストアへの保存後に、イベントの関連付けなどを行うサード パーティ製品に転送するよう指定します。

■ プロファイルの作成

プロファイルは、選択の際に表示されるデータフィルタおよびタグのセットを指定します。データフィルタでは、クエリまたはレポートに表示されるデータが制限されます。タグフィルタでは、クエリ タグ リストまたはレポート タグ リストに表示されるタグが制限されます。

詳細情報:

[エージェントグループを作成する方法](#) (P. 647)

[エージェント管理の設定方法](#) (P. 650)

[サブスクリプション更新を適用する方法](#) (P. 657)

サービス設定および監視

管理者ロールを割り当てられたユーザだけが、[管理]タブの[サービス]サブタブから利用できるサービスを設定し、管理することができます。CA Enterprise Log Manager のインストール直後のすべてのサービスの設定

サービスに関する管理者タスクには、以下が含まれます。

- 以下を含むグローバル サービスの設定
 - 更新間隔
 - セッション タイムアウト
 - RSS フィードにポストされたアラートを表示する際にユーザ認証を要求するかどうかの指定
 - 非表示にするタグ
 - デフォルト プロファイル
- イベント ログ ストア サービスの設定
 - グローバル レベルでの、すべての CA Enterprise Log Manager サーバに適用するサービスの設定
 - ローカル レベルでの、自動アーカイブの設定

収集 CA Enterprise Log Manager サーバ上のイベント ログ ストアには、新しいログのホット データベースが保存されます。設定された最大行数に達すると、このホット データベースは圧縮されてウォーム データベースになります。

- 自動アーカイブが収集サーバとレポートサーバ間に設定されていると、このウォーム データベースがレポートサーバにコピーされ、収集サーバから削除されます。
- 自動アーカイブがレポートサーバと CA Enterprise Log Manager サーバではないリモートサーバ間に設定されていると、自動アーカイブ設定に基づいてウォーム データベースがリモートサーバに毎日または一時間ごとにコピーされます。デフォルトでは、設定したディスク容量または時間制限に達するまで、レポートサーバはデータベースを保持します。ユーザが[リモート ELM サーバ]チェックボックスをオンにする場合のみ、データベースがレポートサーバから自動的に削除されます。

- レポートサーバからリモートストレージサーバに自動アーカイブが設定されていない場合、手動でウォーム データベースのバックアップを作成し、長期保存用ストレージにそのデータベースを移動させます。ウォーム データベースは、最大アーカイブ日数に設定された日数に達するまで、レポートサーバ(サーバが 2 台の環境では管理/レポートサーバ)のイベントログ ストアに保存されます。ただし、使用可能な領域がアーカイブ ディスク領域で設定された割合を下回った場合を除きます。この場合、ウォーム データベースは、最も古いものから削除されます。

■ レポートサーバ サービスの設定

レポートサーバ サービスは、保持ポリシー、レポートの印刷/電子メール送信用フォーマット、レポートおよびアラートのキー設定済み値など、レポートおよびアラートの処理を実行します。また、イベント/アラート出力と動的な値などの CA IT PAM プロセス用、およびアラートの SNMP トラップの宛先用の統合設定を処理します。

■ サブスクリプション更新の設定

サブスクリプション更新とは、CA サブスクリプション サーバによって提供される、CA Enterprise Log Manager サーバ、管理サーバ上の CA EEM コンポーネント、およびエージェント用のバイナリ ファイルおよび非バイナリ ファイルを指します。

■ CA Enterprise Log Manager サーバの連携の管理

管理サーバで、連携の子およびピアまで拡張するクエリを設定できます。CA Enterprise Log Manager サーバは、以下の 2 つの目的で連携できます。

- 収集サーバは、各ホット データベースを自動アーカイブしてウォーム データベースにし、関連するレポートサーバに送信します。収集サーバとレポートサーバ間の連携を作成します。連携が選択された管理サーバにクエリを実行したときに、ローカルのウォーム データベースからだけでなく、収集サーバのホット データベースからも結果を得ることができます。
- 複数のレポートサーバを作成すると、複数のイベントログ ストアにウォーム データベースを分散して配置することができます。レポートサーバでメッシュ状の連携関係を構築し、各レポートサーバの子として収集サーバを連携させることができます。メッシュ構成の任意のレポートサーバから連携クエリを実行すると、メッシュ接続された(ピア)サーバと、それらのすべての子サーバの両方からデータが返されます。

注: 長期保管用ストレージからアーカイブ済みデータベースを復元する目的で復元ポイント CA Enterprise Log Manager を作成する場合は、対象のサーバを連携から除外することをお勧めします。

- システム ステータスの監視と管理

詳細情報:

[バックアップおよび復元の自動化](#) (P. 189)

[アーカイブ カタログのクエリ](#) (P. 200)

[自動アーカイブ済みファイルの復元](#) (P. 202)

[アーカイブ済みデータベースを復元するための復元スクリプト](#) (P. 203)

[ODBC サーバの注意事項](#) (P. 164)

[サポート診断ファイルの作成](#) (P. 179)

[ホスト サーバの再起動](#) (P. 180)

[ELM サービスの再起動](#) (P. 180)

[サービスのステータスおよびバージョンの確認](#) (P. 181)

[システム ステータスの自己監視イベントの確認](#) (P. 181)

ユーザとアクセスの管理

管理者ルールを割り当てられたユーザだけが、[管理]タブの[ユーザとアクセスの管理]サブタブから利用できる、ユーザ アカウント、ポリシー、およびその他のアプリケーション オブジェクトを設定し、管理することができます。CA Enterprise Log Manager にログオンするには、ユーザに、ログインのためのルールおよび認証情報が設定されたユーザ アカウントが必要です。管理者は、事前定義済みルールおよびポリシーを使用し、ユーザ アカウントの定義によって、ユーザ アクセスを設定できます。カスタム ルールおよびポリシーの作成はオプションです。

ユーザおよびアクセスに関する管理者タスクには、以下が含まれます。

- 新しいグローバル ユーザ(ユーザ ストアがデフォルトの場合は、CA Enterprise Log Manager ユーザ ストア)の定義
 新規ユーザを追加する際、グローバル ユーザを作成します。名前、場所、電話番号などの詳細は共有できるため、グローバルであると考えられます。グローバル ユーザは、アプリケーション固有の詳細を除いたユーザ アカウント情報です。
- 参照されたユーザの読み出し(ユーザ ストアが参照されたユーザ ストアである場合)
 グローバル ユーザの詳細は、設定されたユーザ ストアに保存されます。設定されたユーザ ストアは外部ディレクトリである場合もあります。
- 新規ユーザまたは参照されたユーザに事前定義済みまたはカスタムのアプリケーション グループ(ルール)を割り当てます。
 アプリケーションの詳細は常に、管理サーバのリポジトリに保存されます。この詳細は、外部ユーザ ストアを設定する際に、読み取り専用形式でロードされます。
- ユーザ アカウントの編集、削除、および表示
- カスタム アプリケーション グループ(ルール)および関連するポリシーの作成
 ユーザ ロールの作成では、新しいアプリケーション ユーザ グループを定義してから、指定したリソースに対して許可されるアクションを定義するポリシーを作成します。ユーザ ロールには、事前定義済みのアプリケーション ユーザ グループか、ユーザ定義のアプリケーション グループを指定できます。事前定義済みアプリケーション グループ (Administrator、Analyst、および Auditor) では詳細な担当職務を十分カバーできない場合は、カスタム ユーザ ロールを作成する必要があります。カスタム ユーザ ロールを作成するには、カスタム アクセス ポリシーを設定し、事前定義済みポリシーを変更して、この新しいルールを追加する必要があります。

- カスタム アプリケーション グループおよび関連するポリシーの編集、削除、および表示
- CALM アプリケーション アクセス ポリシーの編集

CALM アプリケーション アクセス ポリシーは、CA Enterprise Log Manager へのアクセスが可能なユーザを定義する、アクセス制御リストタイプのスコープポリシーです。デフォルトでは、(グループの) Administrator、(グループの) Analyst、および(グループの) Auditor がアクセスを許可されています。
- アクセス ポリシーの作成、編集、削除、および表示

アクセス ポリシーは、アプリケーション リソースへの ID (ユーザまたはユーザグループ) のアクセス権を許可または拒否するルールです。
- アクセス フィルタの設定、編集、削除、および表示

アクセス フィルタは、管理者以外のユーザまたはグループが表示できるイベント データを制御するために、管理者が設定できるフィルタです。たとえば、アクセス フィルタを設定して、指定した ID がレポートに表示できるデータを制限できます。アクセス フィルタは自動的に責任ポリシーに変換されます。

詳細情報:

[グローバル グループの作成](#) (P. 40)

[グローバル ユーザの作成](#) (P. 41)

[グローバル ユーザへのロールの割り当て](#) (P. 43)

[すべてのアクセス ポリシーのバックアップ](#) (P. 65)

[アクセス ポリシーの復元](#) (P. 70)

[カスタム ユーザ ロールおよびアクセス ポリシーの設定](#) (P. 88)

[既存ポリシーへの ID の追加](#) (P. 95)

[CALM アクセス ポリシーの作成](#) (P. 96)

[動的ユーザ グループ ポリシーの作成](#) (P. 106)

[既存のポリシーをベースにしたポリシーの作成](#) (P. 103)

[スコープ ポリシーの作成](#) (P. 99)

[アクセス フィルタの作成](#) (P. 108)

[アプリケーション ユーザ グループ \(ロール\) の作成](#) (P. 92)

[カスタム ロールによる CA Enterprise Log Manager へのアクセスの許可](#) (P. 93)

[新しいポリシーのテスト](#) (P. 105)

[カレンダーの作成](#) (P. 110)

既定の設定でアカウントを作成する方法

一時的なテスト環境を設定している場合は、ユーザ アカウント用の既定の設定を使用し、必須フィールドのみを設定すれば、ユーザとアクセスの管理を迅速に設定できます。事前定義済み設定を使用して最小の設定を完了するには、以下のように **CA Enterprise Log Manager** ユーザ用のユーザ アカウントを作成します。

- デフォルトユーザ ストアを使用している場合は、ユーザ名でアカウントを作成し、事前定義済みアプリケーショングループ (Administrator、Analyst、Auditor) を割り当てて、一時パスワードを割り当てます。
- 外部ユーザ ストアを参照する場合は、名前でグローバル ユーザを検索し、事前定義済みロール (Administrator、Analyst、Auditor) を割り当てて、一時パスワードを割り当てます。

詳細情報:

[グローバル ユーザの作成](#) (P. 41)

[グローバル ユーザへのロールの割り当て](#) (P. 43)

[参照されたユーザ アカウントを管理する方法](#) (P. 44)

グローバル グループの作成

グローバル グループを作成できるかどうかは、ユーザ ストアの設定によって決まります。以下を考慮してください。

- デフォルトのユーザ ストアを使用する場合は、グローバル グループの作成は任意のタスクです。
- 外部ユーザ ストアを参照する場合は、グローバル グループおよびユーザ アカウントが自動的にデフォルトのユーザ ストアにロードされます。必要に応じて、これらのグローバル グループ用にカスタム ポリシーを作成できますが、新しいグローバル グループを作成することはできません。
- 参照されたユーザ ストアが **CA SiteMinder** である場合、この **CA** 製品で定義されているグローバル グループをそのまま使用することも、既存のグループ メンバシップからグローバル グループを新規作成することもできます。

グローバル グループの作成方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. 左側ペインの[グループ]をクリックします。
[グループの検索]ペインおよび[ユーザ グループ]ペインが表示されます。
3. [グローバル グループ]フォルダの横の[新規グローバル グループ]ボタンをクリックします。
[新規グローバル ユーザ グループ]ペインが表示されます。
4. 名前、および必要に応じて、その説明を入力します。
5. このグローバル グループにほかのグローバル グループを含める場合は、以下を実行します。
 - a. グループを表示するための検索条件を入力し、[検索]をクリックします。
 - b. 含めるグループを[選択済みグローバル ユーザ グループ]リストに移動させます。
 - c. 選択するグループがすべてリストに含まれるまで繰り返します。
6. [保存]をクリックします。
確認が表示されます。

詳細情報:

[ユーザ ロールの計画](#) (P. 87)

グローバル ユーザの作成

ユーザ ストアが **CA Enterprise Log Manager** ユーザ ストアとして設定されている場合 (デフォルト) のみ、新規ユーザを作成できます。新規ユーザ アカウントを作成できるのは、**Administrator** だけです。

外部ユーザ ストアを参照する場合は、ユーザ アカウントは自動的に読み取り専用レコードとしてデフォルトのユーザ ストアにロードされます。ユーザを新規作成する必要がある場合は、外部ユーザ ストア内で実行する必要があります。新しいレコードは、自動的にロードされます。

CA Enterprise Log Manager 製品を使用するには、ユーザがグローバル ユーザ アカウントを持っている必要があります。アカウントは、ログイン時にアクティブである必要があります。アカウントは、管理者によって一時停止された場合、パスワード ポリシー違反によりロックされた場合、または、有効なアカウント時間が経過したために無効になった場合に、非アクティブになることがあります。

新しいグローバル ユーザ アカウントを作成する方法

1. [管理] タブをクリックし、[ユーザとアクセスの管理] サブタブをクリックします。
2. [ユーザ] ボタンをクリックします。
3. 作成するアカウントがまだ存在していないことを確認します。[グローバル ユーザ] を選択し、[実行] をクリックします。名前が結果に表示されなければ、次へ進みます。
4. [ユーザ] ツリーの左にある [新規ユーザ] ボタンをクリックします。
[新規ユーザ] ページが表示されます。
5. [名前] エントリ フィールドにユーザ名を入力します。

6. (オプション)アプリケーション ユーザ グループを割り当てます。
 - a. [アプリケーション ユーザの詳細の追加]をクリックします。
 - b. 使用可能なユーザ グループを 1 つ以上選択し、[移動]ボタンをクリックして、[選択されたユーザ グループ]ボックスに選択したグループを移動させます。

注: ここで上記を実行しない場合は、後でグローバル ユーザのアカウントを編集して、アプリケーション ユーザ グループを割り当てることができます。
7. [グローバル ユーザの詳細]の[一般情報]を入力します。
8. (オプション)グローバル ユーザ グループを割り当てます。
9. [認証情報]をすべて入力します。
 - a. アカウントをロックするまでのログイン試行失敗回数のしきい値を設定するには、[不正なログイン カウント]に数値を入力します。カウントに 0 を設定すると、制限がないことになります。
 - b. ユーザにパスワード ポリシーに準拠しないパスワードを許可するのでない限り、[パスワード ポリシーを上書き]チェック ボックスをオフのままにします。
 - c. [パスワードの確認]ボックスに新しいパスワードをもう一度入力します。
 - d. ユーザによるパスワードの変更を許可するには、[次のログイン時にパスワードを変更]を選択します。
 - e. アカウントを新規作成する場合は、[一時停止]チェック ボックスをオフのままにします。
 - f. [新しいパスワード]および[パスワードの確認]にパスワードを入力します。
 - g. このユーザに一時的なアクセスのみを許可する場合は、ユーザ アカウントの有効化および無効化の日付範囲を入力します。
 - h. ユーザ アカウントの有効化を後日に延期する場合は、アカウントを有効にする日付を入力します。
10. [保存]をクリックします。
11. [閉じる]をクリックします。

グローバル ユーザへのロールの割り当て

既存ユーザ アカウントを検索し、対象のユーザが実行するロールのアプリケーション ユーザ グループを割り当てることができます。外部ユーザ ストアを参照する場合は、検索によってそのユーザ ストアからロードされたグローバル レコードが返されます。設定したユーザ ストアが CA Enterprise Log Manager ユーザ ストアである場合は、検索によって CA Enterprise Log Manager 内のユーザ用に作成されたレコードが返されます。

ユーザ アカウントを編集できるのは、Administrator だけです。

ロール(アプリケーション ユーザ グループ)を既存ユーザに割り当てる方法

1. [管理] タブをクリックし、[ユーザとアクセスの管理] サブタブをクリックします。

2. 左側ペインの[ユーザ]をクリックします。

[ユーザの検索] ペインおよび[ユーザ] ペインが表示されます。

3. [グローバル ユーザ] を選択し、検索条件を入力して、[実行] をクリックします。

ロードされたユーザ アカウントの検索の場合、[ユーザ] ペインにはパスが表示され、パス ラベルには参照された外部ディレクトリが反映されます。

重要: 外部ユーザ ストア内にあるすべてのエントリが表示されるのを避けるには、検索のたびに条件を入力してください。

4. CA Enterprise Log Manager アプリケーション グループのメンバシップを持っていないグローバル ユーザを選択します。

[ユーザ] ペインに、フォルダ名およびグローバル ユーザの詳細と、該当する場合はグローバル グループ メンバシップが表示されます。

5. [アプリケーション ユーザの詳細の追加] をクリックします。

「CAELM」ユーザの詳細ペインが展開されます。

6. [使用可能なユーザ グループ] から目的のグループを選択し、右方向矢印をクリックします。

選択したグループが、[選択されたユーザ グループ] ボックスに表示されます。

7. [保存] をクリックします。

8. 追加を確認します。
 - a. [ユーザの検索]ペインで、[アプリケーション ユーザの詳細]をクリックし、[実行]をクリックします。
 - b. 表示された結果に、新規アプリケーション ユーザの名前が表示されていることを確認します。
9. [閉じる]をクリックします。

参照されたユーザ アカウントを管理する方法

外部ユーザ ストアを参照する場合は、グローバル ユーザ アカウント情報を使用できます。CA Enterprise Log Manager から外部ユーザ ストア内のユーザレコードを更新することはできませんが、アプリケーションレベルで詳細情報を割り当てることができます。

次に、外部ユーザ ストアに保存されたアカウントを使用するユーザについて、アクセス権を管理する方法の例を示します。

- ユーザ アカウントに事前定義済みアプリケーション ユーザ グループ、すなわちロールを追加します。
- ユーザに付与するアクセス権を提供する事前定義済みポリシーにグローバル グループを追加します。
- カスタム ロールおよび関連付けられたポリシーを作成し、ユーザ アカウントにこのカスタム ロールを追加します。

ユーザの有効化のガイドライン

アカウントの有効化機能を使用する場合は、以下のガイドラインに留意してください。

- すぐに多数のユーザ アカウントを作成する場合、[再開日]を使用して、すべてのアカウントまたは選択したアカウントを有効にする将来の日付を指定します。これにより、アクセス権を段階的に拡張して新規ユーザに提供するトレーニングとの調整を図ることができます。
- 外部監査担当者用の一時アカウントを作成する場合、[再開日]および[停止日]設定を使用して、特定の間隔を指定できます。
- あるユーザの不審な動作を発見した場合、すぐに該当するアカウントを一時停止に設定することで、ユーザがいずれの **CA Enterprise Log Manager** サーバにもログインできないようにすることができます。
- ユーザが会社を辞める場合、ユーザ レコード全体を削除して一時停止に設定するか、無効ステータスにする有効期限を入力します。

詳細情報:

[グローバル ユーザの作成](#) (P. 41)

[ユーザ アカウントの編集](#) (P. 46)

[ユーザ アカウントの削除](#) (P. 50)

ユーザ アカウントの編集

ユーザ アカウントを作成および編集できるのは、**Administrator** だけです。以下のいずれかの場合に、ユーザを検索して、選択したユーザ アカウント情報を表示できます。

- CA Enterprise Log Manager ロール、すなわちアプリケーション グループ メンバシップをグローバル ユーザに割り当てる場合。アカウント情報は、参照されたユーザ ストアからロードされています。
- ローカル ユーザ ストア内にあるアカウントのグローバル ユーザの詳細を更新する場合
- ユーザ アカウントを一時停止する場合
- パスワードを忘れて、またはアカウントがロックされて、パスワード ポリシーによってユーザ アカウントのアンロックが許可されないために、ユーザ アカウントのパスワードをリセットする場合
- ユーザ アカウントを無効にする、または有効なアカウントの期間をリセットする場合

重要： [認証] 領域の [不正なログイン カウント] には何も入力しないでください。このフィールドに表示される値は、システムによって更新されます。

ユーザ アカウントの編集方法

1. [管理] タブをクリックし、[ユーザとアクセスの管理] サブタブをクリックします。
2. 左側ペインの [ユーザ] をクリックします。
[ユーザの検索] ペインが表示されます。

3. 以下の方法のいずれかを使用し、[ユーザの検索]ペインで検索条件を指定します。
 - グローバル ユーザのアプリケーションの詳細を追加するには、[グローバル ユーザ]を選択し、検索条件を入力して、[実行]をクリックします。
 - 既存の CA Enterprise Log Manager ロールを持つユーザのアカウントを編集するには、[アプリケーション ユーザの詳細]を選択し、検索条件を入力して、[実行]をクリックします。

注: 検索条件では、値としてワイルドカードを指定する場合は、演算子「LIKE」を使用し、完全な文字列を指定する場合は、演算子「EQUAL」を使用します。以下に例を示します。

- グループ メンバシップ LIKE Aud*
- グループ メンバシップ EQUALS Auditor

検索条件に一致するユーザの名前が、[ユーザ]ペインに表示されます。

4. 編集するアカウントのユーザ名をクリックします。
右側ペインに、選択したアカウントが表示されます。
5. ロールを追加するには、[アプリケーション ユーザの詳細]を選択し、[使用可能なユーザ グループ]から適切なロールを選択して、[選択されたユーザ グループ]に移動させます。
6. グローバル ユーザの詳細を更新するには、既存の詳細を、[グローバル ユーザの詳細]セクション内の新しい詳細で置き換えます。

注: 詳細の更新は、デフォルトのユーザ ストアを使用している場合にのみ可能です。

7. 認証設定を更新するには、以下のうち必要な作業を実行します。
 - すべてのパスワード ポリシーによって実行される確認からこのユーザを除外するには、[パスワード ポリシーを上書き]チェック ボックスをオンにします。
 - このユーザをどの **CA Enterprise Log Manager** サーバにもログインできないようにするには、[一時停止]チェック ボックスをオンにします。
 - ユーザがログインできるように、このアカウントをアクティブにするには、[一時停止]チェック ボックスをオフにします。
 - パスワード ポリシーによってパスワードのアンロックを許可しないように設定されており、このユーザのパスワードがロックされた場合は、[パスワードのリセット]を選択し、新しいパスワードを 2 回入力して、[次のログイン時にパスワードを変更]を選択します。

注: [不正なログイン カウント]フィールドには、ログインの試行が失敗するたびに自動的に 1 が加算され、ログインの試行に成功すると 0 にリセットされます。ログイン試行が指定した回数失敗したらユーザ アカウントをロックするよう設定されたパスワード ポリシーの値に、加算された値が達するか超えた場合に、ユーザ アカウントがロックされます。

 - [再開日]をクリックして開始日を設定し、[停止日]をクリックして終了日を設定することで、このアカウントを有効にする期間を設定します。ユーザは、開始日の 1 日の始まりから終了日の 1 日の終わりまで、アクセス権が与えられます。1 日限りのアクセスを許可するには、開始日と終了日を同じ日に指定します。
8. [保存]をクリックします。

ユーザ アカウントへの更新が保存され、有効になります。

ユーザ パスワードのリセット

パスワードを忘れたユーザのためにパスワードをリセットできます。設定された回数を超えてユーザがログインを試み、パスワードを忘れたためにログインに失敗してロックアウトされた場合は、該当するパスワード ポリシーで許可されていれば、パスワードをリセットして、そのユーザのアカウントをアンロックできます。

ユーザ パスワードのリセット方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. [ユーザ]ボタンをクリックします。
3. 編集するユーザ アカウントを検索します。
 - a. [アプリケーション ユーザの詳細]を選択します。
 - b. [値]フィールドにユーザ名を入力します。[値]フィールドは、[属性]が「ユーザ名」に、[演算子]が「LIKE」に設定されています。
 - c. [実行]をクリックします。
4. [ユーザ]ツリーのユーザ名をクリックします。
選択されたユーザ アカウントの詳細が表示されます。
5. [認証]ペインで[パスワードのリセット]を選択します。
[新しいパスワード]フィールドおよび[パスワードの確認]フィールドが表示されます。
6. [新しいパスワード]および[パスワードの確認]の各フィールドにパスワードを入力します。
7. [保存]をクリックし、[閉じる]をクリックします。

ユーザ アカウントの削除

CA Enterprise Log Manager で作成されたあらゆるグローバル ユーザ アカウントを削除できます。

以下の方法のどちらかを使用すれば、削除せずにユーザ アカウントを非アクティブにできます。

- 停止日を設定して、指定された日付の時点でアカウントを無効にできます。
- アカウントを一時停止して、関連付けられたユーザが CA Enterprise Log Manager インターフェースにアクセスできないようにすることができます。

グローバル ユーザの削除方法

1. [管理]タブ -[ユーザとアクセスの管理]サブタブ -[ユーザ]ボタンをクリックします。

[ユーザの検索]ペインおよび[ユーザ]ペインが表示されます。

2. [グローバル ユーザ]または[アプリケーション ユーザの詳細]を選択し、検索条件を入力して、[実行]をクリックします。

3. 既存ユーザのリストから、削除するユーザを選択します。

選択したユーザのレコードが右側ペインに表示されます。

4. [削除]をクリックします。

このユーザの削除の確認が表示されます。

5. [OK]をクリックします。

グローバル ユーザが正常に削除されたことを示す確認メッセージが表示されます。

注: [ユーザの検索]ペインで再度[実行]をクリックすると、表示されているリストに、削除されたユーザが含まれなくなります。

第 3 章: ポリシー

カスタム ロールを作成するには、事前定義済みポリシーの編集およびカスタム ポリシーの作成が必要です。これらのタスクを開始する前に、各事前定義済み ロールに関連付けられた事前定義済みポリシーを確認しておく役立ちます。編集を行う前には、事前定義済みアクセス ポリシーをバックアップしておくことをお勧めします。

このセクションには、以下のトピックが含まれています。

[ポリシーの概要](#) (P. 52)

[事前定義されたアクセス ポリシー](#) (P. 52)

[すべてのアクセス ポリシーのバックアップ](#) (P. 65)

[アクセス ポリシーの復元](#) (P. 70)

ポリシーの概要

アクセス ポリシーは、アプリケーション リソースまたはグローバル リソースへの ID (ユーザまたはユーザ グループ) のアクセス権を許可または拒否するルールです。CA Enterprise Log Manager は、ID、リソース、リソース クラスを照合し、フィルタを評価して、特定のユーザにポリシーを適用するかどうかを決定します。言い換えると、ポリシーには、特定のリソースの特定の ID に対して許可または拒否されるアクションが記載されています。特定のリソースへのアクセスを拒否するポリシーは、同じリソースへのアクセスを許可するポリシーよりも優先されます。

CA Enterprise Log Manager では、以下のタイプのアクセス ポリシーをサポートします。

- CALM アクセス ポリシー
- 委任ポリシー
- 動的なユーザ グループ ポリシー (カスタム アプリケーション グループ への代替アプローチ)
- 責任ポリシー (アクセス フィルタを作成する際に自動的に作成)
- スcope ポリシー

CA Enterprise Log Manager には、3 つの CA Enterprise Log Manager アプリケーション ユーザ グループ (Administrator、Analyst、および Auditor) 用に、事前定義済みの CALM アクセス ポリシーおよびスコープ ポリシーが標準で用意されています。さまざまなロールを実行するユーザに対して、既定のアプリケーション ユーザ グループのみを適用するのであれば、これらのポリシーで十分です。

重要： CA Enterprise Log Manager で提供される事前定義済みポリシーのバックアップを取ることをお勧めします。意図せず CALM アクセス ポリシーが削除されてしまうと、そのポリシーがバックアップから復元されるまで、ユーザは CA Enterprise Log Manager にアクセスできなくなります。

事前定義されたアクセス ポリシー

標準装備の機能を使用する場合は、事前定義されたアプリケーション グループ (Administrator、Analyst、または Auditor) を各ユーザ用のロールとして割り当てることができ、アクセス ポリシーを作成する必要はありません。必要なポリシーはすべて事前に定義されており、そのまま使用できます。

詳細情報:

[全ユーザのポリシーの確認 \(P. 53\)](#)[Auditor 用のポリシーの確認 \(P. 57\)](#)[Analyst 用のポリシーの確認 \(P. 59\)](#)[Administrator のポリシーの確認 \(P. 62\)](#)[リソースとアクション \(P. 80\)](#)

全ユーザのポリシーの確認

すべてのユーザのポリシーを確認できます。**CALM** アプリケーション アクセス ポリシーを編集して、カスタム ロールを定義します。すべてのカスタム ロールをこのポリシーに ID として追加する必要があります。

全ユーザのポリシーの確認方法

1. [管理] タブをクリックし、[ユーザとアクセスの管理] サブタブをクリックします。
2. 左側のペインで、[アクセス ポリシー] をクリックします。
3. 以下のようにして **CALM** アプリケーション アクセス ポリシーを表示します。
 - a. [名前に一致するポリシーを表示] を選択します。
 - b. 「CALM*」と入力します。
 - c. [実行] をクリックします。
4. **CALM** アプリケーション アクセス ポリシーを調べます。

このポリシーは、デフォルトのアプリケーション ユーザ グループ (Administrator、Analyst、および Auditor) のすべてのメンバ、および CA Enterprise Log Manager API を使用するその他のユーザに、リスト表示されたリソースの読み取りおよび書き込みアクセスを許可します。

アクセス ポリシー				
名前/説明	ResourceClassName	オプション	ID	アクション リソース
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	明示的な許可	ug:Administrator ug:Analyst ug:Auditor CALM_API_UT	read write ApplicationInstance AppObject Policy User GlobalUser

リスト表示されたリソースは以下のとおりです。

- ApplicationInstance リソースは、CA Enterprise Log Manager 製品を指す CAELM です。
- Policy は、アクセス ポリシーを指します。
- User は、CA Enterprise Log Manager アプリケーション ユーザ グループに追加された任意のユーザです。
- GlobalUser は、CA Enterprise Log Manager 内のユーザ ストアに定義されたか、CA Enterprise Log Manager から参照される任意のユーザです。
- Profiles フォルダに対する pozFolder 値を持つ AppObject は、プロファイルを指します。
- フレックスフォルダに対する pozFolder 値を持つ AppObject は、クエリに基づいたウィザードの[結果の条件]の手順で、時間範囲のドロップダウンリストへの入力に使用する、動的時間帯 XML を指します。

CALM アプリケーション アクセス フィルタは、各リソースに対するアクションの制限を指定します。

フィルタ			
WHERE	(req:resource	== val:ApplicationInstance	
AND	req:action	{}	val:read)
OR	(req:resource	== val:Policy	
AND	req:action	{}	val:read)
OR	(req:resource	== val:User	
AND	req:action	{}	val:read,write
AND	name:cn	== req:identity	)
OR	(req:resource	== val:GlobalUser	
AND	req:action	{}	val:read
AND	name:cn	== req:identity	)
OR	(req:resource	== val:AppObject	
AND	req:action	== val:read	
AND	name:pozFolder	*--* val:/CALM_Configuration/Content/Profiles	)
OR	(req:action	== val:read	
AND	req:resource	== val:AppObject	
AND	name:pozFolder	*--* val:/CALM_Configuration/flex	)

5. 以下のようにして全ユーザのポリシーを検索します。
 - a. 左側のペインで、[アクセス ポリシー]をクリックします。
 - b. [ID に一致するポリシーを表示]を選択します。ほかの選択を解除します。
 - c. [ID の追加]フィールドに[すべての ID]と入力します。
 - d. [追加]をクリックします。
 - e. [実行]をクリックします。

CEG ポリシーとデフォルト データ アクセス ポリシーを含む 4 つのポリシーが表示されます。(明示的に[すべての ID]と入力しなかった場合は、ほかにも多くポリシーが表示されます。)

6. デフォルト データ アクセス ポリシーを調べます。

CALM リソースクラスに対する事前定義されたデフォルト データ アクセス ポリシーは、アクセスフィルタで指定された範囲の CA Enterprise Log Manager データへのアクセスをすべてのユーザに許可します。アクセスフィルタは、dataaccess/CALM/Data に対する FulfillOnGrant アクションを含む責任ポリシーに変換されます。

アクセス ポリシー					
<< < 1 / 1 > >>					
名前/説明	ResourceClassName	オプション	ID	アクション	リソース
Default Data Access Policy All users have access to all the data, the obligation is that access is restricted by the AccessScope	CALM	明示的な許可	[すべての ID]	dataaccess Data	

7. スコープ ポリシーの CEG ポリシーを調べます。

事前定義された CEG ポリシーは、CALM アプリケーションにアクセスできるすべてのユーザに対して、共通イベント文法フィールドの表示を許可します。この結果、すべてのユーザが自分で実行するクエリ用のグローバルフィルタとローカル フィルタを設定できるようになるため、すべてのユーザの単純フィルタと詳細フィルタ用のドロップダウンリストに CEG フィールドが表示されるようになります。クエリを作成して編集する権限を持つユーザは、自分が作成して編集するクエリ用のフィルタを設定できます。また、このポリシーによって、すべてのユーザが[グローバル設定]の設定内容を表示できるようになります。

アクセス ポリシー					
<< < 1 / 1 > >>					
名前/説明	ResourceClassName	オプション	ID	アクション	リソース
CEG Policy All users of the CAELM have read only access on the CEG Fields. All users have read only access to the CAELM Global Configuration	SafeObject	明示的な許可	[すべての ID]	read	AppObject
フィルタ					
WHERE (name:pozFolder == val:/CALM_Configuration/Content/CEG) OR (name:pozFolder *-- val:/CALM_Configuration)					

Auditor 用のポリシーの確認

Auditor 用の各事前定義ポリシーを調べると、以下のタスクを実行するのに必要なリソースに対し、アプリケーションのアクセスがどのように制限されるかを確認できます。

- レポートのスケジュールと注釈
- レポートの表示

Auditor 用の事前定義ポリシーの確認方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. 左側のペインで、[アクセス ポリシー]をクリックします。
3. 以下のようにして **Auditor** 用のポリシーを検索します。
 - a. [ID に一致するポリシーを表示]を選択します。
 - b. [ID の追加]フィールドに「ug:Auditor」と入力します。
 - c. [追加]をクリックします。
 - d. [実行]をクリックします。

[すべての ID] と ug:Auditor 用のポリシーがすべて表示されます。

4. 監査担当者用スケジュール/注釈権限ポリシーを調べます。

すべての **CALM** アクセスポリシーは、アプリケーション固有のリソースに対して実行できるアクションを定義します。このポリシーは、アプリケーション ユーザ グループに割り当てられたユーザに対して **Auditor** ロールを付与し、レポートのスケジュールと注釈の追加を許可します。

アクセス ポリシー - "CALM"				
名前/説明	ResourceClassName	オプション	ID	アクション
Auditor Schedule- Annotate Rights. Auditors can schedule and Annotate reports	CALM	明示的な許可	ug:Auditor	schedule annotate
				Report

このポリシーを、分析担当者用作成/スケジュール/注釈ポリシー、および管理者用作成ポリシーと比較します。

5. 分析担当者および監査担当者用レポート サーバ アクセス ポリシーを調べます。

このスコープ ポリシーにより、監査者は、レポート サーバにレポート先を設定したり、イベント ログ ストアへのアクセス権が必要な連携レポートを作成したりすることができるようになります。このポリシーが適用されるリソースは、アプリケーション オブジェクトがレポート サーバとイベント ログ ストアである AppObject です。

アクセス ポリシー					
名前/説明	ResourceClassName	オプション	ID	アクション	リソース
Analyst Auditor Report Server Access Policy Analyst ,Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	明示的な許可	ug:Analyst ug:Auditor ug:Administrator CALM_API_UT	read	AppObject

フィルタ

WHERE (指定された属性: pozFolder *--* 値: CALM_Configuration/Modules/calmReporter)
OR (指定された属性: pozFolder *--* 値: CALM_Configuration/Modules/logDepot)

注: 特定の CALM アクセス ポリシー (つまり、CALM リソース クラス用のポリシー) には通常、SafeObject リソース クラス用の関連するスコープ ポリシーがあります。

6. 監査担当者用レポート表示ポリシーを調べます。

このスコープ ポリシーは、レポートへの読み取りアクセスをユーザに許可します。このポリシーが適用されるリソースは、AppObject です。

スコープ ポリシー					
名前/説明	ResourceClassName	オプション	ID	アクション	リソース
Auditor View Report Policy Auditor can view all the Reports	SafeObject	明示的な許可	ug:Auditor	read	AppObject

AppObject は、レポートの表示権限を付与するフィルタによって、特定のアプリケーション リソースに絞り込まれています。パスは、すべてのレポートのコンテンツを格納する EEM フォルダ パスです。

フィルタ
WHERE (name:pozFolder *--* val:/CALM_Configuration/Content/Reports)

Analyst 用のポリシーの確認

Analyst 用の各事前定義ポリシーを調べると、以下のタスクを実行するのに必要なリソースに対し、アプリケーションのアクセスがどのように制限されるかを確認できます。

- レポートのスケジュールと注釈 (Auditor のタスク)
- レポートの表示 (Auditor のタスク)
- レポートとタグの作成
- アラート(クエリ)の作成とスケジュール
- レポート、アラート、およびタグの編集

Analyst 用の事前定義ポリシーの確認方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. 左側のペインで、[アクセス ポリシー]をクリックします。
3. 以下のようにして Analyst 用のポリシーを検索します。
 - a. [ポリシーと一致する名前を表示します]チェック ボックスをオフにします。
 - b. [ID に一致するポリシーを表示]を選択します。
 - c. [ID の追加]フィールドに「ug:Analyst」と入力します。
 - d. [追加]をクリックします。
 - e. [実行]をクリックします。
4. ug:Analyst 用のすべてのポリシーが表示されます。ug:Analyst ユーザグループを含む [すべての ID] のポリシーが表示されます。

5. 分析担当者用作成/スケジュール/注釈ポリシーを調べます。

この CALM アクセスポリシーは、アプリケーション固有のリソースに対して実行できるアクションを定義します。このポリシーは、CA Enterprise Log Manager のアプリケーション ユーザ グループに割り当てられたユーザに Analyst ロールを付与し、レポートの作成、スケジュール、および注釈の追加のほか、アクション アラートの作成とスケジュール、タグの作成を許可します (Auditor はレポートのスケジュールと注釈の追加のみが可能です)。

アクセス ポリシー - "CALM"						
名前/説明	ResourceClassName	オプション	ID	アクション	リソース	フィルタ
Default Data Access Policy All users have access to all the data, the obligation is that access is restricted by the AccessScope	CALM	明示的な許可	[すべての ID]	dataaccess	Data	
Auditor Schedule-Annotate Rights Auditors can schedule and Annotate reports	CALM	明示的な許可	ug:Auditor	schedule annotate	Report	
Admin Agent Manager Policy Access Rights for Administrator for Agent Management	CALM	明示的な許可	ug:Administrator	edit	AgentConfiguration AgentAuthenticationKey Connector ALL_GROUPS Integration	
Administrator Create policy Administrator can create any object	CALM	明示的な許可	ug:Administrator	create schedule annotate edit	Report Alert Profile Tag Integration EventGrouping EventForwarding Database	
Analyst Create-Schedule-Annotate policy Analyst can create/schedule Reports, schedule Action Alerts,Annotate Reports	CALM	明示的な許可	ug:Analyst	create schedule annotate	Report Alert Tag	

6. 分析担当者および監査担当者用レポート サーバアクセス ポリシーを調べます。

このスコープ ポリシーは、任意のレポートサーバのスケジュール権限をアナリストに与えます。このポリシーが適用されるリソースは、AppObject です。

アクセス ポリシー						
名前/説明	ResourceClassName	オプション	ID	アクション	リソース	
Analyst Auditor Report Server Access Policy Analyst ,Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	明示的な許可	ug:Analyst ug:Auditor ug:Administrator CALM_API_UT	read	AppObject	

フィルタにより、AppObject は特定のリソースに絞り込まれています。

フィルタ	
WHERE	(name:pozFolder *--* val:CALM_Configuration/Modules/calmReporter)
OR	(name:pozFolder *--* val:CALM_Configuration/Modules/logDepot)

- 末尾が **calmReporter** のフィルタは、すべてのレポート サーバに対する読み取りアクセスを許可します。レポートをスケジュールする場合は、作成されたレポートを表示する宛先レポート サーバを指定します。
- 末尾が **logDepot** のフィルタは、すべてのイベント ログ ストアに対するアクセスを許可します。レポートが連携するように定義されている場合、アクセス可能なすべてのイベント ログ ストアのデータに対して、クエリが実行されます。アクセス可能かどうかは、階層統合で、レポートが開始されるサーバの階層内の位置に依存します。

7. 分析担当者用レポート表示/編集ポリシーを調べます。

このスコープ ポリシーは、**Analyst** ロールを割り当てられたユーザに対して、レポートの表示、編集、または削除を許可します。このポリシーが適用されるリソースは、**AppObject** です。

スコープ ポリシー					
名前/説明	ResourceClassName	オプション	ID	アクション	リソース
Analyst Report View-Edit Policy Analyst can View/Edit any Report	SafeObject	明示的な許可	ug:Analyst	read write	AppObject

AppObject は、以下のフィルタによってレポートを対象とするよう絞り込まれています。このフィルタは、**EEM** フォルダの **CALM_Configuration/Content/Reports** に保存された作成済みレポートを表示する権限を付与します。

フィルタ
WHERE (name:pozFolder *--* val:/CALM_Configuration/Content/Reports)

注: このポリシーによって許可されたレポート編集機能は、**CEG** の列を使ってレポートへのフィルタを追加する権限を付与する **CEG** ポリシーによって拡張されます。

Administrator のポリシーの確認

CA Enterprise Log Manager アプリケーションとそのすべての機能に対するフルアクセス権を付与するユーザには、**Administrator** ロールを割り当てます。

Administrator 用の各事前定義ポリシーを調べると、以下のタスクを実行するユーザにどのようなアクセス権が付与されるかを確認できます。

- **EventGrouping** の作成 (つまり、共通イベント文法を使った抑制ルールと集約ルールの作成)。
- 統合の作成 (つまり、共通イベント文法を使ったデータ マッピング ファイル およびメッセージ解析ファイルの作成)。
- **EventForwarding** の作成 (つまり、イベントをサード パーティ システムに転送するためのルールの作成)。
- データベースの実行 (つまり、バックアップされて外部アーカイブ ソリューションに移動済みのデータベースの名前を照会する[カタログ クエリのアーカイブ]の実行)。
- ポリシーの表示または編集。
- ユーザ定義カレンダーの表示または編集。
- 任意のアプリケーション オブジェクトの表示または編集。アプリケーション オブジェクトとは、レポートテンプレート、クエリテンプレート、スケジュールされたレポートジョブ、アラートジョブ、プロファイル、サービス設定、データマッピング (DM) ファイル、メッセージ解析 (XMP) ファイル、抑制および集約ルール、およびイベント転送ルールのことです。
- **AppObject** の **iPoz** 属性を使ったフィルタの作成。
- [管理] - [ユーザとアクセスの管理] - [EEM フォルダ]でのフォルダの表示、およびそれらのフォルダに含まれるユーザ定義データの編集
- 任意のアプリケーション ユーザ、アプリケーション ユーザ グループ、またはグローバル ユーザに関する詳細の表示または編集。
- 任意のアナリストまたは監査者のタスク。

Administrator 用の事前定義ポリシーの確認方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. 左側のペインで、[アクセス ポリシー]をクリックします。

3. 以下のようにして Administrator 用のポリシーを検索します。

- [ID に一致するポリシーを表示]を選択します。
- [ID の追加]フィールドに「ug:Administrator」と入力します。
- [追加]をクリックします。
- [実行]をクリックします。

[すべての ID] と ug:Administrator 用のポリシーがすべて表示されます。

4. CALM アクセスポリシーである管理者用作成ポリシーを調べます。

このポリシーは、アプリケーション固有のリソースに対して実行できるアクションを定義します。このポリシーは、アプリケーション ユーザ グループに割り当てられたユーザに Administrator ロールを付与し、指定されたリソースに適用される指定されたアクションの実行を許可します。

アクセス ポリシー					
名前/説明	ResourceClassName	オプション	ID	アクション	リソース
Administrator Create policy Administrator can create any object	CALM	明示的な許可	ug:Administrator	create schedule annotate edit	Report Alert Profile Tag Integration EventGrouping EventForwarding Database

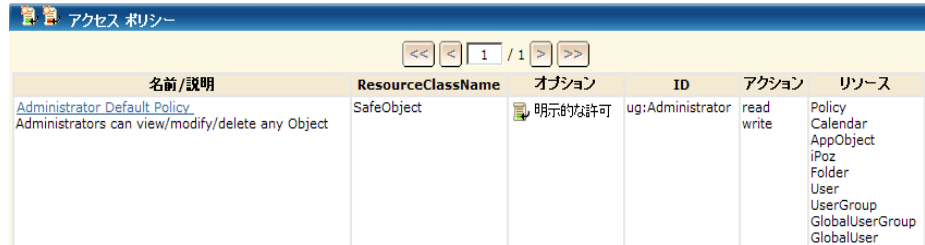
5. CALM アクセスポリシーの管理エージェント マネージャ ポリシーを調べます。

このポリシーは、管理者に対して、エージェントグループの作成、すべてのエージェントグループの編集、コネクタの設定、および統合の作成の権限を与えます。このポリシーでは、管理者は、エージェントが収集されたイベントを転送する宛先 CA Enterprise Log Manager サーバのアプリケーション インスタンス用のエージェント認証キーを編集できます。設定されたエージェント認証キーは、デフォルトでは複数のアプリケーション インスタンスにわたってすべての CA Enterprise Log Manager サーバに適用されますが、特定のアプリケーション インスタンスの専用キーとして設定することもできます。

アクセス ポリシー					
<< < 1 > >> / 1					
名前/説明	ResourceClassName	オプション	ID	アクション	リソース
Admin Agent Manager Policy Access Rights for Administrator for Agent Management	CALM	明示的な許可	ug:Administrator	edit	AgentConfiguration AgentAuthenticationKey Connector ALL_GROUPS Integration

6. スコープ ポリシーの管理者用デフォルト ポリシーを調べます。

このポリシーは、リソース一覧の表示、編集、または削除権限を Administrator に付与します。リスト表示されるリソースには、CA Enterprise Log Manager 固有ではないリソースと AppObject があります。AppObject とは、アプリケーション固有のオブジェクト、つまり、CALM 管理者用作成ポリシー、および CALM 管理エージェント マネージャ ポリシーでリスト表示されるリソースです。



名前/説明	ResourceClassName	オプション	ID	アクション	リソース
Administrator Default Policy Administrators can view/modify/delete any Object	SafeObject	明示的な許可	ug:Administrator	read write	Policy Calendar AppObject iPoz Folder User UserGroup GlobalUserGroup GlobalUser

登録済み製品用のアクセス ポリシー

製品が CA Enterprise Log Manager に登録される際、新しい証明書が生成され、すべてのタグ、クエリ、およびレポートへの読み取り専用アクセスを許可するための特定のアクセスポリシーが更新されます。特に、登録済み製品を認証する際に使用される証明書名は、以下のポリシーに ID 証明書名として追加されます。

- CALM アプリケーション アクセス
- 分析担当者および監査担当者用レポート サーバ アクセス ポリシー
- 分析担当者用レポート表示/編集ポリシー

ポリシーに証明書名が追加されると、CA 製品、サードパーティ製品、または CA カスタマのユーザが、タグ別のクエリおよびレポートのリストを取得することができます。これらのユーザは、独自のユーザ インターフェース内にリストを表示し、必要な精製済みイベント データを取得することができます。

すべてのアクセス ポリシーのバックアップ

事前定義済みアクセス ポリシーのエクスポートは、アクセス ポリシーが意図せず削除されるか破損した場合に備えてバックアップを保存しておく際に推奨される方法です。

重要：ポリシーの破損は、システムまたは CA EEM サービスの再起動中に発生することがあるため、後で復元できるように現在のバックアップを保存しておくことが重要です。また、新しい CA Enterprise Log Manager のインストール後やカスタム ポリシーの作成後などに、CA EEM を定期的にバックアップしてください。

各種アクセス ポリシーのポリシーをすべてエクスポートできます。ポリシーをエクスポートすると、XML ファイルが選択したタイプのポリシーごとに作成されます。XML ファイルは圧縮され、CAELM[1].xml ドキュメントが含まれた CAELM[1].xml.gz という名前の zip ファイルになります。エクスポートされた ZIP ファイルを任意のディレクトリに保存します。

保存されたバックアップ ファイルを復元するには、内部ユーザ ストアのある CA Enterprise Log Manager のディレクトリ /opt/CA/LogManager/EEM に保存されたバックアップ ファイルをコピーする必要があります。ローカル ディレクトリへの保存後にコピーすることも、復元が必要になってからコピーすることも可能です。

ポリシーがエクスポートされる際のフォーマットは、エクスポートされているオブジェクトの数によって変わります。

- エクスポートされるオブジェクト数が多数の場合は、*filename.tar.gz* が使用されます。
- エクスポートされるオブジェクト数が少数から中程度の場合は、*filename.xml.gz* が使用されます。

エクスポートを行う際に、*filename* (CAELM [n])を意味のある名前に変更することをお勧めします。たとえば、CAELM_CalmAccessPolicies、CAELM_EventPolicies、および CAELM_ScopingPolicies の、事前定義済みポリシーが保存されている 3 つのポリシー フォルダからファイルをエクスポートします。

注：拡張子 (xml.gz または tar.gz) は変更しないでください。

アクセス ポリシー定義が含まれている XML ファイルを ZIP ファイルから抽出し、アクセス ポリシーの復元で使用する SAFEX ユーティリティへの入力として使用できます。

すべてのアクセス ポリシーをバックアップする方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. 以下の要領で、事前定義済み CALM アクセス ポリシーをバックアップします。
 - a. [アクセス ポリシー]ボタンをクリックします。
 - b. [CALM]をクリックします。
ポリシー テーブルの、[アクセス ポリシー (CALM)]が表示されます。
 - c. [エクスポート]ボタンをクリックします。
 - d. 開くか保存するかを尋ねる[ファイルのダウンロード]ダイアログ ボックスが表示されます。
 - e. (オプション) [開く]をクリックし、ZIP ファイル CAELM[1].xml.gz を開きます。CAELM[1].xml をダブルクリックし、XML フォーマットのファイルを確認します。
 - f. [保存]をクリックしてファイルを保存します。
[名前を付けて保存]ダイアログ ボックスが表示されます。
 - g. 保存するターゲットフォルダを選択し、必要に応じてファイル名を変更して、[保存]をクリックします。
ファイル名を変更しない場合は、ZIP ファイルは CAELM[1].xml.gz という名前で保存されます。
 - h. [閉じる]をクリックします。
ダウンロードの完了を知らせるダイアログ ボックスが閉じます。ポリシー リストは左側ペインに表示されたままです。

3. 以下の要領で、事前定義済みイベント ポリシーをバックアップします。
 - a. [イベント ポリシー]をクリックします。
ポリシー テーブルの[イベント ポリシー]が表示されます。
 - b. [エクスポート]ボタンをクリックします。
 - c. 開くか保存するかを尋ねる[ファイルのダウンロード]ダイアログ ボックスが表示されます。
 - d. [保存]をクリックしてファイルを保存します。
既存の **CAELM[1].xml.gz** ファイルを置き換えるかどうかを尋ねるメッセージが表示されます。
 - e. [いいえ]をクリックします。
 - f. ファイル名フィールドに一意の名前を入力し、[保存]をクリックします。
たとえば、エントリを編集して **CAELM[2].xml.gz** とするか、**CAELM_EventPolicies** のようなポリシー タイプの名前を入力します。
 - g. [閉じる]をクリックします。
ダウンロードの完了を知らせるダイアログ ボックスが閉じます。ポリシー リストは左側ペインに表示されたままです。

4. 以下の要領で、事前定義済みスコープ ポリシーをバックアップします。
 - a. [スコープ ポリシー]をクリックします。
[スコープ ポリシー]ポリシー テーブルが表示されます。
 - b. [エクスポート]ボタンをクリックします。必要に応じて、水平にスクロールして、右上のボタンを表示します。
 - c. 開くか保存するかを尋ねる[ファイルのダウンロード]ダイアログ ボックスが表示されます。
 - d. [保存]をクリックしてファイルを保存します。
既存の **CAELM[1].xml.gz** ファイルを置き換えるかどうかを尋ねるメッセージが表示されます。
 - e. [いいえ]をクリックします。
 - f. ファイル名フィールドに一意の名前を入力し、[保存]をクリックします。
たとえば、エントリを編集して **CAELM[3].xml.gz** とするか、**CAELM_ScopingPolicies** のようなポリシー タイプの名前を入力します。
 - g. [閉じる]をクリックします。
ダウンロードの完了を知らせるダイアログ ボックスが閉じます。ポリシー リストは左側ペインに表示されたままです。
5. [閉じる]をクリックします。
アクセス ポリシーのリストが閉じます。

例 -- CALM アクセス ポリシーの CAELM[1].xml

以下は、CAELM[1].xml ファイル内の、あるポリシーのエントリです。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <Safex>
  <Attach label="CAELM" />
  <Add />
- <AddOrModify>
  - <Policy folder="/" name="Auditor Schedule-Annotate Rights">
    <Description>Auditors can schedule and Annotate reports</Description>
    <ResourceClassName>CALM</ResourceClassName>
    <PolicyType>policy</PolicyType>
    <Disabled>False</Disabled>
    <ExplicitDeny>False</ExplicitDeny>
    <PreDeployment>False</PreDeployment>
    <RegexCompare>False</RegexCompare>
    <Resource>Report</Resource>
    <Action>schedule</Action>
    <Action>annotate</Action>
    <Identity>ug:Auditor</Identity>
    <Attribute name="CreateTimestamp">20080926053329</Attribute>
  </Policy>
```

アクセス ポリシーの復元

アクセス ポリシーの削除や変更によって問題が発生した場合は、アクセス ポリシーを復元できます。誤ってアクセス ポリシーを削除した場合や、アクセス ポリシーが破損した場合、そのポリシーで ID を使って参照されていたユーザは、そのポリシーを再定義または復元するまで CA Enterprise Log Manager にアクセスできません。

アクセス ポリシーを復元するには、ポリシー用の SAFEX スクリプトを実行する必要があります。

エクスポートによって作成されたファイルの拡張子が `xml.gz` と `tar.gz` のどちらであるかによって、以下の 2 つの手順のいずれかを使用します。

ファイル名.xml.gz という名前のバックアップからアクセス ポリシーを復元する方法

1. 保存されたバックアップ ファイルを管理 CA Enterprise Log Manager (通常は最初にインストールされたサーバ) の以下のディレクトリにコピーします。

```
/opt/CA/LogManager/EEM
```

2. 以下のコマンドを実行して XML ファイルを取得します。

```
gunzip ファイル名.xml.gz
```

これによってファイル名.xml が作成されます。

3. (オプション) バックアップしたグループ内のポリシーのうち 1 つだけを復元する場合は、以下の手順を実行します。

- a. XML ファイルを開きます。
- b. 復元しないポリシーについて、以下のタグで囲まれている XML 行を削除します。

```
<Policy folder="/ name=ポリシー名> および </Policy>
```

- c. ファイルを保存します。

4. 以下のコマンドを実行します。**EEM** サーバのホスト名は、管理 CA Enterprise Log Manager のホスト名を指します。

```
./safex -h eemserverhostname -u EiamAdmin -p パスワード -f ファイル名.xml
```

CA Enterprise Log Manager サーバが FIPS モードの場合は、**-fips** オプションを指定してください。

復元されるファイル名.xml に定義されたポリシー (複数可) は、適切なポリシー タイプに追加され、有効になります。

ファイル名.tar.gz という名前のバックアップからアクセス ポリシーを復元する方法

1. 保存されたバックアップ ファイルを管理 CA Enterprise Log Manager (通常は最初にインストールされたサーバ) の以下のディレクトリにコピーします。

```
/opt/CA/LogManager/EEM
```

2. 以下のコマンドを実行して XML ファイルを取得します。

```
gunzip ファイル名.tar.gz
```

これによってファイル名.tar が作成されます。

3. 以下のコマンドを実行します。

```
tar -xvf ファイル名.tar
```

これによってファイル名.xml が作成されます。

4. (オプション) バックアップしたグループ内のポリシーのうち 1 つだけを復元する場合は、以下の手順を実行します。

- a. XML ファイルを開きます。
- b. 復元しないポリシーについて、以下のタグで囲まれている XML 行を削除します。
<Policy folder="/" name=ポリシー名> および </Policy>
- c. ファイルを保存します。

5. 以下のコマンドを実行します。*EEM* サーバのホスト名は、管理 CA Enterprise Log Manager のホスト名を指します。

```
./safex -h eemserverhostname -u EiamAdmin -p パスワード -f ファイル名.xml
```

バックアップがない場合に CALM アクセス ポリシーを再作成する方法

バックアップがない場合は、CALM アプリケーション アクセス ポリシーを再作成できます。

1. CALM アプリケーション アクセス ポリシーを再作成します。「事前定義ポリシー」を参照してください。
2. 以下の図に示されたとおりに、フィルタを定義します。パスの一部は、以下のとおりです。
 - /CALM_Configuration/Content/Profiles
 - /CALM_Configuration/flex

ロジック	(	左のタイプ/値	演算子	右のタイプ/値	)
NONE	(	request	STRING	value	
		resource	EQUAL ==	ApplicationInstance	
AND	(	request	STRING	value	)
		action	WITHINSET {}	read	
OR	(	request	STRING	value	)
		resource	EQUAL ==	Policy	
AND	(	request	STRING	value	)
		action	WITHINSET {}	read	
OR	(	request	STRING	value	)
		resource	EQUAL ==	User	
AND	(	request	STRING	value	)
		action	WITHINSET {}	read,write	
AND	(	named attribute	STRING	request	)
		cn	EQUAL ==	identity	
OR	(	request	STRING	value	)
		resource	EQUAL ==	GlobalUser	
AND	(	request	STRING	value	)
		action	WITHINSET {}	read	
AND	(	named attribute	STRING	request	)
		cn	EQUAL ==	identity	
OR	(	request	STRING	value	)
		resource	EQUAL ==	AppObject	
AND	(	request	STRING	value	)
		action	EQUAL ==	read	
AND	(	named attribute	STRING	value	)
		pozFolder	CONTAINS *.*	ration/Content/Profiles	
OR	(	request	STRING	value	)
		action	EQUAL ==	read	
AND	(	request	STRING	value	)
		resource	EQUAL ==	AppObject	
AND	(	named attribute	STRING	value	)
		pozFolder	CONTAINS *.*	CALM_Configuration/flex	

このポリシーがあれば、任意の管理者がログインしてほかのポリシーを作成できます。

第 4 章: カスタム ロールおよびカスタム ポリシー

このセクションには、以下のトピックが含まれています。

[ポリシー作成時のガイドライン](#) (P. 73)

[ユーザ ロールの計画](#) (P. 87)

[カスタム ユーザ ロールおよびアクセス ポリシーの設定](#) (P. 88)

[ユーザ アカウントとアクセス ポリシーの保守](#) (P. 110)

[例: 管理者以外のユーザへのアーカイブ管理の許可](#) (P. 116)

[ユーザ: Win-Admin のデータ アクセスを制限するシナリオ](#) (P. 120)

[ロールのアクセス制限: PCI-Analyst シナリオ](#) (P. 134)

[カスタム統合のポリシーの例](#) (P. 141)

[抑制ルールおよび集約ルール用のポリシーの例](#) (P. 143)

ポリシー作成時のガイドライン

すべての CALM アクセス ポリシーおよびスコープ ポリシーは、特定の ID に対して許可または拒否する特定のリソースに対するアクションを指定します。CALM リソース クラス用のポリシーは、指定した ID に対して、アプリケーション リソース (CALM リソースとも呼ばれます) に対するアクションの実行を許可または拒否します。SafeObject クラスの AppObject リソース用のポリシーは、指定した ID に対して、アプリケーションレベルのリソースに対する書き込みおよび読み取りのアクションをフィルタの指示に従って許可または拒否します。SafeObject リソース クラス用のその他のポリシーは、指定した ID に、グローバル リソースへの書き込みおよび読み取りアクションを許可または拒否します。

作成するポリシーのタイプは、アクセスを制限するリソースによって異なります。リソースごとのポリシー要件の概要は以下のとおりです。

- AppObject 用の CALM ポリシーおよびスコープ ポリシーが必要なリソース
 - EventForwarding
 - EventGrouping
 - Integration (エージェント以外)
 - Profile
 - Report

- CALM ポリシーのみが必要なリソース
 - AgentAuthenticationKey
 - AgentConfiguration
 - Alert
 - ALL_GROUPS
 - Connector
 - Database
 - Integration (エージェント関連)
 - Tag
- グローバル リソース用のスコープ ポリシーのみが必要なリソース
 - Calendar
 - Folder
 - GlobalUser
 - GlobalUserGroup
 - iPoz
 - Policy
 - User
 - UserGroup

以下のガイドラインでは、ポリシーの作成方法の違いを説明します。これらの違いは、制御するリソースに基づいています。

EventForwarding、EventGrouping、Integration、Profile、および Report へのアクセスを制御する方法

以下のアプローチは、CALM リソース、EventGrouping、Integration、Profile、および Report に関するポリシーにのみ適用します。これらのアプリケーション リソースには、CALM ポリシーと 2 つのスコープ ポリシーが必要です。

1. Report や Integration などの 1 つ以上のアプリケーションリソース用の CALM ポリシーを作成します。指定したリソースに対して有効な 1 つ以上のアプリケーション固有のアクション(作成、スケジュール、注釈など)を指定します。指定したアクションを許可または拒否する ID を追加します。
2. 読み取りアクションと書き込みアクションの両方を使って AppObject リソースに対する関連スコープ ポリシーを作成します。ID がリソースを編集または削除できる(ただし、作成はできない)ようにするには、書き込みアクションを指定します。ID がリソースを表示できるようにするには、読み取りアクションを指定します。AppObject リソースと関連するアプリケーションリソースを再度関連付けるフィルタを作成します。このフィルタに、指定したリソースのコンテンツを格納する EEM フォルダ パスカ、または関連するアプリケーションリソースのためにアクセスできる必要があるモジュールを示す EEM フォルダ パスを指定します。関連する CALM ポリシーに追加した同じ ID をこのポリシーにも追加します。
3. 読み取りアクションを使って AppObject リソースに関する 2 つ目の関連スコープ ポリシーを作成します。ID がリソースを表示できるようにするには、読み取りアクションを指定します。AppObject リソースと関連するアプリケーションリソースを再度関連付けるフィルタを作成します。このフィルタに、指定したリソースのコンテンツを格納する EEM フォルダ パスカ、または関連するアプリケーションリソースのためにアクセスできる必要があるモジュールを示す EEM フォルダ パスを指定します。このポリシーに、より低い権限を持つユーザまたはユーザ グループを ID として追加します。

Alert、Database、Tag、およびエージェント関連リソースへのアクセスを制御する方法

以下の方法は、アクセスを許可または制限する CALM ポリシーのみを必要とするアプリケーションリソースに適用されます。

- **Connector** または **Tag** などのリソース用の **CALM** アクセス ポリシーを作成します。対象の ID でリソースの作成、編集、削除、およびその他の有効なアクションを実行できるように、編集アクションを指定します。このアクションを許可または拒否する ID を追加します。

注: エージェント関連リソースへのアクセスを許可すると、[管理]タブの[ログ収集]サブタブに表示されるエージェント エクスプローラ フォルダまたはそのサブフォルダのボタンを使用できるようになります。**Alert** リソースへのアクセスを許可すると、その ID は[アラート]タブにアクセスできるようになります。**Tag** リソースへのアクセスを許可すると、その ID はカスタム クエリまたはレポートのタグを作成できるようになります。**Database** へのアクセスを許可すると、その ID はアーカイブ クエリを実行できるようになります。

CAELM アプリケーションで使用されるグローバル リソースへのアクセスを制御する方法

以下の方法は、アクセスを制限するスコープ ポリシーのみを必要とするグローバルリソースに適用されます。

1. **User** や **Policy** などの 1 つ以上のグローバルリソース用のスコープ ポリシーを作成します。対象の ID でリソースを作成、編集、または削除できるようにするには、書き込みアクションを指定します。このアクションを許可または拒否する ID を追加します。
2. **User** や **Policy** などの 1 つ以上のグローバルリソース用のスコープ ポリシーを作成します。対象の ID でグローバルリソースを表示できるようにするには、読み取りアクションを指定します。このアクションを許可または拒否する ID を追加します。

注: グローバルリソースは、[管理]タブの[ユーザとアクセスの管理]サブタブ上のボタンを使ってアクセスできるリソースです。

詳細情報:

[CALM アクセス ポリシーのタイプ](#) (P. 77)

[リソースとアクション](#) (P. 80)

[CALM リソースと EEM フォルダ](#) (P. 83)

[グローバルリソースと CA EEM の機能](#) (P. 86)

[CALM アクセス ポリシーの作成](#) (P. 96)

CALM アクセス ポリシーのタイプ

CALM 用のアクセス ポリシーまたはスコープ ポリシーを作成するときは、以下の 3 つのタイプから 1 つを選択します。

- アクセス ポリシー
- アクセス制御リスト
- ID アクセス制御リスト

この選択は、アクセス ポリシー設定の詳細のレベルに影響します。そこでは、アクセス ポリシーが最も広範囲になっています。

注: ここに示す例は CALM リソース クラス用のアクセス ポリシーであるため、CA Enterprise Log Manager に固有のアクションおよびリソースが含まれます。

アクセス ポリシーでは、選択したすべての ID に許可する、選択したすべてのリソースに対して有効なアクションを指定します。CA Enterprise Log Manager 用の汎用ポリシーを作成する場合は、CALM リソース クラスに属するリソースを追加し、表示されたリストからアクションを選択します。選択したアクションが、そのアクションが有効である選択済みリソースに適用されます。この例では、ポリシーによって、選択した各アクションが、作成が有効であるすべての選択済みリソース上で実行できるようになります。

アクセス ポリシーの設定	
リソース	アクション
リソースの追加: + Alert Data Database EventGrouping Integration Profile Report Tag AgentConfiguration AgentAuthenticationKey	create schedule annotate dataaccess edit [すべてのアクション] ☒ ☒ ☒ ☒ ☒ ☐

アクセス制御リストでは、選択した ID ごとに、各リソースに対して有効なアクションを個別に指定します。リソース中心のポリシーを作成するときは、各リソースに対してどのアクションが許可されるかを指定します。有効であるという理由だけで、特定のリソース用のアクションを選択する必要はありません。たとえば、レポートの作成を許可することはできますが、アラートの作成は、有効なアクションであるとしても、許可することはできません。アクセス制御リストは、一度に 1 つの ID に実装する場合には最もきめ細かなポリシーです。

アクセス制御リストの設定						
リソース		アクション				フィルタ
リソースの追加: 		create	schedule	annotate	dataaccess	edit
☐	Alert		☒	☒	☐	☐
☐	Data		☐	☐	☒	☐
☐	Database		☐	☐	☐	☒
☐	EventGrouping		☒	☐	☐	☐
☐	Integration		☒	☐	☐	☒
☐	Profile		☒	☐	☐	☐
☐	Report		☒	☒	☒	☐
☐	Tag		☒	☐	☐	☐
☐	AgentConfiguration		☐	☐	☐	☒
☐	AgentAuthenticationKey		☐	☐	☐	☒
☐	ALL_GROUPS		☐	☐	☐	☒
☐	Connector		☐	☐	☐	☒

ID 制御リストでは、選択した ID に許可する、適用可能なすべての選択済みリソースへのアクションを指定します。ID 中心のポリシーを作成する際に、各アクションが適用される、リスト表示されたすべてのリソースに対して、どの ID がどのアクション(作成、スケジュール、注釈、編集)を実行できるかを指定します。**Auditor** がアラートをスケジュールできないように制限する場合は、スケジュールを空白にしておきます。ただし、スケジュールを空白にすると、**Auditor** によるレポートのスケジュールも制限されます。

ID アクセス制御リストの設定

ID の入力/検索

タイプ: ユーザ ID の検索

ID:

選択された ID

ID		create	schedule	annotate	dataaccess	edit
[デフォルト]		☐	☐	☐	☐	☐
Administrator		☒	☒	☒	☒	☒
Analyst		☐	☒	☒	☒	☐
Auditor		☐	☐	☒	☒	☐

リソース

Alert
Data
Database
EventGrouping
Integration
Profile
Report
Tag
AgentConfiguration
AgentAuthenticationKey

リソースとアクション

ポリシーを作成する際に、アクセス フィルタを必要とするアクセス ポリシーを設定します。アクセス フィルタは、管理者以外のユーザまたはグループが表示できるイベント データを制御するために、管理者が設定できるフィルタです。たとえば、アクセス フィルタでは、指定したユーザまたはグループに対して、レポートで表示されるデータを制限できます。アクセス フィルタは、EEM 責任ポリシーに自動的に変換されます。アクセス フィルタは、多くの場合、ユーザ アクセスを制限するオブジェクトへの相対パスを使って表されます。インターフェースの[EEM フォルダ]領域に、これらの相対パスが表示されます。

通常、作成やスケジュールなどのアクションを許可するポリシーは、CALM リソース クラスと、レポート、タグ、DM ファイルおよび MP ファイル、抑制ルールおよび集約ルールなどの CALM リソースを使って定義されます。読み取りおよび書き込みアクションを許可するポリシーは、SafeObject リソース クラスと AppObject リソースを使って定義されます。編集アクションは、CALM リソース クラス内のエージェント関連リソースに対して有効な唯一のアクションです。

CALM リソース クラスに属するオブジェクトに関して許可されるアクションは、具体的には以下のとおりです。

アクション	Resource	説明
注釈	Report	レポートに関するコメントを記録します。
Create	EventForwarding	特定のサードパーティ アプリケーションに特定のイベント転送ルールを作成します。
Create	EventGrouping	共通イベント文法を使って抑制ルールと集約ルールを作成します。
Create	Integration	共通イベント文法を使ってデータ マッピング ファイルとメッセージ解析ファイルを作成します。
Create	Profile	プロファイルの作成
Create	Report	レポートおよびクエリを作成します。
Create	Tag	レポートおよびクエリ用のタグを作成します。
データ アクセス	Data	CALM イベント データにアクセスします。データ アクセス フィルタによって制限できます。

アクション	Resource	説明
Edit	AgentConfiguration	エージェントグループを作成します。収集用のソースと処理用の転送先を使って、インストール済みのエージェントを設定します。
Edit	AgentAuthenticationKey	エージェントのインストール時に指定されたエージェント認証キーを作成および編集します。
Edit	ALL_GROUPS	使用可能なすべてのエージェントグループを編集します。 注: リソースとしてエージェントグループ名を指定することにより、特定のエージェントグループにアクセスを限定できます。
Edit	Connector	コネクタを設定します。
Edit	Database	アーカイブ カタログのクエリ条件と一致する既存のログを特定し、データベースのカatalogを再作成します。
Edit	Integration	統合の詳細を編集します。
Schedule	Alert	アクション アラートをスケジュールします。
Schedule	Report	レポートおよびクエリをスケジュールします。

ユーザが **SafeObject** リソース クラスに属するオブジェクトを表示または編集できるようにするアクションは、以下のとおりです。

アクション	Resource	説明
読み取り	AppObject	レポート テンプレート、クエリ テンプレート、タグ、スケジュールされたレポートジョブ、アラートジョブ、サービスの設定、データマッピング (DM) ファイル、メッセージ解析 (XMP) ファイル、抑制ルールと集約ルール、およびイベント転送ルールを表示します。
読み取り	Calendar	[管理]の[ユーザとアクセスの管理]の[カレンダー]にカレンダーを表示します。
読み取り	Folder	[管理]の[ユーザとアクセスの管理]の[EEM フォルダ]にフォルダを表示します。
読み取り	GlobalUser	[管理]の[ユーザとアクセスの管理]の[ユーザ]で[グローバル ユーザ]に関するクエリを実行したときに一覧表示されるユーザに関する情報を表示します。

アクション	Resource	説明
読み取り	iPoz	[管理]の[ユーザとアクセスの管理]の[ユーザストア]にユーザストアの設定を表示します。 [管理]の[ユーザとアクセスの管理]の[パスワードポリシー]にパスワードポリシーの設定を表示します。
読み取り	Policy	[管理]の[ユーザとアクセスの管理]の[アクセスポリシー]にポリシーを一覧表示します。
読み取り	User	[管理]の[ユーザとアクセスの管理]の[ユーザ]で[アプリケーション ユーザの詳細]に関するクエリを実行したときにユーザの詳細を表示します。
読み取り	UserGroup	[管理]の[ユーザとアクセスの管理]の[ユーザ]で[アプリケーション ユーザの詳細]に関するクエリを実行したときに一覧表示されるユーザのアプリケーション グループ メンバシップを表示します。
書き込み	AppObject	レポートテンプレート、クエリテンプレート、タグ、スケジュールされたレポートジョブ、アラートジョブ、サービスの設定、データマッピング (DM) ファイル、メッセージ解析 (XMP) ファイル、抑制ルールと集約ルール、およびイベント転送ルールを編集および削除します。
書き込み	Calendar	ユーザ定義カレンダーを編集します。
書き込み	Folder	[EEM フォルダ]の構造に追加されたユーザ定義データを編集します。
書き込み	GlobalUser	グローバル ユーザの詳細を編集します。
書き込み	iPoz	ユーザストアおよびパスワードのポリシーを設定します。
書き込み	Policy	ユーザ定義および事前定義のポリシーを編集します。
書き込み	User	アプリケーション ユーザの詳細を編集します。
書き込み	UserGroup	アプリケーション ユーザグループを作成、編集、または削除します。

CALM リソースと EEM フォルダ

EventForwarding、EventGrouping、統合、プロファイル、またはレポートを含む、ゼロから作成するすべてのカスタム CALM ポリシーに対して、AppObject に関するスコープ ポリシーを作成します。スコープ ポリシーには、対応する CALM ポリシー内で挙げられている各 CALM リソースの EEM パスをフィルタリングする読み取り/書き込みアクセスが含まれています。CALM ポリシー用の ID である同じユーザグループが、このポリシーにも ID として割り当てられます。ポリシー セットを完成するには、読み取り専用スコープ ポリシーを作成し、リソースの表示のみが許可された ID を割り当て、EEM フォルダ パスに関するフィルタを入力します。

注: CALM ポリシーにそれをサポートするスコープ ポリシーが必要かどうかは、CALM ポリシーが使用するリソースによって決まります。たとえば、Database、Tag、および Alert リソースは CALM の専用リソースであり、これらのリソースにスコープ ポリシーは必要ありません。エージェント関連リソースにもスコープ ポリシーは必要ありません。

EEM フォルダは、[管理]タブの[ユーザとアクセスの管理]サブタブに表示されます。[抑制]などのフォルダを選択すると、そのパスが表示されます。以下の例を参照してください。

EEM フォルダ

▼ CALM_Configuration

▶ Modules

▼ Content

Library

▼ Rules

Suppression

Forwarding

Summarization

▶ Reports

CEG

Mapping

Parsing

▶ Profiles

flex

▼ AgentManager

AgentGroupPozObjects

Templates

EncryptionKeys

Status

Integrations

IndexFiles

Agents

System

Calendars

Policies

Users

UserGroups

フォルダの詳細

名前	パス
Suppression	/CALM_Configuration/Content/Rules/Suppression

ポリシー定義の[フィルタ]セクションに示されるように、「pozFolder CONTAINS」で始まる式の値として EEM フォルダ パスを指定します。以下に例を示します。

フィルタ

ロジック	(	左のタイプ/値	演算子	右のタイプ/値	)
なし	(	指定された属性 pozFolder	STRING CONTAINS *--*	値 CALM_Configuration/M	)
OR	(	指定された属性 pozFolder	STRING CONTAINS *--*	値 CALM_Configuration/M	)

以下の表に、特定の CALM リソースへのアクセスを許可(または拒否)する CALM ポリシーに関連するスコープ ポリシーのフィルタに指定する値のガイドラインを示します。

注: CALM リソースとフォルダは一対一で対応しません。

作成するスコープ ポリシーによってコンテンツへのアクセスが許可される CALM リソース	追加するフィルタによって指定される EEM フォルダ パス
EventForwarding	pozFolder CONTAINS /CALM_Configuration/Content/Rules/Forwarding
EventGrouping	pozFolder CONTAINS/CALM_Configuration/Content/Rules/Summarization pozFolder CONTAINS/CALM_Configuration/Content/Rules/Suppression
Integration (サーバ)	pozFolder CONTAINS/CALM_Configuration/Content/Mapping pozFolder CONTAINS/CALM_Configuration/Content/Parsing
Profile	pozFolder CONTAINS /CALM_Configuration/Content/Profiles
Report	pozFolder CONTAINS/CALM_Configuration/Content/CEG pozFolder CONTAINS/CALM_Configuration/Content/Reports
作成するスコープ ポリシーによってアクセスが要求される CALM モジュール	追加するフィルタによって指定される EEM フォルダ パス
エージェント マネージャ	pozFolder CONTAINS /CALM_Configuration/Modules/AgentManager
[イベント ログ ストア]	pozFolder CONTAINS/CALM_Configuration/Modules/logDepot
レポート サーバ	pozFolder CONTAINS/CALM_Configuration/Modules/calmReporter

作成するスコープ ポリシーによってアクセスが要求される CALM モジュール	追加するフィルタによって指定される EEM フォルダ パス
サブスクリプション モジュール	pozFolder CONTAINS/CALM_Configuration/Modules/Subscription

グローバル リソースと CA EEM の機能

スコープ ポリシーは、CALM ポリシーと同じような目的で作成できますが、製品固有のリソースではなく、グローバル リソースを対象とする点が異なります。グローバル リソースは、複数の CA 製品で共有されるリソースです。特定のグローバル リソースへのアクセスを許可または拒否するポリシーを作成できます。グローバル リソースにアクセスするには、[管理]タブの[ユーザとアクセスの管理]サブタブ上のボタンを使用します。

以下の表は、指定したリソースがグローバル リソースである場合に、指定した ID に対して読み取りおよび書き込みを許可または拒否するスコープ ポリシーを作成するときのガイドとして使用してください。

タスク	アクション	グローバル リソース
グローバル ユーザ、グローバル ユーザ グループ、アプリケーション ユーザ グループ (ロール) の表示、作成、編集、削除、およびグローバル ユーザへのアプリケーション グループ (ロール) の追加、またはあるロールを持つグローバル ユーザの作成	読み取り/書き込み	User UserGroup GlobalUser GlobalUserGroup
ポリシーの作成、編集、コピー、エクスポート、無効化、テスト、表示、削除、およびポリシーへのカレンダーの追加	読み取り/書き込み	Policy Calendar
アクセスフィルタの作成、編集、コピー、表示、削除、および EEM フォルダの表示	読み取り/書き込み	Policy
カレンダーの作成	読み取り/書き込み	Calendar
ユーザ ストアの設定、およびパスワード ポリシーの作成、編集、表示	読み取り/書き込み	iPoz

グローバル リソース用のフィルタを作成するときは、例として **CALM** アプリケーション アクセス ポリシー用のフィルタを参照してください。フィルタが持つ機能の 1 つは、どのアクションがどのリソースに対して実行されるかを指定することです。事前定義されたポリシーに対する[編集]をクリックすると、ロジックの入力方法を示す例としてソースを調べることができます。

ユーザ ロールの計画

事前定義済みアプリケーション ユーザ グループ (Administrator、Analyst、および Auditor) が各環境のニーズに合わない場合は、新しいアプリケーション ユーザ グループを備えたカスタム ロールを作成できます。たとえば、ユーザ アカウントを管理するユーザの小規模なグループを作成し、**CA Enterprise Log Manager** の関連のない機能にはアクセスできないようにするには、**UserAccountAdministrator** というロールを定義し、そのロールのスコープ ポリシーを作成してから、ロールを **CALM** アプリケーション アクセス ポリシーに追加して、ユーザ アカウントの管理を担当するユーザにそのロールを割り当てます。

CA Enterprise Log Manager のユーザ計画は、以下の手順で構成されます。

- **CA Enterprise Log Manager** の管理、分析、および監査を実行するために必要なユーザ数の決定
- **CA Enterprise Log Manager** へのアクセス権を与えるユーザの特定

関連するアクセス ポリシーを持つカスタム ロールを作成する場合は、以下の方法に考慮してください。

- 各 **CA Enterprise Log Manager** ユーザを割り当てるロールの特定
- 各ロールに必要な **CA Enterprise Log Manager** リソースへのアクセス タイプの特定

また、ユーザ定義ロール(アプリケーション グループ)の代わりに、次の方法を使用することも検討してください。

- 動的ユーザ グループを作成する動的ユーザ グループ ポリシーの設定。
- グローバル グループの作成、およびアプリケーション グループとしての処理。すなわち、グローバル グループのユーザへの割り当て、および ID としてのポリシーへの割り当て。

物理的な所在地でアクセスを制限するためにポリシーを作成し、同一ユーザに複数の CA 製品に関する同じレベルの権限を付与する場合に、この方法が役立つことがあります。たとえば、ロケーション A で複数の CA 製品の管理を担当するユーザに、Location-A_Admin のグローバル グループを割り当てます。各 CA 製品のポリシーを作成し、その製品がインストールされたロケーション A のサーバに対して管理者権限を与えるよう設定できます。

詳細情報:

[グローバル グループの作成](#) (P. 40)

カスタム ユーザ ロールおよびアクセス ポリシーの設定

ユーザ ロールには、事前定義済みのアプリケーション ユーザ グループか、ユーザ定義のアプリケーション グループを指定できます。事前定義済みアプリケーション グループ (Administrator、Analyst、および Auditor) では詳細な担当職務を十分カバーできない場合は、カスタム ユーザ ロールを作成する必要があります。カスタム ユーザ ロールを作成するには、カスタム アクセス ポリシーを設定し、事前定義済みポリシーを変更して、この新しいロールを追加する必要があります。

管理者は、以下の要領でユーザ ロールおよび対応するポリシーを作成できます。

1. CA Enterprise Log Manager のユーザが担当する各ロールに対して
 - アクセスを許可する必要があるリソースを特定します。
 - 各リソース上で許可するアクションを特定します。
 - このロールが適用される ID、すなわち個人を特定します。

注: ID は、スーパー グループを構成するよう設計されたほかのアプリケーション グループである場合もあります。

2. 事前定義済みアプリケーション グループの権限範囲が広すぎる場合には、アプリケーション グループを新規作成して、特定した個人にこのアプリケーション グループを割り当てます。割り当てられたユーザが実行するロールを説明するような言葉を用いて、ユーザ定義アプリケーション グループの名前を付けることをお勧めします。
3. 新規アプリケーション グループを、アクセス制御リスト方式の **CALM** アプリケーション アクセス ポリシーに追加します。
4. 新規ロールが 1 つ以上のリソースに対して、作成などのアクションを実行できる必要がある場合は、以下の手順を実行します。
 - a. 指定された **CA Enterprise Log Manager** リソースに対し、新規アプリケーション グループが作成などの有効なアクションを実行することを許可する **CALM** ポリシーを設定します。
 - b. **AppObject** リソースへの読み取り/書き込みアクセスを新規アプリケーション グループに許可するスコープ ポリシーを設定し、指定されたリソースが **EEM** フォルダに保存されていることを説明するフィルタを入力します。各フィルタには、名前付き属性 **pozFolder**、**CONTAINS**、および値を入力します。この値は、**/CALM_Configuration** で始まる **EEM** フォルダ パスです。
5. 新規ロールが特定の **CA Enterprise Log Manager** リソースのみを表示する必要がある場合は、**AppObject** への読み取りアクセスを許可するスコープ ポリシーを設定し、「名前付き属性 **pozFolder CONTAINS 値**」というフィルタを入力します。この値は、リソースが保存されている、**/CALM_Configuration** で始まる **EEM** フォルダ パスです。
6. ポリシーをテストします。
7. ユーザ アカウントに新規ロールを割り当てます。

管理者は、アクセスフィルタを使用して、ユーザ アクセスの制限を作成することもできます。特定の種類のアクセス制限を 1 人の個人のみに適用する場合は、そのユーザへのアプリケーション グループ、すなわちロールの割り当てを省略できます。1 人のユーザのアクセスを制限するには、以下の手順に従います。

1. ユーザを作成します。ロールは割り当てません。
2. ユーザを **CALM アクセス ポリシー** に追加して、ユーザに **CA Enterprise Log Manager** アプリケーションへのアクセス権を与えます。
3. **SafeObject** への読み取りまたは書き込みアクセスを許可するスコープ ポリシーを作成し、名前付き属性 **pozFolder** がリソースの **EEM フォルダ** の値と等しいというフィルタを入力します。たとえば、リソースがレポートである場合、名前付き属性 **calmTag** がレポート タグの値と等しくなるように設定します。
4. カスタム アクセスフィルタを作成します。

管理者は、**CA Enterprise Log Manager** リソースへのユーザ アクセスをカスタマイズできます。以下の例について考えます。

- 異なる管理者グループに、特定の管理責任を割り当てるロールを作成します。たとえば、**UserAccountAdministrator** のようなロールを作成します。このロールを持つユーザに、ユーザとグループの管理に必要な機能へのアクセスのみを許可するポリシーを作成します。そのようなポリシーには、**User** および **UserGroup** リソースに加えて、**GlobalUser** リソースへの読み取りおよび書き込みアクセス権を定義する必要があります。
- タグに基づいて、分析担当者の責任をさまざまなタイプのレポートおよびクエリに分配するロールを作成します。たとえば、**SystemAccessAnalyst** および **PCIAAnalyst** のようなロールを作成し、この制限された分析担当者ロールの 1 つだけに分析担当者を割り当てます。次に、タグに基づいて、これらのリソースのサブセットにアクセスを許可するポリシーを作成します。たとえば、**SystemAccessAnalyst** ロールにシステム アクセス タグの付いたレポートとクエリへのアクセスを許可するポリシーを作成し、**PCIAAnalyst** ロールに **PCI** タグの付いたレポートとクエリへのアクセスを許可する別のポリシーを作成します。ほかのタグについても、それに基づくロールおよびポリシーを別途作成します。このようにして、アクセスを制限するポリシーを、アクセスフィルタを使用して作成します。

管理者は、以下のアプローチのいずれかを使用して、サーバ ベースのポリシーを作成できます。

- データの制限

データ アクセス フィルタを作成し、`receiver_name` フィールド用のフィルタを設定し、`systemstatus` や `syslog` のような値を指定して、特定のログへのアクセスを制限できます。

- 設定の制限

選択済みリソースとして `AppObject` を設定した `SafeObject` リソース クラスに関するポリシーを作成して、特定の `CA Enterprise Log Manager` へのアクセスを制限できます。すなわち、特定のホスト上にあるレポート サーバ設定のみにアクセスできるよう制限するには、以下のようなフィルタを定義します。

```
pozFolder contains /CALM_Configuration/Modules/calmReporter/LogServer01
```

詳細情報:

[カスタム統合のポリシーの例](#) (P. 141)

[抑制ルールおよび集約ルール用のポリシーの例](#) (P. 143)

[アクセス フィルタの作成](#) (P. 108)

[ユーザ: Win-Admin のデータ アクセスを制限するシナリオ](#) (P. 120)

[ロールのアクセス制限: PCI-Analyst シナリオ](#) (P. 134)

アプリケーション ユーザ グループ(ロール)の作成

必要なロールをサポートするためのアプリケーションユーザ グループを新規作成できます。新しいアプリケーションユーザ グループを作成したら、そのグループ用のアクセス ポリシーを作成する必要があります。

新規グループに新しいアクセス ポリシーが不要となるケースとしては、新規グループが既存グループへのメンバシップを与えられる場合などがあります。次のようなシナリオを考えてみましょう。データ マッピングとメッセージ解析ファイルの作成専門の個人用ロールと、抑制ルールおよび集約ルールの作成専門の個人用ロール、さらに、この 2 つの業務のどちらも実行できる人のための第 3 のロールが必要であるとします。このような場合は、アプリケーション ユーザ グループを **AdminDMMP** という名前で定義し、統合リソースへのアクセス許可を与えるためのポリシーを割り当てます。また、別のグループを **AdminSS** という名前で定義して、イベントグループ化リソースへのアクセス許可を与えるためのポリシーを割り当てます。その後、第 3 のグループを **AdminDMMPSS** という名前で作成し、これに **AdminDMMP** グループおよび **AdminSS** グループへのメンバシップを付与します。この 3 番目のグループは、自動的に 2 つのメンバシップグループからポリシーを継承します。

新たにアプリケーション グループやロールを作成せずに、事前定義済みの **Analyst** ロールや **Auditor** ロールの機能を拡張することができます。たとえば、**Analyst** が抑制ルールと集約ルールを作成できるようにし、**Auditor** がこれらのルールを表示できるようにするには、集約ルールと抑制ルールを作成する権限を許可する **CALM** ポリシー、およびカスタム ルールを表示または編集する権限を許可する **スコープ** ポリシーを作成して、これらのポリシーを **Analyst** ロールに割り当てます。その後、集約ルールと抑制ルールを表示する権限を許可する **スコープ** ポリシーを作成して、**Auditor** グループに割り当てます。

新規ロールを作成できるのは、**Administrator** だけです。

アプリケーションユーザ グループ(ロール)の新規作成方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. [グループ]をクリックします。
3. [ユーザ グループ]リストの[アプリケーション グループ]フォルダの左にある[新しいアプリケーション グループ]ボタンをクリックします。
4. グループ名と説明を入力します。

5. 2 つ以上のユーザ定義アプリケーション グループに対して定義されたことがあるアクセス権をこの新規ユーザ グループに与える場合は、それらのアプリケーション グループを選択して、メンバシップを付与します。そうでない場合は、選択はできません。

注: この新規グループが既存グループから構成されている場合は、各コンポーネントグループの既存のポリシーがこのグループに適用されます。ポリシーを追加する必要はありません。

6. [保存]をクリックします。
7. [閉じる]をクリックします。

詳細情報:

[手順 2: PCI-Analyst ロールの作成 \(P. 136\)](#)

[抑制ルールおよび集約ルール用のポリシーの例 \(P. 143\)](#)

カスタム ロールによる CA Enterprise Log Manager へのアクセスの許可

アプリケーション ユーザ グループ、すなわちロールを作成する場合は、必ず事前定義済みの CALM アプリケーション アクセス ポリシーにそれを追加します。このポリシーに明示的に追加された ID のみが、CA Enterprise Log Manager にアクセスできます。ID は、個人ユーザでも、ユーザ グループのメンバでもかまいません。

新規ユーザ グループに割り当てられたユーザが CA Enterprise Log Manager にログインできない場合は、CALM アプリケーション アクセス ポリシーの ID にこのグループが含まれていることを確認してください。

ユーザ定義のアプリケーション ユーザ グループに CA Enterprise Log Manager へのアクセスを許可する方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]をクリックして、左側ペインの[アクセス ポリシー]をクリックします。
2. [スコープ ポリシー]をクリックし、[CALM アプリケーション アクセス]を選択します。

3. [ID]から、以下の要領で、新規アプリケーション グループを検索します。
 - a. [タイプ]で、[アプリケーション グループ]を選択します。
 - b. [ID の検索]をクリックします。
 - c. 属性を「名前」、演算子を「LIKE」のままにします。[検索]をクリックします。

表示された ID リストに、新規アプリケーション グループの名前が表示されます。
 - d. 新規アプリケーション グループの名前を選択し、[移動]ボタンをクリックして、[選択された ID]ボックスにグループ名を移動させます。
4. [保存]をクリックします。

既存ポリシーへの ID の追加

アプリケーションユーザ グループを新規作成する際、状況に応じて、新規グループを既存ポリシーに追加できます。ロールを与えず、アクセスフィルタでアクセスを制限するユーザを作成する場合に、既存ポリシーにそのユーザを追加できます。

重要： インストール済みのアクセス ポリシーに変更を加える場合、これらのポリシーはロックも保護もされていないため、それらを削除しないように十分注意してください。

誤って事前定義済みアクセス ポリシーを削除してしまうと、復元するまで、ユーザは CA Enterprise Log Manager サーバにアクセスできなくなります。safex ユーティリティを使用して、ポリシーをリストアできます。

既存ポリシーに ID を追加する方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]をクリックして、左側ペインの[アクセス ポリシー]をクリックします。
2. ポリシー タイプをクリックし、新規アプリケーション ユーザ グループに適用するポリシーを選択します。[ID]ペインを表示します。
3. [タイプ]で、[アプリケーション グループ]を選択します。
4. [ID の検索]をクリックします。
5. 属性を「名前」、演算子を「LIKE」のままにします。[検索]をクリックします。
表示された ID リストに、新規アプリケーション グループの名前が表示されます。
6. 新規アプリケーション グループの名前を選択し、[移動]ボタンをクリックして、[選択された ID]ボックスにグループ名を移動させます。
7. [保存]をクリックします。

詳細情報：

[手順 4: 既存ポリシーへの PCI-Analyst の追加 \(P. 137\)](#)

CALM アクセス ポリシーの作成

1 つ以上の CALM リソースに対する 1 つ以上の有効なアクションを許可 (または拒否) する CALM アクセス ポリシーを作成できます。

以下の CALM リソースはアプリケーション固有のものです。すなわち、CA Enterprise Log Manager 製品によってのみ使用されるリソースです。

- Alert
- AgentConfiguration
- AgentAuthenticationKey
- ALL_GROUPS
- Connector
- Data
- Database
- EventGrouping
- Integration
- Profile
- Report
- Tag

ゼロから CALM ポリシーを新規作成する方法

1. [管理] タブをクリックし、[ユーザとアクセスの管理] サブタブをクリックします。
2. [アクセス ポリシー] をクリックします。
3. CALM フォルダの左にある[新規アクセス ポリシー] ボタンをクリックします。
4. 意味のあるポリシー名、および必要に応じて、短い説明を入力します。
5. このポリシーが一時的なものである場合は、適用される日付範囲を備えたカレンダーを選択します。
6. [リソース クラス名] を「CALM」のままにします。

7. 以下の基準に応じて、[一般]パネルの[タイプ]を選択します。
 - 選択したすべての ID に対して、適用先として選択したすべてのリソースに選択したすべてのアクションの実行を許可または拒否するアクセス ポリシーを選択します。
 - 選択したすべての ID に対して、選択した 1 つのリソースに選択したアクションのみの実行を許可または拒否するアクセス制御リストを選択します。

注: 複数のリソース用のフィルタを保存することはできません。これを行うには、個別のポリシーを、リソース/フィルタの組み合わせごとに 1 つずつ作成します。
 - 選択した各 ID に対して、適用先として選択したすべてのリソースに選択したアクションの実行を許可または拒否する ID アクセス制御リストを選択します。
8. 以下の要領で、[ID]領域を使用して、このポリシーが適用されるユーザまたはグループを選択します。
 - a. [タイプ]で「アプリケーション グループ」またはほかの選択肢のいずれかを選択し、[ID の検索]を選択し、[検索]をクリックします。
 - b. 利用可能な ID の中から ID を選択し、[移動]ボタンをクリックして、[選択された ID]ボックスに移動させます。
9. ポリシー タイプがアクセスポリシーである場合は、以下の要領で、アクセスポリシー設定を完了します。
 - a. [リソースの追加]フィールドに CALM リソースを入力し、[追加]をクリックします。
 - b. 選択した ID が選択したすべてのリソースに実行できるアクションをすべて選択します。有効なアクションには、注釈付け、作成、データ アクセス、編集、およびスケジュールが含まれます。アクションが有効である場合、そのアクションをあるリソースについては実行を許可し、別のリソースについては許可しないということとはできません。

10. ポリシー タイプがアクセス制御リストである場合は、以下の要領で、アクセス制御リスト設定を完了します。
 - a. [リソースの追加]フィールドに **CALM** リソースを入力し、[追加]をクリックします。
 - b. 選択した **ID** がこのリソースに実行できるアクションをすべて選択します。有効なアクションには、注釈付け、作成、データ アクセス、編集、およびスケジュールのうち、1 つ以上が含まれます。
 - c. このポリシーによって対処されるリソースごとに、上記の 2 つの手順を繰り返します。

このタイプでは、作成などのアクションをあるリソースについては実行を許可し、別のリソースについては許可しないということが可能です。
11. ポリシー タイプが **ID** アクセス制御リストである場合は、以下の要領で、**ID** アクセス制御リスト設定を完了します。
 - a. 選択した **ID** ごとに、アクションが有効であるすべてのリソースに対して許可または拒否するアクションを選択します。
 - b. 追加するリソースごとに、[リソースの追加]フィールドに **CALM** リソース名を入力し、[追加]をクリックします。
12. 上部にあるチェック ボックスを確認し、該当するものをオンにします。
 - アクセスを許可するポリシーからアクセスを拒否するポリシーに変更するには、[明示的な否認]を選択します。
 - 新規の場合に、このポリシーを一時的に非アクティブにするには、[無効]をオンにします。
 - テスト目的でこのポリシーを使用していて、カスタム ラベルを使用してポリシーを分類する場合は、[導入前]をオンにしてから、[ラベルの割り当て]をオンにし、ラベルを追加します。
13. 左側ペインで[保存]をクリックし、[閉じる]をクリックします。

スコープ ポリシーの作成

任意のグローバルリソースに関するスコープ ポリシーを作成できます。スコープ ポリシーのアクションは、読み取りおよび書き込みに制限されます。

- 以下のグローバルリソースは、多くの CA 製品 (アプリケーション) によって使用されます。
 - Calendar
 - GlobalUser
 - GlobalUserGroup
 - iPoz
 - Policy
 - User
 - UserGroup
 - AppObject
- グローバルリソース AppObject によって、アプリケーション固有のリソースおよびモジュールに関するスコープ ポリシーを作成できます。これを行うには、アプリケーション固有のコンテンツまたはモジュールが保存される関連の EEM フォルダを指定するフィルタを追加します。
 - AppObject リソースに関するフィルタ内で使用できる EEM コンテンツフォルダには、以下のものがあります。
 - EventGrouping
 - Integration (サーバ)
 - Profile
 - Report
 - AppObject リソースに関するフィルタ内で使用できる CA Enterprise Log Manager モジュール フォルダには、以下のものがあります。
 - [イベントログストア]
 - レポートサーバ
 - サブスクリプション

既存の設定を流用できるポリシーがない場合は、最初からポリシーを作成できます。作成した CALM ポリシーに関連したスコープ ポリシーを作成する場合は、関連する CALM ポリシー内にあるものと同じ ID を指定します。

Administrator のみがアクセス ポリシーを作成、編集、削除、表示できます。

明示的な許可のスコープ ポリシーを新規作成する方法

1. [管理] タブをクリックし、[ユーザとアクセスの管理] サブタブをクリックします。
2. [アクセス ポリシー] をクリックします。
3. [スコープ ポリシー] フォルダの左側にある[新規スコープ ポリシー] ボタンをクリックします。
4. ポリシーに意味のある名前を付けます。たとえば、ポリシーが適用されるロールやスコープ内のタスクを名前に含めます。この命名規則の使用方法については、事前定義済みポリシーの名前を参考にしてください。
5. 暗号化された名前が何を意味するかを十分にわかる短い説明を入力します。
6. 通常、リソース クラス名として **SafeObject** をそのまま使用します。
7. 以下の基準に従って[一般] パネルでタイプを選択します。
 - 選択したすべての ID について、選択したすべての適応対象のリソースに対して選択したすべてのアクションを実行することを許可するか拒否するには、アクセス ポリシーを選択します。
 - 選択したすべての ID について、選択した 1 つのリソースに対して選択したアクションのみを実行することを許可するか拒否するには、アクセス 制御リストを選択します。

注: 複数のリソースを対象とするフィルタを保存することはできません。回避策は、リソースとフィルタの組み合わせごとに個別のポリシーを作成することです。
 - 選択した各 ID について、選択したすべての適応対象のリソースに対して選択したアクションを実行することを許可するか拒否するには、ID アクセス制御リストを選択します。
8. ポリシー タイプがアクセス ポリシーまたはアクセス制御リストである場合は、[ID] 領域を使用して、このポリシーが適用されるユーザまたはグループを選択します。
 - a. [タイプ] で[アプリケーション グループ]を選択し、[ID の検索]をクリックして、[検索]をクリックします。
 - b. 使用可能な ID から必要な ID を選択し、[移動] ボタンをクリックして、それらを[選択された ID] ボックスに移動します。

9. ポリシー タイプがアクセス ポリシーである場合、デフォルトでは、すべてのアクションがすべてのリソースに対して選択されます。このポリシーをカスタマイズするには、以下のようにアクセス ポリシー設定を完了します。
 - a. [リソースの追加]ドロップダウン リストからリソースを選択し、[追加]をクリックします。
 - 読み取りまたは書き込みアクセスが設定されるリソースが **CA Enterprise Log Manager** 固有のリソースである場合は、[AppObject]を選択します。
 - [管理]タブの[ユーザとアクセスの管理]サブタブにある[ユーザ]ボタンへのアクセスについては、[ユーザ]と[グローバル ユーザ]を選択します。
 - [管理]タブの[ユーザとアクセスの管理]サブタブにある[グループ]ボタンへのアクセスについては、[ユーザ グループ]と[グローバル ユーザ グループ]を選択します。
 - [管理]タブの[ユーザとアクセスの管理]サブタブにある[アクセス ポリシー]、[EEM フォルダ]、および[テスト ポリシー]ボタンへのアクセスについては、[ポリシー]を選択します。
 - [管理]タブの[ユーザとアクセスの管理]サブタブにある[カレンダー]ボタンへのアクセスについては、[Calendar]を選択します。
 - [管理]タブの[ユーザとアクセスの管理]サブタブにある[パスワード ポリシー]および[ユーザ ストア]ボタンへのアクセスについては、[iPoz]を選択します。
 - b. 表示アクセスを許可/拒否するには[読み取り]を選択します。編集アクセスを許可/拒否するには[書き込み]を選択します。いずれも選択しない場合は、すべてのアクションが選択されます。
 注: 作成アクセスを許可/拒否するには、**CALM** アクセス ポリシーを定義し、**CA Enterprise Log Manager** リソースを個別に選択する必要があります。
 - c. 必要に応じて、選択したリソースに適用する汎用のフィルタを追加します。

10. ポリシー タイプがアクセス制御リストである場合は、以下のようにアクセス制御リスト設定を完了します。
 - a. [リソースの追加]ドロップダウンリストからリソースを選択し、[追加](+) ボタンをクリックします。
 - b. アクションについて、「読み取り」、「書き込み」、またはその両方を選択します。
 - c. [フィルタの編集]ボタンをクリックして、フィルタフォームを開きます。左辺のタイプ/値、演算子のタイプ/値、右辺のタイプ/値について値を選択または入力することにより、関連するリソース用のフィルタを作成します。
 - d. フィルタに値としてリソース名が含まれる場合は、[リソース名を正規表現として扱う]チェックボックスをオンにします。それ以外の場合は、このチェックボックスをオフのままにします。

重要: リソースとフィルタの組み合わせごとに **1 つのポリシーを定義**します。

11. ポリシー タイプが ID アクセス制御リストである場合は、ID アクセス制御リスト設定を以下のように完了します。
 - a. タイプについて、表示されたオプションの **1 つ**を選択します。たとえば、[アプリケーショングループ]を選択し、[ID の検索]リンクをクリックします。[検索]ボタンをクリックして、選択したタイプのメンバを表示します。
 - b. ID を選択し、移動ボタンをクリックして、[選択された ID]ペインに入力します。
 - c. 選択した各 ID について、[読み取り]、[書き込み]、またはその両方を指定します。

ID に固有のアクションは、選択したすべてのリソースに適用されます。つまり、指定した ID は表示、表示と編集、選択したすべてのリソースの編集のみのいずれかが可能です。
 - d. ID に固有のアクションが許可または拒否されるリソースを追加します。

12. 以下のチェック ボックスを確認し、該当するチェック ボックスをオンにします。

- アクセスを許可するポリシーから、アクセスを拒否するポリシーにポリシーを変更するには、[明示的な否認]をオンにします。
- 新規の場合は、[Disabled]をオンにして、このポリシーを一時的に非アクティブ化します。
- テスト目的でポリシーを使用する場合や、カスタム ラベルでポリシーを分類する場合は、[導入前]をオンにし、[ラベルの割り当て]を選択して、ラベルを追加します。

13. [保存]をクリックし、左のペインで[閉じる]をクリックします。

詳細情報:

[手順 3: Win-Admin システム アクセス ポリシーの作成](#) (P. 124)

既存のポリシーをベースにしたポリシーの作成

既存のアクセス ポリシーをコピーして変更することで、新しいアクセス ポリシーを作成できます。この手順によって、現在の要件を満たすのに、既存ポリシーの仕様へのわずかな変更しか必要ない場合に、仕様を手動で複製する時間を省くことができます。

アクセス ポリシーの作成、編集、削除、および表示を実行できるのは、Administrator だけです。

既存のポリシーをベースにポリシーを作成する方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. [アクセス ポリシー]をクリックします。
3. テンプレートとして使用するポリシーのタイプに応じて、[CALM]または[スコープ ポリシー]を選択します。
4. 名前のリンクをクリックし、コピーするポリシーを開きます。
5. [名前を付けて保存]をクリックします。
[Explorer ユーザー プロンプト]ダイアログ ボックスが表示されます。

6. オープン ポリシーをベースにする新規ポリシーの名前を入力し、[OK]をクリックします。

7. 必要な変更を加えます。

たとえば、コピーされた ID を、このポリシーが適用されるロール (ユーザ定義アプリケーション ユーザ グループ) の名前に置き換えます。コピーされたリソース上で許可されるアクションへの変更を検討します。[フィルタ]をクリックして新規ロールの追加フィルタを指定することを検討します。

8. [保存]をクリックし、[閉じる]をクリックします。

9. 新規ポリシーの定義を検証します。

a. すべてのポリシーを表示するために、ポリシー タイプを再度選択します。

b. 新規ポリシーを元のポリシーと比較し、意図した変更がすべて新規ポリシーに反映されていることを確認します。

c. [閉じる]をクリックします。

10. ポリシーをテストします。

詳細情報:

[手順 5: 分析担当者用レポート表示/編集ポリシーをベースにしたポリシーの作成 \(P. 138\)](#)

新しいポリシーのテスト

テスト ポリシー機能を使用すると、新規作成したポリシーの構文が正しいかどうかをテストできます。テスト ポリシー機能では、定義したアクセス ポリシーにアドホック クエリを実行できます。権限とは、「{ID}はタイプ{リソース クラス}および名前{リソース}のリソースに対して、{アクション}を、[次の{属性}]を使い、[{指定時刻}]に実行可能か?」というリクエストであると考えられます。ALLOW という結果が返されれば、入力した ID は、指定したリソースに対する指定したアクションを、指定した属性を使用して指定した時刻に実行することができます。

テストを開始する前にポリシーを用意しておきます。

ポリシーのテスト方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. [テスト ポリシー]をクリックします。
[権限チェックのパラメータ]ページが表示されます。
3. チェック対象が、[導入前]を選択し、ラベルを追加したポリシーである場合は、導入前のポリシーを対象に含め、関連付けられたラベルを追加することを示すチェック ボックスをオンにします。
4. エントリフィールドに値を入力します。ポリシーがフィルタを含んでいる場合は、ポリシーに表示される順にフィルタを指定します。
5. [権限チェックの実行]をクリックします。
6. 結果を確認し、以下の方法のいずれかを実行します。
 - 結果が **ALLOW** であれば、実稼働環境で使用する前に、この新規ポリシーで ID として指定したユーザで **CA Enterprise Log Manager** にログオンし、ポリシーの有効性、スコープ、および範囲をテストします。
 - 結果が **DENY** である場合は、クエリの入力事項を確認します。内容が正しい場合はポリシーに戻り、そうでない場合は必要な訂正を行います。

動的ユーザ グループ ポリシーの作成

動的ユーザ グループは、1 つ以上の共通属性を共有するグローバル ユーザから構成されます。動的ユーザ グループは、特殊な動的ユーザ グループ ポリシーによって作成されます。このポリシーでは、リソース名が動的ユーザ グループ名で、メンバシップのベースがユーザ属性およびグループ属性に設定されたフィルタ セットになります。

ユーザ、アプリケーション グループ、グローバル グループ、または動的グループから構成される動的グループを作成できます。たとえば、[名前]、[説明]、または[グループのメンバシップ]に基づいて、グローバル グループまたはアプリケーション グループの動的グループを作成できます。あるいは、以下のようなグローバル ユーザ プロファイルの共通属性に基づいて、複数のロールを備えたユーザの動的グループを作成できます。

- 職種
- 部署またはオフィス
- 都市、都道府県、または国

動的ユーザ グループ ポリシーを作成できるのは、Administrator だけです。

動的ユーザ グループ ポリシーを作成する方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. [アクセス ポリシー]をクリックします。
3. [新規動的グループ ポリシー]をクリックします。
[新規動的グループ ポリシー]ページが表示されます。
4. [名前]に、このユーザ グループが共有する内容がわかるようなグループ名を入力します。任意で、説明を入力します。
5. ポリシー タイプを選択します。デフォルトは「アクセス ポリシー」です。

6. 以下の要領で、ID を選択します。
 - a. [タイプ]で、「ユーザ」、「アプリケーショングループ」、「グローバルグループ」、または「動的グループ」を選択し、[ID の検索]をクリックします。
 - b. [属性]、[演算子]、および[値]に、このグループのメンバシップの基準を設定する構文を入力し、[検索]をクリックします。
 たとえば、「ユーザ」を選択した場合は、「役職 Like マネージャ」と入力し、[検索]をクリックして、役職が「マネージャ」であるユーザをすべて検索します。
 - c. 表示された ID からこの動的グループのメンバである ID を選択し、[移動]矢印をクリックして、[選択された ID]ボックスに選択した ID を移動させます。
7. [アクション]で、「所属」を選択します。
8. [リソースの追加]フィールドに、[名前]フィールドで入力した値を入力し、[追加]ボタンをクリックします。これは、選択した ID が作成したばかりの動的グループリソースに所属することを示します。
9. 任意で、さらにフィルタを追加します。
10. [保存]をクリックします。
11. [動的ユーザ グループ ポリシー]リンクをクリックし、新規作成した動的ユーザグループを確認します。以下に例を示します。

動的ユーザ グループ ポリシー					
<< < 1 > >> / 1					
名前/説明	ResourceClassName	オプション	ID	アクション	リソース
Non-Administrators	SafeDynamicUserGroup	明示的な許可	ug:Auditor ug:ResourceAccessAnalyst ug:CALM-Analyst ug:Analyst	belong	Non-Administrators
QA Group	SafeDynamicUserGroup	明示的な許可	User1 User2 User3	belong	QA Group
Security Officers	SafeDynamicUserGroup	明示的な許可	Administrator1 User3	belong	Security Officers

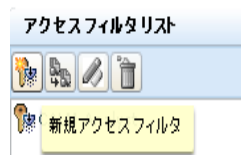
アクセス フィルタの作成

アクセス フィルタを作成し、フィルタ基準と一致するログ データへのアクセスを制限できます。デフォルトでは、すべての CA Enterprise Log Manager アプリケーション ユーザに、アクティブな CA Enterprise Log Manager サーバ、メッシュ統合に含まれるピアサーバ、または階層統合の子サーバに含まれるイベントログストアに保存されたイベントログ データへのクエリアクセス権があります。

データアクセス フィルタを作成すると、アクセス権を、1 つ以上の特定の CA Enterprise Log Manager サーバのイベントログストアに制限できます。個人またはグループにアクセス フィルタを適用できます。

ユーザ定義ロール用のアクセス フィルタを作成する方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. [新規アクセスフィルタ]をクリックします。



アクセス フィルタの設計ウィザードが表示されます。

3. [詳細]に、フィルタの名前と説明を入力します。
4. [ID]をクリックします。ID のタイプを選択し、[検索]ボタンをクリックして使用可能な ID を表示し、シャトル コントロールを使用してこのアクセス フィルタを適用する ID を選択します。

たとえば、この目的のために作成したアプリケーション グループを選択します。

5. アクセスフィルタを設定します。
 - a. [アクセスフィルタ]をクリックします。
 - b. [新規イベントフィルタ]ボタンをクリックします。



- c. アクセスフィルタを定義する表現を 1 つ以上追加します。
 - d. [保存して閉じる]をクリックします。
- 作成したアクセスフィルタが表示されます。
6. [閉じる]をクリックします。

詳細情報:

[手順 4: Win-Admin データ アクセスフィルタの作成 \(P. 128\)](#)
[アプリケーション ユーザ グループ \(ロール\) の作成 \(P. 92\)](#)

ユーザ アカウントとアクセス ポリシーの保守

Administrator は、ユーザ アカウントおよびアクセス ポリシーに関する以下の保守タスクを実行できます。

- ユーザ アカウントをロックし、ユーザが CA Enterprise Log Manager にログインできないようにする
- パスワード ポリシーによって、ロックされたユーザ アカウントのアンロックが許可されていない場合に、ロックされたユーザ アカウントをアンロックする
- 新しいユーザ アカウントの追加
- 既存のユーザ アカウントの編集
- CA Enterprise Log Manager へのアクセスがなくなった個人が所有しているユーザ アカウントのロックまたは削除
- 既存のアクセス ポリシーの編集
- 必要なくなったアクセス ポリシーの削除
- 委任ポリシーの作成、編集、および削除
- それに対応する自動生成された責任ポリシーが付与されたアクセス フィルタの作成、編集、および削除
- 制限されたアクセス権を持つ既存ロールからスーパー ロールの作成
- 新しいカスタム ロールおよび対応するアクセス ポリシーの追加

カレンダーの作成

ある期間にユーザ アクセスを制限しやすくするためにカレンダーを新規作成できます。カレンダーはアクセス ポリシーの一部として機能します。カレンダーを定義する際、時間単位、曜日単位、または日付単位で、時間ブロックを条件に含めたり除外したりできます。

カレンダーの作成方法

1. [管理] タブをクリックし、[ユーザとアクセスの管理] をクリックして、[カレンダー] ボタンをクリックします。
[カレンダー] ページが表示されます。
2. カレンダーリストの左上で、[新規カレンダー] アイコンをクリックします。
[新規カレンダーの詳細] ペインが表示されます。

3. 目的のポリシーを示す名前を入力し、使用目的に関する説明を加えます。
4. カレンダー アイコンを使用し、カレンダーの開始日および終了日を設定します。
5. [包含時間ブロックの追加]または[除外時間ブロックの追加]をクリックし、カレンダーの主な有効期間内の例外期間を作成します。
6. [保存]をクリックし、[閉じる]をクリックします。

詳細情報:

[ポリシーへのカレンダーの追加](#) (P. 111)

ポリシーへのカレンダーの追加

ポリシーを作成する際、指定した ID が指定したリソース上で選択したアクションを実行できる時間を指定する既存カレンダーを選択できます。カレンダーでは、開始日、終了日、および時間単位または曜日単位の時間ブロックを定義できます。

カレンダーをポリシーに追加する方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. このカレンダーを適用するポリシーを開きます。
 - a. [アクセス ポリシー]をクリックします。
 - b. ポリシー タイプを選択します。
 - c. ポリシーを選択します。
3. [カレンダー]ドロップダウンリストを開き、このポリシー用に作成したカレンダーを選択します。

The screenshot shows a configuration window for a policy named 'ResourceAccessAnalyst Create-Schedule-Annotate policy'. The 'Calendar' dropdown menu is open, displaying several options. The first option is 'ResourceAccessAnalyst Schedule', which is highlighted. Other visible options include '<なし>' (None), 'Auditor-scheduled alerts', and 'ResourceAccessAnalyst Schedule-...'. The 'Name' field contains 'ResourceAccessAnalyst Create-Schedule-Annotate policy' and the 'Description' field contains 'ResourceAccessAnalyst can create, schedule, annotate Reports, schedule Alerts, and create tags'.

4. [保存]をクリックし、既存ポリシーへのカレンダーの追加を保存します。

詳細情報:

[カレンダーの作成](#) (P. 110)

例: 営業日へのアクセス制限

特定のユーザ グループに CA Enterprise Log Manager へのアクセスを許可する時間帯や曜日を制限できます。これを行うには、アクセスを許可する時間帯のカレンダーを作成し、カスタム ロールを作成し、CA Enterprise Log Manager へのアクセス権を提供するポリシーを基に新規ポリシーを作成して、このポリシーにカレンダーおよびカスタム ロールを割り当てます。

例 -- 外部監査担当者の CA Enterprise Log Manager へのアクセス権を平日に限定する

あるグループの CA Enterprise Log Manager へのアクセス権を営業日に限定するには、平日用のカレンダーを作成し、監査担当者専用のアクセス権を付与するポリシーにこのカレンダーを追加します。

たとえば、外部監査担当者の CA Enterprise Log Manager へのアクセス権を営業時間に限定する場合は、年間のすべての月の平日、すなわち月曜日から金曜日の、午前 9 時～午後 5 時を指定するカレンダーを作成します。

全数

フォルダ:
名前: Weekdays 9-5
説明:
発効日: 2008年11月17日 2:29:00
失効日: 2009年12月31日 6:00:00

包含時間ブロック

新

名前: 新

開始時刻: 00 : 00 期間: 00 : 00
繰り返しの間隔: 00 : 00

= 選択済み

平日のマスク

日	月	火	水	木	金	土
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				末日

月のマスク

1月	2月	3月
4月	5月	6月
7月	8月	9月
10月	11月	12月

外部監査担当者のロールを作成します。

[CALM アプリケーション アクセス]スコープ ポリシーを開き、「外部監査担当者 -CALM アプリケーション アクセス」という名前で保存して、「平日 9-5 カレンダ」を選択し、[ID]で「外部監査担当者」ユーザ グループを選択します。

重要: カレンダ機能は、アクセス権を付与するポリシーとのみ一緒に使用します。アクセスを拒否するポリシーと共に使用しないでください。

詳細情報:

[カレンダの作成](#) (P. 110)

[アプリケーション ユーザ グループ \(ロール\) の作成](#) (P. 92)

[既存のポリシーをベースにしたポリシーの作成](#) (P. 103)

[ポリシーへのカレンダの追加](#) (P. 111)

アクセス ポリシーのエクスポート

事前定義済みポリシーであるかカスタム ポリシーであるかにかかわらず、必要に応じて、選択したタイプのポリシーをすべてエクスポートできます。ポリシーのエクスポートは、現在のバックアップを保存するのに効果的な方法です。

エクスポートすると、選択したポリシーごとに XML ファイルが作成され、すべての XML ファイルが CAELM[1].xml.gz という名前の 1 つのファイルに圧縮されます。

アクセス ポリシーをエクスポートする方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. [アクセス ポリシー]をクリックします。
3. エクスポートするアクセス ポリシーを選択し、[エクスポート]をクリックします。
[ファイルのダウンロード]ダイアログ ボックスが表示されます。
4. [保存]をクリックし、一意の名前でファイルを保存します。
5. [閉じる]をクリックします。

詳細情報:

[すべてのアクセス ポリシーのバックアップ](#) (P. 65)

カスタム ポリシーの削除

以下のいずれかの場合に、カスタム ポリシーを削除できます。

- あるカスタム ポリシーを別の名前でも保存していて、名前以外の変更を加える予定がないため、重複ポリシーを削除する必要がある場合
- ポリシーに定義された ID がアクティブなメンバではなくなり、ポリシーを使用しなくなった場合

重要： 事前定義済みポリシーを削除しないように注意してください。万一削除した場合は、バックアップをエクスポートしていれば復元できます。

カスタム ポリシーの削除方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. [アクセス ポリシー]をクリックします。
3. 削除するポリシーのタイプに応じて、[CALM]または[スコープ ポリシー]を選択します。
4. 削除するポリシーの名前をクリックします。
5. [削除]をクリックします。
6. [OK]をクリックし、削除を確定します。

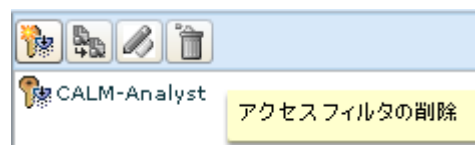
アクセス フィルタおよび責任ポリシーの削除

データ アクセス制限を削除するには、フィルタによって生成されたアクセス フィルタおよび責任ポリシーを削除します。

アクセス ポリシーのフィルタによって生成された責任ポリシーは削除しないでください。

アクセス フィルタおよび責任ポリシーを削除する方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]をクリックします。
[アクセス フィルタ リスト]が左ペインの上部に表示されます。
2. 削除するフィルタを選択し、[アクセス フィルタの削除]をクリックします。



アクセスフィルタの削除を確認する警告メッセージが表示されます。

3. [はい]をクリックし、選択したアクセス フィルタおよび関連する責任ポリシーを削除します。

例：管理者以外のユーザへのアーカイブ管理の許可

Administrator 以外のグループに自動アーカイブの管理を許可する必要があると仮定します。ArchiveAdministrator という名前のグループ、および、リソース データベースへの編集アクションを許可する CALM ポリシーを作成します。これによって、クエリ用にデータベースのアーカイブ カタログへの読み取りアクセス権を、カタログ再作成用にアーカイブ カタログへの書き込みアクセス権を、および手動アーカイブ用に LMArchive ユーティリティまたは自動アーカイブされたデータベースの復元用に restore-ca-elm シェル スクリプトの使用権限を許可することができます。

指定した非管理者ユーザがアーカイブ処理を実行できるようにする方法

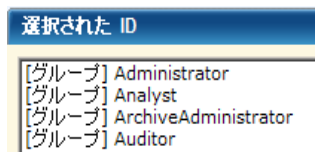
1. ArchiveAdministrator という名前のロールを作成します。
 - a. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
 - b. [グループ]を選択します。
 - c. [新規アプリケーション グループ]をクリックします。
 - d. 名前として「ArchiveAdministrator」を入力します。
 - e. [保存]をクリックします。

アプリケーション グループ、すなわちロールとして ArchiveAdministrator が作成されます。
 - f. [閉じる]をクリックします。

アクセス ポリシーの設定	
リソース	アクション
	create
	schedule
	annotate
	dataaccess
	edit
リソースの追加:	[すべてのアクション]
Database	☐ ☐ ☐ ☐ ☒ ☐

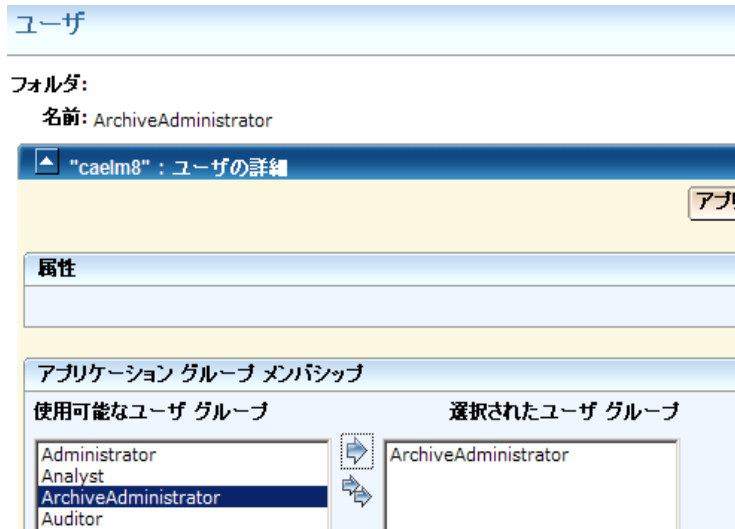
結果	ポリシー	委任者	ID	リソース クラス	リソース	アクション
許可	ArchiveAdministratorpolicy		ArchiveAdministrator	CALM	Database	edit

4. ArchiveAdministrator ロールに CA Enterprise Log Manager へのログオン権限を付与します。
 - a. [アクセス ポリシー]で[CALM]をクリックします。
 - b. [CALM アプリケーション アクセス]を選択します。
 - c. [ID]から、アプリケーショングループ ArchiveAdministrator を検索し、[選択された ID]に移動させます。



- d. [保存]をクリックします。[閉じる]をクリックします。[閉じる]をクリックします。
- [ユーザとアクセスの管理]タブが、左側ペインに各種ボタンと共に表示されます。

5. 1人以上のユーザに **ArchiveAdministrator** ロールを割り当てます。
 - a. [ユーザ]をクリックします。
 - b. このロールを割り当てるユーザ名を、[ユーザの検索]の値として入力し、[実行]をクリックします。
 選択したユーザ名前が、[ユーザ]フォルダの下に表示されます。
 - c. 選択したユーザのリンクを選択します。
 - d. [アプリケーション ユーザの詳細の追加]をクリックします。
 - e. **ArchiveAdministrator** を[選択されたユーザ グループ]リストに移動させます。



- f. [保存]をクリックします。[閉じる]をクリックします。
 - g. このロールを割り当てるユーザごとに、繰り返します。
 - h. [閉じる]をクリックします。

6. (オプション) CA Enterprise Log Manager からの結果を確認します。
 - a. [ログアウト]をクリックし、管理者としてログアウトします。
 - b. ロール **ArchiveAdministrator** を割り当てたユーザとしてログインします。
 - c. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
 - d. [カタログ クエリのアークाइブ]を選択します。
 - e. [クエリ]ボタンおよび[カタログ再作成]ボタンを使用できることを確認します。
7. (オプション) **ArchiveAdministrator** ロールで定義したユーザの認証情報を使用して **restore-ca-elm** 復元スクリプトを実行し、ポリシーが期待どおりに動作することを確認します。

詳細情報:

[自動アーカイブ済みファイルの復元](#) (P. 202)

ユーザ: Win-Admin のデータアクセスを制限するシナリオ

ユーザが表示できるレポートを、指定したタグが付いたレポートに制限できます。また、そのレポート上に表示できるデータを、指定したイベントソースから生成されたデータに制限できます。特定のタグが付いたレポートへのアクセスの制限は、アクセスポリシーを使用して行います。特定の **CA Enterprise Log Manager** サーバに返されたイベントへのデータアクセスの制限は、アクセスフィルタを使用して行います。アクセスフィルタが定義されている場合、ロールの割り当ては任意です。すなわち、ユーザを新規作成し、ロールを割り当てずに、アクセスフィルタを使用して、そのユーザのデータアクセスを制限できます。

米国に 4 つのデータセンターを持つ **ABC** 社のシナリオを考えます。管理者は、ヒューストン地域の管理者に、ヒューストン地域のドメイン コントローラによって処理される **Windows** イベントへの読み取りアクセス権を与える必要があります。ヒューストンドメイン コントローラにインストールされた **CA Enterprise Log Manager** サーバによって処理される **Windows** イベントは、ホスト名が文字列「**ABC-HOU-WDC**」で始まるソースから送信されます。

この例では、Win-Admin というユーザを作成し、このユーザが「システム アクセス」タグが付いたデータのみを表示できるようにし、これらのレポート上のデータを、既知の命名規則で始まるホスト名が付いたイベントソースからのイベントに制限する方法を、順を追って説明します。

この例では、以下の各手順の詳細を説明します。

1. 新規ユーザ Win-Admin を作成します。
2. Win-Admin に CA Enterprise Log Manager への基本的なアクセス権を付与します。CALM アプリケーション アクセス ポリシーにこの ID を追加します。
3. Win-Admin のレポートへのアクセス権を、「システム アクセス」というタグが付いたものに制限します。レポートが保存されている EEM フォルダを指定し、calmTag が「システム アクセス」と等しいことを指定するフィルタを備えた、AppObject への読み取りアクセス権に関するスコープ ポリシーを作成します。ポリシーをテストします。
4. Win-Admin が表示できるデータが、Win-Admin の地域のドメイン コントローラによって生成されたデータに制限されます。Win-Admin が表示できるクエリおよびレポートのデータを、「ABC-HOU-WDC」で始まるホスト名を持つイベント ソースからの Windows イベントに制限するアクセス フィルタを作成し、「Win-Admin データ アクセス」と名前を付けます。
5. Win-Admin ユーザとして CA Enterprise Log Manager にログオンし、ポリシーによって提供されるアクセスを評価します。
6. アクセス制限が厳しすぎて、意図したタスクをユーザが実行できない場合は、追加のポリシーを使用してアクセス権を拡張します。

手順 1: Win-Admin ユーザの作成

アクセスフィルタを使用してデータアクセスを指定する場合は、ロール(アプリケーショングループ)を割り当てずにユーザを作成できます。

この方法でデータアクセスの制限を完了するには、最初にユーザを作成します。

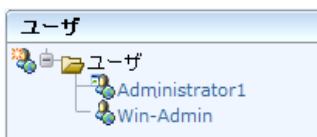
グローバル ユーザ アカウントが外部ディレクトリからのインポートに使用できない場合のみ、ユーザを作成します。そのようなアカウントを作成する場合、アプリケーション ユーザの詳細は追加しません。このシナリオ例では、Win-Admin はユーザ名です。

新規ユーザ

フォルダ:

名前: Win-Admin

ユーザを検索する場合、新しい名前はリスト内に表示されます。



詳細情報:

[グローバル ユーザの作成](#) (P. 41)

手順 2: CALM アプリケーション アクセス ポリシーへの Win-Admin の追加

Win-Admin という名前のユーザのデータアクセスを制限する 2 番目の手順は、この ID に CA Enterprise Log Manager アプリケーションへのアクセス権を与えることです。

CALM アプリケーション アクセス ポリシーに新規ユーザを追加します。この手順は、ID を検索する際にタイプとしてユーザを指定する以外、新しいロールに CA Enterprise Log Manager へのアクセス権を与える手順と同じです。

全般

フォルダ:
名前: ExternalAuditors-CALM Application Access
説明: This policy defines who all can access the CALM Application

カレンダー: Weekdays 9-5
リソース クラス名: SafeObject

タイプ: ☒ アクセス ポリシー
☐ アクセス制御リスト
☐ ID アクセス制御リスト

☐ 明示的な否認
☐ 無効
☐ 導入前
☐ ラベルの割り当て

ID

ID の入力検索
タイプ: ユーザ ID の検索

選択された ID
[グループ] External Auditors

詳細情報:

[カスタム ロールによる CA Enterprise Log Manager へのアクセスの許可 \(P. 93\)](#)

手順 3: Win-Admin システム アクセス ポリシーの作成

手順 2 では、CA Enterprise Log Manager アプリケーションにログオンするためのアクセス権を付与しました。

手順 3 では、ログオン後の CA Enterprise Log Manager アプリケーションへのアクセス権の制限、すなわちスコープを設定します。最も広いレベルでは、指定した ID に、読み取り専用のアクセス権、または読み取りおよび書き込み両方のアクセス権を付与できます。

ポリシー タイプを選択すると、許可されるアクションを指定する際の詳細レベルが決定します。

- アクセス ポリシーでは、選択したアクセス可能なリソースに対して、選択したアクションが許可されます。
- アクセス制御リスト ポリシーでは、追加されたリソースごとに許可されるアクションを指定できます。
- ID アクセス制御リスト ポリシーでは、ID 別に、アクセス可能なリソースへの許可されるアクションを指定できます。

対象リソースの EEM フォルダを指定するフィルタを作成し、そのフォルダへの制限を指定することで、リソースへの制限付きアクセスを許可できます。

以下の例では、一般的な読み取りアクセスに特定の機能への制限を追加して、アクセス権を制限する方法を説明します。具体的には、手順 3 で、Win-Admin ユーザがシステム アクセスレポートのみを表示できるよう制限します。以下の例では、Win-Admin システム アクセスというスコープ ポリシーを作成し、SafeObject と AppObject への読み取りアクセス権を付与し、システム アクセス タグが付いたレポートのみにアクセスできるようフィルタを作成する方法を説明します。また、ポリシーのテスト方法と、検証後に導入前設定を削除する方法についても説明します。

アプリケーションアクセスを読み取り専用、または読み取りおよび書き込みに指定するよう設計されたスコープ ポリシーで、[一般]領域のリソースクラス名を「SafeObject」に指定します。以下の例では、Win-Admin システム アクセスというポリシー名が表示されています。テストが完了し、実稼働環境で使用可能であることが確認できるまで、新規ポリシーでは[導入前]チェック ボックスをオンにすることをお勧めします。

新規スコープ ポリシー 保存 閉じる

全般

フォルダ:
 名前: Win-Admin System Access
 説明:
 カレンダ: <なし>
 リソース クラス名: SafeObject
 タイプ: ☒ アクセス ポリシー
 ☐ アクセス制御リスト
 ☐ ID アクセス制御リスト

☐ 明示的な否認
☐ 無効
☒ 導入前
☒ ラベルの割り当て

ラベル: Win-Admin
 ラベルを追加: +

ユーザまたはグループのどちらかにアクセス権を付与できます。この例では、アクセス権は新規ユーザの Win-Admin に付与されます。

ID

ID の入力/検索
 タイプ: ユーザ ID の検索
 ID: →

選択された ID
 [ユーザ] Win-Admin 🗑️ ▲ ▼

CA Enterprise Log Manager 用に作成された「最高レベルの」ポリシーは CALM アクセス ポリシーで、ここでは CAELM はアプリケーション インスタンスです。このスコープ ポリシーは、アプリケーション オブジェクトである AppObject に対する読み取りアクションを許可するためのものです。AppObject は、すべてのアプリケーション機能を指します。

アクセス ポリシーの設定

リソース	アクション
リソースの追加: ApplicationInstance + ▲ ▼	read (読み取り) write (書き込み) [すべてのアクション]
AppObject 🗑️	☒ ☐ ☐

フィルタを指定すれば、すべてのオブジェクトに対して許可したアクションに、さらに制限を加えることができます。通常、フィルタは 2 つ 1 組で指定します。1 つは、特定の機能に関連するデータが保存された CA EEM フォルダを指定するフィルタで、2 つ目は、その場所にあるオブジェクトへの制限を指定するフィルタです。以下の例における 1 つ目のフィルタは、レポートリソースが保存されたフォルダへの CA EEM フォルダ アクセスを制限しています。具体的には、「pozFolder contains /CALM_Configuration/Content/Reports」と指定されています。2 つ目のフィルタは、calmTag がシステム アクセスと等しいと指定することで、システム アクセス タグの付いたレポートだけにアクセスできるよう制限しています。

ロジック	(	左のタイプ/値	演算子	右のタイプ/値	)
なし	(	指定された属性 pozFolder	STRING CONTAINS *--*	値 /CALM_Configuration/C	
AND		指定された属性 calmTag	STRING EQUAL ==	値 System Access	)

ポリシーを保存したら、確認のために検索できます。ポリシーの検索には、名前、ID またはリソースを使用できます。値の一部だけを入力して検索することも可能です。また、複数の条件も入力できます。このシナリオの例は、以下のとおりです。

フル ネームで検索すると、目的のポリシー 1 つを表示できます。

ポリシーの検索

明示的な許可 明示的な否認

☒ ポリシーと一致する名前を表示します

名前: Win-Admin System Acc

ID のみで検索すると、この ID に適用されるポリシーが、ほかの ID にも適用されるものも含めてすべて表示されます。

ポリシーの検索

明示的な許可 明示的な否認

☐ ポリシーと一致する名前を表示します

☒ ID に一致するポリシーを表示

ID: Win-Admin

リソースが **AppObject** であるポリシーのみを検索すると、ID に読み取り専用または読み取り/書き込みアクセスを許可する、システム提供のポリシーおよびカスタム ポリシーがすべて表示されます。

検索するカスタム ポリシーがポリシー テーブル上に表示されている場合は、フィルタなどの値を確認してください。修正を必要とするものが見つかった場合は、名前リンクをクリックすれば、ポリシーが再表示されて、編集できるようになります。

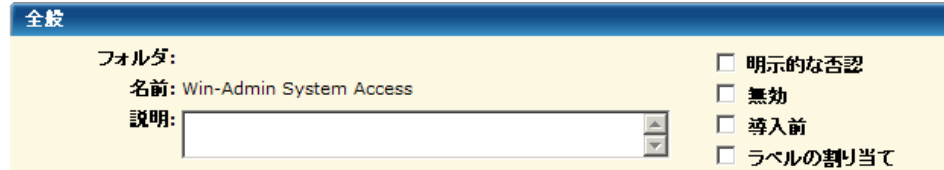
Win-Admin System Access	SafeObject	明示的な許可	Win-Admin	read	AppObject
Win-Admin Report View POI					

新規ポリシーごとにテストを行うことをお勧めします。必ず、レベルの高い属性から、フィルタに入力した順序で、属性と値のペアを入力してください。

結果が **ALLOW** であることを確認します。

権限チェックの結果										すべてクリア
☐ デバッグ情報を表示 ☒ 責任を表示										
チェック時刻	導入前のラベル	結果	ポリシー	委任者	ID	リソースクラス	リソース	アクション	時間	指定された属性
2009年9月29日 3:07:04	Win-Admin	許可	CALM Application Access		Win-Admin	SafeObject	ApplicationInstance	read		pozFolder /CALM_Configuration/Content/Reports calmTag System Access

結果が **ALLOW** であることを確認した後で、ポリシーの[導入前]設定をオフにします。オフにしないと、Win-Admin としてログインし、このユーザに付与した権限を評価できません。



詳細情報:

[新しいポリシーのテスト](#) (P. 105)

手順 4: Win-Admin データ アクセス フィルタの作成

手順 3 で、Win-Admin ユーザはシステム アクセスレポートのみを表示できるよう制限されています。このレベルのアクセスで、Win-Admin ユーザは、ABC 社の 4 つの地域すべてのシステム アクセスレポートを表示することが可能になります。

手順 4 では、Win-Admin ユーザが表示できるデータを、ヒューストンにあるドメインコントローラのシステム アクセスレポートに制限するためのアクセスフィルタを作成します。

データアクセスフィルタの作成は、名前の指定から開始します。このシナリオで使用する名前は、Win-Admin データ アクセスです。



アクセスフィルタに適用される ID を[ID]領域で指定します。フィルタはユーザまたはグループに適用できます。このシナリオでは、このアクセスフィルタは Win-Admin ユーザにのみ適用されます。

[アクセスフィルタ]で、CEG 列の値に関する各条件を定義します。「LIKE」演算子の後ろの値には、以下のワイルドカード文字のどちらかを含めることができます。

- _ (アンダースコア文字) - 任意の 1 文字を表します。
- % (パーセント記号) - 任意の数の文字を含む文字列を表します。

このシナリオの最初のフィルタでは、すべての Windows イベントには NT- というプレフィックスが付けられる規則性を利用します。データを Windows イベントに制限するには、event_logname CEG 列に「NT-%」という文字列を含むデータが入っている必要があることを指定します。さらに、特定のドメインコントローラからの Windows イベントのみを対象にするため、この例では、event_source_hostname に、ローカルの表記規則を使用した文字列を含むデータが入っている必要があることを明示します。値「ABC-HOU-WDC%」は、会社、地域、およびドメインコントローラタイプの接頭辞を示す略語をハイフンでつなぐという命名規則に基づいています。

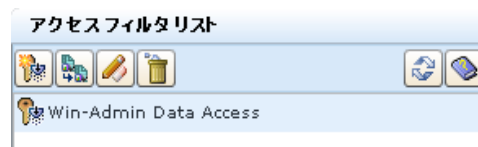
詳細フィルタ			
フィルタコントロールに条件文を定義して、イベントをフィルタします。			
ロジック (	列	演算子	値
	event_logname	Like	NT-%
And	event_source_hostname	Like	ABC-HOU-WDC%

注: 標準化された命名規則を持つイベントソースがない場合は、希望する event_source_hostnames でキー設定済み値リストを作成し、値としてキー設定済み値リスト名を使用できます。

フィルタが 2 つしかなく、論理が **AND** の場合、丸かっこは必要ありません。以下のような複雑な表現を入力する場合に、丸かっこが必要になります。

