

CA Virtual Assurance for Infrastructure Managers

管理ガイド

リリース 12.6



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 © 2011 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 Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- CA eHealth®
- CA Embedded Entitlements Manager (CA EEM)
- CA IT Asset Manager
- CA IT Client Manager
- CA NSM (CA Network and Systems Management)
- CA Patch Manager
- CA Server Automation
- CA Service Desk Manager (CA SDM)
- CA Spectrum®
- CA SystemEDGE
- CA Virtual Assurance for Infrastructure Managers
- CA Software Delivery

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。

目次

第 1 章: はじめに	13
対象読者	13
関連ドキュメント	13
規則	14
 第 2 章: 概要	 17
アーキテクチャ	17
データベース	20
管理 DB	20
パフォーマンス DB	21
ユーザ インターフェース	21
ユーザ インターフェースへのアクセス	22
 第 3 章: ユーザの管理	 23
ユーザ アクセス制御	23
Active Directory	24
ネイティブ セキュリティ	25
パスワード管理	29
CA Embedded Entitlements Manager 管理者パスワード (EiamAdmin) の変更	29
データベース管理者 (sa) パスワードの変更	30
ネイティブ セキュリティのシステム ユーザ パスワードの変更	31
Active Directory セキュリティのシステム ユーザ パスワードの変更	33
外部ディレクトリ ユーザのためのタスク	34
ユーザ グループの作成	34
グループへのユーザの割り当て	35
ユーザ グループからのユーザまたはユーザ グループの削除	36
ユーザ グループに対するサービスへのアクセス権の割り当て	37
ユーザ グループ権限の設定	37
ユーザ グループの削除	38
ユーザまたはユーザ グループの検索	38
vCenter Server でのユーザ スコープ認証	39

第 4 章: リソースの設定 43

ディスカバリ.....	43
環境管理の設定要件.....	43
環境の検出.....	44
複数の vCenter AIM の管理.....	51
名前を変更した vCenter Server の管理.....	53
Solaris ゾーン管理の要件.....	54
LPAR 管理の要件.....	54
sysedge.cf ファイルの編集による SNMPv1 トラップの設定.....	55
イベント転送.....	56
SNMP 用の Windows の設定.....	57
イベント転送のための CA Virtual Assurance の設定.....	58
SNMP V3 エンジン ID.....	59

第 5 章: リソースの管理 61

マネージャ コンポーネント.....	61
Application Insight Module (AIM).....	62
モニタの設定.....	63
リソースの検出.....	64
システムの検出.....	64
ネットワークの検出.....	65
ネットワークの削除.....	67
ネットワーク ディスカバリのキャンセル.....	67
リソースの管理.....	68
サービスの作成.....	68
サービスの編集.....	70
管理対象の仮想環境.....	72
VMware vCenter Server.....	74
Solaris ゾーン.....	90
Microsoft Hyper-V Server.....	92
IBM PowerVM (LPAR).....	94
Microsoft Cluster Service.....	100
Cisco UCS.....	104
Cisco UCS の概要.....	106
Cisco UCS マネージャ サーバの追加.....	107
UCS AIM サーバの登録.....	108

UCS サーバの削除	109
SNMP データ ポーラーの設定	110
サービス ポーラーの設定	111
UCS トラップ管理	111
サービス プロファイル	112
複数のマルチインスタンス AIM の使用	114
システム管理	114
SystemEDGE 機能	116
サービスレスポンス モニタリング	128
リモート モニタリング	132
エージェントの設定	133
エージェントの視覚化	134
セキュリティおよび保守	138
第 6 章: 管理ポリシー	141
ルールとアクション	141
CA SDM の設定	143
CA SDM チケット ステータス設定の構成	144
ルールの設計	144
自動化ポリシーの作成	145
ルールの作成	146
事前定義済みアクション タイプの使用	149
カスタムアクションの作成	153
アクションシーケンスの定義	155
スケジュールの定義	156
ポリシーのユース ケース	158
ユース ケース: サーバをサービスに追加する	158
ユース ケース: 新規ルールをサービスに追加する	159
ユース ケース: アクションを定義する	159
データ収集の設定	160
メトリック収集に関する重要な点	161
データ センター用のデータ収集の設定	164
サーバ用のデータ収集の設定	165
仮想リソース用のデータ収集の設定	167
パフォーマンスしきい値の設定	170
メトリックフィルタの設定	171

ポリシーの UCS アクション タイプ	174
ブレード電源アクションの作成	175
サービス プロファイル	176
ポリシー設定	178
SystemEDGE ポリシーを作成する方法	180
SRM ポリシーを作成する方法	192
マシンへのポリシーの適用	196
ポリシー適用の進捗状況の確認	197
適用されるポリシーの設定と表示	198
エージェント ポリシーのダッシュボード ビュー	200
例: ユーザ固有のメトリック (MIB 拡張) をモニタする方法	201
例: 特定の Windows パフォーマンスレジストリのメトリックをモニタする方法	203

第 7 章: プロビジョニング リソース 205

イメージング サービス	205
VMware vCenter プロビジョニング	206
VMware vCenter および vSphere ユーザ権限	206
仮想マシン (vCenter Server) の追加	211
仮想マシン (Hyper-V Server) の追加	214
Solaris ゾーンの追加	215
IBM AIX コンピュータの論理パーティションの追加	217
追加プロビジョニング情報	219
リモート展開	220
リモート展開アーキテクチャ	221
展開コンポーネント	222
複数の配布サーバの使用	223
配布サーバが接続するドメイン サーバの変更	223
スケーラビリティ	224
監査証跡	224
展開の制限	225
展開認証情報の制限	226
非特権ユーザ アカウントを使用した UNIX/Linux へのリモート展開	227
展開のサイジング キー ファクタ	228
カスタム ポートを使用した SystemEDGE エージェントの展開/インストール	229
展開パッケージライブラリ	230
展開パッケージ設定ファイル	233

展開パッケージ	234
デフォルト パッケージ ラッパー	236
書き込みコミュニティを含まないエージェント設定	238
新規パッケージ ラッパーの作成	238
パッケージ ラッパーの変更	239
展開ジョブ	247
展開ジョブのステータスの追跡	248
展開履歴の表示	249
展開ダッシュボード ビュー	250
インフラストラクチャ展開プロセス	251
CA Virtual Assurance インフラストラクチャを自動展開するための前提条件	253
IPv6 アドレスを使用したインフラストラクチャ展開に関する注意事項	255
IDManager が使用する転送パッケージのプロトコル	256
インフラストラクチャ展開プライマ ソフトウェアの手動インストール	256
Windows での展開プライマ インストール	257
Linux または UNIX での展開プライマ インストール	257
展開管理証明書のプライマ インストールへの提供	258
Windows 上の展開管理証明書	258
Linux または UNIX 上の展開管理証明書	258
Linux の Compatibility Library	259
ファイアウォール ソフトウェアを実行している Windows Vista™、Windows 2008、および Windows XP コンピュータへの展開	261
 第 8 章: トラップの管理	 263
SNMP Trap Receiver	263
SNMP トラップ レシーバ設定ファイル	264
SystemEDGE トラップの転送	269
 第 9 章: レポート	 271
レポートの可用性	271
レポートの実行	271
 第 10 章: リモート モニタリング	 273
概要	273
リモート モニタリングの利点	273

機能と利点.....	274
エージェントレスのモニタ対象システム.....	274
重要業績評価指標メトリック	275
視覚化.....	275
設定.....	275
アクセス制御	276
回復力.....	276
スケーラビリティ.....	276
統合.....	276
オートメーション.....	277
アーキテクチャ.....	277
ユース ケース シナリオ	279
設定の前提条件.....	281
リモート モニタ システムの設定.....	282
リモート モニタリング メトリックの収集エンジンとレポートのサポート	285
リモート モニタリングを使用したシステムの管理.....	285

第 11 章: Exchange Server および Active Directory 用 AIM 287

概要	287
アーキテクチャ.....	288
機能	290
Exchange Server および Active Directory 用 AIM のメリット	291
パフォーマンス	291
ESAD AIM のインストール	291
Exchange Server と Active Directory をモニタするための設定の適用	293
コマンド モードの NodeCfgUtil による ESAD AIM の設定.....	294
ダイアログ モードの NodeCfgUtil による ESAD AIM の設定.....	296
ESAD AIM のアンインストール	297

第 12 章: シナリオおよびベスト プラクティス 299

vCenter Server 管理コンポーネントを設定する方法	300
確認要件.....	301
vCenter Server 管理コンポーネント間のインタラクションの確認.....	302
新しい vCenter Server 接続のマネージャへの追加	304
vCenter Server の AIM インスタンスの追加	309

リソース ツリーでの vCenter Server フォルダの表示の確認	316
ポリシー アクションを使ってパフォーマンスの問題を特定する方法	317
CPU メトリックのアクションの作成	319
CPU メトリックによって割り当てを増加させるルールの作成.....	320
CPU メトリックによって割り当てを減少させるルールの作成.....	320
スケーラビリティのベスト プラクティス.....	321
リモート展開およびポリシー設定の概要.....	321
ハードウェアの仕様	323
データベースに関する考慮事項.....	323
ネットワークに関する考慮事項.....	324
スケーラビリティに関する推奨事項.....	324
ポリシーおよび階層型テンプレートをサーバに適用する方法	337
階層型テンプレート概念.....	338
ポリシーの作成	339
サーバワークロード用のテンプレートの作成	352
ポリシーとテンプレートのサーバへの適用と設定の確認	369
(オプション) サーバのベース ポリシーおよびテンプレートの管理	371
(オプション) ポリシーまたはテンプレートの更新	372
(オプション) サーバへのポリシー/テンプレート更新の適用と更新の確認	373

付録 A: FIPS 140-2 の暗号化 375

FIPS の概要	375

付録 B: トラブルシューティング 377

Solaris ゾーン環境でのポーリング間隔設定の調整.....	378
属性にゼロの値が表示される	378
ブラウザにイベントの連続するスペースが表示されない	378
CA NSM が Windows でトラップの受信に失敗する.....	379
Cisco UCS フォルダが UI 内に表示されない	379
DB トランザクション ログ サイズが予期せずに増加する	380
廃止された Solaris ゾーン AIM 属性で常に N/A またはゼロが表示される.....	380
dpmvc virtualswitch コマンドでの空のタスク ID.....	381
ローカル モニタとリモート モニタに同じ値が表示されない.....	381
Solaris Lists SPARC および x86 システムへのリモートでの展開	382
PMM が AIM のポーリングを停止する.....	383

vCenter Server を削除すると、別の管理対象 vCenter Server のオブジェクトが非表示になる	384
vCenter Server のパスワードを変更するとデータ収集に失敗する	384
モニタされたシステムがダウンしている場合は Solaris ゾーン AIM がリセットされる.....	385
Microsoft SQL サーバに接続できない.....	385
SystemEDGE のアップグレード	385
プロビジョニング画面およびポリシー画面でユーザ インターフェースが応答しません	386
vCenter Server AIM 属性にゼロが表示される	386
vCenter Server の接続に失敗した	387
vCenter AIM インスタンスのステータスアイコンに「無効」が表示される.....	390
vCenter AIM インスタンスのステータスアイコンに「ディスクバリが進行中」が表示される	391
vCenter AIM インスタンスのステータスアイコンに「エラー」が表示される.....	391
vCenter AIM インスタンスのステータスアイコンに「複数インスタンス」が表示される	393
vCenter AIM インスタンスのステータスアイコンに「警告」が表示される.....	394
VM 使用率の値が電源オフ後にすぐに更新されない	394
アップグレード後の空白の[クエリ結果]タブ	395

用語集	397

索引	411

第 1 章: はじめに

このセクションには、以下のトピックが含まれています。

[対象読者](#) (P. 13)

[関連ドキュメント](#) (P. 13)

[規則](#) (P. 14)

対象読者

このガイドは、CA Virtual Assurance をインストールおよび設定して、仮想環境を管理するために使用する管理者を対象としています。読者が、お使いの環境で使用されるオペレーティング システム、仮想化技術、および SNMP に精通していることを前提とします。

関連ドキュメント

CA Virtual Assurance のマニュアルは、次のマニュアルで構成されています。

管理ガイド

ユーザの環境の仮想リソースを管理するために、CA Virtual Assurance を管理および使用する方法を調査します。

インストール ガイド

簡単なアーキテクチャ情報、さまざまなインストール方法、インストール後の設定情報、および導入時の手順が含まれます。

オンライン ヘルプ

CA Virtual Assurance ユーザ インターフェースを使用するためのウィンドウの詳細、および手順の説明を提供します。

リファレンス ガイド

AutoShell、CLI コマンド、MIB 属性、およびパフォーマンス メトリックに関する詳細情報を提供します。

リリース ノート

オペレーティング システムのサポート、システム要件、発行済みの修正プログラム、各国語のサポート、既知の問題、およびドキュメント ロードマップに関する情報を提供します。

サービス レスpons モニタリング ユーザ ガイド

SRM のインストールおよび設定の詳細について説明します。

SystemEDGE ユーザ ガイド

SystemEDGE のインストールおよび設定の詳細について説明します。

SystemEDGE リリース ノート

オペレーティング システムのサポート、システム要件、および機能に関する情報を提供します。

規則

このガイドでは、以下の規則を使用します。

大文字と小文字の区別

このガイドで言及されるクラス、コマンド、ディレクティブ、環境パラメータ、関数、プロパティの名前はすべて大文字と小文字を区別します。また、記載されているとおりに正確に入力する必要があります。システム コマンドと環境変数名は、オペレーティング システムの要件に応じて、大文字と小文字が区別される場合があります。

相互参照

ほかのガイド、またはこのガイドのほかのセクション内の情報へ参照は、以下の形式で記述されます。

ガイド名

別のガイドの名前を示します。

「章名」

このガイドまたは別のガイドの章の名前を示します。

同義語

属性、オブジェクト、オブジェクト識別子 (OID) などの用語は、このドキュメントでは「変数」と同義です。

SystemEDGE エージェント、CA SystemEDGE などの用語は、このドキュメントでは SystemEDGE と同義です。

構文

構文とユーザ入力では、以下の形式を使用します。

斜体

実際の値を指定する必要がある変数名またはプレースホルダを示します。

{a|b}

オペランド **a** または **b** を選択する必要があることを示します。

[] または [[]]

オプションのオペランドを示します。

構文例

以下の例は、上記の規則を使用しています。

```
modify -t ZONE [-m zoneserver] -p psetname {-min mincpu|-max maxcpu} pset -session ssh
```

オペランド **-min** および **-max** は必須ですが、プロセッサ セット内の CPU の最小数または最大数のどちらを定義するかに応じて、いずれか **1** つのみを使用します。オペランド **-m** は、指定しなくてもこのコマンドは機能します。コマンドのほかの部分は記載されているとおりに入力する必要があります。

デフォルト ディレクトリ

パス ステートメント内で使用する `sysedge_home` は、SystemEDGE がインストールされているディレクトリを示します。**デフォルト: C:\Program Files\CA\SystemEDGE.**

インストール パス

パスステートメント内で使用する *Install_Path* は、CA Virtual Assurance または CA Virtual Assurance コンポーネントがインストールされているディレクトリを示します。

デフォルト

- Windows x86: C:\Program Files\CA
- Windows x64: C:\CA、C:\Program Files (x86)\CA、または C:\Program Files\CA
- UNIX、Linux: /opt/CA

第 2 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。

[アーキテクチャ](#) (P. 17)

[データベース](#) (P. 20)

[ユーザ インターフェース](#) (P. 21)

アーキテクチャ

CA Virtual Assurance は、複雑なデータセンターの負荷要求に動的に対応するための物理リソースと仮想リソースを自動的にモニタリングする、ポリシーベースの製品です。サービス指向アーキテクチャを使用する CA Virtual Assurance は、データセンターを継続的に分析することで、必要なタスクを実行するためのサーバの最適なプロビジョニングを確実に行います。Web ベースの CA Virtual Assurance ユーザ インターフェースを使用すると、データセンターを管理し、データセンター内の個々の管理対象コンピュータに関する詳細情報を取得できます。

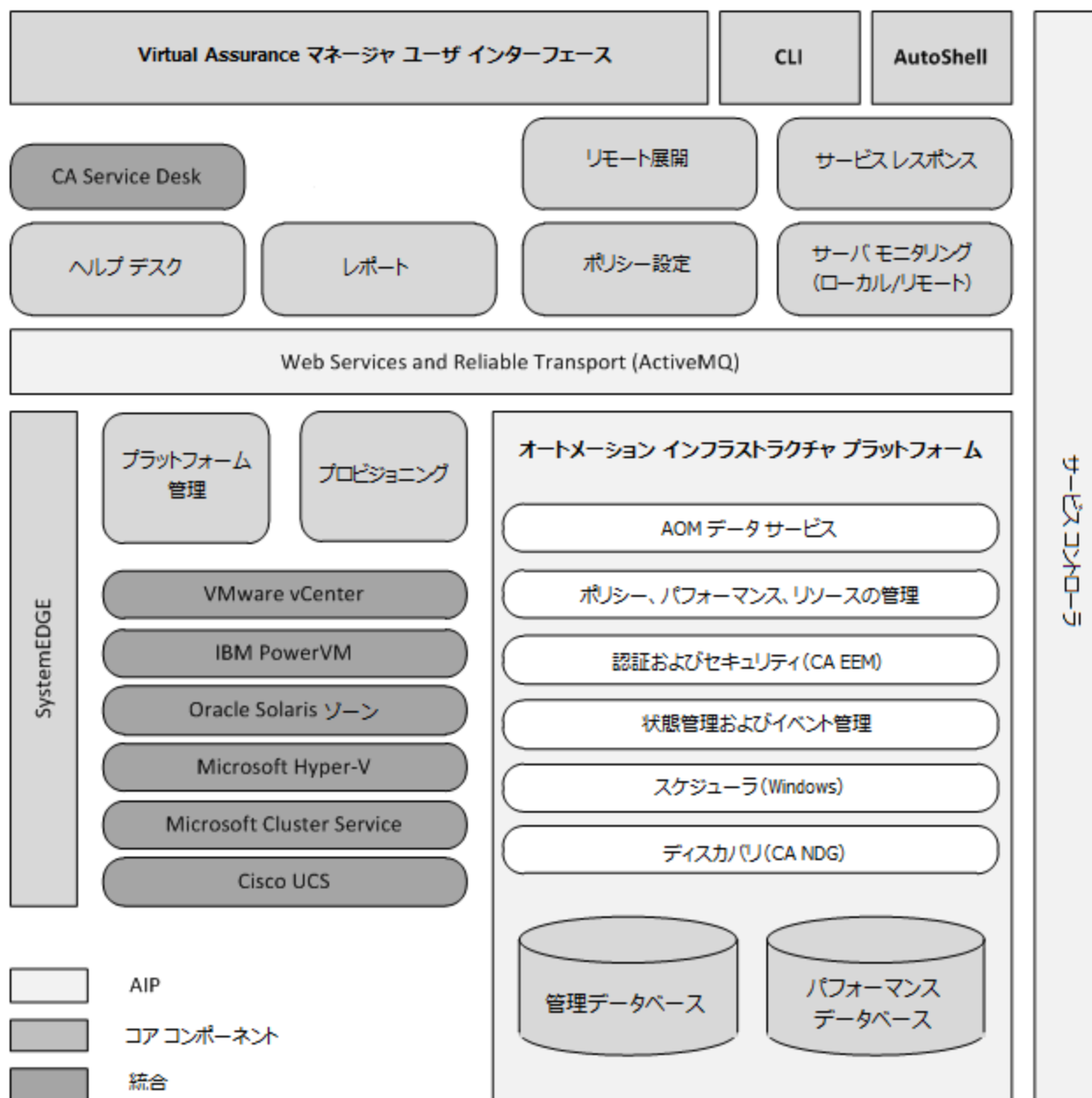
CA Virtual Assurance は、以下の外部テクノロジーと統合されています。

- 仮想マシン (VM) 管理のための VMware vCenter Server
- 仮想マシン (VM) 管理のための Microsoft System Center。オプションで、プロビジョニングのための Microsoft System Center Virtual Machine Manager (SCVMM) と統合されます
- AIX 仮想化管理のための IBM Logical Partitioning (LPAR)
- Solaris ゾーン仮想化管理
- Cisco Unified Computing System
- Microsoft Cluster Service

CA Virtual Assurance は以下の既存テクノロジーを活用します。

- 要求のエスカレーションと解決のための CA SDM 統合
- セキュリティを高める CA Embedded Entitlements Manager
- 軽量なスタンドアロン ディスカバリ機能のための Common Discovery

以下の図は製品のアーキテクチャを表しています。



各コンポーネントは起動時、サービスコントローラに登録されます。サービスコントローラは、すべてのコンポーネントの場所とステータスを識別するための中心的なコンポーネントです。登録が完了したコンポーネントは、**Web** サービス記述言語 (**WSDL**) による場所を提供し、他のコンポーネントがサブスクライブしてデータセンターの変更に関するリアルタイム通知を受信するためのイベントを発行します。

プロビジョニング コンポーネントは、**vCenter Server**、**Hyper-V**、および **Solaris** ゾーンに対してプロビジョニング機能を提供します。また、**SystemEDGE** と、**CA Virtual Assurance** によって提供される **AIM** を、リモート サーバにリモート展開することもできます。

リソース マネージャ コンポーネントは、ユーザ定義サービスの作成や更新など、製品内の全リソースの更新を担当します。

開始コンポーネントは、ジョブのスケジューリングのために **Microsoft** スケジューラとの統合を実現します。たとえば、長期間にわたって実行する保守タスクおよびアクションは、ジョブとしてスケジュールできます。

CA Embedded Entitlements Manager はセキュリティおよび役割ベースの管理全般に使用されます。

CA Virtual Assurance イベント マネージャは、**CA Virtual Assurance** コンポーネントによって生成されたすべてのイベントをキャプチャし、**SNMP** 転送を行います。**SNMP** 転送は、**SNMP** トラップを受信できる任意の **CA** 製品またはサードパーティ製品にイベントを転送するのに使用されます。

ポリシー コンポーネントは、収集されたデータを分析します。

パフォーマンス モニタ コンポーネントは、**SystemEDGE** と連携してシステム パフォーマンス データを収集します。**SystemEDGE** は基本的なシステム メトリックの収集元のサーバにインストールする必要があります。ただし、サーバに追加ソフトウェアをインストールせず (ゼロ フットプリント)、リモート モニタリング **AIM** を使用して **Windows** サーバをリモートでモニタする場合を除きます。すべてのパフォーマンス メトリックはパフォーマンス データベースに格納されます。

管理 DB に管理対象サーバが入力されると、これらのサーバがパフォーマンス メトリックを収集できるかどうかを判断するため、パフォーマンス モニタは情報の収集を開始します。

ポリシー コンポーネントは、収集されたデータを分析して、どのユーザ定義ビジネスルールで違反があったかを判断し、ターゲット サーバまたはサービスに対してアクションを実行します。特定の問題を解決するルールおよびアクションは事前に定義します。ポリシー コンポーネントは、指定されたパラメータを使用して、インテリジェントな決定を行います。サーバまたはサービスが特定されたら、状況を解決するためのさまざまなアクションを実行できます。たとえば、カスタムスクリプトを実行したり、新しいシステムをプロビジョニングしたりできます。

最後に、グラフィカル ユーザ インターフェースから直接生成されるカスタマイズ可能なグラフやチャート、または **CA Virtual Assurance** によって生成されるレポートを通して、データ センターのパフォーマンスを直接モニタできます。**CA Virtual Assurance** では、現在のコンポーネント ステータスの表示、コンポーネントの設定、設定の検証、またはユーザ アクセスリストの作成を行うこともできます。

データベース

製品は、管理データベースとパフォーマンス データベースの両方を使用します。

管理 DB

管理 DB は、管理データの説明用モデルに基づく、すべての管理対象オブジェクトの共通データリポジトリです。管理 DB には、サーバ、サービス、ルール、アクション、仮想プラットフォーム オブジェクト、イベント、アラート、およびこれらのオブジェクトの関係に関する情報が格納されます。

CA Virtual Assurance は、管理 DB を使用して、以下の情報を格納します。

- サーバ情報
- サービス関係
- サービスしきい値
- ルールおよびアクション
- イベント
- 他のコンポーネントの認証情報

注: 管理データベースの設定の詳細については、「*リファレンス ガイド*」の「*コマンドライン ユーティリティ*」の章を参照してください。

パフォーマンス DB

パフォーマンス DB は、データ センター内のサーバから収集されたメトリックをすべて格納するリポジトリです。

CA Virtual Assurance は、パフォーマンス DB を使用して、以下の情報を格納します。

- 収集されるメトリックの種類と収集元サーバ
- これらのメトリックの値(期間内に集計された)
- サーバレベルの記録間隔
- サーバレベルのしきい値(全体的なサーバ使用率)
- データ センター レベルの記録間隔
- データ センター レベルのしきい値

このデータベースに保存されたデータは、さまざまな機能に使用されます。たとえば、この DB のデータを使用して、履歴レポートが作成されます。CA Virtual Assurance はまた、このデータベースのデータと、ユーザが作成したルールを使用して、論理的なビジネスの意思決定を行います。

注: パフォーマンス データベースの設定の詳細については、セクション「`dpmutil set|get perf` コマンド - パフォーマンス データベースの設定」を参照してください

ユーザ インターフェース

CA Virtual Assurance の Web ベース ユーザ インターフェースを使用すると、中央の場所からデータ センターを管理できます。CA Virtual Assurance の組み込みコンポーネントの機能を使用すれば、各コンポーネントのインターフェースを個別に開く必要はありません。

たとえば、問題を管理するための CA SDM も、レポートを作成するための JasperReports (デフォルトのレポート エンジン)も、CA Virtual Assurance の Web ベース ユーザ インターフェースから使用できます。また、CA Embedded Entitlements Manager の機能を使って Active Directory を活用し、CA EEM を開かずにユーザ インターフェースからユーザと権限を管理することもできます。

より高度な機能を実行するときは、各コンポーネントのユーザ インターフェースに直接アクセスすることも当然可能です。たとえば、ネイティブ セキュリティを使用するために **CA Embedded Entitlements Manager** を開く場合があります。コンポーネントがインストールされているサーバに直接ログインして、そのユーザ インターフェースに直接アクセスできます。あるいは、**CA Virtual Assurance UI** の [管理] タブにある [設定] ページに移動して、コンポーネントを選択し、[アクション] ドロップダウン メニューから製品のホーム ページを起動できます。

ユーザ インターフェースへのアクセス

仮想システムと物理システムの検出およびプロビジョニング、ポリシーの作成、ジョブのスケジューリングなどを行うときは、ユーザ インターフェースにアクセスします。[スタート] ショートカット メニューは **CA Virtual Assurance** サーバ上でのみ利用できます。まず、マネージャ サーバに直接アクセスする必要があります。次に、[スタート] メニューを使って製品の一部の機能 (CLI や **Autoshell** など) を使用します。別のサーバからインターフェースにアクセスするユーザは、Web ブラウザに URL を入力する必要があります。

ユーザ インターフェースにアクセスする方法

1. **CA Virtual Assurance** サーバで、[スタート]、[プログラム]、[CA]、[CA Virtual Assurance]、[Launch CA Virtual Assurance] の順に選択します。

CA Virtual Assurance ログイン ページが以下の URL に表示されます。

`https://servername:port/UI`

servername

グラフィカル ユーザ インターフェースがインストールされているサーバの名前を指定します。

port

サーバがリスンしているポートを指定します。

デフォルト: 8443

2. 管理者のログイン認証情報を入力し、[ログイン] をクリックします。
ダッシュボードが表示されます。

第 3 章：ユーザの管理

このセクションには、以下のトピックが含まれています。

[ユーザ アクセス制御](#) (P. 23)

[パスワード管理](#) (P. 29)

[外部ディレクトリ ユーザのためのタスク](#) (P. 34)

[vCenter Server でのユーザ スコープ認証](#) (P. 39)

ユーザ アクセス制御

CA Embedded Entitlements Manager で、CA Virtual Assurance コンポーネント間のすべての通信が確保されます。以下の設定のいずれかを選択できます。

- Active Directory
- ネイティブ セキュリティ

注：外部ディレクトリの設定の詳細については、CA Embedded Entitlements Manager でインストールされる「CA EEM 導入ガイド」およびオンライン ヘルプを参照してください。これらのドキュメントは、[スタート]-[プログラム]-[CA]-[Embedded Entitlements Manager]-[ドキュメント]を選択して CA Embedded Entitlements Manager のインストール場所で見つけるか、または CA サポート オンライン Web サイト(<http://www.ca.com/jp/support>)で見つけることができます。

Active Directory

既存の Active Directory 設定に接続したときは、事前定義済みのユーザおよびユーザグループが、ユーザの中央レポジトリと一貫しています。CA Technologies では、CA Virtual Assurance または CA Embedded Entitlements Manager を使用するのではなく、Active Directory 内でユーザを作成および変更することを推奨します。

CA Virtual Assurance は、LDAP (Lightweight Directory Access Protocol) を使用して、Microsoft Active Directory サーバの読み取りおよび書き込みを行います。デフォルトでは、LDAP トラフィックはセキュリティが保証されずに送信されます。このため、サーバと Microsoft Active Directory の間の通信ではセキュリティが保証されません。Microsoft Active Directory のセキュリティを確保するために、SSL (セキュアソケットレイヤ) を使用する LDAP (LDAPS) を使用してください。この場合は、Microsoft の認証機関または別の認証機関のいずれかから、正しくフォーマットされた証明書をインストールします。

注: データを安全に送信するための Active Directory の設定の詳細については、Microsoft の Web サイトを参照してください。ナレッジベース記事「サードパーティの証明機関が SSL 経由で LDAP を有効にする方法」を検索してください。LDAPS を使用するように Active Directory を設定した後は、データを安全に送信できます。

Active Directory でのセキュリティ上の考慮事項

Microsoft Active Directory サーバに対する読み取りと書き込みでは、Lightweight Directory Access Protocol (LDAP) が使用されます。LDAP トラフィックはデフォルトで、セキュリティで保護されずに転送されます。このため、サーバと Microsoft Active Directory の間の通信はセキュリティで保護されません。Microsoft Active Directory をセキュリティで保護するには、LDAP over Secure Sockets Layer (SSL) - LDAPS を使用します。Microsoft または Microsoft 以外の認証局から発行された適切に書式設定された証明書をインストールする必要があります。

その要件は Microsoft サポート技術情報の記事で解説されています。

注: データを安全に転送するための Active Directory の設定方法の詳細については、Microsoft Web サイトにある Microsoft サポート技術情報の記事「サードパーティの証明機関が SSL 経由で LDAP を有効にする方法」を参照してください。Active Directory で LDAPS を使用するための設定を行ったら、データを安全に転送できます。

ネイティブ セキュリティ

[ネイティブ セキュリティ]を使用して、CA EEM 管理者は、特に CA Virtual Assurance のためのユーザ、ユーザ グループ、およびポリシーを作成できます。これは、この情報がローカルのストアに存在するためです。[ネイティブ セキュリティ]では、独自のユーザとユーザ グループのセットを手動で定義する必要があります。これらのユーザとユーザ グループは、ディレクトリ サービスで現在定義されているものとは一致していない場合があります。

CA Embedded Entitlements Manager が CA Virtual Assurance で動作するしくみ

CA Embedded Entitlements Manager には、以下のキー オブジェクトが含まれます。

- ID (ユーザおよびユーザ グループ)
- リソース
- ポリシー

CA Embedded Entitlements Manager は、以下の機能を提供します。

認証

ユーザを認証します。認証されたユーザは、その後の認可処理で使用できます。

認証

ユーザが特定のリソースにアクセスすることを可能にします。リソースとは、任意の論理または物理エンティティです。CA Virtual Assurance の典型的なリソースは、ユーザ インターフェース コンポーネント (タブ、コマンド、ドロップダウン リストなど) です。リソース クラスに関連付けられたポリシーのセットで、認可が制御されます。これらのポリシーは、CA Virtual Assurance に CA Embedded Entitlements Manager を統合する主な方法です。

CA EEM ユーザ インターフェースへのアクセス

ネイティブ セキュリティを使用するために、CA Embedded Entitlements Manager ホーム ページにログインします。また、[スタート]メニューから CA Embedded Entitlements Manager ドキュメントを利用できます。さらに、ログインした後は、ホーム ページでオンライン ヘルプを利用できます。

CA Embedded Entitlements Manager ユーザ インターフェースにアクセスする方法

1. [スタート]-[プログラム]-[CA]-[Embedded Entitlements Manager]-[EEM UI]を選択します。

CA Embedded Entitlements Manager のログイン ウィンドウが表示されます。

注: ログオン時にセキュリティ証明書リクエストを受信した場合は、それを回避して続行します。セキュリティ証明書メッセージが表示されないようにするには、任意のベンダーから証明書を取得して、サーバにそれを適用します。セキュリティ証明書のインストールの詳細については、Apache Tomcat の Web サイトを参照してください。

2. アプリケーションのドロップダウンリストから[AIP]を選択します。
[ユーザ名]フィールドには「EiamAdmin」が入力されています。
3. [パスワード]フィールドにパスワードを入力し、[ログイン]をクリックします。

CA Embedded Entitlements Manager ホーム ページの、デフォルトで表示されるホーム ページが表示されます。

CA EEM ユーザの作成

CA Virtual Assurance へのアクセス権を付与するには、CA EEM ユーザを作成します。この手順では、CA Virtual Assurance の CA EEM が使用する共通データストアに CA EEM ユーザを手動で追加する方法について説明します。また、外部ディレクトリを参照してユーザを追加することもできます。

注: 外部ディレクトリへの参照によるユーザの追加の詳細については、CA EEM と共にインストールされる「CA EEM 導入ガイド」およびオンライン ヘルプを参照してください。

CA EEM ユーザを作成する方法

1. CA Embedded Entitlements Manager Web サイトのホーム ページで[ID の管理]をクリックします。
デフォルトで[ユーザ]ページが選択されています。
2. [ユーザの検索]セクションにある[アプリケーション ユーザの詳細]オプションを選択します。
3. [属性]ドロップダウンリストで[ユーザ名]を、[演算子]ドロップダウンリストで[LIKE]を選択されたままにし、[値]フィールドは空白のままにして、[実行]をクリックします。

すべての CA Virtual Assurance ユーザが[ユーザ]ペインの階層ツリーにリスト表示されます。

4. 左側のペインにある[新規ユーザ]アイコンをクリックします。
[新規ユーザ]ペインが右側に表示されます。
5. このユーザのユーザ ID をユーザ名フィールドに入力して、[ユーザの詳細]ペインの[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。
6. [アプリケーション グループ メンバシップ]ペインの[利用可能なユーザ/ユーザ グループ]からアプリケーション グループを選択して右矢印をクリックします。

アプリケーション グループが[選択したユーザ/ユーザ グループ]に追加されます。

注: このユーザを、1 つ以上の動的グループまたはグローバル グループに追加することもできます。詳細については、CA EEM のマニュアルを参照してください。

7. [認証]ペインの[新しいパスワード]および[パスワードの確認]フィールドに、このユーザのパスワードを入力して[保存]をクリックします。

[ユーザ]ペインの下に確認メッセージが表示されます。

デフォルト ユーザ グループの作成

ユーザ グループを使用して、ビジネス上の役割ごとにユーザを論理的にグループ化できます。ユーザ グループを作成して、複数のユーザに同じアクセス権限を付与することができます。この手順では、アプリケーション グループの作成についてのみ記述しますが、この後の手順で、そのアプリケーション グループのためのポリシーの作成について説明します。また、グローバル グループ、動的グループ、および個別のユーザのためのポリシーも作成できます。

ユーザ グループを作成する方法

1. [CA Embedded Entitlements Manager にアクセス]ホーム ページの[ホーム]タブで[ID の管理]をクリックします。

デフォルトで[ユーザ]ページが選択されています。

2. [グループ]をクリックし、[アプリケーション グループを表示]チェック ボックスをオンにして[実行]をクリックします。

利用可能なアプリケーション グループがすべて、[ユーザ グループ]ペインの[アプリケーション グループ]の下にリスト表示されます。

3. 左側のペインの[新しいアプリケーション グループ]をクリックします。

[新しいアプリケーション ユーザ グループ]ページが右側のペインに表示されます。

4. 新しいアプリケーション グループの名前を入力し、[保存]をクリックします。

新しいアプリケーション ユーザ グループが作成されます。

パスワード管理

ユーザ認証情報は、CA Virtual Assurance コンポーネント間の通信にとって不可欠です。CA Virtual Assurance は、ユーザおよびパスワード情報を内部に格納します。CA Virtual Assurance が統合する外部コンポーネントまたはアプリケーションのパスワードを変更する場合は、整合性を保つために、これらのパスワードを CA Virtual Assurance で変更します。そうしないと、CA Virtual Assurance が正しく動作しません。

以下の領域を考慮してください。

- Active Directory セキュリティ
- ネイティブ セキュリティ
- CA Embedded Entitlements Manager 管理者
- データベース sa ユーザ (SQL 認証)

CA Embedded Entitlements Manager 管理者パスワード(EiamAdmin)の変更

CA Embedded Entitlements Manager 管理者パスワード(EiamAdmin)を変更する場合は、CA Embedded Entitlements Manager でパスワードを変更し、さらに CA Virtual Assurance でも変更します。

CA Embedded Entitlements Manager で管理者パスワード(EiamAdmin)を変更する方法

1. [スタート]-[プログラム]-[CA]-[Embedded Entitlements Manager]-[EEM UI]に移動し、ユーザ インターフェースを開きます。
[ログイン]ダイアログ ボックスが表示されます。
2. 現在の EiamAdmin パスワードでログインします。
ユーザ インターフェースが開きます。
3. [設定]および[EEM サーバ]をクリックします。
[EEM サーバ]ペインが表示されます。
4. [EiamAdmin パスワード]をクリックします。
[新しいパスワード]および[パスワードの確認]フィールドが表示されます。

5. パスワードを入力し、[保存]をクリックします。

これで、新しい EiamAdmin パスワードを使用して CA Embedded Entitlements Manager にログインできます。

CA Virtual Assurance で管理者パスワード(EiamAdmin)を変更する方法

1. [スタート]-[プログラム]-[CA]-[CA Virtual Assurance]-[CA Virtual Assurance コマンド プロンプト]に移動します。

コマンド プロンプトが表示されます。

2. 以下のコマンドを入力します。

```
dpmutil -set -eiam
```

dpmutil コマンドが、必要な認証情報の入力を要求します。

情報を入力してコマンドを完了します。

3. CAAIPApache および CAIPTomcat サービスを再利用します。

認証情報が一致し、CA Virtual Assurance が予期したとおりに動作します。

注: いずれの場合も、*Install_path¥Apache¥logs¥error.log* にある Apache のログ ファイルで、製品が適切に起動したことを確認できます。最後のエントリが「Validating EEM is available」である場合は、認証情報にまだ問題があります。「-set -eiam」および「-set -sysuser」に使用した認証情報を、CA Embedded Entitlements Manager UI へのログインに使用できることを確認します。その後、有効な認証情報を使用して dpmutil コマンドを再度実行します。

データベース管理者(sa)パスワードの変更

Microsoft SQL 認証を使用しており、Microsoft SQL ユーザ(通常は「sa」ユーザ)のパスワードを変更する場合は、CA Virtual Assurance パスワードも変更します。

Microsoft SQL Server のデータベース管理者(sa)パスワードを変更する方法

1. Microsoft SQL Server Management Studio を開いてログインします。
2. オブジェクト エクスプローラーで[セキュリティ]、[ログイン]を展開します。
3. sa を開き、右側のペインでパスワードを変更します。

注: 詳細については、Microsoft SQL Server のドキュメントを参照してください。

CA Virtual Assurance のデータベース管理者 (sa) パスワードを変更する方法

1. [スタート]-[プログラム]-[CA]-[CA Virtual Assurance]-[CA Virtual Assurance コマンド プロンプト]に移動します。

コマンド プロンプトが表示されます。

2. 以下のコマンドを入力します。

```
dpmutil -set -mgmtdb
```

dpmutil コマンドが、適切な認証情報の入力を要求します。

情報を入力してコマンドを完了します。

3. パフォーマンス データベースが同じサーバおよびデータベース ユーザ (sa)を使用している場合は、以下のコマンドを入力します。

```
dpmutil -set -perfdb
```

dpmutil コマンドが、適切な認証情報の入力を要求します。

情報を入力してコマンドを完了します。

4. CAAIPApache および CAIPTomcat サービスを再利用します。

認証情報が一致し、CA Virtual Assurance が予期したとおりに動作します。

ネイティブ セキュリティのシステム ユーザ パスワードの変更

CA Virtual Assurance では、Apache サービスの開始または停止などのために、**sys_service** システム ユーザが正しく機能することが必要です。ネイティブ セキュリティでのインストール中に、**sys_service** システム ユーザとそのパスワードを指定します。インストール プログラムは、CA Embedded Entitlements Manager および CA Virtual Assurance 内に **sys_service** 認証情報を格納します。後で CA Embedded Entitlements Manager 内の **sys_service** のパスワードを変更する場合は、すべての CA Virtual Assurance サービスが引き続き実行されるように、CA Virtual Assurance でもパスワードを変更します。

CA Embedded Entitlements Manager で sys_service パスワードを変更する方法

1. [スタート]-[プログラム]-[CA]-[Embedded Entitlements Manager]-[EEM UI]に移動し、ユーザ インターフェースを開きます。

[ログイン]ダイアログ ボックスが表示されます。

2. 現在の EiamAdmin パスワードでログインします。

ユーザ インターフェースが開きます。

3. [ID の管理およびユーザの検索]をクリックします。
[ユーザ]ペインにユーザが表示されます。
4. `sys_service` ユーザをクリックします。
右側のペインにユーザ プロパティが表示されます。
5. [認証]セクションまでスクロールし、[パスワードのリセット]をクリックします。
[新しいパスワード]および[パスワードの確認]フィールドが表示されます。
6. パスワードを入力し、[保存]をクリックします。
これで、新しいパスワードが CA Embedded Entitlements Manager に格納されました。

CA Virtual Assurance で `sys_service` ユーザ パスワードを変更する方法

1. [スタート]-[プログラム]-[CA]-[CA Virtual Assurance]-[CA Virtual Assurance コマンド プロンプト]に移動します。
コマンド プロンプトが表示されます。
2. 以下のコマンドを入力します。

```
dpmutil -set -sysuser
```

`dpmutil` コマンドが、必要な認証情報の入力を要求します。
情報を入力してコマンドを完了します。
3. CAAIPApache および CAIPTomcat サービスを再利用します。
認証情報が一致し、CA Virtual Assurance が予期したとおりに動作します。

Active Directory セキュリティのシステム ユーザ パスワードの変更

インストールされた CA Virtual Assurance が Active Directory に接続するように設定されている場合は、CA Virtual Assurance をインストールするユーザが自動的に CA Embedded Entitlements Manager に登録されます。この登録によって、CA Virtual Assurance が Active Directory ドメインからユーザを認証できるようになります。ユーザ パスワードが変更されると、CA Embedded Entitlements Manager がユーザを認証できなくなるため、ユーザは CA Virtual Assurance ユーザ インターフェイスにログインできません。以下のようにユーザ パスワードを変更します。

Active Directory のユーザ パスワードを変更する方法

1. [スタート]-[プログラム]-[CA]-[Embedded Entitlements Manager]-[EEM UI]に移動し、ユーザ インターフェイスを開きます。
[ログイン]ダイアログ ボックスが表示されます。
2. 現在のパスワードでログインします。
ユーザ インターフェイスが開きます。
3. [設定]および[EEM サーバ]をクリックします。
[EEM サーバ]ペインが表示されます。
4. 左側のペインの[グローバル ユーザ/グローバル グループ]をクリックして、デフォルト オプション[外部ディレクトリから参照]を選択されたままにします。
5. タイプをデフォルトの[Microsoft Active Directory]のままにし、[パスワード] および[パスワードの確認]フィールドに新しいパスワードを入力して[保存]をクリックします。
6. CA Embedded Entitlements Manager を閉じます。
7. [スタート]-[プログラム]-[CA]-[CA Virtual Assurance]-[CA Virtual Assurance コマンド プロンプト]に移動します。
コマンド プロンプトが表示されます。

8. 以下のコマンドを入力します。

```
dpmutil -set -sysuser
```

Sysuser は、CA Virtual Assurance をインストールするユーザと同じユーザです。dpmutil コマンドが、手順 5 で指定した、必要な認証情報の入力を要求します。

情報を入力してコマンドを完了します。

9. CAAIPApache および CAIPTomcat サービスを再利用します。

認証情報が一致し、CA Virtual Assurance が予期したとおりに動作します。

注: いずれの場合も、*Install_path¥Apache¥logs¥error.log* にある Apache のログファイルで、製品が適切に起動したことを確認できます。最後のエントリが「Validating EEM is available」である場合は、認証情報にまだ問題があります。「-set -eiam」および「-set -sysuser」に使用した認証情報を、CA Embedded Entitlements Manager UI へのログインに使用できることを確認します。有効な認証情報を使用して dpmutil コマンドを再度実行します。

外部ディレクトリ ユーザのためのタスク

どの外部ディレクトリを使用しているかにかかわらず、CA Virtual Assurance ユーザ インターフェースからユーザ アクセス制御タスクを完了できます。

ユーザ グループの作成

ユーザ グループを使用すると、ビジネス上の役割に従ってユーザを論理的にグループ化できます。ユーザ グループを作成して、複数のユーザに同じアクセス権限を付与することができます。

ユーザ グループを作成する方法

1. [管理]をクリックします。
[管理]ページが表示されます。

2. [ユーザ グループ]をクリックします。
[ユーザ グループ]ページが表示されます。
3. ユーザ グループの名前を入力します。ビジネス上の役割またはサービスに基づく名前を使用できます。
4. (オプション)説明を入力します。
5. [保存]をクリックします。
新規ユーザ グループが左側のペインに表示されます。

グループへのユーザの割り当て

ユーザは、自身のユーザ グループに割り当てられたアクセス権限を継承します。既存のユーザ グループに新規ユーザを追加して、そのユーザにユーザ グループのアクセス権限を付与することができます。管理者ユーザ グループは事前定義済みグループで、デフォルトでリストに表示されます。

グループにユーザを割り当てる方法

1. [管理]をクリックします。
[管理]ページが表示されます。
2. [ユーザ グループ]をクリックします。
[ユーザ グループ]ページが表示されます。
3. [ユーザ グループ]を展開して、リストからユーザ グループを選択します。
サブメニューが表示されます。
4. [メンバシップ]サブメニューを選択します。
一連のメンバシップ ペインが表示されます。
5. 追加するユーザの名前を[値]テキストボックスに入力して、[検索]をクリックします。
検索結果が[利用可能なユーザ/ユーザ グループ]ペインに表示されるか、一致するものが見つからなかったことを知らせるメッセージが表示されます。ユーザ名が確実でない場合は、[ユーザまたはユーザ グループを検索 \(P. 38\)](#)できます。
6. 追加するユーザを[利用可能なユーザ/ユーザ グループ]ペインで選択し、右矢印  をクリックします。
ユーザ名が[選択したユーザ/ユーザ グループ]ペインに移動します。

7. [保存]をクリックして、ユーザの追加を完了します。
ユーザには、そのユーザ グループのアクセス権限が付与されます。

ユーザ グループからのユーザまたはユーザ グループの削除

既存の CA Virtual Assurance ユーザ グループからユーザとユーザ グループを削除できます。管理者ユーザ グループは事前定義済みグループで、デフォルトでリストに表示されています。

ユーザ グループからユーザまたはユーザ グループを削除する方法

1. [管理]-[設定]をクリックします。
[設定]ページが表示されます。
2. [ユーザ グループ]を選択します。
[ユーザ グループ]メニューが左側のペインに表示されます。
3. [ユーザ グループ]を展開し、リストからユーザ グループを選択します。
サブメニューが右側のペインに表示されます。
4. [メンバシップ]サブメニューを選択します。
一連のメンバシップ ペインが表示されます。
5. [選択したユーザ/ユーザ グループ]ペインから削除するユーザまたはユーザ グループを選択して、左矢印をクリックします。
ユーザまたはユーザ グループが[利用可能なユーザ/ユーザ グループ]ペインに移動します。
6. ユーザとユーザ グループの削除が完了したら、[保存]をクリックします。

ユーザ グループに対するサービスへのアクセス権の割り当て

ユーザのグループが複数存在する環境では、通常、各グループで他のグループのリソースが表示されないようにする必要があります。管理者は、ユーザのグループに特定のリソースを割り当てることができます。管理者によっては、自分がメンバであるグループにのみ、リソースを割り当てることができます。ただし、グループ *AIPAdmins* の管理者には、リソースを割り当てるための完全なアクセス権があります。

ユーザ グループにサービスへのアクセス権を割り当てる方法

1. [管理]をクリックします。
[管理]ページが表示されます。
2. [ユーザ グループ]をクリックします。
[ユーザ グループ]ページが表示されます。
3. 左ペインで、権限を設定するユーザ グループを選択して[サービス アクセス権]をクリックします。
システムに定義されたサービスをリスト表示するツリーが表示されます。
4. アクセスを付与または制限するサービスを選択して[保存]をクリックします。
ユーザ グループには、関連付けられたサービスに割り当てられたアクセス権限が付与されます。

ユーザ グループ権限の設定

ユーザ インターフェースの機能領域および特定の機能へのユーザ グループのアクセス権を制御できます。*AIPAdmins* ユーザ グループにはデフォルトで、すべての機能領域および機能へのアクセス権があります。

ユーザ グループ権限を設定する方法

1. [管理]をクリックします。
[管理]ページが表示されます。
2. [ユーザ グループ]をクリックします。
[ユーザ グループ]ページが表示されます。
3. 権限を設定するユーザ グループを選択して[権限]をクリックします。
[権限]ページが表示されます。

4. アクセスを付与または制限する機能領域または機能を選択して、[保存]をクリックします。

ユーザ権限が更新されます。

ユーザ グループの削除

不要になったユーザ グループは削除できます。

ユーザ グループを削除する方法

1. [管理]をクリックします。
[管理]ページが表示されます。
2. [ユーザ グループ]をクリックします。
[ユーザ グループ]ページが表示されます。
3. [ユーザ グループ]を右クリックし、[ユーザ グループを削除します]を選択します。
ユーザ グループが削除されます。

ユーザまたはユーザ グループの検索

追加または削除するユーザまたはユーザ グループを検索できます。

ユーザまたはユーザ グループを検索する方法

1. [管理]をクリックします。
[管理]ページが表示されます。
2. [ユーザ グループ]をクリックします。
[ユーザ グループ]ページが表示されます。
3. [ユーザ グループ]を展開して、リストからユーザ グループを選択します。
ユーザ グループのページが右ペインに表示されます。
4. [メンバシップ]をクリックします。
[ユーザ/ユーザ グループ]ページが表示されます。

5. [アイデンティティ]ドロップダウンリストで[ユーザ]または[ユーザ グループ]を選択します。検索する属性を[属性]ドロップダウンリストで選択し、LIKE 演算子を選択されたままにしておきます。[値]フィールドに値(またはワイルドカードを含む部分的な値)を入力して[検索]をクリックします。
一致するユーザまたはユーザ グループ名のリストが[利用可能なユーザ/ユーザ グループ]リストに表示されます。

vCenter Server でのユーザ スコープ認証

vCenter Server 環境でユーザ スコープ認証を有効にするには、インストールパス¥VirtualAssurance¥conf ディレクトリ内の `caaipconf.cfg` ファイルに設定エントリを追加します。このエントリはインストール後に存在しなくなるため、ユーザ スコープ認証はデフォルトで無効になります。この場合 CA Virtual Assurance では、[管理]タブの vCenter Server 設定ペインで指定されている、vCenter Server 認証用のユーザが使用されます。