```
(event_logname like NT-%
And event_source_hostname=ABC-%)
Or (event_logname like CALM-%
And event_source_hostname=XYZ-%)
```

データアクセスフィルタを保存すると、その名前がアクセスフィルタリストに表示されます。



Win-Admin ユーザ名と一致するポリシーを検索すると、すべての ID 用の 3 つのポリシーに加え、さらに 3 つのポリシーとして、Win-Admin が追加された CALM アプリケーションアクセスポリシー、ゼロから作成した Win-Admin システムアクセスポリシー、およびユーザがアクセスフィルタを定義すると自動的に追加されるデータポリシーが表示されます。データポリシーは、以下のように、リストの最初に表示されます。責任ポリシーの下に表示することもできます。CA Enterprise Log Manager で直接、責任ポリシーを作成することはありません。

名前/説明	ResourceClassName	オプション	ID	アクション	リソース
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	明示的な許可	ug:Administrator ug:Analyst ug:Auditor Win-Admin	read write	ApplicationInstance Policy User GlobalUser
d70238aa-caelm634ad71aa7-949d3bf0-a ラベル: DataPolicy	SafeObligation	明示的な許可	Win-Admin	FulfillOnGrant	dataaccess/CALM/Data
Win-Admin System Access ラベル: Win-Admin	SafeObject	明示的な許可 導入前	Win-Admin	read	AppObject

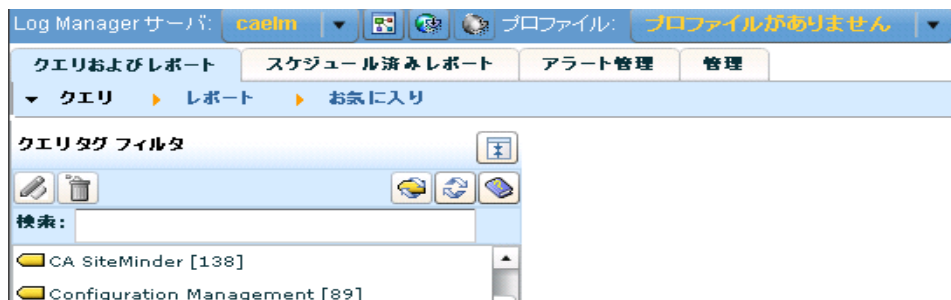
詳細情報:

[アクセスフィルタの作成](#) (P. 108)

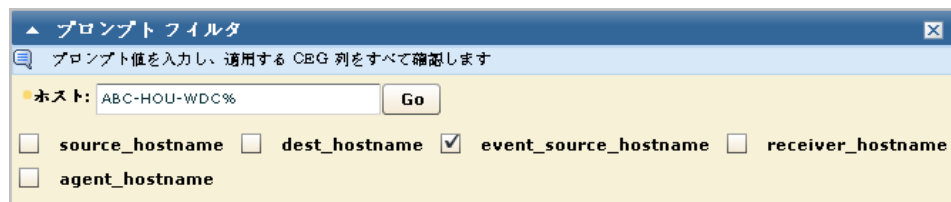
手順 5: Win-Admin ユーザとしてのログオン

特定のユーザまたは特定のアプリケーション ユーザ グループのポリシーを作成する前に、そのユーザまたはグループ メンバとして実際にログオンし、実行可能なこととそうでないことを判別します。最初に、制限が期待どおり適切に動作していることを確認します。次に、対象ユーザが実行可能であるべきタスクを実行できることを確認します。

このシナリオでは、「システム アクセス」のタグが付いたレポートまたはアクションアラートのみを表示しようとしていると想定します。例では、使用可能なクエリタグフィルタは、「システム アクセス」だけです。このため、期待どおりであることが確認されます。



アクセスフィルタを短時間でテストするには、プロンプト機能を使用します。ただし、この機能は Win-Admin ユーザには使用できません。すべてのプロンプトクエリには、「イベントビューア」のタグが付いています。プロンプトフィルタへのアクセス権は、ポリシー フィルタ「calmTag=イベントビューア」を使用して付与することができます。



アクセスフィルタをテストする最良の方法は、レポートに表示されているデータの確認です。次のようなアクセスフィルタについて考えます。

[event_logname] CEG 列が「NT」から始まり、[event_source_hostname] CEG 列が「ABC-HOU-WDC」（ABC 社、場所がヒューストン、Windows ドメイン コントローラの略語）から始まる。

```
event_logname Like NT-% AND event_source_hostname Like ABC-HOU-WDC%
```

Custom Access All Events

Analyst Auditor	SafeObject	顯示的允許	ug:Analyst read	AppObject

Win-Admin がレポートを作成できるようにするには、Win-Admin システム アクセス ポリシーに書き込みアクセス権を追加する必要があります。これを行うには、Win-Admin システム アクセス ポリシーを開いて編集し、許可されたアクションに「書き込み」を追加する必要があります。

Win-Admin System Access Win-Admin Report View POI	SafeObject	 明示的な許可	Win-Admin	read	AppObject

Win-Admin がプロンプトを使用できるようにするには、Win-Admin システム アクセス用のフィルタを変更し、属性「calmTag」が「システム アクセス」か「イベントビューア」のどちらかと等しくなるように指定します。

フィルタ					
ロジック	(	左のタイプ/値	演算子	右のタイプ/値	)
なし		指定された属性 pozFolder	STRING CONTAINS *--*	値 /CALM_Configuration/C	
AND	(	指定された属性 calmTag	STRING EQUAL ==	値 System Access	
OR		指定された属性 calmTag	STRING EQUAL ==	値 Event Viewer	)

ロールのアクセス制限: PCI-Analyst シナリオ

事前定義済みロールに類似したロールを作成し、事前定義済みポリシーをベースとしたポリシーを短時間で作成できます。ユーザ定義ロールが、同じリソースタイプに対して同じアクセスを提供するという点では事前定義済みロールに似ている一方、事前定義済みロールにないフィルタに基づいてアクセスを制限するという点で異なっているという場合があります。この事前定義済みロールが ID として追加されているポリシーが複数存在することがあります。新しいロールに適用する目的でいずれかのポリシーを設定する場合は、既存のポリシーに新しいロールを追加することができます。設定に、タイプ、リソース、アクション、またはフィルタの変更が必要な場合は、既存ポリシーのコピーから新規ポリシーを作成できます。

この例では、PCI タグが付いたレポートをのみを利用する **Analyst** ロールの作成方法について、順を追って説明します。このロールの関連ポリシーは、すべての **Analyst** に適用される既存ポリシーのコピーから作成します。

プロセスには、以下の手順が含まれます。

1. 必要とするポリシーを計画します。まず、新規ロールで活用する既存ポリシーを特定します。
2. 新規アプリケーション ユーザ グループ(ロール)として、**PCI -Analyst** を作成します。
3. **PCI-Analyst** に **CA Enterprise Log Manager** への基本的なアクセス権を付与します。**CALM** アプリケーション アクセス ポリシーにこの ID を追加します。
4. **PCI-Analyst** に、**Analyst** が持っているのと同じレポート サーバへのアクセス権およびレポート作成機能を付与します。特定したポリシーに **PCI-Analyst** の ID を追加します。
5. **PCI calmTag** のタグが付いたレポートのみにアクセスできるよう制限します。レポートを表示および編集する機能を許可するポリシーをテンプレートとして使用して、レポートを変更します。
6. **PCI-Analyst** ロールを評価用のテスト ユーザに割り当てます。
7. テスト ユーザとしてログインし、アクセスを評価します。

ロールとポリシーによって許可されたアクセスが、期待どおりであれば、PCI レポートの分析を行う全ユーザにこのロールを割り当てます。

手順 1: 作成するロールとポリシーの計画

Analyst と同様のロールを作成する必要があり、同時に PCI 関連のレポートおよびクエリへのアクセスを制限する必要もあると仮定します。機能の内容がわかるロール名 (PCI-Analyst など) を検討します。

新規ロール、すなわちアプリケーション ユーザ グループの作成を開始する前に、新規ロールをサポートするのに必要なポリシーを検討します。テンプレートとして使用できそうな既存ポリシーを特定することをお勧めします。[ID] リストから、検討中のロールと類似したロールを探します。

このシナリオ例では、ug:Analyst がこれに該当します。[ポリシーの検索] で、[ID に一致するポリシーを表示] チェック ボックスをオンにし、ID 「ug:Analyst」を入力して、[実行] をクリックします。表示されるポリシーには、すべての ID に適用されるポリシーと、ID に ug:Analyst が明示的に指定されているポリシーが含まれます。

名前/説明	ResourceClassName	オプション	ID	アクション	リソース
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	明示的な許可	ug:Administrator ug:Analyst ug:Auditor Win-Admin	read write	ApplicationInstance AppObject Policy User GlobalUser
Analyst Auditor Report Server Access Policy Analyst Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	明示的な許可	ug:Analyst ug:Auditor	read	AppObject
Analyst Create-Schedule-Annotate policy Analyst can create/schedule Reports, create profiles, schedule Action Alerts, Annotate Reports	CALM	明示的な許可	ug:Analyst	create schedule annotate	Report Alert Tag Profile
Analyst Report View-Edit Policy Analyst can View/Edit any Report	SafeObject	明示的な許可	ug:Analyst	read write	AppObject

このロールが含まれているポリシー名は、以下のとおりです。

- CALM アプリケーション アクセス スコープ ポリシー
- 分析担当者および監査担当者用レポート サーバ アクセス スコープ ポリシー
- 分析担当者用レポート表示/編集スコープ ポリシー
- 分析担当者用作成/スケジュール/注釈 CALM ポリシー

候補となる各ポリシーで、定義を検討し、以下の操作からいずれかを選んで実行します。

- 新規ロールを、ポリシーを適用する ID に追加します。変更を加えずにこのポリシーを新規ロールに適用する場合は、これが最適な選択です。

この操作は、この例では以下のポリシーに適しています。

- CALM アプリケーション アクセス ポリシー。CA Enterprise Log Manager へのアクセス権を与える ID をすべて定義します。
- 分析担当者および監査担当者用レポート サーバ アクセス ポリシー。使用可能なすべてのレポート サーバに関するレポートとアラートのスケジュールを許可する ID をすべて定義します。このロールは、レポートサーバに関する制限がないことが必要です。
- 分析担当者用作成/スケジュール/注釈ポリシー

- 新しい名前でポリシーを保存し、定義を変更します。

この操作は、この例では以下のポリシーに適しています。以下のポリシーでは、新規コピーに新しい ID のみが含まれ、「PCI」というタグが付けられたレポートへの読み取り/書き込みアクセスを制限するフィルタが追加されています。

- 分析担当者用レポート表示/編集ポリシー

手順 2: PCI-Analyst ロールの作成

カスタム ロールを作成して、複数のユーザが CA Enterprise Log Manager アプリケーションで実行するタスクをすべて提供することができます。ロールとアプリケーション ユーザ グループは同じものです。

ロールのアクセスを制限するには、最初にロールを作成します。

既存ロールのスーパーセットではないカスタム ロールを作成する場合は、[使用可能なユーザ グループ]を選択しないでください。

全般	
フォルダ:	/UserGroups
名前:	PCI-Analyst
説明:	Role can perform Analyst functions scoped to PCI

詳細情報:

[アプリケーション ユーザ グループ \(ロール\) の作成](#) (P. 92)

手順 3: CALM アプリケーション アクセス ポリシーへの PCI-Analyst の追加

新規ロールを作成したら、次に、このロールに CA Enterprise Log Manager アプリケーションへの基本的なログオン機能を与えます。デフォルトでは、事前定義済みロールにしかログオン アクセス権が与えられていません。CALM アプリケーション アクセス ポリシーにこのアプリケーション グループを追加します。

詳細情報:

[カスタム ロールによる CA Enterprise Log Manager へのアクセスの許可](#) (P. 93)

手順 4: 既存ポリシーへの PCI-Analyst の追加

新規ロールがサブセットになっているアプリケーション ユーザ グループに適用するポリシーを特定したら、新規ロールを現在の ID リストに追加します。

このシナリオの場合は、PCI-Analyst ロールを以下の既存ポリシーに追加します。

- 分析担当者および監査担当者用レポート サーバ アクセス ポリシー
- 分析担当者用作成/スケジュール/注釈ポリシー

詳細情報:

[既存ポリシーへの ID の追加](#) (P. 95)

手順 5: 分析担当者用レポート表示/編集ポリシーをベースにしたポリシーの作成

既存ポリシーを基にポリシーを作成する場合は、既存ポリシーをコピーし、新しい名前で保存します。次に、名前を変更し、新規ロールに合わせて説明を編集して、既存 ID を新しい ID に置き換えます。テンプレートとして使用しているポリシーのアクセス権が、新規作成したロールには範囲が広すぎる場合、アクセス権を制限するためのフィルタを作成します。

この PCI-Analyst シナリオでは、分析担当者用レポート表示/編集ポリシーをコピーして新しい名前で保存してから、この新規ポリシーを開いて ID を PCI-Analyst グループに置き換え、PCI calmTag というタグの付いたレポートだけにアクセスできるようフィルタを追加します。

フィルタ

ロジック	(	左のタイプ/値	演算子	右のタイプ/値	)
なし		指定された属性 pozFolder	STRING CONTAINS *-*	値 /CALM_Configuration/C	
AND		値 calmTag	STRING EQUAL ==	値 PCI	

ポリシーをまったく新しく作成する場合と同じように、既存ポリシーをベースにしたポリシーをテストすることをお勧めします。フィルタを持つポリシーをテストする場合は必ず、ポリシーに入力されたとおり正確にフィルタを入力してください。ID にグループ名を入力する場合は、必ず、ug:PCI-Analyst のように、プレフィックスとして ug: を付加してください。

権限チェックのパラメータ

リソース クラス: SafeObject
 アクション: 書き込み
 リソース: AppObject
 ID: ug:PCI-Analyst

時間:

+ 指定された属性の追加

属性	値	削除
pozFolder	/CALM_Configuration/C	
calmTag	PCI	

権限チェックの実行

権限チェックの結果

☒ デバッグ情報を表示 ☒ 責任を表示

チェック時刻	導入前のラベル	結果	ポリシー	委任者	ID	リソース クラス	リソース	アクション
2009年10月10日 3:29:20		許可	PCI-Analyst PCI Report View-Edit policy		ug:PCI-Analyst	SafeObject	AppObject	write

詳細情報:

[既存のポリシーをベースにしたポリシーの作成](#) (P. 103)

[新しいポリシーのテスト](#) (P. 105)

手順 6: PCI-Analyst ロールへのユーザの割り当て

新規ロールおよびサポート ポリシーを作成したら、このロールを割り当てたユーザでログオンし、設定したアクセス権が必要条件を満たしているかどうか評価することをお勧めします。検証が終わったら、ロールの設計意図であるタスクを実行するすべてのユーザのアカウントに、この新規ロールを追加できます。

新規ロールをテストする目的で一時的なユーザ アカウントを作成し、テスト完了後にこのアカウントを削除できます。または、**Test-User** というユーザを作成しておき、テストのたびに割り当てるロールを変更して再利用することもできます。

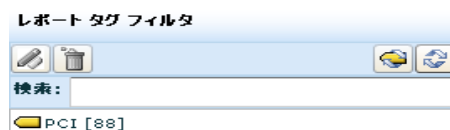
詳細情報:

[グローバル ユーザへのロールの割り当て](#) (P. 43)

手順 7: PCI-Analyst としてのログインとアクセス権の評価

ポリシーが、PCI というタグの付いたレポートおよびアラートへのアクセスを制限できているかどうかを検証します。ユーザに **PCI-Analyst** ロールを割り当て、その新規ユーザとして **CA Enterprise Log Manager** にログインします。

レポートタグを表示します。PCI タグの付いたレポートのみが表示されることを確認します。



レポートをスケジュールします。PCI タグの付いたレポートのみがスケジュールされることを確認します。

レポートの選択

レポートを個別またはタグ別に選択します。

ジョブ名:

選択タイプ: ☒ レポート ☐ タグ

レポート

使用可能なタグ

☒ PCI [88]

レポートを作成します。新規レポートで使用可能なタグが、PCI のみであることを確認します。

レポートの詳細

このレポートの名前、説明を入力し、タグを選択してください

名前:

説明:

タグ

使用可能なタグ

- ☒ Action Alerts
- ☒ Basel II
- ☒ CA Access Control
- ☒ CA Identity Manager
- ☒ CA SiteMinder
- ☒ COBIT

カスタム統合のポリシーの例

1 つのカスタム ロール、1 つの CALM ポリシー、および 1 つのスコープ ポリシーを作成することで、管理者でないユーザーにカスタム統合を作成する権限を与えることができます。関連するスコープ ポリシーを備えた 1 つのカスタム ロールを作成することで、ほかの管理者でないユーザーにカスタム統合を表示する権限を与えることができます。両方のカスタム ロールを CALM アプリケーション アクセス ポリシーに追加し、これらのロールにユーザーを割り当てます。

以下の手順例で、これを実行する方法を示します。

1. 「Create-DM-XMP-Files」というアプリケーション ユーザ グループを作成します。
2. 「View-DM-XMP-Files」というアプリケーション ユーザ グループを作成します。
3. Create-DM-XMP-Files および View-DM-XMP-Files に、CA Enterprise Log Manager 製品 へのアクセス権を付与します。

名前/説明	ResourceClassName	オプション	ID	アクション	リソース
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	明示的な許可	ug:Administrator ug:Analyst ug:Auditor ug:Create-DM-XMP-Files ug:View-DM-XMP-Files	read write	ApplicationInstance AppObject Policy User GlobalUser

4. CA Enterprise Log Manager にログオンし、データ マッピング ファイルおよびメッセージ解析ファイルの作成権限を Create-DM-XMP-Files に付与する CALM ポリシーを、共通イベント文法を使用して作成します。

名前/説明	ResourceClassName	オプション	ID	アクション	リソース
Integration-Create policy Can create data mapping and message parsing files using common event grammar.	CALM	明示的な許可	Create-DM-XMP-Files	create	Integration

5. EEM フォルダ /CALM_Configuration/Content/Mapping または /CALM_Configuration/Content/Parsing に保存されたカスタム DM ファイル および XMP ファイルを編集および表示する権限を Create-DM-XMP-Files に付与するスコープ ポリシーを、共通イベント文法を使用して作成します。

名前/説明	ResourceClassName	オプション	ID	アクション	リソース
Edit-DM-XMP-Files with CEG Policy Can edit data mapping files and message parsing files using common event grammar saved to the EEM folders /CALM_Configuration/Content/...	SafeObject	明示的な許可	Create-DM-XMP-Files	read write	AppObject

フィルタ

WHERE name:pozFolder *--* val:/CALM_Configuration/Content/Mapping
OR name:pozFolder *--* val:/CALM_Configuration/Content/Parsing

6. EEM フォルダ `/CALM_Configuration/Content/Mapping` または `/CALM_Configuration/Content/Parsing` に保存されたカスタム DM ファイルおよび XMP ファイルを表示する権限を `View-DM-XMP-Files` に付与するスコープ ポリシーを作成します。

注: CEG ポリシーを使用すると、共通イベント文法を表示する権限がすべての ID に付与されます。

名前/説明	ResourceClassName	オプション	ID	アクション	リソース
View-DM-XMP-Files Can View data mapping files and message parsing files.	SafeObject	 明示的な許可	View-DM-XMP-Files	read	AppObject

フィルタ

WHERE (name:pozFolder *--* val:/CALM_Configuration/Content/Mapping
OR name:pozFolder *--* val:/CALM_Configuration/Content/Parsing)

7. ポリシーをテストします。
8. `Create-DM-XMP-Files` および `View-DM-XMP-Files` の両方にユーザを割り当てます。

抑制ルールおよび集約ルール用のポリシーの例

1 つのカスタム ロール、1 つの CALM ポリシー、および 1 つのスコープ ポリシーを作成することで、管理者でないユーザーにカスタム抑制ルールおよびカスタム集約ルールを作成する権限を与えることができます。関連するスコープ ポリシーを備えた 1 つのカスタム ロールを作成することで、ほかの管理者でないユーザーにカスタム抑制ルールおよびカスタム集約ルールを表示する権限を与えることができます。両方のカスタム ロールを CALM アプリケーション アクセス ポリシーに追加し、これらのロールにユーザーを割り当てます。

以下の手順例で、これを実行する方法を示します。

1. 「Create-SUP-SUM-Rules」というアプリケーション ユーザ グループを作成します。
2. 「View-SUP-SUM-Rules」というアプリケーション ユーザ グループを作成します。
3. 両方のロールに CA Enterprise Log Manager 製品 へのアクセス権を付与します。

名前/説明	ResourceClassName	オプション	ID	アクション	リソース
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	 明示的な許可	ug:Administrator ug:Analyst ug:Auditor ug:Create-Sup-Sum-Rules ug:View-Sup-Sum-Rules	read write	ApplicationInstance Policy User GlobalUser

4. 抑制ルールおよび集約ルールを作成する権限またはインポートする権限を Create-SUP-SUM-Rules に付与する CALM ポリシーを、CA Enterprise Log Manager にログインして作成します。

名前/説明	ResourceClassName	オプション	ID	アクション	リソース
EventGrouping-Create policy Can create custom summarization and suppression rules or import rules.	CALM	 明示的な許可	Create-Sup-Sum-Rules	create	EventGrouping

5. EEM フォルダ /CALM_Configuration/Content/Rules/Suppression または /CALM_Configuration/Content/Rules/Summarization に保存されているカスタム集約ルールまたはカスタム抑制ルールを表示または編集する権限を Create-SUP-SUM-Rules に付与するスコープ ポリシーを作成します。

名前/説明	ResourceClassName	オプション	ID	アクション	リソース
View-Edit-SUP-SUM-Rules Can view or edit suppression and summarization rules that have been saved to Content/Rules/Summarization or Content/Rules Suppression folders.	SafeObject	 明示的な許可	Create-Sup-Sum-Rules	read write	AppObject

フィルタ	
WHERE	name:pozFolder *--* val:/CALM_Configuration/Content/Rules/Summarization
OR	val:pozFolder *--* val:/CALM_Configuration/Content/Rules/Suppression

6. カスタム集約ルールまたはカスタム抑制ルールを表示する権限を View-SUP-SUM-Rules に付与するスコープ ポリシーを作成します。

名前/説明	ResourceClassName	オプション	ID	アクション	リソース
View-SUP-SUM-Rules Can view suppression and summarization rules that have been saved to Content/Rules/Summarization or Content/Rules Suppression folders.	SafeObject	 明示的な許可	ug:View-Sup-Sum-Rules	read	AppObject

フィルタ	
WHERE	name:pozFolder *--* val:/CALM_Configuration/Content/Rules/Summarization
OR	val:pozFolder *--* val:/CALM_Configuration/Content/Rules/Suppression

7. ポリシーをテストします。
8. 新規ロールにユーザを割り当てます。たとえば、外部監査担当者が集約ルールおよび抑制ルールを表示できるようにする必要がある場合があります。これを許可するには、対象のユーザに View-Sup-Sum-Rules と類似のロールを割り当てることができます。

作成/編集/表示タスクおよび表示のみのタスク用に 2 つの新規ロールを明示的に作成する代わりに、事前定義済みの **Analyst** ロールおよび **Auditor** ロールの適用範囲を拡張できます。たとえば、前の手順の手順 1、2、3、および 8 を割愛し、代わりに、「Analyst」を ID として EventGrouping Create ポリシーおよび View-Edit-SUP-SUM-Rules に割り当て、ユーザグループ「Auditor」を ID として View-SUM-SUP-Rules に割り当てることができます。

詳細情報:

[アプリケーション ユーザ グループ \(ロール\) の作成](#) (P. 92)

[カスタム ロールによる CA Enterprise Log Manager へのアクセスの許可](#) (P. 93)

[新しいポリシーのテスト](#) (P. 105)

[グローバル ユーザへのロールの割り当て](#) (P. 43)

第 5 章：サービスおよび CA アダプタ

このセクションには、以下のトピックが含まれています。

[サービスタスク](#) (P. 148)

[サービスホストの削除](#) (P. 149)

[グローバル設定の編集](#) (P. 149)

[グローバルサービス設定の編集](#) (P. 152)

[ローカルサービスの設定の編集](#) (P. 153)

[サービスの設定](#) (P. 154)

[CA アダプタ環境設定タスク](#) (P. 171)

[システムステータスタスク](#) (P. 178)

サービス タスク

すべての CA Enterprise Log Manager サーバに適用されるグローバル設定を設定できます。2 種類の異なるサービス設定を表示および編集できます。1 つはグローバル サービス設定で、環境内の各サービスの全インスタンスに適用されます。もう 1 つはローカル サービス設定で、選択した個々のサービス ホストのみに適用されます。

注: グローバル設定はグローバル サービス設定とは異なります。前者はすべての CA Enterprise Log Manager サーバの動作を制御し、後者は選択したサービスの動作を制御します。たとえば、すべてのサービスに更新間隔を設定する(グローバル設定)ことや、すべてのレポートサーバにレポート保持ポリシーを設定する(グローバル サービス設定)ことが可能です。

また、サービス設定領域に自己監視イベントを表示することもできます。

使用可能なサービスは以下のとおりです。

- エージェント マネージャ
- アラート サービス
- 関連サービス
- イベント ログ ストア
- インシデント サービス
- ODBC サーバ
- クエリ サービス
- レポート サーバ
- ルール テスト サービス
- サブスクリプション サービス
- システム ステータス

一部のサービスは、サービス名別またはホスト別で表示できます。システム ステータス サービスを使用して、個々の CA Enterprise Log Manager サーバの情報を収集し、管理することが可能です。

詳細情報:

[グローバル サービス設定の編集 \(P. 152\)](#)

[ローカル サービスの設定の編集 \(P. 153\)](#)

サービス ホストの削除

CA Enterprise Log Manager サーバをアンインストールする場合、管理サーバのリポジトリからホスト設定を削除する必要があります。この参照を削除することで、管理サーバの登録済み CA Enterprise Log Manager サーバリストが最新の状態に保たれます。

サービス ホストを削除する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
[サービスリスト]が表示されます。
2. リスト上部の[次の基準でサービスを表示]ダイアログ ボックスで[ホスト]をクリックします。
サービス ホストの展開可能なツリー リストが表示されます。
3. 削除するホストを選択し、[削除]をクリックします。
ホストがリストから削除されます。

重要: ホストを削除する際、警告は表示されません。[削除]をクリックするとホストがただちに削除されるため、削除するホストは十分に確認する必要があります。

グローバル設定の編集

すべてのサービスのグローバル設定を設定できます。有効範囲外の値を保存しようとする、CA Enterprise Log Manager によって、デフォルトの最小値または最大値のどちらか適切なほうに設定されます。設定の一部は相互に依存しています。

グローバル設定の編集方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
[サービスリスト]が表示されます。
2. [サービスリスト]内の[グローバル設定]をクリックします。
[グローバル サービス設定]詳細ペインが開きます。

3. 以下の設定項目のうち、必要なものを変更します。

更新間隔

サーバコンポーネントが設定の更新を適用する間隔を秒単位で指定します。

最小: 30

最大: 86400

セッション タイムアウト

非アクティブ セッションの最大長を指定します。自動リフレッシュが有効に設定されている場合は、セッションはタイムアウトになりません。

最小: 10

最大: 600

自動リフレッシュを許可

レポートまたはクエリを自動リフレッシュできるようにします。この設定により、管理者は自動リフレッシュをグローバルに無効にすることができます。

自動リフレッシュ間隔

レポート表示がリフレッシュされる間隔を秒単位で指定します。この設定は、[自動リフレッシュを許可]の選択に依存します。

最小: 1

最大: 60

自動リフレッシュの有効化

すべてのセッションで自動リフレッシュを設定します。自動リフレッシュはデフォルトでは有効になっていません。

アクション アラートの参照には認証が必要

監査者またはサードパーティ製品にアクション アラート RSS フィードを表示しないようにします。この設定は、デフォルトでは有効になっていません。

デフォルトのレポート

デフォルトのレポートを指定します。

デフォルトのレポートの起動を有効化

[レポート]サブタブをクリックしたときにデフォルトのレポートを表示します。この設定は、デフォルトでは有効になっています。

4. 以下のレポートまたはクエリタグ設定のうち、必要なものを変更します。

レポート タグを隠す

指定されたタグが任意のタグリストに表示されないようにします。レポートタグを非表示にすると、使用可能なレポートのビューを単純化できます。

クエリ タグを隠す

選択されたタグを非表示にします。非表示にされたタグは、メインのクエリリストまたはアクション アラートのスケジュールのクエリリストには表示されません。クエリタグを非表示にすることにより、使用可能なクエリのビューをカスタマイズできます。

5. 以下のダッシュボード設定項目のうち、必要なものを変更します。

デフォルト ダッシュボードの起動を有効化

[クエリおよびレポート] タブをクリックしたときに、デフォルトのレポートを表示します。この設定は、デフォルトでは有効になっています。

デフォルト ダッシュボード

6. 以下のプロファイル設定のうち、必要なものを変更します。

デフォルト プロファイルの有効化

デフォルトプロファイルを設定します。

デフォルト プロファイル

デフォルトプロファイルを指定します。

プロファイルを隠す

選択されたプロファイルを非表示にします。インターフェースがリフレッシュされるか更新間隔が期限切れになると、非表示のプロファイルは表示されなくなります。プロファイルを非表示にすることにより、使用可能なプロファイルのビューをカスタマイズできます。

注: [リセット] をクリックすると、最後に保存した値に戻すことができます。変更を保存するまで、1 回の変更でも複数の変更でもリセットすることができます。変更を保存したら、変更を個々にリセットします。

7. [保存] をクリックします。

グローバル サービス設定の編集

グローバル サービス設定を編集できます。グローバル サービス設定とは、環境内にある特定のサービスのインスタンスすべてに適用される設定です。グローバル サービス設定が、グローバル設定と異なるローカル サービス設定よりも優先されることはありません。

最大設定値および最小設定値については、各サービスのセクションで詳しく説明されています。有効範囲外の値を保存しようとする、**CA Enterprise Log Manager** によって、デフォルトの最小値または最大値のどちらか適切なほうに設定されます。

グローバル サービス設定を編集する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
[サービスリスト]が表示されます。
2. 設定を編集するサービスを選択します。
[グローバル サービス設定]が[詳細]ペインに表示されます。
3. 必要な設定変更を加えます。

注: [リセット]をクリックすると、エントリフィールドを最後に保存された値に戻すことができます。単一の変更でも複数の変更でも、[保存]をクリックした時点までリセットすることができます。変更内容がすでに保存されている場合は、変更を1つ1つ戻す必要があります。

4. 変更が終了したら、[保存]をクリックします。

ホストに異なるローカル設定が定義されている場合を除き、すべての設定変更が、選択したサービスの全ホストに適用されます。

ローカル サービスの設定の編集

ローカル サービスの設定を、サービス別またはホスト サーバ別に表示または編集できます。ローカル サービス設定を使用すると、環境全体には当てはまらない、または必要でないサービスや設定を制御し、特定のホストに対してのみグローバル設定より優先させることができます。たとえば、特定の **CA Enterprise Log Manager** サーバで、ほかのサーバより長い期間アクション アラートの保持が必要になる場合があります。ローカル設定を使用して、これを制御します。

最大設定値および最小設定値については、各サービスのセクションで詳しく説明されています。有効範囲外の値を保存しようとする、**CA Enterprise Log Manager** によって、デフォルトの最小値または最大値のどちらか適切なほうに設定されます。

ローカル サービス設定の編集方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
[サービスリスト]が表示されます。
2. 設定を編集するサービスの横の矢印をクリックします。
サービス表示が展開され、各サービス ホストが表示されます。
3. 目的のサービス ホストをクリックします。
選択したサービス設定が[詳細]ペインに表示されます。
4. 必要な設定変更を加えます。ローカル設定のすべてのエントリ フィールド、メニュー、およびコントロールに、ローカル/グローバル設定ボタンが表示されます。このボタンをクリックすることで、以下の 2 つの状態を切り替えることができます。

グローバル設定: 

ローカル設定: 

ボタンをクリックすると、グローバル設定からローカル設定に切り替わり、関連する値が使用できるようになります。設定が有効になるためには、値がローカル設定用に設定されたままである必要があります。値がグローバル設定用に設定された場合は、そのリスナ用のグローバル設定が有効になります。

注: [リセット]をクリックすると、すべての使用可能な設定に対して、最近保存された設定値が表示されます。単一の変更でも複数の変更でも、[保存]をクリックした時点までリセットすることができます。変更内容がすでに保存されている場合は、変更を 1 つ 1 つ戻す必要があります。

5. 変更が終了したら、[保存]をクリックします。
加えた変更はすべて、選択したサービス ホストにのみ適用されます。

サービスの設定

このセクションでは、以下の **CA Enterprise Log Manager** サービスで設定変更を加える際に確認すべき詳細とサービスのガイドラインについて説明します。

- アラート サービス - アクション アラートの配信設定 (SMTP サーバ、CA IT PAM、および SNMP トラップ設定を含む) を制御します。
- 相関サービス - インシデント作成用の相関ルールおよびイベントルーティングを制御します。
- イベント ログ ストア - 精製および記録済みの元のイベントをすべて格納します。
- インシデント サービス - イベント相関に基づくインシデントの作成および格納を制御します。
- ODBC サーバ - Business Objects の Crystal Reports のような外部アプリケーションから CA Enterprise Log Manager イベント ログ ストアにアクセスできるようにします。
- レポート サーバ - レポートとアラートの配布、フォーマット、および保持を制御します。
- サブスクリプション サービス - コンテンツおよび設定の更新を管理サーバに転送し、バイナリの更新をサブスクリプション クライアントに転送します。

詳細情報:

[サブスクリプション](#) (P. 221)

アラート サービスに関する注意事項

アラート サービスは、アクション アラートの配信を制御します。アラート サービス設定領域では、以下のタスクを実行できます。

- [電子メール設定]領域で、メール サーバ、管理者電子メール、および SMTP のポートと認証情報を設定する
- アクション アラート用の CA IT PAM 統合を設定する
- アクション アラート配信用の SNMP トラップをセットアップする

詳細情報:

[SNMPトラップの宛先との統合の設定](#) (P. 156)

イベント/アラート出力への CA IT PAM 統合の設定

次のいずれかのタイプ、または両方のタイプの CA IT PAM プロセスを活用するように CA IT PAM 統合を設定できます。

- イベント/アラート出力プロセス - サードパーティシステムの処理を呼び出すプロセス
- 動的値プロセス - 入力キーを受け取り、そのキーの現在の値をカンマ区切り値 (*.csv) ファイルとして返すプロセス

以下の手順は、共通の設定、およびイベント/アラート出力に特有の設定の両方に対応します。イベント/アラート出力のために IT PAM 統合を設定する場合は、記録された詳細を参照します。

イベント/アラート出力プロセスのために IT PAM 統合を設定する方法

1. [管理] タブをクリックし、[サービス] サブタブをクリックします。
2. [アラート サービス] をクリックします。
[グローバル サービス設定]: [アラート サービス] ダイアログ ボックスが表示されます。
3. [IT PAM] 領域までスクロールします。
4. CA IT PAM がインストールされているサーバの完全修飾ホスト名を入力し、デフォルトポート番号 8080 を受け入れ、CA IT PAM の有効なログイン認証情報を入力します。
5. サンプルの EventAlertOutput.xml を使用するためにインポートした場合は、[イベント/アラート出力プロセス] のデフォルト エントリを受け入れます。このサンプルをインポートしていない場合は、このエントリを、パス名が前に付いているカスタムのイベント/アラート出力プロセスの名前に置換します。

注: IT PAM クライアントの [フォルダ] の下に、プロセスの [名前] と [パス] を表示できます。

6. サンプルの **EventAlertOutput.xml** を使用するためにインポートした場合は、**ReportedBy**、**Severity**、**Priority**、および **EndUser** のデフォルト値を次のように定義します。
 - a. パラメータを選択し、[デフォルト値の追加]をクリックします。
[値の追加]ダイアログ ボックスが表示されます。
 - b. デフォルト値を入力し、[OK]をクリックします。
7. カスタムのイベント/アラート出力プロセスを指定した場合は、表示されたパラメータを削除し、独自のパラメータを追加します。その後でそれぞれのデフォルト値を定義します。
8. [保存]をクリックします。
「確認: 設定の変更が正常に保存されました」というメッセージが表示されます。

SNMPトラップの宛先との統合の設定

レポートサーバのグローバル サービス設定の一部として、**SNMP 統合**を設定します。設定には **1** つの **SNMP**トラップの宛先の **IP** アドレスとポートが含まれます。

CA Enterprise Log Manager から **SNMP**トラップを受信し解釈できるように宛先製品の準備を行う前後に、**SNMP 統合**を設定できます。

SNMPトラップの受信者用のアラートを作成する場合、**1** つ以上の宛先を指定できます。この設定はデフォルトの設定となります。このデフォルト設定は、レポートサーバでリスト表示されるすべてのサーバに適用されます。

SNMP 統合を設定する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [アラート サービス]をクリックします。
[グローバル サービス設定]:[アラート サービス]ダイアログ ボックスが表示されます。
3. [SNMP 設定]領域までスクロールします。
4. **SNMP**トラップの宛先サーバのホスト名の **IP** アドレスを入力します。
5. デフォルトのポート「**162**」を使用するか、この値を変更します。
6. [保存]をクリックします。

関連サービスに関する注意事項

関連サービスは、関連サーバ上で適用される関連ルールを制御します。このサービスは、ユーザがルールを適用するときにアクティブになります。

関連サービスの設定ページで、通知の宛先とルールを関連付け、ルールを有効化または無効化できます。選択した関連サーバにイベントをルーティングする CA Enterprise Log Manager サーバを選択したり、イベント制限値を設定したりできます。

イベント制限値

累積が有効な場合に、1つのインシデント当たりいくつかのイベントが保持されるかを定義します。イベント制限値によって、アクティビティが多い時期における関連によって引き起こされる不適当なトラフィックを防ぐことができます。この制限に達すると、それ以上のイベントは失われます。たとえば、制限が 100 に設定されている場合、1つのルールに 100 までのイベントを記録して累積することができます。これには、最初の認証イベントも含まれます。イベント制限に達するまで累積は続行されます。通常は、上限値または制限値によってルールがリセットされます。

また、適用される関連ルールを削除して非アクティブにすることも可能です。

適用されるリストからルールを削除する方法

1. 削除する関連ルールの行を強調表示します。
2. (オプション) Ctrl キーを押しながらクリックするか、Ctrl キーを押しながら Shift キーを押すことによって複数の行を選択できます。
3. [削除]をクリックします。

強調表示されたルールがアクティブなリストから削除されます。

4. [保存]をクリックして設定を確認します。保存していない場合は、[リセット]をクリックして、削除したルールをリストに戻すことができます。

注: この手順では、関連ルールはアクティブなリストから削除されるだけです。それらはルールライブラリから削除されません。

イベント ログ ストアに関する注意事項

イベント ログ ストアは、連携されたイベント ログ ストア システムを使用します。このシステムでは、各ホスト サーバが自身のローカル イベント ログ ストアを管理しつつ、環境内のほかのイベント ログ ストアと連携することが可能です。サーバにイベント情報のクエリを実行する際には、自身のローカル イベント ログ ストアに加えて、連携によって接続しているほかのすべてのイベント ログ ストアも検索することが可能です。この連携によって、柔軟なストレージとイベント データのアーカイブが可能となっています。

イベント ログ ストアのアーカイブ設定では、データをアーカイブする頻度および保存する場所を指定できます。ホット(アクティブ) イベント ログ ストアおよびウォーム(アーカイブされた) イベント ログ情報の両方にクエリが実行されます。コールド ストレージ(リモート)内のイベント情報にクエリは実行されません。

以下のイベント ログ ストアおよびアーカイブに関する値を設定できます。

最大行数

イベント ログ ストアのホット データベースに含めることができるイベントの最大数を設定します。イベント数がこの値に達すると、イベント ログによってホット データベース内のすべてのイベント情報が圧縮され、ウォームデータベースに移動されます。

最小: 50000

最大: 100000000

最大アーカイブ日数

アーカイブ済みファイルが、削除されるまでにアーカイブ内で保持される日数を設定します。

最小: 1

最大: 28000

アーカイブ ディスク領域

最も古いアーカイブ ファイルの自動削除が開始されるディスクの空き領域の割合を定義します。たとえば、デフォルト値は **10** です。使用可能なイベント ログ ストア領域が **5** パーセント未満になると、領域を増やすために、イベント ログによって最も古いアーカイブ ファイルが削除されます。

最小: 10

最大: 90

ポリシーのエクスポート

外部のバックアップ元からアーカイブに復元された(解凍済み)ファイルが、削除されるまでにイベントログストア内に保持される時間数を定義します。

最小: 0

最大: 168

集約/抑制ルール

使用可能な集約ルールまたは抑制ルールのうち、どれを受信したイベントに適用するかを制御します。ルールによるイベントの分析を開始する前に、管理者は、新しい集約ルールまたは抑制ルールを適用する必要があります。

転送ルール

使用可能なイベント転送ルールのうち、どれを受信したイベントに適用するかを制御します。

連携の子

使用可能なイベントログストアのうち、どれを現在のサーバの子として設定するかを制御します。これによって、連携の「ツリー」を個別に設定し、クエリのアクセスレベルを制御することができます。この設定は、ローカル設定としてのみ使用できます。

ログ記録関連の設定値は、個々の CA Enterprise Log Manager モジュールによる内部メッセージの記録方法を制御します。これらは、ローカル設定としてのみ使用できます。ログ記録関連の設定値は通常、トラブルシューティングの目的で使用されます。通常、これらの設定を変更する必要はありません。変更する場合は、ログファイルとログ記録について十分に理解する必要があります。

ログレベル

ログ記録ファイルに記録される詳細情報のタイプおよびレベルを定義します。ドロップダウンリストは、詳細さのレベル順に並んでおり、最も詳細でない選択肢が最初に、最も詳細な選択肢が一番下になっています。

すべてのロガーに適用

ログレベル設定が、ログのプロパティファイルによるすべてのログ設定より優先されるかどうかを制御します。この設定は、ログレベル設定がデフォルト設定より低い(より詳細に表示される)場合にのみ適用されます。

自動アーカイブ設定は、スケジュール済みデータベースアーカイブジョブを有効にし、制御します。これによって、ウォームデータベースがリモートサーバへと移されます。

注: スケジュール済みデータベースジョブをある CA Enterprise Log Manager サーバから別のサーバまたはリモートサーバに移動する前に、これらのサーバ間で非対話型の認証を設定しておく必要があります。詳細については、「CA Enterprise Log Manager 実装ガイド」の非対話型の認証の設定に関するセクションを参照してください。

以下の自動アーカイブ値を設定できます。

有効

自動アーカイブジョブを実行するように設定します。自動アーカイブは、ほかの設定によって制御される scp ユーティリティを使用します。

バックアップタイプ

バックアップタイプを制御します。完全アーカイブはデータベース情報をすべてコピーします。増分アーカイブはまだバックアップされていないデータベースをすべてコピーします。

デフォルト: 増分

間隔

アーカイブジョブを日単位で実行するか時間単位で実行するかを指定します。日単位ジョブは、[開始時間]で設定した時間に実行されます。時間単位ジョブは、毎正時に実行されます。

開始時間

毎日のアーカイブジョブが実行される時間を、サーバの現地時間に基づいて、正時単位で設定します。値は 24 時間形式です。

制限: 0 ～23 の範囲で設定し、0 は午前 0 時を、23 は午後 11 時を表します。

EEM ユーザ

アーカイブ クエリの実行、アーカイブ データベースのカatalog再作成、LMArchive ユーティリティの実行、および検査用にアーカイブ データベースを復元する `restore-ca-elm` シェル スクリプトの実行が可能なユーザを指定します。このユーザには、事前定義済みの **Administrator** ロール、またはデータベースリソースへの編集アクションを許可するカスタム ポリシーに関連付けられたカスタム ロールが割り当てられている必要があります。

デフォルト: ログ マネージャ管理者ユーザ

EEM パスワード

EEM ユーザ フィールドで定義された権限を持つユーザのパスワードを指定します。

リモート サーバ

自動アーカイブ ジョブによるデータベース情報のコピー先となるリモートサーバのホスト名または IP アドレスを指定します。

リモート ユーザ

リモートサーバに接続するために `scp` ユーティリティが使用するユーザ名を指定します。

デフォルト: `caelmservice`

リモート ロケーション

リモートサーバ上のアーカイブ ファイルの宛先を指定します。

デフォルト: `/opt/CA/LogManager`

リモート ELM サーバ

リモートサーバを管理サーバとするかどうかを指定します。リモートサーバが管理サーバの場合、コピーが完了すると、リモートマシンに自身のカタログを再作成するよう通知した後、ローカル マシンでは自動アーカイブ ジョブによってデータベースが削除されます。

関連イベント受信スパン

インシデント作成の許容可能な時間差異を定義します。2 つの値を使用して、現在の CA Enterprise Log Manager サーバ時間の後(将来)の値と、現在の CA Enterprise Log Manager サーバ時間の前(過去)の値を設定します。イベントがこの時間枠の外にある場合、そのイベントは関連用として転送されません。

詳細情報:

[ログ ストレージ](#) (P. 183)

[抑制ルールまたは集約ルールの適用](#) (P. 520)

インシデント サービスに関する注意事項

選択した CA Enterprise Log Manager サーバについて、インシデント サービスがイベントを格納し、インシデントを作成する方法を制御できます。以下の値を設定できます。

有効期限

サービスがインシデント データベース内のインシデントを保持する日数を指定します。値が 0 の場合、イベントは削除されません。期限切れになったインシデントは表示されません。

インシデント生成制限

単一の相関ルールがインシデントを作成する頻度を指定して、不要なインシデントを減らします。インシデント生成制限の目的のため、ルールの異なるバージョンは別個のルールと見なされます。したがって、環境内にルールの複数のバージョンを適用した場合は、それらは個別に制限されます。制限値は以下のとおりです。

有効

インシデント生成制限が適用されるかどうかを示します。

カウント

単一のルールによって生成されるインシデント数のしきい値を設定します。値が 0 より大きい場合、この値は[時間]値と一緒に機能します。指定された数に達すると、インシデント サービスは[ブロックされた時間]制限値を適用します。したがって、[カウント]を 3 に設定し、[時間]を 10 に設定した場合は、単一のルールが 10 秒内に 3 つを超えるインシデントを生成した後に制限が適用されます。

時間

単一のルールによって生成されるインシデント数のしきい値を秒単位で設定します。値が 0 より大きい場合、この値は[カウント]値と一緒に機能します。指定された数に達すると、インシデント サービスは[ブロックされた時間]制限値を適用します。したがって、[カウント]を 3 に設定し、[時間]を 10 に設定した場合は、単一のルールが 10 秒内に 3 つを超えるインシデントを生成した後に制限が適用されます。

ブロックされた時間

ルールによるインシデントの作成をブロックする期間を秒単位で指定します。この制限に達すると、期間が経過するまでルールはインシデントを作成しません。

ODBC サーバの注意事項

SAP Business Objects の Crystal Reports のような外部アプリケーションから CA Enterprise Log Manager イベント ログ ストアにアクセスするには、ODBC クライアントまたは JDBC クライアントをインストールします。

この設定領域では、以下のタスクを実行できます。

- ODBC および JDBC によるイベント ログ ストアへのアクセスを有効にします。
- ODBC または JDBC クライアントと CA Enterprise Log Manager サーバの間の通信に使用されるサービス ポートの設定。
- ODBC または JDBC クライアントと CA Enterprise Log Manager サーバの間の通信を暗号化するかどうかの指定。

フィールドの説明は以下のとおりです。

[サービスの有効化]

ODBC と JDBC のクライアントがイベント ログ ストアのデータにアクセスできるかどうかを示します。このチェック ボックスをオンにすると、外部からのイベントへのアクセスが有効になります。外部からのアクセスを無効にするには、チェック ボックスをオフにします。

現在、ODBC サービスは FIPS と互換性はありません。FIPS モードで実行する場合は、ODBC および JDBC のアクセスを無効にするために、このチェック ボックスをオフにします。これによって、非準拠の場合はアクセスできなくなります。FIPS モードでの操作向けに ODBC サービスおよび JDBC サービスを無効にする場合、この値を連携内の各サーバに設定したことを確認してください。

[サーバリスニング ポート]

ODBC サービスまたは JDBC サービスで使用するポート番号を指定します。デフォルト値は 17002 です。Windows のデータ ソースまたは JDBC の URL 文字列に異なる値が指定された場合、CA Enterprise Log Manager サーバは接続の試行を拒否します。

[暗号化 (SSL)]

ODBC クライアントと CA Enterprise Log Manager サーバの間の通信に暗号化を使用するかどうか示します。Windows のデータ ソースまたは JDBC の URL 文字列の対応する値がこの設定と一致しない場合、CA Enterprise Log Manager サーバは接続の試行を拒否します。

[セッション タイムアウト (分)]

自動的に終了する前に、アイドル セッションを開いておく時間 (分) の長さを指定します。

ログ レベル

ログ記録ファイルに記録される詳細情報のタイプおよびレベルを定義します。ドロップダウンリストは、詳細さのレベル順に並んでおり、最も詳細でない選択肢が最初になっています。

すべてのロガーに適用

ログレベル設定が、ログのプロパティファイルによるすべてのログ設定より優先されるかどうかを制御します。この設定は、ログレベル設定がデフォルト設定より低い (より詳細に表示される) 場合にのみ適用されます。

レポート サーバに関する注意事項

レポートサーバは、自動配信レポートの管理、それらのレポートの PDF 形式のレイアウト、およびアクション アラートとレポート保持を制御します。レポートサーバ設定領域では、以下のタスクを実行できます。

- [レポート設定] 領域に、会社名とロゴ、フォント、およびその他の PDF レポート設定を設定する。
- [アラート保持] 領域に、保持される全アクション アラートおよび保持される日数を設定する。

最大アクション アラート数

レポートサーバがレビュー用に保持するアクション アラートの最大数を定義します。

最小: 50

最大: 1000

アクション アラート保持

アクション アラートが保持される日数を定義します。最大日数まで保持されます。

最小: 1

最大: 30

- [レポート保持] 領域に、スケジュール済みレポートの反復タイプごとに保持ポリシーを設定する。

- 保持ユーティリティがレポートを検索し、保持ポリシーに基づいて自動的に削除するかどうか、削除する場合はその頻度を設定する。たとえば、レポート保持ユーティリティを日単位で実行する場合、指定した最長有効期間を過ぎたレポートが日単位で削除されます。

ルールのテスト サービスに関する注意事項

ルールのテスト サービスは、CA Enterprise Log Manager で関連ルールがどのようにテストされるかを制御します。以下のルールのテスト値を設定できます。

イベント制限値

累積が有効な場合に、1つのインシデント当たりいくつのイベントが保持されるかを定義します。イベント制限値によって、アクティビティが多い時期における相関によって引き起こされる不適当なトラフィックを防ぐことができます。この制限に達すると、それ以上のイベントは失われます。たとえば、制限が 100 に設定されている場合、1つのルールに 100 までのイベントを記録して累積することができます。これには、最初の認証イベントも含まれます。イベント制限に達するまで累積は続行されます。通常は、上限値または制限値によってルールがリセットされます。

同時実行のルールのテスト最大数

1つの CA Enterprise Log Manager サーバ上で同時に実行できるルールテストの数を定義します。

サブスクリプションに関する注意事項

プロキシ/クライアント サーバ システムによってサブスクリプション更新が提供されます。インストールする最初のサーバは、デフォルトのサブスクリプションプロキシサーバとして設定され、CA サブスクリプションサーバに定期的に接続し、更新がないか確認します。以降にインストールしたサーバは、そのプロキシサーバのクライアントとして設定され、プロキシサーバに定期的に接続して更新を確認します。接続に失敗した場合は、自己監視イベントがログに記録されます。

デフォルトのシステムを使用すれば、各サーバが CA サブスクリプションサーバに直接接続する必要がなくなり、ネットワークトラフィックが軽減されますが、すべてを設定することも可能です。必要に応じて、プロキシサーバを追加できます。

また、オフラインプロキシサーバを作成することによってインターネットトラフィックをさらに低減できます。オフラインプロキシサーバには更新情報が格納され、クライアントが接続したときにその情報が提供されます。オンラインプロキシのダウンロードパスにあるすべての要素をオフラインプロキシサーバのダウンロードパスに手動でコピーして、すべてのオフラインプロキシサーバをサポートします。オフラインプロキシは、インターネットまたはインターネット接続されたサーバにアクセスできない CA Enterprise Log Manager サーバが存在する環境に設定する必要があります。

サブスクリプション サービスを設定する際は、特定の設定値とそれらの相互作用に関する以下の情報を考慮してください。

デフォルトのサブスクリプション プロキシ

サブスクリプション サービス用のデフォルトのプロキシ サーバを定義します。デフォルトのサブスクリプション プロキシは、インターネットにアクセスする必要があります。ほかにサブスクリプション プロキシが定義されていない場合、このサーバは、CA サブスクリプション サーバからサブスクリプション更新を取得し、すべてのクライアントにバイナリ更新をダウンロードし、CA Enterprise Log Manager ユーザ ストアにコンテンツ更新を配布します。ほかのプロキシが定義されている場合は、サブスクリプション プロキシリストが設定されていない場合、または設定されているリストをすべて使用したとき、クライアントが更新を取得するためにこのサーバに接続します。デフォルト値は、お使いの環境にインストールされた最初のサーバです。この値は、グローバル設定としてのみ使用できます。

公開鍵

更新に署名する際に使用されるシグネチャをテストおよび検証するために使用する鍵を定義します。公開鍵/秘密鍵のペアが更新されると、公開鍵値に対する更新がプロキシによってダウンロードされ、プロキシによって公開鍵が更新されます。この値は、グローバル設定としてのみ使用できます。

重要: この値は手動では更新できません。

サブスクリプション プロキシ

ローカル サーバをサブスクリプション プロキシとするかどうかを制御します。[サブスクリプション プロキシ]チェックボックスがオフにされると、サーバはサブスクリプション クライアントになります。

今すぐ更新

選択されたサーバに対してオンデマンド更新サイクルを即座に開始します。オンデマンド更新は、一度に 1 つのサーバに対してのみ実行できます。このオプションはグローバルに使用できません。サブスクリプションプロキシサーバを更新してから、サブスクリプションクライアントを更新します。

オンラインのサブスクリプション プロキシ

ローカルサーバをオンラインサブスクリプションプロキシとするかどうかを制御します。オンラインサブスクリプションプロキシは、インターネットアクセスを使用して、CA サブスクリプションサーバからサブスクリプションの更新を取得し、それらを CA Enterprise Log Manager 環境に配布します。サーバをオンラインサブスクリプションプロキシとして指定するには、[サブスクリプションプロキシ]チェックボックスおよび[オンラインのサブスクリプションプロキシ]オプションの両方をオンにします。この値は、ローカル設定としてのみ使用できます。

オフラインのサブスクリプション プロキシ

ローカルサーバをオフラインサブスクリプションプロキシとするかどうかを制御します。オフラインサブスクリプションプロキシは、オンラインサブスクリプションプロキシから手動のディレクトリコピー (scp を使用) によってサブスクリプション更新を取得するサーバです。オフラインサブスクリプションプロキシは、インターネットにアクセスする必要はありません。サーバをオフラインサブスクリプションプロキシとして指定するには、[サブスクリプションプロキシ]チェックボックスおよび[オフラインのサブスクリプションプロキシ]オプションの両方をオンにします。この値は、ローカル設定としてのみ使用できます。

注: オフラインサブスクリプションの設定に関する重要な情報については、「CA Enterprise Log Manager 管理ガイド」を参照してください。

RSS フィード URL

CA サブスクリプションサーバの URL を定義します。オンラインサブスクリプションプロキシが CA サブスクリプションサーバおよびダウンロードサブスクリプション更新にアクセスする際に、この URL を使用します。

ダウンロード可能なモジュール

CA Enterprise Log Manager 環境に適用するためにダウンロード可能なモジュールを選択できます。[参照]をクリックするとこのダイアログ ボックスを表示されます。選択したモジュールは[モジュール]リストに表示されます。

選択したモジュールは、サブスクリプション更新中に CA サブスクリプションサーバからダウンロードされます。ダウンロードするモジュールは、グローバルレベルで選択できます。デフォルトによって、設定済みのほかのサブスクリプションプロキシも更新中にこれらのモジュールをダウンロードします。また、モジュールのダウンロード先として個々のプロキシサーバおよびクライアントサーバをローカルレベルで選択することもできます。この場合、グローバル設定は無視され、選択したモジュールのみが指定のサーバにダウンロードされます。クライアント用に選択されたモジュールは、クライアントにインストールされた対応するモジュールを更新する際に使用されます。プロキシ用に選択されていないモジュールを選択してクライアント用にダウンロードできます。プロキシは、クライアント用としてモジュールを取得しますが、プロキシ自身にはインストールしません。

注: RSS フィード URL が入力されていない場合は、設定してください。これを設定することによって、システムは RSS フィードを読み込み、次の更新間隔で、ダウンロードする使用可能なモジュールのリストを表示します。

ダウンロード用に選択したモジュール

RSS フィードブラウザダイアログ ボックスで選択されたモジュールが表示されます。デフォルトサブスクリプションプロキシおよび他のすべてのオンラインプロキシは、更新処理中に CA サブスクリプションサーバからこれらのモジュールをダウンロードします。リストに表示されているモジュールは、グローバルレベルのダウンロード対象として選択されたモジュールか、またはローカルレベルで特定のサーバ用に選択されたモジュールです。

HTTP プロキシ サーバ

このサーバが、更新の際に、直接ではなく HTTP プロキシを介して CA サブスクリプションサーバに接続するかどうかを制御します。

使用するプロキシ アドレス

HTTP プロキシの完全な IP アドレスを指定します。

ポート

HTTP プロキシに接続する際に使用するポート番号を指定します。

HTTP プロキシ ユーザ ID

HTTP プロキシに接続する際に使用するユーザ ID を指定します。

HTTP プロキシ パスワード

HTTP プロキシに接続する際に使用するパスワードを指定します。

スケジュール

CA Enterprise Log Manager サーバがサブスクリプション更新を要求する開始時刻および頻度を指定します。このスケジュールに従って、オンライン サブスクリプション プロキシ サーバ(デフォルト プロキシ サーバを含む)は CA サブスクリプション サーバに接続し、プロキシ クライアントはプロキシ サーバに接続します。スケジュールは、すべての CA Enterprise Log Manager サーバを対象としてグローバルに設定できますが、特定のサーバに対して無効にすることもできます。

クライアント更新用サブスクリプション プロキシ

すべてのクライアントまたは選択したクライアントが、製品およびオペレーティング システムの更新のために接続するプロキシをラウンド ロビン方式で設定できます。上矢印/下矢印を使用して、クライアントがサブスクリプション プロキシに接続する順序を制御できます。クライアントは、正常に接続できた最初のプロキシから更新をダウンロードします。設定されたどのプロキシも使用可能でない場合、クライアントはデフォルトのサブスクリプション プロキシに接続します。

コンテンツ更新のサブスクリプション プロキシ

ユーザ ストアにコンテンツ更新を配布する際に使用するプロキシを選択できます。オフライン プロキシかオンライン プロキシを選択できます。この値は、グローバル設定としてのみ使用できます。

注: 冗長性を確保するために、複数のサーバをコンテンツ更新用のサブスクリプション プロキシとして選択することを検討します。

詳細情報:

[更新用の空きディスク領域 \(P. 235\)](#)

[サブスクリプション公開鍵について \(P. 236\)](#)

システム ステータス サービス

システム ステータス サービスを使用して、CA Enterprise Log Manager サーバに関する情報、および CA Enterprise Log Manager サーバを制御するための情報を収集します。個々の CA Enterprise Log Manager サーバのみのシステム ステータスを表示します。すべての設定およびオプションはローカル レベルで適用されます。

システム ステータス サービスでは次のタブが提供されています。

- [管理] - サービスおよびホスト サーバを管理し、サポート診断ファイルを作成します。
- [ステータス] - システム サービスとプロセスのステータスおよびバージョンを確認します。
- [自己監視イベント] - システム ステータスおよびコンポーネント ステータスに関連するイベントを確認します。

詳細情報

[システム ステータス タスク](#) (P. 178)

[サポート診断ファイルの作成](#) (P. 179)

[ホスト サーバの再起動](#) (P. 180)

[ELM サービスの再起動](#) (P. 180)

[サービスのステータスおよびバージョンの確認](#) (P. 181)

[システム ステータスの自己監視イベントの確認](#) (P. 181)

CA アダプタ環境設定タスク

ローカルリスナは、さまざまなタイプの CA アダプタを使用して、特定のタイプのソースからネイティブ イベントを受信および収集します。

2 種類の異なるアダプタ設定を表示および編集できます。

- グローバル設定は、SAPI コレクタのすべてのインスタンスなど、環境内にあるすべての単一アダプタのインスタンスに適用されます。
- ローカル設定は、単一の SAPI コレクタなど、選択した個別のアダプタ ホストに適用されます。

また、各アダプタのグローバル設定領域またはローカル設定領域から、各アダプタ サービスまたはアダプタ ホストの自己監視イベントを表示できます。

詳細情報

[グローバルアダプタ設定の編集 \(P. 172\)](#)

[ローカルアダプタ設定の編集 \(P. 173\)](#)

[アダプタの自己監視イベントの表示 \(P. 174\)](#)

[アダプタステータスの表示 \(P. 175\)](#)

[SAPI サービスに関する注意事項 \(P. 176\)](#)

[iTechnology イベント サービスに関する注意事項 \(P. 178\)](#)

グローバル アダプタ設定の編集

グローバル アダプタ設定を編集できます。グローバル サービス設定とは、環境内にある特定の CA アダプタのインスタンスすべてに適用される設定です。たとえば、お使いの環境内で稼働中のすべての SAPI コレクタに適用される設定を変更できます。グローバル アダプタ設定が、グローバル 設定と異なるローカルアダプタ設定よりも優先されることはありません。

グローバル アダプタ設定を編集する方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [CA アダプタ]フォルダをクリックします。
フォルダが展開され、各アダプタのサブフォルダが表示されます。
3. 設定を編集するアダプタのフォルダを選択します。
[グローバル サービス設定]が[詳細]ペインに表示されます。
4. 必要な設定変更を加えます。

注: [リセット]をクリックすると、設定値が最近保存された状態に復元されます。単一の変更でも複数の変更でも、[保存]をクリックした時点までリセットすることができます。変更内容がすでに保存されている場合は、変更を 1 つ 1 つ戻す必要があります。

5. 変更が終了したら、[保存]をクリックします。

ホストに異なるローカル設定が定義されている場合を除き、ユーザが行ったすべての設定変更が、選択したアダプタの全ホストに適用されます。

ローカル アダプタ設定の編集

ローカル アダプタ設定を表示および編集できます。ローカル アダプタ設定を使用すると、環境全体には当てはまらない、または必要でない設定を制御できます。この設定は、特定のアダプタ ホストにおいてのみ、グローバル設定より優先されます。たとえば、特定の SAPI アダプタ ホストで、待ち受けポートを変更しなければならない場合があります。ローカル設定を使用して、この動作を設定できます。

ローカル アダプタ設定を編集する方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [CA アダプタ]フォルダをクリックします。
フォルダが展開され、各アダプタのサブフォルダが表示されます。
3. 設定を編集するアダプタのフォルダを選択します。
サービス表示が展開され、アダプタ ホストが表示されます。
4. 目的のアダプタ ホストをクリックします。
選択したホスト設定が[詳細]ペインに表示されます。
5. 必要な設定変更を加えます。ローカル設定のすべての値エントリフィールド、メニュー、およびコントロールに、ローカル/グローバル設定ボタンが表示されます。このボタンをクリックすることで、以下の 2 つの状態を切り替えることができます。

グローバル設定: 

ローカル設定: 

ボタンをクリックすると、グローバル設定からローカル設定に切り替わり、関連するエントリフィールドが使用できるようになります。設定が有効になるためには、エントリフィールドがローカル設定用に設定されたままである必要があります。値がグローバル設定用に設定された場合は、そのアダプタのグローバル設定が有効になります。

注: [リセット]をクリックすると、すべての使用可能な設定に対して、最近保存された設定値が表示されます。単一の変更でも複数の変更でも、[保存]をクリックした時点までリセットすることができます。変更内容がすでに保存されている場合は、変更を 1 つ 1 つ戻す必要があります。

6. 変更が終了したら、[保存]をクリックします。
加えた変更はすべて、選択したアダプタ ホストにのみ適用されます。

アダプタの自己監視イベントの表示

各アダプタ サービスホストの自己監視イベントを表示することで、アダプタ サービスのアクティビティを監視し、問題のトラブルシューティングを実行できます。各アダプタのグローバル設定領域またはローカル設定領域から、事前フィルタ済みイベントを表示することができます。

アダプタの自己監視イベントを表示する方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [CA アダプタ]フォルダをクリックします。
フォルダが展開され、各アダプタ サービスのサブフォルダが表示されます。
3. アダプタ サービスのフォルダを選択して、そのサービスの自己監視イベントを表示するか、フォルダを展開してアダプタ ホストを選択し、そのアダプタ ホストの自己監視イベントのみを表示します。
アダプタ設定が[詳細]ペインに表示されます。

4. [自己監視イベント]タブをクリックします。

イベントビューアウィンドウが開き、適切にフィルタされたイベントが表示されます。たとえば、手順 3 で[iTechnology イベントプラグイン]フォルダを選択すると、iTechnology イベントプラグインの全インスタンスの自己監視イベントが表示されます。[iTechnology イベントプラグイン]フォルダ内の特定のホストを選択すると、その特定の iTechnology ホストに関連するイベントだけが表示されます。

注: 連携構造によって、可視化されるイベントを制御できます。連携が設定されていない場合は、選択したホストにかかわらず、ローカル イベントのみが表示されます。

詳細情報

[アダプタステータスの表示](#) (P. 175)

[グローバルアダプタ設定の編集](#) (P. 172)

[ローカルアダプタ設定の編集](#) (P. 173)

アダプタ ステータスの表示

開始時刻、実行中の状態、イベント配信情報と統計など、CA アダプタサービスの現在のステータスを表示できます。iTechnology イベント プラグイン サービスのステータスは表示できません。

アダプタ ステータスの表示方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [CA アダプタ]フォルダをクリックします。
フォルダが展開され、各アダプタ サービスのサブフォルダが表示されます。
3. ステータスを表示するアダプタのフォルダを選択します。
サービス表示が展開され、各アダプタ ホストが表示されます。
4. 目的のアダプタ ホストをクリックします。
選択したホスト設定が[詳細]ペインに表示されます。
5. [ステータス]タブをクリックします。
[ステータス情報]が表示されます。

注: ステータス情報は、ローカル設定パネルにのみ表示されます。

SAPI サービスに関する注意事項

CA Enterprise Log Manager は、CA Audit Submit Application Programming Interface (SAPI) サービスの 2 つのインスタンスを使用します。1 つは SAPI コレクタとして、もう 1 つは SAPI ルータとしてインストールされます。SAPI サービスは通常、既存の CA Audit クライアントおよび統合された製品からイベントを受信する際に使用されます。以下の設定を使用して、SAPI アダプタを設定できます。

リスナの有効化

選択したサービスを有効にします。この設定は、デフォルトでは有効になっています。

SAPI ポート

ポートマップ機能に登録されない場合のために、選択したサービス用の特定のポート番号を設定します。デフォルト値の 0 では、[登録]チェックボックスがオンになっている場合、サービスはランダムに決定されたポートを使用します。

注: ポート番号は、SAPI コレクタと SAPI ルータで異なっている必要があります。同じポートが両方のサービスに対して設定されている場合、2 つ目のサービスは機能しません。

登録

サービスをシステム ポートマップ機能に登録するかどうかを制御します。[登録]をオンにし、[SAPI ポート]フィールドに 0 を入力すると、サービスが開始するたびに、ランダムなポートが選択されます。これは、両方のフィールドのデフォルト設定です。[登録]がオンになっていない場合、SAPI ポートを指定する必要があります。

暗号化キー

CA Audit 環境で非標準の暗号化キーを使用する場合に、暗号化キーを定義します。SAPI アダプタは、受信した SAPI イベントを読み込む際にその非標準の暗号化キーを使用します。

イベントの順序指定

受信された順序と同じ順序でイベントをイベントログストアに送信します。イベントの順序指定が無効の場合、あるイベントがほかのイベントより早く解析されて転送されると、順序が変更されることがあります。イベントの順序指定を有効にすると、イベントキューのサイズが増大し、パフォーマンスに影響を及ぼすことがあります。

イベントの絞り込み

イベント処理キューの最大イベント数を定義し、リソース処理を制御できます。このフィールドに 0 を入力すると、絞り込みは行われません。このしきい値を越えるイベントはソースで保留されます。

キュー当たりのスレッド数

各プロトコルの処理スレッド数を定義します。処理スレッド数を多くすると、イベントの順序指定が無効の場合は処理速度が向上します。イベントの順序指定が有効の場合は、スレッド数は影響しません。処理スレッド数を多くすると、パフォーマンスに影響を及ぼす可能性があります。

暗号文とデータ マッピング

- [暗号文]シャトル コントロールを使用して、受信メッセージを復号化する際にサービスが使用する使用可能な暗号文を指定できます。
- [データ マッピング ファイル]シャトル コントロールを使用して、データ マッピングの際にサービスが使用する使用可能な DM ファイルを指定できます。

ログ記録関連の設定値は、個々の CA Enterprise Log Manager モジュールによる内部メッセージの記録方法を制御します。これらは、ローカル設定としてのみ使用できます。ログ記録関連の設定値は通常、トラブルシューティングの目的で使用されます。通常、これらの設定を変更する必要はありません。変更する場合は、ログ ファイルとログ記録について十分に理解する必要があります。

ログレベル

ログ記録ファイルに記録される詳細情報のタイプおよびレベルを定義します。ドロップダウンリストは、詳細さのレベル順に並んでおり、最も詳細でない選択肢が最初に、最も詳細な選択肢が一番下になっています。

すべてのロガーに適用

ログレベル設定が、ログのプロパティファイルによるすべてのログ設定より優先されるかどうかを制御します。この設定は、ログレベル設定がデフォルト設定より低い(より詳細に表示される)場合にのみ適用されます。

iTechnology イベント サービスに関する注意事項

iTechnology サービスは、iGateway デーモンによって送信されるイベントを制御します。DM ファイル シャトル コントロールを使用して、サービスがイベント マッピングに使用する使用可能なデータ マッピング (DM) ファイルを設定することで、サービスを構成できます。

イベント プラグイン サービスは、主なデータ マッピング ファイルの大部分を含むようにあらかじめ設定されています。

ログ記録関連の設定値は、個々の CA Enterprise Log Manager モジュールによる内部メッセージの記録方法を制御します。これらは、ローカル設定としてのみ使用できます。ログ記録関連の設定値は通常、トラブルシューティングの目的で使用されます。通常、これらの設定を変更する必要はありません。変更する場合は、ログ ファイルとログ記録について十分に理解している必要があります。

ログ レベル

ログ記録ファイルに記録される詳細情報のタイプおよびレベルを定義します。ドロップダウンリストは、詳細さのレベル順に並んでおり、最も詳細でない選択肢が最初に、最も詳細な選択肢が一番下になっています。

すべてのロガーに適用

ログレベル設定が、ログのプロパティファイルによるすべてのログ設定より優先されるかどうかを制御します。この設定は、ログレベル設定がデフォルト設定より低い(より詳細に表示される)場合にのみ適用されます。

システム ステータス タスク

システム ステータス サービスの内部から次の処理を実行できます。

- システム サービスのステータスおよびバージョンを確認します。
- システム コンポーネントおよび使用状況に関連する自己監視イベントを確認します。
- サポート診断ファイルを作成します。
- ELM サービスを再起動します。
- CA Enterprise Log Manager サーバが実行されているホストサーバを再起動します。
- FIPS モードおよび FIPS 非準拠モードでの操作を有効にします。

詳細情報:

[サポート診断ファイルの作成](#) (P. 179)

[ホスト サーバの再起動](#) (P. 180)

[ELM サービスの再起動](#) (P. 180)

[サービスのステータスおよびバージョンの確認](#) (P. 181)

[システム ステータスの自己監視イベントの確認](#) (P. 181)

サポート診断ファイルの作成

選択した CA Enterprise Log Manager サーバで実行しているサービスのステータスおよびバージョンを確認できます。[サポート診断]をクリックすると、CA Enterprise Log Manager で提供された LmDiag.sh スクリプトが実行されます。

このユーティリティによって、CA のサポート担当者に送信できるように、システム情報とログ ファイルが圧縮された .tar ファイルにまとめられます。FTP または別のファイル転送方法を使用してこのファイルを転送することもできます。

注: 結果ファイルの一部の情報(IP アドレス、システム構成、ハードウェアのログ、プロセスのログなど)は、機密情報である場合があります。このファイルを保存および転送する場合は、安全な方法を使用してください。

診断ファイルを作成する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [システム ステータス]エントリを展開します。
3. 特定の CA Enterprise Log Manager サーバを選択します。
[システム ステータス]の[サービスの設定]に、[管理タブ]が表示されます。
4. [サポート診断]をクリックします。
5. 生成された診断ファイルをダウンロードするためのファイルの場所を選択します。

ユーティリティによってファイルが作成され、そのファイルを指定された場所にダウンロードします。ファイルがコピーされると、ユーティリティは自動的に終了します。

ホスト サーバの再起動

選択した CA Enterprise Log Manager サーバで実行しているサービスのステータスおよびバージョンを確認できます。

重要: この機能は、必要時や CA サポートから指示されたときにのみ使用してください。CA Enterprise Log Manager サーバを再起動すると、再起動が完了するまでイベントログの受信、解析、格納が停止します。管理サーバを再起動すると、ほかの関連するサーバの管理用の CA Enterprise Log Manager セッションは、ログアウトしてからもう一度ログインしなおす必要があります。

ホスト サーバを再起動する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [システム ステータス]エントリを展開します。
3. 特定の CA Enterprise Log Manager サーバを選択します。
[システム ステータス]の[サービスの設定]に、[管理タブ]が表示されます。
4. [ホストの再起動]をクリックします。

ELM サービスの再起動

選択した CA Enterprise Log Manager サーバで実行中の ELM サービスを再起動できます。

重要: この機能は、必要時や CA サポートから指示されたときにのみ使用してください。ELM サービスを再起動すると、影響を受ける CA Enterprise Log Manager サーバは再起動が完了するまでイベントログの受信、解析、および格納を停止します。管理サーバを再起動すると、ほかのサーバの現在のセッションおよびほかのすべての CA Enterprise Log Manager セッションは、ログアウトしてからもう一度ログインしなおす必要があります。

ELM サービスを再起動する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [システム ステータス]エントリを展開します。
3. 特定の CA Enterprise Log Manager サーバを選択します。
[システム ステータス]の[サービスの設定]に[管理タブ]が表示されます。
4. [ELM サービスの再起動]をクリックします。

サービスのステータスおよびバージョンの確認

選択した CA Enterprise Log Manager サーバで実行しているサービスのステータスおよびバージョンを確認できます。

ステータスを確認する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [システム ステータス]エントリを展開します。
3. 特定の CA Enterprise Log Manager サーバを選択します。
4. [ステータス]タブをクリックします。

システム ステータスの自己監視イベントの確認

選択した CA Enterprise Log Manager サーバで実行しているサービスのステータスおよびバージョンを確認できます。ステータス メッセージには、プロセッサやディスク使用量、CPU の平均負荷、メモリ使用量、ハードウェア アクセスおよび使用状況に関連するイベントや、その他のイベントが含まれます。

自己監視イベントを確認する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [システム ステータス]エントリを展開します。
3. 特定の CA Enterprise Log Manager サーバを選択します。
4. [自己監視イベント]タブをクリックします。

第 6 章: ログ ストレージ

このセクションには、以下のトピックが含まれています。

[ログ ストレージについて](#) (P. 184)

[イベントログ データベースの状態](#) (P. 186)

[バックアップおよび復元の自動化](#) (P. 189)

[データ整合性検証](#) (P. 190)

[復元用の非対話型認証の設定](#) (P. 194)

[アーカイブ カタログのクエリ](#) (P. 200)

[自動アーカイブ済みファイルの復元](#) (P. 202)

[アーカイブ済みデータベースを復元するための復元スクリプト](#) (P. 203)

[手動によるアーカイブ済みデータベースのバックアップ](#) (P. 205)

[手動による元のイベントログ ストアへのアーカイブの復元](#) (P. 209)

[手動による新規イベントログ ストアへのアーカイブの復元](#) (P. 215)

[LMArchive によるバックアップ/復元の追跡](#) (P. 219)

ログ ストレージについて

CA Enterprise Log Manager によってログ ストレージの 2 つの面を管理できます。

- 各レポート サーバのアーカイブ ディレクトリにあるログ ファイルのデータベースを、リモート ストレージ サーバ上に作成したアーカイブ ディレクトリにバックアップします。リモート ストレージ サーバは、オフサイトに移動するまでアーカイブ 済みデータベースを保持するための一時的な場所です。
- ログ ファイルのデータベースを、リモート ストレージ サーバ上のアーカイブ ディレクトリから、元のレポート サーバまたは復元ポイント サーバ専用として設定した CA Enterprise Log Manager に復元します。復元後は、クエリおよびレポートを使用して内容を確認できます。

以下の 2 つの方法のどちらかで、イベント ログ データベースのバックアップを管理できます。

- (推奨) 自動アーカイブによってウォーム データベースを定期的に CA Enterprise Log Manager レポート サーバからリモート ストレージ サーバに移動するように CA Enterprise Log Manager を設定します。自動アーカイブ プロセスでは、データベースがバックアップされたことが CA Enterprise Log Manager レポート サーバに通知されます。

注: 「CA Enterprise Log Manager 実装ガイド」の「自動アーカイブについて」を参照してください。

- CA Enterprise Log Manager サーバ上のデータベースを手動でバックアップし、オンサイトのストレージ場所にそれらをコピーします。LMArchive ユーティリティによって CA Enterprise Log Manager サーバに通知して、これらのデータベースをバックアップ済みとしてマークします。

オフサイトの保管場所へのバックアップ済みファイルの移動は、復元に必要になったときにネットワークに戻す場合と同様、CA Enterprise Log Manager の外部で実行するタスクです。

アーカイブ カタログにクエリを実行して、復元するデータベース ファイルを特定します。以下の 2 つの方法のどちらかで、必要に応じてデータベースを復元できます。

- 以下の方法のどちらかを使用して、元のレポート サーバにデータベースを復元できます。

- リモートストレージ サーバと元のレポート サーバ間で非対話型の認証を設定する場合は、**restore-ca-elm.sh** スクリプトを実行してアーカイブ データベースを元のレポート サーバに復元します。

復元したファイルには、ウォーム ファイルの有効期間として設定された日数が経過するまで、クエリおよびレポート作成を実行できます。

- アーカイブ データベースを手動でバックアップしている場合は、元の同じアーカイブ ディレクトリにファイルをコピーし、この **CA Enterprise Log Manager** に復元を通知します。LMArchive コマンドライン ユーティリティのオプションを使用して、データベースが復元されたことを **CA Enterprise Log Manager** に通知できます。

復元したファイルには、解凍済みファイルの有効期間として設定された時間数が経過するまで、クエリおよびレポート作成を実行できます。

- 以下の方法のどちらかを使用して、アーカイブされたデータベースを、復元されたイベント ログを調べるための専用の復元ポイント サーバに復元できます。

- リモートストレージ サーバから **CA Enterprise Log Manager** 復元ポイントへの非対話型の認証を設定する場合は、**restore-ca-elm.sh** スクリプトを実行して、アーカイブ データベースを復元ポイントに復元します。

- 非対話型の認証を設定していない場合は、リモートストレージ サーバから復元ポイントサーバのアーカイブ ディレクトリにアーカイブ データベースを手動でコピーします。次に、ログ収集エクスプローラの[カタログ クエリのアーカイブ]で[カタログ再作成]を選択して、この **CA Enterprise Log Manager** に復元を通知します。

この通知の結果、カタログが再構築され、データベース ファイルがクエリおよびレポートで使えるようになります。この使用可能期間は、削除されるまでの経過日数としてウォーム ファイルに設定されている値が、復元されたファイルの日数をどれくらい超えているかに基づいて変化します。このため、ウォーム ファイルの最大期間が、すべての専用復元ポイント上で適切に設定されていることが重要となります。

イベントログ データベースの状態

3 つのサーバ(収集、レポート、およびリモート ストレージ)に自動アーカイブを設定すると、すべてのイベントログ データベースは、ホット、ウォーム、コールドの 3 つの状態に順番に移行します。このアーキテクチャでは、圧縮されていないログのホット データベースは、収集サーバ上にのみ存在します。レポートサーバには圧縮されたウォーム データベースが保存され、リモートストレージサーバにはコールド データベースのみ保存されます。復元シェルスクリプトを使用してコールド データベースを復元すると、復元されてウォーム状態になります。LMArchive ユーティリティを使用して手動で復元すると、データベースが復元されて解凍済みの状態になります。

以下の 4 つのイベントログ ストレージ状態はそれぞれ、未圧縮、圧縮済み、バックアップおよび移動済み、復元済みのデータベースを表しています。

ホット

ホット データベース状態は、収集サーバ(新しく処理されたイベントが挿入されるサーバ)のイベントログ ストア内にある、圧縮されていない単一のデータベースの状態です。圧縮してウォーム データベースにするまでにホット データベースに格納する新規記録の最大数(最大行数)を設定できます。また、自動アーカイブをスケジュールして、収集サーバから設定したレポートサーバに 1 時間おきにウォーム データベースを移動することができます(ホット データベースは、自己監視イベントを挿入するためにレポートサーバ上にも存在します)。

ウォーム

ウォーム データベース状態は、レポート サーバのイベント ログ ストア内に保存されているデータベースの状態です。レポート サーバとリモートストレージサーバ間の自動アーカイブを日単位で設定すると、ウォーム データベースはリモートストレージサーバに移動されるまで保持され、移動後はレポートサーバから自動的に削除されます。レポートサーバとリモートストレージサーバ間に自動アーカイブを設定しない場合、ウォーム データベースは、経過日数が[アーカイブの最大日数]に設定された値に達するか、[アーカイブ ディスク領域]に設定されたしきい値に達するまで保持できます。これらのしきい値のどちらかに達すると、データベースは削除され、状態がコールドに変更されます。自動アーカイブを設定しない場合は、削除される前にウォーム データベースをサードパーティ製のツールを使用して手動でバックアップし、LMArchive ユーティリティを実行して、バックアップおよび移動したデータベースの名前を **CA Enterprise Log Manager** に通知する必要があります。コールド データベースの復元後に `restore-ca-elm.sh` スクリプトまたは[カタログ再作成]ボタンを使用してカタログ再作成を実行すると、ウォーム状態になります。

コールド

コールド データベース状態は、リモートストレージサーバ上のデータベースに適用されます。データベースがリモート管理サーバに自動アーカイブされ、レポートサーバから削除されると、コールド データベースの記録がレポートサーバ上に作成されます。手動で処理する場合は、LMArchive ユーティリティを `-notify arch` オプションを使用して実行すると、コールド データベースの記録が作成されます。レポートサーバのアーカイブ カタログにクエリを実行して、復元するコールド データベースを特定できます。

解凍済み

解凍済みのデータベースとは、アーカイブ ディレクトリに復元された物理的なコールド データベースに適用される状態で、管理者が `-notify rest` オプションを使用して LMArchive ユーティリティを実行し、CA Enterprise Log Manager に復元を通知した後に適用されます。解凍済みデータベースは、[ポリシーのエクスポート]に設定された時間数の間保持されます。

どの状態のデータベースに対してもクエリを実行できます。通常のクエリでは、レポートサーバ上のホット データベースとウォーム データベース、および存在する場合は、解凍済みデータベースからイベント データが返されます。連携クエリでは、ホット データベースを保存する連携された収集サーバなど、連携内のすべてのサーバからイベント データが返されます。アーカイブ クエリでは、レポートサーバ上に存在しないデータベース、すなわちコールド状態のデータベースのリストが返されます。アーカイブ クエリによって表示された物理データベースは、オンサイトストレージ用に使用されているリモートストレージサーバ、またはオンサイトストレージのどちらかに存在します。

詳細情報

[バックアップおよび復元の自動化](#) (P. 189)

[手動によるアーカイブ済みデータベースのバックアップ](#) (P. 205)

[手動による元のイベント ログ ストアへのアーカイブの復元](#) (P. 209)

[手動による新規イベント ログ ストアへのアーカイブの復元](#) (P. 215)

バックアップおよび復元の自動化

バックアップ処理を行うことで、古いデータベースの削除によるデータの紛失を防ぐことができます。アーカイブ済みデータベースをバックアップするための推奨される方法は、自動アーカイブの使用です。自動アーカイブは、アーカイブされたデータベースをサーバのペア間でスケジュールに従って自動転送することです。ソースサーバと宛先サーバ間の自動アーカイブでは、非対話型の認証が必要となります。非対話型の認証では、パスフレーズのない RSA 公開鍵認証を使用します。非対話型の認証および自動アーカイブは、以下の間で設定できます。

- 個々の収集サーバから対応するレポートサーバへ
- 個々のレポートサーバから対応するリモートストレージサーバへ

注: 詳細については、「実装ガイド」を参照してください。

復元プロセスでは、アーカイブされたデータベースを調査のためにリモートストレージから CA Enterprise Log Manager サーバに移動します。アーカイブされたデータベースの推奨される復元方法は、`restore-ca-elm.sh` スクリプトを使用することです。この復元ユーティリティは、アーカイブされたデータベースの転送を自動化します。自動アーカイブ プロセスと同様、`restore-ca-elm.sh` スクリプトは非対話型の認証を使用します。非対話型の認証および復元スクリプトの実行は、以下の間で設定できます。

- リモートストレージサーバから個々の元のレポートサーバへ
- リモートストレージサーバから単一の復元ポイントサーバへ

自動アーカイブは、定期的なスケジュールで実行されるように設定します。復元は、必要に応じて実行します。

データ整合性検証

管理者権限を持つユーザとしてログインしている場合、アーカイブされたデータまたはカタログが再作成されたデータの改ざんを検証できます。検証を行うことにより、アーカイブされたデータのセキュリティを確保し、適用される規制の要件を満たすことができます。CA Enterprise Log Manager は、デジタル署名を使用してデータベースを検証します。データベースが破損している場合、またはそのシグネチャが存在しないか破損している場合は、データ整合性検証によってそのデータベースが改ざんされたと見なされます。

整合性検証は、以下の方法で設定できます。

- データを復元してカタログを再作成するときに自動的に
- 選択したサーバ上でスケジュールされた時間で
- 必要な場合にオンデマンドで

これらの検証の結果は、データ整合性インターフェースから参照できます。改ざんされたデータベースはすべて隔離され、[検疫されたデータベース]リストに表示されます。

詳細情報:

[自動整合性検証の有効化](#) (P. 190)

[データ整合性検証のスケジュール](#) (P. 191)

[データ整合性のオンデマンド検証](#) (P. 191)

[検疫されたデータベースのシグネチャの再生成](#) (P. 192)

自動整合性検証の有効化

データを復元するか、またはカタログを再作成したときにデータ整合性検証が自動的に実行されるように設定できます。

自動データの整合性検証を有効にする方法

1. [管理]タブをクリックし、[サービス]サブタブを展開します。
2. [イベント ログ ストア]ノードを選択してグローバル自動検証を有効にするか、または[イベント ログ ストア]ノードを展開して CA Enterprise Log Manager サーバを選択し、ローカル自動検証を有効にします。
3. [カタログ再作成および復元の整合性検証]を選択します。

データ整合性検証のスケジュール

設定した時間に選択した CA Enterprise Log Manager サーバ上でデータ整合性検証が日単位で実行されるようにスケジュールできます。スケジュールされた整合性検証によって改ざんが検出されたデータベースは、自動的に隔離されます。

データ整合性検証をスケジュールする方法

1. [管理]タブをクリックし、[サービス]サブタブを展開します。
2. [イベントログストア]ノードを選択してグローバル検証を有効にするか、または[イベントログストア]ノードを展開して CA Enterprise Log Manager サーバを選択し、ローカル検証を設定します。
3. [有効]を選択します。
4. (オプション) 選択したサーバから認識できる連携サーバ上でスケジュールされた検証を実行するには、[連携]を選択します。
5. [毎日の開始時刻]を設定します。

データ整合性のオンデマンド検証

データ整合性検証は、選択した CA Enterprise Log Manager サーバ上でいつでも実行できます。

データ整合性のオンデマンド検証を実行する方法

1. [管理]タブをクリックし、[アーカイブ管理]サブタブをクリックします。
2. [データ整合性]フォルダを展開し、検証の実行先となる CA Enterprise Log Manager サーバを選択します。
3. 検証の時間範囲を選択します。
4. (オプション) 選択したサーバから認識できる連携サーバ上で検証を実行するには、[連携]を選択します。
5. [今すぐ検証]をクリックします。

検証されたデータベースのリストが表示されます。検出された不正変更されたデータベースは、赤いアイコンで表示されます。また、それらは検疫されたデータベースリストにも表示されます。

検疫されたデータベースのシグネチャの再生成

検疫されたデータベースのデジタル署名を再生成して、クエリの対象にすることができます。

検疫されたデータベースのシグネチャを再生成する方法

1. [管理]タブをクリックし、[アーカイブ管理]サブタブをクリックします。
2. [データ整合性]フォルダを展開し、検疫されたデータベースが存在する **CA Enterprise Log Manager** サーバを選択します。
3. 右側のペインで、[検疫されたデータベース]タブをクリックします。
4. 再生成するシグネチャの対象となるデータベースを選択します。
5. [シグネチャの生成]をクリックします。

確認のメッセージが表示されます。

キーの循環

アーカイブされたデータベース ファイルのセキュリティを設定するために使用する登録キーを循環させて、セキュリティを強化できます。

登録キーは、データベース ファイルのセキュリティを確保するための暗号化された公開鍵と秘密鍵の組み合わせです。キーを循環させた場合、古い公開鍵は保持されるため、CA Enterprise Log Manager は古い秘密鍵を使用したファイルを検証できます。

登録キーを循環させる方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [データ整合性]フォルダを展開し、[キーの循環]をクリックします。

確認メッセージが表示されます。

キーのインポート

アーカイブされたデータベース ファイルのセキュリティを確保するために使用する登録キーを外部ソースからインポートできます。インポートを使用すると、ほかの古い CA Enterprise Log Manager サーバ、または前のサーバによって使用されていたキーを保持できます。たとえば、公開鍵のバックアップリストをメンテナンスする場合、インポートを実行して、新しく構築された CA Enterprise Log Manager サーバ上で古いデータベース シグネチャを検証できます。

登録キーをインポートする方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [データ整合性]フォルダを展開し、[キーのインポート]をクリックします。
[ファイルのインポート]ダイアログ ボックスが表示されます。
3. インポートする XML キー ファイルを参照し、[OK]をクリックします。
確認メッセージが表示されます。

注: キーは XML 形式のみでインポートできます。

キーのエクスポート

アーカイブされたデータベース ファイルのセキュリティを確保するために使用する登録キーをエクスポートできます。エクスポートを使用すると、キーをバックアップしておき、後で他の CA Enterprise Log Manager サーバにインポートできます。

登録キーをインポートする方法

1. [管理]タブをクリックし、[サービス]サブタブを展開します。
2. [データ整合性]フォルダを展開し、[キーのエクスポート]をクリックします。
[エクスポート]ダイアログ ボックスが表示されます。
3. エクスポート先を選択し、[保存]をクリックします。

復元用の非対話型認証の設定

リモートストレージサーバと宛先サーバの間で非対話型の認証を設定したら、`restore-ca-elm.sh` シェル スクリプトを実行してアーカイブ データベースをオンデマンドで復元できます。復元の場合、リモートストレージサーバがソースであり、レポートサーバの **CA Enterprise Log Manager** または復元ポイント **CA Enterprise Log Manager** が宛先となります。

このプロセスは、宛先がレポートサーバか、専用の復元ポイントかによって若干異なります。

- 専用の復元ポイントを使用する場合は、非対話型の認証を一度設定して、それをすべての復元で使用します。この手順では、必要な所有権を使用して復元ポイント上の `.ssh` ディレクトリを設定し、鍵ファイルに対する権限を設定します。
- リモートストレージサーバから複数のレポートサーバにアーカイブ データベースを復元する場合、各サーバ ペア間で非対話型の認証をセットアップします。鍵のペアは一度作成し、同じペアの公開鍵を各宛先レポートサーバにコピーします。たとえば、リモートストレージサーバから各レポートサーバに公開鍵を `authorized_keys_RSS` としてコピーします。各レポートサーバで、既存の `authorized_keys` ファイルに `authorized_keys_RSS` ファイルを連結します。既存のファイルには、各収集サーバからコピーされた公開鍵が含まれます。

どちらのプロセスでも、リモートストレージサーバが自動アーカイブ用の宛先サーバとして動作するように設定済みであること(そのためには非対話型の認証が必要)を前提としています。準備ができていない場合は、「実装ガイド」の「リモートストレージサーバ上での所有権を備えたディレクトリ構造の作成」を参照してください。

例: リモートストレージから復元ポイントへの認証の設定

専用の CA Enterprise Log Manager サーバをリストア ポイントとして使用すると、非対話型の認証が簡単になります。リモートストアサーバと復元ポイントの間でいったん認証をセットアップすれば、認証用の追加手順を行わずに `restore-ca-elm.sh` スクリプトをすべての復元で使用できます。

ストレージサーバから復元ポイント CA Enterprise Log Manager への非対話型の認証を設定するには、以下の手順を行います。

1. リモートストレージサーバから、RSA 公開鍵/秘密鍵のペアを生成します。公開鍵を `authorized_keys` として復元ポイントの `/tmp` ディレクトリにコピーします。
2. 復元ポイントから、`/opt/CA/LogManager` に `.ssh` ディレクトリを作成し、所有権を `caelmservice` に設定します。`/tmp` ディレクトリから `.ssh` ディレクトリに `authorized_keys` をコピーします。所有権を変更し、`authorized_keys` に対する権限を設定します。
3. リモートストレージサーバと復元ポイントの間で非対話型の認証が正常に設定されたことを検証します。

鍵の生成と公開鍵の復元ポイントへのコピー

リモートストレージサーバから、`caelmservice` ユーザとして RSA 鍵のペアを生成します。次に、復元ポイント CA Enterprise Log Manager の `/tmp` ディレクトリに、公開鍵ファイル `id_rsa.pub` を `authorized_keys` としてコピーします。復元ポイントは、復元されたデータの検査する専用サーバです。

ストレージサーバ上に `/opt/CA/LogManager/.ssh` ディレクトリ構造が存在し、所有権が `caelmservice` ユーザおよびグループに設定されていることを前提としています。このディレクトリには、レポートサーバからコピーされる `authorized_keys` が格納されます。鍵のペアを生成したら、`id_rsa.pub` を `/opt/CA/LogManager/.ssh` ディレクトリに保存します。

リモートストレージから復元ポイントサーバへの認証用の RSA 公開鍵/秘密鍵のペアを生成する方法

1. ストレージに使用されているリモートサーバに、SSH を使用して `caelmadmin` ユーザでログインします。
2. 次のコマンドを使用して、ユーザを `root` アカウントに切り替えます。

`su -`

3. 次のコマンドを使用して、ユーザを **caelmservice** アカウントに切り替えます。

```
su - caelmservice
```

4. **caelmservice** ユーザとして **RSA** 鍵のペアを生成します。

```
ssh-keygen -t rsa
```

5. 以下のプロンプトが表示されるたびに、**Enter** キーを押してデフォルト値をそのまま使用します。

- 鍵を保存するファイルを入力します
(**/opt/CA/LogManager/.ssh/id_rsa**)。
- パスフレーズを入力します (パスフレーズを使用しない場合は空にします)。
- 同じパスフレーズを再度入力します。

6. ディレクトリを **/opt/CA/LogManager** に変更します。

7. 以下のコマンドを使用して、**.ssh** ディレクトリの権限を変更します。

```
chmod 755 .ssh
```

8. **id_rsa.pub** 鍵の保存先である **.ssh** に移動します。

```
cd .ssh
```

9. 公開鍵を **authorized_keys** として復元ポイント サーバの **/tmp** ディレクトリにコピーします。

```
scp id_rsa.pub caelmadmin@<restore_point>:/tmp/authorized_keys
```

公開鍵ファイルの使用準備

復元ポイント サーバで **.ssh** ディレクトリを作成し、所有権を **caelmservice** に設定します。次に、**/tmp** ディレクトリから **.ssh** ディレクトリに **authorized_keys** をコピーします。最後に、公開鍵ファイルの所有権と権限を設定します。

非対話型の認証用の公開鍵を復元ポイント サーバ上で準備する方法

1. **ssh** を使用して、復元ポイント **CA Enterprise Log Manager** サーバに **caelmadmin** としてログインします。
2. ユーザを **root** に切り替えます。
3. ディレクトリを **CA Enterprise Log Manager** ディレクトリに変更します。

```
cd /opt/CA/LogManager
```

4. **.ssh** ディレクトリを作成します。

```
mkdir .ssh
```


5. `.ssh` の所有権を `caelmservice` ユーザおよびグループに変更します。

```
chown caelmservice:caelmservice .ssh
```

6. ディレクトリを `/opt/CA/LogManager/.ssh` に変更します。

7. `authorized_keys` ファイルを `/tmp` から `.ssh` にコピーします。

```
cp /tmp/authorized_keys
```

8. `authorized_keys` ファイルの所有権を `caelmservice` に変更します。

```
chown caelmservice:caelmservice authorized_keys
```

9. `authorized_keys` ファイルに対する権限を変更します。

```
chmod 755 authorized_keys
```

例: ストレージ サーバからレポート サーバへの認証の設定

アーカイブされたデータベースをリモートストレージサーバから元のレポートサーバ(そのデータベースが自動アーカイブされたサーバ)に復元できます。この方法の利点は、CA Enterprise Log Manager アーカイブ データベースのカタログを再作成する必要がないということです。元のレポートサーバは、復元するログファイル データベースをすでに認識しています。複数のレポートサーバが存在する場合は、リモートストレージサーバと各レポートサーバの間で非対話型の認証を設定します。`authorized_keys` ファイルは、レポートサーバの `.ssh` ディレクトリに存在します。この `authorized_keys` ファイルには、そのレポートサーバに自動アーカイブした収集サーバで生成された各鍵 ペアの公開鍵が含まれています。そのため、信頼済み鍵ファイルをサフィックス付きで作成し、元の `authorized_keys` に連結します。

リモートストレージサーバからレポート CA Enterprise Log Manager への非対話型の認証を設定するには、以下の手順を行います。

1. リモートストレージサーバから、以下の操作を行います。
 - a. リモートストレージからレポートサーバへの認証用の RSA 公開鍵/秘密鍵のペアを生成します。
 - b. ストレージサーバからレポートサーバの /tmp ディレクトリに公開鍵を `authorized_keys_RSS` としてコピーします。
2. レポートサーバから、以下の操作を行います。
 - a. `.ssh` から /tmp に現在の `authorized_keys` をコピーします。
 - b. /tmp ディレクトリの `authorized_keys_RSS` を `authorized_keys` ファイルに連結します。
 - c. 連結された `authorized_keys` ファイルを `.ssh` ディレクトリにコピーします。
3. リモートストレージサーバから、サーバ間で非対話型の認証が正常に設定されたことを検証します。
4. リモートストレージサーバとレポートサーバの組み合わせごとに、これらの手順を繰り返します。

鍵の生成と公開鍵のレポートサーバへのコピー

リモートストレージサーバから、`caelmservice` ユーザとして RSA 鍵のペアを生成し、次に、公開鍵を `authorized_keys_RSS` として CA Enterprise Log Manager サーバの /tmp ディレクトリにコピーします。レポートサーバには、通常 `.ssh` ディレクトリに `authorized_keys` ファイルが格納されています。このファイルには、さまざまな収集サーバからの公開鍵を連結したデータが含まれています。この既存の `authorized_keys` ファイルに追加できるように、一意の名前を付けて公開鍵を送信します。

RSA 公開鍵/秘密鍵のペアを生成し、公開鍵をリモートストレージからレポートサーバにコピーする方法

1. `ssh` を使用して、リモートストレージサーバに `caelmadmin` ユーザとしてログインします。
2. ユーザを `root` に切り替えます。
3. 次のコマンドを使用して、ユーザを `caelmservice` アカウントに切り替えます。

```
su - caelmservice
```

4. caelmservice ユーザとして RSA 鍵のペアを生成します。

```
ssh-keygen -t rsa
```

5. 以下のプロンプトが表示されるたびに、Enter キーを押してデフォルト値をそのまま使用します。

- 鍵を保存するファイルを入力します (/opt/CA/LogManager/.ssh/id_rsa)。
- パスフレーズを入力します (パスフレーズを使用しない場合は空にします)。
- 同じパスフレーズを再度入力します。

6. 次のコマンドを使用して、.ssh ディレクトリの権限を変更します。

```
chmod 755 .ssh
```

7. .ssh ディレクトリに移動します。

8. レポートサーバの /tmp ディレクトリに、id_rsa.pub を authorized_keys_RSS としてコピーします。

```
scp id_rsa.pub caelmadmin@<reporting_server>:/tmp/authorized_keys_RSS
```

既存公開鍵ファイルの更新

レポートサーバの /tmp ディレクトリに公開鍵 authorized_keys_RSS をコピーします。次に、既存の公開鍵ファイルを使用するための準備を行います。この準備では、authorized_keys_RSS を authorized_keys に追加します。適切な所有権および権限は、既存の authorized_keys ファイルにすでに設定されています。

authorized_keys に authorized_keys_RSS を追加して適切な場所にコピーする方法

1. ssh を使用して、レポート CA Enterprise Log Manager サーバに caelmadmin としてログインします。
2. ユーザを root に切り替えます。
3. ディレクトリを authorized_keys_RSS が存在する /tmp ディレクトリに変更します。
4. 既存の authorized_keys を .ssh からカレント ディレクトリ /tmp にコピーします。

```
cp /opt/CA/LogManager/.ssh/authorized_keys
```

5. リモートストレージ サーバから公開鍵を含んでいる `authorized_keys` ファイルに公開鍵の内容を追加します。

```
cat authorized_keys_RSS >> authorized_keys
```

6. ディレクトリを `/opt/CA/LogManager/.ssh` に変更します。
7. `authorized_keys` ファイルを `/tmp` からカレント ディレクトリ `.ssh` にコピーします。

```
cp /tmp/authorized_keys
```

アーカイブ カタログのクエリ

クイックまたは詳細フィルタを使用して、コールド (リモートに保存された) データベースのローカル アーカイブ カタログを検索するクエリを作成できます。クエリ結果は、調査を実施するために復元する必要があるバックアップ データベース ファイルを特定するのに役立ちます。

アーカイブ カタログにクエリを実行する方法

1. [管理] タブをクリックし、[アーカイブ管理] サブタブをクリックします。
[アーカイブ エクスプローラ] フォルダ リストが表示されます。
2. [アーカイブのクエリおよびカタログ再作成] フォルダをクリックします。
[アーカイブ クエリ] ダイアログ ボックスが詳細 ペインに表示されます。
3. クエリの期間を選択するか入力します。
4. [フィルタの追加] をクリックし、列を選択して、検索列に値を入力します。複数のフィルタを追加できます。
5. 入力した値を持つログを、クエリを実行する対象から除外する場合は、[除外] チェック ボックスをオンにします。

注: カタログにない列を指定してフィルタを作成した場合、**CA Enterprise Log Manager** は空集合ではなく、指定した期間内のデータベースをすべて返します。カタログにある一部の列を知っているだけでも、有用なアーカイブ クエリを作成できます。

6. (オプション) [詳細フィルタ] タブをクリックして詳細フィルタを追加します。列が入力した値と適切な関係を保持する場合は、イベント情報を表示します。列を選択し、演算子を選択して、値を選択または入力します。演算子の説明を、以下に示します。

関係演算子

等しい、等しくない、より小さい、より大きい、以下、以上。

含む

列にワイルドカード文字(%)を含むテキスト エントリと一致するパターンが含まれる場合に、イベント情報を含めます。L% には L で始まる値が含まれます。%L% には、最初の文字または最後の文字が L である場合を除き、L を含む値が含まれます。

含まない

列に指定したパターンが含まれていない場合にイベント情報を含めます。

設定あり

引用符で囲まれた一連の入力値のうち、1 つ以上が対象の列に含まれている場合に、イベント情報を含めます。設定に複数の値がある場合は、カンマで区切る必要があります。

設定なし

引用符で囲まれた一連の入力値のうち、1 つ以上が対象の列に含まれている場合に、イベント情報を含めます。設定に複数の値がある場合は、カンマで区切る必要があります。

一致する

入力した 1 つ以上の文字に一致する任意のイベント情報を含め、キーワードの検索を可能にします。

キー設定済み

レポートサーバの設定中にキー値として設定したすべてのイベント情報を含めます。ビジネス上の関連性など、組織のグループを設定する際にキー値を使用します。

キー設定なし

レポートサーバの設定中にキー値として設定していないすべてのイベント情報を含めます。ビジネス上の関連性など、組織のグループを設定する際にキー値を使用します。

7. [クエリ]をクリックします。

クエリの結果が表示されます。クエリ条件に一致するレコードを含むファイルが、`$IGW_LOC` を基準とするフル相対パスと共に表示されます。以下に例を示します。

```
../../LogManager/data/archive/<databaseFilename>
```

```
<remoteHostname>../../LogManager/data/archive/<databaseFilename>
```

自動アーカイブ済みファイルの復元

アーカイブ済みファイルを、外部ストレージから自動アーカイブ用として設定されたリモート サーバにコピーする場合は、`restore-ca-elm.sh` スクリプトを使用してファイルを復元することができます。この代替手段は、`LMArchive` ユーティリティを手動で使用するよりも推奨される方法です。

自動アーカイブ済みファイルを復元する方法

1. `caelmadmin` 認証情報を使用して、データベースを復元するイベント ログ ストアがある CA Enterprise Log Manager サーバにログインします。
2. コマンドプロンプトで、以下を入力して、ユーザを `root` に切り替えます。

```
su - root
```

3. 以下のショートカットを使用して、ディレクトリを `/opt/CA/SharedComponents/iTechnology` に変更します。

```
cd $IGW_LOC
```

4. コマンドプロンプトで、ユーザを `caelmservice` アカウントに切り替えます。

```
su - caelmservice
```

5. 以下のコマンドを実行します。`userid` および `pwd` は、Administrator ロールを備えた CA Enterprise Log Manager ユーザ アカウントの認証情報です。

```
restore-ca-elm.sh -euser userid -epasswd pwd -rhost hostname -ruser userid -rlocation path -files file1,file2,file3...
```

注: Administrator 以外が `restore-ca-elm` シェル スクリプトを実行できるようにするには、カスタム ロールおよびカスタム ポリシーを作成します。その後、このカスタム ロールを割り当てられたユーザは、`userid` および `pwd` に認証情報を指定できます。

詳細情報:

[アーカイブ済みデータベースを復元するための復元スクリプト](#) (P. 203)

[例: 管理者以外のユーザへのアーカイブ管理の許可](#) (P. 116)

[バックアップおよび復元の自動化](#) (P. 189)

アーカイブ済みデータベースを復元するための復元スクリプト

リモートストレージ サーバのコールド データベースに存在するデータに対してクエリを実行したり、レポートを作成することはできません。このようなデータにクエリを実行したりレポートを作成するには、そのデータが **CA Enterprise Log Manager** サーバにウォーム状態で存在する必要があります。復元シェルスクリプト `restore-ca-elm.sh` は、特定のコールド データベースとそのデジタル署名を、指定の **CA Enterprise Log Manager** サーバに移動し、ウォーム状態に復元するコマンドライン ユーティリティです。この復元ユーティリティを使用して、このデータベースを元のレポート サーバに戻したり、専用の復元ポイントに移動したりすることができます。復元スクリプトを実行するには、非対話型の認証を設定しておく必要があります。

復元スクリプトは、ファイルの復元先の **CA Enterprise Log Manager** サーバから実行します。コマンドで特定するリモート ホストとは、リモートストレージ サーバを指します。コールド データベースはリモートストレージ サーバのアーカイブ ディレクトリに存在します。

元のレポート サーバまたは復元ポイント サーバのいずれかにデータベース ファイルを復元するための要件は、次のとおりです。

- RSA 鍵ファイルの所有権がリモート サーバに設定されている。
- `/opt/CA/LogManager` フォルダに対するアクセス許可がリモート サーバの `caelmservice` に付与されている。

復元ポイント サーバにファイルを復元する場合は、次の追加のアクションを実行します。

1. リモートストレージ サーバから復元ポイント サーバに RSA 鍵をコピーします。
2. 復元ポイント サーバで RSA 鍵ファイルの所有権を設定します。

コマンドの形式は以下のとおりです。

```
restore-ca-elm.sh -euser userid -epasswd pwd -rhost hostname -ruser userid -rlocation  
path -files file1,file2,file3...
```

-euser *username*

Administrator ロールを持つ CA Enterprise Log Manager ユーザ アカウント
のユーザ名を指定します。

-epasswd *pwd*

ユーザ名に関連付けられた CA Enterprise Log Manager パスワードを指定し
ます。

-rhost *host*

コールド データベース ファイルがアーカイブ ディレクトリに存在するリモート
ホストのホスト名または IP アドレスを指定します。リモートホストは CA
Enterprise Log Manager サーバではありません。

-ruser *remote user*

/opt/CA/LogManager のパスに対するアクセス許可を持ち、認証された鍵
ファイルを含む .ssh フォルダの所有権を持つユーザ アカウントを指定しま
す。通常、このユーザ アカウントは caelmservice ユーザ アカウントです。

-rlocation *path*

リモートストレージサーバのデータベースファイルへのパスを指定します。
リモートストレージサーバが UNIX サーバである場合、パスは
/opt/CA/LogManager/data/archive です。

files *file1,file2,file3...*

復元するデータベースを、スペースを入れずにカンマで区切ったリストで指
定します。

例: 復元シェル スクリプト

以下のコマンド例は、アーカイブ済みデータベースファイルの復元先の CA Enterprise Log Manager から実行されます。Administrator1、calm_r12 のアカウント認証情報を持つユーザが実行します。アーカイブ済みデータベースをオフサイトストレージから移動した宛先リモートサーバの名前は、NY-ストレージ-Svr です。このリモートサーバは、RSA 公開鍵がコピーされている .ssh フォルダの所有権を持つ caelmservice アカウントで設定されています。このアカウントは、ディレクトリ構造 /opt/CA/LogManager に関するフル権限も持っています。このコマンドによって、復元されるファイルが NY-Storage-Svr サーバの data/archive ディレクトリパスにあることが指定され、復元されるデータベースファイルが NY-Storage-Svr_20081206192014.db.cerod として識別されます。

```
restore-ca-elm.sh -euser Administrator1 -epasswd calm_r12 -rhost NY-Storage-Svr  
-ruser caelmservice -rlocation /opt/CA/LogManager/data/archive -files  
NY-Storage-Svr_20081206192014.db.cerod
```

手動によるアーカイブ済みデータベースのバックアップ

CA Enterprise Log Manager は、データがホットストレージからウォームストレージに移動されるたびに、ユーザの設定で制御されたとおりに、自動的にアーカイブ済みデータベースを新規作成します。ウォームデータベースをリモートサーバに移動するよう自動アーカイブを設定することを推奨しますが、独自のツールを使用してアーカイブデータベースのバックアップを実行した後で、LMArchive ユーティリティを実行してシステムにバックアップの実行を通知することもできます。

自動方式か、ここで説明する手動方式を使用して、ウォームデータベースを毎日バックアップすることをお勧めします。ウォームストレージのアーカイブファイルは、指定した時間の経過後、またはディスク領域が指定した割合まで減少した場合に自動的に削除されるため、このタスクは重要です。

手動によるウォームデータベースのバックアップは、以下の手順で構成されます。

1. まだバックアップされていないウォームデータベースの特定
2. バックアップの実行
3. バックアップの記録

詳細情報

[バックアップされていないデータベースの特定](#) (P. 206)

[バックアップの実行](#) (P. 207)

[バックアップの記録](#) (P. 208)

バックアップされていないデータベースの特定

LMArchive ユーティリティによるバックアップ済みとしてマークされていないアーカイブ済みデータベースのリストを表示できます。信頼できる結果を得るためには、アーカイブ済みデータベースをバックアップする際に、このユーティリティが `-notify arch` オプションを使用して実行されている必要があります。

重要： 混乱を避けるために、バックアップの完了を **CA Enterprise Log Manager** に通知して、情報を最新の状態に維持してください。

バックアップ済みとしてマークされていない現在のアーカイブ済みデータベースファイルの名前をすべて表示する方法

1. **caelmadmin** の認証情報を使用して、アーカイブのためにバックアップの必要なデータベースが保存されたイベント ログ ストアがある CA Enterprise Log Manager サーバにログインします。
2. コマンドプロンプトで、以下を入力して、ユーザを **root** に切り替えます。

```
su - root
```

3. 以下のショートカットを使用して、ディレクトリを `/opt/CA/SharedComponents/iTechnology` に変更します。

```
cd $IGW_LOC
```

4. 以下のコマンドを実行します。**username** および **pwd** は、Administrator ロールを持つ CA Enterprise Log Manager ユーザアカウントの認証情報です。

```
LMArchive -euser username -epassword pwd -list inc
```

例: バックアップ済みとしてマークされていない、現在のすべての CA Enterprise Log Manager アーカイブ済みファイルの表示

以下のコマンドを管理者が実行すると、バックアップ済みとしてマークされていないすべてのウォーム データベースのリストがリクエストされます。

```
LMArchive -euser Administrator1 -epassword calmr12 -list inc
```

バックアップ済みとしてマークされていないアーカイブ ファイルのリストが、以下のような形式で表示されます。

```
CAELM アーカイブ済みファイル(未バックアップ):  
calm04_20091206192014.db.cerod  
calm04_20091206192014.db.sig
```

バックアップの実行

CA Enterprise Log Manager レポート サーバから CA Enterprise Log Manager サーバではないリモートストレージサーバへの自動アーカイブを設定していない場合は、アーカイブされたデータベースを手動でバックアップし、別のディスクやサーバなどの安全な保存場所に移動する必要があります。

重要: 必ず、CA Enterprise Log Manager レポート サーバから削除される前に、データベースをバックアップして移動させてください。

アーカイブの最大日数として設定された値に達するか、ディスク領域の割合がアーカイブ ディスク領域として設定された値を下回ると、ウォーム データベースは自動的に削除されます。ファイルが削除されることによってデータが失われるのを防ぐため、定期的にバックアップを実行してください。

ウォーム データベースを手動でバックアップする方法

1. caelmadmin 認証情報を使用して、ターゲット データベースが格納されたイベントログ ストアがある CA Enterprise Log Manager レポート サーバにログインします。
2. 以下を入力して、ユーザを root に切り替えます。

```
su - root
```
3. ディレクトリを /opt/CA/LogManager/data/archive に変更します。
4. 各サイトでの手順に従って、選択したバックアップ ツールを使用してウォーム データベースをバックアップし、オンサイトの一時保管サーバか、長期保存用のオフサイトの保管場所に移動します。

バックアップの記録

1 つ以上のアーカイブ済みデータベースのバックアップを実行するたびに、バックアップを実行した CA Enterprise Log Manager に履歴を残すようにします。

注: バックアップの記録に失敗すると、LMArchive ユーティリティを使用したバックアップ済みデータベースをリスト表示する際に、不正なデータがレポートされます。

特定のアーカイブ済みデータベースのバックアップを記録する方法

1. caelmadmin の認証情報を使用して、バックアップ済みデータベースが保存されたイベント ログ ストアがある CA Enterprise Log Manager サーバにログオンします。
2. コマンドプロンプトで、以下を入力して、ユーザを root に切り替えます。

```
su - root
```

3. 以下のショートカットを使用して、ディレクトリを /opt/CA/SharedComponents/iTechnology に変更します。

```
cd $IGW_LOC
```

4. 以下のコマンドを実行します。username および pwd は、Administrator ロールを持つ CA Enterprise Log Manager ユーザ アカウントの認証情報です。

```
LMArchive -euser username -epassword pwd -notify arch -files file1,file2,file3...
```

例: ファイルがバックアップされたことを CA Enterprise Log Manager に通知する

Administrator1 という名前の管理者が以下のコマンドを実行すると、ウォームデータベース (calm04_20091206192014.db.cerod) がバックアップされたことが CA Enterprise Log Manager イベント ログ ストアに通知されます。バックアップしたデータベースは、長期保存用に外部ストレージに手動で移動できます。

```
LMArchive -euser Administrator1 -epassword calmr12 -notify  
arch -files calm04_20091206192014.db.cerod
```

アーカイブ ファイルの通知が、以下のような形式で表示されます。

ファイル calm04_20091206192014.db.cerod のアーカイブ通知を送信しました...

手動による元のイベント ログ ストアへのアーカイブの復元

クエリまたはレポートを目的として、CA Enterprise Log Manager サーバ上のアーカイブ ディレクトリにコールド データベース ファイルを復元しなければならないことがあります。これは、セキュリティ違反を調査する際や、1 年ごとや半年ごとのコンプライアンス監査の際などに必要となります。使用する手順は、以下の 2 つの要因によって異なります。

- 復元しようとしているファイルのバックアップ時に、自動アーカイブを使用したかどうか
- ファイルの復元先を、元のレポート サーバにするか、専用の復元ポイントサーバなど別のサーバにするか

別のサーバに復元する場合は、「新規イベント ログ ストアへのアーカイブの復元」を参照してください。

元のレポート サーバにファイルを復元する場合は、以下の手順に従います。

1. 復元するファイルを特定し、アーカイブ ディレクトリを判断して、アーカイブされたデータベースの復元を準備します。
2. 自動アーカイブ用に設定したリモート サーバ上か、元のレポート サーバ上のアーカイブ ディレクトリに、外部ストレージからデータベースを移動します。
3. 自動アーカイブ用に設定したリモート ストレージ サーバにアーカイブ済みファイルを移動した場合は、レポート CA Enterprise Log Manager にログオンし、`restore-ca-elm.sh` スクリプトを使用して、リモート ストレージ サーバから自動アーカイブ ファイルを復元します。
4. 元のレポート CA Enterprise Log Manager サーバ上のアーカイブ ディレクトリにアーカイブ済みファイルを移動した場合は、LMArchive ユーティリティを使用して、手動でアーカイブ済みファイルを復元します。
5. 終了日を復元したデータベースの日付に設定したクエリを実行し、クエリ結果を調べて、解凍済みデータベースにクエリを実行できることを確認します。

詳細情報

[アーカイブ済みデータベースの復元の準備 \(P. 210\)](#)

[アーカイブ済みデータベースのアーカイブ ディレクトリへの移動 \(P. 212\)](#)

[自動アーカイブ済みファイルの復元 \(P. 202\)](#)

[手動によるアーカイブ済みファイルの復元 \(P. 213\)](#)

[復元の検証 \(P. 214\)](#)

アーカイブ済みデータベースの復元の準備

アーカイブ済みデータベースを復元する前に、以下を確認しておく必要があります。

- 復元するファイルの名前
- オフサイトストレージから取得したファイルのコピー先のアーカイブ ディレクトリパス。このパスは常に `/opt/CA/LogManager/data/archive` です。

CA Enterprise Log Manager [管理]タブ -[ログ収集エクスプローラ]を使用して、単純フィルタまたは詳細フィルタを指定し、アーカイブ カタログにクエリを実行できます。または、ここで説明するように、コマンドライン ユーティリティを使用することもできます。

必要な情報がすでに手元にある場合は、この手順をスキップしてください。

アーカイブ済みデータベースの復元を準備する方法

1. caelmadmin 認証情報を使用して、データベースを復元するイベント ログ ストアがある CA Enterprise Log Manager サーバにログオンします。
2. コマンドプロンプトで、以下を入力して、ユーザを `root` に切り替えます。

```
su - root
```

3. 以下のショートカットを使用して、ディレクトリを `/opt/CA/SharedComponents/iTechnology` に変更します。

```
cd $IGW_LOC
```

4. バックアップされ、外部ストレージに移動されたファイルが含まれているファイルリストから、復元するデータベースを特定します。このアーカイブ カタログ内にあるすべてのアーカイブ済みファイルのリストを表示するには、以下のコマンドを実行します。userid および pwd は、Administrator ロールを持つ CA Enterprise Log Manager ユーザアカウントの認証情報です。

```
LMArchive -euser userid -epassword pwd -list all
```

すべてのアーカイブ済みファイルのリストが表示されます。

5. (オプション) 手動バックアップから復元する場合は、特定されたコールドアーカイブ ファイルをコピーするアーカイブ ディレクトリの場所を決定します。以下のコマンドを実行します。userid および pwd は、Administrator ロールを備えた CA Enterprise Log Manager ユーザアカウントの認証情報です。

```
LMArchive -euser userid -epassword pwd -list loc
```

アーカイブ ディレクトリが表示されます。

例: 現在のすべての CA Enterprise Log Manager アーカイブ ファイルの表示

以下のコマンドが CA Enterprise Log Manager 管理者 Administrator1 によって実行されると、イベント ログ ストアのアーカイブ ディレクトリにあるすべてのデータベースのリストが要求されます。

```
LMArchive -euser Administrator1 -epassword calmr12 -list all
```

現在のアーカイブ ファイルのリストが、以下のようなフォーマットで表示されます。

CAELM アーカイブ済みファイル:

```
calm04_20091206191941.db.cerod  
calm04_20091206191958.db.cerod  
calm04_20091206192014.db.cerod  
calm04_20091206191941.db.sig  
calm04_20091206191958.db.sig  
calm04_20091206192014.db.sig
```

例: CA Enterprise Log Manager アーカイブ ディレクトリの表示

以下のコマンドが CA Enterprise Log Manager 管理者 Administrator1 によって実行されると、アーカイブ済みデータベースのディレクトリの場所が要求されます。

```
LMArchive -euser Administrator1 -epassword calmr12 -list loc
```

以下は、標準的な応答です。

CAELM アーカイブの場所(ローカル ホスト):

```
../../LogManager/data/archive
```

アーカイブ済みデータベースのアーカイブ ディレクトリへの移動

オフサイトにアーカイブ済みファイルを移動した場合は、各サイトでの手順に従ってファイルを読み出し、オンサイトに戻してください。

元の CA Enterprise Log Manager サーバ、または非対話型の認証用に設定されたリモートサーバのいずれかのアーカイブ ディレクトリに、アーカイブ済みデータベースを移動します。アーカイブ ディレクトリは、`/opt/ca/LogManager/data/archive` です。

外部ストレージからネットワークにアーカイブ済みデータベースを移動する方法

1. 以下の方法のいずれかを実行して、外部ストレージからネットワークに、復元するデータベースファイルを移動します。
 - 自動アーカイブを使用して、リモートサーバに自動的にアーカイブ済みファイルを移動する場合は、このリモートサーバ上のアーカイブ ディレクトリにファイルをコピーします（このリモートサーバは、すでに、アーカイブ済みデータベースが復元される CA Enterprise Log Manager サーバとの非対話型認証用に設定されています）。
 - 自動アーカイブを使用しない場合は、元の CA Enterprise Log Manager サーバ上のアーカイブ ディレクトリにアーカイブ済みファイルをコピーします。
2. アーカイブ済みファイルの場所に応じて、以下のいずれかの作業を実行します。
 - アーカイブ済みファイルが、自動アーカイブ用に設定されたリモートサーバ上にある場合は、`restore-ca-elm.sh` スクリプトを使用して、自動アーカイブ済みファイルを復元します。
 - アーカイブ済みファイルが、元の CA Enterprise Log Manager サーバ上のアーカイブ ディレクトリにある場合は、`LMArchive` ユーティリティを使用してアーカイブ済みファイルが復元されたことを CA Enterprise Log Manager に通知します。通知すると、復元されたファイルが解凍済みの状態に設定されます。

詳細情報:

[自動アーカイブ済みファイルの復元](#) (P. 202)

[手動によるアーカイブ済みファイルの復元](#) (P. 213)

手動によるアーカイブ済みファイルの復元

長期保管用ストレージからアーカイブ ディレクトリに 1 つ以上のデータベースを復元した後は、アーカイブ ディレクトリの所有権を **caelmservice** ユーザに変更してから、**LMArchive** ユーティリティを使用してデータベースを復元したことを **CA Enterprise Log Manager** に通知する必要があります。**root** が所有するアーカイブ済みファイルは、**LMArchive** ユーティリティでは認識されません。

-notify rest オプションを使用して **LMArchive** を実行すると、アーカイブ済みデータベースファイルの状態がコールドから解凍済みに変更され、クエリやレポートで使えるようになります。

管理者は、[イベント ログ ストア サービスの設定]の[ポリシーのエクスポート]設定を使用して、解凍されたアーカイブ済みデータベースがアーカイブ ディレクトリから自動的に削除されるまで保持される時間数を設定できます。

手動でアーカイブ済みデータベース ファイルを復元する方法

1. **caelmadmin** の認証情報を使用して、復元済みデータベースが格納されたイベント ログ ストアがある **CA Enterprise Log Manager** サーバにログオンします。

2. コマンドプロンプトで、以下を入力して、ユーザを **root** に切り替えます。

```
su - root
```

3. ディレクトリを **/data** ディレクトリに変更します。以下に例を示します。

```
cd /opt/CA/LogManager/data
```

4. **caelmservice** アカウントにアーカイブ ディレクトリ (**/opt/CA/LogManager/data/archive**) の所有権を割り当てます。

```
chown -R caelmservice:caelmservice archive
```

アーカイブ ファイルの所有権が、非ログイン アカウントである **caelmservice** (内部オペレーティング システム ユーザ)に変更されます。

5. 以下のショートカットを使用して、ディレクトリを **/opt/CA/SharedComponents/iTechnology** に変更します。

```
cd $IGW_LOC
```

6. 以下のコマンドを実行します。*username* および *pwd* は、Administrator ロールを持つ CA Enterprise Log Manager ユーザアカウントの認証情報です。

```
LMArchive -euser username -epassword pwd -notify rest -files file1,file2,file3
```

復元の確認メッセージが表示されます。CA Enterprise Log Manager によって、指定したファイルがデフロスティング(解凍)されます。解凍済みファイルは、設定した時間数の間保持されます。保持時間は、最大 7 日間まで設定できます。

注: これで、復元されたアーカイブ ファイルに含まれているイベント データにクエリとレポートを実行できるようになりました。

例: データベースが復元されたことを CA Enterprise Log Manager に通知する

Administrator ロールを持った CA Enterprise Log Manager ユーザが以下のコマンドを実行すると、指定したコールド データベース *calm04_20091206192014.db* がアーカイブ ディレクトリにコピーされたことが CA Enterprise Log Manager イベント ログ ストアに通知されます。

```
LMArchive -euser Administrator1 -epassword calmr12 -notify  
rest -files calm04_20091206192014.db.cerod
```

復元の確認メッセージが、以下のような形式で表示されます。

ファイル *calm04_20091206192014.db* の復元通知を送信しました...

復元の検証

クイック クエリを実行することで、復元されたデータベースが分析可能であることをすばやく検証できます。通常のクエリを実行すると、ウォーム状態または解凍済みの復元されたデータベースのデータが表示されます。

プロセスの例を示します。

1. 復元されたデータベースに格納されているイベントの詳細のタイプを表示するよう設計されたサブスクリプション クエリをコピーします。
2. クエリの実設計ウィザードの手順に進み、新たに解凍したデータベースファイルに対応する結果の条件と日付範囲を入力します。
3. クエリを保存します。
4. クエリを実行します。

手動による新規イベント ログ ストアへのアーカイブの復元

1 年ごとや半年ごとにコンプライアンス監査を行うために、クエリの実行やレポート作成を目的として、コールドストレージに保存されたファイルの復元が必要になることがあります。CA Enterprise Log Manager の 1 つを、コールド データの調査用復元ポイントとして機能するよう指定すると、この CA Enterprise Log Manager に新しいデータベースを復元するたびに、強制的にカタログを再構築する必要があります。カタログの再構築、すなわちカタログ再作成は、データが作成されたサーバとは異なるサーバにデータを復元する場合にのみ必要になります。

重要: このサーバについて、イベント ログ ストアのアーカイブの最大日数設定が適切であることを確認してください。設定が適切でない場合、復元されたファイルはすぐに削除されます。

必要な場合は、iGateway が再起動されたときに、カタログ再作成が自動的に実行されます。iGateway がシャットダウンされる前にデータベースのカタログ作成が完了していない場合は、iGateway の再起動後にカタログの再作成プロセスが実行されます。iGateway が停止している間に 1 つ以上のデータベースがアーカイブ データベース ディレクトリに追加された場合、次に iGateway が起動したときに、カタログ再作成プロセスが実行されます。

外部ストレージから、バックアップされたものとは異なる CA Enterprise Log Manager へのアーカイブ済みファイルの復元は、以下の手順から構成されます。

1. 復元するデータベースを特定します。そのためには、フィルタを使用してアーカイブ カタログにクエリを実行してください。
2. 外部ストレージから、特定されたコールド アーカイブ ファイルをネットワークに移動します。
3. 移動したデータベースをアーカイブ ディレクトリにコピーします。アーカイブ ディレクトリを表示するには、`-list loc` オプションを使用して `LMArchive ユーティリティ` を実行します。
4. アーカイブ カタログを再構築します(カタログの再作成)。
単一のデータベースを追加するためにアーカイブ カタログを再構築すると、数時間かかる場合があります。カタログ再作成プロセスが完了するまで待機してから、復元されたデータベースのイベント ログに対してクエリおよびレポート作成を実行して、検証を開始してください。
5. クエリを発行して、復元結果を検証します。

注: CA Enterprise Log Manager を復元ポイント専用として使用する場合は、必ず連携から除外してください。

詳細情報:

[アーカイブ済みデータベースのアーカイブ ディレクトリへの移動](#) (P. 212)

[復元されたアーカイブの最大アーカイブ日数の設定](#) (P. 217)

[復元されたデータベースのカタログへの追加](#) (P. 218)

[復元の検証](#) (P. 214)

[例: 管理者以外のユーザへのアーカイブ管理の許可](#) (P. 116)

復元されたアーカイブの最大アーカイブ日数の設定

復元ポイント専用の CA Enterprise Log Manager のイベントログストアを設定する際は、[アーカイブの最大日数]を最大値の **28000** に設定し、グローバル設定よりも優先されるようにすることをお勧めします。アーカイブ済みデータベースファイルが削除されるまでの保存日数が、復元されたデータベースファイルの経過日数よりも少なく設定されていると、ファイルはウォーム状態に復元された直後にシステムによって削除されます。

注: この手順は、新規イベントログストアに復元されたファイルにのみ適用されます。

アーカイブの最大日数が、復元されたファイルの経過日数を超えるように設定する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [サービスリスト]の[イベントログストア]フォルダを展開し、復元ポイント専用の CA Enterprise Log Manager を選択します。
3. [アーカイブの最大日数]の横の切り替えボタンをクリックして、ローカル設定に切り替え、エントリフィールドを有効にします。
4. 復元するファイルのうち最も古い日数を超えるように、日数の値をフィールドに設定します。最大値は **28000** です。
5. [保存]をクリックします。

復元されたデータベースのカatalogへの追加

復元するデータベースを、作成されたサーバとは異なるサーバ上のアーカイブディレクトリに直接コピーする場合は、アーカイブ カatalogを再構築し、復元したデータベースを追加します。

以下のどちらかに該当する場合は、Catalogの再作成を実行しないでください。

- **restore-ca-elm.sh** スクリプトを使用してアーカイブ済みデータベースを復元する場合。復元シェルスクリプトによってCatalog再作成が実行されます。
- 復元されたデータベースを作成されたサーバと同じサーバ上のアーカイブディレクトリに直接コピーし、**-notify rest** オプションを使用した **LMArchive** で、データベースが復元されたことを **CA Enterprise Log Manager** に通知する場合。

-notify rest オプションを使用した **LMArchive** の場合と同様、Catalog再作成プロセスによって、復元されたデータベースが「解凍済み」の状態ではなく「ウォーム」状態に設定されます。このため、復元済みデータベースは、イベントログストア設定で定義されたエクスポート ポリシーではなく、通常のアーカイブ ルールに従います。

アーカイブ Catalogを再構築して、復元したデータベースを追加する方法

1. [管理]タブをクリックし、[アーカイブ管理]サブタブをクリックします。
[アーカイブ管理]フォルダリストが表示されます。
2. [アーカイブのクエリおよびCatalog再作成]フォルダをクリックします。
[Catalog再作成]などの 3 つのボタンが、[クイック フィルタ]タブおよび[詳細フィルタ]タブの上に表示されます。
3. [Catalog再作成]をクリックします。
成功を確認するメッセージが表示されます。復元されたデータベースが、ウォーム状態でCatalogに追加されます。

LMArchive によるバックアップ/復元の追跡

LMArchive は、CA Enterprise Log Manager サーバ上のイベント ログ ストアに対するウォーム データベースのバックアップおよび復元を追跡するコマンドラインユーティリティです。*LMArchive* を使用して、アーカイブが可能なウォーム データベース ファイルのリストを照会します。リスト表示されたデータベースをバックアップし、長期的な(コールド)ストレージに移動させた後、このデータベースがバックアップされた CA Enterprise Log Manager サーバに関する記録を作成する際にも *LMArchive* を使用します。元の CA Enterprise Log Manager サーバにコールド データベースを復元した後には、*LMArchive* を使用して CA Enterprise Log Manager に通知します。これにより、コールド データベース ファイルが解凍済みの状態として認識され、クエリの実行が可能になります。

コマンドの形式は以下のとおりです。

```
LMArchive -euser username -epassword pwd {-list [loc|all|inc] | -notify [arch|rest]  
-files file1,file2,file3...}
```

-euser *username*

Administrator ロールを持つ CA Enterprise Log Manager ユーザ アカウントのユーザ名を指定します。

-epassword *pwd*

ユーザ名に関連付けられた CA Enterprise Log Manager パスワードを指定します。

-list [loc | all | inc]

アーカイブ ディレクトリの配置場所、すべてのウォーム データベースとコールド データベースの名前、およびウォーム データベースのみの名前の、いずれかのリストにクエリを実行します。

loc

アーカイブ ディレクトリの場所をリクエストします。

all

イベント ログ ストアのアーカイブ ディレクトリにあるすべてのファイル名のリストをリクエストします。

inc

アーカイブされていない現在のウォーム データベース ファイルのファイル名の増分リストをリクエストします。このリクエストによって、バックアップ、外部ストレージへの移動、およびコールド状態への変更が行われていないファイル名が返されます。このユーティリティの通知コマンドを使用して移動が通知されると、ファイルがコールド状態に設定されます。

-notify [arch | rest]

CA Enterprise Log Manager イベント ログ ストアに、指定されたファイルが正常にバックアップまたは復元されたことを通知します。

arch

CA Enterprise Log Manager イベント ログ ストアに、指定されたファイルが正常にバックアップされたことを通知します。

rest

CA Enterprise Log Manager イベント ログ ストアに、指定されたファイルが正常に復元されたことを通知します。

-files *file1,file2,file3...*

バックアップまたは復元されたデータベース ファイルの名前を指定します。

詳細情報:

[ログ ストレージについて](#) (P. 184)

[バックアップされていないデータベースの特定](#) (P. 206)

[バックアップの記録](#) (P. 208)

[アーカイブ済みデータベースの復元の準備](#) (P. 210)

[手動によるアーカイブ済みファイルの復元](#) (P. 213)

第 7 章: サブスクリプション

このセクションには、以下のトピックが含まれています。

[サブスクリプションによる CA Enterprise Log Manager バージョン 12.5 へのアップグレード \(P. 221\)](#)

[グローバル サブスクリプション ステータスの表示 \(P. 223\)](#)

[サーバのサブスクリプション ステータスの表示 \(P. 224\)](#)

[グローバル サブスクリプション設定の編集 \(P. 226\)](#)

[サーバのローカル サブスクリプション設定の編集 \(P. 227\)](#)

[オフライン サブスクリプション用のモジュールのダウンロードと選択 \(P. 229\)](#)

[オンデマンド更新について \(P. 231\)](#)

[更新用の空きディスク領域 \(P. 235\)](#)

[サブスクリプション公開鍵について \(P. 236\)](#)

[サブスクリプションの自己監視イベント \(P. 236\)](#)

[エージェントおよびコネクタへのサブスクリプション更新の適用 \(P. 242\)](#)

サブスクリプションによる CA Enterprise Log Manager バージョン 12.5 へのアップグレード

CA Enterprise Log Manager をバージョン 12.5 にアップグレードするには、最初に Log Manager 製品バージョン 12.5 にアップグレードしてから、ほかのすべての CA Enterprise Log Manager モジュール (コンテンツ、統合、エージェント モジュールなど) を更新します。すべてのアップグレード タスクは、サブスクリプションを通して実行します。

重要: 新しい CA Enterprise Log Manager サーバをネットワーク内にインストールする前に、管理 CA Enterprise Log Manager サーバをアップグレードしてください。そのようにすると、新しいサーバを正しく登録できます。

CA Enterprise Log Manager バージョン 12.5 にアップグレードする方法

1. Log Manager バージョン 12.5 にアップグレードする方法

注: アップグレードされた CA Enterprise Log Manager 12.5 ユーザ インターフェースでは、サブスクリプション モジュールとサブスクリプション サービスの両方が[管理]タブの[サービス]サブタブに表示されます。サブスクリプション モジュールは、12.5 の更新前のインターフェースおよび機能を反映し、12.5 へのアップグレード中にすべての CA Enterprise Log Manager サーバ間の適切な通信を保証します。特定の CA Enterprise Log Manager サーバ上で Log Manager 製品を 12.5 にアップグレードしたら、サブスクリプション サービスのみを使用して以後のすべてのサブスクリプション タスクおよび設定変更を実行します。

2. その他のすべての CA Enterprise Log Manager モジュールを更新します。

重要: 手順 1 の実行後、アップグレードされた CA Enterprise Log Manager 12.5 ユーザ インターフェースでは、サブスクリプション モジュールとサブスクリプション サービスの両方が表示されます。この手順を含む以後のすべてのサブスクリプション タスクは、サブスクリプション モジュールではなくサブスクリプション サービスのみを使用して実行してください。サブスクリプション モジュールは、12.5 へのアップグレード中にすべての CA Enterprise Log Manager サーバ間の適切な通信を保証するために存在します。このため、アップグレード後のサブスクリプション タスクでは使用しないでください。

3. エージェントまたはコネクタ モジュールが更新の間に存在した場合、更新されたエージェントまたはコネクタをインストールします。

4. サードパーティ製品および他の CA 製品 (CA Access Control など) を再登録します。これらの製品は、オープン API コールを使用して、それぞれのネイティブ インターフェースに CA Enterprise Log Manager レポートを表示します。

この手順が完了すると、このリリースで変更された証明書が更新されます。詳細については、「CA Enterprise Log Manager API プログラミング ガイド」を参照してください。

注: これらの手順の実行に関する詳細は、「CA Enterprise Log Manager 12.5 リリース ノート」の「サブスクリプションによる CA Enterprise Log Manager バージョン 12.5 へのアップグレード」を参照してください。サブスクリプション アップグレードに関連する既知の問題については、「リリース ノート」を参照してください。

詳細情報:

[エージェントおよびコネクタへのサブスクリプション更新の適用 \(P. 242\)](#)

グローバル サブスクリプション ステータスの表示

サブスクリプション サービスは、設定されたスケジュールに従って、またはオンデマンド更新時に、選択されたサブスクリプション モジュールを CA Enterprise Log Manager サーバにダウンロードおよび配布します。[サブスクリプション ダッシュボード]では、CA Enterprise Log Manager サーバの現在のサブスクリプション ステータスを参照できます。

[サブスクリプション ダッシュボード]には、CA Enterprise Log Manager サーバによって現在ダウンロードまたはインストールされているすべての更新の進捗状況が表示されます。また、現在進行中のコンテンツ更新の状態に加え、インストール済みのすべてのコンテンツ更新のリストも参照できます。

サブスクリプションのグローバル ステータスを表示する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [サブスクリプション サービス]をクリックします。

サブスクリプション サービスの[グローバル サービス設定]が表示され、[サブスクリプション ダッシュボード]タブが選択されます。

3. コンテンツ更新のステータスを表示するには、[コンテンツ サブスクリプション ステータス]ウィンドウを参照します。

コンテンツ更新が進行中である場合、進捗バーおよびステータス メッセージで更新のステータスが示されます。最新の進捗状況を表示するには、[リフレッシュ]ボタンをクリックします。

4. これまでにインストールされたすべてのコンテンツ更新のリストを表示するには、[カタログの参照]をクリックします。

[コンテンツ]ウィンドウが表示されます。コンテンツ タイプをクリックすると、現在までにインストールされたすべての関連する更新の名前、日付、およびバージョンが表示されます。

5. 任意の CA Enterprise Log Manager サーバのサブスクリプション ステータスを表示するには、[サーバ]ウィンドウを参照します。

いずれかの CA Enterprise Log Manager サーバで更新が進行中である場合は、進捗バーがそのサーバの[進捗]列に表示されます。最新の進捗状況を表示するには、[リフレッシュ]ボタンをクリックします。

また、[サーバ]ウィンドウには、各 CA Enterprise Log Manager サーバに関する以下の情報も表示されます。

状態

CA Enterprise Log Manager サーバのサブスクリプション ステータスが表示されます。サブスクリプション ステータスは、アイドル、待機中、ダウンロード中、インストール中、完了、および失敗です。

メッセージ

指定された CA Enterprise Log Manager サーバのサブスクリプション ステータスに関連するどんなメッセージが表示されます。

日付

指定された CA Enterprise Log Manager サーバによって実行された最後の更新アクションの日付が表示されます。

サーバのサブスクリプション ステータスの表示

サブスクリプション サービスは、設定されたスケジュールに従って、またはオンデマンド更新時に、選択されたサブスクリプション モジュールを CA Enterprise Log Manager サーバにダウンロードおよび配布します。特定の CA Enterprise Log Manager サーバの現在のサブスクリプション ステータスは、グローバル[サブスクリプション ダッシュボード]またはサーバのローカル[状態]画面で参照できます。

CA Enterprise Log Manager サーバのサブスクリプション ステータスを表示する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [サブスクリプション サービス]をクリックします。

サブスクリプション サービスの[グローバル サービス設定]が表示され、[サブスクリプション ダッシュボード]タブが選択されます。

3. 以下のいずれかの操作を行います。

- [サーバ]ウィンドウ中で、対象サーバのステータス情報を確認します。更新が進行中である場合は、進捗バーがそのサーバの[進捗]列に表示されます。[リフレッシュ]ボタンをクリックして、最新の進捗状況を表示します。また、[サーバ]ウィンドウには、各 **CA Enterprise Log Manager** サーバに関する追加情報(状態、メッセージ、日付など)も表示されます。

または

- より詳細な情報を参照するには、[サーバ]ウィンドウで対象のサーバの名前をクリックしてローカル[状態]画面を開きます。更新が進行中である場合は、進捗バーおよびステータスメッセージが[ステータス]画面に表示され、更新の進捗状況が示されます。[リフレッシュ]ボタンをクリックして、最新の進捗状況を表示します。また、[サーバ]ウィンドウには、各 **CA Enterprise Log Manager** サーバに関する以下の情報も表示されます。

状態

CA Enterprise Log Manager サーバのサブスクリプションステータスが表示されます。サブスクリプションステータスは、アイドル、待機中、ダウンロード中、インストール中、完了、および失敗です。

メッセージ

指定された CA Enterprise Log Manager サーバのサブスクリプションステータスに関連するどんなメッセージが表示されます。

日付

指定された CA Enterprise Log Manager サーバによって実行された最後の更新アクションの日付が表示されます。

グローバル サブスクリプション設定の編集

実装段階で、お使いの環境用にグローバル サブスクリプションを設定できます。個々のサーバのローカル設定によってグローバル設定を無効にしない限り、すべての CA Enterprise Log Manager サーバはこれらのグローバル設定を継承して使用します。

デフォルトでは、最初にインストールされたサーバがデフォルトのサブスクリプション プロキシとなり、その後インストールされるすべてのサーバはサブスクリプション クライアントとして設定されます。他のプロキシが設定されないか利用可能でない場合、デフォルトのプロキシはサブスクリプション クライアントに更新をダウンロードします。

グローバル設定はいつでも変更できます。変更された設定はすべてのサーバに継承されます。ただし、その設定より優先される設定がローカルで特定のサーバに設定されている場合を除きます。

グローバルレベルでのみ作成および編集が可能な設定には、以下のものがあります。

- デフォルトのサブスクリプション プロキシ
- 公開鍵 - バージョン
- コンテンツ更新のサブスクリプション プロキシ

グローバル サブスクリプション設定を編集する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [サブスクリプション サービス]をクリックします。

サブスクリプション サービス用の[グローバル サービス設定]が表示されます。

3. [管理]タブをクリックします。
4. 右ペインで、グローバル サービス設定のサブスクリプション サービス設定を参照します。設定を確認し、必要であれば変更を加えます。

注: フィールドレベルの詳細については、オンライン ヘルプを参照してください。

5. [保存]をクリックします。

詳細情報:

[サブスクリプション更新を適用する方法](#) (P. 657)

サーバのローカル サブスクリプション設定の編集

サブスクリプションの実装時には、お使いの環境用にグローバル サブスクリプション設定を編集できます。たとえば、サブスクリプション スケジュールやプロキシリストなどです。個々の CA Enterprise Log Manager サーバはこれらのグローバル設定を継承します。

このグローバル設定は、各サーバにおいてローカル設定を適用することによっていつでも無効にできます。グローバル設定を無効にする場合は、サーバのサブスクリプション ロールを考慮する必要があります。

サーバのサブスクリプション設定を編集する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [サブスクリプション サービス]を展開し、設定するサーバを選択します。
選択した CA Enterprise Log Manager サーバの[サブスクリプション サービス 設定]が表示されます。
3. [管理]タブをクリックします。

4. サーバのサブスクリプション ロールを変更する場合は、以下のいずれかを実行します。
 - サーバをサブスクリプション クライアントとして指定するには、[サブスクリプション プロキシ]チェック ボックスをオフにします。
 - サーバをオンラインのサブスクリプション プロキシとして指定するには、[サブスクリプション プロキシ]チェック ボックスをオンにして[オンラインのサブスクリプション プロキシ]を選択します。
 - サーバをオフラインのサブスクリプション プロキシとして指定するには、[サブスクリプション プロキシ]チェック ボックスをオンにして[オフラインのサブスクリプション プロキシ]を選択します。

注: サーバのロールをサブスクリプション プロキシからサブスクリプション クライアントに変更する場合は、このプロキシを使用するサブスクリプション クライアントの設定を考慮する必要があります。サーバをプロキシからクライアントに変更する場合は、グローバルおよびローカルの[クライアント更新用サブスクリプション プロキシ]リストからそのサーバをすぐに削除します。

重要: サーバのロールをオフライン サブスクリプション プロキシに変更する場合は、それがいずれかのプロキシリストに含まれているかどうかを調べる必要があります。オンラインとオフラインの両方のサブスクリプション プロキシが混在して設定されている環境では、オンライン サブスクリプション クライアント用のプロキシリストにオフライン プロキシを含めないようにしてください。

5. 継承されたグローバル設定を無効にするには、選択したフィールドのグローバル/ローカルのトグル ボタンをクリックしてローカル サービス設定に切り替えます。

注: グローバル設定を復元するには、再度ボタンをクリックします。グローバル設定は次の更新開始時刻に復元されます。

6. このサーバ用にダウンロードするモジュールが、グローバル設定から継承されたモジュールと異なる場合は、ローカル設定に切り替え、[参照]をクリックして目的のモジュールを選択します。

注: サブスクリプション プロキシ用に選択したモジュールに、そのプロキシから更新を取得するクライアントのダウンロードリストで選択されているすべてのモジュールが最低限含まれていることを確認してください。

7. このサーバが継承したものとは異なる HTTP プロキシ サーバを使用してサブスクリプションの更新をダウンロードする場合は、ローカル設定に切り替えて目的の HTTP プロキシを設定します。

8. このサーバが継承したものとは異なるスケジュールを使用してサブスクリプションの更新をダウンロードする場合は、ローカル設定に切り替えてスケジュールを編集します。
9. このサーバが、別の **CA Enterprise Log Manager** サブスクリプション プロキシから更新をダウンロードする場合は、ローカル設定に切り替えて、該当する **CA Enterprise Log Manager** プロキシ サーバを[クライアント更新用サブスクリプション プロキシ]に追加します。

このサーバは、指定されたプロキシ サーバに接続してサブスクリプション更新をダウンロードし、層型のプロキシ構造を形成します。

10. [保存]をクリックします。

オフライン サブスクリプション用のモジュールのダウンロードと選択

オフライン サブスクリプション更新ファイルは、**CA** オフライン サブスクリプション **FTP** サイトで、**.zip** ファイルのパッケージで提供されています。新しいモジュールが利用可能になると、**FTP** フィードに表示されます。使用可能なモジュールのリストを定期的にチェックして、最新の更新がダウンロードされていることを確認します。また、**CA** サポートサイト(<http://ca.com/support>)をチェックして、新しい **Log Manager** サービス パックおよびバージョンが使用可能であるかどうかを確認してください。

オフライン サブスクリプション プロキシ用にダウンロードするモジュールを選択するには、**CA FTP** サイトからオフライン更新ファイル パッケージをダウンロードし、お使いのオフライン プロキシに手動でコピーする必要があります。その後、どのモジュールをダウンロードしてインストールするかを選択できます。反対に、オフライン サブスクリプション クライアントは、そのオフライン プロキシに手動でインストールされたすべての更新を自動的に受信します。ローカルレベルでそのクライアントにどのモジュールが選択されているかは関係ありません。

オフライン サブスクリプション モジュールをダウンロードおよび選択する方法

1. インターネットまたは FTP アクセスに対応するシステムで、FTP オフライン サブスクリプション サイトへ移動します:

`ftp://ftp.ca.com/pub/elm/connectors/ftp/outgoing/pub/elm/ELM_Offline_Subscription`

ディレクトリ インデックスには、主な CA Enterprise Log Manager リリースごとにフォルダが表示されます。

2. 実行する更新用の適切な .zip ファイルをダウンロードします。

注: CA Enterprise Log Manager r12.5 リリース用のフォルダには、サブフォルダと .zip ファイルが含まれています。サブフォルダには、旧バージョンから r12.5 にアップグレードするためのモジュールが含まれます。.zip ファイルには、バージョン r12.5 への定期的なルーチン更新を実行するためのモジュールが含まれます。オフライン サブスクリプションを使用して旧バージョンから r12.5 にアップグレードする場合は、「リリース ノート」の「CA Enterprise Log Manager へのアップグレード」を参照してください。ルーチン更新を実行している場合は、.zip ファイルを選択します。

3. ディスクなどの物理メディア、または scp を使用する場合は、オフライン プロキシ上の以下のファイル パスに .zip ファイルを手動でコピーします。

`/opt/CA/LogManager/data/subscription/offline`

4. CA Enterprise Log Manager 環境内のシステムにログインします。
5. [管理]タブをクリックし、[サービス]サブタブをクリックします。
6. [サブスクリプション サービス]を展開し、設定するオフライン プロキシ サーバを選択します。

選択した CA Enterprise Log Manager サーバの[サブスクリプション サービス 設定]が表示されます。

注: オフライン サブスクリプション クライアントは、そのオフライン プロキシに手動でインストールされたすべてのモジュールを自動的に受信します。プロキシ サーバのコンテンツによって、サブスクリプション クライアントがどの更新を受信するかが制御されます。オフライン クライアントに対してローカルレベルで選択されたモジュールは関係しません。

7. [管理]タブをクリックします。
8. [ファイル]ドロップダウンで、サーバにコピーしたオフライン更新用 .zip ファイルを選択し、[参照]をクリックします。

[ダウンロード可能なモジュール]ダイアログ ボックスが表示されます。

9. ダウンロードするモジュールを選択します。

10. [OK]をクリックします。

[ダウンロード可能なモジュール]ダイアログ ボックスが閉じられ、選択したモジュールが[ダウンロード用に選択したモジュール]リストに表示されます。

11. [保存]をクリックします。

オフライン サブスクリプション クライアントでこれらのモジュールをダウンロードできるようになりました。これは、設定されたサブスクリプション スケジュールに従って自動的に行われるか、またはユーザが手動更新を開始することによってオンデマンドで実行されます。

12. (オプション) [今すぐ更新]をクリックします。

オフライン プロキシ サーバが、選択されたモジュールで自身を更新します。

注: オフライン プロキシによる更新は、設定したサブスクリプション スケジュールに従って自動的に行われるようにできますが、新しいファイルを転送した場合は常に手動更新を実行することをお勧めします。これにより、オフライン サブスクリプション クライアントで更新が要求された場合にその更新が使用可能な状態であることが保証されます。

オンデマンド更新について

オンデマンド更新がスケジュールされた更新と異なる点は、即座に実行され、選択されたサーバのみを更新することです。オンデマンド更新は、一度に 1 つの **CA Enterprise Log Manager** サーバのみを対象として実行できます。サブスクリプション クライアント上でオンデマンド更新を実行するには、まずそのプロキシサーバを更新する必要があります。

通常は、スケジュールされた更新によって、すべてのサーバが最新のバイナリ ファイルで更新され、管理サーバが最新の設定およびコンテンツ ファイルで更新されています。しかし、単一のサーバに対しては、スケジュールされていない更新を実行する方が適している場合もあります。

以下のような場合は、オンデマンド更新の使用を検討してください。

- サブスクリプション イベントが失敗した場合、または管理サーバに関する警告がレポートされた場合。次に例を示します。

EEM サーバへの接続に失敗しました。

EEM のコンテンツのインストール中にエラーが発生しました

管理サーバを選択して、[今すぐ更新]をクリックします。管理サーバがコンテンツ更新用のプロキシとして設定される場合、管理サーバは **CA** サブスクリプション サーバから新しい更新をダウンロードします。その後、管理サーバはコンテンツ更新をコンテンツリポジトリにプッシュします。このサーバがクライアント用のプロキシとして設定される場合、サーバはそのクライアントに先着順にバイナリ更新を提供します。

注: スケジュールされた次の更新セッションまで待機することもできます。次の更新セッション時に、未完了の処理が再開されて完了します。

- サブスクリプション イベント失敗のメッセージが、ダウンロードが中断されたことを示していた場合。ダウンロードが **1** つのプロキシ サーバのみで中断された場合は、オンデマンド更新を実行して、ダウンロードを再試行します。オンデマンド更新は、エラーの発生直後にエラーが通知された場合に実行することをお勧めします。プロキシの開始時刻とクライアント開始時刻の間が十分にある場合、そのプロキシから更新を取得するクライアントによってスケジュールされた更新が開始される前に、プロキシのオンデマンド更新を完了できます。
- 新しい **CA Enterprise Log Manager** をインストールしてプロキシとして設定し、使用する前に最新の更新が適用されていることを確認する場合。
- クライアントが必要とするモジュールがダウンロードするモジュールとして選択されていないことがわかった場合。しかし、そのモジュールがプロキシによってダウンロード対象のモジュールとして選択されている場合。クライアントで[今すぐ更新]を実行し、不足している更新をインストールします。
- オフライン サブスクリプション パッケージをダウンロードし、オフライン サブスクリプション プロキシにコピーした場合。新規ファイルを転送した場合は常にオフライン プロキシ上で手動更新を実行するようにすると、オフライン サブスクリプション クライアントが更新を要求したときにその更新が利用可能であることが保証されます。

オンデマンド更新の開始

[今すぐ更新]機能を使用して、サーバをオンデマンドで更新できます。続けて 2 つ以上のサーバを更新する場合は、次のサーバで処理が始まる前に、前のサーバの処理が完了していることを必ず確認してください。そのためには、自己監視イベントを確認します。

サブスクリプション設定を最近変更した場合は、オンデマンド更新を実行する前に、更新間隔(デフォルトは 300 秒)が経過するまで待機してください。更新が完了すると、CA Enterprise Log Manager によって自己監視イベントが生成されます。

注: スケジュールされた更新が進行中である場合、[今すぐ更新]をクリックしても影響はありません。[今すぐ更新]の処理が進行中に、スケジュールされた更新の開始時刻になった場合、スケジュールされたプロセスは実行されません。オンデマンド処理が完了すると、スケジュールされた更新サイクルが再開します。

重要: ダウンロードするモジュールにコンテンツ更新が含まれる場合は、他のオンデマンド更新を実行する前にコンテンツプロキシを更新します。

サーバをオンデマンドで更新する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [サービスリスト]の[サブスクリプション サービス]を展開します
3. コンテンツ更新用のプロキシであるサーバを選択し、ダウンロード対象として選択されたモジュールを検査します。モジュールにコンテンツ更新が含まれている場合は、[今すぐ更新]をクリックします。

CA サブスクリプション サーバから更新が取得されます。コンテンツ更新用プロキシとして、サーバはコンテンツ更新をコンテンツリポジトリにプッシュします。また、オンラインプロキシとしてバイナリ更新もダウンロードします。

4. 更新するサーバを選択し、そのロールを確認します。
5. ロールがクライアント更新用サブスクリプションプロキシである場合は、[今すぐ更新]をクリックします。

ダウンロードに選択されたモジュールでサーバが更新されます。

6. そのサーバがオンライン プロキシを持つクライアントである場合は、以下を実行します。
 - a. [クライアントのサブスクリプション プロキシ]リストで選択されたアイテムからこのクライアント用のプロキシを特定します。
 - b. クライアントのプロキシを選択し、[今すぐ更新]をクリックします。
 - c. クライアントを選択し、[今すぐ更新]をクリックします。ダウンロードに選択されたモジュールでサーバが更新されます。
7. そのサーバがオフライン サブスクリプション プロキシである場合は、以下を実行します。
 - a. CA オフライン サブスクリプション FTP サイトからオフライン更新パッケージをダウンロードします。
 - b. その更新を、オフライン プロキシの次のダウンロード パスに手動でコピーします。
`.../data/subscription/offline`
 - c. オフライン プロキシを選択し、オフライン更新 .zip ファイルを選択して [参照]をクリックし、目的のモジュールを選択します。
 - d. [今すぐ更新]をクリックします。ダウンロードに選択されたモジュールでサーバが更新されます。
8. そのサーバがオフライン プロキシを持つクライアントである場合は、以下の処理を行います。
 - a. 手順 7 で説明したように、オフライン プロキシを更新します。
 - b. クライアントを選択し、[今すぐ更新]をクリックします。

オフライン プロキシにインストールされたすべてのモジュールでサーバが更新されます。

注: オフライン サブスクリプション クライアントは、そのオフライン プロキシに手動でインストールされたすべてのモジュールを自動的に受信します。オフライン クライアントに対してローカル レベルで選択されたモジュールは関係しません。

更新用の空きディスク領域

ディスクを定期的にクリーンアップすると、CA Enterprise Log Manager サーバでサブスクリプションの更新を正常に行うことができます。サブスクリプションの更新プロセスが開始されたときに使用可能なディスク領域が 5 GB より小さい場合、サブスクリプション サービスは自己監視イベントを発行し、ダウンロード プロセスを一時停止します。

サブスクリプション更新用に十分なディスク領域を確保する方法

1. 定期的に使用可能なディスク領域を監視します。または、使用可能なディスク領域の残量が指定された量を下回った場合に通知するようアクション アラートを設定します。
2. ディスク クリーンアップ ツールを使用して、ディスク領域を解放します。
3. 自己監視イベントによってクリーンアップの必要が警告された場合は、ダウンロードが正常に行われるように十分なディスク領域を解放します。

詳細情報:

[例: ディスク空き容量低下用のアクション アラートの作成 \(P. 463\)](#)

サブスクリプション公開鍵について

サブスクリプション プロキシは、CA サブスクリプション サーバによって使用される秘密鍵に対応する 1 セットの公開鍵を管理します。サブスクリプション プロキシによって、秘密鍵を使用してデジタル署名された ZIP ファイルの形で、サブスクリプション更新がダウンロードされます。更新によって、更新の署名を確認する際に使用する公開鍵が特定されます。署名を検証することで、サブスクリプション プロキシは更新が CA サブスクリプション サーバから提供されていることを確認します。特定のサブスクリプション処理に使用されるのは、1 組の公開鍵/秘密鍵ペアのみです。秘密鍵は更新に署名する際に使用され、公開鍵は署名を検証するために使用されます。公開鍵は各 CA Enterprise Log Manager サーバに保存されており、更新されることもあります。

初期設定の公開鍵は、CA Enterprise Log Manager のインストール時に、サブスクリプション設定ファイルに保存されます。新しい秘密鍵が必要な場合には、新しい鍵を必要とする更新サイクルに先立って、関連する公開鍵がサブスクリプション更新と同時にダウンロードされます。

重要: CA テクニカル サポートからの明確な指示がない限り、サブスクリプションの[公開鍵]フィールドを手動で更新しないでください。

サブスクリプションの自己監視イベント

以下として構成された CA Enterprise Log Manager サーバに関し、サブスクリプション更新プロセスの成否を監視できます。

- デフォルトのサブスクリプション プロキシ
- もしあれば、追加のオンライン サブスクリプション プロキシ
- もしあれば、オフライン サブスクリプション プロキシ
- サブスクリプション クライアント

注: ここで説明するイベントでは、エージェント用のサブスクリプション更新を追跡しません。

以下の内容に対して、成功がレポートされます。

- CA Enterprise Log Manager サーバ(サブスクリプション プロキシおよびサブスクリプション クライアントの両方)のスタートアップおよびシャットダウン
- オンラインまたはオフラインのサブスクリプション プロキシからサブスクリプション クライアントへのコンポーネントの正常なダウンロード
- サブスクリプション クライアントによるコンポーネントの正常なインストール

以下の内容に対して、失敗およびエラーがレポートされます。

- オンラインまたはオフラインのサブスクリプション プロキシからサブスクリプション クライアントへのコンポーネントのダウンロードの失敗
- サブスクリプション クライアントによるコンポーネントのインストールの失敗
- エラー状況

サブスクリプション イベントの監視

サブスクリプション用自己監視イベントを表示することで、サブスクリプション更新プロセスの成否を監視できます。

サブスクリプション処理イベントを監視する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [サービスリスト]の[サブスクリプション サービス]をクリックします。
3. サブスクリプション サービス、または[サブスクリプション サービス]の下に表示されているホストの[自己監視イベント]タブをクリックします。

4. 表示されたイベントの詳細を確認します。

自己監視イベント用に表示されるフィールドの中には、ベンダー間で共通のアクションを表すための CEG による標準的な表現方法が反映されているものがあります。[推奨されるモデル]は、`event_category`、`event_class` (カテゴリ内)、`event_action` (クラス内)、`event_result`、および `event_severity` という階層に基づいています。このレポートに表示される CA 重大度は、CA による重大度解釈です。

CA 重大度

イベントの重大度を指し、以下のように分類されます。

- 不明 - 不明のイベント、CEG にマッピングされていないイベント、または未分類イベント
- 情報 - 一般システム操作情報、セキュリティ関連情報、または通知
- 警告 - 異常な変更、正常だが重大な状況、操作の失敗、またはパフォーマンスの低下
- マイナー インパクト - システム、機能、またはセキュリティへのマイナーの影響
- メジャー インパクト - システム、機能、またはセキュリティへの重大な影響
- クリティカル - 早急な対応が必要です。セキュリティ違反の可能性があります。

日付

イベントが発生した日付

受信者

現在のプロセスを正常に完了できなかったコンポーネント。これはサブスクリプション プロキシまたはサブスクリプション クライアントのどちらかである可能性があります。サブスクリプション プロキシである場合は、デフォルトのプロキシ、オンライン プロキシ、またはオフライン プロキシのいずれかである可能性があります。

受信側ホスト

受信側である CA Enterprise Log Manager サーバのホスト名

カテゴリ

イベントのカテゴリ。設定管理は、サブスクリプション サービス イベントの `event_category` です。

ユーザ

イベント情報に指定されたアクションを開始したユーザ名またはユーザ ID です。これは、CEG の `source_username` フィールドです。

アクション

イベントが生成される原因となったアクション。これは、CEG の `event_action` フィールドです。

結果

成功の場合は **S**、失敗の場合は **F**。イベントアクションの結果は、CEG の `event_result` フィールドです。アクションは、ほかに「許可」、「拒否」、「削除」、および「不明」があります。

結果の説明

メッセージテキスト。[結果]列に「失敗」と表示されている場合は、[結果の説明]を確認します。

5. イベントビューアに詳細が表示されます。ここで、更新の開始時間などの設定値に加えた変更といった変更を表示できます。