対照的に、ユーザ スコープ認証が有効な場合は、vCenter Server 環境での操作を認証するために、現在ログインしているユーザ(ユーザ インターフェース)が使用されます。ユーザ スコープ認証が意味するのは、vCenter Server 内で適切なユーザおよびその権限が指定されているということです。CA Virtual Assurance ユーザ インターフェースにログインするには、同じユーザを CA EEM 内でも指定する必要があります。

ユーザ スコープ認証を有効にする方法

1. vCenter Server で、必要なユーザおよびその権限(管理者または読み取り専用)を指定します。
2. CA EEM で同じユーザを指定します。
3. CA Virtual Assurance マネージャ サーバに切り替え、インストールパス `¥VirtualAssurance¥conf` ディレクトリに移動します。
4. テキスト エディタで `caaipconf.cfg` ファイルを開き、AIP 製品セクションに以下のエントリを追加します。

```
<property name="USER_SCOPED_AUTHENTICATION">
  <value>VC</value>
  <displayName>The vCenter PMM component uses the currently logged in user for
  authenticating vCenter Server platform operations.</displayName>
</property>
```

Result:

```
<properties targetNamespace="http://www.ca.com/cfg/types/2008/05">
  <product name="AIP">
    ...
    <property name="USER_SCOPED_AUTHENTICATION">
      <value>VC</value>
      <displayName>The vCenter PMM component uses the currently logged in
      user for authenticating vCenter Server platform operations.</displayName>
    </property>
    ...
  </product>
  ...
</properties>
```

5. ファイルを保存します。
CA Virtual Assurance によって変更が自動的に検出されます。
6. 現在ログインしているユーザについて、VMware 環境を管理するための CA Virtual Assurance 内での権限が、vCenter Server 内で指定されているものと同じであることを確認します。

注: ユーザ スコープ認証を無効にする場合は、`caaipconf.cfg` ファイルからエントリを削除します。

例

初期シナリオ: CA Virtual Assurance のインストール中、ユーザ CA は CA Virtual Assurance ユーザ インターフェイスにログインするように設定されました。vCenter Server で、**管理者**は管理者権限を持つユーザです。CA Virtual Assurance は vCenter Server 環境での操作を認証するために **管理者**を使用するように設定されています(ユーザ インターフェイスの[管理]タブ、[vCenter Server 設定]ペインを参照)。ユーザ スコープ認証は、デフォルトで無効になっています。

以下のシナリオはたとえば、適切な vCenter Server 設定を使用した完全カスタム インストールに準じています。

以下を仮定します。

- 2 人の追加ユーザが vCenter Server 上で設定されます: **Superuser** (管理者)および **Reader** (読み取り専用権限)
- **Superuser**と **Reader** は CA EEM に追加されます。
- ユーザ スコープ認証は有効です

CA Virtual Assurance に **Superuser**としてログインすると、vCenter Server を管理するための管理者権限を持ちます。

CA Virtual Assurance に **Reader**としてログインすると、vCenter Server をモニタするための読み取り専用権限を持ちます。

ユーザ スコープ認証を無効にすると、CA Virtual Assurance にログインするすべてのユーザが vCenter Server 管理者権限を持ちます。ユーザ スコープ認証を無効にすると、CA Virtual Assurance では、ユーザ インターフェイスの[管理]タブにある[vCenter Server 設定]ペインで指定されたユーザ **管理者**が使用します(この例の初期シナリオも参照)。

第 4 章: リソースの設定

CA Virtual Assurance のインストール後は、このセクションで説明するタスクを実行する必要があるかどうかを確認してください。インストールに応じて、追加の設定手順が必要な場合があります。

このセクションには、以下のトピックが含まれています。

[ディスカバリ](#) (P. 43)

[環境管理の設定要件](#) (P. 43)

[sysedge.cf ファイルの編集による SNMPv1 トラップの設定](#) (P. 55)

[イベント転送](#) (P. 56)

ディスカバリ

CA Virtual Assurance をインストールした後に、ネットワーク デバイスとモニタ対象サーバで使用される SNMP 読み取りおよび書き込み認証情報を [SNMP 設定] パネルに追加します。[管理] タブの [設定] を開き、[SNMP 設定] パネルにアクセスします。

注: ディスカバリを開始する前に SNMP 認証情報を追加します。

ディスカバリがすでに実行されている場合は、再度システムを検出します。

環境管理の設定要件

まだ検出されていない環境があり、インストール中に設定していない AIM がある場合は、必要なプログラムをインストールするか、このセクションの説明に従って AIM を設定します。

環境の検出

カスタム CA Virtual Assurance マネージャ インストールを使用する場合、AIM のインストール中に仮想環境および Microsoft クラスタを検出することができます。可能な場合は、インストールの各ダイアログ ボックスに、管理対象サーバに関する必要なデータを入力します。インストール中に設定をスキップし、後ほど設定を実行することもできます。

カスタム インストール後に AIM を設定して仮想環境を検出するには、以下のいずれかを実行します。

- ユーザ インターフェースから[管理]タブを開き、[設定]-[プロビジョニング]に移動して、認証情報を追加して AIM を設定する適切なサーバタイプを選択します。CA Virtual Assurance は自動的に物理コンポーネントおよび仮想コンポーネントを検出し、管理データベースに取り込みます。
- Windows AIM サーバ上で NodeCfgUtil.exe ユーティリティを使用して、仮想環境管理に必要なデータを追加します。ユーティリティは `SystemEDGE_install_path¥plugins¥AIPCommon` ディレクトリにあります。次に、CA Virtual Assurance マネージャから AIM サーバを再検出します。このオプションでは、必要な手順を手動で実行できます。

以下のガイドラインを考慮してください。

- 仮想環境および Microsoft クラスタへのアクセスに指定されたユーザには、リモートアクセスのための十分な権限が必要です。
- Hyper-V Server を管理するには、Hyper-V Server に SystemEDGE および Hyper-V AIM をインストールします。SystemEDGE と Hyper-V AIM は、同じ Hyper-V Server 上で実行する必要があります。次に、AIM を設定し、Hyper-V Server を検出します。
- CA Virtual Assurance マネージャ サーバ上で実行されない SystemEDGE および AIM が、これらに関連付けられた CA Virtual Assurance マネージャと同じ SNMP 設定を使用することを確認します。
- VMware Infrastructure または vSphere を管理するには、対応する vCenter Server の認証情報を入力します。
- すべての VMware VM に VMware ツールをインストールします。VMware ツールが VM にインストールされていない場合は、いくつかの機能が適切に動作しません。

VMware ツールは、VM の仮想化を最適化します。これらのツールがない場合は、多くの機能を利用できません。詳細については、VMware のマニュアルを参照してください。

AIM サーバから vCenter Server、Solaris ゾーン サーバ、HMC/IVM サーバ、Microsoft クラスタ、Cisco UCS サーバ、Active Directory または Exchange Server を検出する方法

1. Windows AIM サーバで NodeCfgUtil.exe ユーティリティを実行して、対応する AIM の設定データを更新します。

NodeCfgUtil.exe ユーティリティは、このデータを zone.cfg、vc.cfg、ucs.cfg、lpar.cfg、mscs.cfg、または esad.cfg に格納します。

2. マネージャ サーバでユーザ インターフェイスを開き、[リソース]、ナビゲーション ペインの[データセンター]の順にクリックします。

3. 右クリックし、[管理]-[検出]を選択します。

ディスカバリ オプションが表示されます。

4. 以下のいずれかを選択します。

- システムの検出
- ネットワークの検出

対応するダイアログ ボックスが表示されます。

5. 管理対象にする vCenter Server、Solaris ゾーン サーバ、Microsoft クラスタ、Cisco UCS サーバ、または HMC/IVM サーバのシステム名を入力します。あるいは、ディスカバリ プロセス用のネットワークプロパティを入力できます。[OK]をクリックします。

CA Virtual Assurance が検出プロセスを開始します。

検出されたリソースが[エクスプローラ]ペインに表示されます。

関連項目

[vCenter Server 管理コンポーネントを設定する方法 \(P. 300\)](#)

ダイアログ モードの NodeCfgUtil による AIM の設定

NodeCfgUtil を使用して、vCenter Server、IBM LPAR、Solaris ゾーン、Microsoft クラスタ、Cisco UCS サーバ、Exchange Server、Active Directory (ESAD) 用の各 AIM の設定を変更できます。このユーティリティをダイアログ モードで使用する と、適切な AIM が管理するノードを設定できます。

注: NodeCfgUtil.exe は Windows 管理者として実行される必要があります。

次の手順に従ってください:

1. 管理者としてログインし、AIM が存在するシステムで Windows エクスプローラを開き、`SystemEDGE_InstallPath¥plugins¥AIPCommon` ディレクトリに移動して、NodeCfgUtil.exe を起動します。NodeCfgUtil で、インストールされた AIM が検出され、その後に表示されるダイアログ ボックスには、それらの AIM のみのリストが含まれます。
2. **1** を入力して、新しい管理対象ノードを追加します。
NodeCfgUtil で検出できるのは、インストールされた AIM のみです。
3. 画面上の指示に従って、設定を完了します。各ノードには、認証用の有効なユーザ名とパスワードが必要です。
4. 設定が正常に完了したら、**0** を入力して前のメニューに戻るか、またはユーティリティを終了します。

NodeCfgUtil は、`SystemEDGE_InstallPath¥plugins¥AIPCommon` ディレクトリに、Solaris ゾーン (zone.cfg)、vCenter Server (vc.cfg)、Microsoft クラスタ (mscs.cfg)、UCS (ucs.cfg)、LPAR (lpar.cfg)、または ESAD (esad.cfg) 用の設定ファイルを書き込みます。また、NodeCfgUtil ユーティリティを使用して、既存のエントリの編集または削除を実行できます。対応するダイアログ ボックスには、目的に応じた名前が付けられています。

注: サーバ エントリを削除すると、NodeCfgUtil は、このサーバに削除のマークを付けますが、それだけではユーザ インターフェースからもデータベースからもサーバは削除されません。ユーザ インターフェースとデータベースからサーバを削除するには、AIM が実行されている Windows サーバを再検出してください。新しいディスカバリ プロセスが削除マークを検出し、対応するサーバをユーザ インターフェースとデータベースから削除します。

例

以下の例は、vCenter AIM の設定に正常に追加された myvc5 サーバに関する [管理対象ノードのインストール] ダイアログを示します。AIM は現在、vCenter Server サーバを管理できる状態です。vCenter AIM はマルチインスタンス AIM です。したがって、この手順を繰り返し、この AIM で管理する vCenter Server をさらに追加できます。

**** 管理対象ノードの選択 ****

1. IBM LPAR
2. Solaris ゾーン
3. VMware vCenter
4. Cisco UCS
5. Microsoft クラスター
0. 前のメニューに戻る

選択項目を入力してください: 3

VMware vCenter ノードの以下の情報を入力します...

(いずれかの時点で前のメニューに戻るには、Ctrl + Q キーを入力します)

1. サーバ名: myvc5
2. ユーザ名: administrator
3. パスワード: *****
4. ポート [デフォルト=443]:
5. プロトコル [デフォルト=https]:

CAAC1016 認証しています。お待ちください...

CAAC1019 認証に成功しました。

CAAC1023 ノードが正常に追加されました。

キーをどれか押してください。

以下の例は、ESAD AIM の設定に正常に追加された mydomain に関する[管理対象ノードのインストール]ダイアログを示します。管理エンティティは **Active Directory** に設定されます。管理モードはドメイン全体に設定されます。詳細については、NodeCfgUtil コマンド モードを参照してください。ESAD AIM はマルチインスタンス AIM です。したがって、この手順を繰り返し、この AIM で管理するエンティティをさらに追加できます。

**** 管理対象ノードの選択 ****

1. Microsoft クラスタ
2. Microsoft Exchange Server および Active Directory
0. 前のメニューに戻る

選択項目を入力してください: 2

Microsoft Exchange Server および Active Directory ノードの以下の情報を入力します...

(いずれかの時点で前のメニューに戻るには、Ctrl + Q キーを入力します)

1. ドメイン名: mydomain
2. ユーザ名: administrator
3. パスワード: *****
4. 管理エンティティ: 0
5. 管理モード: 0

CAAC1016 認証しています。お待ちください...

CAAC1018 認証に成功しました。

キーをどれか押してください。

コマンドモードの NodeCfgUtil による AIM の設定

NodeCfgUtil.exe を使用して、IBM LPAR、Solaris ゾーン、VMware vCenter、Microsoft クラスタ、Cisco UCS、Exchange Server および Active Directory (ESAD) 用の AIM 設定を変更できます。このユーティリティをコマンドモードで使用する場合、AIM 設定に追加できるのは管理対象ノードのみです。

注: NodeCfgUtil.exe は Windows 管理者として実行される必要があります。

このコマンドの形式は、以下のとおりです。

- (1) nodecfgutil -help
- (2) nodecfgutil {lpar|zone|mscs} -u *user* -p *password* -h {*pvmname*|*hostname*|*cluster_name*}
- (3) nodecfgutil lpar -u *user* -p *password* -h *pvmname* -s *serial*
- (4) nodecfgutil {vc|ucs} -u *user* -p *password* -h *hostname* -t *port* -c *protocol*
- (5) nodecfgutil esad -u *user* -p *passwd* -d *domainname* -e *entity* -o *option*

-help

コンソールに関する使用情報が表示されます。

lpar|ucs|vc|zone|mscs|esad

仮想環境または物理環境を指定します。

-u *user*

管理者ユーザの名前を指定します。

-p *password*

そのユーザのパスワードを指定します

-h *hostname*

対応する AIM で管理されるサーバの名前を指定します。

-d *domainname*

ESAD AIM でモニタするドメインの名前を指定します。

-h *pvmname*

LPAR AIM で管理する IBM PowerVM サーバ (HMC または IVM) の名前を指定します。

-h *cluster_name*

MSCS クラスタの名前を指定します

-s *serial*

HMC/IVM シリアル番号を指定します。

-t *port*

(vCenter および Cisco UCS のみ) ポート番号を指定します。

-c *protocol*

(vCenter および UCS のみ) プロトコル (HTTP、https) を指定します。

リターンコード: 0 は成功、-1 は失敗

-e *entity*

管理対象エンティティを指定します。

0

Active Directory をモニタリングの対象にします。

1

Exchange Server をモニタリングの対象にします。

2

Active Directory および Exchange Server の両方をモニタリングの対象にします。

-o *option*

管理のオプションを指定します。

0

ドメイン全体をモニタリングの対象にします。

1

ドメインの特定のホストをモニタリングに対象にします。

コマンド モードの NodeCfgUtil で AIM を設定する方法

1. AIM が存在するシステムでコマンド プロンプトを開きます。

コマンド プロンプトが表示されます。

2. 以下のコマンドのいずれかを入力します。

```
(1) nodecfgutil -help
(2) nodecfgutil {lpar|zone|mscs} -u user -p password -h {pvmname|hostname|mscs}
(3) nodecfgutil lpar -u user -p password -h pvmname -s serial
(4) nodecfgutil {vc|ucs} -u user -p password -h hostname -t port -c protocol
(5) nodecfgutil esad -u user -p passwd -d domainname -e {0|1|2} -o {0|1}
```

(1) コンソールに関する使用情報が表示されます。

(2) Solaris ゾーン、LPAR、MSCS に対して認証を実行し、正しい認証情報を格納します。

(3) LPAR に対して認証を実行し、正しい認証情報を格納します。

(4) vCenter または Cisco UCS に対して認証を実行し、正しい認証情報を格納します。

(5) Exchange Server および Active Directory に対して認証を実行し、正しい認証情報を格納します。

このユーティリティは、vCenter Server (vc.cfg)、Solaris ゾーン (zone.cfg)、Cisco UCS (ucs.cfg)、LPAR (lpar.cfg) または ESAD (esad.cfg) の各環境設定ファイルを `sysedge_InstallLpath¥plugins¥AIPCommon` ディレクトリに書き込みます。

複数の vCenter AIM の管理

設定が同じである複数の AIM がある場合、vCenter PMM は、同じ認証情報で設定された AIM のうち、最初に検出されたものを選択します。選択された管理対象 AIM が希望した AIM ではない場合は、vCenter Server を切り替えることができます。vCenter PMM は、vCenter Server を追加したか、削除したか、または切り替えたかどうかに応じて、以下の手順に従います。

vCenter Server の追加

1. vCenter Server 認証情報の検証および保存。
2. vCenter Server 設定を備えた AIM の検出。
3. AIM 設定の保存および必要なオブジェクトの作成。

vCenter Server の削除

1. vCenter Server 認証情報の削除。
2. オブジェクトの削除。
3. AIM 設定の削除。

vCenter Server の切り替え

1. AIM とデータベースの両方への AIM 設定の保存。
2. 新しい設定に基づくオブジェクトの削除および再作成。

注: vCenter Server 認証情報の追加または削除と、設定エントリの追加または削除が行われる時間の間には、わずかな遅れが発生する場合があります。

展開を成功させるには、更新の前に、AIM が正しく設定および検出されることを確認します。

インストール中に vCenter Server AIM を設定していない場合は、vCenter Server リソースを管理できるように、以下の手順を実行します。

複数の vCenter AIM を管理する方法

1. サーバに vCenter AIM をインストールし、インストール中またはその後に、そのサーバで利用可能なコマンドラインから NodeCfgUtil ユーティリティを使用して AIM を設定します。
2. CA Virtual Assurance に、vCenter Server AIM を実行するシステムを検出させます。
3. [管理]-[設定]-[vCenter Server]を選択して移動します。

[vCenter Server] ペインおよび[vCenter AIM サーバ] ペインが表示されます。

4. 管理対象にする vCenter Server を[vCenter Server] ペインに追加します。vCenter Server 環境の有効な認証情報を使用します。

[vCenter AIM サーバ] ペインには、利用可能な vCenter AIM と vCenter Server の 1 対 1 の関係のリストが表示されます。表示された管理対象 AIM が希望した AIM でない場合は、vCenter Server を切り替えることができます。

名前を変更した vCenter Server の管理

管理対象 vCenter Server の名前を変更した場合は、それに応じて、CA Virtual Assurance および vCenter AIM を[管理]タブで設定します。

名前を変更した vCenter Server を管理する方法

1. 名前を変更した vCenter Server を検出します。
2. [管理]-[設定]-[vCenter Server]を選択して移動します。
[vCenter Server]ペインおよび[vCenter AIM サーバ]ペインが表示されます。
3. プラス(+)のボタンをクリックして、名前を変更した vCenter Server を [vCenter Server]ペインに追加します。vCenter Server 環境の有効な認証情報を使用します。
名前を変更した vCenter Server が、通常の状態で見出しに表示されます。
4. [vCenter AIM サーバ]ペインに移動して、vCenter AIM サーバと vCenter Server (前の名前)の 1 対 1 の関係を選択します。[設定]ボタンをクリックします。
その関係のサーバ名を示すダイアログ ボックスが表示されます。
5. 名前を変更した vCenter Server をドロップダウン メニューで選択して[OK]をクリックします。
新しい関係がアクティブになり、CA Virtual Assurance が、新しい名前での vCenter Server の管理を開始します。

重要: 前の名前に関連するデータは、データベースから削除されます。

Solaris ゾーン管理の要件

Solaris ゾーンの管理のために CA Virtual Assurance に必要なユーザ アカウントが、Solaris サーバ上の以下の設定と許可に適合するかどうかを確認します。

- Solaris サーバでのユーザのプロンプトは「#」(デフォルト)である必要があります。
- Solaris ユーザには、以下のコマンドを実行する権限が必要です。
 - zlogin
 - zoneadm
 - zonecfg
- ユーザには、グローバルゾーンから zlogin で個別の Solaris ゾーンにログインし、以下のコマンドを実行する権限が必要です。
 - uname -a
 - sar
 - prstat
 - netstat

製品インストール中に、または NodeCfgUtil.exe ユーティリティを介して、CA Virtual Assurance へのこのユーザ名および対応するパスワードを、Solaris ゾーン AIM が存在する管理対象ノードに追加します。

LPAR 管理の要件

以下のコンポーネントがインストールされていることを確認します。

- HMC/IVM サーバへの接続が設定された Windows サーバ上の LPAR AIM を備えた SystemEdge
- 1 つ以上の電源システムに接続された HMC/IVM サーバ

sysedge.cf ファイルの編集による SNMPv1 トラップの設定

SystemEDGE¥data¥port<n> ディレクトリにある sysedge.cf ファイルには、SNMPv1 トラップ コミュニティの定義が含まれており、これが、SNMPv1 トラップ メッセージの送信先を SystemEDGE に指示します。SystemEDGE のインストール中に、または sysedge.cf ファイルの編集によって、トラップ送信先および SNMPv1 コミュニティを設定できます。任意の数の管理システムにトラップを送信するようにエージェントを設定できます。

sysedge.cf ファイルを編集して SNMPv1 トラップを設定する方法

1. SE_Install_Dir¥data¥port<num> ディレクトリ (Windows) または SE_Install_Dir/config/port<num> ディレクトリ (UNIX、Linux) に移動して、sysedge.cf ファイルのバックアップコピーを作成します。
2. テキスト エディタで sysedge.cf を開き、ファイルの上部でトラップ送信先セクションを見つけます。

トラップ送信先セクションには、トラップ送信先およびコミュニティの簡単な説明が含まれます。

3. SNMPv1 トラップを送信する管理システムごとに、トラップ送信先セクションの最後に行を追加します。構文は以下のとおりです。

```
trap_community community-name [IP-address | hostname] [port-number]
```

community-name

SNMP コミュニティを指定します (public や admin など)。

IP-address

(オプション) ターゲットシステムの IP アドレスを指定します。

デフォルト: 127.0.0.1

hostname

(オプション) ターゲットシステムの名前を指定します。

デフォルト: localhost

port-number

(オプション) トラップの送信先のポートを指定します。

デフォルト: 162

4. ファイルを保存して閉じます。
5. 以下のいずれかを実行します。
 - Windows サービスコントロールから **SystemEDGE** サービスを再起動して **SystemEDGE** を再起動し、変更をアクティブにします。
 - Windows コマンド プロンプトから以下のコマンドを実行して **SystemEDGE** を再起動し、変更をアクティブにします。

```
net stop sysedge
net start sysedge
```
 - UNIX または Linux 端末のウィンドウから以下のコマンドを実行して **SystemEDGE** を再起動し、変更をアクティブにします。

```
/etc/init.d/sysedge restart (Linux, Solaris)
/etc/init.d/sysedge restart (HP-UX)
/etc/rc.d/sysedge restart (AIX)
```

例

sysedge.cf に以下の行を追加して、**mycommunity** というコミュニティ名のトラップを 2 つのシステムに送信します。最初のシステムの IP アドレスは **192.168.5.26** です。2 番目のシステムはホスト **atlanta-noc** で、ポート番号 **1692** でリスンします。

```
trap_community mycommunity 192.168.5.26
trap_community mycommunity atlanta-noc 1692
```

注: **sysedge.cf** が定義するのは **SNMPv1** トラップ コミュニティのみです。**SNMPv2c** または **SNMPv3** トラップの設定の詳細については、**SE_Install_Dir¥doc** ディレクトリ (Windows) または **/opt/EMPSysedge/doc** ディレクトリ (UNIX、Linux) にインストールされた「**SystemEDGE ユーザ ガイド**」を参照してください。

イベント転送

このセクションでは、**SNMP** (簡易ネットワーク管理プロトコル) 管理サーバまたはサードパーティ **SNMP** 管理サーバにイベントを転送するように **CA Virtual Assurance** を設定する方法について説明します。

SNMP 用の Windows の設定

SNMP サービスおよび SNMP トラップ サービスは Windows と共にインストールされますが、典型的なセットアップの一部ではありません。SNMP サービスおよびトラップ サービスが実行されていることを確認してください。

SNMP 用に Windows を設定する方法

1. [スタート]-[コントロール パネル]-[管理ツール]-[サービス]をクリックします。
[サービス]ダイアログ ボックスが表示されます。
2. 以下のうち、1 つを指定します。
 - SNMP サービスと SNMP トラップ サービスがリストに含まれる場合は、[イベント転送]設定を続行します。
 - SNMP サービスと SNMP トラップ サービスがリストに含まれない場合は、手順 3 から続行します。
3. [スタート]-[コントロール パネル]-[プログラムの追加と削除]-[Windows コンポーネントの追加と削除]をクリックします。
[Windows コンポーネントウィザード]ダイアログ ボックスが表示されます。
4. リストを下へスクロールし、[管理とモニタ ツール]を選択して[次へ]をクリックします。
Windows インストール メディアを使用するよう求められます。
5. 画面上の指示に従って、インストールを実行します。
6. 手順 1 を繰り返して、SNMP サービスと SNMP トラップ サービスが実行されていることを確認します。

イベント転送のための CA Virtual Assurance の設定

CA またはサードパーティのイベント管理サーバにイベントを転送するために CA Virtual Assurance を設定します。

イベント転送のために CA Virtual Assurance を設定する方法

1. CA Virtual Assurance ユーザ インターフェースを開きます。
2. [管理]をクリックします。
[管理]ページが表示されます。
3. [設定]をクリックします。
[設定]ページが表示されます。
4. 左側のペインで[イベント]をクリックします。
[イベント]ペインが表示されます。
5. [+] (追加)をクリックします。
[転送]および[タイプ]フィールドが自動的に入力されています。

注: これらのフィールドが入力されていない場合は、Apache Tomcat を再起動してください。

6. [タイプ]ドロップダウンリストで **SNMP v1** または **v3** を選択して、次に[転送]ドロップダウンリストで[有効]を選択します。

SNMP v3トラップを選択した場合は、追加の設定パラメータ用のパネルが表示されます。
7. [サーバ]フィールドに管理サーバの名前を入力します。
8. SNMP 用の別のポート番号を入力するか、デフォルトポート **162** (自動的に入力されている)のままにします。
 - SNMP v3 を選択した場合は、手順 9 から続行します。
 - SNMP v1 を選択した場合は、手順 13 にスキップします。

9. ドロップダウンリストで[セキュリティレベル]を選択します。有効なオプションは、以下のとおりです。

NoAuthNoPriv

追加のセキュリティパラメータはありません。

AuthNoPriv

認証設定のみ。

AuthPriv

認証と暗号化。

10. [ユーザ名]フィールドにリモート管理サーバのユーザ名を入力します。
11. ドロップダウンリスト内のオプションから認証プロトコルを選択し、パスワードを指定します。

MD5

128 ビット ハッシュ値を備えたメッセージダイジェスト アルゴリズム 5 (MD5) 暗号ハッシュ関数を定義します。

SHA

セキュア ハッシュ アルゴリズム (SHA) 暗号ハッシュ関数を定義します。

注: このオプションは、セキュリティレベル **AuthNoPriv** および **AuthPriv** にのみ有効です。

12. ドロップダウンリストで[暗号化プロトコル]を選択します。有効なオプションは DES と AES です。パスワードを指定します。

注: このオプションは、セキュリティレベル **AuthPriv** にのみ有効です。

13. [OK]をクリックします。

確認メッセージが表示されます。

14. [保存]をクリックして、更新されたイベント転送レコードを保存します。

設定が更新されて、設定情報が表示されます。これで、CA Virtual Assurance が、イベントを転送するように設定されました。

SNMP V3 エンジン ID

SNMPv3 標準では、各エンジン(トラップ送信者)に ID が必要です。各管理プラットフォーム(ターゲットアプリケーション)は、エンジン ID を異なる方法で認識します。CA Virtual Assurance など、一部の管理プラットフォームでは、実際の 16 進数のエンジン ID が正しく設定されている必要があります。

CA Virtual Assurance の場合は、16 進数のエンジン ID が、コンピュータ名と文字列 DCAMTrap の組み合わせをシードとして使用して構築されます。たとえば、コンピュータ名が COMP999 の場合、エンジン ID のシードは COMP999-DCAMTrap です。CA Virtual Assurance は、アルゴリズムでシードを使用してエンジン ID を計算します。コンピュータ名は、一意性を確保するために使用されます。16 進数値は、CA Virtual Assurance インストール ディレクトリの下 の出力ファイルに書き込まれます。このファイルの名前は dem_snmp3_engine_id.dat です。このファイルは、別の管理サーバにイベントを転送するように CA Virtual Assurance を設定した後に作成されます。

第 5 章: リソースの管理

このセクションには、以下のトピックが含まれています。

[マネージャ コンポーネント](#) (P. 61)

[リソースの検出](#) (P. 64)

[管理対象の仮想環境](#) (P. 72)

[Cisco UCS の概要](#) (P. 106)

[複数のマルチインスタンス AIM の使用](#) (P. 114)

[システム管理](#) (P. 114)

マネージャ コンポーネント

CA Virtual Assurance は、モニタする環境を管理し、そのプラットフォーム上でアクションを実行する機能を提供します。データコレクタは、すべてのサーバーエージェントのモニタリングとしきい値の設定を制御します。プラットフォーム管理モジュール (PMM) は、SNMP を使用してすべての管理対象システム上のデータコレクタをポーリングする Web サービスです。PMM は、データコレクタから受信した MIB のオブジェクト値やトラップを含むすべての情報を CA Virtual Assurance のアーキテクチャに適合するプロパティに変換し、データベース内に対応する管理対象オブジェクトの表現を作成します。各 PMM は特定の仮想プラットフォーム専用です。コマンドを実行すると、PMM は関連する AIM にアクションの実行を指示します。

関連項目

[Application Insight Module \(AIM\)](#) (P. 62)

[モニタの設定](#) (P. 63)

Application Insight Module (AIM)

Application Insight Module (AIM) は、アプリケーション固有のイベントとプロセスをモニタおよび管理する機能を追加します。AIM は SystemEDGE の機能拡張です。

VMware vCenter Server 用の AIM

VMware vCenter Server の管理下にあるシステムを管理およびモニタする機能を提供します。この AIM は、SystemEDGE がインストールされている任意の Windows システムで実行できます。AIM は vCenter Server ソフトウェアと通信して、関連付けのある VMware vCenter Server が管理するすべての ESX サーバの全体ビューを取得します。

IBM PowerVM 用の AIM (LPAR)

LPAR を含むシステム全体を管理およびモニタする機能を提供します。この AIM は、SystemEDGE がインストールされている任意の Windows システムで実行できます。AIM は Secure Shell (SSH) 接続を介して HMC/IVM と通信します。したがって、関連付けられた HMC/IVM システムを介して POWER システム上の LPAR と通信できます。HMC/IVM システム、および AIM が実行されている Windows サーバで、SSH が有効になっていることを確認してください。

Microsoft Hyper-V 用の AIM

Microsoft Hyper-V 環境を管理およびモニタする機能を提供します。Hyper-V サーバ用の SystemEDGE AIM は、Hyper-V サーバで実行されます。

Microsoft Cluster Service 用の AIM

Microsoft のクラスタをモニタする機能を提供します。この AIM は、SystemEDGE がインストールされている任意の Windows システムで実行できます。Microsoft Cluster Service と通信して、モニタ対象のクラスタ、ノード、サービス、およびアプリケーションの全体ビューを取得します。

Solaris ゾーン用の AIM

ゾーンを実行するように設定された Solaris 10 システムを管理およびモニタする機能を提供します。この AIM は、SystemEDGE がインストールされている任意の Windows システムで実行できます。SSH 接続を介して、管理対象の Solaris ゾーンサーバと通信します。管理対象の Solaris サーバ、および AIM が実行されている Windows サーバで、SSH が有効になっていることを確認してください。

Cisco Unified Computing System (UCS)用の AIM

CA Virtual Assurance は Cisco UCS と対話して、デバイスを照会し、統計情報を収集します。Cisco UCS は、各種リソースを異種システムとして管理するのではなく、ネットワーク、ハードウェア、ストレージ、および仮想化の各リソースを 1 つの連携システムに統合します。

サービス レスポンス モニタ用の AIM

Windows、UNIX、または Linux サーバで実行されているサービスの健全性と応答性をモニタする機能を提供します。

リモート モニタリング用の AIM

リモート(エージェントレス) Windows システムを管理およびモニタする機能を提供します。

Exchange Server および Active Directory 用 AIM

クラウドおよび社内運用の両方のインフラストラクチャ上の Exchange Server および Active Directory をモニタする機能を提供します。AIM によって、ドメインおよび Exchange Server の管理、保守、およびアップグレードを実施できます。

関連項目

[環境の検出](#) (P. 44)

モニタの設定

仮想リソースまたは仮想属性をモニタするかどうかを指定するには、そのモニタ状態を変更します。オブジェクトを選択して、その設定を管理対象外に変更すると、PMM は要求を処理し、AIM で値を管理対象外に設定します。現在のモニタ設定は MIB 属性に保持され、子オブジェクトも管理対象外に変更されます。トラップは、親の設定変更と状態変更に関して生成されます。その後のポーリングおよび記録サイクルで親オブジェクトとその子のトラップは生成されません。

オブジェクトを選択して、その設定を管理対象に変更すると、PMM は要求を処理し、AIM でその値を管理対象に設定します。現在のモニタ設定は MIB 属性に保持され、子オブジェクトも管理対象に変更されます。設定変更トラップは親に関して生成されます。次のポーリングおよび記録サイクルで親オブジェクトとその子の状態が評価され、必要に応じて状態変更トラップが生成されます。

関連項目:

[リソースの管理](#) (P. 68)

リソースの検出

管理するサーバまたはサブネット全体を検出して追加できます。データセンターに追加された、以前は管理対象外であったサーバまたは新しいサーバは、検出可能です。

注: CA Virtual Assurance ディスカバリには、ホスト名解決が必要です。検出されたサーバの IP アドレスが変わった場合は、IP アドレスが CA Virtual Assurance で自動的に解決されません。その結果、ディスカバリプロファイルで管理データベースが更新されません。IP アドレスが変わった場合は、サーバを再検出してください。

システムの検出

検出、管理、およびサービスへの割り当て(オプション)の対象となる単一のシステムを指定できます。

注: SystemEDGE または CA Performance Lite Agent は HMC/IVM サーバにインストールできません。したがって、IBM Power Series サーバについて HMC/IVM システム データを収集することはできません。管理ガイドの「リソースの設定」の章も参照してください。

システムを検出する方法

1. [リソース]-[管理]-[システムの検出]を選択します。

2. 以下のフィールドを指定します。

システム名

サーバの名前または IP アドレスを指定します。

3. (オプション) [次へ] をクリックします。
[拡張ディスカバリおよび SNMP 情報] ダイアログ ボックスが表示されます。
4. (オプション) [拡張ディスカバリ] を有効にして、SoftAgent 技術を使用した詳細な検出が実行されるようにします。
5. (オプション) [SNMP デフォルトを上書きする] を有効にして、SNMP 情報を使用した詳細なディスカバリが実行されるようにします。
6. [終了] をクリックします。

システムが検出されると、成功のメッセージが表示されます。検出されたサーバは自動的に管理されますが、サブネット ディスカバリ内のサーバは管理されません。

ネットワークの検出

検出対象となるネットワークのセグメントを指定できます。ネットワーク検出する IP アドレスをユーザ インターフェースで指定するときは、CIDR (Classless Inter-Domain Routing) 表記法を使用します。この表記法は以下の例に示すとおり、アドレスと、サブネット プレフィックスとして使用するビットの数で構成されます。

172.24.143.0/24

ワイルドカードと範囲を使用することもできます。

172.24.143.*

172.24.143.{1-255}

ネットワークを検出する方法

1. [リソース]-[管理]-[ネットワークの検出] をクリックします。

2. 以下のフィールドを指定します。

ネットワーク名

ネットワークの名前を指定します。

ネットワークアドレス

ネットワーク IP アドレスを指定します。このフィールドにカーソルを置くと、アドレスの例が表示されます。

除外アドレス

(オプション) ディスカバリから除外するネットワークアドレスを指定します。

3. [ディスカバリ方法]の以下のオプションから **1** つを選択して、対応するフィールドに入力します。

Ping スweep

ネットワーク内の IP アドレスをすべて検出します。

DNS

ドメイン ネーム システム (DNS) サーバに登録されているホスト名を検出します。ドメイン名と DNS サーバ名を各フィールドに入力します。

4. (オプション) [次へ] をクリックします。
[拡張ディスカバリおよび **SNMP 情報**] ダイアログ ボックスが表示されます。
5. (オプション) [拡張ディスカバリ] を有効にして、**SoftAgent** 技術を使用した詳細な検出が実行されるようにします。
6. (オプション) [**SNMP デフォルトを上書きする**] を有効にして、**SNMP 情報** を使用した詳細なディスカバリが実行されるようにします。
7. [終了] をクリックします。

ネットワークが検出されると、成功のメッセージが表示されます。検出されたサーバは自動的に管理されますが、サブネット ディスカバリ内のサーバは管理されません。

ネットワークの削除

検出済みのネットワークを削除できます。ただし、すでに検出済みのシステムはそれらのステータスを保持します。

ネットワークを削除する方法

1. [リソース]-[管理]-[検出されたネットワークの管理]を選択します。
検出されたネットワークのリストが、右ペイン内に表示されます。
2. 削除するネットワークを選択し、[ネットワークリスト]ツールバーで[-] (削除) をクリックします。
確認のためのメッセージが表示されます。
3. [OK]をクリックします。
ネットワークはネットワークリストから削除されます。

ネットワーク ディスカバリのキャンセル

進行中のネットワーク ディスカバリはキャンセルできます。

ネットワーク ディスカバリをキャンセルする方法

1. [リソース]をクリックし、[管理]ペインを開きます。
2. [管理]セクションで[検出されたネットワークの管理]をクリックします。
3. ディスカバリをキャンセルする進行中のネットワークを選択し、[ネットワークリスト]ツールバーで[-] (キャンセル) をクリックします。
選択したネットワークのディスカバリをキャンセルするかどうかを確認するメッセージが表示されます。

リソースの管理

検出済みのリソースは、管理対象リソースのリストに追加することにより、パフォーマンスをモニタできます。

リソースを管理する方法

1. [リソース]をクリックし、[管理]ペインを開きます。
2. [管理]セクションで[システムの管理]をクリックします。
3. ドロップダウンリストから[管理対象外サーバ]を選択します。

管理対象外リソースのリストが表示されます。

4. 管理するリソースを選択し、[アクション]ドロップダウンメニューで[管理]をクリックします。

リソースを管理対象にするかどうかを確認するメッセージが表示されます。

5. [管理対象]フォルダを展開します。

リソースが[管理対象]リスト内に表示されます。また、メトリック収集が次の記録サイクルで開始されます。

サービスの作成

モニタするサーバを、ビジネス ニーズでの必須リソースを反映する論理サービスにまとめることができます。

サービスを作成する方法

1. [リソース]をクリックし、[エクスプローラ]ペインを開きます。
2. [データ センター]または[CA Virtual Assurance サービス]などの親サービスノードを選択します。
3. [管理]を右クリックし、[新しいサービス]をクリックします。

[サービス: 新規]ダイアログ ボックスが表示されます。

4. [サービス名]フィールドに新規サービスの名前を入力し、[サービスの優先度]フィールドで優先度レベルを設定します。

注: サービス名では以下の文字はサポートされていません: % " ' < > / ¥ : ` ~ ;

サービスの優先度

1 回のポーリング サイクルでアクションを実行する順序を指定します。

例:

ServiceA: 優先度 3

ServiceB: 優先度 1

ServiceC: 優先度 2

それぞれのルールがすべて **true** として評価された場合、アクションは ServiceB、ServiceC、ServiceA の順序で実行されます。

5. 遅延回数を変更するか、または表示されるデフォルトを受け入れます。

遅延

アクションをトリガする前に、ルールが **True** と評価される必要がある頻度を定義します。

6. 下限しきい値と上限しきい値のパーセンテージを変更するか、またはデフォルトを受け入れます。

下限および上限しきい値(%)

サービス全体の下限および上限しきい値を指定します。

制限: サービスレベルでは全体的な使用率メトリックのみを評価できません。

7. サービスを **CCA** サーバに割り当てることができます。サーバの同じリストを持つ **CCA** サービスが自動的に作成されます。

注: CCA サーバが検出しないサーバは CCA サービスに追加されません。問題が発生していないかどうかをイベントテーブルで確認します。

また、サービス内のすべてのサーバに適用される管理プロファイルも選択できます。

8. [サーバ]セクションの[利用可能なサーバ]リストから新規サービスのサーバを選択し、右向き矢印をクリックします。

注: 利用可能なサーバのリストが長い場合は、リストをフィルタしてサーバのセットを減らします。これを行うには、[フィルタ]矢印をクリックし、フィルタ条件を入力して[検索]をクリックします。

サーバが[選択済みサーバ]セクションに移動します。

9. [アクション]ドロップダウンメニューで[保存]をクリックします。

新しいサービスが保存され、[エクスプローラ]ペインに表示されます。

サービスレベルで、スナップショットの作成、コンポーネントの表示、ディスクカバリまたは変更の検出を実行できます。サービスを右クリックし、関連するオプションを選択します。

サービスの編集

既存のサービスを編集して、名前の変更、設定の変更、またはグループに対するリソースの追加または削除を行うことができます。

サービスを変更する方法

1. [リソース]をクリックし、[エクスプローラ]ペインを開きます。
2. サービスを選択し、[管理]を右クリックして、[サービスの編集]をクリックします。

[サービス: 編集]ダイアログ ボックスが表示されます。

3. 必要に応じて、[サービスの優先度]フィールドで優先度レベルを、または下限しきい値および上限しきい値のパーセンテージを変更します。

サービスの優先度

1 回のポーリング サイクルでアクションを実行する順序を指定します。

例:

ServiceA: 優先度 3

ServiceB: 優先度 1

ServiceC: 優先度 2

それぞれのルールがすべて **true** として評価された場合、アクションは **ServiceB**、**ServiceC**、**ServiceA** の順序で実行されます。

- 遅延の発生頻度を変更するか、またはデフォルトを受け入れます。

遅延

アクションをトリガする前に、ルールが **True** と評価される必要がある頻度を定義します。

下限および上限しきい値(%)

サービス全体の下限および上限しきい値を指定します。

制限: サービスレベルでは全体的な使用率メトリックのみを評価できません。

- サービスに追加するサーバを[サーバ]セクションの[利用可能なサーバ]リストから選択し、次に、右向き矢印をクリックします。

注: 利用可能なサーバのリストが長い場合は、リストをフィルタしてサーバのセットを減らします。これを行うには、[フィルタ]矢印をクリックし、フィルタ条件を入力して[検索]をクリックします。

サーバが[選択済みサーバ]セクションに移動します。

- サービスから削除するサーバを[サーバ]セクションの[選択済みサーバ]リストから選択し、次に、左向き矢印をクリックします。

サーバは[選択済みサーバ]セクションから[利用可能なサーバ]セクションに移動します。

- [保存]をクリックします。
[サーバ]リストが更新されます。

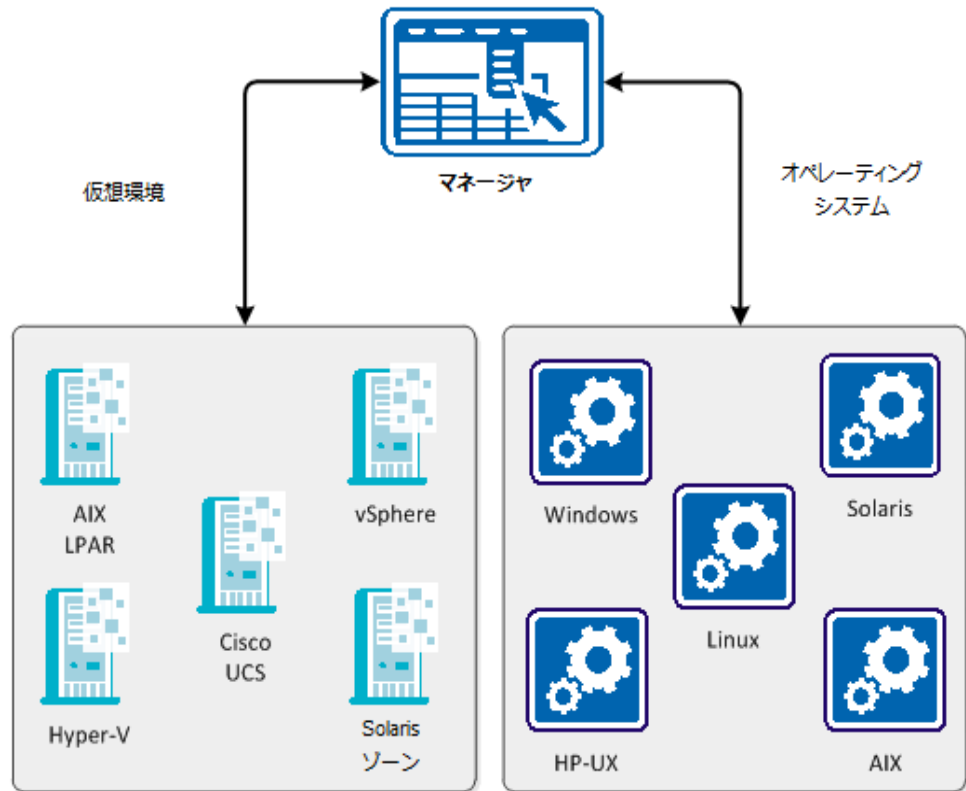
管理対象の仮想環境

CA Virtual Assurance は、仮想環境を管理するために設計されていますが、Linux、UNIX、または Windows オペレーティングシステムを実行するホストの検出と管理も行います。以下のリストは、この製品の管理機能の概要についての説明です。

- vCenter Server、Solaris ゾーン、Hyper-V、Cisco UCS、および LPAR 環境の管理。必要な CA Virtual Assurance コンポーネントは、1 つ以上の Windows ホスト(個別の Windows AIM サーバまたは CA Virtual Assurance マネージャ)上にあります。これらのホストで必要なコンポーネントは次のとおりです。
 - vCenter Server、Solaris ゾーン、Hyper-V、Cisco UCS、または LPAR 用の Application Insight Module (AIM)
 - SystemEDGE
- AIX、HP-UX、Linux、Solaris、または Windows オペレーティングシステムを実行するホストの管理。これらのホストで推奨されるコンポーネントは次のとおりです。
 - SystemEDGE、Advanced Encryption、リモート モニタリング AIM (Windows サーバのみ)、サービスレスポンス モニタリング (SRM) AIM

注: プラットフォーム固有の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。

仮想環境とオペレーティング システム



関連項目

[VMware vCenter Server](#) (P. 74)

[Solaris ゾーン](#) (P. 90)

[Microsoft Hyper-V Server](#) (P. 92)

[IBM PowerVM \(LPAR\)](#) (P. 94)

[Microsoft Cluster Service](#) (P. 100)

[Cisco UCS](#) (P. 103)

VMware vCenter Server

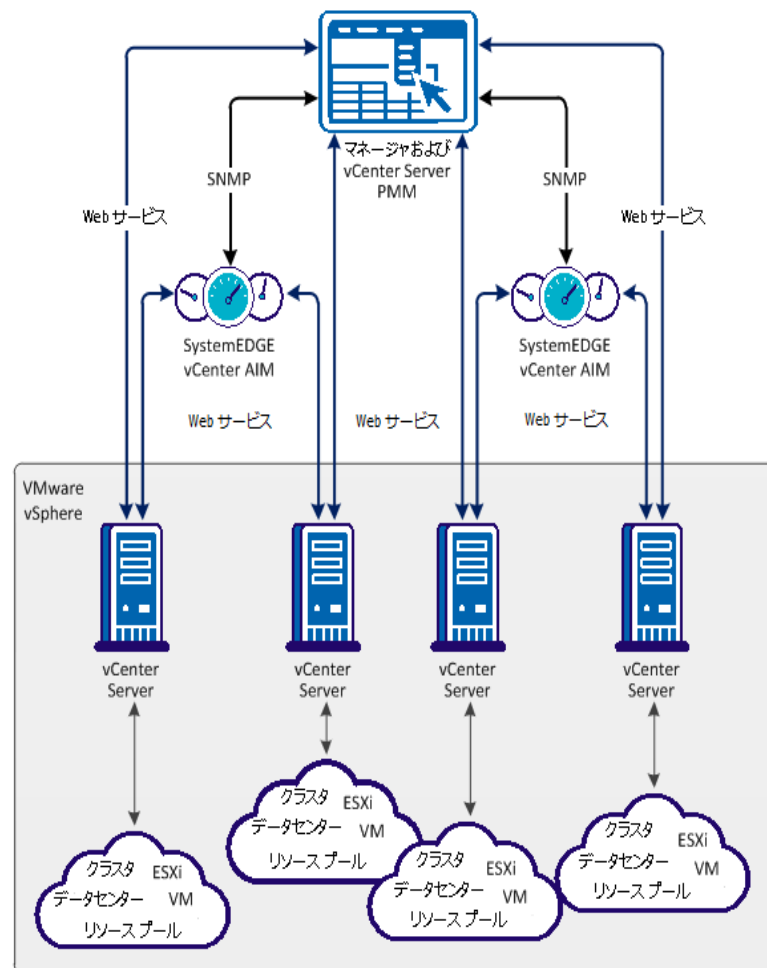
VMware vCenter Server は、仮想化された IT 環境の設定、プロビジョニング、および管理を集中管理する場所を提供します。SystemEDGE と VMware vCenter Server 用の AIM は、CA Virtual Assurance マネージャ サーバまたは任意の Windows サーバ上で実行されます。この AIM は、Web サービスを使用して 1 つ以上の VMware vCenter Server とリモート通信し、SNMP を使用してマネージャ サーバ上の vCenter Server PMM とリモート通信します。

VMware vCenter Server PMM は、接続およびすべての VMware vCenter Server 操作の運用上のサポートを提供します。PMM は、接続の管理、VM 関連操作の実行、VMware vCenter Server から取得したデータのデータベースへの入力を行います。プロビジョニング サービスは、クローニング、電源操作、リソースおよび共有の調整などの VMware vCenter Server 操作を実行します。

vCenter Server 管理コンポーネント間のインタラクション

以下の図は、vCenter Server 管理に関与するコンポーネントがどのように対話するかを示しています。SystemEDGE と vCenter Server AIM は、1 つの Windows サーバ上で実行する必要があります。この AIM は、1 つ以上のリモート vCenter Server と通信して、仮想環境を管理します。vCenter Server AIM はデータを収集し、vCenter Server と関連付けられた物理および仮想リソースをすべて表示します。

vCenter Server 管理コンポーネント間のインタラクション



インストール中に、またはユーザ インターフェースの[管理]タブを使用して vCenter Server 管理を設定できます。

注: VMware ツールは、VM の仮想化を最適化します。このツールを VMware 環境内の各 VM にインストールすることをお勧めします。VMware ツールがインストールされていない VM では、この製品の一部の機能が利用できないか、または正常に機能しません。この理由により、VMware ツールがインストールされていない VM はサポートされていません。

関連項目

[複数の vCenter AIM の管理](#) (P. 51)

リモートおよびマルチインスタンスの vCenter Server サポート

vCenter Server AIM は、1 つ以上の vCenter Server インスタンスと通信します。ただし、複数のリモート vCenter Server AIM を持つ CA Virtual Assurance マネージャを使用して複数の vCenter 環境を管理する場合は、以下を考慮してください。