```
属性 [UpdateStartTime] の設定変更 新しい値 :[17] はサブスクリプションのために calmsunbulktest01 のローカル ファイルに更新されました
event_category=Configuration Management,event_class=Configuration Management,event_action=Configuration Change,event_sequence=Configuration Change,ideal_model=Security Management
System,event_count=1,event_logname=CALM,event_summarized=F,receiver_name=Subscription,receiver_version=12.0.0.19,receiver_hostname=calmsunbulktest01,receiver_hostaddress=130.200.137.21
1,receiver_hostdomainname=ca.com,receiver_timezone=
14400,receiver_time_gmt=1202765006,receiver_processid=3922,receiver_processname=igateway,dest_objectclass=Subscription,dest_objectname=Subscription,event_source_hostname=calmsunbulktest
01,event_result=S,result_string= Configuration change for Attribute [UpdateStartTime] New value :[17] has been updated successfully to local file on calmsunbulktest01 for Subscription
```

サブスクリプション イベントの詳細の表示

サブスクリプションを設定すると、自己監視イベントを表示できます。サブスクリプションの更新後に、更新が各サーバに正常に完了されたことを確認できます。アップグレードが完了したら、影響を受ける各サーバで、以下の自己監視イベントメッセージを確認します。

- <component> は、<proxyname> プロキシに正常にダウンロードされ、EEM にインストールされました。
- <component> は、<proxyname> プロキシに正常にダウンロードされました。
- <component> は、<clientname> クライアントに正常にインストールされました。

また、トラブルシューティングの目的で、サブスクリプションの自己監視イベントを表示できます。

イベントビューアにサブスクリプション イベントの詳細を表示する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [サービスリスト]の[サブスクリプション サービス]をクリックします。
3. サブスクリプション サービス、または[サブスクリプション サービス]の下に表示されているホストの[自己監視イベント]タブをクリックします。
4. [結果の説明]列を確認します。たとえば、この列には、「サブスクリプション クライアントに、更新を取得するよう選択されたモジュールがありません」などのイベントが表示される場合があります。

結果の説明
Subscription Client - calmrhbuildtest01 is communicating with the proxy - calmrhbuildtest01 for getting the Subscription updates.
Subscription client has no modules selected for getting updates. Please select the modules for getting the updates from the Proxy.
Unable to connect to the specified RSSFeed URL. Please check the URL again.
Unable to connect to the specified RSSFeed URL. Please check the URL again.
No modules are selected for getting updates. Please select the modules for getting the updates from the Subscription server.

5. 詳細を確認する結果説明をダブルクリックします。
イベントビューアが開きます。

6. 結果セクションにスクロール ダウンし、`result_string` 用に表示されたテキストを確認します。

イベントビューア - イベント詳細 - System Self Monitoring Events Detail		
コピー ☒ 空の行を表示しない		
表示	名前	値
☒	event_result	F
☒	result_string	Subscription client has no modules selected for getting updates. Please select the modules for getting the updates from the Proxy. If the modules are not available in the list to be selected, add a valid RSS Feed URL to the Subscription global configuration. If the proxy (to which this client is polling) is offline, then manually copy the updates to the download path(for the modules to appear).

エージェントおよびコネクタへのサブスクリプション更新の適用

定期的な更新、サービスパック、およびポイントリリースは、すべてサブスクリプションによって提供されます。ダウンロードするモジュールには、通常、エージェントおよび統合が含まれます。エージェントを管理するサブスクリプションクライアントにこれらのモジュールをダウンロードする場合、エージェントを管理するサブスクリプションクライアントが正常に更新されていることを確認してから、エージェントにこれらの更新を適用する必要があります。エージェントの更新は、コネクタの更新の前に適用される必要があります。

サブスクリプション更新を使用して CA Enterprise Log Manager エージェントをアップグレードする方法

1. アップグレードにエージェント モジュールが含まれている場合は、以下の要領で、プラットフォーム別にエージェントを更新します。
 - a. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
 - b. エージェント更新をすべてのエージェントに一度に適用するか、選択したエージェントグループまたは個別のエージェントに適用するかを、単一のプラットフォームが該当するレベルに応じて決定します。
 - エージェントがすべて同じプラットフォームにインストールされている場合は、[エージェント エクスプローラ]を選択し、[サブスクリプション]をクリックします。
 - エージェントグループが同じプラットフォームにインストールされたエージェントから構成されている場合は、[エージェント エクスプローラ]を選択し、[エージェントグループ]を選択して、[サブスクリプション]をクリックします。
 - 上記以外の場合は、[エージェント エクスプローラ]を展開し、[エージェントグループ]を展開して、[エージェント]を選択し、[サブスクリプション]をクリックします。
- サブスクリプションウィザードが表示されます。
- c. [エージェント エクスプローラ]または[エージェントグループ]を選択した場合は、[エージェントの更新]を選択し、[プラットフォーム]ドロップダウンリストからプラットフォームを選択して、[検索]をクリックし、[バージョンの選択]手順をクリックします。
 - d. [エージェント]を選択した場合は、[エージェントの更新]を選択し、[バージョンの選択]手順をクリックします。
 - e. リスト表示された各エージェントで、[バージョンの更新]を選択します。
 - f. [保存して閉じる]をクリックします。

- g. 成功を確認します。[ステータスとコマンド]をクリックします。[設定の成功]をクリックします。適用された設定のバージョンを確認します。
 - h. すべてのエージェントの更新に必要なだけ繰り返します。
2. アップグレードに統合モジュールが含まれている場合は、以下の要領で、エージェントのコネクタを更新します。
- a. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
 - b. コネクタの更新をすべてのエージェント上のすべてのコネクタに一度に適用するか、選択したエージェントグループ内のエージェントのコネクタまたは個別のエージェントのコネクタに適用するかを決定します。
 - c. [エージェント エクスプローラ]、[エージェントグループ]、または[エージェント]を選択します。次に、[サブスクリプション]をクリックします。
 - d. [更新選択リスト]から[コネクタの更新]を選択します。
 - e. 必要に応じて、以下のドロップダウンリストの 1 つ以上から値を選択し、デフォルトの[すべて]、[エージェントグループ]、[プラットフォーム]、[統合]を変更します。[検索]をクリックします。
 - f. [バージョンの選択]手順をクリックします。
 - g. [すべて選択]をクリックしてリストのメンバすべてを選択するか、更新するコネクタに対応する行を個別に選択します。 個別に選択した行には、適用する更新バージョンを選択します。
 - h. [保存して閉じる]をクリックします。
3. 更新を確認します。サブスクリプション ウィザードを再度実行します。[バージョンの選択]手順を選択して現在のバージョンを表示し、表示されたバージョンが更新用に選択したバージョンであることを確認します。[キャンセル]をクリックします。

詳細情報:

[サブスクリプション更新を適用する方法](#) (P. 657)

[更新リストウィザードの表示](#) (P. 658)

[更新するエージェントまたはコネクタの選択](#) (P. 659)

[エージェントまたはコネクタ統合のバージョンの更新](#) (P. 660)

第 8 章：フィルタおよびプロファイル

このセクションには、以下のトピックが含まれています。

[グローバルフィルタおよびローカルフィルタ](#) (P. 247)

[プロファイルの作成方法](#) (P. 251)

[プロファイルのインポート](#) (P. 255)

[プロファイルのエクスポート](#) (P. 256)

[プロファイルの設定](#) (P. 257)

[グローバルフィルタの作成](#) (P. 258)

[グローバルクエリに関する値の設定](#) (P. 260)

[グローバルフィルタの編集](#) (P. 261)

[グローバルフィルタの削除](#) (P. 261)

[ローカルフィルタの作成](#) (P. 262)

[ローカルフィルタの編集](#) (P. 263)

[ローカルフィルタの削除](#) (P. 263)

第 9 章: グローバル フィルタおよびローカル フィルタ

フィルタを設定または編集して、表示されるイベントまたはインシデント情報を絞り込むことができます。メイン **CA Enterprise Log Manager** ウィンドウからグローバル フィルタのダイアログ ボックスにアクセスできます。ローカル フィルタは、個々のクエリまたはレポート内、または[インシデント]領域から追加できます。また、グローバル フィルタ インターフェースを使用して、アプリケーション内のすべてのクエリ設定を設定することができます。

各タイプのフィルタには独自の作成ダイアログ ボックスがあり、専用のボタンから起動します。

グローバル フィルタ

現在のセッションのみで表示するすべてのレポートまたはクエリに適用され、さまざまなタイプのイベントを同一の方法で表示できます。[グローバル フィルタ]ボタンはメイン **CA Enterprise Log Manager** ウィンドウの上部にある[Log Manager サーバ]メニューの横に表示されます。グローバル フィルタを使用して、たとえば、先週に受信したイベントや特定のホストから受信したイベントをすべて表示できます。また、インシデント用のグローバル フィルタ(構造は同じ)も設定できますが、それらはインシデントおよびそのコンポーネント イベント情報にのみ適用されます。

注: グローバル フィルタのデフォルト設定では、過去 6 時間分のデータが返されます。

ローカル フィルタ

現在のレポート、クエリ、またはインシデントビューにのみ適用されます。[ローカル フィルタ]ボタンは、クエリまたはレポート内の詳細ペイン、および[インシデント]ペインの最上部に表示されます。新しいレポートを表示するとき、ローカル フィルタが適用または保存されるようにするには、レポートをそのフィルタ セットと共に気に入りとして保存しておく必要があります。ローカル フィルタにより、たとえば、他のレポートビューを変更することなく、マルチホストレポートビューに 1 つのホストのみが表示されるように、現在のビューを絞り込むことができます。

このセクションには、以下のトピックが含まれています。

[単純フィルタについて](#) (P. 248)

[単純フィルタの設定](#) (P. 249)

[プロファイルフィルタについて](#) (P. 250)

単純フィルタについて

クエリの設計ウィザードまたはプロファイルの設計ウィザードを初めて使用する場合は、事前に、単純フィルタタイプについて十分に理解してください。

単純フィルタの例

各タイプの単純フィルタの例を、以下に示します。

フィルタタイプ	値	説明
推奨されるモデル	アンチウイルス	以下のような製品が生成するイベント データのみを表示します。 ■ CA Anti-Virus ■ McAfee VirusScan ■ Symantec Antivirus Corporate Edition ■ Trend Micro OfficeScan
イベント カテゴリ/ イベント クラス	システム アクセス/ログイン アクティビティ	システムにログインしているユーザに関連するイベント データのみを表示します。
イベント ログ名	Cisco PIX Firewall	Cisco PIX Firewall デバイスが生成するイベント データのみを表示します。

イベント ログ名以外は、フィルタタイプは共通イベント文法 (CEG) に基づいています。

- 製品テクノロジ ベースフィルタについて理解するには、「推奨されるモデル リスト」を参照してください。
- 製品カテゴリ/クラス/アクション ベースフィルタについて理解するため、「イベント クラスリスト」および「イベント クラスリスト」を参照してください。

これらのリストは、「共通イベント文法」セクション下のオンライン ヘルプにあります。

単純フィルタの設定

単純フィルタを設定し、表示やレポートが必要なイベント データの条件を設定できます。単純フィルタをクエリ の設計ウィザードで設定すると、レポートやアラートで使用されたクエリによって返されるイベント データを制限できます。単純フィルタをプロファイルの設計ウィザードで設定すると、プロファイルが適用されたときに、レポートやクエリ結果に表示されるイベント データが制限されます。

1. ウィザードを開きます。
 2. 設定する単純フィルタのタイプを決定します。
 - テクノロジ ベース
 - カテゴリ ベース、カテゴリおよびクラス ベース、またはカテゴリ、クラス、およびアクション ベース
 - 製品 ベース
 3. テクノロジ ベースのフィルタを設定するには、[推奨されるモデル]チェックボックスをオンにして、[推奨されるモデル]ドロップダウンリストから値を選択します。
 4. 「セキュリティ イベント カテゴリ」、「カテゴリおよびクラス」、または「カテゴリ、クラス、およびアクション」をベースにフィルタを設定するには、以下を実行します。
 - a. [イベント カテゴリ]チェック ボックスをオンにし、関連するドロップダウンリストから値を選択します。
 - b. (オプション)。[イベント クラス]チェック ボックスをオンにし、ドロップダウンリストから値を選択します。
 - c. (オプション)。[イベント クラス]チェック ボックスをオンにした場合は、[イベントアクション]チェック ボックスをオンにし、ドロップダウンリストから値を選択します。
- 注:** テクノロジ ベースフィルタで、このタイプ フィルタを設定することもできます。
5. 製品ベースのフィルタを設定するには、[イベント ログ名]チェック ボックスをオンにして、ドロップダウンリストから値を選択します。
 6. ウィザードを完了します。

プロファイル フィルタについて

プロファイルはフィルタのセットです。タグ フィルタ、データ フィルタ、またはその組み合わせを持つプロファイルを作成できます。クエリタグ フィルタを使用すると、選択用に表示されるクエリが制限され、レポートタグ フィルタを使用すると、選択用に表示されるレポートが制限されます。データ フィルタを使用すると、レポートまたはクエリ結果に表示されるデータが制限されます。プロファイル フィルタは、クエリ、レポート、スケジュール済みアラート、およびスケジュール済みレポートに適用されます。

レポート用およびクエリ用のタグ フィルタを個別に選択できます。タグ フィルタには以下のものがありますが、これらに限定されるわけではありません。

- COBIT、FISMA、GLBA、HIPAA、NERC、PCI、SAS、SOX 70、SOX などの標準ベースのタグ
標準ベースのタグ フィルタは、クエリタグではなくレポートタグに適用されます。
- コンテンツ セキュリティ、ホスト セキュリティ、ネットワーク セキュリティ、運用 セキュリティ、リソース アクセス、システム アクセスなどのセキュリティ イベント カテゴリ タグ
- CA Access Control、CA Identity Manager、CA SiteMinder などの製品タグ

単純なデータ フィルタを選択するか、詳細なデータ フィルタを作成できます。それぞれについての簡単な説明を以下に示します。

- 単純なデータ フィルタは、以下のいずれかをベースにできます。
 - 選択されたテクノロジー(システム ソフトウェア、ホスト アプリケーション ソフトウェアおよびサービス、ネットワーク アプリケーション ソフトウェアおよびサービス)
 - 選択された CEG イベント カテゴリ、選択された CEG イベント カテゴリおよびクラス、選択された CEG イベント カテゴリ、クラスおよびアクション
 - 選択された製品
- 詳細なデータ フィルタは、1 つ以上の WHERE 句から構成されたユーザ定義 SQL クエリをベースにします。WHERE 句は、CEG 列、選択した演算子、および指定した値で構成し、クエリではこれに基づいて CEG 列が選択されます。

プロフィールの作成方法

環境のニーズに従ってプロフィールを作成できます。プロフィールを使用すると **CA Enterprise Log Manager** ビューを絞り込むことができます。たとえば、アクセス制御に関連するレポート、クエリ、およびイベントのみを表示する **CA Access Control** プロフィールを作成できます。

プロフィール ウィザードを使用して、プロフィールを作成するプロセスは、以下の手順で構成されます。

1. プロフィール ウィザードの表示
2. プロファイル名の指定および説明情報の入力
3. 単純フィルタや詳細フィルタを使用して表示される情報の特定
4. タグ フィルタを使用して表示されるクエリおよびレポートの指定

詳細情報:

[プロフィールの詳細の追加](#) (P. 252)

[データフィルタの作成](#) (P. 253)

[タグ フィルタの作成](#) (P. 254)

プロフィール ウィザードを開きます。

プロフィールを新規作成、または既存のプロフィールを編集するには、プロフィール ウィザードを開く必要があります。

プロフィール ウィザードを開く方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。

ライブラリフォルダリストが表示されます。

2. [プロフィール]フォルダを選択します。

[プロフィール]ボタンが[詳細]ペインに表示されます。

3. [新規プロフィール]ボタンをクリックします。 

プロフィール ウィザードが開きます。

ウィザードの使用時の操作

- ウィザードを閉じずにルール ファイルを保存するには、[保存]をクリックします。
- ルール ファイルを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

プロフィールの詳細の追加

プロフィールに名前を付ける方法 参照用に、任意で説明情報を入力することもできます。

プロフィールに名前を付ける方法

1. プロフィール ウィザードを開きます。
2. 新しいプロフィールの名前を入力します。名前は最大 80 文字までで、特殊文字を含めることができます。
3. (オプション)説明情報を入力します。
4. [データフィルタ]手順に進みます。

データ フィルタの作成

単純フィルタや詳細フィルタを使用して、プロファイルに表示される情報をフィルタできます。各プロファイルには、少なくとも 1 つのフィルタが設定されている必要があります。

プロファイル データ フィルタの設定方法

1. プロファイル ウィザードを開きます。
2. まだ指定していない場合はプロファイル名を入力してから、「データ フィルタ」の手順に進みます。
[フィルタ]ダイアログ ボックスが開いて、[単純フィルタ]タブが表示されます。
3. 必要な単純フィルタを作成します。たとえば、[イベント ログ名]チェック ボックスをオンにし、「CA Access Control」と入力して、CA Access Control のイベントを検索できます。
4. (オプション) [詳細フィルタ]タブをクリックします。
[詳細フィルタ]ダイアログ ボックスが表示されます。
5. 必要に応じて詳細フィルタを作成します。
6. 適切な矢印をクリックして次に実行するウィザード手順に進むか、[保存して閉じる]をクリックします。
[保存して閉じる]をクリックすると、新規プロファイルがリストに表示されます。それ以外の場合は、選択したウィザード手順が表示されます。

詳細情報

[単純イベント フィルタの作成](#) (P. 569)

[詳細イベント フィルタの作成](#) (P. 572)

[詳細フィルタの使用](#) (P. 487)

タグ フィルタの作成

プロファイル用のタグ フィルタを作成し、ユーザがプロファイルを適用したときに CA Enterprise Log Manager インターフェースに表示されるクエリまたはレポートのカテゴリ タグを制御できます。たとえば、CA SiteMinder 用のタグ フィルタを作成すると、CA Enterprise Log Manager インターフェースには、CA SiteMinder タグがあるレポートおよびクエリのみが表示されます。

タグ フィルタの作成方法

1. プロファイル ウィザードを開きます。
2. まだ指定していない場合はプロファイル名を入力してから、[タグ フィルタ] の手順に進みます。

[フィルタ]ダイアログ ボックスが開いて、[レポートタグ フィルタ]サブタブが表示されます。
3. [新規イベントフィルタ]をクリックします。

タグ フィルタ テーブルの 1 行目がアクティブになります。
4. [タグ]セルをクリックし、表示するクエリまたはレポートのタグ名を選択するか、入力します。入力する場合、入力するに従って使用可能なタグ名が絞り込まれて表示されます。
5. (オプション) [新規イベントフィルタ]を再度クリックし、さらに詳細なフィルタを追加します。

タグ フィルタ テーブルの 2 行目がアクティブになり、[ロジック]列に「AND」と表示されます。
6. (オプション) [ロジック]セルをクリックし、演算子「AND」または「OR」のどちらかを選択します。
7. (オプション) [タグ]セルをクリックし、表示するタグ名を選択するか、入力します。入力する場合、入力するに従って使用可能なタグ名が絞り込まれて表示されます。
8. (オプション) 左かっこおよび右かっこのセルをクリックして、必要なかっこの数を入力します。
9. (オプション) [クエリタグ フィルタ]サブタブをクリックし、手順 3 から手順 8 を繰り返して、必要なクエリタグ フィルタを作成します。
10. すべてのフィルタ ステートメントを入力したら、[保存]をクリックします。

詳細情報:

[データフィルタの作成](#) (P. 253)

プロファイルのインポート

プロファイルをインポートすることで、ある環境から別の環境にプロファイルを移動することができます。たとえば、テスト環境で作成したプロファイルをライブ環境にインポートできます。

プロファイルをインポートする方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。
ライブラリフォルダリストが表示されます。
2. [プロファイル]フォルダの横の矢印をクリックして、そのフォルダを展開します。
[プロファイル]ボタンが[詳細]ペインに表示されます。
3. [プロファイルのインポート]をクリックします。
[ファイルのインポート]ダイアログ ボックスが表示されます。
4. インポートするファイルを参照し、[OK]をクリックします。
プロファイル ウィザードが表示され、選択したプロファイルの詳細が表示されます。
5. 必要な変更を行い、[保存して閉じる]をクリックします。インポートしたプロファイルの名前が管理データベース内に存在するプロファイルと同じ場合は、名前の変更を要求するメッセージが表示されます。
インポートしたプロファイルが、適切なフォルダに表示されます。

プロフィールのエクスポート

プロフィールをエクスポートできます。これによって、環境間でプロフィールを共有できます。たとえば、テスト環境で作成したプロフィールをライブ環境にエクスポートできます。

プロフィールをエクスポートする方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。
ライブラリフォルダリストが表示されます。
2. [プロフィール]フォルダの横の矢印をクリックして、そのフォルダを展開します。
プロフィールフォルダが表示されます。
3. エクスポートするプロフィールが含まれているフォルダをクリックします。
フォルダが展開され、各ファイルが表示されます。
4. エクスポートするプロフィールを選択し、[プロフィールのエクスポート]をクリックします。
[エクスポートの場所]ダイアログボックスが表示されます。
5. エクスポートされるプロフィールを保存する場所を入力または参照し、[保存]をクリックします。
エクスポートの成功を確認するダイアログボックスが開きます。
6. [OK]をクリックします。
プロフィールがエクスポートされます。

プロファイルの設定

使用可能なプロファイルを選択して環境に適用し、プロファイルの期間に応じて使用可能なクエリとレポートを制限できます。プロファイルを設定するには、メイン **CA Enterprise Log Manager** ウィンドウ上部の[プロファイル]ドロップダウンメニューから必要なプロファイルを選択します。

注: 選択したプロファイルをデフォルトプロファイルに設定するには、**CA Enterprise Log Manager** メイン ウィンドウ上部にある[デフォルトプロファイルに設定]オプションをクリックします。選択したプロファイルが、ログインしているユーザのデフォルトプロファイルに設定されます。

グローバルフィルタの作成

グローバルフィルタを作成できます。グローバルフィルタを使用すると、すべてのクエリおよびレポート、またはインシデントを同一の条件で表示できます。グローバルフィルタを作成する場合は、イベントまたはインシデントのどちらに適用されるかどうかを選択します。単一のグローバルフィルタを両方に適用することはできません。また、グローバルフィルタ インターフェースを使用して、アプリケーション内のすべてのクエリ設定を設定することができます。

グローバルフィルタの作成方法

1. メイン ウィンドウ 上部の[グローバル フィルタ]ボタンをクリックします。
[グローバル フィルタ および 設定] ダイアログ ボックスが表示されます。
2. [イベント] タブ または [インシデント] タブ をクリックして、グローバル フィルタ の適用先を選択します。
3. フィルタによる検索時間を、[時間帯] ドロップダウン リストを使用して指定します。
4. [一致] チェック ボックス をオン にして、使用可能なすべての元のイベントをフィルタする条件となる値を入力します。

注： 専用の一致構文を使用することによって、元のイベントの複数の値、句、または部分的な値を検索できます。

5. [フィルタの追加] をクリックしてフィルタに含めるイベント フィールド を指定します。

[列] ドロップダウン メニュー および [値] エントリ フィールド が表示されます。

6. フィルタに使用するイベント フィールド を選択し、フィルタ後のレポートに表示するフィールドを、フィールドに含まれる値で指定します。[フィルタの追加] を再度クリックすると、複数のイベント フィールド 名 および 値 を入力できます。[除外] ボタン をオン にすると、選択したイベント フィールド 名 に入力した値を除くすべての値が含まれます。

注： 文字列型フィールドでグローバル フィルタを作成した場合、[クイック フィルタ] リスト に追加されます。数値または時刻フィールドでグローバル フィルタを作成した場合、[詳細フィルタ] リスト に追加されます。

7. (オプション) [詳細フィルタ] タブ をクリックし、より詳細なフィルタ条件を追加します。
8. (オプション) [設定] タブ をクリックし、グローバル 設定 を選択します。これらの設定は、アプリケーション全体に適用されます。

9. (オプション) 今後のセッションのために、同一ユーザとしてログインしている間フィルタ設定を保持するには、ダイアログ ボックス下部の[デフォルトに設定]を選択します。
10. [保存]をクリックします。
[グローバル フィルタおよび設定]ダイアログ ボックスが閉じ、新しいフィルタがレポートに適用されます。

詳細情報:

[詳細フィルタの使用 \(P. 487\)](#)

[グローバル クエリに関する値の設定 \(P. 260\)](#)

グローバル クエリに関する値の設定

[グローバル フィルタ]ダイアログ ボックスを使用すると、環境内のすべてのレポートおよびクエリに適用する、アプリケーション全体にわたる条件を設定できます。デフォルトとして設定しない限り、グローバル設定は現在のセッションに適用されます。

グローバル クエリ設定の定義方法

1. メイン ウィンドウ上部の[グローバル フィルタ]ボタンをクリックします。
[グローバル フィルタおよび設定]ダイアログ ボックスが開いて[クイック フィルタ]タブが表示されます。
2. [設定]タブをクリックします。
タブが開き、以下の値が表示されます。

ローカル タイム ゾーン

レポートとクエリのすべての日付/時間フィールド用のタイムゾーンを制御します。レポートとクエリでは、CA Enterprise Log Manager サーバのタイムゾーンではなく、ドロップダウンリストから選択したタイムゾーンが採用されます。

連携されたデータにクエリを実行

使用可能なすべての連携サーバにクエリを適用できるようになります。この設定は、デフォルトでは有効になっています。この設定をオフにすると、ローカル イベント ログ ストアに保存されたイベント データのみがクエリの対象となります。これによって、ターゲット イベントがローカルであることがわかっている場合には、ローカル イベント ログ ストアをすばやく確認できます。

クエリの自動リフレッシュの有効化

クエリごとに設定された間隔で表示を自動的にリフレッシュすることができます。

3. (オプション)設定をデフォルトとして現在のセッションの後も保持するには、ダイアログ ボックス下部の[デフォルトに設定]を選択します。
4. 必要に応じて変更を加え、[保存]をクリックします。
[グローバル フィルタおよび設定]ダイアログ ボックスが閉じ、新しいフィルタが適用されます。

グローバルフィルタの編集

既存のグローバルフィルタを編集できます。

グローバルフィルタの編集方法

1. メインウィンドウ上部の[グローバルフィルタ]ボタンをクリックします。
[グローバルフィルタおよび設定]ダイアログボックスが開いて[クイックフィルタ]タブが表示されます。
2. 必要に応じてパラメータを変更または追加します。個々のクイックフィルタパラメータは、その隣にある[削除]アイコンをクリックして削除できます。
3. [保存]をクリックします。
[グローバルフィルタおよび設定]ダイアログボックスが閉じ、編集されたフィルタが適用されます。

グローバルフィルタの削除

グローバルフィルタを削除し、すべてのレポートをデフォルトの状態に戻すことができます。

グローバルフィルタを削除するには、CA Enterprise Log Manager メインウィンドウ上部の[グローバルフィルタのクリア]をクリックします。

ローカル フィルタの作成

ローカル フィルタを作成すると、表示しているクエリまたはレポート、または[インシデント]領域に表示されているインシデントのスコープを絞り込むことができます。

ローカル フィルタの作成方法

1. フィルタするクエリまたはレポートを開くか、[インシデント]タブをクリックし、ペイン上部の[ローカル フィルタ]ボタンをクリックします。
[ローカル フィルタ]ダイアログ ボックスが開いて、[クイック フィルタ]タブが表示されます。
2. (オプション) イベントではなく表示されているインシデントをフィルタする場合は、[インシデント]タブをクリックします。
3. (オプション) [一致]チェック ボックスをオンにし、イベントまたはインシデントの検索条件となる値を入力します。

注: 専用の一致構文を使用することによって、複数の値、句、または部分的な値を検索できます。

4. [フィルタの追加]をクリックします。
5. フィルタに使用するイベントフィールドを選択し、フィルタ後のレポートに表示するフィールドを、フィールドに含まれる値で指定します。[フィルタの追加]を再度クリックすると、複数の列の値を入力できます。[除外]ボタンをオンにすると、選択したイベントフィールド名に入力した値を除くすべての値が含まれます。
6. (オプション) [詳細フィルタ]タブをクリックし、より詳細なフィルタ条件を追加します。
7. [保存]をクリックします。

フィルタが表示に適用されます。[お気に入り]に設定することで、このレポート表示を保存できます。

ローカル フィルタの編集

既存のローカル フィルタを編集できます。

ローカル フィルタの編集方法

1. クエリまたはレポート ペイン、または[インシデント]ビューの最上部にある[ローカル フィルタ]ボタンをクリックします。
[ローカル フィルタ]ダイアログ ボックスが開いて、[クイック フィルタ]タブが表示されます。
2. 必要に応じて値を変更または追加します。個々のフィルタ設定は、[削除]アイコンをクリックするか、またはチェック ボックスをオフにして一致の値を削除することによって、削除できます
3. [保存]をクリックします。

編集したフィルタが表示に適用されます。

ローカル フィルタの削除

ローカル フィルタを削除し、クエリ、レポート、またはインシデントビューを前の状態に戻すことができます。

ローカル フィルタを削除するには、表示しているクエリ、レポート、またはインシデントの最上部にある[ローカル フィルタのクリア]ボタンをクリックします。

第 10 章：クエリおよびレポート

このセクションには、以下のトピックが含まれています。

[クエリおよびレポートについて](#) (P. 266)

[タグ タスク](#) (P. 270)

[クエリの表示](#) (P. 270)

[レポートの表示](#) (P. 272)

[選択されたレポートの表示の無効化](#) (P. 273)

[例：PCI レポートの実行](#) (P. 274)

[プロンプト](#) (P. 278)

[クエリの作成方法](#) (P. 295)

[クエリの編集](#) (P. 313)

[カスタム クエリの削除](#) (P. 313)

[選択されたクエリの表示の無効化](#) (P. 314)

[クエリ定義のエクスポートとインポート](#) (P. 314)

[レポートの作成方法](#) (P. 317)

[例：既存のクエリによるレポートの作成](#) (P. 320)

[例：連携および連携されたレポートの設定](#) (P. 323)

[レポートの編集](#) (P. 328)

[カスタム レポートの削除](#) (P. 328)

[レポート定義のエクスポート](#) (P. 330)

[レポート定義のインポート](#) (P. 331)

[キー設定済みリストのあるレポートの使用準備](#) (P. 332)

[キー設定済みリストを使用したレポートの表示](#) (P. 349)

クエリおよびレポートについて

以下の方法でクエリを使用できます。

- クエリを実行して、イベントまたはインシデント データをほぼリアル タイムで表示できます。
- 事前定義済みレポートを選択して、複数の関連するクエリの結果を表示できます。
- 選択したクエリから構成されるレポートを作成できます。
- プロンプトクエリを使用して、事前に選択した特定の情報を検索できます。
- 最新のデータにクエリを実行するようスケジュールし、責任者に電子メールで通知するアクション アラートを発行できます。アクション アラートは、サードパーティ製のリーダを使用して表示できる RSS フィードにも追加されます。
- アクション アラートを表示、レポート、または作成する独自のクエリを作成できます。

クエリおよびレポートには以下の 2 つのタイプがあります。

- サブスクリプション クエリおよびレポートは、CA によって事前に定義され、インストール時に CA Enterprise Log Manager アプリケーションと共にインストールされるか、サブスクリプション更新で追加されます。
- ユーザ クエリおよびレポートは、ユーザが作成します。クエリやレポートは、まったく新しく作成することも、ベースとなるサブスクリプション クエリやレポートに変更を加えて作成することもできます。

CA Enterprise Log Manager では、サブスクリプションによって幅広いクエリとレポートのリストを提供しています。Auditor、Analyst、または Administrator のロールを割り当てられている場合は、すべてのサブスクリプション クエリおよびレポートを表示できます。さらに、表示されているサブスクリプション クエリまたはレポート上で、以下の操作を実行できます。

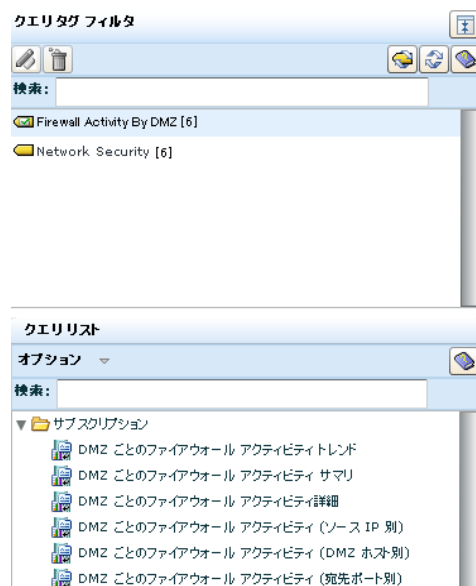
- 表示されているデータのリフレッシュ
- ローカル フィルタを編集して、表示させないデータを非表示にする
- ローカル フィルタをクリアして、フィルタされていないクエリまたはレポートを再表示する
- 表示されているクエリまたはレポートをお気に入りのリストに追加する
- クエリの印刷
- 選択したクエリまたはレポートを表示するオプションを変更する
- 表示されたクエリまたはレポートを閉じる

以下の操作は、Analyst または Administrator のロールを割り当てられているユーザのみ実行できます。

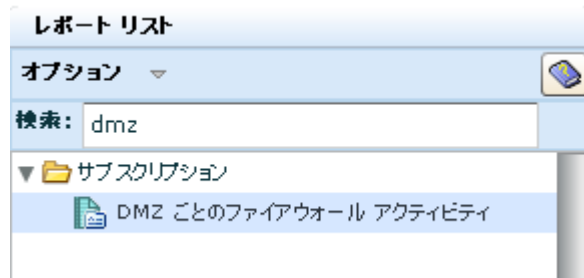
- ユーザ クエリまたはレポートをゼロから新規作成する
- サブスクリプション クエリまたはレポートをコピーし、ユーザ クエリまたはレポートのベースとして使用する
- ユーザ クエリまたはレポートの編集
- ユーザ クエリまたはレポートのエクスポート
- ユーザ クエリまたはレポートの削除
- 選択したユーザ クエリまたはレポートへの変更の保存
- ユーザ クエリまたはレポートの定義のインポート

クエリおよび関連するレポートの例

「DMZ ごとのファイアウォール アクティビティ」というクエリ タグについて考えます。タグが、このトピックに関する 6 つの個別クエリに関連付けられていることに注目してください。



クエリリストに表示されるクエリは、レポートで使用されています。[レポート]タブから、「DMZ ごとのファイアウォール アクティビティ」というレポートを表示できます。



以下の図では、名前だけが表示されています。各名前が、レポート内の 6 つのクエリのうちの 1 つを反映していることに注目してください。レポートには通常、サマリ、トレンド、および詳細のクエリ結果が含まれています。

DMZ ごとのファイアウォール アクティビティ



タグ タスク

タグを使用すると、レポートやクエリをカテゴリに関連付けて参照を容易にしたり、お使いの環境に関するレポート用に組織のフレームワークを提供したりすることができます。また、カテゴリタグによって、仕事をロール別やイベントのタイプ別に簡単に分類することもできます。

レポートまたはクエリには、事前定義されたタグを使用するか、または独自のカスタムタグを作成することができます。たとえば、[月単位]タグを作成して、毎月のスケジュールが必要なレポートに追加すれば、参照や表示が容易になります。これによって、ジョブ自体を編集しなくても、[月単位]タグを新しいジョブに追加したり、不要になったジョブから削除したりするだけで、レポートジョブにレポートを追加したり削除したりすることができます。

個々のクエリやレポート用のカスタムタグは、クエリまたはレポートの作成プロセスや、編集プロセスの間に追加できます。新しいタグを作成すると、タグのタイトルがタグリストに表示され、そのタグを選択してほかのレポートやクエリに追加できるようになります。

カスタムタグの名前は、変更や削除が可能です。レポートやクエリを編集して、カスタムタグをレポートやクエリから削除できます。

クエリの表示

Auditor、Analyst、または Administrator のロールを割り当てられているすべてのユーザは、すべてのクエリを表示できます。事前定義済みクエリが、[サブスクリプション]フォルダの下にリスト表示されます。最初のカスタムクエリを定義すると、カスタムクエリの保存用として[ユーザ]フォルダがクエリリストに追加されます。これ以降、カスタムクエリはすべてこの[ユーザ]フォルダに追加されます。

クエリの表示方法

1. [クエリおよびレポート]タブをクリックし、[クエリ]サブタブをクリックします。
[クエリ タグ フィルタ]の最大化ボタン、[クエリ リスト]、[オプション]メニュー、および[検索]テキストボックスが、左側ペインに表示されます。

2. 以下の方法のいずれかで、表示するクエリを選択します。
 - クエリリストをスクロールし、表示するクエリを選択します。
 - [検索]ボックスにキーワードを入力し、名前にキーワードと一致する言葉が含まれているクエリのみを表示します。
 - 最大化ボタンをクリックし、クエリタグフィルタリストを表示します。表示されたタグを選択するか、タグの[検索]ボックスにキーワードを入力して表示されるタグを制限します。タグを選択して、関連するクエリを表示します。表示するクエリを選択します。
 - カスタム クエリを検索する場合は、[サブスクリプション]フォルダを折りたたみ、[ユーザ]フォルダを展開して、[ユーザ]フォルダリストをスクロールします。

選択したクエリが、ページのメイン ペインに表示されます。

3. (オプション) 以下の操作のうち必要なものを実行します。
 - 必要なデータのみを表示するフィルタを設定するには、[ローカル フィルタの編集]をクリックします。元のクエリ表示に戻すには、[ローカル フィルタのクリア]をクリックします。
 - 表示されているクエリまたはレポートをお気に入りのリストに追加するには、[お気に入りへの追加]をクリックします。
 - データを最新の状態にリフレッシュするには、[リフレッシュ]をクリックします。
 - クエリを印刷するには、[印刷]をクリックします。
4. 表示されているクエリを閉じるには、[閉じる]をクリックします。

レポートの表示

Auditor、Analyst、または Administrator のロールを割り当てられているすべてのユーザが、すべてのレポートを表示できます。事前定義済みレポートが、[サブスクリプション]フォルダの下にリスト表示されます。最初のカスタムレポートを定義すると、カスタムレポートの保存用として[ユーザ]フォルダがレポートリストに追加されます。これ以降、カスタムレポートはすべてこの[ユーザ]フォルダに追加されます。

レポートリストからレポートを選択すると、その時点で内部イベントログストアに存在しているログレコードに関するレポートを構成するためのクエリが実行されます。右側ペインに表示されるレポートの結果は、アクティブな CA Enterprise Log Manager サーバおよびその子サーバのイベントログストアに基づいています。

レポートの表示方法

1. [クエリおよびレポート]タブをクリックし、[レポート]サブタブをクリックします。

[レポートタグフィルタ]の最大化ボタン、[検索]エントリフィールド、[レポートリスト]、および[オプション]メニューが、左側ペインに表示されます。

2. まだ選択されていない場合は、[オプション]メニューから[選択されたレポートの表示]を選択します。

これによって、選択されたレポートが右側ペインに表示されます。

3. 以下の方法のいずれかで、表示するレポートを選択します。

- レポートリストをスクロールし、表示するレポートを選択します。
- レポートの[検索]エントリフィールドにキーワードを入力し、フィルタされたリストから表示するレポートを選択します。
- 最大化ボタンをクリックし、レポートタグフィルタリストを表示します。表示されたタグを選択するか、タグの[検索]ボックスにキーワードを入力して表示されるタグを制限します。タグを選択して、関連するレポートを表示します。表示するレポートを選択します。
- カスタムレポートを検索する場合は、[サブスクリプション]フォルダを折りたたみ、[ユーザ]フォルダを展開して、[ユーザ]フォルダリストをスクロールします。

選択したレポートが、ページのメインペインに表示されます。

4. (オプション) 以下の操作のうち必要なものを実行します。
 - 必要なデータのみを表示するフィルタを設定するには、[ローカル フィルタの編集]をクリックします。元のレポート表示に戻すには、[ローカル フィルタのクリア]をクリックします。
 - 表示されているレポートをお気に入りのリストに追加するには、[お気に入りへの追加]をクリックします。
 - データを最新の状態にリフレッシュするには、[リフレッシュ]をクリックします。
 - レポートを印刷するには、[印刷]をクリックします。
5. [閉じる]をクリックして、表示されているレポートを閉じます。

選択されたレポートの表示の無効化

レポートをロードせずに変更できるように、レポート リストを設定できます。通常、リストからレポートを選択すると、詳細ウィンドウにレポートが表示されます。

このデフォルト モードを無効にすると、リストからレポートを選択したときに、表示されるのを待つことなくすぐにレポートを編集でき、時間を節約できます。これは特に、複数のレポートを編集する必要があり、加えるべき変更の内容がすでにわかっている場合に便利です。

レポートの作成または編集が可能なのは **Administrator** モードまたは **Analyst** モードのユーザのみであるため、これらのユーザだけが選択されたレポートの表示設定を無効にできます。

選択されたレポートの表示を無効化する方法

1. [レポートリスト] 上部の[オプション]をクリックします。
[オプション]メニューが表示されます。
2. [選択されたレポートの表示]の横のチェック ボックスをオフにします。
[選択されたレポートの表示]が再度オンにされるまで、リストから選択されたレポートは表示されません。

詳細情報

[レポートの作成方法](#) (P. 317)

[レポートの編集](#) (P. 328)

例: PCI レポートの実行

PCI セキュリティ標準協議会は、セキュリティ管理、ポリシー、および手順の要件を含む PCI データセキュリティ標準 (PCI DSS) の開発を行っているオープングローバルフォーラムです。クレジットカード保有者のデータを保存、処理、または送信する組織は、12 の要件を詳述した PCI DSS バージョン 1.2 に準拠する必要があります。

CA Enterprise Log Manager には、あらかじめ PCI レポートが組み込まれているため、システムがイベントログの収集および処理を開始した直後からレポートを表示できます。

このセクションでは、PCI レポートについてと、このレポートをスケジュールして配信する方法について、例を使ってわかりやすく説明します。例では、レポートで使用される PCI DSS 要件に関連する数を参考として示しています。

詳細情報:

[PCI タグが付いたレポートのリストの表示](#) (P. 274)

[特定の PCI DSS 規制のレポートの検索](#) (P. 275)

PCI タグが付いたレポートのリストの表示

PCI タグが付いた事前定義済みレポートのリストを表示することで、PCI コンプライアンスを証明するための CA Enterprise Log Manager レポートの使用方法について評価を開始できます。

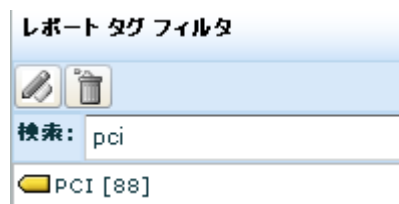
PCI タグが付いたレポートの使用方法を確認する方法

1. [クエリおよびレポート] タブをクリックし、[レポート] サブタブをクリックします。

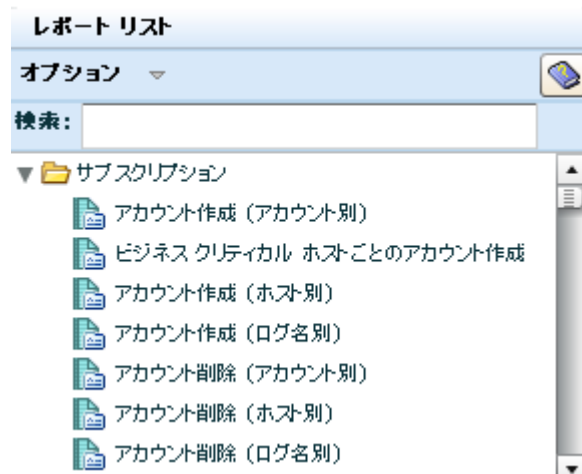
[レポートタグ フィルタ] および [レポートリスト] が表示されます。

2. タグの [検索] フィールドに「PCI」と入力します。

PCI タグが表示されます。



3. PCI タグに関連付けられたレポートリストを確認します。



特定の PCI DSS 規制のレポートの検索

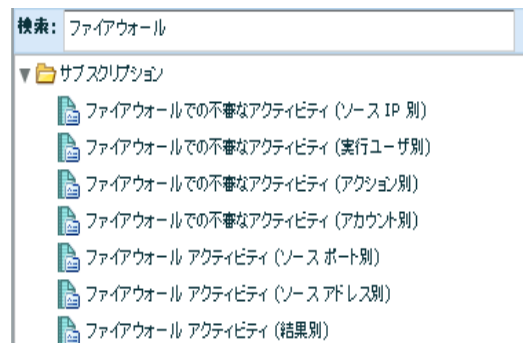
特定の PCI DSS 規制に関連するキーワードを使用して、事前定義済みレポートを検索できます。以下の手順で、いくつかの例を説明します。

注: ここで言及している数は、レポートが扱う PCI DSS 要件に関連する数です。

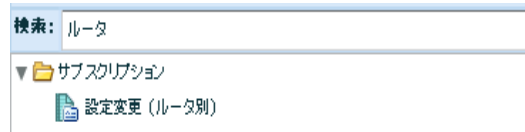
特定の PCI DSS 規制に関連するレポートのリストを表示する方法

1. [クエリおよびレポート]タブをクリックし、[レポート]サブタブをクリックします。
2. ファイアウォール設定への変更(1.1.1)を扱うレポートを特定するには、[検索基準]として「ファイアウォール」と入力します。

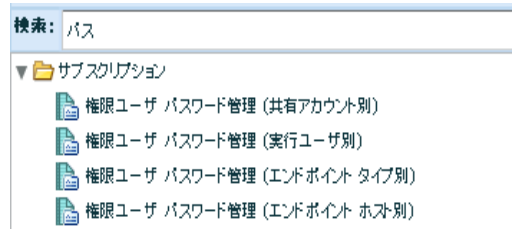
以下のようなレポートのリストが表示されます。[ファイアウォール設定変更]というタイトルのレポートに注目します。



3. 同期を確認した後のルータ設定への変更 (1.3.6) を扱うレポートを特定するには、[検索基準]として「ルータ」と入力します。



4. 強力なアクセス制御手段の 1 つである、パスワード管理 (8.5) を扱うレポートを特定するには、[検索基準]として「パスワード」と入力します。



5. 情報セキュリティポリシーの管理手段の 1 つである、ユーザ アカウントの追加、変更、および削除 (12.5.4) を扱うレポートを特定するには、[検索基準]として「アカウント」と入力します。



単一の PCI レポートの操作

PCI レポートなどのレポートに対して、以下のような操作が可能です。

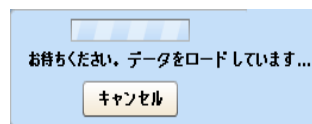
- [レポートリスト]からレポート名を選択してレポートを表示する
- レポートの印刷
- 選択した受信者に電子メールでレポートを送信するオプションを有効にして、レポートをスケジュールする
- スケジュールしたレポートジョブの表示
- 作成されたレポートを表示します。

選択したレポートを表示または操作する方法

1. [クエリおよびレポート]タブをクリックし、[レポート]サブタブをクリックします。
2. まだ選択していない場合は、[レポートリスト]の[オプション]ドロップダウンリストから[選択されたレポートの表示]を選択します。
3. レポートリストからレポート名を選択します。

作成されたレポートに、基礎をなすクエリの結果が表示されます。通常は、サマリ、トレンド、および詳細に加え、レポート固有のクエリが含まれます。

4. 特定のクエリのロードを無効にするには、[キャンセル]を選択します。



5. 表示されたレポートを印刷するには、右ペインの[レポートの印刷]をクリックします。

[印刷]ダイアログ ボックスが表示されたら、プリンタを選択して[印刷]をクリックします。

6. 後で確認するためにレポートの作成をスケジュールするには、[レポートのスケジュール]をクリックします。

レポートのスケジュールウィザードが、[選択されたレポート]領域にレポートが表示された状態で表示されます。

7. 「リソース アクセス(ホスト別)レポート ジョブ」のようなジョブ名を入力します。
すべてをデフォルトのままにすると、ジョブが反復なしでただちに実行されるようスケジュールされ、レポートが電子メール通知なしで PDF 形式で作成されます。データは、現在のサーバ、連携されたピア、および連携された子サーバから取得されます。
8. [保存して閉じる]をクリックします。
9. スケジュールしたジョブを表示します。[スケジュール済みレポート]タブをクリックし、[レポートのスケジュール]サブタブをクリックします。
スケジュールしたジョブが表示されます。

スケジュール済みジョブ									
☐	ジョブ名	有効	サーバ	ステータス	反復	スケジュール済み時刻	タイムゾーン	作成者	フォーマット
☐	リソースアクセス(ホスト別)	はい	caelm2	スケジュール済み完了	今すぐ	2010-09-28 火曜日 午前 12:12:33	America/New_York	Admin	PDF

10. 作成されたレポートを表示します。
 - a. [スケジュール済みレポート]タブをクリックし、[作成済みレポート]サブタブをクリックします。
 - b. (オプション) 表示される行を制限するには、「すべて」以外の反復を選択するか、「すべて」以外のフォーマットを選択するか、「過去 1 時間」の期間を選択します。
 - c. (オプション) [リフレッシュ]をクリックします。
11. 作成されたレポートを確認した後、レポートの作成を繰り返し実行する必要がある場合は、レポートジョブを変更できます。以下の手順を実行します。
 - a. [レポートのスケジュール]サブタブから、作成済みレポートを選択し、[編集]をクリックします。
 - b. [ジョブのスケジュール]手順を選択し、発生間隔のオプションを選択します。
 - c. [保存して閉じる]をクリックします。

プロンプト

プロンプトは、入力した値と選択した CEG フィールドに基づいた結果を表示する特別なタイプのクエリです。入力した値が選択した CEG フィールドの 1 つ以上に表示されているイベント行のみが返されます。

プロンプトクエリ結果に対して、以下のアクションを実行できます。

- [元のイベントの表示]を選択して、精製済みイベントのビューを、対応する元のイベントとその発生時間に置き換えることができます。
- [一致]フィールドに文字列を入力し、[実行]を選択して、エントリと一致するデータが含まれている行のみに表示をフィルタすることができます。
- [クエリデータのエクスポート]オプションを選択して、PDF 文書、Excel スプレッドシート、または XML ファイルにクエリ結果をエクスポートできます。
- [結果の条件]を選択して、指定した日付範囲別の表示のフィルタ、返される行の制限設定、および表示された時間の精度の変更を実行できます。また、結果の条件をデフォルトにリセットすることもできます。
- [ローカル フィルタの表示/編集]を選択して、クイック フィルタまたは詳細フィルタを指定できます。
- 選択したローカル プリンタへクエリを印刷できます。
- 手動で、または[自動リフレッシュ]を選択して、クエリ データをリフレッシュできます。

コネクタ プロンプトの使用

エージェント上に設定された各コネクタは、特定のイベントソースから元のイベントを収集し、CA Enterprise Log Manager 収集サーバのイベント ログ ストアにイベントを送信します。イベント精製プロセスによって、元のイベントが精製済みイベントに変換され、レポート CA Enterprise Log Manager サーバにアーカイブされます。コネクタ プロンプトは、指定した名前を持つコネクタによって元のイベントとして収集された、レポート サーバ上のイベントに対してクエリを実行します。コネクタには、デフォルト名かユーザ定義名が付いています。コネクタの名前をコピーし、コネクタ プロンプトのフィールドに貼り付けて[実行]をクリックすると、プロンプトクエリ結果が表示されます。

コネクタ プロンプトを使用して、以下を実行できます。

- 同じ統合に基づいたすべてのコネクタからのイベントの表示。これは、コネクタの展開時にデフォルトのコネクタ名を使用した場合に可能です。
- 新しいコネクタによってイベントが取得されているかどうかの確認。指定した名前を持つコネクタが複数のエージェント上にある場合は、[一致]フィールドにエージェント名を入力して、クエリ結果を、新しいコネクタによって取得されたイベントに限定します。

アクティブなコネクタの名前をコピーする方法

1. [管理]タブをクリックします。
[ログ収集エクスプローラ]が表示されます。
2. [エージェント エクスプローラ]をクリックします。
[エージェント ステータス モニタ]が表示され、特定の列にコネクタ名がリスト表示されます。
3. プロンプトクエリで使用するコネクタを右クリックし、[コネクタ名のコピー]を選択します。

コネクタ プロンプトを使用する方法

1. [クエリおよびレポート]を選択します。
[クエリリスト]に、[プロンプト]フォルダおよび[サブスクリプション]フォルダが表示され、[ユーザ]フォルダも表示される場合があります。
2. [プロンプト]を展開し、[コネクタ]を選択します。
コネクタ プロンプトに、[コネクタ]フィールド、および以下の **CEG** フィールドが表示されます。プロンプトが機能するよう、選択された状態にしておく必要があります。
agent_connector_name
コネクタの名前です。
3. [コネクタ]フィールドを右クリックし、[貼り付け]を選択します。
[エージェント ステータス モニタ]からコピーしたコネクタ名が、[コネクタ]フィールドに表示されます。
4. [実行]をクリックします。
コネクタ プロンプトクエリの結果が表示されます。
5. 以下の説明を使用して、クエリ結果を解釈します。

CA 重大度

イベントの重大度を示します。値には、重大度が大きくなる順に、情報、警告、マイナー インパクト、メジャー インパクト、クリティカル、および致命的、があります。

日付

イベントが発生した日付を示します。

カテゴリ

対応するイベントアクションの上位レベルのカテゴリを示します。たとえば、「システム アクセス」は認証アクション用のカテゴリです。

[アクション]

アクションを示します。可能性のあるアクションは、イベントのクラスによって決定されます。

エージェント名

コネクタが実行されているエージェントを示します。

ホスト

コネクタによるイベント収集元のイベントソース ホストを示します。

実行ユーザ

イベントのソースアクタ、すなわちアクションを開始した ID を示します。実行ユーザは、ソース ユーザ名またはソース プロセス名として表される場合があります。

アカウント

元のイベントが収集されたイベントソースのあるホストにコネクタが接続を試行したときに認証に使用されたアカウントのユーザ名を示します。これは、通常、権限レベルの低いアカウントです。このアカウントの認証情報は、イベントソースに設定され、コネクタのログ センサにも設定されます。

Result

対応するアクションのイベント結果のコードを示します。「S」は成功、「F」は失敗、「A」は許可、「D」は廃棄、「R」は拒否、「U」は不明を表します。

コネクタ名

プロンプトフィルタフィールドに入力されたコネクタの名前

6. (オプション) [元のイベントの表示]を選択します。

新しいコネクタによって収集された最初のイベントは、アクション「システム起動」のイベントで、末尾が「`result_string=<コネクタ名>` コネクタは正常に開始しました」となっています。

ホストプロンプトの使用

ホストプロンプトは、指定したホスト名が選択した精製済みイベントの CEG フィールドに表示されるイベントに対してクエリを実行します。元のイベントデータが精製されると、イベントの詳細に複数の CEG ホスト名が含まれることがあります。次のシナリオを考えます。

1. `source_hostname` にあるイベントイニシエータが、`dest_hostname` にあるターゲットに、アクション `event_action` を試行します。

注: `source_hostname` と `dest_hostname` は、異なるホストである場合も、同じホストである場合もあります。

2. このイベントが `event_source_hostname` 上のリポジトリに記録されます。

注: `event_source_name` は、`source_hostname` または `dest_hostname` と異なるホストである場合も、同じホストである場合もあります。

3. `agent_hostname` にインストールされた CA Enterprise Log Manager エージェントが、`event_source_hostname` に記録されたイベントのコピーを作成します。

注: `agent_hostname` はエージェント ベースのログ収集では `event_source_name` と同じですが、エージェントレス ログ収集や直接ログ収集では異なります。

4. `agent_hostname` にある CA Enterprise Log Manager エージェントが、CA Enterprise Log Manager 収集サーバに `event_logname` のイベントのコピーを送信します。

ホスト プロンプトを使用する方法

1. [クエリおよびレポート]を選択します。
[クエリリスト]に、[プロンプト]フォルダおよびほかのクエリ用の 1 つ以上のフォルダが表示されます。
2. [プロンプト]を展開し、[ホスト]を選択します。
ホスト プロンプトが表示されます。
3. このクエリの基となるホストの名前を入力します。
4. ホスト名エントリと一致するデータにクエリを実行するフィールドを選択します。

source_hostname

イベント アクションが開始されたホストの名前です。

dest_hostname

アクションの宛先またはターゲットであるホストの名前です。

event_source_hostname

イベントが発生したときにイベントを記録するホストの名前です。

たとえば、WinRM に基づいたコネクタを展開し、Windows Server 2008 ホストのイベントビューアからイベントを収集できます。指定した Windows Server 2008 ホストから取得されたイベントを選択するには、そのサーバのホスト名を入力し、このフィールドを選択します。

receiver_hostname

agent_hostname と同じです。

agent_hostname

CA Enterprise Log Manager エージェントが展開されているホストの名前です。

5. [実行]をクリックします。
ホスト プロンプト クエリの結果が表示されます。

6. 以下の説明を使用して、クエリ結果を解釈します。

CA 重大度

イベントの重大度を示します。値には、重大度が大きくなる順に、情報、警告、マイナー インパクト、メジャー インパクト、クリティカル、および致命的、があります。

日付

イベントが発生した日付を示します。

ソース ユーザ

イベント アクションを開始した `source_hostname` 上のユーザの名前を示します。

Result

対応するアクションのイベント結果のコードを示します。「S」は成功、「F」は失敗、「A」は許可、「D」は廃棄、「R」は拒否、「U」は不明を表します。

エージェント ホスト

イベントを収集した **CA Enterprise Log Manager** エージェントがインストールされているホストの名前を示します。

受信側ホスト

エージェント ホストと同じです。

カテゴリ

対応するイベント アクションの上位レベルのカテゴリを示します。たとえば、「システム アクセス」は認証アクション用のカテゴリです。

[アクション]

ソース ユーザによって実行されたイベント アクションを示します。

ログ名

イベントを収集したコネクタによって使用されたログ名を示します。同じ統合に基づいたすべてのコネクタは、ログ名が同じであるログ ファイルでイベントを送信します。

IP プロンプトの使用

IP プロンプトは、指定した IP アドレスが選択した精製済みイベント CEG フィールドに表示されるイベントに対してクエリを実行します。元のイベント データが精製されると、イベントの詳細に複数の CEG IP アドレスが含まれることがあります。次のシナリオを考えます。

1. `source_address` にあるイベント イニシエータが、`dest_address` にあるターゲットに、アクション `event_action` を試行します。
注: `source_address` と `dest_address` は、異なる場合も同じである場合もあります。
2. このイベントが `event_source_address` にあるリポジトリに記録されます。
注: `event_source_address` は `source_address` や `dest_address` と異なる場合も、どちらかと同じまたは両方と同じである場合もあります。
3. `agent_address` にインストールされた CA Enterprise Log Manager エージェントが、`event_source_address` に記録されたイベントのコピーを作成します。
注: `agent_address` は、エージェント ベースのログ収集では `event_source_address` と同じですが、エージェントレス ログ収集や直接ログ収集では異なります。
4. `agent_address` にあるエージェントが、CA Enterprise Log Manager 収集サーバに `event_logname` のイベントのコピーを送信します。

IP プロンプトを使用する方法

1. [クエリおよびレポート]を選択します。
[クエリリスト]に、[プロンプト]フォルダおよびほかのクエリ用の 1 つ以上のフォルダが表示されます。
2. [プロンプト]を展開し、[ホスト]を選択します。
IP プロンプトが表示されます。
3. このクエリの基となる IP アドレスを入力します。
4. IP アドレス エントリと一致するデータにクエリを実行するフィールドを、以下の中から 1 つ以上選択します。

`source_address`

アクションが開始されたホストの IP アドレスです。

`dest_address`

アクションの宛先またはターゲットであるホストの IP アドレスです。

event_source_address

イベントが発生したときに元のイベントを記録するホストの IP アドレスです。

たとえば、WinRM に基づいたコネクタを展開し、Windows Server 2008 ホストのイベントビューアからイベントを収集できます。指定した Windows Server 2008 ホストから取得されたイベントを選択するには、そのサーバの IP アドレスを入力し、このフィールドを選択します。

receiver_hostaddress

agent_address と同じです。

agent_address

CA Enterprise Log Manager エージェントが展開されているホストの IP アドレスです。

5. [実行]をクリックします。

IP プロンプト クエリの結果が表示されます。

6. 以下の説明を使用して、クエリ結果を解釈します。

CA 重大度

イベントの重大度を示します。値には、重大度が大きくなる順に、情報、警告、マイナー インパクト、メジャー インパクト、クリティカル、および致命的、があります。

日付

イベントが発生した日付を示します。

Result

対応するアクションの結果のコードを示します。表示される文字は、「S」は成功、「F」は失敗、「A」は許可、「D」は廃棄、「R」は拒否、「U」は不明を表します。

宛先ポート

宛先ホスト(イベントアクションのターゲット)の通信ポートを示します。

送信元 IP

イベントアクションが開始された IP アドレスを示します。

宛先 IP

イベントアクションのターゲットとなったホストの IP アドレスを示します。

イベントソース IP

イベントが最初に記録されたリポジトリのあるホストの IP アドレスを示します。

エージェント IP

イベントソースからのイベントの収集を実行する CA Enterprise Log Manager エージェントがあるホストの名前を示します。

受信側 IP

エージェント IP と同じです。

カテゴリ

対応するイベントアクションの上位レベルのカテゴリを示します。たとえば、「システム アクセス」は認証アクション用のカテゴリです。

[アクション]

イベントアクションを示します。

ログ名

イベントを収集したコネクタによって使用されたログ名を示します。

ログ名プロンプトの使用

同じ統合に基づいたコネクタでは、イベントソースから収集されたイベントログが、事前に定義された名前を持つログファイルの形で **CA Enterprise Log Manager** 収集サーバに返されます。ログ名プロンプトが、指定されたログ名を含むイベントに対してクエリを実行します。

ログ名プロンプトを使用して、指定した名前を持つログファイルで転送されたイベントにクエリを実行します。各コネクタは、1つの統合に基づいています。各統合には、1つの事前定義済みログ名が使用されています。指定されたログ名に対するクエリによって、同じ統合または類似した統合に基づいたコネクタを使用する別のエージェントによって収集されたイベントの結果が返されます。

さまざまな命名規則が、ログに名前を付ける際に使用されます。

- 統合名。「CA Federation」は、CA_Federation_Manager 統合のログ名です。
- 製品名。「McAfee Vulnerability Manager」は、McAfee_VM と McAfee_VM_CM 両方のログ名です。「MS AD Rights Management Services」は、Microsoft_Active_Directory_RMS と Microsoft_Active_Directory_RMS_ODBC 両方のログ名です。
- ベンダー名。「Oracle」は、Oracle10g、Oracle9i、Oracle_AppLog、および Oracle_Syslog のログ名です。
- ログタイプ。「UNIX」は、AIX_Syslog、HPUX_Syslog、Linux_Syslog、SLES_Syslog、および Solaris_Syslog といった統合のログ名です。

新しいリリースまたはプラットフォームが追加される際、再利用されるログ名があります。たとえば、「NT-Security」は、NTEventLog、Windows2k8、および WinRM といった統合のセキュリティログのログ名です。

ログ名プロンプトを使用する方法

1. [クエリおよびレポート]を選択します。
[クエリリスト]に、[プロンプト]フォルダおよびほかのクエリ用の1つ以上のフォルダが表示されます。
2. [プロンプト]を展開し、ログ名を選択します。
ログ名プロンプトフィルタが表示され、以下のフィールドが表示されます。

event_logname

特定の統合と関連付けられたログファイルの名前です。

3. 表示させたいイベントが転送される際に使用されるログ名を選択し、[実行]をクリックします。

ログ名プロンプト クエリの結果が表示されます。

4. 以下の説明を使用して、クエリ結果を解釈します。

CA 重大度

イベントの重大度を示します。値には、重大度が大きくなる順に、情報、警告、マイナー インパクト、メジャー インパクト、クリティカル、および致命的、があります。

日付

イベントが発生した日付を示します。

カテゴリ

対応するイベントアクションの高位のカテゴリを示します。たとえば、「システム アクセス」は認証アクション用のカテゴリです。

[アクション]

対応する実行ユーザによって実行されたイベントアクションを示します。

ホスト

コネクタによるイベント収集元であるイベントソース ホストを示します。

実行ユーザ

イベントのソース アクタ、すなわちアクションを開始した ID を示します。実行ユーザは、ソース ユーザ名またはソース プロセス名として表される場合があります。

アカウント

認証に使用されたアカウントのユーザ名を示します。コネクタによってイベントソースへの接続が試行される際に、認証が行われます。認証には、通常、権限レベルの低いアカウントが使用されます。コネクタの展開時に、管理者によって、イベントソースにこのアカウントの認証情報が設定され、次に、ログ センサにこのアカウントが指定されます。

Result

対応するアクションのイベント結果のコードを示します。「S」は成功、「F」は失敗、「A」は許可、「D」は廃棄、「R」は拒否、「U」は不明を表します。

ログ名

プロンプトフィルタフィールドに入力されたログ名

ポート プロンプトの使用

ポートプロンプトは、指定したポートが選択した精製済みイベントの CEG フィールドに表示されるイベントに対してクエリを実行します。元のイベントデータが精製されると、イベントの詳細に複数の CEG ポート番号が含まれることがあります。次のシナリオを考えます。

1. ソース ホスト上のイベント イニシエータは、受信 **dest_port** 通信ポートを経由して宛先ホスト上にあるターゲットへのイベント アクションを開始する際に、送信 **source_port** 通信ポートを使用します。

注: **source_port** と **dest_port** は、ローカル イベントの場合は同じものです。そうでない場合は、ホスト固有のものになります。

2. このイベントは、イベントソースのリポジトリに記録されます。
3. CA Enterprise Log Manager エージェントが、イベントソースに記録されたイベントのコピーを作成します。
4. エージェントが、CA Enterprise Log Manager 収集サーバに、**outbound port**、**receiver_port** 経由で、イベントのコピーを送信します。

注: エージェントは、デフォルトでは、ポート **17001** を使用して、CA Enterprise Log Manager 収集サーバへの通信を確保します。

ポートプロンプトを使用する方法

1. [クエリおよびレポート]を選択します。
[クエリリスト]に、[プロンプト]フォルダおよびほかのクエリ用の 1 つ以上のフォルダが表示されます。
2. [プロンプト]を展開し、[ポート]を選択します。
ポートプロンプトが表示されます。
3. このクエリの基となるポート番号を入力します。
4. ポート番号エントリと一致するデータにクエリを実行するフィールドを選択します。

source_port

アクションを開始するために使用された通信ポートです。

dest_port

アクションのターゲットである宛先ホストの通信ポートです。

receiver_port

CA Enterprise Log Manager 収集サーバと通信するためにエージェントが使用するポートです。

5. [実行]をクリックします。
ポートプロンプトクエリの結果が表示されます。
6. 以下の説明を使用して、クエリ結果を解釈します。

CA 重大度

イベントの重大度を示します。値には、重大度が大きくなる順に、情報、警告、マイナー インパクト、メジャー インパクト、クリティカル、および致命的、があります。

日付

イベントが発生した日付を示します。

送信元 IP

イベントアクションが開始されたホストの IP アドレスを示します。

Result

対応するアクションのイベント結果のコードを示します。「S」は成功、「F」は失敗、「A」は許可、「D」は廃棄、「R」は拒否、「U」は不明を表します。

ソース ポート

アクションを開始するために使用された送信ポートを示します。

宛先ポート

宛先ホストの受信ポートを示します。

受信側ホスト

イベントログを **CA Enterprise Log Manager** サーバに送信するために使用されたエージェントの送信ポートを示します。

カテゴリ

対応するイベントアクションの上位レベルのカテゴリを示します。たとえば、「システム アクセス」は認証アクション用のカテゴリです。

[アクション]

イベントアクションを示します。

ログ名

イベントを収集したコネクタによって使用されたログ名を示します。

ユーザ プロンプトの使用

各イベントは、2 つのアクタ、ソースおよび宛先に関する情報を表します。

- ソース アクタは、イベントを発生させるアクションを開始します。
ソース アクタは、ユーザ (`source_username`) である場合も、プロセス (`source_processname`) である場合もあります。
- 宛先、すなわち「**dest**」アクタは、アクションのターゲットです。
宛先アクタは、ユーザ (`dest_username`) である場合も、オブジェクト (`dest_objectname`) である場合もあります。

ユーザ プロンプトは、指定したアクタが選択した精製済みイベントの CEG フィールドに表示されるイベントに対してクエリを実行します。次のシナリオを考えます。

1. ソース アクタ `source_username` または `source_processname` が、ターゲット アクタ `destination_username` または `destination_objectname` にアクションを試行します。
2. このイベントは、イベントソースのリポジトリに記録されます。
3. CA Enterprise Log Manager エージェントが、イベントソースに記録されたイベントのコピーを作成し、CA Enterprise Log Manager サーバに送信します。

ユーザ プロンプトを使用する方法

1. [クエリおよびレポート]を選択します。
[クエリリスト]に、[プロンプト]フォルダおよびほかのクエリ用の 1 つ以上のフォルダが表示されます。
2. [プロンプト]を展開し、[ユーザ]を選択します。
ユーザ プロンプトが表示されます。
3. このクエリの基となるユーザの名前を入力します。
4. ユーザ名エントリと一致するデータにクエリを実行するフィールドを選択します。

`source_username`

イベントアクションを開始したユーザの名前です。

`dest_username`

アクションのターゲットであるユーザの名前です。

`source_objectname`

イベント情報で参照されたアクションに関連するオブジェクトの名前です。

`dest_objectname`

アクションのターゲットであるオブジェクトの名前です。

5. [実行]をクリックします。
ユーザ プロンプト クエリの結果が表示されます。

6. 以下の説明を使用して、クエリ結果を解釈します。

CA 重大度

イベントの重大度を示します。値には、重大度が大きくなる順に、情報、警告、マイナー インパクト、メジャー インパクト、クリティカル、および致命的、があります。

日付

イベントが発生した日付を示します。

宛先ホスト

イベント アクションのターゲットであるユーザがあるホストの名前を示します。

Result

対応するアクションのイベント結果のコードを示します。「S」は成功、「F」は失敗、「A」は許可、「D」は廃棄、「R」は拒否、「U」は不明を表します。

ソース ユーザ

イベント アクションを開始したユーザを示します。

ソース オブジェクト

イベント アクションに関連したソース ホストのオブジェクトを示します。

宛先ユーザ

イベント アクションのターゲットとなったユーザを示します。

宛先オブジェクト

イベント アクションに関連したホストのオブジェクトを示します。

カテゴリ

対応するイベント アクションの上位レベルのカテゴリを示します。たとえば、「システム アクセス」は認証アクション用のカテゴリです。

[アクション]

イベント アクションを示します。

ログ名

イベントを収集したコネクタによって使用されたログ名を示します。

クエリの作成方法

[クエリの設計]ウィザードを使用すると、カスタム クエリを作成できます。クエリを作成する場合は、イベント データベースまたはインシデント データベースのどちらに適用するかを選択します。サーバのイベント データベースには、そのサーバが受信したすべてのイベントに関する情報が格納されます。サーバのインシデント データベースには、相関ルールによって指定されたインシデントおよびそのコンポーネント イベントの要素に関する情報が格納されます。

また、クエリの設計ウィザードを使用して、カスタム クエリやエクスポート クエリ情報を削除したり、サブスクリプション クエリをコピーしてカスタム クエリを作成し、そのクエリを編集したりすることもできます。クエリの作成、削除、および編集は、**Administrator** ロールまたは **Analyst** ロールを持ったユーザにしか実行できません。

クエリの設計ウィザードを使用したクエリの作成は、以下の手順で構成されます。

1. クエリの設計ウィザードの表示
2. ID およびタグの詳細の追加
3. クエリ列の選択
4. (オプション)クエリ条件およびフィルタの設定
5. 日付範囲と結果の条件の設定
6. (オプション)クエリ表示の視覚化オプションの選択
7. (オプション)クエリのドリルダウン値の追加

詳細情報:

[クエリの設計ウィザードの表示](#) (P. 296)

[詳細フィルタの使用](#) (P. 487)

[クエリ表示の視覚化の作成](#) (P. 311)

[ドリルダウンレポートの追加](#) (P. 312)

クエリの設計ウィザードの表示

カスタムレポートの新規作成、クエリのコピーの作成、または既存のクエリの編集を実行するには、クエリの設計ウィザードを開く必要があります。

クエリの設計ウィザードを開く方法

1. [クエリおよびレポート]タブをクリックし、[クエリ]サブタブをクリックします。
[クエリリスト]が表示されます。
2. [オプション]をクリックし、[新規作成]を選択します。
クエリの設計ウィザードが表示されます。

ウィザードを使用する際に

- ウィザードを閉じずにクエリを保存するには、[保存]をクリックします。
- クエリを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

詳細情報

[結果の条件の設定方法](#) (P. 489)

[クエリ表示の視覚化の作成](#) (P. 311)

[ドリルダウンレポートの追加](#) (P. 312)

クエリの詳細の追加

クエリを作成する最初の手順は、識別情報の入力と組み込むタグの設定です。

新しいクエリを追加する方法

1. クエリの設計ウィザードを開きます。
2. 必須であるクエリ名、およびオプションとして、レポートで使用されるショートネームを入力します。ショートネームは、クエリがレポートに含まれている場合にレポートの個別のクエリペインに表示されます。
3. クエリを適用するデータベースを選択します。

イベント

イベントデータベースにクエリを適用します。このデータベースには、現在のサーバが受信した、または連携によって使用可能なすべての元のイベント情報および精製されたイベント情報が格納されます。

インシデント

インシデントデータベースにクエリを適用します。このデータベースには、イベント関連システムによって作成されたインシデント、およびそれらのインシデントを作成するために使用されたイベント情報が格納されます。インシデントを作成するために使用され、インシデントデータベースに格納されるイベントの特定のコンポーネントは、関連ルールによって設定されます。

4. [説明]エントリフィールドに、必要な設計メモを入力します。

注: クエリ構造に関する情報用に、このフィールドを使用することをお勧めします。たとえば、特定のフィールドや機能がクエリに含まれる理由を入力します。

5. [タグ]シャトルコントロールを使用してクエリに関連付けるタグを1つ以上選択します。
6. (オプション) カスタムカテゴリタグを追加するには、[カスタムタグの追加]エントリフィールドにタグ名を入力し、[タグの追加]ボタンをクリックします。
カスタムタグが、選択済みの状態で[タグ]シャトルコントロールに表示されます。
7. (オプション) ネストされた1つ以上のカスタムタグを追加するには、タグを選択するか、または親カテゴリのタグ名、円記号、子タグの名前の順に入力して、[タグの追加]をクリックします。たとえば、「Regulations¥Industry Standards」のように入力します。この形式を保持しながら、さらにタグを追加できます(a¥b¥c など)。

注: ネストされたカスタム タグの 1 つを削除すると、ネスト先のすべてのカスタム タグ (親タグを含む) も削除されます。カスタム タグをサブスクリプション タグの内部にネストし、その後削除した場合は、カスタム タグのみが削除されます。

プロセスを完了すると、リストに新しいタグが表示されます。親タグを展開するとネストされたカスタム タグが表示されます。

8. 適切な矢印をクリックして次に実行する「クエリの設計」の手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、新規クエリが[クエリリスト]に表示されます。それ以外の場合は、選択したクエリの設計手順が表示されます。

クエリ列の追加

クエリを作成するには、イベント ログ ストアから必要なイベント情報を取得する SQL 文を作成します。クエリの設計ウィザードを使用すると、このプロセスが自動化されます。

クエリの SQL 文の作成方法

1. クエリの設計ウィザードを開きます。
2. まだ指定していない場合は名前とタグを入力してから、[クエリ列]の手順に進みます。
3. (オプション) [一意のイベントのみ]チェック ボックスをオンにします。
4. 左側にある[使用可能な列]のリストから、[選択済みの列]ペイン内の[列]フィールドにドラッグすることによって、クエリを実行する CEG 列を設定します。CEG 列は、入力された順序でクエリ表示に表示されます。
5. (オプション) 各列に以下を含めた設定を選択します。

表示名

表形式やイベント ビューア形式の表示用に、列の別名を入力できます。表示名を入力しなかった場合、「event_count」などの元のフィールド名が列名として使用されます。

関数

以下の SQL 関数のいずれかを列の値に指定できます。

- **COUNT** - イベントの合計数を返します。
- **AVG** - `event_count` 値の平均を返します。この関数は `event_count` フィールドに対してのみ使用できます。
- **SUM** - `event_count` 値の合計を返します。この関数は `event_count` フィールドに対してのみ使用できます。
- **TRIM** - クエリを実行するテキスト文字列内のスペースを削除します。
- **TOLOWER** - クエリを実行するテキスト文字列を小文字に変換します。
- **TOUPPER** - クエリを実行するテキスト文字列を大文字に変換します。
- **MIN** - イベントの最低値を返します。
- **MAX** - イベントの最高値を返します。
- **UNIQUECOUNT** - 一意のイベント数を返します。

グループの順序

クエリ表示を設定して選択属性によってグループ化された選択列を表示します。たとえば、ソース名でイベントをグループ化するようにクエリを設定することができます。さまざまな列に適用されている順序を制御することができます。最初の列の値が同一である場合は、2 番目が指定されます。たとえば、同じソースからの複数のイベントを `username` によってグループ化できます。

並び順

選択値の並び順を制御します。さまざまな列に適用されている順序を制御することができます。最初の列の値が同一である場合は、2 番目が指定されます。

降順

デフォルトの昇順ではなく、列の値を降順(最高値から最低値へ)に表示されるように設定します。

NULL でない

行に値が含まれていない場合に、表やイベントビューアに行を表示するかどうかを制御します。[NULL でない]チェック ボックスをオンにすると、行に表示可能な値が含まれていない場合はクエリ結果から行が削除されます。

表示

表形式やイベントビューア形式において、列を表示するかどうかを制御します。この設定を使用すると、表示自体に表示させずに、列データを詳細ビューで使えるようにすることができます。

注: 1 つの列に対して TRIM、TOLOWER、TOUPPER 以外の関数、またはグループの順序設定を選択した場合、他の列にも同じ設定を選択する必要があります。そうしないと、CA Enterprise Log Manager でエラー メッセージが表示されます。

6. (オプション) [選択列] ペインの上部にある上矢印と下矢印を使用して必要に応じて列の順序を変更します。
7. 矢印をクリックして次に完了するクエリ的设计の手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、新規クエリが[クエリリスト]に表示されます。それ以外の場合は、選択したクエリ的设计手順が表示されます。

クエリ フィルタの設定

単純フィルタや詳細フィルタを使用して、クエリによって返される情報をフィルタできます。単純フィルタを使用すると、単一条件のフィルタ ステートメントが簡単に作成できます。詳細フィルタを使用すると、ネスト構造のステートメントなど、より複雑な SQL 言語ステートメントを作成できます。

クエリ フィルタの設定方法

1. クエリの設計ウィザードを開きます。
2. まだ指定していない場合は名前とタグを入力してから、「クエリ フィルタ」の手順に進みます。
[クエリ フィルタ] ダイアログ ボックスが開いて、[単純フィルタ] タブが表示されます。
3. 決まった CEG フィールドの値を検索する単純フィルタを必要なだけ作成します。
4. (オプション) [詳細フィルタ] タブをクリックします。
5. (オプション) 必要に応じて詳細フィルタを作成します。
6. 矢印をクリックして次に完了するクエリの設計の手順に進むか、[保存して閉じる]をクリックします。
[保存して閉じる]をクリックすると、新規クエリが[クエリ リスト]に表示されます。それ以外の場合は、選択したクエリの設計手順が表示されます。

詳細情報:

[単純イベントフィルタの作成](#) (P. 569)

[詳細イベントフィルタの作成](#) (P. 572)

[詳細フィルタの使用](#) (P. 487)

単純イベント フィルタの作成

単純フィルタを作成して、共通の値に対する検索パラメータを設定できます。たとえば、[理想モデル]フィールドを「コンテンツ管理」に設定して、理想モデル CEG フィールドの値を持つすべてのイベントを特定することができます。単純フィルタは、イベントおよびインシデントクエリ、抑制および集約ルール、イベント転送ルールを含む多くの機能で使用されます。

単純フィルタを作成する方法

1. 定義する単純フィルタフィールドのチェックボックスをオンにして、ドロップダウンリストから値を選択するか、テキストフィールドに値を入力します。
2. 必要な単純フィルタをすべて追加したら、[保存]をクリックします。

詳細情報

[詳細フィルタの使用](#) (P. 487)

[詳細イベントフィルタの作成](#) (P. 572)

詳細フィルタの使用

SQL ベースの詳細フィルタを使用すると、イベントまたはインシデントデータベースに対してクエリを行う機能を修飾（クエリ対象の絞り込みやシンプルフィルタへの条件の追加など）できます。[詳細フィルタ]インターフェースでは、フィルタ要件に応じてロジック、列、演算子、および値を入力する形式を指定することによって、適切なフィルタ構文を作成できるようにします。

注: このセクションには、詳細フィルタに使用される SQL 用語の概要が含まれています。詳細フィルタの機能を十分に活用するには、SQL および共通イベント文法を完全に理解しておく必要があります。

以下の SQL 条件は、複数のフィルタステートメントを結合します。

AND

結合されたすべての用語が **TRUE** の場合は、イベント情報を表示します。

または

結合された用語のいずれかが **TRUE** の場合は、イベント情報を表示します。

HAVING

条件文を追加することによって、メインの SQL 文の条件を絞り込みます。たとえば、特定のホストからのイベント用に詳細フィルタを設定している場合に、「having」ステートメントを追加して、このホストからのイベントのうち指定した重大度のものだけを返すようにすることができます。

以下の SQL 演算子は詳細フィルタによって使用され、基本条件を作成します。

関係演算子

列が入力した値と適切な関係を保持する場合は、イベント情報を表示します。次の関係演算子を使用できます。

- 等しい
- 等しくない
- < (より小さい)
- > (より大きい)
- ≤ (以下)
- ≥ (以上)

たとえば、[> (より大きい)]を使用すると、設定した値よりも大きい値の選択列からイベント情報が含まれます。

に近い

入力したパターンが列に含まれている場合に、%を使用して該当するパターンを設定し、イベント情報を含めます。たとえば、L% は L で始まる任意の値を返しますが、%L% は L が最初の文字にも最後の文字にも含まれない任意の値を返します。

に近くない

列に指定したパターンが含まれていない場合にイベント情報を含めます。

設定が含まれている

引用符で囲まれた一連の入力値のうち、1 つ以上が対象の列に含まれている場合に、イベント情報を含めます。セット内に複数の値がある場合は、カンマで区切る必要があります。

設定が含まれていない

引用符で囲まれた一連の入力値のうち、1 つ以上が対象の列に含まれていない場合に、イベント情報を含めます。セット内に複数の値がある場合は、カンマで区切る必要があります。

一致する例

入力した 1 つ以上の文字に一致する任意のイベント情報を含め、キーワードの検索を可能にします。

キー設定済み

レポートサーバの設定中にキー値として設定したすべてのイベント情報を含めます。ビジネス上の関連性など、組織のグループを設定する際にキー値を使用できます。

キー未設定

レポートサーバの設定中にキー値として設定していないすべてのイベント情報を含めます。ビジネス上の関連性など、組織のグループを設定する際にキー値を使用できます。

詳細イベント フィルタの作成

詳細フィルタは、クエリの作成、レポートのスケジュール、アラート ジョブ、ローカル フィルタおよびグローバル フィルタなど、多くの機能によって使用されます。

詳細フィルタの作成方法

1. スケジュール済みレポート ジョブまたはアクション アラート ジョブを作成する場合は、[イベント] タブまたは[インシデント] タブをクリックして適切なフィルタ タイプを設定します。レポートまたはアラート ジョブにはイベント クエリとインシデント クエリの両方が含まれる場合があるため、フィルタ タイプを別々に設定できます。
2. [新規イベント フィルタ] をクリックします。
イベント フィルタ テーブルの最初の行が有効になり、その[ロジック] および[演算子] 列にそれぞれデフォルト値「AND」および「等しい」が設定されます。
3. (オプション) 必要に応じて、[ロジック] セルをクリックし、ロジック値を変更します。
4. [列] セルをクリックし、ドロップダウン メニューからイベント情報列を選択します。
5. [演算子] セルをクリックし、ドロップダウン メニューから演算子を選択します。
6. [値] セルをクリックし、該当する値を選択します。
7. (オプション) 左かっこおよび右かっこのセルをクリックして、必要なかっこの数を入力します。
8. (オプション) 手順 1 から 6 を必要に応じて繰り返して追加のフィルタ ステートメントを追加します。
9. すべてのフィルタ ステートメントを入力したら、[保存] をクリックします。

詳細情報:

[単純イベント フィルタの作成](#) (P. 569)

[詳細フィルタの使用](#) (P. 487)

結果の条件の設定方法

クエリに日付の範囲およびその他の結果の条件(行の制限や基本の表示時間など)を設定することができます。結果の条件は、クエリの実行時間までであればいつでも変更できるため、ベースクエリやフィルタを変更することなくクエリを変更する便利な手段として利用できます。

スケジュール済みレポートジョブまたはアクション アラートジョブを作成する場合は、ジョブを構成するイベントおよびインシデントクエリの結果条件を必要に応じて設定できます。

以下のタイプの結果の条件を設定できます。

- クエリの検索期間を制御する日付範囲条件
- 最大行数などの表示条件
- 特定の日付以降最も新しくグループ化されたイベントや、設定した数のイベントを含むグループ化されたイベントなど、グループ化されたイベントの条件

注: クエリを作成する際に少なくとも 1 列がグループ化されていなければ、クエリ表示から結果の条件を編集することはできません。

時間または日付範囲の設定

クエリの時間または日付範囲の条件を設定できます。これにより、検索対象となるイベント ログ ストアの範囲が絞り込まれ、クエリ効率が向上します。

事前定義済み時間範囲を使用するか、またはカスタム時間範囲を作成できます。カスタム時間範囲が適切に機能するように、開始時間と終了時間の両方を設定する必要があります。単にワнтаイム パラメータを設定する場合、この条件はクエリ SQL の「Where」句として表されます。

結果の条件を設定する方法

1. [結果の条件] ダイアログ ボックスを開きます。
2. スケジュール済みレポート ジョブまたはアクション アラート ジョブを作成する場合は、[イベント] タブまたは[インシデント] タブをクリックして適切なフィルタ タイプを設定します。レポートまたはアラート ジョブにはイベント クエリとインシデント クエリの両方が含まれる場合があるため、フィルタ タイプを別々に設定できます。
3. ドロップダウンリストから、事前定義済み時間範囲を選択します。たとえば、昨日受信したイベントを表示する場合は、「前日」を選択します。

注: アクション アラートまたはスケジュール済みレポートを作成する場合、インターフェースには以下のデフォルトの時間範囲が表示されます。

- アクション アラート: 過去 5 分
- スケジュール済みレポート: 過去 6 時間

4. (オプション) 以下のサブ手順を使用して、カスタム時間範囲を作成します。
 - a. [日付範囲の選択] 領域の[動的終了時間] エントリ フィールドの横にある[編集]をクリックします。クリックすると、クエリの検索対象とする期間の終了時間を設定できます。

[動的時間の指定] ダイアログ ボックスが表示されます。
 - b. パラメータのベースに使用する参照時間を選択し、[追加]をクリックします。
 - c. 必要な時間パラメータを選択し、[OK]をクリックします。複数の時間パラメータを追加できます。
 - d. パラメータの追加が完了したら、[OK]をクリックします。

[動的時間の指定]ダイアログ ボックスが閉じられ、選択した値が[動的終了時間]領域に表示されます。複数のパラメータを入力した場合、各パラメータが先頭から参照され、それらのパラメータから終了時間のステートメントが生成されます。たとえば、[動的終了時間]領域で[月初]を追加し、[曜日]に[火曜日]を設定すると、その月の最初の火曜日にクエリが終了します。

注:「日数」や「時間数」のような数値を使用する場合、過去の時間を設定するには、負の数字を入力する必要があります。正の数字を使用すると将来の終了時間が設定され、少なくとも 1 つの評価されたイベントがログ ストアにある限り、クエリは結果を送信し続けます。

たとえば、[動的開始時間]領域で[今すぐ]を追加し、[分数 - 10]と設定すると、選択した終了期間の 10 分前にクエリが実行されます。

- e. クエリの検索期間の開始時間を設定するには、[動的開始時間]領域で手順 2 を繰り返します。

日付範囲を入力しない場合、クエリはログ ストア内のすべてのイベントに適用されます。無効な日付範囲を入力した場合、クエリの結果が何も返されない場合があります。

- 5. 矢印をクリックして次に完了するクエリ的设计の手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックした場合は、新しいクエリがクエリリストに表示されます。それ以外の場合は、選択したクエリ的设计の手順が表示されます。

詳細情報:

[結果の条件の設定方法](#) (P. 489)

[表示とグループの条件の設定](#) (P. 492)

表示とグループの条件の設定

クエリの表示を制御する条件と、グループ化の方法に基づいてイベントを検索する条件を設定できます。

表示とグループの条件を設定する方法

1. [結果の条件]ダイアログ ボックスを開きます。
2. スケジュール済みレポートジョブまたはアクション アラート ジョブを作成する場合は、[イベント]タブまたは[インシデント]タブをクリックして適切なフィルタタイプを設定します。レポートまたはアラートジョブにはイベント クエリとインシデントクエリの両方が含まれる場合があるため、フィルタタイプを別々に設定できます。
3. [結果]チェック ボックスを使用して、必要な以下の表示条件を有効にします。

デフォルトのクエリ制限値

この値は、アクション アラートとレポートのスケジュールのみに使用可能です。アラートまたはレポートジョブを設定して、ジョブでクエリごとに行の制限値を使用するようにします。ジョブの作成時に他の結果値を選択した場合、CA Enterprise Log Manager ではコンポーネントのクエリ内の行の制限値を無視します。

行の制限値

クエリが最新のイベントから表示するイベントの最大行数を設定します。

制限なし

クエリでフィルタに一致するすべてのイベントを取得するよう設定します。その場合、イベント数が大きくなる可能性があるため、その点を考慮してクエリを作成する必要があります。

その他を表示

最大行数を超えたために表示されていない結果があることを示します。これにより、該当するタイプのすべてのイベントのコンテキストで選択したイベントを比較できます。たとえば、イベントビューア表示について[行の制限値]で「10」を選択し、[その他を表示]を選択した場合は、10を超える残りのイベントはすべて、[その他]というタイトルの1つのエントリとして表示されます。この設定は、行の制限値を選択したときのみ有効です。

時間粒度

クエリ表示で使用する[期間]フィールドの詳細レベルを設定します。

4. [結果の条件]を使用して、さまざまなタイプのグループ化されたイベント条件がクエリされます。たとえば、選択した日付以降の最新のグループ化されたイベントや特定数のグループ化されたイベントを検索するように、クエリを設定することもできます。グループ化されたイベントは、クエリの作成手順で機能およびグループの順序を設定した、精製済みイベントです。

グループの条件では、時間範囲フィールドと同じ時間ステートメント体系を使用します。

5. 矢印をクリックして次に完了するクエリの設計の手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックした場合は、新しいクエリがクエリリストに表示されます。それ以外の場合は、選択したクエリの設計の手順が表示されます。

詳細情報:

[結果の条件の設定方法](#) (P. 489)

クエリ表示の視覚化の作成

新規クエリ表示を作成するには、イベント情報の表示方法を制御する視覚化の詳細を設定する必要があります。

クエリ表示の視覚化を作成する方法

1. クエリの設計ウィザードを開きます。
2. まだ指定していない場合は名前とタグを入力してから、「視覚化」の手順に進みます。
3. クエリ表示にイベントビューアまたはグラフのいずれを使用するかを選択します。

イベントビューアを選択した場合は、視覚化の手順は完了です。イベント列は、クエリ列の作成手順で配置した順序で[イベントビューア]表示に表示されます。

4. グラフを選択した場合は、1 つ以上のグラフ タイプを選択できます。複数のグラフ タイプを選択すると、ユーザはレポート表示内でグラフ間を前後に切り替えることができます。各タイプの横に表示されている上矢印と下矢印によって、[視覚化の変更]メニューに表示される順序を変更できます。

注: この手順中に表を追加しなくても、表は常に視覚化として使用できます。

5. X(水平)軸として表示するイベントを[列]ドロップダウン メニューから選択し、表示するラベル テキストがある場合は入力し、[表示タイプ]メニューから以下のオプションのいずれか 1 つを選択します。
 - カテゴリ - 文字列またはテキスト値の列 (source_username など) にこのオプションを使用します。
 - 線形 - 数値 (event_count など) にこのオプションを使用します。値が広範囲に及ぶ場合は、[対数軸]チェック ボックスをオンにして、軸を対数にすることができます。
 - 日時 - このオプションを使用して時間値をローカルの日付/時間で表示します。
6. [Y 軸設定]メニューを使用して手順 4 を繰り返して、Y (垂直)軸列、ラベル、および種類のオプションを設定します。
7. 適切な矢印をクリックして次に実行する「クエリの設計」の手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、新規クエリが[クエリリスト]に表示されます。それ以外の場合は、選択したクエリの設計手順が表示されます。

ドリルダウン レポートの追加

1 つ以上のドリルダウンレポートをクエリに追加できます。ドリルダウンレポートを使用すると、クエリの表示要素をクリックして、別の関連レポートを表示することができます。

ドリルダウンレポートを追加する方法

1. クエリの設計ウィザードを開きます。
 2. まだ指定していない場合は名前とタグを入力してから、「ドリルダウン」の手順に進みます。
 3. [ドリルダウンの追加]をクリックします。
 4. 名前を入力するか、ドリルダウン アイテムとして使用可能にするレポートを参照します。
 5. ドリルダウン レポートの対象となる使用可能なパラメータを 1 つ以上選択し、[選択されたパラメータ]リストに移動します。ドリルダウンレポートは、選択されたパラメータを使用して、クエリの対象を維持します。
 6. 適切な矢印をクリックして次に実行する「クエリの設計」の手順に進むか、[保存して閉じる]をクリックします。
- [保存して閉じる]をクリックすると、新規クエリが[クエリリスト]に表示されます。それ以外の場合は、選択したクエリ的设计手順が表示されます。

クエリの編集

既存のカスタム クエリを編集することができます。サブスクリプション クエリは編集できません。ただし、サブスクリプション クエリをコピーし、そのコピーを編集することは可能です。クエリを編集すると、加えた変更によって、そのクエリを使用するすべてのレポートが影響を受けます。

クエリの編集方法

1. [クエリおよびレポート]タブをクリックし、[クエリ]サブタブをクリックします。
[クエリ タグ フィルタ]リストおよび[クエリリスト]が表示されます。
2. [クエリリスト]内の[ユーザ]フォルダを展開し、編集するクエリを選択します。
3. リスト上部の[オプション]をクリックし、[編集]を選択します。
クエリの実設計ウィザードが開き、選択したクエリの詳細が表示されます。
4. 必要に応じて変更を加え、[保存]をクリックします。

カスタム クエリの削除

カスタム クエリを削除できます。サブスクリプション クエリは削除できません。

クエリの削除方法

1. 削除するクエリを選択します。
2. リスト上部の[オプション]をクリックし、[削除]を選択します。
確認のダイアログが表示されます。
3. [はい]をクリックします。
削除したクエリが[クエリリスト]から削除されます。

詳細情報

[選択されたクエリの表示の無効化](#) (P. 314)

[クエリの編集](#) (P. 313)

[クエリ定義のエクスポートとインポート](#) (P. 314)

選択されたクエリの表示の無効化

クエリをロードせずに変更できるように、クエリリストを設定できます。通常、リストからクエリを選択すると、詳細ウィンドウにクエリが表示されます。

このデフォルトモードを無効にすると、リストからクエリを選択したときに、表示されるのを待つことなくすぐにクエリを編集でき、時間を節約できます。これは特に、複数のクエリを編集する必要があり、加えるべき変更の内容がすでにわかっている場合に便利です。

注: クエリの作成または編集が可能なのは **Administrator** モードまたは **Analyst** モードのユーザのみであるため、これらのユーザだけが選択されたクエリの表示設定を無効にできます。

選択されたクエリの表示を無効化する方法

1. [クエリリスト] 上部の [オプション] をクリックします。
[オプション] メニューが表示されます。
2. [選択されたクエリの表示] の横のチェックボックスをオフにします。
[選択されたクエリの表示] が再度オンにされるまで、リストから選択されたクエリは表示されません。

クエリ定義のエクスポートとインポート

ほかの管理サーバでできるように、カスタムクエリの詳細をエクスポートおよびインポートすることができます。これにより、**CA Enterprise Log Manager** 間で、またはテスト環境からライブ環境に、正常なカスタムクエリを転送できます。

詳細情報

[クエリ定義のインポート](#) (P. 316)

[クエリ定義のエクスポート](#) (P. 315)

クエリ定義のエクスポート

ユーザが作成したクエリの詳細をほかの管理サーバでできるようにエクスポートすることができます。エクスポートファイルは **XML** ファイルとして保存されます。

クエリの詳細をエクスポートする方法

1. [クエリおよびレポート]タブをクリックし、[クエリ]サブタブをクリックします。
[クエリリスト]が表示されます。
2. リスト上部の[オプション]をクリックし、[エクスポート]を選択します。
[ユーザ クエリ定義のエクスポート]ダイアログ ボックスが表示され、ユーザが作成した使用可能なレポートが表示されます。
3. シャトル コントロールを使用してエクスポートするクエリを選択し、[エクスポート]をクリックします。
[エクスポート]ダイアログ ボックスが表示されます。
4. **XML** エクスポートファイルを保存する場所を入力または参照し、[保存]をクリックします。
クエリ ファイルは選択した場所に保存され、確認ダイアログ ボックスが表示されます。
5. [OK]をクリックして[閉じる]をクリックします。
[ユーザ クエリ定義のエクスポート]ダイアログ ボックスが閉じます。

詳細情報

[クエリ定義のエクスポートとインポート](#) (P. 314)

[クエリ定義のインポート](#) (P. 316)

クエリ定義のインポート

クエリ定義 XML ファイルをローカル管理サーバでできるようにインポートすることができます。

レポートの詳細をインポートする方法

1. [クエリおよびレポート]タブをクリックし、[クエリ]サブタブをクリックします。
[クエリリスト]が表示されます。
2. リスト上部の[オプション]をクリックし、[インポート]を選択します。
[ファイルのインポート]ダイアログ ボックスが開きます。
3. ファイルをインポートする場所を入力または参照し、[OK]をクリックします。
[結果のインポート]ウィンドウが表示されます。
4. [別のファイルのインポート]をクリックして手順 3 を繰り返すか、または[閉じる]をクリックします。
[結果のインポート]ウィンドウが閉じます。

詳細情報

[クエリ定義のエクスポートとインポート](#) (P. 314)

[クエリ定義のエクスポート](#) (P. 315)

レポートの作成方法

お使いの環境のカスタムレポートを作成するには、このセクションで説明するプロセスを使用してまったく新しいレポートを作成する方法と、テンプレートとして事前定義されたレポートを使用する方法があります。カスタムレポートは、表示およびスケジュールされたレポートテンプレートとして設定できます。

また、カスタムレポートを編集または削除したり、レポート情報をエクスポートしたりすることも可能です。これらのカスタム設定のタスクは、**Administrator** ロールまたは **Analyst** ロールを持ったユーザとしてログインしている場合にのみ実行できます。

レポートデザインウィザードを使用して新規レポートを作成するプロセスは、以下の手順で構成されます。

1. レポートデザインウィザードの表示
2. レポートの詳細の追加 - 新規レポートの命名およびカテゴリ タグの割り当て
3. レポートレイアウトの設計 - クエリに含めるレポートおよび表示方法の選択

レポート デザイン ウィザードの表示

カスタムレポートをゼロから新たに作成したり、既存レポートをベースに作成するには、レポート デザイン ウィザードを起動する必要があります。

レポート デザイン ウィザードを表示する方法

1. [クエリおよびレポート]タブをクリックし、[レポート]サブタブをクリックします。

[レポートリスト]ページが表示されます。

2. [オプション]をクリックし、[新規]または[コピー]を選択します。

[レポート デザイン]ウィザードが表示されます。

ウィザードを使用する際に

- ウィザードを閉じずに保存するには、[保存]をクリックします。
- レポートを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

レポートの詳細の追加

新規レポートは、まったく新しく作成することも、既存レポートのコピーから作成することもできます。レポートを作成する場合は、レポートに名前を付け、関連付けるサブスクリプションまたはカスタム タグを追加します。

レポートの詳細を追加する方法

1. レポート デザイン ウィザードを開きます。
2. レポート名を入力します。参照用に、オプションのデザイン情報を入力することもできます。
3. [タグ]シャトル コントロールを使用してレポートに関連付けるタグを 1 つ以上選択します。
4. (オプション) カスタム カテゴリ タグを追加するには、[カスタム タグの追加] エントリ フィールドにタグ名を入力し、[タグの追加] ボタンをクリックします。
[選択されたタグのリスト]と同じカスタム タグが表示されます。
5. (オプション) ネストされた 1 つ以上のカスタム タグを追加するには、タグを選択するか、または親カテゴリのタグ名、円記号、子タグの名前の順に入力して、[タグの追加]をクリックします。たとえば、「**Regulations¥Industry Standards**」のように入力します。この形式を保持しながら、さらにタグを追加できます (a¥b¥c など)。

注: ネストされたカスタム タグの 1 つを削除すると、ネスト先のすべてのタグ (親タグを含む) も削除されます。カスタム タグをサブスクリプション タグの内部にネストし、その後削除した場合は、カスタム タグのみが削除されます。

プロセスを完了すると、リストに新しいタグが表示されます。親タグを展開するとネストされたカスタム タグが表示されます。
6. 「レイアウト」の手順に進むか、少なくとも 1 つのクエリがすでに選択されている場合は[保存して閉じる]をクリックします。

レポートレイアウトの設計

グリッド サイズと寸法を指定し、グリッドの各セクションに表示するクエリを選択して、レポートの構造を設計できます。

レポートレイアウトの設計方法

1. レポート デザイン ウィザードを開きます。新規レポートの場合は、名前を入力し、タグを選択して、「レイアウト」の手順に進みます。
2. レポートに表示する行数と列数を、[レポートレイアウト] ペインの[グリッド 行]領域および[グリッド列]領域で選択または入力します。これらの設定によって、レポートに含めるクエリ表示領域の数を制御します。最大 **10** までの行および列を含めることができます。

指定数の行、列、および対応するクエリ表示が[レポートレイアウト]ペインに表示されます。

注: 個々のクエリ表示領域の右側および下部にある矢印を使用すると、必要に応じて水平方向または垂直方向に拡張または縮小することができます。

3. (オプション)クエリ表示領域の最小ピクセル サイズを、[幅の最小値]領域および[高さの最小値]領域で選択します。
4. 各表示領域に表示するクエリを[クエリリスト]からレポートレイアウトの適切な領域にドラッグします。
5. (オプション) 各クエリ表示領域の上部にある[編集]をクリックすると、配置したクエリを編集したり、新規クエリを作成したりできます。
6. [保存して閉じる]をクリックします。

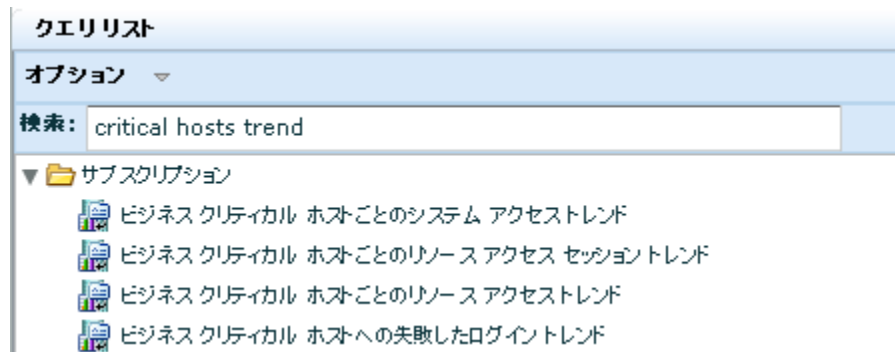
レポート デザイン ウィザードが閉じます。[ユーザ]フォルダ下の[レポートリスト]に、新規レポートが表示されます。

例：既存のクエリによるレポートの作成

事前定義済みクエリから構成されるカスタムレポートを作成し、各環境仕様に合わせてカスタマイズできます。

既存のクエリからレポートを作成する方法

1. カスタムレポートに含めるクエリを特定します。
 - a. 表示されていない場合は、[クエリおよびレポート]タブをクリックし、[クエリ]サブタブをクリックします。
 - b. [検索]フィールドにキーワードまたはキーフレーズを入力し、その内容を含んだ選択対象クエリを表示します。たとえば、「クリティカル ホストトレンド」と入力します。
 - c. カスタムレポートに含めるクエリの名前を指定します。たとえば、以下の図でリスト表示されている、システム アクセス、リソース アクセス、およびアカウント作成に関するビジネス クリティカル ホストのトレンドレポートを定義できます。



2. 初めてレポートにクエリを含める場合は、コピーを作成し、カスタム タグを追加します。
 - a. クエリを選択し、[オプション]ドロップダウン リストから[コピー]を選択します。
 - b. クエリの名前を変更し、追加するカスタム タグを入力します。たとえば、「ビジネス クリティカル ホストごとのシステム アクセストrend」のコピーの名前を、「ビジネス クリティカル ホストごとのカスタム システム アクセストrend」に変更します。

- c. カスタム タグを追加します。たとえば、「Critical_Assets_Trend」と入力し、[タグの追加]をクリックします。

- d. [移動]ボタンをクリックし、事前を選択したタグを[使用可能なタグ]領域に移動します。たとえば、「システム アクセス」を移動します。追加されるのは、選択したタグだけです。

- e. [保存して閉じる]をクリックします。
3. ほかのクエリをレポートに含める場合は、コピーを作成し、作成済みのカスタムタグを選択します。
- a. クエリを選択し、[オプション]ドロップダウンリストから[コピー]を選択します。
- b. クエリの名前を変更し、新規作成したカスタムタグを選択します。たとえば、「ビジネスクリティカル ホストごとのリソース アクセストレンド」のコピーの名前を、「リソースクリティカル ホストごとのカスタム システム アクセストレンド」に変更し、「Critical_Assets_Trend」を[選択されたタグ]リストに移動して、事前を選択したタグを削除します。
- c. [保存して閉じる]をクリックします。

コピーしたクエリが、[ユーザ]の下に表示されます。

4. クエリがキー設定済みリストに関連付けられている場合、そのキー設定済みリストの値を定義します。
5. 以下のように、レポート作成プロセスを開始します。
 - a. [クエリおよびレポート]タブをクリックし、[レポート]サブタブをクリックします。
 - b. [レポートリスト]の下の[オプション]ドロップダウンリストから[新規作成]を選択します。

[レポート デザイン]ウィザードが表示されます。

カスタム タグとして、Critical_Assets_Trend を追加します。
6. レポートレイアウトを設計します。

レポート レイアウト

左のクエリライブラリからクエリをグリッドにドラッグ アンド ドロップするか、[クエリ]をクリックしてクエリを選択します。

Grid Rows: 3 Columns: 1

Custom Account Creations by Business Critical Hosts Trend
Custom Account Creations by Business Critical Hosts Trend

Custom Resource Access by Business Critical Hosts Trend
Custom Resource Access by Business Critical Hosts Trend

Custom System Access by Business Critical Hosts Trend
Custom System Access by Business Critical Hosts Trend

7. [保存して閉じる]をクリックします。
8. 作成したカスタム タグに基づいてレポートをスケジュールします。
9. レポートを表示します。

注: 新規作成したレポートを調べ、必要な情報が可能な限り最善の方法で提供されているか確認することをお勧めします。

例：連携および連携されたレポートの設定

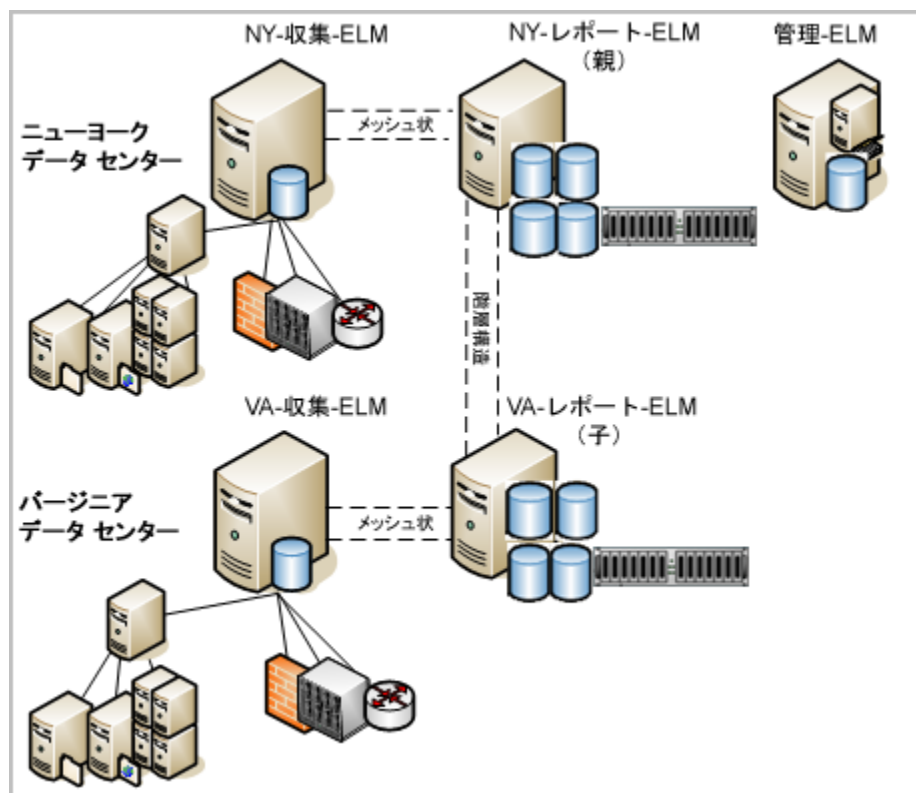
ボリュームが大きく、地理的に離れた複数のデータ センターからログを収集し、レポート作成を設定すると、1 つのデータ センターだけを使用して分散データのクエリを実行できます。

ボリュームの大きな 2 つのデータ センターがニューヨークとバージニアにあり、ニューヨークが本社であるというシナリオ例を考えます。各データ センターには、受信イベント ログを収集して処理し、それらをレポート サーバに送信する収集サーバがあります。レポート サーバでは、クエリ、アラート、およびレポートが処理されます。ほとんどのクエリ、アラート、およびレポートは、エージェントによって収集されたイベント データをターゲットとしています。これらのイベントソースからのデータを統合するには、レポート サーバおよび収集サーバ間の連携が必要になります。

クエリ、アラート、およびレポートの中には、CA Enterprise Log Manager サーバによって生成された自己監視イベントをターゲットにするものがあります。このタイプのデータの統合には、連携内に管理サーバを含める必要があります。自己監視イベントデータの統合が必要ない場合は、連携から管理サーバを除外できます。このサーバからの自己監視イベントを、連携していないローカルレポートを使用して監視できます。例を簡潔にするために、この連携では管理サーバを除外します。含める必要がある場合は、NY- レポーティング -ELM および管理 -ELM 間のメッシュ統合を作成します。

サーバ名は以下のとおりです。

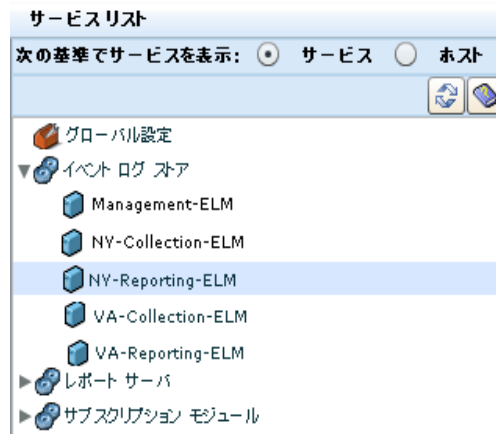
- 管理 -ELM
- NY-Collection-ELM
- NY-Reporting-ELM
- VA- 収集 -ELM
- VA- レポート -ELM



ニューヨーク サイトから実行されるすべてのレポートおよびアラートに、バージニア サイトからのデータをすべて含め、バージニア サイトから実行されるすべてのレポートおよびアラートには、ローカルで収集されたデータのみを含めたいと、ニューヨークの管理者が考えているとします。

以下の例は、サーバを連携させ、このシナリオ用の基準を満たすようレポートを設定する方法を示しています。自動アーカイブを設定する手順は、この例には含まれていませんが、ボリュームの大きなアーキテクチャの場合は自動アーカイブを設定する必要があります。

1. 管理者の認証情報で CA Enterprise Log Manager にログインします。
2. [管理]タブをクリックして、[サービス]サブタブを選択します。
3. 以下の要領で、NY-レポート-ELM が親で、VA-レポート-ELM が子である階層統合を作成します。
 - a. イベントログストアサービスを展開し、階層統合で親となるサーバの名前を選択します。この場合は、「NY-レポート-ELM」に相当します。



- b. 使用可能な連携の子リストから「VA-レポート-ELM」を選択し、[選択済み]リストに移動させます。



4. 以下の要領で、一方が他方の子である、NY-レポート-ELM と NY-レポート-ELM 間のメッシュ統合を作成します。
 - a. [イベントログストア]リストから「NY-レポート-ELM」を選択します。
 - b. 使用可能な連携の子から「NY-収集-ELM」を選択し、[選択済み]リストに移動させます。
 - c. [イベントログストア]リストから「NY-収集-ELM」を選択します。
 - d. 使用可能な連携の子から「NY-レポート-ELM」を選択し、[選択済み]リストに移動させます。

5. 以下の要領で、一方が他方の子である、VA- レポート -ELM と VA- レポート -ELM 間のメッシュ統合を作成します。
 - a. [イベント ログ ストア] リストから「VA- レポート -ELM」を選択します。
 - b. 使用可能な連携の子から「VA- 収集 -ELM」を選択し、[選択済み] リストに移動させます。
 - c. [イベント ログ ストア] リストから「VA- 収集 -ELM」を選択します。
 - d. 使用可能な連携の子から「VA- レポート -ELM」を選択し、[選択済み] リストに移動させます。
6. 以下の要領で、VA- レポート -ELM 用のグローバル レポート サーバ設定およびローカルの上書き内容を設定します。地理的に離れたサーバでは通常、複数のメール サーバが使用されます。
 - a. [サービスリスト] から [アラート サービス] を選択します。
 - b. NY - レポート - ELM ノードから、メール サーバ オプションに必要なグローバルまたはローカルの設定を指定します。
 - c. 電子メール レポートを使用する場合は、[レポート サーバ] を選択し、NY - レポート - ELM ノードを選択します。
 - d. グローバルまたはローカルの PDF 形式オプション、またはレポートとアラート保持に関するレポート オプションを設定します。

7. NY- レポート -ELM から実行されるようスケジュールされた各レポートに対して、以下を実行します。
 - a. [スケジュール済みレポート]タブをクリックし、[レポートのスケジュール]タブをクリックします。
 - b. [レポートのスケジュール]をクリックします。
 - c. スケジュールするレポートを選択し、必要に応じて手順 2、3、4、および 5 を完了します。
 - d. [サーバの選択]をクリックし、使用可能なサーバリストから「NY- レポート -ELM」を選択して、[選択済みサーバ]リストに移動させ、連携クエリをデフォルトの[はい]のままにします。
 - e. [保存して閉じる]をクリックします。

The screenshot shows the 'Server Selection' (サーバの選択) dialog box. At the top, there are six numbered steps: 1. Report Selection, 2. Report Filter, 3. Result Conditions, 4. Job Scheduling, 5. Execution, and 6. Server Selection. Step 6 is highlighted. Below the steps, there is a 'Time Zone' (タイムゾーン) dropdown set to '(GMT-04:00) America/New_York'. The main area is divided into two sections: 'Available Servers' (使用可能なサーバ) on the left and 'Selected Servers' (選択されたサーバ) on the right. The 'Selected Servers' section contains a table with two columns: 'Server' (サーバ) and 'Link Query' (連携クエリ). The table has one row with 'NY-Reporting-ELM' and 'はい' (Yes).

サーバ	連携クエリ
NY-Reporting-ELM	はい

作成されるレポートには、NY- レポート -ELM、そのピアの NY- 収集 -ELM、その子の VA- レポート -ELM、およびその子のピア VA-Collection-ELM からのデータが含まれます。

注： VA- レポート -ELM から実行される連携クエリには、VA- レポート -ELM およびそのピア VA- 収集 -ELM からのデータが含まれます。NY- レポート -ELM からのデータは含まれません。これは、このサーバが階層統合の親であるためです。

レポートの編集

カスタム レポートを編集できます。

注: 複数のレポートを編集する場合は、[選択されたレポートを表示]オプションを無効にできます。これによって、レポートが[詳細]ペインに表示されるのを待たずに、レポートを選択したり編集したりすることができます。

レポートの編集方法

1. 編集するレポートを[レポートリスト]から選択します。
2. リスト上部の[オプション]をクリックし、[編集]を選択します。
レポート デザイン ウィザードが開き、選択したレポートの詳細が表示されます。
3. 必要な変更を加えて、[保存して閉じる]をクリックします。
[ユーザ]フォルダ下の[レポートリスト]に、編集されたレポートが表示されます。

カスタム レポートの削除

カスタム レポートを削除することができます。サブスクリプションレポートは削除できません。

カスタム レポートを削除する方法

1. レポートリストから削除するカスタム レポートを選択します。
2. リスト上部の[オプション]をクリックし、[削除]を選択します。
確認のダイアログが表示されます。
3. [はい]をクリックします。
削除したレポートが[レポートリスト]から削除されます。

詳細情報

[レポートの作成方法](#) (P. 317)

[レポートの編集](#) (P. 328)

例: 30 日以上経過した日単位レポートの削除

レポートサーバのグローバル設定によってレポート保持に関するポリシーを実装できます。以下のように、レポートのスケジュールの反復間隔別に異なる保持ポリシーを設定できます。

- ワンタイムレポート保持
- 日単位レポート保持
- 週単位レポート保持
- 月単位レポート保持
- 年単位レポート保持

レポート保持ユーティリティのデフォルト値の「実行しない」をいずれかの間隔に変更する必要があります。ユーティリティに設定する実行頻度が、設定済みの削除頻度と対応していることを確認します。たとえば、日単位レポートを実行して 1 日経過したら削除する必要がある、その日単位レポートを午前 6 時と午後 6 時に実行するよう設定している場合は、レポート保持ユーティリティを少なくとも 12 時間おきに実行するよう設定します。

例: 30 日以上経過したすべての日単位レポートの削除

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
[サービスリスト]に、サービス別にサービスが表示されます。
2. [レポートサーバ]をクリックします。
[グローバル サービス設定]の[レポートサーバ]が表示されます。
3. 以下のガイドラインを使用して、この設定を完了します。
 - 作成後 30 日を経過したすべての日単位レポートの削除を自動化するには、30 日経過後に削除するよう、日単位レポートの保持ルールを設定します。
 - 必ず、指定した時間数、日数、または週数おきに実行されるようレポート保持ユーティリティを設定してください。

レポート保持ユーティリティ	実行しない	指定した間隔後に実行	指定した間隔後に削除
ワンタイムレポート保持	☐	☐	☒
日単位レポート保持	☐	☐	☒
週単位レポート保持	☐	☐	☒
月単位レポート保持	☐	☐	☒
年単位レポート保持	☐	☐	☒

4. [保存]をクリックします。

レポート定義のエクスポート

ユーザが作成したファイルの詳細をほかの管理サーバでできるようにエクスポートすることができます。エクスポートファイルは XML ファイルとして保存されます。エクスポートされたレポート定義には、そのレポート内にあるすべてのクエリの定義が含まれています。

レポートの詳細をエクスポートする方法

1. [クエリおよびレポート]タブをクリックし、[レポート]サブタブをクリックします。
[レポートリスト]が表示されます。
2. リスト上部の[オプション]をクリックし、[エクスポート]を選択します。
[ユーザ定義のエクスポート]ダイアログ ボックスが表示され、使用可能なユーザが作成したレポートが表示されます。
3. シャトル コントロールを使用してエクスポートするレポートを選択し、[エクスポート]をクリックします。
[エクスポート]ダイアログ ボックスが表示されます。
4. XML エクスポート ファイルを保存する場所を入力または参照し、[保存]をクリックします。
レポートファイルは選択した場所に保存され、確認ダイアログ ボックスが表示されます。
5. [OK]をクリックして[閉じる]をクリックします。
[ユーザレポート定義のエクスポート]ダイアログ ボックスが閉じます。

詳細情報

[レポート定義のインポート](#) (P. 331)

レポート定義のインポート

レポート定義 XML ファイルをローカル管理サーバでできるようにインポートすることができます。

レポートの詳細をインポートする方法

1. [クエリオよびレポート]タブをクリックし、[レポート]サブタブをクリックします。
[レポートリスト]が表示されます。
2. リスト上部の[オプション]をクリックし、[インポート]を選択します。
[ファイルのインポート]ダイアログ ボックスが開きます。
3. ファイルをインポートする場所を入力または参照し、[OK]をクリックします。
[結果のインポート]ウィンドウが表示されます。
4. [別のファイルのインポート]をクリックして手順 3 を繰り返すか、または[閉じる]をクリックします。
[ユーザ レポートとクエリオよびクエリ定義のインポート]ウィンドウが閉じます。

詳細情報

[レポート定義のエクスポート](#) (P. 330)

キー設定済みリストのあるレポートの使用準備

すべてのレポートは、1 つ以上のクエリから構築されます。事前定義済みレポートで使用する一部のクエリは、特定の属性フィールドにキーの値のリストをコンパイルするための条件として使用される値が含まれている場合に、指定されたテーブルからのすべての値を選択するように設計されています。たとえば、アセットテーブルには **IsCritical** フィールドがあります。**IsCritical** が「はい」と等しい場合、アセットテーブルからすべてのアセット名を選択するクエリは、重要なアセットの名前だけを選択します。これらの名前は **CA Enterprise Log Manager** に返され、**Critical_Asset** キーの値がリフレッシュされます。

キー設定済みリストを備えた事前定義済みレポートを使用する準備には、次のタスクが含まれます。

- (オプション) **CA IT PAM** を使用している場合は、動的値のインポートを有効にします。
- 事前定義済みの値を持っていない事前定義済みキーに対して、キー設定済みリストを作成します。
- 事前定義済みの値を持っている事前定義済みキーのキー設定済みリストをカスタマイズします。
- 使用する事前定義済みレポートで、使用するキー設定済みリストの保守を行います。キー設定済みリストを現在の値で更新します。

さらに、キー設定済みリストを使用するカスタムレポートに新しいキーを追加して、その新しいキーに値を追加することができます。また、独自に設計したオンデマンドのクエリの **Business_Critical_Sources** キーや **ELM_System_Lognames** キーに対して、値を追加することもできます。

動的値のインポートの有効化

動的値のインポートを有効化するのに必要な手順は、CA IT PAM ユーザにのみ適用されます。

CA IT PAM を使用しており、ファイル、データベース、ホストおよびユーザなどのリストが格納された既存のテーブルまたはスプレッドシートがある場合には、このデータを活用できます。ユーザはテーブルまたはファイルを読み取り、キーに関連する値を選択して、そのキーに対応する CA Enterprise Log Manager 値のリストにそれらの値を返すプロセスを作成できます。

動的値をインポートする方法

1. CA IT PAM で、オンデマンドで生成する必要がある各キー値のリストについてプロセスを作成します。

注: プロセスでデータベース テーブルを読み取る場合は、SQL Server 2005 データベースが格納されたサーバ上に CA IT PAM エージェントをインストールしてください。

2. CA Enterprise Log Manager で、動的値用に CA IT PAM 統合を設定します。

詳細情報:

[値リストを生成する CA IT PAM プロセスの作成](#) (P. 334)

[動的な値のための CA IT PAM 統合の設定](#) (P. 335)

動的値プロセスについて

動的値プロセスは、レポートやアラートで使用されている選択済みキーの値を登録または更新する際に呼び出される CA IT PAM プロセスです。ファイル、データベース、ホスト、ユーザなど、環境を構成するもののマスタリストをすでに格納しており、このマスタリストは関係する値セットのクエリを実行できる属性を考慮して設計されていることを前提としています。CA IT PAM を使用すると、CA Enterprise Log Manager にデータを返すクエリを実行するために呼び出すことができるプロセスを作成できます。このデータは、キーに基づいたレポートとアラートでキー値として使用します。値リストを動的に作成することができることは、変更の多いキーリストを現在値で更新された状態を保つ便利な方法です。

値リストを生成する CA IT PAM プロセスの作成

各キーの値リストをオンデマンドで生成できるようにするために、CA IT PAM でプロセスを作成できます。プロセスの作成の詳細については、CA IT PAM のドキュメントを使用します。各プロセスは、InputKey、ValueList、および FaultString ローカル プロセス パラメータ、および Success と Failure 計算演算子に関する CA Enterprise Log Manager の要件を満たす必要があります。

以下のガイドラインに従ってください。

- プロセスは、選択したキーを InputKey として受け入れる必要があります。
- プロセスは、次の 2 つのローカル プロセス パラメータを定義する必要があります。
 - ValueList (値リストを取得します)。
 - FaultString (エラー文字列を取得します)。

注: CA Enterprise Log Manager では、これらの正確なパラメータ名を出力インターフェースのパラメータとして使用する必要があります。

- プロセスには次の 2 つの計算演算子が含まれている必要があります。
 - 成功計算演算子: Process.ValueList=<値のカンマ区切りリストを含む変数>
 - 失敗計算演算子: Process.FaultString=<エラー メッセージを含む変数>

スクリプトを作成する場合は、次の追加のガイドラインを考慮します。

- スクリプトがデータベース テーブルから列を選択する場合、IT PAM エージェントは SQL Server 2005 がインストールされているサーバに存在する必要があります。SQL Servers は[すべてのタッチポイント]下のドメインに表示されている必要があります。キー データを含む SQL Server は、SQL Server 用のエージェント名を表示する必要があります。
- インライン スクリプトでは、必要なリストを取得するために sqlcmd ユーティリティを実行する必要があります。

詳細情報:

[動的な値のための CA IT PAM 統合の設定](#) (P. 335)

動的な値のための CA IT PAM 統合の設定

次のいずれかのタイプ、または両方のタイプの CA IT PAM プロセスを活用するように CA IT PAM 統合を設定できます。

- イベント/アラート出力プロセス - ヘルプ デスク製品などのサードパーティシステムの処理を呼び出すプロセス
- 動的値プロセス - 入力キーを受け取り、そのキーの現在の値をカンマ区切り値 (*.csv) ファイルとして返すプロセス

どちらか一方の目的のために設定するには、CA IT PAM を起動してログインする必要があります。以下の値を確認しておきます。

- CA IT PAM サーバの完全修飾ホスト名、または IP アドレス
- ポート(デフォルトは 8080)
- CA Enterprise Log Manager が CA IT PAM にログインするために使用するユーザ名およびパスワード

動的な値のために **CA IT PAM** を設定するには、設定済みの動的値プロセスによって動的に生成される値のリストをインポートします。特定のレポートおよびアラートで使用されるキー設定済みの値を設定またはリフレッシュする場合に、インポートが行われます。

以下の手順は、共通の設定、および動的値固有の設定の両方に対応します。

動的値プロセスのために CA IT PAM 統合を設定する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [レポート サーバ]をクリックします。
[グローバル サービス設定]の[レポート サーバ]が表示されます。
3. [IT PAM]領域までスクロールします。
4. 次のエントリによって **CA IT PAM** にアクセスできるようにします。
 - a. **CA IT PAM** がインストールされているサーバの完全修飾ホスト名を入力します。
 - b. デフォルトのポート番号 **8080** を受け入れます。
 - c. **CA IT PAM** の有効なログイン認証情報を入力します。
5. [動的値プロセス]フィールドでプロセスのパスを入力します。
動的値をインポートする場合、このプロセスパスがデフォルトになります。
6. [保存]をクリックします。
[確認: 設定の変更が正常に保存されました。]というメッセージが表示されます。

キー設定済みリストを管理する方法

キー設定済みリストは、一部の事前定義済みレポート、およびアクション アラートとして使用できるようにタグが付けられた一部の事前定義済みクエリの中で使用されます。これらのレポートを使用する、またはこれらのクエリを使用するアラートを作成する予定がある場合は、以下の方法を自由に組み合わせてキー設定済みリストを管理できます。

- 任意の選択したキー用にキー値を直接追加できます。また、すべてのキー値を選択して、編集または削除することができます。
- CSV リストに格納されたキー値をインポートできます。あるいは、CSV ファイルとして値の現在のリストをエクスポートして、その CSV ファイルを更新し、値リストにインポートして読み込むこともできます。
- 動的に現在のリストを生成し、値リストに読み込む CSV ファイルとして値を返す CA IT PAM プロセスを実行できます。

キー設定済みリストを使用するカスタムレポートを作成する予定がある場合は、カスタム キーを追加してから、その値を追加またはインポートすることができます。

まずクエリで使用するキー設定済みリスト(複数可)を指定し、そのクエリが含まれるレポートまたはアラートをスケジュールする前にそのリストを更新できます。

詳細情報:

[キー設定済みリストの作成](#) (P. 338)

[キー設定済みリストの手動更新](#) (P. 339)

[エクスポート/インポートによるキー設定済みリストの更新](#) (P. 340)

[例: CSV によるキー設定済みリストの更新](#) (P. 341)

[アクション アラートとしてタグが付いたクエリの使用](#) (P. 353)

キー設定済みリストの作成

キー設定済みリストを使用すると、グループを作成し、そのグループに値を割り当てることができます。その後、グループ名に対してクエリを実行すると、グループ内の任意の値が正の結果を返します。値は個々に割り当てすることも、.csv ファイルからインポートすることもできます。カスタム キー設定済みリストを作成することも、定義済みリストに値を追加することもできます。

たとえば、権限付与レポート用の一部のクエリは、「Privileged_Groups」というキー値を検索します。クエリにこの値が含まれていれば、グループに割り当てられた値のいずれかがフィールドに含まれている行がすべて返されます。

キー設定済みリストを作成する方法

1. [管理] タブをクリックし、[ライブラリ] サブタブをクリックして、[キー設定済みリスト] フォルダを展開します。
2. [新規] をクリックして新しいリストを作成するか、または値を追加するリストを選択します。
[キー設定済みリストの詳細] が右ペインに表示されます。
3. キー設定済みリストの名前および説明を入力し、タイプを選択します。
4. 複数の値をインポートする場合は、手順 8 に進みます。値を個々に追加する場合は、手順 5 に進みます。
5. [キー設定済みリストの値] テーブルの上部にある[追加] をクリックします。
[ユーザ] 列に行が強調表示されます。
6. その行をクリックして値を入力します。
7. 手順 4 および 5 を繰り返して値を追加します。
8. [キー設定済みリストの詳細] 領域の上部にある[インポート] をクリックし、インポートする値が格納されているファイルを検索して[OK] をクリックします。
値が[値] 領域に表示されます。
注: インポートできるのは、特殊文字が含まれていない .csv ファイルだけです。
9. 目的の値をすべて追加したら、[保存] をクリックします。
[キー設定済みリスト] フォルダの[ユーザ] フォルダに新しいリストが表示されます。

キー設定済みリストの手動更新

キー設定済みリストを複数の方法で更新できます。そのうちの 1 つの方法は、値を手動で追加し、編集し、削除することです。

キー設定済みリストを手動で更新する方法

1. [管理] タブをクリックし、[ライブラリ] サブタブをクリックして、[キー設定済みリスト] フォルダを展開します。
2. [キー設定済みリスト] フォルダを展開し、更新するキー設定済みリストを選択します。
3. キー設定済みリストに値を追加するには、以下の手順を実行します。
 - a. 値を追加するキーを選択します。
 - b. [値の追加] をクリックします。
 - c. [名前] フィールドに値の名前を入力し、[OK] をクリックします。
追加された値が選択されたキーの[値]リストに表示されます。
 - d. 追加する値ごとに、これらの手順を繰り返します。
4. キー設定済みリストの値を削除するには、以下の手順を実行します。
 - a. 不要な値を持つキーを選択します。
 - b. 削除する値をクリックし、[値の削除] をクリックします。
確認メッセージが表示されます。
 - c. [OK] をクリックします。
選択されたキーの[値]リストから値が削除されます。
 - d. 削除する値ごとに、これらの手順を繰り返します。
5. キー設定済みリストの値を編集するには、以下の手順を実行します。
 - a. 変更する値を持つキーを選択します。
 - b. 変更する値を選択し、[値の編集] をクリックします。
 - c. [名前] フィールドでエントリを編集し、[OK] をクリックします。
選択されたキーの[値]リストに、名前が変更された値が表示されます。
 - d. 編集する値ごとに、これらの手順を繰り返します。
6. [保存] をクリックします。
選択されたキーの値が更新されます。

エクスポート/インポートによるキー設定済みリストの更新

キーに対応する値を Excel スプレッドシートに格納する場合は、カンマ区切り値リスト (*.csv) としてそのスプレッドシートを保存し、インポートにより、選択したキー設定済みリストを読み込むことができます。

CSV ファイルに格納したキー設定済みリストの値を更新する方法は、以下のとおりです。

- CSV ファイルには指定したキーの最新の値が格納されているが、表示された[値]リストが最新の値でない場合は、CSV ファイルから直接値をインポートできます。
- CSV ファイルを作成して、そのファイルを古い値で更新する必要がある場合は、エクスポート、編集、インポートの順序で実行します。

エクスポートまたはインポートによりキー設定済みリストを更新する方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックして、[キー設定済みリスト]フォルダを展開します。
2. [キー設定済みリスト]フォルダを展開し、更新するキー設定済みリストを選択します。
3. 最新の値が格納されている CSV ファイルから選択したキーの値を更新するには、以下の手順に従います。
 - a. [キー値]リストで、更新するキーを選択します。
 - b. [値]リスト ツールバーで、[値のインポート]をクリックします。
[ファイルのインポート]ダイアログ ボックスが表示されます。
 - c. [参照]をクリックし、選択したキーの値を含む CSV ファイルが保存されているフォルダへ移動します。
 - d. インポートするファイルを選択して[開く]をクリックし、次に[OK]をクリックします。

[値]リストが CSV ファイルからの値で更新されます。

4. CSV ファイルが存在しないかまたは最新でないキーを選択して値を更新するには、以下の手順に従います。
 - a. [キー値]リストで、更新するキーを選択します。
 - b. [値]ツールバーで、[値のエクスポート]をクリックし、CSV ファイルを保存する場所に移動して[保存]をクリックします。
成功の確認メッセージが表示されます。
 - c. [OK]をクリックします。
 - d. エクスポートされたファイルに移動し、スプレッドシートを開き、既存の列を必要に応じて修正または削除します。スクロールして最後の列まで表示し、新しいエントリを追加します。次に、CSV ファイルとしてファイルを保存します。
 - e. 同じキーを選択し、[値のインポート]をクリックします。
 - f. [参照]をクリックし、保存したファイルを選択し、[開く]をクリックします。
 - g. [OK]をクリックします。
ファイルがアップロードされます。[値]リストの末尾までスクロールすると、新規エントリが追加されていることを確認できます。

例: CSV によるキー設定済みリストの更新

以下の 3 つの方法で、キー設定済みリストの値を入力できます。

- 手動によるキー値の入力
- CSV ファイルからのキー値のインポート
- 指定された CA IT PAM プロセスからのキー値のインポート

次の例をガイドとして使用し、ユーザ定義のキー設定済みリストの値を更新します。ここでは、値は Excel スプレッドシートに格納され、カンマ区切りの値リスト (*.csv)として保存されています。

CSV ファイルを使用してキー設定済みリストを更新する方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックして、[キー設定済みリスト]フォルダを展開します。
2. [キー設定済みリスト]フォルダを展開し、更新するキー設定済みリスト (Default_Accounts など)を選択して、[値のエクスポート]をクリックします。
エクスポートダイアログボックスが開き、デフォルトのファイル名として file.csv が表示されます。

3. エクスポートするファイルを保存するディレクトリを選択します。ファイル名を変更し(「Default_Accounts.csv」など)、[保存]をクリックします。
確認メッセージが表示されます。
4. [OK]をクリックします。
5. エクスポートされた.csv ファイルを参照して開き、スクロールで最後の列を表示し、エントリを追加します。必要に応じて、Default_Accounts のキー設定済みリストから削除したいデフォルトのエントリ列を削除します。
6. .csv ファイルを保存して閉じて、CA Enterprise Log Manager インターフェースに戻ります。
7. ここで更新するリスト(Default_Accounts リスト)に対して[値のインポート]をクリックします。
8. [参照]をクリックし、保存したファイルを選択し、[開く]をクリックします。
9. [OK]をクリックします。
ファイルがアップロードされます。[値]リストの末尾までスクロールすると、新しいエントリが追加されていることを確認できます。

動的値プロセスを使用したキー設定済みリストの更新

CA IT PAM プロセスを使用して CA Enterprise Log Manager クエリで使用されるキーに関連付けられた値のリストを生成する場合は、CA Enterprise Log Manager から IT PAM 動的値プロセスを実行して指定されたキーの値を更新します。インポートすると、指定されたキーのすべての値を手動で入力する時間を節約できます。1 つのキーの値が変更された場合、キーを選択して動的値のインポートを繰り返すことにより、CA Enterprise Log Manager でそれらのキーをリフレッシュできます。

CA IT PAM からキー設定済みリスト値をインポートする前に、動的な値のための CA IT PAM 統合を設定します。

CA IT PAM からキー設定済みリストの値をインポートする方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックして、[キー設定済みリスト]フォルダを展開します。
2. [キー設定済みリスト]フォルダを展開し、更新するキー設定済みリストを選択します。
3. インポートする値のキーを作成するには、次の手順を使用します。
 - a. [キー設定済みリストの値]テーブルの上部にある[追加]をクリックします。
[ユーザ]列で最初に利用可能な行が選択されています。
 - b. その行をクリックし、新しいキーの名前を入力します。
 - c. [保存]をクリックします。
4. 既存のキーの動的値をリフレッシュするには、次の手順を使用します。
 - a. キーを選択します。
 - b. 詳細ペインの上部にある[動的値リストのインポート]をクリックします。
[動的値リストのインポート]ダイアログ ボックスが表示されます。
 - c. 選択したキーの値を生成する IT PAM 動的値プロセスの名前を入力して、[OK]をクリックします。
関連する CA IT PAM プロセスが実行され、結果を含むファイルが返されます。また、選択したキーの値がリフレッシュされます。
 - d. [保存]をクリックします。

詳細情報:

[動的値のインポートの有効化](#) (P. 333)

[動的値プロセスについて](#) (P. 333)

[値リストを生成する CA IT PAM プロセスの作成](#) (P. 334)

[動的な値のための CA IT PAM 統合の設定](#) (P. 335)

クエリで使用するキー設定済みリストの確認

常にキー設定済みリストを現在の値で更新することをお勧めします。特定のレポートまたはアラートで使用するキー設定済みリストを更新するには、最初にレポートまたはアラートで使用するクエリを識別します。次に、ソースクエリまたはクエリで使用するキー設定済みリストを特定します。多くの場合、キー設定済みリストを使用するクエリは、クエリ名のキー設定済みリスト名を参照します。たとえば、クエリ名に「Default Accounts」または「Privileged Group」が含まれるクエリがあります。

クエリで使用するキー設定済みリストを確認する方法

1. クエリ設計ウィザードで、確認するキー設定済みリストを使用するクエリのコピーを開きます。
2. [クエリフィルタ]の手順をクリックし、次に[詳細フィルタ]タブをクリックします。
3. キー設定済みリストを使用するクエリには、[キー設定あり]という演算子を持つフィルタがあります。値は、キー設定済みリストの名前(Default_Accounts など)です。
4. [キャンセル]をクリックします。クエリのコピーは保存されません。

事前定義済みレポート用のキー設定済み値の作成

事前定義済みレポートで使用する一部の事前定義済みキーには、事前定義済み値がないものがあります。これらのレポートを効果的に使用するには、それぞれのキー設定済みリストに値を入力する必要があります。また、事前定義済み値があるキー設定済みリストにカスタム値を追加できます。

事前定義済み値がないキー設定済みリストの例は以下のとおりです。

- Critical_Assets
- DMZ_Hosts
- EPHI_Database
- Business_Critical_Sources

任意のキー設定済みリストに手動でまたはインポートで値を追加できます。

詳細情報:

[キー設定済みリストの手動更新](#) (P. 339)

[エクスポート/インポートによるキー設定済みリストの更新](#) (P. 340)

[例: CSV によるキー設定済みリストの更新](#) (P. 341)

Critical_Assets 用のキー設定済み値の作成

このトピックでは、事前定義済み値がないキー設定済みリストにカスタム値を追加する例を示します。この例の説明に従って、他の既存のキー設定済みリストに値を追加しています。

特定のレポートおよびクエリを使用して、ビジネス クリティカル ホスト別にアクティビティを監視できます。これを実行するには、まず、**Critical_Assets** 用キー値リストの値として、これらのホストを特定する必要があります。

Critical_Assets リストを使用するレポートには以下が含まれます。

- ビジネス クリティカル ホストごとのアカウント作成
- ビジネス クリティカル ホストへの失敗したログイン
- ビジネス クリティカル ホスト別リソース アクセス セッション
- ビジネス クリティカル ホストごとのリソース アクセス
- ビジネス クリティカル ホストごとのシステム アクセス

CA Access Control、CA Identity Manager、および CA SiteMinder の同様のレポートでは、**Critical_Assets** キー設定済みリストを使用します。たとえば、「CA Access Control - ビジネス クリティカル ホストごとのアカウント作成」のようなレポートです。

Critical_Assets リストを使用するクエリには以下が含まれます。

- 過去 1 日間のクリティカル システムでの、管理者アカウントによる 6 回以上の夜間ログイン
- 過去 1 週間のクリティカル システムでの、管理者アカウントによる 6 回以上の週末ログイン
- システム例外アクティビティ ...

クリティカル アセットに対するカスタム クエリを作成する場合は、以下のようにフィルタを定義します。

列	演算子	値
dest_hostname	キー設定済み	Critical_Assets

他のキー設定済みリスト用のフィルタを定義するには、値を必要なリスト値で置き換えます。たとえば、フィルタ値を `EPHI_Database` に設定して、そのキー設定済みリストに属するホスト名を識別できます。

Critical_Assets 用のキー設定済み値を作成する方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックして、[キー設定済みリスト]フォルダを展開します。
2. [キー設定済みリスト]フォルダを展開し、**Critical_Assets** を選択します。
3. 以下の操作のいずれかを実行して、このリストを作成します。
 - [値の追加]をクリックし、キー設定済みリストに含める新しい値を個々に入力します。
 - Excel スプレッドシートを作成し、行を 1 つだけ使用して、各列に値を 1 つずつ入力します。csv ファイルとして保存します。[値のインポート]をクリックし、編集済みリストをインポートします。
 - このキーの値が **CA IT PAM** 動的値プロセスによって動的に生成される場合は、[動的値リストのインポート]をクリックします。
4. [保存]をクリックします。

スケジュール済みジョブにより生成されたこのキー設定済みリストを使用するレポートは、以後、更新された値のデータを反映するようになります。

管理者用のキー設定済み値の作成

このトピックでは、複数の値がすでに設定されている事前定義のキー設定済みリストにカスタム値を追加する例を示します。この例の説明に従って、他の既存のキー設定済みリストに値を追加できます。

事前定義済みレポートとそれらに関連するクエリを使用して、管理者ごとにアクティビティを監視できます。事前定義済み値には、**Administrator**、**root**、**sa**、および **admin** があります。リストをカスタマイズするには、管理者用のキー値リストの値として、環境内で管理者権限を持つほかのアカウントを識別します。

このキーを使用するカスタム クエリを作成する場合は、次のようにフィルタを定義します。

列	演算子	値
dest_username	キー設定済み	管理者

他のキー設定済みリスト用のフィルタを定義するには、値を必要なリスト値で置き換えます。たとえば、フィルタ値を `EPHI_Database` に設定して、そのキー設定済みリストに属するホスト名を識別できます。

管理者用のキー設定済み値をカスタマイズする方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックして、[キー設定済みリスト]フォルダを展開します。

ユーザ定義値を追加するキーのリストが、メインのペイン下部に表示されます。

2. 「管理者」キーを選択します。

事前定義済み値が表示されます。

3. 以下の操作のいずれか(複数可)を実行して、このリストを更新します。

- 次の手順を使用して、リストを手動で更新します。
 - [値の追加]をクリックし、キー設定済みリストに含める新しい値を入力します。
 - 値を選択し、[値の削除]をクリックしてリストから値を削除します。
 - 値を選択し、[値の編集]をクリックして値を変更し、[OK]をクリックします。
- 次の手順を使用して、エクスポートおよびインポートによってリストを更新します。
 - a. [値のエクスポート]をクリックして、現在のリストをエクスポートします。
 - b. エクスポートしたリストを開き、リストを編集して値を変更してから、ファイルを保存します。
 - c. [値のインポート]をクリックし、編集済みリストをインポートします。
- [値のインポート]をクリックして、更新された `csv` ファイルの値をインポートします。
- このキーに対する値が、設定済みの **CA IT PAM** 動的値プロセスによって動的に生成される場合は、[動的値リストのインポート]をクリックします。

4. [保存]をクリックします。

スケジュール済みジョブにより生成されたこのキー設定済みリストを使用するレポートは、以後、更新された値のデータを反映するようになります。

キー設定済みリストを使用したレポートの表示

レポートの生成をスケジュールする前に、レポートの結果を表示できます。特定の事前定義済みのレポートでキー設定済みリストを使用します。このリストではキーは事前に定義されていますが、値はユーザ定義です。キーの値を追加またはインポートしたら、キー設定済みリストを使用してレポートを表示してみることをお勧めします。

キー設定済みリストを使用してレポートを表示する方法

1. [クエリおよびレポート]タブをクリックし、[レポート]サブタブをクリックします。
2. キー設定済みリストを使用するレポートを選択します。
3. 結果を表示します。

第 11 章: アクション アラート

このセクションには、以下のトピックが含まれています。

[アクション アラートについて](#) (P. 352)

[アクション アラートとしてタグが付いたクエリの使用](#) (P. 353)

[アラートで使用するその他のクエリの指定](#) (P. 355)

[アクション アラートのクエリのカスタマイズ](#) (P. 356)

[アクション アラートに関する注意事項](#) (P. 367)

[CA IT PAM イベント/アラート出力プロセスの使用](#) (P. 370)

[SNMPトラップの操作](#) (P. 408)

[アクション アラートを作成する方法](#) (P. 453)

[例: ディスク空き容量低下用のアクション アラートの作成](#) (P. 463)

[例: 自己監視イベント用のアラートの作成](#) (P. 467)

[例: イベントフローの停止時に管理者に電子メールを送信](#) (P. 470)

[アクション アラート保持の設定](#) (P. 473)

[例: Business Critical Sources 用のアラートの作成](#) (P. 474)

[アクション アラートの編集](#) (P. 477)

[アクション アラートの無効化または有効化](#) (P. 478)

[アクション アラートの削除](#) (P. 479)

アクション アラートについて

アクション アラートは、クエリ条件が満たされた場合にイベントを生成するよう特化したレポートです。さまざまな状況や事態を自動通知することができ、環境の監視に役立ちます。たとえば、イベントトレンド情報の提供、ディスク使用量の追跡、アクセスの失敗回数がしきい値を超えた際の通知などを、アクション アラートに設定できます。

アクション アラートは、ただちに行動する必要のあるいくつかのイベントのために収集された大量のデータを選別するのに適しています。アクション アラートを使用すると、ログ収集ネットワーク内で発生するほぼすべての要素について通知を受け取ることができます。アラートを作成して通知できる情報には、受信または送信トラフィックの急激な増加、特定のポートのトラフィック、ある特権リソースのアクセス、ファイアウォールやデータベース、キー サーバのようなさまざまなネットワーク エンティティへの設定変更などがあります。

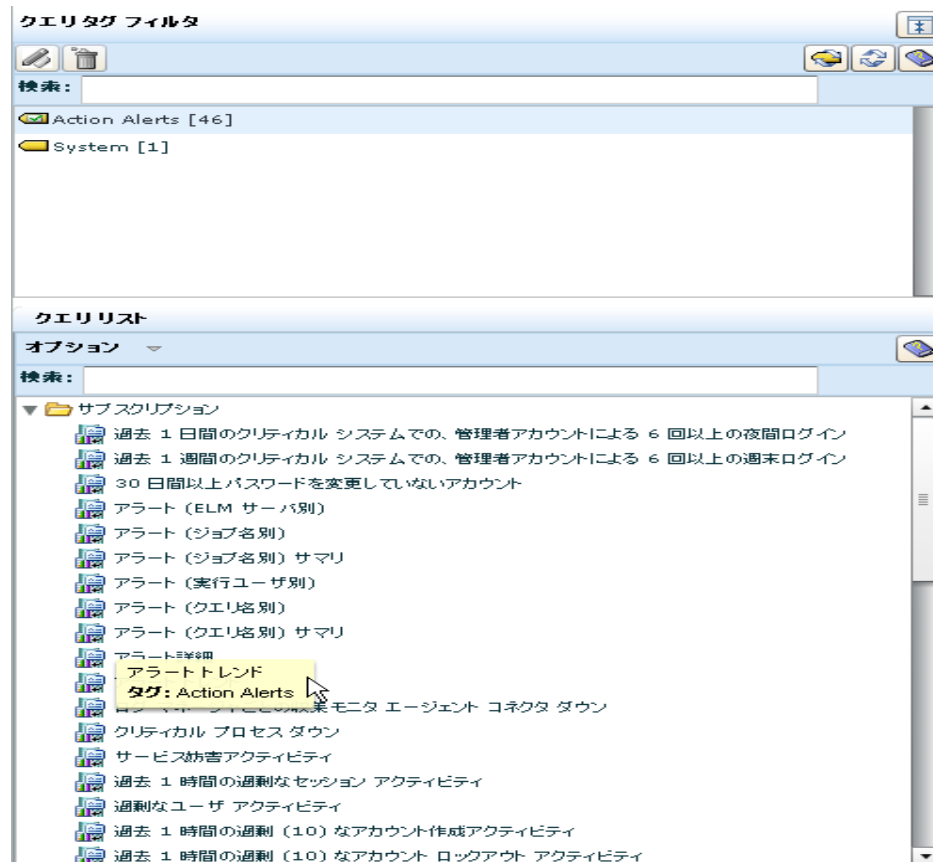
アクション アラートは、以下の方法で作成できます。

- アクション アラートウィザードを使用する
- クエリ表示から作成する
- ユーザが作成したクエリを使用する

スケジュール オプションは、アラート作成の重要な一部で、アラート ジョブを実行する期間と間隔を制御できます。

アクション アラートとしてタグが付いたクエリの使用

CA Enterprise Log Manager では、アクション アラートタグが付いた多数のクエリが提供されます。アクション アラートというタグが付いたクエリのリストを表示するには、[クエリおよびレポート]タブ-[クエリ]サブタブをクリックし、[アクション アラート]を選択します。このタグが付いたクエリが、[クエリ リスト]に表示されます。クエリ名の上にカーソルを移動すると、そのクエリのタグが表示されます。



このクエリからアクション アラートをスケジュールする前に、各クエリの実行内容について詳細な情報を入手できます。「使用可能なディスク領域の低下」などのクエリについての説明および詳細を表示するには、クエリリストからそのクエリを選択し、クエリ名の上にカーソルを移動します。

説明、クエリのフィルタ、クエリ条件などのクエリのサマリが表示されます。

ロフファイルがありません ▼ ログイン名

管理

自動リフレッシュ

使用可能なディスク領域が少なくなっています

元のイベントの表示 一致: GO

バージョン: 12.0.5002.0

Tags: Action Alerts

Query Last Refreshed at: Tue Sep 29 2009 2:25:58 pm

ディスク使用率

グローバル フィルタ

Last 6 hours

From: Tue Sep 29 2009 08:25:08 AM

To: Tue Sep 29 2009 02:25:08 PM

Local Filters:

AND event_trend GREATER 80

AND receiver_name EQUAL SystemStatus

AND dest_objectclass EQUAL Disk space

Query Conditions:

event_category: Operational Security

Result conditions:

最小数: 1 (グループ化されたイベント数)

ローカル タイムゾーン: America/New_York

Execution time: 514 秒

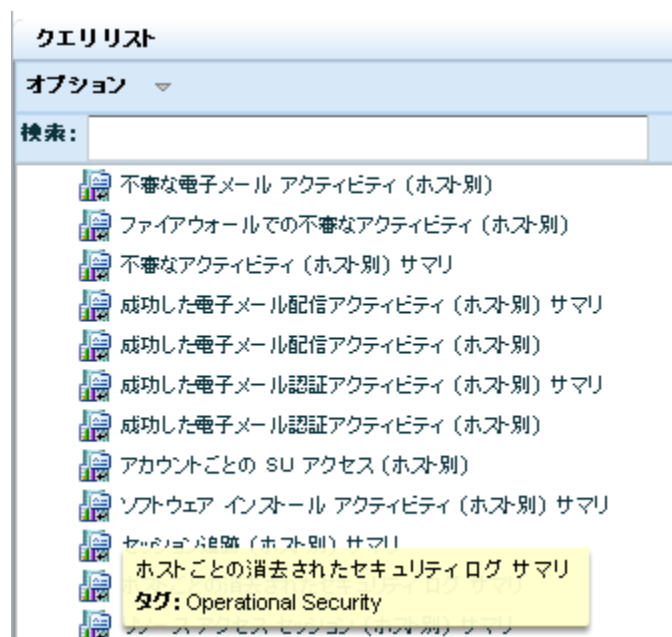
クエリを変更せずにスケジュールすることも、またはクエリをコピーして新しい名前を付け、要件に応じてカスタマイズすることもできます。たとえば、使用可能なディスク領域が **20%** ではなく **25%** 未満になった場合に、アラートを生成することができます。事前定義済みクエリを基にしてユーザ定義クエリを作成し、アクション アラートとして選択できます。

注: タイトルが「権限グループ」または「デフォルト アカウント」というクエリを使用する場合は、その前に、対応するキー設定済みリストに独自のキー設定済み値を追加することを検討してください。

アラートで使用するその他のクエリの指定

重大と評価されたイベントだけを取得するため、スケジュールされたアクションアラートに含める候補対象のアクション アラートとしてタグ付けされないクエリがあります。

たとえば、「ホストごとの消去されたセキュリティログ詳細」クエリは、イベントアクションが「セキュリティログ消去」であるすべてのイベントを取得します。このクエリのタグは「操作上のセキュリティ」だけです。



アクション「セキュリティログ消去」は CEG にリスト表示されます。CEG は、以下の 2 つのイベントタイプのセキュリティレベルを 6(重大)にマップして定義しています。

カテゴリ	クラス	アクション	結果	セキュリティレベル
操作上セキュリティ	セキュリティログ アクティビティ	セキュリティログ クリア	Success	6
操作上セキュリティ	セキュリティログ アクティビティ	セキュリティログ クリア	Failure	6

このクエリを使用するアラートをスケジュールすることをお勧めします。

詳細情報:

[重大なイベント用の単純フィルタの指定](#) (P. 357)

アクション アラートのクエリのカスタマイズ

アラートは、重大なイベントの発生時に、適切な担当者、プロセス、または製品に通知するように設計されます。アラートの基準となるクエリを指定する場合は、高いセキュリティレベルでイベントを取得するようにクエリを設計することを検討してください。

重大なイベントの定義を指定したら、重大なイベントを取得するクエリを指定できます。クエリが存在しない場合は作成できます。

以下のプロセスについて考えてみます。

1. CA が非常に重大と考えているイベントタイプ(カテゴリ、クラス、アクション、および結果別に定義されている)を指定します。
2. これらの重大なイベントだけを取得するように設計された事前定義済みクエリを指定します。
3. 重大なイベントを含むイベントを取得するように設計された事前定義済みクエリ(重大なイベントだけを取得するようにカスタマイズ可能)を指定します。
4. 事前定義済みクエリが存在しない場合は、カスタム クエリを作成します。
5. これらのクエリを頻繁に実行するアラートをスケジュールします。

詳細情報:

[重大なイベント用の単純フィルタの指定](#) (P. 357)

[重大なイベントだけを取得するためのクエリのカスタマイズ](#) (P. 361)

[重大なイベントだけを取得するクエリを作成](#) (P. 359)

重大なイベント用の単純フィルタの指定

イベントの重大度は、「通知」から「致命的」までさまざまです。CA では、イベントの重大度に、カテゴリ、クラス、アクション、および結果の CEG モデルに基づいて、2 ～ 7 の数値を割り当てています。重大度 7 はシステム シャットダウン イベントに割り当てられます。重大度 6 は、高いセキュリティを示す、緊急の注意が必要なイベントに割り当てられます。

カスタム クエリを作成する、またはアラートで使用する事前定義済みクエリをカスタマイズする予定がある場合は、重大なイベントタイプの CEG モデル定義を確認することをお勧めします。モデル定義は単純フィルタの基本です。つまり、イベント カテゴリ、イベント クラス、イベント アクション、およびイベントの結果に対して指定した内容に基づいたイベントを取得するクエリを作成できます。

単純フィルタ	
有効な単純フィルタを選択し、配置します	
☐ 理想モデル:	
☒ イベント カテゴリ:	
☒ イベント クラス:	
☒ イベント アクション:	
☐ イベント ログ名:	
☒ イベントの結果:	

重大なイベント用の単純フィルタを指定する方法

1. [ヘルプ]リンクをクリックします。
2. [共通イベント文法]を展開し、[セキュリティレベルの割り当て]を選択します。
3. スプレッドシートにテーブルをコピーし、[セキュリティレベル]の高い順に並べ替えます。

その結果、テーブルには **CA** のセキュリティレベルの割り当てに基づいて、最も重大度の高いものから順にイベントタイプが表示されます。

以下に例を示します。結果は現在の **CEG** 定義を反映します。

カテゴリ	クラス	アクション	結果	セキュリティレベル
操作上セキュリティ	システム アクティビティ	システム シャットダウン	Success	7
操作上セキュリティ	システム アクティビティ	システム シャットダウン	Failure	7
設定管理	設定管理	設定エラー	Success	6
データ アクセス	オブジェクト管理	制御ファイル作成	Success	6
ホスト セキュリティ	アンチウイルス アクティビティ	スキャン エラー	Success	6
ホスト セキュリティ	アンチウイルス アクティビティ	ウイルス駆除	Failure	6
ホスト セキュリティ	アンチウイルス アクティビティ	ウイルス検出	Success	6
ホスト セキュリティ	アンチウイルス アクティビティ	ウイルス検疫	Failure	6
ホスト セキュリティ	IDS/IPS アクティビティ	シグネチャ違反	Success	6
ネットワーク セキュリティ	シグネチャ違反アクティビティ	シグネチャ違反	Success	6
操作上セキュリティ	システム アクティビティ	システム起動	Failure	6
操作上セキュリティ	セキュリティログ アクティビティ	セキュリティログ クリア	Success	6
操作上セキュリティ	セキュリティログ アクティビティ	セキュリティログ クリア	Failure	6

カテゴリ	クラス	アクション	結果	セキュリティレベル
システム アクセス	認証アクティビティ	認証フォールバック	Failure	6
システム アクセス	認証アクティビティ	認証開始	Failure	6

重大なイベントだけを取得するクエリの作成

通知対象のタイプのイベントを取得する事前定義済みクエリがない場合は、新規にクエリを作成することもできます。以下の重大なイベントタイプについて考えてみます。

カテゴリ	クラス	アクション	結果	セキュリティレベル
ホスト セキュリティ	アンチウイルス アクティビティ	ウイルス検疫	Failure	6
ホスト セキュリティ	IDS/IPS アクティビティ	シグネチャ違反	Success	6
ネットワーク セキュリティ	シグネチャ違反アクティビティ	シグネチャ違反	Success	6

例: ウイルス検疫失敗だけを取得するクエリの作成

すべてのウイルス検疫失敗の通知を受け取る必要があるとします。キーワード「検疫」がクエリリストに表示される可能性は低いです。このような場合、必要なクエリを作成して、このクエリを実行するアラートをスケジュールすることができます。

ウイルス検疫失敗を取得するクエリの作成

1. [クエリおよびレポート]をクリックします。
2. [クエリリスト]の[オプション]の下で、[新規]を選択します。
クエリの実設計ウィザードが、[詳細]の手順が表示された状態で表示されます。
3. 名前を入力します。
たとえば、「アラート: ウイルス検疫失敗」と入力します。
4. カスタム タグを入力します。
たとえば、「ウイルス検疫」と入力します。
5. [クエリ列]の手順をクリックし、必要な列を追加します。
6. [クエリフィルタ]の手順をクリックします。
7. このイベントの CEG エントリに基づいて単純フィルタを入力します。
たとえば、[カテゴリ]に[ホスト セキュリティ]、[クラス]に[アンチウイルス アクティビティ]、[アクション]に[ウイルス検疫]、[結果]に[F]をそれぞれ選択します。

単純フィルタ	
有効な単純フィルタを選択し、配置します	
☐ 理想モデル:	
☒ イベント カテゴリ:	Host Security
☒ イベント クラス:	Antivirus Activity
☒ イベント アクション:	Virus Quarantine
☐ イベント ログ名:	
☒ イベントの結果:	

8. [結果の条件]の手順を選択し、[事前定義済み範囲]ドロップダウンリストから[過去 5 分間]を選択して、適時にアラート通知されるようにします。
9. [保存して閉じる]をクリックします。

重大なイベントだけを取得するためのクエリのカスタマイズ

アクション アラートとしてタグ付けされない事前定義済みクエリは、レポート用に設計されます。レポートには、すべての重大度レベルのイベントを反映するデータを含めることをお勧めします。一部のクエリを選択して、重大なイベントだけを取得するようにカスタマイズできます。その場合は、それほど重大ではないイベントと重大なイベントの両方を取得するクエリを指定して、コピーし、重大なイベントだけを取得するようにフィルタを入力して、アラートでの選択対象としてそのクエリを保存します。

事前に、重大なイベントの定義がリストされたスプレッドシートを手元に用意しておいてください。この例は、以下の CEG 情報を基にしています。

カテゴリ	クラス	アクション	結果	セキュリティレベル
操作上セキュリティ	システム アクティビティ	システム シャットダウン	Success	7
操作上セキュリティ	システム アクティビティ	システム シャットダウン	Failure	7

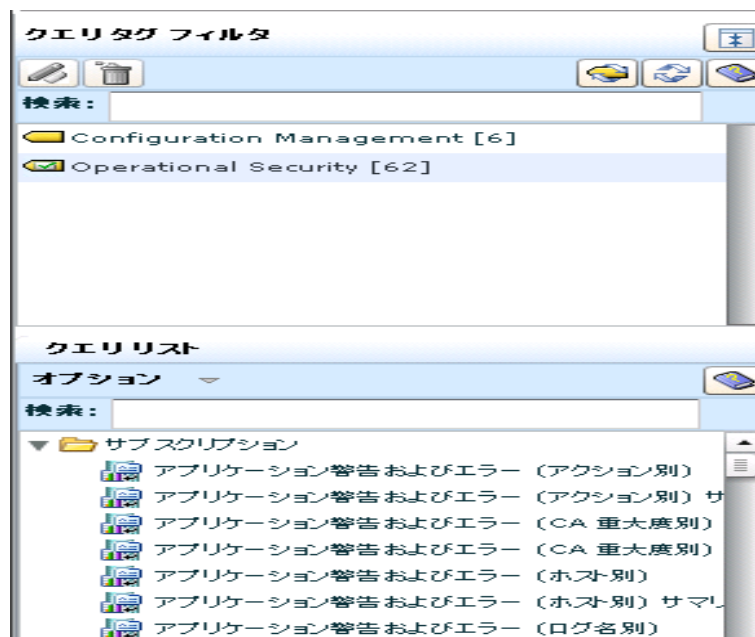
カスタマイズするクエリは、システム シャットダウンとシステム起動の両方のイベントを取得します。

重大なイベントだけを取得するようにクエリをカスタマイズする方法

1. [クエリおよびレポート] タブをクリックします。
2. 重大なイベントの[カテゴリ]と一致するクエリ タグ フィルタを選択します。
たとえば、[操作上のセキュリティ]を選択します。

- クエリリストを確認し、指定したイベントタイプの[クラス]または[アクション]にあるキーワードを含む名前を持ったクエリを探します。

たとえば、キーワード「システム シャットダウン」は、「ホストごとのシステム起動/シャットダウン」という語句で始まるクエリに含まれています。



- 「ホストごとのシステム起動/シャットダウン詳細」クエリをコピーします。クエリを強調表示し、[オプション]ドロップダウンリストから[コピー]を選択します。

- [クエリフィルタ]をクリックし、デフォルトと重大なイベント タイプのテーブル エントリを比較します。

このクエリについては、[操作上のセキュリティ]だけが選択されています。

- [クラス]と[アクション]に入力する値をテーブルから参照します。

たとえば、[クラス]には[システム アクティビティ]を、[アクション]には[システム シャットダウン]を選択します。

- [詳細フィルタ]タブを選択して、変更が必要かどうかを決定します。

それぞれ、`event_action` フィルタが「システム起動」と等しい、「シャットダウン」はこのカスタム クエリに関係がないという理由により、各行で[削除]をクリックします。

- このフィルタを結果のフィルタで置換します。

たとえば、`event_result` が成功か失敗のいずれかと等しいというフィルタを作成します。

ロジック	列	関数	演算子	値
	event_result		等しい	S
Or	event_result		等しい	F

9. [詳細]をクリックし、クエリに、アラートに使用することを示す名前を付けます。

たとえば、「アラート： ホストごとのシステム シャットダウン詳細」と入力します。必要に応じて説明を変更します。

10. [結果の条件]をクリックします。 重大な条件の場合は、頻繁にクエリを実行することを検討します。

たとえば、[事前定義済み範囲]で[過去 5 分間]を選択すると、この重大なイベントが発生したかどうかのクエリを 5 分ごとに実行します。

11. [保存]をクリックします。

このクエリを使用するアラートを作成すると、システム シャットダウンが成功したか、シャットダウンの試行に失敗したかが、担当者、製品、またはプロセスに通知されます（製品への通知は SNMP トラップによって行われ、プロセスへの通知は IT PAM イベント/アラート出力プロセスによって行われます）。

変更候補のクエリ

アラートで使用するために、選択した事前定義済みクエリを変更することを検討します。クエリをカスタマイズするには、CEG 分析に基づいた単純フィルタを追加します。[日付範囲の選択]を事前定義済み範囲である[過去 5 分間]に設定して、速やかに通知されるようにします。いくつかの例を以下に示します。

成功した設定エラー用のクエリ

1. 「設定エラー アクティビティ詳細」クエリをコピーします。

このクエリは失敗だけでなく成功も返します。成功だけが必要です。

2. 以下のように単純フィルタを設定します。

カテゴリ	クラス	アクション	結果	セキュリティレベル
設定管理	設定管理	設定エラー	Success	6

3. 「アラート： 成功した設定エラー」として保存します。

成功した制御ファイル作成用のクエリ

1. 「データ操作アクティビティ詳細」クエリをコピーします。
このクエリはデータ アクセス アクションをすべて取得します。
2. 以下のように単純フィルタを設定します。

カテゴリ	クラス	アクション	結果	セキュリティレベル
データ アクセス	オブジェクト管理	制御ファイル作成	Success	6

3. 「アラート: 成功した制御ファイル作成」として保存します。

アンチウイルス スキャン失敗用のクエリ

1. 「ウイルス アクティビティ(アクション別)」クエリをコピーします。
このクエリは、すべてのアンチウイルス ホスト セキュリティ アクションをフィルタします。
2. 以下の定義を参考にしてください。

カテゴリ	クラス	アクション	結果	セキュリティレベル
ホスト セキュリティ	アンチウイルス アクティビティ	スキャン エラー	Success	6

3. 以下のように単純フィルタを定義します。

ウイルス アクティビティ (アクション別) のコピー

単純フィルタ 詳細フィルタ

単純フィルタ

有効な単純フィルタを選択し、配置します

☒ 理想モデル: Antivirus

☒ イベント カテゴリ: Host Security

☒ イベント クラス: Antivirus Activity

☒ イベント アクション: Virus Scan

☒ イベント ログ名:

☒ イベントの結果: F

4. 「アラート: ウイルス スキャン失敗」として保存します。

ウイルス駆除失敗用のクエリ

事前定義済みの「ウイルス検出/駆除アクティビティ詳細」クエリを使用すると、結果が成功の場合と失敗の場合の両方のアクションを取得できます。これだけで十分な場合もありますが、必要に応じて、重大なイベント用の CEG テーブルに示された結果を指定するこのクエリに基づいて、2 つのクエリを別途作成できます。

1. 「ウイルス検出/駆除アクティビティ詳細」クエリをコピーします。
2. 失敗の結果を指定する単純フィルタを作成します。

カテゴリ	クラス	アクション	結果	セキュリティレベル
ホスト セキュリティ	アンチウイルス アクティビティ	ウイルス駆除	Failure	6

3. 詳細フィルタを削除します。
4. 「アラート: ウイルス駆除失敗」として保存します。

成功したウイルス検出用のクエリ

事前定義済みの「ウイルス検出/駆除アクティビティ詳細」クエリを使用すると、結果が成功の場合と失敗の場合の両方のアクションを取得できます。これだけで十分な場合もありますが、必要に応じて、重大なイベント用の CEG テーブルに示された結果を指定するこのクエリに基づいて、2 つのクエリを別途作成できます。

1. 「ウイルス検出/駆除アクティビティ詳細」クエリをコピーします。
2. ウイルス検出アクティビティ限定の成功の結果を指定する単純フィルタを作成します。

カテゴリ	クラス	アクション	結果	セキュリティレベル
ホスト セキュリティ	アンチウイルス アクティビティ	ウイルス検出	Success	6

3. 詳細フィルタを削除します。
4. 「アラート: ウイルス検出」として保存します。

アクション アラートに関する注意事項

特別な設定をしなくても CA Enterprise Log Manager から任意のアクション アラートの結果を表示することができます。さらに、アクション アラートを以下の宛先へ送信できます。

- RSS フィード
- 電子メール受信者
- SNMPトラップの宛先 (CA Spectrum や CA NSM など)
- CA IT PAM イベント/アラート出力プロセス

管理者は、[管理]タブの[サービス]サブタブをクリックし、[レポート サーバ]の[グローバル設定]または[グローバル サービス設定]のいずれかの下で、これらの宛先を設定します。

アラートをスケジュールする前に、必ずこれらの宛先を以下のように設定してください。

- フィードリーダーを使用するには、[グローバル設定]の[アクション アラートの参照には認証が必要]チェック ボックスがオフになっていることを確認します。

RSS フィード URL は以下のとおりです。*elmhostname* は CA Enterprise Log Manager サーバのホスト名です。

`https://{elmhostname}:5250/spin/cal/alm/getActionQueryRssFeeds.csp`

- 電子メール受信者にアラートを送信するには、[レポート サーバ]の[グローバル サービス設定]で[電子メール設定]セクションが設定されていることを確認します。
- (オプション) SNMP の宛先へアラートを送信するには、[レポート サーバ]の[グローバル サービス設定]で[SNMP 設定]セクションが設定されていることを確認します。
- CA IT PAM イベント/アラート出力プロセスにアラートを送信するには、[レポート サーバ]の[グローバル サービス設定]で[IT PAM]セクションが設定されていることを確認します (アラートに必要なでない値は動的値プロセス用の値のみです)。

アクション アラートの結果の条件を指定する際には、以下を考慮してください。

- 事前定義済み範囲の既定の動的開始時間および動的終了時間を使用する。
 - 事前定義済み範囲「過去 5 分間」は、動的終了時間が「今すぐ」「-2 分」に、動的開始時間が「今すぐ」「-7 分」に設定されています。このデフォルトの範囲およびほかの事前定義済み時間範囲を使用すると、イベントがデータベースに保存される適切な時間を有効にできます。

注: 動的終了時間を「今すぐ」や「今すぐ」「-1 分」に変更しないでください。事前定義済みの値をこのように変更すると、URL が宛先から起動されたときに、完了していないデータが表示されます。たとえば、値の 1 つがイベント数である場合、URL から表示されたときに表示される数が、CA Enterprise Log Manager から表示されたときに表示される数よりも小さくなる場合があります。

- 完了していないデータがデフォルト設定で表示される場合は、動的終了時間を拡張する。たとえば、「今すぐ」「-10 分」に設定します。

アクション アラートのスケジュールを作成する際には、以下を考慮してください。

- 反復間隔は、クエリが実行される間隔です。すなわち、反復間隔を 5 分に指定すると、クエリが 5 分ごとに、つまり 1 時間に 12 回実行されることになります。実行されたときにクエリが結果を返した場合にのみ、アクション アラートが生成されます。
- テストされた状況が発生した場合に、どの程度すばやく対処する必要があるかに応じて、反復間隔を設定します。
 - 状況改善策をすぐに講じる必要がある場合は、できるだけ迅速に通知されるよう、反復間隔を短く設定します。
 - 状況の追跡が必要でも、対応を必要としない場合は、反復間隔を長く設定します。
- CA Enterprise Log Manager サーバの時間が NTP サーバと同期されていない場合は、反復間隔を 5 分ごとなど短い間隔に設定しないでください。

重要: クエリが短い間隔で実行されるよう設定されている場合は、完全な結果が返されるように、CA Enterprise Log Manager サーバの時間を NTP サーバと同期する必要があります。

以下のフィルタ オプションについて検討します。

- 含まれるクエリで定義されたフィルタを使用する場合は、アクションは必要ありません。
- アラートに含まれるクエリにその他のフィルタを適用する場合は、[アラート フィルタ]の手順でフィルタを定義します。
- 複数のアラートジョブに同じフィルタのセットを適用する場合は、プロファイルを使用します。

CA Enterprise Log Manager レポート サーバのアクション アラート用にしきい値を設定する前に、以下を考慮してください。

- RSS フィードを適度なサイズに保つために、許可するアラートの最大数を設定します。有効なアラートの反復間隔が短いほど、1 つまたは複数のクエリによって結果が返されたときにフィードがすぐにいっぱいになります。
- データの必要な期間より長く RSS フィードがアラートを保持しないようにするために、アクション アラート保持の最も古いレコードを保持する最大日数を指定します。
- アラートの RSS フィードを確認する頻度を検討します。この頻度は、レコードを保存しておく期間を計画する際に役立ちます。
- 常にすべてのジョブの中で最新の結果が RSS フィードに表示されるようにする場合は、実行頻度の高いアラートでキューが満杯になり、より古くて実行頻度の低いアラートが削除されることがないような保持条件を設定します。

詳細情報:

[アクションアラート保持の設定 \(P. 473\)](#)

[例: ディスク空き容量低下用のアクションアラートの作成 \(P. 463\)](#)

CA IT PAM イベント/アラート出力プロセスの使用

CA Enterprise Log Manager に統合された CA IT PAM イベント/アラート出力プロセスを使用するには、以下のタスクをいくつか組み合わせて実行する必要があります。

- サンプルのイベント/アラート出力プロセスのインポート
- 統合要件を満たす CA IT PAM イベント/アラート出力プロセスの作成
- CA IT PAM 統合の設定およびデフォルトのイベント/アラート出力プロセスの指定
- 選択したクエリ結果からのイベント/アラート出力プロセスの実行
- CA IT PAM プロセスを行単位で実行するアラートのスケジュール
- CA IT PAM プロセスをクエリ単位で実行するアラートのスケジュール

詳細情報:

[サンプルのイベント/アラート出力プロセスのインポート \(P. 379\)](#)

[イベント/アラート出力プロセスを作成するためのガイドライン \(P. 387\)](#)

[例: 選択したクエリ結果を使用したイベント/アラート出力プロセスの実行 \(P. 394\)](#)

[例: 行ごとに IT PAM プロセスを実行するアラートの送信 \(P. 400\)](#)

[例: クエリごとに IT PAM プロセスを実行するアラートの送信 \(P. 405\)](#)

CA IT PAM イベント/アラート出力プロセスについて

CA Enterprise Log Manager では、対応が必要なイベントが検出されます。望ましくないイベントが発生するとすぐに、アラートを生成できます。CA IT PAM と統合することにより、イベント/アラート出力プロセスを実行するアラートを使用できます。イベント/アラート出力プロセスは、その他の製品による適切な対応を呼び出すよう設計されています。すなわち、イベント/アラート出力プロセスとは、指定されたオブジェクト上で指定されたアクションを実行するようその他の製品に命じる CA IT PAM プロセスです。

CA Enterprise Log Manager、CA IT PAM およびサードパーティ製品が連動して使用環境を保護します。CA Enterprise Log Manager では、望ましくないイベントの検出が自動化されます。また、IT PAM イベント/アラート出力プロセスは、適切な応答をするようにその他の製品を呼び出します。

統合には、CA IT PAM サーバへの接続の設定、実行するプロセスの指定、およびプロセスパラメータのデフォルト値での指定が必要です。

CA IT PAM プロセスは、表示されたクエリ結果 (行) からのオンデマンドでの実行、またはスケジュール済みアラートからの実行が可能です。どちらの場合も、サマリや説明などのパラメータ値を、CA IT PAM プロセスの宛先となる製品のサポートについての詳細を提供するためにカスタマイズできます。

詳細情報:

[CA IT PAM 統合をサポートするアーキテクチャ \(P. 372\)](#)

[イベント/アラート出力プロセスと連携するプロセス \(P. 372\)](#)

[CA IT PAM 統合のしくみ \(P. 374\)](#)

[例: イベント/アラート出力プロセスのデータフロー \(P. 377\)](#)

CA IT PAM 統合をサポートするアーキテクチャ

アラートから CA IT PAM のイベント/アラート出力プロセスを実行するには、次のネットワークコンポーネントが必要です。

- CA Enterprise Log Manager の作業環境。たとえば次のようなものが含まれます。
 - イベントソースからの元のイベントをキャプチャするコネクタを備えたエージェント
 - 元のイベントを絞り込み、それをレポートサーバに送信する CA Enterprise Log Manager 収集サーバ
 - スケジュールされたアラートやオンデマンドのクエリを処理する CA Enterprise Log Manager レポートサーバ
- 所定の改善策を実行するために別の製品を呼び出すプロセスが設定されている CA IT Process Automation Manager r2.1 (CA IT PAM) サーバ
- CA IT PAM プロセスによって使用される製品を備えたサーバ(たとえばヘルプ デスク製品を備えたサーバなど)

イベント/アラート出力プロセスと連携するプロセス

CA IT PAM のイベント/アラート出力プロセスを活用するためのワークフローの概要は、次のとおりです。

1. CA IT PAM 統合の設定でサンプルプロセスを使用するかどうかを決定します。サンプルプロセスを使用する場合の利点は、すぐに結果がわかるという点です。統合の結果をよく理解するまで、自分のプロセスの更新を保留できます。サンプルプロセスを使用するには CA サービス デスクが必要です。
2. 次のいずれか、または両方の手順を実行します。
 - サンプルプロセスをインポートし、CA サービス デスクの接続パラメータを指定します
 - CA Enterprise Log Manager 統合の要件を満たすイベント/アラート出力プロセスを作成します
3. サンプルプロセスまたは作成したプロセスから、CA IT PAM 統合の詳細を収集します。
4. イベント/アラート出力のために CA IT PAM 統合を設定します。

5. サードパーティ製品でイベント/アラート出力プロセスの結果をモニタするユーザが **CA Enterprise Log Manager** にユーザ アカウントを持っており、ログインに使用する認証情報を把握しておくようにします。このようなアカウントに監査者のロールを割り当てることができます。

注: ユーザがログインしたときにユーザが実行できるのは、関連するクエリ結果を含むページを表示することだけです。

6. イベント/アラート出力プロセスの実行を自動化する準備をします。
 - a. 設定済みの **CA IT PAM** プロセスに従ってサードパーティ製品がアクションを実行できるデータを返すクエリ(複数可)を識別します。
 - b. クエリがキー設定済みリストを使用する場合は、キー設定済みリストに必要な値が入力されていることを確認します。
 - c. クエリ結果に対してイベント/アラート出力プロセスを実行し、プロセスが正常に実行されたことを確認します。
7. 説明した手順と次のガイドラインを使用して、アクション アラートのスケジュールを設定します。
 - a. [アラートの選択]では、次の手順を実行します。
 - ジョブ名を入力します。
 - [選択タイプ]が[クエリ]であることを確認します。
 - 計画の作成中に識別したクエリ(複数可)を選択します。
 - b. [宛先]の手順で、[IT PAM プロセス]タブを選択し、イベント/アラート出力の詳細を次のように指定します。
 - そのアラートを基礎とするクエリを選択します。
 - 結果を返すクエリごとに 1 回プロセスを実行するのか、返される行ごとに 1 回プロセスを実行するのかを指定します。
 - IT PAM プロセスのパラメータ値を指定します。1 行ごとにプロセスを実行する場合にのみ、[サマリ]と[説明]のパラメータ値にフィールド値およびテキストを含めることができます。
 - c. スケジュールするほかのアクション アラートと同様に残りの手順の詳細を指定し、保存してウィザードを閉じます。

8. 次のように結果をモニタします。
 - a. [アクション アラート ジョブ]リストにこのジョブが含まれていることを確認します。
 - b. 自己監視イベントであるイベント通知アクションをモニタし、IT PAM プロセスの実行結果が成功であることを確認します。
 - c. (オプション) CA Enterprise Log Manager から IT PAM プロセスによって渡されたイベント/アラート出力情報に対応するサードパーティ製品にログオンします。

詳細情報:

[サンプルのイベント/アラート出力プロセスのインポート \(P. 379\)](#)

[イベント/アラート出力プロセスを作成するためのガイドライン \(P. 387\)](#)

[例: 選択したクエリ結果を使用したイベント/アラート出力プロセスの実行 \(P. 394\)](#)

[イベント/アラート出力プロセスに送信するイベントのクエリの設計 \(P. 398\)](#)

[通知の宛先の設定 \(P. 457\)](#)

[例: 行ごとに IT PAM プロセスを実行するアラートの送信 \(P. 400\)](#)

CA IT PAM 統合のしくみ

次のようにセットアップされていることを前提とします。

- レポート サーバの設定ページで CA IT PAM が設定されており、実行するイベント/アラート出力プロセスが指定されている。
- 宛先として CA IT PAM を使用するアラートがスケジュールされており、1 行ごとにプロセスを 1 回実行するように指定されている。サマリと説明のステートメントのエントリを許可するパラメータには、CEG フィールドを含むステートメントが入力されている。
- 宛先として CA IT PAM を使用する別のアラートがスケジュールされており、クエリごとにプロセスを 1 回実行するように指定されている。サマリと説明のステートメントのエントリを許可するパラメータには、文字テキストが入力されている。

エンド ツー エンド プロセスには、次のような複数のソースによるアクションが含まれます。

- イベントソースによる元のイベントの生成
- CA Enterprise Log Manager によるイベントの収集、および精製
- 精製済みイベントがクエリ条件を満たす場合の CA Enterprise Log Manager によるアラートの生成
- CA Enterprise Log Manager による CA IT PAM へのイベントおよびアラート出力の送信
- サードパーティシステムでの CA IT PAM による設定済みのイベント/アラート出力プロセスの実行
- 以下のいずれか 1 つ:
 - 適切なアクションを判断し、そのアクションを実行するサードパーティシステムのユーザによるデータの評価
 - サードパーティシステムによるイベントの発生に対する自動応答。

プロセスの概要を次に示します。

1. イベントソースによって、元のイベントが生成されます。
2. エージェントは、コネクタに基づいて元のイベントの一部を収集し、元のイベントを収集サーバに転送します。
3. 収集サーバは元のイベントを正規化して分類し、精製済みイベントをレポートサーバに転送します。

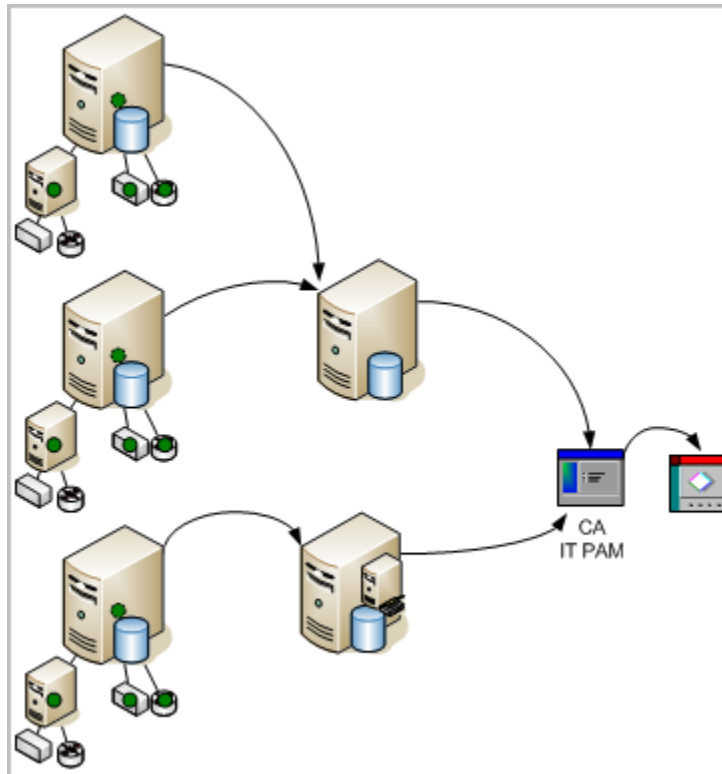
たとえば、任意のシステムで設定が変更されると、ログが作成され、設定変更として分類されます。イベントでは、変更時刻、変更されたホスト、変更を実行したユーザ、および変更の結果がキャプチャされます。
4. レポートサーバは、スケジュール済みの各アラート用に選択されたクエリを実行します。

5. 精製済みイベントがクエリ条件を満たす場合、レポートサーバはアラートを生成し、CA IT PAM に次の情報を転送します。
 - アラート詳細
 - 表示されるプロセス パラメータとその値
 - 非表示のプロセス パラメータに送信される CEG フィールド
 - イベントの詳細
 - サマリおよび説明のステートメントで使用可能なフィールドのエントリによって、行ごとにイベントの詳細が送信されます。このステートメントでは、アラート用に選択されたクエリを構成する CEG フィールド変数を使用して、イベントを記述します。
 - イベントの詳細を行レベルで表示する CA Enterprise Log Manager ページへの URL を使用して、クエリごとにイベントの詳細が送信されます。
6. 送信が成功すると、CA IT PAM は設定済みのイベント/アラート出力プロセスに定義されたとおりに引き続き処理を行います。
7. サードパーティ製品が CA サービス デスクであり、プロセスがサンプルのイベント/アラート出力プロセスである場合は、次のような状況が発生します。
 - ヘルプ デスクのチケットがオープンされ、番号が割り当てられます。アラートの定義からのパラメータ値を使用して、チケットのフィールドに入力されます。URL を受信した場合は、サマリステートメントと一緒に表示されます。
 - CA サービス デスクは CA IT PAM にチケット番号を返します。
8. CA IT PAM は CA Enterprise Log Manager にチケット番号を渡します。
9. CA Enterprise Log Manager は自己監視イベントとしてチケット番号を表示します。

例：イベント/アラート出力プロセスのデータフロー

次の図の矢印は、以下のデータフローを示しています。

- 収集サーバからレポートサーバへ
- レポートサーバから CA IT PAM へ
- CA IT PAM から CA IT PAM プロセスが CA Enterprise Log Manager の出力を送信する製品 (CA サービス デスクなど)

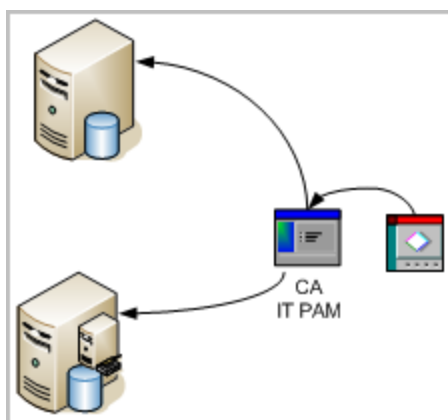


CA Enterprise Log Manager は、送信が成功したという通知を受け取ると、CA IT PAM に実行されたプロセスのステータスをポーリングします。CA IT PAM がステータス更新を送るとすぐに、CA Enterprise Log Manager はその結果に関する自己監視イベントを作成します。処理のシーケンスは次のとおりです。

1. CA IT PAM は、実行されたプロセスが成功したのか、あるいは失敗したのかを CA Enterprise Log Manager に通知します。
2. CA Enterprise Log Manager は、受信した結果を使用して通知作成の自己監視イベントを生成します。

CA IT PAM プロセスが、プロセスのパラメータ値とクエリによって取得されたイベントデータを使用して、ヘルプデスク チケットを作成する場合の例を考えてみます。次の図の矢印は、以下のデータフローを示しています。

- ヘルプ デスク製品から CA IT PAM へ
- CA IT PAM からソースの CA Enterprise Log Manager レポート サーバへ



サンプルのイベント/アラート出力プロセスのインポート

CA IT PAM 統合をすぐにテストし、既知の値を使用して設定手順を練習できるようにするためのサンプル プロセスが用意されています。このサンプルはアプリケーションと一緒に DVD にあります。このサンプルの IT PAM プロセスを使用する場合は、ヘルプ デスク アプリケーションとして CA サービス デスクを使用していることを前提とします。

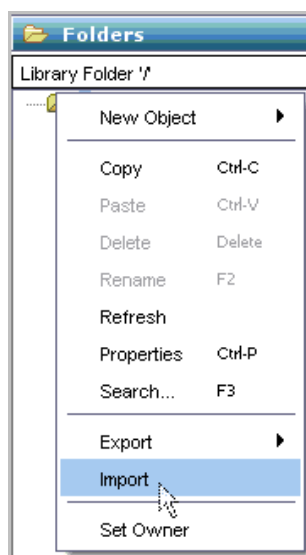
そして、CA Enterprise Log Manager で CA IT PAM を設定し、選択したクエリ結果を使用して、サンプルの CA IT PAM プロセスを実行するテストを設定できます。CA Enterprise Log Manager が CA IT PAM と連携するしくみについてよく理解したら、独自のプロセスのコンプライアンスを確認し、その値を実稼働環境で統合する CA IT PAM の設定に置き換えることができます。

サンプル プロセスをインポートして IT PAM 統合をテストする方法

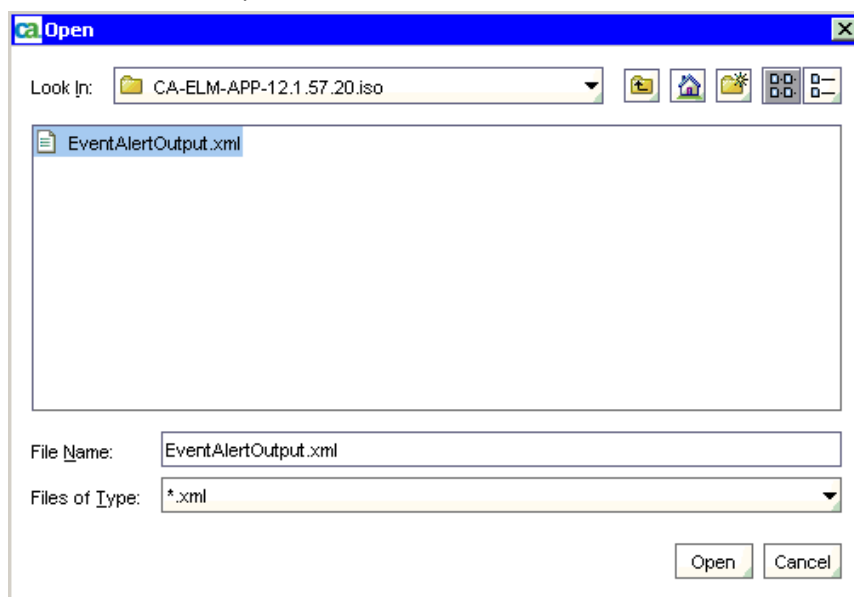
1. CA IT PAM を起動して、ログオンします。
2. IT PAM クライアントを起動します。



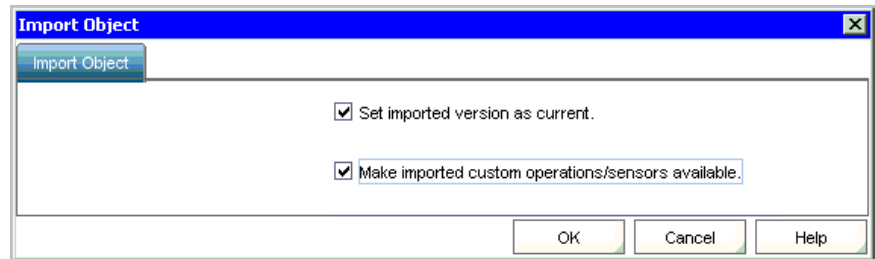
3. CA/IT PAM のアプリケーション DVD にあるサンプルの IT PAM プロセス (EventAlertOutput.xml) をインポートします。このサンプルでは必要な値がすべて定義されています。
 - a. [ファイル]、[ライブラリ ブラウザを開く]を選択します。
 - b. 左ペインの[フォルダ]をクリックし、ルートフォルダで[インポート]をクリックします。



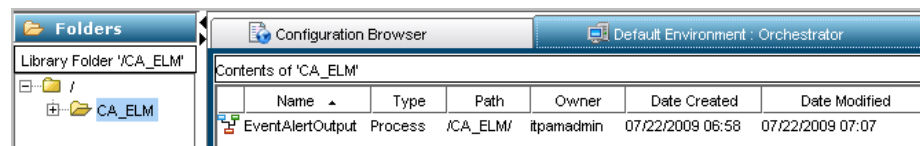
- c. 抽出された ISO イメージからサンプルの IT PAM プロセス (EventAlertOutput.xml) を選択し、[開く]をクリックします。



- d. [オブジェクトのインポート]ダイアログ ボックスの両方のオプションを選択し、[OK]をクリックします。



結果として表示された内容には、正確な名前とパスが表示されます。たとえば、名前は **EventAlertOutput** で、パスは **/CA_ELM/** となります。



4. サービス デスクの接続パラメータを指定します。
 - a. [ServiceDesk 接続パラメータ]タブをクリックして、Request_Create の ServiceDesk の接続パラメータを表示します。
 - b. 次の構文を使用して、サービス デスクの URL を指定します。
 "http://<server name>:8080/axis/services/USD_R11_WebService"
 - c. [サービス デスクのユーザ ID とパスワード]に対して、サービス デスクの有効なログイン認証情報を入力します。
5. (オプション) インポートしたプロセスをテストし、そのプロセスがスタンドアロンプロセスとして動作することを確認します。
6. IT PAM クライアントを閉じて[サイン アウト]をクリックし、CA IT PAM を終了します。

サンプルのイベント/アラート出力プロセスの表示

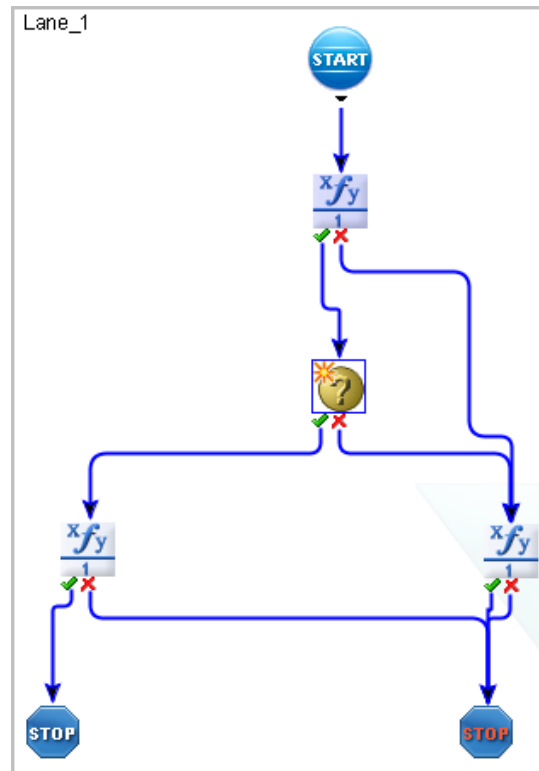
サンプルのイベント/アラート出力プロセスをインポートすると、CA IT PAM でその設計を検討できます。以下のガイドラインを使用すると、サンプルプロセスのコンテキストでの **CA Enterprise Log Manager** 要件を理解できます。この手順では、**Web** サービスの接続パラメータを接続する場所、および計算演算子を定義する方法がわかります。さらに、製品固有の要件も確認できます。たとえば、サードパーティ製品として **CA Service Desk** を設定する場合には、**CA Service Desk** モジュールの **Request_Create** 演算子、および重大度と優先度の値を管理する事前計算演算子を使用する必要があります。

サンプルのイベント/アラート出力プロセスを理解するためのガイドライン

1. ターゲットプロセスのモデルを表示します。
 - a. CA IT PAM を起動してログインします。
 - b. [ITPAM クライアント]をクリックします。
 - c. [ファイル]メニューから、[ライブラリ ブラウザを開く]を選択します。
 - d. [フォルダ]タブから、ターゲットプロセスのモデルが格納されたライブラリフォルダを選択します。

プロセスの名前とパスがメイン ペインに表示されます。
 - e. プロセスの名前とパスを含む行をダブルクリックします。

以下のようなモデルが表示されます。このモデル例は、CA Enterprise Log Manager の最小要件を満たしています。



2. ServiceDesk の[基本パラメータ]がどのように CA Enterprise Log Manager 要件を満たしているかに注目してください。

- a. [Request_Create_1]アイコンをダブルクリックします。



Request_Create 演算子は、アクションアラートクエリによって返されたデータをターゲット製品 (アプリケーション) に渡します。同様の演算子は、CA Enterprise Log Manager から実行するあらゆるプロセスに必要です。

- b. ServiceDesk の[基本パラメータ]で、ローカル プロセスのパラメータが以下の構文を使用して指定されていることに注目してください。

BasicParameter=Process.LocalParameter

注: ローカル プロセスのパラメータとは、CA IT PAM を設定する際に CA Enterprise Log Manager に追加するイベント/アラート出力プロセス パラメータです。

- c. ターゲット アプリケーションは CA Service Desk 製品なので、以下のローカル プロセスのパラメータが、下の表のように定義されます。

ServiceDesk の基本パラメータ	ローカル パラメータ	Service Desk のフィールド	Notes
要求作成者 ID	Process.ReportedBy	担当者、レポート作成者	CA Service Desk 内の有効な「連絡先」
まとめ	Process.Summary	まとめ	(空白のまま)
説明	Process.Description	説明	(空白のまま)
カスタマ ID	Process.EndUser	影響を受けるエンドユーザ	CA Service Desk 内の有効な「連絡先」
優先度	Process.Priority	優先度	1 ～ 5
重大度	Process.Severity	重大度	1 ～ 5

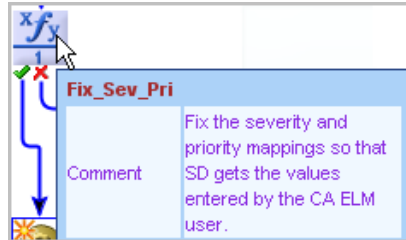
以下の例は、ServiceDesk 基本パラメータに対する有効なローカル パラメータを示しています。エントリでは、大文字と小文字が区別されます。つまり、Process.ReportedBy の「R」と「B」を大文字にするなど、表示されたとおりに入力する必要があります。

The screenshot shows a window titled 'Properties of Request_Create_1'. Inside, there is a tab labeled 'ServiceDesk Basic Parameters'. The tab contains the following fields:

- *Request Creator ID:
- *Summary:
- *Description:
- *Customer ID:
- *Request Type: (dropdown arrow)
- *Priority: (dropdown arrow)
- *Severity: (dropdown arrow)
- *Impact: (dropdown arrow)
- *Urgency: (dropdown arrow)

3. [ServiceDesk 接続パラメータ]タブをクリックして、Request_Create の ServiceDesk の接続パラメータを表示します。
 - Service Desk URL: 「http://<サーバ名>:8080/axis/services/USD_R11_WebService」
 - Service Desk ユーザ ID: 「<SD ユーザ>」
 - パスワード: 「<SD パスワード>」

4. CA Service Desk については、CA Enterprise Log Manager に入力される重大度および優先度の値が CA Service Desk によって正しく解釈されるように調整が必要なことに注目してください。
 - a. 計算前演算子が、Start 演算子の後で Create_Process 演算子の前に表示されます。以下の例では、Fix_Sev_Pri という名前の演算子です。



- b. [プロパティ]の[計算]では、以下のマッピングが定義されます。


```
if (Process.Priority == 1) Process.Priority = "pri:504";
else if (Process.Priority == 2) Process.Priority = "pri:503";
else if (Process.Priority == 3) Process.Priority = "pri:502";
else if (Process.Priority == 4) Process.Priority = "pri:501";
else if (Process.Priority == 5) Process.Priority = "pri:500";

if (Process.Severity == 1) Process.Severity = "sev:800";
else if (Process.Severity == 2) Process.Severity = "sev:801";
else if (Process.Severity == 3) Process.Severity = "sev:802";
else if (Process.Severity == 4) Process.Severity = "sev:803";
else if (Process.Severity == 5) Process.Severity = "sev:804";
```
5. 以下の戻り値または出力インターフェースのパラメータは、CA Enterprise Log Manager で必要な形式にフォーマットされます。
 - ResultString
 - FaultString
6. 要求作成が成功した場合の計算演算子を表示します。この形式は CA Enterprise Log Manager から実行するすべてのイベント/アラート出力プロセスで使用する必要があります。
 - a. 要求作成が成功した場合の計算演算子のアイコンをクリックします。
 - b. [計算]タブを選択して、ソースコードフィールドの[...]をクリックします。
 - c. 成功計算演算子がソースコードでどのように定義されているかに注目してください。

```
Process.ResultString = "Request " + Request_Create_1.newRequestNumber + "
created in CA Service Desk.";
```

7. 失敗した場合の計算演算子を表示します。この形式は CA Enterprise Log Manager から実行するすべてのイベント/アラート出力プロセスで必要です。
 - a. 失敗した場合の計算演算子のアイコンをクリックします。
 - b. [計算]タブを選択して、ソースコードフィールドの[...]をクリックします。
 - c. 失敗計算演算子がソースコードでどのように定義されているかに注目してください。Process.FaultString が適切な SOAP 変数にマッピングされていることがわかります。

```
Process.FaultString = Request_Create_1.SoapErrorResponse;
```

イベント/アラート出力プロセスを作成するためのガイドライン

CA IT PAM プロセスを CA Enterprise Log Manager から実行するには、所定のガイドラインを満たす必要があります。CA IT PAM プロセスを CA Enterprise Log Manager から実行する前に、プロセスに以下が含まれていることを確認してください。

- Web サービスの接続パラメータ
- サードパーティ製品からのレスポンスを表現するリテラルと変数を備えたステートメントに Process: ResultString をマップする成功計算演算子
- 適切な SOAP レスポンス変数に Process: FaultString をマップする失敗計算演算子

ターゲットの IT PAM プロセスがサードパーティ製のヘルプ デスク製品用である場合は、上記に加えて、プロセスに以下も含まれていることを確認してください。

- 製品固有のオペレータ
たとえば、BMC Remedy モジュールをターゲットにするプロセスは Create_Help_Desk_Case 演算子と一緒に定義します。
- ローカル プロセス パラメータの ReportedBy、Summary、Description、EndUser、Priority および Severity にマップされた製品固有のパラメータ
たとえば、BMC Remedy モジュールをターゲットにするプロセスは、HelpDesk Create Case パラメータに対してローカル パラメータをマップします。

通常、CA IT PAM プロセスには、デフォルトのプロセスパラメータのみが含まれ、それぞれサードパーティ製品のフィールドにマップされています。オプションで、**CEG** フィールドを指定されたプロセスのプロセスパラメータとして追加できます。以下の例は、データセットに含まれている次の **CEG** フィールドを示したものです。

- event_severity
- event_count
- event_datetime

ReportedBy	
Severity	
Summary	
Description	
Priority	
ResultString	
FaultString	
EndUser	
event_severity	
event_count	
event_datetime	

Main Editor | Exception Handler | Lane Change Handler | **Dataset**

各基本パラメータは、Service Desk フィールドにマップされています。たとえば、ReportedBy プロセス パラメータは、Assignee という CA Service Desk フィールドにマップされています。CEG フィールドをプロセス パラメータとして追加すると、基本パラメータの値として参照することができます。たとえば、CEG フィールド event_datetime の値を、CA Service Desk の Description フィールドにデフォルトで表示されるように定義できます。Service Desk の基本パラメータの Description フィールドに Process.event_datetime を追加すれば、この定義を実現できます。

Properties of 'Request_Create_1'

ServiceDesk Basic Parameters

*Request Creator ID:
Process.ReportedBy

*Summary:
Process.Summary

*Description:
Process.Description + " Time of event = " + Process.event_datetime

このプロセスを実行するアラートを作成する際、[フィールド値をパラメータとして送信]リストに表示される CEG フィールドを確認してください。リスト表示されたパラメータの中に、プロセス パラメータとして定義した CEG フィールドがあれば、そのフィールドを選択します。以下の例について考えます。

- データセットに定義された 3 つすべての CEG フィールドが、[システム イベント数 (イベントアクション別)]というクエリ用に表示されます。そのため、3 つすべてを選択し、パラメータとして CA IT PAM に送信します。

システム イベント数 (イベント アクション別)

☒ IT PAM プロセスを行単位で実行

● IT PAM プロセス: /CA_ELM/EventAlertOutput

フィールドの選択: event_action

ReportedBy: +

Severity: +

Priority: +

EndUser: +

Summary: +

Description: +

フィールド値をパラメータとして送信:

選択	使用可能なフィールド
☐	event_action
☐	event_count
☐	event_datetime

- データセットに定義された 3 つの CEG フィールドのうちの 2 つは、Admin アカウントによるログインが 5 人より多いクエリの場合に表示されます。この 2 つのフィールドを選択して、CA IT PAM にパラメータとして送信します。

過去 1 日間のクリティカル システムでの、管理者アカウントによる 6 回以上の夜間ログイン

☒ IT PAM プロセスを行単位で実行

IT PAM プロセス: /CA_ELM/EventAlertOutput

フィールドの選択: dest_hostname

ReportedBy: ServiceDesk

Severity: 4

Priority: 4

EndUser: ServiceDesk

Summary:

Description:

フィールド値をパラメータとして送信:

選択	使用可能なフィールド
☐	dest_hostname
☐	dest_username
☒	event_action
☒	event_datetime
☐	event_logname
☐	event_result

詳細情報:

[サンプルのイベント/アラート出力プロセスの表示 \(P. 382\)](#)

CA IT PAM 統合の詳細の収集

CA IT PAM 統合に必要な詳細の多くは、CA IT PAM 製品およびプロセス設定の一部です。CA IT PAM を起動して、設定に必要な詳細を検索したり、最初に詳細を収集して記録し、記録した値を入力することによって簡単に設定することができます。

インポートしたサンプル プロセス、または CA Enterprise Log Manager の要件を満たすように変更した独自のプロセスのいずれかを参照できます。

CA IT PAM 統合の詳細を収集する方法

1. ローカルの CA IT PAM サーバにログオンし、それが CA IT Process Automation Manager 2.1 であることを確認します。
2. [ITPAM クライアント]リンクをクリックします。

3. IT PAM 設定の最初の 4 つのフィールド用の詳細を収集します。
 - a. [設定]ブラウザをクリックします。
 - b. [プロパティ]タブをクリックします。
 - c. IT PAM サーバに入力する値として、[サーバ名]の値を記録します。
 - d. [IT PAM ポート]としてポート 8080 を受け入れます。
 - e. CA IT PAM 管理者から CA Enterprise Log Manager のログイン認証情報を取得し、[ユーザ名]と[パスワード]用にそれらを記録します。

IT PAM の[設定]フィールド	説明	使用する値
IT PAM サーバ	CA IT PAM がインストールされているサーバの完全修飾ホスト名。 この値は、[設定]ブラウザの[プロパティ]タブの[サーバ名]フィールドに表示されます。	
IT PAM ポート	デフォルトはポート 8080 です。 この値は、[設定]ブラウザの[プロパティ]タブの[ドメイン URL]フィールドに表示されます。	8080
ユーザ名	IT PAM にログインしてプロセスを実行するために CA Enterprise Log Manager が使用するユーザ ID。 CA IT PAM 管理者から取得します。 例: itpamadmin	
パスワード	ユーザ名に関連付けられているパスワード。 CA IT PAM 管理者から取得します。	

4. CA Enterprise Log Manager から実行する予定のプロセスのプロセス パスと名前を記録します。
 - a. ITPAM クライアントの[ファイル]メニューから、[ライブラリ ブラウザを開く]を選択します。
 - b. [フォルダ]タブで、イベント/アラート出力プロセスを含むライブラリ フォルダを選択します。
 - c. イベント/アラート出力プロセスのプロセス パスと名前を記録します。
 - d. それ以外のプロセスの場合は、指定されたキーの現在の値を返すプロセスを含むライブラリ フォルダを選択します。
 - e. 動的値プロセスのパスと名前を記録します。

IT PAM プロセス固有のフィールド	説明と例	使用する値
イベント/アラート出力プロセス	パスおよびプロセス名。 アラートまたは CA サービス デスクなどの外部製品への URL を使用して設定された詳細を渡すために作成されたプロセスを識別します。 例: /CA_ELM/EventAlertOutput	
動的値プロセス	パスおよびプロセス名。 入力キーの値を収集し、解析用に csv ファイルにその値を返すために作成されたプロセスを識別します。 例: /CA_ELM/ValuesList	

- 5. イベント/アラート出力プロセスのパラメータを収集します。
 - a. 参照したイベント/アラート出力プロセスをダブルクリックして、そのプロセスを開きます。
 - b. [メイン エディタ] タブで **Request_Create** アイコンをクリックし、プロパティを表示します。
 - c. サービス デスクの[基本パラメータ]を表示します。
 - d. プロセスによってプレフィクスが付けられたパラメータを記録します: パラメータが表示された内容と正確に一致しない場合は、最初の列の下になります。
 - e. [データセット] タブをクリックします。
 - f. **Local_Dataset** の各パラメータをクリックし、デフォルト値がある場合はその値を記録します。

イベント/アラート出力プロセス パラメータ	説明と例	使用する値
ReportedBy	有効な ServiceDesk ユーザ名です。	
Summary	このテキストは、Service Desk リクエストのサマ リフィールドに表示されます。たとえば「CA ELM から作成されたリクエスト」などです。	---
Description	このテキストは、Service Desk リクエストの説明 フィールドに表示されます。	---
EndUser	有効な ServiceDesk ユーザ名です。	
Priority	デフォルトの優先度を設定します。デフォル トが設定されていない場合は、1 ～ 5 の値を 記録します。 例: 3	
Severity	デフォルトの重大度を設定します。デフォル トが設定されていない場合は、1 ～ 5 の値を 記録します。 例: 4	

例：選択したクエリ結果を使用したイベント/アラート出力プロセスの実行

すべてのユーザは、CA IT PAM プロセスをオンデマンドで実行できます。次のいずれかの目的のために、選択したクエリ結果を使用して、設定済みの CA IT PAM イベント/アラート出力プロセスを実行できます。

- 現在のニーズに基づいて、オンデマンドでイベント/アラート出力プロセスを実行する。
- 宛先として CA IT PAM プロセスを使用してこのクエリ用のスケジュール済みアラートを作成する前に、処理結果をテストする。

表示されたクエリ結果の行から CA IT PAM プロセスを実行できます。ここでは、結果がグラフではなく表として表示されることを前提としています。次のいずれかの方法でクエリ結果の行を表示できます。

- 結果を返すクエリリストからクエリを選択します。
- レポートリストからレポートを選択し、結果を返すクエリを選択します。
- プロンプトを起動して結果を返します。

注：次のトピックでは、クエリリストからクエリを選択したときにクエリ結果の行が表示されることを前提としています。

CEG フィールドに返されるデータを詳しく理解するには、オンライン ヘルプで「共通イベント文法 (CEG) リファレンス ガイド」を参照してください。

表示されたクエリ結果の行に基づいて設定済みの CA IT PAM プロセスを実行する方法

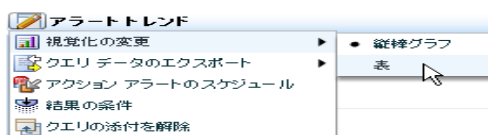
1. [クエリおよびレポート] タブをクリックし、[クエリ] サブタブをクリックします。
[クエリ タグ フィルタ] と [クエリ リスト] が表示されます。
2. (オプション) [クエリ リストで]、デフォルト アカウントなどの検索条件を入力します。

デフォルト アカウントによるログインを反映したイベントは、CA IT PAM イベント/アラート出力プロセスに転送するのに適した候補です。

- 結果を表示するクエリリストからクエリを選択します。

または、[レポート]サブタブを表示し、[レポートリスト]からオプションを選択し、個別のクエリビューに切り替え、そのビューからクエリを選択します。

- 結果がグラフで表示される場合は、クエリ名のドロップダウンリストから[視覚化の変更]を選択し、[表]を選択します。



- CA IT PAM プロセスを実行するクエリ結果の行を選択します。
- このクエリ結果の行を右クリックし、ドロップダウンリストから[IT PAM プロセスの実行]を選択します。

アラート詳細

☐ 元のイベントの表示 一致: **実行**

CA 重大度	日付	クエリ名	ジョブ名
情報	2009-11-20 金曜日 午前 11:34:23	CPU Utilization Trend	Default Account Logins
情報	2009-11-20 金曜日 午前 11:13:18	Cont	stined for CA NSM
情報	2009-11-20 金曜日 午前 11:08:16	Cont	stined for CA NSM
情報	2009-11-20 金曜日 午前 10:43:16	Cont	stined for CA NSM
情報	2009-11-20 金曜日 午前 10:38:16	Cont	stined for CA NSM
情報	2009-11-20 金曜日 午前 10:08:16	Cont	stined for CA NSM
情報	2009-11-20 金曜日 午前 10:03:16	Cont	stined for CA NSM
情報	2009-11-20 金曜日 午前 9:58:16	Cont	stined for CA NSM

Right-click context menu options:

- 詳細イベントの表示
- グローバル フィルタへの追加
- このセルからのカスケード クエリ (インクルード)
- このセルからのカスケード クエリ (エクスクルード)
- イベントのコピー
- すべてのイベントのコピー
- IT PAM プロセスの実行**
- 集約ルールを作成
- 抑制ルールを作成
- 設定...
- Adobe Flash Player 10 について

[IT PAM プロセスの実行]ダイアログ ボックスが表示されます。このダイアログ ボックスには、レポート サーバ サービスの IT PAM 設定に定義されたプロセス名とプロセスのパラメータが含まれています。また、選択した CEG フィールドに返される変数データを入力できる[フィールドの選択]ドロップダウンリストもあります。

7. フィールドには以下のように入力します。

- a. 表示されるプロセス パラメータ用に示されたデフォルト値を確認し、変更する必要がある値を識別します。

これらのパラメータとその値は CA IT PAM 統合設定から取得されたものです。

- b. 表示されたデフォルト値を変更するには、新しい値を入力します。
- c. 変数の値を指定するには、ダイアログの一番上にある[フィールドの選択]ドロップダウンリストから CEG フィールドを選択し、その値が適用されたテキストボックスの隣の[フィールドの追加]をクリックします。
- d. 空白のフィールドには値を入力し、変数を選択してそれを追加するか、選択した変数を含む文を入力します。

サマリの例: On (event_datetime), the (dest_username) account performed a (event_action) action on the (dest_hostname) host.

説明の例: The action result (event_result), is logged in the (event_logname) log. The CA Severity is (event_severity).

- e. CA IT PAM プロセスで追加の CEG フィールドを参照するパラメータを指定する場合は、表示されたリストからパラメータとして送信するフィールドを選択します。

以下に例を示します。表示には、カスタムの IT PAM イベント/アラート出力プロセスに定義されたほかのフィールドが含まれる場合があります。

IT PAM プロセスの実行

IT PAM プロセス: /CA_ELM/EventAlertOutput

フィールドの選択: event_severity

ReportedBy:

Severity:

Priority:

EndUser:

Summary:

Description:

フィールド値をパラメータとして送信:

選択	使用可能なフィールド
☐	agent_address
☐	agent_connector_name
☐	agent_group
☐	agent_hostdomainname
☐	agent_hostname
☐	agent_id

フィールドの追加

OK キャンセル

8. [OK]をクリックします。

進行状況のダイアログ ボックスが表示され、その後には CA IT PAM プロセスが正常に実行されたかどうかを示すメッセージと、正常に実行された場合はプロセスの実行結果が表示されます。

以下に例を示します。ここでは、リクエスト 4590 がサービス デスクで作成されたという結果になっています。



9. [OK]をクリックします。

10. CA サービス デスクの結果を参照するには、ログオンし、メッセージの番号を使用して[リクエスト]を検索します。

たとえば、[リクエスト]を選択し、4590 と入力します。

リクエスト

11. サービス デスクの結果は次のように表示されます。

27 リクエストの詳細 編集(s) 変更要求の作成(s) インシデントの作成(s) クイック プロファイル

影響を受けるエンド ユーザ	リクエスト領域	ステータス	優先度
ServiceDesk		オープン	3

詳細

レポート作成者	担当者	グループ	構成アイテム
ServiceDesk	ServiceDesk		
重大度	緊急度	影響度	アクティブ
4- HD マネージャにエスカレート	4- 極めて迅速に	1- 組織全体	はい
チャージ バック ID	コールバック日/時間	根本原因	

変更

変更要求に起因

概要情報

概要	アクティビティ時間の合計		
2009年8月 月曜日 午前 11:58:59、アカウントsu が ホストca-elm上で、アラート作成のアクションを実行しました。	00:01:24		
説明			
アクションの結果は、CALMロケに記録されます。CAの重大度は2です			
オープン日/時間	最終変更	解決日/時間	クローズ日/時間
2009/11/11 09:24 am	2009/11/11 09:26 am		

12. 手順 7 で決定した、サマリおよび説明の予定のデータと、[サマリ情報]の下に表示されたサマリおよび説明のデータを比較します。このデータには、CA 重大度のデータが含まれます。

イベント/アラート出力プロセスに送信するイベントのクエリの設計

CA IT PAM 統合を設定したら、イベント/アラート出力を生成するアラートをスケジュールする最初の手順に進みます。その手順とは、そのアラートに基づくクエリのリストをコンパイルすることです。通常、これらはポリシー違反を示唆するイベントのクエリです。次のいくつかのアプローチを組み合わせることで実行できます。

- 現在スケジュールされているアラートを分析し、イベント/アラート出力プロセスを実行する必要があるものを識別します。たとえば、イベント/アラート出力プロセスがヘルプ デスク アプリケーションに通知する場合、ヘルプ デスク チケットを開く必要があるアラートを識別します。
- ポリシーを分析し、ログに記録されたイベントまで違反をさかのぼることができるポリシーを特定し、そのようなイベントのためのクエリを作成します。
- ほかの事前定義済みクエリの結果を確認し、改善策を実施する際にヘルプ デスク 製品などのサードパーティ製品が使用できるデータを識別します。
- CA IT PAM イベント/アラート出力プロセスがサードパーティのヘルプ デスク 製品でチケットを作成する場合は、イベント ログとしてキャプチャされるヘルプ デスク チケットの典型的なタイプを確認します。

CA IT PAM のイベント/アラート出力プロセスを実行するアラートに基づくクエリを特定または設計する方法

1. ヘルプ デスクのチケットを必要とする各イベントに対して、そのイベントのデータを取得する 1 つ以上のクエリを識別、変更、または作成します。
 - このような条件でイベントを収集する個々の事前定義済みクエリを識別します。
 - 事前定義済みクエリをカスタマイズする必要がある場合は、クエリをコピーし、ニーズに合わせてそのコピーを変更します。
 - ヘルプ デスクの通知を必要とする特定のタイプのイベントを収集する事前定義済みクエリが存在しない場合は、必要とするクエリ(複数可)を作成します。
2. IT イベントを検索するクエリで、そのフィールドの 1 つに複数の既知の値がある場合は、事前に定義されたキー設定済みリストを使用するか、キー設定済みリストをカスタマイズするか、新しいキー設定済みリストを作成します。このようなキーの値が csv ファイルで存在する場合は、それをインポートします。IT PAM プロセスによって生成されたリストの場合は、そのプロセスを動的値プロセスとして設定し、キーを作成して、CA IT PAM から値をインポートします。

3. CA IT PAM イベント/アラート出力プロセスを、結果を返すクエリごとに実行するのか、結果の行ごとに実行するのかを決定します。
4. クエリをテストします。
 - a. キャプチャするイベントを生成する条件を作成します。
 - b. クエリまたはクエリのセットを手動で実行します。
 - c. ヘルプ デスクの担当者が必要なフォローアップを実行するのにそのクエリ結果が十分かどうかを評価します。
 - d. 十分でない場合、必要な情報を提供できるようにクエリまたはクエリのセットを変更し、再テストします。

このような準備を行うことにより、クエリまたはクエリのセットをそれぞれ実行するアラートのスケジュールを設定する場合に、問題解決に必要なデータがイベント/アラートの出力結果に必ず含まれるようになります。

詳細情報:

[アクション アラートのクエリのカスタマイズ](#) (P. 356)

例：行ごとに IT PAM プロセスを実行するアラートの送信

行またはクエリごとに、CA IT PAM のイベント/アラート出力プロセスを実行するアラートを送信できます。この例では、行ごとにプロセスを実行する手順について説明します。この例には、CA IT PAM と、CA IT PAM が詳細を送信するサードパーティ製品の両方を使用する担当者が、このタイプのアラートのために表示できる内容が含まれます。

指定されたクエリの IT PAM プロセスを実行するアラートを作成する前に、データを返す CEG 列を識別しておくことをお勧めします。これらの列は、アラートのサマリと説明のステートメントを作成する場合に選択する列です。

注：クエリをコピーし、[クエリ列]の手順をクリックします。表示できるように設計されたフィールドについては、表示名に対応する列名に注意します。たとえば、[アカウント]列に入力するために使用される CEG フィールドは `dest_username` です。

選択済みの列		
 		
表示名	列	可視
	event_summarized	☐
Account	dest_username	☒
Host	dest_hostname	☒
Log Name	event_logname	☒
Action	event_action	☒
Result	event_result	☒
Session ID	dest_objectvalue	☐

デフォルト アカウントのメンバが正常にログインしたときにアラートを生成する方法

1. [アラート管理]タブをクリックし、[アラートのスケジュール]サブタブをクリックします。
2. [アクション アラートのスケジュール]をクリックします。

アクション アラートのスケジュール ウィザードが表示されます。

3. 以下の要領で、[アラートの選択]の手順を完了します。
 - a. 「デフォルトのアカウントのログイン」などのジョブ名を入力します、
 - b. [アクション アラート]タグをクリックします。
 - c. [過去 24 時間におけるデフォルト アカウントごとのログイン成功]を選択し、[選択されたクエリ]リストに移動させます。

クエリの選択

タグまたは個別のクエリを選択して、アラートを実行するクエリを定義します。

ジョブ名: Default Account Logins ☒ 有効

選択タイプ: ☒ クエリ ☐ タグ

クエリ

使用可能なタグ	選択されたクエリ
Action Alerts [46]	過去 24 時間におけるデフォルト アカウントごとのログイン成功

4. クエリを実行する日付範囲と、表示する最大行数を選択します。
 - a. [結果の条件]をクリックします。
 - b. 「今すぐ」および「今すぐ」「-1 時間」などの日付範囲を選択します。
 - c. 行の制限値を 10 にするなど、結果の表示パラメータを選択し、時間粒度には event_datetime を選択します。
 - d. グループ化されたイベント数はスキップします。
5. スケジュールを定義します。
6. クエリによって取得されたイベント データと共に IT PAM プロセスに渡すアラート データを定義します。
 - a. [宛先]の手順をクリックします。
 - b. [IT PAM プロセス]タブを選択します。
 - c. [過去 24 時間におけるデフォルト アカウントごとのログイン成功]を選択します。
 - d. [IT PAM プロセスを行単位で実行]を選択します。
 - e. 設定された IT PAM プロセスが実行する予定のものではない場合は、IT PAM プロセスのパスを変更します。IT PAM プロセスには、スラッシュ (/) で始まるフル パスが含まれている必要があります。

- f. (オプション) 文字テキストと変数を使用して、サマリステートメントを作成します。ここで、行の収集されたデータを絞り込む場合、変数は CEG フィールドから取得されます。次の例では、変数を使用してサマリステートメントを作成します。

The (dest_username) account performed the (event_action) action on (dest_hostname)

最初のステートメントは次のように作成されています。

- 「The」を入力します。
 - [フィールドの選択]ドロップダウンリストから **dest_username** を選択し、[サマリ]フィールドの隣の + をクリックします。
 - 「account performed the」を入力します。
 - [フィールドの選択]ドロップダウン リストから **event_action** を選択し、[サマリ]フィールドの隣の + をクリックします。
 - 「action on」を入力します。
 - [フィールドの選択]ドロップダウンリストから **dest_hostname** を選択し、[サマリ]フィールドの隣の + をクリックします。
- g. (オプション) 文字テキストと、CEG フィールドから取得したテキストを使用して、説明を作成します。[フィールドの選択]ドロップダウンリストから目的のフィールドを選択し、+ をクリックします。以下に例を示します。

The (event_logname) log shows the result of (event_result) on (event_datetime)

The(event_result) of the (event_action) is logged in the (event_logname) log.

The (event_logname) log shows the (event_action) action had a result of (event_result).

- h. [フィールド値をパラメータとして送信]には、指定された IT PAM プロセスがプロセス パラメータとして使用する CEG フィールドをそれぞれ選択します。

注: 選択したプロセスはパラメータとして CEG フィールド名を使用しないため、この例ではフィールドは確認されません。カスタム プロセスがこのようなパラメータを使用するかどうかを判断するには、CA IT PAM イベント/アラート出力プロセスの[データセット]タブを表示します。

過去 24 時間におけるデフォルト アカウントごとのログイン成功

☒ IT PAM プロセスを行単位で実行

IT PAM プロセス: /CA_ELM/EventAlertOutput

フィールドの選択: dest_hostname

ReportedBy: +

Severity: +

Priority: +

EndUser: +

Summary: +

Description: +

フィールド値をパラメータとして送信:

選択	使用可能なフィールド
☐	dest_hostname
☐	dest_username
☐	event_action
☐	event_datetime
☐	event_logname
☐	event_result

7. サーバを選択します。
8. [保存して閉じる]をクリックします。
ジョブが[アクション アラート ジョブ]に表示されます。

アクションアラートジョブ								
☐	ジョブ名	有効	サーバ	反復	開始時間	終了時間	タイムゾーン	作成者
☐	Configuration Changes destined for CA	はい	etr65111-blade12	5 分	2009-11-20 金曜日 午前 11:35:20		Asia/Calcutta	admin

9. [アラート管理]、[自己監視イベント]の順にクリックして、結果を表示します。
情報行の一部のビューは次のようになります。

アクション	結果	結果の説明
Configuration Warning	F	Unable to connect to the specified RSSFeed URL http://securityupdates.ca.com/CA-ELM#12.1/RSSFeed.xml. Please check the URL again.
Configuration Warning	F	Unable to connect to the specified RSSFeed URL http://securityupdates.ca.com/CA-ELM#12.1/RSSFeed.xml. Please check the URL again.
Configuration Warning	F	Unable to connect to the specified RSSFeed URL http://securityupdates.ca.com/CA-ELM#12.1/RSSFeed.xml. Please check the URL again.

10. [アラート管理]タブ、[アクション アラート]サブタブの順にクリックします。スケジュール設定したアラートを選択し、クエリ結果を表示します。

アラート名		カテゴリ		日付		
Default Account Logins		Successful Login by Default Accounts in last 24 hours		Mon, 03 Aug 2009 14:38:07 EDT		
Default Account Logins						
Alert name(Default Account Logins) Alert created by(su) Federated job(Yes) Tags (Action Alerts) Time Zone (America/New_York) Reports on successful login activity by user accounts listed in Default_Accounts keyed list during the last 24 hour time frame Rows Returned(1)						
日付		アカウント	ホスト	ログの名前	動作	結果
Mon Aug 03 2009 02:35:09 PM		su	ca-elm	CALM	Login Attempt	S

11. CA IT PAM から返された結果の自己監視イベントタブを確認します。

成功メッセージの部分的な例は次のとおりです。ここでは、このメッセージがレポートサーバの自己監視イベントに表示されます。Results = の後にチケット番号が続くことに注意してください。

行動	結果	検索結果の説明
Notification Creation	S	IT PAM process ran successfully. Results = [Request 631 created in CA Service Desk.]

12. (オプション)CA サービス デスクに関する結果を次のように確認します。
- CA サービス デスクにログオンします。
 - [リクエスト]を選択し、発行番号を入力します。
 - リクエスト番号のリンクをクリックして、問題の詳細とサマリ情報を確認します。

詳細情報:

[イベント/アラート出力プロセスを作成するためのガイドライン](#) (P. 387)

例: クエリごとに IT PAM プロセスを実行するアラートの送信

行またはクエリごとに、CA IT PAM のイベント/アラート出力プロセスを実行するアラートを送信できます。この例では、クエリごとにプロセスを実行する手順について説明します。この例には、CA IT PAM が詳細を送信するサードパーティ製品を使用する担当者が、このタイプのアラートのために表示できる内容が含まれます。

クエリごとに CA IT PAM のイベント/アラート出力プロセスを実行するアラートを送信する方法

1. [アラート管理]タブをクリックし、[アラートのスケジュール]サブタブをクリックします。
2. [アクション アラートのスケジュール]をクリックします。
アクション アラートのスケジュール ウィザードが表示されます。
3. 以下の要領で、[アラートの選択]の手順を完了します。
 - a. ジョブ名を入力します。
 - b. クエリを選択します。
4. (オプション) クエリを実行する日付範囲と、表示する最大行数を選択します。
 - a. [結果の条件]をクリックします。
 - b. 「今すぐ」および「今すぐ」「-1 時間」などの日付範囲を選択します。
 - c. 結果の表示パラメータを選択します。
5. スケジュールを定義します。
6. クエリによって取得されたイベント データと共に IT PAM プロセスに渡すアラート データを定義します。
 - a. [宛先]の手順をクリックします。
 - b. [IT PAM プロセス]タブを選択します。
 - c. 送信するクエリを選択します。

☒ 過去 24 時間におけるデフォルト アカウントごとのログイン成功

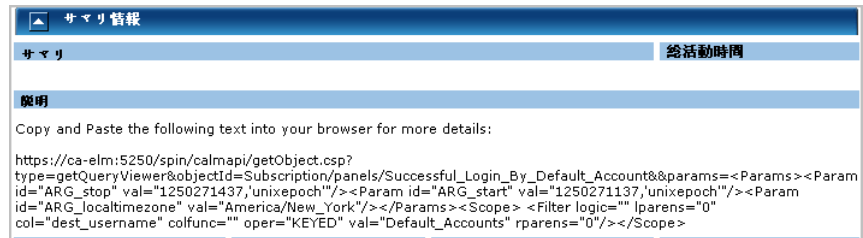
- d. クエリごとにレポートされるレポートが必要な場合は、[IT PAM プロセスを行単位で実行]を空白のままにします。
- e. オプションで、[サマリ]と[説明]のフィールドに文字テキストを入力します。

7. サーバを選択します。
8. [保存して閉じる]をクリックします。
ジョブが[アクション アラート ジョブ]に表示されます。
9. [アラート管理]タブ、[アクション アラート]サブタブの順にクリックします。スケジュール設定したアラートを選択し、クエリ結果を表示します。
10. CA IT PAM から返された結果を持つ通知作成アクションの自己監視イベントタブを確認します。ヘルプ デスク製品の場合は、サードパーティアプリケーションで作成されたリクエスト番号が成功メッセージに含まれます。

行動	結果	検索結果の説明
Notification Creation	S	IT PAM process ran successfully. Results = Request 2936 created in CA Service Desk.

11. (オプション) ヘルプ デスク担当者に表示される内容を確認するには、次のように CA Service Desk に関する結果を確認します。
 - a. CA サービス デスクにログオンします。
 - b. リクエストを選択し、通知の作成の結果説明に表示された番号を入力します。[実行]をクリックします。

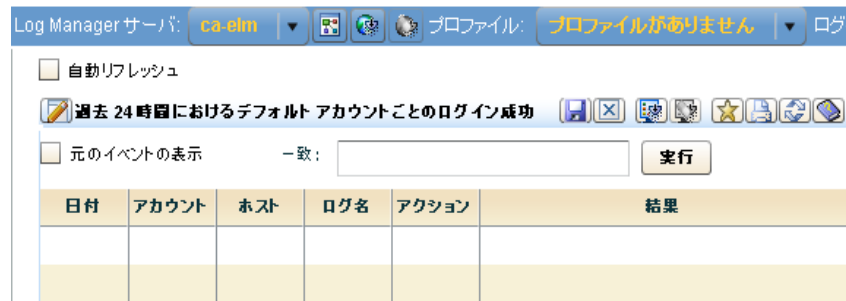
- c. [サマリ情報]セクションに表示された URL をコピーし、ブラウザにその URL を貼り付けます。



CA Enterprise Log Manager ログオン ダイアログ ボックスが表示されます。

- d. CA Enterprise Log Manager にログインします。監査者のような低い権限のロールを持つアカウントを使用できます。

クエリによって返されたイベント データは、クエリのデフォルトビューの形式(すなわち表またはグラフ)で表示されます。



表示が表形式である場合、元のイベントデータを表示できます。

詳細情報:

[通知の宛先の設定 \(P. 457\)](#)

SNMPトラップの操作

障害管理システムおよびネットワーク運用センター(NOC)は、通常 SNMPトラップを受信します。宛先製品に応じて、SNMP v2トラップまたは SNMP v3トラップなどのアラートをシステムに送信できます。

SNMPトラップを使用するために必要なタスクは以下のとおりです。

- CA NSM への各アクション アラート用のカスタム MIB を作成します。
- CA Enterprise Log Manager からの SNMPトラップの受信先の製品を準備します。
- 1 つ以上の SNMPトラップ宛先を指定したアラートをスケジュールします。

デフォルト SNMPトラップ宛先の設定はオプションです。

SNMPトラップについて

SNMP は Simple Network Management Protocol の略語で、指定された宛先にアラート メッセージを送信するためのオープン規格です。SNMP には、SNMPv1、SNMPv2 および SNMPv3 の 3 つのバージョンがあります。CA Enterprise Log Manager では、SNMPv2 または SNMPv3 のいずれかを使用して、アラートを生成するイベントが発生したときに 1 つ以上のサードパーティ管理システムにアラートを知らせることができます。

CA Enterprise Log Manager では、スケジュールされたクエリが最近精製されたイベントのイベントログ データベースから結果を返す場合、アラートが生成されます。スケジュールされたクエリは、宛先として SNMPトラップを使用して設定できます。トラップ受信者である宛先管理システムでは、毎秒およそ 200 個の割合でトラップを処理できます。通常、トラップ受信者は UDP ポート 162 (snmptrap の Well-Known ポート) でリスンします。

CA Enterprise Log Manager が備える柔軟性によって、独自のカスタム アラートを作成し、SNMPトラップとして送信することができます。たとえば、クリティカルなイベントが発生したという通知を送信するアラートを定義できます。あるいは、設定変更などのイベント用のアラートを定義することもできます。SNMPトラップとして送信するアラートを指定できます。

トラップとして送信するアラート用の単純なフィルタの例

業務に悪影響を与えるイベント(サービスのシャットダウン、デバイスの障害、リソースの削除など)は、ネットワーク運用センター(NOC)の監視対象となります。そのようなイベントが発生した場合は、アクションアラートを生成してNOCにルーティングできます。その目的のために、カスタムクエリで単純フィルタを使用して、カスタムアラートを作成できます。以下に、単純フィルタの例を示します。

■ デバイス エラー

単純フィルタ	
有効な単純フィルタを選択し、配置します	
☒ 理想モデル:	Network Device
☒ イベント カテゴリ:	Operational Security
☒ イベント クラス:	Device and Port Activity
☒ イベント アクション:	Device Error

■ リソース削除

単純フィルタ	
有効な単純フィルタを選択し、配置します	
☒ 理想モデル:	Network Management
☒ イベント カテゴリ:	Resource Access
☒ イベント クラス:	Resource Activity
☒ イベント アクション:	Resource Deletion

■ システム シャットダウン

単純フィルタ	
有効な単純フィルタを選択し、配置します	
☒ 理想モデル:	Operating System
☒ イベント カテゴリ:	Operational Security
☒ イベント クラス:	System Activity
☒ イベント アクション:	System Shutdown

MIB ファイルについて

SNMPトラップは、標準的な Management Information Base (MIB、管理情報ベース)ファイルまたは企業固有の MIB のいずれかで定義されます。

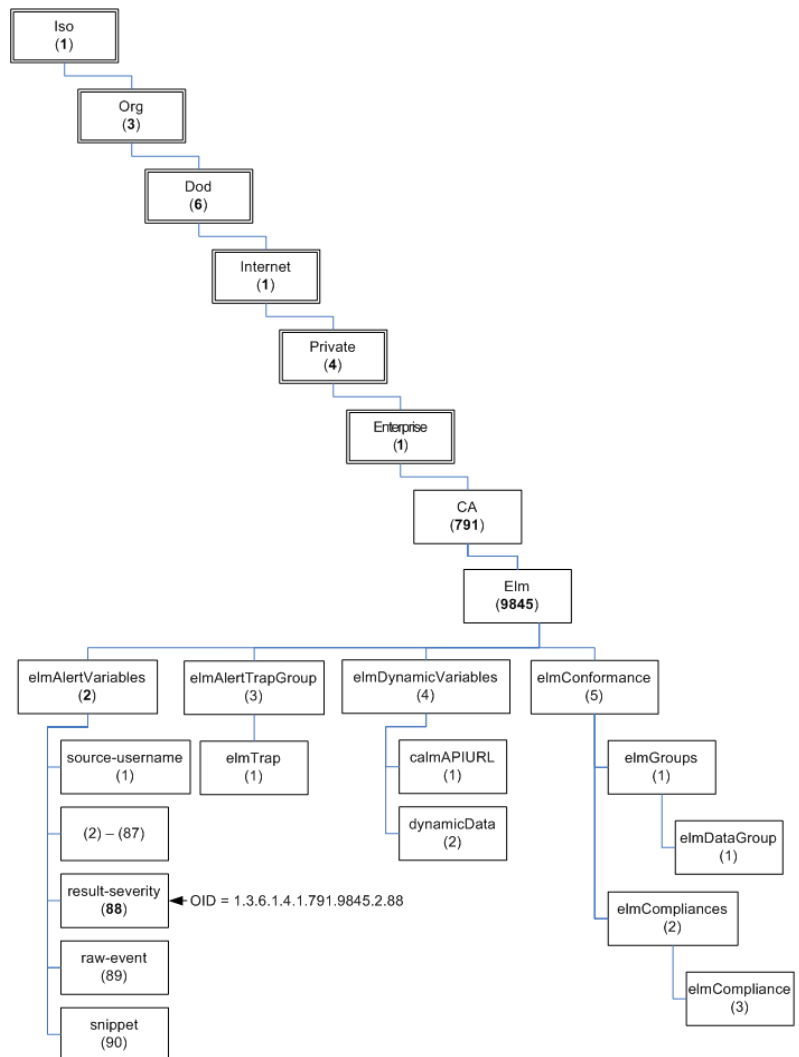
MIB ツリーでは、民間企業はそれぞれ一意の番号を持ち、その親ノードの番号が前に付いています。CA, Inc. には IANA によって **private enterprise number 791** が割り当てられています。CA のアプリケーションによって SNMPトラップで送信されたデータは、すべて **1.3.6.1.4.1.791** で始まるオブジェクト ID に関連付けられています。CA に属する **CA Enterprise Log Manager** アプリケーションは、識別子として **9845** という番号を持っています。CA Enterprise Log Manager アクションアラートによって送信された SNMPトラップ データは、すべて **1.3.6.1.4.1.791.9845** で始まるオブジェクト ID (OID)に関連付けられています。

CA Enterprise Log Manager では MIB ファイルを 1 つ用意しています。この MIB の名前は **CA-ELM.MIB** です。この MIB によって、1 つのトラップを備えたアクションアラートによって送信できるすべてのフィールドが定義されます。このトラップには、CA Enterprise Log Manager で利用可能な CEG フィールドがすべて含まれます。

アクションアラートが SNMPトラップの宛先に送信される際、送信されるデータに URL が含まれます。受信トラップを監視する各ユーザは、アクションアラートによって送信された URL を参照できます。URL を参照すると、CA Enterprise Log Manager ページが起動し、読みやすい形式でクエリ結果が表示されます。この機能によって、SNMPトラップとして送信されたデータを解釈するために MIB を使用する必要がありません。

CA-ELM MIB ツリー

CA-ELM.MIB ファイルの構造を MIB ツリーの形式で表示できます。CEG フィールドは、elmAlertVariables の下に一意の SNMP オブジェクト識別子を使用して定義されます。たとえば、result_severity には 1.3.6.1.4.1.791.9845.2.88 の OID があります。



CA-ELM.MIB ファイル

CA Enterprise Log Manager MIB ファイル(CA-ELM.MIB)は、インストール DVD にあります。CA Enterprise Log Manager MIB は CEG ソースドキュメントから生成され、各 CEG フィールド(elmAlertVariables)の OID が格納されています。

CA-ELM.MIB ファイルは、以下のようにインポートから始まります。

```
CAELM-MIB DEFINITIONS ::= BEGIN

    IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32, NOTIFICATION-TYPE
            FROM SNMPv2-SMI
        MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
            FROM SNMPv2-CONF
            DisplayString
            FROM SNMPv2-TC;
```

以下に、CA Enterprise Log Manager MIB ツリーの表現を示します。この表現では、最上位ノードに iso(1)、org(3)、dod(6)、internet(1)、private(4)、enterprises(1) が含まれています。実際の CA-ELM.MIB の形式はこの表現とは異なります。

```
ca OBJECT IDENTIFIER ::= { enterprises 791 }
elm MODULE-IDENTITY... ::= { ca 9845 }
    elmAlertVariables ::= { elm 2 }
        source-username ::= { elmAlertVariables 1 }
        source-domainname ::= { elmAlertVariables 2 }
        source-groupname ::= { elmAlertVariables 3 }
        ...
        result-severity ::= { elmAlertVariables 88 }
        raw-event ::= { elmAlertVariables 89 }
        snippet ::= { elmAlertVariables 90 }
    elmAlertTrapGroup ::= { elm 3 }
        elmTrap ::= { elmAlertTrapGroup 1 }

    elmDynamicVariables ::= { elm 4 }
        calmAPIURL ::= { elmDynamicVariables 1 }
        dynamicData ::= { elmDynamicVariables 2 }
    elmConformance ::= { elm 5 }
        elmGroups ::= { elmConformance 1 }
            elmDataGroup ::= { elmGroups 1 }
        elmCompliances ::= { elmConformance 2 }
            elmCompliance ::= { elmCompliances 3 }
```


CA-ELM.MIB ファイルは 1 つのトラップを定義します。このトラップは、以下のよう
に定義されます。

```
elmTrap NOTIFICATION-TYPE
    OBJECTS
    { source-username, source-domainname, source-groupname, source-uid, source-gid, source-
      hostname, source-hostdomainname, source-address, source-mac-address, source-port, source-
      processname, source-objectname, source-objectattr, source-objectid, source-objectclass,
      source-objectvalue, dest-username, dest-domainname, dest-groupname, dest-uid, dest-gid,
      dest-hostname, dest-hostdomainname, dest-address, dest-mac-address, dest-port, dest-
      objectname, dest-objectattr, dest-objectid, dest-objectclass, dest-objectvalue,
      agent-name, agent-address, agent-hostname, agent-hostdomainname, agent-version, agent-
      id, agent-connector-name, agent-group, event-source-hostname, event-source-hostdomain-
      name, event-source-address, event-source-processname, receiver-name, receiver-hostname,
      receiver-hostaddress, receiver-hostdomainname, receiver-port, receiver-time-gmt, receiver-
      timezone, receiver-version, event-protocol, event-logname, event-euuid, event-count,
      event-summarized, event-duration, event-time-year, event-time-month, event-time-monthday,
      event-time-weekday, event-time-hour, event-time-minute, event-time-gmt, event-datetime,
      event-year-datetime, event-month-datetime, event-day-datetime, event-hour-datetime,
      event-quarterhour-datetime, event-minute-datetime, event-timezone, event-sequence,
      event-trend, event-action, event-id, event-category, event-class, ideal-model,
      event-severity, event-result, result-string, result-signature, result-code, result-version,
      result-priority, result-scope, result-severity, raw-event, snippet }
    STATUS current
    DESCRIPTION
        "The ELM SNMP Trap."
    ::= { elmAlertTrapGroup 1 }
```

elmAlertTrapGroup は 1.3.6.1.4.1.791.9845.3 で、elmTrap は次のノードによって
定義されます。デフォルトの elmTrap ID は、1.3.6.1.4.1.791.9845.3.1 です。
ユーザ定義のカスタムトラップ ID の範囲は、1.3.6.1.4.1.791.9845.3.2 から
1.3.6.1.4.1.791.9845.3.999 です。

重要: CA Spectrum にトラップを送信するための最良の方法は、デフォルト
elmTrap ID を使用することです。CA NSM にトラップを送信するための最良の方法は、
カスタム MIB 内の elmTrap ID を参照するカスタム Trap ID を指定すること
です。

オブジェクト ID (OID) と CEG フィールドのマッピング

以下の表は、MIB ツリーの `elmAlertVariables` 以下の各オブジェクト ID (OID) に対応する CEG フィールドを示しています。新しいフィールドが CEG に追加されるにつれて、ツリーのこのブランチが増えていきます。MIB への更新がないかどうかを必ずチェックして、ユーザの SNMP トラップ宛先製品で確実に最新のバージョンを利用できるようにしておいてください。

オブジェクト ID (OID)	CEG フィールド
1.3.6.1.4.1.791.9845.2.1	source-username
1.3.6.1.4.1.791.9845.2.2	source-domainname
1.3.6.1.4.1.791.9845.2.3	source-groupname
1.3.6.1.4.1.791.9845.2.4	source-uid
1.3.6.1.4.1.791.9845.2.5	source-gid
1.3.6.1.4.1.791.9845.2.6	source-hostname
1.3.6.1.4.1.791.9845.2.7	source-hostdomainname
1.3.6.1.4.1.791.9845.2.8	source-address
1.3.6.1.4.1.791.9845.2.9	source-mac-address
1.3.6.1.4.1.791.9845.2.10	source-port
1.3.6.1.4.1.791.9845.2.11	source-processname
1.3.6.1.4.1.791.9845.2.12	source-objectname
1.3.6.1.4.1.791.9845.2.13	source-objectattr
1.3.6.1.4.1.791.9845.2.14	source-objectid
1.3.6.1.4.1.791.9845.2.15	source-objectclass
1.3.6.1.4.1.791.9845.2.16	source-objectvalue
1.3.6.1.4.1.791.9845.2.17	dest-username
1.3.6.1.4.1.791.9845.2.18	dest-domainname
1.3.6.1.4.1.791.9845.2.19	dest-groupname
1.3.6.1.4.1.791.9845.2.20	dest-uid
1.3.6.1.4.1.791.9845.2.21	dest-gid
1.3.6.1.4.1.791.9845.2.22	dest-hostname

オブジェクト ID (OID)	CEG フィールド
1.3.6.1.4.1.791.9845.2.23	dest-hostdomainname
1.3.6.1.4.1.791.9845.2.24	dest-address
1.3.6.1.4.1.791.9845.2.25	dest-mac-address
1.3.6.1.4.1.791.9845.2.26	dest-port
1.3.6.1.4.1.791.9845.2.27	dest-objectname
1.3.6.1.4.1.791.9845.2.28	dest-objectattr
1.3.6.1.4.1.791.9845.2.29	dest-objectid
1.3.6.1.4.1.791.9845.2.30	dest-objectclass
1.3.6.1.4.1.791.9845.2.31	dest-objectvalue
1.3.6.1.4.1.791.9845.2.32	agent-name
1.3.6.1.4.1.791.9845.2.33	agent-address
1.3.6.1.4.1.791.9845.2.34	agent-hostname
1.3.6.1.4.1.791.9845.2.35	agent-hostdomainname
1.3.6.1.4.1.791.9845.2.36	agent-version
1.3.6.1.4.1.791.9845.2.37	agent-id
1.3.6.1.4.1.791.9845.2.38	agent-connector-name
1.3.6.1.4.1.791.9845.2.39	agent-group
1.3.6.1.4.1.791.9845.2.40	event-source-hostname
1.3.6.1.4.1.791.9845.2.41	event-source-hostdomainname
1.3.6.1.4.1.791.9845.2.42	event-source-address
1.3.6.1.4.1.791.9845.2.43	event-source-processname
1.3.6.1.4.1.791.9845.2.44	receiver-name
1.3.6.1.4.1.791.9845.2.45	receiver-hostname
1.3.6.1.4.1.791.9845.2.46	receiver-hostaddress
1.3.6.1.4.1.791.9845.2.47	receiver-hostdomainname
1.3.6.1.4.1.791.9845.2.48	receiver-port
1.3.6.1.4.1.791.9845.2.49	receiver-time-gmt
1.3.6.1.4.1.791.9845.2.50	receiver-timezone

オブジェクト ID (OID)	CEG フィールド
1.3.6.1.4.1.791.9845.2.51	receiver-version
1.3.6.1.4.1.791.9845.2.52	event-protocol
1.3.6.1.4.1.791.9845.2.53	event-logname
1.3.6.1.4.1.791.9845.2.54	event-euuid
1.3.6.1.4.1.791.9845.2.55	event-count
1.3.6.1.4.1.791.9845.2.56	event-summarized
1.3.6.1.4.1.791.9845.2.57	event-duration
1.3.6.1.4.1.791.9845.2.58	event-time-year
1.3.6.1.4.1.791.9845.2.59	event-time-month
1.3.6.1.4.1.791.9845.2.60	event-time-monthday
1.3.6.1.4.1.791.9845.2.61	event-time-weekday
1.3.6.1.4.1.791.9845.2.62	event-time-hour
1.3.6.1.4.1.791.9845.2.63	event-time-minute
1.3.6.1.4.1.791.9845.2.64	event-time-gmt
1.3.6.1.4.1.791.9845.2.65	event-datetime
1.3.6.1.4.1.791.9845.2.66	event-year-datetime
1.3.6.1.4.1.791.9845.2.67	event-month-datetime
1.3.6.1.4.1.791.9845.2.68	event-day-datetime
1.3.6.1.4.1.791.9845.2.69	event-hour-datetime
1.3.6.1.4.1.791.9845.2.70	event-quarterhour-datetime
1.3.6.1.4.1.791.9845.2.71	event-minute-datetime
1.3.6.1.4.1.791.9845.2.72	event-timezone
1.3.6.1.4.1.791.9845.2.73	event-sequence
1.3.6.1.4.1.791.9845.2.74	event-trend
1.3.6.1.4.1.791.9845.2.75	event-action
1.3.6.1.4.1.791.9845.2.76	event-id
1.3.6.1.4.1.791.9845.2.77	event-category
1.3.6.1.4.1.791.9845.2.78	event-class

オブジェクト ID (OID)	CEG フィールド
1.3.6.1.4.1.791.9845.2.79	ideal-model
1.3.6.1.4.1.791.9845.2.80	event-severity
1.3.6.1.4.1.791.9845.2.81	event-result
1.3.6.1.4.1.791.9845.2.82	result-string
1.3.6.1.4.1.791.9845.2.83	result-signature
1.3.6.1.4.1.791.9845.2.84	result-code
1.3.6.1.4.1.791.9845.2.85	result-version
1.3.6.1.4.1.791.9845.2.86	result-priority
1.3.6.1.4.1.791.9845.2.87	result-scope
1.3.6.1.4.1.791.9845.2.88	result-severity
1.3.6.1.4.1.791.9845.2.89	raw-event

カスタム MIB

CA-ELM.MIB ファイル コンテンツから選択した **varbind** を追加することで、定型のテキストからカスタム MIB ファイルを作成できます。単一のアラート用のカスタム MIB ファイルには、CA-ELM.MIB ファイルの内容の一部が含まれています。アラート用のカスタム MIB は、以下の点で CA-ELM.MIB とは異なります。

- カスタム MIB は、そのアラートによって送信されるフィールドのみを定義します。
- カスタム MIB は、それらのフィールドを送信順に表示するトラップを定義します。
- カスタム MIB トラップは、1.3.6.1.4.1.791.9845.3.x (x は 1 から 999 の値) という OID で定義されます。

注: カスタム MIB を使用するアラートは、この OID をカスタムトラップ ID の値として指定します。

- カスタム MIB には、クエリに計算されたフィールドが含まれる場合にのみ **dynamicData varbind** が含まれます。

計算は任意のフィールドに適用できます。**event_count** フィールドは、計算が(常にではないが)一般的に適用されるフィールドの例です。「システム イベント数 (イベントアクション別)」クエリの **event_count** は、**Sum** で計算される計算フィールドです。あるフィールドが計算フィールドかどうかを調べるには、そのフィールドが定義されているクエリを調べます。以下に、計算フィールドである **event_count** の定義の例を示します。

```
System_Event_Count_By_Event_Action.xml:    <Column columnname="event_count"
datatype="I" displayname="Count" functionname="sum" resultname="event_count"
sortdesc="true" sortorder="1" visible="true"/>
```

カスタム MIB 用の定型テキスト

以下に、カスタム MIB 用の定型テキストを示します。このサンプルを使用してカスタム MIB を作成する場合は、文字列 **###** で示されている場所にカスタム データを挿入するか、カスタム データで置き換えることができます。データを変更するセクションでは、オプションでその説明を変更できます。

```
CAELM-MIB DEFINITIONS ::= BEGIN
    IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32, NOTIFICATION-TYPE
            FROM SNMPv2-SMI
        MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
            FROM SNMPv2-CONF
        DisplayString
            FROM SNMPv2-TC;
```

```
elm MODULE-IDENTITY
    LAST-UPDATED "200907050600Z"
    ORGANIZATION "CA"
    CONTACT-INFO
        "100 Staples drive
        Framingham MA"
    DESCRIPTION
        "Contains objects describing data for ELM events"
    REVISION "200907050600Z"
    DESCRIPTION
        "Custom MIB <###>."
    ::= { ca 9845 }

ca OBJECT IDENTIFIER ::= {enterprises 791}
elmAlertTrapGroup OBJECT IDENTIFIER ::= { elm 3 }
elmAlertVariables OBJECT IDENTIFIER ::= { elm 2 }
elmDynamicVariables OBJECT IDENTIFIER ::= { elm 4 }
elmConformance OBJECT IDENTIFIER ::= { elm 5 }
elmGroups        OBJECT IDENTIFIER ::= { elmConformance 1 }
elmCompliances OBJECT IDENTIFIER ::= { elmConformance 2 }

<### Insert elmAlertVariable varbind for each query field ###>

<### Insert the following dynamicData varbind only if query includes calculated fields
###>
dynamicData OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        " This field contains all the elm dynamic variables and data in name=value format."
    ::= { elmDynamicVariables 2 }

calmAPIURL OBJECT-TYPE
    SYNTAX OCTET STRING
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The OPEN API URL which points to the query result."
    ::= { elmDynamicVariables 1 }
```

```

elmTrap NOTIFICATION-TYPE
  OBJECTS { <### insert list of query fields with hyphens ###> }
  STATUS current
  DESCRIPTION
    "The ELM SNMP Trap."
  ::= { elmAlertTrapGroup <### insert custom trap ID node number ###> }

elmCompliance MODULE-COMPLIANCE
  STATUS current
  DESCRIPTION
    "The compliance information."
  MODULE -- this module
    GROUP elmDataGroup
    DESCRIPTION
      "This group is mandatory."
  ::= { elmCompliances 3 }
-- units of conformance

elmDataGroup OBJECT-GROUP
  OBJECTS { <### insert list of query fields with hyphens ###> }
  STATUS current
  DESCRIPTION
    "A collection of objects providing information specific to
    ELM data."
  ::= { elmGroups 1 }
END

```

例: 平均 CPU 負荷トレンド クエリ用のカスタム MIB 33 の作成

CA NSM に SNMP トラップとして送信されるクエリごとにカスタム MIB を作成します。各クエリは、カスタムトラップ ID に関連付けられます。カスタム MIB は、アクション アラートに表示される順にトラップに追加されたフィールドを定義します。

以下の例では、アクション アラート用のクエリとして平均 CPU 負荷トレンドが選択されています。選択されているフィールドは、event_datetime と event_trend です。

☒ 平均 CPU 負荷トレンド	平均 CPU 負荷トレンド SNMPトラップで送信するフィールド: ☒ event_datetime ☒ event_trend

カスタムトラップ ID は、1.3.6.1.4.1.791.9845.3.33 です。

カスタムトラップ ID: 1.3.6.1.4.1.791.9845.3. 

33 で終わるカスタムトラップ ID 用のカスタム MIB を作成する方法

1. カスタム MIB にテキストをコピーするために、CA-ELM.MIB のコピーを開きます。
2. エディタを開き、カスタム MIB の定型テキストをコピーして、新しい名前を付けてファイルを保存します。たとえば、Custom MIB n.mib という名前で保存します。この例では n は 33 となり、これはアクション アラートのクエリに対して指定したカスタムトラップ ID の最終ノードです。
3. (オプション) elm MODULE-IDENTITY の下の <###> を 33 に置き換えます。以下に例を示します。

Custom MIB 33."

4. 以下の定型テキストを CA-ELM.MIB のテキストに置き換えます。

```
<### Insert elmAlertVariable varbind for each query field in trap sequence ###>
```

event_datetime の elmAlertVariable varbind をコピーし、次に event_trendCopy の varbind をコピーします。これらの varbind は、SNMP トラップとして送信される順番に MIB に表示される必要があります。以下に例を示します。

```
event-datetime OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
```

```
"The calendar date and time expressed in the event information"
    ::= { elmAlertVariables 65 }
```

```
event-trend OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
```

```
"Trending data for this event."
    ::= { elmAlertVariables 74 }
```

5. どちらのフィールドも計算フィールドではないので、以下の定型テキストを削除します。

```
<### Insert the following dynamicData varbind only if query includes calculated fields ###>
dynamicData OBJECT-TYPE
    SYNTAX DisplayString
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        " This field contains all the elm dynamic variables and data in name=value format."
    ::= { elmDynamicVariables 2 }
```

6. elmTrap の下にある以下の定型テキストを見つけます。

```
OBJECTS <### insert list of query fields with hyphens ###> }
```

このテキストを、選択したクエリフィールドのリストに置き換えます。

```
OBJECTS { event-datetime,event-trend }
```

7. elmTrap の下にある以下の定型テキストを見つけます。

```
::= { elmAlertTrapGroup <### insert custom trap ID node number ###> }
```

このテキストを、以下のテキストに置き換えます。

```
::= { elmAlertTrapGroup 33 }
```

8. elmDataGroup の下にある以下の定型テキストを見つけます。

```
OBJECTS { <### insert list of query fields with hyphens ###> }
```

このテキストを、以下のテキストに置き換えます。

```
OBJECTS { event-datetime,event-trend }
```

9. ファイルを保存します。

例:カスタム MIB 33

以下の例は、SNMPトラップ(33で終わるカスタムトラップIDを持つ)として送信されるアクションアラート用に作成されたカスタムMIBです。カスタムトラップIDは1.3.6.1.4.1.791.9845.3.33です。選択したクエリは平均CPU負荷トレンドで、SNMPトラップで送信されるフィールドはevent_datetime および event_trend です。

```
CAELM-MIB DEFINITIONS ::= BEGIN
    IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32, NOTIFICATION-TYPE
            FROM SNMPv2-SMI
        MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
            FROM SNMPv2-CONF
        DisplayString
            FROM SNMPv2-TC;

    elm MODULE-IDENTITY
        LAST-UPDATED "200907050600Z"
        ORGANIZATION "CA"
        CONTACT-INFO
            "100 Staples drive
             Framingham MA"
        DESCRIPTION
            "Contains objects describing data for ELM events"
        REVISION "200907050600Z"
        DESCRIPTION
            "Custom MIB 33."
        ::= { ca 9845 }

    ca OBJECT IDENTIFIER ::= { enterprises 791}
    elmAlertTrapGroup OBJECT IDENTIFIER ::= { elm 3 }
    elmAlertVariables OBJECT IDENTIFIER ::= { elm 2 }
    elmDynamicVariables OBJECT IDENTIFIER ::= { elm 4 }
    elmConformance OBJECT IDENTIFIER ::= { elm 5 }
    elmGroups OBJECT IDENTIFIER ::= { elmConformance 1 }
    elmCompliances OBJECT IDENTIFIER ::= { elmConformance 2 }

    event-datetime OBJECT-TYPE
        SYNTAX DisplayString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
            "The calendar date and time expressed in the event information"
        ::= { elmAlertVariables 65 }
```

```
event-trend OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Trending data for this event."
        ::= { elmAlertVariables 74 }

calmAPIURL OBJECT-TYPE
    SYNTAX OCTET STRING
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "The OPEN API URL which points to the query result."
        ::= { elmDynamicVariables 1 }

elmTrap NOTIFICATION-TYPE
    OBJECTS { event-datetime,event-trend }
    STATUS current
    DESCRIPTION
        "The ELM SNMP Trap."
        ::= { elmAlertTrapGroup 33 }

elmCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
        "The compliance information."
    MODULE -- this module
        GROUP elmDataGroup
        DESCRIPTION
            "This group is mandatory."
        ::= { elmCompliances 3 }
-- units of conformance

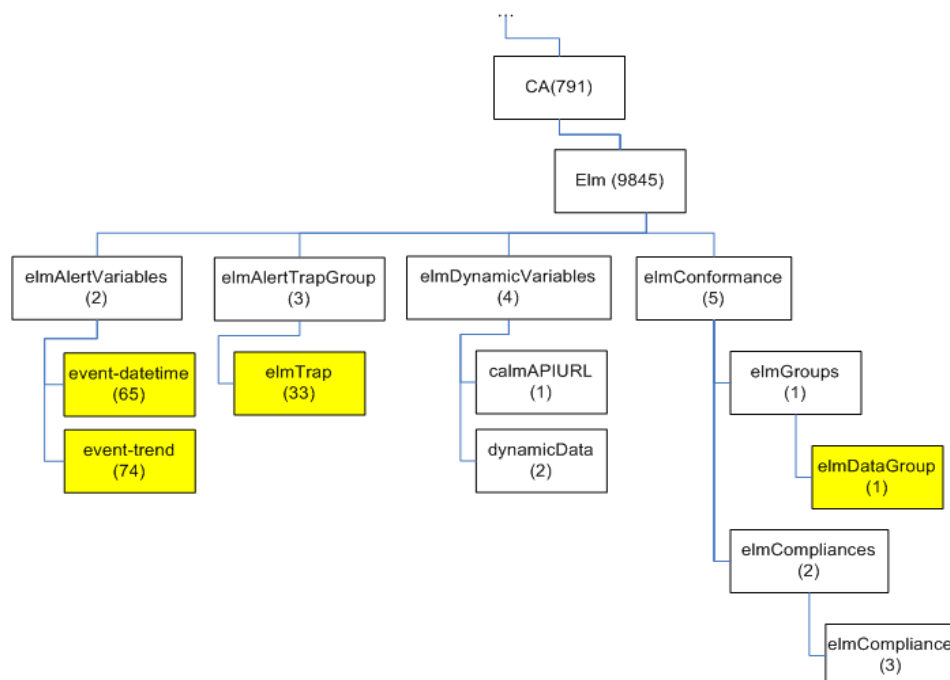
elmDataGroup OBJECT-GROUP
    OBJECTS { event-datetime,event-trend }
    STATUS current
    DESCRIPTION
        "A collection of objects providing information specific to
        ELM data."
        ::= { elmGroups 1 }
END
```

例: カスタム MIB 33 の MIB ツリー

カスタム MIB 用の MIB ツリーは、以下の点で CA-ELM.MIB 用の MIB ツリーとは異なります。

- **elmAlertVariables** の下のオブジェクトは、クエリ内のフィールドに制限されます。以下のフィールドが選択された例を参照してください。
 - event_datetime
 - event_trend
- クエリフィールドのみを含んでいる **elmTrap** は、すべての CEG フィールドを含んでいる CA-ELM.MIB の **elmTrap (1)** を置き換えます。elmTrap が 33 である例を参照してください。この **elmTrap** 識別子は、カスタムトラップ ID 1.3.6.1.4.1.791.9845.3.33 の最終ノードを参照します。

以下の図に、MIB ツリー形式のカスタム MIB 33 を示します。強調表示されたブロックは、このカスタム MIB と CA-ELM.MIB の違いを示しています。カスタム MIB では、**elmAlertVariables** の下に 2 つのフィールドのみが定義されています。カスタム **elmTrap** には 2 つのクエリフィールドのみが含まれ、一意の番号 33 が定義されています。**elmDataGroup** には 2 つのクエリフィールドのみが含まれています。



MIB の使用に関する考慮事項

システムが MIB を使用して CA Enterprise Log Manager から受信する SNMP トラップを理解するには、それを構成しているオブジェクト識別子 (OID) が何を定義しているかを知っている必要があります。そのための要件は以下のとおりです。

- CA-ELM.MIB ファイルをインポートおよびコンパイルし、最新の状態に保ちます。
- (CA NSM のみ) SNMP トラップとして送信されるスケジュールされたアラートごとに 1 つのカスタム MIB を作成し、インポートおよびコンパイルします。

注: クエリに基づくアラートが、トラップとして同じフィールドを同じ順序で送信する場合、それらに対しては同じカスタム MIB を使用できます。

たとえば、以下のクエリはどれも、`dest_hostname` および `event_count` フィールドの値を返します。

- 5 回失敗したシステム アクセス (システム別)
- 過去 7 日間の失敗した復元アクティビティ (ホスト別) サマリ
- 過去 7 日間の失敗したバックアップ アクティビティ (ホスト別) サマリ
- 過去 1 時間の過剰 (25) な設定失敗
- 過去 1 時間の過剰 (25) な設定変更
- 過去 1 時間の過剰 (10) な SU アクティビティ (ホスト別)
- クリティカル ホストでのクリティカルまたは致命的なイベント サマリ

これらのクエリに基づくアラートを個別に作成する場合、それらのアラートは同じカスタムトラップ ID を指定し、同じカスタム MIB を使用して解釈されます。

宛先製品で受信された SNMP トラップを監視する場合は、以下の 2 つの方法で CA Enterprise Log Manager から送信されたトラップを解釈できます。

- トラップ内の送信された URL から SNMP トラップ結果ページを起動します。
- インポートされた MIB を参照するアプリケーションを使用します。

SNMP トラップを使用する手順

SNMP トラップを使用するには、以下の手順が必要です。

1. SNMP トラップを送信できるように CA Enterprise Log Manager を準備します。
 - SNMP トラップのデフォルトの宛先を設定します。
 - SNMP トラップとしてアラートを送信する場合に指定できる追加の各 SNMP トラップ宛先の IP アドレスおよびポートを指定します。
 - CA Spectrum、CA NSM、または別の SNMP トラップ受信先の監視対象となるクエリ結果を含むアラートを指定します。
2. CA Enterprise Log Manager から SNMP トラップを受信できるように SNMP トラップの宛先製品を準備します。
 - CA Spectrum を宛先にする場合は、以下の手順に従います。
 - Spectrum のマニュアルに従って、イベント モデルを作成します。イベント モデルが存在しない場合は、宛先でトラップ結果を表示できません。
 - CA Spectrum が SNMP v3 トラップを受信するように設定します。
 - CA NSM を宛先にする場合は、以下の手順に従います。
 - Windows Server 2003 EE SP1 上に NSM r11.2 GA ビルドをインストールし、パッチを適用して aws_snmpex.dll ファイルを更新します。
 - SNMP v3 トラップを含む SNMP トラップを受信できるように CA NSM を設定します。

3. (オプション) CA Enterprise Log Manager から MIB を使用して SNMP トラップを解釈できるように SNMP トラップ宛先を準備します。

- SNMP トラップの宛先となる製品からアクセスできる場所へ CA Enterprise Log Manager MIB をダウンロードします。

重要: CA-ELM.MIB は、インストール DVD に収められています。CA Enterprise Log Manager 製品ページからこの MIB の最新のバージョンをダウンロードできます。

- CA-ELM.MIB ファイルをインポートおよびコンパイルします。
- (CA NSM のみ) SNMP トラップとして送信されるアラートごとにカスタム MIB を作成し、トラップとして 1.3.6.1.4.1.791.9845.3.x (x は 999 以下の整数) を定義します。すべてのカスタム MIB をすべてインポートおよびコンパイルします。

重要: この手順は任意です。CA Enterprise Log Manager から受信したトラップは、トラップ内の送信された URL からトラップ結果ページを起動することによって解釈できます。

4. SNMP トラップの宛先を使用してアラートをスケジュールします。
5. アラートが SNMP トラップとして正常に送信されたことを確認します。
6. (オプション) 送信された SNMP トラップの結果をトラップ宛先から監視します。
 - トラップ宛先で SNMP トラップ結果を表示します。
 - URL を起動して、アラートによって送信されたチャートまたはグラフ形式のデータを表示します。

SNMP トラップの宛先との統合の設定

レポートサーバのグローバル サービス設定の一部として、SNMP 統合を設定します。設定には 1 つの SNMP トラップの宛先の IP アドレスとポートが含まれます。

CA Enterprise Log Manager から SNMP トラップを受信し解釈できるように宛先製品の準備を行う前後に、SNMP 統合を設定できます。

SNMP トラップの受信者用のアラートを作成する場合、1 つ以上の宛先を指定できます。この設定はデフォルトの設定となります。このデフォルト設定は、レポートサーバでリスト表示されるすべてのサーバに適用されます。

SNMP 統合を設定する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [アラート サービス]をクリックします。
3. SNMP トラップの宛先サーバのホスト名の IP アドレスを入力します。
4. デフォルトのポート「162」を使用するか、この値を変更します。
5. [保存]をクリックします。

アラートから SNMP トラップを受信するための CA Spectrum の準備

CA Enterprise Log Manager からトラップを受信および解釈するネットワーク内の宛先に、SNMP トラップ形式のアラートを送信できます。トラップを受信する各製品には、それぞれ独自の要件があります。

CA Spectrum が CA Enterprise Log Manager アクション アラートからトラップ受信するには、以下の準備を行います。

- CA Spectrum のサウスバウンド ゲートウェイ統合を作成します。これは、CA Enterprise Log Manager が生成した SNMP トラップなど、サードパーティシステムからの任意の受信アラート データ ストリームの形式をサポートできる統合ポイントです。
- CA Enterprise Log Manager ノードのモデルを作成し、SNMP v3 トラップの受信を有効にします。
- CA Enterprise Log Manager MIB をダウンロードします。
- CA Enterprise Log Manager MIB を CA Spectrum にインポートします。

サウスバウンド ゲートウェイ統合を作成するプロセスについては、Spectrum の「Southbound Gateway Toolkit Guide」を参照してください。サウスバウンド ゲートウェイ統合の作成には、SNMP トラップを AlertMap ファイル内の CA Spectrum イベントにマップし、必要なモデルを定義する必要があります。サウスバウンド ゲートウェイの統合ポイントでは、サードパーティシステムからのアラート データを受け付け、OneClick 内にそれを表示します。

Support Online の CA Enterprise Log Manager 製品 ページから MIB ファイルをダウンロードするか、インストール DVD から MIB ファイルを取得したら、CA Spectrum にそれをインポートできます。CA Spectrum OneClick でインポート用の MIB ツールを使用する場合の詳細については、「CA Spectrum Device Management User Guide」を参照してください。

SNMP v3 トラップを受信するための CA Spectrum の設定

CA Enterprise Log Manager から CA Spectrum に SNMP V3 トラップを送信できるようにするには、最初に CA Spectrum に CA Enterprise Log Manager アプリケーションのモデルを作成する必要があります。これによって、SNMP v3 トラップが、モデルを作成した CA Enterprise Log Manager ノードに転送されます。

Spectrum がアクション アラートから SNMP v3 トラップを受信できるようにするモデルの作成方法

1. CA Spectrum がインストールされている Windows サーバにログオンします。
2. Spectrum OneClick コンソールにアクセスします。
 - a. [スタート]メニューから、[すべてのプログラム]-[CA]-[SPECTRUM コントロール パネル]をクリックします。

SPECTRUM コントロール パネルが表示され、画面下部にステータス インジケータが表示されます。
 - b. ステータスに「実行中」と表示されていない場合は、[プロセス制御]の下に[SpectroSERVER の開始]をクリックします。
 - c. ステータスに「実行中」と表示されたら、[OneClick 管理]をクリックします。

OneClick 管理 - SPECTRUM コントロール パネルが表示され、[ホスト]が「localhost」に、[ポート]が「80」に設定されます。
 - d. [OK]ボタンをクリックします。

ログイン ダイアログ ボックスが表示されます。
 - e. 認証情報を入力します。

[Spectrum NFM OneClick]ページが表示されます。
 - f. [コンソールの起動]をクリックします。

ログイン - [SPECTRUM OneClick ログイン]ダイアログ ボックスが表示され、ローカル ホストの SPECTRUM OneClick に接続できます。
 - g. [OK]ボタンをクリックします。

コンソール - SPECTRUM OneClick が表示され、[ナビゲーション]ペイン、[内容]ペイン、および[コンポーネント詳細]ペインが表示されます。

3. [ナビゲーション]ペインの[エクスプローラ]タブで、最上位のノードを展開し、[Universe]を選択します。
[内容]ペインおよび[コンポーネント詳細]ペインのタイトルに、ユニバースタイプのユニバースが表示されます。
4. [内容]ペインで、[トポロジ]タブをクリックします。
タブ上の 2 番目のボタンをクリックすると、タイプ別に新しいモデルを作成し、このビューに追加できます。
5. [モデルの新規作成]をクリックします。
モデルタイプの選択 - [SPECTRUM OneClick]ダイアログ ボックスが表示されます。
6. [すべてのモデルタイプ]タブをクリックします。
7. [フィルタ]フィールドに文字列を入力します。たとえば、「gn」と入力します。
「Gn」で始まるモデルタイプが、リストに表示されます。
8. 目的のモデルタイプを選択し、[OK]をクリックします。たとえば、「GnSNMPDev」を選択し、OK をクリックします。
[タイプ <選択したモデルタイプ> のモデルを作成]が開きます。
9. [タイプのモデルの作成]ダイアログ ボックスを、以下のように完了します。
 - a. [名前]フィールドに CA Enterprise Log Manager サーバのホスト名を入力します。
 - b. [ネットワーク アドレス]フィールドに同じサーバの IP アドレスを入力します。
 - c. デフォルトの「161」が必要なものと異なる場合は、[エージェントのポート]フィールドにポートを入力します。たとえば、「162」と入力します。
 - d. SNMP 通信オプションとして[SNMP v3]を選択します。
 - e. [プロファイル]をクリックします。
[SNMP v3 プロファイルの編集]ウィンドウが開き、既存プロファイルのリストがあれば表示されます。

10. プロファイルを追加するには、以下の手順に従います。

- a. プロファイル名を入力し、ユーザ ID を入力します。
- b. これは **SNMP v3** 用なので、認証タイプとして[プライバシーありで認証]を選択します。
- c. 次の 4 つのフィールドで、8 文字の認証パスワードを 2 回、8 文字のプライバシー パスワードを 2 回入力します。
- d. [追加]をクリックし、リストにプロファイルを追加します。
- e. [OK]をクリックします。

追加したプロファイルが、[タイプのモデルの作成]ダイアログ ボックスの[V3 プロファイル]ドロップダウンリストの一番上に表示されます。

11. [接続の検出]を選択し、[OK]をクリックします。

[モデルの作成]進行状況インジケータが表示されます。処理が完了すると、作成されたモデルが[トポロジ]タブ上にグラフィック形式で、入力したホスト名と選択したモデル タイプと共に表示されます。

CA Enterprise Log Manager MIB のダウンロード

Support Online の CA Enterprise Log Manager 製品ページから MIB ファイルをダウンロードできます。あるいは、インストール DVD から MIB を取得できます。CA Enterprise Log Manager MIB をダウンロードしたら、SNMPトラップの宛先として設定する各製品にその MIB をインポートまたはコンパイルできます。

CA Enterprise Log Manager MIB をダウンロードする方法

1. CA Spectrum をインストールしたサーバにログオンします。
2. CA Support Online を起動してログオンします。
3. CA Enterprise Log Manager の製品ページにアクセスします。
4. ネットワークに CA Enterprise Log Manager MIB ファイルをダウンロードします。
5. SNMPトラップを CA Spectrum に送信する予定である場合は、CA Spectrum に CA Enterprise Log Manager MIB をインポートします。
6. SNMPトラップを CA NSM に送信する予定である場合は、CA NSM に CA Enterprise Log Manager MIB をインポートします。手順については CA NSM のマニュアルを参照してください。

CAELM-MIB の CA Spectrum へのインポート

CA Enterprise Log Manager から CA Spectrum に SNMP トラップを送信する前に、CA Spectrum OneClick MIB ツールを使用して、CA Enterprise Log Manager MIB をインポートおよびコンパイルできます。

注: CA-ELM.MIB で参照される SNMPv2 MIB は、CA Spectrum で事前にロードされています。

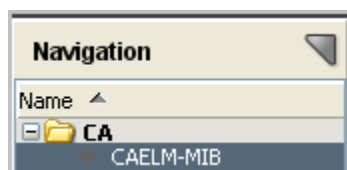
CA Spectrum に CA-ELM.MIB をインポートする方法

1. CA Spectrum にログオンします。
2. OneClick コンソールを起動します。
3. [ツール]、[ユーティリティ]、[MIB ツール]の順にクリックします。
[MIB ツール: MIB を追加]ダイアログ ボックスが開きます。
4. [参照]をクリックし、CA-ELM.MIB をダウンロードした場所へ移動し、このファイルを選択します。
5. [コンパイル]をクリックします。

成功メッセージによって、CA Enterprise Log ManagerMIB が OneClick Web サーバの次のディレクトリに正常に格納されたことが示されます。

<\$SPECROOT>/MibDatabase/userContrib

6. [MIB ツール: MIB を追加]ダイアログ ボックスを閉じます。
CAELM-MIB が CA 下の[ナビゲーション]バーに追加されます。



階層で、cai を展開して、下位のツリー オブジェクトとそれに関連する OID を持つ elm を表示します。

Name	Object ID
cai	1.3.6.1.4.1.791
elm	1.3.6.1.4.1.791.9845
elmAlertVariables	1.3.6.1.4.1.791.9845.2
elmAlertTrapGroup	1.3.6.1.4.1.791.9845.3
elmDynamicVariables	1.3.6.1.4.1.791.9845.4
elmConformance	1.3.6.1.4.1.791.9845.5

例: CA Spectrum への設定変更のアラート通知

初めて CA Spectrum に SNMP トラップを送信する前に、この宛先に関連する結果を返すクエリを識別しておくことをお勧めします。Spectrum を宛先として最初のアラートのスケジュールを設定する場合、進行状況を追跡し、CA Enterprise Log Manager に表示された結果と CA Spectrum のインターフェースに表示された結果を比較することもできます。CA Spectrum へのトラップの送信がルーチンになると、これらの準備を行ったり、再びステップを追跡したりすることがなくなります。

次の例は、次のような初期プロセスを実行することを目的としています。

- SNMP トラップを CA Spectrum に送信するための準備
- SNMP トラップを CA Spectrum に送信する
- SNMP トラップが正常に送信されたかどうかを確認する
- CA Spectrum によって受信された SNMP トラップを表示する

詳細情報:

[CA Spectrum への SNMPv2 トラップの送信](#) (P. 434)

[アラートジョブの進行状況の追跡](#) (P. 437)

[CA Spectrum での SNMP トラップの表示](#) (P. 438)

CA Spectrum への SNMPv2 トラップの送信

以下の例では、SNMPv2 トラップに関する設定変更を CA Spectrum に通知するアラートを作成する方法について説明します。

SNMPv2 トラップを CA Spectrum に送信する方法

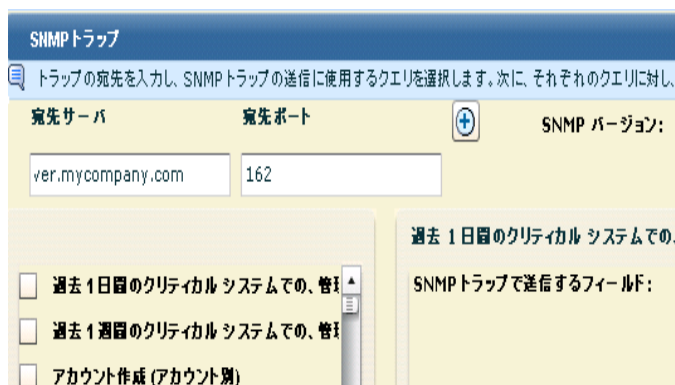
1. アラートのスケジュール ウィザードを開きます。
 - a. [アラート管理] タブをクリックし、[アラートのスケジュール] サブタブをクリックします。
 - b. [アクション アラートのスケジュール] ボタンをクリックします。

2. [アラートの選択]の手順を完了します。
 - a. ジョブ名を入力します。この操作はどのアラートでも必要です。
 - b. [選択タイプ]が[クエリ]であることを確認します。
SNMPトラップの宛先を選択すると、タグに基づいたアラートを送信できません。
 - c. 選択するクエリに「アクション アラート」のタグが付いている場合は、[アクション アラート タグ]をクリックし、表示されたリストをフィルタします。
 - d. 特定したクエリを選択します(複数可)。



3. (オプション)このウィザードのオンライン ヘルプの説明に従って、[アラート フィルタ]、[結果の条件]、および[ジョブのスケジュール]の手順を完了します。
4. SNMPトラップの詳細を設定します。
 - a. [宛先]の手順をクリックします。
 - b. [SNMPトラップ]タブをクリックします。

設定した SNMPトラップの宛先、およびウィザードの手順 1 で選択したクエリが表示されます。



注: デフォルトでは、SpectroSERVER は標準の SNMP トラップ ポート 162 でリスンします。変更した場合、ポートは SS ディレクトリにある SPECTRUM .vnmrc ファイルの snmp_trap_port パラメータと一致させる必要があります。

- c. (オプション)。設定した宛先サーバに加えて最大 9 つのサーバにトラップを送信には、[追加] ボタンをクリックし、サーバの IP アドレスおよびポートを入力します。
- d. トラップにフィールドをすべて含めるクエリの場合は、そのクエリを選択します。

選択したクエリのフィールドが、デフォルトですべて選択されます。選択したクエリの名前が、フィールドリストに表示されます。

- e. トラップに選択したフィールドを含めるクエリの場合は、クエリを選択し、送信しないフィールドをオフにします。

- f. アプリケーションから受信したトラップ用に選択したトラップの宛先でサポートされている SNMP バージョンを選択します。

注: 一部のトラップの宛先では、デバイスによって直接送信される場合はバージョン 3 のトラップを受信しますが、デバイスからイベントを収集するアプリケーションからはバージョン 2 のトラップしか受信しません。この例では、バージョン 2 を受信します。

5. サーバを選択し、クエリ結果を、選択したサーバから結果を返すか、このサーバおよびその子(階層の場合)またはピア(メッシュの場合)連携サーバから返すかを指定します。
6. [保存して閉じる] をクリックします。

ジョブが [アクション アラート ジョブ] に表示されます。ウィザードの最初の手順で [有効] チェック ボックスをオフにしていない場合は、「有効」として ([有効] 列が「true」) 表示されます。簡単な例を次に示します。

アクション アラート ジョブ							
☐	ジョブ名	有効	サーバ	反復	開始時間	終了時間	タイムゾーン
☐	Configuration Changes destined for CA	はい	etr8511f-blade12	5 分	2009-11-20 金曜日 午後 3:43:29		Asia/Calcutta

アラート ジョブの進行状況の追跡

作成したアラート用に選択したクエリによって返された結果を表示できます。例の Configuration_Changes_Alert の結果は、見出し[ホスト]および[数]の下のカ Enterprise Log Manager に表示されます。

- 1. [アラート管理]タブを選択し、[アクション アラート]サブタブを選択します。
- 2. スケジュールしたアラートの名前をクリックします。
- 3. そのアラートの結果を表示します。

結果の例は、以下のとおりです。

アラート名		
Configuration_Changes_Alert	Excessive(25) Configuration Changes in Last Hour	Thu, 25 Jun 2009 14:59:28 EDT
Configuration_Changes_Alert		
Alert name(Configuration_Changes_Alert) Alert created by(su) Federated job(Yes) Tags (Action Alerts) Time Zone (America/New_York) Lists Excessive Configuration Changes (more than 25) in last hour. Rows Returned(1)		
ホスト	数	
ca-elm	2	

CA Spectrum での SNMP トラップの表示

これらのトラップの受信のために作成した CA Spectrum イベント モデルで CA Enterprise Log Manager アラートによって送信された SNMP トラップを表示できます。受信したトラップは、[イベント]タブに表示されます。
Configuration_Changes_Alert の例では、「ca-elm」と「2」という結果が、OID 1.3.6.1.4.1.791.9845.2.22 および 1.3.6.1.4.1.791.9845.2.2 で CA Spectrum に表示されます。

CA Spectrum に SNMP トラップを表示する方法

1. CA Spectrum 認証情報を使用して CA Spectrum にログインします。
2. [Spectrum コントロール パネル]を表示して、Spectroserver を起動します。
Spectroserver が起動します。
3. [OneClick 管理者]をクリックしてログインします。
Spectrum NFM OneClick アプリケーションが表示されます。
4. [コンソールの起動]をクリックします。
Spectrum OneClick コンソールが表示されます。
5. CA Enterprise Log Manager 用に作成したフォルダを展開します。
6. Universe の下にある、CA Enterprise Log Manager から送信されたトラップの受信のために作成したイベント モデルを選択します。
7. 右側のパネルで[イベント]タブを選択し、CA Enterprise Log Manager から送信されたトラップを表示します。
「ca-elm」と「event_count=2」という、CA Enterprise Log Manager で表示したものと同じ値が表示されます。

上記とは関係ありませんが、CA Enterprise Log Manager アラートによって送信された SNMP トラップが CA Spectrum OneClick にどのように表示されるかの例は以下のとおりです。リンクの URL をブラウザに貼り付けることにより、詳細が CEG 形式で表された CA Enterprise Log Manager テーブルを表示することができます。

```

イベント
Trap 6.1 received from unknown SNMP device with IP address 155.35.29.12 and community string 'public'. Trap identifier 1.3.6.1.4.1.791.9845.3.
Trap var bind data:
OID: 1.3.6.1.2.1.1.3.0 Value: 30000
OID: 1.3.6.1.6.3.1.1.4.1.0 Value: 1.3.6.1.4.1.791.9845.3.1
OID: 1.3.6.1.4.1.791.9845.2.65 Value: Tue Sep 22 2009 01:32:30 PM
OID: 1.3.6.1.4.1.791.9845.2.44 Value: epSIM
OID: 1.3.6.1.4.1.791.9845.2.45 Value: etr85111-blade7.ca.com
OID: 1.3.6.1.4.1.791.9845.2.77 Value: Unknown Category
OID: 1.3.6.1.4.1.791.9845.2.75 Value: Unknown Action
OID: 1.3.6.1.4.1.791.9845.2.81 Value: Success
OID: 1.3.6.1.4.1.791.9845.4.1 Value:
https://etr85111-blade7.ca.com:5250/spin/calmap/getObject.csp?type=getQueryViewer&objectId=Subscription/panels/System\_All\_Events\_Detail&params=;Params><Param id=ARG\_stop val=1253606639,'unixepoch"/><Param id=ARG\_start val=1253606339,'unixepoch"/><Param id=ARG\_localtimezone val=Asia/Calcutta"/></Params>

```

詳細情報:

[例: CA Spectrum への設定変更のアラート通知 \(P. 434\)](#)

アラートから SNMP トラップを受信するための CA NSM の準備

CA Enterprise Log Manager からトラップを受信および解釈するネットワーク内の宛先に、SNMP トラップ形式のアラートを送信できます。トラップを受信する各製品には、それぞれ独自の要件があります。

CA NSM がアラートからトラップを受信するには、以下の準備を行います。

- 宛先の CA NSM システムが CA Enterprise Log Manager から SNMP トラップデータを受信するためのシステム要件を満たしていること確認します。
- SNMP v3 のサポートの有効化、さまざまなファイルでのポート割り当ての変更、必要なサービスの開始など、SNMP トラップを受信するための CA NSM の準備を行います

CA NSM がアクション アラートから受信したトラップを解釈するには、以下の準備を行います。

- SNMP トラップとして CA NSM に送信する各アラート用のカスタム MIB を作成します。
- CA-ELM.MIB およびすべてのカスタム MIB をインポートおよびコンパイルします。

CA NSM システム要件

システムが以下の CA Enterprise Log Manager インターフェース要件を満たす場合は、CA NSM に SNMPトラップを送信することができます。

- CA NSM のバージョンが CA NSM r12.2 (GA ビルド) の場合
- CA NSM が Windows Server 2003 EE SP1 にインストールされている場合
- ユーザがパッチ T5MK056.caz を適用済みの場合 (aws_snmpex.dll ファイルが更新され、CA NSM で CA Enterprise Log Manager からの SNMP v3 トラップを受信可能になっている)

パッチを適用する方法

1. パッチを CA サポートからダウンロードします。
2. CA NSM がインストールされているサーバにログオンします。
3. SNMPトラップ サービスを停止します。
 - a. [スタート]メニューから、[プログラム]-[管理ツール]-[サービス]を選択します。
[サービス]リストが表示されます。
 - b. [SNMPトラップ サービス]を選択して右クリックし、ポップアップメニューから[停止]を選択します。
4. すべての CA NSM サービスを停止します。
 - a. コマンドプロンプトを起動します。
 - b. 以下のコマンドを入力します。

```
Unicntrl stop all
```
5. ダウンロードパッチファイル T5MK056.caz を C:¥temp フォルダにコピーします。
6. cazipxp を含むパッチファイルを解凍します。

```
Cazipxp.exe -u T5MK056.caz
```

7. 上書きする前に、既存の `aws_snmpex.dll` をバックアップします。
 - a. `C:\Program Files\CA\SC\CCS\AT\SERVICES\BIN` に移動します。
 - b. `aws_snmpex.dll` を右クリックして、[コピー]を選択します。
コピーされた `aws_snmpex.dll` がフォルダに追加されます。
8. `temp` フォルダから `bin` フォルダ (`C:\Program Files\CA\SC\CCS\AT\SERVICES\BIN`) に `aws_snmpex.dll` をコピーします。
これでシステム要件が満たされたので、CA Enterprise Log Manager から SNMP トラップを受信するよう CA NSM を設定できます。

SNMPトラップを受信するための CA NSM の設定

SNMPトラップとしてアラートを直接 CA NSM に送信できるようにするには、トラップを受信するように CA NSM を設定する必要があります。CA NSM に SNMPv2 トラップと SNMPv3 トラップの両方を送信できます。

CA Enterprise Log Manager アラートから SNMPトラップを受信するように CA NSM を設定する方法

1. CA NSM にログオンします。
2. 次のように SNMP バージョン 3 のサポートを有効にします。
 - a. コマンドプロンプトを開きます。[スタート]メニューから、[実行]をクリックし、`cmd` を入力し、[OK] をクリックします。
 - b. 次のように入力します。
`caogui settings`
[EM の設定]ウィンドウが表示されます。
 - c. [イベント管理]タブをクリックします。
 - d. [SNMP - SNMP バージョン 3 のサポートの有効化]の説明までスクロールして表示します。
 - e. 行を選択し、SNMP の設定の列で「Y」と入力して[はい]を選択し、SNMP バージョン 3 のサポートを有効にします。
 - f. [はい]をクリックして、変更を確定します。
 - g. ウィンドウを閉じます。

3. 次のように、SNMP サービスが使用するポートを、現在のポート(たとえば 5162)からポート 162 に変更します。
 - a. Windows のエクスプローラを開きます。
 - b. .../System32/drivers/etc フォルダに移動します。通常、このフォルダは C:¥WINDOWS の下にあります。
 - c. サービス ファイルをバックアップします。サービスを右クリックし、[コピー]を選択します。
 - d. メモ帳などのテキスト エディタでサービス ファイルを開き、次のようなエントリまでスクロールします。

```
snmptrap    162/udp    snmp-trap    #SNMP trap
```
 - e. snmptrap の行を編集してポート番号 162 を別の値(5162 など)に置換します。ポート 162 を割り当てる catrapmuxd の行を追加します。

```
snmptrap    5162/udp
catrapmuxd  162/udp    catrapmuxd  #CA Trap Multiplexer
```
 - f. ファイルを保存して閉じます。
4. CA Trap Multiplexer 設定ファイル(catrapmux.conf)を次のように変更します。
 - a. C:¥Program Files¥CA¥SC¥CCS¥WVEM¥CAIUSER に移動します。
 - b. メモ帳などのテキスト エディタで、CATRAPMUX.CONF を開きます。
 - c. ファイルの最後までスクロールします。次のエントリを含めるように、必要に応じてファイルを編集します。

```
CATRAPMUX_CMD: 6161
AWS_SNMP: 6162
catrapd: 6163
snmptrap: 5162
```

注: 最初の 3 つのエントリはデフォルト設定を表します。
 - d. ファイルを保存して閉じます。

5. `snmpv3.dat` という設定ファイルに行を追加し、**SNMP v3 セキュリティ パラメータ**を設定します。
 - a. `C:\Program Files\CA\SC\CCS\CommonResourcePackages\Misc` に移動します。
 - b. テキスト エディタで `snmpv3.dat` を開き、ファイルの最後に次の行を追加します。

```
*.*.*.*.* test1234:AuthPriv:MD5:test1234:DES:test1234
```

注: これらは、**SNMPトラップ**を **CA NSM** が受信できるように、アラートウィザードの**[V3 セキュリティ パラメータ]**ダイアログ ボックスに入力する必要があるパラメータと同じパラメータです。ユーザ名とパスワードはここで設定したものです。認証プロトコルは **MD5** で、暗号化プロトコルは **DES** です。

- c. ファイルを保存して閉じます。
6. 次の手順を使用して、**CA Trap Multiplexer** サービスをインストールします。
 - a. コマンド プロンプトを起動します。
 - b. 以下のコマンドを実行します。

```
catrapmuxd uniconfig
```

CA Trap Multiplexer は、ステータスが開始済みのサービスリストに追加されます。

7. **CA Trap Multiplexer** が実行されていることを確認し、**SNMPトラップ サービス**を開始します。
 - a. **[スタート]**メニューから、**[プログラム]-[管理ツール]-[サービス]**を選択します。
[サービス]リストが表示されます。
 - b. **CA Trap Multiplexer** のステータスを確認します。ステータスが**[開始]**であることを確認します。
 - c. **[SNMPトラップ サービス]**を選択して右クリックし、ポップアップ メニューから**[開始]**を選択します。

8. [スタートアップの種類]を[自動]にして、すべてのサービスを開始します。
 - a. コマンドプロンプトを起動します。
 - b. 以下のコマンドを実行します。

```
Unicntrl start all
```

これで、CA NSM は CA Enterprise Log Manager によって送信されたスケジュール済みアラートに基づいて SNMP v3 トラップを受信するように設定されました。

例: CA NSM に対する設定変更のアラート

以下の例では、CA NSM に設定変更のアラートを送信するプロセスを示します。このプロセスには、以下の手順が含まれます。

- CA NSM への SNMP トラップの送信
- SNMP トラップが正常に送信されたことの確認
- CA NSM 上の EM コンソールへのアクセス
- CA NSM で受信された SNMP トラップの表示

CA NSM への SNMPv3 トラップの送信

CA NSM に送信するアラートを計画する場合は、ネットワーク運用センターの監視対象となるクエリ結果を指定します。たとえば、設定変更を検出するクエリを検討します。以下の例では、設定変更詳細クエリに基づいてスケジュールされたアラートを送信する方法を示します。このアラートでは、SNMP トラップ宛先として CA NSM を指定します。

CA NSM に SNMPv3 トラップを送信する方法

1. アラートのスケジュール ウィザードを開きます。
 - a. Analyst または Administrator の認証情報を使用して、CA Enterprise Log Manager にログオンします。
 - b. [アラート管理]タブをクリックし、[アラートのスケジュール]サブタブをクリックします。
 - c. [アクション アラートのスケジュール]ボタンをクリックします。

2. [アラートの選択]の手順を完了します。
 - a. ジョブ名を入力します。たとえば、「CA NSM に送信する設定変更」と入力します。
 - b. 選択タイプがクエリであることを確認します。SNMPトラップの宛先を選択すると、タグに基づいたアラートを送信できません。
 - c. 特定したクエリを選択します(複数可)。たとえば、[設定変更詳細]を選択します。
3. (オプション)このウィザードのオンライン ヘルプの説明に従って、[アラートフィルタ]、[結果の条件]、および[ジョブのスケジュール]の手順を完了します。
4. [宛先]の手順をクリックし、[SNMPトラップ]タブをクリックします。
5. 宛先サーバおよびポートのエントリを確認します。正しくない場合は、宛先サーバおよびポートの正しい IP アドレスを入力します。さらに宛先サーバを追加するには、[追加]をクリックして、追加の宛先を入力します。
6. SNMP のバージョン情報を指定します。デフォルトでは[SNMP Version 2]が選択されます。
 - a. [バージョン 3]をクリックします。CA NSM は SNMP v3トラップを受信するように設定されます。
 - b. [V3 セキュリティ]をクリックします。

[SNMP バージョン 3 セキュリティ パラメータ]ダイアログ ボックスが表示されます。

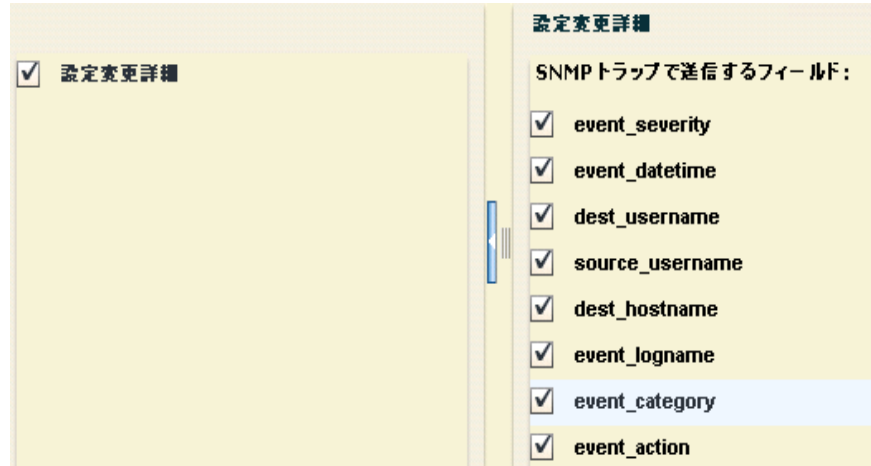
重要: このダイアログ ボックスのエントリは、CA NSM が CA Enterprise Log Manager アラートから SNMPトラップを受信できるように設定した snmpv3.dat の設定と一致する必要があります。推奨される設定は、以下のとおりです。

```
*.*.*.* *.* <ユーザ名>:AuthPriv:MD5:<パスワード>:DES:<パスワード>
```
 - c. [認証]チェック ボックスをオンにします。[ユーザ名]に設定したユーザ名を入力し、[パスワード]に設定したパスワードを入力して、[プロトコル]で[MD5]を選択します。
 - d. [暗号化]チェック ボックスをオンにします。[パスワード]に設定したパスワードを入力し、[プロトコル]で[DES]を選択します。
 - e. [OK]をクリックします。

7. SNMPトラップとして送信するクエリを選択します。

この例では、[設定変更詳細]を選択すると、選択内容に従って、そのクエリのフィールドが表示されます。必要に応じて、トラップから除外するフィールドをすべてオフにすることもできます。

重要: このアラート用のカスタム MIB を作成する場合は、ここで選択するフィールドを以下に示す順序で指定してトラップを定義します。



8. 関連する elmTrap OID の最終ノード x の番号を選択します。すべての elmTrap OID は、1.3.6.1.4.1.791.9845.3.x として定義されます。

カスタムトラップ ID の初期ノードは、CA-ELM.MIB 内にあらかじめ定義されています。最終ノード番号は、カスタム MIB 内に定義されたトラップに固有のもので、トラップは固有のフィールド セットを反映します。カスタム MIB ファイルは、定義した CA Enterprise Log Manager アラートによって送信されるトラップを定義します。カスタムトラップ ID によって参照されるカスタムトラップでは、フィールドはアラートによって送信されるフィールドと同じ順序で表示されます。カスタム MIB 内のトラップ用の OID が

1.3.6.1.4.1.791.9845.3.63 である場合は、カスタムトラップ ID 用のスピナーから 63 を選択します。または、アラートを最初に定義した場合は、選択したクエリフィールドを定義する 1.3.6.1.4.1.791.9845.3.63 のトラップをカスタム MIB に追加します。

9. (オプション) サーバを選択します。

10. [保存して閉じる]をクリックします。

[アクション アラート ジョブ]リストに、設定した名前のジョブが表示されます。

詳細情報:

[CA NSM 上の EM コンソールへのアクセス](#) (P. 448)

アラート ジョブの進行状況の追跡

アラートをスケジュールする際、最初に行われるときのアラート ジョブの進行状況を追跡することをお勧めします。進行状況を追跡すると、ジョブが正常に実行されているかどうか、およびレポートされた結果が送信予定のものになっているかどうかを確認できます。

アラート ジョブの進行状況をモニタし、結果をプレビューする方法

- 1. [アクション アラート ジョブ]リスト上で、作成したアラート ジョブを表示します。一部の例を次に示します。

アクション アラート ジョブ					
☐	ジョブ名	有効	サーバ	反復	開始時間
☐	Configuration Changes destined for CA	はい	etr8511f-blade3	5 分	2009-12-07 月曜日 午後 7:13:30

- 2. (オプション)アラート ジョブの進行状況を追跡するには、[システム自己監視イベント詳細]を表示します。 任意の行をダブルクリックし、[イベントビューア]を表示します。 **result_string** をスクロールして、[結果の説明]に表示されたメッセージ全体を確認します。

アクション	結果	結果の説明
Notification Creation	S	SNMP trap for Action Query [Configuration Change Detail] Alert Name [Configuration Changes destined for CA NSM] on reportServer [etr8511f-blade3] was successful.
Resource Creation	S	Creation of job file while executing action alert for Alert Name [Configuration Changes destined for CA NSM] was Successful.
Alert Creation	S	Run Action Query [Configuration Change Detail] Alert Name [Configuration Changes destined for CA NSM] on reportServer [etr8511f-blade3] was successful.
Resource Modify	S	Update RSSFeed Alert Name [Configuration Changes destined for CA NSM] on reportServer [etr8511f-blade3] recurrence [5 minutes] was successful.
Resource Execution	S	Query [Configuration Change Detail] run over logDepot [localhost] was successful.

- 3. 作成したアラート用に選択したクエリから返された結果をプレビューします。
 - a. [アラート管理]タブを選択し、[アクション アラート]サブタブを選択します。
 - b. スケジュールしたアラートの名前をクリックします。
 - c. そのアラートの結果を表示します。

注: 通常、ここに表示されるデータは、宛先サーバに送信された URL を参照したときに表示されるデータです。両者に違いがあり、同じにする必要がある場合は、アクション アラートを編集し、[結果の条件]の動的終了時間をリセットします。たとえば、「今」「-10 分」に設定します。

CA NSM 上の EM コンソールへのアクセス

CA NSM から CA Enterprise Log Manager によって送信された SNMP トラップを表示できます。SNMP トラップは EM コンソールにメッセージとして表示されます。

CA NSM 上の EM コンソールにアクセスする方法

1. SNMP トラップの宛先であり、CA NSM がインストールされているサーバにログインします。
2. [スタート]メニューから、[プログラム]-[CA]-[Unicenter]-[NSM]-[エンタープライズ管理]-[EM クラシック]の順に選択します。

Windows ウィンドウ用の EM が表示されます。

3. [Windows]をダブルクリックします。
[<ホスト名> (Windows)]ウィンドウが表示されます。
4. [イベント]をダブルクリックします。
[イベント<ホスト名> (Windows)]ウィンドウが表示されます。
5. [Console Log]をダブルクリックします。
[EM コンソール(<ホスト名>)]が表示されます。

詳細情報:

[CA NSM での SNMP トラップの表示](#) (P. 449)

CA NSM での SNMP トラップの表示

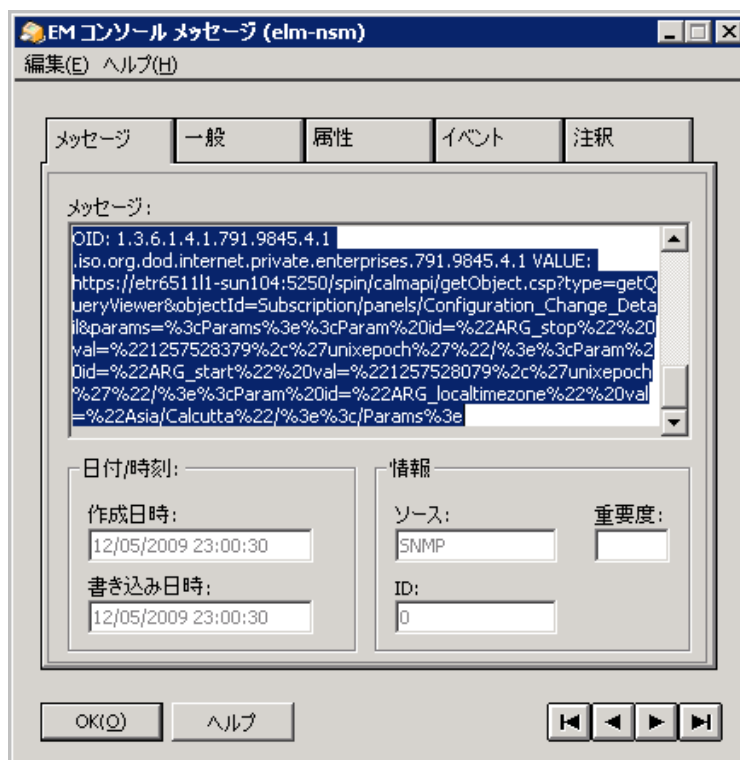
設定変更詳細クエリを実行するようスケジュールされたアラートの例を考えます。この例では、カスタムトラップ ID が 1.3.6.1.4.1.791.9845.3.63 に設定されています。9 つのフィールドが SNMP トラップとして送信されています。

設定変更詳細クエリに基づくアラートによって送信された SNMP トラップを表示する方法

1. SNMP トラップが CA NSM に正常に送信されたことが自己監視イベントによって示されたら、CA NSM 上の EM コンソールにアクセスします。
2. SNMP トラップの受信を示すログメッセージが表示されるまで待ちます。このトラップのメッセージに、カスタムトラップ ID、1.3.6.1.4.1.791.9845.3.63 が含まれています。

```
%CATD_I_060, SNMPTRAP: -u auth user 791 155.35.7.63 etr651111-sun104.ca.com 6 63 0:05:00 12 OID: 1.3.6.1.2.1.1.3.0 system.sys
UpTime.0 VALUE: (30000) 0:05:00.00 OID: 1.3.6.1.6.3.1.1.4.1.0 .iso.org.dod.internet.snmpV2.snmpModules.1.1.4.1.0 VALUE: 1.3.6.1.
4.1.791.9845.3.63 OID: 1.3.6.1.4.1.791.9845.2.80 .iso.org.dod.internet.private.enterprises.791.9845.2.80 VALUE: 2 OID: 1.3.6.1.4.1
,791.9845.2.65 .iso.org.dod.internet.private.enterprises.791.9845.2.65 VALUE: Fri Nov 06 2009 10:53:53 PM OID: 1.3.6.1.4.1.791.9
%CATD_I_060, SNMPTRAP: -u auth user 791 155.35.7.63 etr651111-sun104.ca.com 6 63 0:05:00 12 OID:
```

- このメッセージをダブルクリックし、コピーできる形式でメッセージを表示します。



- メッセージをコピーし、一時テキスト ファイルに貼り付けます。
次のような結果が表示されます。

```
%CATD_I_060, SNMPTRAP: -u auth user 791 155.35.7.63 etr6511l1-sun104.ca.com 6 63  
0:05:00 12
```

以下のデータが SNMP トラップとして受信されるよう指定します。