- 各 vCenter Server が、1 つの AIM と一意に関連付けられていることを確認します。
- CA Virtual Assurance マネージャのユーザ インターフェースで[管理]を使用して、または適切な AIM サーバで NodeCfgUtil を使用して、あいまいな関連付けをすべて削除します。

複数の AIM が特定の vCenter Server を管理している場合は、管理、ディスカバリ、またはモニタリングに関する問題が発生する可能性があります。

注: eHealth、Spectrum Infrastructure Manager、または NSM 環境で CA Virtual Assurance マネージャを使用せずに vCenter Server AIM を実行した場合、AIM はシングル インスタンス モードのみをサポートします。

VM のホットプラグ サポート

CA Virtual Assurance は、VM でホットプラグ オプションが有効かどうかを検出します。CA Virtual Assurance は、VM の電源がオンのときに、ホットプラグ対応 VM の以下の調整をサポートします。

- vCPU の追加
- vRAM の追加

注: ホットプラグ オプションを有効または無効にする方法については、「VMware vSphere 仮想マシン管理ガイド」を参照してください。

VM のデバイス管理

デバイス管理には、以下が含まれます。

- vDisk の追加と削除
- vNIC の追加と削除

vNetwork 標準スイッチ (vSwitch)

CA Virtual Assurance は、抽出されたネットワーク デバイスである標準 vSwitch のポリシーおよびプロパティをモニタします。vSwitch で、VM 間のトラフィックを内部的にルーティングして、外部ネットワークにリンクできます。vSwitch によって、複数のネットワーク アダプタの帯域幅を組み合わせ、それらの間の通信トラフィックのバランスが調整されます。vSwitch で、物理 NIC フェールオーバーを処理できます。

vSwitch で、物理イーサネット スイッチがモデル化されます。デフォルトの vSwitch 用論理ポート番号は 120 です。VM の 1 つのネットワーク アダプタを各ポートに接続できます。vSwitch と関連付けられた各アップリンク アダプタは、1 つのポートを使用します。vSwitch 上の各論理ポートは、単一のポートグループのメンバです。各 vSwitch には、1 つ以上のポートグループを割り当てることもできます。2 つ以上の VM を同じ vSwitch に接続すると、それらの間のネットワークトラフィックはローカルにルーティングされます。アップリンク アダプタが vSwitch に付けられている場合は、アダプタが接続された外部ネットワークに各 VM がアクセスできます。

分散仮想スイッチ(DVS)

CA Virtual Assurance は、vSphere 環境で、以下の分散仮想スイッチをサポートします。

- VMware vNetwork 分散スイッチ (vDS、vSphere コンポーネント)
- Cisco Nexus 1000V スイッチ (vSphere と統合)

CA Virtual Assurance は、vSphere 環境の分散仮想スイッチを検出し、イベントを介して、そのポリシーとプロパティをモニタします。CA Virtual Assurance VM プロビジョニングでは、vNetwork 分散スイッチおよび Cisco Nexus 1000V スイッチがサポートされます。

DVS は、それに関連付けられているすべてのホストにわたる 1 つの仮想スイッチとして動作します。DVS は、これらのホスト用の同じスイッチ (同じ名前、同じネットワーク ポリシー) およびポート グループを表します。これらのプロパティは複数のホスト間でマイグレートされるため、VM で、一貫したネットワーク設定を維持できるようになります。

各 DVS は、vNetwork 標準スイッチと同様に、VM が使用できるネットワーク ハブです。DVS は、VM 間で内部的にトラフィックを転送するか、物理 NIC (アップリンク アダプタ) に接続して外部ネットワークにリンクすることができます。

分散仮想ポートグループ (dvPort グループ) は、DVS と関連付けられたポートグループであり、各メンバーポートのポート設定オプションを指定します。dvPort グループは、DVS によるネットワークへ接続方法を定義します。

分散仮想アップリンク (dvUplinks) は、ESX または ESXi のホスト上で、物理 NIC (vmnics) のある程度の抽象化を提供します。各物理 NIC は、1 つの dvUplink にマップされます。dvPort グループから dvUplink へのマッピングは、VM が、DVS によるネットワークへのアクセスに使用するの、ESX または ESXi のホスト上のどの物理 NIC であるかを定義します。

Cisco Nexus 1000V スイッチは、Virtual Ethernet Module (VEM) と Virtual Supervisor Module (VSM) で構成されています。Cisco Nexus 1000V スイッチに関連付けられた各 ESX または ESXi ホストでは、VEM が VMware vSwitch の代わりにハイパーバイザ カーネル内でモジュールとして実行されます。VSM は、1 つの論理的なスイッチとして複数の VEM を制御し、ESX または ESXi のホスト上の VM 内で動作します。

詳細については、<http://pubs.vmware.com> にある VMware vNetwork 分散スイッチのマニュアルまたは <http://www.cisco.com/go/1000vdocs> にある Cisco Nexus 1000V スイッチのマニュアルを参照してください。

注: Cisco Nexus 1000V スイッチを使用する場合は、VSM VM が、CA Virtual Assurance ユーザ インターフェイスに特殊な VM として表示されません。VSM VM に適用するルールおよびアクションが Cisco Nexus 1000V スイッチに影響しないことを確認してください。

イベントによる分散仮想スイッチのモニタリング

以下のイベントで分散仮想スイッチをモニタできます。

- スイッチの追加:

分散仮想スイッチ VM-dvSwitch がデータセンター MyDC に追加されました。
vSphere: vcserver.mycomp.com

- スイッチの削除:

分散仮想スイッチ VM-dvSwitch がデータセンター MyDC から削除されました。
vSphere: vcserver.mycomp.com

- ポートグループの追加:

分散仮想ポートグループ VM dvPortGroup が仮想分散スイッチ VM-dvSwitch に追加されました。データセンター: MyDC、vSphere: vcserver.mycomp.com

- ポートグループの削除:

分散仮想ポートグループ VM dvPortGroup が仮想分散スイッチ VM-dvSwitch から削除されました。データセンター: MyDC、vSphere: vcserver.mycomp.com

- アップリンクの追加:

分散仮想アップリンク VM DVUplink が分散仮想スイッチ VM-dvSwitch に追加されました。データセンター: MyDC、vSphere: vcserver.mycomp.com

- アップリンクの削除:

分散仮想アップリンク VM DVUplink が分散仮想スイッチ VM-dvSwitch から削除されました。データセンター: MyDC、vSphere: vcserver.mycomp.com

イベントで分散仮想スイッチをモニタする方法

1. [ダッシュボード]タブをクリックし、[イベント]パネルまでスクロールして、[テーブル フィルタを表示]アイコンをクリックします。
[フィルタ]パネルが表示されます。
2. モニタする分散仮想スイッチ イベント用の適切なフィルタを指定して、[適用]をクリックします。
[イベント]パネルに、フィルタされたイベントのリストが表示されます。

vApp のサポート

vApp は、VM の集合を 1 つの単位として扱う特殊なリソースプールです。vApp は Open Virtualization Format (OVF)を使用します。OVF は、多層アプリケーションのすべてのコンポーネントと、アプリケーションに関連付けられた運用ポリシーおよびサービスレベルを規定し、カプセル化するための標準です。CA Virtual Assurance は vApp 上で操作を実行できます。vApp 上の操作は vApp 内のすべての VM にプロパゲートされます。

任意の vApp を小さくパーティション分割することで、特定のグループや特定の目的のためにリソースを分割して割り当てることができます。VM、リソースプール、または vApps のようなリソースを既存の vApp に追加できます。また、vApp を階層的に構成して、ネストすることもできます。

CA Virtual Assurance は、vApp に対する以下の操作をサポートします。

- VMware vApp のプロビジョニング
- リソースの追加
- vApp のクローン作成
- vApp の電源オン
- vApp の電源オフ
- vApp の中断
- VMware vCenter からの削除
- VMware vCenter からの登録解除

イベントによる vApp のモニタリング

以下のイベントで vApp をモニタできます。

- vApp の追加:

vApp *MyvApp* が親リソース プールのリソースに追加されました。vSphere
vcserver.mycomp.com

- vApp の削除:

vApp *MyvApp* が親リソース プールのリソースから削除されました。vSphere,
vcserver.mycomp.com

以下のトラップを使用できます。

- ResPoolvAppAddedTrap: vApp をリソース プールまたは vApp に追加します。
- ResPoolvAppRemovedTrap: vApp をリソース プールまたは vApp から削除します。
- ResPoolvAppVConfigChangeTrap: vApp 内の vApp エンティティの設定データが変更されました。
- VMAddedTovAppTrap: VM が vApp に追加されました。
- VMRemovedFromvAppTrap: VM が vApp から削除されました。
- VMvAppVConfigChangeTrap: vApp 内の VM エンティティの設定データが変更されました。

イベントで vApps をモニタする方法

1. [ダッシュボード]タブをクリックし、[イベント]パネルまでスクロールして、[テーブル フィルタを表示]アイコンをクリックします。
[フィルタ]パネルが表示されます。
2. モニタする vApp イベント用の適切なフィルタを指定して、[適用]をクリックします。
[イベント]パネルに、フィルタされたイベントのリストが表示されます。

クラスタ内の vCenter Server

vCenter Server がクラスタ内に存在する場合、vCenter Server AIM はこのクラスタの外部で実行される必要があります。クラスタ ホストを指すように vCenter Server AIM を設定します。vCenter Server が正常に起動すると、AIM がフェールオーバーを検出でき、その内部キャッシュに再度読み込みを行います。

フォールトトレランス

VMware vSphere では、高可用性 (HA) のために設定されたクラスタに定義された VM 上でフォールトトレランス (FT) を有効にすることができます。フォールトトレランスは、クラスタ内の別の ESX サーバ上でセカンダリ VM を作成します。セカンダリ VM は、ワークロードを実行しているプライマリ VM とのロックステップモードで作動します。障害が発生した場合は、セカンダリ VM が、すぐに障害発生時点からワークロードの実行を引き継ぎます。CA Virtual Assurance は、クラスタ内のプライマリおよびセカンダリ VM を検出して管理します。

VM 管理に関しては、CA Virtual Assurance が、プライマリおよびセカンダリ VM を単一の VM として扱い、フォールトトレランスを有効にして、そのフォールトトレランスプロパティを表示します。プライマリ VM が左側のペイン (最初のクラスオブジェクト) に表示され、その FT プロパティが右側のペインに表示されます。セカンダリ VM のプロパティ (2 番目のクラスオブジェクト) は、右側のペインにのみリスト表示されます。セカンダリ VM 上では、起動、停止、クローンなどの VM 操作を実行できません。

[一般情報] パネルに表示された VM の数は、実行中の非 FT VM とプライマリ FT VM の数に基づいています。セカンダリ FT VM は、VM の全体の合計数には含まれていません。

CA Virtual Assurance は、環境内のさまざまなレベルで FT VM データを収集します。

フォールトトレランスの要件

VM がフォールトトレラントである場合は、以下の操作が無効である必要があります。

- VM のクローン作成
- インベントリから削除します (登録解除)
- スナップショット
- テンプレートに変換します

VM のフォールトトレランス プロパティ

CA Virtual Assurance では、各 VM について、以下が表示されます。

フォールトトレランス ステータス

VM フォールトトレランス ステータスを示します。

フォールトトレラントでない

VM がフォールトトレラントではないことを示します。

保護されています

VM がフォールトトレラントであり、保護されていることを示します。

保護されていない (起動中)

フォールトトレランスが起動中であり、VM が保護されていないことを示します。

保護されていない (セカンダリ VM が必要)

フォールトトレランスが有効であるが、セカンダリ VM を必要とすることを示します。

保護されていない (無効)

フォールトトレランスが無効であり、VM が保護されていないことを示します。

保護されていない (VM が実行されていない)

フォールトトレランスが有効であるが、VM が実行されていないことを示します。

セカンダリの場所

セカンダリホストの場所を識別します。

ESX ホストのフォールトトレランス属性

ESX ホストのフォールトトレランス属性は以下のとおりです。

フォールトトレランス

ホストでフォールトトレランスが有効になっているかどうかを識別します。

フォールトトレランス バージョン

ホスト上で実行中のフォールトトレランスのバージョンを識別します。

注: 相互の互換性があるのは、フォールトトレランスのバージョンが同じであるホストのみです。

プライマリ VM の合計 (AIM で計算)

このホストに設定されたプライマリ VM の総数を示します。

セカンダリ VM の合計 (AIM で計算)

このホストに設定されたセカンダリ VM の総数を示します。

電源オン プライマリ VM (AIM で計算)

このホスト上で実行中 (電源がオン) のプライマリ VM の総数を示します。

電源オン セカンダリ VM (AIM で計算)

このホスト上で実行中 (電源がオン) のセカンダリ VM の総数を示します。

VM での論理ボリューム管理

CA Virtual Assurance は、仮想ディスクの論理ボリュームの管理をサポートします。たとえば、VM で C: ドライブを管理できます。

VMware vCenter Server アーキテクチャ

以下の主要コンポーネントが VMware vCenter Server アーキテクチャに含まれます。

VMware vCenter Server

仮想化された IT 環境の設定、プロビジョニング、管理を制御するための中心点を提供します。vCenter Server は、Microsoft Windows プラットフォーム上でサービスとして実行されます。

注: vCenter Server のシステム要件については、リリース ノートを参照してください。

データベース

vCenter Server で管理される物理サーバ、リソース プール、データ センター、および仮想マシンに関する永続的な情報を格納します。

VMware vCenter Server エージェント

vCenter Server を備えた ESX サーバに接続します。

仮想インフラストラクチャ クライアント

任意の Windows コンピュータから vCenter Server または個別の ESX サーバへのリモート接続を提供します。

仮想インフラストラクチャ Web アクセス

クライアントのインストールなしで、vCenter Server に接続します。

この環境で CA Virtual Assurance AIM は、仮想化された環境のコンポーネント間の論理的および物理的な関係を検出します。AIM は、仮想化された環境全体を表示します。

vCenter Server 用 AIM は、以下のリソースタイプをモニタします。

vCenter Server

vCenter Server コンピュータのヘルス状態に関する情報を提供します。たとえば、CPU、データストア、およびメモリ使用率に関するステータスおよびデータが提供されます。

データセンター

ホスト、仮想マシン、リソース プール、またはクラスタのコンテナとして機能します。仮想設定が特定の部門の要件を満たす場合は、データセンターで組織構成を表すことができます。また、データセンターを使用して、テストまたは組織の目的のための分離された仮想環境を築くこともできます。

ESX ホスト

ESX サーバが実行される物理サーバの計算およびメモリリソースをすべて表します。

リソース プール

単一のホストまたはクラスタの物理的な計算およびメモリリソースのパーティションを定義します。任意のリソース プールをより小さなリソース プールに分割して、特定のグループや特定の目的のためにリソースを分割して割り当てることができます。また、リソース プールを階層構造で整理したり、ネストしたりすることもできます。

仮想マシン

ゲスト オペレーティング システムおよびアプリケーションが実行可能な仮想化された x86 環境を指定します。仮想マシンを作成すると、特定のホスト、クラスタ、またはリソース プールに割り当てられ、さらにデータストアに割り当てられます。仮想マシンは、物理デバイスがそのワークロードに応じてエネルギーを動的に使用するのと同様に、その物理ホスト上でリソースを動的に使用します。

データストア

データセンター内の基礎となる物理ストレージリソースの組み合わせの仮想表現を指定します。たとえば、サーバ上のローカル ディスクが **SAN** ディスク配列を使用して物理ストレージリソースを提供する、などです。

仮想ディスク

仮想ゲストオペレーティングシステム内にディスクドライブを定義します。仮想ディスクは、ローカル ホストまたはリモートファイルシステムに存在する特定のファイルまたはファイルのセットです。仮想ディスクは、オペレーティングシステム内の物理ディスクドライブと同様に動作します。

仮想スイッチ

物理スイッチと同様に動作します。各 **ESX** サーバには、ポートグループで仮想マシンに接続する、それ自体の仮想スイッチがあります。これらの仮想スイッチは、**ESX** サーバ上の物理イーサネットアダプタにもアップリンク接続されています。仮想マシンは、仮想スイッチ アップリンクに接続された物理イーサネットアダプタで外部の世界と通信します。

物理 NIC

ESX サーバ上の物理イーサネットアダプタを指定します。

仮想 NIC

仮想マシン上の仮想イーサネットアダプタを指定します。ゲストオペレーティングシステムは、仮想イーサネットアダプタが物理イーサネットアダプタであるかのように、デバイスドライバを介して仮想イーサネットアダプタと通信します。仮想イーサネットアダプタには、それ自体の **MAC** アドレス、1 つ以上の **IP** アドレスがあり、物理 **NIC** とまったく同様に標準イーサネットプロトコルに応答します。

ハードウェア センサ

CPU、メモリ、ファン、電圧、ストレージ、温度、および電源に関する物理情報を提供します。ハードウェア センサには、**vCenter Server** 経由で **ESX** サーバでアクセスできます。

リソース割り当て

利用可能なリソース容量では、リソースコンシューマの需要が満たされない場合、仮想マシン、**vApp**、およびリソース プールのリソースの量をカスタマイズします。

共有、予約、および制限の設定を使用して、仮想マシン、リソース プール、または **vApp** に提供される **CPU** およびメモリのリソース量を決定します。

リソース割り当ての共有

共有は、共有相手に対する仮想マシン、リソースプール、または **vApp** の相対的な優先度または重要性を指定します。ある仮想マシンに、別の競合仮想マシンの **2 倍** のリソース共有がある場合、**2 倍** のリソースを消費できます。

共有には、通常、自然数を指定します。デフォルトを使用するか、または各仮想マシンに共有の特定の数値(相対値)を割り当てることができます。

共有の指定は、リソースを共有する仮想マシン、**vApp**、またはリソースプールに対してのみ影響します。リソースを共有する仮想マシンまたはリソースプールは階層で同じ親を持ちます。予約および制限によって制限される相対的な共有の値に従ってリソースを共有します。仮想マシンに共有を割り当てるときには、オンになっている他の仮想マシンに相対する、その仮想マシンの優先度を常に指定します。

たとえば、競合が発生すると、**2000** の共有を持つ仮想マシンには、**1000** の共有を持つ仮想マシンよりも多くの **CPU** 時間が割り当てられます。共有は他の共有に相対して設定されます。このため、共有の値ではなく相対的な大きさが意味を持ちます。**1000**、**2000**、**3000** の共有の値を持つ **3** 台の仮想マシンは、**1**、**2**、**3** の共有の値を持つ **3** 台の仮想マシンと同じように動作します。任意の数スキーム(**1**、**2**、**3** や **1000**、**2000**、**3000** など)を使用できます。数値間に余裕を残して設定する場合、将来、より容易にリソースプールにリソースを追加できます。

リソースで競合が発生していないとき、共有は仮想マシンの操作に影響しません。共有の指定は、リソースプールまたは **vApp** のバランスを保つのに役立ちます。

リソース割り当ての予約

予約は、仮想マシン、リソースプール、または vApp に対する、保証された CPU またはメモリの最小割り当て量を指定します。vSphere は、予約されていない十分なリソースが仮想マシンで利用できる場合に限り、仮想マシンをオンにすることを許可します。サーバは、物理サーバの負荷が高いときにも、予約されたリソース量を保証します。予約はメガヘルツまたはメガバイトの単位で定義します。

たとえば、2 GHz の CPU を利用できるとします。VM1 に 1000 MHz および VM2 に 1000 MHz の予約を指定します。現在、仮想マシンはそれぞれ必要な場合に 1 GHz を取得することが保証されています。ただし、VM1 が 500 MHz しか使用していない場合、VM2 は 1.5 GHz を使用できます。

予約のデフォルトは 0 です。最低限必要な CPU またはメモリの量を、仮想マシンで常に利用できることを保証するために、予約を指定できます。

リソース割り当ての制限

制限は、仮想マシン、リソースプール、または vApp の CPU またはメモリの最大割り当て量を制限します。サーバは仮想マシンに予約された量より多く割り当てることができますが、制限を超えて割り当てることはできません。システム上で利用されていない場合でも、制限を超えて、CPU またはメモリを割り当てることはできません。制限はメガヘルツまたはメガバイトの単位で定義します。

デフォルトでは、CPU とメモリの制限は、無制限に設定されています。メモリ制限が無制限に設定されていると、vSphere は、仮想マシンを作成するときに、有効にメモリの量を決定します。通常、制限を指定する必要はありません。

リソース割り当てのベスト プラクティス

ESX/ESXi 環境に適したリソース割り当て設定 (共有、予約、および制限) を指定します。

以下のガイドラインは、仮想インフラストラクチャの最適なパフォーマンスを実現するうえで役立ちます。

- 利用可能なリソースの総数を頻繁に変更する可能性がある場合、共有を使用して、複数の仮想マシンにわたってリソースを割り当てます。共有を使用しているときに、ホストをアップグレードする場合、共有の数値は変更されません。たとえば、各共有がより多くのメモリまたは CPU を表すようになったとしても、仮想マシンはそれぞれ同じ優先度のままになります。
- 使用したい量ではなく、許容できる最小限の CPU またはメモリの量を指定するために、予約を使用します。ホストは、仮想マシンの共有の数、予測される需要、および制限に基づいて、利用可能な追加のリソースを割り当てます。仮想マシンの追加または削除など、環境を変更しても、予約によって指定されたリソースの量は変更されません。
- 仮想マシンの予約を指定するとき、すべてのリソースをコミットするのではなく、予約しない部分が適切に残るように計画してください。予約する量がすべてのシステム容量の限界に近づくと、予約やリソースプールの階層を変更することが困難になります。
- 詳細については、www.vmware.com にある vSphere 関連のドキュメントを参照してください。

Solaris ゾーン

Solaris ゾーンは、仮想化されたオペレーティング システムを定義します。これにより、分離された安全な環境が提供され、アプリケーションを実行できます。この環境では、各アプリケーションおよびサービスにリソースを割り当てることができ、プロセスが他のゾーンに影響しないようにします。Solaris は、1 つのエンティティとして各ゾーンを管理します。コンテナは 1 つのゾーンで、オペレーティング システムのリソース管理も使用します。Solaris ゾーン PMM は、Solaris ゾーン環境のヘルス管理、管理、およびプロビジョニングを提供します。

Solaris ゾーン コンテナ リソースは、次の 3 レベルで管理できます。

Solaris ゾーン ゾーン管理

Solaris サーバはゾーンを使用して、分離された環境でアプリケーションを実行します。これにより、アプリケーションが物理的に別のコンピュータ上で実行されているように見えます。サーバ上の各ゾーンは、リソースプールからそのリソースを取得します。このゾーンには、仮想ネットワーク インターフェース、ファイル システム、メモリ、および他の専用ユニットが含まれます。

Solaris ゾーン プロジェクト管理

プロジェクトは、個別のワークロード エンティティに分割するアプリケーションまたはアプリケーションのセットです。ゾーンは、ワークロードと設定に従って、ゾーン内の他のリソースまたはプロジェクトとは別に、プロジェクトにリソースを割り当てます。

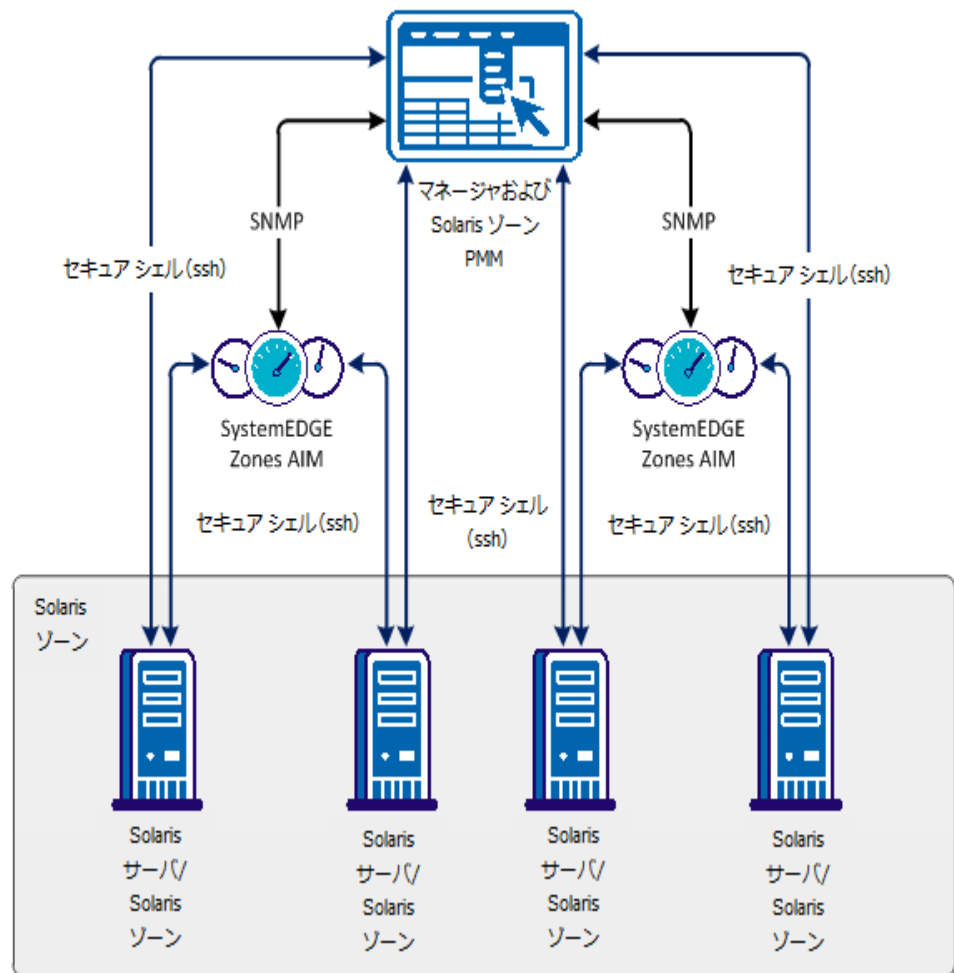
Solaris ゾーン リソース プール管理

リソース プールは、プロセッサ セット設定用の永続的な設定メカニズム、およびクラス割り当てのスケジューリングを提供します。リソース プールは、ゾーン内のプロジェクトおよびタスクに、それらの設定に従って動的にリソースを割り当てることができます。

Solaris ゾーン管理コンポーネント間のインタラクション

以下の図に、Solaris ゾーン管理に關与するコンポーネントがどのように相互作用するのかを示します。管理対象ノードは、SystemEDGE および Solaris ゾーン AIM が実行される Windows サーバです。AIM と Solaris ゾーン サーバの間の通信は SSH (Secure Shell) に基づいています。

Solaris ゾーン管理コンポーネント間のインタラクション



各 Solaris ゾーン サーバに必要な接続情報を追加するには、カスタム インストール、ユーザ インターフェースの[管理]タブまたは管理対象ノードで **NodeCfgUtil.exe** ユーティリティを使用します。接続情報は管理対象ノード上の設定ファイルに書き込まれます。AIM は設定ファイルをポーリングし、ユーザの Solaris ゾーン環境をモニタし始めます。

Microsoft Hyper-V Server

Windows Server 2008 R2 Hyper-V (ハイパーバイザベースのサーバ仮想化技術)が、Windows Server 2008 R2 の不可欠な機能として利用可能で、これにより、サーバ仮想化を実行できます。Hyper-V Server 用 SystemEDGE AIM は、Hyper-V Server コンピュータ上で実行されます。

Hyper-V Server PMM は、接続と、すべての Hyper-V Server 操作の運用上のサポートを提供します。PMM は、接続の管理、VM 関連の操作の実行、Hyper-V Server から取得したデータのデータベースへの入力を担当します。

Hyper-V Server 用 AIM は、以下のリソースタイプをモニタします。

Hyper-V Server

Hyper-V が実行されている物理サーバの計算機能とメモリリソースをすべて表します。Hyper-V AIM は、Hyper-V Server コンピュータのヘルス状態に関する情報を提供します。たとえば、CPU とメモリ使用率に関するステータスおよびデータが提供されます。

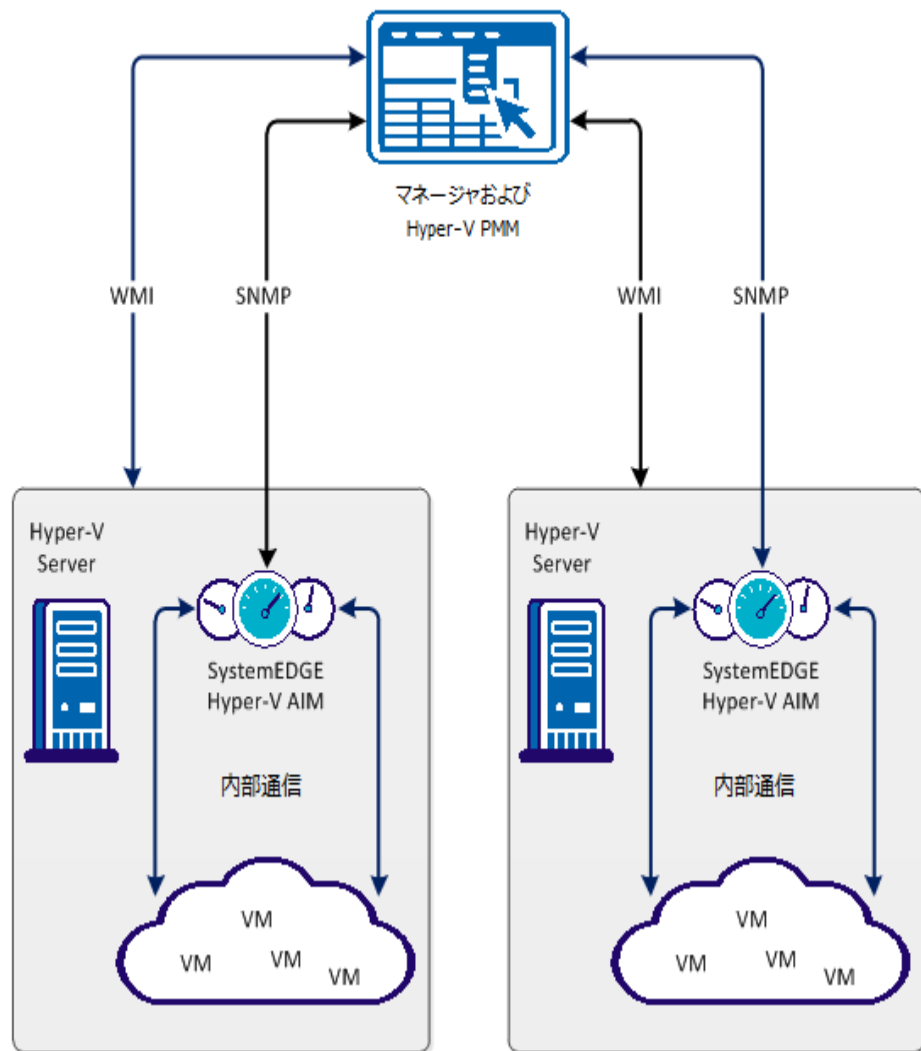
仮想マシン

ゲストオペレーティングシステムおよびアプリケーションが実行可能な仮想化された x86 環境を指定します。仮想マシンを作成すると、特定のホスト、クラスタ、またはリソースプール、およびデータストアに割り当てられます。仮想マシンは、物理デバイスがそのワークロードに応じてエネルギーを動的に使用するのと同様に、その物理ホスト上でリソースを動的に使用します。

Hyper-V Server 管理コンポーネント間のインタラクション

以下の図は、Hyper-V 管理に関与するコンポーネントがどのように対話するかを示しています。SystemEDGE および Hyper-V AIM は、Windows 2008 (Hyper-V) サーバ上で実行され、仮想環境を管理します。Hyper-V AIM はデータを収集し、Hyper-V Server と関連付けられた物理および仮想リソースをすべて表示します。

Hyper-V Server 管理コンポーネント間のインタラクション



インストール中に、またはユーザ インターフェースの[管理]タブを使用して Hyper-V 管理を設定できます。

IBM PowerVM (LPAR)

PowerVM システムで、IBM AIX はシステムを論理パーティション (LPAR) に分割する機能を提供します。論理パーティションはそれぞれ独立したシステムとして実行されます。また、パーティション間でリソースを分散することもできます。通常、各システムにはディスクリソースおよびネットワーク インターフェースを仮想化する仮想 I/O サーバ (VIOS) という専門のパーティションがあります。システムを分割することにより、個別のコンピューティング ニーズを考慮しながら、仮想リソースを動的に共有できます。PowerVM システムには、ハードウェア管理コンソール (HMC) または Integrated Virtualization Manager (IVM) のいずれかである仮想化マネージャコンポーネントがあります。HMC は、個別のシステム上で実行されるアプライアンスで、複数の PowerVM サーバを管理するために使用されます。IVM は仮想 I/O サーバに対する拡張で、ローカル PowerVM サーバのみを管理できます。

PowerVM AIM を使用して、SystemEDGE で LPAR のリソースをモニタリングできます。

LPAR Performance Management Module (PMM) は、すべての LPAR 操作に対する接続と運用上のサポートを提供します。PMM は、接続管理、ハードウェア管理コンソール (HMC) または Integrated Virtualization Manager (IVM) からのデータ取得、さまざまな LPAR 関連操作の実行、データベースへの取り込み、およびすべての HMC/IVM インタラクションに対する Web サービス/SSH の提供を行います。

HMC/IVM から管理対象システムおよび LPAR のデータを取得し、以下の LPAR 関連操作を実行できます。

サーバレベル

サーバレベルで、以下のタスクを実行できます。

- LPAR のプロビジョニング
- LPAR の削除

電源操作レベル

電源操作レベルで、以下のタスクを実行できます。

- LPAR のアクティブ化
- LPAR のシャットダウン
- LPAR の再起動

リソース調整レベル

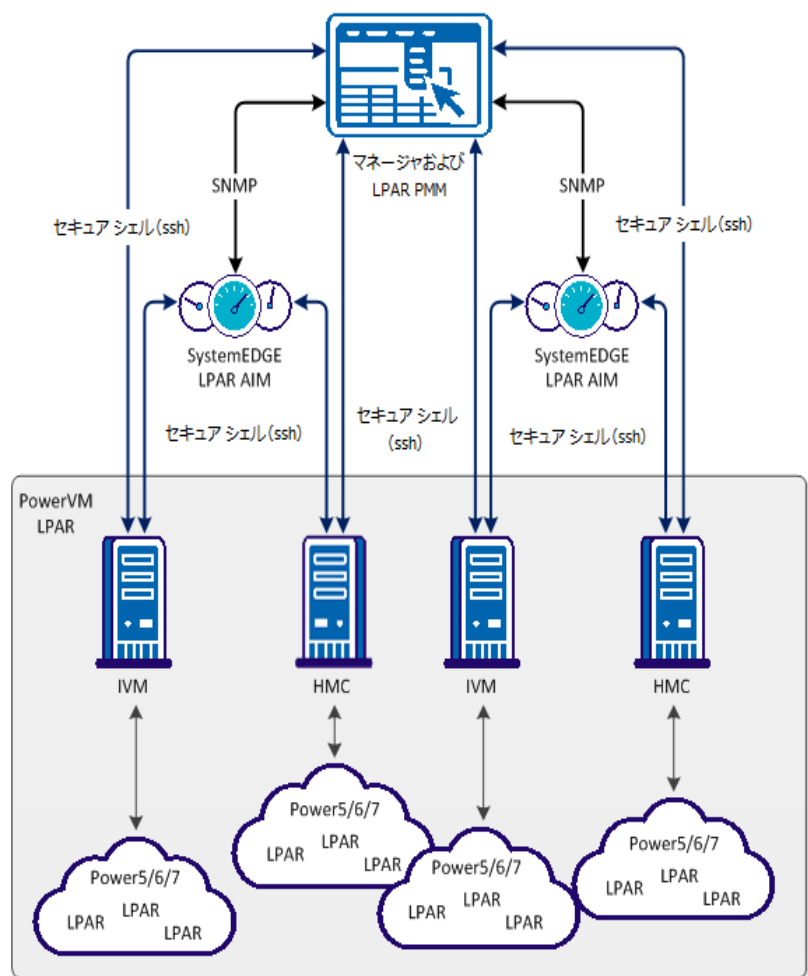
リソース調整レベルで、以下のタスクを実行できます。

- LPAR プロセッサおよびメモリ ユニットの追加
- LPAR プロセッサおよびメモリ ユニットの削除

AIX LPAR 管理コンポーネント間のインタラクション

以下の図は、IBM LPAR 管理に関与するコンポーネントがどのように対話するかを示しています。AIM サーバとは、SystemEDGE および LPAR AIM が稼働する Windows サーバです。AIM と HMC/IVM サーバの間の通信は SSH (Secure Shell) に基づいています。CA Virtual Assurance は複数の HMC サーバまたは IVM サーバ接続できるため、CA Virtual Assurance ではお使いの LPAR 環境全体のビューが取得できます。

PowerVM Server 管理コンポーネント間のインタラクション



必要な各 HMC/IVM サーバおよび仮想 I/O サーバに要求される接続情報を追加するには、以下のいずれかの方法を使用します。

- カスタム インストール時
- ユーザ インターフェースの[管理]タブ(オンライン ヘルプを参照)
- AIM サーバ上の NodeCfgUtil.exe ユーティリティ

接続情報は管理対象ノード上の設定ファイルに書き込まれます。LPAR AIM は設定ファイルをポーリングし、HMC/IVM を通じて LPAR 環境のモニタリングを開始します。

LPAR モニタリング

LPAR リソースをモニタするには、UI 機能を使用せず、`sysedge.cf` ファイル内に LPAR AIM MIB に基づく SystemEDGE モニタおよび SystemEDGE コンポーネントオブジェクトモデルを作成します。適切なオブジェクトクラスを使用し、LPAR リソースに応じてオブジェクト インスタンスを指定します。作成されてモニタされた LPAR オブジェクトは、LPAR AIM がインストールされているコンピュータシステムにそれらの状態を伝達します。以下の例のように、`monObjInstance` 属性に HMC、POWER5/POWER6/POWER7 および LPAR システム情報を提供することをお勧めします。

例

`sysedge.cf` ファイル用の以下のモニタ定義は、`powersys` という名前の POWER5 または POWER6 のシステムの **Alive** ステータスを監視するように設定されています。`lpar01` という名前の LPAR は、2 以上になるように設定されています。すなわち、警告 -3、マイナー -4 などです。

```
monitor oid monCurrState.53001 98 0x0 60 absolute > 2 'Lpar System status' '' 'System'
'hmc/powersys/Total' Alive critical
monitor oid monCurrState.53006 99 0x0 60 absolute > 2 'Lpar01 System status' ''
'System' 'hmc/powersys/lpar01/Total' Alive critical
```

注: モニタのインスタンス名は `lpar://` から開始することはできません。

以下のテーブルでは、`sysedge.cf` ファイル用のモニタ定義例に一致するセルフモニタテーブルの例について説明します。

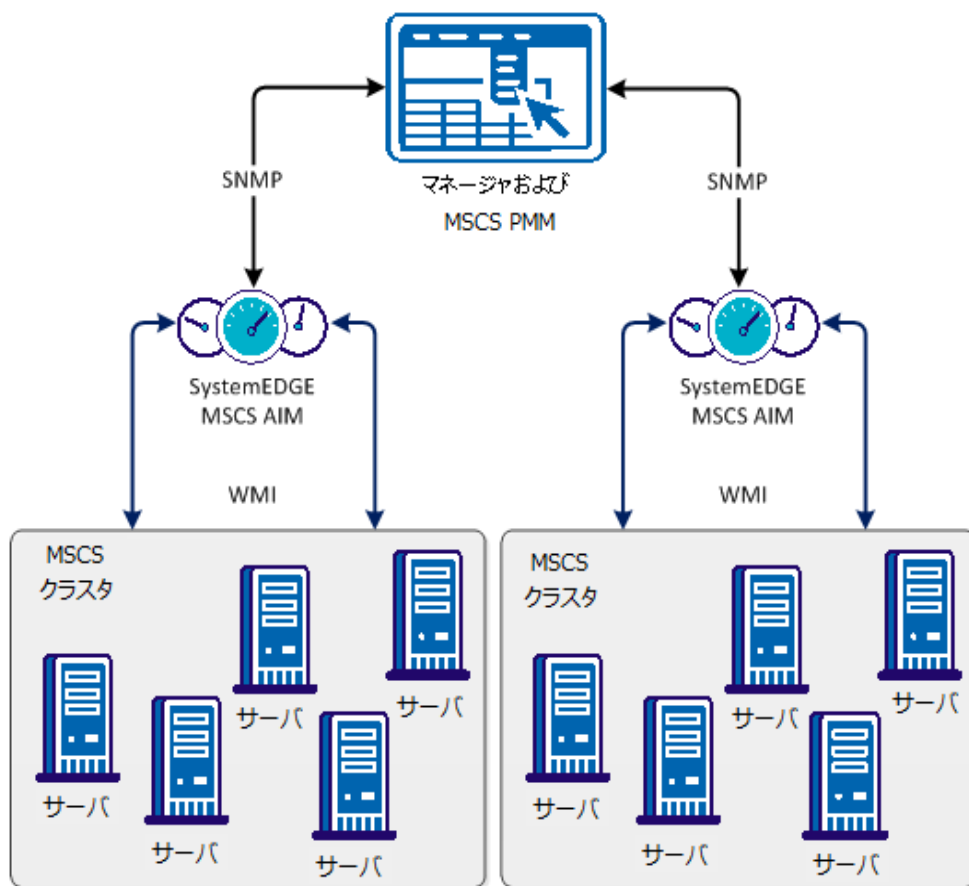
mon Index	monOID	mon ObjClass	monObjInstance	mon ObjAttribute	mon Severity	mon CurrState
530001	lparAimStatSys Status.1	System	lpar://hmc/powersys /Total	Alive	critical	ok
530002	lparAimStatSys CPUUsage PerMil.1	CPU	lpar://hmc/powersys /Total	PercentUsed	warning	ok
530003	lparAimStatSys CPUUsage PerMil.1	CPU	lpar://hmc/powersys /Total	PercentUsed	minor	ok
530004	lparAimStatSys MemoryUsage PerMil.1	Memory	lpar://hmc/powersys /Total	PercentUsed	warning	warning

mon Index	monOID	mon ObjClass	monObjInstance	mon ObjAttribute	mon Severity	mon CurrState
530005	lparAimStatSys MemoryUsage PerMil.1	Memory	lpar://hmc/powersys /Total	PercentUsed	minor	minor
530006	lparAimStatLP Status.1.1	System	lpar://hmc/powersys /lpar01/Total	Alive	critical	critical
530007	lparAimStatLPCPU Usage.1.1	CPU	lpar://hmc/powersys /lpar01/Total	PercentUsed	warning	ok
530008	lparAimStatLPCPU Usage.1.1	CPU	lpar://hmc/powersys /lpar01/Total	PercentUsed	minor	ok
530009	lparAimStatLP MemoryUsage.1.1	Memory	lpar://hmc/powersys /lpar01/Total	PercentUsed	warning	ok
530010	lparAimStatLP MemoryUsage.1.1	Memory	lpar://hmc/powersys /lpar01/Total	PercentUsed	minor	ok
530011	lparAimStatLP Status.1.2	System	lpar://hmc/powersys /lpar02/Total	Alive	critical	critical
530012	lparAimStatLPCPU Usage.1.2	CPU	lpar://hmc/powersys /lpar02/Total	PercentUsed	warning	ok
530013	lparAimStatLPCPU Usage.1.2	CPU	lpar://hmc/powersys /lpar02/Total	PercentUsed	minor	ok
530014	lparAimStatLP Memory Usage.1.2	Memory	lpar://hmc/powersys /lpar02/Total	PercentUsed	warning	ok

Microsoft Cluster Service

Microsoft Cluster Service (MSCS) は 2 つ以上のサーバを一緒に接続し、それらが単一のコンピュータとしてクライアントに表示されるようにします。クラスタ化によって、フェイルセーフアプリケーションを保有することができます。Microsoft SQL Server のようなクラスタ対応アプリケーションは一度にノード上で実行されます。そのノードがダウンした場合、別のノードがサービスを引き継ぎます。クラスタ化によって、アプリケーションが絶えず稼働されていることを確認することができます。

MSCS 管理コンポーネント間のインタラクション



パフォーマンス モニタリングでは、CPU やメモリ使用などのメトリック収集用のクラスタおよび個別のクラスタ ノードへのリモートアクセスが必要です。クラスタ固有の情報は各ノードで利用できます。MSCS AIM は、WMI (ポート 135) を使用してクラスタと通信します。

Microsoft クラスタの概要

Microsoft Cluster Service (MSCS) は 2 つ以上のサーバを一緒に接続し、それらを単一のコンピュータとしてクライアントに表示します。クラスタ化によって、フェイルセーフアプリケーションを保有することができます。Microsoft SQL Server のようなクラスタ対応アプリケーションは一度に 1 つのノード上で実行されます。そのノードがダウンした場合、別のノードがサービスを引き継ぎます。クラスタ化によって、アプリケーションが絶えず稼働されていることを確認することができます。

Microsoft クラスタ コンポーネントが CA Virtual Assurance にインストールされている場合、管理者は[管理]タブを使用して、クラスタを登録し管理できます。

関連項目

[クラスタの登録](#) (P. 102)

[クラスタの削除](#) (P. 102)

[クラスタ プロパティの変更](#) (P. 103)

[クラスタの登録](#) (P. 102)

[クラスタの削除](#) (P. 102)

[クラスタ プロパティの変更](#) (P. 103)

クラスタの登録

ユーザ インターフェースの[管理]ページを使用して、Microsoft クラスタを登録できます。

ユーザ インターフェースから Microsoft クラスタを登録する方法

1. [管理]をクリックします。
[管理]ページが表示されます。
2. [設定]ペインの[プロビジョニング]セクションで、[Microsoft クラスタ]をクリックします。
[Microsoft クラスタ]セクションが右側に表示されます。
3. [登録済み Microsoft クラスタ]ツールバー上で「+」(追加)をクリックします。
[新規クラスタの登録]ダイアログ ボックスが表示されます。
4. 必要なクラスタ名およびアクセス識別情報を入力し[OK]をクリックします。
Microsoft クラスタが登録されます。

注: クラスタを登録する場合は、クラスタ ホスト名を使用します。

クラスタの削除

ユーザ インターフェースの[管理]ページを使用して、Microsoft クラスタを削除できます。

クラスタを削除する方法

1. [管理]をクリックします。
[管理]ページが表示されます。
2. [設定]ペインの[プロビジョニング]セクションで、[Microsoft クラスタ]をクリックします。
[Microsoft クラスタ]セクションが右側に表示されます。
3. 削除する項目クラスタを選択します。
4. [登録済み Microsoft クラスタ]ツールバー上で「-」(削除)をクリックします。
確認プロンプトが表示されます。
5. [OK]をクリックします。
クラスタが削除されます。

クラスタ プロパティの変更

ユーザ インターフェースの[管理]ページを使用して、Microsoft クラスタ プロパティを変更できます。

クラスタ プロパティを変更するには、以下の手順に従います。

1. [管理]をクリックします。
[管理]ページが表示されます。
2. [設定]ペインの[プロビジョニング]セクションで、[Microsoft クラスタ]をクリックします。
[Microsoft クラスタ]セクションが右側に表示されます。
3. 編集するクラスタを選択します。
4. [登録済み Microsoft クラスタ]ツールバー上の[編集]アイコンをクリックします。
[クラスタ プロパティの変更]ダイアログ ボックスが表示されます。
5. 必須プロパティを編集し、[OK]をクリックします。
クラスタ プロパティが変更されます。

Cisco UCS

Cisco Unified Computing System (Cisco UCS) は Cisco のデータ センター ソリューションです。このソリューションでは、ペア ファブリック インターコネクト スイッチを 2 つまでのスイッチ、40 のシャーシおよび 320 のブレード サーバ(ブレード)と統合します。スイッチ上で実行される Cisco UCS Manager は、ネットワーク、ストレージおよびブレードの管理機能を提供し、仮想化もサポートします。CA Virtual Assurance は Cisco UCS と対話し、ハードウェア リソースや健全性とデバイスの統計などの UCS デバイス情報をクエリします。CA Virtual Assurance は UCS AIM および PMM を使用して、Cisco UCS をサポートします。Cisco UCS インターフェースおよびそれらの操作の詳細については、Cisco UCS のドキュメントを参照してください。

管理者は、管理ユーザ インターフェースまたは dpmutil CLI コマンドのいずれかを使用して、UCS Manager を登録できます。dpmutil を使用する場合は、nodecfgutil.exe を実行して UCS AIM を設定します。

注: CLI コマンドの詳細については、「リファレンス ガイド」を参照してください。

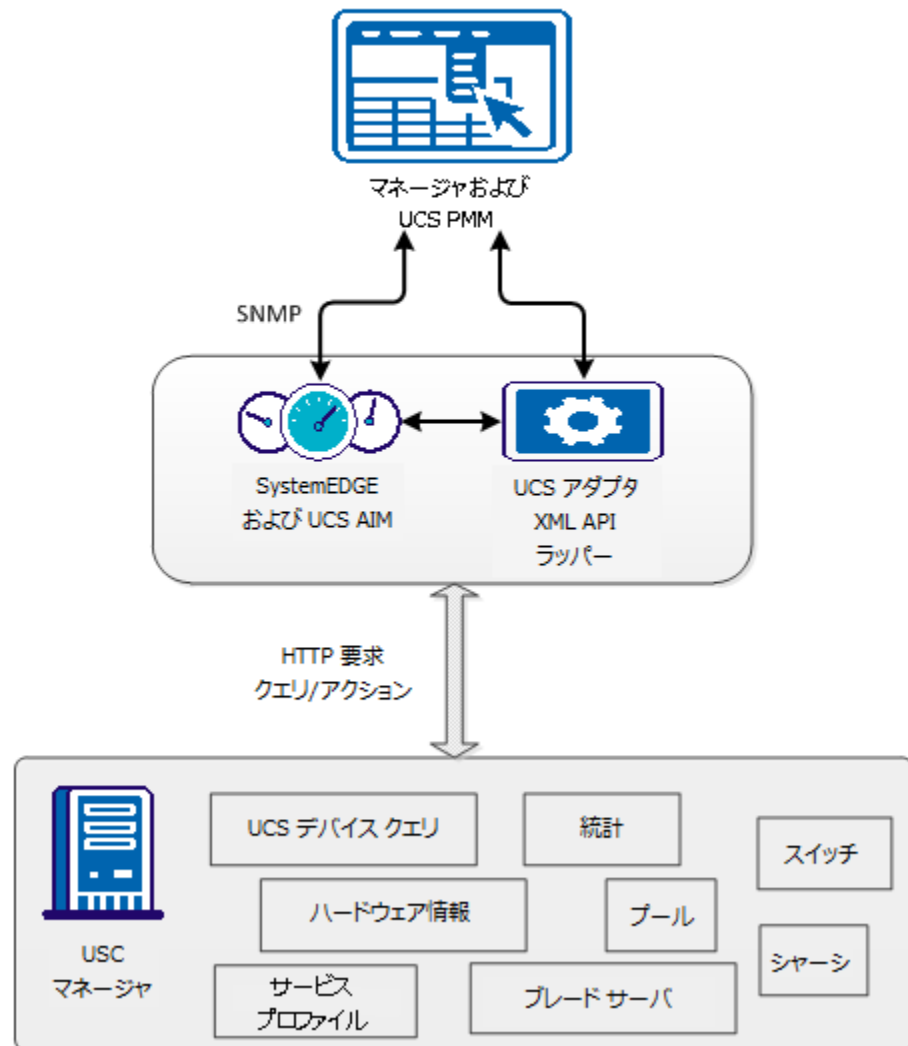
関連項目:

[Cisco UCS 管理コンポーネント間のインタラクション](#) (P. 105)

Cisco UCS 管理コンポーネント間のインタラクション

Cisco UCS 統合では、UCS デバイスおよび統計データの取得やデバイスの設定を行うための SNMP get/set 要求を提供するため、SystemEDGE 用の UCS AIM が必要となります。UCS プラットフォーム管理モジュール (PMM) から、UCS デバイスや統計情報のクエリが行われ、管理 DB 内にデータが保存されます。Cisco UCS Manager とのインタラクション用に、Cisco から XML API が提供されています。API を使用すると、CA Virtual Assurance で UCS Manager が提供するハードウェア、統計、プール (UUID、MAC、WWPN、WWNN)、およびサービスプロファイル情報にアクセスできるようになります。

Cisco UCS 管理コンポーネント間のインタラクション



XML API によって、特定のデバイスプロパティの設定や、プールおよびサービスプロファイルの管理を行う機能も提供されます。プールおよびサービスプロファイルの管理は、プール範囲の競合を検出するために、CA Virtual Assurance で複数の UCS Manager にわたって管理されるユースケースの 1 つです。

この図は、Cisco UCS 統合で使用されるコンポーネントを示しています。UCS アダプタと Cisco UCS Manager 間の通信プロトコルは、HTTP または HTTPS です。

Cisco UCS の概要

Cisco Unified Computing System (Cisco UCS) は Cisco のデータセンター ソリューションです。このソリューションでは、ペア ファブリック インターコネクト スイッチを 2 つまでのスイッチ、40 のシャーシおよび 320 のブレード サーバ(ブレード)と統合します。スイッチ上で実行される Cisco UCS Manager は、ネットワーク、ストレージおよびブレードの管理機能を提供し、仮想化もサポートします。CA Virtual Assurance は Cisco UCS と連携して、ハードウェアリソース、およびヘルス状態とデバイスの統計などの UCS デバイス情報のクエリを実行します。CA Virtual Assurance は UCS AIM および UCS PMM を使用して、Cisco UCS をサポートします。Cisco UCS インターフェースおよびそれらの操作の詳細については、Cisco UCS のドキュメントを参照してください。

管理者は、管理ユーザ インターフェースまたは `dpmutil` CLI コマンドを使用して、UCS Manager を追加したり、UCS AIM を登録したりできます。

注: CLI コマンドの詳細については、「リファレンス ガイド」を参照してください。

関連項目：

[Cisco UCS マネージャ サーバの追加](#) (P. 107)

[UCS AIM サーバの登録](#) (P. 108)

[UCS サーバの削除](#) (P. 109)

[SNMP データ ポーラーの設定](#) (P. 110)

[サービス ポーラーの設定](#) (P. 111)

[UCS トラップ管理](#) (P. 111)

[サービス プロファイル](#) (P. 112)

[SNMP データ ポーラーの設定](#) (P. 110)

[サービス ポーラーの設定](#) (P. 111)

[UCS トラップ管理](#) (P. 111)

[サービス プロファイル](#) (P. 112)

[サービス プロファイルの作成または更新を実行する方法](#) (P. 113)

Cisco UCS マネージャ サーバの追加

Cisco UCS コンポーネントがインストールされている場合は、dpmutil CLI コマンドまたはユーザ インターフェースの[管理]ページを使用して、Cisco UCS Manager サーバを追加できます。

注: CLI コマンドの詳細については、「リファレンス ガイド」を参照してください。

ユーザ インターフェースで UCS Manager を追加する方法

1. [管理]をクリックします。
[管理]ページが表示されます。
2. [設定]をクリックします。
[設定]ページが表示されます。
3. [Cisco UCS サーバ]をクリックします。
[Cisco UCS サーバ]ページが表示されます。
4. [Cisco UCS サーバ]ツールバーで[+] (追加)をクリックします。
[Cisco UCS サーバの追加]ダイアログ ボックスが表示されます。
5. 必要なサーバ識別情報を入力し、[OK]をクリックします。
サーバが追加されます。

UCS AIM サーバの登録

Cisco UCS コンポーネントがインストールされている場合は、`dpmutil` コマンドまたはユーザ インターフェースの[管理]ページを使用して、UCS AIM サーバを登録できます。

注: CLI コマンドの詳細については、「リファレンス ガイド」を参照してください。

ユーザ インターフェースで UCS AIM サーバを登録する方法

1. [管理]をクリックします。
[管理]ページが表示されます。
2. [設定]ペインの[プロビジョニング]セクションで、[Cisco UCS サーバ]をクリックします。
[UCS AIM サーバ]セクションが右側に表示されます。
3. [UCS AIM サーバ]ツールバーで[+] (追加)をクリックします。
[Cisco UCS AIM サーバの追加]ダイアログ ボックスが表示されます。
4. 必要なサーバおよび SNMP アクセス識別情報を入力して、[OK]をクリックします。
UCS AIM サーバが登録されます。

UCS サーバの削除

ユーザ インターフェースの[管理]ページを使用して、Cisco UCS サーバを削除できます。

UCS サーバを削除する方法

1. [管理]をクリックします。
[管理]ページが表示されます。
2. [設定]ペインの[プロビジョニング]セクションで、[Cisco UCS サーバ]をクリックします。
[Cisco UCS サーバ]ページが表示されます。
3. 削除するサーバを選択します。
4. サーバ ツールバーの[-] (削除)をクリックします。
確認のプロンプトが表示されます。
5. [OK]をクリックします。
サーバが削除されます。

SNMP データ ポーラーの設定

SNMP データ ポーラーは、UCS AIM から Cisco デバイスの情報を取得します。ポーリングされる要素には次のものが含まれます。

- スイッチ
- シャシー (ファン、PSU)
- ブレード (メイン ロジック ボード、メモリ)
- 電力消費
- 温度

ポーリング間隔を設定する方法

1. `¥conf¥caucsconf.cfg` ファイルを、以下のように編集します。

```
<property name="CONFIG_KEY_UCS_AIM_POLL_INTERVAL">  
  <!-- UCS AIM ポーリング間隔 -->  
  <value>300</value>  
  <displayName>UCS AIM ポーリング間隔</displayName>  
</property>
```
2. ファイルを保存します。

サービス ポーラーの設定

サービス ポーラーは、プールおよびサービス プロファイル情報を UCS Manager から直接取得します。ポーリングされる要素には次のものが含まれます。

- UUID プール
- MAC プール
- ワールド ワイド ノード名 (WWNN) プール
- ワールド ワイド ポート名 (WWPN) プール
- サーバ プール
- サービス プロファイル

デフォルトのサービス ポーリング間隔は 300 秒です。

ポーリング間隔をリセットする方法

1. `caucscfg` ファイルを、以下のように編集します。

```
<property name="CONFIG_KEY_UCS_SERVICE_POLL_INTERVAL">  
  <!-- UCS サービス間隔(秒) -->  
  <value>300</value>  
  <displayName>UCS Manager ポーリング間隔</displayName>  
</property>
```

2. ファイルを保存します。

UCS トラップ管理

UCS PMM は、UCS トラップ表示をリスンします。UCS トラップはすべて、イベントとして転送されます。

デフォルトポート 162 の `trapreceiver` に UCS トラップを転送するには、`SystemEDGE` を設定します。

サービス プロファイル

サービス プロファイルには、インターフェース、ファブリック接続性、およびネットワークとサーバの ID など、Cisco UCS ハードウェアに関する設定情報が含まれます。特定の UCS Manager 用の、または CA Virtual Assurance 管理 DB に一元化されたサービス プロファイルを作成できます。UCS Manager 上のサービス プロファイルは 管理 DB にインポートでき、そこから他の UCS Manager にエクスポートできます。

サービス プロファイルで、オペレーティング システムからの Cisco UCS ハードウェアの抽出のサポートが可能になります。サービス プロファイルを追加または削除して、サービスをオンラインまたはオフラインにすることができます。1 つのブレードから別のブレードにサービス プロファイルを割り当て直すことで、サービス (オペレーティング システムとアプリケーション) のセットを別のサーバに移動できます。

サービス プロファイル情報には、次のものを含めることができます。

- デバイス UUID または仮想 UUID プールごとのブレード サーバ
- ローカル ストレージ、RAID、または SAN (HBA、WWNN、および WWNN プール) の任意の設定内のストレージ
- ネットワーキング (MAC、vNIC 0、vNIC 1、および MAC プール)
- サーバの起動順序または他のポリシー
- サーバ割り当てのタイプ (後で割り当て、スロットを事前にプロビジョニング、既存のサーバをプロビジョニング、プールからサーバを選択)

サービス プロファイルの作成また更新を実行する方法

CA Virtual Assurance には、管理者がサービス プロファイルを作成できるウィザードが用意されています。また、事前定義済みポリシー オプションを使用してサービス プロファイルを更新できます。システム、ネットワーク、およびストレージの管理者は、協力して、一意の ID 特性や必須の接続特性を持つサービス プロファイルを作成できます。

サービス プロファイル ウィザードでは、Cisco 環境における知識と経験を活用できる Cisco UCS Manager インターフェースのサブセットが提供されます。

例: サービス プロファイルの作成

CA Virtual Assurance ユーザ インターフェースで、[作成]-[サービス]-[プロファイル]オプションを選択し、作成するサーバ プロファイルの名前を指定して、サーバ プロファイルを以下のいずれにするかを選択します。

- ハードウェア ベース
- デフォルトのネットワークおよびストレージの接続を使用するシンプルなサーバ プロファイル
- 既存のサービス プロファイル テンプレート ベース
- 明示的に作成する必要があるカスタム サービス プロファイル

ウィザードでは、選択されたオプションに基づいたインタビュー プロセスに従い、必要な ID 情報や接続情報を指定します。デフォルトを使用することも、ID (UUID)、ネットワーク (MAC/VLAN)、ストレージ (WWN/vHBA)、およびブート ポリシー情報を明示的に指定することもできます。

複数のマルチインスタンス AIM の使用

同じタイプ (vCenter Server、Solaris ゾーン、LPAR、MSCS、または Cisco UCS) の複数のリモート AIM を備えた CA Virtual Assurance マネージャを使用して特定の仮想環境を管理する場合は、以下を考慮してください。

各 vCenter Server、Solaris ゾーン サーバ、HMC/IVM サーバ、または Cisco UCS サーバが、1 つの AIM に一意に関連付けられていることを確認します。CA Virtual Assurance マネージャのユーザ インターフェイスで[管理]を使用して、または適切な AIM サーバで NodeCfgUtil を使用して、あいまいな関連付けをすべて削除します。

複数の AIM がこのようなサーバを管理している場合は、これによって管理、ディスカバリ、またはモニタリングに関する問題が発生します。

例

3 つの vCenter Server が以下のように 2 つの AIM で管理されています。

- vCenter Server 1 および vCenter Server 2 は vCenter Server AIM 1 で管理されています。
- vCenter Server 2 および vCenter Server 3 は vCenter Server AIM 2 で管理されています。

この場合、vCenter Server 2 は、vCenter Server AIM 1 および vCenter Server AIM 2 と関連付けられており、この関連付けは一意ではありません。AIM 1 または AIM 2 から、これらの 2 つの関連付けの 1 つを削除すると、関連付けを一意にすることができます。

システム管理

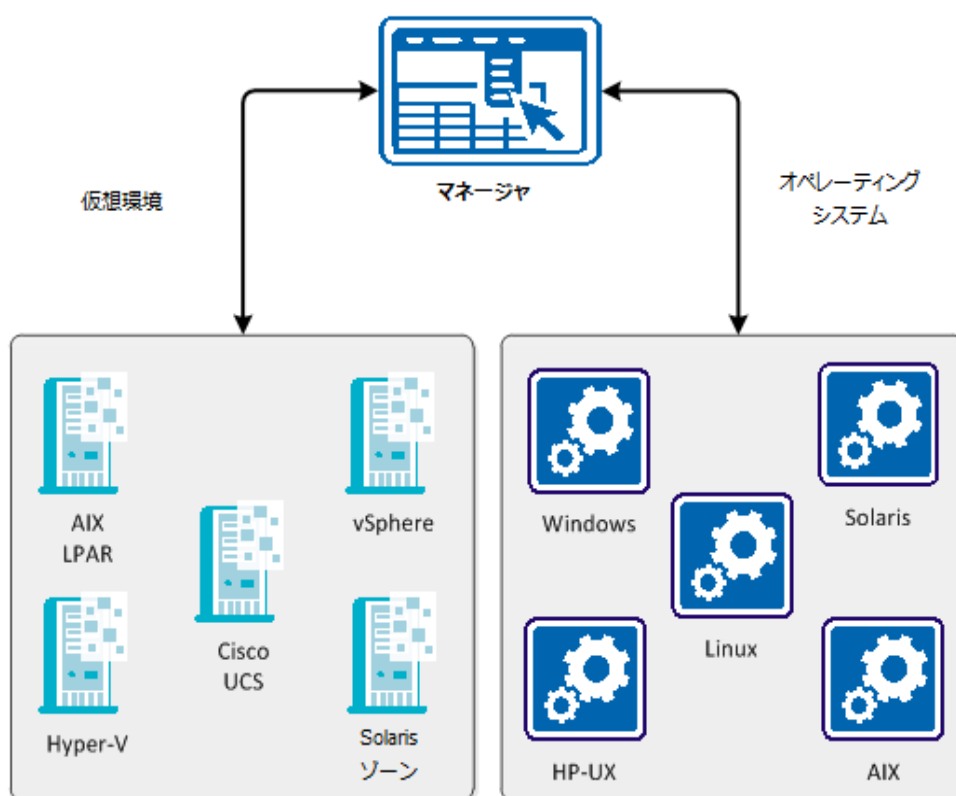
CA Virtual Assurance は、仮想環境を管理するよう設計されていますが、システム (管理対象ノード) の検出や管理も行います。CA Virtual Assurance は、管理対象ノード上の以下のオペレーティング システムをサポートしています。

- AIX
- HP-UX
- Linux、zLinux
- Solaris (Intel、SPARC)
- Windows

管理対象ノードの利用可能な管理コンポーネントは、次のとおりです。

- SystemEDGE
- Advanced Encryption AIM
- リモート モニタリング AIM (Windows サーバのみ)
- サービスレスポンス モニタリング (SRM) AIM
- CA Performance LiteAgent

仮想環境とオペレーティング システム



SystemEDGE は、CA Virtual Assurance でのシステム管理の基礎であり、以下の利点を備えています。

- すべての管理対象システムへの、一元化されたリモート エージェント展開
- 一元化されたリモート エージェント設定

- エージェントのオブジェクト モデルからのステータス情報を含む、モニタされたすべてのメトリックの視覚化
- サービスレスポンス モニタ AIM のリモート展開および設定
- 強化されたエージェント セキュリティ オプション

エージェント機能の詳細については、「[SystemEDGE ユーザ ガイド](#)」を参照してください。

関連項目

[SystemEDGE 機能](#) (P. 116)
[サービスレスポンス モニタリング](#) (P. 128)
[リモート モニタリング](#) (P. 132)
[エージェントの設定](#) (P. 133)
[エージェントの視覚化](#) (P. 134)
[セキュリティおよび保守](#) (P. 138)

SystemEDGE 機能

SystemEDGE は、物理および仮想システムの SNMP ベースのモニタリングを提供する軽量エージェントです。このエージェントを使用して、システム設定、パフォーマンス、ユーザ、ファイル システムなどの重要なシステム情報にアクセスします。指定したしきい値または条件に基づいて、この情報をモニタし、モニタに基づいたオブジェクトを作成して集計オブジェクト状態を維持します。

SystemEDGE は、以下の MIB からのモニタリング メトリックをサポートします。

- MIB-II (RFC 1213)
- Host Resources MIB (RFC 1514)
- Systems Management MIB (CA 固有)
- IF-MIB (一部) (RFC 2233)
- IP-MIB (一部) (RFC 4293)
- TCP-MIB (一部) (RFC 4022)
- UDP-MIB (一部) (RFC 4113)

Systems Management MIB のモニタリング テーブルを使用して、以下のタイプのインテリジェントなモニタリングを有効にすることができます。

セルフ モニタリング

エージェントがサポートする任意の整数ベース MIB オブジェクトのモニタリングを提供します。セルフ モニタ テーブルにエントリを作成して、モニタするオブジェクト、比較演算子、しきい値、および重大度を指定します。エージェントは、このエントリに従って自動的にオブジェクトをモニタします。エージェントはオブジェクトをモニタし、指定されたしきい値および重大度値に従って現在の状態を維持します。しきい値に違反すると、エージェントが状態変更トラップを送信します。

プロセスとサービスのモニタリング

任意のプロセス、Windows サービス、またはアプリケーションのモニタリングを提供します。プロセス モニタ テーブルにエントリを作成して、プロセスまたはサービスが実行されているかをモニタするか、指定されたしきい値に対してプロセス テーブル オブジェクトをモニタします。エージェントはプロセスをモニタし、指定されたしきい値および重大度値に従って現在の状態を維持します。しきい値に違反するか、プロセス(実行中または停止中)の状態が変わると、エージェントは状態変更トラップを送信します。

プロセス グループ モニタリング

プロセスのグループを定義し、そのグループの変更をモニタする機能を提供します。プロセス グループ モニタ テーブルでエントリを作成してプロセス グループを定義します。このグループをエージェントがモニタします。プロセス グループが変更された場合は、エージェントがトラップを送信します。

ログ ファイルおよびディレクトリ モニタリング

正規表現として指定された文字列を検索して、任意の UTF-8 エンコーディング システムまたはアプリケーション ログ ファイルのモニタリングを提供します。ログ モニタ テーブルのエントリを作成します。エージェントは、指定されたログ ファイルで、ユーザ定義の正規表現に一致する行をモニタします。一致する行が見つかり、エージェントがトラップを送信します。送信されたトラップに含まれる重大度をモニタに関連付けることができます。

Windows イベント モニタリング

イベントソースなどのさまざまなフィルタを使用して、Windows イベント ログ エントリのモニタリングを提供します。NT イベント モニタ テーブルのエントリを作成します。エージェントは、イベント ログで、ユーザ定義の正規表現に一致するイベントをモニタします。一致する行が見つかり、エージェントがトラップを送信します。

履歴の収集

マネージャ側ベースライニングおよび傾向分析用の履歴データ収集を提供します。履歴制御テーブルでエントリを作成します。エージェントは、時間が経つにつれてメトリックを収集します。メトリックを使用して、特定の期間中の平均システムパフォーマンスの図を提供します。

モニタリング機能および SystemEDGE アーキテクチャの詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

関連項目

[システム管理 MIB](#) (P. 118)

[状態管理モデル](#) (P. 121)

[オブジェクト集計の設定](#) (P. 122)

[ステートレスなモニタリング](#) (P. 124)

[管理対象モードおよびレガシー モード](#) (P. 125)

[SystemEDGE AIM](#) (P. 126)

システム管理 MIB

システム管理 MIB は、根本的なシステムおよびそのアプリケーションのヘルス状態およびパフォーマンスをモニタするためのオブジェクトを含む民間企業 MIB です。

システム管理 MIB 内でモニタできる、オブジェクトを備えたグループおよびテーブルを以下に示します。

システム グループ (sysedgeSystem)

ホスト名、CPU タイプ、およびオペレーティング システムのバージョンなどの基本システム情報が含まれます。

マウントされたデバイス テーブル (devTable)

ホスト上でマウントされたデバイスとファイル システムに関する情報が含まれます。ファイル システム スペースなどの値のモニタを作成できます。または、このテーブルに列値を設定して、マウントされたデバイスをマウント解除できます。

カーネル設定グループ (kernelConfig)

CPU の数、仮想メモリの量、およびクロック速度などのカーネル情報が含まれます。このグループを使用して、カーネルの設定方法およびカーネルのバージョンをモニタできます。

ブート設定グループ (bootconf)

ルートファイルシステム、ダンプファイルシステム、およびスワップ領域に関する情報が含まれます。このテーブルをモニタして、ルートファイルシステム名、ファイルシステムブロック、およびファイルシステムタイプなどの値を追跡します。

ストリーム グループ (streams)

ストリーム I/O サブシステムに関する情報が含まれます。使用中のストリームの数、ストリーム割り当て失敗の数、およびキュー内のストリームの数など、このグループ内のオブジェクトをモニタして、サブシステムのヘルス状態をモニタできます。

ユーザ テーブル (userTable)

システム上のユーザ アカウントに関する情報が含まれます。

グループ テーブル (groupTable)

システム上のユーザ グループに関する情報が含まれます。

プロセス テーブル (processTable)

実行中のプロセスに関する情報が含まれます。このテーブルをモニタして、現在実行されているプロセスを追跡できます。また、特定の属性を設定して、プロセスを制御することもできます。たとえば、**processkill** 列の値を 9 に設定して、プロセスを強制終了できます。

Who テーブル (whoTable)

システムに現在ログオンしているユーザに関する情報が含まれます。このテーブル内の属性をモニタして、任意の特定の時間にシステムを使用しているユーザを追跡できます。

リモート シェル グループ (remoteshell)

リモートシステムでシェル スクリプトとプログラムを実行するための属性が含まれます。このテーブルで属性を設定して、コマンド、その引数、および出力ファイルの名前を指定します。

カーネル パフォーマンス グループ (kernelperf)

ホストオペレーティングシステムのヘルス状態およびパフォーマンスに関する情報が含まれます。現在のプロセスおよび開いているファイルの数、アクティブなジョブの数、およびスケジューラキュー内のジョブの数などの属性をモニタできます。

プロセス間通信テーブル(msgqueTable、shmemTable、semTable)

メッセージキュー、共有メモリ、およびセマフォに関する情報が個別のテーブルに含まれます。これらのテーブルをモニタして、プロセス間の通信を調整します。

メッセージ バッファ割り当てテーブル(mbufAllocTable)

システムがどのようにメッセージ バッファを使用しているかに関する情報が含まれます。このテーブルの属性をモニタして、バッファリクエストが拒否された回数または遅れた回数などの情報を追跡します。

ストリーム バッファ割り当てテーブル(strbufAllocTable)

Streams サブシステムによって使用されるバッファのバッファ割り当ておよび使用状況の統計に関する情報が含まれます。

I/O バッファ キャッシュ グループ(ioBufferCache)

基本ディスク I/O の I/O バッファ割り当ておよび使用状況に関する情報が含まれます。このテーブルをモニタして、I/O バッファ アクティビティのピーク時などの情報を追跡します。

ディレクトリ名のルックアップ キャッシュ グループ(dnlc)

ディレクトリおよびファイル名キャッシュのパフォーマンスに関する情報が含まれます。

AIX 論理パーティション グループ(logicalPartition)

IBM AIX 論理パーティション (LPAR) に関する情報が含まれます。各パーティションの物理または論理 CPU などの属性、および各パーティションの CPU の数をモニタできます。

トラップ コミュニティ テーブル(trapCommunityTable)

設定済みコミュニティ、ユーザ、およびトラップ デスティネーションなどの SNMP 情報が含まれます。

NT システム グループ(ntSystem)

Windows システムに固有の情報が含まれます。このグループには、システム、スレッド、レジストリ、サービス、システム パフォーマンス、キャッシュ パフォーマンス、メモリ パフォーマンス、ページファイル パフォーマンス、およびイベント モニタの各グループが含まれ、Windows システム上のこれらの領域の属性をモニタします。

RPC 統計グループ(rpc)

カーネルリモートプロシージャコールに関する情報が含まれます。このテーブルをモニタして、RPC アクティビティのピーク時を検出するためのカウンタおよび統計などの属性を追跡します。

NFS 統計グループ(nfs)

カーネルの NFS 機能に関する情報を含みます。このテーブルをモニタして、NFS アクティビティのピーク時を検出するための統計およびカウンタなどの属性を追跡します。

ディスク統計テーブル(diskStatsTable)

ディスク I/O に関する情報が含まれます。

CPU 統計テーブル(cpuStatsTable)

各 CPU のパフォーマンス統計が含まれます。アイドル モードでの経過時間、および待機モードでの経過時間などの属性をモニタできます。

Systems Management MIB にはまた、モニタリング テーブルおよびオブジェクト集計をサポートするためのテーブルも含まれます。

状態管理モデル

SystemEDGE エージェントは、CA Virtual Assurance 管理モデル全体に統合された、セルフ モニタおよびプロセス モニタ用の状態管理モデルをサポートします。エージェントは、さまざまな重大度の複数のモニタを単一の管理対象オブジェクトに集計します。このオブジェクトの状態は、最高の重大度の違反されたモニタに対応します。

エージェントは、割り当てられた重大度値に従って、個々のモニタ状態を計算します。計算結果の状態は、以下のいずれかです。

- 不明(1)
- OK (2)
- 警告(3)
- マイナー(4)

- メジャー (5)
- 重大 (6)
- 致命的 (7)
- 稼働中 (11)
- ダウン (12)

注: モニタの重大度が「なし」の場合は、状態が「稼働中」と「ダウン」のいずれかに切り替わります。

Systems Management MIB の集計テーブルは、オブジェクト クラス、インスタンス、および属性値を使用して、同じ値のモニタを 1 つのエントリに集計します。このエントリは、モニタされたオブジェクトを表し、このオブジェクトに対して集計状態が維持されます。

注: オブジェクト クラス、インスタンス、および属性の値をモニタに入力しない場合は、エージェントが、意味のあるデフォルト情報を入力します。デフォルトセルフ モニタ値は、モニタされた OID をインスタンス、クラス、および属性値にマップする `sysedge.oid` ファイルを使用するモニタされた OID に基づいています。デフォルトプロセス モニタ値は、プロセス正規表現とモニタされた属性に基づいています。

集計テーブルは、しきい値違反によってオブジェクトのすべてのモニタが最悪の状態になる場合にのみ、テーブル内の現在の状態を更新し、状態変更トラップを送信します。たとえば、3 つのモニタで CPU 使用率をモニタしており、その 1 つが 60 パーセント (割り当てられた重大度が「警告」)、もう 1 つが 80 パーセント (重大度が「重大」)、もう 1 つが 100 パーセント (重大度が「致命的」) で、エージェントが 82 パーセントの CPU 使用率を返したと仮定します。この値は、60 パーセントおよび 80 パーセントのモニタでしきい値違反を引き起こします。ただし、エージェントは、80 パーセントのモニタに対する 1 つの状態変更トラップのみを送信し、集計状態を「重大」変更します。

オブジェクト集計の設定

デフォルトでは、SystemEDGE がモニタを集計し、オブジェクト クラス、インスタンス、および属性プロパティに同じ値を含む管理対象オブジェクトを生成します。たとえば、SysHealth のクラス、CPU のインスタンス、および SysTime の属性を備えたすべてのモニタが組み合わせられ、集計管理対象オブジェクトとなります。

SystemEDGE ポリシーを定義するときに、より高いレベルでオブジェクトを集計するよう、エージェントを設定できます。また、オブジェクト集計および状態管理モデルに関連するエージェント動作の他の側面も設定できます。

次の手順に従ってください:

1. [リソース]タブをクリックして[設定]ペインを開き、[ポリシー]を展開して[SystemEDGE]をクリックします。
[利用可能ポリシー]ページが表示されます。
2. [利用可能ポリシー]テーブルでポリシーを選択します。
ポリシーの[サマリ]ページが表示されます。
3. [制御設定]をクリックします。
[コントロール]ページが表示されます。
4. [モニタを集計]をクリックします。
[モニタを集計]ページが表示されます。
5. 集計レベルを指定するチェックボックスを1つ以上、オンにします。

これらはデフォルトより高い集計レベルを表し、最も高いレベルでは1つの最上位エージェントオブジェクトにすべてのモニタを集計できます。集計レベルを指定すると、指定したレベルまでステータスをプロパゲートする層構造のオブジェクトアーキテクチャを作成できます。

6. 以下の追加設定を設定して、[ポリシーの保存]をクリックします。

すべての集計済みモニタのレガシートラップを送信します。

管理対象オブジェクトを形成するすべてのモニタのレガシートラップを送信するかどうかを指定します。デフォルトでは、オブジェクト内の他のモニタでしきい値違反が発生しても、エージェントは、最も重大度の高いモニタの状態変更トラップを送信するのみです。

すべての集計済みモニタのコマンドを実行します。

管理対象オブジェクトを形成するすべてのモニタのアクションコマンドを実行するかどうかを指定します。デフォルトでは、オブジェクト内の他のモニタでしきい値違反が発生しても、エージェントは、最も重大度の高いモニタのアクションコマンドを実行するのみです。

集計設定が設定されます。変更を有効にするには、ポリシーを適用または再適用します。

関連項目:

[SystemEDGE ポリシー制御設定の定義 \(P. 181\)](#)

ステートレスなモニタリング

ステートレスなモニタは、オブジェクトステータス情報の取得も、オブジェクトモデルによる全体的オブジェクト状態の維持も行いません。これらのモニタは重大度値を維持しますが、この重大度の目的は、個々のモニタの重要性の追跡であるため、オブジェクト状態の計算には使用されません。以下のテーブルは、ステートレスなモニタリングをサポートします。

- プロセスグループ モニタ
- ログファイル モニタ
- NT イベント モニタ

これらのモニタは、CA Virtual Assurance ユーザ インターフェイスで設定できますが、その結果であるデータは表示できません。定義されたモニタに基づいて、以下のいずれかが検出された場合は、エージェントが送信するトラップを調べる必要があります。

- プロセスグループの変更
- 指定した正規表現に一致するログファイル メッセージ
- ディレクトリしきい値違反
- 指定した基準に一致する Windows イベント ログ イベント

プロセスグループ、ログファイル、および Windows イベント モニタの作成の詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

管理対象モードおよびレガシー モード

SystemEDGE を展開 (またはスタンドアロン方式でインストール) するときに、管理対象モードでエージェントを実行するように指定できます。管理対象モードでは、エージェントの展開元である CA Virtual Assurance マネージャ ノード (またはスタンドアロン エージェント インストールで指定したマネージャ ノード) によってエージェントが管理されます。管理対象モードでエージェントを実行すると、リモート設定および CA Virtual Assurance ユーザ インターフェースからの高度な視覚化など、すべての CA Virtual Assurance エージェント管理機能が有効になります。また、管理対象モードでは、CA Virtual Assurance が、エージェント設定のプライマリソースとして確立されます。管理対象モードのエージェントが CA Virtual Assurance の外部で変更された場合、CA Virtual Assurance 管理者は、その変更をブロックまたは上書きすることができます。

また、SystemEDGE を、レガシー モードで、または設定を制御する CA Virtual Assurance マネージャなしで実行することもできます。レガシー モードで実行されるエージェントが使用できるのは、レガシー モニタ、または状態の維持と計算を行わないモニタだけではありません。

CA Virtual Assurance からエージェントを展開するときは、パッケージラッパーの設定で「管理対象モードでの実行」チェックボックスを使用して、管理対象モードで実行するかどうかを指定します。エージェントを CA Virtual Assurance とは別にインストールするときは、管理対象モードで実行するためにエージェントの CA Virtual Assurance マネージャ ノードを使用します。

SystemEDGE AIM

Application Insight Module (AIM) は、SystemEDGE エージェントを拡張してアプリケーション固有のモニタリングを提供するか、またはベースエージェントに存在しない専門のモニタリング機能を提供します。以下の AIM が CA Virtual Assurance で提供されます。

- リモート モニタリング
- サービスレスポンス モニタ (SRM) AIM
- VMware vCenter Server AIM
- Solaris ズーン AIM
- Hyper-V AIM
- MSCS AIM
- Cisco UCS AIM
- LPAR AIM

これらの AIM と SystemEDGE は、CA Virtual Assurance ユーザ インターフェースで設定して展開することができます。

SystemEDGE の詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

リモート設定および展開

CA Virtual Assurance は、一元化された場所から、ファイルベースの設定および展開までの SystemEDGE のエンドツーエンドの管理を提供します。ファイルベースの設定によって、以下が実行されます。

- コミュニティ文字列、操作パラメータ、トラップ コミュニティ、AIM ロードなど、Systems Management Empire MIB の読み取り専用領域の設定のような、SNMP マネージャで SNMP SET を使用して実行できない変更を可能にする
- 確認可能な配信を有効にし、生じるセキュリティ脆弱性を SNMP より少なくします。
- 完全なリモートエージェント設定および配信を有効にし、ローカルでの手動ファイル操作の必要性を最小にするか、除去します。

CA Virtual Assurance マネージャは、サポートされている各プラットフォームの SystemEDGE のインストール パッケージを提供します。展開ソリューションを使用すると、認証情報およびインストール パラメータを指定でき、必要な情報をすべて指定すると、展開パッケージを保存して、企業内の管理対象システムに展開できます。

CA Virtual Assurance ユーザ インターフェースから、`sysedge.cf` ファイルのエージェント設定パラメータをすべて設定し、モニタ テーブルのグラフィカル表示を使用して、自動モニタリング エントリを作成することができます。プロファイルとしてエージェント設定を保存し、そのプロファイルを、管理対象システムに展開する展開パッケージに適用することができます。また、インストールされたエージェントにポイント設定変更を行い、それらの変更をすぐに適用できます。

設定変更を展開すると、CA Virtual Assurance によってファイル内のテンプレート 命令を使用して `sysedge.cf` ファイルがコンパイルされ、CA Virtual Assurance ユーザ インターフェースで入力した情報を適用して設定および自動モニタリングが行われます。コンパイルされた `sysedge.cf` ファイルは、CAM (CA メッセージ) を転送機構として使用して、指定されたシステムに送信されます。CAM は、インストール中に指定されたデータ ディレクトリにファイルを送信します。

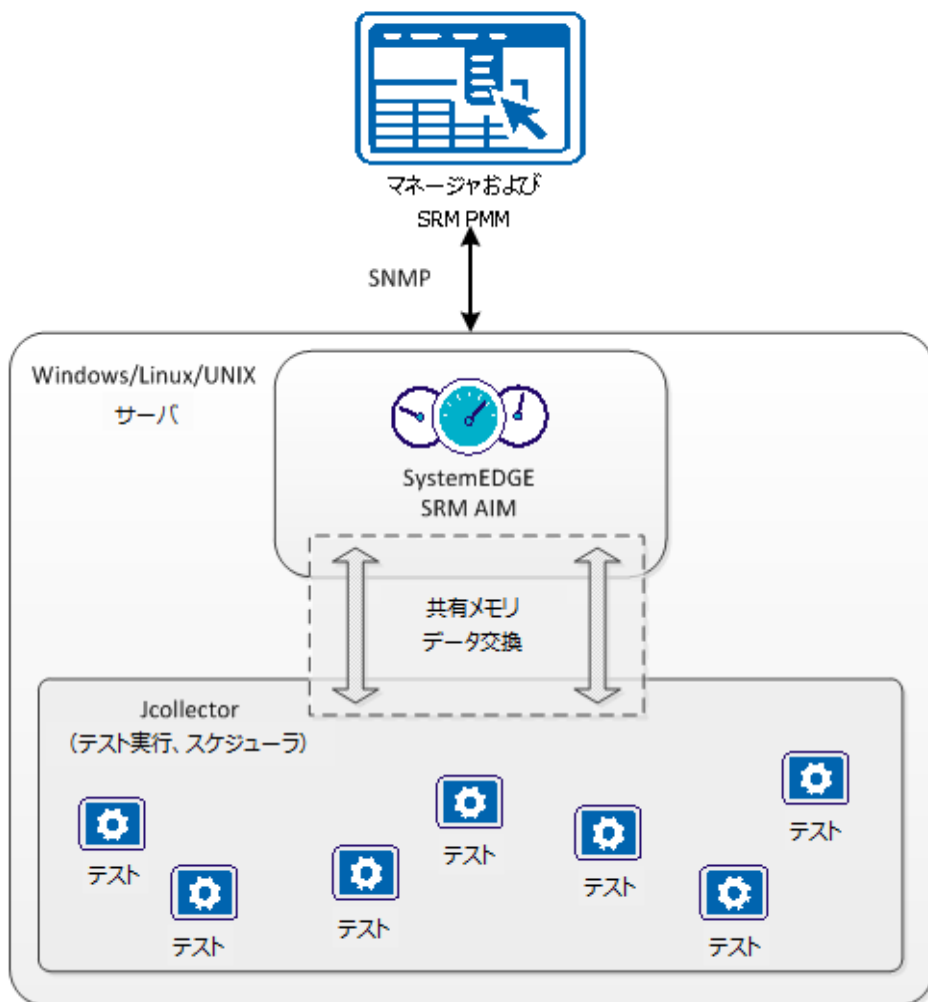
SystemEDGE エージェントは、設定ファイルが含まれる CAM メッセージをリスニングして、ファイルが検出されると、ファイルの構文が正しいことを確認してから、自動的にファイルをロードして使用します。CA Virtual Assurance でエージェントを設定すると、エージェントウォーム スタートがトリガされます。その結果、エージェントに加えた変更が自動的に適用され、再起動する必要がなくなります。

サービス レスポンス モニタリング

サービスレスポンス モニタリング Application Insight Module (SRM AIM)は、SystemEDGE の拡張機能(プラグイン)です。SRM は、ローカル システムまたはリモートシステム上で実行される論理サービスまたは物理サービスの応答に関するデータを取得します。Java ベースでマルチスレッド対応の SRM は、複数のサーバにまたがって複数のテスト設定を処理します。SRM は、事前設定されたテストまたはカスタム テストを実行して、実行の経過時間とスループットを測定します。

このような関係を以下の図に示します。

サービス レスポンス モニタリング コンポーネント間のインタラクション



svcrsp.cf 設定ファイルには、テスト仕様が含まれます。SRM AIM はこの設定ファイルを読み取り、共有メモリセグメント内でテスト仕様を利用可能な状態にします。SRM Jcollector コンポーネントは共有メモリから各テスト設定を読み取ります。Jcollector はテストを実行し、このタイミングプロセスの結果を収集して、SRM AIM に結果を伝達します。SystemEDGE はこれらの結果および関連付けのある情報を CA Virtual Assurance に送信します。

サービスレスポンス モニタ (SRM) AIM は、DNS、DHCP、SQL などの重大なシステム サービスの可用性と応答時間を、定義済みしきい値に基づいてモニタします。SRM テストを作成して、この機能を有効にします。SRM テストを使用すると、以下を実行できます。

- システム サービスの可用性と応答時間のテスト
- ユーザが影響を受ける前の、複雑な多層インフラストラクチャ内での可視性の取得による問題の特定
- 遅延、停止、およびパフォーマンスの問題のリアルタイム通知の取得
- DNS や DHCP などのサービスがサービスレベル アグリーメントに準拠して実行されていることの確認
- キャパシティ計画、トラブルシューティング、または長期にわたる動作での傾向分析のための履歴データの保守

CA Virtual Assurance は、SRM AIM の以下の機能を提供します。

- SystemEDGE エージェントによるリモート展開
- リモートテスト設定
- テストの視覚化

SRM AIM アーキテクチャの詳細については、「SRM ユーザ ガイド」を参照してください。

関連項目

[SRM テスト](#) (P. 130)

SRM テスト

SRM AIM は、以下の反応時間テストを提供します。

Active Directory

Windows Active Directory サービスが正しく動作して、共有ファイルとリソースを管理していることを確認します。

カスタム

重要なカスタム サービスまたは他のタスクが効率よく動作していることを確認します。

DHCP

DHCP (Dynamic Host Configuration Protocol) サーバが応答して、リクエストに対処していることを確認します。

DNS

DNS (Domain Name System) サーバがホスト名を処理して、解決リクエストに対処していることを確認します。

ファイル I/O

ファイル システム全体での読み取り、書き込み、および比較の作業を確認します。

FTP および TFTP

ユーザが、指定されたサーバにログインして、ファイルのアップロードとダウンロードを実行できることを確認します。

HTTP および HTTPS

ユーザがビジネス Web サーバに接続できることを確認し、特定のテキストが Web ページ上に表示されるかどうかを決定します。

LDAP

LDAP サーバへの接続を確認して、ユーザリクエストおよび LDAP クエリ用のアクセスを確認します。

NIS

NIS マップリクエストが処理されていることを確認します。

NNTP

ユーザが Usenet ニュースグループ サーバおよび社内掲示板に接続できることを確認します。

PING

ネットワーク デバイスが存在し、ネットワークを介してアクセス可能であることを確認します。

電子メール

電子メール サーバが利用可能であり、電子メールを効率よく処理していることを確認します。SRM は、IMAP、MAPI、POP3、SMTP、および SMTP サーバから発信される往復の電子メールのテストをサポートします。

SNMP

SNMP エージェントが SNMPv1 GET リクエストに応答していることを確認します。

SQL クエリ

SQL データベース サーバが利用可能で、短いクエリを処理していることを確認します。

TCP

システムが接続リクエストをリスンして、処理していることを確認します。

仮想ユーザ

記録可能な(通常は WinTask で)実際のユーザトランザクション(キーボード入力とマウスのクリック)の継続的な応答時間および可用性データを取得して、ビジネス タスクが正常に実行されていることを確認します。

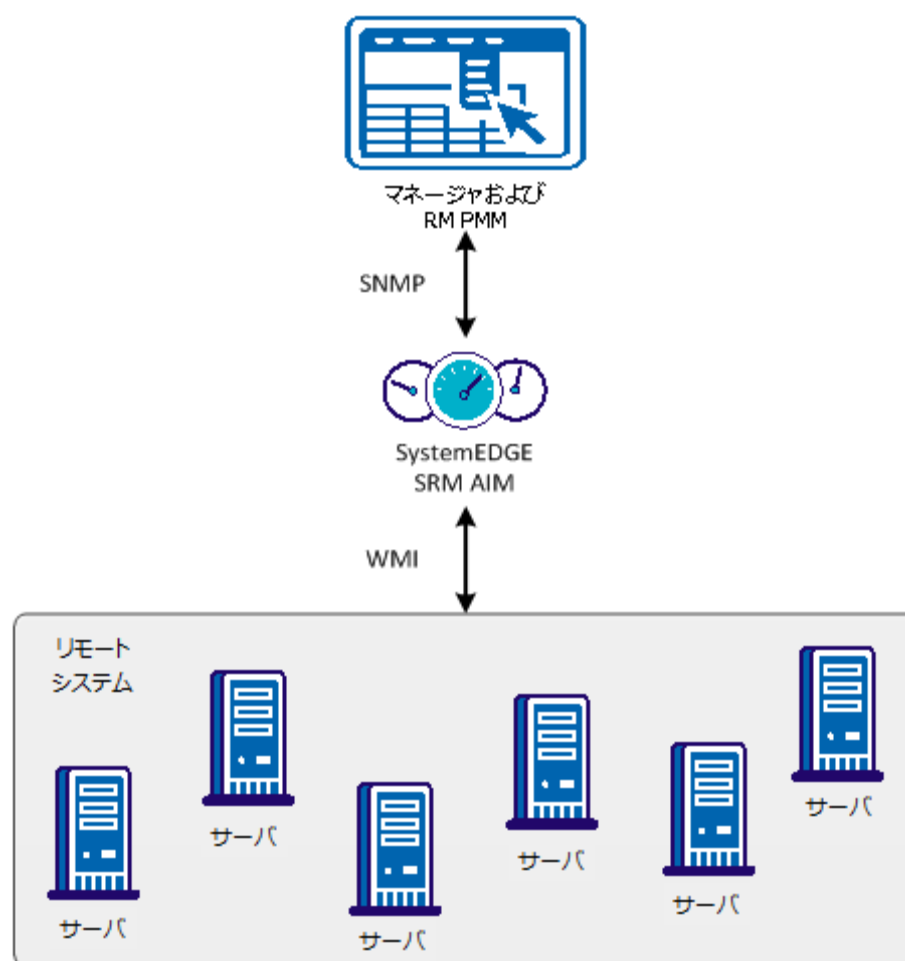
リモート モニタリング

リモート モニタリング AIM は、DCOM を使用する `root¥CIMV2` ネームスペースへの WMI 接続を通じて、RM システムにアクセスします。DCOM には、ローカル システム管理者のユーザおよびパスワード認証情報が必要です。Windows コンピュータをモニタする場合は、RM AIM がファイルに格納しているこれらの認証情報を提供する必要があります。パスワードは暗号化されます。

リモート モニタリングは、モニタされた RM システム上で WMI クエリを実行し (ポート 135)、Windows システム情報 (Win32_ComputerSystem) を収集して提供します。WMI ではポート 135 を使用します (デフォルト)。

このような関係を以下の図に示します。

リモート モニタリング コンポーネント間のインタラクション



エージェントの設定

CA Virtual Assurance ユーザ インターフェースでは、以下の 2 つの種類の SystemEDGE 設定が利用可能です。

ポイント設定

ポリシーを展開することなく、エージェントに単一の一時的な変更を加えることができます。たとえば、セルフ モニタしきい値を変更するか、一時プロセス モニタを追加するか、または SRM テストのセルフ モニタを作成することができます。ポリシーを展開すると、ポイント設定が上書きされます。

ポリシー設定

1 つの操作で、管理対象マシンのセットに展開できるエージェント設定ポリシーを作成します。たとえば、共通モニタおよび SRM テストのセットを含むポリシーを定義し、企業内のすべてのシステムにそのポリシーを展開して、同一の重要なシステム メトリックが確実にモニタされるようにすることができます。

CA Virtual Assurance ユーザ インターフェースからの管理対象モードのエージェントの設定は、その他のすべての設定形式より優先されます。sysedge.cf 設定ファイルまたは SNMP SET を介してユーザがローカル エージェントを手動で変更した場合は、ポリシーが適用された後に、これらの変更が CA Virtual Assurance ポリシー設定で上書きされます。

関連項目

[ポイント エージェント設定の実行 \(P. 133\)](#)

[ポリシー設定 \(P. 178\)](#)

ポイント エージェント設定の実行

CA Virtual Assurance を使用すると、ポリシーの作成も適用も行わずに、単一のエージェントへの単一またはポイント設定変更を実行することができます。この機能は、単一のシステムのモニタリング設定を一時的に変更するためのものです。以下のシナリオで、ポイント設定変更が有用または必要となる場合の例を説明します。

- 一時的に考慮される、個々のシステムに特有の変更すべて
- 一時的な異常に対処するための変更
- 一般的なモニタリング ポリシーにこれらをコミットする前の、さまざまなモニタリングの重大度としきい値を使用した実験用の変更

ポイント設定変更を行う場合、CA Virtual Assurance は、すべての既存のポリシーまたはローカル設定に加えて、システムへの変更を適用します。ただし、次回にポリシーをシステムに適用するときは、ポイント設定変更がポリシーによって上書きされます。ポイント設定変更は、ベース ポリシーにマージされるまで、またはポリシー アプリケーションによって上書きされるまで、ポリシー例外としてレポートされます。

ポイント設定は、セルフおよびプロセス モニタに対して実行できます。

ポイント エージェント設定を実行する方法

1. [リソース]をクリックして、[エクスプローラ]ペインで設定するシステムを選択します。

システム情報が右側のペインに表示されます。

2. 右側のペインの[設定]をクリックして、[セルフ モニタ]または[プロセス モニタ]を選択します。

既存のセルフまたはプロセス モニタが表示されます。

3. ツールバーの[+] (新規)をクリックします。

新しいセルフまたはプロセス モニタを作成するためのフィールドが表示されます。

4. 必要なフィールドに入力し、[保存]をクリックします。

注: 詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

モニタが保存され、更新されたセルフまたはプロセス モニタのリストに表示されます。

また、既存のセルフまたはプロセス モニタの変更、削除、またはコピーも実行できます。

エージェントの視覚化

CA Virtual Assurance ユーザ インターフェースは、管理対象モードのエージェントを備えたシステムのモニタリング情報を表示します。プラットフォーム管理モデル(PMM)は、エージェント情報を解釈して変換し、この情報が根本的な CA Virtual Assurance AIP アーキテクチャに適合して、AOM データベースに表示されるようにします。PMM は、ベース SystemEDGE エージェントおよび SRM AIM で利用可能です。

CA Virtual Assurance ユーザ インターフェイスで視覚化できるエージェント データには、以下が含まれます。

- 状態管理モデルを使用して作成された管理対象オブジェクト。
- すべての管理対象オブジェクトの状態
- 個々のモニタ
- SRM テスト

関連項目

[管理対象オブジェクト状態の表示](#) (P. 135)

[SystemEDGE モニタの表示](#) (P. 136)

[SRM テストの表示](#) (P. 137)

[ダッシュボード ステータスビュー](#) (P. 137)

管理対象オブジェクト状態の表示

CA Virtual Assurance ユーザ インターフェイスは、管理対象モードで実行しているエージェントを備えたシステムの **SystemEDGE** 管理対象オブジェクトをすべて表示します。

管理対象オブジェクト状態を表示するには、[リソース]をクリックして、[管理対象]を展開し、システムを選択します。

システムの[サマリ]ページが右側のペインに表示されます。

[マシン ステータス情報]ペインには、管理対象オブジェクトの総数および最大のオブジェクト重大度が含まれます。

[管理対象オブジェクト]テーブルには、各管理対象オブジェクトに関する以下の情報が含まれます。

- ヘルス状態
- 稼働ステータス(アクティブまたは非アクティブ)
- オブジェクトクラス、インスタンス、および属性
- 現在のモニタされている値およびしきい値

このテーブルから、管理対象オブジェクトを選択して[アクション]-[定義に移動]をクリックし、管理対象オブジェクトを形成するモニタを表示できます。

SystemEDGE モニタの表示

CA Virtual Assurance ユーザ インターフェースには、管理対象モードで SystemEDGE を実行しているシステムの定義済みのセルフ モニタとプロセス モニタがすべて表示されます。各モニタに関する詳細を表示し、モニタの追加、削除、変更、コピーなどの[ポイント設定を実行](#) (P. 133)できます。

SystemEDGE モニタを表示する方法

1. [リソース]をクリックして[管理対象]を展開し、いずれかのシステムを選択します。

システムの[サマリ]ページが右側のペインに表示されます。

2. [設定]をクリックして、[セルフ モニタ]または[プロセス モニタ]をクリックします。

[セルフ モニタ]または[プロセス モニタ]ペインが表示されます。

[セルフ モニタ]および[プロセス モニタ]ペインには、以下のモニタ プロパティをリスト表示した表が含まれます。

- インデックス
- 状態
- ステータス

注: この状態は、モニタが関連付けられた管理対象オブジェクトの状態と同じではない場合があります。管理対象オブジェクトの状態は、オブジェクトを構成するすべてのモニタの中で最悪の現在の状態です。

- オブジェクトのクラス、インスタンス、および属性

注: これらの列の値が同じであるモニタは、同じ管理対象オブジェクトの一部です。

- 現在モニタされているオブジェクトの値、演算子、およびしきい値
- 重大度
- トラップ数
- 最後のトラップ
- フラグ

SRM テストの表示

CA Virtual Assurance ユーザ インターフェースには、SRM AIM を備えた管理対象モードで SystemEDGE を実行するシステムに対する SRM テストが表示されます。