```
OID: 1.3.6.1.2.1.1.3.0 system.sysUpTime.0 VALUE: (30000) 0:05:00.00
```

100 分の 1 秒単位でアップタイムのオブジェクト ID を指定します。これは SNMP で既知の OID です。

OID: 1.3.6.1.6.3.1.1.4.1.0 .iso.org.dod.internet.snmpV2.snmpModules.1.1.4.1.0
VALUE: 1.3.6.1.4.1.791.9845.3.63

snmpTrapOID のオブジェクト ID を指定します。値は、アラートを設定したときに指定したカスタムトラップ ID です。

OID:
1.3.6.1.4.1.791.9845.2.80 .iso.org.dod.internet.private.enterprises.791.9845.2.80 VALUE: 2

event_severity の OID および重大度の値として「2」を指定します。「2」は「通知」を表わします。

OID:
1.3.6.1.4.1.791.9845.2.65 .iso.org.dod.internet.private.enterprises.791.9845.2.65 VALUE: Fri Nov 06 2009 10:53:53 PM

event_datetime の OID および、これらの値を持つイベントが発生した日時を値(日付)として指定します。

OID:
1.3.6.1.4.1.791.9845.2.17 .iso.org.dod.internet.private.enterprises.791.9845.2.17 VALUE:

dest_username のオブジェクト ID を、値なしで指定します。

OID:
1.3.6.1.4.1.791.9845.2.1 .iso.org.dod.internet.private.enterprises.791.9845.2.1 VALUE:

source_username のオブジェクト ID を、値なしで指定します。

OID:
1.3.6.1.4.1.791.9845.2.22 .iso.org.dod.internet.private.enterprises.791.9845.2.22 VALUE: etr851l2-elm5

dest_hostname のオブジェクト ID を、URL を起動したときにクエリ結果が表示されるサーバのホスト名と共に、指定します。

OID:
1.3.6.1.4.1.791.9845.2.53 .iso.org.dod.internet.private.enterprises.791.9845.2.53 VALUE: EiamSdk

event_logname のオブジェクト ID、および、この詳細が格納されているログ ファイルの名前(EiamSdk)を指定します。

OID:
1.3.6.1.4.1.791.9845.2.77 .iso.org.dod.internet.private.enterprises.791.9845.2.77 VALUE: Configuration Management

event_category のオブジェクト ID、および設定変更詳細クエリと関連付けられたカテゴリの値を指定します。

OID:

1.3.6.1.4.1.791.9845.2.75 .iso.org.dod.internet.private.enterprises.791.9845.2.75 VALUE: Configuration Change

event_action のオブジェクト ID、および設定変更詳細クエリと関連付けられたアクションの値を指定します。

OID:

1.3.6.1.4.1.791.9845.2.81 .iso.org.dod.internet.private.enterprises.791.9845.2.81 VALUE: S

event_result のオブジェクト ID および値として成功を表す「S」を指定します。

OID:

1.3.6.1.4.1.791.9845.4.1 .iso.org.dod.internet.private.enterprises.791.9845.4.1 VALUE:
https://etr651111-sun104:5250/spin/calmap/api/getObject.csp?type=getQueryViewer&objectId=Subscription/panels/Configuration_Change_Detail&params=%3cParams%3e%3cParam%20id=%22ARG_stop%22%20val=%221257528379%2c%27unixepoch%27%22/%3e%3cParam%20id=%22ARG_start%22%20val=%221257528079%2c%27unixepoch%27%22/%3e%3cParam%20id=%22ARG_localtimezone%22%20val=%22Asia/Calcutta%22/%3e%3cParams%3e

elmDynamicVariables 下の calmAPIURL のオブジェクト ID を指定します。値は CA Enterprise Log Manager API への URL です。ログイン後に、クエリ結果をグラフまたはグラフィックビューで確認できます。

5. メッセージの最後にある URL をコピーし、ブラウザに貼り付けて、URL を起動します。
6. CA Enterprise Log Manager API にログオンします。

[設定変更詳細]グラフ ビューが表示されます。以下の例を参照してください。



The screenshot shows a web application window titled "設定変更詳細" (Configuration Change Detail). It includes a search bar with "一致:" and a "実行" (Execute) button. Below is a table with columns: CA 重大度 (CA Severity), 日付 (Date), アカウント (Account), 実行ユ... (Execution User), ホスト (Host), ログ名 (Log Name), カテゴリ (Category), アクション (Action), and 結果 (Result). The table contains one row of data.

CA 重大度	日付	アカウント	実行ユ...	ホスト	ログ名	カテゴリ	アクション	結果
情報	2009-11-20 金曜日 午前 7:27:32			etr65112-elm5	EiamSdk	Configuration Management	Configuration Change	S

アクション アラートを作成する方法

アクション アラートのスケジュール ウィザードを使用してアクション アラートを作成するプロセスは、主に以下の手順で構成されます。

1. アクション アラートのスケジュール ウィザードの表示
2. アラートの基準となるクエリまたはタグの選択 単一のジョブでイベント データベース、インシデントデータベース、またはその両方に対してクエリを実行できます。
3. (オプション)アラートクエリを詳細に定義する詳細フィルタの設定
4. (オプション) 日付範囲と結果の条件の設定
5. (オプション)アラートジョブの反復頻度およびアクティブ化のタイミングの定義
6. (オプション) 自動的なアラート電子メールおよび受信者の設定
7. (オプション) データのクエリを、選択したサーバにのみ実行するか、選択したサーバおよびその子サーバすべてに実行するかを選択

詳細情報:

[アクション アラートのスケジュール ウィザードの表示](#) (P. 454)

[詳細イベントフィルタの作成](#) (P. 572)

[結果の条件の設定方法](#) (P. 489)

[通知の宛先の設定](#) (P. 457)

[アラートジョブ クエリの宛先の定義](#) (P. 462)

アクション アラートのスケジュール ウィザードの表示

アクション アラートジョブを作成するには、アクション アラートのスケジュール ウィザードを起動する必要があります。

アクション アラートのスケジュール ウィザードを表示する方法

1. [アラート管理]タブをクリックします。
[アラート サーバ]リストが表示されます。
2. アラートジョブをスケジュールするサーバを選択します。
[サーバの詳細]ペインに選択したサーバが表示され、デフォルトで[作成済みアラート]タブが表示されます。
3. [アラートのスケジュール]タブをクリックし、[アラートのスケジュール]ボタンをクリックします。

アクション アラートのスケジュール ウィザードが表示されます。

ウィザードを使用する際に

- アクション アラートを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

詳細情報

[電子メール通知の宛先設定](#) (P. 458)

[アラートジョブ クエリの宛先の定義](#) (P. 462)

アラート クエリの選択

新しいアクション アラート ジョブのベースとして、タグまたはクエリを選択します。クエリは、追加されるフィルタと共に、アラートが生成される状況を定義します。たとえば、ホストまたはポートのトラフィックを監視するアラートを作成するには、すべてのイベントに対するクエリを使用し、監視するソース ホストを定義するフィルタを追加して、イベントのしきい値を選択します。

注: アクション アラート クエリ カテゴリには、各種の一般的なアラート要件に合わせて設計されたクエリが含まれています。

アラート クエリの選択方法

1. アクション アラートのスケジュール ウィザードを開きます。
2. ジョブ名を入力します。
3. タイムゾーンドロップダウン メニューから、レポートをスケジュールするタイムゾーンを選択します。
4. タグで、または 1 つ 1 つレポートを選択するために、[タグ]または[クエリ]オプション ボタンのをオンにします。

注: タグでアラートをスケジュールすると、ジョブ自身を変更することなくアラートを追加できます。[ID 管理]タグを選択した場合、そのタグが付けられたアラートはすべて、スケジュール済み実行時間にジョブに追加されます。クエリに[ID 管理]タグを追加することで、ジョブに新しいアラートを追加できます。この機能はカスタム タグにも適用されます。

(オプション) 選択操作の完了後すぐにではなく、後でアクション アラートを有効にする場合は、[有効]チェック ボックスをオフにします。[パスワードを記憶させる]チェック ボックスはデフォルトでオンになっています。

注: 無効な状態のアラート ジョブを作成する機能は、反復アラートで使用するための機能です。ユーザがジョブの[有効]チェック ボックスをオフにして 1 回のみジョブ(「今すぐ」または「一度」のジョブ)を作成すると、作成したジョブがスケジュール済みアラートのリストから削除されます。

5. (オプション) 1 つ以上のタグを選択し、表示されるタグおよび個別レポートを絞り込みます。この機能は、レポートリストの動作と連動します。
6. タグまたは個々のクエリを選択し、シャトル コントロールを使用してそれらを[選択されたクエリ]領域に追加します。単一のアラート ジョブでイベントクエリとインシデントクエリの両方を選択できます。
7. 次に実行するスケジュール手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、アラートジョブがスケジュールされます。それ以外の場合は、選択した手順が表示されます。

詳細情報:

[詳細イベントフィルタの作成](#) (P. 572)

[結果の条件の設定方法](#) (P. 489)

アラートジョブ スケジュール用パラメータの設定

開始時間と終了時間を設定することで、アラートが適用される期間を制御できます。また、クエリが反復される頻度を制御することで、アラート表示の詳細レベルを制御できます。

アラートジョブ スケジュール用パラメータを設定する方法

1. アクション アラートのスケジュール ウィザードを開き、必要な情報を入力して、「ジョブのスケジュール」の手順に進みます。
2. 必要な反復間隔を設定します。間隔が短いと、表示は詳細になりますが、ネットワークトラフィックが増大します。

間隔の設定を短くする前に、CA Enterprise Log Manager が NTP サーバと同期されていることを確認します。

3. アラートジョブに必要な開始時間および終了時間を設定します。
4. 次に実行するスケジュール手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、アラートジョブがスケジュールされます。それ以外の場合は、選択した手順が表示されます。

通知の宛先の設定

アラートの通知用の宛先を、次の中から 1 つ以上設定できます。

■ [電子メール]

アラート用の自動電子メール通知を設定して、しかるべき担当者に自分の職務割り当てや責任に応じたアラートが送信されるようにすることができます。アラート通知電子メールを送信する前に、CA Enterprise Log Manager 環境にメール サーバを設定してください。

■ IT PAM プロセス

サードパーティ製品の通知を必要とする条件でアラートが使用される場合に、指定された CA IT PAM プロセスを実行できます。CA IT PAM との統合はレポートサーバの下で設定する必要があります。また、アラートからプロセスを実行できるようにするには、IT PAM でプロセスを定義する必要があります。

■ SNMP トラップ

1 つ以上のネットワークオペレーション センター (NOC) に、アラートによってキャプチャされたイベント データを送信できます。SNMP v2 または SNMP v3 のトラップを使用すると、CA Spectrum または CA NSM などの管理サーバをターゲットにできます。アラートのスケジュールを設定する手順で宛先を指定します。SNMP を使用してアラートを送信できるようにするには、SNMP との統合を設定しておく必要があります。

注: 宛先を設定しない場合、アラートの結果は RSS フィードのみに公開されます。

詳細情報:

[電子メール通知の宛先設定](#) (P. 458)

[CA IT PAM 情報の設定](#) (P. 459)

[例: CA Spectrum への設定変更のアラート通知](#) (P. 434)

[例: 行ごとに IT PAM プロセスを実行するアラートの送信](#) (P. 400)

[例: クエリごとに IT PAM プロセスを実行するアラートの送信](#) (P. 405)

電子メール通知の宛先設定

アラートジョブ用の自動電子メール通知を設定して、しかるべき担当者に自分の職務割り当てや責任に応じたアラートが送信されるようにすることができます。この手順はオプションです。

アラート通知電子メールを設定するには、事前にメール サーバを CA Enterprise Log Manager 環境用に設定する必要があります。

アラート通知の設定方法

1. アクション アラートのスケジュール ウィザードを開き、必要な情報を入力して、[宛先]の手順に進みます。
2. [電子メール通知を有効にする]チェック ボックスをオンにします。
3. 少なくとも 1 人の受信者電子メール アドレスを入力します。複数のアドレスをカンマで区切って入力できます。
4. (オプション) 通知電子メール用の[差出人]テキスト、件名行、およびメッセージ本文を入力します。

注: メッセージ本文は HTML 形式で作成されるため、入力するすべてのテキストが 1 行で表示されます。1 行の後に改行を入れるためには、テキストの行末に
 を入力します。

詳細情報:

[CA IT PAM 情報の設定](#) (P. 459)

CA IT PAM 情報の設定

アラートの生成時に **CA IT PAM** プロセスを実行するアラート ジョブを設定できます。

クエリ結果行ごとにプロセスを **1** 回実行できます。あるいは、行の数にかかわらず、設定したプロセスを **1** 回実行することもできます。行ごとに **1** 回実行する場合は、**CA IT PAM** にイベント データを渡すサマリと説明のステートメントを **CEG** フィールドを使用して定義します。クエリでデータを収集するために定義したフィールドを選択します。クエリごとに **1** 回実行する場合は、**URL** が自動的に **CA IT PAM** に渡され、起動時にイベント データのすべての行が表示されます。**CA IT PAM** プロセスに応答するサード パーティ製品では、**URL** が、入力したサマリ テキストに追加されます。たとえば、**CA Service Desk** がサード パーティ製品だとすると、**URL** は、**CA Service Desk** の[サマリ]フィールドに表示されます。

アラートの生成時に CA IT PAM プロセスを実行する方法

1. アクション アラートのスケジュール ウィザードを開き、必要な情報を入力して、[宛先]の手順に進みます。
2. [IT PAM プロセス]タブをクリックします。
このアラート ジョブ用の各クエリのチェック ボックスが左ペインに表示されます。
3. **CA IT PAM** プロセスに送信するクエリを選択し、以下のいずれかを実行します。
 - [IT PAM プロセスを行単位で実行]チェック ボックスをオンにして、設定したプロセスを返された行ごとに **1** 回実行します。
 - [IT PAM プロセスを行単位で実行]チェック ボックスをオフにして、返された行の数にかかわらず、設定したプロセスを **1** 回実行します。
4. プロセス パラメータのデフォルト エントリを確認し、必要に応じて変更します。未定義のフィールドで、サマリと説明の情報を入力できる場合は、わかりやすいステートメントを入力します。[IT PAM プロセスを行単位で実行]チェック ボックスをオンにした場合は、**CEG** フィールドを使用してイベント データを渡します。**CEG** フィールドを選択し、ターゲットフィールドの横にある[追加]をクリックします。
5. **CA IT PAM** プロセスがデータ セット内のローカル パラメータとして **CEG** フィールドで定義されている場合は、[フィールド値をパラメータとして送信]リストでそれらの **CEG** フィールドを選択します。
6. 左ペインからの別のクエリを選択し、手順 **3** ~ **6** を繰り返します。

注: スケジュールされたアラートジョブのクエリから結果が返されると、設定したプロセスの実行に必要なすべての情報およびパラメータが CA IT PAM に送信されます。

詳細情報:

[電子メール通知の宛先設定](#) (P. 458)

SNMPトラップ情報の設定

1 つ以上のサード パーティの管理システムにアラートを送信可能なアラート ジョブに **SNMP**トラップ情報を設定することができます。選択したクエリから結果が返されると、すべての選択したクエリから返されたすべての選択したフィールドについてのデータを含むトラップが、すべての選択された **SNMP**トラップ宛先に送信されます。この手順はオプションです。

SNMPトラップ情報を設定する方法

1. アクション アラートのスケジュール ウィザードを開き、必要な情報を入力して、[宛先]の手順に進みます。
2. [SNMPトラップ]タブを選択します。
[SNMPトラップ]タブが開き、[宛先サーバ]と[宛先ポート]のフィールドと、アクション アラートに含まれるクエリのリストが表示されます。それぞれにチェック ボックスが付いています。
3. 宛先サーバおよびポートのデフォルトのエントリを確認します。正しくない場合は、正しい IP アドレスまたは完全修飾ホスト名、およびポート番号を入力します。
4. (オプション) [追加]をクリックして、追加の宛先サーバと宛先ポートを入力します。
5. (オプション) **SNMP v3** を使用するアラートを送信するには、[SNMP Version 3]を選択します。[SNMP Version 2]がデフォルトです。
6. [SNMP Version 3]を選択する場合は、[V3 セキュリティ]ボタンをクリックし、[SNMP バージョン 3 セキュリティ パラメータ]ダイアログ ボックスで認証または暗号化を設定します。

重要: このダイアログ ボックスのエントリは、**CA NSM** が **CA Enterprise Log Manager** アラートから **SNMP**トラップを受信できるように設定した **snmpv3.dat** の設定と一致する必要があります。推奨される設定は、以下のとおりです。

..*.* *.* <ユーザ名>:AuthPriv:MD5:<パスワード>:DES:<パスワード>

- a. [認証]チェック ボックスをオンにします。[ユーザ名]に設定したユーザ名を入力し、[パスワード]に設定したパスワードを入力して、[プロトコル]で[MD5]を選択します。
- b. [暗号化]チェック ボックスをオンにします。[パスワード]に設定したパスワードを入力し、[プロトコル]で[DES]を選択します。

7. SNMPトラップに含める必要があるすべてのクエリの横にあるチェックボックスをオンにします。たとえば、リストに 3 つのクエリが表示されている場合は、SNMP で送信するクエリを 1 つ、2 つまたは 3 つすべてのいずれにも設定できます。

クエリを選択すると、各クエリに含まれるフィールドが、それぞれチェックボックスがオンになった状態で表示されます。任意のフィールドを選択してオフにし、アラートからそのフィールドを削除できます。

8. 各クエリに関連付けるカスタムトラップ ID を入力します。これにより、必要な場合に単一のアラートで異なるクエリを異なるトラップ ID に送信できます。
9. 次に実行するスケジュール手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、アラートジョブがスケジュールされます。それ以外の場合は、選択した手順が表示されます。

詳細情報:

[電子メール通知の宛先設定](#) (P. 458)

[CA IT PAM 情報の設定](#) (P. 459)

アラートジョブ クエリの宛先の定義

アラートジョブによってクエリを実行する、連携されたイベントログストアを選択できます。

レポート先の選択方法

1. アクション アラートのスケジュール ウィザードを開き、必要な情報を入力して、「サーバの選択」の手順に進みます。
2. クエリを実行する使用可能なサーバをすべて選択し、シャトルコントロールを使用して[選択されたサーバ]領域に移動します。
3. (オプション)このアラートジョブの連携クエリを無効にする場合は、[連携されたクエリ]エントリをクリックしたときに表示されるドロップダウンメニューから「いいえ」を選択します。レポートクエリはデフォルトでは連携されています。
4. 次に実行するスケジュール手順に進むか、[保存して閉じる]をクリックします。

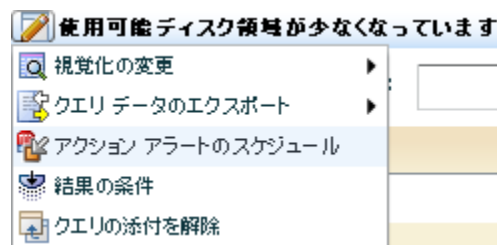
[保存して閉じる]をクリックすると、アラートジョブがスケジュールされます。それ以外の場合は、選択した手順が表示されます。

例：ディスク空き容量低下用のアクション アラートの作成

「使用可能ディスク空き容量の低下」は、「アクション アラート」タグの付いた事前定義済みクエリの 1 つです。アクション アラートタグの付いたクエリは、特にアラートとして使用されることを意図していますが、スケジュールしない限りアラートは生成されません。

以下の例は、事前定義済みの「ディスク空き容量低下」クエリからアクション アラートを生成する方法を示します。

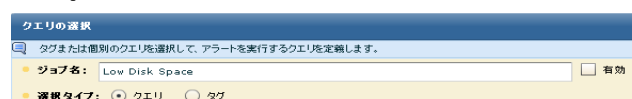
1. [クエリおよびレポート]タブをクリックし、[クエリ]サブタブをクリックします。
[クエリ タグ]ペインおよび[クエリ リスト]ペインが表示されます。
2. [アクション アラート]タグをクリックします。
[クエリ リスト]に、アクション アラートタグが付いたクエリが表示されます。
3. [クエリ リスト]内の[使用可能ディスク領域の減少]クエリをクリックします。
メインのペインに、[使用可能ディスク領域の減少]クエリが表示されます。
4. [オプション]をクリックし、[アクション アラートのスケジュール]を選択します。



アクション アラートのスケジュール ウィザードが、「アラートの選択」手順を選択した状態で表示されます。[選択されたクエリ]で、[使用可能ディスク領域の減少]があらかじめ選択されています。



5. 「ディスク領域の低下」のようなジョブ名を入力します。この時点では[有効]チェック ボックスをオフにします。これにより、作業完了前にアクション アラート スケジュールを保存して閉じても、ジョブが開始される危険性はありません。



6. [アラートフィルタ]を入力またはスキップできます。フィルタは加算式です。すなわち、一連のフィルタが評価される際には、論理演算子の **AND** を使用してフィルタが結合されます。
7. [結果の条件]をクリックし、クエリ定義で設定したものよりも優先させる結果の条件を入力します。
 - a. アラートによって過去 **1 時間**のディスク領域が評価されるよう指定するには、[動的終了時間]で日付範囲として「今」を入力し、[動的開始時間]で「今」および「-1 時間」を入力します。
 - b. クエリによって結果が返されたときにのみ通知されるよう指定し、最初に返された結果のみを表示するには、[行の制限値]チェック ボックスをオンにし、値として「1」を選択します。動的時間帯は時間単位であるため、[時間粒度]として `event_hour_datetime` を選択します。
 - c. このクエリには適用しないので、[グループ化されたイベント数]は空白にしておきます。

日付範囲と結果の条件

このクエリに対する有効な日付範囲および結果の条件を選択してください。

日付範囲の選択

結果として表示するイベントの日付の範囲を選択してください。

事前定義済み範囲: 過去 1 時間

動的終了時間: now

動的開始時間: now, -1 hours

結果

結果の表示パラメータを選択してください。

☒ 行の制限値: 1

☐ その他を表示

☒ 時間粒度: event_hour_datetime

8. [ジョブのスケジュール]をクリックし、スケジュールを定義します。デフォルトでは終了日を指定せず、ジョブをただちに開始します。反復間隔を設定します。たとえば、毎時間クエリを実行するよう間隔を設定します。

スケジュールの定義

同じ日時に開始および停止するようアクション アラートをスケジュールするか、各アラートを個別にスケジュールします。

反復間隔: 1 時間

9. [宛先]手順をクリックします。[電子メール通知を有効にする]チェックボックスをオンにし、[電子メールの宛先]フィールドに電子メールアドレスを入力します。任意で、件名および電子メール テキストを入力します。または、必要な受信者に電子メールを送信し、[差出人]フィールドに送信者の電子メールアドレスを入力します。複数の電子メール アドレスを入力する場合は、カンマ(セミコロンは付加)で区切ります。

電子メール

電子メール アドレスを指定するには、このチェックボックスを選択してください。

☒ 電子メール通知を有効化

電子メールの宛先: username@company.com 開始: username@company.com

件名: Low Disk Space Notification

電子メール テキスト: Disk space has dropped below 20%.

10. [サーバの選択]をクリックします。デフォルトでは、クエリは現在の CA Enterprise Log Manager サーバ上で実行されます。このサーバ上のクエリおよび使用できるすべての連携クエリを実行する場合は[連携]を選択します。
11. [アラートの選択]をクリックします。[有効]を選択します。
12. [保存して閉じる]をクリックします。

アクション アラート ジョブが[アラートのスケジュール]サブタブに表示されます。

アクション アラート ジョブ							
ジョブ名	有効	サーバ	反復	開始時間	終了時間	タイムゾーン	作成者
Low Disk Space	true	caeln5	1 hour	Mon Sep 28 2009 10:12:08 am		America/New_York	nttest

13. [アラート管理]タブ -[アクション アラート]をクリックし、このアクション アラートの結果を表示します。

例: ディスク空き容量低下用のアクション アラートの作成

リクエストしたとおりに、電子メール通知が受信されます。 例を以下に示します。

件名: Low disk space Notification																				
<table border="1"><tr><td colspan="2">CA Log Manager</td></tr><tr><td>RSSリンク</td><td>https://calmrhbuildtest01:5250/spin/calm/getActionQueryResult.csp?id=J-8424346294223181834-calmrhbuildtest011220531049152-3207977576_actionquery_1220536215721</td></tr><tr><td>アラート名</td><td>Low Available Disk Space</td></tr><tr><td>クエリ名</td><td>使用可能ディスク領域が少なくなっています</td></tr><tr><td>生成日</td><td>2009年10月21日 10時27分11秒 EDT</td></tr><tr><td>タグ</td><td>[Action Alerts]</td></tr><tr><td>作成者</td><td>Administrator1</td></tr><tr><td>サーバ</td><td>calmrhbuildtest01</td></tr><tr><td colspan="2">コメント</td></tr><tr><td colspan="2">Disk space has dropped below 20%</td></tr></table>	CA Log Manager		RSSリンク	https://calmrhbuildtest01:5250/spin/calm/getActionQueryResult.csp?id=J-8424346294223181834-calmrhbuildtest011220531049152-3207977576_actionquery_1220536215721	アラート名	Low Available Disk Space	クエリ名	使用可能ディスク領域が少なくなっています	生成日	2009年10月21日 10時27分11秒 EDT	タグ	[Action Alerts]	作成者	Administrator1	サーバ	calmrhbuildtest01	コメント		Disk space has dropped below 20%	
CA Log Manager																				
RSSリンク	https://calmrhbuildtest01:5250/spin/calm/getActionQueryResult.csp?id=J-8424346294223181834-calmrhbuildtest011220531049152-3207977576_actionquery_1220536215721																			
アラート名	Low Available Disk Space																			
クエリ名	使用可能ディスク領域が少なくなっています																			
生成日	2009年10月21日 10時27分11秒 EDT																			
タグ	[Action Alerts]																			
作成者	Administrator1																			
サーバ	calmrhbuildtest01																			
コメント																				
Disk space has dropped below 20%																				

[RSS リンク]をクリックすると、以下のようなページが表示されます。

CA ELM アクション アラート 結果セット		
タイトル: 使用可能なディスク領域の低下		
作成者: Administrator1		
実行日: 2009-12-01 火曜日 午後 4:14:00		
event_hour_datetime	receiver_hostname	dest_objectvalue

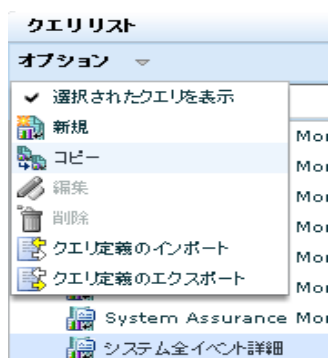
例：自己監視イベント用のアラートの作成

すべての自己監視イベント用の事前定義済みクエリは、「システム全イベント詳細」です。このクエリをコピーし、特定の自己監視イベントに基づくアラートを定義する際のベースとして使用できます。

たとえば、オペレーティング システムを再起動するよう求めるモジュールがサブスクリプション更新でダウンロードされたときに、自己監視イベントが生成されます。この自己監視イベントは、**1** 回だけ生成されます。この自己監視イベントを見落とした場合に備えて、オペレーティング システムの再起動を促すアラートを作成することができます。

以下の例を参考にしてください。

1. 以下の要領で、すべての自己監視イベント用クエリを基にクエリを作成します。
 - a. [クエリおよびレポート] タブをクリックし、[クエリ] サブタブをクリックします。
 - b. [クエリリスト] の [システム全イベント詳細] を選択し、[オプション] ドロップダウンリストを展開して、[コピー] を選択します。



クエリ的设计ウィザードが、[詳細] 手順が選択された状態で表示されます。

- c. コピーされたクエリの名前を新しい名前 (OS 再起動アラートなど) に置き換えます。必要に応じて、ショート ネームおよび新しい説明を追加します。
- d. [使用可能なタグ] から [アクション アラート] を選択し、[選択されたタグ] に移動させます。

2. 以下の要領で、クエリフィルタを作成します。

- a. 「クエリフィルタ」の手順に進みます。[詳細フィルタ]タブをクリックします。
- b. [新規イベントフィルタ]をクリックします。[列]で「event_logname」を選択し、[演算子]を「等しい」のままにし、[値]で「CALM」を選択します。
- c. [新規イベントフィルタ]をクリックします。[列]で「receiver_name」を選択し、[演算子]を「等しい」のままにし、「サブスクリプション」と入力します。
- d. [新規イベントフィルタ]をクリックします。[列]で「result_string」を選択し、[演算子]を「等しい」のままにし、「OS 更新がこのホストにインストールされました。この更新を有効にするために、マシンを再起動してください」というメッセージを入力します。

詳細フィルタ			
フィルタ エントリに条件文を定義して、イベントをフィルタします。			
ロジック	列	演算子	値
(	event_quarterhour_datetime	等しい	CALM
And	receiver_name	等しい	Subscription
And	result_string	等しい	OS Updates are installed on this host. Please restart the machine for these updates to have effect!!
)			

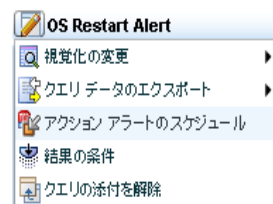
3. [保存して閉じる]をクリックします。

[ユーザ]フォルダ下の[クエリリスト]に、新規アラートが表示されます。



4. 以下の要領で、ユーザ定義クエリのアクション アラートをスケジュールします。

- a. [ユーザ]フォルダでクエリを選択します。
- b. 右側ペインで[編集]ボタンをクリックし、[OS 再起動アラート]ドロップダウンリストを表示して、[アクション アラートのスケジュール]を選択します。



アクションアラートのスケジュールウィザードが、[アラートの選択]手順が表示された状態で表示されます。[選択されたクエリ]の「OS 再起動アラート」が事前に選択されています。

- c. ジョブ名を入力します。たとえば、「オペレーティング システムの再起動アラート」と入力します。
5. 以下の要領で、イベントフィルタを追加します。
 - a. [アラートフィルタ]をクリックします。
 - b. [新規イベントフィルタ]をクリックします。
 - c. [列]で「receiver_hostname」を選択し、[演算子]を「等しい」のままにし、[値]でローカル CA Enterprise Log Manager の名前を入力します。

詳細フィルタ				
フィルタコントロールに条件文を定義して、イベントをフィルタします。				
ロジック	(	列	演算子	値
		receiver_hostname	等しい	caeln6

6. 以下の要領で、再起動が必要な場合にアラートを生成する頻度を指定します。
 - a. [ジョブのスケジュール]をクリックします。
 - b. アラート生成頻度の反復間隔を設定します。たとえば、1 日 1 回の場合は「1」と「日」を選択します。
7. アラートを電子メールで送信するには、以下の要領で、電子メール情報を指定します。
 - a. [宛先]手順をクリックします。
 - b. [電子メール通知を有効化]チェックボックスをオンにし、電子メールアドレスおよびほかの追加情報のうち必要なものを入力します。
8. 以下の要領で、通知を、現在のサーバの再起動が必要な場合に限定します。
 - a. [サーバの選択]をクリックします。
 - b. [連携クエリ]で「いいえ」を選択します。

9. [保存して閉じる]をクリックし、アラートジョブを保存します。

アクション アラートジョブが、[アラート管理]タブの[アラートのスケジュール]サブタブに表示されます。

アクション アラートジョブ						
ジョブ名	▼	有効	サーバ	反復	開始時間	終了時間
Restart Operating System Alert		true	caeln5	1 day	Tue Sep 29 2009 5:13:51 pm	

例：イベントフローの停止時に管理者に電子メールを送信

管理者は、どのエージェント上のどのコネクタがイベントの収集を停止したときにも通知を受け取る必要があります。イベント収集の停止したことがインジケータで示されたときに、この通知を自動化できます。収集サーバが任意のコネクタからイベントを受信してから、インジケータで示されるまでの経過時間を設定できます。経過時間に、目的の分、時間または日数の数値を設定できます。連携内のすべての収集サーバにクエリを拡張できます。

コネクタのダウン時に送信される電子メールの数を制限するには、今までにイベントを収集してきたコネクタだけを考慮します。たとえば、1時間以上前にはイベントを収集したが、この1時間以内にはイベントを収集しなかったコネクタについてのみ行を返すアラートを設定します。

このデータをキャプチャするには、事前定義済みの「ログ マネージャごとの収集 モニタ エージェントコネクタ ダウン」クエリを選択します。アラートの[結果の条件]で定義したとおり、イベントを受信しなかった場合、このクエリはコネクタ名とエージェント名を返します。以下の例を参考にして、1時間～2時間前の期間にイベントを送信したコネクタから1時間以内にイベントを受信しなかった場合にアラートを生成します。アラートの宛先には、通知対象の個人の電子メールアドレスを指定します。クエリの実行スケジュールには、経過時間以上の間隔を指定します。

注: アラートの作成前に、[管理] - [レポート サーバ]以下の[電子メール設定]を設定する必要があります。

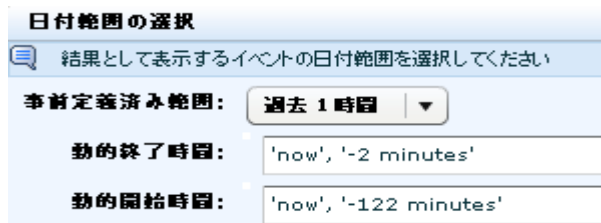
コネクタがイベント収集を停止した際に管理者に電子メールを送信する方法

1. このアラートを実行するサーバを選択します。ハブとスポークのアーキテクチャでは、収集サーバを選択して、できるだけ早く条件をキャプチャできるようにします。
2. [アラート管理]タブを選択し、[アラートのスケジュール]サブタブを選択します。
3. [アクション アラートのスケジュール]をクリックします。
4. 「コネクタ ダウン」などのジョブ名を入力します。
5. [使用可能なクエリ]から[ログ マネージャごとの収集 モニタ エージェント コネクタ ダウン]を選択し、[選択されたクエリ]リストに移動させます。



6. [結果の条件]をクリックします。
7. 時間を過去 2 時間に設定します。
 - a. [事前定義済み範囲]で[過去 1 時間]を選択します。

この選択によって、動的終了時間が「今すぐ」「-2 分」に設定されます。
 - b. [動的開始時間]の[動的な時間文字列の編集]をクリックします。
 - c. 動的な時間文字列で、「62」を「122」に置き換えます。
 - d. [OK]をクリックします。



8. 結果の条件を設定します。
 - a. [次の日付より前で最後にグループ化されたイベント]を選択して、[編集]をクリックします。
 - b. [参照時間]で[今]を選択し、[動的時間文字列に参照時間を追加]をクリックします。
 - c. [時間をシフト]のスピナーを 1 回クリックして「-1」を表示し、ドロップダウンリストから[時間]を選択して、[動的時間文字列に時間のシフトを追加]をクリックします。
 - d. [OK]をクリックします。

結果の条件

グループ化されたイベントの結果の条件を選択します

☐ 次の日付より後で最初にグループ化されたイベント:

☐ 次の日付より後で最後にグループ化されたイベント:

☒ 次の日付より前で最後にグループ化されたイベント: 'now', '-1 hours'

9. [ジョブのスケジュール]の手順をクリックし、反復間隔を定義します。たとえば、間隔を 1 時間に設定します。

スケジュールの定義

同じ日時に開始および停止するようアクション アラートをスケジュールするか、各アラートを個別にスケジュールします

反復間隔: 1 時間

10. [宛先]をクリックし、[電子メール]タブを入力します。
 - a. [電子メール通知を有効化]を選択します。
 - b. [電子メールの宛先]に管理者の電子メール アドレスを入力します。
 - c. [電子メールの送信者]に自分の電子メール アドレスを入力します。
 - d. [件名]フィールドに件名を入力します。たとえば、「コネクタがダウンしている可能性があります」と入力します。
 - e. 電子メール テキストを入力します。たとえば、「過去 1 時間以内にコネクタがイベントの送信を停止しました。」と入力します。

11. [サーバの選択]の手順をクリックし、必要に応じて[連携]をオフにします。
12. [保存して閉じる]をクリックします。

このアラートを、日付範囲に時間ではなく日数を指定してクエリするよう定義し、1日に1回実行されるようスケジュールすることもできます。この場合、動的終了時間は「今すぐ」に、動的開始時間は「今すぐ」「-2」に、[次の日付より前で最後にグループ化されたイベント]は「今すぐ」「-1日」に設定されます。

アクション アラート保持の設定

レポートサーバに保存されるアクション アラートの数および保持期間を制御できます。

アクション アラートの保持条件の設定方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
[サービスリスト]が表示されます。
2. グローバル設定の場合は[レポートサーバ]を、ローカル設定の場合は[レポートサーバホスト]をクリックします。
[レポートサーバの設定]ペインが表示されます。
3. [最大アクション アラート数]エントリフィールドに値を入力します。このしきい値を超えると、アラートが古いものから順に削除されます。
4. [アラート保持]エントリフィールドに日数を入力します。この日数を経過したアクション アラートは削除されます。
注: いずれか一方のしきい値を超えると、アクション アラートは削除されます。
5. [保存]をクリックします。

例: Business_Critical_Sources 用のアラートの作成

Business_Critical_Sources キー設定済みリストを備えたカスタム クエリを作成し、このクエリに基づくアラートをスケジュールできます。このキー設定済みリストには、デフォルト値および関連する事前定義済みクエリやアラートがありません。ガイドとして、以下のエンド ツー エンド プロセスを使用します。

1. エージェントをインストールします。
2. そのエージェント上のコネクタを、各ビジネス クリティカル ソースからイベントを収集するように設定します。

ステータスの詳細		
選択して: 再起動 開始 停止		
選択	コネクタ	エージェント
☐	NTEventLog_コネクタ	USER001LAB.ca.com

3. Business_Critical_Sources ユーザ定義リスト(キー)のホスト名値を定義します。
 - a. [管理]タブをクリックし、[サービス]サブタブをクリックします。
 - b. [サービスリスト]から[レポート サーバ]を選択します。
 - c. [ユーザ定義リスト(キー)]領域の Business_Critical_Sources を選択します。
 - d. [値]領域の[値の追加]をクリックし、ビジネス クリティカル ソースのホスト名を入力します。

キー値	値
Privileged_Groups	USER001LAB
Business_Critical_Sources	

- e. イベントが収集されるビジネス クリティカル ソースごとに、最後の手順を繰り返します。
- f. [保存]をクリックします。

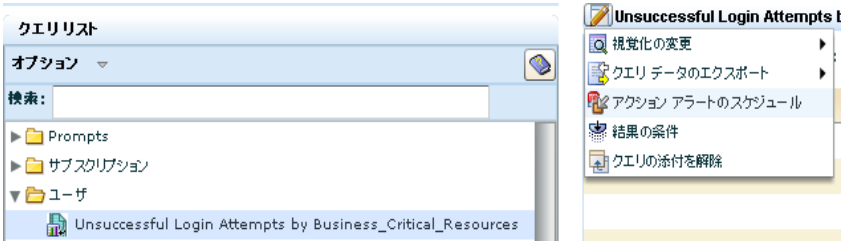
4. ビジネス クリティカル ソースへのログイン試行の失敗に関するクエリを作成します。
- a. [クエリおよびレポート]をクリックします。
 - b. [クエリリスト]下の[検索]フィールドに「ログイン」と入力します。
 - c. [失敗したログイン試行(ホスト別)]を選択し、[オプション]ドロップダウンリストから[コピー]を選択します。
- クエリの設計ウィザードが、[失敗したログイン試行(ホスト別)のコピー]という名前で開きます。
- クエリの名前を、「失敗したログイン試行(Business_Critical_Sources 別)」に変更します。
- d. [クエリフィルタ]手順を選択します。
 - e. [詳細フィルタ]タブをクリックします。
 - f. [新規イベントフィルタ]をクリックします。



- g. [列]で「source_hostname」を選択し、[演算子]で「キー設定済み」を選択して、[値]で「Business_Critical_Sources」を選択します。

列	演算子	値
source_hostname	キー設定済み	Business_Critical_Sources

- h. [保存して閉じる]をクリックします。
5. このカスタム クエリに基づくアラートをスケジュールします。
- a. [クエリおよびレポート]タブをクリックします。
 - b. [クエリリスト]の[ユーザ]フォルダ下にある[失敗したログイン試行(Business_Critical_Sources 別)]を選択します。
 - c. [編集]ドロップダウンリストから「アクション アラートのスケジュール」を選択します。



アクション アラートのスケジュール ウィザードが表示されます。

- d. 「失敗したログイン試行(ビジネス クリティカル リソース別)」のようなジョブ名を入力します。
 - e. [ジョブのスケジュール]をクリックし、スケジュールを定義します。
 - f. 必要に応じて、[宛先]に電子メール オプションを指定します。
 - g. [保存して閉じる]をクリックします。
6. ジョブがスケジュールされていることを確認します。
- a. [アラート管理]タブをクリックし、[アラートのスケジュール]サブタブをクリックします。
 - b. 入力したジョブ名がリスト表示されることを確認します。

アクション アラート ジョブ	
ジョブ名	有効
Unsuccessful Login Attempts by Business Critical Resources	true

7. アラートが生成されるかどうかをチェックします。
- a. [アラート管理]タブをクリックします。[アクション アラート]サブタブが表示されます。
 - b. リスト表示されたアラートを確認し、入力したジョブ名が表示されるかどうかを判別します。

アクション アラートの編集

既存のアクション アラートを編集できます。

アクション アラートの編集方法

1. [アラート管理]タブをクリックします。
[アラート サーバ]リストが表示されます。
2. 編集するアクション アラートがスケジュールされているサーバを選択します。
[サーバの詳細]ペインが表示され、デフォルトで[作成済みレポート]タブが表示されます。
3. [スケジュール済みアラート]タブをクリックし、編集するアラートを選択して、リスト上部の[編集]ボタンをクリックします。
アクション アラートのスケジュール ウィザードが表示されます。
4. 必要な変更を加えて、[保存して閉じる]をクリックします。
[アクション アラート]リストに、編集されたアクション アラートが表示されます。

アクション アラートの無効化または有効化

スケジュールされたクエリを実行するアクション アラートに関連付ける必要がなくなった場合、1 つ以上のアクション アラートを無効にできます。以前に無効にされたアクション アラートを有効にして、保存されたスケジュールに従って実行できます。

アクション アラート ジョブを無効または有効にする方法

1. [アラート管理] タブをクリックし、[アラートのスケジュール] サブタブをクリックします。

[アクション アラート ジョブ] リストが表示され、[有効] 列に各ジョブのステータスが表示されます。ジョブが有効である場合、[有効] の値は **true** になります。ジョブが無効である場合、[有効] の値は **false** になります。

2. 必要なジョブ (複数可) を選択し、[選択済み を有効化] または [選択済み を無効化] をクリックします。

[アクション アラート ジョブ] リストに、有効または無効にされたすべてのジョブの新しいステータスが表示されます。

注: アラート ジョブを無効にする機能は、反復アラートに使用することを目的としています。1 回だけ実行する ([一度] を使用する) 場合にアラート ジョブを無効にすると、そのジョブが [アクション アラート ジョブ] リストから削除されます。

アクション アラートの削除

不要なアクション アラートを削除できます。

アクション アラートの削除方法

1. [アラート管理]タブをクリックします。
[アラート サーバ]リストが表示されます。
2. 削除するアクション アラートが保存されているサーバを選択します。
[サーバの詳細]ペインが表示されます。
3. [スケジュール済みアラート]タブをクリックし、行をクリックして削除するアラートを選択し、リスト上部の[削除]ボタンをクリックします。削除するアラートジョブを複数選択することもできます。

注: 各アラートジョブの横のチェック ボックスは、アラートジョブを有効化/無効化するために使用します。

確認のダイアログが表示されます。

4. [はい]をクリックします。
正常に削除されたことを示すメッセージが表示されます。
5. [OK]をクリックします。
アラートジョブが[アラートジョブ]リストから削除されます。

第 12 章：スケジュール済みレポート

このセクションには、以下のトピックが含まれています。

[作成済みレポートの表示](#) (P. 481)

[作成済みレポートの表示](#) (P. 483)

[レポートジョブをスケジュールする方法](#) (P. 484)

[例：共通のタグを持つレポートのスケジュール](#) (P. 495)

[例：日単位 PCI レポートを PDF として電子メールで送信する](#) (P. 499)

[スケジュール済みレポートジョブの編集](#) (P. 500)

[スケジュールされたレポートジョブの有効化および無効化](#) (P. 501)

[スケジュールされたレポートジョブの削除](#) (P. 502)

[自己監視イベント](#) (P. 502)

[自己監視イベントの表示](#) (P. 503)

作成済みレポートの表示

作成済みレポートは、表示するほかに、任意の場所にコピーを作成することもできます。作成済みレポートは、CA Enterprise Log Manager をインストールしたソフトウェア アプライアンス上の、次のパスに保存されています。

/opt/CA/LogManager/data/reports

作成済みレポートを表示する方法

1. [スケジュール済みレポート] タブをクリックします。

タブが開き、デフォルトでローカル CA Enterprise Log Manager ホストが表示されます。

2. 表示する生成されたレポートがスケジュールされているサーバを選択します。

選択したサーバが詳細ペインに表示されます。

3. 表示されない場合は、[作成済みレポート] タブをクリックします。

[作成済みレポートリスト] が表示されます。

4. 表示するレポートの名前をクリックします。

[保存] ダイアログ ボックスが表示されます。

5. [保存] をクリックし、レポートを保存する場所を指定します。

詳細情報:

[フィルタレポート \(P. 482\)](#)

[作成済みレポートの表示 \(P. 483\)](#)

[レポートジョブをスケジュールする方法 \(P. 484\)](#)

[自己監視イベント \(P. 502\)](#)

フィルタレポート

フィルタを設定し、使用可能な作成済みレポートやスケジュール済みレポートジョブの表示を再設定できます。

作成済みレポートやスケジュール済みレポートのフィルタリング

1. フィルタする定期レポートや作成済みレポートがあるレポート サーバを選択し、[作成済みレポート]タブまたは[スケジュール済みレポート]タブをクリックします。

作成済みレポートまたはスケジュール済みレポートのリストが表示されます。

2. 対応するドロップダウンメニューを使用して、表示されているレポートをフィルタする際の反復やフォーマットのタイプを選択します。

リストに、フィルタ条件を満たすレポートが表示されます。

詳細情報

[作成済みレポートの表示 \(P. 481\)](#)

[作成済みレポートの表示 \(P. 483\)](#)

作成済みレポートの表示

レポートの追跡やレビューなどのために、作成済みレポートに注釈を追加できます。

作成済みレポートに注釈を追加する方法

1. 注釈を追加する作成済みレポートがあるレポート サーバを選択し、[作成済みレポート] タブをクリックします。
[作成済みレポートリスト] が表示されます。
2. 注釈を追加するレポートの横にある[注釈] アイコンをクリックします。
[レポートの注釈] ダイアログ ボックスが開き、以前の注釈が作成者の名前や作成日時と共に表示されます。
3. 必要な注釈を入力し、[保存] をクリックします。
注釈がダイアログ ボックスに表示されます。ダイアログ ボックスは開いたままで、さらに注釈を入力できます。
4. (オプション) 手順 3 を繰り返して、さらに注釈を追加します。
5. 追加すべき注釈がない場合は、[閉じる] をクリックします。
[レポートの注釈] ダイアログ ボックスが閉じます。

詳細情報

[作成済みレポートの表示](#) (P. 481)

[フィルタレポート](#) (P. 482)

レポートジョブをスケジュールする方法

レポートのスケジュールウィザードを使用してレポートジョブを作成するプロセスは、主に以下の手順で構成されます。

1. スケジュールのレポートウィザードの表示
2. レポートテンプレートの選択 - レポートジョブのスケジュール設定を開始するには、ジョブ用のテンプレートとして使用するレポートまたはタグを選択する必要があります。単一のテンプレートやタグ、または複数のテンプレートやタグを選択できます。
3. レポートフィルタの選択 - 必要に応じて、詳細イベントフィルタを適用し、返されるレポートをさらにカスタマイズできます。
4. 日付範囲と結果の条件の設定 - レポートクエリで検索する日付範囲などの条件を設定できます。
5. ジョブのスケジュール - レポートが実行される日時を、1 回限りのレポートおよび反復レポートの両方に設定する必要があります。あらかじめ用意された反復パターンから選択することもできます。
6. レポートフォーマットと宛先の選択 - 必要なレポートフォーマットおよび電子メール配信オプションを選択できます。
7. サーバの選択 - レポートの照会先のサーバを選択し、さらにサーバの連携ホストを照会するかどうかを選択する必要があります。

レポートのスケジュール ウィザードの表示

1 つ以上の反復レポートのレポート ジョブを新規作成するには、レポートのスケジュール ウィザードを起動する必要があります。

レポートのスケジュール ウィザードを表示する方法

1. [スケジュール済みレポート] タブをクリックします。
[レポート サーバ] リストが表示されます。
2. レポートをスケジュールするサーバを選択します。
[レポート サーバの詳細] ペインに選択したサーバが表示され、デフォルトで[作成済みレポート] タブが表示されます。
3. [レポートのスケジュール] タブをクリックし、[レポートのスケジュール] をクリックします。

レポートのスケジュール ウィザードが表示されます。

ウィザードを使用する際に

- スケジュール済みレポートを保存してウィザードを閉じるには、[保存して閉じる] をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット] をクリックします。

詳細情報

[スケジュール用パラメータの設定](#) (P. 493)

[詳細イベントフィルタの作成](#) (P. 572)

[結果の条件の設定方法](#) (P. 489)

[レポートクエリ ターゲットの選択](#) (P. 495)

レポートの選択

レポートジョブを作成する最初の手順は、レポートテンプレートの選択です。同じフィルタ、スケジュール、および宛先設定を共有する複数のレポートジョブをスケジュールする場合は、複数のレポートやタグをテンプレートとして選択します。

複数のレポートを選択した場合、ジョブはレポート別に表示されます。たとえば、2つの個別レポートを選択した場合、両者は同じスケジュール フィルタ オプションを共有しますが、[作成済みレポート]リストに、レポート名をタイトルとして、別々に表示されます。

Administrator ロールを持つユーザは、後で使用するためにレポートジョブを無効な状態で作成できます。**Administrator** ロールと **Analyst** ロールを持つユーザであれば、ジョブの有効化と無効化を後から切り替えることが可能です。[スケジュール済みレポート]タブを表示すると、無効な状態になっているレポートの[有効]列には、値として **FALSE** が表示されます。

レポート テンプレートを選択する方法

1. ジョブ名を入力します。
2. タイムゾーンドロップダウン メニューから、レポートをスケジュールするタイムゾーンを選択します。
3. タグで、または 1 つ 1 つレポートを選択するために、[タグ]または[レポート]オプション ボタンのをオンにします。

注: タグでレポートをスケジュールすると、ジョブ自身を変更することなくレポートを追加できます。「ID 管理」タグを選択した場合、そのタグが付けられたレポートはすべて、スケジュール済み実行時間にジョブに追加されます。この機能はカスタム タグにも適用されます。

4. (オプション) 1 つ以上のタグを選択し、表示されるタグおよび個別レポートを絞り込みます。この機能は、レポートリストの動作と連動します。
5. (オプション) [有効]チェック ボックスをオフにし、このレポートジョブを無効の状態で作成します。[有効]チェック ボックスはデフォルトでオンになっています。

注: 無効な状態のレポートジョブを作成する機能は、反復レポートで使用するための機能です。ユーザがジョブの[有効]チェック ボックスをオフにして 1 回のみジョブ(「今すぐ」または「一度」のジョブ)を作成すると、作成したジョブがスケジュール済みレポートのリストから削除されます。

6. (オプション) レポートを生成した後もレポート設定を保持するには、[実行後に保持]チェック ボックスを選択します。

注: レポートの生成後、レポートテンプレートを編集し、そのレポートを再スケジュールすることができます。

7. レポートテンプレートとして使用するタグまたは個別レポートを選択し、シャトル コントロールを使用してそれらを[選択されたレポート]領域に追加します。
8. 次に実行するスケジュール手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、レポートがスケジュールされます。それ以外の場合は、選択した手順が表示されます。

詳細フィルタの使用

SQL ベースの詳細フィルタを使用すると、イベント ログ ストアにクエリを実行するすべての機能の条件を指定し、クエリの絞り込みやクイック フィルタのカスタマイズを行うことができます。[詳細フィルタ]インターフェースでは、フィルタ要件に応じてロジック、列、演算子、および値を入力する形式を指定することによって、適切なフィルタ構文を作成できるようにします。

注: このセクションには、詳細フィルタに使用される SQL 用語の概要が含まれています。詳細フィルタの機能を十分に活用するには、SQL および共通イベント文法を完全に理解しておく必要があります。

以下の SQL 条件は、複数のフィルタ ステートメントを結合します。

AND

結合されたすべての用語が **TRUE** の場合は、イベント情報を表示します。

OR

結合された用語のいずれかが **TRUE** の場合は、イベント情報を表示します。

HAVING

条件文を追加することによって、メインの SQL 文の条件を絞り込みます。たとえば、特定のホストからのイベント用に詳細フィルタを設定している場合に、「having」ステートメントを追加して、このホストからのイベントのうち指定した重大度のものだけを返すようにすることができます。

以下の SQL 演算子は詳細フィルタによって使用され、基本条件を作成します。

関係演算子

列が入力した値と適切な関係を保持する場合は、イベント情報を表示します。次の関係演算子を使用できます。

- 等しい
- 等しくない
- < (より小さい)
- > (より大きい)
- ≤ (以下)
- ≥ (以上)

たとえば、[> (より大きい)]を使用すると、設定した値よりも大きい値の選択列からイベント情報が含まれます。

に近い

入力したパターンが列に含まれている場合に、%を使用して該当するパターンを設定し、イベント情報を含めます。たとえば、L% は L で始まる任意の値を返しますが、%L% は L が最初の文字にも最後の文字にも含まれない任意の値を返します。

に近くない

列に指定したパターンが含まれていない場合にイベント情報を含めます。

設定が含まれている

引用符で囲まれた一連の入力値のうち、1 つ以上が対象の列に含まれている場合に、イベント情報を含めます。セット内に複数の値がある場合は、カンマで区切る必要があります。

設定が含まれていない

引用符で囲まれた一連の入力値のうち、1 つ以上が対象の列に含まれていない場合に、イベント情報を含めます。セット内に複数の値がある場合は、カンマで区切る必要があります。

一致する例

入力した 1 つ以上の文字に一致する任意のイベント情報を含め、キーワードの検索を可能にします。

キー設定済み

レポート サーバの設定中にキー値として設定したすべてのイベント情報を含めます。ビジネス上の関連性など、組織のグループを設定する際にキー値を使用できます。

キー未設定

レポート サーバの設定中にキー値として設定していないすべてのイベント情報を含めます。ビジネス上の関連性など、組織のグループを設定する際にキー値を使用できます。

結果の条件の設定方法

クエリに日付の範囲およびその他の結果の条件(行の制限や基本の表示時間など)を設定することができます。結果の条件は、クエリの実行時間までであればいつでも変更できるため、ベースクエリやフィルタを変更することなくクエリを変更する便利な手段として利用できます。

以下のタイプの結果の条件を設定できます。

- クエリの検索期間を制御する日付範囲条件
- 最大行数などの表示条件
- 特定の日付以降最も新しくグループ化されたイベントや、設定した数のイベントを含むグループ化されたイベントなど、グループ化されたイベントの条件

注: クエリを作成する際に少なくとも 1 列がグループ化されていなければ、クエリ表示から結果の条件を編集することはできません。

時間または日付範囲の設定

クエリの時間または日付範囲の条件を設定できます。これにより、検索対象となるイベント ログ ストアの範囲が絞り込まれ、クエリ効率が向上します。

事前定義済み時間範囲を使用するか、またはカスタム時間範囲を作成できます。カスタム時間範囲が適切に機能するように、開始時間と終了時間の両方を設定する必要があります。単にワントタイム パラメータを設定する場合、この条件はクエリ SQL の「Where」句で指定します。

結果の条件を設定する方法

1. [結果の条件] ダイアログ ボックスを開きます。
2. ドロップダウンリストから、事前定義済み時間範囲を選択します。たとえば、昨日受信したイベントを表示する場合は、「前日」を選択します。

注: アクション アラートまたはスケジュール済みレポートを作成する場合、インターフェースには以下のデフォルトの時間範囲が表示されます。

- アクション アラート: 過去 5 分
- スケジュール済みレポート: 過去 6 時間

3. (オプション) 以下のサブ手順を使用して、カスタム時間範囲を作成します。
 - a. [日付範囲の選択] 領域の[動的終了時間] エントリ フィールドの横にある[編集]をクリックします。クリックすると、クエリの検索対象とする期間の終了時間を設定できます。

[動的時間の指定] ダイアログ ボックスが表示されます。
 - b. パラメータのベースに使用する参照時間を選択し、[追加]をクリックします。
 - c. 必要な時間パラメータを選択し、[OK]をクリックします。複数の時間パラメータを追加できます。
 - d. パラメータの追加が完了したら、[OK]をクリックします。

[動的時間の指定] ダイアログ ボックスが閉じられ、選択した値が[動的終了時間] 領域に表示されます。複数のパラメータを入力した場合、各パラメータが先頭から参照され、それらのパラメータから終了時間のステートメントが生成されます。たとえば、[動的終了時間] 領域で[月初]を追加し、[曜日]に[火曜日]を設定すると、その月の最初の火曜日にクエリが終了します。

注: 「日数」や「時間数」のような数値を使用する場合、過去の時間を設定するには、負の数字を入力する必要があります。正の数字を使用すると将来の終了時間が設定され、少なくとも 1 つの評価されたイベントがログストアにある限り、クエリは結果を送信し続けます。

たとえば、[動的開始時間]領域で[今すぐ]を追加し、[分数 - 10]と設定すると、選択した終了期間の 10 分前にクエリが実行されます。

- e. クエリの検索期間の開始時間を設定するには、[動的開始時間]領域で手順 2 を繰り返します。

日付範囲を入力しない場合、クエリはログストア内のすべてのイベントに適用されます。

- 4. 矢印をクリックして次に完了するクエリ的设计の手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックした場合は、新しいクエリがクエリリストに表示されます。それ以外の場合は、選択したクエリ的设计の手順が表示されます。

詳細情報

[結果の条件の設定方法](#) (P. 489)

[表示とグループの条件の設定](#) (P. 492)

表示とグループの条件の設定

クエリの表示を制御する条件と、グループ化の方法に基づいてイベントを検索する条件を設定できます。

表示とグループの条件を設定する方法

1. [結果の条件]ダイアログ ボックスを開きます。
2. [結果]チェック ボックスを使用して、必要な以下の表示条件を有効にします。

[行の制限値]

クエリが最新のイベントから表示するイベントの最大行数を設定します。

最小: 1

最大: 5000

[その他を表示]

最大行数を超えたために表示されていない結果があることを示します。これにより、該当するタイプのすべてのイベントのコンテキストで選択したイベントを比較できます。たとえば、イベントビューア表示について [行の制限値] で「10」を選択し、[その他を表示]を選択した場合は、10を超える残りのイベントはすべて、[その他]というタイトルの 1 つのエントリとして表示されます。この設定は、行の制限値を選択したときのみ有効です。

[時間粒度]

クエリ表示で使用される[期間]フィールドの詳細レベルを設定します。

3. [結果の条件]を使用して、さまざまなタイプのグループ化されたイベント条件がクエリされます。たとえば、選択した日付以降の最新のグループ化されたイベントや特定数のグループ化されたイベントを検索するように、クエリを設定することもできます。グループ化されたイベントは、クエリの作成手順で機能およびグループの順序を設定した、精製済みイベントです。

グループの条件では、時間範囲フィールドと同じ時間ステートメント体系を使用します。

4. 矢印をクリックして次に完了するクエリ的设计の手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックした場合は、新しいクエリがクエリリストに表示されます。それ以外の場合は、選択したクエリ的设计の手順が表示されます。

詳細情報

[結果の条件の設定方法](#) (P. 489)

スケジュール用パラメータの設定

スケジュール済みレポートを実行する時間、反復の有無、および反復の間隔を制御できます。

スケジュール用パラメータの設定方法

1. レポートのスケジュール ウィザードを開き、「ジョブのスケジュール」の手順に進みます。
2. [繰り返しなし]または[繰り返し]ラジオ ボタンを使用して、レポートの作成時間と、必要に応じて反復パターンを選択します。

注：環境内でサマータイムを使用している場合は、切り替え時間にレポートをスケジュールしないでください。この時間にスケジュールすると、レポートは作成されません。たとえば、サマータイムが3月8日の午前2時に開始する場合、2:00:00 から 2:59:59 の間はレポートをスケジュールすることはできません。

3. 次に実行するスケジュール手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、レポートがスケジュールされます。それ以外の場合は、選択した手順が表示されます。

詳細情報

[詳細フィルタの使用](#) (P. 487)

[結果の条件の設定方法](#) (P. 489)

[レポートクエリターゲットの選択](#) (P. 495)

フォーマットと通知の設定の選択

レポートを、PDF、Excel、XML のいずれのフォーマットで生成するかを選択できます。また、自動電子メール通知を設定できます。

フォーマットと通知の設定方法

1. レポートのスケジュール ウィザードを開き、「宛先」の手順に進みます。
2. [レポートフォーマット]ドロップダウン メニューから目的のフォーマットを選択します。

注: PDF 形式の場合、軸のラベルを見やすくするため、グラフに表示できるデータ ポイント数は最大 **100** に制限されています。表示するグラフのデータ ポイントが **100** を超えている場合、**CA Enterprise Log Manager** で発行された PDF には、最初の **100** ポイントのみが表示されます。

3. レポートが生成されるときに通知を送信する場合は、[電子メール]チェックボックスをオンにします。

[電子メールの詳細]フィールドが表示されます。

4. 通知を受信するユーザの電子メール アドレスを入力します。複数のアドレスは、カンマを使用して区切ります。
5. (オプション) 件名、返信先電子メール、アドレス、本文テキストなど、その他の詳細を入力します。
6. (オプション) 通知電子メールに、選択したフォーマットでレポートのコピーを添付するには、[レポートの添付]を選択します。
7. 次に実行するスケジュール手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、レポートがスケジュールされます。それ以外の場合は、選択した手順が表示されます。

詳細情報:

[詳細フィルタの使用](#) (P. 487)

[結果の条件の設定方法](#) (P. 489)

[スケジュール用パラメータの設定](#) (P. 493)

[レポートクエリターゲットの選択](#) (P. 495)

レポート クエリ ターゲットの選択

レポート クエリが検索対象とする連携されたイベント ログ ストアを選択できます。

レポート先の選択方法

1. レポートのスケジュール ウィザードを開き、「サーバの選択」の手順に進みます。
2. クエリを実行する使用可能なサーバをすべて選択し、シャトル コントロールを使用して[選択されたサーバ]領域に移動します。
3. (オプション)このレポートの連携クエリを無効にする場合は、[連携されたクエリ]エントリをクリックしたときに表示されるドロップダウン メニューから「いいえ」を選択します。レポート クエリはデフォルトでは連携されています。
4. 次に実行するスケジュール手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、レポートがスケジュールされます。それ以外の場合は、選択した手順が表示されます。

詳細情報

[詳細フィルタの使用](#) (P. 487)

[結果の条件の設定方法](#) (P. 489)

[スケジュール用パラメータの設定](#) (P. 493)

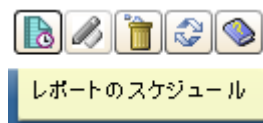
例：共通のタグを持つレポートのスケジュール

終了日と間隔を指定して作成した 1 つ以上のレポートをスケジュールできます。

Auditor、Analyst、および Administrator が、レポートをスケジュールできます。

レポートのスケジュール方法

1. [スケジュール済みレポート]タブをクリックし、[レポートのスケジュール]サブタブをクリックして、[レポートのスケジュール]をクリックします。



レポートのスケジュール ウィザードが、手順 1 の「レポートの選択」が選択された状態で表示されます。



2. ジョブ名を入力し、[レポート]をクリックしてレポートを個別に選択できるようにするか、[タグ]をクリックして、指定したタグに関連付けられたすべてのレポートを選択できるようにします。

以下の例では、[リソース アクセス]タグを選択すると、このタグが付けられた 6 つのレポートを簡単に選択できます。

3. (オプション) [レポートフィルタ]をクリックし、レポートを必要なデータのものに制限するためのイベントフィルタを新規作成します。

- (オプション) [結果の条件]をクリックし、このクエリの日付範囲か結果の条件、あるいはその両方を選択します。たとえば、最近 6 時間以内に発生したイベントを検索する場合は、[動的終了時間]で「今」を選択し、[動的開始時間]で「今」および「-6 時間」を選択します。[行の制限値]を選択し、250 などの数を選択します。

クエリ結果の条件 - System Self Monitoring Events Detail

クエリフィルタは、クエリのデフォルト フィルタを上書きします。これは現在表示中のレポートにのみ適用されます

日付範囲と結果の条件

このクエリに対する有効な日付範囲および結果の条件を選択してください

日付範囲の選択

結果として表示するイベントの日付範囲を選択してください

事前定義済み範囲: []

動的終了時間: 'now' [] []

動的開始時間: 'now' '-6 hours' [] []

結果

結果の表示パラメータを選択してください

☐ 行の制限値: 1 [] []

☐ その他を表示

☐ 時間粒度: event_datetime []

結果の条件

グループ化されたイベントの結果の条件を選択します

☐ 次の日付より後で最初にグループ化されたイベント: [] [] []

☐ 次の日付より後で最後にグループ化されたイベント: [] [] []

☐ 次の日付より前で最後にグループ化されたイベント: [] [] []

☐ 最小数: 1 [] [] (グループ化されたイベント数)

☐ 最大数: 1 [] [] (グループ化されたイベント数)

- [スケジュール済みジョブ]を選択して今すぐ生成を行うようスケジュールするか、別のオプションを選択し、詳細を指定します。

6. [宛先]をクリックし、Excel スプレッドシート、PDF、XML のいずれのフォーマットでレポートを作成するかを指定します。スプレッドシートは表データに適しています。PDF はグラフィックに適しています。任意で、電子メール通知を送信できます（電子メール アドレス間の区切り文字にはカンマを使用します）。レポートを添付せずに、スケジュール済みレポートが作成されたことを通知するためだけ電子メールを送信することも、電子メールの添付ファイルとしてレポートを送信することも可能です。

レポート先

電子メール アドレスを指定するには、このチェックボックスを選択してください。

レポート フォーマット: PDF ▼

☒ 電子メール通知を有効化

● 電子メールの宛先: 開始:

件名:

電子メール テキスト:

レポートの添付: ☐

注: 管理者は、レポートが、指定した保存期間の経過後に削除されるように設定できます。電子メール コピーの保存は、手動によるアーカイブに代わるバックアップ手段として使用できます。

7. [サーバの選択]をクリックし、レポートするサーバを 1 つ以上選択し、そのサーバの連携にもクエリを実行するかどうかを指定します。
8. [保存して閉じる]をクリックします。

選択したレポートの作成がスケジュールされます。

スケジュール済みジョブ				
ジョブ名	サーバ	タイプ	スケジュール済み時刻	作成者
All Resource Access Reports	caelm5	タグ	Mon Sep 28 2009 9:33:57 am	admin

例：日単位 PCI レポートを PDF として電子メールで送信する

指定したレポートを、選択したフォーマットで、指定した相手に必要な間隔で自動的に送信することができます。

スケジュール済みレポートを PDF としてフォーマット設定し、電子メールに添付するには、[管理]タブの[サービス]サブタブ下にある[レポート サーバのグローバル サービス設定]で、以下のとおりに設定する必要があります。

- メール サーバ オプション：
 - メール サーバ
 - SMTP ポート(25)
 - 管理者電子メール
 - SMTP ユーザ名およびパスワード
- PDF の仕様：
 - 企業/製品名
 - 企業/製品ロゴ URL
 - ヘッダ フォントおよびフォント サイズ
 - データフォントおよびフォント サイズ
 - 用紙の向き、幅、および高さ

例：すべての日単位 PCI レポートを PDF として平日に監査担当者の受信トレイに送信する

1. [スケジュール済みレポート]タブをクリックし、[レポートのスケジュール]サブタブをクリックします。

ツールバーに、[レポートのスケジュール]ボタンが表示されます。

2. [レポートのスケジュール]をクリックします。
[レポートの選択]手順が表示されます。

3. 以下の要領で、レポートを選択します。
 - a. [ジョブ名]に「PCI レポート」と入力します。
 - b. [選択タイプ]で「タグ」を選択します。
 - c. [使用可能なタグ]から「PCI」を選択し、[選択されたタグ]に移動させます。

4. 以下の要領で、ジョブをスケジュールします。
 - a. [ジョブのスケジュール]手順をクリックします。
 - b. [繰り返し]の下で「日単位」を選択します。
 - c. 「平日」を選択します。
5. 以下の要領で、レポート先およびフォーマットを指定します。
 - a. [宛先]タブをクリックします。
 - b. デフォルトのレポートフォーマットを「PDF」のままにします。
 - c. [電子メール通知を有効化]を選択します。
 - d. 監査担当者の電子メール アドレスを入力します。次の構文を使用します: <email_name>@<company>.com
 - e. [レポートの添付]を選択します。
6. [保存して閉じる]をクリックします。

スケジュール済みレポート ジョブの編集

スケジュール済みレポートジョブを編集できます。

スケジュール済みレポート ジョブの編集方法

1. [スケジュール済みレポート]タブをクリックします。
[レポート サーバ]リストが表示されます。
2. 編集するレポートがスケジュールされているサーバを選択します。
選択したサーバが[レポート サーバの詳細]ペインに表示されます。
3. 編集するレポートを選択し、リスト上部の[編集]ボタンをクリックします。
レポートのスケジュール ウィザードが表示されます。
4. 必要な変更を行い、[保存して閉じる]をクリックします。
5 分以内にリストがリフレッシュされ、編集したレポートが[スケジュール済みジョブ]リストに表示されます。すぐに表示するには、[リフレッシュ]をクリックします。

詳細情報:

[レポートジョブをスケジュールする方法 \(P. 484\)](#)

[スケジュールされたレポートジョブの削除 \(P. 502\)](#)

スケジュールされたレポート ジョブの有効化および無効化

レポートに関連付けられたクエリを実行する必要がなくなった場合、1 つ以上のスケジュールされたレポートを無効にできます。また、以前に無効にされたスケジュール済みのレポート ジョブを有効にして、保存されたスケジュールに従って実行できます。

スケジュールされたレポートジョブを無効または有効にする方法

1. [スケジュール済みレポート] タブをクリックし、[レポートのスケジュール] サブタブをクリックします。

[スケジュール済みジョブ] リストが表示され、[有効] 列に各ジョブのステータスが表示されます。ジョブが有効である場合、[有効] の値は **true** になります。ジョブが無効である場合、[有効] の値は **false** になります。

2. 必要なジョブ (複数可) を選択し、[選択済みを実効化] または [選択済みを実効化] をクリックします。

[スケジュール済みジョブ] リストに、有効または無効にされたすべてのジョブの新しいステータスが表示されます。

注: レポートジョブを実効化する機能は、反復レポートに使用することを目的としています。1 回だけ実行する ([一度] を使用する) 場合にレポートジョブを実効化すると、そのジョブが [スケジュール済みジョブ] リストから削除されます。

スケジュールされたレポート ジョブの削除

スケジュールされたレポート ジョブを削除できます。

スケジュール済みレポート ジョブの削除方法

1. [スケジュール済みレポート]タブをクリックします。
[レポート サーバ]リストが表示されます。
2. 削除するレポートがスケジュールされているサーバを選択します。
選択したサーバが[レポート サーバの詳細]ペインに表示されます。
3. [レポートのスケジュール]タブをクリックし、行をクリックして削除するジョブを選択し、リスト上部の[削除]ボタンをクリックします。削除するジョブを複数選択できます。

注: 各レポートジョブの横のチェック ボックスは、レポート ジョブを有効化/無効化するために使用します。

確認のダイアログが表示されます。

4. [はい]をクリックします。
レポート ジョブが[スケジュール済みジョブ]リストから削除されます。

詳細情報:

[レポートジョブをスケジュールする方法](#) (P. 484)

[スケジュール済みレポートジョブの編集](#) (P. 500)

自己監視イベント

ほとんどのユーザ アクションでは、自己監視イベントが生成されます。このイベントを使用すると、サーバ上のアクションおよびサーバを使用したアクションの内容とその成否を追跡することができます。自己監視イベントは、[スケジュール済みレポート]タブおよび[アラート管理]タブに、サーバ別にイベントビューア形式で表示されます。また、自己監視イベントレポートを使用して、通常のレポートまたはスケジュール済みレポートとして参照することもできます。

詳細情報

[自己監視イベントの表示](#) (P. 503)

[レポートジョブをスケジュールする方法](#) (P. 484)

自己監視イベントの表示

[アラート管理]タブおよび[スケジュール済みレポート]タブから、各サーバの自己監視イベントを表示できます。各タブの表示はフィルタ処理され、関連アラートやレポートの監視イベントが表示されます。フィルタを削除すれば、自己監視イベントをすべて表示できます。

自己監視イベントの表示方法

1. [スケジュール済みレポート]タブまたは[アラート管理]タブをクリックします。

[レポートサーバ]リストまたは[アラートサーバ]リストが表示されます。

2. ローカル自己監視イベントを表示するサーバを選択します。

選択したサーバが、[詳細]ペインに表示されます。

3. [自己監視イベント]タブをクリックします。

[自己監視イベントビューア]ペインが表示され、レポート関連またはアラート関連の自己監視イベントが表示されます。[自己監視イベント]ペインから、以下のタスクを含む、通常のレポートタスクを実行できます。

- イベントビューア タスク
- グローバル フィルタまたはローカル フィルタ
- お気に入りの設定
- エクスポート

第 13 章：抑制ルールおよび集約ルール

このセクションには、以下のトピックが含まれています。

[イベント精製コンポーネントのバージョン](#) (P. 505)

[抑制ルールおよび集約ルール タスク](#) (P. 506)

[Windows イベント 560 の抑制ルールの作成](#) (P. 529)

イベント精製コンポーネントのバージョン

あるカスタム イベント精製コンポーネントを作成および編集すると、CA Enterprise Log Manager によってそのコンポーネントの以前のバージョンが保持されます。これによって、以前のバージョンを参照することが可能になります。以下のコンポーネントのバージョンを表示またはコピーできます。

- メッセージ解析ファイル
- データ マッピング ファイル
- 抑制ルール
- 集約ルール

カスタム コンポーネントを新規作成すると、バージョンは **1.0** になります。同じオブジェクトの新バージョンを編集して保存すると、バージョンは **2.0** になります。選択や適用のための該当するインターフェース領域には、両方のバージョンが表示されます。

たとえば、「NewRule」というカスタム抑制ルールを作成した場合、適用のための [イベント ログ ストア] インターフェースリストには「NewRule バージョン 1.0」と表示されます。その後、そのファイルを編集すると、[イベント ログ ストア] リストには「NewRule バージョン 2.0」と表示されます。

対象のリストにイベント精製コンポーネントの古いバージョンを表示できます。これらは読み取り専用になっており、編集できません。古いバージョンをコピーして編集し、新規バージョンとすることができます。たとえば、先の例であれば、2.0 が存在すれば、NewRule バージョン 1.0 を編集することはできません。バージョン 1.0 をコピーして、それを編集する必要があります。編集したものを保存すると、バージョン 3.0 が作成されます。

詳細情報

[抑制ルールまたは集約ルールの編集](#) (P. 525)

抑制ルールおよび集約ルール タスク

抑制ルールおよび集約ルールを使用すると、特定のイベントを除外したり統合したりすることによって、イベントフローの制御およびイベントログ ストア サイズの管理を行うことができます。抑制ルールを使用すると、条件と一致するネイティブ イベントが記録されなくなります。集約ルールを使用すると、複数のネイティブ イベントが統合されて、単一の精製済みイベントとして扱われ、元のコンポーネント イベントの代わりに表示されます。

重要： 特定のネイティブ イベントが記録または表示できなくなる可能性があるため、抑制ルールおよび集約ルールの作成や使用には細心の注意を払ってください。抑制および集約のカスタム ルールは、導入前にテスト環境でテストすることをお勧めします。

抑制および集約のタスクはすべて、インターフェースの[ログ収集]領域から実行できます。抑制および集約のカスタム ルールを作成、編集、および削除することができます。

詳細情報

[抑制ルールを作成する方法](#) (P. 508)

[集約ルールを作成する方法](#) (P. 513)

[抑制ルールまたは集約ルールの適用](#) (P. 520)

[抑制ルールまたは集約ルールのコピー](#) (P. 524)

[抑制ルールまたは集約ルールの編集](#) (P. 525)

[抑制ルールまたは集約ルールの削除](#) (P. 526)

[抑制ルールまたは集約ルールのインポート](#) (P. 527)

[抑制ルールまたは集約ルールのエクスポート](#) (P. 528)

抑制ルールによる影響

抑制ルールを使用すると、イベントログストアへのイベントの挿入や、コネクタによるイベントの収集が抑制されるため、抑制ルールの計画中には、その影響を考慮する必要があります。抑制ルールは、常にコネクタに添付されます。エージェントまたはグループレベルで、あるいは **CA Enterprise Log Manager** サーバ自体に抑制ルールを適用できます。配置した場所にはさまざまな影響があります。

- エージェントレベルまたはグループレベルで抑制ルールが適用されると、イベントの収集が抑制され、**CA Enterprise Log Manager** サーバに送信されるネットワークトラフィックの量が削減されます。
- **CA Enterprise Log Manager** サーバに抑制ルールが適用されると、データベースへのイベントの挿入が抑制され、保存される情報の量が削減されます。

特に、複数の抑制ルールを作成する場合や、イベントの発生量が多い場合、イベントが **CA Enterprise Log Manager** サーバに到達した後でイベントに抑制ルールを適用する際に起こりうる、パフォーマンスに関する注意事項があります。

たとえば、ファイアウォールからのイベントや、同じアクションに重複したイベントを作成する一部の **Windows** サーバからのイベントには、抑制が必要となる場合があります。これらのイベントを収集しなければ、保存が必要なイベントログの送信処理を速めることができ、**CA Enterprise Log Manager** サーバの処理時間を短縮できます。このような場合には、エージェントコンポーネントに 1 つ以上の適切な抑制ルールを適用します。

複数のプラットフォーム、または環境全体で発生する特定のタイプのイベントをすべて抑制する必要がある場合は、**CA Enterprise Log Manager** サーバに 1 つ以上の適切な抑制ルールを適用します。イベントが **CA Enterprise Log Manager** サーバに到達すると、抑制に関連するイベント評価が行われます。サーバに多数の抑制ルールを適用すると、サーバはイベントログストアへのイベント挿入に加えて、抑制ルールの適用を実行する必要が生じるため、パフォーマンスが低下する恐れがあります。

小規模な環境では、**CA Enterprise Log Manager** サーバで抑制を実行できます。また、集約(集合)が使用されている導入環境でも、サーバへの抑制の適用を選択できます。大量のイベント情報を生成するイベントソースから少数のイベントのみを挿入する場合には、エージェントレベルまたはエージェントグループレベルで不要なイベントを抑制するよう選択すれば、**CA Enterprise Log Manager** サーバ上の処理時間を短縮できます。

抑制ルールを作成する方法

抑制ルールを使用すると、多くのルーチンや既知の予測可能なトランザクションによってイベントログストアが肥大化したり、環境全体のイメージが把握しにくくなったりするのを防ぐことができます。たとえば、必要なセットのみをイベントソースが送信するように設定できない場合などは特に、不要な **syslog** 情報イベントを削除する抑制ルールが役立ちます。

抑制ルールウィザードを使用して抑制ルールを作成するプロセスは、以下の手順で構成されます。

1. 抑制ルールウィザードの表示
2. ルールの命名 - ルール名および説明情報の入力
3. イベントの選択 - CEG 正規化属性およびオプションの詳細フィルタリングを使用し、抑制するイベントを特定

注: 抑制ルールを作成したら、環境内で使用できるようにそのルールを適用する必要があります。

詳細情報

[抑制ウィザードの表示](#) (P. 509)

[抑制ルールの命名](#) (P. 509)

[抑制ルールまたは集約ルールの適用](#) (P. 520)

抑制ウィザードの表示

抑制ルールを新規作成するか、既存の抑制ルールを編集するには、抑制ウィザードを開きます。

抑制ウィザードを開く方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [イベント精製ライブラリ]フォルダの横にある矢印をクリックして展開し、[抑制および集約]フォルダを選択します。
[抑制]ボタンおよび[集約]ボタンが[詳細]ペインに表示されます。

3. [新規抑制ルール]をクリックします。 

抑制ウィザードが開きます。

ウィザードを使用する際に

- ウィザードを閉じずにルール ファイルを保存するには、[保存]をクリックします。
- ルール ファイルを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

詳細情報

[抑制ルールの命名](#) (P. 509)

抑制ルールの命名

抑制ルールの名前を指定する必要があります。参照用に、任意で説明情報を入力することもできます。

抑制ルールの名前を指定する方法

1. 抑制ウィザードを開きます。
2. 新規ルールの名前を入力します。
3. (オプション)説明情報を入力します。
4. 「フィルタリング」の手順に進みます。

詳細情報

[抑制ルールを作成する方法](#) (P. 508)

抑制するイベントの選択

CEG イベント正規化フィールドの単純フィルタを設定して、ルールで抑制するネイティブ イベントを指定する必要があります。これらの 4 つのフィールドはイベント専用クラスの一部であり、CEG で記述されたすべてのイベントに使用できます。これらのフィールドにより、正確にイベントを指定できます。

[単純フィルタ]タブを使用すると、必要なイベント正規化フィールドの組み合わせを指定できます。また、イベント識別の詳細用に詳細フィルタを使用することもできます。抑制ルールには、少なくとも 1 つの単純フィルタを指定する必要があります。

抑制ルール イベントを選択する方法

1. 抑制ウィザードを開き、必要な情報を入力して、「フィルタリング」の手順に進みます。
2. 適切なチェック ボックスを選択した後、値を選択または入力して、必要なイベントを選択する単純フィルタを作成します。以下のフィールドを使用できます。

理想モデル

ファイアウォールやネットワーク デバイスなど、イベントに関連するさまざまなテクノロジのクラスを指定します。

イベント カテゴリ

理想モデル内のイベントのさまざまなカテゴリを指定します。たとえば、アカウント、ユーザ グループ、およびロール関連のイベントはすべて、「ID 管理」イベント カテゴリに記録されます。各イベント カテゴリには 1 つ以上のクラス(サブ カテゴリ)があるため、選択する内容に応じて、[イベント クラス]メニューで使用可能な項目が変化します。

イベント クラス

特定のイベント カテゴリについて、より詳細にイベントを分類できます。たとえば、ID 管理イベントは、3 つのクラス(アカウント、グループ、または ID)に分類されます。各イベント クラスには 1 つ以上の関連アクションがあるため、選択する内容に応じて、[イベント アクション]メニューで使用可能な項目が変化します。

イベントアクション

各イベント カテゴリおよびイベント クラスに共通するアクションを指定します。たとえば、ID 管理カテゴリのアカウント管理には、アカウントの作成、削除、および変更の各アクションが含まれます。

3. 該当する矢印をクリックして次に完了するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、新規ルールがリストに表示されます。それ以外の場合は、選択した手順が表示されます。

新しくルールを作成すると、バージョン 1.0 として保存されます。後でこのルールを編集すると、新しいルールを保存するたびに新バージョンとして保存されます。以前のバージョンを表示し、必要に応じて適用したりコピーしたりすることができます。

詳細情報:

[単純イベントフィルタの作成](#) (P. 569)

[詳細イベントフィルタの作成](#) (P. 572)

[詳細フィルタの使用](#) (P. 511)

詳細フィルタの使用

詳細フィルタを使用すると、イベントログ ストアの抑制または集約関連のクエリを利用できます。[詳細フィルタ]インターフェースでは、抑制ルールまたは集約ルールの要件に応じてロジック、列、演算子、および値を入力する形式を指定することによって、適切なフィルタ構文を作成できるようにします。

注: このセクションには、抑制ルールおよび集約ルールの詳細フィルタで使用する用語の概要が含まれています。詳細フィルタの機能を十分に活用するには、フィルタ用語および共通イベント文法を深く理解する必要があります。

以下の用語を使用すると、複数のフィルタ ステートメントを結合します。

AND

結合された **すべての**用語が **TRUE** の場合は、イベント情報を表示します。

OR

結合された用語の**いずれかが** **TRUE** の場合は、イベント情報を表示します。

以下の SQL 演算子は詳細フィルタによって使用され、集約または抑制の基本条件を作成します。

一致

入力した英数字の文字列のうち、1 つ以上の文字に一致する任意のイベント情報を含めます。また、キーワードによる検索を可能にします。この検索では大文字と小文字が区別されます。

一致(大文字と小文字を区別しない)

入力した英数字の文字列のうち、1 つ以上の文字に一致する任意のイベント情報を含めます。また、キーワードによる検索を可能にします。この検索では大文字と小文字は区別されません。

一致しない

入力した英数字の文字列のうち、1 つ以上の英数字に一致しないすべてのイベント情報を含めます。この検索では大文字と小文字が区別されます。

一致しない(大文字と小文字を区別しない)

入力した英数字の文字列のうち、1 つ以上の英数字に一致しないすべてのイベント情報を含めます。この検索では大文字と小文字は区別されません。

正規表現に一致

入力した 1 つ以上の正規表現文字に一致するすべてのイベント情報を含めます。マルチバイト環境で検索する場合、またワイルドカードを使用して検索する場合に使用できます。

正規表現に一致しない

入力した 1 つ以上の正規表現文字に一致しないすべてのイベント情報を含めます。マルチバイト環境で検索する場合、またワイルドカードを使用して検索する場合に使用できます。

関係演算子

列が入力した値と適切な関係を保持する場合は、イベント情報を表示します。次の関係演算子を使用できます。

- 等しい(数値)
- 等しくない(数値)
- より大きい(数値)
- 以上(数値)
- より小さい(数値)

- 以下(数値)

たとえば、[> (より大きい)]を使用すると、設定した値よりも大きい値の選択列からイベント情報が含まれます。

これらの演算子はすべて、数値のみを検知します。ほかの文字を検索するには、必要に応じて「一致」演算子のどちらかを選択します。

集約ルールを作成する方法

集約ルールを使用すると、同じタイプの複数のネイティブ イベントを統合して、単一の精製済みイベントとして扱うことができます。これによって、イベントログストアの領域を節約し、イベント分析を容易に行うことができます。

たとえば、単一ユーザーによるログイン試行の失敗 3 回分を単一の精製済みイベントとして記録する集約ルールを作成できます。つまり、イベントログストアには、イベントが 3 つではなく 1 つだけ記録されることになります。

集約ルール ウィザードを使用して集約ルールを作成または編集するプロセスは、主に以下の手順で構成されます。

1. 集約ルール ウィザードの表示
2. 集約のしきい値 - 集約イベントを作成するネイティブ イベントの数または頻度の設定
3. イベントの選択 - CEG 正規化属性およびオプションの詳細フィルタリングを使用し、集約するイベントを特定
4. 集約 - 最終集約イベントをレポートに表示する方法の制御

注: 集約ルールを作成したら、環境内で使用できるようにそのルールを適用する必要があります。

詳細情報

[集約ウィザードの表示](#) (P. 514)

[集約のしきい値の設定](#) (P. 514)

[集約表示の設定](#) (P. 518)

[抑制ルールまたは集約ルールの適用](#) (P. 520)

集約ウィザードの表示

集約ルールを新規作成するか、既存の集約ルールを編集するには、集約ウィザードを開きます。

抑制ウィザードを開く方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [イベント精製ライブラリ]フォルダの横にある矢印をクリックして展開し、[抑制および集約]フォルダを選択します。
[抑制]ボタンおよび[集約]ボタンが[詳細]ペインに表示されます。
3. [新規集約ルール]をクリックします。

集約ウィザードが開きます。

ウィザードを使用する際に

- ウィザードを閉じずにルール ファイルを保存するには、[保存]をクリックします。
- ルール ファイルを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

詳細情報

[集約のしきい値の設定](#) (P. 514)

[集約表示の設定](#) (P. 518)

集約のしきい値の設定

集約ルールを作成または編集するには、一般情報を入力し、集約のしきい値を設定します。しきい値は、集約イベントの作成のトリガとなるイベント数または発生間隔、あるいはその 2 つを組み合わせたものです。

集約のしきい値を設定する方法

1. 集約ウィザードを開きます。
2. 新規ルールの名前を入力します。参照用に、任意で説明情報を入力することもできます。

- 以下の[イベントの集約]メニューを使用して、単一の精製済みイベントを作成する際にルールで使用するため、ネイティブ イベント数および経過時間を指定して、組み合わせを定義します。

イベント数しきい値の有効化

ルールがイベントのしきい値を使用するかどうかを制御します。イベントのしきい値は 1 よりも大きくする必要があります。このチェック ボックスをオンにすると、最大イベント数の値が設定されます。このチェック ボックスをオフにし、イベントのタイムアウト期間を有効にすると、イベントを集約する際に期間のみが考慮されます。両方を有効にすると、該当する元のイベントが少なくとも 1 つ発生すれば、指定したすべての時間帯で集約イベントが作成されます。

最大イベント数

集約イベントのトリガとなるネイティブ イベントの数を定義します。指定した数のネイティブ イベントが発生すると、集約イベントが作成されます。

最小: 2

最大: 5000

イベントのタイムアウト期間の有効化

ルールがタイムアウト期間のしきい値を使用するかどうかを制御します。このチェック ボックスをオンにすると、期間の値が設定されます。このチェック ボックスをオフにすると、イベント数のしきい値に達した場合にのみ、集約イベントが発生します。

期間

指定したタイプのイベントが発生した場合に、集約イベントのトリガとなる経過時間を秒単位で定義します。このしきい値に達すると、該当するネイティブ イベントが少なくとも 1 つ発生していれば、集約イベントが作成されます。[期間]を「0」に設定すると、最大イベント数に達した場合にのみ集約イベントが作成されます。

最小: 0

最大: 86400

たとえば、失敗したログイン試行を集約するルールの場合、[最大イベント数]メニューで「3」を、[期間]メニューで「10」を選択すると、少なくとも 1 回ログインに失敗すると、ログイン試行が 3 回失敗した後か、または 10 秒おきに集約イベントが作成されます。

- 適切な矢印をクリックして次に実行するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、新規ルールがリストに表示されます。それ以外の場合は、選択した手順が表示されます。

詳細情報

[集約表示の設定](#) (P. 518)

集約用イベントの選択

CEG イベント正規化フィールドに単純フィルタを設定し、ルールに従って集約するネイティブ イベントを指定します。これらの 4 つのフィールドはイベント専用クラスの一部であり、CEG で記述されたすべてのイベントに使用できます。これらのフィールドにより、イベントを指定できます。

[単純フィルタ]タブを使用して必要なイベント正規化フィールドの組み合わせを指定できます。また、イベント識別の詳細用に詳細フィルタを使用することもできます。抑制ルール用に少なくとも 1 つの単純フィルタを指定します。

集約ルール イベントの選択方法

1. 集約ウィザードを開き、「フィルタリング」の手順に進みます。
2. 該当するチェック ボックスを選択し、必要に応じて値を選択するか、または入力して、対象のイベントを選択するための単純フィルタを作成します。以下のフィールドが利用できます。

推奨されるモデル

イベントに関連するさまざまなテクノロジーのクラスを指定します。たとえば、ファイアウォールやネットワーク デバイスが推奨されるモデルに相当します。

イベント カテゴリ

イベントのさまざまなカテゴリを指定します。たとえば、アカウント、ユーザ グループ、およびロール関連のイベントはすべて、「ID 管理」イベント カテゴリに記録されます。各イベント カテゴリには 1 つ以上のクラス(サブ カテゴリ)があるため、選択する内容に応じて、[イベント クラス]メニューで使用可能な項目が変化します。

イベント クラス

特定のイベント カテゴリについて、より詳細にイベントを分類できます。たとえば、ID 管理イベントは、3 つのクラス(アカウント、グループ、または ID)に分類されます。各イベント クラスには 1 つ以上の関連アクションがあるため、選択する内容に応じて、[イベント アクション]メニューで使用可能な項目が変化します。

イベント アクション

各イベント カテゴリおよびイベント クラスに共通するアクションを指定します。たとえば、ID 管理カテゴリのアカウント管理には、アカウントの作成、削除、および変更の各アクションが含まれます。

3. 該当する矢印をクリックして次に完了するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、新規ルールがリストに表示されます。それ以外の場合は、選択した手順が表示されます。

詳細情報:

[単純イベントフィルタの作成](#) (P. 569)

[詳細イベントフィルタの作成](#) (P. 572)

[集約表示の設定](#) (P. 518)

[集約のしきい値の設定](#) (P. 514)

集約表示の設定

集約ルールは、ネイティブ イベントが精製済みイベントでどのように表示されるかを制御します。[フィールド別に集約]および[集計したフィールド]を選択して、集約表示を設定します。

集約ルール表示の設定方法

1. 集約ウィザードを開き、「集約」の手順に進みます。
2. シャトル コントロールを使用して、精製済みイベントを集約する際に使用するフィールドを 1 つまたは複数選択します。

フィールド別に集約

集約される情報をグループ化する際に使用するフィールドを 1 つまたは複数選択します。たとえば、ログインの失敗を集約するルールの場合は、`source_username` を選択すれば、一意のユーザごとに、条件に一致するログイン失敗イベントの数が表示されます。ルールを完成させるには、1 つ以上の[フィールド別に集約]フィールドを選択する必要があります。

3. (オプション) 精製済みイベントを集計する際に使用するフィールドを 1 つまたは複数選択します。

集計したフィールド

[フィールド別に集約]によって集約された情報を分割する際に使用するフィールドを 1 つまたは複数選択します。たとえば、ログインの失敗を集約するルールの場合、[フィールド別に集約]で `source_username` を選択し、[集計したフィールド]として `dest_hostname` を選択します。この表示では、一意のユーザごとに、条件に一致するログイン失敗イベントの数が、ログインを試みたホスト別に分けて表示されます。

集計したフィールドの情報は、集約されたイベントの元のイベントフィールドに保持されます。前述の例では、ユーザがログインを試みた一意のホストが、それぞれ発生数と共に `hostname1:2,hostname2:5` という形式で保存されます。この例では、ホスト 1 に対する 2 回の試行とホスト 2 に対する 5 回の試行を表しています。

集計したフィールドは任意です。ルールを完成させるのに、集計したフィールドを選択する必要はありません。

4. 適切な矢印をクリックして次に実行するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、新規ルールがリストに表示されます。それ以外の場合は、選択した手順が表示されます。

新しくルールを作成すると、バージョン 1.0 として保存されます。後でこのルールを編集すると、新しいルールを保存するたびに新バージョンとして保存されます。以前のバージョンを表示し、必要に応じて適用したりコピーしたりすることができます。

詳細情報

[集約のしきい値の設定](#) (P. 514)

抑制ルールまたは集約ルールの適用

抑制ルールまたは集約ルールを作成したら、環境内で使用できるようにそのルールを適用する必要があります。この機能によって、抑制ルールや集約ルールが適切なテストや承認を経ずにアプリケーションに適用されるのを防ぐことができます。

抑制ルールや集約ルールを適用する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
[サービスリスト]が表示されます。
2. [イベント ログ ストア]アイコンをクリックします。
[イベント ログ ストアの設定]ペインが表示されます。
3. 適切なシャトル コントロールを使用し、適用する抑制ルールまたは集約ルールを特定して選択します。
4. [保存]をクリックします。
ルールが正常に適用されたことを確認するメッセージが表示されます。

エージェント コンポーネントに抑制と集約を適用する方法

環境内のエージェントグループ、エージェント、またはコネクタに、抑制ルールか集約ルール、あるいはその両方を割り当てることができます。これらのルールを使用して、CA Enterprise Log Manager サーバで適用されている抑制ルールや集約ルールを置き換えたり、補足したりすることができます。これにより、イベント精製を実行する場所を制御して、イベント送受信プロセスをカスタマイズできます。

たとえば、Windows エージェントグループがある場合、不要な Windows イベントを削除する抑制ルールをグループ内のエージェントに関連付けることができます。これによって、CA Enterprise Log Manager サーバですべての受信イベントに対して Windows 固有のチェックを行う必要がなくなります。

エージェント フォルダ階層のさまざまなレベルで抑制ルールまたは集約ルールを適用できます。

- [エージェント エクスプローラ]フォルダから、任意のエージェントグループ、個別のエージェント、またはコネクタにルールを適用できます。
- 特定のエージェントグループ フォルダから、そのグループ内のすべてのエージェント、およびそれらに割り当てられたすべてのコネクタにルールを適用できます。
- 各エージェントから、そのエージェントおよび割り当てられたすべてのコネクタのみにルールを適用できます。

エージェント コンポーネントに抑制ルールや集約ルールを適用するプロセスは、以下の手順で構成されます。

1. ルールの管理ウィザードの表示
2. ターゲット(エージェントグループ、エージェント、またはコネクタ)の選択
3. 適用する抑制ルールの選択
4. 適用する集約ルールの選択

また、ルールの管理ウィザードを使用して、複数のエージェントグループ、エージェント、またはコネクタから、抑制ルールや集約ルールを削除できます。

詳細情報:

[集約ルールの管理ウィザードを開く](#) (P. 521)

[抑制と集約のターゲットの選択](#) (P. 522)

[適用する抑制ルールの選択](#) (P. 522)

[適用する集約ルールの選択](#) (P. 523)

集約ルールの管理ウィザードを開く

エージェントグループ、または個々のエージェントやコネクタに抑制ルールや集約ルールを適用するには、ルールの管理ウィザードを使用できます。

ルールの管理ウィザードを開くには、以下の手順に従います。

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダ リストが表示されます。

2. [エージェント エクスプローラ]フォルダをクリックし、[抑制/集約ルールの管理]をクリックします。

ルールの管理ウィザードが表示されます。

ウィザードの使用時の操作

- ウィザードを閉じずにファイルを保存するには、[保存]をクリックします。
- ファイルを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

抑制と集約のターゲットの選択

エージェント コンポーネントに抑制ルールまたは集約ルールを適用するには、ルールのターゲットを選択します。

ターゲットを選択するには、以下の手順に従います。

1. ルールの管理ウィザードを開きます。
2. ルールの適用先として、エージェント グループ、エージェント、またはコネクタのいずれかを選択します。
3. (オプション) ルールを追加するのではなく削除する場合は、[削除]を選択します。
4. シャトル コントロールを使用して、必要なターゲットを選択します。

注: エージェント名とコネクタ名を検索できます。エージェントまたはコネクタが使用可能リストに表示されない場合は、[検索]をクリックして、使用可能なエージェントまたはコネクタをすべて表示してください。

5. 必要なルールの適用手順に進みます。

適用する抑制ルールの選択

エージェント グループ、エージェント、またはコネクタへの抑制ルールの割り当てを完了するには、適用するルールを選択します。

抑制ルールを選択する方法

1. 抑制ルールの適用ウィザードを開き、「抑制ルールの適用」の手順に進みます。

2. シャトル コントロールを使用して、適用する使用可能なルールを選択します。

注: [抑制ルール パターン] フィールドを使用して、抑制ルールを検索できます。

3. [保存して閉じる] をクリックします。

選択したルールが、選択したターゲットに適用されます。

適用する集約ルールの選択

エージェント グループ、エージェント、またはコネクタへの集約ルールの割り当てを完了するには、適用するルールを選択します。

集約ルールを選択するには、以下の手順に従います。

1. 集約ルールの管理ウィザードを開き、[集約ルールの適用] の手順に進みます。

2. シャトル コントロールを使用して、適用する使用可能なルールを選択します。

注: [集約ルール パターン] フィールドを使用して、集約ルールを検索できます。

3. ルールの適用が完了したら、[保存して閉じる] をクリックします。

4. 選択したルールが、選択したターゲットに適用されます。[ターゲットの選択] の手順で[削除] を選択した場合は、選択したルールが削除されます。

抑制ルールまたは集約ルールのコピー

抑制ルールまたは集約ルールをコピーし、既存のルールを基にして新規ルールを作成できます。

抑制ルールや集約ルールをコピーする方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [イベント精製ライブラリ]フォルダの横にある矢印をクリックして展開し、[抑制および集約]フォルダを選択します。
[抑制]ボタンおよび[集約]ボタンが[詳細]ペインに表示されます。
3. コピーするルールが含まれている[抑制および集約]フォルダをクリックします。
フォルダが開き、ルールが表示されます。
4. コピーするルールを選択し、[選択された項目のコピー]をクリックします。

抑制ウィザードまたは集約ウィザードが開き、ルールが表示されます。
5. 必要な変更を加え、[保存して閉じる]をクリックします。
ルールが所定のリストに表示されます。

抑制ルールまたは集約ルールの編集

抑制ルールや集約ルールを編集できます。

抑制ルールまたは集約ルールの編集方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [イベント精製ライブラリ]フォルダの横にある矢印をクリックして展開し、[抑制および集約]フォルダを選択します。
[抑制]ボタンおよび[集約]ボタンが[詳細]ペインに表示されます。
3. 編集するルールが含まれている[抑制および集約]フォルダをクリックします。
4. 編集するルールを選択し、[抑制ルールまたは集約ルールの編集]アイコンをクリックします。
抑制ウィザードまたは集約ウィザードが表示され、選択したルールが表示されます。
5. 必要な変更を加えて、[保存して閉じる]をクリックします。
ルールが、編集したルールの新バージョンとして、該当するリストに表示されます。

詳細情報

[イベント精製コンポーネントのバージョン](#) (P. 505)

抑制ルールまたは集約ルールの削除

不要な抑制ルールや集約ルールを削除できます。

抑制ルールまたは集約ルールの削除方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [イベント精製ライブラリ]フォルダの横にある矢印をクリックして展開し、[抑制および集約]フォルダを選択します。
[抑制]ボタンおよび[集約]ボタンが[詳細]ペインに表示されます。
3. 削除するルールが含まれている[抑制および集約]フォルダをクリックします。
4. 削除するルールを選択し、[抑制ルールまたは集約ルールの削除]アイコンをクリックします。現在のバージョンがデフォルトで選択されています。[詳細]ペインの[バージョン]プルダウンリストから、削除する古いバージョンを選択できます。
確認のダイアログが表示されます。ルールを統合に適用している場合、警告が表示されます。ルールを削除すると、統合からもそのルールが削除されます。
5. [はい]をクリックします。
削除したルールが、該当するリストから削除されます。

抑制ルールまたは集約ルールのインポート

抑制ルールまたは集約ルールをインポートすることで、ある環境から別の環境にルールを移行することができます。たとえば、テスト環境で作成したルールをライブ環境にインポートできます。

抑制ルールまたは集約ルールのインポート方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [イベント精製ライブラリ]フォルダの横にある矢印をクリックして展開し、[抑制ルールおよび集約ルール]フォルダを選択します。
[抑制/集約ルールのインポート]ボタンおよび[抑制/集約ルールのエクスポート]ボタンが[詳細]ペインに表示されます。
3. [抑制/集約ルールのインポート]をクリックします。
[ファイルのインポート]ダイアログ ボックスが表示されます。
4. インポートするファイルを参照し、[OK]をクリックします。
抑制ウィザードまたは集約ウィザードが表示され、選択したルールの詳細が表示されます。
5. 必要な変更を加え、[保存して閉じる]をクリックします。インポートしたルールの名前が管理データベース内に存在するルールと同じ場合は、名前の変更を要求するメッセージが表示されます。
インポートしたルールが、適切な抑制フォルダまたは集約フォルダに表示されます。

抑制ルールまたは集約ルールのエクスポート

抑制ルールや集約ルールをエクスポートできます。これによって、環境間でルールを共有できます。たとえば、テスト環境で作成されたルールをライブ環境にエクスポートできます。

抑制ルールまたは集約ルールのエクスポート方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [イベント精製ライブラリ]フォルダの横にある矢印をクリックして展開し、[抑制ルールおよび集約ルール]フォルダを選択します。
[抑制ルールまたは集約ルールのエクスポート]ボタンが[詳細]ペインに表示されます。
3. エクスポートするファイルが含まれている[抑制ルール]フォルダまたは[集約ルール]フォルダをクリックします。
フォルダが展開され、各ファイルが表示されます。
4. エクスポートするルールを選択し、[抑制ルールまたは集約ルールのエクスポート]をクリックします。現在のバージョンがデフォルトで選択されています。
[詳細]ペインの[バージョン]プルダウンリストからエクスポート対象として古いバージョンを選択できます。
[エクスポートの場所]ダイアログ ボックスが表示されます。
5. エクスポートされるルールを格納する場所を入力または参照し、[保存]をクリックします。
エクスポートの成功を確認するダイアログ ボックスが開きます。
6. [OK]をクリックします。
ルールがエクスポートされます。

Windows イベント 560 の抑制ルールの作成

Windows サーバ上でオブジェクト アクセス監査を有効にすると、非常に多くのイベントトラフィックが発生し、一部を削除する必要がある場合があります。たとえば、管理者が Microsoft 管理コンソール (mmc.exe) を開くたびに、Windows は 2 つのイベントを生成します。これらのイベントの ID 値は 560 と 562 です。

この例では、event_id が 560 の Windows イベントを抑制するルールを新規作成します。以下の手順説明にある手順を実行すると、ウィザードの使用方法が理解できるだけでなく、お使いのネットワーク環境で実際に使用可能な抑制ルールを作成できます。

この例の作業を開始するには、管理者のロールおよび権限を持ったユーザとして CA Enterprise Log Manager サーバにログインする必要があります。EiamAdmin ユーザとしてログインすると、抑制ルールの作成および編集を実行できません。

Windows の 560 イベント用の抑制ルールを作成する方法

1. 抑制ルール ウィザードを開きます。
2. 名前エントリフィールドに「Windows イベント 560 の抑制」と入力し、説明として、「OS によって同タイプのリソース アクセスにイベント 562 も作成されるため、このルールによって Window イベント 560 を抑制する。イベント 560 の保持はコンプライアンス上必要なし。」と追記します。
3. 「フィルタリング」の手順に進み、以下の単純フィルタを選択します。
 - a. 推奨されるモデル値、オペレーティング システム
 - b. イベント カテゴリ値、リソース アクセス
 - c. イベント クラス値、リソース オープン
 - d. イベント アクション値、リソース アクティビティ

4. [詳細フィルタ]タブをクリックし、[新規イベントフィルタ]ボタンをクリックします。

新しいフィルタ行がテーブルに表示されます。各テーブルセル内の値または空白をクリックして、新しい値を選択または入力できます。

[論理演算子]フィールドには、デフォルト値の「AND」が入力されています。抑制する必要があるイベントに複数の異なるタイプが含まれている場合は、新しい行に論理演算子「OR」を用いてイベント ID を入力します。

5. 詳細なフィールドフィルタ値を設定します。
 - a. [列]フィールドの値をクリックし、`event_id` フィールドを選択します。
 - b. [演算子]フィールドをクリックし、「等しい」を選択します。
 - c. [値]セルをクリックし、値 **560** を入力します。

6. [保存して閉じる]をクリックします。

ウィザードによって、自動的に[ユーザ]フォルダが作成され、作成した抑制ルールが保存されます。[抑制ルール]フォルダを展開すると、このフォルダを表示できます。

第 14 章：マッピングおよび解析

このセクションには、以下のトピックが含まれています。

[イベント状態](#) (P. 532)

[マッピングおよび解析ルール タスク](#) (P. 534)

[メッセージ解析ファイルを作成する方法](#) (P. 534)

[データ マッピング ファイルを作成する方法](#) (P. 553)

[イベント転送ルール タスク](#) (P. 566)

イベント状態

環境でのイベントに関する情報は、CA Enterprise Log Manager による最初の発生から最終の表示まで、多くのステージを通過します。「イベント」という用語はこれらのステージのいずれか 1 つを指す場合があるため、環境で可能なイベント状態については以下の用語を使用します。

ネイティブ イベント

イベントの発生要因となる状態またはアクションが最初に発生した段階、認証の失敗、ファイアウォール違反などを指します。該当するコネクタまたはリスナ サービスによってネイティブ イベントが送信され、必要に応じて解析とマッピングが行われます。その後、ネイティブ イベントはイベントログストアに挿入され、元のイベントや絞り込まれたイベントとしての表示に使用できます。

元のイベント

該当する監視エージェントによって送信された情報を指します。元のイベントには、ネイティブのイベントに関する情報が、多くの場合、**syslog** の文字列または名前と値のペアの形で格納されます。この情報は、抑制ルールまたは集約ルールによって変更されない限り、格納され検索可能です。抑制されたイベントは、イベントログストアに記録されません。1 セットの集約されたイベントは、集約の結果を示す 1 つのイベントとして記録されます。

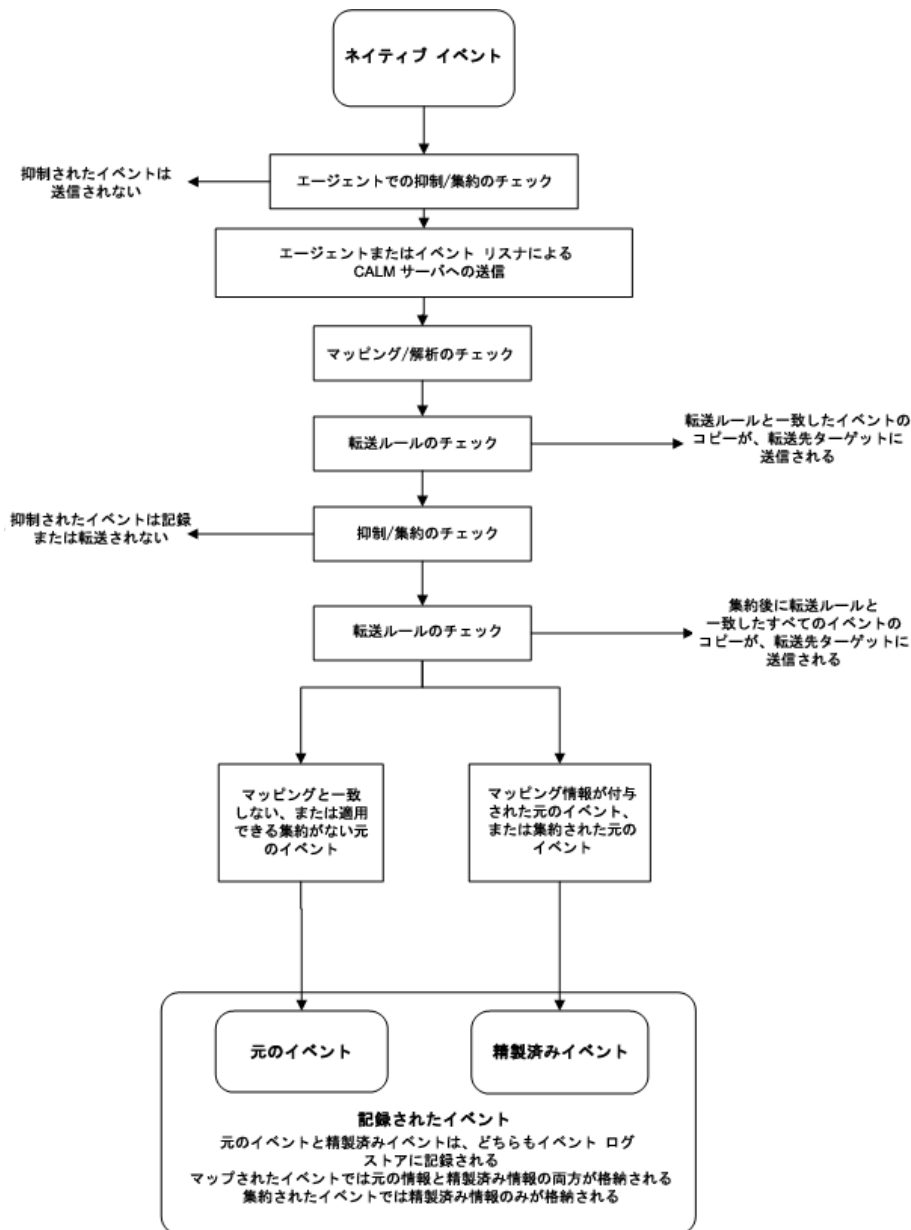
精製済みイベント

CA Enterprise Log Manager によってマッピングと集約が行われたイベント情報を指します。この情報は格納され検索可能です。

記録されたイベント

イベントログストア内の元のイベントまたは精製済みイベントの情報を指します。抑制または集約されない限り、元のイベントと精製済みイベントは常に記録されます。マッピングされたイベントでは、元の情報も再設定された情報も使用可能です。この情報は格納され検索可能です。

イベント状態に関する情報については、以下の図を参照してください。



詳細情報:

[抑制ルールおよび集約ルール タスク](#) (P. 506)

[マッピングおよび解析ルール タスク](#) (P. 534)

マッピングおよび解析ルール タスク

メッセージ解析 (XMP) ファイルおよびデータ マッピング (DM) ファイルのペアによって、特定のタイプのイベントソースからデータが収集され、正規化されます。受信されるネイティブ イベントの大部分に対して、解析処理と、その後続けてマッピング処理が実行され、報告可能なイベントが作成され、イベントログストアに挿入されます。SAPI または iTechnology によって転送されたイベントは解析を必要とせず、直接データのマッピング処理が実行されます。

注: これらの高度な機能を十分に活用するには、お使いの環境における元のイベントおよび収集されたイベント、解析するターゲット フィールド、正規表現構文、CEG、および DM ファイルと XMP ファイル、そのイベント解析方法について、完全に理解している必要があります。

XML ベースの XMP ファイルによって、受信した元のイベントのデータが読み込まれ、指定した内容に応じて、名前と値のペアが作成されます。その後、DM ファイルによって、メッセージの解析で割り当てられたイベントの名前と値のペアが共通イベント文法にマッピングされます。解析ファイルとマッピング ファイルの新規作成は、一連のプロセスと考えてください。たとえば、解析が効率的で完全であるほど、マッピングの時間を短縮して処理効率を上げることができます。

詳細情報

[イベント精製コンポーネントのバージョン](#) (P. 505)

[メッセージ解析ファイルを作成する方法](#) (P. 534)

[データ マッピング ファイルを作成する方法](#) (P. 553)

メッセージ解析ファイルを作成する方法

解析ファイル ウィザードを使用して、メッセージ解析 (XMP) ファイルを作成、編集、および分析することができます。解析ファイルによって、受信した元のイベントのデータが読み込まれ、名前と値のペアが作成され、データ マッピング プロセスの実行前でもマッピングを作成することができます。これによって、全体的なマッピング効率が向上します。

注: 共通イベント文法 (CEG) 名は、イベント解析では考慮されないため、これを使用すると、名前/値ペアを作成する際の柔軟性が向上します。選択の際に CEG フィールドを使用できますが、フィールド名と値は CEG 値に制限されません。

XMP ファイルの作成または編集は、以下の手順で構成されます。

1. 解析ファイル ウィザードの表示
2. ファイル名、ログ名、サポート情報などのファイル詳細の入力
3. ファイル テストと作成用のサンプル イベントの特定
4. ファイルによって解析されるすべてのイベントに適用されるグローバル値の設定
5. イベント解析を開始するための事前一致文字列の作成または編集
6. フィルタ添付を解析するための事前一致フィルタの選択
7. イベント解析を完了するための解析フィルタの作成または編集
8. 新しい XMP ファイルまたは編集された XMP ファイルの分析および保存

詳細情報

[ファイル詳細の定義](#) (P. 536)

[サンプル イベントのロード](#) (P. 538)

[グローバル フィールドの追加](#) (P. 539)

[事前一致フィルタの作成](#) (P. 540)

[XMP ファイルの分析](#) (P. 552)

解析ファイル ウィザードの表示

メッセージ解析ファイルを作成するか、既存のメッセージ解析ルールを編集するには、解析ファイル ウィザードを開く必要があります。

解析ファイル ウィザードを開く方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。
2. [イベント精製ライブラリ]フォルダの横の矢印をクリックしてフォルダを展開し、[マッピングおよび解析]フォルダを選択します。

製品統合のボタンが詳細ペインに表示されます。

3. [新規メッセージ解析ルール]をクリックします。 

解析ファイル ウィザードが開きます。

ウィザードの使用時の操作

- ウィザードを閉じずに保存するには、[保存]をクリックします。
- ファイルを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

ファイル詳細の定義

名前、ソース、リファレンス情報など、新しい解析ファイルの詳細を追加できます。新しく作成または編集されたファイルは、[マッピングおよび解析]領域の[ユーザ フォルダ]に表示されます。

新規解析ファイルの詳細を追加する方法

1. 解析ファイルウィザードを開きます。
2. 以下のサブ手順の説明に従って、[解析ファイル情報]領域を指定します。
 - a. ファイルの名前を入力します。ファイル名は必須で、使用できない文字は、/ ¥ : * ? " < > ^ ; ' , & { } [] . または | です。
 - b. ファイルを解析するイベントタイプのログ名を識別するためのソースログ名を入力します。オートコンプリート機能によって、入力と共に使用可能なログ名が表示されます。選択したログ名が、精製済みイベントの `event_logname` フィールドに表示されます。
 - c. 必要に応じて、参照用に説明を追加します。
3. (オプション) 以下の補足手順の説明に従って、参照用にサポート情報を追加します。
 - a. [サポート情報]領域の[製品の追加]をクリックします。
新しいサポート情報行が表示されます。
 - b. [新しい製品]テキストまたは[新しいバージョン]テキストをクリックしてエントリフィールドを有効にし、必要な製品/バージョン情報を入力します。
4. 適切な矢印をクリックして次に実行するウィザード手順に進むか、[保存して閉じる]をクリックします。
[保存して閉じる]をクリックすると、新規ファイルが[解析ファイル]ユーザーフォルダに表示されます。それ以外の場合は、選択した手順が表示されます。

サンプル イベントのロード

新しい XMP ファイルをテストするにあたって、サンプル イベントを利用し、イベント ログ ストアの検索やログ ファイルへのアクセスを実行できます。サンプル イベントは、ほかのウィザード手順で解析ファイルを作成する際このファイルをテストするためのテンプレートになります。また、サンプル イベントを使用して、ウィザードの最終手順で解析出力をテストできます。

サンプル イベントの利用方法

1. 解析ファイル ウィザードを開き、「イベントのロード」の手順に進みます。

[イベントのロード]画面が表示されます。

2. [サンプル イベントの検索]領域にあるラジオ ボタンの[ログ ストア]または[ログ ファイル]を選択します。

- [ログ ストア]を選択した場合

- a. [解析列]ドロップダウン メニューから適切なサンプル イベントソースのタイプを選択します。WMI イベントソースの場合は `result_string` を、syslog イベントソースの場合は `raw_event` を選択します。
- b. [クエリタグ フィルタ]および[クエリリスト]を使用して、サンプル イベントの利用に使用するクエリを選択します。

クエリが表示され、ウィザードの進行中、解析をテストする際に使用できるサンプル イベントが表示されます。

注: サンプル イベントの検索には、すべての既存のクエリやカスタム クエリを使用できます。カスタム クエリを使用する場合は、メッセージ解析ファイルの設計手順を開始する前に、カスタム クエリの作成とテストを実行しておくことをお勧めします。分析しやすいように、サンプル イベントファイルのイベント数は 1500 未満にして使用することをお勧めします。

- [ログ ファイル]を選択した場合は、[参照]で目的のログ ファイルを選択し、[アップロード]をクリックします。

ログ ファイルのイベントが、[サンプル イベント]ペインに表示されます。ウィザードの進行中、解析をテストする際に、イベントを使用できます。

注: ウィザードでは、ファイル内の各行がイベントとみなされます。複数行で構成されるイベントはサポートされません。

3. 適切な矢印をクリックして、次に実行するウィザード手順に進みます。

[保存して閉じる]をクリックすると、新規ファイルが[解析ファイル]ユーザフォルダに表示されます。それ以外の場合は、選択した手順が表示されます。

グローバル フィールドの追加

グローバル フィールドはフィールド名を特定の値に一致させる静的なペアであり、ユーザが追加できます。解析プロセスでは、解析対象のすべてのイベントにグローバル フィールドが追加されます。そのため、それらのフィールドは推奨されるモデルのようなデフォルト値の使用に最適です。

グローバル フィールドを追加する方法

1. [解析ファイル]ウィザードを開き、[グローバル フィールド]の手順に進みます。

[グローバル フィールド]画面が表示されます。

2. [グローバル フィールド]領域の[グローバル フィールドの追加]をクリックします。

新しいグローバル フィールド行がフィールド テーブルに表示され、[新しいグローバル フィールド]および[新しい値]エントリが表示されます。

3. [New Global Field]テキストをクリックして、必要な名前情報を入力します。入力に応じてオートコンプリート機能によって使用可能な CEG フィールド名が表示されます。1 つの CEG 名をクリックして選択するか、非 CEG フィールド名を入力します。
4. [New Global Field]テキストをクリックして、必要な名前情報を入力します。
5. (オプション) 必要に応じて手順 2 ～ 4 を繰り返して、その他のグローバル フィールドを追加します。
6. 該当する矢印をクリックして次に完了するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、新規ファイルが[解析ファイル]ユーザフォルダに表示されます。それ以外の場合は、選択した手順が表示されます。

事前一致フィルタの作成

事前一致フィルタを作成することで、解析するイベント情報の検索結果を XMP ファイルが絞り込む際の効率を向上させることができます。事前一致フィルタによって選択済みテキスト文字列が識別され、イベントの選択プロセスが絞り込まれます。その後、解析フィルタによってイベントの選択プロセスが完了します。解析ファイルが「じょうご」だとすれば、事前一致フィルタは入り口側、解析フィルタは出口側に相当します。

事前一致フィルタが完全であるほど、解析プロセスの効率は向上します。これは、事前一致カテゴリによって絞り込むことで、イベントの解析に必要な処理負荷が軽減されるためです。

たとえば、アクセス試行イベントを解析する場合は、「login」というテキストを検索する事前一致フィルタを作成し、適切な解析フィルタをその事前一致フィルタに追加します。

注: 事前一致フィルタを削除すると、関連付けられている解析フィルタや各種のフィルタも削除されます。

事前一致フィルタの作成方法

1. [解析ファイル]ウィザードを開き、「一致と解析」の手順に進みます。
ウィザードの[事前一致フィルタ]リストに、既存の事前一致フィルタがすべて表示されます。各フィルタの横には、サンプル イベントへの事前一致数が丸かっこで囲まれて表示されます。
2. [事前一致フィルタ]リスト上部の[事前一致文字列の追加]をクリックするか、編集する事前一致文字列を選択します。

注: 事前一致フィルタを選択するには、[検索]フィールドに事前一致文字列の最初のいくつかの文字を入力します。入力した文字列に一致する事前一致文字列がすべて表示されます。検索結果として表示されている事前一致文字列では、上下矢印を使用して事前一致文字列を移動することはできません

3. [事前一致文字列] エントリ フィールドにフィルタが検索するテキストを入力します。

入力したテキストに一致するすべてのサンプル イベントがすぐに表示され、検出および解析された一致イベント数も併せて表示されます。

4. (オプション) 一致しないサンプル イベントもすべて表示するには、[一致しないイベントに基づいて事前一致文字列を追加]をクリックします。

現在一致していないすべてのサンプル イベントが、新しい事前一致フィルタを作成する際に参照しやすいように、[イベント]領域に表示されます。

5. (オプション) 必要に応じて、さらに事前一致フィルタを追加または編集します。

6. [事前一致フィルタ]リストの横の上矢印/下矢印を使用して、解析プロセスで事前一致を検索する順序を設定します。より多くのイベントと一致する事前一致フィルタが優先順位リストの上位に来るよう設定すると、解析プロセスの効率を向上させることができます。

7. 該当する矢印をクリックして次に完了するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックした場合、新しいファイルが[解析ファイル ユーザ]フォルダに表示されます。それ以外の場合は、選択した手順が表示されます。

解析フィルタの作成

解析フィルタを作成して、XMP ファイルによるイベントデータの解析方法を定義できます。各解析フィルタには、事前一致フィルタが関連付けられています。解析プロセスによって、事前一致文字列が検出された後、その事前一致に関連付けられた各解析フィルタを使用して、指定された情報が検出されます。解析プロセスは、最初に一致したものを返します。

メッセージ解析ウィザードの[一致と解析]の手順にある[解析フィルタの追加]ボタンをクリックすると、解析ファイル フィルタ ウィザードが開始します。効果的な解析フィルタを作成するには、正規表現構文について十分に理解しておく必要があります。

解析フィルタの作成方法

1. 解析ファイル フィルタ ウィザードを開き、[フィルタの詳細]ページにフィルタ名および任意で説明を入力します。
2. [新規追加]をクリックして、フィルタによって解析されるすべてのイベントに表示する静的フィールド値を追加します。

静的フィールド行が表示され、[新しいフィールド]セルおよび[新しい値]セルが表示されます。

3. [新しいフィールド]セルおよび[新しいフィールド]セルにエントリを入力します。オートコンプリート機能によって、[新しいフィールド]セルへの入力と共に使用可能な CEG フィールド名が絞り込まれ、選択肢メニューが表示されます。
4. (オプション) 必要に応じて手順 2 ～ 3 を繰り返し、静的フィールド値を追加します。
5. [正規表現]の手順に進みます。

[解析表現のテスト]画面が表示され、現在の正規表現が表示されます。正規表現のすぐ下に、[イベント]ペインがあります。以前にサンプル イベントをロードしていれば、この領域に 1 つ以上のサンプル イベントが表示されます。正規表現を作成すると、ウィザードによって、その正規表現に対してこれらのイベントをテストできます。

6. [ライブラリに対してトークンを追加または削除します]をクリックして、現在のフィルタで使用するために追加できる事前定義済み正規表現のリストを表示します。追加するトークンを選択し、[OK]をクリックして、[解析トークン]リストに追加します。

7. (オプション) [新しい正規表現トークン]をクリックして、解析トークンを作成し、[トークンの詳細]ペインに正規表現構文を入力します。現在の環境用のカスタム表現が作成されます。[解析トークン]ペインの一番上の[選択したトークンをライブラリに追加します]をクリックして、カスタムトークンをローカルライブラリに追加できます。

注: 新しい日時トークンを作成する場合、「日時の値として処理する」チェックボックスをオンにして、時間の値を解析する際の形式を入力してください。この値は表示形式には影響しません。

8. [正規表現]エントリフィールドにフィルタ用の正規表現文を追加します。[解析トークン]リストから表現をドラッグアンドドロップできます。[正規表現]エントリフィールドで、表現を直接入力および編集することもできます。

注: [解析トークン]リストでトークンを選択すると、[トークンの詳細]ペインにその正規表現構文が表示されます。特定のルール of 解析トークン マッピングを表示して、ほかの解析ルールで再度利用することができます。

9. (オプション) 表示するキー ペアがターゲット イベントに含まれている場合は、[動的な名前/値のペア]チェックボックスをオンにしてください。詳細については、「動的な解析」を参照してください。
10. (オプション) 動的な解析を使用する場合は、動的なペア エントリフィールドに動的な解析表現を入力してください。たとえば、以下のように入力します。

```
( _PAIR_KEY_ ) = ( _PAIR_VALUE_ ) ;
```

ペア内部が等号で区切られ、ペアどうしがセミコロンで分割されて表示されます。表現を追加すれば、ペアを別の形式で表示することができます。詳細については、「動的な解析」を参照してください。

11. [イベント]ペインおよび[解析されたイベント]ペインを使用して、ファイルによるサンプル イベントの解析方法をプレビューします。解析フィルタ正規表現を変更すると、サンプル イベントの解析された部分が青いテキストで強調表示され、動的に解析されたペアが緑色で表示されます。解析の有効性を検証できます。
12. (オプション) [イベント]ペイン下の[戻る]矢印および[進む]矢印を使用して、使用可能なサンプル イベント間を移動し、追加テストを行うサンプル イベントを切り替えます。
13. 正規表現に問題がなければ、[保存して閉じる]をクリックします。[リセット]を使用すると、正規表現を最初の状態に戻すことができます。

解析ファイル フィルタ ウィザードが閉じ、解析ファイル ウィザードの[一致と解析]の手順に戻ります。

詳細情報:

[動的解析](#) (P. 544)

[解析トークン](#) (P. 545)

[ライブラリへのカスタムトークンの追加](#) (P. 549)

動的解析

動的解析を使用すると、複数の名前と値のペアを変更しないで表示できます。この点は静的解析と異なります。静的解析では、値を抽出し、CEG などのあらかじめ定義されたフィールドにそれらの値を設定します。動的解析が便利なのは、アプリケーションやフォーマットがキー ペアに記録するイベント データを変更しないで、つまり、CEG の名前やその他の値に解析しないで表示する場合です。動的解析を適用できれば、解析パフォーマンスも向上します。

動的解析が可能な正規表現には、以下の 4 つの要素が含まれます。

1. ペアのキーのインジケータ「(_PAIR_KEY_)」
2. ペアの値のインジケータ「(_PAIR_VALUE_)」
3. ペアのキーと値の区切り文字
4. ペアの指定全体と次の指定の区切り文字

使用する区切り文字は、解析対象のイベントソースの構造と一致する必要があります。イベントソースが区切り文字としてカンマを使用する場合、正規表現でも同様にカンマを使用する必要があります。

例