SRM テストを表示する方法

1. [リソース]をクリックして[管理対象]を展開し、いずれかのシステムを選択します。

システムの[サマリ]ページが右側のペインに表示されます。

2. [詳細]をクリックして[SRM テスト]をクリックします。

[SRM テスト]ペインが表示されます。

[SRM テスト]ペインには、以下のテスト プロパティをリスト表示する表が含まれます。

- インデックス番号
- オブジェクト クラス名
- テストの名前とタイプ
- テスト送信先
- 間隔
- ステータス
- 最終結果
- エラー総数

ダッシュボード ステータス ビュー

ダッシュボードには、エージェント ステータスを追跡するための以下のビューがあります。

SystemEDGE マシン ステータス

管理対象モードで実行されている SystemEDGE を備えたすべてのシステム、および各システムでのすべての管理対象オブジェクトの最悪の現在の状態のリストである表を表示します。デフォルトでは、現在の状態が「重大」以上である 1 つ以上の管理対象オブジェクトを備えたシステムのみが表示されます。[フィルタの表示]をクリックして、状態とマシン名に基づいてビューの内容をフィルタします。表内のシステム名をクリックして、システム上のすべての管理対象オブジェクトの詳細を表示します。

SystemEDGE オブジェクトの状態

現在の状態が「重大」以上である SystemEDGE 管理対象オブジェクトすべてのリストである表を表示します。[フィルタの表示]をクリックして、状態、マシン名、クラス、インスタンス、および属性に基づいてビューの内容をフィルタします。システム名をクリックして、システム上のすべての管理対象オブジェクトの詳細を表示します。

セキュリティおよび保守

CA Virtual Assurance は、以下に示す、SystemEDGE エージェントのための強化されたセキュリティと保守のオプションを提供します。

- ユーザ インターフェイスで設定可能な保守モード
- SystemEDGE エージェントの設定の単一ポイント
- CA Virtual Assurance の外部で実行された変更をブロックする機能
- CA Virtual Assurance の外部で実行された変更の通知、および不要な変更を無視または拒絶する機会

関連項目

[保守モードの有効化](#) (P. 138)

保守モードの有効化

CA Virtual Assurance で SystemEDGE 保守モードを有効にできます。このモードでは、エージェントが、すべてのモニタ エントリの処理およびトラップ送信を停止します。保守モードは、エージェントのシステムが計画に従って停止中に、誤ったアラームトラップを受信しないようにする場合に便利です。

保守モードでは、エージェントはメトリックの収集を続行し、SNMP 要求に応答しますが、すべてのモニタおよび履歴収集の処理を一時停止します。エージェントは、保守期間の初めにすべてのモニタの現在値を保存して、保守期間の最後の現在値と比較します。また、必要な場合は、現在値に応じてトラップを送信します。

次の手順に従ってください:

1. [エクスプローラ]ペインを開きます。
利用可能なグループ、サービス、およびシステムが表示されます。
2. [管理対象]を展開し、システムを選択します。
3. [リソース]タブをクリックし、[モニタリング ソフトウェア]をクリックします。
[マシンの詳細]ペインが表示されます。
4. [保守モード]オプションを[有効]に設定し、[適用]をクリックします。
エージェントがウォーム スタートを実行し、保守モードが有効になります。

エージェントで保守モードを終了するには、単に[保守モード]チェック ボックスをオフにして[適用]をクリックします。

第 6 章：管理ポリシー

このセクションには、以下のトピックが含まれています。

[ルールとアクション](#) (P. 141)

[ポリシーのユースケース](#) (P. 158)

[データ収集の設定](#) (P. 160)

[ポリシーの UCS アクションタイプ](#) (P. 174)

[ポリシー設定](#) (P. 178)

ルールとアクション

ルールとアクションを設定するには、まずルールとアクションについて理解し、それらが相互にまたは他のコンポーネントと対話する方法について理解する必要があります。これらのインタラクションを理解することによって、ルールとアクションをセットアップしてデータセンターを効率的に管理する最適な方法を決定することができます。

CA Virtual Assurance はメトリックを収集して分析し、リソースを分配する方法に関する分析に基づいて最適な決定を行います。たとえば、CA Virtual Assurance がサーバまたはサービスを高稼働率または低稼働率であると判断した場合は、新しいコンピュータをプロビジョニングできます。

使用状況はサーバレベルおよびサービスレベルでモニタされます。サーバレベル モニタリングでは、特定のサーバの診断問題に関与するため、重要なパフォーマンス インジケータのみが使用されます。サービスレベル モニタリングでは全体としてサービスに関する問題を診断し、全体の使用率がパフォーマンス インジケータとして使用されます。

ルールはサーバレベルまたはサービスレベルで作成できます。ルールを作成してパフォーマンス メトリックおよび生成されたイベントを評価します。ルールは、個別の条件または条件の組み合わせで構成されます。アクションが実行されるようにするには、全体を **true** の状態に評価する必要があります。ルールは独自のルールを作成するか、またはルール テンプレートのセットを選択し、自動化ポリシーを使用して生成することもできます。

注： パフォーマンス メトリックおよび説明のリストについては、「リファレンス ガイド」を参照してください。

デフォルトでは、ルールはデータセンターレベルで収集設定に定義されている記録間隔(デフォルト = 300 秒)で評価されるか、モニタされたメトリック値が原因でイベントが発生した場合に評価されます。データセンターとは異なる間隔を設定する場合は、特定のサーバを設定してデフォルトのデータセンターの記録間隔を上書きすることができます。サーバレベルルールは設定されたサーバレベルの記録間隔で評価されます。サービスレベルルールは、そのサービス内のすべてのサーバの中で最も短い記録間隔で評価されます。記録間隔を変更する場合は、ポリシー マネージャ サービスを停止して再起動し、ルールを評価するために更新された間隔を取得して使用します。

メトリックは評価データのソースです。メトリックルールが **true** に評価すると、アクションはトリガされます。ルールが **true** に評価するには遅延が超過している必要があります。あるシナリオでは、ルールの一度だけの違反でアクションがトリガされるようにするために遅延を **1** に設定しますが、他のインスタンスでは、一度だけのイベントでのルールのトリガを望まない場合があります。

たとえば、**CA Virtual Assurance** が、呼び出しを管理したり、問題の解決策を追跡したり、企業ナレッジを共有したり、IT 資産を管理するカスタム サポートアプリケーションの **CA SDM** に統合されるとします。アクションがトリガされた場合に自動的にチケットがオープンされるようにするには、アクションが **CA SDM** と対話するよう設定します。これはサードパーティの承認が必要なアクションに役立ちます。サードパーティが **CA SDM** でユーザのチケットを承認した後で、アクションは自動的に実行されます。

また、開始コンポーネントを使用して、指定された時刻にアクションが実行されるようにスケジュールすることもできます。ジョブを作成するときに、アクションの最新のパラメータが保存されます。ジョブがサブミットされた後でアクションの詳細を変更しても、すでに実行されるようにスケジュールされていたジョブには影響を及ぼしません。すでにスケジュールされているジョブのアクションの詳細を変更する必要がある場合は、アクションを使用するジョブを開いて再度それを保存し、それを新しいアクションの詳細で更新します。

CA SDM の設定

バージョン 12.5 以前の CA SDM リリースについては、適切なチケット ステータスコードで CA SDM を正しく設定することにより、必要に応じて問題が自動的に開くようにアクションを設定できます。

注: CA Virtual Assurance および CA SDM のリリース番号は、2 つの製品がデータベースを共有しない限り、同じである必要はありません。

CA SDM 設定する方法

1. Web ブラウザに以下の情報を入力することにより CA SDM サーバにログインします。

`http://servicedesk_servername:8080`

CA SDM のスプラッシュ画面が表示されます。

2. ユーザ名とパスワードを入力して、[ログイン]をクリックします。

CA SDM のメイン ページが表示されます。

3. [管理]をクリックし、左側のペインに Service Desk ツリー ノードを展開します。

4. [要求/インシデント/問題]を選択して[ステータス]を選択します。

[要求/インシデント/ステータスリスト]が表示されます。

5. [新規作成]をクリックします。

[新しい要求ステータスの作成]ウィンドウが表示されます。

6. [シンボル]テキスト ボックスに[承認済み]を入力し、[レコード ステータス]ドロップ ダウン リストから[アクティブ]を選択し、[コード]テキスト ボックスに[APP]を入力し、[保存]をクリックします。

リストに新しい要求ステータスが表示されます。

7. [シンボル]テキスト ボックスに[拒否]を入力し、[レコード ステータス]ドロップ ダウン リストから[アクティブ]を選択し、[コード]テキスト ボックスに[REJ]を入力し、[保存]をクリックします。

リストに新しい要求ステータスが表示されます。

CA SDM のセットアップが完了し、アクションがトリガされると、自動的に要求を開始できます。

CA SDM チケット ステータス設定の構成

CA SDM の 12.5 以前のバージョンではヘルプ デスク チケットに APP (承認済み) および REJ (拒否) のデフォルトのステータスコードの設定が使用されていました。CA Virtual Assurance では、ヘルプ デスク チケットの承認時に開始される操作を実行するためにこれらの承認コードを使用し検索します。これらの操作には限定されていませんが、アクションの実行、システムの予約などが含まれます。CA SDM のバージョン 12.5 を使用している場合は、新規チケット ステータスコードがサポートされています。PRBAPP (承認済み) および PRBREJ (拒否) は CA Virtual Assurance の既存の承認コードに関連付ける必要があります。新しいコードをサポートし、製品を正しく動作するには、以下の手順に従って設定ファイルを更新します。

チケット ステータス設定を変更する方法

1. テキスト エディタを使用して CA Virtual Assurance *Install_Path*\conf ディレクトリにある *caaipconf.cfg* ファイルを開いて[ヘルプ デスク]セクションにスクロールします。
2. 以下のようにして特殊なステータスコードのプロパティを検索します。

```
<property name="SPECIAL_STATUS_CODE">
  <!-- APP_CODE=PRBAPP;REJ_CODE=PRBREJ;(each code must be terminated by a
    semicolon) -->
  <value/>
  <displayName>SD R12.5 以降に追加されたコードのタイプ</displayName>
</property>
```

3. 以下のようにしてコードを非コメント化して変更します。

```
<property name="SPECIAL_STATUS_CODE">
  <value>APP_CODE=PRBAPP;REJ_CODE=PRBREJ;</value>
  <displayName>SD R12.5 以降に追加されたコードのタイプ</displayName>
</property>
```

CA Virtual Assurance は CA SDM 12.5 のステータスコードを使用できるように設定されました。

4. ファイルを保存して閉じ、設定の変更を有効にします。

ルールの設計

ルールとアクションをセットアップする場合は、以下の点について考慮します。

- 分析する VM、サーバ、およびサービス
- CA Virtual Assurance が違反を検出したときに実行するアクション

- 汎用にするルールと特殊にするルール スクリプトまたはバッチ ファイルが含まれる汎用ルールを計画する場合は環境への影響を慎重に考慮します。
- 評価の対象として興味のあるメトリック
- アクションがトリガされるまでに、ルールに違反する回数 アクションを過度に実行すると、環境でパフォーマンスに負の影響を与えることを考慮します。

注: ヘルプ デスク承認要件を指定するアクションは、アクションのスケジュールには使用できません。スケジュール済みアクションに同じアクションを必要とする場合は、ヘルプ デスク承認要件が含まれない、2 つ目のアクションを作成します。

自動化ポリシーの作成

[自動化ポリシーの作成]ウィザードを使用して、2 つの事前定義済みポリシータイプに基づいた自動化ルールを作成することができます。

- 仮想マシン動的リソースブローカ - CPU とメモリの割り当てが、定義済みの使用率しきい値に基づいて動的に変更されます。
- 全体的使用率メトリックのしきい値モニタリング - ヘルス状態は全体的な使用率に従って設定されます。

次の手順に従ってください:

1. [管理]ペインを開き、[自動化ポリシーの作成]をクリックします。
[自動化ポリシーの作成]ウィザードが表示されます。
2. [ポリシー タイプ]を選択し、[次へ]をクリックして、ターゲットリソースを選択し、ルールの条件を設定します。
[ポリシー サマリ]に結果が表示されます。
3. [終了]をクリックします。
ポリシーが確認され、対応するルールが作成されます。

ルールの作成

ルールは、ルール条件が **True** と評価された場合にアクションを実行するトリガとして機能します。

注: 元の作成者または管理者のみがルールを編集または削除できます。

次の手順に従ってください:

1. [リソース]をクリックし、[エクスプローラ]ツリーのサーバまたはサービスを選択します。

2. [ポリシー]タブをクリックし、次に、[ルール]タブをクリックします。

[ルール]ページが表示されます。

3. [+] (新しいルールの追加)をクリックします。

[ルール/テンプレート]ウィザードが表示されます。

4. [識別]セクションでルールに意味のある名前を入力し、次に、[ルール]を選択してルールを作成します。

注: 複数のルール定義で利用できるルール テンプレートを作成するには [テンプレート]を選択します。

5. [有効]を選択してルールをアクティブにします。

6. [許可される実行回数]として[無制限]を選択するか、[最大]を選択して最大再試行回数を入力します。

注: ルールが実行される回数に制限を設定することで、再試行が過度に発生してシステムの応答時間が遅くなる事態を防ぐことができます。

7. [次へ]をクリックします。

[テンプレートのモデル化およびアクションの選択]セクションが表示されます。

8. テンプレートにルールをモデル化するかどうか定義します。既存のテンプレートを選択するか、または新規テンプレートの名前を入力し、[有効]を選択してテンプレートへのすべての変更を継承します。

9. リストからルールのアクションを選択します。[次へ]をクリックします。

[ルールの定義式]セクションが表示されます。

10. [ルールの評価式]セクションで以下のフィールドを入力することにより、ルールの条件式を作成します。

ソース

ルールが評価するデータのソースを指定します。ソースは[全体的な使用率]、[イベント]、または特定のサーバ メトリックにすることができます。

演算子

[値]フィールドに入力する値に対しソース データを評価する方法を指定します。有効な演算子はソースによって異なります。たとえば、[全体的な使用率]を選択した場合、以下の演算子が有効です。

"=" "!=" "<" "<=" ">" ">="

[イベント]を選択した場合、値は以下のとおりです。

contains

文字列またはサブ文字列と完全に一致します。[値]フィールドにワイルドカードは使用できません。

RegEx（正規表現）

指定された正規表現に一致する文字列が検索された場合は **true** の値を返します。指定された正規表現に一致する文字列が検索されなかった場合は **false** の値を返します。

NotRegEx

指定された正規表現に一致する文字列が検索されなかった場合は **true** の値を返します。指定された正規表現に一致する文字列が検索された場合は **false** の値を返します。

重要：ルールとアクション名に一致させる文字列が含まれていないことを確認します。このベストプラクティスにより、イベントが次のルール評価サイクルで一致した場合に、アクションの追加の実行を回避することができます。

例：[値]フィールドに一致する文字列としてしきい値が含まれる場合、以下のイベントが一致します。

イベント A: メモリのしきい値が超えました。

イベント B: しきい値

値

選択された演算子がソース データを評価するための、数値または英数文字列を指定します。

遅延

アクションをトリガする前に、ルールが **True** と評価される必要がある頻度を定義します。定義するアクションによっては 1 回発生した後でトリガされる場合があります。その他のアクションでは多数の発生が永続的な問題を示した後でのみ、トリガされる必要があります。**注:** ソースが[イベント]に設定された場合、[遅延]はデフォルトでは無効になります。

論理演算子

論理演算子 **AND** または **OR** を使用することによって、複数の数式を定義します。[新規]をクリックして各定義を完成し、定義された数式のリストに数式を追加します。定義する最後の数式はデフォルトでは[NOOP]に設定されます。

条件式は、ルールが **true** と評価されたときに、アクションをトリガするために使用されます。[設定の確認]セクションが表示されます。

11. ルールの詳細を確認し、ページの一番上で[次へ]をクリックします。

12. [終了]をクリックして更新をコミットします。

ルールまたはテンプレートがルールリストに追加されます。

13. [ルールリストに戻る]リンクをクリックしてルールが追加されたことを確認します。

例: サーバレベル ルールの設定

この例では、サーバが CPU とメモリのしきい値を 3 回以上越えた場合、またはサーバが検出されたことを示すイベントが発生した場合のルールを設定します。

ルールの式:

1. CPU 使用率 % > 80 (遅延 3) AND
2. メモリ使用率 % > 50 (遅延 3) OR
3. 検出されたイベント RegEx.*
4. NOOP が検出されたイベント RegEx.*

アクション: 200 の CPU 共有を追加する(最大 8000)

事前定義済みアクション タイプの使用

ルールには、事前定義済みアクション タイプを選択できます。ルールの条件が **true** に評価された場合、定義したアクションが実行されます。

次の手順に従ってください:

1. [ポリシー] タブをクリックし、次に、[アクション & ルール] タブをクリックします。

[アクション & ルール] ページが表示されます。

2. [アクション] タブをクリックします。

[アクション] ページが表示されます。

3. [+] (新しいアクションの追加) をクリックします。

[アクションの定義: 新規] ページが表示されます。

4. [名前] テキスト ボックスでアクションに意味のある名前を入力し、以下のメニューを使用して、事前定義済みアクション タイプを選択します。

- [カテゴリ] - 製品の機能領域フィルタ。すべてのアクション タイプをリスト表示するには、[すべてのカテゴリ] を選択します。
- [タイプ] - 利用可能なアクション タイプ
- [環境] - 適用可能なプラットフォーム (たとえば VMware vCenter または Microsoft Hyper-V)

[詳細] セクションが表示されます。セクション内に表示されるオプションは、選択したアクション タイプによって異なります。

5. [アクションの開始] ドロップダウン メニューで、以下の設定のいずれか 1 つを選択します。

遅延なし

そのアクションを使用するルールが再度トリガされた場合に同じアクションをすぐに再実行できるように指定します。

遅延時間

アクションを使用するルールが再度トリガされた場合に、同じアクションを再実行できるまでに待機する必要がある時間を秒数で指定します。

注: アクションがスケジュール済みジョブによって実行される場合は、[アクションの開始] 設定は効力がありません。

6. [アクションの完了]ドロップダウンリストで以下の設定のいずれか1つを選択します。

待機なし

アクションが完了するまで待機せずにアクション シーケンスの次のアクションを実行するように指定します。

最大待機時間

アクション シーケンスで次のアクションが実行される前に完了するアクションに対して最大待機時間を分数で指定します。

完了まで待機

アクションが完了するのを待機するように指定します。アクション シーケンスの次のアクションは、このアクションが完了した後に限って実行されます。

注: [アクションの完了]ドロップダウンリストは、長期に実行されるアクションにのみ表示されます。

7. 要求された情報をフィールドに入力します。
8. チケットがサードパーティによる承認が必要な場合は、[ヘルプ デスク承認]チェック ボックスをオンにします。

注: このオプションを使用するには、CA SDM を設定する必要があります。

[チケットタイプ]および[テンプレート]フィールドが有効になります。

注: ヘルプ デスク承認要件を指定するアクションは、アクションのスケジュールには使用できません。スケジュール済みアクションに同じアクションを必要とする場合は、ヘルプ デスク承認要件が含まれない、2 つ目のアクションを作成します。

9. チケットを承認後に自動的にクローズする場合は、[承認または拒否時にチケットを自動的にクローズ]を選択します。
10. [チケットタイプ]ドロップダウンリストからチケット タイプを選択します。以下のタイプは有効なオプションですが、設定によって異なります。

- デフォルト
- インシデント
- 問題
- 要求

[テンプレート]ドロップダウンリストは選択したチケット タイプに関連付けられたテンプレートで更新されます。

11. [テンプレート]ドロップダウン リストからテンプレートを選択します。

使用しているチケット モデルに応じて事前定義された値が各フィールドに入力されます。

12. [保存]をクリックします。

確認メッセージにより、正常に保存されたことが通知されます。

テストのために[アクション]ページからアクションを実行するには、アクションを選択して[アクションの実行]アイコンをクリックします。

アクション タイプ

利用可能なアクション タイプにはいくつかのカテゴリがあります。

注: 任意の操作で特殊文字または予約文字を使用する場合、オペレーティング システムおよびシェル動作を考慮する必要があります。動作には、オペレーティング システム シェルによって実行されるカスタム スクリプトの呼び出しが含まれています。シェル動作、および特殊文字をエスケープする方法の詳細については、Microsoft TechNet の Web サイト

<http://technet.microsoft.com/en-us/library/cc723564.aspx> を参照してください。

事前定義済みアクション タイプ

事前定義済みアクション タイプは、ルールにアクションを作成する場合に使用できる一般的に用いられるアクションです。アクション タイプは呼び出しコマンドライン ユーティリティです。すべてのアクション タイプは、ユーザ インターフェースの[ポリシー]ページの[アクション & ルール]ページにリスト表示されています。

注: アクション タイプの詳細な説明については、「オンライン ヘルプ」を参照してください。

カスタム アクション タイプ

完全なコマンドラインを入力する代わりに、代替文字列を使用して、カスタム アクション タイプを作成できます。カスタム アクション タイプは事前定義済みアクション タイプのドロップダウンリストに追加されます。ユーザ インターフェースの[管理]ページで、一般的に、カスタム アクションへのユーザ アクセスを制御したり、個別のカスタム アクションへのアクセスを制御できます。

[コマンド スクリプトの実行]アクション タイプでは、サーバ上で複数のアクションを実行できる文字列代替を提供します。文字列代替によって、より柔軟なルールを提供し、カスタム スクリプトの必要性を削減します。以下の文字列代替が利用可能です。

- %ACTIONNAME%
- %EVENTMESSAGE%
- %EVENTSOURCE%
- %RULENAME%
- %SERVER%
- %SERVICE%

以下の文字列代替はアクション シーケンスで実行されるアクションにのみ有効です。

- %STDOUT% - 標準出力
- %STDERR% - 標準エラー
- %EXITCODE% - アクション終了コード

アクション シーケンス

アクション シーケンスはアクション タイプとして処理され、[ポリシー]ページで他のアクション タイプと共にドロップダウンリストに表示されます。アクション シーケンスでは、指定されたシーケンスでルールに複数のアクションを定義し、単一のアクションとしてそれらを実行することができます。名前指定したアクションのシーケンスを保存できます。また、そのシーケンスは繰り返して使用できるように管理データベースに保存されます。ユーザ インターフェースの[ポリシー]-[アクション & ルール]ページを使用して、ジョブとしてアクション シーケンスをスケジュールできます。アクション シーケンスに対する CA SDM サポートは、他のアクション タイプに対する処理とは異なります。シーケンスで実行される個々のアクションにヘルプ デスク承認を設定できますが、ヘルプ デスク承認をアクション シーケンス全体に設定することはできません。

アクション シーケンスを使用する場合は以下の重要な点を考慮します。

- 無限ループを作成するシーケンスは設定しないでください。アクション シーケンスは同期的に実行されますが、いくつかのアクションは非同期的に実行されます。そのため、特定のアクションに対して返される時にタスクが完了していることを期待する場合は、注意して使用してください。一般的に長期間実行している同期的なアクションには `-wait` パラメータがあり、戻る前、または指定されたタイムアウトの後で、タスクが完了するまで待機させます。
- アクション シーケンスに関連付けられているアクションを削除しようとすると、製品によって、そのアクションが削除されないように阻止されます。
- アクション シーケンスが異常終了した場合は、ポリシー マネージャが再起動するときに、最新の既知のシーケンスで再起動します。進行中のアクション シーケンスは、手動でユーザ インターフェースまたは Web サービスから取り消すことができます。
- アクション シーケンスで実行しているカスタム アクションに `%STDOUT%` (標準出力)、`%STDERR%` (標準エラー)、または `%EXITCODE%` (アクションリターンコード) の代替文字列アクションを指定する場合、前のアクションの標準出力/標準エラー/終了コードは、現在のアクションにパイプ処理することができます。パイプ処理では、次のアクションの入力に最初のアクションの出力を使用します。アクションの出力をリダイレクトすると、それを次のアクションにパイプ処理することはできません。たとえば、カスタム アクション `ipconfig` が `ipconfig_output.txt` という名前のテキストファイルにリダイレクトされた場合、次のアクションのパイプ処理にその出力を使用することはできません。

カスタム アクションの作成

代替パラメータを定義することによりカスタマイズされたアクション タイプを作成できます。カスタム アクション タイプは、事前定義済みアクション タイプと共に [アクション タイプ] ドロップダウンリストに追加されます。

次の手順に従ってください:

1. [エクスプローラ] ペインで [データ センター] ノードを選択します。
2. [リソース]-[ポリシー] をクリックし、次に、[カスタム アクション タイプ] タブをクリックします。

[カスタム アクション タイプ] ページが表示されます。

3. [+] (追加) をクリックします。
[カスタム アクション タイプ: 新規追加] セクションが表示されます。
4. 以下のフィールドに入力して新しいアクション タイプと代替パラメータを定義し、次に、[保存] をクリックします。

アクション タイプ名

新しいアクション タイプの名前を定義します。

コマンド

アクション タイプのコマンドライン構造を定義します。コマンドの一部として置換する場合に、%SERVER%、\$MYKEY\$ などの代替パラメータを定義できます。代替キーは、1 つのコマンドあたり 1 回のみ使用できます。たとえば、%SERVER% 代替キーは、コマンド内で 1 回のみ使用できます。

代替キー

代替キーに一意の文字列を定義します。代替キー名はコマンドに定義されている名前と一致する必要があります。複数の代用キーを定義する場合は、それぞれの代替キーを個別に定義する必要があります。

プロンプト

アクションを作成するときに入力する代替パラメータに関連付けられた引数名を定義します。

デフォルト値

デフォルト代替キー値を定義します。

新しいパラメータが代替パラメータリストに表示されます。

5. [アクション] ドロップダウンリストから[保存] を選択します。
カスタム アクション タイプが保存されます。

アクション シーケンスの定義

ルールには、アクション シーケンスを定義できます。ルールの条件が **true** に評価された場合、定義したアクション シーケンスが実行されます。また、カスタム条件を作成し、シーケンスにそれらを構築することもできます。

注: アクション シーケンスは、ジョブとしてスケジュールしたり、`dmpolicy runaction` CLI コマンドを使用して実行することもできます。

次の手順に従ってください:

1. [エクスプローラ]ペインで[データ センター]ノードを選択します。
2. [リソース]-[ポリシー]をクリックし、次に、[アクション]タブをクリックします。
[アクション]ページが表示されます。
3. [+] (新しいアクションの追加) をクリックします。
[アクションの定義: 新規]セクションが表示されます。
4. アクション シーケンスに意味のある名前を入力し、[タイプ]ドロップダウン メニューから[アクション シーケンスの実行]を選択します。
[条件ロジック]セクションが表示されます。
5. 異常終了の後にシーケンスを再起動するには、[中断の場合再起動]チェックボックスをオンのままの状態にします。シーケンスは、実行された前回のアクションを再起動して続行します。異常終了の後にシーケンスを続行しない場合は、このチェックボックスをオフにします。
6. アクション シーケンスにアクションを追加するには、[アクション シーケンス]ペインで[+] (アクションの追加) をクリックします。[アクションの追加]は、アクション シーケンスの最後に新しいアクションを追加します。シーケンスの途中にアクションを挿入する場合は、挿入位置の後のアクションをすべて削除します。新しいアクションを挿入した後、削除したアクションを再定義します。
7. アクション シーケンスの条件ロジックを構築する条件を選択します。新しい条件ロジックは、条件ロジック シーケンスの最後にのみ追加できます。シーケンスの途中に新しい条件ロジックを挿入する場合は、挿入位置の後の条件ロジックをすべて削除します。新しい条件ロジックを挿入した後、削除した条件ロジックを再定義します。

- 追加の条件ロジックシーケンスにそれぞれ条件ロジック評価のタイプを選択します。出力タイプには、以下のものがあります。

ReturnCode

アクションリターンコードを評価します。

注: リターンコードの評価用の有効な比較演算子は、==、!=、>、<、>=、<= です。

STDOUT

特定の文字列の標準出力を検索します。

STDERR

特定の文字列の標準エラーを検索します。

注: STDOUTとSTDERRの有効な比較演算子は「指定の語句を含む」および「次を含まない」です。

注: [論理演算子]フィールド(AND/OR)を使用して条件をリンクできます。
[論理演算子]は、最終条件では **NOOP** に自動的に設定されます。

新しい条件ロジックはシーケンスに追加されます。

- 条件の入力が完了したら、[条件の保存]をクリックします。

条件が保存されます。

- [アクション シーケンス]ペインで[保存]をクリックします。

アクションが保存されます。

テストのために[アクション]ページからアクションを実行するには、アクションを選択して[アクションの実行]アイコンをクリックします。

スケジュールの定義

事前定義された時刻にアクションが実行されるようにスケジュールできます。たとえば、デフォルトの **Windows** スケジューラを使用して毎日実行される必要があるアクションをスケジュールしたり、保守タスクのように定期的に実行されるアクションをスケジュールできます。

次の手順に従ってください:

- [エクスプローラ]ペインで[データ センター]ノードを選択します。

2. [リソース]-[ポリシー]をクリックし、次に、[スケジュール済みアクション]タブをクリックします。

[スケジュール済みアクション]ページが表示されます。

3. 以下のフィールドを指定します。

名前

スケジュール済みアクションの名前を定義します。

事前通知

スケジュールされたアクションが実行される前にイベントを生成するかどうかを指定します。イベントがダッシュボードに表示されます。

事後通知

スケジュールされたアクションが実行された後でイベントを生成するかどうかを指定します。イベントがダッシュボードに表示されます。

頻度

スケジュール済みアクションが実行される頻度を指定します：一度のみ、日単位、週単位、月単位(日)または月単位(曜日)。

日付

スケジュール済みアクションを開始する日付を定義します。

時間

スケジュール済みアクションを実行する時間を定義します。

注：ジョブのスケジュールには使用されないため、秒を入力する必要はありません。

タイプ

スケジュールしているアクションに使用されたアクション タイプを指定します。

注：スケジューラでは、代替パラメータを含むアクションがサポートされていません(唯一の例外は %AutoIncrement(0)% と %AutoDecrement(0)% です)。代替パラメータが含まれるアクションは、ポリシー ルール評価を介してのみ実行できます。

アクション

各アクション タイプにすでに作成されたアクションをリスト表示します。

注：リストには、ヘルプ デスクの承認要件を指定するアクションは含まれていません。

4. ドロップダウンリストから[保存]を選択します。

アクションがスケジュールされることを確認するメッセージが表示されます。スケジュールされたアクションが、[スケジュール済みアクション]リストのスケジュール済みのジョブのリストに表示されます。

注: ヘルプ デスク承認要件を指定するアクションは、アクションのスケジュールには使用できません。スケジュール済みアクションに同じアクションを必要とする場合は、ヘルプ デスク承認要件が含まれない、2 つ目のアクションを作成します。

ポリシーのユース ケース

以下のシナリオでは、ポリシーを実装するためのいくつかのユース ケースについて説明します。

関連項目:

[ユース ケース: サーバをサービスに追加する \(P. 158\)](#)

[ユース ケース: 新規ルールをサービスに追加する \(P. 159\)](#)

[ユース ケース: アクションを定義する \(P. 159\)](#)

ユース ケース: サーバをサービスに追加する

このユース ケースでは、サーバを事前に作成されたサービスに追加するプロセスについて示します。

1. サーバをサービスに追加するための前提条件を確認します。
 - サービスが存在している。
 - サーバが存在している。
 - サービスにはすでに優先度が割り当て済みである。
 - ユーザにはサービスを変更するアクセス権がある。

2. サーバをサービスに追加します。
3. サーバをサービスに追加した結果を確認します。
 - このサーバは現在サービスのメンバである。
 - このサーバは現在サービスの使用率に含まれている。
 - このサービスを含めたことで、使用率に対するすべてのサービスルールに影響する。

ユース ケース: 新規ルールをサービスに追加する

このユース ケースでは、新規ルールをサービスに追加するプロセスを説明します。

1. ルールをサービスに追加するための前提条件を確認します。
 - サービスが存在している。
 - ユーザにルールを作成するアクセス権がある。
 - サーバがサービス内にある。
2. このサービスに対するルールの定義を作成します。
3. ルールをサービスに追加した結果を確認します。
 - 新規ルールが作成されている。
 - 新規ルールがルールの条件に有効なすべてのサービスについて評価している。

ユース ケース: アクションを定義する

このユース ケースでは、スケジューリング ジョブまたはポリシー ルールで使用するアクションを定義するプロセスについて示します。

1. アクションを定義するための前提条件を確認します。
 - ユーザにアクションを定義するアクセス権がある。
 - 目的のアクション定義に必要なリソースが検出されている。

2. CA Virtual Assurance ユーザ インターフェイスでアクションの属性およびアクションの名前を定義します。
3. サーバをサービスに追加した結果を確認します。
 - アクションはユーザによって提供された説明で作成されている。
 - アクションは現在ルールで利用できる。
 - アクションは現在ジョブスケジューリングで利用できる。

注: ヘルプ デスク承認要件を指定するアクションは、アクションのスケジュールには使用できません。スケジュール済みアクションに同じアクションを必要とする場合は、ヘルプ デスク承認要件が含まれない、2 つ目のアクションを作成します。

データ収集の設定

以下のデータがデータ センターに収集される方法を制御できます。

- メトリック収集が発生する時間間隔。
- メトリック(フィルタリング)を収集するシステム。
- 各サーバに収集されるメトリック。
- データの経過期間およびデータの有効期限(データを保持する期間)。

関連項目:

[メトリック収集に関する重要な点](#) (P. 161)

[データ センター用のデータ収集の設定](#) (P. 164)

[サーバ用のデータ収集の設定](#) (P. 165)

[仮想リソース用のデータ収集の設定](#) (P. 167)

[パフォーマンスしきい値の設定](#) (P. 170)

[メトリックフィルタの設定](#) (P. 171)

メトリック収集に関する重要な点

メトリックを選択する場合に、十分な情報を得たうえでの決定を行うために、以下の点について確認し、CA Virtual Assurance のパフォーマンスおよびアプリケーション メトリック収集について理解します。

- CA Virtual Assurance はどのようにしてメトリック データを収集するのですか。CA Virtual Assurance は、リモートコンピュータ上で CA パフォーマンス エージェントまたは SystemEDGE エージェントと通信して指定されたシステム メトリックを収集します。CA パフォーマンス エージェントは NSM パフォーマンス エージェントの軽量バージョンです。NSM パフォーマンス エージェントがインストールされている場合は、CA Virtual Assurance もそのエージェントをポーリングできます。

注: CA パフォーマンス エージェントは NSM パフォーマンス エージェントとは異なる動作をするため、Linux 上で収集できるメトリックは使用するエージェントによって異なります。

NSM パフォーマンス エージェントまたは SystemEDGE エージェントをすでに使用していない限り、CA パフォーマンス エージェントまたは SystemEDGE エージェントが基本システム メトリックを収集する任意のサーバにインストールされている必要があります。NSM パフォーマンス エージェントまたは SystemEDGE エージェントが存在する場合、CA パフォーマンス エージェントは必要ありません。必要な場合は、製品のユーザ インターフェースを使用して SystemEDGE エージェントをインストールできます。すべてのパフォーマンス メトリックはパフォーマンス DB 内に格納されます。

- どのようにして全体的な使用率が計算されますか。全体的な使用率とは、CA Virtual Assurance によって管理されたサーバで現在収集されているすべてのメトリックの集計です。この計算は、メトリックの値および通常操作のパラメータを定義するユーザ定義のしきい値に基づいています。ユーザ インターフェースの[ポリシー]、[メトリック]、[しきい値]セクションで[全体使用率計算に含める]を選択しない限り、収集用に選択した任意の新しいメトリックは全体的な使用率の計算に使用されません。これを行うと、サーバの状態を評価するときに、CA Virtual Assurance は **false** の結果を表示しません。

- メトリック評価によって全体的な使用率にどのような影響がありますか。テーブルに示されたメトリックの詳細は、**CA Virtual Assurance** が異なるメトリックを評価する方法を理解するのに役立ちます。各メトリックのメソッドのプロパティには**厳密**または**補足**のいずれかが設定されています。厳密値が高いと、全体的な使用率の増加を示すため、低い厳密値よりも悪いシナリオになります。補足値が高いと、全体的な使用率の減少を示すため、肯定的なシナリオになります。一般的に、厳密値が高いと全体的な使用率にマイナスに影響し、厳密値が低いと全体的な使用率にプラスに影響します。対照的に、補足値が高いと全体的な使用率にプラスに影響し、補足値が低いと全体的な使用率にマイナスに影響します。たとえば、[メモリ: コミットされた使用中のバイト数の割合]の値が増加すると、システムの全体的な使用率は増加します。[メモリ: 利用可能 (MB)]の値が増加すると、全体的な使用率は減少します。

- デフォルトメトリックとは何ですか。デフォルトメトリック定義は、すべてのサポートされているプラットフォームの[フィルタ]セクションのメトリックリストにあります。デフォルトメトリックインジケータはメトリックリストにあり、[デフォルト]列で[はい]の値を使用して検索できます。新しいサーバが追加された場合、CA Virtual Assuranceはこのリストを使用してメトリックの定義を取得します。プラットフォーム、タイプ、サブタイプ、インスタンスおよび[フィルタ]セクションで収集するデータのタイプを設定できます。各サーバのメトリックフィルタおよび定義はパフォーマンスDBに格納されます。
- 現在システムでパフォーマンスデータを利用できますか。デフォルトでは、データを収集できない場合、データの欠如はサーバの重大度に反映されないため、CA Virtual Assuranceがサーバの状態に悪影響を及ぼすことはありません。イベントリストを確認するか、または特定のシステムを選択することによって、メトリックデータが収集されたかどうかを特定できます。ただし、これをより迅速に特定するための手段が必要な場合、またはパフォーマンスデータが重大である場合は、パフォーマンスデータを収集できないときにシステムの状態を自動的に警告または重大に変更するようにCA Virtual Assuranceを設定できます。パフォーマンスデータが利用できないシステムを簡単に識別できるようにするには、CA Virtual Assurance *install_path*\conf ディレクトリに配置されている *caaipconf.cfg* ファイルを変更します。テキストエディタでファイルを開いてヘルス状態のプロパティを以下のようにして検索します。

```
<プロパティ名="CONFIG_KEY_DEFAULT_HEALTH_STATE">
    <!-- 有効な値: 0 (不明)、5 (OK)、10 (警告)、15 (マイナーな障害)、20 (メジャーな障害)、
25 (重大な障害) -->
    <!-- CA_ComputerSystem に関連付けられた CA_CollectionState オブジェクトの
HealthState の値を変更します -->
    <!-- 30 に設定された場合、CE は HealthState を設定しません。 -->
    <value>5</value>
    <displayName>メトリックまたはデータ収集で問題が発生した場合はデフォルトのノードのヘルス
状態</displayName>
</property>
```

XML 要素の値によって囲まれた値を 5 (OK) または 10 (警告) などのほかのサポートされている値の 1 つに変更することによって、CA Virtual Assurance はパフォーマンスデータが収集されなかった場合、希望する状態を反映します。

例:

```
<プロパティ名="CONFIG_KEY_DEFAULT_HEALTH_STATE">
    <!-- 有効な値: 0 (不明)、5 (OK)、10 (警告)、15 (マイナーな障害)、20 (メジャーな障害)、
25 (重大な障害) -->
    <!-- CA_ComputerSystem に関連付けられた CA_CollectionState オブジェクトの
HealthState の値を変更します -->
    <!-- 30 に設定された場合、CE は HealthState を設定しません。 -->
    <value>10</value>
```

```
<displayName>メトリックまたはデータ収集で問題が発生した場合はデフォルトのノードのヘルス  
状態</displayName>  
</property>
```

<value> が「10」に変更されたため、パフォーマンス データが利用可能でないシステムは、CA Virtual Assurance ユーザ インターフェースに警告の状態が表示されます。

注: パフォーマンス メトリックおよび説明のリストについては、「リファレンス ガイド」を参照してください。

データ センター用のデータ収集の設定

データ センター レベルでデータ収集を設定できます。データ センター レベル ポリシーはすぐに有効になります。

次の手順に従ってください:

1. [リソース]をクリックして、[エクスプローラ]ペインで[データ センター]フォルダを選択します。
2. 右クリックし、[ポリシー]-[収集の設定]を選択します。
[設定]ダイアログ ボックスが表示されます。
3. [収集設定]セクションで以下のフィールドに入力します。

[データ記録間隔 (秒)]

パフォーマンス DB にデータが収集されて保存される頻度を定義します。

デフォルト: 300 秒

[ポーリングされたデータの保持 (日数)]

パフォーマンス DB にポーリングされたデータを保存する期間を定義します。この数を定義する場合は、収集された管理対象システム、サービスおよびメトリックの数を考慮します。保存されたポーリング済みデータオブジェクトが徐々に蓄積されて、パフォーマンスに影響を与える場合があります。パフォーマンスの問題が発生する場合は、保存日数の数を減らします。

デフォルト: 14 日

[日単位ロールアップ データの保持 (日数)]

パフォーマンス DB に日単位データの平均を保存する期間を定義します。

デフォルト: 365 日

4. [しきい値]セクションにしきい値の制限を入力し、[保存]をクリックします。
これで、設定が保存されました。

サーバ用のデータ収集の設定

個々のサーバにデータ収集を設定できます。このプロシージャを使用してデータセンターのデータを収集する特定のサーバを設定します。また、モニタするメトリックを選択し、個々のメトリックにしきい値を設定し、全体的な使用率にメトリックを含めることができます。

次の手順に従ってください:

1. [エクスプローラ]ペインを開きます。
利用可能なグループ、サービス、およびシステムが表示されます。
2. [データ センター]フォルダを開き、サーバが属するサービスを選択します。
3. 右クリックし、[ポリシー]を選択します。
[ポリシー]サブメニューが表示されます。
4. [メトリック]をクリックします。
メトリックウィザードが表示されます。
5. データ収集を設定するサーバを選択します。
6. [間隔の設定]ダイアログ ボックスで以下のフィールドに入力します。

デフォルトを使用

オンにした場合はデフォルトとしてデータ センター レベルを指定します。
チェック ボックスをオフのままにする場合は、指定した値が代わりに使用されます。

[データ記録間隔 (秒)]

パフォーマンス DB にデータが収集されて保存される頻度を定義します。

デフォルト: 300 秒

[日単位ロールアップ データの保持 (日数)]

パフォーマンス DB に日単位データの平均を保存する期間を定義します。

デフォルト: 365 日

[ポーリングされたデータの保持 (日数)]

パフォーマンス DB にポーリングされたデータを保存する期間を定義します。この数を定義する場合は、収集された管理対象システム、サービスおよびメトリックの数を考慮します。保存されたポーリング済みデータオブジェクトが徐々に蓄積されて、パフォーマンスに影響を与える場合があります。パフォーマンスの問題が発生する場合は、保存日数の数を減らします。

デフォルト: 14 日

7. [利用可能なメトリック]セクションからモニタするメトリックを選択し、下向き矢印をクリックします。

選択されたメトリックは、[収集対象として選択されたメトリック]セクションに移動します。

注: デフォルトメトリック(CPU とメモリ)を無効にし、他のメトリックを有効にする場合、新しく選択したメトリックのしきい値を変更するまで、全体的な使用率は表示されません。

8. 各サーバでモニタするパフォーマンスメトリックを設定し、各メトリックのしきい値境界を設定できます。しきい値を設定するメトリックを選択し、以下のフィールドに入力します。

上限しきい値

選択したメトリックグループの使用率の上限を定義します。

デフォルト: 80%

下限しきい値

選択したメトリックグループの使用率の下限を定義します。

デフォルト: 20%

全体使用率計算に含める

選択したメトリックを全体的な使用率の計算用を含めて CA Server Automation によって評価されるように指定します。

9. [終了]をクリックして設定を保存します。

仮想リソース用のデータ収集の設定

仮想プラットフォームおよびこれらのプラットフォームで作成されて管理された仮想リソース用のデータ収集を設定できます。特定の仮想マシンまたは他のリソースを設定し、データセンターのデフォルトとは異なる間隔でデータを収集する場合は、このプロシージャを使用します。また、モニタするメトリックを選択し、個々のメトリックにしきい値を設定し、全体的な使用率にメトリックを含めることもできます。

以下の仮想プラットフォーム オブジェクト用のデータ収集を設定できます。

- vCenter Server
- vCenter データ センター
- vCenter ESX Server
- vCenter 仮想マシン
- Hyper-V
- Microsoft クラスタ

- Microsoft クラスタ ノード
- IBM AIX LPAR サーバ
- IBM 論理パーティション
- Solaris ゾーン サーバ
- Solaris ゾーン

仮想リソース用のデータ収集の設定

1. [リソース]をクリックし、[エクスプローラ]ペインを開きます。
2. [データセンター]または[Microsoft Cluster Service]フォルダを展開し、次に任意のサブフォルダを展開し、設定するオブジェクトを選択します。

そのオブジェクトのサブタブが右側のペインに表示されます。

注: トップレベルフォルダ (VMware vCenter Server など) を選択した場合、またはデータが収集されないオブジェクト (vCenter クラスタなど) を選択した場合は、そのフォルダまたはオブジェクトに含まれている特定のオブジェクトを選択してデータ収集を設定する必要があります。

注: トップレベルフォルダとして **MS Cluster Service** を選択すると、クラスタとそれらのノードが表示されます。

3. 右クリックし、[ポリシー]-[サーバ メトリック収集の設定]を選択します。

注: トップレベルフォルダとして **Solaris** ゾーンを選択すると、[システム]セクションの[ハードウェア クラス]列には値[その他]が常に表示されます。

4. [利用可能なメトリック]セクションからモニタするメトリックを選択し、次に、下方向キーをクリックします。

選択したメトリックは、[収集対象として選択されたメトリック]セクションに移動します。

注: デフォルト メトリック (CPU とメモリ) を無効にし、他のメトリックを有効にする場合、新しく選択したメトリックのしきい値を変更するまで、全体的な使用率は表示されません。

5. [保存]をクリックして選択したメトリックを適用します。
6. リソースを右クリックし、[ポリシー]-[収集の設定]を選択します。
7. [収集設定]セクションで以下のフィールドに入力します。

デフォルトを使用

オンにした場合はデフォルトとしてデータ センター レベルを指定します。チェック ボックスをオフのままにする場合は、指定した値が代わりに使用されます。

[データ記録間隔 (秒)]

パフォーマンス DB にデータが収集されて保存される頻度を定義します。

デフォルト: 300 秒

[日単位ロールアップ データの保持 (日数)]

パフォーマンス DB に日単位データの平均を保存する期間を定義します。

デフォルト: 365 日

[ポーリングされたデータの保持 (日数)]

パフォーマンス DB にポーリングされたデータを保存する期間を定義します。この数を定義する場合は、収集された管理対象システム、サービスおよびメトリックの数を考慮します。保存されたポーリング済みデータオブジェクトが徐々に蓄積されて、パフォーマンスに影響を与える場合があります。パフォーマンスの問題が発生する場合は、保存日数の数を減らします。

デフォルト: 14 日

8. [保存]をクリックして、設定を保存します。

注: デフォルトのしきい値が使用されます。しきい値を変更する場合は、これらを別々に実行する必要があります。

パフォーマンスしきい値の設定

各サーバでモニタするパフォーマンス メトリックを設定し、各メトリックのしきい値境界を設定できます。

次の手順に従ってください:

1. [エクスプローラ]ペインを開きます。
利用可能なグループ、サービス、およびシステムが表示されます。
2. [データセンター]フォルダおよび任意のサブフォルダを展開し、設定するサーバを選択します。仮想サーバに移動して仮想マシンまたは論理パーティションなどの特定の仮想リソースを選択します。
3. 右クリックし、[ポリシー]を選択します。
[ポリシー]サブメニューが表示されます。

4. [しきい値の設定]をクリックします。
[しきい値の設定]が表示されます。
5. しきい値を設定するメトリックを選択し、以下のフィールドに入力します。
上限しきい値 (%)
選択したメトリックグループの使用率の上限を定義します。
デフォルト: 80%
下限しきい値 (%)
選択したメトリックグループの使用率の下限を定義します。
デフォルト: 20%
[全体的な使用率の計算用を含める]
選択したメトリックを全体的な使用率の計算用を含めて CA Virtual Assurance によって評価されるように指定します。
6. [変更]をクリックして設定を保存します。

メトリック フィルタの設定

モニタするパフォーマンス メトリックに応じてメトリックをデータセンターのメトリック フィルタに追加したり、メトリック フィルタから削除したりすることができます。

注: NSM パフォーマンス エージェントのユーザに利用可能なパフォーマンス メトリックの詳細については、NSM ドキュメント セットの「*NSM Systems Performance Metrics Help*」を参照してください。

メトリック フィルタを設定する方法

1. [エクスプローラ] ペインで[データ センター]フォルダを選択します。
2. 右クリックし、[ポリシー]-[収集条件の設定]を選択します。
[収集条件]ダイアログ ボックスが表示されます。

3. 以下のいずれかを実行します。

- 既存のメトリックのチェック ボックスをオンにして既存のエントリを変更します。選択されたメトリックの情報は、[詳細]セクションのフィールドに入力されます。任意の変更を加えて、[更新]をクリックします。
- OS を選択し、[詳細]セクションのフィールドに入力して新しいメトリックを追加して、[追加]をクリックします。

メトリックが保存されます。

[詳細]セクションには以下のフィールドがあります。

OS

モニタされているメトリックのオペレーティング システムを定義します。

タイプ

モニタされているメトリックのタイプを定義します。

例:

[タイプ]: CA ディスク グループ

[サブタイプ]: 毎秒(平均) 書き込みます

サブタイプ

メトリックのどの側面がモニタされているか定義します。

例:

[タイプ]: CA ディスク グループ

[サブタイプ]: 毎秒(平均) 読み取ります

インスタンス

MIB 階層の管理対象オブジェクトのインスタンスを定義します。

例:

タイプ: `vmvcaim.StatClusterEffectiveCPU`

サブタイプ: `1.3.6.1.4.1.546.16.52.2.7.2.1.14`

インスタンス: `%3 [%2]`

`%<n>` の `<n>` は、[インスタンス]の下にリスト表示される数値で、それぞれの AIM MIB テーブル内の `n` 番目の列に対応する任意の値に一致します。たとえば、すべての行エントリ(同じ管理対象オブジェクトのインスタンス)には `vmvcAimStatClusterTable`。これは、メトリックがユーザ入力なしで利用可能な場合、すべてのインスタンスの管理対象オブジェクトのメトリックを瞬時に収集するのに役立ちます。

上限しきい値 (%)

選択したメトリックグループの使用率の上限を定義します。

デフォルト: 80%

下限しきい値 (%)

選択したメトリックグループの使用率の下限を定義します。

デフォルト: 20%

遅延

しきい値イベントが生成されるまでに発生したしきい値違反の連続回数を定義します。このオプションを設定し、しきい値を評価するためのイベントがいっぱいになるのを防ぎます。アクションを定義して、しきい値違反イベントをログ記録し、しきい値モニタリングのルールをセットアップすることができます。

方法

収集方法が補足的であるか、補足的なデルタであるか、厳密であるか、または厳密なデルタであるかを指定します。補足的なメソッドには、セットのサブセット内にまだ含まれていないメトリックが含まれます。厳密なメソッドは、指定された厳密なメトリックを収集します。

カテゴリ

モニタされたメトリックがシステム、アプリケーションまたは SNMP メトリックかどうか指定します。

選択されたメトリックをデフォルトで収集

収集エンジンがデフォルトでフィルタによって指定されたメトリックを収集するかどうか指定します。メトリック フィルタがデフォルトとして設定されない場合、収集エンジンは指定されたメトリックを自動的に収集しません。

[全体的な使用率の計算用に含める]

選択したメトリックを全体的な使用率の計算用に含めて CA Virtual Assurance によって評価されるように指定します。

[収集用にアクティブ化]

収集に利用可能なメトリックを評価する場合にメトリック フィルタの使用が有効であると指定します。

4. 削除する任意のメトリックのチェック ボックスをオンにし、次に、[削除]をクリックします。

選択したエントリが削除されます。

ポリシーの UCS アクション タイプ

CA Virtual Assurance では、ブレードの電源操作およびサービス プロファイル操作に対して Cisco UCS アクション タイプが提供されます。

関連項目：

[ブレード電源アクションの作成](#) (P. 175)

[サービス プロファイル](#) (P. 112)

[サービス プロファイルの作成または更新を実行する方法](#) (P. 113)

[サービス プロファイルとブレードの関連付け](#) (P. 178)

ブレード電源アクションの作成

ブレード電源操作を行うためのアクションを定義できます。

ブレード電源アクションを作成する方法

1. [リソース]をクリックし、[エクスプローラ]ペインを開きます。
2. [データ センター]ノードを選択し、[ポリシー]をクリックします。
3. [アクション]をクリックします。
[アクション]ページが表示されます。
4. [+] (新しいアクションの追加)をクリックします。
[アクションの定義: 新規]ページが表示されます。
5. [タイプ]ドロップダウンリストで[電源の設定]をクリックします。
6. [環境]ドロップダウンリストで[Cisco UCS]をクリックします。
[電源の設定]フォームが表示されます。
7. 電源操作を実行するブレードを指定するために、ブレードが含まれる UCS Manager とシャーシを選択します。
8. 電源操作を選択し、[アクション]ドロップダウン メニューの[保存]をクリックします。
ブレード電源アクションが作成されます。

サービス プロファイル

サービス プロファイルには、インターフェース、ファブリック接続性、およびネットワークとサーバの ID など、Cisco UCS ハードウェアに関する設定情報が含まれます。特定の UCS Manager 用の、または CA Virtual Assurance 管理 DB に一元化されたサービス プロファイルを作成できます。UCS Manager 上のサービス プロファイルは 管理 DB にインポートでき、そこから他の UCS Manager にエクスポートできます。

サービス プロファイルで、オペレーティング システムからの Cisco UCS ハードウェアの抽出のサポートが可能になります。サービス プロファイルを追加または削除して、サービスをオンラインまたはオフラインにすることができます。1 つのブレードから別のブレードにサービス プロファイルを割り当て直すことで、サービス (オペレーティング システムとアプリケーション) のセットを別のサーバに移動できます。

サービス プロファイル情報には、次のものを含めることができます。

- デバイス UUID または仮想 UUID プールごとのブレード サーバ
- ローカル ストレージ、RAID、または SAN (HBA、WWNN、および WWNN プール) の任意の設定内のストレージ
- ネットワーキング (MAC、vNIC 0、vNIC 1、および MAC プール)
- サーバの起動順序または他のポリシー
- サーバ割り当てのタイプ (後で割り当て、スロットを事前にプロビジョニング、既存のサーバをプロビジョニング、プールからサーバを選択)

サービス プロファイルの作成また更新を実行する方法

CA Virtual Assurance には、管理者がサービス プロファイルを作成できるウィザードが用意されています。また、事前定義済みポリシー オプションを使用してサービス プロファイルを更新できます。システム、ネットワーク、およびストレージの管理者は、協力して、一意の ID 特性や必須の接続特性を持つサービス プロファイルを作成できます。

サービス プロファイル ウィザードでは、Cisco 環境における知識と経験を活用できる Cisco UCS Manager インターフェースのサブセットが提供されます。

例: サービス プロファイルの作成

CA Virtual Assurance ユーザ インターフェースで、[作成]-[サービス]-[プロファイル]オプションを選択し、作成するサーバ プロファイルの名前を指定して、サーバ プロファイルを以下のいずれにするかを選択します。

- ハードウェア ベース
- デフォルトのネットワークおよびストレージの接続を使用するシンプルなサーバ プロファイル
- 既存のサービス プロファイル テンプレート ベース
- 明示的に作成する必要があるカスタム サービス プロファイル

ウィザードでは、選択されたオプションに基づいたインタビュー プロセスに従い、必要な ID 情報や接続情報を指定します。デフォルトを使用することも、ID (UUID)、ネットワーク (MAC/VLAN)、ストレージ (WWN/vHBA)、およびブート ポリシー情報を明示的に指定することもできます。

サービス プロファイルとブレードの関連付け

サービス プロファイルは、ブレードとの関連付けと関連付け解除、およびフェールオーバー時に適用する設定を行うことができます。

UCS サービス プロファイルを調整する方法

1. 右クリックし、[ポリシー]を選択します。
[ポリシー]サブメニューが表示されます。
2. 右クリックし、[ポリシー]-[アクション & ルール]を選択します。
[アクション & ルール]ページが表示されます。
3. [アクション]をクリックします。
[アクション]ページが表示されます。
4. [+] (新しいアクションの追加) をクリックします。
[アクションの定義: 新規]ページが表示されます。
5. [タイプ]ドロップダウンリストでアクション タイプ[サービス プロファイルの設定]をクリックします。
[サービス プロファイルの設定]フォームが表示されます。
6. サービス プロファイルを適用する UCS リソースの詳細を指定します。プロファイル操作を選択します。

注: ヘルプ デスクの承認が必要な場合は、必要に応じて情報を入力します。
7. [アクション]ドロップダウンの[保存]をクリックします。
サービス プロファイルの関係が変更されます。

ポリシー設定

CA Virtual Assurance ユーザ インターフェースから一元化されたリモート展開を使用して、1 回の操作で管理対象エージェントを設定し、その設定を複数のシステムに設定を適用できます。ポリシー設定を使用すると、SystemEDGE と SRM AIM を一元化された場所で設定し、一貫性、信頼性、安全性のいずれにも優れた方法で企業全体にポリシーを配布できます。

CA Virtual Assurance を使用したリモートポリシー設定には、以下の利点があります。

- 複数のモニタリング プラットフォームにわたって使用する、プラットフォームに依存しないモニタリング ポリシーの作成
- 単一のサーバにもサーバのグループにも設定ポリシーを適用可能
- 1 つのポリシーに組み合わせることができるモニタリング テンプレートの作成
- 設定イベントおよびアクションの監査証跡
- イベントとレポートを通じた企業全体にわたるポリシー コンプライアンスの追跡
- 展開ソリューションとの統合、および、展開と同様、ターゲット システム上のフットプリントの最小化
- 数千の同時設定への拡張
- 複数のエージェント設定ソース (CA Virtual Assurance、NSM、SystemEDGE など) に対するサポート、および CA Virtual Assurance を通じた変更の受け入れまたは拒否
- SystemEDGE によってロードされた AIM のリモートからの制御
- 将来のポリシー設定するための既存の SystemEDGE 設定のインポート
- 個々に OID 番号を入力する必要がなくなる多数のモニタ定義設定時の選択リスト
- 手動でインデックスを定義する必要がなく、競合を回避できる自動モニタ インデックス割り当て

関連項目

[SystemEDGE ポリシーを作成する方法](#) (P. 180)

[SRM ポリシーを作成する方法](#) (P. 192)

[マシンへのポリシーの適用](#) (P. 196)

[ポリシー適用の進捗状況の確認](#) (P. 197)

[適用されるポリシーの設定と表示](#) (P. 198)

[エージェント ポリシーのダッシュボードビュー](#) (P. 200)

[例: ユーザ固有のメトリック \(MIB 拡張\) をモニタする方法](#) (P. 201)

[例: 特定の Windows パフォーマンス レジストリのメトリックをモニタする方法](#) (P. 203)

SystemEDGE ポリシーを作成する方法

モニタのセット、ロードする AIM、基本設定、その他エージェントの実行方法とモニタ対象を制御する設定を定義するには、SystemEDGE ポリシーを作成します。作成したポリシーは、管理対象モードで SystemEDGE エージェントを実行する任意の数のシステムに適用できます。ポリシーを使用すると、ローカルで手動によって設定できるすべての設定操作を実行できるうえに、統合されたインターフェース、選択リスト、およびリモートシステムへの動的展開といった利点が得られます。

SystemEDGE ポリシーを作成するには、以下の手順に従います。

1. [リソース]タブをクリックして[設定]ペインを開き、[ポリシー]を展開して[SystemEDGE]をクリックします。
[SystemEDGE]ペインが表示されます。
2. [利用可能ポリシー]ツールバーの[+] (新規)をクリックします。
[新規 SystemEDGE ポリシー]ダイアログ ボックスが表示されます。
3. ポリシーの名前と説明、および既存のポリシーをベースにするかどうかを入力し、[OK]をクリックします。
ポリシーが作成され、右側のペインに設定画面が表示されます。
4. [ポリシーに含めるモニタを定義します](#) (P. 180)。
5. [制御設定を定義します](#) (P. 181)。
6. [SNMP 設定を定義します](#) (P. 188)。
7. [MIB 拡張を定義します](#) (P. 192)。
8. [ポリシーの保存]をクリックします。
ポリシーが保存されます。

モニタ定義

ポリシーを設定する際、[モニタ]タブをクリックすると、現時点で定義済みのすべてのモニタのサマリが表示されます。[モニタ]タブには、以下のモニタを定義するためのサブタブがあります。

- セルフ モニタ
- プロセス モニタ
- ログ ファイル モニタ

- Windows イベント モニタ
- 履歴モニタ
- プロセス グループ モニタ

これらの各サブタブから、モニタの新規作成、既存のモニタの変更と削除、およびモニタのコピーを実行できます。設定ポリシーを使用してモニタを定義すると、ローカルのファイル操作では利用できない、以下の機能上の利点が得られます。

- 直観的なフィールド名
- 自動インデックス作成
- モニタを特定のプラットフォームに制限できるプラットフォーム指定
- 個々の OID 番号を覚えて入力する必要がない、セルフ モニタ用のオブジェクト クラスおよび属性の選択リスト
- ほかのモニタ内の主要なプロパティの選択リスト
- ログ ファイルとディレクトリのどちらをモニタするかを指定でき、利用可能なフィールドを動的に調節するログ ファイル モニタリングのモニタ タイプ指定
- フラグ設定用に 16 進数の文字列を入力する必要のない、フラグ設定用の個別チェック ボックス

注: これらの 16 進法フラグの説明については、`sysedge.cf` 設定ファイルまたは「SystemEDGE ユーザ ガイド」を参照してください。

- モニタに統合された保守ウィンドウ設定

設定ポリシーの個別モニタを定義する方法の詳細については、オンライン ヘルプを参照してください。

SystemEDGE ポリシー制御設定の定義

SystemEDGE ポリシー コントロール設定を使用して、以下のエージェント動作を制御できます。

- セキュリティ設定
- SNMP の設定
- MIB テーブルへのデータのロード
- UNIX の設定
- パフォーマンス モニタリングの設定

ポリシーで定義された制御設定をすべてのマシンに適用できます。

次の手順に従ってください:

1. [リソース]タブをクリックして[設定]ペインを開き、[ポリシー]を展開して[SystemEDGE]をクリックします。
[利用可能ポリシー]ページが表示されます。
2. [利用可能ポリシー]テーブルでポリシーを選択します。
ポリシーの[サマリ]ページが表示されます。
3. [制御設定]をクリックします。
[コントロール]ページが表示されます。
4. (オプション)[デフォルトを使用]をクリックします。
デフォルトの選択ペインが表示されます。デフォルトの設定を変更できます。
5. 以下の制御設定を行います。

SNMP

以下の基本的な SNMP プロパティを定義できます。

バインド アドレス

エージェントがバインドし、受信 SNMP リクエストをリスンするインターフェースを指定します。有効なアドレスは IPv4 または IPv6 のアドレスです。

注: 対応するデフォルトのポートはインストール中に指定します。

バインド ポート

SNMPトラップを送信するために、エージェントがバインドするトラップポートを指定します。bind_address が指定されていない場合、エージェントは利用可能なすべての UDP アドレスにバインドします。

デフォルト: システムによって選択されたポート

IP ファミリ

エージェントの通信方法(IPv4 のみ、IPv6 のみ、またはその両方)を指定します。デフォルトでは、エージェントは、IPv4、IPv6 の順に使用を試行します。

FIPS モード

FIPS 準拠の暗号化を使用するように、エージェントを指定します。CA eTrust 公開鍵インフラストラクチャ ライブラリを有効にするには、[非 FIPS モード]を選択します。この方法が失敗する場合は、内部の最低限のセキュリティソリューションにフォールバックします。FIPS 準拠の暗号化を有効にするには、[FIPS 共存モード]を選択します。この方法が失敗する場合は、CA eTrust 公開鍵インフラストラクチャ ライブラリにフォールバックします。RSA BSAFE Crypto-C Micro Edition FIPS を有効にするには、[FIPS のみのモード]を選択します。この方法が失敗する場合は、暗号化は実行されません。

デフォルト: 非 FIPS モード

トラップ ソース

トラップを送信するために使用されるソース アドレスを指定します。有効なアドレスは IPv4 アドレス、IPv6 アドレス、またはホスト名です。

デフォルト: エージェントのホスト名

セキュリティ設定

以下のセキュリティ基本設定を定義できます。

認証トラップ

エージェントが認識できないという、コミュニティ名を備えた SNMP メッセージをエージェントが受信した場合に、認証失敗トラップを送信します。

デフォルト: 無効

プロセス セット

プロセステーブルおよび Running Software テーブルで、エージェントシステム上で実行されているプロセスや他のソフトウェアにアクセスできます。これらのテーブルで SNMP セットを許可すると、セキュリティの問題が発生する場合があります。

リモート シェル グループ

管理システムは、リモートシェルグループを使用して、エージェントシステム上でシェル スクリプトおよびプログラムを実行するようにエージェントに対してリモートから指示できます。このタイプの情報が漏えいすると、潜在的なセキュリティリスクが発生する可能性があります。

実行アクション

しきい値違反が発生したときに、モニタリング テーブルを使用したアクション コマンドの実行を有効にします。アクション コマンドおよびスクリプトを実行する機能が原因で、セキュリティ上の問題が発生する可能性があります。

MIB テーブルへのデータのロード

Systems Management MIB の以下のテーブルに入力します。

- プロセス テーブル
- ユーザ グループ テーブル
- Who テーブル
- トラップ コミュニティ テーブル
- ミラー テーブルのモニタ
- ミラー テーブルを集計
- トップ プロセス テーブル

各テーブルには、MIB で公開可能な機密情報か、ディスク領域を節約するために無効にできる重要でない情報のいずれかが含まれています。デフォルト設定では、プロセス テーブルを除くすべてのテーブルにデータをロードできます。

その他

以下のその他の設定を定義できます。

SNMP を使用してエージェントが更新されるのを許可

SNMP SET を使用したエージェントの更新を許可します (書き込みコミュニティの削除など)。エージェントで SNMP セットを許可した場合、この方法で更新すると、SNMP セットの変更が通知され、システムのポリシー詳細を表示すると例外が発生します。

マネージャに設定の更新を通知

エージェントが処理する SNMP 設定リクエストすべてについて、エージェントによるマネージャへの通知送信を可能にします。

ウォーム スタートのディスカバリ

ウォーム スタート設定が更新されるたびに、すべてのデバイスでエージェントが再検出されます。デバイスが多数あるシステムを管理している場合、ウォーム スタートのたびにディスカバリが実行されると、非常に多くの時間とリソースを消費する場合があります。

Perl 互換正規表現を使用

Perl 互換正規表現 (PCRE) を使用すると、正規表現をサポートするモニタを定義するときに i18n 互換の正規表現を指定できます。正規表現の例には、ログ ファイル、プロセス、プロセスグループ、Windows サービスおよび Windows イベントがあります。また、このオプションを使用して、より複雑な正規表現を作成できます。このオプションは、SystemEDGE エージェント 5.1.0 以降のバージョンで提供されています。

インデックスの競合を自動的に解決する

インデックスの競合を解決できるようにします。すべてのマシンに階層型テンプレートを適用するとき、インデックスはテンプレート内に追加されたモニタに割り当てられます。割り当てられたインデックスがベース ポリシーまたは別のテンプレート内の既存のインデックスと競合する場合、このオプションは一意的なインデックス値を再割り当てします。

注: ベース ポリシー内に含まれるインデックスは、配信された設定で常に維持されます。このオプションが無効な場合、競合するインデックスを解決できません。ただし、マシンに階層型テンプレートを適用するとき、競合するインデックスは、競合するインデックスが発生した階層型テンプレート上にエラーとして表示されます。

履歴パフォーマンス モニタリング

パフォーマンス キューブ AIM に対して以下の設定を定義できます。パフォーマンス キューブ AIM では、履歴パフォーマンスを管理するための履歴情報を Systems Performance キューブに収集します。

収集間隔

履歴テーブルからパフォーマンス キューブに情報を収集する頻度を指定します。

インデックス範囲の開始

インデックスの予約済み範囲の開始を指定します。デフォルトでは、エージェントはこの範囲でパフォーマンスキューブ データを収集するための履歴コントロール エントリを作成します。この予約済み範囲は、SRM (サービスレスポンス モニタリング) がパフォーマンスデータを収集するよう設定されている場合などに使用されます。

インデックス範囲の終了

インデックスの予約済み範囲の終了を指定します。デフォルトでは、エージェントはこの範囲でパフォーマンスキューブ データを収集するための履歴コントロール エントリを作成します。この予約済み範囲は、SRM (サービスレスポンス モニタリング) がパフォーマンスデータを収集するよう設定されている場合などに使用されます。

UNIX 制御設定

UNIX システム上で実行されるエージェントに対して、以下の設定を定義できます。

サブプログラム グループ

サブプログラムを実行するルート以外のグループ名を指定します。

サブプログラム ユーザ

サブプログラムを実行するルート以外のユーザ名を指定します。

Linux Freemem を含む

空きメモリの計算に、システム バッファ、ディスク キャッシュ メモリ、またはその両方を含めるかどうかを指定します。

システム デバイスのクエリ

以下のシステム デバイス メトリックのクエリを有効にできます。

- シリアル デバイス ステータス
- フロッピー ディスク ステータス
- ディスク サイズ、容量、説明、およびその他のプロパティ(ディスクのプロープ)
- NFS ファイル システム ステータス
- HP-UX グラフィックス ステータス

これらのメトリックに対してクエリを実行すると、潜在的なエージェントブロックに関する問題が発生する可能性があります。デフォルト設定では、シリアル デバイス ステータスおよび NFS ファイル システム ステータスに対するクエリのみが有効になっています。

6. [プラグイン]をクリックします。

[プラグイン]ペインが表示されます。このペインで、エージェントを使用してロードする AIM を指定します。

7. 以下のいずれかを実行します。

- [利用可能なすべてのプラグインをロードします]を選択して、エージェントシステムで利用可能なすべての AIM をロードします。
- [テーブルで選択されたプラグインをロードします]を選択します。
- [外部プラグイン]ツールバーの[+] (新規)をクリックし、外部プラグインテーブルに AIM を追加します。

注: 利用可能な AIM の詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

AIM ロードが設定されます。

8. [モニタを集計]をクリックします。

[「オブジェクト集計の設定 \(P. 122\)」](#)の説明に従って、モニタの集計を設定します。

制御設定が定義されます。

9. [ポリシーの保存]をクリックします。

ポリシーが保存されます。

関連項目:

[オブジェクト集計の設定](#) (P. 122)

トラップとコミュニティの定義

SNMP 設定では、エージェントが使用するコミュニティ、およびエージェントがトラップを送信する宛先を定義します。

次の手順に従ってください:

1. [リソース]タブをクリックして[設定]ペインを開き、[ポリシー]を展開して[SystemEDGE]をクリックします。
[利用可能ポリシー]ページが表示されます。
2. [利用可能ポリシー]テーブルでポリシーを選択します。
ポリシーの[サマリ]ページが表示されます。
3. [トラップ & コミュニティ]タブをクリックします。
[コミュニティ]ページが表示されます。
4. 以下のいずれかを選択して[アクション]をクリックし、[適用]を選択します。
 - サーバ固有 SNMP 設定のみを含める
 - サーバ固有 SNMP 設定およびすべてのデフォルト設定を含める
 - [サーバ固有 SNMP 設定および選択されたデフォルト設定を含める]を選択します。

[SNMP 設定]が更新され、[コミュニティ]テーブル内のコミュニティ ページに以下が表示されます。

名前

コミュニティ文字列の名前を指定します。

ポート

SNMP のポートを指定します。

SNMP バージョン

コミュニティが使用する SNMP バージョンを指定します。

アクセス権

コミュニティが、読み書きまたは読み取り専用のいずれの権限を持つかを指定します。

注: 少なくとも 1 つの読み取り専用コミュニティと、1 つの読み書きコミュニティを追加してください。

コミュニティ/ユーザ

コミュニティ名を指定します。

認証プロトコル

SNMPv3 データを認証するプロトコルを指定します。

プライバシー プロトコル

SNMPv3 データを認証するプロトコルを指定します。

アクセス制御リスト

IP アドレスのスペース区切りリストを指定して、コミュニティの使用をこれらのアドレスのみに制限します。リストを空にしておくと、エージェントは、関連付けられたコミュニティ名を使用するあらゆるシステムに対してアクセス権を付与します。アクセスリストは、SNMPv1 を使用するコミュニティについてのみ有効です。

注: SNMPv2c および SNMPv3 のアクセスリストの定義の詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

5. (オプション) 必要に応じて、他のコミュニティを追加、更新、または削除します。
6. [ポリシーの保存]をクリックします。
ポリシーが保存されます。

7. [トラップ先]をクリックします。
[トラップ先]ページが表示されます。
8. 以下のコントロールを使用して、トラップ先を定義し、[追加]をクリックします。

トラップ タイプ

SNMP バージョンに応じて、送信するトラップのタイプを指定します。

デスティネーション

トラップを送信する IPv4 アドレスまたは IPv6 アドレスを指定します。

ポート

トラップを送信する UDP ポートを指定します。

コミュニティ

トラップで送信されるコミュニティ名を指定します。

エンコーディング

(オプション)トラップ内の[制御設定]ペインの[トラップソース]フィールドで定義したソースアドレスを含める方法を指定します。このパラメータはトラップソースが IPv6 アドレスに変換される場合に重要です。3 桁の XYZ の形式(先頭の未使用桁をゼロで埋める)でエンコーディングパラメータを入力します。

デフォルト: 000

X

4 バイトの IPv4 ソースアドレスフィールド(SNMPv1トラップのみ)の拡張を制御します。16 バイトの IPv6 アドレスを含めるのに、ソースアドレスフィールドを拡張しない場合は 0 を入力し、ソースアドレスフィールドを拡張する場合は 1 を入力します。

Y、Z

トラップの varbind (Y)または UDP パケット(Z、SNMPv1トラップのみ)にソース情報を含めるかどうかを制御します。これらの桁に以下のいずれかを入力します。

0: トラップの varbind または外部 UDP パケットは変更されません。

1: varbind またはパケットに trap_source パラメータ(IPv4/IPv6 アドレスまたはホスト名)をそのまま含めます。

2: trap_source パラメータを、可能であれば IPv4 アドレスとして(続いて IPv6 アドレス、ホスト名の順に試行)含めます。

3: trap_source パラメータを、可能であれば IPv6 アドレスとして(続いて IPv4 アドレス、ホスト名の順に試行)含めます。

4: trap_source パラメータを、可能であればホスト名として(続いて IPv4、IPv6 の順に試行)含めます。

5: 2 の優先順位に従い、ホスト名を含めます。

6: 3 の優先順位に従い、ホスト名を含めます。

7: 1 の優先順位に従い、ホスト名を含めます(trap_source が IPv6 アドレスの場合)。

トラップソース

(オプション)トラップソースとして使用する IPv4 アドレス、IPv6 アドレス、またはホスト名を指定します。

デフォルト: グローバルトラップ

トラップ先が[定義済みトラップ先]テーブルに表示されます。

9. (オプション) 必要に応じて、他のトラップ先を追加、更新、または削除します。

10. [ポリシーの保存]をクリックします。

ポリシーが保存されます。

注: 詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

MIB 拡張の定義

MIB 拡張を定義すると、ローカル ファイル操作では利用できない機能が利用できるようになります。ポリシー設定機能により、フィールド名、および、オブジェクトタイプなどのキー プロパティのリストが提供されます。

ポリシーまたはモニタリング テンプレートを設定する場合に[MIB 拡張] タブをクリックすると、以下のオブジェクトが追加できます。

- MIB 拡張
- Windows パフォーマンス
- Windows レジストリ

注: テンプレート内の MIB 拡張は、モニタされたシステムに MIB 拡張を直接適用することを目的としてサポートされています。ポリシー内で使用するための MIB 拡張は、ポリシー内に直接作成する必要があります。

SRM ポリシーを作成する方法

実行するテスト、モニタするしきい値、基本設定、その他エージェントの実行方法とモニタ対象を制御する設定を定義するには、SRM ポリシーを作成します。作成したポリシーは、SRM AIM と共に管理対象モードで SystemEDGE エージェントを実行する任意の数のシステムに適用できます。ポリシーを使用すると、ローカルで手動によって設定できるすべての設定操作を実行できるうえに、統合されたインターフェース、選択リスト、およびリモートシステムへの動的展開といった利点が得られます。

SRM ポリシーを作成するには、以下の手順に従います。

1. [リソース]タブをクリックして[設定]ペインを開き、[ポリシー]を展開して[サービスレスポンス]をクリックします。
[サービスレスポンス]ペインが表示されます。

2. [利用可能ポリシー]ツールバーの[+] (新規)をクリックします。
[新規サービスレスポンス モニタリング ポリシー]ダイアログ ボックスが表示されます。
3. ポリシーの名前と説明、および既存のポリシーをベースにするかどうかを入力し、[OK]をクリックします。
ポリシーが作成され、右側のペインに設定画面が表示されます。
4. [ポリシーに含めるテストを定義します](#) (P. 193)。
5. [テストのしきい値を定義します](#) (P. 193)。
6. [制御設定を定義します](#) (P. 194)。
7. [ポリシーの保存]をクリックします。
ポリシーが保存されます。

テスト定義

SRM ポリシーを設定する際、[テスト]タブをクリックすると、現時点で定義済みのすべてのテストのサマリが表示されます。[テスト]ペインで、新しいテストの定義と変更、および既存のテストの削除とコピーを実行できます。設定ポリシーを使用してテストを定義すると、ローカルのファイル操作では利用できない、以下の機能上の利点が得られます。

- 直観的なフィールド名
- 主要なプロパティの選択リスト
- テスト タイプを指定するための選択リスト。指定したテストに関連するプロパティでペインが動的に更新されます。
- しきい値定義をテストに追加するためのテーブル

設定ポリシーのテストを定義する方法の詳細については、オンライン ヘルプを参照してください。

しきい値定義

SRM テストによって収集された属性のしきい値モニタを定義し、任意の既存テストに追加できます。これらのモニタによって、SystemEDGE セルフ モニタ エントリが作成され、SRM テストのステータス情報を追跡することができます。設定ポリシーを使用してモニタしきい値を定義すると、手動のファイル操作では利用できない、以下の機能上の利点が得られます。

- 直観的なフィールド名
- モニタする属性を選択するための選択リスト
- 必要に応じてさまざまな重大度を柔軟に定義できる、警告、マイナー、メジャー、重大、および致命的の各値用フィールド
- [テスト]タブでのしきい値と任意の SRM テストの動的な関連付け

テストのモニタしきい値を定義する方法の詳細については、オンライン ヘルプを参照してください。

SRM 制御設定の定義

SRM 制御設定では、通常は `svcrsp.cf` ファイルで制御する、以下のような AIM 動作のさまざまな要素を定義します。

- セキュリティ設定
- ログレベル
- インデックス予約

SRM ポリシー内に定義されている制御設定は、ポリシーが適用されるすべてのマシンに適用されます。

次の手順に従ってください：

1. [リソース]タブをクリックして[設定]ペインを開き、[ポリシー]を展開して[サービスレスポンス]をクリックします。
[利用可能ポリシー]ページが表示されます。
2. [利用可能ポリシー]テーブルでポリシーを選択します。
ポリシーの[サマリ]ページが表示されます。
3. 目的のポリシーのページで[制御設定]タブをクリックします。
[制御]ペインが表示されます。
4. 以下の制御設定を行います。

最大スレッド数

テストを実行する際に `jcollector` が使用するスレッドの数を指定します。

ログレベル

SRM AIM のログレベルを指定します。デフォルトは[警告]です。

外部スクリプトを許可する

外部スクリプトの実行を許可するかどうかを指定します。

ファイル I/O テストの実行を許可する

ファイル I/O テストの実行を許可するかどうかを指定します。

信頼できない SSL 証明書を許可する

信頼された SSL 証明書がないサイトでの SSL テストを許可するかどうかを指定します。

Java bin の場所

Java 実行可能ファイルの場所を定義します。

注: AIX 上の完全パスおよびバイナリを指定してください。

環境内の CLASSPATH の上書き

ロードする追加クラスを定義します。定義されない場合、環境内の CLASSPATH を上書きします。

コレクタなし

SystemEDGE で jcollector を開始するかどうかを指定します。

JRE 内部キャッシュのバイパス

JRE 内部キャッシュをバイパスするかどうかを指定します。

IPv4 (HP-UX)用の TOS なし

TOS を無効にするかどうかを指定します。

共有メモリ名

共有メモリの ID を定義します。

予約されたテスト インデックス

テスト インデックスの予約済み範囲を定義します。

制御設定が定義されます。

5. [ポリシーの保存]をクリックします。

ポリシーが保存されます。

マシンへのポリシーの適用

設定ポリシーを作成したら、企業全体でマシンに適用する必要があります。設定ポリシーを適用すると、すべてのポリシー設定が含まれたコンパイル済み設定ファイルが、指定されたすべてのエージェントマシンに **CA Virtual Assurance** によってプッシュされ、エージェントが自動的にウォーム スタートした後、新規ポリシーが実装されます。

また、以下のいずれかが発生した場合にも、マシンにポリシーを再適用できます。

- ポリシーを更新した。
- エージェントマシン上の設定が変更されたことを知らせる通知を受信した。

次の手順に従ってください：

1. [リソース]タブをクリックして[設定]ペインを開き、[ポリシー]を展開して、[SystemEDGE]または[サービスレスポンス]を選択します。

[利用可能ポリシー]ページが表示されます。

2. [利用可能ポリシー]テーブルでポリシーを選択します。

ポリシーの[サマリ]ページが表示されます。

3. 適用するポリシーを選択します。

[ポリシー詳細]が右ペインに表示されます。

4. [アクション]をクリックし、[適用]を選択します。

ポリシーを適用するマシンを選択するためのタブが表示されます。[このポリシーを実行しているマシンを更新]タブでは、すでにポリシーを実行しているマシンにポリシーを適用できます。[このポリシーを実行していないマシンに適用]タブでは、ポリシーのないマシンまたは別のポリシーを使用しているマシンにポリシーを適用できます。

5. (オプション) [このポリシーを実行しているマシンを更新]タブから、以下のいずれかを実行します。
 - 現在ポリシーを実行しているすべてのマシンにこのポリシーを展開するには、[このポリシーを使用してすべてのマシンを更新]を選択します。このオプションは、グローバルに適用する設定ポリシーの変更を行った場合に便利です。
 - 以下の条件のいずれかを満たすマシンのみを更新するには、[選択したマシングループを更新]を選択します。
 - 期限切れバージョンのポリシーを実行している。
 - ポリシー例外が発生した。
 - 現在のバージョンのポリシーを実行している。これらのオプションのいずれかを選択します。ポリシー例外は、適用されるポリシー内で示されていないエージェントにユーザがポイント設定変更を適用すると発生します。
 - [詳細]を選択し、ポリシーが再適用されるマシンを[マシンを選択]ペインで手動で選択します。
6. (オプション) [このポリシーを実行していないマシンに適用]タブから、ポリシーを適用するマシンを選択します。
7. [ポリシーの適用]をクリックします。
ポリシーの適用が開始されます。

ポリシー適用の進捗状況の確認

個々のポリシーに対して、ポリシー適用操作の進捗状況を詳細に確認できます。

次の手順に従ってください:

1. [リソース]タブを選択して[設定]ペインを開き、[ポリシー]を展開して、[SystemEDGE]または[サービスレスポンス]を選択します。
[利用可能ポリシー]ページが表示されます。
2. [利用可能ポリシー]テーブルでポリシーを選択します。
ポリシーの[サマリ]ページが表示されます。

3. [管理対象マシン]タブをクリックします。

[管理対象マシン]ページに現在ポリシーを実行しているマシンのリストが表示され、ここで設定ステータスを表示できます。

4. (オプション)[例外の表示]をクリックします。

[ポリシー例外]ペインが表示され、ポリシーが最後に適用されてからシステムに適用された **SNMP SET** を参照できます。

注: この画面は **SystemEDGE** ポリシーに対してのみ表示されます。

5. (オプション)[設定の表示]をクリックします。

[ポリシー設定]ペインが表示され、エージェントに配信された設定ファイルを参照できます。

6. (オプション)[エラーの表示]をクリックします。

[ポリシー エラー]ペインが表示されます。ポリシーを正常に適用できなかった場合、ポリシーが拒否されたときにエージェントによって返されたエラーのリストを参照できます。

適用されるポリシーの設定と表示

ポリシー機能では、個別のサーバ、サーバグループ、またはサービスに適用されたポリシーおよびテンプレートを管理できます。以下の操作を実行できます。

- ポリシーおよびテンプレートの更新
- 例外の表示。例外は、ポリシーまたはテンプレートが最後に適用された後でシステムに適用された **SNMP** セットです。
- ポリシー設定の表示
- ポリシー エラーの表示
- ポリシーの一括更新
- テンプレートの削除

次の手順に従ってください:

1. [エクスプローラ]ペインを開きます。

利用可能なグループ、サービス、およびシステムが表示されます。

2. システムまたはサービスを選択します。[リソース]ページをクリックし、[モニタリング ソフトウェア]をクリックします。

[マシンの詳細]ページが表示されます。

3. [ポリシー]をクリックします。

[ポリシー]ページに、SystemEDGE と SRM のポリシーおよび SystemEDGE テンプレートのリストが表示されます。

注: [フィルタ]には、[保留]、[配信] (成功)、[設定完了]、および[失敗]のいずれかである階層型テンプレートのリストが表示されます。

4. ポリシーおよびテンプレートを一括更新できます。[ポリシーとテンプレート]テーブルで、一括更新するポリシーまたはテンプレートを選択し、[アクション]をクリックして以下のいずれかのオプションを選択します。

- SystemEDGE ポリシーの一括更新
- サービスレスポンス ポリシーの一括更新
- SystemEDGE テンプレートの一括更新

注: ポリシーが単一のサーバに適用されている場合は、ポリシー名を入力するためのプロンプトが表示されます。

ポリシーの一括更新:

選択したポリシーがサービス グループに適用される場合、ポリシーを適用するマシンを選択するオプションがダイアログ ボックスに表示されます。

テンプレートの一括更新:

[利用可能なテンプレート]からテンプレートを選択するオプションがダイアログ ボックスに表示されます。テンプレートを選択した後に、以下のいずれかのオプションをクリックします。

- [選択されたテンプレートをすべてのマシンに対してセットとして適用する] - すべてのマシンに適用されている既存のテンプレートを削除し、選択されたテンプレートをすべてのマシンに適用します。
 - [選択したテンプレートをすでにマシンへ適用済みである既存のセットに追加する] - 選択されたテンプレートをすべてのマシンに追加します。選択されたテンプレートに、マシンに適用されている既存のテンプレートが含まれる場合は、既存のテンプレートが再適用されます。
5. [ポリシーの適用]をクリックして、マシンにポリシーまたはテンプレートを適用します。

[ポリシー]ページで、ポリシーまたはテンプレートのマシンへの適用に関する進捗状況を確認できます。

6. (オプション) [設定の表示]アイコンをクリックします。

[ポリシー設定]ページが表示されます。テンプレートを含むマシンでは、ポリシー、テンプレート、および **SystemEDGE** 設定ファイルが表示されます。サービスレスポンス モニタを含むマシンでは、さらにサービスレスポンス モニタの設定ファイルも表示されます。

7. [ポリシーの保存]をクリックします。

ポリシーが保存されます。

エージェント ポリシーのダッシュボードビュー

ダッシュボードで以下のビューを使用して、エージェント ポリシー割り当てを追跡できます。

ポリシー ステータス サマリ

ポリシーの数を示す円グラフとリストが表示されます。システムは次の 5 つの状態にいずれかになります。

未設定

SystemEDGE エージェントがインストールされていますが、ポリシーは設定されません。

インストール済みエージェント

SystemEDGE エージェントがインストールされています。

設定完了

SystemEDGE エージェントがインストールされ、ポリシーが設定されます。

構成エラー

SystemEDGE がインストールされ、ポリシーが設定されていますが、最終設定に失敗しました

インストール済みエージェント(未管理)

SystemEDGE がインストールされていますが、ポリシー設定を通じて管理できないモードで実行されています。

ポリシー内訳

すべてのポリシーと各ポリシーに含まれるシステムの数を示す円グラフとリストが表示されます。

非標準ポリシーを含むマシン

適用されたポリシーへの標準以外の変更が含まれるシステムをリスト表示するテーブルが表示されます。

例: ユーザ固有のメトリック(MIB 拡張)をモニタする方法

次の例では、ユーザ固有のメトリックをモニタする方法を、手順を追って説明します。

ユーザ固有のメトリック(MIB 拡張)をモニタする方法

1. 必要なデータを返すプログラムを作成します。たとえば、いくつかの固定データを返すシンプルな DOS バッチ スクリプトをエージェントシステム上に作成します。

```
@echo off  
echo 99
```

2. テキスト エディタを開き、C: ドライブ上の **data.bat** にこれらの 2 行を保存します。

3. このバッチ ファイルを参照する MIB 拡張を作成します。

- a. ユーザ インターフェースから、[ポリシー]をクリックし、[ナビゲーション] ペインで[設定]を開き、[ポリシー]ツリーを展開して、SystemEDGE ポリシーを開きます。

[ポリシー詳細]が右ペインに表示されます。

- b. [MIB 拡張]タブをクリックします。

[MIB 拡張]ページが表示されます。

- c. フィールドに以下のデータを追加します。

インデックス: 1 (これが 1 つ目の MIB 拡張である場合)

タイプ: integer

拡張コマンド: C:¥data.bat

アクセス権: 読み取り専用

- d. [追加]をクリックします。

MIB 拡張がポリシーに追加されます。

- e. [ポリシーの保存]をクリックします。

ポリシーが保存されます。

4. 新しいモニタの値を確認するためのしきい値モニタを作成します。
 - a. [モニタ]をクリックし、[しきい値]をクリックします。
[しきい値モニタの詳細: 編集]ペインが表示されます。
 - b. フィールドに以下のデータを追加します。
インデックス: (自動的に追加されます)
プラットフォーム: OS 非依存
オブジェクト クラス: extensionGroup [スカラ変数を新規追加して拡張された MIB]
オブジェクト属性: 1
オブジェクト インスタンス名: MyData
間隔: 60
重大度: メジャー アラーム
演算子: 次の値以上
値: 50
スケール: 1
サンプル タイプ: 絶対値
 - c. [保存]をクリックします。
ポリシーが保存されます。しきい値が「50」の「メジャー」アラームが追加されます。上で作成したスクリプトは常に値「99」を返すため、すぐにこのしきい値に違反することになります。
 - d. [アクション]をクリックし、[適用]をクリックしてポリシーをコンピュータに適用します。
[選択したマシン]ペインが表示されます。
 - e. 選択したマシンが正しいことを確認して、[適用]をクリックします。
MIB 拡張が追加されたポリシーが、選択したコンピュータに適用されます。
[ポリシーに戻る]をクリックします。
[ポリシー詳細]ペインが表示されます。

エージェントが設定されたら、[リソース]タブでこのしきい値モニタの状態を表示できます。「メジャー」しきい値が違反されていることがわかります。

例：特定の Windows パフォーマンス レジストリのメトリックをモニタする方法

次の例では、ユーザ固有のメトリックをモニタする方法を、手順を追って説明します。

ユーザ固有のメトリック(MIB 拡張)をモニタする方法

1. Windows パフォーマンスレジストリのメトリック用に MIB 拡張を作成します。
 - a. ユーザ インターフェースから、[ポリシー]をクリックし、[ナビゲーション] ペインで[設定]を開き、[ポリシー]ツリーを展開して、SystemEDGE ポリシーを開きます。
[ポリシー詳細]が右ペインに表示されます。
 - b. [MIB 拡張]タブをクリックします。
[MIB 拡張]ページが表示されます。
 - c. [Windows パフォーマンス]をクリックします。
[Windows パフォーマンス定義済み拡張]ペインが表示されます。
 - d. フィールドに以下のデータを追加します。
インデックス: 1 (この拡張が 1 つ目である場合)
タイプ: integer
オブジェクト: システム
カウンタ: プロセス数(実行中のプロセスの合計を指定します)。
システム メトリックには「インスタンス」がないため、このフィールドは空白のままになります。
 - e. [追加]をクリックします。
MIB 拡張がポリシーに追加されます。
 - f. [ポリシーの保存]をクリックします。
ポリシーが保存されます。
2. 新しいモニタの値を確認するためのしきい値モニタを作成します。
 - a. [モニタ]をクリックし、[しきい値]をクリックします。
[しきい値モニタの詳細: 編集]ペインが表示されます。

- b. フィールドに以下のデータを追加します。

インデックス: (自動的に追加されます)

プラットフォーム: OS 非依存

オブジェクト クラス: ntRegPerf (NT レジストリおよびパフォーマンス グループ)

オブジェクト属性: 1

オブジェクト インスタンス名: NumProcesses

間隔: 60

重大度: 警告アラーム

演算子: 次の値以上

値: 50

スケール: 1

サンプル タイプ: 絶対値

- c. [保存]をクリックします。

ポリシーが保存されます。しきい値が「50」の「警告」アラームが追加されます。

- d. [アクション]をクリックし、[適用]をクリックしてポリシーをコンピュータに適用します。

[選択したマシン]ペインが表示されます。

- e. 選択したマシンが正しいことを確認して、[適用]をクリックします。

MIB 拡張が追加されたポリシーが、選択したコンピュータに適用されます。

[ポリシーに戻る]をクリックします。

[ポリシー詳細]ペインが表示されます。

エージェントが設定されたら、[リソース]タブでこのしきい値モニタの状態を表示できます。

第 7 章: プロビジョニング リソース

このセクションには、以下のトピックが含まれています。

[イメージング サービス \(P. 205\)](#)

[VMware vCenter プロビジョニング \(P. 206\)](#)

[仮想マシン \(Hyper-V Server\) の追加 \(P. 214\)](#)

[Solaris ゾーン の追加 \(P. 215\)](#)

[IBM AIX コンピュータの論理パーティションの追加 \(P. 217\)](#)

[追加プロビジョニング情報 \(P. 219\)](#)

[リモート展開 \(P. 220\)](#)

[インフラストラクチャ展開プロセス \(P. 251\)](#)

[ファイアウォール ソフトウェアを実行している Windows Vista™、Windows 2008、および Windows XP コンピュータへの展開 \(P. 261\)](#)

イメージング サービス

CA Virtual Assurance は、必要に応じて、新しい仮想マシン、論理パーティション、または Solaris ゾーンをプロビジョニングし、既存のリソースを再イメージングできます。プロビジョニングの機能を使用すると、クローン作成、マイグレート、VM プロパティの設定と変更、および LPAR と Solaris ゾーン の作成と管理ができます。

イメージング サービス コンポーネントは以下のテクノロジーを使用および統合して、プロビジョニング操作を行います。

- ゾーンのプロビジョニングのための Solaris ゾーン サーバ
- VM のプロビジョニングのための VMware vCenter Server 統合。VM のプロビジョニングでは、標準スイッチと分散仮想スイッチがサポートされます。
- VM のプロビジョニングのための Hyper-V 統合。このテクノロジーは、設定なしですぐに使用できる Hyper-V サーバ上のローカル テンプレートに基づきます。また、既存の SCVMM イメージライブラリを再利用するための Microsoft System Center Virtual Machine Manager (SCVMM) をオプションで統合できます。

イメージング サービスによって、以下のアクションのイベントが生成されます。

- イメージング ジョブがイメージング サーバにサブミットされた。

- イメージング ジョブ ステータスの変更が発生した。
- イメージング ジョブが成功した後、ターゲット コンピュータが検出された。

VMware vCenter プロビジョニング

イメージング サービスは、VC PMM と通信し、CA Virtual Assurance 用の VM プロビジョニングを提供するために VMware vCenter Server と統合します。この統合によって、イメージング サービスは、電源オン、電源オフ、CPU やメモリの共有の設定、VM のマイグレート、または新しい VM の作成およびプロビジョニングなどの操作を VM 上で実行することができます。

このドキュメントでは、VMware vCenter Server に精通していることを前提にしています。VMware によって vCenter Server に課された要件および制限はすべて、CA Virtual Assurance に有効です。

注: VMware vCenter Server および vSphere に関するドキュメントについては、Web サイト <http://pubs.vmware.com> を参照してください。

VMware vCenter および vSphere ユーザ権限

CA Virtual Assurance がサポートするすべての VMware vCenter 操作では VMware 製品にユーザ権限が設定されている必要があります。最小要件をここで説明します。ユーザによっては役割に応じて追加の権限が必要な場合があります。これらの権限は VMware vCenter バージョン 2.5、4.0 および 4.1 に適用されます。

権限は [All Privileges]、[仮想マシン] 下の [Edit Role] ダイアログ ボックスで設定します。

ユーザは [Administration, Configuration, Provisioning: vCenter Server] ページに配置されています。権限を設定した後、以下の手順を実行して VM プロビジョニングが失敗しないことを確認します。

- ユーザを VMware でホストおよびクラスターレベルに追加します。詳細については、<http://kb.vmware.com/kb/1008192> を参照してください。

注: 権限を設定する方法の詳細については、VMware のドキュメントを参照してください。

電源操作

ユーザに電源操作(電源の調整アクション)を実行させるには、[Interaction]の下で以下のオプションを選択します。

- 電源オン
- 電源オフ
- 一時停止
- リセット

リソース調整

リソース調整権限によって、ユーザは以下の操作を実行できます。

- CPU 制限の設定
- CPU 予約の設定
- メモリ制限の設定
- メモリ予約の設定

リソース調整権限を設定するには、[設定]の下での[Change Resource]を選択します。

共有調整

共有調整権限によって、ユーザは以下の操作を実行できます。

- メモリの設定
- メモリの追加
- メモリの削除
- CPU の設定
- CPU の追加
- CPU の削除

共有調整権限を設定するには、[設定]の下で以下の設定を選択します。

- [Change CPU Count]
- メモリ
- 設定

VM の削除

[VM の削除] 権限によって、ユーザは仮想マシンを削除できます ([VC 仮想マシンの削除])。

VM の削除権限を設定するには、[インベントリ] の下で [削除] を選択します。

VM およびテンプレートの変換

VM およびテンプレートの変換権限によって、ユーザはテンプレートを VM に変換し、VM をテンプレートに変換できます。

VM およびテンプレートの変換権限を設定するには、以下の設定を選択します。

[プロビジョニング] の下で

- [Mark As Template]
- [Mark as Virtual Machine]

[リソース] の下で

- [Assign Virtual Machine to Resource Pool]

クローン作成

クローン作成権限によって、ユーザは、VM からテンプレートへのクローン作成、または VM から VM へのクローン作成などのクローン作成操作を実行できます。

vCenter クローン作成権限を設定するには、以下の設定を選択します。

[インベントリ] の下で

- 作成
- 削除
- 移動

[インタラクション]の下で

- 電源オン
- 電源オフ
- 一時停止
- リセット
- [Device connection]
- [Tools Install]

[設定]の下で

- [Add Existing Disk]
- 新しいディスクの追加
- [Change CPU Count]
- メモリ
- [Modify Device Settings]
- 設定
- [Change Resource]

[プロビジョニング]の下で

- カスタマイズ
- クローン
- テンプレートの展開
- [Mark As Template]
- [Mark as Virtual Machine]
- [Read Customization Specifications]
- [Modify Customization Specification]

[リソース]の下で

- [Assign Virtual Machine to Resource Pool]

VMotion

VMotion 権限によって、ユーザはある物理サーバから別のサーバに VM をマイグレートできます。

VMotion 権限を設定するには、[リソース]の下で以下の設定を選択します。

- マイグレート
- [Relocate]
- [Query VMotion]

VM スナップショット

VM スナップショット権限によって、ユーザはスナップショットを作成できます。

VM スナップショット権限を設定するには、[状態]の下で以下の設定を選択します。

- スナップショットの作成
- スナップショットに戻す
- スナップショットの削除
- スナップショットの名前変更

関連項目

[vCenter Server でのユーザ スコープ認証](#) (P. 39)

仮想マシン(vCenter Server)の追加

VMを追加する場合は、以下の2つの方法のいずれかを使用できます。

- 事前定義済みテンプレートのクローンを作成する
- 既存の VM およびカスタマイズ仕様のクローンを作成する (カスタマイズ仕様でゲスト OS の特性を定義する)

VM プロビジョニングは標準スイッチと分散仮想スイッチをサポートします。分散仮想スイッチに接続している VM にプロビジョニングする場合、ユーザ インターフェイス内の適切な検出済み dvPort グループを指定できます。dvPort グループは、分散仮想スイッチを介してネットワークに接続が行われる方法を定義します。

VMを追加する方法

1. [エクスプローラ] ペインで [VMware vCenter サーバ] を右クリックし、[プロビジョニング]-[VMware VM のプロビジョニング] を選択します。

[VMware vCenter プロビジョニング] ダイアログ ボックスが表示されます。

2. ドロップダウンリストからオプションを選択して設定を指定します。

注: クローン作成用にリスト表示される仮想マシンは、CA Virtual Assurance によってモニタされている仮想マシンに制限されます。VM へのアクセスはセキュリティを確保するために制限されます。利用できないシステムのクローンを作成する場合は、他のシステムと同じようにそのシステムを検出し、それをドロップダウンリストで利用可能にします。

3. 使用するユーザ名、パスワードおよびホスト名を入力します。入力しない場合、仕様で指定された名前がデフォルトで使用されます。

注: Windows および Linux のユーザ名およびパスワードが、カスタマイズ仕様ファイルで定義されたものと一致する必要があります。

4. 以下のいずれかのオプションを選択し、[次へ] をクリックします。

- VC 仮想マシンは既存の VM を使用する
- VC テンプレートはテンプレートを使用して新しい VM を作成する
- VC 仕様は利用可能なリストからカスタマイズ仕様を選択する

[仮想マシン メモリ] ページが表示されます。

5. (オプション)VM 用のメモリを調節し[次へ]をクリックします。

メモリ

VM テンプレートまたは VM に定義されたメモリ値をフィールドに入力します。

デフォルト: 最低 4 MB および最大 16 GB

注: caimgconf.cfg ファイル内のこれらの値を設定します。

[仮想マシン CPU] ページが表示されます。

6. (オプション)VM 用の CPU を調節し[次へ]をクリックします。

仮想プロセッサ

VM テンプレートまたは VM に定義された仮想プロセッサの数をフィールドに入力します。

デフォルト: 最低 1 CPU および最大 4 CPU

注: caimgconf.cfg ファイル内のこれらの値を設定します。

[ディスク] ページが、選択済み VM または選択したテンプレートからのデフォルト値が入力されたフィールドと共に表示されます。

7. (オプション)ドライブ サイズを設定し、[ドライブの追加]をクリックしてドライブを追加し、ハード ディスクに関連付けるデータストアおよび使用する SCSI コントローラをドロップダウン リストから設定し、[次へ]をクリックします。