```
(_PAIR_KEY_) = (_PAIR_VALUE_) ;
```

この例で、キーと値の区切り文字は「=」です。ペアの区切り文字は「;」です。

他の正規表現の後にこの表現を使用することにより、XMP ファイルでは、解析されたイベントに表示されるキー ペアをすべて特定し表示できます。

解析トークン

解析トークンは、解析フィルタを構築する際に使用できる正規表現テンプレートです。CA Enterprise Log Manager には、事前定義済み解析トークンで構成された解析トークンライブラリが含まれています。たとえば、_IP_ トークンは、一般的な IP アドレス形式を解析する正規表現を設定する際に使用できます。解析フィルタを使用して IP アドレスを抽出する場合、毎回完全な正規表現言語を作成しなくても、フィルタに _IP_ トークンを挿入すれば済みます。

また、独自のカスタム解析トークンを作成し、ローカルライブラリに追加したり、別の CA Enterprise Log Manager 環境にエクスポートして使用したりすることもできます。カスタムトークンをエクスポートする場合は、まずライブラリに追加します。また、カスタムトークンを別の CA Enterprise Log Manager 環境からインポートすることも可能です。テスト環境で解析トークンを作成して、ライブ環境に移動させることができます。

詳細情報:

[日時トークンの値](#) (P. 546)

[ライブラリへのカスタムトークンの追加](#) (P. 549)

[ライブラリからのカスタムトークンの削除](#) (P. 550)

[解析トークンのインポート](#) (P. 551)

[解析トークンのエクスポート](#) (P. 552)

日時トークンの値

CA Enterprise Log Manager は、日時解析トークンのさまざまな構文オプションをサポートしています。これらのオプションを解析ファイルの日時形式で使用して、使用日時スタンプの表示をカスタマイズできます。

日時トークンは、以下のいずれかで構成されます。

- 通常の文字（「%」とスペース文字は除く）。入力されたとおりに表示される文字。時間値を区切るためのコロンなど。

または

- 変換指定。変換指定は、「%」文字に、出力表示を定義する変換文字を付加して構成される。当月を表示する %m など。

CA Enterprise Log Manager では、以下の変換指定をサポートしています。

%a または %A

ローカルの曜日の名前を、完全形または短縮形で表示します。Windows では、この指定で利用できるのは US 英語のみです。

%b または %B または %h

ローカルの月の名前を、完全形または短縮形で表示します。Windows では、この指定で利用できるのは US 英語のみです。

%c

ローカルの日付と時間を表示します。

%C

世紀を表す数 (0 ~ 99) を表示します。

%d または %e

月内の日付 (1 ~ 31) を表示します。

%D

日付をアメリカ式 (月/日/年) で表示します。%m/%d/%y と入力した場合と同じです。

注: %d/%m/%y は、ヨーロッパで使われる構文です。ISO 8601 標準形式は %Y-%m-%d です。

%H

時間を 24 時間形式 (0 ~ 23) で表示します。

%I

時間を 12 時間形式(1 ~ 12)で表示します。

%j

年内の日付(1 ~ 366)を表示します。

%m

月を表す数(1 ~ 12)を表示します。

%M

分(0 ~ 59)を表示します。

%n

任意のスペースを挿入します。

%p

ある場合は、ローカルで AM または PM に相当するものを表示します。

%r

時刻を 12 時間形式(時間:分:秒 AM/PM)で表示します。**%l:%M:%S %p** と入力した場合と同じです。ローカルの LC_TIME セクションの **t_fmt_ampm** が空の場合、この動作は定義されません。

%R

時刻を 24 時間形式(時間:分)で表示します。**%H:%M** と入力した場合と同じです。

%S

秒を表示します(0 ~ 60。60 はうるう秒の場合に発生します)。

%t

任意のスペースを表示します。

%T

時刻を 24 時間形式(時間:分:秒)で表示します。**%H:%M:%S** と入力した場合と同じです。

%U

週を表す数を表示します。日曜を週の 1 日目とします(0 ~ 53)。1 月の最初の日曜が、週 1 の 1 日目となります。

%w

曜日を表す数(0 ~ 6)を、日曜 =0 として表示します。

%W

週を表す数(0 ～ 53)を、月曜を週の 1 日目として表示します。1 月の最初の月曜が、週 1 の 1 日目となります。

%x

ローカルの日付形式を使用して、日付を表示します。

%X

ローカルの時刻形式を使用して、時刻を表示します。

%y

現在の世紀(0 ～ 99)で年を表示します。世紀が指定されていない場合、69 ～ 99 の範囲内の値は 20 世紀(1969 ～ 1999)の年を指し、00 ～ 68 の範囲内の値は 21 世紀(2000 ～ 2068)の年を指します。

%Y

世紀を含めて、年を表示します(1991 年など)。

%z

RFC-822/ISO 8601 標準タイムゾーン指定を表示します。この指定は Windows では利用できません。

デフォルトの CA Enterprise Log Manager 日時トークン形式は、以下のとおりです。

%d/%b/%Y:%H:%M:%S %z

ライブラリへのカスタムトークンの追加

カスタム解析トークンをトークン ライブラリに追加し、ほかのユーザが利用できるようにできます。たとえば、メッセージ解析ファイルの作成プロセス中に作成したカスタムトークンがほかの解析にも役立つ場合には、ライブラリに追加して、再使用できます。

以下の手順は、解析ファイルや解析フィルタの作成中にトークンを追加することを想定しています。

カスタム解析トークンをライブラリに追加するには、以下の手順に従います。

1. メッセージ解析ウィザードを開き、[一致および解析]の手順に進みます。
2. 解析ファイル フィルタ ウィザードを開き、[正規表現]の手順に進みます。
3. [新しい正規表現]をクリックして、解析トークンを作成し、[トークンの詳細]ペインに正規表現構文を入力します。
4. 新しい解析トークンを選択し、[選択したトークンをライブラリに追加します]をクリックします。

確認のダイアログ ボックスが表示されます。

5. [はい]をクリックします。
6. (オプション) [ライブラリに対してトークンを追加または削除します]をクリックし、新しいトークンを表示します。

[解析トークン ライブラリ] ダイアログ ボックスが表示され、カスタムトークンが黒で、事前定義済みトークンが緑で表示されます。

ライブラリからのカスタムトークンの削除

不要なカスタムトークンや使わなくなったカスタムトークンをトークン ライブラリから削除できます。事前定義済みトークンを削除することはできません。

ライブラリからカスタムトークンを削除するには、以下の手順に従います。

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [イベント精製ライブラリ]フォルダの横の矢印をクリックしてフォルダを展開し、[マッピングおよび解析]フォルダを選択します。
製品統合のボタンが詳細ペインに表示されます。
3. [新規メッセージ解析ルール]をクリックします。
解析ファイル ウィザードが開きます。
4. [一致および解析]の手順に進みます。
5. 事前一一致フィルタを選択し、[編集]をクリックします。または、[解析フィルタ]リストの上部の[解析フィルタの追加]をクリックします。
解析ファイル フィルタ ウィザードが表示されます。
6. [正規表現]の手順に進みます。
7. [ライブラリに対してトークンを追加または削除します]をクリックします。
[解析トークン ライブラリ] ダイアログ ボックスが表示され、カスタムトークンが黒で、事前定義済みトークンが緑で表示されます。
8. 削除するカスタムトークンを 1 つ以上選択し、[選択したトークンをライブラリから削除します]をクリックします。
確認のダイアログが表示されます。
9. [はい]をクリックし、[OK]をクリックします。

解析トークンのインポート

解析トークンをインポートして、別の管理サーバで作成したカスタム解析トークンを現在のサーバに、たとえば、テスト環境から実動環境に追加できます。

解析トークンをインポートするには、以下の手順に従います。

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [イベント精製ライブラリ]フォルダの横の矢印をクリックしてフォルダを展開し、[マッピングおよび解析]フォルダを選択します。
製品統合のボタンが詳細ペインに表示されます。
3. [新規メッセージ解析ルール]をクリックします。
解析ファイル ウィザードが開きます。
4. [一致および解析]の手順に進みます。
5. 事前一一致フィルタを選択し、[編集]をクリックします。または、[解析フィルタ]リストの上部の[解析フィルタの追加]をクリックします。
解析ファイル フィルタ ウィザードが表示されます。
6. [正規表現]の手順に進みます。
7. [解析トークン]ペインの一番上の[ユーザトークンのインポート]をクリックします。
[ファイルのインポート]ダイアログ ボックスが表示されます。
8. インポートするトークン(.tok)ファイルを参照し、[OK]をクリックします。
確認のダイアログが表示されます。
9. ファイルをインポートする場合は「はい」をクリックし、ライブラリ内のほかのユーザトークンを上書きします。

解析トークンのエクスポート

トークン ライブラリに追加した解析トークンをエクスポートして、現在の管理サーバ上で作成したカスタム解析トークンを別のサーバに移動できます。たとえば、カスタムトークンをテスト環境からライブ環境にエクスポートできます。

解析トークンをエクスポートするには、以下の手順に従います。

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダ リストが表示されます。
2. [イベント精製ライブラリ]フォルダの横の矢印をクリックしてフォルダを展開し、[マッピングおよび解析]フォルダを選択します。
製品統合のボタンが詳細ペインに表示されます。
3. [新規メッセージ解析ルール]をクリックします。
解析ファイル ウィザードが開きます。
4. [一致および解析]の手順に進みます。
5. 事前一一致フィルタを選択し、[編集]をクリックします。または、[解析フィルタ]リストの上部の[解析フィルタの追加]をクリックします。
解析ファイル フィルタ ウィザードが表示されます。
6. [正規表現]の手順に進みます。
7. [解析トークン]ペインの一番上の[ユーザトークンのエクスポート]をクリックします。
ダウンロードの場所を選択するダイアログ ボックスが表示されます。
8. エクスポートされたファイルを保存する場所を選択し、[保存]をクリックします。
エクスポートされたファイルが選択した場所に保存されます。

XMP ファイルの分析

メッセージ解析ユーティリティを使用して、新しいファイルや編集済みファイル进行分析し、サンプル イベントに対する解析ファイルの効果を測定できます。分析によって、ファイルを保存する前に変更を加え、ファイルの有効性を改善することができます。

ユーティリティでは、選択したサンプル イベント セットに対する XMP ファイルの分析を、以下のプロセスで実行します。

1. XMP ファイルに定義された事前一一致文字列を含むすべてのイベントを特定します。ユーティリティは、事前一一致文字列ごとに検索を実行し、その文字列を含んでいるすべてのイベントを検出します。
2. 事前一一致イベントごとに、イベントを解析してトークンを作成する最初の解析フィルタを検出します。

XMP ファイルの分析方法

解析ウィザードを開き、「解析の分析」の手順に進みます。ウィザードには、事前一一致文字列およびフィルタの一致数が表示されます。一致数が多いほど、新しい XMP ファイルや編集済み XMP ファイルの効率は向上します。これによって、未解析のままの重要な情報がないかどうかを判別することもできます。

XMP ファイルのサイズとサンプル イベントの数がどちらも大きい場合は、XMP 分析の処理にある程度の時間がかかる場合があります。通常は 1 分以上かかることはありません。あまりにも長くかかっている場合はこのプロセスをキャンセルし、イベントの数を減らして再分析できます。

新しくルールを作成すると、バージョン 1.0 として保存されます。後でこのルールを編集すると、新しいルールを保存するたびに新バージョンとして保存されます。以前のバージョンを表示し、必要に応じて適用したりコピーしたりすることができます。

データ マッピング ファイルを作成する方法

マッピング ファイル ウィザードを使用して、データ マッピング ファイルの作成および編集を実行できます。データ マッピング ファイルによって、解析済みテキスト文字列またはフィールド/値ペアが CEG 互換フィールドにマッピングされ、ネイティブ イベントが精製済みイベントに変換されます。これを実行するために、マッピング ファイル ウィザードを使用して、さまざまなタイプのマッピングを作成および編集することができます。

DM ファイルを作成または編集するプロセスは、以下の手順で構成されます。

1. マッピング ファイル ウィザードの表示
2. ファイル詳細の入力
3. 解析ファイルを使用するサンプル イベントの特定と追加
4. 必要に応じた直接マッピングの設定
5. 必要に応じた関数マッピングの設定
6. 必要に応じた条件付きマッピングの設定
7. 必要に応じたブロック マッピングの設定

注: ブロック マッピングを使用して、直接マッピングや関数マッピングを設定できます。これは、手順 4 および 5 のマッピング設定の代替となります。

8. 完了した DM ファイルの分析および保存

DM ファイルを作成する際には、ファイル内の個別のマッピング タイプだけでなく、ファイル自体のデータ マッピングの優先順位も考慮してください。完了した DM ファイルによって、マッピング タイプ画面(ウィザードの手順 4 から 7)の順序でイベント情報がチェックされます。重複するマッピング タイプが存在する場合、DM ファイルが最後に検出した値が割り当て値になります。

たとえば、DM ファイルが、あるネイティブ イベント値の直接マッピングを検出し、その後に同じ値の別の条件付きマッピングを検出した場合、精製済みイベントには条件付きマッピングの結果が使用されます。

特定のマッピング タイプ内部で重複しているマッピングは、タイプによって扱われ方が異なります。

- 直接マッピングおよび関数マッピング -- DM ファイルは、最後に検出した一致値を使用します。重複している関数マッピングが検出された場合は、最後の関数が呼び出されます。たとえば、最初の関数が見つからなかった場合や期待どおりに機能しなかった場合に 2 番目の関数を呼び出すよう重複マッピングを設定することができます。
- 条件付きマッピングおよびブロック マッピング -- DM ファイルは、最初に検出した値を適用し、検索を停止します。パフォーマンス向上のため、これらのマッピング タイプでは、より一般的な条件がファイルの最初に来るよう定義してください。

マッピング順の設計主旨に関する詳細情報は、各マッピング タイプ手順に記載されています。

詳細情報

[ブロック マッピングの設定](#) (P. 564)

[マッピング分析の実行](#) (P. 566)

マッピング ファイル ウィザードの表示

DM ファイルを新規作成するか、既存の DM ファイルを編集するには、マッピング ファイル ウィザードを起動する必要があります。

マッピング ファイル ウィザードを表示する方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。
2. [イベント精製ライブラリ]フォルダの横の矢印をクリックしてフォルダを展開し、[マッピングおよび解析]フォルダを選択します。
製品統合のボタンが詳細ペインに表示されます。

3. [新規マッピング ファイル]をクリックします。 

マッピング ファイル ウィザードが表示されます。

ウィザードの使用時の操作

- ウィザードを閉じずにファイルを保存するには、[保存]をクリックします。
- ファイルを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

詳細情報

[concat 関数マッピングの設定](#) (P. 561)

[ブロック マッピングの設定](#) (P. 564)

[マッピング分析の実行](#) (P. 566)

ファイル詳細の指定

新しい DM ファイルのファイルの詳細を指定します。サブスクリプション ファイルを、別の名前でカスタム ファイルとして保存できます。

マッピング ファイルの詳細を指定する方法

1. マッピング ファイル ウィザードを開きます。
2. DM ファイルの名前を入力します。ファイル名は必須で、使用できない文字は、/ ¥ : * ? “ < > ^ ; " , & { } [] . または | です。
3. サンプル イベントの解析に使用する解析ファイルの名前とバージョンを、[解析ファイル] ドロップダウンリストから選択します。

ログ名フィールドに、入力した解析ファイルの名前が自動的に挿入されます。

4. (オプション) 説明を入力します。
5. (オプション) [サポート情報] 領域の [製品の追加] をクリックし、参照用に製品名およびバージョンを入力します。
6. 該当する矢印をクリックして次に完了するウィザード手順に進むか、[保存して閉じる] をクリックします。

[保存して閉じる] をクリックすると、新規ファイルが [マッピング ファイル] ユーザ フォルダに表示されます。それ以外の場合は、選択した手順が表示されます。

サンプル イベントの利用

マッピング ファイル ウィザードを使用して、DM ファイルの分析に使用するサンプル イベントを検索できます。イベント ログ ストアを検索することも、ログ ファイルから直接サンプル イベントを利用することも可能です。サンプル イベントによって、ウィザードの最終手順でマッピング 出力をテストするためのテンプレートが得られます。

サンプル イベントの利用方法

1. マッピング ファイル ウィザードを開き、[サンプル イベント] の手順に進みます。

[サンプル イベント] 画面が表示されます。

2. [サンプル イベントの検索]領域にあるオプション ボタンの[ログ ストア]または[ログ ファイル]を選択します。
3. [ログ ストア]を選択した場合
 - a. [解析列]ドロップダウン メニューから適切なサンプル イベントソースのタイプを選択します。WMI イベントソースの場合は **result_string** を、syslog イベントソースの場合は **raw_event** を選択します。
 - b. [クエリ タグ フィルタ]および[クエリ リスト]を使用して、サンプル イベントの利用に使用するクエリを選択します。

クエリが表示され、サンプル イベントが表示されます。

注: サンプル イベントの検索には、すべての既存のクエリやカスタム クエリを使用できます。カスタム クエリを使用する場合は、データ マッピング ファイルの設計手順を開始する前に、カスタム クエリの作成とテストを実行しておくことをお勧めします。
4. [ログ ファイル]を選択した場合
 - a. [参照]で目的のログ ファイルを選択し、[アップロード]をクリックします。

ログ ファイルのイベントが、[サンプル イベント]ペインに表示されます。

注: ウィザードでは、ファイル内の各行がイベントとみなされます。複数行で構成されるイベントはサポートされません。
 - b. 解析済みサンプルに含める動的なペアの値がサンプル ログ ファイルに含まれている場合は、[動的フィールドの抽出]をクリックします。
5. 該当する矢印をクリックして次に完了するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、新規ファイルが[マッピング ファイル]ユーザ フォルダに表示されます。それ以外の場合は、選択した手順が表示されます。

詳細情報:

[動的解析](#) (P. 544)

直接マッピングの設定

直接マッピングは、ネイティブ イベントと単一の精製済みイベント値を 1 対 1 対応で設定します。そのため、直接マッピングは、デフォルト値のほか、一般的な値でも `ideal_model` フィールドのようにめったに変化しないものに対してのみ使用することをお勧めします。

マッピングに設定できる精製済みイベント値の定義は、以下のとおりです。

テキスト値

特定の CEG フィールド用の特定のテキストを設定します。適切なイベントがマッピングされるたびに、この値が表示されます。たとえば、CEG `ideal_model` フィールドを「ファイアウォール」に設定すると、そのマッピングを含むすべてのルールで、`ideal_model` フィールドに「ファイアウォール」と表示されます。

フィールド値

特定の CEG フィールドまたは解析済みフィールドに含まれる、元のイベントフィールドの内容を設定します。フィールド値は、ドル記号「\$」を前に付けることでテキスト値と区別します。たとえば、CEG `event_logname` フィールドを「\$ ログ」に設定すると、ネイティブ イベントの[ログ]フィールドに表示されるすべてのテキストがマップ済みイベントに表示されます。

直接マッピングの設定方法

1. マッピング ファイル ウィザードを開き、名前を入力し、マッピング ファイル用のログ名を選択して、[直接マッピング]の手順に進みます。

[直接マッピング]画面が表示され、現在のマッピングまたはデフォルト マッピングが表示されます。[名前]列に CEG フィールド名または解析済みフィールド名が表示されます。[値]列にテキスト値またはフィールド値のどちらかが表示されます。

注: 解析済みフィールド値を表示するには、[サンプル イベントの利用]の手順で解析ファイルを選択してください。

2. [直接マッピングの追加]をクリックして新しいマッピング エントリを表の下部に追加して選択するか、現在の直接マッピングを選択して編集します。

そのフィールド用の直接マッピングがあれば、[マッピングの詳細]領域に表示されます。

3. 使用可能であれば、[フィールド]ドロップダウン メニューからマッピング先の **CEG** フィールドまたは解析済みイベント フィールドを選択します。入力し始めると、オートコンプリート機能によって、使用可能な **CEG** フィールドのリストが絞り込まれます。
4. [値の追加] エントリ フィールドに新しい値を入力し、その横にある[直接マッピングの追加]をクリックします。値の前に「\$」を入力すると、テキスト値ではなくフィールド値を表します。

[選択されたフィールド] 領域に値が表示されます。

5. (オプション) 1 つのフィールドに複数の直接マッピングを入力し、上矢印や下矢印を使用して、**DM** ファイルがマッピング分析する順序を設定することができます。精製済みイベントには、**DM** ファイルによって最後に検出された直接マッピングが表示されます。

注: 複数の値を追加するとマッピングのパフォーマンスが低下するため、この機能の使用は控えめにしてください。

6. (オプション) シャトル コントロールを使用して、不要な値を[使用可能なフィールド] 領域に移動し、現在のマッピング用として分析されないようにします。
7. 必要な直接マッピングをすべて追加したら、適切な矢印をクリックして次に実行するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、新規ファイルが[マッピング ファイル] ユーザー フォルダに表示されます。それ以外の場合は、選択した手順が表示されます。

関数マッピングの設定

関数マッピングでは、精製済みイベントとして表示する精製済みイベント情報を取得または定義するために、関数を使用した値と **CEG** フィールドをリンクします。すべての関数マッピングは、**CEG** フィールド名、事前定義済みフィールド値またはクラスフィールド値、および関数から構成されます。

たとえば、関数マッピングでは、**concat** 関数を使用して一連のネイティブ イベントの値を連結し、単一の **CEG** フィールドと関連付けることができます。

重複した関数マッピングがある場合、**DM** ファイルでは最後に検出されたものが使用されます。最初の関数が見つからなかった場合や期待どおりに機能しなかった場合に 2 番目の関数を呼び出すよう重複マッピングを設定することができます。

関数マッピングの設定方法

1. マッピング ファイル ウィザードを開き、名前を入力し、マッピング ファイル用のログ名を選択して、[関数マッピング]の手順に進みます。

[関数マッピング]画面が表示され、現在のマッピングまたはデフォルトマッピングが表示されます。[名前]列には **CEG** フィールド名または解析済みフィールド名が、[関数]列には現在リンクされている関数が、[値]列にはテキストまたはフィールド値が表示されます。

注: 解析済みフィールド値を表示するには、[ファイル詳細の指定]の手順で解析ファイルを選択してください。

2. [関数マッピングの追加]をクリックして新しいマッピング エントリを追加するか、現在のマッピングを選択して編集します。

マッピング エントリが[マッピングの詳細]ペインに表示されます。

3. [フィールド]ドロップダウン メニューからマッピング先の **CEG** フィールドを選択します。入力し始めると、オートコンプリート機能によって、使用可能な **CEG** フィールドのリストが絞り込まれます。

4. [関数]ドロップダウン メニューからマッピングに使用する関数を選択します。

注: 複数のターゲット値を指定するため、連結 (**concat**) 関数はほかのものとは働きが異なります。詳細については、「**concat** 関数マッピングの設定」を参照してください。

5. [値の追加]エントリフィールドにマッピングのターゲット値を入力し、その横にある[値の追加]ボタンをクリックします。値の前に「\$」を入力すると、特定の値ではなくフィールド値を表します。

[選択されたフィールド]領域に値が表示されます。

6. (オプション)1 つのフィールドに複数のマッピングを入力し、上矢印や下矢印を使用して、**DM** ファイルがマッピング分析する順序を設定することができます。

注: 複数の値を追加するとマッピングのパフォーマンスが低下するため、必要に応じて、スタンドアロンの関数マッピングのみを使用してください。

7. (オプション)シャトル コントロールを使用して、不要な値を[使用可能なフィールド]領域に移動し、現在のマッピング用として分析されないようにします。
8. 必要な関数マッピングをすべて追加したら、適切な矢印をクリックして次に実行するウィザード手順に進むか、[保存して閉じる]をクリックします。
[保存して閉じる]をクリックすると、新規ファイルが[マッピング ファイル] ユーザ フォルダに表示されます。それ以外の場合は、選択した手順が表示されます。

concat 関数マッピングの設定

concat 関数マッピングは、関数マッピングの一種です。1 つのターゲットフィールドまたは値を指定するほかの関数マッピングと異なり、**concat** 関数では複数のマッピング ターゲットを指定し、これらを連結して 1 つの CEG フィールドと関連付けます。

データ マッピング ウィザードを使用して、**concat** 関数マッピングを作成できます。**concat** マッピングはほかの関数マッピングとは異なるため、作成手順も多少異なったものになります。

concat 関数マッピングの設定方法

1. マッピング ファイル ウィザードを開き、名前を入力し、マッピング ファイル用のログ名を選択して、「関数マッピング」の手順に進みます。
[関数マッピング]画面が表示され、現在のマッピングまたはデフォルトマッピングが表示されます。[名前]列には CEG フィールド名が、[関数]列には現在リンクされている関数が、[値]列にはテキストまたはフィールド値が表示されます。
2. [関数マッピングの追加]をクリックして新しいマッピング エントリを追加します。
マッピング エントリが[マッピングの詳細]ペインに表示されます。
3. [フィールド]ドロップダウン メニューからマッピング先の CEG フィールドを選択します。

4. [関数]ドロップダウン メニューから **concat** 関数を選択します。
[フォーマット]フィールドおよび[値]フィールドが表示されます。
注: **concat** 関数の値は、[関数マッピング]ペインに {...} と表示されます。これは、値が 1 つではなく、値のセットであることを表しています。
5. (オプション) [フォーマット]フィールドに指定子を入力し、ターゲットフィールドの配置を制御します。フォーマット指定子(%s)は、フィールドの位置を示します。%s 以外の指定子はすべて、最終のテーブル コレクタフィールドに含められる静的サポート データとみなされます。たとえば、2 つのターゲットフィールドをコロンで区切るには、[フォーマット]フィールドに「%s:%s」と入力します。
6. [Concat 値]領域の[concat 値の追加]をクリックし、ターゲット入力/値ペアを追加します。
7. [値の追加]エントリフィールドに値を入力し、[値の追加]をクリックします。
[選択されたフィールド]領域に値が表示されます。
8. 連結する値を追加するには、手順 6 および 7 を繰り返します。少なくとも 2 つのターゲット値を追加する必要があります。
9. 必要な **concat** マッピングをすべて追加したら、適切な矢印をクリックして次に実行するウィザード手順に進むか、[保存して閉じる]をクリックします。
[保存して閉じる]をクリックすると、新規ファイルが[マッピング ファイル]ユーザフォルダに表示されます。それ以外の場合は、選択した手順が表示されます。

条件付きマッピングの設定

条件付きマッピングでは、CEG フィールドが可能性のあるさまざまな結果にリンクされ、特定のフィールド用にデフォルトや条件値を設定することができます。たとえば、条件付きマッピングを使用して、成功値や失敗値をマッピングしたり、イベントソースを名前やグループで識別したりすることができます。

条件付きマッピングによって、特定の CEG フィールドに、デフォルト値と 1 つ以上の条件値が割り当てられます。条件値ごとに条件を設定できます。イベントが条件と一致すると、選択されたフィールドに適切な条件値が割り当てられます。一致しない場合は、精製済みイベント フィールドにデフォルト値が表示されます。

重複した条件付きマッピングがある場合、DM ファイルでは最初に検出されたものが使用され、それ以上の分析は行われません。パフォーマンスを向上させるために、一般的な条件を最初に定義してください。

注： スタンドアロンの条件付きマッピングは、ブロック マッピングより遅くなります。必要な場合は、単独で使用することをお勧めします。

条件付きマッピングの設定方法

1. マッピング ファイル ウィザードを開き、名前を入力し、マッピング ファイル用のログ名を選択して、[条件付きマッピング]の手順に進みます。

[条件付きマッピング]画面が表示され、現在のデフォルト マッピングが表示されます。[フィールド]列に **CEG** フィールド名または解析済みフィールド名が、[値]列に現在のデフォルト値が表示されます。

注： 解析済みフィールド値を表示するには、[ファイル詳細の指定]の手順で解析ファイルを選択してください。

2. [条件付きフィールド マッピング]リストで[条件付きマッピングの追加]をクリックし、新しい行を選択します。

[マッピングの詳細]ペインが表示され、[フィールド]ドロップダウンリストおよび[値]シャトル コントロールが表示されます。

3. [フィールド]メニューからマッピング先の **CEG** フィールドを選択します。入力始めると、オートコンプリート機能によって、使用可能な **CEG** フィールドのリストが絞り込まれます。

4. [値の追加]エントリフィールドに必要なデフォルト マッピングを入力し、[値の追加]をクリックして、[選択されたフィールド]ペインに表示します。不要な値を削除するには、[使用可能なフィールド]ペインにそれらを移動します。

5. [条件値]リストの[条件値の追加]をクリックします。

新しい値が表示されます。

6. [新しい値]のテキストを選択して強調表示し、名前を変更します。

新しい名前がリストに表示され、フィルタ ダイアログ ボックスが[詳細]ペインに表示されます。

7. 条件値を定義するフィルタを作成します。たとえば、1 つ以上のフィルタを作成して、`event_source_address` フィールドを IP アドレスにリンクし、地理的なグループなど、ビジネス グループに属するイベントソースを特定することができます。
8. 必要な条件付きマッピングをすべて追加したら、適切な矢印をクリックして次に実行するウィザード手順に進むか、[保存して閉じる]をクリックします。
[保存して閉じる]をクリックすると、新規ファイルが[マッピング ファイル] ユーザ フォルダに表示されます。それ以外の場合は、選択した手順が表示されます。

ブロック マッピングの設定

ブロック マッピングを使用すると、選択した条件を、定義された一連のマッピングにリンクして、条件によって有効になるマッピング カスケードを作成できます。ブロック マッピングには、直接マッピングや関数マッピングを組み合わせで使用できます。どちらのタイプの内部ブロック マッピングも、スタンドアロンのマッピングの場合とまったく同じように機能します。

単一のマッピング ファイルに対し、必要に応じていくつでもブロックを作成できます。各ブロックには名前と条件が含まれます。

あるブロックに重複したマッピングがある場合、DM ファイルでは最初に検出されたものが使用され、それ以上の分析は行われません。パフォーマンスを向上させるために、一般的な条件を最初に定義してください。

ブロック マッピングの設定方法

1. マッピング ファイル ウィザードを開き、名前を入力し、マッピング ファイル用のログ名を選択して、「ブロック マッピング」の手順に進みます。
[ブロック マッピング]画面が表示され、現在のブロック マッピングが表示されます。
2. [ブロック マッピング]ペインで、[ブロック マッピングの追加]をクリックします。
[ブロック マッピング]リストに新しいブロックが表示されます。

3. [新しいブロック]テキストを選択します。
[ブロック定義]ペインが開いて、「手順 1 条件の定義」が表示されます。
4. ブロック名を入力し、このブロックの条件を定義するフィルタを作成します。
たとえば、イベントプロセスの成功が検出された場合にブロック マッピング
を実行するには、`event_result` を「=S」と定義します。
5. 手順 2 のバーをクリックし、スタンドアロンのマッピング手順と同じプロセスを
使用して必要な直接マッピングをすべて入力します。
6. 手順 3 のバーをクリックし、スタンドアロン マッピング手順と同じプロセスを使
用して必要な関数マッピングをすべて入力します。
7. 必要なブロック マッピングをすべて追加したら、適切な矢印をクリックして次
に実行するウィザード手順に進むか、[保存して閉じる]をクリックします。
[保存して閉じる]をクリックすると、新規ファイルが[マッピング ファイル]
ユーザフォルダに表示されます。それ以外の場合は、選択した手順が表示
されます。

詳細情報

[詳細フィルタの使用](#) (P. 487)

マッピング分析の実行

マッピング ウィザードを使用して、データ マッピング ファイルを分析し、マッピング ファイルの効率を向上させるための変更をテストして実行することができます。サンプル イベントは **DM** ファイルでテストされ、結果が **CEG** で検証されます。

マッピング分析を実行するには、マッピング ファイル ウィザードの[マッピング分析手順]をクリックします。ウィザードに、「サンプル イベント」の手順で入力したサンプル イベントの解析結果を示す表が表示されます。

完了した **DM** ファイルには、マッピングが保存され、マッピング タイプ画面(ウィザード手順 4 から 7)の順序でイベント情報が分析されます。重複するマッピングが存在する場合、**DM** ファイルが最後に検出した値が割り当て値になります。たとえば、**DM** ファイルが、あるネイティブ イベント値の直接マッピングを検出し、その後に同じ値の別の条件付きマッピングを検出した場合、精製済みイベントには条件付きマッピングの結果が表示されます。マッピング順の設計主旨に関する詳細情報は、各マッピング タイプ手順に記載されています。

新しくルールを作成すると、バージョン **1.0** として保存されます。後でこのルールを編集すると、新しいルールを保存するたびに新バージョンとして保存されます。以前のバージョンを表示し、必要に応じて適用したりコピーしたりすることができます。

イベント転送ルール タスク

イベント転送ルールを使用すると、外部のアプリケーションやシステム内のリモートリスナに転送する **CA Enterprise Log Manager** イベントを選択できます。転送ルールを使用して、転送するイベントの特定、転送するタイミングの設定、受信方法の制御を実行できます。受信イベントが転送ルール フィルタに一致すると、**CA Enterprise Log Manager** によってイベントのコピーが作成されて転送されます。イベントは、イベント ログ ストア内にも記録されます。

イベント転送ルール タスクは、**CA Enterprise Log Manager** インターフェースの[ログ収集]領域から実行します。イベント転送ルールの作成、編集、および削除を実行できます。また、イベント転送ルールのインポートおよびエクスポートも可能です。

詳細情報:

[イベント転送ルールを作成する方法 \(P. 567\)](#)

イベント転送ルールを作成する方法

イベント転送ルールを使用して、外部のアプリケーションに CA Enterprise Log Manager イベントを送信できます。たとえば、syslog を使用して、CA NSM にイベントを送信できます。イベント転送ルールを使用すると、転送するイベントの条件の設定や、1 つ以上の受信者の設定を行うことができます。

イベント転送ルールウィザードを使用して転送ルールを作成するプロセスは、以下の手順で構成されます。

1. 転送ルールウィザードの表示
2. ルールの名前と、任意で説明の入力
3. 転送するイベントを特定するための単純フィルタや詳細フィルタの作成
4. 転送の宛先や、転送されるイベントに含める CEG フィールドなどのルールの属性の設定

詳細情報:

[転送ルールの名前指定](#) (P. 568)

[単純イベントフィルタの作成](#) (P. 569)

[詳細イベントフィルタの作成](#) (P. 572)

[詳細フィルタの使用](#) (P. 511)

[転送ルール属性の設定](#) (P. 573)

転送ルール ウィザードを開く

転送ルールを作成するか、既存の転送ルールを編集するには、転送ルールウィザードを開きます。

転送ルール ウィザードを開くには、以下の手順に従います。

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。
2. [転送ルール]フォルダを選択します。

転送ルールのボタンが詳細ペインに表示されます。

3. [新規転送ルール]をクリックします。 

転送ルール ウィザードが開きます。

ウィザードの使用時の操作

- ウィザードを閉じずにルール ファイルを保存するには、[保存]をクリックします。
- ルール ファイルを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

転送ルールの名前指定

転送ルールの名前を指定する必要があります。参照用に、説明情報を入力することもできます。

転送ルールの名前を指定するには、以下の手順に従います。

1. 転送ルール ウィザードを開きます。
2. ルールの名前を入力します。名前は必須で、使用できない文字は、/ ¥ : * ? < > ; ' , & { } [] . または | です。
3. (オプション) 参照用に、ルールの説明情報を入力します。
4. [フィルタリング]の手順に進みます。

単純イベント フィルタの作成

単純フィルタを作成して、共通の CEG フィールドに検索パラメータを設定できます。たとえば、[理想モデル]フィールドを「コンテンツ管理」に設定して、理想モデル CEG フィールドの値を持つすべてのイベントを特定することができます。単純フィルタは、クエリ、抑制および集約ルール、イベント転送ルールを含む多くの機能で使用されます。

単純フィルタを作成する方法

1. [理想モデル]チェック ボックスを選択します。または、定義するイベントフィールドを選択し、ドロップダウンリストから値を選択するか、このテキストフィールドに必要な値を入力します。
2. (オプション)クエリフィルタを作成する場合、[ソース]、[宛先]または[エージェント]フィールドのいずれかのチェック ボックスを選択し、該当するテキストフィールドに必要な値を入力します。
3. 手順 1 から 2 を繰り返して、その他の単純フィルタを追加します。
4. 必要な単純フィルタをすべて追加したら、[保存]をクリックします。

詳細情報

[詳細フィルタの使用](#) (P. 487)

[詳細イベント フィルタの作成](#) (P. 572)

詳細フィルタの使用

SQL ベースの詳細フィルタを使用すると、イベントログストアにクエリを実行するすべての機能の条件を指定し、クエリの絞り込みやクイック フィルタのカスタマイズを行うことができます。[詳細フィルタ]インターフェースでは、フィルタ要件に応じてロジック、列、演算子、および値を入力する形式を指定することによって、適切なフィルタ構文を作成できるようにします。

注: このセクションには、詳細フィルタに使用される SQL 用語の概要が含まれています。詳細フィルタの機能を十分に活用するには、SQL および共通イベント文法を完全に理解しておく必要があります。

以下の SQL 条件は、複数のフィルタ ステートメントを結合します。

AND

結合された すべての用語が TRUE の場合は、イベント情報を表示します。

OR

結合された用語のいずれかが **TRUE** の場合は、イベント情報を表示します。

HAVING

条件文を追加することによって、メインの **SQL** 文の条件を絞り込みます。たとえば、特定のホストからのイベント用に詳細フィルタを設定している場合に、「**having**」ステートメントを追加して、このホストからのイベントのうち指定した重大度のものだけを返すようにすることができます。

以下の **SQL** 演算子は詳細フィルタによって使用され、基本条件を作成します。

関係演算子

列が入力した値と適切な関係を保持する場合は、イベント情報を表示します。次の関係演算子を使用できます。

- 等しい
- 等しくない
- < (より小さい)
- > (より大きい)
- ≤ (以下)
- ≥ (以上)

たとえば、[> (より大きい)]を使用すると、設定した値よりも大きい値の選択列からイベント情報が含められます。

に近い

入力したパターンが列に含まれている場合に、**%**を使用して該当するパターンを設定し、イベント情報を含めます。たとえば、**L%** は **L** で始まる任意の値を返しますが、**%L%** は **L** が最初の文字にも最後の文字にも含まれない任意の値を返します。

に近くない

列に指定したパターンが含まれていない場合にイベント情報を含めます。

設定が含まれている

引用符で囲まれた一連の入力値のうち、**1** つ以上が対象の列に含まれている場合に、イベント情報を含めます。セット内に複数の値がある場合は、カンマで区切る必要があります。

設定が含まれていない

引用符で囲まれた一連の入力値のうち、1 つ以上が対象の列に含まれていない場合に、イベント情報を含めます。セット内に複数の値がある場合は、カンマで区切る必要があります。

一致する例

入力した 1 つ以上の文字に一致する任意のイベント情報を含め、キーワードの検索を可能にします。

キー設定済み

レポートサーバの設定中にキー値として設定したすべてのイベント情報を含めます。ビジネス上の関連性など、組織のグループを設定する際にキー値を使用できます。

キー未設定

レポートサーバの設定中にキー値として設定していないすべてのイベント情報を含めます。ビジネス上の関連性など、組織のグループを設定する際にキー値を使用できます。

詳細イベント フィルタの作成

詳細フィルタは、クエリの作成、レポートのスケジュール、ローカル フィルタおよびグローバル フィルタなど、多数の機能によって使用されます。

詳細フィルタの作成方法

1. [新規イベントフィルタ]をクリックします。
イベントフィルタ テーブルの最初の行が有効になり、その[ロジック]および[演算子]列にそれぞれデフォルト値「AND」および「等しい」が設定されます。
2. (オプション) 必要に応じて、[ロジック]セルをクリックし、ロジック値を変更します。
3. [列]セルをクリックし、ドロップダウン メニューからイベント情報列を選択します。
4. [演算子]セルをクリックし、ドロップダウン メニューから演算子を選択します。
5. [値]セルをクリックし、該当する値を選択します。
6. (オプション) 左かっこおよび右かっこのセルをクリックして、必要なかっこの数を入力します。
7. (オプション) 手順 1 から 6 を必要に応じて繰り返して追加のフィルタ ステートメントを追加します。
8. すべてのフィルタ ステートメントを入力したら、[保存]をクリックします。

詳細情報

[詳細フィルタの使用](#) (P. 487)

[レポートジョブをスケジュールする方法](#) (P. 484)

転送ルール属性の設定

転送終了ポイント、転送されるイベントに含める CEG フィールド、宛先設定など、転送ルールの必須属性を設定します。

ルールの属性を設定するには、以下の手順に従います。

1. 転送ルール ウィザードを開き、[ポリシー属性]の手順に進みます。
2. [アクション]領域で転送ルールのアクションを設定します。
 - a. 該当するドロップダウンリストで、**syslog** ファシリティおよび **syslog** 重大度を選択します。ルールによって転送されるイベントに、設定した **syslog** 属性が含まれます。
3. [一般情報]領域で **CA Enterprise Log Manager** イベント転送に関する情報を設定します。
 - a. ルールによって特定されたイベントを、抑制および集約の前に送信するか後に送信するかを選択します。
 - 「前」を選択した場合、すべての受信イベントが転送ルール フィルタに対して検証されます。
 - 「後」を選択した場合、精製済みイベントのみが転送ルール フィルタに対して検証されます。抑制されたイベントは転送されず、集約されたイベントは、集約前の詳細な状態ではなく、集約された状態でのみ転送されます。

注: 「前」を選択すると、イベントが精製されないため、システム パフォーマンスへの影響が大きくなります。

 - a. 転送されるイベント内で表示する **CEG** フィールドを選択します。**CEG** フィールドを選択しない場合は、元のイベント値のみが送信されます。**CEG** フィールドをすべて選択する場合は、元のイベントを転送するために **raw_event** も選択してください。
4. [宛先]領域で転送先情報を設定します。
 - a. [宛先の追加]をクリックし、宛先行を作成します。
 - b. [ホスト]列のテキストをクリックし、宛先のホスト名または IP アドレスを追加します。IP アドレスは、IPv4 と IPv6 のどちらも使用できます。
 - c. [ポート]列のセルをクリックし、ターゲット アプリケーションがリスンするポート番号を追加します。
 - d. [プロトコル]列のテキストをクリックし、TCP または UDP を選択して、使用する転送プロトコルを設定します。

- e. 手順 a ～ d を繰り返し、次の宛先を追加します。
5. [保存]または[保存して閉じる]をクリックします。
[転送ルール]フォルダ下の[ユーザ]サブフォルダに、新規ルールが表示されます。

転送された syslog イベントについて

syslog パケットの最大サイズ (PRI、Header、Tag、Content フィールドを含む) は、1024 バイトです。このため、転送されたイベントには、ユーザが指定した CEG 名前/値ペアをすべて含むことができない場合があります。

CA Enterprise Log Manager により、必要に応じて、長さが 1024 バイト未満になるように、メッセージ値が切り捨てられます。転送ルールによって CEG フィールドを生成された syslog イベントに含めるよう指定されている場合は、生成された syslog イベントの Content フィールドに、指定された CEG 名前/値ペアが含まれます。

名前/値ペアには、単純フィルタルールと一致したイベントから得た `CEG_field_name: field_value` という形式があります。文字列「null」は、CEG フィールドが null 値であることを示します。これらの CEG フィールドは、転送ルールで指定された順になっています。

転送ルールで指定された CEG フィールドの順序は重要です。指定された値部分が CA Enterprise Log Manager によって切り捨てられる場合がありますが、CEG フィールド名は切り捨てられません。次の完全な CEG フィールド名、コロン、関連する値の 1 バイト以上を特定できなかった場合、CA Enterprise Log Manager は、syslog Contents フィールドを、前の CEG 名前/値ペアで終了します。

転送ルールの編集

転送ルールを編集できます。

転送ルールを編集する方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。
2. [転送ルール]フォルダを展開し、編集するファイルが含まれているフォルダをクリックします。
3. 編集するルールを選択し、[転送ルールの編集]アイコンをクリックします。
転送ルール ウィザードが開き、選択したルールが表示されます。
4. 必要な変更をルールに加え、[保存して閉じる]をクリックします。
ルールが、編集したルールの新バージョンとして、該当するリストに表示されます。

転送ルールの削除

不要な転送ルールを削除できます。

転送ルールを削除する方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。
2. [転送ルール]フォルダを展開し、削除するファイルが含まれているフォルダをクリックします。
3. 削除するルールを選択し、[転送ルールの削除]アイコンをクリックします。
現在のバージョンがデフォルトで選択されます。詳細ペインの[バージョン]プルダウンリストから削除する以前のバージョンを選択できます。
確認のダイアログが表示されます。
4. [はい]をクリックします。
削除したルールが、該当するリストから削除されます。

転送するルールのインポート

転送ルールをインポートすることで、ある環境から別の環境にルールを移行することができます。たとえば、テスト環境で作成したルールをライブ環境にインポートできます。

転送ルールをインポートする方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。
2. [転送ルール]フォルダを選択します。
転送ルールのボタンが詳細ペインに表示されます。
3. [転送ルールのインポート]をクリックします。
[ファイルのインポート]ダイアログ ボックスが表示されます。
4. インポートするルールを参照し、[OK]をクリックします。
転送ルール ウィザードが表示され、選択したルールの詳細が表示されます。
5. 必要な変更をルールに加え、[保存して閉じる]をクリックします。インポートしたルールの名前が管理データベース内に存在するルールと同じ場合は、名前の変更を要求するメッセージが表示されます。
インポートしたルールが、[イベント転送ルール]ユーザ フォルダに表示されます。

転送するルールのエクスポート

転送ルールをエクスポートすることで、ある環境から別の環境にルールを移行することができます。たとえば、テスト環境で作成したルールをライブ環境にエクスポートできます。

転送ルールをエクスポートする方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。
2. [転送ルール]フォルダを展開し、エクスポートするファイルが含まれているフォルダをクリックします。
3. エクスポートするルールを選択し、[転送ルールのエクスポート]をクリックします。現在のバージョンがデフォルトで選択されます。詳細ペインの[バージョン]プルダウンリストからエクスポートする以前のバージョンを選択できます。

[エクスポートの場所]ダイアログ ボックスが表示されます。

4. エクスポートされるルールを格納する場所を入力または参照し、[保存]をクリックします。

エクスポートの成功を確認するダイアログ ボックスが開きます。

5. [OK]をクリックします。

ルールがエクスポートされます。

注: エクスポートされたルールを調べる場合、ファシリティと重大度の値は単なる数値で表示されます。これらの値に関する説明文を、ウィザード インターフェイスを使用して特定できます。

第 15 章：統合およびコネクタ

このセクションには、以下のトピックが含まれています。

[統合とコネクタのタスク](#) (P. 579)

[統合の作成方法](#) (P. 581)

[syslog リスナの作成方法](#) (P. 589)

[新しい統合バージョンの作成](#) (P. 596)

[統合の削除](#) (P. 597)

[統合定義のエクスポートおよびインポート](#) (P. 597)

[コネクタの作成方法](#) (P. 599)

[コネクタの表示](#) (P. 602)

[コネクタガイドの表示](#) (P. 603)

[コネクタの編集](#) (P. 604)

[保存済み設定について](#) (P. 604)

[保存済み設定の作成](#) (P. 605)

[コネクタを一括して設定する方法](#) (P. 606)

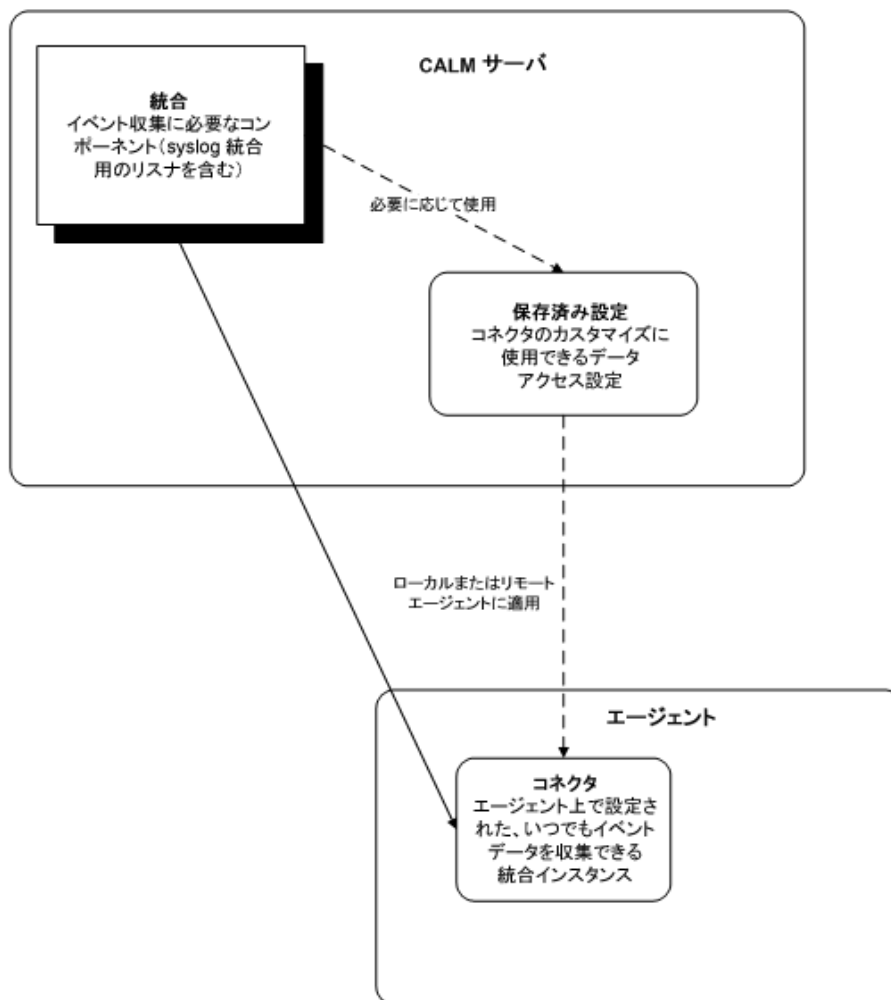
[複数コネクタの設定の更新](#) (P. 612)

統合とコネクタのタスク

統合は、コネクタ用のテンプレートです。統合には、ログ センサ、XMP ファイルと DM ファイル、オプションの抑制ルールなど、特定のタイプのソースからイベント情報を収集する際に必要なコンポーネントがすべて含まれています。統合は CA によって提供されます。ユーザーが独自に統合を作成することもできます。

カスタム統合を作成したり、事前定義済み統合のコピーを変更したりすることができます。また、独自の XMP ファイルや DM ファイルを作成して、カスタム統合はもちろん、特定のデータ アクセス情報が含まれている保存済み統合も使用できます。

イベントを分析し、必要な統合を作成した後、以下の図で示すように、保存済みの設定を使用してコネクタを作成し、エージェントに適用できます。



詳細情報

[統合定義のエクスポートおよびインポート](#) (P. 597)

[保存済み設定について](#) (P. 604)

[コネクタの表示](#) (P. 602)

[コネクタの編集](#) (P. 604)

統合の作成方法

統合ウィザードを使用して、統合を作成および編集できます。統合は、お使いの環境からイベントを収集または受信する設定済みコネクタのテンプレートとして使用できます。

WMI と ODBC の統合など、複数のタイプの統合を作成できます。これによって、指定したタイプのイベントが能動的に収集されます。また、**syslog** 統合を作成できます。この統合では、イベントが受動的に受信されます。**syslog** 統合は、複数のソースからのイベントを受信できます。このため、**syslog** 統合およびコネクタを作成するプロセスは、多少異なったものになります。

この高度な機能を十分に活用するには、お使いの環境内のイベントソースとその通信タイプについて、完全に理解している必要があります。さらに、正規表現構文、CEG、DM ファイルと XMP ファイル、およびそのイベント解析方法について、完全に理解している必要があります。

統合の作成は、以下の手順で構成されます。

1. 統合ウィザードの表示
2. 統合コンポーネントの追加
3. 抑制ルールを選択
4. 集約ルールを選択
5. デフォルト設定の定義 この手順は、**syslog** 統合には適用されません。

サブスクリプション統合をコピーして、カスタム ユーザ統合を作成することもできます。

詳細情報:

[統合コンポーネントの追加](#) (P. 583)

[抑制ルールと集約ルールの適用](#) (P. 584)

[デフォルト設定の定義](#) (P. 585)

統合ウィザードの表示

統合を新規作成するか、既存の統合を編集するには、統合ウィザードを開きます。

統合ウィザードを開く方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。
2. [イベント精製ライブラリ]フォルダの横にある矢印をクリックして展開し、[統合]フォルダを選択します。
[統合]ボタンが[詳細]ペインに表示されます。

3. [新規統合]をクリックします。 

統合ウィザードが表示されます。

ウィザードの使用時の操作

- ウィザードを閉じずにファイルを保存するには、[保存]をクリックします。
- ファイルを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

詳細情報:

[統合コンポーネントの追加](#) (P. 583)

統合コンポーネントの追加

統合を作成するには、イベントを収集するために使用されるログ センサ、XMP ファイル、DM ファイルなど、統合の主要な詳細情報を設定します。

統合コンポーネントを追加する方法

1. 統合ウィザードを開きます。
2. 新規統合の名前を入力します。
3. ドロップダウンリストから、以下に示す必要な統合コンポーネントを選択します。

[センサ]

ログ ソースからイベントを読み取るために統合が使用するログ センサを定義します。

[設定ツール]

選択されたログ ストアに接続するために統合が使用するツール バイナリを定義します。ほとんどの統合では設定ツールは必要ありません。

[プラットフォーム]

統合の監視対象となるアプリケーションのオペレーティング システムではなく、統合エージェントが動作できるオペレーティング システムを参照します。オペレーティング システムは、センサ設定および設定ツールの設定を基にウィザードによって自動的に選択されます。

4. 統合の説明を入力します。
5. シャトル コントロールを使用して、統合がイベントを精製する際に使用する XMP ファイルおよび DM ファイルを選択します。
6. 必要に応じて、[ターゲット フィールド] エントリ フィールドに、統合が解析する元のイベントの情報が含まれているネイティブ フィールドの名前を入力します。イベント タイプによっては、特定の 1 つのフィールドに元のイベント情報が含まれていて、統合ではそのフィールドをターゲットにする必要がある場合があります。たとえば、NT イベントのログ イベントの場合、このフィールドは「メッセージ」です。
7. 該当する矢印をクリックして次に完了するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックした場合、新しい統合がユーザ フォルダ リストに表示されます。それ以外の場合は、選択した手順が表示されます。

抑制ルールと集約ルールの適用

統合に抑制ルールと集約ルールを適用して、イベント精製をカスタマイズできます。統合がコネクタとして設定されている場合、抑制ルールおよび集約ルールはイベント ログ ストアへ送信される前に適用されます。抑制と集約のチェックは、イベント ログ ストアでの抑制および集約のチェックに加えて実行されます。

たとえば、抑制ルールを適用して、不要な **Windows** イベントが **WMI** エージェントに送信されないようにすることができます。ネットワーク トラフィックが緩和され、これらのイベントはイベント ログ ストアに到達しません。

重要： 特定のネイティブ イベントについて、ログの記録と確認が一切できなくなるため、抑制ルールの作成や使用には細心の注意を払ってください。抑制ルールは、導入前にテスト環境でテストすることをお勧めします。

抑制ルールと集約ルールを適用するには、以下の手順に従います。

1. 統合ウィザードを開き、[抑制ルール]の手順または[集約ルール]の手順に進みます。
2. (オプション) [ルール パターン] エントリフィールドに入力して、使用可能なルールを検索します。入力と共に、入力内容と一致するルールが表示されます。
3. シャトル コントロールを使用して、必要なルールを選択します。
4. 該当する矢印をクリックして次に完了するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックした場合、新しい統合がユーザ フォルダリストに表示されます。それ以外の場合は、選択した手順が表示されます。

詳細情報：

[抑制ルールおよび集約ルール タスク](#) (P. 506)

[統合コンポーネントの追加](#) (P. 583)

[デフォルト設定の定義](#) (P. 585)

[ファイル ログ設定の設定](#) (P. 586)

デフォルト設定の定義

デフォルトの設定を使用して、統合データ アクセス設定を制御できます。たとえば、WMI 通信のために接続するドメイン コントローラを設定できます。

syslog 統合は syslog リスナから設定値を継承するため、syslog 統合を作成する場合はこの手順は適用されません。

デフォルト設定を定義する方法

1. 統合ウィザードを開き、[デフォルトの設定]の手順に進みます。
2. 必要なフィールドを入力します。
3. (オプション)デフォルト設定の横にある[非表示]ボタンをクリックすると、コネクタの作成中、非表示にできます。非表示にした設定は、この統合を基にコネクタを作成するユーザには表示されません。これによって、コネクタを展開するために統合を使用する際に、デフォルト設定を変更できないように設定できます。
4. 該当する矢印をクリックして次に完了するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックした場合、新しい統合がユーザ フォルダ リストに表示されます。それ以外の場合は、選択した手順が表示されます。

詳細情報:

[統合コンポーネントの追加](#) (P. 583)

ファイル ログ設定の設定

ファイル ログ センサを使用して、統合用のデータ アクセス設定を制御できます。ほとんどのイベント収集には **CA** によって提供されたデフォルト設定を使用できますが、カスタム統合用にそれらの設定を変更することもできます。

ファイル ログ設定の定義方法

1. 統合ウィザードを開き、「ファイル ログ」センサ タイプを選択して、「デフォルトの設定」の手順に進みます。
2. 統合のアンカー レートを設定または編集します。

UpdateAnchorRate

アンカー値が作成されるしきい値をイベント数で定義します。イベント処理が中断されると、エージェントによって、再処理が開始される最新のアンカーが参照されます。アンカー レートを低く設定すると、イベントが失われる可能性は減りますが、アンカー値が作成される頻度が高くなるため、パフォーマンスに影響を与えます。アンカー レートを高く設定すると、処理が中断された場合に多数のイベントが再処理されるため、作業負荷が増大します。

デフォルト: 4

先頭からの読み取り

イベント処理が中断された場合に、エージェントがファイルを先頭から読み取り始めるかどうかを制御します。チェック ボックスがオフになっている場合は、エージェントはアンカー レートを使用して、イベントの読み取りを再開します。チェック ボックスがオンになっている場合は、コネクタを初めて展開する際、センサはログ ファイルを先頭から読み取ります。データベースのサイズおよびイベント生成の頻度によって、**CA Enterprise Log Manager** ログ センサがリアルタイム イベントと同期するにはある程度時間がかかることがあります。

3. 対象とするイベントソースの以下の設定値を設定または編集します。

ファイル アーカイブ ディレクトリ

ローテーション後にログ ファイルが保存されるパスを定義します。アーカイブ ディレクトリとディレクトリ名は同じである場合があります。

ファイル マスク

イベントソースログ ファイルを特定するために使用するテキスト文字列を設定します。ファイル マスクにワイルドカードを使用できます。たとえば、「`messages.txt`」という名前のログ ファイルを特定するために、「メッセージ*」というマスクを入力できます。

ファイル ローテーション タイプ

イベントの送信元である製品によって使用されるファイル ローテーション タイプに一致するよう統合を設定します。実際のローテーション タイプは、製品によって設定されます。以下の設定が、CA Enterprise Log Manager 統合でサポートされています。

- **NewFile** - 統合ターゲットが **logrotate** などのユーティリティによってローテーションされる際に使用されます。
- **FileSize** - 統合ターゲットが既定のサイズしきい値に基づいている場合に使用されます。
- **FileAge** - 統合ターゲットが既定の期間に基づいている場合に使用されます。更新は、通常、午前 0 時またはその前後に実行されます。

ディレクトリ名

イベントソースログ ファイルのパスを定義します。

イベント区切り文字

複数行のログ ファイルで、個々のログ エントリを区切る正規表現を定義します。ログ センサが指定された区切り文字を検出するたびに、新しいイベントの読み取りを開始します。この結果、CA Enterprise Log Manager が 1 つのログ ファイルから複数のイベント エントリを受け取ることができるようになります。たとえば、各ログ ファイル エントリに一意の日時スタンプが含まれている場合、そのタイム スタンプ形式の正規表現を区切り文字として使用できます。

4. (オプション) イベントソース値をさらに追加するには、[繰り返し]をクリックします。 

設定値フィールドのセットが追加表示され、別のイベントソースからのイベント収集用に値を入力できます。

5. 該当する矢印をクリックして次に完了するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックした場合、新しい統合がユーザ フォルダ リストに表示されます。それ以外の場合は、選択した手順が表示されます。

syslog リスナの作成方法

リスナ ウィザードを使用して、**syslog** リスナを作成または編集できます。リスナによって、CA Enterprise Log Manager サーバへの **syslog** イベントのルーティングが制御されます。

注: ほとんどすべての目的でサブスクリプション(事前定義済み) **syslog** リスナを使用できます。あるユーザが **syslog** 受信を調節するためにカスタムリスナの使用が必要になる場合がありますが、この目的のための手順も含まれています。

この高度な機能を十分に活用するには、お使いの環境内の **syslog** イベントソースについて、完全に理解している必要があります。

統合の作成は、以下の手順で構成されます。

1. リスナ ウィザードの表示
2. コンポーネントの追加
3. 抑制ルールを選択
4. 集約ルールを選択
5. デフォルト設定の定義

詳細情報:

[リスナ ウィザードの表示](#) (P. 590)

[リスナ コンポーネントの追加](#) (P. 591)

[デフォルト設定の定義](#) (P. 593)

[抑制ルールおよび集約ルールの適用](#) (P. 592)

[syslog タイム ゾーンの追加](#) (P. 595)

リスナ ウィザードの表示

syslog リスナを新規作成するか、既存の syslog リスナを編集するには、リスナ ウィザードを開きます。

リスナ ウィザードを開く方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダ リストが表示されます。
2. [イベント精製ライブラリ]フォルダの横にある矢印をクリックして展開し、[リスナ]フォルダを選択します。
[統合]ボタンが[詳細]ペインに表示されます。

3. [新規リスナ]をクリックします。

リスナ ウィザードが表示されます。

ウィザードを使用する際に

- ウィザードを閉じずにファイルを保存するには、[保存]をクリックします。
- ファイルを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

リスナ コンポーネントの追加

syslog リスナを作成するには、名前や設定ツールなどの詳細を設定します。

リスナ コンポーネントを追加する方法

1. リスナ ウィザードを開きます。
2. 新しいリスナの名前を入力します。
3. (オプション)ドロップダウンリストから以下のコンポーネントを選択します。

[設定ツール]

選択されたログストアに接続するために統合が使用するツール バイナリを定義します。ほとんどの統合では設定ツールは必要ありません。

注: リスナのセンサ タイプは常に **syslog** です。

4. (オプション)リスナの説明を入力します。
5. 該当する矢印をクリックして次に完了するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックした場合、新しい統合がユーザ フォルダリストに表示されます。それ以外の場合は、選択した手順が表示されます。

抑制ルールおよび集約ルールの適用

syslog リスナに抑制ルールと集約ルールの両方を適用して、イベント精製をカスタマイズできます。リスナとコネクタを併用すると、受信イベントが **CA Enterprise Log Manager** に送信される前に、適用した抑制ルールおよび集約ルールと照合して検証されます。

たとえば、**CA Access Control** のイベントのみを受信するリスナを作成する場合、**CA Access Control** の正常に作成されたファイル アクセスルールを適用することができます。受信イベントの検証に必要なルールのみが使用されるため、処理量の増大を防ぐことができます。

重要： 特定のネイティブ イベントについて、ログの記録と確認が一切できなくなるため、抑制ルールの作成や使用には細心の注意を払ってください。抑制ルールは、導入前にテスト環境でテストすることをお勧めします。

抑制ルールや集約ルールを適用する方法

1. リスナ ウィザードを開き、「抑制ルール」の手順または[集約ルール]の手順に進みます。
2. (オプション)ルール パターン エントリフィールドに入力して、使用可能なルールを検索します。入力するに従って、入力内容と一致するルールが表示されます。
3. シャトル コントロールを使用して、必要なルールを選択します。
4. 該当する矢印をクリックして次に完了するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、新規リスナがユーザ フォルダ リストに表示されます。それ以外の場合は、選択した手順が表示されます。

デフォルト設定の定義

デフォルトの設定を使用して、syslog リスナのデータアクセス設定を制御できます。たとえば、トラステッド ホストまたはデフォルトの通信ポートを設定できます。

デフォルト設定を定義する方法

1. リスナ ウィザードを開き、[デフォルトの設定]の手順に進みます。
2. 以下のような、必要な値を変更または追加します。

イベントの順序指定

受信された順序と同じ順序でイベントをイベントログ ストアに送信するのに役立ちます。イベントの順序指定が無効の場合、あるイベントがほかのイベントより早く解析されて転送されると、順序が変更されることがあります。イベントの順序指定を有効にすると、イベントの処理や送信が低速になり、パフォーマンスに影響を及ぼすことがあります。

キュー当たりのスレッド数

各プロトコルの処理スレッド数を定義します。処理スレッド数を多くすると、イベントの順序指定が無効の場合は処理速度が向上します。イベントの順序指定が有効の場合は、スレッド数は影響しません。処理スレッド数を多くすると、パフォーマンスに影響を及ぼす可能性があります。

キュー サイズ

受信イベント情報用のキュー サイズを、イベント数で設定します。キューは、イベントの処理および送信を行う際に使用されます。バッファがいっぱいになると、イベントが処理されて空きができるまで、それ以上のイベントは受信できません。

[ポート]

リスナが UDP または TCP でイベントを受信する際に使用するポートを設定します。複数のポートを指定する場合、サービスは各ポートを順番にバインドしようとします。あらかじめ syslog のデフォルトポートが設定されています。syslog イベントをほかのポートにルーティングしている場合には、それに応じた CA Enterprise Log Manager 受信ポートを設定してください。

重要： エージェントが UNIX システム上で root 以外のユーザとして実行されている場合、syslog リスナ ポートを 1024 よりも大きいポート番号に変更してください。この場合、デフォルトの UDP ポートの 514 がオープンにならないため、syslog イベントは収集されません。

[Trusted Host]

IPv4 または IPv6 の信頼できる IP アドレスを定義します。トラステッド ホストからの通信のみが許可されます。トラステッド ホストを指定しない場合、利用可能なすべての **syslog** イベントソースからのイベントが受信されます。トラステッド ホストの **event_source_address** フィールドに記録されているとおりに、正確な IP アドレスを入力してください。ワイルドカードまたはサブネットアドレスを使用することはできません。

[Time Zones]

syslog イベントソース コンピュータ用にタイムゾーンを追加できます。**syslog** は通常、時間を記録しません。完全な IP アドレスとタイムゾーンによってソースシステムを識別し、**CA Enterprise Log Manager** サーバとは異なるタイムゾーンに属する **syslog** ソースからのイベントを受信し、正しく調整します。サーバと同じタイムゾーンにある **syslog** ソースはリスト表示されません。

3. 該当する矢印をクリックして次に完了するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、新規リスナがユーザ フォルダリストに表示されます。それ以外の場合は、選択した手順が表示されます。

syslog タイム ゾーンの追加

1 つ以上の syslog イベントソース コンピュータにタイムゾーンを追加し、CA Enterprise Log Manager サーバとは異なるタイムゾーンに属する syslog ソースからのイベントを受信し、正しく調整します。

統合を作成する際、コネクタを設定する際、または保存済み設定を作成する際に、syslog タイム ゾーンを追加できます。

注: サマータイムが適用される環境にタイムゾーンを追加する場合は、該当するタイムゾーン エントリがエージェント ホスト システム上に存在することを確認してください。該当するエントリがない場合、syslog タイム ゾーンはサマータイムの変更を処理できず、イベントにはサマータイム期間中不正確なタイム スタンプが表示されます。

syslog タイム ゾーンを追加する方法

1. 以下の方法のいずれかを実行して、syslog タイム ゾーン インターフェースにアクセスします。
 - タイムゾーンを追加する syslog 統合を開き、[デフォルトの設定]の手順に進みます。
 - タイムゾーンを追加する syslog コネクタを開き、[コネクタの設定]の手順に進みます。
 - タイムゾーンを追加する保存済み設定を開きます。syslog タイム ゾーン インターフェースが表示されます。
2. [タイム ゾーン]領域上部の[フォルダの作成]をクリックします。

新しいタイム ゾーン フォルダがリスト領域に表示され、タイム ゾーン ドロップダウンリストが右ペインに表示されます。
3. ドロップダウンリストからタイム ゾーンを選択します。

選択したゾーンが、フォルダの横に表示されます。
4. フォルダの横の矢印をクリックします。

フォルダが展開され、選択したタイム ゾーン用の無題のイベントソース コンピュータが 1 つ表示されます。
5. コンピュータ アイコンをクリックします。

IP アドレス エントリ フィールドが表示されます。
6. IP アドレスを入力します。

コンピュータ アイコンの横に、入力したアドレスが表示されます。

7. (オプション) イベントソースコンピュータを追加するには、既存のイベントソースを選択し、[項目の追加]をクリックします。

フォルダが閉じます。フォルダを開き、新しい無題のイベントソースコンピュータを表示します。手順 6 に進みます。

8. (オプション) タイムゾーンを追加するには、[フォルダの作成]をクリックします。

新しい無題のタイムゾーンフォルダが表示されます。手順 3 に進みます。

9. 必要なタイムゾーンフォルダとイベントソースアドレス項目の作成がすべて終わったら、[保存]をクリックします。

詳細情報:

[コネクタ設定の設定](#) (P. 601)

[保存済み設定の作成](#) (P. 605)

新しい統合バージョンの作成

既存のユーザ作成 (カスタム) 統合から新しいバージョンを作成できます。

新しい統合バージョンを作成する方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。
2. [イベント精製ライブラリ]および[統合]フォルダを展開し、必要な統合が含まれているユーザフォルダをクリックします。
3. ユーザ統合を選択し、[バージョンの新規作成]をクリックします。
4. 新規統合ウィザードが表示され、選択した統合の詳細が表示されます。
5. 必要な変更を行い、[保存して閉じる]をクリックします。

リストに新しい統合バージョンが表示されます。

統合の削除

カスタム統合を削除できます。サブスクリプション統合は削除できません。

カスタム統合を削除する方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。
2. [イベント精製ライブラリ]および[統合]フォルダを展開し、削除する統合が含まれているユーザフォルダをクリックします。
3. リストから削除する統合を選択します。
4. リスト上部の[削除]をクリックします。
確認のダイアログが表示されます。
5. [はい]をクリックします。
統合がリストから削除されます。

統合定義のエクスポートおよびインポート

ほかの管理サーバでできるように、統合の詳細をエクスポートおよびインポートすることができます。これにより、CA Enterprise Log Manager 間で、またはテスト環境からライブ環境に、正常に作成されたカスタム統合を転送できます。

詳細情報

[統合定義のインポート](#) (P. 598)

[統合定義のエクスポート](#) (P. 598)

統合定義のインポート

統合定義 XML ファイルをローカル管理サーバでできるようにインポートすることができます。

統合の詳細をインポートする方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダ ツリーが表示されます。
2. [統合]フォルダを展開し、統合をインポートするサブフォルダに移動します。
3. [統合のインポート]をクリックします。
[ファイルのインポート]ダイアログ ボックスが開きます。
4. ファイルをインポートする場所を入力または参照し、[OK]をクリックします。
クエリファイルが現在のフォルダにインポートされ、確認ダイアログ ボックスが表示されます。
5. [OK]をクリックします。

統合定義のエクスポート

ほかの管理サーバでできるように、統合の詳細をエクスポートできます。エクスポート ファイルは XML ファイルとして保存されます。

統合の詳細をエクスポートする方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダ ツリーが表示されます。
2. [統合]フォルダを展開し、エクスポートする統合が保存されているサブフォルダに移動します。
3. [統合のエクスポート]をクリックします。
ダウンロード ダイアログ ボックスが表示されます。
4. XML エクスポート ファイルを保存する場所を入力または参照し、[保存]をクリックします。
クエリファイルが選択した場所に保存され、確認ダイアログ ボックスが表示されます。
5. [OK]をクリックします。

コネクタの作成方法

環境内の特定のオペレーティング システムまたはデバイスからイベントを収集するコネクタを作成できます。新規コネクタウィザードから、統合またはリスナをテンプレートとして使用し、コネクタを作成します。新規作成したすべてのコネクタが、環境内のエージェントに適用されます。

WMI と ODBC の統合など、複数のタイプのコネクタを作成できます。これによって、指定したタイプのイベントが能動的に収集されます。また、**syslog** コネクタを作成できます。このコネクタでは、イベントが受動的に受信されます。**syslog** コネクタは、ほかのタイプとは異なり、複数のソースからのイベントを受信できます。このため、**syslog** コネクタを作成するプロセスは、多少異なったものになります。

コネクタを作成するプロセスは、以下の手順で構成されます。

1. コネクタウィザードの表示
2. **syslog** コネクタ用のリスナの選択など、コネクタの詳細の追加
3. 抑制ルール の適用
4. 集約ルール の適用
5. コネクタ設定の設定

詳細情報:

[コネクタウィザードの表示](#) (P. 599)

[コネクタの詳細の追加](#) (P. 600)

[抑制ルールおよび集約ルールの適用](#) (P. 601)

[コネクタ設定の設定](#) (P. 601)

コネクタ ウィザードの表示

コネクタを新規作成するか、既存のコネクタを編集するには、コネクタウィザードを開く必要があります。

コネクタ ウィザードを開く方法

1. [管理] タブをクリックし、[ログ収集] サブタブをクリックします。
[ログ収集] フォルダ リストが表示されます。

2. [エージェント エクスプローラ]フォルダを展開し、コネクタを追加または編集するエージェントグループを選択します。

選択したグループに属するエージェントが表示されます。

3. コネクタを追加または編集するエージェントを選択します。
[エージェント管理]ボタンが[詳細]ペインに表示されます。

4. [新規コネクタ]をクリックします。

コネクタウィザードが表示されます。

ウィザードを使用する際に

- ウィザードを閉じずにファイルを保存するには、[保存]をクリックします。
- ファイルを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

コネクタの詳細の追加

コネクタを識別するための名前と説明を追加できます。また、コネクタのテンプレートとして使用する統合を選択する必要があります。

コネクタの詳細を追加する方法

1. コネクタの設計ウィザードを開きます。

ウィザードでは、画面上部に、現在のエージェントのプラットフォームとプラットフォームのバージョンが表示されます。

2. コネクタの名前を入力します。
3. **syslog** コネクタを作成する場合は[リスナ]ラジオ ボタンをクリックし、ほかのタイプの場合は[統合]ラジオ ボタンをクリックします。
4. テンプレートとして使用する統合を選択します。[統合]ドロップダウンリストに、現在のプラットフォーム バージョンおよびイベントソースタイプで使用可能な統合がすべて表示されます。
5. (オプション) [統合]ドロップダウンリストの使用可能なエージェント プラットフォームのすべてのバージョンに対して統合を作成するには、[プラットフォーム バージョン チェックのバイパス]を選択します。
6. コネクタの説明を入力します。

- 次に実行する手順に進むか、[保存して閉じる]をクリックします。
[保存して閉じる]をクリックすると、コネクタがコネクタリストに表示されます。

抑制ルールおよび集約ルールの適用

コネクタを作成または編集する際に、コネクタによって処理されるイベントに適用する抑制ルールと集約ルールを選択できます。追加した抑制ルールや集約ルールは、イベントが **CA Enterprise Log Manager** サーバに送信される前に適用されます。

抑制ルールや集約ルールを適用する方法

- コネクタの設計ウィザードを開き、[抑制ルールの適用]の手順または[集約ルール]の手順に進みます。
使用可能な抑制ルールのリストが表示されます。
- (オプション)ルール パターン エントリフィールドに入力して、使用可能なルールを検索します。入力するに従って、入力内容と一致するルールが表示されます。
- シャトル コントロールを使用して、必要なルールを **1** つ以上選択します。
- 次に実行する手順に進むか、[保存して閉じる]をクリックします。
[保存して閉じる]をクリックすると、コネクタがコネクタリストに表示されます。

コネクタ設定の設定

コネクタを作成または編集する際、各種設定項目を設定し、コネクタによるイベントの送受信方法を決定できます。各コネクタの設定項目を設定するか、保存済み設定を使用できます。

保存済み設定は、再利用可能なデータ アクセス設定の集合です。保存済み設定を複数のコネクタに適用することができます。

コネクタ設定の定義方法

- コネクタの設計ウィザードを開き、[コネクタの設定]の手順に進みます。
- syslog** リスナまたはログ センサを選択した場合は、コネクタが使用する統合を **1** つ以上選択します。

3. ドロップダウンリストから必要な保存済み設定を選択するか、表示されている設定値を変更します。コネクタは、統合から、または **syslog** コネクタの場合はリスナから設定内容を継承します。
4. (オプション) 選択した統合のコネクタガイドを表示するには、[ヘルプ]リンクをクリックします。表示されたガイドで詳細を確認できます。
5. [保存して閉じる]をクリックします。
コネクタリストにコネクタが表示されます。

コネクタの表示

各エージェントのコネクタリストを開いて、そのエージェントに関連付けられたコネクタを表示および編集できます。

コネクタの表示方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [エージェント エクスプローラ]フォルダおよび[エージェント グループ]フォルダを展開し、各エージェントを表示します。
3. 表示するコネクタが設定されているエージェントを選択します。
4. [コネクタの表示]をクリックします。
[エージェント コネクタ]リストが表示され、選択したエージェント上に設定されているコネクタが表示されます。

コネクタガイドの表示

各タイプの **CA Enterprise Log Manager** コネクタのセットアップおよび設定情報が含まれるガイドを表示できます。このガイドには、イベントを受信するようにターゲット製品およびコネクタ自体を設定する方法に関する指示が含まれています。

また、コネクタログ名のような参照情報、コネクタが **CA Enterprise Log Manager** に送信するイベントのタイプも含まれています。

コネクタガイドを表示する方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。
2. [イベント精製ライブラリ]、[統合]、および[サブスクリプション]フォルダを展開して、個々の統合を表示します。
3. コネクタの作成に使用する統合を選択します。
統合の詳細が右のペインに表示されます。
4. [統合名]のすぐ上の青い[ヘルプ]リンクをクリックします。

その統合に関するコネクタガイドが新しいブラウザ ウィンドウに表示されます。

コネクタの編集

既存のコネクタを編集できます。コネクタを編集すると、新しいバージョンが作成されます。

コネクタの編集方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [エージェント エクスプローラ]フォルダおよび[エージェント グループ]フォルダを展開し、各エージェントを表示します。
3. 表示するコネクタが設定されているエージェントを選択します。
4. [コネクタの表示]をクリックします。
[エージェント コネクタ]リストが表示され、選択したエージェント上に設定されているコネクタが表示されます。
5. 編集するコネクタの横の[編集]をクリックします。
コネクタ ウィザードが開き、選択したコネクタが表示されます。
6. 必要な変更を加えて、[保存して閉じる]をクリックします。
リストに編集したコネクタが表示されます。

保存済み設定について

保存済み設定は、コネクタがデバイスまたはログ ソースからイベントを収集できるようにするための、再利用可能な設定の集合です。保存済み設定を使用すると、まったく新しい統合を作成することなく、一定のカスタマイズが可能になります。

設定の内容は統合タイプによって異なります。たとえば、**syslog** コネクタの場合はトラステッド ホストを保存でき、**WMI** コネクタの場合は **WMI** サーバの連絡先情報を保存できます。

保存済み設定を使用することで、これらのグループ化された情報を保存し、複数のコネクタに適用できます。各保存済み設定は特定の統合に関連付けられているため、その統合を使用するコネクタの保存済み設定のみを使用できます。

詳細情報

[保存済み設定の作成](#) (P. 605)

[統合とコネクタのタスク](#) (P. 579)

保存済み設定の作成

保存済み設定を作成して、特定の統合に関連付けることができます。

保存済み設定を作成する方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [イベント精製ライブラリ]フォルダを開き、保存済み設定を作成する統合に移動します。
統合の詳細が、[詳細]ペインに表示されます。
3. [保存済み設定]をクリックします。
[保存済み設定リスト]が表示されます。
4. [新規]をクリックします。
[保存済み設定]ダイアログ ボックスが表示され、選択した統合のデフォルト設定値が表示されます。
5. 必要な設定値を入力し、[保存して閉じる]をクリックします。
確認のメッセージが表示されます。
6. [OK]をクリックします。
保存済み設定が、リストに表示されます。

コネクタを一括して設定する方法

複数のコネクタを一括して作成して、イベント収集ソースを設定できます。同じ統合を使用して、複数のコネクタを同時に作成し、環境内のさまざまなエージェント上に展開できます。

設定プロセスは、イベントソースの選択、抑制ルールの適用、集約ルールの適用、およびコネクタ設定の設定で構成されます。この機能を利用するには、事前に、設定するイベントソースのホスト名と IP アドレスなどの識別情報のリストを作成します。リストは、カンマ区切り値(.csv)形式である必要があります。

コネクタ一括展開ウィザードを使用して、収集ソースを設定するプロセスは、以下の手順で構成されます。

1. コネクタ一括展開ウィザードの表示
2. ソースの詳細の選択
3. 抑制ルールの適用
4. 集約ルールの適用
5. コネクタ設定の設定
6. エージェントの選択およびソースのマッピング

詳細情報:

[収集ソースの設定ウィザードの表示](#) (P. 606)

[ソースの詳細の選択](#) (P. 608)

[抑制ルールの適用](#) (P. 609)

[集約ルールの適用](#) (P. 609)

[コネクタの設定](#) (P. 610)

[エージェントの選択およびソースのマッピング](#) (P. 611)

収集ソースの設定ウィザードの表示

エージェント上にコネクタを作成するには、コネクタ一括展開ウィザードを開きます。

コネクタ一括展開ウィザードを開くには、以下の手順に従います。

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。

2. [エージェント エクスプローラ]フォルダをクリックし、[収集ソースの設定]をクリックします。

収集ソースの設定ウィザードが表示されます。

ウィザードの使用時の操作

- ウィザードを閉じずに更新を適用するには、[保存]をクリックします。確認のメッセージが表示されます。
- 更新を適用してウィザードを閉じるには、[保存して閉じる]をクリックします。確認のメッセージは表示されません。

ソースの詳細の選択

ソースの詳細を選択し、接続する統合とその接続先イベントソースを特定します。この手順を完了するには、必要なイベントソースの詳細のリストが .csv ファイル内にある必要があります。

注: .csv ファイルには、コネクタの作成に必要な情報が格納されています。 .csv ファイル内の各列によって、コネクタ設定フィールドが特定され、フィールドの値が格納されます。たとえば、イベントを送信するホストの IP アドレスをリスト表示する [IP アドレス] 列を含めることができます。

「[統合の作成方法 \(P. 581\)](#)」セクションに、ログ センサのタイプ別の固有の設定フィールドについて記載されています。

ソースの詳細を選択するには、以下の手順に従います。

1. コネクター括展開ウィザードを開きます。
2. [統合] ドロップダウンリストから、ソースで使用する統合を選択します。
3. [バージョン] ドロップダウンリストから統合のバージョンを選択します。
4. 使用する収集ソースファイルを保存した場所を参照します。収集ソースは .csv ファイルである必要があります。

選択した収集ソースファイルの最初の 100 行が [ソース ファイル コンテンツ] 領域に表示され、確認することができます。1 行目は、[列ヘッダ] 行として設定されており、手順 5 でサンプル サイズを調節した場合でも、ヘッダとして残ります。

5. [送信者] 行および [宛先] 行のドロップダウンリストを使用して、収集ソースファイルの使用部分を絞り込みます。

選択した収集ソースファイルの一部が [ソース ファイル コンテンツ] 領域に表示され、確認することができます。[[送信者] 行] を 1 より大きい値に変更しておけば、列ヘッダは影響を受けません。

6. 次の手順に進みます。

詳細情報:

[統合の作成方法 \(P. 581\)](#)

抑制ルールの適用

一括設定変更に適用する抑制ルールを選択できます。

抑制ルールを適用する方法

1. コネクター括展開ウィザードを開き、[抑制ルール of 適用] の手順に進みます。
2. シャトル コントロールを使用して、適用する使用可能なルールを選択します。

注: [抑制ルール パターン] フィールドを使用して、抑制ルールを検索できます。

3. 次の手順に進みます。

集約ルール of 適用

一括設定変更に適用する集約ルールを選択できます。

集約ルールを適用するには、以下の手順に従います。

1. コネクター括展開ウィザードを開き、[集約ルール of 適用] の手順に進みます。
2. シャトル コントロールを使用して、適用する使用可能なルールを選択します。

注: [集約ルール パターン] フィールドを使用して、集約ルールを検索できます。

3. 次の手順に進みます。

コネクタの設定

一括接続作成用に、コネクタの設定を設定できます。作成した各コネクタは、手順 1 で .csv ファイルから収集したソースか保存済み設定のどちらかを使用して、この手順で設定する設定を共有します。

コネクタ設定の定義方法

1. コネクタ一括展開ウィザードを開き、[コネクタの設定]の手順に進みます。
ページに、手順 1 で設定した[ソースフィールド]が表示されます。ソースファイルの各ヘッダ列が、ソースフィールドとして表示されます。また、ページには、[センサの設定]領域に、選択した統合用のデフォルトのセンサの設定が表示されます。
2. 次の 2 つの方法のどちらかを使用して、コネクタの設定を設定します。
 - 該当するドロップダウンリストから[保存済み設定]を選択する。
 - 必要な設定エントリフィールドにソースフィールドのエントリをドラッグアンドドロップして、[センサの設定]領域の各設定を設定する。ソースフィールド値がない必須フィールドは手動で設定する。
たとえば、ソースリストに[ユーザ名]列があるとします。設定しているセンサタイプに[ユーザ名]センサの設定フィールド存在する場合は、ソースリストの[ユーザ名]列をここにドラッグします。
3. (オプション)必要に応じて、[繰り返し]をクリックして、[センサの設定]フィールドを追加します。
4. 次の手順に進みます。

エージェントの選択およびソースのマップ

設定したコネクタを作成するエージェントを選択できます。手順 1 で選択するイベントソースを、コネクタ展開のターゲットとするエージェントにマップします。

エージェントを選択してソースをマップするには、以下の手順に従います。

1. コネクタ一括展開ウィザードを開き、[エージェントの選択およびソースのマップ]の手順に進みます。

ページに、手順 1 でアップロードしたソースに基づいて、ソースのリストが表示されます。各ソースに行順に番号が付与されます。「ソース 1」がソースリストで指定した 1 行目を表します。

2. ターゲットにするエージェントを、エージェントグループ、プラットフォーム、またはエージェント名で検索します。
3. 必要な 1 つ以上のソースを、各ターゲット エージェント フォルダにドラッグし、コネクタ マッピングを保存するためにクリックします。
4. [保存]または[保存して閉じる]をクリックします。

選択したソースに基づくコネクタが、選択したエージェント上に設定されます。

複数コネクタの設定の更新

1 つ以上のデフォルト設定の変更により、同じログ センサを使用する複数のコネクタを更新できます。たとえば、ログ ファイル センサを使用して、複数のコネクタ上のログ ファイルのローテーション タイプを変更できます。

複数コネクタの設定を更新する方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックします。
2. [イベント精製ライブラリ]、[統合]、および[サブスクリプション]の各フォルダを展開します。
3. 設定の変更を適用するログ センサ タイプを使用する統合を選択します。
4. [バッチによる更新をコネクタに適用]をクリックします。
[コネクタの更新]ウィザードが開き、[コネクタの選択]ページが表示されます。
5. 更新を適用するコネクタを選択し、[デフォルトの設定]ページに進みます。
6. 更新する各フィールドに必要な値を入力し、フィールドの横のチェック ボックスをオンにします。
7. [実行]をクリックします。
確認メッセージが表示されます。

第 16 章：イベント相関およびインシデント管理

このセクションには、以下のトピックが含まれています。

[相関ルール タスク](#) (P. 615)

[インシデント管理タスク](#) (P. 627)

[インシデント詳細の表示](#) (P. 628)

第 17 章：相関ルール タスク

相関ルールは、環境内の不審なアクティビティまたは危険な状態を識別するためのイベント パターンをレポートできます。イベントが相関ルールの基準と一致するたびに、CA Enterprise Log Manager はインシデントを作成します。

管理者ロールを持っている場合、以下の相関ルール タスクを実行できます。

- 相関ルールを作成、編集、削除する
- 相関ルール グループを作成する
- 相関ルールをインポートまたはエクスポートする
- 相関ルールを適用し、環境内の通知宛先を関連付ける

このセクションには、以下のトピックが含まれています。

[相関ルールについて](#) (P. 616)

[定義済み相関ルールの使用](#) (P. 617)

[相関ルールとキー設定済みリストの使用](#) (P. 621)

[例：テスト用の CSV ファイルの作成](#) (P. 622)

[インシデント通知について](#) (P. 622)

[インシデント通知を設計および適用する方法](#) (P. 623)

相関ルールについて

定義済みの相関ルールを適用したり、相関ルール ウィザードを使用して環境に合わせてカスタム相関ルール作成したり、既存のルールを修正したりできます。相関ルールを使用すると、攻撃などのセキュリティリスクとなる可能性のあるイベントのグループを識別できます。相関ルールを作成または編集するには、管理者ロールを持っている必要があります。

相関ルールを作成する場合は、3 つのタイプのどれを作成するかを選択する必要があります。ルール テンプレートは、インシデントと見なすイベントを定義します。使用可能なテンプレートは以下のとおりです。

- 単純なフィルタ - 単一のイベントまたは状態を検索できます。このテンプレートでは、単一のイベントからインシデントを作成します。
- カウント テンプレート - 一連の同一のイベントを検索できます。相関ルールで検索する同じタイプのイベントの数を指定できます。設定した数のイベントがルールによって検出されると、インシデントがトリガされます。
- 状態の移行テンプレート - 関連する一連のイベントを検索できます。1 つの特定のイベントまたは状態が発生し、続いて 1 つ以上のイベントまたは状態が発生すると、ルールはインシデントを作成します。相関ルールで検索する状態およびその数を指定できます。

注: 相関を効果的に行うには、すべての受信イベントを参照する必要があります。そのため、抑制または集約ルールをエージェントレベルで適用しないようにすることを検討してください。エージェントで抑制または集約されたイベントは、相関およびインシデントの作成用として考慮されません。

イベント相関によって、ネットワークトラフィックが大幅に増加する場合があります。そのため、専用の相関サーバを割り当てることを検討してください。サーバのロールの詳細については、「[CA Enterprise Log Manager 実装ガイド](#)」を参照してください。

相関サービスで処理するインシデントメッセージが大量に存在する場合、相関サービスは最大 10,000 メッセージのキューを保持します。この数を超えるメッセージは失われます。CA Enterprise Log Manager は、これが発生した場合に自己監視イベントを生成します。

詳細情報:

[インシデント通知について](#) (P. 622)

定義済み相関ルールの使用

CA Enterprise Log Manager には、ユーザの環境で使用するさまざまな定義済み相関ルールが用意されており、これらはタイプまたは規制要件別に整理されています。たとえば、ライブラリ インターフェースの相関ルール フォルダには PCI というフォルダがあります。このフォルダには、さまざまな PCI 要件のルールが格納されています。また、ID というフォルダには、許可および認証に関する汎用ルールが含まれています。

ルールには 3 つのタイプがあり、各カテゴリにはそれらのいずれかまたはすべてが含まれています。このトピックでは、各タイプの 1 つを選択および適用する例を示します。

例 - 単純ルールの選択および適用

単純相関ルールは、1 つの状態または発生の存在を検出します。たとえば、通常の営業時間外のアカунト作成アクティビティを警告するルールを適用できます。ルールを適用する前に、適切な通知の宛先を作成しておく必要があります。

通常の営業時間外のアカунト作成ルールを選択および適用する方法

1. [管理] タブをクリックし、[ライブラリ] サブタブをクリックして、相関ルール フォルダを展開します。
2. [PCI] フォルダ、[要件 8] フォルダの順に展開して、[通常の営業時間外のアカунト作成ルール] を選択します。
ルールの詳細が右ペインに表示されます。
3. ルールの詳細を参照して、対象の環境内でルールが適切であることを確認します。この場合、フィルタはアカウント作成アクションを定義し、通常の営業時間を時間および曜日で設定します。
4. (オプション) 必要な場合は、ペインの上部にある[編集]をクリックしてフィルタ設定を変更します。たとえば、通常の労働時間を変更して現地の仕様に合わせることができます。
[ルールの管理] ウィザードが開き、ルールの詳細がロードされます。
5. [ルールの管理] ウィザードに通知の詳細を追加します。通知の詳細では、通知の宛先で指定された宛先に送信されるメッセージの内容を指定します。
6. ルールの作成が完了したら、ウィザードの[保存して閉じる]をクリックします。定義済み相関ルールを編集して保存すると、CA Enterprise Log Manager は自動的に新しいバージョンを作成し、元のバージョンを保存します。

7. [サービス]サブタブをクリックし、[関連サービス]ノードを展開します。
8. ルールを適用するサーバを選択します。関連サーバを識別した場合は、そのサーバを選択する必要があります。
9. [ルール設定]領域の[適用]をクリックし、[通常の営業時間外のアカウント作成]ルールの新バージョンおよびそれに関連付ける通知の宛先を選択します。
10. [OK]をクリックして、ダイアログ ボックスを閉じてルールをアクティブにします。

例 - カウント ルールの選択および適用

カウント関連ルールは、一連の同一状態または発生を識別します。たとえば、管理者アカウントによる 5 回以上のログイン失敗を警告するルールを適用できます。ルールを適用する前に、適切な通知の宛先を作成しておく必要があります。

[管理者アカウントによる 5 回失敗したログイン]ルールを選択および適用する方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックして、関連ルールフォルダを展開します。
2. [脅威管理]フォルダ、[不審なアカウントおよびログイン アクティビティ]フォルダの順に展開し、[管理者アカウントによる 5 回失敗したログイン]ルールを選択します。
ルールの詳細が右ペインに表示されます。
3. ルールの詳細を参照して、対象の環境内でルールが適切であることを確認します。この場合、フィルタは、キー設定済みリスト「Administrators」に属するユーザ名として管理者アカウントを定義し、カウントしきい値を 60 分内に 5 つのイベントに設定します。
4. (オプション) 必要な場合は、ペインの上部にある[編集]をクリックしてフィルタ設定を変更します。たとえば、時間しきい値を 30 分内に 3 つのイベントに変更できます。
[ルールの管理]ウィザードが開き、ルールの詳細がロードされます。
5. [ルールの管理]ウィザードに通知の詳細を追加します。通知の詳細では、通知の宛先で指定された宛先に送信されるメッセージの内容を指定します。

6. ルールの作成が完了したら、ウィザードの[保存して閉じる]をクリックします。定義済み相関ルールを編集して保存すると、CA Enterprise Log Manager は自動的に新しいバージョンを作成し、元のバージョンを保存します。
7. [サービス]サブタブをクリックし、[相関サービス]ノードを展開します。
8. ルールを適用するサーバを選択します。相関サーバを識別した場合は、そのサーバを選択する必要があります。
9. [ルール設定]領域の[適用]をクリックし、[管理者アカウントによる 5 回失敗したログイン]ルールの新バージョンおよびそれに関連付ける通知の宛先を選択します。
10. [OK]をクリックして、ダイアログ ボックスを閉じてルールをアクティブにします。

例 - 状態の移行ルールの選択および適用

状態の移行相関ルールは、一連の状態または発生を識別します。たとえば、同じユーザ アカウントによるログイン失敗後のログイン成功を警告するルールを適用できます。ルールを適用する前に、適切な通知の宛先を作成しておく必要があります。

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックして、相関ルールフォルダを展開します。
2. [ID]フォルダ、[認証]フォルダの順に展開し、[失敗したログイン、その後成功]ルールを選択します。

ルールの詳細が右ペインに表示されます。

3. ルールの詳細を参照して、対象の環境内でルールが適切であることを確認します。この場合、詳細ペインにはルールで追跡する 2 つの状態が表示されます。最初の状態は、同じユーザ アカウントまたは ID による 5 回以上のログイン失敗です。2 番目の状態は、同じユーザまたは ID によるログイン成功です。
4. (オプション) 必要な場合は、ペインの上部にある[編集]をクリックして状態設定を変更します。

[ルールの管理]ウィザードが開き、ルールを構成する 2 つの状態が表示されます。

5. 変更する状態をダブルクリックします。

[状態定義]ウィザードが開き、状態の詳細が表示されます。

6. 必要に応じて状態を変更したら、[保存して閉じる]をクリックして[ルール
の管理]ウィザードに戻ります。たとえば、最初の状態は 10 分以内の 5 回の
ログイン失敗をチェックします。ログイン失敗しきい値または時間、あるいは
その両方を変更できます。
7. [ルール
の管理]ウィザードに通知の詳細を追加します。通知の詳細では、
通知の宛先で指定された宛先に送信されるメッセージの内容を指定しま
す。
8. ルールの作成が完了したら、ウィザードの[保存して閉じる]をクリックします。
定義済み相関ルールを編集して保存すると、CA Enterprise Log Manager は
自動的に新しいバージョンを作成し、元のバージョンを保存します。
9. [サービス]サブタブをクリックし、[相関サービス]ノードを展開します。
10. ルールを適用するサーバを選択します。相関サーバを識別した場合は、そ
のサーバを選択する必要があります。
11. [ルール設定]領域の[適用]をクリックし、[失敗したログイン、その後成功]
ルールの新バージョンおよびそれに関連付ける通知の宛先を選択します。
12. [OK]をクリックして、ダイアログ ボックスを閉じてルールをアクティブにしま
す。

詳細情報:

[インシデント通知について](#) (P. 622)

[相関ルールについて](#) (P. 616)

[通知デフォルトの設定](#) (P. 624)

相関ルールとキー設定済みリストの使用

すべての相関ルールは、1 つ以上のフィルタから構築されます。一部の事前定義済みルールフィルタは、特定の属性フィールドにキー値のリストをコンパイルするための条件として使用される値が含まれていた場合に、指定されたテーブルからのすべての値を選択するように設計されています。

相関ルールの作成または適用時にキー設定済みリストを使用して、事前定義されたまたはカスタムの値をルールフィルタに適用できます。キー設定済みリストを手動または自動で更新し、リストを最新の状態に保つことができます。キー設定済みリストは、レポートで使用するのと同様の方法で相関ルールに使用できます。

キー設定済みリストの使用の詳細については、このガイドの「クエリおよびレポート」の章を参照してください。

詳細情報:

[キー設定済みリストのあるレポートの使用準備](#) (P. 332)

[キー設定済みリストを管理する方法](#) (P. 337)

[事前定義済みレポート用のキー設定済み値の作成](#) (P. 345)

例: テスト用の CSV ファイルの作成

この例では、相関ルールテスト用の CSV ファイルの作成方法を示します。この例では、単一のユーザによる 5 回のログイン失敗とその後のログイン成功を検索するルールをテストします。

ログイン失敗後の成功ルールをテストするための CSV ファイルを作成する方法

1. 管理者として CA Enterprise Log Manager にログインし、[クエリおよびレポート] タブをクリックします。
2. [過去 1 時間に 5 回失敗したログイン (実行ユーザ別)] クエリを検索します。
3. このクエリを実行し、結果を参照します。結果が存在する場合は、次の手順に進みます。存在しない場合は、ダミーのユーザを作成してログアウトし、その新しいダミー ユーザを使用してログイン失敗を行います。
4. クエリを CSV にエクスポートし、その CSV ファイルを Exce で開きます。
5. 必要に応じて、他のユーザ詳細を追加します。たとえば、ログイン成功を反映した情報を追加します。
6. 必要なすべてのイベント情報を追加したら、CSV ファイルを保存します。
7. テストするルールをライブラリ エクスプローラで開き、詳細ペインの[ルールのテスト] タブをクリックします。
8. CSV ファイルをロードし、適切なインシデントが作成されることを確認します。

インシデント通知について

インシデントに関する情報を渡す通知を設定して、インシデントの作成時に自動的にトリガされるようにするか、またはインシデントの参照後に手動で実行できます。いずれの場合も、環境内で使用する通知の宛先を最初に定義する必要があります。

通知は、以下の 2 つのコンポーネントで作成する必要があります。

1. 通知の宛先。これは、使用可能な宛先タイプの任意の組み合わせです。たとえば、宛先には電子メール アドレス、SNMP サーバ認証情報、IT PAM プロセス名が含まれます。宛先は複数のルールに割り当てることができます。

2. 通知の詳細。これらは個別のルールに追加され、通知によって送信される情報(電子メールの件名および本文、SNMP データ、IT PAM プロセス パラメータなど)です。

自動通知では、関連ルールに通知の詳細および宛先を関連付ける必要があります。両方のコンポーネントが存在する場合、ルールがインシデントを作成するたびに、自動通知が指定された宛先に送信されます。通知の宛先と詳細の組み合わせにより、通知をモジュール方式で設定できます。たとえば、同じ通知情報を異なる地域サービス デスクまたは IT 担当者に転送できます。

また、既存のインシデントから宛先を割り当てることができます。インシデントを開いて通知の宛先を割り当てると、ルールで指定された通知の詳細は即座に送信されます。通知を手動で送信するには、ルールに通知を組み込む必要があります。

詳細情報:

[通知デフォルトの設定](#) (P. 624)

[関連ルールについて](#) (P. 616)

インシデント通知を設計および適用する方法

関連ルール用の通知をセットアップできます。通知を使用すると、検出されたインシデントについてのキー情報を指定のスタッフに渡すか、または CA IT PAM サービス デスク チケットを自動的に作成できます。

環境内で通知を設定するには、以下の手順に従います。

1. 通知の宛先を計画および作成します。
2. 定義済みの関連ルールを選択するか、または環境内で使用するカスタムルールを作成します。
3. 設定する通知の詳細を関連ルールに追加します。
4. CA Enterprise Log Manager サーバに関連ルールを適用し、通知の宛先を割り当てます。

詳細情報:

[関連ルールについて](#) (P. 616)

[通知デフォルトの設定](#) (P. 624)

[関連サービスに関する注意事項](#) (P. 157)

通知デフォルトの設定

相関ルールに通知の詳細を設定して通知の内容(宛先ではない)を指定できます。たとえば、電子メールの件名および本文を設定できます。送信先アドレスは、通知の宛先によって制御されます。このシステムを使用すると、標準的な内容を(詳細を使用して)設定し、さまざまな受信者に(宛先を使用して)送信できます。

単一のルールに設定する通知の詳細に、使用可能な宛先タイプを自由に組み合わせる追加できます。

通知の詳細を設定する方法

1. 相関ルールウィザードを開き、必須のルール定義を入力して、[通知の詳細]ステップに進みます。
2. 電子メール タブをクリックし、以下の手順に従って電子メール通知情報を追加します。
 - a. 通知電子メールの件名を入力します。
 - b. (オプション) 電子メール タブのいずれかのフィールドにテキストを入力するときには、データフィールド ドロップダウンリストおよび[追加]ボタンを使用してデータフィールド変数を挿入できます。たとえば、`agent_address` を選択して[追加]をクリックします。
「%agent_address%」がテキストフィールドに表示されます。ルールによって電子メールが生成されると、`agent_address` 変数の代わりに実際の値が表示されます。
 - c. 通知電子メールの本文を入力します。
注: メッセージ本文は HTML 形式で作成されるため、入力するすべてのテキストが 1 行で表示されます。1 行の後に改行を入れるためには、テキストの行末に `<BR/>` を入力します。
3. [プロセス]タブをクリックし、以下の手順に従って CA IT PAM プロセスパラメータを追加します。
 - a. 以下のように、インシデント情報の送り先となる IT PAM プロセスの名前を入力します。
`/CA_ELM/EventAlertOutput`
 - b. [パラメータの追加]をクリックして、パラメータとその値を指定します。
[プロセスパラメータの追加]ダイアログ ボックスが開きます。
 - c. [名前]フィールドにパラメータ名(「Severity」など)を入力します。

- d. 値領域に入力するか、またはドロップダウンリストから CEG フィールドを選択して[データフィールドの追加]をクリックすることによって値を定義します。指定した CEG フィールドから指定したパラメータにイベント情報が渡されます。前の手順の例を引き続き使用し、IT PAM Severity パラメータの値として「event_severity」を選択します。
- e. 手順 a ～ c を繰り返して、必要に応じてパラメータおよび値を追加します。
- f. 現在のパラメータの CEG フィールドをすべて追加したら、[OK]をクリックします。

注: 値を入力し、必要に応じて複数の CEG フィールドを追加して、パラメータを定義できます。たとえば、アカウント推測ルールで使用する通知の説明パラメータを定義する場合は、以下のように入力します。

このインシデントは、10 分以内に発生した %dest_hostname% 上の %dest_identity_unique_name% による 4 回の失敗ログインをレポートします。

%value% という構造は、手順 b に示すように CEG フィールドを選択して [データフィールドの追加] ボタンを使用した結果です。

4. SNMP タブを選択し、以下の手順に従って SNMP トラップ設定を追加します。
 - a. SNMP 転送先によって要求されるカスタムトラップ ID を調節します。
 - b. 入力領域に送信する CEG フィールドの名前を入力します。フィールドへの入力に応じて、ドロップダウンリスト内で選択可能な値が絞り込まれます。
 - c. [追加]をクリックします。
 - d. 選択したフィールド領域に CEG フィールド名が表示されます。そのフィールドのイベント情報がこの通知テンプレートを使用して送信されます。少なくとも 1 つの CEG フィールドを指定する必要があります。
 - e. 手順 b ～ c を繰り返して、追加の CEG フィールドを送信します。
5. 該当する矢印をクリックして次に完了するウィザード手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、新規ルールが該当のフォルダに表示されます。それ以外の場合は、選択した手順が表示されます。

詳細情報:

[相関ルールについて](#) (P. 616)

[インシデント通知について](#) (P. 622)

第 18 章：インシデント管理タスク

CA Enterprise Log Manager インシデントは、相関ルールによって識別されて関連付けられる 1 つ以上のイベントで構成されます。相関ルールがその条件を満たす 1 つ以上のイベントを検出するたびに、CA Enterprise Log Manager はインシデントを作成します。

管理者ロールを持っている場合、以下のインシデント管理タスクを実行できます。

- 相関ルールによって環境内に作成されたインシデントの詳細を表示する
- インシデントリストをフィルタするか、結果の条件を設定して、特定のインシデントまたはインシデントタイプを検索し、またはインシデントビューを絞り込む
- 通知の宛先を既存のインシデントに適用して、電子メール宛先などの応答を制御する
- インシデント情報をエクスポートする
- インシデントに基づいてアクション アラートをスケジュールする
- 既存のインシデントを 1 つの新しいインシデントにマージする

注：インシデント管理タスクの詳細については、CA Enterprise Log Manager オンライン ヘルプを参照してください。

インシデント詳細の表示

環境内に作成されたインシデントの詳細(ステータス、優先度、履歴情報など)を表示できます。表示できるのは、ログインしている関連サーバにルーティングされたインシデントのみです。関連サービスを設定することによって、CA Enterprise Log Manager サーバがイベントをルーティングする方法を制御できます。

インシデントの詳細の表示方法

1. [インシデント]タブをクリックし、参照するインシデントを選択し、インシデント行をダブルクリックします。

[詳細]ダイアログ ボックスが開き、名前、日付、重大度などのインシデントの基本的な詳細が表示されます。
2. 適切なドロップダウン メニューを使用して、[優先度]または[ステータス]の設定を変更します。
3. (オプション)[履歴]タブをクリックし、インシデントに追加されたイベントの数や時間の情報、またはトリガされた自動通知を確認します。
4. [OK]または[適用]をクリックします。

詳細情報:

[関連サービスに関する注意事項 \(P. 157\)](#)

第 19 章：エージェント

このセクションには、以下のトピックが含まれています。

- [エージェント インストールの計画](#) (P. 629)
- [エージェント設定の計画](#) (P. 632)
- [エージェント管理タスク](#) (P. 637)
- [エージェント認証キーの更新](#) (P. 638)
- [エージェント バイナリのダウンロード](#) (P. 639)
- [エージェントの設定](#) (P. 640)
- [エージェント ダッシュボードの表示](#) (P. 643)
- [エージェントまたはコネクタのステータスの表示と管理](#) (P. 645)
- [エージェント グループを作成する方法](#) (P. 647)
- [エージェント管理の設定方法](#) (P. 650)
- [サーバ IP アドレスの変更の影響からエージェントを保護する方法](#) (P. 654)
- [サブスクリプション更新を適用する方法](#) (P. 657)

エージェント インストールの計画

エージェントのインストールを計画する際、計画者は、必要なエージェントの数やインストール場所を決定する必要があります。この計画は、エージェントをインストールする担当者が実施しても、ネットワーク管理者やシステム アーキテクトが実施してもかまいません。

エージェントのインストールを計画する方法

- 必要な情報を記録するのに適したエージェント インストール計画表の電子版を作成します。以下のサンプルの表と列見出しを利用できます。

イベントソースプラットフォーム	イベントソースが実行されているホストの名前または IP アドレス	以下のいずれか 1 つ： - エージェントレス - 直接 - エージェントレス - 収集ポイント - エンドポイント上のエージェント	イベントソースをインストールするホストの名前または IP アドレス

2. ログ収集のターゲットとなる各イベントソースを特定し、エージェント計画表にその場所およびプラットフォームを記録します。
3. 以下のような、各ソリューション タイプのコストおよびメリットを検討します。

	メリット	コストまたは制限
エージェントレス -CA Enterprise Log Manager から直接 - インストールされるエージェントなし	エージェントのインストールは必要ありません。	ソフトウェア アプライアンス プラットフォームと互換性のあるイベントソースの収集にしか対応できません。 エージェントレス - 収集ポイントのコストも当てはまります。
エージェントレス - 収集ポイント上のエージェント	イベントソースを実行するホストにエージェントをインストールする必要はありません。 共通のポイントに収集処理を統合することにより、インストールの必要なエージェントの数を、エージェント ベースの収集よりも減らせます。	抑制ルールは CA Enterprise Log Manager サーバにしか適用できません。このため、ネットワークトラフィックの削減効果は得られません。 ソースと CA Enterprise Log Manager サーバ間のイベントの通信は暗号化されません。 イベントソースにリモートでアクセスできる必要があります。
エージェント ベース - エンドポイント上のエージェント	CA Enterprise Log Manager サーバではなくソースに抑制ルールを適用できます。これによって、収集ポイントと CA Enterprise Log Manager サーバ間のネットワークトラフィックが削減されます。 ソースと CA Enterprise Log Manager サーバ間のログの通信が暗号化されます。 3 つのソリューションの中で、最も多くのイベント ボリュームが提供されます。	イベントソースの実行マシンにエージェントをインストールする必要があります。

4. イベントソースごとに、必要なソリューションを記録します。
5. エージェント計画表を、列 3 で並べ替え、その後列 2 で並べ替えます。これにより、同じホスト上で実行されているエージェント ベースのすべてのイベントソースが、ブロックに分けて表示されます。

6. エージェント ベースでイベントソースがマッピングされている場合は、同じ名前のブロック内で最初のイベントソースを検索し、そのデータを列 2 から列 4 にコピーします。これによって、1 つ以上のイベントソースが実行されている各ホストのエントリが 1 つのみになります（イベントソース数にかかわらず、特定のホスト上にエージェントは複数はありません）。
7. エージェントレス収集ポイントにマッピングしたイベントソースの場合は、以下の要領で、エージェントのインストール場所を計画します。
 - a. リモートエージェントの候補に挙げられているイベントソースへの対応に必要な収集ポイントの数を特定します。
 - b. ネットワーク上の場所の共通の領域別に、リモートエージェントの候補に挙げられているイベントソースのグループ化を計画します。
 - c. イベントソースの各グループに対して、収集ポイントとして使用するサーバを特定します。これは専用サーバの場合もあります。列 4 に決定を記録します。
8. ソリューションをマッピングせずにイベントソースを記録しており、レガシー CA アダプタを使用している場合は、「CA Enterprise Log Manager 実装ガイド」で詳細を確認してください。
9. エージェントのインストールを担当するユーザに、エージェント計画テーブルの 4 番目の列に記録したデータを提供します。

エージェント設定の計画

EiamAdmin ユーザは、最適な収集方法の決定に基づいてエージェントをインストールします。評価する方法には、以下のものがあります。

- CA Enterprise Log Manager サーバから直接のエージェントレス ログ収集。
直接収集と呼ばれることもあります。
- 収集ポイントからのエージェントレス ログ収集
- イベントソースが実行されているホストからのエージェント ベースのログ収集

インストールに先だって行われる分析によって、エージェントとコネクタを設定する管理者が必要とする情報の一部を明確化できる場合があります。

エージェント設定の最初の手順は、EiamAdmin から、またはエージェントがインストールされている場所を文書化する際に使用された代替ユーザから、エージェント計画スプレッドシートを取得することです。最初の管理者を設定した後、EiamAdmin ユーザから管理者に、注釈付きのエージェント インストール計画ワークシートが提供されます。最初の管理者は、ワークシートを受け取ると、設定の開始に必要な各エージェントのコネクタを計画します。

管理者は、EiamAdmin によってインストールされた各エージェントを設定します。さらに管理者は、収集方法(エージェントレスで直接、エージェントレスで収集ポイントから、あるいはエージェント ベースで)にかかわらず、各イベントソースのコネクタを設定します。各エージェント上にコネクタを設定するには、エージェントによって収集されるイベントの送信元 CA Enterprise Log Manager サーバにログオンします。

注: エージェントに設定するコネクタが少ないほど、パフォーマンスは向上します。

エージェント インストールがサイレント モードで実行される場合は、このプロセスは適用されません。この場合は、インストーラがコネクタを設定します。エージェント上に設定されたコネクタによって、エージェントは特定のイベントソースから元のイベントを収集できるようになります。コネクタによって、元のイベントが精製済みイベントに変換され、精製済みイベントが CA Enterprise Log Manager に転送されます。

エージェント グループの作成は任意です。カスタム エージェントグループを作成しない場合、エージェントはデフォルト エージェントグループに割り当てられます。管理者は、以下の場合にエージェントグループを作成します。

- 同一エージェントグループのエージェントによって収集されたイベントのレポートを有効にする場合。
- 別の管理者ユーザによる別のエージェントグループへの割り当てを有効にする場合（ユーザ アクセスを、アクセス ポリシーが付与されたエージェントグループを指定して制限することができます）。

収集されたイベントログは、処理および初期保存のために **CA Enterprise Log Manager** サーバに送信されます。管理者は、各エージェントまたは各エージェントグループのログを受信するサーバを設定する必要があります。エージェントグループにサーバを割り当てることで、エージェントグループ内のすべてのエージェントに簡単にサーバを割り当てることができます。

直接ログ収集の計画

CA Enterprise Log Manager のインストール時に、直接ログ収集に使用できるデフォルトのエージェントも併せてインストールされます。デフォルトのエージェントの使用は、別途エージェントをインストールする必要があるため、直接収集と呼ばれます。デフォルトのエージェントはほぼすべてのイベントソースからイベントを収集できますが、以下の制限があります。

- ログ センサは、ソフトウェア アプライアンス上で実行できる必要があります。ただし、ログ センサの中には、**WMI** ログ センサなど、特定のプラットフォームに関連付けられているものがあります。
- イベントソースにリモートでアクセスできる必要があります。

デフォルトのエージェントを設定する方法は、個別にインストールされたエージェントの設定と同じです。デフォルト エージェントによる直接ログ収集は、小規模なシステムに最も適しています。

直接ログ収集用イベントソース

CA Enterprise Log Manager では、CA Enterprise Log Manager サーバ上で実行して、エージェントレス直接ログ収集を簡略化することができるログ センサを提供します。このマニュアルのリリース時点で、以下がサポートされています。

- syslog
- WinRM
- ODBC
- TIBCO

デフォルト エージェントにサポートされている統合を判別するには、以下の手順に従います。

1. [管理]タブの[ログ収集]サブタブ下にある[エージェント エクスプローラ]から CA Enterprise Log Manager サーバを選択します。
2. [コネクタの新規作成]をクリックします。

[統合]ドロップダウンに、デフォルト エージェント上に展開するためのコネクタを作成する際の基となる統合が含まれています。コネクタは、統合を基に作成します。各統合は、特定のイベントソースからイベントを取得するように設計されています。

サポートされているログ センサおよび統合の全リストについては、[テクニカル サポート](#)の CA Enterprise Log Manager 製品のページを参照してください。

注: ログ センサは、データベース、syslog、ファイル、SNMP などの特定のログ タイプから読み込むよう設計された統合コンポーネントです。

エージェントレス ログ収集の計画

エージェントレス ログ収集は、複数のリモートイベントソースからイベントを集める収集サーバ上にエージェントを 1 つインストールすることで、実装できます。

収集サーバによるエージェントレス ログ収集の構成を計画する際には、以下の点を考慮する必要があります。

- エージェントに設定するコネクタが少ないほど、パフォーマンスは向上します。
- あるエージェント上に設定する最適なコネクタ最大数は、エージェントを専用サーバにインストールするかどうか、サーバの性能、ターゲットにするイベントソースの種類によって異なります。一般的に、単一のエージェント上には 40 から 50 程度のコネクタを設定するのが適切です。
- 同一の収集サーバと接続する複数のエージェント上に設定された同種のコネクタをグループ化しても、パフォーマンス上のメリットはありません。同じ論理で、同種のイベントソースから連携内の特定の **CA Enterprise Log Manager** サーバにイベントを転送しても、パフォーマンス上のメリットはありません。

エージェント ベースのログ収集の計画

インストーラを使用してローカル イベントソースのあるサーバ上にエージェントをインストールした後、インストール済みエージェントに、管理者はローカルで実行されている各イベントソースのコネクタを設定します。

同じタイプのイベントソースを持つターゲット サーバが多数ある場合は、これらのターゲット サーバをグループ化してエージェントグループとし、エージェントグループレベルで設定を行うことを検討してください。

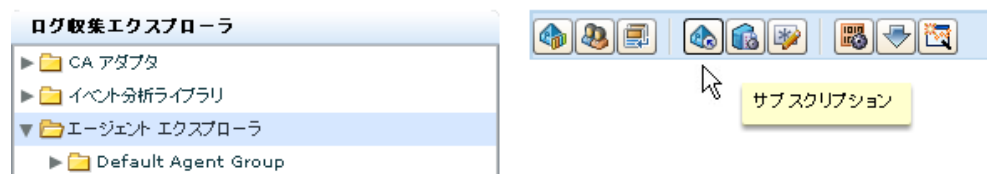
syslog の直接収集では、送信が保証されない可能性があります。これに対処するために、**syslog** イベントソースにインストールされたエージェント上に **syslog** リスナを設定してください。

設定するレベルの選択

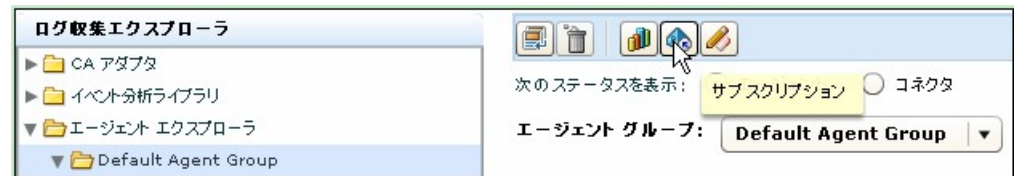
[サブスクリプション]、[抑制ルールの適用]、[ステータスとコマンド]の各オプションを、さまざまなレベルから選択できます。たとえば、サブスクリプション設定は、以下のレベルから開始できます。

- エージェント エクスプローラ
- デフォルトのエージェントグループまたはユーザ定義エージェントグループ
- エージェント

すべてのグループ内のすべてのエージェントにオプションが適用されるよう設定するには、エージェント エクスプローラを選択して、実行するアクションのボタンをクリックします。



選択したグループ内のすべてのエージェントにオプションが適用されるよう設定するには、グループ名を選択して、実行するアクションのボタンをクリックします。



1 つのエージェントのみにオプションが適用されるよう設定するには、エージェントを選択して、実行するアクションのボタンをクリックします。



エージェント管理タスク

エージェント エクスプローラで、環境内のイベント収集エージェントを表示および管理できます。[エージェント エクスプローラ]インターフェースを使用して、以下の領域の管理タスクを実行できます。

- エージェント設定 — エージェントの名前の変更、および、エージェントが属するグループおよび関連するグループの設定を実行できます。
- エージェント グループ — 地理別、ビジネスでの重要性別、イベントソースタイプ別などの、エージェントのグループ化を実行できます。グループ化したエージェントを、必要に応じて別の CA Enterprise Log Manager サーバに割り当てることもできます。
- サブスクリプション — 使用可能な更新を表示し、エージェントに割り当てることができます。
- エージェントのコマンドおよびステータス — エージェントの現在のステータスを表示し、必要に応じてエージェントを開始および停止できます。

詳細情報

[エージェント バイナリのダウンロード](#) (P. 639)

[エージェント認証キーの更新](#) (P. 638)

[エージェント グループを作成する方法](#) (P. 647)

[サブスクリプション更新を適用する方法](#) (P. 657)

[エージェント管理の設定方法](#) (P. 650)

エージェント認証キーの更新

CA Enterprise Log Manager サーバに登録する際にエージェントによって使用されるキーを表示および更新できます。このキーを定期的に変更することで、許可されていないエージェントが環境内にインストールされるのを防ぐことができます。デフォルトでは、キーは、すべてのアプリケーション インスタンスのすべての CA Enterprise Log Manager サーバで同じです。ただし、このキーをアプリケーション インスタンス別に一意に設定できます。

エージェントのインストール担当者は、エージェント インストール ウィザードで [認証コード] としてこのエージェントキーを入力する必要があります。

エージェント認証キーを更新する方法

1. [管理] タブをクリックし、[ログ収集] サブタブをクリックします。
[ログ収集] フォルダ リストが表示されます。
2. [エージェント エクスプローラ] フォルダをクリックします。
[エージェント管理] ボタンが [詳細] ペインに表示されます。
3. [エージェント認証キー] ボタンをクリックします。
[エージェント認証キー] ペインが表示されます。
4. [新しいキー] および [キーの確認] フィールドに新しいキーを入力し、[保存] をクリックします。
成功を確認するメッセージが表示されます。

エージェント バイナリのダウンロード

ほかのインストール メディアを使用せずに、エージェント バイナリをダウンロードし、ローカル コンピュータにインストールできます。

エージェントのインストールの詳細については、「[CA Enterprise Log Manager エージェント インストール ガイド](#)」を参照してください。

エージェント バイナリをダウンロードする方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダ リストが表示されます。
2. [エージェント エクスプローラ]フォルダをクリックします。
詳細ペインにエージェント管理ボタンが表示されます。
3. [エージェント バイナリのダウンロード]ボタンをクリックします。
[エージェント バイナリ リスト]が表示され、利用可能なエージェントおよび現在のバージョンが表示されます。
4. ダウンロードするエージェントをクリックします。
ダウンロード ダイアログ ボックスが表示されます。
5. エージェント バイナリ ファイルを保存する場所を選択し、[保存]をクリックします。
選択した場所にファイルが保存され、確認メッセージが表示されます。

エージェントの設定

インストールおよび登録されているエージェントに[エージェント エクスプローラ]からアクセスして、設定できます。

エージェントの設定方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [エージェント エクスプローラ]フォルダをクリックします。
フォルダが展開され、[エージェントグループ]フォルダが表示されます。
3. 設定するエージェントを選択し、ペイン上部の[編集]ボタンをクリックします。
[エージェントの詳細]が[詳細]ペインに表示されます。
4. 以下の項目などの、必要な変更を加えます。

[ユーザ名]

エージェントを実行するユーザ名を定義します。

ポート

CA Enterprise Log Manager と通信するためにエージェントが使用するポートを設定します。

エージェントグループ

エージェントが属するグループを定義します。

ファイルの最大数

イベント受信ファイル キューに作成できるファイルの最大数を設定します。ファイル数の上限は 1000 です。

1 ファイルあたりの最大サイズ

イベント受信ファイル キューのファイルの最大サイズを MB で設定します。ファイルが最大サイズに達すると、CA Enterprise Log Manager によって新規ファイルが作成されます。サイズの上限は 2048 MB です。

イベント送信モード

エージェントが使用する以下の送信方式を定義します。

- フェールオーバー - エージェントによって、Log Manager サーバリスト内の最初のサーバにイベントが送信されます。通信が切断されると、エージェントによって、通信が回復するまで、リスト表示された順に各サーバへの通信が試みられます。
- ラウンドロビン - エージェントによって、1 時間ごとに Log Manager サーバリスト内の次のサーバに通信を試行し、リストにある各サーバに順番にイベントが送信されます。この間隔は設定変更できません。

イベント暗号化の有効化

送信されるイベントが AES128 を使用して暗号化されるようエージェントを設定します。イベント暗号化を有効にすると、パフォーマンスに影響します。

リクエスト送信スケジュールの有効化

特定の期間内でのみエージェントがイベントを送信するよう設定します。[リクエスト送信スケジュールの有効化]チェック ボックスをオンにすると、[開始時間]および[終了時間]フィールドが表示されます。以下の条件に従って、必要な GMT 時間の値を 24 時間形式で入力します。

- 開始時間と終了時間の値の間には最低 1 時間が必要です。
- 開始時間の値が終了時間の値より大きい場合、終了時間は開始時間の翌日に設定されます。たとえば、開始時間を「23」に設定し、終了時間を「6」に設定すると、送信期間は午後 11 時 (GMT) から翌日の午前 6 時 (GMT) まで実行されます。

Log Manager サーバ

エージェントがイベントをルーティングする CA Enterprise Log Manager サーバ、およびエージェントが接続する順序を制御します。シャトルコントロールを使用して、使用可能なサーバを選択し、選択したサーバの右側にある矢印ボタンを使用して、通信優先度を設定します。

注: エージェントの更新は、CA Enterprise Log Manager サーバを更新してから実行してください。CA Enterprise Log Manager サーバは、サーバの現在のバージョン番号と同じかそれ以前のエージェントをサポートします。エージェントを設定または更新したときに、収集されたイベントが正常に保存されるようにするために、イベントがエージェントと同じかそれより高いレベルの CA Enterprise Log Manager サーバにのみ送信されることを確認してください。

5. [保存]をクリックします。

詳細情報

[エージェントグループを作成する方法](#) (P. 647)

改変された設定ファイルの処理

エージェントは、実行中に、メモリに格納された設定ファイルを使用します。エージェントの実行中に第三者によって設定ファイルが改変されると、エージェントは改変されたファイルを使用しません。CA Enterprise Log Manager サーバから新しい設定を受信すると、エージェントは再起動前に、ディスクファイルを受信したファイルに置き換えます。このようにして、改変されたファイルは自動的に正しいファイルに置き換えられます。

第三者によってファイル改変後に外部ソースからエージェントが再起動されると、エージェントはファイルが改変されシャットダウンされたことを検出します。エージェントは、改変されたファイルに含まれる CA Enterprise Log Manager サーバリストのデータなどの設定データを許可しません。

[エージェント エクスプローラ]には、エージェントが「応答なし」と表示されます。エージェント設定をリセットするには、CA Enterprise Log Manager サーバステータスおよびコマンド ツールを使用します。この操作の後、エージェントは正常に動作を再開します。

エージェント ダッシュボードの表示

エージェント ダッシュボードを表示して、お使いの環境のエージェントのステータスを表示することができます。また、ダッシュボードには、現在の **FIPS** モード (**FIPS** または **FIPS** 非準拠)などの詳細情報および使用状況の詳細情報が表示されます。この詳細情報には、1 秒あたりに読み込むイベント数、CPU 使用率、最終更新日と最終更新時刻が含まれます。

エージェント ダッシュボードを表示するには、以下の手順に従います。

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示されます。
2. [エージェント エクスプローラ]フォルダを選択します。
詳細ペインにエージェント管理ボタンが表示されます。

3. [エージェント ステータス モニタ/ダッシュボード]をクリックします。

エージェントの検索パネルが表示され、詳細なグラフ内に利用可能なすべてのエージェントのステータスが表示されます。以下に例を示します。

合計: 10 実行中: 8 保留: 1 停止済み: 1 応答なし: 0

4. (オプション) エージェント検索条件を選択し、表示されたエージェントのリストを絞り込みます。以下の条件を 1 つ以上選択できます。
- エージェント グループ— 選択したグループに割り当てられたエージェントのみが返されます。
 - プラットフォーム— 選択したプラットフォーム上で実行されているエージェントのみが返されます。
 - ステータス— 「実行中」など、選択したステータスのエージェントのみが返されます。
 - エージェント名パターン— 指定したパターンを含むエージェントのみが返されます。
5. [ステータスの表示]をクリックします。

検索条件に一致するエージェントのリストが表示されます。表示には、以下の情報が含まれます。

- ローカル コネクタの名前およびバージョン
- 現在の CA Enterprise Log Manager サーバ
- エージェントの FIPS モード (FIPS または FIPS 非準拠)
- 最後に記録された、エージェントによって処理される 1 秒あたりのイベント数負荷
- 最後に記録された CPU 使用率の値
- 最後に記録されたメモリ使用率の値
- 最新の設定更新
- 設定の更新ステータス

エージェントまたはコネクタのステータスの表示と管理

必要に応じて、環境内のエージェントまたはコネクタのステータスを監視したり、エージェントを再起動したり、コネクタを起動、停止および再起動することができます。

エージェント エクスプローラのフォルダ階層のさまざまなレベルからエージェントまたはコネクタを表示できます。必要に応じて、使用可能なビューを次のようにレベルごとに絞り込みます。

- エージェント エクスプローラ フォルダからは、現在の **CA Enterprise Log Manager** サーバに割り当てられたすべてのエージェントまたはコネクタを表示できます。
- 特定のエージェントグループ フォルダからは、そのエージェントグループに割り当てられたエージェントとコネクタを表示できます。
- 個々のエージェントからは、そのエージェントに割り当てられたエージェントとコネクタだけを表示できます。

3 つのすべてのレベルからエージェント用の FIPS モード (FIPS または FIPS 非準拠) を指定できます。

エージェントまたはコネクタのステータスを表示する方法

1. [管理] タブをクリックし、[ログ収集] サブタブをクリックします。
[ログ収集] フォルダ リストが表示されます。
2. [エージェント エクスプローラ] フォルダを選択します。
詳細ペインにエージェント管理ボタンが表示されます。
3. [ステータスとコマンド] をクリックします。 
[ステータス] パネルが表示されます。
4. [エージェント] または [コネクタ] を選択します。
エージェントまたはコネクタの検索パネルが表示されます。

5. (オプション) エージェントまたはコネクタの更新の検索条件を選択します。検索語を入力しない場合は、使用可能な更新がすべて表示されます。検索を絞り込むには、次の条件を 1 つ以上選択できます。
 - [エージェント グループ]: 選択したグループに割り当てられたエージェントおよびコネクタだけを返します。
 - [プラットフォーム]: 選択したオペレーティング システムで実行されているエージェントおよびコネクタだけを返します。
 - エージェントの名前パターン: 指定したパターンを含むエージェントおよびコネクタだけを返します。
 - (コネクタのみ) [統合]: 選択した統合を使用しているコネクタだけを返します。

6. [ステータスの表示] をクリックします。

詳細なグラフが表示され、検索と一致するエージェントまたはコネクタのステータスが表示されます。以下に例を示します。

合計: 10 実行中: 8 保留: 1 停止済み: 1 応答なし: 0

注: エージェントの設定を更新する場合、このエージェントの更新ステータスと連携内の他のエージェントを同期するには、CA Enterprise Log Manager で最大 5 分必要になります。

7. (オプション) ステータス表示をクリックして、グラフの下にある[ステータス] ペインに詳細を表示します。

注: エージェントまたはコネクタの[オンデマンド] ボタンをクリックすると、ステータス表示をリフレッシュすることができます。

8. (オプション) コネクタを表示している場合は、任意のコネクタを選択して、[再起動]、[開始]、または[停止] をクリックします。エージェントを表示している場合は、任意のエージェントを選択して、[再起動] をクリックします。

エージェント グループを作成する方法

エージェント グループを作成して、場所やオペレーティング システムなどの便利なカテゴリ別にエージェントを整理できます。エージェントグループ ウィザードを使用してエージェントグループを作成するプロセスは、以下の手順で構成されます。

1. エージェントグループ ウィザードの表示
2. グループの詳細の入力
3. エージェントの追加

詳細情報

[エージェントグループ ウィザードの表示](#) (P. 647)

[エージェントグループの詳細の追加](#) (P. 648)

エージェントグループ ウィザードの表示

エージェントグループを作成、または既存のエージェントグループを編集するには、エージェントグループを開きます。

エージェントグループ ウィザードを開く方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。

[ログ収集]フォルダ リストが表示されます。

2. [エージェント エクスプローラ]フォルダをクリックします。

詳細ペインにエージェント管理ボタンが表示されます。

3. [新規エージェントグループ]ボタンをクリックします。 

エージェントグループ ウィザードが表示されます。

ウィザードの使用時の操作

- ウィザードを閉じずにファイルを保存するには、[保存]をクリックします。
- ファイルを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

エージェントグループの詳細の追加

エージェントグループに、識別するための詳細を追加できます。

エージェントグループの詳細を追加する方法

1. エージェントグループウィザードを開きます。
2. グループの名前、および任意で参考用の説明を入力します。
3. [イベント送信モード]を選択します。
4. (オプション) 追加するサーバの最初のいくつかの文字を[名前パターン]フィールドに入力します。

検索に一致するサーバが[使用可能なサーバ]領域に表示されます。

5. シャトルコントロールを使用して追加するサーバを選択し、上下矢印を使用してエージェントグループ表示に表示する順序に並べ替えます。
6. 次の手順に進むか、[保存して閉じる]をクリックします。

[保存して閉じる]をクリックすると、グループが作成されます。それ以外の場合は、選択した手順が表示されます。

エージェントグループへのエージェントの追加

管理目的でグループにエージェントを追加できます。たとえば、物理的な所在地やオペレーティングシステム別にグループを作成できます。

注: エージェントグループのプロパティは、エージェントグループ内のすべてのエージェントに適用されます。

グループにエージェントを追加する方法

1. エージェントグループウィザードを開き、「エージェント」の手順に進みます。
2. (オプション) エージェント検索条件を選択します。検索語句を入力しない場合、すべてのエージェントが表示されます。検索を絞り込むには、次の条件を1つ以上選択できます。
 - エージェントグループ - 選択したグループに割り当てられたエージェントのみが返されます。
 - プラットフォーム - 選択したプラットフォーム上で実行されているエージェントのみが返されます。
 - エージェント名パターン - 指定したパターンを含むエージェントのみが返されます。
3. [検索]をクリックします。

検索と一致するエージェントが、[使用可能なエージェント]領域に表示されます。
4. シャトルコントロールを使用して、追加するエージェントを選択し、上下矢印を使用して、エージェントグループ表示に表示する順序に並べ替えます。

注: CA Enterprise Log Manager サーバが設定されていないエージェントグループにエージェントを移動することはできません。
5. [保存して閉じる]をクリックします。

エージェントグループが、リストに表示されます。

注: ユーザが作成したエージェントグループからエージェントを削除すると、削除したエージェントはデフォルトのエージェントグループに移動します。また、このエージェントはデフォルトのエージェントグループのプロパティを継承します。ただし、デフォルトのエージェントグループからエージェントを削除することはできません。

エージェント管理の設定方法

連携された環境内の複数の CA Enterprise Log Manager サーバにレポートするようエージェントまたはエージェントのグループを設定できます。これによって、選択した CA Enterprise Log Manager サーバにグループまたはエージェントからイベント情報が送信されるように設定できます。

Log Manager サーバの割り当てウィザードを使用して、エージェント管理を設定するプロセスは、以下の手順で構成されます。

1. Log Manager サーバの割り当てウィザードの表示
2. 割り当てるエージェント ターゲットまたはエージェント グループ ターゲットの選択
3. エージェントまたはグループを割り当てる CA Enterprise Log Manager サーバの選択

詳細情報

[Log Manager サーバの割り当てウィザードの表示](#) (P. 651)

[ターゲット エージェントの選択](#) (P. 652)

[ログ マネージャの選択](#) (P. 653)

Log Manager サーバの割り当てウィザードの表示

エージェントまたはエージェントのグループの割り当てを設定するには、Log Manager サーバの割り当てウィザードを開きます。

Log Manager サーバの割り当てウィザードを開く方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
[ログ収集]フォルダリストが表示され、[エージェント管理]ボタンが[詳細]ペインに表示されます。

2. [Log Manager サーバ]ボタンをクリックします。

Log Manager サーバの割り当てウィザードが表示されます。

ウィザードを使用する際に

- ウィザードを閉じずに保存するには、[保存]をクリックします。
- 割り当てを保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

詳細情報

[エージェント管理の設定方法](#) (P. 650)

[ターゲットエージェントの選択](#) (P. 652)

[ログ マネージャの選択](#) (P. 653)

ターゲット エージェントの選択

イベントの受信およびアーカイブのためにサーバにエージェントを割り当てるには、特定の CA Enterprise Log Manager サーバに割り当てるエージェントまたはグループを選択する必要があります。

ターゲット エージェントの選択方法

1. Log Manager サーバの割り当てウィザードを開きます。
2. エージェントをグループ単位で割り当てるか個々に割り当てるかを選択します。
3. [グループ]を選択する場合は、シャトル コントロールを使用して、割り当てるグループを選択します。検索エントリフィールドを使用し、名前の一部を入力して、グループを検索できます。入力と共に、使用可能なグループがフィルタされます。
4. [エージェント]を選択する場合は、シャトル コントロールを使用して、割り当てるエージェントを個別に選択します。[エージェントグループ]および[プラットフォーム]の各ドロップダウンリストと検索エントリフィールドを使用しエージェントを検索できます。
5. [Log Manager サーバの選択]に進みます。

詳細情報

[エージェント管理の設定方法 \(P. 650\)](#)

[Log Manager サーバの割り当てウィザードの表示 \(P. 651\)](#)

[ログ マネージャの選択 \(P. 653\)](#)

ログ マネージャの選択

エージェントまたはエージェントグループを割り当てる CA Enterprise Log Manager サーバを選択する必要があります。

ログ マネージャ サーバの選択方法

1. Log Manager サーバの割り当てウィザードを開き、ターゲット エージェントを選択して、[ログ マネージャの選択] 手順に進みます。
2. シャトル コントロールを使用して、エージェントまたはエージェントグループを割り当てるサーバを選択します。[名前パターン] エントリ フィールドに入力し、利用可能なリストを検索します。
3. [保存して閉じる] をクリックします。

エージェントまたはグループ化されたエージェントが、選択したサーバに割り当てられます。

詳細情報

[エージェント管理の設定方法 \(P. 650\)](#)

[Log Manager サーバの割り当てウィザードの表示 \(P. 651\)](#)

[ターゲット エージェントの選択 \(P. 652\)](#)

サーバ IP アドレスの変更の影響からエージェントを保護する方法

エージェントをインストールする際、収集したイベントでエージェントが最初に接続するプライマリ CA Enterprise Log Manager サーバを割り当てます。エージェントを設定する際、順序付けリスト内のほかの CA Enterprise Log Manager サーバを追加します。収集したログをプライマリ サーバに送信する準備ができたエージェントがプライマリ サーバに接続できない場合、エージェントは、使用可能なサーバが見つかるまでセカンダリ サーバに 1 つずつ接続します。セカンダリサーバの順序付けリストを設定すると、エージェントからサーバへのログ配信が保証されます。エージェントは一度に 1 つの CA Enterprise Log Manager にのみイベントを送ることができます。すなわち、イベントの重複はありません。

エージェントを管理するよう選択したサーバに新しい IP アドレスが割り当てられると、リスト上のサーバに収集済みイベントを転送するエージェントの機能が影響を受けます。予防的な措置を講じることによって、サーバが IP アドレスを手動でまたは動的に再割り当てされた場合でも、これらのサーバを使用するエージェントに対してサーバの高可用性を維持するのに役立ちます。

インストールされた CA Enterprise Log Manager の IP アドレスは、以下の場合に変わることがあります。

- DHCP による動的な再割り当て

シングル サーバシステムの CA Enterprise Log Manager サーバは、DHCP によって IP アドレスが割り当てられるよう設定されています。このサーバがエージェントを管理するよう選択された後のある時点で、DHCP が新しい IP アドレスを割り当てます。これは、CA Enterprise Log Manager が IP アドレスリースが期限切れになるまで長時間オフラインであった場合に発生することがあります。IP アドレスが動的に変更される場合、ユーザ通知は必要ありません。

- 手動による再割り当て

CA Enterprise Log Manager サーバは静的な IP アドレスで設定されています。新しいサブネットを展開する過程で IP アドレスが再割り当てされるサイトプロセスでは、新しい IP アドレスは CA Enterprise Log Manager サーバに手動で割り当てます。

それらのサーバの IP アドレスが変更される可能性がある場合、適切な処置を講じて、エージェントに対するサーバの高可用性を確保してください。

詳細情報:

[動的 IP アドレスを持つサーバの可用性の確保 \(P. 655\)](#)

[静的 IP アドレスを再割り当てする際のサーバの可用性の確保 \(P. 655\)](#)

動的 IP アドレスを持つサーバの可用性の確保

シングル サーバ CA Enterprise Log Manager をインストールする際に DHCP を選択する場合は、各エージェントをインストールする際にその CA Enterprise Log Manager のホスト名 (IP アドレスではない) を指定してください。こうすることで、CA Enterprise Log Manager サーバの IP アドレスが DHCP によって再割り当てされる際の影響が、このサーバを使用するエージェントに及ばないようになります。

エージェントをインストールする際に CA Enterprise Log Manager サーバの IP アドレスを指定すると、動的 IP アドレスが変更されたときには、エージェントを再インストールして、シングル システム CA Enterprise Log Manager サーバの可用性を回復する必要があります。この潜在的な問題を避けるために、もう 1 つ CA Enterprise Log Manager サーバをインストールし、すべてのエージェント向けのセカンダリ サーバとして追加することをお勧めします。これによって、サーバの高可用性を確保できます。

静的 IP アドレスを再割り当てする際のサーバの可用性の確保

静的 IP アドレスで CA Enterprise Log Manager サーバをインストールし、後で再割り当てを行う予定がある場合は、以下のワークフローを使用してこれらのサーバの順序付けリストを作成し、常にエージェントへの高可用性を確保します。デフォルトでエージェントによって 5 分ごとに設定情報がリフレッシュされるため、手順の後にエージェントを再起動する必要はありません。

重要: エージェントがマルチサーバシステム内の 1 つの CA Enterprise Log Manager サーバのみで設定されている場合は、必ず新しい IP アドレスを割り当てる前に、順序付けリストに 2 つ目のサーバを追加してください。この操作を行わない場合は、サーバの可用性を回復するために、サーバ IP アドレスの割り当て後にエージェントを再インストールし、再設定する必要が生じることがあります。

サーバに静的 IP アドレスを再割り当てする際に、エージェントが順序付けリスト上の CA Enterprise Log Manager サーバに接続できるようにする方法

1. 唯一の CA Enterprise Log Manager である CA Enterprise Log Manager サーバに IP アドレスの再割り当てを計画している場合は、元の CA Enterprise Log Manager 上の CA EEM を参照する一時的な CA Enterprise Log Manager をインストールします。
2. 1 つ以上の追加 CA Enterprise Log Manager サーバが、マルチサーバシステム内のどのエージェントにも設定されていない場合は、順序付けリストに少なくとも 1 つ追加サーバを割り当てます。

- a. [エージェント エクスプローラ]を選択し、[Log Manager サーバ]をクリックします。

Log Manager サーバ ウィザードが、[ターゲットの選択]手順が選択された状態で表示されます。

- b. 割り当てを行う方法に応じて、[エージェント]または[グループ]を選択します。
- c. [使用可能]リストから対象のエージェントまたはグループをターゲットとして選択し、[選択済み]リストに移動させます。
- d. [Log Manager サーバの選択]手順をクリックします。
- e. [使用可能]リストから「CA Enterprise Log Manager」を選択し、[選択済み]リストに移動させます。
- f. [保存して閉じる]をクリックします。

3. Log Manager サーバの割り当てウィザードを使用して、エージェントまたはエージェント グループ設定から CA Enterprise Log Manager サーバの順序付けリストの半分を削除します。

4. 選択したリストから削除したサーバに、新しい静的 IP アドレスを割り当てます。

5. 新しい IP アドレスを割り当てたサーバを再度追加します。

6. エージェントがその設定情報をリフレッシュするのを待ちます。

注: 手動でエージェントを再起動することで、情報をすぐにリフレッシュできます。

7. 順序付けリストの残りの半分の半分を削除します。

注: 一時サーバを追加している場合は、フェイルオーバー目的でこれを保持することも、アンインストールしてから削除することもできます。

8. IP アドレスを再割り当てします。
9. これらのサーバを再度追加し、元の順序付けリストを復元します。

詳細情報:

[エージェント管理の設定方法](#) (P. 650)

[サービスホストの削除](#) (P. 149)

サブスクリプション更新を適用する方法

エージェントまたはコネクタに **CA** サブスクリプション更新を適用できます。更新リストウィザードを使用してサブスクリプションパッケージを適用するプロセスは、以下の手順で構成されます。

1. 更新リストウィザードの表示
 2. 以下の更新タイプのうち 1 つの選択、および使用可能な更新パッケージの検索条件の指定
 - エージェントの更新
 - コネクタの統合更新
- 注:** エージェントおよびコネクタの更新がある場合、更新が正常に完了するように、エージェント更新を先に適用する必要があります。
3. 最新バージョンに更新するエージェントまたはコネクタの選択

詳細情報

[更新リストウィザードの表示](#) (P. 658)

[更新するエージェントまたはコネクタの選択](#) (P. 659)

[エージェントまたはコネクタ統合のバージョンの更新](#) (P. 660)

更新リスト ウィザードの表示

エージェントまたはコネクタを最新のバージョンに更新するには、更新リスト ウィザードを開きます。

更新リスト ウィザードを開く方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。

[ログ収集]フォルダ リストが表示されます。

2. [エージェント エクスプローラ]フォルダをクリックします。

[エージェント管理]ボタンが[詳細]ペインに表示されます。

3. [サブスクリプション]ボタンをクリックします。 

更新リスト ウィザードが表示されます。

ウィザードを使用する際に

- ウィザードを閉じずに保存するには、[保存]をクリックします。
- 進行状況を保存してウィザードを閉じるには、[保存して閉じる]をクリックします。
- ウィザードの表示を最後に保存した設定に戻すには、[リセット]をクリックします。

更新するエージェントまたはコネクタの選択

更新候補のエージェントまたはコネクタに検索条件を指定して、使用可能な更新を確認できます。

更新するエージェントまたはコネクタを選択する方法

1. 更新リストウィザードを開きます。

[更新選択リスト]が表示されます。

2. [エージェントの更新]または[コネクタの更新]を選択します。

注: エージェントおよびコネクタの更新がある場合、更新が正常に完了するように、エージェント更新を先に適用する必要があります。

3. エージェントまたはコネクタ更新の検索条件を完了します。

- a. ドロップダウンリストから[エージェントグループ]を選択します。
- b. ドロップダウンリストから[プラットフォーム]を選択します。
- c. ワイルドカードを使用して、エージェント名パターンを入力します。
- d. (コネクタ統合の更新のみ)ドロップダウンリストから[統合]を選択します。

4. [検索]をクリックします。

検索条件と一致する更新パッケージが、次のウィザード手順である「バージョンの選択」に表示されます。更新パッケージを表示して適用するために、「バージョンの選択」の手順に進む必要があります。

詳細情報:

[更新リストウィザードの表示](#) (P. 658)

[エージェントまたはコネクタ統合のバージョンの更新](#) (P. 660)

エージェントまたはコネクタ統合のバージョンの更新

リスト表示された各エージェントまたはコネクタのバージョンを、ダウンロードされた更新バージョンと比較して、更新が必要かどうかを判断し、現在のバージョンを別のバージョンに置き換えるかどうかを指定できます。

エージェントまたはコネクタを更新する方法

1. 更新リストウィザードを開き、更新を検討するエージェントまたはコネクタを選択します。
2. 「バージョンの選択」の手順に進みます。

検索条件に一致するエージェントまたはコネクタのリストが表示されます。

- 各エージェントが、現在のバージョンと、利用可能な更新バージョンを表示するドロップダウンリストと共に表示されます。
 - 各コネクタが、現在の統合バージョンと、利用可能な更新バージョンを表示するドロップダウンリストと共に表示されます。
3. (オプション)バージョンにかかわらず、選択したオペレーティング システム用の利用可能な更新をすべて表示するには、[OS バージョンのバイパス]を選択します。
 4. 更新を適用するエージェントまたはコネクタを選択し、[保存して閉じる]をクリックします。

エージェントによって更新がインストールされ、現在のバージョンが選択したエージェントまたは統合の更新で置き換えられます。

注: 選択した更新を適用した後、これらの詳細を調べて、すべてのエージェントまたはコネクタに、最新のバージョンが適用されているかどうかを確認できます。

第 20 章：カスタム証明書

このセクションには、以下のトピックが含まれています。

[カスタム証明書の実装](#) (P. 661)

[管理 CA Enterprise Log Manager サーバへの信頼されたルート証明書の追加](#) (P. 662)

[その他のすべての CA Enterprise Log Manager サーバへの信頼されたルート証明書の追加](#) (P. 664)

[アクセス ポリシーへの証明書共通名の追加](#) (P. 665)

[新しい証明書の展開](#) (P. 666)

カスタム証明書の実装

インストールプロセスによって 2 つの証明書が生成され、CA Enterprise Log Manager サーバの `/opt/CA/SharedComponents/iTechnology` ディレクトリに格納されます。インストールされた証明書は、そのまま使用できます。これらの証明書の名前は以下のとおりです (`ApplicationName` は CA Enterprise Log Manager 製品の CAELM です)。

- **`ApplicationNameCert.cer`**

この証明書は、管理サーバと通信するすべての CA Enterprise Log Manager サービスによって使用されます。この証明書のエントリは、`CALM.cnf` ファイル下にも存在します。

- **`ApplicationName_AgentCert.cer`**

この証明書は、CA Enterprise Log Manager サーバと通信するすべてのエージェントによって使用されます。

重要：アクティブなエージェントが存在する環境で `CAELM_AgentCert.cer` 証明書をカスタム証明書に置き換えるには、これらのエージェントを再インストールする必要があります。

カスタム証明書を使用するには、まずルート証明機関 (CA) から信頼されたルート証明書を取得する必要があります。証明機関は、複数の証明書をツリー構造で発行できます。信頼されたルート証明書の下すべての証明書は、ルート証明書の信頼性を継承します。このプロセスでは、両方の証明書を置き換える場合、カスタム サービス証明書とカスタム エージェント証明書の信頼されたルートが同じであることを前提としています。

拡張子が .cer のカスタム証明書のみがサポートされます。通常、信頼されたルート証明書を取得したら、以下の手順に従ってカスタム証明書を実装します。

1. 管理 CA Enterprise Log Manager サーバまたはスタンドアロン CA EEM の iAuthority.conf に信頼されたルート証明書を追加します。
2. CAELM_AgentCert.cer を置き換える場合は、管理 CA Enterprise Log Manager の iControl.conf に信頼されたルート証明書を追加し、次に、残りの各 CA Enterprise Log Manager でこの追加操作を繰り返します。
3. CAELMCert.cer を置き換える場合は、このカスタム証明書の共通名を管理 CA Enterprise Log Manager またはスタンドアロン CA EEM の AdministerObjects スコープ ポリシーに追加します。
4. 各 CA Enterprise Log Manager サーバの iTechnology フォルダにカスタム証明書を追加し、各設定ファイルに各証明書の名前およびパスワードを追加します。

管理 CA Enterprise Log Manager サーバへの信頼されたルート証明書の追加

まず、証明機関(CA)から PEM 形式の信頼されたルート証明書を取得します。次に、管理サーバまたはスタンドアロン CA EEM の iTechnology SPIN Web インターフェースにこの信頼されたルート証明書を追加します。

管理 CA Enterprise Log Manager に信頼されたルート証明書を追加する方法

1. 管理 CA Enterprise Log Manager サーバまたはスタンドアロン CA EEM の CA iTechnology SPIN Web インターフェースにアクセスします。

`https://<management_ELM_hostname>:5250/spin`
`https://<EEM_hostname>5250/spin`
[CA iTechnology SPIN] ページが表示されます。
2. ドロップダウンリストから[iTech 管理者]を選択し、[実行]をクリックします。
iTechnology 管理者ページが開き、ログインリンクが表示されます。
3. [ログイン]をクリックします。
CA iTechnology ログイン ダイアログ ボックスが表示されます。
4. EiamAdmin 認証情報を入力し、iAuthority を選択して[ログイン]をクリックします。

5. iAuthority タブを選択し、以下のように iAuthority.conf に信頼されたルートを追加します。
 - a. 証明書のラベルを入力します。ラベルとして「myself」を入力しないでください。
 - b. .cer ファイルを検索して選択します。
 - c. [信頼されたルートの追加]をクリックします。

確認メッセージが表示され、iAuthority.conf (管理サーバまたはスタンドアロン CA EEM のみに存在するファイル)に信頼されたルートが追加されることが示されます。

6. スタンドアロン CA EEM を使用する場合は、最後の手順に進みます。
7. CAELM_AgentCert.cer 証明書をカスタム証明書に置き換える場合は、以下のように iControl.conf に信頼されたルートを追加します。
 - a. 設定タブを選択します。
 - b. 前の手順と同じ証明書ラベルを入力します。
 - c. 前の手順と同じルート PEM (.cer)ファイルを検索して選択します。
 - d. [信頼されたルートの追加]をクリックします。

確認メッセージが表示され、カスタム証明書の信頼されたルートが管理 CA Enterprise Log Manager サーバの iTechnology ディレクトリの iControl.conf ファイルに追加されることが示されます。

8. [ログアウト]をクリックし、iTechnology SPIN を閉じます。

その他のすべての CA Enterprise Log Manager サーバへの信頼されたルート証明書の追加

CAELM_AgentCert.cer 証明書をカスタム証明書に置き換える場合は、残りの各 CA Enterprise Log Manager サーバの iTechnology SPIN Web インターフェースに信頼されたルート証明書を追加する必要があります。この手順では、CA iControl に信頼されたルート証明書を追加します。CAELMCert.cer 証明書のみを置き換える場合、この手順は必要ありません。

各非管理 CA Enterprise Log Manager サーバの CA iControl に信頼されたルート証明書を追加する方法

1. 非管理サーバが実行されている iGateway の SPIN UI にログインします。以下の URL を使用します。

`https://<ELM_hostname>:5250/spin/`

[CA iTechnology SPIN] ページが表示されます。

2. ドロップダウンリストから [iTech 管理者] を選択し、[実行] をクリックします。

iTechnology 管理者 ページが開き、ログインリンクが表示されます。

3. [ログイン] をクリックします。

CA iTechnology ログイン ダイアログ ボックスが表示されます。

4. EiamAdmin 認証情報を入力し、iAuthority を選択して [ログイン] をクリックします。

5. [設定] タブを選択し、以下のように信頼されたルートを追加します。

a. 前の手順と同じ証明書ラベルを入力します。

b. .cer ファイルを検索して選択します。

c. [信頼されたルートの追加] をクリックします。

カスタム証明書の信頼されたルートが iTechnology ディレクトリの iControl.conf ファイルに追加されます。確認のメッセージが表示されます。

6. [ログアウト] をクリックし、iTechnology SPIN を閉じます。

アクセス ポリシーへの証明書共通名の追加

CAELMCert.cer 証明書は、すべての CA Enterprise Log Manager サービスが CA Enterprise Log Manager 管理サーバと通信するために使用します。

CAELMCert.cer をカスタム証明書に置き換える場合、このカスタム証明書の共通名 (cn) を管理サーバまたはスタンドアロン CA EEM サーバの AdministerObjects ポリシーに追加する必要があります。

注: このポリシーから、[User] CERT_CAELM アイデンティティ (デフォルト証明書の共通名) を削除する必要はありません。

AdministerObjects ポリシーにカスタム証明書の共通名を追加する方法

1. 該当する URL を入力して、CA Enterprise Log Manager 管理サーバまたはスタンドアロン CA EEM サーバにアクセスします。

`https://<management_server_hostname>:5250/spin/calm`

`https://<EEM_server_hostname>:5250/spin/eiam`

2. CA Enterprise Log Manager 管理サーバに管理権限でログインします。スタンドアロン CA EEM にアクセスする場合は、EiamAdmin ユーザとしてログインします。
3. 管理タブ、ユーザおよびアクセス管理サブタブ、および左ペインのアクセスポリシー リンクをクリックします。スタンドアロン CA EEM にログインした場合は、[アクセスポリシーの管理] タブをクリックします。
4. スコープ ポリシー リンクをクリックします。

メインのペインに、スコープ ポリシーの [ポリシー テーブル] が表示されます。

5. スクロールして Administer Objects ポリシーを見つけ、AdministerObjects リンクを選択します。

AdministerObjects ポリシーが編集モードで開きます。

6. カスタム証明書の共通名 (cn) を以下のように追加します。

- a. ID フィールドにカスタム証明書の共通名を入力します。

- b. 矢印をクリックして、エントリを移動させます。

[選択された ID] リストに、[ユーザ]<カスタム証明書 cn> が表示されます。

7. [保存]をクリックします。

このポリシーにリスト表示されたリソースへの読み取りおよび書き込みアクセスを許可された ID としてカスタム証明書の共通名を追加する際に、**AdministerObjects** ポリシーも一緒に保存されます。

8. [閉じる]をクリックし、CA Enterprise Log Manager ユーザ インターフェースからログアウトします。

新しい証明書の展開

CA Enterprise Log Manager では 2 つの証明書を使用します。定義済み証明書的一方または両方をカスタム証明書に置き換えることができます。新しい証明書を展開するには、ソフトウェア アプライアンスにログオンし、iGateway を停止し、新しい証明書を追加し、証明書ファイルを変更して iGateway を再起動します。

新しい証明書を展開する前に、以下を確認します。

- 信頼されたルート証明書が、CA Enterprise Log Manager サーバが使用する管理サーバまたはスタンドアロン CA EEM の iTechnology iAuthority に追加されている。
- CAELM_AgentCert.cer 証明書をカスタム証明書に置き換える場合は、各 CA Enterprise Log Manager サーバの iTechnology iControl に信頼されたルート証明書が追加されている。
- カスタム証明書の共通名が AdministerObjects アクセス ポリシーに追加されている。これは、CAELMCert.cer を置き換えるカスタム証明書を指しています。

新しい証明書の登録方法

1. CA Enterprise Log Manager サーバがインストールされているホストにアクセスします。
2. **caelmadmin** 認証情報を使用して、CA Enterprise Log Manager サーバにログオンします。
3. コマンド プロンプトで、以下を入力して、ユーザを **root** に切り替えます。