データストア

VM が作成される、VMware ESX ホストのデータストア名を識別します。

ドライブ サイズ

ドライブ サイズを指定して VM により多くのハード ディスクを追加することができます。

制限: 最小のドライブ サイズは 1 MB ですが、選択したデータストア用のドライブ サイズを超過することはできません。

SCSI コントローラ

仮想アダプタとして使用する SCSI コントローラを指定します。

[ネットワーク] ページが表示され、テーブルに選択されたテンプレートからのデフォルト値が入力されます。

8. (オプション) [ネットワーク管理] テーブルのセルの内部をクリックすると、ドロップダウン リストがアクティブになり、任意の設定を変更できます。

カスタム仕様が DHCP の使用を指定している場合は、テーブル内のネットワーク接続セルのみを編集できます。ネットワーク接続は、現在標準および分散仮想スイッチの両方のネットワークをサポートしています。以下の命名規則に基づいて、標準スイッチと分散仮想スイッチの名前を区別できます。

- 標準スイッチの名前はネットワーク名です。
- 分散仮想スイッチの名前は、**dvPort** グループ名の後に、丸かっこで囲まれた分散仮想スイッチ名を連結したもの (**dvPortGroupName** (**dvSwitchName**)) です。

カスタム仕様が静的 IP アドレスの使用を指定している場合は、NIC セル以外のセルをすべて編集できます。**CA Virtual Assurance** はカスタム仕様のネットワークが[ユーザに通知]を設定することをサポートしていません。この設定を使用するカスタム仕様はフィルタで除外され利用できません。

[次へ]をクリックします。

9. [コンピュータの追加]をクリックします。

確認メッセージがペインの一番上に表示されます。

注: イメージングには時間がかかるため、オペレーティング システムのインストール中の遅延を予想しておく必要があります。より効率的なディスカバリのために、検出再試行時間、または **caimgconf.cfg** ファイル (**install_path¥CA¥productname¥conf** にあります) 内の間隔を調節できます。

10. [リフレッシュ]をクリックすると新しい VM が左ペインに表示されます。

データ センターに新しいクローン作成された VM があります。ダッシュボードにイメージング プロセスのイベントを表示できます。また、イメージング ジョブ レポートを生成できます。

仮想マシン(Hyper-V Server)の追加

データセンターに VM を作成できます。VM を作成するには、事前定義済みテンプレートを使用する必要があります。

注: Hyper-V の[ストレージの合計]の値には、テンプレートから VM を作成するのに必要な総容量が含まれます。この値は、すべての仮想ディスク、VM の RAM サイズ、スナップショットおよびバッファが含まれた複数のファクタの組み合わせです。この情報を使用して、選択済みテンプレートに基づいた VM を作成するのに必要なストレージの最大容量の指針にします。

VM を作成する方法

1. [リソース]-[エクスプローラ] を選択します。
[エクスプローラ] ペインが表示されます。
2. Hyper-V リソースを右クリックし、[プロビジョニング]-[Hyper-V VM のプロビジョニング]を選択します。
3. 以下の詳細を指定して[次へ]をクリックします。
 - SCVMM サーバおよび Hyper-V サーバ。
 - VM を作成するために使用するテンプレート名。
 - VM を作成するデスティネーション パス。
 - 作成する VM の名前。
 - VM が作成された後で VM を開始するかどうかを指定します。[仮想マシン メモリ] ページが表示されます。
4. VM メモリの詳細を指定し[次へ]をクリックします。
[ゲスト OS カスタマイズ] ページが表示されます。
5. ゲストのオペレーティング システムの詳細を指定し[次へ]をクリックします。
[ネットワーク管理] ページが表示されます。
6. VM のネットワークの詳細を指定し[次へ]をクリックします。

注: カスタム仕様が DHCP の使用を指定している場合は、テーブル内のネットワーク接続セルのみを編集できます。カスタム仕様が静的 IP アドレスの使用を指定している場合は、NIC セル以外のセルをすべて編集できます。CA Virtual Assurance はカスタム仕様のネットワークが[ユーザに通知]を設定することをサポートしていません。この設定を使用するカスタム仕様はフィルタで除外され利用できません。

7. [コンピュータの追加]をクリックします。

確認メッセージがペインの一番上に表示されます。

注: イメージングには時間がかかるため、オペレーティング システムのインストール中の遅延を予想しておく必要があります。より効率的なディスクバリのために、検出再試行時間、または `caimgconf.cfg` ファイル (`install_path¥CA¥productname¥conf` にあります) 内の間隔を調節できます。

Solaris ゾーンの追加

Solaris ゾーン サーバは、ゾーンを使用してアプリケーションを独立した環境で実行し、それらが物理的に別のシステムで実行されているように表示します。サーバ上の各ゾーンは、リソース プールからリソースを選択し、仮想ネットワーク インターフェース、ファイル システム、メモリ、および他の専用ユニットを追加します。ゾーンを作成する場合は、この情報をすべて指定する必要があります。作成したゾーンは自動的にインストールされます。

Solaris ゾーンを追加する方法

1. [リソース] タブを選択し、[エクスプローラ] ペインの [ゾーン ホスト] を右クリックして、[プロビジョニング]-[ゾーンのプロビジョニング] を選択します。
[Solaris ゾーン プロビジョニング] ウィザードが表示されます。
2. [ゾーン ID およびタイプ] ページで以下のフィールドに入力し [次へ] をクリックします。

ホスト

ゾーンを作成するホストを定義します。

名前

ゾーンの名前を定義します。

説明

(オプション) ゾーンの説明を定義します。

タイプ

ゾーンが [ネイティブ] または [ブランド化] のどちらであるかを定義します。ブランド化ゾーンは既存のゾーン テンプレートに基づきます。

テンプレート名

(オプション) [タイプ] を [ブランド化] に設定した場合、ゾーンの作成元となるテンプレートを定義します。

インストール アーカイブ パス

ゾーン上のインストール アーカイブのディレクトリ パスを定義します。このフィールドは、[タイプ] を [ブランド化] に設定した場合にのみ必要になります。

[CPU、メモリ、その他] ページが表示されます。

3. 以下のフィールドに入力し、[終了] をクリックします。

タイプ

スケジューラタイプを定義します。タスクに割り当てられた CPU 共有の数に基づいて CPU 割り当てを制御するためにフェア シェア スケジューリング クラスを使用するには、[FSS] を選択します。

容量

ゾーンに割り当てる物理メモリ容量をメガバイト単位で定義します。

スワップ メモリ

ゾーンに割り当てるスワップ メモリの量をメガバイト単位で定義します。スワップ メモリは 50 MB 以上である必要があります。

ロック メモリ

ゾーンに割り当てるロック メモリの量をメガバイト単位で定義します。ロック メモリ量は物理メモリ量より少なくなければいけません。

ゾーン パス

ゾーンのルート ディレクトリ パスを定義します。

NIC タイプ

(オプション) NIC タイプを定義します。ドロップダウンリストからタイプを選択します。NIC を選択しないと、ゾーンには NIC カードまたは IP アドレスが割り当てられません。

IP アドレス

(オプション) ゾーンの IP アドレスを定義します。

リソース プール

ゾーンと共に使用するリソース プールを定義します。ドロップダウンリストからプールを選択します。ゾーンと共に新しいリソース プールを使用したい場合は、プールを先に作成します。プールを選択しない場合、デフォルトが使用されます。

自動再起動

グローバル ゾーンが再起動されると、ゾーンを自動的に再起動するかどうかを定義します。

IBM AIX コンピュータの論理パーティションの追加

プロビジョニング ウィザードを使用して、IBM AIX システムに論理パーティションを作成できます。

IBM AIX コンピュータの論理パーティションを追加する方法

1. [リソース]をクリックします。
2. [エクスプローラ]ペインで[IBM PowerVM サーバ]を右クリックし、[プロビジョニング]-[LPAR のプロビジョニング]を選択します。
プロビジョニング ウィザードが開き、[パーティションとメモリ]ページが表示されます。
3. HMC/IVM サーバおよび管理対象システム名を選択します。パーティション名を指定し、HMC サーバを使用する場合はプロファイル名を指定します。パーティション用の最小メモリ、希望メモリ、最大メモリを指定します。[次へ]をクリックします。
[プロセッサ]ページが表示されます。
4. プロセッサの最小数、希望数、および最大数を指定し、共有と専用のどちらのプロセッサを割り当てるかを選択します。共有モードおよび仮想プロセッサの場合は、高度な設定を使用できます。[次へ]をクリックします。
[I/O コンポーネント]ページが表示されます。

5. パーティションに関連付ける I/O デバイスを選択し、[次へ]をクリックします。

注: 各 I/O デバイスについて、その I/O デバイスが論理パーティションをアクティブにするために必要であるか、オプションであるかを指定できます。I/O デバイスが必要である場合は、I/O デバイスが利用不可であるか、別の論理パーティションに使用されていると、パーティションをアクティブにすることができません。I/O デバイスがオプションであり、パーティションがアクティブになったときに希望の I/O デバイスが利用可能な場合は、管理対象システムが I/O デバイスをパーティションに割り当てます。オプションの I/O デバイスが利用可能でない場合は、管理対象システムが I/O デバイスをスキップします。

[I/O プール]ページが表示されます。

6. (オプション)新しい I/O プールを作成するには、[I/O プール]テーブルで [+] (追加)をクリックし、数値を入力して、[保存]をクリックします。

注: パーティションに I/O デバイスを追加するとき、および I/O デバイスは I/O プールに属します。このパーティションをアクティブにすると、管理対象システムは、パーティションに対して定義された I/O プールを自動的に論理パーティションに追加します。

7. [次へ]をクリックします。

HMC サーバが選択された場合、[仮想シリアル]ページが表示されます。

8. (オプション)パーティション用の最大仮想アダプタを指定します。新しい仮想シリアル アダプタを作成するには、[+] (追加)をクリックし、アダプタ ID、リモートパーティション、およびリモートスロット番号を指定します。仮想アダプタが割り当てられており、パーティションプロファイルに必要な仮想アダプタを実行するために十分なメモリが管理対象システムにあることを要求して、そうでない場合は、論理パーティションがアクティブにならないようにすることができます。

9. [次へ]をクリックします。

[仮想イーサネット]ページが表示されます。

10. パーティション用の最大の仮想イーサネットアダプタを指定します。(オプション)新しい仮想イーサネットアダプタを追加するには、[+] (追加)をクリックし、アダプタ ID、仮想 LAN ID、アクセスする外部ネットワーク、トランク優先度、IEEE 802.1 Q 互換性、追加の仮想 LAN ID、およびイーサネットアダプタの必要性を選択します。

11. [次へ]をクリックします。

[仮想 SCSI] ページが表示されます。

12. パーティションの仮想 SCSI デバイスを指定します。(オプション) 新しい仮想 SCSI アダプタを追加するには、[仮想 SCSI アダプタ] テーブル上の[+] (追加) をクリックします。

アダプタ ID を選択し、SCSI アダプタが必要かどうかを指定して、[SCSI デバイス] テーブルでデバイス名を選択します。希望デバイスが[SCSI デバイス] リストにある場合は、[OK] をクリックし、[仮想 SCSI] パネルで[次へ]をクリックして、最後の手順までスキップします。新しい SCSI バックアップ デバイスを追加するには、[SCSI デバイス] テーブル上の[+] (新規バックアップ デバイス) をクリックします。

注: 選択されたデバイスにスロット番号がある場合、それは仮想 I/O サーバパーティションに定義された仮想 SCSI サーバアダプタのスロット番号です。

選択されたデバイスにスロット番号がない場合、仮想 SCSI サーバアダプタにまだ関連付けられていないことを意味します。パーティションを作成するジョブが発生した場合、仮想 SCSI サーバアダプタが作成され、デバイスに割り当てられます。[次へ]をクリックします。

[サマリ] ページが表示されます。

13. サマリを確認して[コンピュータの追加]をクリックします。

論理パーティションが作成されます。

追加プロビジョニング情報

CA サポート オンライン Web サイトには、アプリケーションおよびオペレーティングシステム展開に関する詳細情報が掲載されています。以下のドキュメントには、高度な CA デスクトップおよびサーバ管理トピック、およびシステム要件情報が掲載されています。

- 「CA Desktop and Server Management Advanced Topics」ガイド:

https://support.ca.com/phpdocs/0/common/impcd/r11/troubleshooting/doc/DSM_Adv_topics_r11.pdf

- 「CA Desktop and Server Management Green Books」:

https://support.ca.com/phpdocs/7/common/greenbooks/CA_Unicenter_Desktop_Server_Management_Green_Book_JPN.pdf

- 以下のドキュメントには、プロビジョニングのためにサポートされているオペレーティング システムおよびバージョンが記載されています。

Windows および Linux:

CA Software Delivery 互換性マトリックス:

https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/234/234_compmatrix.html

CA IT Client Manager 互換性マトリックス:

https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/8176/8176_compmatrix.html

注: サポートされる稼働環境およびハードウェアの要件に関する具体的な情報については、リリースノートを参照してください。

リモート展開

CA Virtual Assurance は、SystemEDGE および他のエージェントをすべての管理対象システムにリモートで展開するための包括的なソリューションを提供します。カスタマイズ済みインストール パラメータを含む提供パッケージに基づいて展開テンプレートを作成し、これらのテンプレートを多数の管理対象システムに同時に展開できます。この自動展開ソリューションによって、1 つの場所から、企業全体にわたってエージェントを展開して設定することが可能となります。

リモート展開には、以下の機能があります。

展開設定

ターゲット システムへのソフトウェア パッケージのインストール方法を定義する設定を作成、編集、および削除できます。これらは、「パッケージラッパー」と呼ばれます。

展開ジョブ管理

展開ジョブの作成、開始、および取り消しが可能になり、複数の配布サーバを使用して複数のターゲットにパッケージを同時に展開できます。

展開ジョブ レポート

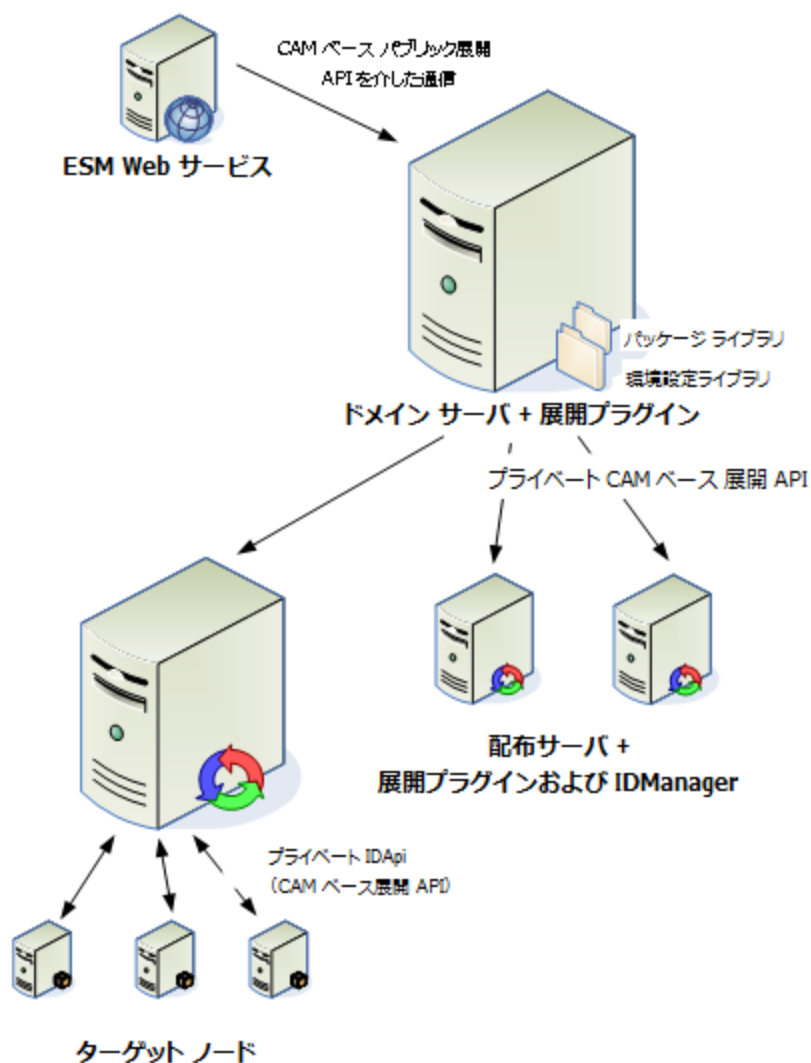
展開ジョブのステータスのクエリ機能を提供します。

展開イベント

管理対象ノードの状態を追跡する展開関連イベントのソースを提供します。

リモート展開アーキテクチャ

展開ソリューションの全体的アーキテクチャは、ドメイン サーバおよび配布サーバコンポーネントによって推進されます。以下の図は、展開関連コンポーネントの概要を表しています。



展開コンポーネント

このセクションでは、展開の主要コンポーネントのリストを示し、簡単に説明します。

ドメイン サーバ

ドメイン サーバは、すべての設定および制御データのリポジトリです。サーバは、展開操作に必要な設定およびソフトウェア パッケージ データの管理を担当し、すべての設定操作を管理しています。詳細なイベント データが、展開プロセス中にドメインおよび配布サーバ間で渡されます。単一のドメイン サーバにより、すべての配布サーバジョブのステータスが維持されます。

配布サーバ

配布サーバは、同じマシンに置かれている **Infrastructure Deployment Manager (IDManager)** サーバを制御します。アーキテクチャでは、複数の配布サーバによって提供される展開サービスが考慮されています。

インフラストラクチャ展開

インフラストラクチャ展開によって展開ジョブが開始され、管理されます。展開プロセス中に、**Infrastructure Deployment Manager (IDManager)** がリモートシステムへのアクセスを提供し、**Infrastructure Deployment Primer (IDPrimer)** が、エージェントソフトウェア パッケージをリモートでインストールするメカニズムを提供します。IDPrimer は、ターゲットコンピュータに展開パッケージ データを転送して、インストールを実行するために使用されます。それ以降の同じターゲットコンピュータへの展開では常に、すでにインストールされた IDPrimer を使用できます。IDManager は、すべての展開操作を制御し、ジョブ ステータスを処理します。

複数の配布サーバの使用

リモート展開ソリューションでは、単一の中央サーバ(マネージャマシン)ですべての展開を管理できますが、以下の要件のいずれかを満たす場合は、中央ドメインサーバを指すリモート配布サーバをインストールすることをお勧めします。

- 2か所以上の地理的な場所にエージェントソフトウェアを展開する必要があるが、それらを単一のマネージャマシンで一元管理する必要がある。

この場合は、それぞれの場所に、中央ドメインサーバに接続する配布サーバを備えた、1つ以上の配布サーバを配置することをお勧めします。

- 場所は1つであるが、展開する必要のあるマシンが数百台ある。

この場合は、サブネット上で論理的に分離された多くの配布サーバをインストールできます。これらの配布サーバは、中央ドメインサーバに接続します。

配布サーバが接続するドメインサーバの変更

ドメインサーバマシンのネットワークアドレスが元のインストールの後に変更される場合は、新しいネットワークアドレスに接続するように配布サーバを再設定する必要があります。

以下に示すように設定を変更する前に、新しいネットワークアドレスが配布サーバから接続可能であることを確認することが重要です。配布サーバが新しいアドレスでドメインサーバに接続できない場合は、展開機能が正しく動作しません。

配布サーバが接続するドメインサーバを変更する方法

1. [スタート]メニューから、[管理ツール]-[サービス]を開きます。
[サービス]ユーザインターフェースが表示され、インストールされたサービスのリストが表示されます。
2. [CA SM 配布サーバ]を右クリックし、[プロパティ]を選択します。
[プロパティ]ダイアログボックスが表示されます。

3. [停止]をクリックして、サービスを停止します。
4. [開始パラメータ]フィールドに、以下のパラメータを入力します。

`-m domainserver`

`domainserver` パラメータで、ドメイン サーバの IP アドレスまたは DNS 名を指定します。

5. [開始]をクリックします。

これで、配布サーバは、入力したドメイン サーバのアドレスに接続しようとします。

スケーラビリティ

展開システムは、複数の配布サーバをスケーラビリティレイヤとして使用して、ある程度のスケーラビリティを提供します。各配布サーバは、1 つの **IDManager** インスタンスと通信します。**IDManager** は、複数のターゲットコンピュータへの複数のコンポーネント展開を管理できます。**CA Virtual Assurance** では、この連合モデルにより、多くの同時展開がサポートされます。

監査証跡

ジョブとタスクは、展開システムの 2 つの基本概念です。展開ジョブは、1 つ以上のターゲットシステムにインストールされる 1 つ以上の設定を指定します。ターゲットシステム上のソフトウェア パッケージの個々のインストールは、タスクによって表されます。展開ジョブ レポートは、展開ジョブのステータスのクエリ機能を提供します。

展開ジョブの状態を作成、制御、および照会することができます。ジョブが開始されると、その個々の展開タスクが、実際の展開を実行する利用可能な配布サーバに委任されます。ジョブの進行につれ、進捗状況を追跡できるため、展開が確実に実行され、問題があれば、迅速に識別して修正できます。

リモート展開は、以下の情報を提供できます。

- 現在、どの展開ジョブが：
 - 非アクティブである(まだ開始されていない)
 - アクティブ
 - 完了しているもののうち、どれが：
 - 成功
 - 部分的に成功
 - 失敗
- どの展開ジョブが：
 - 特定のターゲット マシンに関連付けられているか
 - 特定のパッケージ/パッケージ グループに関連付けられているか
- どのパッケージが特定のターゲット マシンに展開されたか
- どのユーザが特定のパッケージの展開を作成/開始したか
- どのマシンが特定の展開ジョブでターゲットになるか
- どのマシンがアクティブな展開ジョブのターゲットになるか

注: リモート展開は、**noexec** フラグでマウントされた **/tmp** ファイル システムを備えた **UNIX/Linux** システムへのソフトウェアの展開をサポートします。

UI の[ジョブ]ペインには、作成したすべての展開ジョブの表が表示されます。これは、ジョブ ID と説明、含まれるパッケージ、ジョブ ステータスなどのリストです。この表から、ジョブが失敗した理由を含む、特定のジョブに関する詳細を確認できます。このビューにアクセスするには、UI の[ジョブ]フォルダをクリックします。詳細については、オンライン ヘルプを参照してください。

展開の制限

展開を実行する前に、以下の点を考慮してください。

- **CA Virtual Assurance** マネージャ システムにエージェントをインストールする場合は、手動のスタンドアロン エージェント インストールを実行する必要があります。**CA Virtual Assurance** マネージャ システムでのエージェントの展開はサポートされていません。

- 既存のホストオペレーティングシステム サービスを使用して、ターゲットシステムへのリモートアクセスを獲得できるかどうかによって、展開プロセスが異なります。これらのサービスがターゲット ノードで利用可能でない場合は、IDPrimer クライアント パッケージおよび対応するキーをターゲットシステムにインストールすることが必要になります。詳細については、「[インフラストラクチャ展開プライマ ソフトウェアの手動インストール](#)」を参照してください。
- 展開は、サポートされるエージェント プラットフォームの大部分 (すべてではない) でサポートされています。展開のサポートの詳細については、リリースノートを参照してください。

展開認証情報の制限

UI では、ユーザ名とパスワードのフィールドへのエントリはいずれも、64 文字に制限されています。

非特権ユーザ アカウントを使用した UNIX/Linux へのリモート展開

非特権ユーザ アカウントを使用する場合は、`sudo` 設定に関する以下の要件を考慮してください。

- `sudo` では、実行されたプログラムに有効な疑似端末が接続されていることを強制できません。このような検証を特定のユーザ（グローバルに有効である場合）に対して無効にするには、`/etc/sudoers` ファイルに「Defaults: \$username !requiretty」という行を追加します。`$username` は、リモート展開に使用する実際のユーザ名に置換します。

ファイルを編集する標準的な方法は、`visudo` コマンドの使用です。`visudo` コマンドは `$EDITOR` を起動します。編集が完了すると、ファイルの構文が確認されます。結果が有効でない場合、`visudo` はファイルの保存をブロックします。

- `sudo` では、上位のプログラムを実行する前にユーザにパスワードを要求できません。この動作を実行するには、ユーザに権限を与える行に `NOPASSWD:` キーワードが存在することが必要です。
- `sudo` では、必要なコマンドまたはすべての実行が可能である必要があります。上記の要件を満たす設定エントリ（`/etc/sudoers` 内の行）の例は、次のとおりです。

```
$username ALL=(ALL) NOPASSWD: ALL
```

または

```
$username ALL = NOPASSWD: /usr/bin/id,/bin/sh /tmp/idprimer/PifInst -r  
/tmp/idprimer/install.rsp
```

注: `$username` は、リモート展開に使用する実際のユーザ名に置換します。

Solaris では、`pfexec` の以下の要件を考慮してください。

- すべてのローカル ユーザには、以下のコマンドで「プライマリ管理者」プロファイルが付与できます。

```
usermod -P "Primary Administrator" {user}
```

- すべての非ローカル ユーザには、`/etc/user_attr` ファイル内のエントリを手動で追加して、「プライマリ管理者」プロファイルが付与できます。

```
user::::type=normal;profiles=Primary Administrator
```

展開のサイジング キー ファクタ

インフラストラクチャのサイジングやシステム パフォーマンスには、以下のような、大きな影響を与える数多くのキー ファクタがあります。

- 配信するソフトウェア パッケージのサイズ。
- 配信するソフトウェア パッケージの数。
- ソフトウェア パッケージ配信の頻度。
- 展開コンポーネントとターゲット コンピュータの間のネットワーク遅延。
- ネットワーク帯域幅の管理。

ターゲットへの初期展開では、小規模のインストール エージェントである IDPrimer がインストールされます。一度 IDPrimer がインストールされると、同じターゲットへの以降の展開にかかる時間が短縮されます。

理想的な条件下では、1 台の配布サーバで、1 時間あたり約 50～100 個の SystemEDGE パッケージをインストールできます。ただし、展開の前提条件のいずれかを満たしていないために失敗するタスクが多い場合は、配布サーバのスループットが減少します。

推奨事項:

- ターゲット サーバが通常は、ソフトウェアのリモート展開の要件を満たしていることを確認します。
- 1 台の配布サーバでは、500 台のターゲット サーバを問題なく処理できます。
- 追加の配布サーバは、ターゲットのローカルな場所にインストールします。
- 可能な場合は、ターゲットのローカルな配布サーバを使用して展開します。
- 可能な場合は、ネットワークトラフィックが低い期間に展開を開始するようにスケジュールします。

カスタム ポートを使用した SystemEDGE エージェントの展開/インストール

標準以外のポートに SystemEDGE エージェントを展開するには、多くの設定を実行する必要があります。展開後にマネージャが確実にシステムを検出して管理できるようにするには、以下の手順に従います。

1. パッケージ ラッパーを更新します。
 - リモート展開ソリューションを使用している場合は、まず、包装係を設定して、使用するポートを指定する必要があります。ユーザ インターフェイスで[プロビジョニング]-[展開]に移動し、[ポート]フィールドを変更します。書き込みコミュニティ文字列も、ここで更新できます。
2. CA Virtual Assurance で SNMP コミュニティ文字列を更新します。
 - マネージャが標準以外のポートを使用して正常にマシンのモニタリングと管理を行うには、モニタリングと管理に使用する、適切なポート/書き込みコミュニティ文字列の組み合わせを認識している必要があります。そのためには、複数のシステムのモニタリングと管理に使用できるグローバルな SNMP エントリを作成するか、サーバ固有の SNMP エントリを作成することができます。
 - グローバル SNMP 設定を更新する方法: ユーザ インターフェイスで[管理]-[SNMP]に移動し、適切な SNMP コミュニティ文字列/ポートの組み合わせを含む新しいエントリを追加します。
 - サーバ固有の SNMP 設定を更新する方法: [ポリシー]-[エクスプローラ]-[Machine_Name]-[メトリック]-[SNMP 設定]に移動し、必要なポート/書き込みコミュニティ文字列の新しいエントリを追加します。

これらの設定を更新した後は、通常の方法でエージェントを展開/インストールできます。その後、SystemEDGE プラットフォーム管理モジュールがカスタムのポート/書き込みコミュニティ文字列の組み合わせを使用して、サーバを検出、モニタ、および管理を行います。

SystemEDGE エージェント用ポートの再設定

エージェントを再インストールすると、SystemEDGE エージェント用のポートを再設定できます。エージェントを再インストールした後は、再設定するポートの詳細をプロビジョニングで編集しても、設定は変わりません。

展開パッケージ ライブラリ

パッケージ ライブラリには、インストール可能なソフトウェア パッケージの設定可能なセットが含まれており、これを使用して、展開に使用できる製品、バージョン、およびプラットフォームを制御できます。設定されたソフトウェア パッケージの無人インストールに必要なパラメータを定義する標準パッケージ設定を作成すると、これらの製品のインストール方法を制御できます。

各パッケージには、関連付けられたパッケージ設定ファイルが必要です。設定ファイルは、パッケージの詳細とパッケージ インストールの設定方法を説明する情報の両方を提供します。詳細については、「[展開パッケージ設定ファイル \(P. 233\)](#)」セクションを参照してください。

パッケージ ライブラリは、以下のディレクトリにあります。

```
%AllUsersProfile%¥Application
Data¥CA¥SM¥domainserver¥Deployment¥Packages
```

ディレクトリツリーのレイアウトは、IDManager コンポーネントの要件によって定義されます。パッケージライブラリ自体は、2 つのサブディレクトリ、**Public** および **Private** が含まれるトップレベルのパッケージ ディレクトリから構成されます。**Public** ディレクトリには、展開可能なすべてのソフトウェア パッケージが含まれます。

```

..
├── SM
│   ├── CA_LiteAgent
│   ├── CA_ProcProbe_Utility
│   ├── CA_SystemEDGE_AdvancedEncryption
│   ├── CA_SystemEDGE_Core
│   │   ├── 5.6.0
│   │   │   └── ENU
│   │   │       ├── AIX_aix
│   │   │       ├── HPUX_hp
│   │   │       ├── HPUX_ia64
│   │   │       ├── Linux_ia64
│   │   │       ├── Linux_x86
│   │   │       ├── Solaris_sparc
│   │   │       ├── Solaris_x86
│   │   │       ├── Windows_ia64
│   │   │       ├── Windows_x64
│   │   │       └── Windows_x86
│   ├── CA_SystemEDGE_ESAD
│   ├── CA_SystemEDGE_HyperV
│   ├── CA_SystemEDGE_LPAR
│   ├── CA_SystemEDGE_MSCS
│   ├── CA_SystemEDGE_RM
│   ├── CA_SystemEDGE_SRM
│   ├── CA_SystemEDGE_UCS
│   ├── CA_SystemEDGE_Zone
│   └── CA_VMVCAIM

```

トップレベル **Public** ディレクトリには、5 つのサブディレクトリがあります。

コンポーネント名

IDManager インスタンス名である必要があります (CA Virtual Assurance の場合は SM)。

ソフトウェア パッケージ

単一の展開可能なパッケージのすべてのバージョン、ローカリゼーション、およびアーキテクチャが含まれます (CA_SystemEDGE_Core、CA_SystemEDGE_SRM など)。

バージョン

内部に含まれるソフトウェア パッケージのバージョン (5.0.1 など)。

言語

インストール パッケージ言語。例: ENU

アーキテクチャ

アーキテクチャ固有のインストール要素 (Windows_ia64、Solaris_x86 など)。アーキテクチャ ディレクトリ名は、IDManager でサポートされるプラットフォームのいずれかである必要があります。

配布サーバ マシン内で実行される場合、IDManager コンポーネントは配布サーバの下のディレクトリを使用します。これには、その内部使用のために暗号化されたパッケージの一時キャッシュが含まれます。これらのパッケージは、ジョブの完了時に削除する必要があります。

プライベート IDPrimer インストール要素は、別のディレクトリ内に含まれています。これらはデフォルトで、IDManager コンポーネント自体のインストール ディレクトリの下以下のディレクトリに格納されています。

<CA Shared Components>/IDMgrApi/packages/private/idprimer

このディレクトリには、インフラストラクチャ展開コンポーネントでサポートされるすべてのプラットフォームの IDPrimer インストール要素が含まれます。

展開パッケージ ライブラリの保守

次のように、展開パッケージの保守を実行する場合があります。

- 新しい展開パッケージの追加
- 既存のパッケージを新しいパッケージにコピーして、同じベース パッケージ (マスタ イメージ パッチ) のパッチ バージョンを作成します。
- 不要になったパッケージを削除します。
- インストール メディアまたは別の指定ディレクトリから、CA Virtual Assurance 互換のパッケージをパッケージ ライブラリ内にコピーします。
- すべての登録パッケージを新しい名前でもコピーし、そのパッケージ用の新しい UUID を生成します。
- パッケージ ライブラリおよび関連付けられた展開設定データの整合性のチェックを実行します。

パッケージ フィルタ

サーバにアップグレードが適用されている場合は、数が増加するパッケージバージョンをリモート展開で表示できます。このリリースのデフォルト動作では、利用可能な最新のパッケージのみが表示されます。その結果、[パッケージ]-[詳細]タブのデータもフィルタされ、各パッケージの最新バージョンのみが表示されます。このパネルからラッパーを選択すると、選択されたラッパーの位置でツリーが展開されます。

すべてのパッケージを表示する場合は、[パッケージ]情報パネルの[最新パッケージのバージョンのみを表示します]チェックボックスを使用してデフォルトフィルタ動作を上書きできます。このチェックボックスをオンにした場合(デフォルト)は、左側のツリーおよび[パッケージの詳細]タブで古いパッケージバージョンがすべてフィルタされ、表示されなくなります。

フィルタリング動作を変更する方法

1. [パッケージ情報]パネルにある[最新パッケージのバージョンのみ]チェックボックスをオン/オフにします。
2. ユーザ インターフェースで[展開]ビューをリフレッシュします。
最新のパッケージ バージョンが表示されます。

注: UI 内で、パッケージ バージョンが表示される他の場所がすべて影響されるとは限りません。

展開パッケージ設定ファイル

ソフトウェア パッケージ インストール要素に加え、展開可能な各パッケージを、追加のパッケージ設定ファイル `pkginfo_PLATFORM.xml` で参照する必要があります。パッケージ設定ファイルでは、インストールするパッケージとインストールの設定方法が説明されます。この設定ファイルは以下を提供します。

- インストール パッケージのローカライズ可能な説明
- UI で受諾される必要のあるすべてのエンド ユーザ使用許諾契約 (EULA) のテキスト

- マシンで読み取り可能な形式でパッケージ依存性をエンコードできるメカニズム
- 一般的にアクセス可能なインストール パラメータ タイプの文書化
- 一定のレベルの検証を UI 内で実行するための、パラメータ タイプへの追加コンテキスト。
- パッケージ インストール プログラムでパラメータを表すのに使用される、パラメータ名とトークンの間のマッピング (プラットフォームに依存しない方式)
- ターゲット マシンでのインストール要素の実行方法を指定します。
- インストーラ終了コードと、展開システムが解釈したコードの間のマッピング

pkginfo.xml ファイルのローカライズ済み要素を、ロケール固有のファイルを並行使用して提供するか、または単一のファイルに埋め込むことができます。ロード時に、名前がファイル名 pkginfo_PLATFORM.xml に一致するあらゆるファイルをロードして、ローカライズされたメッセージ データを取得できます。

展開システムがパッケージ設定ファイルを、パッケージング ツリー内のプラットフォーム固有のサブディレクトリと並行して見つける必要があります。単一のパッケージ説明ファイルで、複数のプラットフォームでのインストールを説明できます。以下のディレクトリを参照してください。

%AllUsersProfile%¥Application

Data¥CA¥SM¥domainserver¥Deployment¥Packages¥SM¥CA_SystemEDGE_Core¥5.6.0¥ENU

pkginfo_AIX.xml
pkginfo_HPUX.xml
pkginfo_Linux.xml
pkginfo_Solaris_sparc.xml
pkginfo_Solaris_x86.xml
pkginfo_Windows.xml

展開パッケージ

展開パッケージは、企業全体にわたるシステムにモニタリング ソフトウェアを展開するために必要なマテリアルを提供します。以下の展開パッケージが利用可能です。

CCA エージェント

CCA エージェントを提供します。

CA LiteAgent

CA Performance Lite Agent を提供します。

SystemEDGE

コア SystemEDGE エージェントを提供します。

SystemEDGE Advanced Encryption

SystemEDGE の FIPS 140 準拠暗号化パッケージを提供します。

SystemEDGE AIX LPAR

LPAR AIM を提供します。

SystemEDGE ESAD

Exchange Server および Active Directory (ESAD) AIM を提供します。

SystemEDGE Hyper-V

Hyper-V AIM を提供します。

SystemEDGE MSCS

Microsoft クラスタ サポート (MSCS) AIM を提供します。

SystemEDGE RM

リモート モニタリング AIM を提供します。

SystemEDGE Solaris ゾーン

Solaris ゾーン AIM を提供します。

SystemEDGE SRM

SRM AIM を提供します。

SystemEDGE UCS

Cisco UCS AIM を提供します。

SystemEDGE VC

VMware vCenter AIM を提供します。

Solaris ゾーン、リモート モニタリング、vCenter、および SRM の各 AIM はすべて、SystemEDGE 5.6 と Advanced Encryption パッケージの両方に依存します。そのため、これらのパッケージのいずれかを展開する場合は、SystemEDGE と Advanced Encryption がすでにシステムに存在するか、この両方を展開ジョブに含める必要があります。

展開パッケージは、プラットフォーム固有のバージョンに分解でき、展開をサポートするすべてのプラットフォームでパッケージラッパーが利用可能です。

デフォルト パッケージ ラッパー

デフォルトのパッケージラッパーが提供されており、リモート展開を使用して展開できるソフトウェア パッケージにすぐに使用できます。これらのパッケージラッパーには、特定のソフトウェア パッケージ用に可能な部分にデフォルト値を備えたインストーラ パラメータが含まれます。セキュリティ上、デフォルト値の設定が危険である必須パラメータ (SNMP 書き込みコミュニティ文字列、ユーザ名、パスワードなど) がパッケージに必要な部分、または、ユーザの環境に固有であるためにデフォルト値を設定できない部分 (vCenter ホスト名) では、デフォルトパッケージラッパーに、事前入力されるデフォルト値が含まれません。つまり、必須パラメータを含むデフォルト パッケージラッパーは、最初に編集し、必須パラメータ値を入力して保存する必要があります。その後に、それらを展開ジョブで使えるようになります。

以下のパッケージラッパーには、展開の前に入力する必要のある必須パラメータが含まれます。

SystemEDGE RM

このパッケージを展開するためのユーザ名とパスワードを指定します。

SystemEDGE MSCS

このパッケージを展開するための MSCS ホスト名、MSCS ユーザ名、およびパスワードを指定します。

SystemEDGE VC

このパッケージを展開するための vCenter ホスト名、ユーザ名、およびパスワードを指定します。

SystemEDGE LPAR AIM

このパッケージを展開するためのホスト名、ユーザ名、およびパスワードを指定します。

SystemEDGE Solaris ゾーン

このパッケージを展開するためのホスト名、ユーザ名、およびパスワードを指定します。

SystemEDGE UCS

このパッケージを展開するためのホスト名、ユーザ名、パスワード、プロトコル、およびポートを指定します。

SystemEDGE Hyper-V

このパッケージを展開するためのホスト名、ユーザ名、およびパスワードを指定します。

デフォルトパッケージラッパーの必須値の編集が必要なのは、最初の展開の前の 1 回のみです。これらは、パッケージのインストーラ パラメータ値の変更が必要にならない限り、再度編集する必要はありません。必須パラメータが入力されていないデフォルトパッケージラッパーでパッケージの展開を続行した場合は、パッケージラッパーが展開可能な状態ではないことが展開ウィザードで示されます。

詳細については、オンライン ヘルプを参照してください。

書き込みコミュニティを含まないエージェント設定

SystemEDGE パッケージラッパーの書き込みコミュニティの設定は必須ではありませんが、以下を考慮してください。

- SystemEDGE エージェントに **SNMP** 読み取りコミュニティのみが設定されており、書き込みコミュニティが設定されていない場合でも、このエージェントは **SystemEDGE PMM** で検出可能です。ただし、**SNMP** 書き込みコミュニティが設定されたエージェントがない場合は、エージェントにポイント設定変更を実行できません。
- 完全な **vCenter** およびリモート モニタリング機能は、エージェントに書き込みコミュニティが設定されている場合にのみサポートされます。**SNMP** 書き込みコミュニティが設定されたエージェントがない場合は、**CA Virtual Assurance UI** からの **AIM** 設定および管理を実行できません。
- 書き込みコミュニティのないエージェントは、**CA Virtual Assurance UI** からポリシー設定を使用して、インストール後に設定できます。ポリシー設定を使用すると、**SNMP v1/2** より安全な **SNMP v3** を使用するようにエージェントを設定することもできます。

新規パッケージ ラッパーの作成

パッケージラッパーは、特定のパッケージの展開時に使用する、展開メカニズムのプラットフォーム固有の手順を提供します。各パッケージには、リモート展開をサポートする、すべてのプラットフォーム用のデフォルトのパッケージラッパーが含まれています。デフォルトとは異なる設定が必要なシステムがある場合は、新しいパッケージラッパーを作成できます。

次の手順に従ってください：

1. [リソース]-[展開] を選択します。
[展開] ペインに [パッケージ]、[テンプレート]、および [ジョブ] フォルダが表示されます。
2. [パッケージ] を展開します。
利用可能なパッケージのリストが [展開] ペイン内に表示されます。
3. [展開] ペイン内のパッケージ名を右クリックし、[新しいラッパーの作成] を選択します。または、[利用可能なラッパー] ツールバーの [+] (新規) をクリックします。
[新規ラッパー] ダイアログ ボックスが表示されます。

4. ラッパーの名前および説明 (オプション) を入力し、ラッパーがサポートするプラットフォームを指定して、[OK] をクリックします。

ラッパーが作成され、詳細が右側のペインに表示されます。

注: SystemEDGE パッケージラッパーを作成する場合は、[トラップ ポート]、[トラップ先]、および[トラップ コミュニティ]フィールドの間の依存性を考慮してください。これらのフィールドは、どれも設定しないか、すべてを設定するかのいずれかにする必要があります。一部のフィールドを設定した場合は、インストーラがエラー メッセージを表示します。

パッケージ ラッパーの変更

パッケージ ラッパーは、インストール パス、ポート、トラップ コミュニティなど、展開パッケージのプラットフォーム固有のインストール設定セットを定義します。ユーザが作成した、またはデフォルトのパッケージ ラッパーを編集して、このインストール設定のセットを変更することができます。利用可能なプロパティは、パッケージのタイプによってさまざまです。

パッケージ ラッパーを変更する方法

1. [リソース]-[展開] を選択します。

[展開] ペインに[パッケージ]、[テンプレート]、および[ジョブ]フォルダが表示されます。

2. [パッケージ]、パッケージの特定の種類、およびラッパー プラットフォームを展開し、変更するラッパーを選択します。

右側のペインにラッパーの詳細が表示されます。

3. 必要に応じて、パッケージプロパティを変更して[保存]をクリックします。
[プロパティ]ペインに表示されるオプションは、選択したパッケージタイプによって異なります。

パッケージタイプ:

CA AIX LPAR AIM

ホスト名

IBM LPAR サーバへの接続に使用するホスト名を指定します。このパッケージを展開するには、IBM LPAR ホスト名を指定する必要があります。

ユーザ名

IBM LPAR サーバへの接続に使用するユーザ名を指定します。このパッケージを展開するには、IBM LPAR ユーザ名を指定する必要があります。

パスワード

IBM LPAR サーバへの接続に使用するパスワードを指定します。このパッケージを展開するには、IBM LPAR パスワードを指定する必要があります。

シリアル番号

IBM LPAR サーバへの接続に使用するシリアル番号を指定します。このパッケージを展開するには、シリアル番号を指定する必要があります。

CA LiteAgent

共有パス

未設定の場合に CA 共有コンポーネントに使用するルートインストールディレクトリを定義します。

インストール パス

パッケージ用のルートインストール ディレクトリを定義します。

[再起動の抑制]チェック ボックス

抑制されていなければインストールの終わりに発生する可能性のある自動再起動を抑制するかどうかを指定します。

CA Solaris ゾーン AIM

ゾーン ホスト

Solaris ゾーン サーバへの接続に使用するホスト名を指定します。このパッケージを展開するには、Solaris ゾーン ホスト名を指定する必要があります。

ユーザ名

Solaris ゾーン サーバへの接続に使用するユーザ名を指定します。このパッケージを展開するには、Solaris ゾーン ユーザ名を指定する必要があります。

パスワード

Solaris ゾーン サーバへの接続に使用するパスワードを指定します。このパッケージを展開するには、Solaris ゾーン パスワードを指定する必要があります。

SystemEDGE

インストール パス

パッケージ用のルート インストール ディレクトリを定義します。

データ パス

パッケージ用のデータ ディレクトリを定義します。

共有パス

未設定の場合に CA 共有コンポーネントに使用するルート インストール ディレクトリを定義します。

ポート

SystemEDGE ポート番号を定義します。

デフォルト: 161

説明

SNMP システムの説明を定義します。

場所

SNMP システムの場所を定義します。

連絡先

SNMP システムの連絡先を定義します。

読み取りコミュニティ

SNMP 読み取り専用コミュニティ文字列を定義します。

デフォルト: public

読み取り/書き込みコミュニティ

SNMP 読み取り/書き込みコミュニティ文字列を定義します。

トラップ コミュニティ

SNMP トラップ コミュニティ文字列を定義します。

トラップ先

SNMP トラップ先のホスト名を定義します。

トラップ ポート

SNMP トラップ ポートを定義します。

デフォルト: 162

権限分離ユーザ (UNIX/Linux)

SNMP 通信中にエージェントが使用して実行する認証情報のユーザ名を指定します。

このエントリは、別のユーザ アカウントで **SNMP** 通信を実行するようにエージェントに指示します。このエージェントはまた、有効なグループとして、このユーザのデフォルトグループを使用します。

デフォルト: エージェントは **root** アカウントを使用して動作します。

[エージェントの起動]チェック ボックス

インストールの最後に SystemEDGE を自動的に開始するかどうかを指定します。

[再起動の抑制]チェック ボックス

抑制されていなければインストールの終わりに発生する可能性のある自動再起動を抑制するかどうかを指定します。

[ネイティブ エージェントの無効化]チェック ボックス

ネイティブ SNMP エージェントを置換するかどうかを指定します。

[ネイティブ設定を使用]チェック ボックス

ネイティブ SNMP エージェント設定を使用するかどうかを指定します(ネイティブ SNMP エージェントを置換する場合)。

[管理対象モードでの実行]チェック ボックス

管理対象モードで SystemEDGE を実行するかどうかを指定します。

[管理対象ポリシー名]ドロップダウン リスト

利用可能な SystemEDGE ポリシーのリストを指定します。

注: バージョン 4.3 またはバージョン 4.2 パッチ レベル 3 から SystemEDGE をアップグレードする場合、インストーラは以下のパラメータのみを使用します。

CASE_PUBDATADIR
CASE_MANAGER_HOSTNAME
CASE_MANAGER_POLICY_NAME
CASE_START_AFTER_INSTALL
CASE_LEGACY_MODE
CASE_SNMP_PORT
CASE_INSTALL_DOCS
CASE_SNMP_TRAP_COMMUNITY ⁽¹⁾
CASE_SNMP_TRAP_DESTINATION ⁽¹⁾
CASE_SNMP_TRAP_PORT ⁽¹⁾
CASE_SNMP_READ_COMMUNITY ⁽¹⁾
CASE_SNMP_WRITE_COMMUNITY ⁽¹⁾
CASE_SNMP_READ_ALLOWED_MANAGERS ⁽¹⁾
CASE_SNMP_WRITE_ALLOWED_MANAGERS ⁽¹⁾

その他のパラメータは無視されます。

(1) これらのパラメータは特別です。これらの設定は、既存の SystemEDGE 4.x 設定に追加され、これによって、SystemEDGE 4.x マネージャと SystemEDGE 5.x マネージャの両方が機能するようになります。

注: 上記のパラメータの詳細については、「SystemEDGE ユーザ ガイド」の「インストールおよび展開」の章を参照してください。

SystemEDGE Advanced Encryption

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

SystemEDGE Hyper-V

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

SystemEDGE RM**デフォルト WMI ユーザ名**

リモート マシンへの接続に使用するデフォルト ユーザ名を定義します。
このパッケージを展開するには、ユーザ名を指定する必要があります。

デフォルト WMI パスワード

リモート マシンへの接続に使用するデフォルト パスワードを定義します。
このパッケージを展開するには、パスワードを指定する必要があります。

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

SystemEDGE SRM**[スクリプトを許可]チェック ボックス**

テストとしてのスクリプトの実行を許可するかどうかを指定します。

[ファイル I/O テストを許可]チェック ボックス

テストとしてのファイル I/O の実行を許可するかどうかを指定します。

[ユーザ TOS の無効化]チェック ボックス

アプリケーションが送信 IP パケットでサービスビットのタイプを設定しないようにするかどうかを指定します。

[信頼できない SSL の許可]チェック ボックス

未検証の証明書を備えた SSL サイトへのアクセスを許可するかどうかを指定します。

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

SystemEDGE UCS

UCS ホスト名

UCS への接続に使用するホスト名を指定します。このパッケージを展開するには、UCS ホスト名を指定する必要があります。

UCS ユーザ名

UCS への接続に使用するユーザ名を指定します。このパッケージを展開するには、UCS ユーザ名を指定する必要があります。

UCS パスワード

UCS への接続に使用するパスワードを指定します。このパッケージを展開するには、UCS パスワードを指定する必要があります。

UCS プロトコル

HTTP と HTTPS のどちらのプロトコルを使用するかを指定します。

ポート

UCS ポート番号を定義します。

デフォルト: HTTP 用の 80 または HTTPS 用の 443。

SystemEDGE VC

VirtualCenter ホスト名

VirtualCenter への接続に使用するホスト名を指定します。このパッケージを展開するには、VirtualCenter ホスト名を指定する必要があります。

VirtualCenter ユーザ名

VirtualCenter への接続に使用するユーザ名を指定します。このパッケージを展開するには、VirtualCenter ユーザ名を指定する必要があります。

VirtualCenter パスワード

VirtualCenter への接続に使用するパスワードを指定します。このパッケージを展開するには、VirtualCenter パスワードを指定する必要があります。

VirtualCenter ポート

VirtualCenter ポート番号を定義します。

デフォルト: 443

VirtualCenter プロトコル

HTTP と HTTPS のどちらのプロトコルを使用するかを指定します。

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

展開ジョブ

ターゲット システムにエージェントを展開するには、展開ジョブを作成する必要があります。展開ジョブには、適切な時間に適切なシステムに展開パッケージを配信するために CA Virtual Assurance に必要な詳細情報が含まれます。展開ジョブを作成するときは、以下の情報を指定します。