```
su - root
```

4. 以下のショートカットを使用して、ディレクトリを **/opt/CA/SharedComponents/iTechnology** に変更します。

```
cd $IGW_LOC
```

5. iGateway を停止します。

```
./S99gateway stop
```

6. CAELMCert.cer を置き換えるには、以下の手順に従います。

- a. カスタム *ApplicationNameCert.cer* 証明書と *ApplicationNameCert.key* 鍵ファイルを *iTechnology* ディレクトリにコピーします。
- b. *CALM.cnf* ファイルを開きます。証明書名を新しい名前に置き換えます。
- c. 既存の鍵ファイル名を新しい鍵 ファイル名に変更します。

7. CAELM_AgentCert.cer を置き換えるには、以下の手順に従います。

- a. カスタム *ApplicationName_AgentCert.cer* 証明書と *ApplicationName_AgentCert.key* 鍵ファイルを *iTechnology* ディレクトリにコピーします。
- b. *AgentManager.conf* ファイルを開きます。証明書名を新しい名前に置き換えます。
- c. 既存の鍵ファイル名を新しい鍵 ファイル名に変更します。

8. iGateway を開始します。

```
./S99gateway start
```

CAELM_AgentCert.cer を置き換えた場合は、この展開の後に自動的にインストールされたエージェントはすべてカスタム証明書を使用します。

付録 A: アクセシビリティ機能

CA では、さまざまな利用環境のすべてのお客様が、当社の製品およびサポートドキュメントを正しく使用して重要なビジネス業務を遂行できるよう、全力を尽くしています。このセクションでは、CA Enterprise Log Manager に含まれているアクセシビリティ機能について説明します。

アクセシビリティ モード

アクセシビリティ モードを使用するよう CA Enterprise Log Manager を設定し、クエリおよびレポート内のすべてのグラフィック パネルを表形式に切り替えて表示できます。アクセシビリティ モードに切り替えるには、ログイン画面の[アクセシビリティの有効化]チェック ボックスをオンにします。

アクセシビリティ コントロール

CA Enterprise Log Manager 内を移動する際、以下の表に示すようなキーボードショートカットを使用できます。

タスク	キーボード ショートカット
開いているアプリケーションの切り替え	Ctrl + Tab
開いているウィンドウ内のファイルの選択	Ctrl + Tab
ヘルプ	F1
ボタンのクリック	Space または Enter
チェック ボックスのオン/オフ	Space または Enter
メニュー、コンボ ボックスを開く	Ctrl + 下方向キー
リストの移動	Ctrl + 下方向キーでフォーカスの設定 上方向/下方向キーで移動 Space または Enter でリスト項目の選択

タスク	キーボード ショートカット
ラジオ ボタン グループ	Ctrl + 下方向キーでフォーカスの設定 上方向/下方向キーで移動 Space または Enter でリスト項目の選択
作業中のウィンドウを閉じる	Alt + F4
ダブルクリック	Ctrl + D

CA Enterprise Log Manager 言語表示設定

英語以外に以下の言語で CA Enterprise Log Manager インターフェースを表示できます。

- フランス語
- イタリア語
- ドイツ語
- スペイン語
- 日本語

ブラウザ ウィンドウで言語設定を変更します。たとえば、Microsoft Internet Explorer を使用している場合は、[インターネット オプション] ダイアログ ボックスを開き、表示する主要な言語を追加または選択します。

サポートされている 5 つの言語の 1 つを選択すると、CA Enterprise Log Manager インターフェースを開いたときに、適切な言語で表示されます。インターフェース ラベルとタブは翻訳されますが、特定の要素は翻訳されません。タグのタイトルおよびレポート結果内のデータ文字列などは、英語のままになります。

注: CA Enterprise Log Manager が表示された状態で言語を変更した場合は、ブラウザ ウィンドウを最新の状態に更新して、新しい言語を表示してください。ログインした状態で変更した場合は、新しい言語のログイン画面に戻ります。

手動による CA Enterprise Log Manager のローカライゼーション

言語のファイルを自分で作成することで、手動で CA Enterprise Log Manager をローカライズできます。これによって、すでにサポートされている以外の言語で CA Enterprise Log Manager インターフェースを表示することができます。これを行うには、既存のファイルをコピーしてテンプレートとして使用します。

手動で CA Enterprise Log Manager をローカライズする方法

1. CA Enterprise Log Manager サーバ ホストにログインし、`opt/CA/LogManager/local` に移動して、テンプレートとして使用するファイルを選択します。各言語に、以下の 2 つのファイルがあります。

- `content.properties` - レポート名やクエリ名などコンテンツを表すテキストと、説明が含まれています。
- `ui.properties` - タブ ラベルやヘッダなど、インターフェース機能のタイトルを表すテキスト文字列が含まれています。

各ファイル名の前に、標準的な言語プレフィックスが付いています。たとえば、ドイツのコンテンツ ファイルは `de_content.properties` という名前です。英語のインターフェース ファイルは `en_ui.properties` という名前です。

2. 各ファイル タイプを 1 つずつコピーし、標準的なプレフィックスを使用して、名前を変更します。たとえば、ポルトガル語のローカライゼーション ファイルを作成する場合は、ファイルをコピーして、それらを `pt_content.properties` と `pt_ui.properties` という名前に変更します。

注: 標準的な言語プレフィックスは、ご使用のブラウザのサポートされている言語リストで特定できます。

3. ファイルを開き、元の言語文字列を必要な言語に翻訳します。たとえば、英語ファイルをコピーした場合は、各英語テキスト文字列を必要な言語に置換します。
4. 手動で翻訳したファイルを、それらを利用する各 CA Enterprise Log Manager サーバ上の、手順 1 で指定した場所に保存します。
5. ブラウザをターゲット言語に設定し、CA Enterprise Log Manager にログインします。

詳細情報:

[CA Enterprise Log Manager 言語表示設定](#) (P. 670)

付録 B: ODBC と JDBC を使用した収集済みイベントへのアクセス

このセクションには、以下のトピックが含まれています。

[CA Enterprise Log Manager での ODBC/JDBC アクセスについて](#) (P. 673)

[CA Enterprise Log Manager で使用する ODBC および JDBC クエリの作成](#) (P. 674)

[クエリの処理方法](#) (P. 676)

[例: アクセスフィルタを使用して、ODBC の結果を制限する](#) (P. 678)

[例: Crystal Reports と共に ODBC および JDBC クライアントを使用する準備](#) (P. 680)

[ODBC を利用した Crystal Reports からイベント ログ ストアへのアクセス](#) (P. 688)

[JDBC を使用した Crystal Reports からイベントへのアクセス](#) (P. 689)

[Windows システム上の ODBC クライアントの削除](#) (P. 691)

[JDBC クライアントの削除](#) (P. 691)

CA Enterprise Log Manager での ODBC/JDBC アクセスについて

CA Enterprise Log Manager では、イベント ログ ストアへの読み取り専用 ODBC および JDBC アクセスを提供しており、これによって、以下のことを実行できます。

- BusinessObjects の Crystal Reports などの外部レポートユーティリティを使用したカスタムレポートの設定
- 外部アプリケーションを使用した選択済みログ情報の取得

これらの機能により、すでに CA Enterprise Log Manager によって取得されているログ情報を使用して、独自のカスタムレポートを作成し、フォーマットすることができます。また、既存の相関エンジンやマルウェア検出パッケージなどの機能と共に使用するデータを取得できます。

イベント ログ ストアへのアクセスに使用する予定のサーバ上に、CA が提供するクライアントをインストールした後、データソースへの接続を設定してから、データの取得を開始します。サブスクリプション サービスによって、サーバ側コンポーネントがインストールされます。

CA Enterprise Log Manager で使用する ODBC および JDBC クエリの作成

CA Enterprise Log Manager における ODBC および JDBC のサポートは、以下のテーブルへの SELECT ステートメントを使用した読み取り専用クエリに制限されています。

- VIEW_EVENT - イベント データベースからのイベントが格納されます。
- VIEW_INCIDENT - インシデント データベースからのインシデントが格納されます。
- VIEW_INCIDENTEVENT_BYID - インシデント イベント データベースからのインシデント コンポーネント イベントが格納されます。

SELECT 文は、ANSI SQL 形式およびルールに準じて作成してください。SQL 解析エンジンはサーバ側コンポーネントに含まれています。解析には、X3.135-1992「Database Language SQL」仕様で定義されている Entry レベルの SQL の大部分が実装されています。また、解析では、ANSI SQL99 と、Microsoft SQL Server や Oracle などの商用データベースの SQL 機能をサポートしています。ODBC の最小限の文法仕様に準拠しています。

共通イベント文法は、このテーブルのスキーマとしての役割を果たします。スキーマの詳細については、「CEG リファレンス ガイド」を参照してください。

SQL サポートの制限事項

CA Enterprise Log Manager では、ストアードプロシージャコール、データ制御言語 (DCL) コマンド、およびデータ定義言語 (DDL) コマンドをサポートしていません。

CA Enterprise Log Manager では、以下のデータ操作言語 (DML) 操作およびキーワードをサポートしていません。

- UNION
- JOIN
- ネストされた SELECT

- INSERT
- UPDATE
- DELETE
- COMMIT、ROLLBACK などのトランザクション制御演算子

サポートされている SQL 機能

以下は、SELECT 文の作成での使用がサポートされている SQL 関数です。

- `ABS(numeric_exp)`
- `ROUND(numeric_exp, integer_exp)`
- `LCASE(string_exp)`
- `LOWER(string_exp)`
- `LENGTH(string_exp)`
- `LTRIM(string_exp)`
- `RTRIM(string_exp)`
- `SUBSTRING(string_exp, start, length)`
- `UCASE(string_exp)`
- `UPPER(string_exp)`
- `IFNULL (expr, default_val)`
- `ISNULL (expr, default_val)`
- `NVL (expr, default_val)`
- `CONVERT (value_exp, data_type)`
- `CURDATE()`
- `CURTIME()`
- `CURTIMESTAMP()`
- `DATEADD(datepart, number, date)`
- `TIMESTAMPADD(datepart, number, date)`

- DATEDIFF(*datepart*, *startdate*, *enddate*) *datepart* の値には、Year、Day、および second を使用できます。
- TIMESTAMPDIFF(*datepart*, *startdate*, *enddate*) *datepart* の値には、Year、Day、および second を使用できます。
- DAYOFMONTH(*date_exp*)
- DAYOFWEEK(*date_exp*)
- DAYOFYEAR(*date_exp*)
- HOUR(*time_exp*)
- MINUTE(*time_exp*)
- MONTH(*date_exp*)
- NOW()
- SECOND(*time_exp*)
- WEEK(*date_exp*)
- YEAR(*date_exp*)
- AVG([ALL | DISTINCT]*expression*)
- SUM([ALL | DISTINCT]*expression*)
- COUNT({[ALL | DISTINCT]*expression*] | *)
- MAX([ALL | DISTINCT]*expression*)
- MIN([ALL | DISTINCT]*expression*)

クエリの処理方法

CA Enterprise Log Manager では、ODBC や JDBC のクライアントによって開始されたクエリを以下の方法で処理します。

1. SELECT 文がクライアントアプリケーションによって ODBC 接続を介して CA Enterprise Log Manager サーバに送信されます。
2. CA Enterprise Log Manager サーバによって SELECT 文が検証されます。検証に成功したら、CA Enterprise Log Manager サーバによってクエリを表すデータ構造体を作成されます。

エラーが発生した場合は、クライアントドライバに直接エラーを返します。

3. CA Enterprise Log Manager サーバによって SQL 文が使用可能なクエリに変換されます。変換が成功したら、CA Enterprise Log Manager サーバによってクエリが実行されます。
エラーが発生した場合は、クライアントドライバにエラーを返します。
4. 有効期限タイマなどの各クエリの状態情報が CA Enterprise Log Manager サーバによって管理されます。これにより、セッションが終了したりクエリが期限切れになったりした場合にキャンセルできます。
5. CA Enterprise Log Manager サーバによって、クエリ結果が変換され、ODBC クライアントドライバに送信されて、クライアントアプリケーションによってデータが受信されます。

結果列の別名

クエリの状態管理の一部として、CA Enterprise Log Manager では、結果列名に別名を付与することをサポートしています。これによって、カスタムレポート内の共通イベント文法フィールドを独自のラベルや見出しを使用して表示できます。

CA Enterprise Log Manager サーバによって結果セットがクライアントドライバに返送されるときにも、別名は維持され、適切なデータマッピングに使用されます。

結果の制限

ディスク領域を管理するために、CA Enterprise Log Manager では、結果の行数を制限します。CA Enterprise Log Manager では、Transact-SQL の TOP キーワードのサブセットに固定値のみを指定して使用します。キーワードのパーセント変数はサポートしていません。

CA Enterprise Log Manager で使用されるデフォルトの TOP 値は 5000 行で、最大値は 50,000 行です。

CA Enterprise Log Manager 固有のエラーコード

以下は、CA Enterprise Log Manager イベント ログ ストアにアクセス中に発生する可能性のある ODBC および JDBC のエラーコードです。エラーメッセージに、それぞれのエラーの詳細が記載されます。

- 88 - サポートされていません。
付随するエラーメッセージに、サポートされていない機能に関する詳細が記載されます。
- 300 - 一般的なエラー
付随するエラーメッセージに、詳細が記載されます。
- 301 - マルチバイト文字パラメータの変換中にエラーが発生しました
- 302 - 認証エラー
- 304 - OrderBy 節または GroupBy 節内に無効な表現 (列)

以下のエラーは、SQL 文の実行エラーです。

- 305 - クエリの開始中にエラーが発生しました
- 306 - クエリ ステータスの取得中にエラーが発生しました
- 307 - クエリ結果 XML の解析中にエラーが発生しました
- 308 - クエリの実行エラー
- 309 - エラーが発生しましたがクエリは実行されました
- 310 - クエリ結果の取得中にエラーが発生しました
- 311 - クエリのタイムアウト

例: アクセスフィルタを使用して、ODBC の結果を制限する

アクセスフィルタを作成し、ODBC アクセスリクエストに返されるデータを制限できます。名前を指定されたアプリケーショングループのメンバーが ODBC クライアントを使用して CA Enterprise Log Manager イベント データにアクセスする際に、フィルタによって許可された情報のみが表示されます。

この例では、UNIX_Analysts という名前のアプリケーション グループがあり、このグループのすべてのメンバに対してイベント ログ ストアから UNIX のイベントのみを表示しようとする想定しています。この例で作成されたフィルタによって、CA Enterprise Log Manager ユーザ インターフェース内および ODBC による外部リクエストからのイベント データの表示が制限されます。

アクセスフィルタの詳細については、オンライン ヘルプを参照してください。

アクセスフィルタの作成方法

1. 管理者ユーザとして CA Enterprise Log Manager にログインします。
2. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
3. [新規アクセスフィルタ]をクリックします。 アクセスフィルタの設計ウィザードが表示されます。
4. [名前]フィールドに「UNIX 分析担当者」と入力し、[説明]フィールドに「UNIX 分析担当者のアクセスフィルタ」という語句を入力して、ダイアログボックスの一番上の[手順 2 ID]をクリックします。
5. [タイプ]を[アプリケーション グループ]に変更し、[名前]フィールドに「UNIX」と入力して、[ID の検索]をクリックします。
検索条件に一致する ID のリストがシャトル コントロールに表示され、必要な ID を選択できるようになります。
6. [使用可能な ID]リストから[UNIX_Analysts]アプリケーション グループを選択し、右矢印シャトル コントロールをクリックして、選択したグループを[選択された ID]リストに移動させます。
7. ダイアログ ボックスの一番上の[手順 3 アクセスフィルタ]をクリックします。
8. [新規イベントフィルタ] をクリックして行を追加し、[列]の下フィールド領域をクリックします。
9. ドロップダウンリストから[event_logname]を選択し、[値]の下フィールド領域をクリックします。

10. ドロップダウンリストから[UNIX]を選択します。ダイアログ ボックスは以下のようになります。

アクセスフィルタの設計

UNIX_Analysts

保存 保存して閉じる キャンセル

1 2 3

詳細 ID アクセスフィルタ

● = 必須

詳細フィルタ

フィルタ コントロールに条件文を定義して、イベントをフィルタします。

+ -

ロジック	(	列	演算子	値
		event_logname	等しい	Unix

11. [保存して閉じる]をクリックします。

例: Crystal Reports と共に ODBC および JDBC クライアントを使用する準備

BusinessObjects Crystal Reports を使用して ODBC または JDBC クライアントを CA Enterprise Log Manager イベントにアクセスさせるための準備をするには、以下の手順に従います。

1. データベースリソースへのアクセス権を許可する CA Enterprise Log Manager ユーザを作成します。
2. ODBC Service が SSL 暗号化およびポート 17002 を使用していることを確認します。
3. ODBC クライアントをインストールするか、Crystal Reports が存在するサーバに JDBC ファイルをコピーします。
これらのインストールの詳細については、「実装ガイド」を参照してください。
4. オペレーティング システム コンポーネントを設定します。
 - a. Windows の[コントロール パネル]で ODBC データソースを作成し、テストします。
 - b. JDBC クライアントを使用する Crystal Reports 設定ファイルを編集します。

5. CA Enterprise Log Manager による収集用イベントを作成します。

クエリされる種類のイベントがすでにイベント ログ ストアに含まれていることがわかっている場合は、この手順を省略できます。

注: このプロセスおよび関連する例は、基本的な SQL 文の作成と Crystal Reports の使用法が理解されていることを前提としています。Crystal Reports の使用の詳細については、BusinessObjects のオンライン ヘルプを参照してください。

ODBC や JDBC へのアクセス用の CA Enterprise Log Manager ユーザの作成

JDBC クライアントや ODBC クライアントで使用するための ELM_Access という名前のユーザ アカウントを作成するには、この手順を使用します。

データアクセス権が付与された CA Enterprise Log Manager ユーザは、ODBC または JDBC を使用して、イベント データにアクセスできます。CA Enterprise Log Manager と共に提供されるデフォルトの各ユーザ ロールには、この権限が付与されています。この例では、デフォルトの CA Enterprise Log Manager ロールである、管理者、分析担当者、または監査者のどれを付与されたユーザでも作成できます。

新規ユーザを作成するには、以下の手順に従います。

1. 管理者ユーザとして CA Enterprise Log Manager サーバにログインします。
2. [管理] タブをクリックし、[ユーザとアクセスの管理] サブタブをクリックします。
3. [ユーザ] ボタンをクリックして、組み込みの CA EEM ユーザ インターフェースを表示します。
4. [新規ユーザ] をクリックします。[新規ユーザ] ダイアログ ボックスが開きます。
5. [アプリケーション ユーザの詳細の追加] をクリックし、管理者アカウントにアプリケーション権限を付与します。

注: 実稼働環境では、ユーザがデータにアクセスするのに必要な最小限の権限を割り当てます。ユーザのロール、アクセス ポリシー、アクセス フィルタなど、多くの方法でアクセスを制限できます。詳細については、オンライン ヘルプを参照してください。

6. 必要に応じてユーザレコードを完了し、パスワードを割り当て、この例の後でできるように書き留めておきます。
7. ユーザを保存し、[ユーザ]ウィンドウを終了します。

ODBC サービス設定の設定

この手順を使用して、CA Enterprise Log Manager ODBC および JDBC のサービス設定を設定します。

注: この領域に変更を加えると、ODBC および JDBC の通信を有効にするサーバ側プロセスが再起動されます。

ODBC サービスを設定するには、以下の手順に従います。

1. 管理者ユーザとして CA Enterprise Log Manager サーバにログインします。
2. [管理]タブをクリックし、[サービス]サブタブをクリックします。
3. ODBC サービス ノードをクリックします。
4. デフォルト設定を使用します。
 - サービスの有効化: True (CA Enterprise Log Manager サーバ上の ODBC および JDBC の接続を許可する)
 - ポート: 17002
 - 暗号化 (SSL) を選択
 - セッション タイムアウト: 15 分
 - ログ記録レベル: デフォルト値の「設定なし」を使用します。
5. [保存]をクリックします。

「ELM」ODBC データソースの作成

この手順を使用して、「CA-ELM」という名前のデータソースを作成します。

注: データソースを設定する前に、ODBC クライアントをインストールします。

データソースを作成するには、以下の手順に従います。

1. Windows の[コントロール パネル]を開きます。
2. [管理ツール]フォルダを開き、[データソース(ODBC)]ユーティリティを起動します。
3. [追加]ボタンをクリックし、[データソースの新規作成]ダイアログ ボックスを表示します。
4. エントリ「DataDirect OpenAccess SDK 6.0」を選択し、[完了]ボタンをクリックします。

DataDirect OpenAccess SDK ODBC Driver セットアップ ユーティリティの設定画面が表示されます。

5. [データソース名]フィールドに「CA-ELM」と入力し、説明文を入力します。
6. [サービス ホスト]フィールドに CA Enterprise Log Manager サーバの名前を入力します。この例では、ca-elm を使用します。
7. [サービス ポート]フィールドに「17002」と入力します。
8. [暗号化 SSL]チェック ボックスをオンにします。
9. 以下のカスタム プロパティを入力します。

```
querytimeout=600  
(seconds);queryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncriticalErrors=false
```

10. [適用]をクリックし、次に[接続のテスト]をクリックします。

接続パラメータが正しければ、接続成功のメッセージが表示されます。

11. [OK]をクリックして[ODBC データソースの管理]ダイアログ ボックスに戻り、もう一度[OK]をクリックして、ユーティリティを終了します。

ODBC データソースの注意事項

以下は、CA Enterprise Log Manager に関連している ODBC データソースフィールドの説明です。

データソース名

このデータソースの名前を作成します。このデータを使用するクライアントアプリケーションがデータソースに接続する際に、この名前を使用します。

サービス ホスト

クライアントが接続する CA Enterprise Log Manager サーバの名前を指定します。ホスト名または IPv4 アドレスのいずれかを使用できます。

サービス ポート

CA Enterprise Log Manager サーバが ODBC クライアント接続をリスンする TCP サービス ポートを指定します。デフォルト値は **17002** です。ここで設定した値は、ODBC サーバ サービスの設定と一致する必要があります。一致しない場合、接続は失敗します。

サービス データ ソース

このフィールドは空白のままにします。そうでない場合、接続の試行は失敗します。

暗号化 SSL

クライアントと CA Enterprise Log Manager サーバ間の通信で暗号化を使用するかどうかを指定します。デフォルト値では **SSL** は有効です。ここで設定した値は、ODBC サーバ サービスの設定と一致する必要があります。一致しない場合、接続は失敗します。

カスタム プロパティ

イベントログ ストアで使用するための接続プロパティを指定します。プロパティ間の区切り文字は、スペースのないセミコロンです。推奨されるデフォルト値には、以下のものがあります。

querytimeout

この時間データの返信がない場合にクエリが終了するタイムアウト値を秒単位で指定します。以下は、このプロパティで使用する構文です。

```
querytimeout=300
```

queryfederated

連携クエリを実行するかどうかを指定します。この値を **false** に指定すると、データベース接続が確立された CA Enterprise Log Manager サーバ上でのみクエリが実行されます。以下は、このプロパティで使用する構文です。

```
queryfederated=true
```

queryfetchrows

クエリが成功した場合に、1 回のフェッチ操作で取得する行数を指定します。最小値は **1** で、最大値は **5000** です。デフォルト値は **1000** です。以下は、このプロパティで使用する構文です。

```
queryfetchrows=1000
```


offsetmins

この ODBC クライアントのタイムゾーンのオフセットを指定します。値を 0 に指定すると、GMT が使用されます。お使いのタイムゾーンの GMT からのオフセットを設定する際に、このフィールドを使用できます。以下は、このプロパティで使用する構文です。

```
offsetmins=0
```

suppressNoncriticalErrors

データベースが応答しない、ホストが応答しないなどの、クリティカルでないエラーが発生した場合のインターフェース プロバイダの動作を示します。

以下は、このプロパティで使用する構文です。

```
suppressNoncriticalErrors=false
```

Crystal Reports 設定ファイルの編集

CA Enterprise Log Manager JDBC クライアントと共に Crystal Reports を使用するには、最初にいくつかの設定を指定する必要があります。Crystal Reports XML 設定ファイルの設定が済めば、CA Enterprise Log Manager イベント ログ ストアに ANSI SQL 標準クエリを作成し、送信できます。

JDBC 用の Crystal Reports 設定を設定するには、以下の手順に従います。

1. 設定ファイルを編集する前に、必ず、JDBC クライアント JAR ファイルを Crystal Reports サーバにコピーします。
詳細については、「実装ガイド」を参照してください。
2. Crystal Reports が存在するサーバにアクセスします。
3. CRConfig.xml というファイルを見つけて、編集のために開きます。

4. <DataDriverCommon> タグと、その下の <Classpath> タグ セクションを見つけます。
5. JDBC クライアントの JDBC JAR ファイルの場所をクラスパスに追加します。
6. JDBC URL タグ内の値を、以下のように変更します。

```
jdbc:ca-elm://127.0.0.1:17002;encrypted=1;ServerDataSource=Default;CustomProperties=(querytimeout=600;queryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncriticalErrors=false)
```

これらのパラメータの詳細については、「JDBC URL の注意事項」のセクションを参照してください。

製品の接続パラメータの設定に関する追加情報については、Crystal Reports と共に提供されているドキュメントを参照してください。

7. JDBC クラス名タグ内の値を、以下のように変更します。

```
com.ca.jdbc.openaccess.OpenAccessDriver
```

8. ファイルを保存し、終了します。

詳細情報:

[JDBC URL の注意事項](#) (P. 686)

JDBC URL の注意事項

JDBC クライアントを使用して CA Enterprise Log Manager に格納されているイベントデータにアクセスする場合、JDBC クラスパスおよび JDBC URL の両方が必要となります。JDBC クラスパスは、ドライバ JAR ファイルの場所を指定したものです。JDBC URL は、ロードする際に JAR 内のクラスが使用するパラメータを定義したものです。

以下は、完全な JDBC URL の例です。

```
jdbc:ca-elm://127.0.0.1:17002;encrypted=1;ServerDataSource=Default;CustomProperties=(querytimeout=600;queryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncriticalErrors=false)
```

以下で、URL コンポーネントについて説明します。

jdbc:ca-elm:

CA Enterprise Log Manager と共に提供されている JDBC ドライバを指定する、プロトコル:サブプロトコルの文字列を定義します。

//IP Address:Port;

アクセスするデータが格納された CA Enterprise Log Manager サーバを表す IP アドレスを指定します。ポート番号は、通信に使用するポートで、CA Enterprise Log Manager [ODBC サービスの設定] パネルの設定と一致する必要があります。ポートが一致しない場合、接続の試行は失敗します。

encrypted=0|1;

JDBC クライアントと CA Enterprise Log Manager サーバ間の通信に SSL 暗号化を使用するかどうかを決定します。デフォルト値は 0 で、暗号化されず、URL 内での指定が必要ありません。encrypted=1 と設定すると、暗号化が有効になります。接続の暗号化が明示的に設定されます。また、この設定は、CA Enterprise Log Manager [ODBC サービス] ダイアログ ボックスで設定したものと一致する必要があります。一致しない場合は、接続の試行は失敗します。

ServerDataSource=Default

データソースの名前を指定します。CA Enterprise Log Manager イベント ログ ストアへのアクセスの場合は、この値を「Default」に設定します。

CustomProperties= (x; y; z)

このプロパティは ODBC カスタム プロパティと同じものです。明示的に指定しない場合、URL 例で示されたデフォルト値が適用されます。

詳細情報

[ODBC データソースの注意事項 \(P. 683\)](#)

ODBC の例のためのイベントの作成

クエリの例を表示するには、以下のようなアクティビティの失敗を発生させて、関連イベントを作成します。

- 複数回 CA Enterprise Log Manager サーバに不正にログインする。
- イベントが特定の CA Enterprise Log Manager サーバに送信されるエージェントホストに不正にログインする。
- 不正な認証情報を使用してネットワークリソースまたはシステムリソースにアクセスする。

ODBC を利用した Crystal Reports からイベント ログ ストアへのアクセス

ODBC アクセス機能を使用して、BusinessObjects Crystal Reports などのサードパーティ製レポートツールから CA Enterprise Log Manager イベント データにクエリを実行できます。必要なインストールおよび設定が完了したら、CA Enterprise Log Manager イベント ログ ストアに ANSI SQL 標準クエリを作成し、送信できます。

イベント ログ ストアのデータベーススキーマは、共通イベント文法 (CEG) です。CA Enterprise Log Manager オンライン ヘルプに、クエリを作成する際に役立つ CEG 参照コンポーネントがあります。また、標準装備のクエリの基礎を構成している SQL 文を参照することもできますが、CA Enterprise Log Manager の外部からデータベースにアクセスする場合は ANSI SQL を使用してください。

Crystal Reports からイベント データにアクセスするには、以下の手順に従います。

1. 必須のインストールおよび環境設定タスクを完了します。
2. Crystal Reports を起動し、標準レポートウィザードを開きます。
3. [データ]ダイアログ ボックスで ODBC 接続を作成し、Windows の[コントロール パネル]で作成した ODBC データソースを選択します。



4. ADD コマンド機能を使用して、SQL 入力領域でクエリを作成します。

たとえば、以下のようなクエリを作成できます。

```
SELECT source_username as source_username , SUM(event_count) AS  
FUNC_SUM_event_count FROM view_event WHERE event_result = 'F' GROUP BY  
source_username ORDER BY FUNC_SUM_event_count DESC;
```

5. OK をクリックして、クエリ エントリを完了します。

クエリによって返されたデータ列を配置するためのレポート テンプレートが表示されます。

6. 右上隅にある[フィールド エクスプローラ]から、フィールドを、レポート テンプレートに列としてドラッグ アンドドロップします。

クエリを実行すると、フィールドと関連付けられた値が表示されます。Crystal Reports を使用して、必要な視覚化やカスタマイズを作成できます。

7. (オプション)レポート結果を、標準装備のレポート「失敗アクティビティ(実行 ユーザ別)」と比較します。

JDBC を使用した Crystal Reports からイベントへのアクセス

以下のタスクによって、JDBC を使用して、イベント ログ ストアにアクセスできます。

1. クライアントの JDBC JAR ファイルを、Crystal Reports が存在するサーバにコピーします。
2. Crystal Reports 設定ファイルを編集します。
3. Crystal Reports を使用して、クエリを送信します。

注: このプロセスおよび関連する例は、基本的な SQL 文の作成と Crystal Reports の使用方法が理解されていることを前提としています。Crystal Reports の使用の詳細については、BusinessObjects のオンライン ヘルプを参照してください。

JDBC ドライバ JAR ファイルのコピー

ドライバを使用して CA Enterprise Log Manager サーバからイベントにアクセスするには、事前に、関連する JAR ファイルを、アクセスに使用するサーバにコピーします。

ファイルをコピーするには、以下の手順に従います。

1. ISO イメージを開くか、アプリケーション インストール DVD にアクセスします。
2. ¥CA¥ELM¥JDBC ディレクトリに移動します。
3. JAR ファイルを、Crystal Reports が存在するサーバにコピーします。

使用しているレポートパッケージには、これらのファイル用の場所が必要です。アプリケーションと共に提供されているマニュアルを確認してください。

4. 接続を設定する際に、参照パス用にこれらのファイルを配置するディレクトリを書き留めます。

JDBC を利用した Crystal Reports からイベント ログ ストアへのアクセス

JDBC アクセス機能を使用して、BusinessObjects Crystal Reports などのサードパーティ製レポート ツールから CA Enterprise Log Manager イベント データにクエリを実行できます。

イベント ログ ストアのデータベーススキーマは、共通イベント文法 (CEG) です。CA Enterprise Log Manager オンライン ヘルプに、クエリを作成する際に役立つ CEG 参照コンポーネントがあります。また、標準装備のクエリの基礎を構成している SQL 文を参照することもできますが、CA Enterprise Log Manager の外部からデータベースにアクセスする場合は ANSI SQL を使用してください。

Crystal Reports からイベント データにアクセスするには、以下の手順に従います。

1. Crystal Reports を起動し、標準レポートウィザードを開きます。
2. [データ]ダイアログ ボックスで JDBC 接続を作成します。
注: [接続情報]ダイアログ ボックスが表示されたら、[データベース名]に「デフォルト」という値を使用してください。
3. ADD コマンド機能を使用して、SQL 入力領域で以下のクエリを作成し、実行します。

```
SELECT source_username as source_username , SUM(event_count) AS  
FUNC_SUM_event_count FROM view_event WHERE event_result = 'F' GROUP BY  
source_username ORDER BY FUNC_SUM_event_count DESC;
```

4. 右側にある[フィールド エクスプローラ]から、フィールドを、レポート テンプレートに列としてドラッグ アンドドロップします。
クエリを実行すると、フィールドと関連付けられた値が表示されます。Crystal Reports ツールを使用して、必要な視覚化やカスタマイズを作成できます。
5. (オプション)レポート結果を、標準装備のレポート「失敗アクティビティ(実行ユーザ別)」と比較します。

Windows システム上の ODBC クライアントの削除

すべての Windows プラットフォーム上で、クライアント インストール パッケージの[削除]オプションを使用すると、システム情報内の製品のファイルおよびエントリが削除されます。

重要: ローカル ODBC クライアントのインストール ディレクトリに IP ソース ファイルを作成している場合は、Windows システム上の ODBC クライアントを削除する前に、別の場所にファイルをバックアップしてください。

ローカル ODBC クライアントをインストールしていて、別の場所にインストールする必要がある場合は、[削除]オプションを使用します。インストールされているローカル ODBC クライアントを削除してから、新しい場所に再インストールします。

ODBC クライアントを削除するには、以下の手順に従います。

1. Windows の[コントロール パネル]の[プログラムの追加または削除]ユーティリティにアクセスします。
2. CA Enterprise Log Manager ODBC ドライバのエントリを見つけて選択します。
3. [削除]をクリックします。

JDBC クライアントの削除

JDBC クライアントをアンインストールするには、インストール ディレクトリを削除します。

用語集

(ダウンロードする) モジュール

モジュールは、サブスクリプションを通じてダウンロードが可能になるコンポーネント更新の論理グループです。モジュールは、バイナリ更新またはコンテンツ更新、あるいはその両方を含む場合があります。たとえば、すべてのレポートから構成されるモジュールもあれば、すべてのスポンサー バイナリ更新から構成されるモジュールもあります。CA によって、各モジュールの構成要素が定義されます。

○証明書

CA Enterprise Log Manager によって使用される定義済みの証明書は、CAELMCert.cer と CAELM_AgentCert.cer です。すべての CA Enterprise Log Manager サービスは、CAELMCert.cer を使用して管理サーバと通信します。すべてのエージェントは、CAELM_AgentCert.cer を使用してそれぞれの収集サーバと通信します。

Administrator ロール

Administrator ロールは、すべての CA Enterprise Log Manager リソースへのすべての有効なアクションを実行する権限をユーザに付与します。Administrator だけが、ログ収集およびサービスの設定や、ユーザ、アクセス ポリシー、およびアクセス フィルタの管理を許可されます。

Analyst ロール

Analyst ロールは、カスタム レポートおよびカスタム クエリの作成および編集、レポートの編集および注釈付け、タグの作成、レポートおよびアクション アラートのスケジュールを実行する権限をユーザに付与します。Analyst は、すべての Auditor タスクも実行できます。

AppObjects

AppObjects、すなわちアプリケーション オブジェクトは、特定の製品のアプリケーション インスタンス下にある CA EEM に格納された製品固有のリソースです。CAELM アプリケーション インスタンスの場合、これらのリソースには、レポートおよびクエリのコンテンツ、レポートおよびアラート用のスケジュール済みジョブ、エージェントのコンテンツおよび設定、サービス、アダプタ、および統合の設定、データ マッピングファイルおよびメッセージ解析ファイル、抑制ルールおよび集約ルールが含まれます。

Auditor ロール

Auditor ロールは、レポートおよびレポートに格納されているデータへのアクセス権をユーザに付与します。Auditor は、レポート、レポートテンプレートリスト、スケジュール済みレポートジョブリスト、作成済みレポートリストを表示できます。Auditor はレポートをスケジュールし、レポートに注釈を追加できます。アクションアラートを表示する際に認証は不要と設定されていない限り、Auditor には RSS (Rich Site Summary) フィードへのアクセス権はありません。

CA Embedded Entitlements Manager の URL

CA Embedded Entitlements Manager (CA EEM) の URL は、https://<ip_address>:5250/spin/eiam です。ログインするには、アプリケーションとして CAELM を選択し、EiamAdmin ユーザ名に関連付けられたパスワードを入力します。

CA Enterprise Log Manager

CA Enterprise Log Manager は、さまざまなタイプの広く分散したイベントソースからログを収集し、クエリおよびレポートの準備状況をチェックし、外部の長期用ストレージに移動した圧縮済みログのデータベースを記録するのに役立ちます。

CA Enterprise Log Manager の URL

CA Enterprise Log Manager の URL は、https://<ip_address>:5250/spin/calm です。ログインするには、管理者によってアカウントに定義されたユーザ名および関連するパスワードを入力します。または、デフォルトのスーパーユーザ名 EiamAdmin および関連するパスワードを入力します。

CA IT PAM

CA IT PAM は、CA IT Process Automation Manager の略です。この CA 製品は、定義されたプロセスを自動化するものです。CA Enterprise Log Manager では 2 つのプロセスを使用します。CA Service Desk などのローカル製品のイベント/アラート出力プロセスを作成するプロセスと、キー設定済み値としてインポートできるリストを動的に生成するプロセスです。統合には CA IT PAM r2.1 が必要です。

CA Spectrum

CA Spectrum はネットワーク障害管理製品で、CA Enterprise Log Manager に統合して、SNMPトラップの形で送信されるアラートの宛先として使用することができます。

CA アダプタ

CA アダプタは、iTechnology を介してネイティブにイベントを送信するソースに加えて、CA Audit クライアント、iRecorders、SAPI レコーダなどの CA Audit コンポーネントからイベントを受信する、リスナのグループです。

CA サブスクリプション サーバ

CA サブスクリプション サーバは、CA からのサブスクリプション更新のソースです。

CAELM

CAELM は、CA EEM が CA Enterprise Log Manager に使用するアプリケーション インスタンス名です。CA Embedded Entitlements Manager 内の CA Enterprise Log Manager 機能を使用するには、URL `https://<ip_address>:5250/spin/eiam/eiam.csp` を入力し、アプリケーション名として CAELM を選択し、EiamAdmin ユーザのパスワードを入力します。

caelmadmin

caelmadmin ユーザ名およびパスワードは、ソフトウェア アプライアンスのオペレーティング システムにアクセスするのに必要な認証情報です。caelmadmin ユーザ ID は、このオペレーティング システムのインストール中に作成されます。インストーラは、ソフトウェア コンポーネントのインストール中に、CA EEM スーパーユーザ アカウント EiamAdmin 用のパスワードを指定する必要があります。caelmadmin アカウントには、これと同じパスワードが割り当てられます。サーバ管理者は、caelmadmin ユーザとして ssh でログインし、このデフォルトのパスワードを変更することをお勧めします。管理者は root として ssh でログインできませんが、必要な場合には、ユーザを root に切り替えることができます。

caelmservice

caelmservice は、iGateway およびローカル CA EEM サービスを root 以外のユーザとして実行できるようにするサービス アカウントです。caelmservice アカウントは、サブスクリプション更新と共にダウンロードされたオペレーティング システム更新をインストールするために使用されます。

CALM

CALM は、Alert、ArchiveQuery、calmTag、Data、EventGrouping、Integration、および Report の CA Enterprise Log Manager リソースを含んでいる事前定義済み リソース クラスです。このリソース クラスで許されるアクションは、注釈付け (Report)、作成 (Alert、calmTag、EventGrouping、Integration、および Report)、データ アクセス (Data)、実行 (ArchiveQuery)、およびスケジュール (Alert、Report) です。

calmTag

calmTag は、特定のタグに属するレポートとクエリにユーザを制限するスコープポリシーを作成する際に使用される AppObject の名前付き属性です。すべてのレポートおよびクエリは AppObjects で、属性は calmTag になります（これはリソース Tag と混同されないようにするためです）。

CALM アプリケーション アクセス ポリシー

CALM アプリケーション アクセス ポリシーは、CA Enterprise Log Manager にログインできるユーザを定義するアクセス制御リストタイプのスコープ ポリシーです。デフォルトでは、(グループの) Administrator、(グループの) Analyst、および(グループの) Auditor がアクセスを許可されています。

CEG フィールド

CEG フィールドは、異なるイベントソースからの元のイベントのフィールド表示を標準化するために使用されるラベルです。イベント精製中に、CA Enterprise Log Manager によって、元のイベント メッセージが一連の名前/値のペアに解析され、その後、元のイベントの名前が標準の CEG フィールドにマップされます。この精製によって、元のイベントからの CEG フィールドと値で構成された名前/値ペアが作成されます。つまり、同一のデータ オブジェクトやネットワーク要素に対して使用されている、元のイベント内の異なるラベルが、元のイベントを精製する際に、同じ CEG フィールド名に変換されるわけです。CEG フィールドは SNMP トラップに使用された MIB 内の OID にマップされます。

EEM ユーザ

EEM ユーザは、イベント ログ ストアの[自動アーカイブ]セクションで設定し、アーカイブ クエリの実行、アーカイブ データベースのカatalog再作成、LMArchive ユーティリティの実行、および検査用にアーカイブ データベースを復元する restore-ca-elm シェル スクリプトの実行が可能なユーザを指定します。このユーザには、事前定義済みの Administrator ロール、またはデータベース リソースへの編集アクションを許可するカスタム ポリシーに関連付けられたカスタム ロールが割り当てられている必要があります。

EiamAdmin ユーザ名

EiamAdmin は、CA Enterprise Log Manager サーバのインストール実施者に割り当てられるデフォルトのスーパーユーザ名前です。最初に CA Enterprise Log Manager ソフトウェアをインストールする際に、リモート CA EEM サーバがまだ存在していない場合は、インストーラが、このスーパーユーザ アカウント用のパスワードを作成します。存在する場合は、インストーラが既存のパスワードを入力する必要があります。ソフトウェア アプライアンスをインストールした後、インストーラは、ワークステーションからブラウザを開き、CA Enterprise Log Manager 用の URL を入力し、関連するパスワードを使用して EiamAdmin としてログインします。この最初のユーザが、ユーザ ストアを設定し、パスワード ポリシーを作成し、Administrator ロールを持つ最初のユーザ アカウントを作成します。必要に応じて、EiamAdmin ユーザは、CA EEM によって制御された操作を実行できます。

EPHI 関連のレポート

EPHI 関連のレポートは、HIPAA セキュリティに焦点を合わせたレポートです。EPHI は、Electronic Protected Health Information (電子保護健康情報)を表します。これらのレポートは、作成、管理、または送信される患者関連の個人医療情報がすべて電子的に保護されていることを証明するのに役立ちます。

event_action

event_action は、CEG によって使用されるイベント正規化の第 4 レベルのイベント専用のフィールドです。一般的なアクションについて記述します。イベントアクションのタイプには、プロセスの開始、プロセスの停止、アプリケーション エラーがあります。

event_category

event_category は、CEG によって使用されるイベント正規化の第 2 のレベルのイベント専用フィールドです。これによって、特定の ideal_model を備えたイベントをさらに分類できます。イベントカテゴリタイプには、運用セキュリティ、ID 管理、設定管理、リソース アクセス、およびシステム アクセスがあります。

event_class

event_class は、CEG によって使用されるイベント正規化の第 3 レベルのイベント専用のフィールドです。これによって、特定の event_category 内のイベントをさらに分類できます。

FIPS 140-2

FIPS 140-2 は、連邦情報処理標準(Federal Information Processing Standard)です。この連邦標準は、SBU(sensitive but unclassified: 取扱注意だが機密扱いなし)情報を保護するセキュリティシステムで使用される暗号モジュールのセキュリティ要件を規定しています。この標準は、広範囲のアプリケーションおよび環境に対応するために 4 つのセキュリティ品質レベルを定義しています。

FIPS 140-2 互換

FIPS 140-2 互換とは、オプションで FIPS 準拠の暗号ライブラリおよびアルゴリズムを使用して機密データを暗号化および復号化できる製品の呼称です。CA Enterprise Log Manager は、FIPS 準拠のログ収集製品です。CA Enterprise Log Manager では、FIPS モードまたは FIPS 非準拠モードを選択できます。

FIPS 140-2 準拠

FIPS 140-2 準拠とは、認定された暗号モジュール テスト (CMT) 機関によって認証された暗号化アルゴリズムのみをデフォルトで使用する製品の呼称です。CA Enterprise Log Manager は、認証された RSA BSAFE Crypto-C ME および Crypto-J ライブラリに基づく暗号化モジュールを FIPS モードで使用できますが、デフォルトでは使用しない場合があります。

FIPS 非準拠モード

FIPS 非準拠モードはデフォルトの設定です。この設定では、CA Enterprise Log Manager サーバおよびエージェントが FIPS 準拠でない技術を含む暗号化技術を組み合わせて使用できます。代わりに使用される設定は FIPS モードです。

FIPS モード

FIPS モードの設定では、CA Enterprise Log Manager サーバおよびエージェントは RSA の FIPS 準拠の暗号モジュールを使用して暗号化を行う必要があります。代わりに使用される設定は FIPS 非準拠モードです。

HTTP プロキシ サーバ

HTTP プロキシ サーバは、ファイアウォールと同様の働きをするプロキシ サーバで、インターネットトラフィックがプロキシ経由でない企業への出入りを阻止します。送信トラフィックは、ID およびパスワードを指定して、プロキシ サーバをバイパスできます。サブスクリプション管理でローカル HTTP プロキシ サーバを使用するかどうかを設定できます。

ID

CA Enterprise Log Manager の ID は、CAELM アプリケーション インスタンスおよびそのリソースへのアクセスが許可されるユーザまたはグループです。CA 製品用の ID は、グローバル ユーザ、アプリケーション ユーザ、グローバル グループ、アプリケーション グループ、動的グループのいずれかです。

ID アクセス制御リスト

ID アクセス制御リストを使用すると、選択した ID が選択した各リソースに実行できるさまざまなアクションを指定できます。たとえば、ID アクセス制御リストを使用して、ある ID にレポートの作成を許可し、別の ID にレポートのスケジュールおよび注釈付けを許可することができます。ID アクセス制御リストは、リソース中心ではなく ID 中心という点でアクセス制御リストと異なります。

ideal_model

ideal_model は、イベントを表現するテクノロジーを表します。これは、イベントの分類および正規化に使用されるフィールドの階層内で最初の **CEG** フィールドです。推奨されるモデルの例には、アンチウイルス、**DBMS**、ファイアウォール、オペレーティング システム、**Web** サーバがあります。**Check Point**、**Cisco PIX**、**Netscreen/Juniper** のファイアウォール製品は、フィールド「**ideal_model**」では「ファイアウォール」の値を使用して正規化されます。

iTech イベント プラグイン

iTech イベント プラグインは、選択したマッピング ファイルを使用して管理者が設定できる **CA** アダプタです。リモート **iRecorders**、**CA EEM**、**iTechnology** 自身、または **iTechnology** を介してイベントを送信する製品からイベントを受信します。

LMArchive ユーティリティ

LMArchive ユーティリティは、**CA Enterprise Log Manager** サーバ上のイベントログ ストアに対するアーカイブ済みデータベースのバックアップおよび復元を追跡するコマンドライン ユーティリティです。**LMArchive** を使用して、アーカイブが可能なウォーム データベース ファイルのリストを照会します。リスト表示されたデータベースをバックアップし、長期的な (コールド) ストレージに移動させた後、このデータベースがバックアップされた **CA Enterprise Log Manager** に関する記録を作成する際にも **LMArchive** を使用します。元の **CA Enterprise Log Manager** にコールド データベースを復元した後には、**LMArchive** を使用して **CA Enterprise Log Manager** に通知します。そこで、**CA Enterprise Log Manager** によってコールド データベース ファイルがクエリ可能な解凍済み状態に変更されます。

LMSEOSImport ユーティリティ

LMSEOSImport ユーティリティは、監査レポート、ビューア、または監査コレクタからデータを移行する過程で、**SEOSDATA** (既存イベント) を **CA Enterprise Log Manager** にインポートするために使用されるコマンドライン ユーティリティです。このユーティリティは、**Microsoft Windows** および **Sun Solaris Sparc** 上でのみサポートされています。

MIB (management information base、管理情報ベース)

CA Enterprise Log Manager 用 MIB (management information base)である CA-ELM.MIB は、CA Enterprise Log Manager から SNMPトラップという形でアラートを受信する製品でインポートされコンパイルされる必要があります。MIBでは、SNMPトラップ メッセージで使用される各数値オブジェクト識別子 (OID)の源が、そのデータ オブジェクトやネットワーク要素の説明と共に示されます。CA Enterprise Log Manager によって送信された SNMPトラップの MIB では、各データ オブジェクトの説明は、関連する CEG フィールド用になっています。MIBを使用すると、SNMPトラップで送信されたすべての名前/値ペアが、宛先で正しく解釈されるようになります。

NIST

アメリカ国立標準技術研究所 (NIST) は、CA Enterprise Log Manager のベースとして使用された特別文書 800-92「*Guide to Computer Security Log Management*」で推奨事項を提供している米国連邦政府の科学技術機関です。

ODBC および JDBC のアクセス

CA Enterprise Log Manager イベント ログ ストアへの ODBC および JDBC のアクセスでは、サード パーティ レポート ツールを使用したカスタム イベントのレポートや、相関エンジンを使用したイベントの相関、侵入やマルウェアの検知製品を使用したイベント評価など、各種サード パーティ製品でのイベント データの使用をサポートしています。Windows オペレーティング システムを備えたシステムでは、ODBC アクセスを使用します。UNIX や Linux オペレーティング システムを備えたシステムでは、JDBC アクセスを使用します。

ODBC サーバ

ODBC サーバは、ODBC や JDBC のクライアントと、CA Enterprise Log Manager サーバ間の通信に使用されるポートを設定し、SSL 暗号化を使用すべきかどうかを指定する設定済みサービスです。

OID (オブジェクト識別子)

OID (オブジェクト識別子) は、SNMPトラップ メッセージ内で値とペアになっているデータ オブジェクトの一意の数値識別子です。CA Enterprise Log Manager によって送信された SNMPトラップ内で使用されている各 OID は、MIB 内のテキスト形式の CEG フィールドにマップされます。CEG フィールドにマップされた OID の構文は、「1.3.6.1.4.1.791.9845.x.x.x、791」のようになっています。791 は CA の企業番号、9845 は CA Enterprise Log Manager の製品識別子です。

pozFolder

pozFolder は、AppObject の属性で、値は AppObject の親パスです。pozFolder 属性および値は、レポート、クエリ、設定などのリソースへのアクセスを制限するアクセス ポリシー用フィルタで使用されます。

RSS イベント

RSS イベントは、サードパーティ製品やユーザにアクション アラートを送信するために CA Enterprise Log Manager によって生成されるイベントです。このイベントは、各アクション アラート結果のサマリであり、結果ファイルへのリンクでもあります。指定した RSS フィード項目の期間は設定可能です。

SafeObject

SafeObject は、CA EEM 内の事前定義済みリソース クラスです。アプリケーションのスコープ下に保存された AppObjects が属するリソース クラスです。AppObjects へのアクセスを許可するポリシーおよびフィルタを定義するユーザは、このリソース クラスを参照します。

SAPI コレクタ

SAPI コレクタは、CA Audit クライアントからイベントを受信する CA アダプタです。CA Audit クライアントは、組み込みのフェイルオーバーを提供するコレクタ アクションを使用して通信します。管理者は、選択した暗号および DM ファイルなどを使用して、CA Audit SAPI コレクタを設定します。

SAPI ルータ

SAPI ルータは、メインフレームなどの、統合からイベントを受信し、CA Audit ルータに送信する CA アダプタです。

SAPI レコーダ

SAPI レコーダは、iTechnology 以前に CA Audit に情報を送信するために使用されていた技術です。SAPI は、Submit API (アプリケーションプログラミング インターフェース)を表しています。SAPI レコーダの例としては、CA ACF2、CA Top Secret、RACF、Oracle、Sybase、DB2 用の CA Audit レコーダがあります。

scp ユーティリティ

scp セキュア コピー (リモートファイル コピー プログラム) は、ネットワーク上の UNIX コンピュータ間でファイルを転送する UNIX ユーティリティです。このユーティリティは、オンライン サブスクリプション プロキシからオフライン サブスクリプション プロキシにサブスクリプション更新ファイルを転送する際に使用できるよう、CA Enterprise Log Manager のインストール時に利用可能になります。

SNMP

SNMP は、Simple Network Management Protocol の頭字語で、エージェントシステムから 1 つ以上の管理システムにアラートメッセージを SNMP トラップという形で送信するためのオープンスタンダードです。

SNMP トラップの宛先

アクションアラートをスケジュールする際に、1 つ以上の SNMP トラップの宛先は追加できます。各 SNMP トラップの宛先には、IP アドレスとポートが設定されています。宛先は、通常 CA Spectrum や CA NSM などの NOC または管理サーバです。SNMP トラップは、スケジュールしたアラートジョブのクエリによって結果が返されたときに、設定した宛先に送信されます。

SNMP トラップの内容

SNMP トラップは名前/値ペアで構成されます。各名前は OID (オブジェクト識別子)、各値はスケジュールしたアラートから返される値です。アクションアラートから返されるクエリ結果は、CEG フィールドと値で構成されています。SNMP トラップは、この名前/値ペアの名前に使用されている CEG フィールドを OID に置換して、生成されます。各 CEG フィールドの OID へのマッピングは、MIB に格納されています。SNMP トラップには、アラートを設定する際に選択したフィールドの名前/値ペアが含まれます。

varbind

varbind は SNMP 変数バインディングです。各 varbind は、OID、タイプ、および値から構成されています。varbind はカスタム MIB に追加します。

XMP ファイル分析

XMP ファイル分析は、メッセージ解析ユーティリティによって実行されるプロセスです。このプロセスでは、各事前一致文字列が含まれるすべてのイベントを検索し、一致したイベントを 1 つずつ解析して、同じ事前一致文字列を使用していると判明した最初のフィルタを使用しているイベントをトークンに変換します。

アーカイブ カタログ

「カタログ」を参照してください。

アーカイブ クエリ

アーカイブ クエリは、クエリを実行するために、復元して解凍する必要のあるコールド データベースを特定する際に使用されるカタログへのクエリです。通常のクエリがホット データベース、ウォーム データベース、および解凍済みデータベースをターゲットにするのに対して、アーカイブ クエリは、コールド データベースをターゲットにするという点で、通常のクエリと異なります。管理者は、[管理] タブ - [ログ収集] サブタブ - [カタログ クエリのアーカイブ] オプションから、アーカイブ クエリを発行できます。

アーカイブ ログ

ログ アーカイブは、ホット データベースが最大サイズに到達すると発生するプロセスで、このとき、行レベルで圧縮が実行され、状態がホットからウォームに変更されます。削除のしきい値に達する前に、管理者は手動でウォーム データベースをバックアップし、LMArchive ユーティリティを実行して、バックアップ名を記録する必要があります。その後、この情報はアーカイブ クエリによって表示できるようになります。

アーカイブ 済みデータベース

ある CA Enterprise Log Manager サーバ上で「アーカイブ 済みデータベース」に含まれるデータベースとは、クエリの実行が可能だが有効期限が切れる前に手動でバックアップする必要があるすべてのウォーム データベース、バックアップ済みとして記録されているすべてのコールド データベース、およびバックアップから復元済みとして記録されているすべてのデータベースです。

アカウント

アカウントは、CALM アプリケーション ユーザでもあるグローバル ユーザです。1 人の人が、1 つ以上のアカウントを持ち、それぞれに異なるユーザ定義ロールを設定することができます。

アクション アラート用の RSS フィード URL

アクション アラート用の RSS フィード URL は、[https://\[elmhostname\]:5250/spin/calm/getActionQueryRssFeeds.csp](https://[elmhostname]:5250/spin/calm/getActionQueryRssFeeds.csp) です。この URL から、有効期間およびデータ量の最大値の設定に従ってアクション アラートを表示できます。

アクション クエリ

アクション クエリは、アクション アラートをサポートするクエリです。アクション クエリは、繰り返しのスケジュールで実行され、関連付けられているアクション アラートによって規定された条件に対してテストします。

アクション アラート

アクション アラートは、スケジュール済みのクエリジョブです。ポリシー違反、使用状況、ログイン パターンなど、近い将来に注意が必要となるイベントアクションを検出するために使用できます。デフォルトでは、アラートクエリから結果が返されたときに、CA Enterprise Log Manager [アラート] ページに結果が表示され、RSS フィードにも追加されます。アラートをスケジュールする際に、電子メール、CA IT PAM イベント/アラート出力プロセス、SNMP トラップなどの宛先を追加指定できます。

アクセスフィルタ

アクセスフィルタは、管理者以外のユーザまたはグループが表示できるイベントデータを制御するために、管理者が設定できるフィルタです。たとえば、アクセスフィルタを設定して、指定した ID がレポートに表示できるデータを制限できます。アクセスフィルタは自動的に責任ポリシーに変換されます。

アクセスポリシー

アクセスポリシーは、アプリケーションリソースへの ID (ユーザまたはユーザグループ) のアクセス権を許可または拒否するルールです。CA Enterprise Log Manager は、ID、リソース、リソースクラスを照合し、フィルタを評価して、特定のユーザにポリシーを適用するかどうかを決定します。

アプリケーションユーザ

アプリケーションユーザは、アプリケーションレベルの詳細を割り当てられたグローバルユーザです。CA Enterprise Log Manager アプリケーションユーザの詳細には、ユーザグループおよびアクセスへのすべての制限が含まれています。ユーザストアがローカルリポジトリである場合、アプリケーションユーザの詳細には、ログオン認証情報およびパスワードポリシーも含まれています。

アプリケーションリソース

アプリケーションリソースは、CALM アクセスポリシーによって、特定の ID に対する、作成、スケジュール、編集といったアプリケーション固有のアクションの実行が許可または拒否される CA Enterprise Log Manager 固有のリソースです。たとえば、レポート、アラート、統合などがあります。「グローバルリソース」も参照してください。

アプリケーションインスタンス

アプリケーションインスタンスは、すべての許可ポリシー、ユーザ、グループ、コンテンツ、および設定が格納されている CA EEM リポジトリ内の共用領域です。通常、企業内のすべての CA Enterprise Log Manager サーバは、同じアプリケーションインスタンス(デフォルトでは CAELM)を使用します。複数のアプリケーションインスタンスを備えた CA Enterprise Log Manager サーバをインストールできますが、連携できるのは、同じアプリケーションインスタンスを共有するサーバのみです。同じ CA EEM サーバを使用するように設定され、複数のアプリケーションインスタンスを備えたサーバでは、ユーザストア、パスワードポリシー、およびグローバルグループのみが共有されます。複数の CA 製品には、複数のデフォルトのアプリケーションインスタンスがあります。

アプリケーショングループ

アプリケーショングループは、グローバル ユーザに割り当てることができる製品固有のグループです。CA Enterprise Log Manager で使用される事前定義済みアプリケーショングループ、すなわちロールとは、Administrator、Analyst、および Auditor です。これらのアプリケーショングループ、は CA Enterprise Log Manager ユーザのみが使用できます。同じ CA EEM サーバに登録されたほかの製品のユーザへの割り当てには利用できません。ユーザ定義アプリケーショングループは、そのユーザが CA Enterprise Log Manager にアクセスできるように、CALM アプリケーション アクセス デフォルト ポリシーに追加する必要があります。

アラート サーバ

アラート サーバは、アクション アラートおよびアクション アラート ジョブ用のストアです。

イベント

CA Enterprise Log Manager 中のイベントは、指定した各イベントソースによって生成されたログレコードです。

イベントログストレージ

イベントログストレージは、アーカイブ処理の結果です。この処理では、ユーザがウォーム データベースをバックアップし、LMArchive ユーティリティを実行して CA Enterprise Log Manager に通知し、バックアップ済みデータベースをイベントログストアから長期用ストレージに移動させます。

イベント/アラート出力プロセス

イベント/アラート出力プロセスは、CA Enterprise Log Manager で設定されたアラートデータに応答するサードパーティ製品を呼び出す CA IT PAM プロセスです。アラートジョブをスケジュールする際に、宛先として CA IT PAM プロセスを選択できます。CA IT PAM プロセスがアラートによって実行されると、CA Enterprise Log Manager によって CA IT PAM アラートデータが送信され、CA IT PAM によって、イベント/アラート出力プロセスの一環として、アラートデータが独自のプロセスパラメータと共にサードパーティ製品に転送されます。

イベントカテゴリ

イベントカテゴリは、CA Enterprise Log Manager によって使用されるタグで、イベントストアに挿入する前にイベントを機能によって分類するためのものです。

イベントソース

イベントソースは、コネクタによるイベント収集元となるホストです。イベントソースに複数のログストアが含まれ、各ログストアが個別のコネクタによってアクセスされる場合があります。新しいコネクタの展開には、通常、イベントソースを設定する作業が伴います。エージェントがイベントソースにアクセスし、ログストアの1つから元のイベントを読み取れるように設定する必要があります。オペレーティングシステム、複数のデータベース、およびさまざまなセキュリティアプリケーションのそれぞれの元のイベントが、イベントソース上に別々に格納されます。

イベント転送ルール

イベント転送ルールによって、選択したイベントを、イベントログストアへの保存後に、イベントの関連付けなどを行うサードパーティ製品に転送するよう指定します。

イベントの集約

イベント集約は、類似する複数のログエントリを、イベント発生数が格納された単一のエントリに統合するプロセスです。集約ルールによって、イベントの集約方法が定義されます。

イベントフィルタリング

イベントフィルタリングは、CEGフィルタに基づいてイベントを除外するプロセスです。

イベントログストア

イベントログストアは、受信イベントがデータベースに格納される **CA Enterprise Log Manager** サーバ上のコンポーネントです。イベントログストア内のデータベースは、手動でバックアップし、設定された削除時間に達する前に、リモートログストレージソリューションに移動する必要があります。アーカイブされたデータベースは、イベントログストアに復元できます。

イベント収集

イベント収集は、元のイベント文字列をイベントソースから読み取り、設定された **CA Enterprise Log Manager** に送信するプロセスです。イベント収集の後に、イベント精製が実行されます。

イベント精製

イベント精製は、収集された元のイベント文字列が、構成要素のイベントフィールドに解析され、CEGフィールドにマッピングされるプロセスです。クエリを実行して、結果として精製済みイベントデータを表示できます。イベント精製は、イベントの収集後、イベントの格納の前に実行されます。

イベント精製ライブラリ

イベント精製ライブラリは、事前定義済みおよびユーザ定義の統合、マッピングファイルおよび解析ファイル、抑制ルールおよび集約ルールのストアです。

インストーラ

インストーラは、ソフトウェア アプライアンスとエージェントをインストールする個人です。インストール処理中に、**caelmadmin** と **EiamAdmin** というユーザ名が作成され、**EiamAdmin** に指定されたパスワードが、**caelmadmin** に割り当てられます。これらの **caelmadmin** 認証情報は、オペレーティング システムに最初にアクセスする際に必要となります。**EiamAdmin** 認証情報は、**CA Enterprise Log Manager** ソフトウェアに最初にアクセスする際、およびエージェントをインストール際に必要となります。

ウォーム データベース状態

ウォーム データベース状態は、ホット データベースのサイズ(最大行数)を超えたとき、または新規イベントログ ストアへのコールド データベースの復元後にカタログ再作成が実行されたときに、イベント ログのホット データベースが移行する状態です。ウォーム データベースは、経過日数が[アーカイブの最大日数]に設定された値を超えるまで、イベント ログ ストア内で圧縮されて保持されます。ホット、ウォーム、および解凍済みの状態のデータベースに含まれるイベント ログにクエリを実行できます。

エージェント

エージェントは、コネクタによって設定される汎用サービスであり、それぞれが単一のイベントソースから元のイベントを収集して、処理のために **CA Enterprise Log Manager** に送信します。各 **CA Enterprise Log Manager** に、エージェントが 1 つ組み込まれています。また、リモート収集ポイント上にエージェントをインストールし、エージェントをインストールできないホスト上のイベントを収集できます。さらに、イベントソースが実行されているホスト上にエージェントをインストールすると、抑制ルールの適用や **CA Enterprise Log Manager** への転送の暗号化などのメリットが得られます。

エージェント エクスプローラ

エージェント エクスプローラは、エージェント設定用のストアです (エージェントは、収集ポイント上、またはイベントソースが存在するエンドポイント上にインストールできます)。

エージェント管理

エージェント管理は、連携されたすべての **CA Enterprise Log Manager** に関連付けられたすべてのエージェントを制御するソフトウェア プロセスです。これによって、通信相手のエージェントが認証されます。

エージェントグループ

エージェントグループは、選択したエージェントに適用できるタグです。これによって、複数のエージェントに同時にエージェント設定を適用し、グループに基づいたレポートを取得することができます。特定のエージェントは、一度に1つのグループにしか所属できません。エージェントグループは、地理的地域や重要度など、ユーザ定義の基準をベースにします。

カスタム MIB

カスタム MIB は、CA NSM などの SNMP トラップ宛先に送信されるアクションアラート用に作成する MIB です。アクションアラートで指定されたカスタムトラップ ID は、トラップとして送信される選択された CEG フィールドを定義する MIB の存在を前提としています。

カタログ

カタログは、アーカイブされたデータベースの状態を管理する各 CA Enterprise Log Manager 上に格納されたデータベースで、すべてのデータベースについての高機能なインデックスとしても機能します。状態情報(ウォーム、コールド、または解凍済み)には、これまでにこの CA Enterprise Log Manager 上に存在したすべてのデータベース、および解凍済みデータベースとしてこの CA Enterprise Log Manager に復元されたすべてのデータベースの状態が保持されます。インデックス機能は、この CA Enterprise Log Manager 上のイベントログストアにあるすべてのホットおよびウォーム データベースを対象とします。

カタログ再作成

カタログ再作成は、強制的なカタログの再構築です。カタログ再作成は、データが作成されたサーバとは異なるサーバ上のイベントログストアにデータを復元する場合にのみ必要になります。たとえば、CA Enterprise Log Manager の1つを、コールドデータの調査用復元ポイントとして機能するよう指定すると、指定した復元ポイントにデータベースを復元した後、強制的なデータベースのカタログ再作成が必要になります。必要な場合は、iGateway が再起動されたときに、カタログ再作成が自動的に実行されます。単一のデータベースファイルのカタログ再作成に、数時間かかる場合があります。

カレンダー

カレンダーは、アクセスポリシーが有効である時間を制限するための手段です。ポリシーによって、指定した時間の、指定したリソースに対する指定したアクションの実行が、指定した ID に許可されます。

監査レコード

監査レコードには、認証の試行、ファイルへのアクセス、およびセキュリティポリシーや、ユーザアカウント、権限への変更などの、セキュリティイベントが記録されます。管理者は、監査が必要なイベントのタイプ、およびログ記録の対象を指定します。

関数マッピング

関数マッピングは、製品統合用のデータマッピングファイルのオプション部分です。関数マッピングは、ソースイベントから必要な値を直接取得できない場合に **CEG** フィールドを挿入するために使用されます。すべての関数マッピングは、**CEG** フィールド名、事前定義済みフィールド値またはクラスフィールド値、および値を取得または計算する際に使用される関数から構成されます。

管理サーバ

管理サーバは、最初にインストールされる **CA Enterprise Log Manager** サーバに割り当てられるロールです。この **CA Enterprise Log Manager** サーバには、すべての **CA Enterprise Log Manager** で共有されるポリシーなどのコンテンツが格納されるリポジトリが含まれています。通常、このサーバは、デフォルトのサブスクリプションプロキシです。管理サーバはすべてのロールを実行できますが、大部分の実稼働環境では推奨されません。

キー値

キー値は、ユーザ定義値に割り当てられたユーザ定義リスト(キーグループ)です。クエリがキーグループを使用する場合、検索結果には、キーグループ内のキー値のいずれかに一致するものが含まれます。事前定義済みキーグループは複数あり、その中には事前定義済みキー値が含まれているものもあります。事前定義済みキー値は、事前定義済みクエリおよびレポートの中で使用されます。

クエリ

クエリは、アクティブな CA Enterprise Log Manager サーバ、および、指定した場合にはその連携サーバの、イベントログストアを検索する際に使用される条件のセットです。クエリは、クエリの WHERE 句内で指定されたホット、ウォーム、または解凍済みデータベースをターゲットにします。たとえば、WHERE 句によって、ある時間帯に `source_username="myname"` であるイベントにクエリが制限されていて、カタログ データベースに格納されている情報に基づくと、この条件に一致するレコードが 1000 個のデータベースのうち 10 にしか格納されていない場合、クエリはその 10 のデータベースに対してのみ実行されます。クエリは、データの行を最大 5000 まで返すことができます。事前定義済みロールを持つすべてのユーザが、クエリを実行できます。Analyst および Administrator だけが、アクションアラートを配布するためのクエリのスケジュール、含めるクエリの選択によるレポートの作成、またはクエリの実行ウィザードを使用したカスタムクエリの作成を実行できます。「アーカイブ クエリ」も参照してください。

クエリライブラリ

クエリライブラリは、事前定義済みおよびユーザ定義のクエリ、クエリタグ、およびプロンプトフィルタをすべて格納するライブラリです。

グローバルグループ

グローバルグループは、同じ CA Enterprise Log Manager 管理サーバに登録されたアプリケーション インスタンス間で共有されるグループです。すべてのユーザは、1 つ以上のグループに割り当てることができます。アクセス ポリシーを定義する際に、選択したリソースに選択したアクションを実行する権限を許可または拒否された ID としてグローバルグループを使用できます。

グローバル設定

グローバル設定は、同じ管理サーバを使用するすべての CA Enterprise Log Manager サーバに適用される一連の設定です。

グローバルフィルタ

グローバルフィルタは、すべてのレポートの表示内容を制限するために指定できる条件のセットです。たとえば、「過去 7 日間」というグローバル フィルタでは、過去 7 日間に生成されたイベントがレポートされます。

グローバルユーザ

グローバルユーザは、アプリケーション固有の詳細を除いたユーザアカウント情報です。グローバルユーザの詳細およびグローバルグループメンバシップは、デフォルトのユーザストアに統合されるすべての CA アプリケーションで共有されます。グローバルユーザの詳細は、組み込みリポジトリまたは外部ディレクトリに保存できます。

グローバルリソース

CA Enterprise Log Manager 製品のグローバルリソースは、ほかの CA アプリケーションと共有されるリソースです。グローバルリソースに関するスコープ ポリシーを作成できます。たとえば、ユーザ、ポリシー、カレンダーなどがあります。「アプリケーションリソース」も参照してください。

コールド データベース状態

管理者が LMArchive ユーティリティを実行して、データベースがバックアップされたことを CA Enterprise Log Manager に通知すると、ウォーム データベースに、コールド データベース状態が適用されます。管理者は、削除される前に、ウォーム データベースをバックアップし、このユーティリティを実行する必要があります。ウォームデータベースは、経過日数が[アーカイブの最大日数]を超えたときか、設定された[アーカイブ ディスク領域]しきい値に達したときの、どちらか早いほうが発生したときに、自動的に削除されます。アーカイブ データベースにクエリを実行し、ウォーム状態およびコールド状態にあるデータベースを特定することができます。

コネクタ

コネクタは、特定のエージェント上に設定された特定のイベントソース用の統合です。エージェントは、似たタイプまたは異なったタイプの複数のコネクタをメモリにロードできます。コネクタによって、イベントソースから元のイベントを収集したり、変換されたイベントをルールに基づいてイベント ログ ストアに転送して、ホット データベースに挿入したりすることが可能になります。あらかじめ用意されている統合を使用すると、オペレーティング システム、データベース、Web サーバ、ファイアウォール、多種多様なセキュリティアプリケーションなど、さまざまなタイプのイベントソースからの収集を最適化することができます。ゼロから、または統合をテンプレートとして使用して、独自に作成したイベントソース用のコネクタを定義できます。

コンテンツ更新

コンテンツ更新は、CA Enterprise Log Manager 管理サーバ内に格納されているサブスクリプション更新の非バイナリ部分です。コンテンツ更新には、XMP ファイル、DM ファイル、CA Enterprise Log Manager モジュール用の設定更新、公開鍵更新などのコンテンツが含まれています。

コンピュータ セキュリティログ管理

コンピュータ セキュリティログ管理は、NIST によって、「コンピュータ セキュリティログ データの生成、転送、格納、分析、および処理するプロセス」と定義されています。

サービス

CA Enterprise Log Manager サービスは、イベント ログ ストア、レポート サーバ、およびサブスクリプションです。管理者はこれらのサービスをグローバルレベルで設定します。デフォルトで、すべての設定がすべての **CA Enterprise Log Manager** に適用されます。サービスの大部分のグローバル設定は、ローカルレベルで、すなわち、指定されている **CA Enterprise Log Manager** について変更される可能性があります。

サブスクリプション クライアント

サブスクリプション クライアントは、サブスクリプション プロキシ サーバと呼ばれる別の **CA Enterprise Log Manager** サーバからコンテンツ更新を取得する **CA Enterprise Log Manager** サーバです。サブスクリプション クライアントでは、設定されたサブスクリプション プロキシ サーバを定期的にポーリングし、利用可能な場合には新しい更新を取得します。更新を取得したら、ダウンロードされたコンテンツがクライアントによってインストールされます。

サブスクリプション プロキシ(オフライン)

オフライン サブスクリプション プロキシは、オンライン サブスクリプション プロキシから手動のディレクトリ コピー (scp を使用) によってサブスクリプション更新を取得する **CA Enterprise Log Manager** サーバです。オフライン サブスクリプション プロキシは、要求しているクライアントにバイナリ更新をダウンロードし、コンテンツ更新の最新バージョンをまだ受信していない管理サーバに更新を送信するように設定できます。オフライン サブスクリプション プロキシは、インターネットにアクセスする必要はありません。

サブスクリプション プロキシ(オンライン)

オンライン サブスクリプション プロキシは、インターネット アクセス権を持つ **CA Enterprise Log Manager** で、**CA** サブスクリプション サーバからサブスクリプション更新を反復スケジュールで取得します。特定のオンライン サブスクリプション プロキシに、1 つ以上のクライアント用のプロキシ リストを保存することができます。クライアントは、リストに挙げられたプロキシにラウンド ロビン方式で接続し、バイナリ更新を要求します。別のプロキシによってまだ送信されていない場合に、管理サーバに新しいコンテンツ更新および設定更新を送信するよう、特定のオンライン プロキシを設定することができます。オンライン プロキシのサブスクリプション更新ディレクトリを選択して、オフライン サブスクリプション プロキシに更新をコピーするためのソースとして使用できます。

サブスクリプション プロキシ(クライアント用)

クライアント用のサブスクリプション プロキシは、クライアントが **CA Enterprise Log Manager** ソフトウェアおよびオペレーティング システムの更新を取得する際に、ラウンド ロビン方式で接続するサブスクリプション プロキシリストを構成します。あるプロキシがビジーな場合は、リスト内の次のプロキシに接続します。すべてが使用不可で、クライアントがオンラインの場合には、デフォルトのサブスクリプション プロキシが使用されます。

サブスクリプション プロキシ(コンテンツ更新用)

コンテンツ更新用のサブスクリプション プロキシは、**CA サブスクリプション サーバ**からダウンロードされるコンテンツ更新がある **CA Enterprise Log Manager** 管理サーバを更新するために選択されたサブスクリプション プロキシです。冗長性を持たせるために複数のプロキシを設定することをお勧めします。

サブスクリプション プロキシ(デフォルト)

デフォルトのサブスクリプション プロキシは通常、最初にインストールされた **CA Enterprise Log Manager** サーバで、プライマリ **CA Enterprise Log Manager** である場合もあります。デフォルトのサブスクリプション プロキシは、オンライン サブスクリプション プロキシでもあるため、インターネットにアクセスできる必要があります。ほかにオンライン サブスクリプション プロキシが定義されていない場合、このサーバは、**CA サブスクリプション サーバ**からサブスクリプション更新を取得し、すべてのクライアントにバイナリ更新をダウンロードし、**CA EEM** にコンテンツ更新を送信します。ほかのプロキシが定義されている場合でも、このサーバはサブスクリプション更新を取得しますが、更新を取得するためにクライアントによって接続されるのは、サブスクリプション プロキシリストが設定されていない場合、または設定されているリストをすべて使用した場合のみです。

サブスクリプション モジュール

サブスクリプション モジュールは、**CA サブスクリプション サーバ**からのサブスクリプション更新が、すべての **CA Enterprise Log Manager** サーバおよびすべてのエージェントに自動的にダウンロードおよび配布されるようにするサービスです。グローバル設定は、ローカル **CA Enterprise Log Manager** サーバに適用されます。ローカル設定には、サーバがオフライン プロキシ、オンライン プロキシ、サブスクリプション クライアントのどれであるか、などが含まれます。

サブスクリプション更新

サブスクリプション更新は、**CA サブスクリプション サーバ**によって使用可能にされた、バイナリファイルおよび非バイナリファイルを指します。バイナリファイルとは、通常、**CA Enterprise Log Manager** にインストールされる製品モジュール更新です。非バイナリファイルは、コンテンツ更新を指し、管理サーバに保存されます。

サブスクリプション用の RSS フィード URL

サブスクリプション用の RSS フィード URL は、サブスクリプション更新を取得するプロセスでオンライン サブスクリプション プロキシ サーバによって使用される、あらかじめ設定されたリンクです。この URL は、CA サブスクリプション サーバのものであります。

自己監視イベント

自己監視イベントは、CA Enterprise Log Manager によってログに記録されるイベントです。このようなイベントは、ログインしたユーザによって実行された操作や、サービスおよびリソースなどの各種モジュールによって実行された機能によって、自動的に生成されます。SIM 操作自己監視イベントの詳細レポートは、レポートサーバを選択し、[自己監視イベント]タブを開いて、表示することができます。

スコープ ポリシー

スコープ ポリシーはアクセス ポリシーの一種で、AppObjects、ユーザ、グループ、フォルダ、ポリシーなど、管理サーバに保存されたリソースへのアクセスを許可または拒否します。スコープ ポリシーでは、指定されたリソースにアクセスできる ID を定義します。

ソフトウェア アプライアンス

ソフトウェア アプライアンスは、ソフトウェアに加えて基盤となるオペレーティングシステムおよびすべての依存パッケージで構成される、必要な機能をすべて備えたソフトウェア パッケージです。このパッケージは、ソフトウェア アプライアンス インストール メディアから起動することで、エンド ユーザのハードウェアにインストールされます。

タグ

タグは、同じビジネス関連グループに属するクエリやレポートを識別するために使用する言葉またはキー フレーズです。タグを使用すると、ビジネス関連グループに基づいた検索を実行できます。なお、Tag は、ユーザにタグを作成する権限を付与するポリシー内で使用されるリソース名です。

直接ログ収集

直接ログ収集は、イベントソースと CA Enterprise Log Manager ソフトウェアの間に中間エージェントがないログ収集方法です。

データ アクセス

データアクセスは、CALM リソース クラスに関するデフォルト データアクセス ポリシーによってすべての CA Enterprise Log Manager に付与された許可の一種です。すべてのユーザは、データアクセスフィルタによって制限された場所以外にあるすべてのデータにアクセスできます。

データ マッピング (DM)

データ マッピングは、キー値ペアを CEG にマッピングするプロセスです。データ マッピングは DM ファイルによって実行されます。

データ マッピング (DM) ファイル

データ マッピング (DM) ファイルは XML ファイルです。CA 共通イベント文法 (CEG) を使用して、イベントをソース形式から、イベント ログ ストア内でのレポートや分析用として格納できる CEG 準拠形式に変換します。イベント データを保存するには、ログ名ごとに 1 つの DM ファイルが必要になります。ユーザは、DM ファイルのコピーを変更して、指定したコネクタに適用できます。

データベースの状態

データベースの状態には、新規イベントの圧縮されていないデータベースを指す「ホット」、圧縮されたイベントのデータベースを指す「ウォーム」、バックアップされたデータベースを指す「コールド」、および、バックアップ元のイベント ログ ストアに復元されたデータベースを指す「解凍済み」があります。ホット データベース、ウォーム データベース、および解凍済みデータベースにクエリを実行できます。アーカイブ クエリには、コールド データベースに関する情報が表示されます。

デフォルト エージェント

デフォルト エージェントは、CA Enterprise Log Manager サーバと共にインストールされる組み込みエージェントです。syslog イベントに加えて、CA Access Control r12 SP1、Microsoft Active Directory 証明書サービス、Oracle9i データベースなど、syslog 以外の各種イベントソースからのイベントの直接収集用に設定することができます。

デフロスティング

デフロスティングは、データベースの状態をコールドから解凍済みに変更するプロセスです。既知のコールド データベースが復元されたことが LMArchive ユーティリティによって通知されると、CA Enterprise Log Manager によってこのプロセスが実行されます (コールド データベースを元の CA Enterprise Log Manager に復元しない場合は、LMArchive ユーティリティは使用しません。デフロスティングの必要はありません。カタログ再作成によって、復元されたデータベースがウォーム データベースとして追加されます)。

統合

統合は、クエリおよびレポートに表示できるように、未分類のイベントを精製済みイベントに加工する手段です。統合は、特定のエージェントおよびコネクタが多種多様なイベントソースの 1 つからイベントを収集して、CA Enterprise Log Manager に送信できるようにする、要素のセットで実装されます。この要素のセットには、ログ センサ、および特定の製品から読み込むよう設計された XMP ファイルと DM のファイルが含まれています。事前定義済み統合の例には、syslog イベントおよび WMI イベントの処理用の統合などがあります。未分類のイベントの処理を可能にするカスタム統合を作成できます。

動的値プロセス

動的値プロセスは、レポートやアラートで使用されている選択済みキーの値を登録または更新する際に呼び出される CA IT PAM プロセスです。動的値プロセスへのパスは、IT PAM 設定の一部として、[管理]タブの[レポート サーバ サービスリスト]に入力します。これと同じ UI ページの[キー値]に関連付けられた[値]セクションの[動的値リストのインポート]をクリックします。動的値プロセスの呼び出しは、キーに値を追加する際に使用できる 3 つの方法のうちの 1 つです。

ネイティブ イベント

ネイティブ イベントは、元のイベントの発生要因となる状態またはアクションです。ネイティブ イベントは、受信され、必要に応じて解析/マッピングされてから、元のイベントまたは精製済みイベントとして転送されます。失敗した認証はネイティブ イベントです。

非対話型の ssh 認証

非対話型の認証を使用すると、認証用のパスフレーズを入力することなく、あるサーバ上のファイルを別のサーバに移動できます。ソースサーバから宛先サーバへの非対話型の認証の設定は、自動アーカイブの設定前または `restore-ca-elm.sh` スクリプトの使用前に行います。

フィルタ

フィルタは、イベントログ ストア クエリを制限する手段です。

フォルダ

フォルダは、CA Enterprise Log Manager オブジェクトタイプを格納するために CA Enterprise Log Manager 管理サーバが使用するディレクトリ パスの場所です。指定したオブジェクトタイプにアクセスする権限を付与または拒否する際に、スコープ ポリシー内のフォルダを参照します。

プロフィール

プロフィールは、任意の、設定可能なタグおよびデータフィルタのセットです。フィルタは、製品固有、テクノロジー固有、または選択したカテゴリ限定のいずれかになっています。たとえば、製品用のタグ フィルタを使用すると、リスト表示されるタグが、選択した製品タグに制限されます。製品用のデータフィルタを使用すると、作成するレポート、スケジュールするアラート、および表示するクエリ結果に、指定した製品のデータのみが表示されます。必要なプロフィールを作成したら、ログイン時に常に有効になるようにプロフィールを設定できます。複数のプロフィールを作成した場合は、セッション中のアクティビティに複数のプロフィールを 1 つずつ適用できます。事前定義済みフィルタは、サブスクリプション更新と共に提供されます。

プロンプト

プロンプトとは、ユーザが入力した値、および選択した CEG フィールドに基づいて結果を表示する特殊なクエリです。ユーザが入力した値が、選択された 1 つまたは複数の CEG フィールド内に存在するイベントについてのみ、行が返されます。

保存済み設定

保存済み設定は、新しい統合を作成する際にテンプレートとして使用できる統合のデータ アクセス属性の値と共に保存された設定です。

ホット データベース状態

ホット データベース状態は、新規イベントが挿入されるイベント ログ ストア内にあるデータベースの状態です。ホット データベースは、収集サーバ上の設定可能なサイズに到達すると、圧縮され、カタログが作成され、レポートサーバ上のウォーム ストレージに移動されます。さらに、ホット データベース内には、すべてのサーバによって新しい自己監視イベントが保存されます。

マッピング分析

マッピング分析は、データ マッピング (DM) ファイルをテストし、変更を加えるマッピング ファイル ウィザードの手順の 1 つです。サンプル イベントが DM ファイルに対してテストされ、結果が CEG を使用して検証されます。

メッシュ統合

CA Enterprise Log Manager サーバのメッシュ統合は、サーバ間にピア関係を構築するトポロジです。最も単純な形式では、サーバ 2 はサーバ 1 の子であり、サーバ 1 はサーバ 2 の子であります。メッシュ型のサーバのペアには、双方向の関係があります。メッシュ統合では、多くのサーバがすべて相互のピアになるように定義できます。連携クエリでは、選択したサーバおよびそのすべてのピアから結果が返されます。

メッセージ解析

メッセージ解析は、元のイベントログの分析にルールを適用して、タイムスタンプ、IP アドレス、ユーザ名などの関連情報を取得するプロセスです。解析するルールでは、文字一致を使用して特定のイベントテキストを検索し、選択された値にリンクさせます。

メッセージ解析トークン(ELM)

メッセージ解析トークンは、CA Enterprise Log Manager メッセージ解析で使われる正規表現構文を構築するための再使用可能なテンプレートです。トークンは、名前、タイプ、および対応する正規表現文字列で構成されます。

メッセージ解析ファイル(XMP)

メッセージ解析ファイル(XMP)は、解析ルールを適用する特定のイベントソースタイプに関連付けられた XML ファイルです。解析ルールによって、収集された元のイベント内の関連データから名前/値ペアが抽出され、さらなる処理のためにデータマッピングファイルに渡されます。このファイルタイプは、すべての統合で使用され、統合に基づいてコネクタで使用されます。CA アダプタの場合、XMP ファイルは CA Enterprise Log Manager サーバにも適用できます。

メッセージ解析ライブラリ

メッセージ解析ライブラリは、リスナ キューからイベントを受け取り、正規表現を使用して文字列を名前/値ペアにトークン化するライブラリです。

元のイベント

元のイベントは、監視エージェントによって Log Manager コレクタに送信されたネイティブ イベントがトリガとなる情報です。元のイベントは、通常、syslog 文字列または名前/値ペアとしてフォーマットされます。イベントを CA Enterprise Log Manager 内で元の形式で確認できます。

ユーザグループ

ユーザグループは、アプリケーショングループ、グローバルグループ、動的グループのいずれかです。事前定義済み CA Enterprise Log Manager アプリケーショングループは、Administrator、Analyst、および Auditor です。CA Enterprise Log Manager ユーザは、CA Enterprise Log Manager とは別のメンバシップを通して、グローバルグループに属している場合があります。動的グループは、ユーザ定義のグループで、動的グループポリシーによって作成されます。

ユーザストア

ユーザストアは、グローバル ユーザ情報およびパスワード ポリシー用のリポジトリです。CA Enterprise Log Manager ユーザストアは、デフォルトではローカルリポジトリですが、CA SiteMinder を参照したり、Microsoft Active Directory、Sun One、Novell eDirectory などのサポートされている LDAP ディレクトリを参照したりするよう設定できます。ユーザストアの設定内容にかかわらず、管理サーバ上のローカルリポジトリには、ユーザロールや関連付けられたアクセスポリシーなど、ユーザに関するアプリケーション固有の情報が格納されています。

ユーザロール

ユーザロールには、事前定義済みのアプリケーション ユーザグループか、ユーザ定義のアプリケーショングループを指定できます。事前定義済みアプリケーショングループ (Administrator、Analyst、および Auditor) では詳細な担当職務を十分カバーできない場合は、カスタムユーザロールを作成する必要があります。カスタムユーザロールを作成するには、カスタムアクセスポリシーを設定し、事前定義済みポリシーを変更して、この新しいロールを追加する必要があります。

抑制

抑制は、CEG フィルタに基づいてイベントを除外するプロセスです。抑制は SUP ファイルによって実行されます。

抑制ルール

抑制ルールは、精製済みの特定のイベントをレポートに表示されないようにするために設定するルールです。セキュリティ上問題のないルーチンイベントを抑制する永続的な抑制ルールを作成したり、多数の新規ユーザの作成などの計画されたイベントのログ記録を抑制する一時的なルールを作成したりすることができます。

リモートイベント

リモートイベントは、2 つの異なるホスト名 (ソースおよび宛先) を含んだイベントです。リモートイベントは、共通イベント文法 (CEG) 内で使用される 4 つのイベントタイプのタイプ 2 です。

リモートストレージサーバ

リモートストレージサーバは、1 つ以上のレポートサーバから自動アーカイブ済みデータベースを取得するサーバに割り当てられたロールです。リモートストレージサーバでは、必要な年数の間コールドデータベースが保存されます。ストレージに使用されるリモートホストには、通常、CA Enterprise Log Manager やほかの製品をインストールしません。自動アーカイブの場合は、非対話型認証を設定します。

レポート

レポートは、フィルタを備えた事前定義済みクエリやカスタムクエリの実行によって生成されるイベントログ データを、グラフィック形式や表形式で表示したものです。データの取得先には、選択したサーバや、必要な場合はその連携サーバの、イベントログ ストア内にあるホット データベース、ウォーム データベース、および解凍済みデータベースを指定できます。

レポートライブラリ

レポートライブラリは、事前定義済みおよびユーザ定義のレポート、レポートタグ、作成済みレポート、およびスケジュール済みレポートジョブをすべて格納したライブラリです。

レポートサーバ

レポートサーバは **CA Enterprise Log Manager** サーバによって実行されるロールです。レポートサーバは、1 つ以上の収集サーバから、自動アーカイブ済みウォーム データベースを取得します。レポートサーバによって、クエリ、レポート、スケジュール済みアラート、およびスケジュール済みレポートが処理されます。

レポートサーバ

レポートサーバは、アラートを電子メールで送信する際に使用する電子メールサーバ、PDF 形式で保存されるレポートの外観、レポートサーバに保存するレポートや RSS フィードに送信するアラート用ポリシーの保持などの、設定情報を格納するサービスです。

ローカル イベント

ローカル イベントは、単一のエンティティを含んだイベントで、ここでは、イベントのソースおよび宛先が同じホスト マシンです。ローカル イベントは、共通イベント文法 (CEG) 内で使用される 4 つのイベントタイプのタイプ 1 です。

ローカル フィルタ

ローカル フィルタは、現在のレポートに表示されているデータを制限するために、レポートの表示中に設定できる条件のセットです。

ログ

ログは、イベントまたはイベントコレクションの監査レコード、すなわち記録されたメッセージです。ログは、監査ログ、トランザクション ログ、侵入ログ、接続ログ、システム パフォーマンスレコード、ユーザ アクティビティログ、またはアラートのいずれかです。

ログ エントリ

ログ エントリは、システム上またはネットワーク内で発生した特定のイベントについての情報が格納されているログ内のエントリです。

ログ センサ

ログ センサは、データベース、**syslog**、ファイル、**SNMP** などの特定のログ タイプから読み込むよう設計された統合コンポーネントです。ログ センサは再利用されます。通常、ユーザはカスタム ログ センサを作成しません。

ログ レコード

ログ レコードは、個別の監査レコードです。

ログ 解析

ログ 解析は、ログ 管理の後の段階で解析済み値を使用できるように、ログ からデータを抽出するプロセスです。

ログ 分析

ログ 分析とは、対象のイベントを識別するためのログ エントリの検証です。適切なタイミングで分析しないと、ログ の価値はきわめて低くなります。

委任ポリシー

委任ポリシーは、ユーザが別のユーザ、アプリケーション グループ、グローバル グループ、または動的グループに自分の権限を委任できるようにするアクセス ポリシーです。削除または無効化されたユーザによって作成された委任ポリシーを明示的に削除する必要があります。

解析

解析は、メッセージ解析 (MP) と呼ばれ、元のデバイス データを取得し、それをキー/値ペアに変換するプロセスです。解析は **XMP** ファイルによって実行されます。解析は、イベント ソースから収集された元のイベントを表示可能な精製済みイベントに変換する統合プロセスの手順の 1 つで、データ マッピングの前に実行されます。

解析ファイル ウィザード

解析ファイル ウィザードは、CA Enterprise Log Manager 管理サーバに格納された **eXtensible Message Parsing (XMP)** ファイルを作成、編集、および分析するために管理者が使用する CA Enterprise Log Manager の機能です。受信イベントデータの解析のカスタマイズには、事前一致文字列およびフィルタの編集が含まれます。新規作成されたファイルおよび編集されたファイルは、[ログ収集エクスプローラ]、[イベント精製ライブラリ]、[解析ファイル]、[ユーザ フォルダ]に表示されます。

解凍済みデータベース状態

解凍済みデータベース状態は、アーカイブ ディレクトリに復元されたデータベースに適用される状態で、管理者が **LMArchive** ユーティリティを実行して **CA Enterprise Log Manager** に復元を通知した後に適用されます。解凍済みデータベースは、[ポリシーのエクスポート]に設定された時間数の間保持されます。ホット、ウォーム、および解凍済みの状態のデータベースに含まれるイベントログにクエリを実行できます。

階層統合

CA Enterprise Log Manager サーバの階層統合は、サーバ間に階層関係を構築するトポロジです。最も単純な形式では、サーバ 2 はサーバ 1 の子ですが、サーバ 1 はサーバ 2 の子ではありません。すなわち、関係は一方方向のみです。階層統合は、複数のレベルの親子関係を持つことができ、1 つの親サーバが多数の子サーバを持つことができます。連携クエリでは、選択したサーバおよびその子から結果が返されます。

観察されたイベント

観察されたイベントは、ソース、宛先、およびエージェントを含んだイベントで、ここでは、イベントが、イベント収集エージェントによって観察および記録されます。

記録されたイベント

記録されたイベントは、データベースに挿入された後の元のイベント情報または精製済みイベント情報を指します。抑制または集約されていない場合、元のイベントは、常に精製済みイベントです。この情報は保存され、検索の対象になります。

共通イベント文法 (CEG)

共通イベント文法 (CEG) は、イベントがイベントログ ストアに格納される前に、**CA Enterprise Log Manager** により解析ファイルおよびマッピング ファイルを使用して変換される標準形式を提供するスキーマです。CEG は、さまざまなプラットフォームおよび製品からのセキュリティ イベントを定義するための一般的な正規化フィールドを使用します。解析またはマッピングできないイベントは、元のイベントとして格納されます。

視覚化コンポーネント

視覚化コンポーネントは、表、グラフ (線グラフ、棒グラフ、縦棒グラフ、円グラフ)、イベントビューアなど、レポート データを表示する際に使用できるオプションです。

資格管理

資格管理は、ユーザが認証され、CA Enterprise Log Manager インターフェースにログオンした後、実行を許可される内容を制御する手段です。これは、ユーザに割り当てられたロールに関連付けられたアクセス ポリシーを使用して行います。ロール、すなわちアプリケーション ユーザ グループと、アクセス ポリシーは、事前定義済みかユーザ定義のどちらかです。資格管理は、CA Enterprise Log Manager 内部のユーザ ストアによって処理されます。

自動アーカイブ

自動アーカイブは、あるサーバから別のサーバへのアーカイブ データベースの移動を自動化する設定可能なプロセスです。自動アーカイブの最初の段階で、収集サーバが、指定された間隔で新しくアーカイブされたデータベースをレポートサーバに送信します。第 2 段階で、レポートサーバが、古くなったデータベースを長期保存用のリモート ストレージ サーバに送信します。これによって、手動によるバックアップおよび移動の手順が必要なくなります。自動アーカイブでは、ソース サーバから宛先サーバへのパスワードを使用しない認証を設定する必要があります。

収集サーバ

収集サーバは、CA Enterprise Log Manager サーバによって実行されるロールです。収集サーバは、受信イベント ログを精製し、ホット データベースにそれらを挿入し、ホット データベースを圧縮し、関連するレポートサーバに自動アーカイブ、すなわちコピーします。ホット データベースは、設定されたサイズに達すると、収集サーバによって圧縮され、設定されたスケジュールで自動アーカイブされます。

収集ポイント

収集ポイントは、エージェントがインストールされるサーバです。このサーバには、そのエージェントのコネクタに関連付けられたイベントソースが含まれているすべてのサーバに対する、ネットワーク隣接性があります。

集約ルール

集約ルールは、同じタイプの複数のネイティブ イベントを結合して、単一の精製済みイベントとするルールです。たとえば、集約ルールは、同じソースおよび宛先 IP アドレス/ポートを持つ重複イベントを最大 1000 まで、単一の集約イベントで置き換えるように設定できます。このようなルールは、イベント分析を簡略化し、ログトラフィックを軽減します。

精製済みイベント

精製済みイベントは、元のイベントまたは集約されたイベントから派生した、解析またはマッピングされたイベント情報です。CA Enterprise Log Manager では、格納された情報を検索できるように、マッピングおよび解析を実行します。

責任ポリシー

責任ポリシーは、アクセスフィルタを作成したときに自動的に作成されるポリシーです。責任ポリシーを直接、作成、編集、または削除しようとししないでください。代わりに、アクセスフィルタを作成、編集、または削除します。

統合の要素

統合の要素には、センサ、設定ツール、データアクセス ファイル、1 つ以上の XMP メッセージ解析 (XMP) ファイル、および 1 つ以上のデータ マッピング ファイルがあります。

動的ユーザ グループ

動的ユーザ グループは、1 つ以上の共通属性を共有するグローバル ユーザから構成されます。動的ユーザ グループは、特殊な動的ユーザ グループ ポリシーによって作成されます。このポリシーでは、リソース名が動的ユーザ グループ名で、メンバシップのベースがユーザ属性およびグループ属性に設定されたフィルタセットになります。

復元ポイント サーバ

復元ポイント サーバは CA Enterprise Log Manager サーバによって実行されるロールです。「コールド」イベントを調査するには、ユーティリティを使用して、リモートストレージサーバから復元ポイントサーバにデータベースを移動し、そのデータベースをカタログに追加し、クエリを実行します。コールド データベースを専用の復元ポイントに移動するのは、調査のために元のレポートサーバに移動する必要がなくなります。

連携サーバ

連携サーバは、ログ データ収集を配布するためにネットワーク内で相互接続された CA Enterprise Log Manager サーバですが、収集されたデータをレポート用に集約することはありません。連携サーバは、階層型トポロジまたはメッシュ型トポロジで接続することができます。連携されたデータのレポートには、ターゲットサーバからのデータに加えて、そのサーバの子またはピアからのデータがすべて含まれます。

索引

C

- CA Enterprise Log Manager
 - アクセシビリティ モード - 669
 - アンインストール後に削除 - 149
- CA IT PAM との統合
 - しくみ - 374
 - 動的値の生成のための設定 - 335
- CA NSM との統合
 - システム要件 - 440
- CA Spectrum との統合
 - SNMPトラップ用 - 156
 - 参照 - 429
- CA アダプタ
 - ステータスの表示 - 175
 - 定義済み - 171
 - 編集 - 172, 173

L

- LMArchive ユーティリティ - 219

M

- MIB (CA-ELM.MIB)
 - CA Spectrum へのインポート - 433
 - ダウンロード - 432
 - 内容 - 411
 - 場所 - 426
- MIB ツリー
 - CA-ELM MIB - 411
 - カスタム MIB - 425

S

- SNMPトラップ
 - CA NSM での表示 - 448
 - CA Spectrum での表示 - 438
 - CA Spectrum への送信 - 434
 - MIB ツリー - 411
 - アラート宛先としての設定 - 457

- 使用のコンテキスト - 408
- 説明 - 408
- 統合の設定 - 156
- 例 - 434

syslog

- タイムゾーン - 595
- デフォルトの設定 - 593

あ

- アーカイブ カタログ
 - 再構築(カタログ再作成) - 218
- アーカイブ済みデータベース
 - バックアップの記録 - 208
 - バックアップの作成 - 207
 - 復元の記録 - 213
 - リスト、バックアップされていない - 206
- アクション アラート
 - IT PAM プロセスのクエリ単位での実行 - 405
 - IT PAM プロセスの行単位での実行 - 400
 - アラートジョブの宛先の定義 - 462
 - 削除 - 479
 - 詳細フィルタの作成 - 572
 - タグおよびクエリの使用 - 353
 - 定義済み - 352
 - 電子メール通知 - 458
 - 編集 - 477
 - 保持の設定 - 473
 - 有効化 - 478
 - 例 - 463, 467
- アクセシビリティ - 669
- アクセス フィルタ
 - 削除 - 115
 - 作成 - 108
 - 作成の例 - 128
- アクセス ポリシー
 - Administrator の事前定義済み - 62
 - Analyst の事前定義済み - 59
 - Auditor の事前定義済み - 57

-
- CALM アプリケーション アクセス ポリシー - 93
 - ID の追加 - 95
 - 影響の評価 - 139
 - エクスポート - 114
 - 計画 - 88, 135
 - コピーからの作成 - 103
 - コピーからの作成の例 - 138
 - 削除 - 115
 - すべてのユーザの事前定義済み - 53
 - ゼロからの作成の例 - 124
 - 定義済み - 52
 - テスト - 105
 - 登録済み製品用 - 64
 - バックアップ - 65
 - 編集 - 132, 137
 - ユーザ定義の例 - 124
 - アクセス制限シナリオ
 - PCI-Analyst ユーザ グループ - 134
 - Windows 管理者ユーザ - 120
 - イベント
 - 自己監視 - 502, 503
 - 集約 - 513
 - 取得するクエリのカスタマイズ、重大な - 361
 - 取得するクエリの実行、重大な - 359
 - 抑制 - 508
 - イベントリスナ
 - iTechnology - 178
 - SAPI - 176
 - WMI ルータ - 635
 - グローバル設定の編集 - 172
 - 定義済み - 171
 - ローカル設定の編集 - 173
 - イベント/アラート出力プロセス
 - CA Service Desk の例 - 382
 - アラート宛先として指定 - 372
 - クエリの実行 - 398
 - コンプライアンスの保証 - 387
 - 作成 - 387
 - 選択したクエリ結果での実行 - 394
 - データフローの例 - 377
 - 活用する際のワークフロー - 372
 - イベントビューア
 - 自己監視イベントの表示 - 174
 - ステータスの表示 - 175
 - イベントログ データベースの状態 - 186
 - イベント精製ライブラリ
 - コンポーネント バージョン - 505
 - インポート
 - CA IT PAM プロセスのサンプル - 379
 - クエリの詳細 - 316
 - 統合 - 598
 - 抑制ルールおよび集約ルール - 527
 - ライブ レポートの詳細 - 331
 - エージェント
 - グループの作成 - 647
 - 計画 - 629, 632
 - 更新 - 657
 - 更新の適用 - 657
 - 認証キーの更新 - 638
 - マネージャの割り当て - 650
 - エージェント エクスプローラ
 - 使い方 - 636
 - エージェントのインストール
 - 計画 - 629
 - エージェント認証キー
 - 更新 - 638
 - エクスポート
 - アクセス ポリシー - 114
 - クエリの詳細 - 315
 - 統合 - 598
 - 抑制ルールおよび集約ルール - 528
 - レポートの詳細 - 330
- ## か
- カスタム MIB
 - 作成時のガイドライン - 420
 - 使用方法 - 426
 - 説明 - 418
 - ベスト プラクティス - 412
 - 例 - 423
 - カレンダー
 - 作成 - 110
-

- ポリシーへの追加 - 111
- 例 - 112
- 管理タスク
 - エージェント管理 - 637
 - 集約ポリシー - 513
 - 製品統合 - 534
 - 統合 - 579
 - 抑制ポリシー - 508
- キー設定済みリスト
 - アラートの作成方法 - 474
- クエリ
 - アクション アラートのカスタマイズ - 356
 - 削除 - 313
 - 自動表示の無効化 - 314
 - 詳細のインポート - 316
 - 詳細のエクスポート - 315
 - 詳細フィルタ - 487
 - ドリルダウンレポートの追加 - 312
 - 表示 - 270
 - 編集 - 313
 - 編集モード - 314
 - 結果の条件 - 489, 492
- グローバル グループ
 - 作成 - 40
- グローバル設定
 - サービス - 152
- コネクタ
 - 統合更新の適用 - 657
 - 表示 - 602
 - プロンプト - 279
 - 編集 - 604
 - リストの表示 - 658

さ

- サービス
 - ローカル設定の編集 - 153
- サブスクリプション管理
 - 公開鍵 - 236
 - ディスク領域の要件 - 235
- 自己監視イベント
 - 定義済み - 502

た

- タグ
 - レポート組織での使用 - 270
- データ マッピング
 - concat 関数 - 561
 - 作成 - 553
 - 定義済み - 534
 - ファイル作成プロセス - 553
 - ファイルの分析 - 566
 - ブロック マッピング - 564
- 統合
 - インポート - 598
 - エクスポート - 598
 - 定義済み - 579
 - ファイル ログ - 586
- 動的ユーザ グループ ポリシー - 106

は

- バージョン
 - 定義済み - 505
 - 抑制および集約ルール - 525
- フィルタ
 - グローバルの削除 - 261
 - グローバルの編集 - 261
 - 識別、重大なイベント - 357
 - 詳細 - 487
 - 詳細の作成 - 572
 - スケジュール済みレポートへの追加 - 482
- プロファイル
 - 作成 - 251
 - 設定 - 257
 - 説明 - 250
- プロンプト
 - IP アドレス - 285
 - コネクタ - 279
 - 定義済み - 278
 - ポート - 290
 - ホスト - 282
 - ユーザ - 292
 - ログ名 - 288
- ポート

プロンプト - 290

ま

メッセージの解析

作成 - 534

サンプル イベントのロード - 538

事前一致フィルタ - 540

定義済み - 534

ファイル作成プロセス - 534

ファイル詳細の定義 - 536

ファイルの分析 - 552

や

ユーザ アカウント、参照

管理 - 44

ユーザ アカウント

アクティブ化および非アクティブ化 - 45

アプリケーション ユーザ グループの追加 -
43

アプリケーション ユーザ グループの追加の
例 - 139

アンロック - 26

既定の設定を使用した設定 - 39

削除 - 50

作成 - 41

作成の例 - 122

自己管理 - 25

編集 - 46

ユーザおよびアクセス管理

アクセスフィルタの作成 - 108

ユーザ グループ

グローバル - 40

動的 - 106

ユーザ パスワード

変更 - 27

リセット - 49

ユーザ ロール

Administrator - 31

Analyst - 30

Auditor - 28

アプリケーションへのアクセス権の付与 - 93

アプリケーションへのアクセス権の付与の例
- 137

計画 - 87

作成 - 92

作成の例 - 136

ポリシーへの追加 - 95

ポリシーへの追加の例 - 137

レポート作成タスクで - 317

割り当て - 43

割り当ての例 - 139

抑制ルール

影響 - 507

作成 - 508

適用 - 520

ネーミング - 509

抑制ルールおよび集約ルール

定義済み - 506

ルールのインポート - 527

ルールのエクスポート - 528

ルールのコピー - 524

ルールの削除 - 526

ルールの適用 - 520

ルールの編集 - 525

ら

リスナ サービス - 171

例

CA Spectrum への SNMP トラップの送信 -
434

IT PAM プロセス、アラートを使用してクエリ
単位で実行 - 405

IT PAM プロセス、アラートを使用して行単位
で実行 - 400

IT PAM プロセス、手動で実行 - 394

PCI タグに基づいたレポート - 274

PCI 分析担当者用のポリシー - 134

PDF として電子メールで送信するレポートの
スケジュール - 499

Windows 管理者用のポリシー - 120

イベントフローが停止した場合の管理者へ
の電子メールの送信 - 470

- エージェントインストールの計画 - 629
- カレンダー - 112
- 既存クエリからのレポート - 320
- 共通のタグを持つレポートのスケジュール - 495
- 自己監視イベントのアラート - 467
- ディスク領域低下のアラート - 463
- ビジネスクリティカルソースのキー設定済み値を使用したアラート - 474
- マッピングおよび解析ルール アクセス用のポリシー - 141
- 抑制および集約ルール アクセス用のポリシー - 143
- 抑制ルール - 529
- レポート保持 - 329
- 連携および連携されたレポート - 323
- レポート
 - 削除 - 328
 - 作成 - 317, 320
 - 作成済みの注釈 - 483
 - 作成済みの表示 - 481
 - 自動表示の無効化 - 273
 - スケジュール設定 - 484, 495
 - タグ - 270
 - ドリルダウン - 312
 - 表示 - 272
 - 編集 - 328
 - 編集モード - 273
 - 編集モードの設定 - 273
 - 例 - 274
 - レイアウトの作成 - 319
 - レポートの詳細のインポート - 331
 - レポートの詳細のエクスポート - 330
- レポートジョブ
 - 削除 - 502
 - 詳細フィルタ - 487
 - スケジュール設定 - 484
 - フィルタリング - 482
 - 編集 - 500
- レポート管理
 - 作成済みレポートの表示 - 481
 - 新規レポートの作成 - 317

- レポートジョブのスケジュール - 484
- レポートのスケジュール
 - 宛先 - 495
 - 削除 - 502
 - 処理 - 484
 - 反復 - 493
 - 編集 - 500
 - 連携されたクエリ - 495
- 連携
 - 例 - 323
 - レポートジョブへの適用 - 484
- ローカル サーバ
 - 設定 - 153
- ログ センサ
 - file - 586
- ログ収集
 - エージェント ベース - 635
 - エージェントレス - 635
 - 計画 - 632
 - 直接 - 633
- ログ ストレージ
 - バックアップの作成 - 205
 - バックアップの復元 - 209, 215

漢字

- 共通イベント文法 (CEG)
 - CEG フィールド用フィルタリング - 487
 - マッピングおよび解析 - 534
- 結果の条件
 - グループの条件 - 492
 - 設定 - 489
 - 定義済み - 489
- 集約ルール
 - しきい値の設定 - 514
 - 適用 - 520
 - 表示の設定 - 518
 - ルールの作成 - 513
- 証明書、カスタム
 - 実装 - 661
 - 信頼されたルート - 662
 - 展開 - 666

信頼済みルート証明書

iAuthority への追加 - 662

iControl への追加 - 664

動的値

IT PAM 統合の設定 - 335

IT PAM プロセスによる生成 - 334

インポートの有効化 - 333

説明 - 333