ジョブ情報

ジョブ名および、既存のテンプレートに基づいたジョブを作成するかどうかが含まれます。

展開パッケージ

プラットフォーム、展開するパッケージ、および各パッケージ固有のラッパーが含まれます。

マシン情報

パッケージの展開先のシステムと、接続の確立に必要なシステム認証情報が含まれます。

展開時間

展開を、すぐに実行するか、特定の時間だけずらして実行するか、または将来の特定の時間にスケジュールして実行するかを指定します。

また、ジョブを作成した後に、テンプレートとして保存できます。テンプレートには、パッケージとマシンの選択内容が保存されるため、以降のジョブで簡単に再使用できます。

展開ジョブの作成と展開の実行の詳細については、オンライン ヘルプを参照してください。

展開ジョブのステータスの追跡

コンピュータのセットにエージェント パッケージのセットを展開するジョブが開始されたら、その進捗状況とステータスを追跡できます。[ジョブ]フォルダには、作成されたすべての展開ジョブの表が表示され、これには、ジョブ名、含まれるパッケージ、ジョブ ステータスなどのリストが含まれます。この表から、ジョブが失敗した理由を含む、特定のジョブに関する詳細を確認できます。

展開ジョブのステータスを追跡する方法

1. [リソース]-[展開]ペインを選択します。
[展開]ペインに[パッケージ]、[テンプレート]、および[ジョブ]フォルダが表示されます。
2. [ジョブ]フォルダをクリックします。xxxxxx
[ジョブ ステータス]ペインが表示されます。
3. 表示するジョブをクリックします。
[ジョブ情報]ページが表示されます。

4. [タスク ステータス] ペインで、利用可能なフィルタのいずれかを使用して特定のジョブ タスクをフィルタします。あるいは、ページング インターフェースを使用してタスクを特定します。
5. [拡張ステータス] をクリックしてジョブの拡張情報を表示します。

ジョブに関する詳細を含む[拡張済みステータス情報]ダイアログ ボックスが表示されます。

情報

ジョブに関する一般情報を表示します。

メッセージ

ジョブに関するメッセージ(「パッケージの配信に失敗しました」など)を表示します。

理由

失敗の理由を表示します。

アクション

問題を修正するために取るアクションを表示します。

展開失敗の共通の原因には、以下のものがあります。

- マシン可用性が不足
- システム認証情報が無効
- システム ホスト名を解決できない
- パッケージ依存性を実現できない(SRM AIM 展開を成功させるには SystemEDGE が必要、など)。

展開履歴の表示

展開履歴情報は、以下の場所で利用可能です。

[展開] ペイン

完了、アクティブ、保留中、失敗の展開タスクの数、および成功した展開のサマリが表示されます。このビューにアクセスするには、最上位の[展開] フォルダをクリックします。

[ジョブ]ペイン

ジョブ名、含まれるパッケージ、およびジョブ ステータスのリストを含む、作成したすべての展開ジョブの表が表示されます。この表から、ジョブが失敗した理由を含む、特定のジョブに関する詳細を確認できます。展開失敗の共通の原因には、以下のものがあります。

- システム認証情報が無効
- システム ホスト名を解決できない
- パッケージ依存性を実現できない (SRM AIM 展開を成功させるには SystemEDGE が存在する必要がある、など)。

このペインからジョブを再サブミットし、失敗の理由を修正して再展開できます。

このビューにアクセスするには、[ジョブ]フォルダをクリックします。

展開ダッシュボードビュー

ダッシュボードには、展開メトリックを追跡するための以下のビューがあります。

展開タスク サマリ

完了、アクティブ、保留中、および失敗の展開タスクの数を示す円グラフとリストを表示します。

未解決展開タスク

正常に完了しなかった展開のリストを表示します。ジョブ ID をクリックすると、タスクが未解決である理由に関する詳細を表示できます。

アクティブな展開タスク

現在アクティブな展開タスクのリストを表示します。詳細には、関連付けられた展開ジョブ、ターゲット、パッケージ、および現在の状態が含まれます。タスク ID をクリックすると、現在のステータスの詳細を表示できます。

展開パッケージ サマリ

各展開パッケージタイプの展開の数を示す棒グラフを表示します。

完了した展開ジョブ

正常に完了した展開のリストを表示します。ジョブ ID をクリックすると、ジョブに関する詳細を表示できます。

インフラストラクチャ展開プロセス

展開を実行するときの展開プロセスの主要な手順は、以下のとおりです。

1. 管理者のコンピュータから、インフラストラクチャ展開クライアントコンポーネントが、1 つ以上のターゲットコンピュータのリストにエージェントをインストールする要求を IDManager マネージャに発行します。展開マネージャは、クライアントに対してリモートのコンピュータ上で実行されている場合があります。ターゲットのリストは、明示的なマシン名または IPv4 アドレスで構成されています。

注: 検出されたリソースにのみ展開できます。

各ターゲット コンピュータへの展開が成功するには、ターゲット名が明示的に入力されているかコンテナから取得されているかにかかわらず、展開マネージャ コンピュータで表示されているように、ターゲットのアドレスへの解決に適したターゲット名であることが重要です。たとえば、ディレクトリから取得されるターゲットのリストが完全修飾名 (ネットワークドメイン名を持つ) ではない場合、特定のネットワーク設定では展開を継続できないことがあります。

2. IDPrimer がターゲット コンピュータにインストール済みであるかどうかを確認されます。インストールされていない場合は、最初にターゲット コンピュータに IDPrimer がインストールされます。IDManager は、IDPrimer インストールパッケージを配信しようとしています。どのような方法を使用して配信されるかは、ターゲットの動作環境、およびその環境で有効になっているセキュリティによって異なります。IDPrimer イメージがターゲット コンピュータにコピーされた後、インストールが開始されます。

一部のオペレーティング システムには、IDPrimer インストールをリモート起動する方法がありません。この場合は、IDPrimer インストールの手動での実行が必要になる場合があります。

3. IDPrimer インストーラによって、インストーラ自体および CA メッセージ (CAM) コンポーネントがターゲット コンピュータにインストールされます。IDPrimer がインストールされ、IDManager がターゲット コンピュータから「インストール完了」シグナルを受信すると、パッケージ展開を開始することができます。IDManager マネージャで以前に IDPrimer がインストールされており、それを使用して認証を行っている場合は、ユーザ名またはパスワードを再度提供しなくても、その IDManager マネージャでパッケージを展開できます。その後の展開では、IDPrimer によって非対称の暗号化キーを使用して認証が行われ、すでにアクセスが取得された管理者へのアクセスが制限されます。

CA Virtual Assurance UI を介した展開マネージャの使用の詳細については、オンライン ヘルプを参照してください。

関連項目

[CA Virtual Assurance インフラストラクチャを自動展開するための前提条件](#) (P. 253)

[IPv6 アドレスを使用したインフラストラクチャ展開に関する注意事項](#) (P. 255)

[IDManager が使用する転送パッケージのプロトコル](#) (P. 256)

[インフラストラクチャ展開プライマソフトウェアの手動インストール](#) (P. 256)

[Windows での展開プライマ インストール](#) (P. 257)

[Linux または UNIX での展開プライマ インストール](#) (P. 257)

[展開管理証明書のプライマ インストールへの提供](#) (P. 258)

[Windows 上の展開管理証明書](#) (P. 258)

[Linux または UNIX 上の展開管理証明書](#) (P. 258)

[Linux の Compatibility Library](#) (P. 259)

CA Virtual Assurance インフラストラクチャを自動展開するための前提条件

このインフラストラクチャ展開コンポーネントを使用して、ターゲット コンピュータにリモートでエージェント ソフトウェアをインストールできます。このインストールは、ソースおよびターゲット コンピュータ上の基本オペレーティング システムで提供されている機能によってのみ実行でき、企業のネットワーク設定による制限の対象となります。

ソフトウェア展開時の最初のステップは、小規模のプライマ アプリケーションである IDPrimer をターゲット コンピュータにリモート インストールすることです。この IDPrimer ソフトウェアの役割は、その後にソフトウェア コンポーネントのインストール イメージを転送することと、そのインストールの起動を実行することです。ターゲット コンピュータに IDPrimer を配信する場合、展開マネージャは、ターゲットで有効なユーザ クレデンシャルを提供する必要があります。

IDPrimer は、以下のメカニズムのいずれかを使用して、ターゲット システムに転送されます。ターゲット コンピュータのオペレーティング システムを展開マネージャが認識している場合は、適切な転送メカニズムが選択されます。ターゲットのオペレーティング システムを判別できない場合は、以下の各メカニズムが順に試行されます。

- ネットワーク共有を開く

展開マネージャは、ターゲット システムにある **Windows** ネットワーク共有に接続します。デフォルトでは、共有名 **ADMIN\$** を使用しますが、これは、IDManager 設定オプションによって制御されます。このメカニズムは、**Windows** ベースのプラットフォームで実行している展開マネージャからのみ使用可能で、一部の **Windows** ターゲットに対してのみ成功します。**Windows XP Home** などの少し異なる **Windows** バージョンは、この展開のメカニズムをサポートしていません。

- SSH プロトコルを使用してターゲット コンピュータとのネットワーク接続を開き、SFTP を使用してプライマ インストール パッケージを転送する

このメカニズムは、SSH サーバが稼働しているすべてのコンピュータに対して機能しますが、Linux や UNIX コンピュータがターゲットの場合にも役立ちます。

注: Solaris システムに展開する場合は、SunSSH v1.1 (またはそれ以降) または OpenSSH の最新バージョンを使用することをお勧めします。Solaris プラットフォームおよびバージョンに適用可能なパッチの詳細については、Web サイト、<http://opensolaris.org/os/community/security/projects/SSH> をご覧ください。

ターゲット コンピュータでファイアウォールが稼働している場合は、SSH ポート(22)で展開マネージャからの接続が許可されることを確認してください。また、ターゲット コンピュータ上の SSH サーバが、3DES 暗号を含む RSA キーによる暗号化、および HMAC-SHA1 メッセージ認証コード (MAC) を使用するように設定されていることを確認する必要があります。ほとんどの SSH サーバは、デフォルトでこの設定をサポートしますが、そうでない場合は、SSH サーバのドキュメントで詳細を調べてください。

UNIX または Linux エージェントに正常に展開するために、最近の SSH 実装の /etc/ssh/sshd_config 設定ファイルを以下のように設定する必要があります。

- PasswordAuthentication を Yes に設定
- PermitRootLogin を Yes に設定 (または「[非特権ユーザ アカウントを使用した UNIX/Linux へのリモート展開](#) (P. 227)」セクションの説明に従って sudo/pfexec を設定)
- SFTP サブシステムが有効であることを確認

リモート展開では、noexec フラグでマウントされた /tmp ファイル システムを含むシステムへのソフトウェア展開がサポートされます。

IPv4 および IPv6 スタックの両方を実行している IBM AIX システムへ、IPv6 アドレスを使用して展開する場合は、ターゲット コンピュータの SSH サーバが IPv4 向けのポート 22 のみをリスンしている可能性があります。これにより、展開が失敗します。これを修正するには、sshd_config 設定ファイルを編集し、ListenAddress を「::」に設定します。

注: 展開マネージャとターゲット コンピュータの間で FIPS 準拠の SSH 通信を行うには、展開マネージャでの FIPS 専用モードの設定とは別に、ターゲット上で稼働している SSH サーバも FIPS 準拠の暗号化モジュールを使用していることを確認する必要があります。

重要: 現在使用されているオペレーティングシステムでは、ソフトウェアのリモートインストールが推奨されていません。また、明確に禁止されている場合もあります。これらのシステムにソフトウェアを展開しようとする、通常、ステータスが「プライマートランスポートがありません」になり、展開は失敗します。このような場合は、DVD などの物理的な配布メディアを使用せずにインストールを行うなど、他の手段を使用してソフトウェア コンポーネントをインストールしてください。

あるいは、IDPrimer ソフトウェアを備えたマシンを事前インストールまたはプロビジョニングすることができます。こうすると、基本オペレーティングシステムが提供している機能を必要とせずに、展開を実行できます。認証が行われていない場合は、認可された展開を実行する前に、有効な認証情報を入力する必要があります。

ご使用の環境で自動展開が可能かどうかを判別するには、以下のような標準オペレーティングシステム操作を実行して確認します。

- Windows 共有を使用した IDPrimer イメージの配信の場合は、展開要求で提供されるターゲット ユーザ クレデンシャルを使用して、共有 (デフォルト: ADMIN\$) を展開マネージャ ホスト コンピュータから各展開ターゲット コンピュータにマップできる必要があります。
- SSH を使用した IDPrimer イメージの配信の場合、SSH を使用して、展開マネージャから展開ターゲット コンピュータへ接続できる必要があります。

IPv6 アドレスを使用したインフラストラクチャ展開に関する注意事項

IPv6 環境で CA Virtual Assurance 展開サービスを使用する場合は、以下の前提条件を認識している必要があります。

1. マネージャ マシン (および各展開 (配布) サーバ) で、以下のレジストリ キーを 1 に設定する必要があります。
 - HKLM¥System¥CurrentControlSet¥Services¥smb¥Parameters¥IPv6EnableOutboundGlobal (REG_DWORD)
2. Windows 2003 マネージャ マシンには、以下に示す 3 つのホット フィックス 更新を適用する必要があります。
 - <http://support.microsoft.com/kb/947369/en-us>
 - <http://support.microsoft.com/kb/950092/en-us>
 - <http://support.microsoft.com/kb/974927/en-us>

3. ターゲット マシンのホスト名は、グローバル IPv6 アドレスに解決される必要があります。また、IPv6 アドレスの逆引きルックアップは、同じホスト名に解決される必要があります。
4. 各マネージャ マシンで、インフラストラクチャ展開設定ポリシー オプション `usehostnames` の値が `1` であることが必要です。このファイルは、デフォルトでは、以下のディレクトリにあります。

`C:\Program Files\CA\SC\IDMgrApi\config\SM\idconfig.xml`

IDManager が使用する転送パッケージのプロトコル

IDManager は、配布サーバを使用した展開時に、以下のプロトコルを使用してパッケージをターゲット コンピュータに転送します。

Windows ネットワーク共有

配布サーバとターゲット コンピュータが Windows 上にある場合は、このメカニズムを使用します。

SSH/SFTP

配布サーバかターゲット マシンのいずれかが Linux または UNIX 上にある場合は、このメカニズムを使用します。

これらの転送メカニズムの詳細については、「CA Virtual Assurance インフラストラクチャを自動展開するための前提条件」を参照してください。

インフラストラクチャ展開プライマ ソフトウェアの手動インストール

何らかの理由でターゲット コンピュータへの自動展開が不可能な場合でも、プライマ ソフトウェアを手動でターゲット コンピュータにインストールしてソフトウェアを展開できます。この展開は、物理的にプライマ パッケージをインストールするか、またはログイン スクリプトを使用してインストールを実行するかのいずれかによって可能です。

プライマ ソフトウェア自体のインストールだけでなく、セキュリティ キーもインストールする必要があります。このキーは、ターゲット コンピュータへの展開に使用する展開マネージャによって生成されます。

Windows での展開プライマ インストール

Windows を実行しているターゲット コンピュータでの展開プライマのインストールには、以下のアクションが必要です。

- CA Virtual Assurance インストール メディア (DVD) をターゲット コンピュータで利用できるようにするか、プライマ設定ファイルをターゲット コンピュータに手動でコピーします。プライマ設定ファイルは、インストール メディアの以下のディレクトリに格納されています。

```
%PROGRAMFILES%\SC\IDMgrApi\packages\private\idprimer\Windows_x86
```

- ターゲット コンピュータ上で IDPrimer_Setup.exe を実行して、プライマをインストールします。

Linux または UNIX での展開プライマ インストール

Linux または UNIX ターゲット コンピュータでの展開プライマのインストールには、以下のアクションが必要です。

- CA Virtual Assurance インストール メディア (DVD) をターゲット コンピュータで利用できるようにするか、プライマ インストール イメージをターゲット コンピュータに手動でコピーします。プライマ インストール イメージは、インストール メディアの以下のディレクトリに格納されています。

```
%PROGRAMFILES%\SC\IDMgrApi\packages\private\idprimer\Linux_x86
```

- ターゲット コンピュータ上のプライマ インストール イメージが含まれるディレクトリに移動して、以下のインストール コマンドを実行し、プライマをインストールします。

```
# sh installldp
```

展開管理証明書のプライマ インストールへの提供

展開マネージャは、ターゲット コンピュータ上のプライマが展開パッケージを受け取る前にターゲット コンピュータに転送する必要がある証明書を生成します。展開証明書ファイルの名前は **dmkeydat.cer** です。

証明書ファイルの場所は、インストール時に設定されます。証明書ファイルをより安全なエリア、またはフェールオーバーソリューションを提供する 2 つのマネージャが共有する場所へ格納する場合は、別のファイルの保存場所を設定します。後者の場合、証明書を共有すると、展開マネージャがいずれかのマネージャから配信された **IDPrimer** コンポーネントと通信できるようになり、認証クレデンシャルを再度提供する必要もありません。

Windows 上の展開管理証明書

Windows では、展開証明書は以下のディレクトリにあります。

C:\Program Files\CA\SC\IDMgrApi\config\SM

証明書ファイル (**MANAGER1 SM.PMR** のように **.PMR** というサフィックスの) は、ターゲット コンピュータのプライマ インストールフォルダにコピーする必要があります。これは、デフォルトでは以下のフォルダです。

\Program Files\CA\SC\IDPrimer

Linux または UNIX 上の展開管理証明書

Linux と UNIX では、ターゲット コンピュータのプライマ インストールフォルダに展開証明書をコピーする必要があります。これは、デフォルトでは以下のフォルダです。

/opt/CA/SharedComponents/ID/primer/bin

Linux の Compatibility Library

IDPrimer インストーラは、特定の依存ライブラリが存在することを前提としています。これらのライブラリが存在しない場合、インストール済みのコンポーネントが正常に機能しないことがあります。

以下の表では、ソフトウェアライブラリの前提条件の詳細を示します。IDPrimer をインストールするには、これらのライブラリが Linux ホスト上に存在する必要があります。

Linux ディストリビューション/バージョン	必要な RPM パッケージ
Red Hat 5.0 Enterprise Linux	glibc 2.3.3-84 compat-libstdc++ 33-3.2.3-61 64 ビットバージョンの OS 用: ncurses 5.4-1.3 (i386) または ncurses-devel 5.4-13 (i386) zlib 1.1.4-8.1 (i386) または zlib-devel 1.2.1.2-1.2 (i386) libstdc++.so.6
Red Hat 4.0 Enterprise Linux (AS/ES/WS)	glibc 2.3.3-84 compat-libstdc++ 296-2.96-132.7.2 compat-libstdc++ 33-3.2.3-47.3 64 ビットバージョンの OS 用: ncurses 5.4-1.3 (i386) または ncurses-devel 5.4-13 (i386) zlib 1.1.4-8.1 (i386) または zlib-devel 1.2.1.2-1.2 (i386) libstdc++.so.6
SuSE Linux Enterprise Server 10	glibc 2.3.3-84 compat 2004.4.2-3 libstdc++ 3.2.2-38 libstdc++.so.6
SuSE Linux Enterprise Server 9 (SP3)	glibc 2.3.3-84 compat 2003.5.12-56 libstdc++ 3.2.2-38 libstdc++.so.6

SuSE Linux Enterprise Server 9 (x64)	glibc 2.3.3-84 compat 2003.5.12-56 libstdc++ 3.2.2-38 libstdc++.so.6
SuSE Linux 10.1	glibc 2.3.3-84 compat 2004.4.2-3 libstdc++ 3.2.2-38 libstdc++.so.6
SuSE Linux Professional 10	glibc 2.3.3-84 compat 2004.4.2-3 libstdc++ 3.2.2-38 libstdc++.so.6
SuSE Linux Professional 9.3	glibc 2.3.3-84 compat 2003.5.12-56 libstdc++ 3.2.2-38 libstdc++.so.6
SuSE Linux Professional 9.2	glibc 2.3.3-84 compat 2003.5.12-56 libstdc++ 3.2.2-38 libstdc++.so.6
SuSE Linux Professional 9.1	glibc 2.3.3-84 compat 2003.5.12-56 libstdc++ 3.2.2-38 libstdc++.so.6
SuSE Linux Desktop 9	glibc 2.3.3-84 compat 2003.5.12-56 libstdc++ 3.2.2-38 libstdc++.so.6

注: 必須の **Compatibility Library** および追加のシステム パッケージの詳細については、Linux サブライヤのサポート **Web** サイトを参照してください。

ファイアウォールソフトウェアを実行している Windows Vista™、Windows 2008、および Windows XP コンピュータへの展開

ファイアウォールソフトウェアを実行しているコンピュータにエージェントを展開できるようにするには、以下を考慮します。

- Windows Vista™ または Windows 2008 オペレーティング システムが稼働するターゲットコンピュータのファイアウォールがオフ(無効)になっており、そのコンピュータへの展開に失敗する場合は、値が 0x1 の DWORD タイプとして、以下のレジストリ変数を作成または設定する必要があります。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy
```

これが必要である理由は、Windows Vista™ または Windows 2008 におけるユーザアカウント管理(UAC)では、管理権限がローカル ユーザに自動的に付与されないためです。これは、ローカル ユーザが管理者グループのメンバーであっても必要です。

注: この値を設定すると、結果的に UAC アクセストークンのフィルタリングが無効化されます。

Windows Vista™ または Windows 2008 が稼働しているコンピュータに対してローカル管理者アカウントを持っている場合は、この値を設定する意味があります。ドメイン管理者は、これを変更しても影響を受けません。

- Windows Vista™ または Windows 2008 が稼働しているターゲットコンピュータのファイアウォールがオン(有効)になっている場合は、そのコンピュータへの展開を有効にするために、ファイル共有ポートだけでなく、以下のポートも開いている必要があります。

UDP ポート

CAM: 4104

ファイルとプリンタの共有など: 137、138

TCP ポート

IDManager: 135

ファイルとプリンタの共有など: 139、445

- それでも展開が失敗する場合は、Windows Vista™ または Windows 2008 のファイアウォールの以下の「送信の規則」を完全に有効にする必要があります。
 - リモート アシスタンス
 - ネットワーク ディスカバリ
 - ファイルとプリンタの共有
 - コア ネットワーク
- ファイアウォール ソフトウェアを実行する Windows XP コンピュータへのエージェント展開を有効にするには、以下の手順を手動で実行する必要があります。
 1. セキュリティ ポリシー[ネットワーク アクセス: ローカル アカウントの共有とセキュリティ モデル]を[Guest のみ - ローカル ユーザが Guest として認証する]から[クラシック - ローカル ユーザがローカル ユーザとして認証する]に変更します。

クラシック モデルでは、リソースへのアクセスを微調整でき、通常は指定されたリソースへの「読み取り専用」アクセスが可能な、ローカル アカウントを使用するネットワーク ログインがゲスト アカウントにマップされないようにすることができます。
 2. 以下のファイアウォール設定を行います。
 - ファイルおよびプリンタの共有を許可
 - UDP ポート 4104 のオープン
 - TCP ポート 135 のオープン

第 8 章: トラップの管理

このセクションには、以下のトピックが含まれています。

[SNMP Trap Receiver](#) (P. 263)

[SNMP トラップ レシーバ 設定ファイル](#) (P. 264)

[SystemEDGE トラップの転送](#) (P. 269)

SNMP Trap Receiver

SNMP Trap Receiver コンポーネントは、受信 SNMP トラップを受信する CA Virtual Assurance の統合ポイントです。SNMP Trap Receiver コンポーネントは、以下のトラップのタイプをキャッチするユーザ データグラム プロトコル (UDP) ポート (デフォルト 162) 上でリスンします。

- 受信 SNMP v1 トラップ
- 受信 SNMP v2c トラップ
- 受信 SNMP v3 トラップ
- v2c 通知トラップ
- v3 通知トラップ

SNMP Trap Receiver は、SNMP v1、v2c および v3 トラップを同じ方法で処理し、顕著な差異はありません。

トラップ ストーム ウィンドウで重複として表示されないトラップはすべて ActiveMQ に転送されます。そこでは、他のコンポーネントが特定のトラップ ID にリスンします。

SNMPv3 トラップについては、`Install_Path¥CA¥productname¥conf` ディレクトリにある `sysedgev3.cf` ファイルを使用して SNMPv3 トラップ ユーザ認証を設定できます。

注: `sysedgeV3.cf` での SNMPv3 の設定の詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

SNMPトラップ レシーバ設定ファイル

trapreceiver.conf 設定ファイルは、SNMPトラップ レシーバの設定がすべて含まれた、XML のようなファイルです。必要に応じてこれらの設定を変更できるように、このファイルが提供されます。設定を変更することによって、トラップのブロックを有効にしたり、トラップをフォーマットしたり、トラップを CA Virtual Assurance Event Manager に送信したり、トラップを CIM_SNMPTripIndications に変換することができます。これらのトラップは Product Management Modules (PMM) に送信できます。すべての設定において、Apache を再起動することなくファイルを動的に設定できます。ただし、SNMPPort については、Apache を再起動する必要があります。他のすべての変更はそれらを保存してから 30 秒後に有効になります。

Install_Path¥CA¥productname¥config ディレクトリ内に trapreceiver.conf ファイルを配置し、テキスト エディタで開きます。

設定パラメータには以下が含まれます。

SNMPPort

受信 SNMPトラップにトラップ レシーバが接続してリスンする UDP ポートを定義します。別のアプリケーションがこのパラメータによって指定されたポートに接続された場合、トラップ レシーバは開始されません。代わりに、メッセージをイベントマネージャにログし、30 秒ごとにそのポートへ再接続しようとしします。このパラメータが新しいポート番号で変更された場合、トラップ レシーバは新しいポートに接続しようとしします。

デフォルト: 162

注: トラップ レシーバが SNMP ポートに接続された後で SNMPPort の設定を変更する場合は、Apache を再起動して新しいポートを有効にします。

TrapStormTimer

トラップの処理が重複しないようにします。設定可能値は、同一のトラップが TrapStormTimer 値の設定よりも頻繁に受信されないようにします。この値が 0 に設定されている場合、トラップ ストームは無効になります。

デフォルト: 30

PreFilter

設定ファイル内の **Converter** コンポーネントまたは **Subscriber** コンポーネントによって評価される前にすべての受信 **SNMP** トラップをフィルタします。

デフォルト: すべてのトラップ

FilterType

PreFilter にのみ適用されます。オプションは、以下のとおりです。

positive

処理に渡すことができるトラップを特定します。

negative

ブロックされるトラップを特定します。

デフォルト: `<FilterType>negative</FilterType>` または `<FilterType>positive</FilterType>` が含まれていない場合は **positive**。

注: `[negative]` プレフィルタのすべてのフィールドに対してアスタリスク `*` を指定すると、すべてのプレフィルタが無効になり、トラップはブロックされます。

ConvertToDCAEvent (フィルタと形式を含む)

変換されたトラップに説明的な名前を指定します。他のトラップ名を指定する場合は重複できます。

例: <Converter Name="eHealthTrap25">

形式

%s が含まれる文字列を指定し、形式文字列の下にある **varbind** 値のリストによって定義される値を示します。

varbind

形式文字列で %s を置換するために使用される変数を指定します。

有効な値は以下のとおりです。

SourceIP

EnterpriseOID

GenericTrapID

SpecificTrapID

注: SpecificTrapID フィルタ エントリは、受信トラップからの汎用タイプが 6 (enterpriseSpecific) である場合にのみ評価されます。GenericTrapID が * で、受信トラップからの汎用タイプが 0 ~ 5 である場合、GenericTrapID と SpecificTrapID の両方が一致します。

Varbind1、Varbind2 - トラップ内の予期された **varbind** の数以下。形式以下の変数の数は、形式内の %s 値の数と一致する必要があります。

EventSource

(オプション)トラップの **SourceIP** を別の値(受信トラップの特定の **varbind** など)に置換します。ノードからではなく、マネージャから送信されるいくつかの受信トラップは、トラップから送信されています。

デフォルト: SourceIP

EventTarget

(オプション) localhost ノード名を受信トラップからの値(特定の **varbind** など)に置換します。

デフォルト: localhost

SubscribedIndicationHandlers (フィルタとトピックを含む)

サブスクライバに説明的な名前を指定します。他のトラップ名を指定する場合は重複できます。

例: <Subscriber Name="SUNZoneAim_PMM">

トピック

メッセージが CA Virtual Assurance に送信される、ActiveMQ トピック名を指定します。

フィルタ

これらの設定はフィルタとプレフィルタに適用されます。これにより、受信トラップが評価されて、各 Converter または Subscriber が受信トラップを使用するかどうかを決定できます。プレフィルタがトラップをブロックすると、他のフィルタはそれらを評価しません。

SourceIP

IP アドレスの範囲のサブセットである任意の正規表現の文字列変数を指定します。

例:

111.*.*.*

112.223.*.*

112.223.334.5

*

制限: IPv4 アドレスのみ。

EnterpriseOID

エンタープライズ OID の範囲のサブセットである任意の正規表現の文字列変数を指定します。正規表現に表示される任意のピリオド(.)の前に円記号(¥)を使用します。ピリオド(.)は正規表現構文では特殊文字です。

GenericTrapID

トラップ PDU (Protocol Data Unit) の [TrapType] フィールドを比較するために使用される、整数ベースの正規表現を指定します。有効な値は、*、1 桁の整数 0 ～ 6、または範囲 (0 ～ 1) または (0 ～ 6) です。

有効な SNMP TrapType 値には以下が含まれます。

coldStart(0)

warmStart(1)

linkDown(2)

linkup(3)

authenticationFailure(4)

egpNeighborloss(5)

enterpriseSpecific(6)

SpecificTrapID

トラップ PDU の [TrapType] フィールドを比較するために使用される、整数ベースの正規表現を指定します。

有効な値は、以下のいずれか 1 つになります。

*

1 桁の整数

範囲 (1200 ～ 2225) から (165201 ～ 165299)

コメント

同じ行または別の行にコメントを指定します。

<!--

コメントの開始を定義します。

-->

コメントの終了を定義します。

例:

<!-- ポートがすでに接続されている場合、動的に変更されません。Apache を再起動します。 -->

SystemEDGE トラップの転送

CA Virtual Assurance マネージャにトラップを転送するように設定されている場合、SNMPトラップレシーバは SystemEDGE から任意のトラップを受信できます。受信 SNMP トラップはフィルタを使用して評価され、その後、PMM に送信されるか、または CA Virtual Assurance イベントに変換することができます。

注: sysedge.cf と sysedgeV3.cf のファイルを使用して、SNMP トラップを転送する方法の詳細については、製品マニュアル選択ページの「**SystemEDGE ユーザガイド**」を参照してください。

第 9 章: 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。

[レポートの可用性](#) (P. 271)

[レポートの実行](#) (P. 271)

レポートの可用性

CA Virtual Assurance ユーザ インターフェース内の一部のレポートは、CA Virtual Assurance のスタンドアロン インストールでは提供されない機能を必要とするため、利用できない場合があります。以下のレポートを使用するには、CA Virtual Assurance を CA Server Automation と共にインストールする必要があります。

- パッケージ配信失敗/成功
- パッケージング ジョブ履歴
- すべての予約マネージャレポート

他のすべてのレポートは、CA Virtual Assurance のスタンドアロン インストールで正常に機能します。

レポートの実行

データ センター内のサーバおよびサービスに関して CA Virtual Assurance が収集するメトリックに基づいてレポートを実行できます。

次の手順に従ってください:

1. [レポート]をクリックします。
[レポート]ページが表示されます。[レポート]レベルでは、メニューは頻繁に要求された選択内容を提供します。
2. 興味のあるレポートのタイプ用のフォルダを展開します。
カテゴリで利用可能な特定のレポートが表示されます。
3. 実行するレポートを選択します。
右側のペインに進捗状況のインジケータが表示され、空白のペインがレポートの説明と共に表示されます。

4. ドロップダウンリストから開始時刻と終了時刻を選択し、その他のプロンプトの要求に応じて選択し、[レポートの作成]をクリックします。

進捗状況のインジケータが右側のペインに表示されます。また、チャート化されたデータが、このペインに表示されます。

第 10 章: リモート モニタリング

このセクションには、以下のトピックが含まれています。

[概要 \(P. 273\)](#)

[リモート モニタリングの利点 \(P. 273\)](#)

[機能と利点 \(P. 274\)](#)

[アーキテクチャ \(P. 277\)](#)

[ユース ケース シナリオ \(P. 279\)](#)

[設定の前提条件 \(P. 281\)](#)

[リモート モニタ システムの設定 \(P. 282\)](#)

[リモート モニタリングを使用したシステムの管理 \(P. 285\)](#)

概要

リモート モニタリング (RM) を使用すると、エージェントレス システムのヘルス状態をモニタできます。RM により、リモート システムにモニタリング エージェント (SystemEDGE など) をインストールしなくても、柔軟性の高いモニタリング システムを実現できます。

RM では、リモート システムのモニタリングに、RM AIM という中間マネージャを採用しています。RM AIM は、リモートの Windows システム上で WMI クエリを使用してメトリック情報を収集します。

リモート モニタリングの利点

リモート モニタリングには、エージェント ベースのテクノロジーではなく、エージェントレス テクノロジーが含まれているため、どちらの戦略に対しても利点があります。RM または展開したエージェントのどちらを使用するかを判断する際には、以下の情報を使用してください。

RM には以下の利点があります。

- セットアップ、設定、および展開にかかるコストを抑えられる。
- ソフトウェア アップグレードとメンテナンスが簡略化される。
- 展開に要する時間が短く、モニタ対象の環境への影響も少ない。
- 管理対象サーバのリソースの使用量が少ない。

展開したエージェントには以下の利点があります。

- モニタ対象サーバおよびアプリケーションについて、より詳細なデータとよりレベルの高い機能を利用できる。
- 動作に必要なネットワーク帯域幅が小さい。
- 拡張性が高く、数千のサーバにも拡張できる。
- ネットワーク接続が使用不可になっても (エージェントは自律的に動作できるため)、継続してサーバのヘルス状態をモニタし、データ収集を実行できる。
- 管理対象サーバに対するコマンドと制御の機能が強力になる。

機能と利点

リモート モニタリングを使用すると、エンド ユーザの観点からのモニタリングがシームレスに統合されます (すなわち、エージェントと **RM** のどちらであっても、モニタ対象システムの管理インターフェースの外観と操作性が同じになります)。

RM には、ヘルス状態と重要業績評価指標 (KPI) メトリックのモニタリングを通じてシステムを管理できる機能が含まれています。また、**RM** を通じて、システムステータスと使用率メトリックに関するレポートを取得できます。**RM** には、回復力、スケーラビリティ、統合、オートメーションなどの利点が含まれています。以降のセクションで、主要な機能と利点について説明します。

エージェントレスのモニタ対象システム

リモート モニタリングでは、エージェント ベース テクノロジとエージェントレス テクノロジを使用して管理されるシステムに対し、シームレスなヘルス モニタリングを実行できます。

RM マネージャ コンポーネント (**RM PMM**) によって、**RM** システムとそのヘルス状態を表す **CIM** システム オブジェクトが作成されます。

この情報は[ダッシュボード]および[リソース]パネルに示されます。

次の手順に従ってください:

1. [リソース]-[エクスプローラ]を開き、[リモート モニタリング]フォルダを展開します。
検出されたシステムが、コンポーネント ツリー内に表示されます。
2. システムを選択します。
システムのページが右ペイン内に表示されます。
3. [リモート モニタリング]タブを開きます。
エージェントレスの収集済みデータが表示されます。

重要業績評価指標メトリック

リモート モニタリングでは、モニタ対象の RM システムで WMI クエリを実行することにより、Windows メトリック情報が収集されて提供されます。豊富な情報が、さまざまな Win32 CIM クラスで利用可能になり、RM AIM を通じて提供されます。

視覚化

RM UI では、以下の情報を設定できます。

- リモートでのモニタ対象のシステム
- それらのシステムで収集されるメトリック
- それらのメトリックをモニタするかどうか、およびモニタリングの方法(重大度としきい値を含む)

設定

リモート モニタリングは、モニタリングの対象としてリモートシステムが選択されると、モニタリングの設定を行わなくても、そのリモートシステムの KPI がすぐにモニタされます。標準設定のモニタリングしきい値は、ニーズに合わせて調節できます。

また、設定を定義して設定セットに格納し、設定セットを 1 つ以上の RM システムに割り当てることができます。

アクセス制御

ユーザが管理者または非管理者ユーザとして UI にログインすると、セキュリティメカニズムによって認証と許可の機能が提供されます。リモート モニタリングによって、ユーザが管理者であるか非管理者ユーザであるかに基づいて特定のアクション (RM システムの設定など) が許可または禁止されます。

RM AIM は、root¥CIMV2 ネームスペースへの WMI 接続を通じて (DCOM を使用して) RM システムにアクセスします。アクセスには、ローカルの RM システム管理者ユーザおよびパスワード認証情報が必要です。これらの認証情報 (RM システムがモニタされる際にユーザが提供する) は、パスワード暗号化を使用して、ファイルに格納されます。

回復力

RM AIM は、SystemEDGE とは別のプロセスです。RM AIM のエラーが原因で SystemEDGE がクラッシュすることはありません。RM AIM がクラッシュしたり、SystemEDGE のリクエストに応答なくなると、SystemEDGE 内の *RM AIM* アライブチェックによって RM AIM が再起動されます。

スケーラビリティ

1 つの SystemEDGE に対して 1 つの RM AIM があり、各 RM AIM はおよそ 200 の RM システムをモニタできます。1 人のマネージャに対して 1 つの RM PMM があり、各 RM PMM はおよそ 20 の RM AIM を管理できます。デフォルト設定セットには、10 のモニタ対象メトリックと、各メトリックにモニタが 2 つずつ含まれています。

SystemEDGE のスケーラビリティの観点から見れば、これは以下のとおりになります。

- $10 * 2 * 200 = 4000$ 個の monitorTable エントリ
- $10 * 200 = 2000$ 個の aggregateTable エントリ

統合

RM モニタ情報は、SNMP MIB に公開され、Spectrum、eHealth、および NSM のマネージャから容易にアクセスできます。

オートメーション

RM AIM にはコマンドライン ユーティリティ(rmonwatch)が含まれます。これにより、スクリプトを使用して、RM システムとその認証情報をリモートで設定できます。

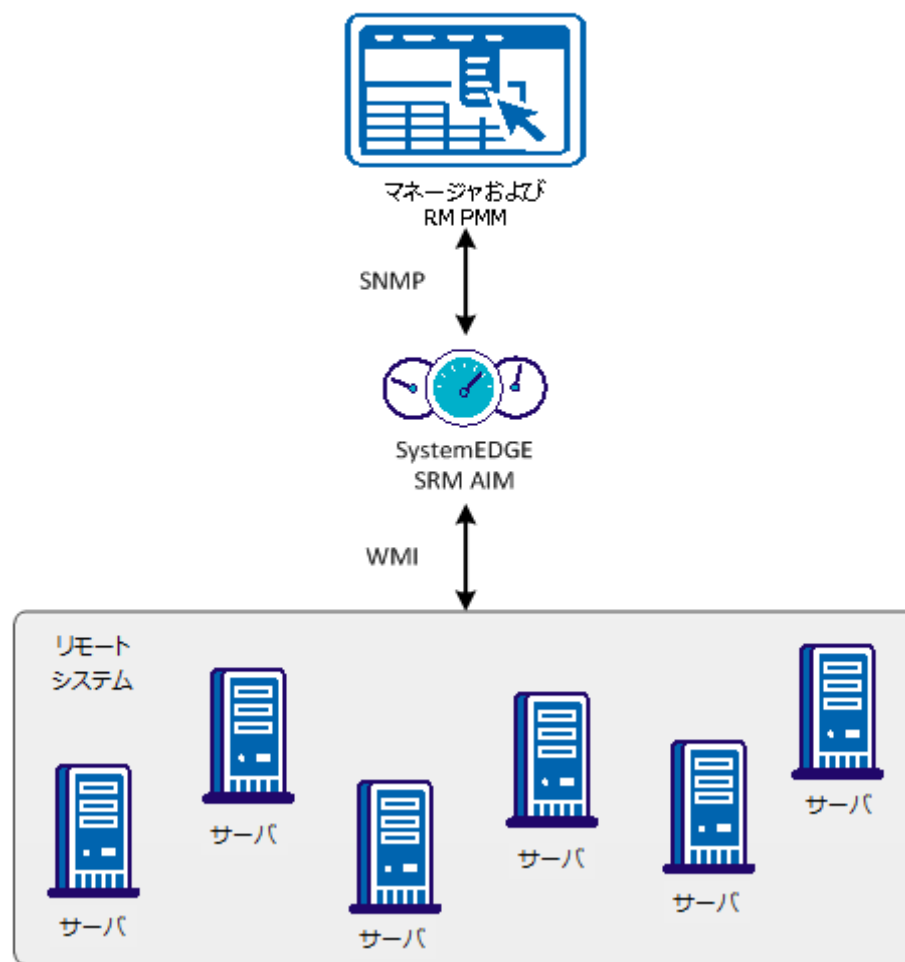
アーキテクチャ

以下の図は、メイン RM コンポーネントの概要を示しています。

1 つ以上の RM AIM が、DCOM/RPC 上で WMI を通じて Windows サーバのモニタリングを実行します。特定のサイトまたはサブネット内では、AIM からモニタ対象 Windows サーバに直接 TCP 接続する必要があります。AIM は展開コンポーネントを通じて展開されます。

プラットフォーム管理モジュール(RM PMM)は、マネージャ インフラストラクチャへのインターフェースを提供し、CIM オブジェクト モデルに管理対象オブジェクトを作成します。PMM は、SNMP を使用して、RM AIM と通信します。

リモート モニタリング コンポーネント間のインタラクション

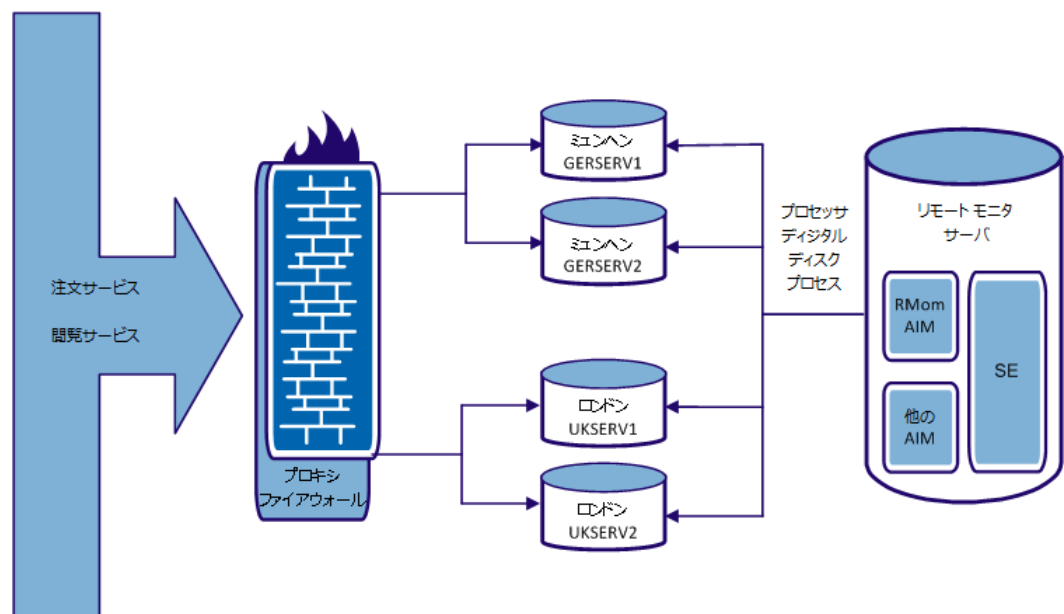


ユース ケース シナリオ

リモート モニタリングの以下のようなユース ケースについて考えてみます。ある企業が、書籍の注文サービスと書籍の閲覧サービスから構成される Web ブックストアを提供しています。

- 注文サービスは、ミュンヘンの 2 つのサーバとロンドンの 1 つのサーバから提供されています。
- 閲覧サービスは、ロンドンの 2 つのサーバとミュンヘンの 1 つのサーバから提供されています。

ミュンヘンのサーバは GERSERV1 および GERSERV2、ロンドンのサーバは UKSERV1 および UKSERV2 です。いずれも、負荷分散とフェールオーバーが設定されています。



サービスのモニタリングは、注文サービスと閲覧サービスとで異なります。この例では、2 つの設定セット(各サービス タイプに 1 つずつ)が定義されています。これらの設定セットには、以下の情報のクエリとモニタが含まれています。

- CPU

CPU アイドル時間合計の割合。

- FSys

それぞれのサービス タイプにとって重要な論理ディスクの空き領域(注文サービスの場合は C:、閲覧サービスの場合は D:)。

- Proc

注文プロセスの作業セットのサイズ(単一のプロセス `order.exe`)または閲覧プロセスのすべての作業セットのサイズ合計(プロセス `browse` のグループ)。

各モニタ対象システムに対して、サービスの役割(注文、閲覧、または両方)に応じて、以下の設定セットが割り当てられます。

システム名	設定セット
GERSERV1	注文
	閲覧
GERSERV2	注文
UKSERV1	注文
	閲覧
UKSERV2	閲覧

設定の前提条件

リモートエージェントを設定する前に、以下の前提条件が満たされていることを確認してください。

- RM システムのファイアウォールとポートの要件

RM AIM システムは、WMI 接続を通じて RM システムにアクセスします。WMI では、エンドポイント マッパー (EPMAP) によって動的に指定される EPMAP ポート TCP (135) と DCOM TCP ポートを使用する DCOM 通信が使用されます。

設定を単純にするために、RM AIM は RM システムと同じファイアウォール境界内に配置する必要があります。

注: 固定ポートの使用法の詳細については、Microsoft MSDN Web サイトの記事「[Setting Up a Fixed Port for WMI](#)」(英語のみ)を検索してください。

- マネージャシステムのファイアウォールとポートの要件

RM AIM では、SystemEDGE によって提供される SNMP インフラストラクチャを利用します。ここでは、追加のポートが必要ありません。

RM 設定は SNMP を使用して実行されます。設定データにはパスワードが含まれるため、RM ではパスワード暗号化を使用します。

- SystemEDGE ポートと SNMP

マネージャシステムは SNMP を通じて SystemEDGE システムにアクセスします。SNMP ポート(UDP 161 受信)が SystemEDGE システム上で開いている必要があります。SystemEDGE システムによって SNMP トラップ(UDP 162 送信)が送信されます。

- SystemEDGE ポートとポリシーベース設定

マネージャシステムは CAM を通じて SystemEDGE システムにアクセスします。UDP (4104)ポートまたは TCP (4105)ポートが SystemEDGE AIM システム上で開いている必要があります。SystemEDGE AIM システムでは、CAM を使用してマネージャシステムにメッセージを送信します。

■ WMI アクセスのベスト プラクティス

RM AIM は、WMI を使用して RM システムズに接続し、認証情報を要求します。ベストプラクティスとして、RM システムは AD ドメイン (RIVER など) のメンバにする必要があります。このメンバシップによって、各 RM システムにローカルのユーザ アカウントを定義しなくても、ドメイン アカウントを使用することができます。AD ドメインの Domain Admins グループのメンバである CARMuser ドメイン アカウントを作成します。

RM のインストール中にユーザ認証情報設定が要求されたときに、ドメイン アカウント (RIVER\CARMuser など) にパスワードを指定します。このドメインのシステム メンバには、追加の設定が不要です。

注: 必要に応じて、CARMuser アクセス権を制限し、ユーザが Domain Admins グループのメンバにならないようにすることができます。この場合、WMI 名前空間アクセスおよび DCOM アクセスを設定する必要があります。WMI 名前空間アクセスおよび DCOM アクセスの定義の詳細については、Microsoft の Web サイトを参照してください。

リモート モニタ システムの設定

設定セットは、RM システムに割り当てられたエンティティです。これにより、収集されるメトリック (WQL クエリ) とメトリックのモニタ方法が定義されます。

設定セットは複数の設定項目で構成されます。設定項目はメトリック定義 (WQL クエリ) とモニタリング定義 (しきい値、重大度など) で構成されます。

RM には、以下のような、すぐに使えるメトリック定義とモニタリング定義の設定セットが用意されています。

- default
- extended
- metricDisk
- metricFS
- metricNet

1 つの RM システムに対して複数のしきい値と重大度の設定を使用して複数のメトリックをモニタする必要がある場合は、標準設定セットのクローンを作成し、システム固有のモニタリングのニーズに合わせてクローンのセットを調整します。

以下の表は RM メトリックとそれらが属する設定セットの一覧です。

メトリック	設定セット
CPU_PercentIdle	default
Disk_PercentIdle	default
Event_SystemErrors	default
FSys_FreeMB	default
FSys_FreeMBDecrease	default
Mem_PercentUsed	default
Net_MACAddress	default
Net_MACIndex	default
Net_QueueLength	default
Proc_PercentCPU	default
Proc_PercentMemory	default
Srvc_StoppedAuto	default
Sys_LastBootTime	default
Sys_LastLocalTime	default
Sys_OSInfo	default
Sys_PhysMemKB	default
Disk_ReadPerSec	extended
Disk_WritePerSec	extended
Disk_QueueLength	extended
Mem_FreeMB	extended
Mem_FreePages	extended
Mem_NonPagedMB_3GB	extended
Mem_PagedMB	extended
Mem_PagedMB_3GB	extended

メトリック	設定セット
Mem_PagingPerSec	extended
Mem_NonPagedMB	extended
Net_PercentBusy	extended
Sys_Is64bit	extended
Sys_Has3GBSwitch	extended
Sys_OSType	extended
BIOS_Version	extended
BIOS_SerialNumber	extended
Disk_AvgDiskBytesPerRead	metricDisk
Disk_AvgDiskBytesPerWrite	metricDisk
Disk_AvgDiskReadQueueLength	metricDisk
Disk_AvgDiskWriteQueueLength	metricDisk
Disk_DiskWritesPersec	metricDisk
Disk_PercentDiskReadTime	metricDisk
Disk_PercentDiskWriteTime	metricDisk
Disk_SplitIOPerSec	metricDisk
Net_PacketsOutboundErrors	metricNet
Net_PacketsReceivedErrors	metricNet
Net_PacketsReceivedDiscarded	metricNet
Net_PacketsReceivedNonUnicastPersec	metricNet
Net_PacketsReceivedUnicastPersec	metricNet
Net_PacketsSentNonUnicastPersec	metricNet
Net_PacketsSentUnicastPersec	metricNet
FSys_PercentFreeSpace	metricFS

注: RM メトリックの詳細については、「リファレンス ガイド」を参照してください。

リモート モニタリング メトリックの収集エンジンとレポートのサポート

収集エンジンとレポートは、デフォルト設定セット内にある **RM** メトリックの固定セットをサポートします。

このため、レポートを使用するすべてのシステムには、デフォルト設定セット(または、それらのメトリックが含まれる設定セットか設定セットグループ)を割り当てる必要があります。

サポートされるデフォルト設定セットのメトリックは以下のとおりです。

- CPU_PercentIdle
- Disk_PercentIdle
- Event_SystemErrors
- Mem_PercentUsed
- FSys_FreeMB
- Fsys_FreeMBDecrease
- Net_QueueLength
- Proc_PercentCPU
- Proc_PercentMemory
- Srvc_StoppedAuto

リモート モニタリングを使用したシステムの管理

システムを管理するのに必要な **RM** 情報と設定にアクセスするには、[リソース] ペインで管理対象リソースを選択し、[リモート モニタリング]をクリックします。[リモート モニタリング] ページでは、以下のアクションを実行できます。

- モニタリング対象のリモートシステムの追加
- クエリの管理
- 認証情報設定の管理
- 設定セットの作成
- 設定エントリの管理

注: UI **RM** サブタブの使用の詳細については、「ユーザ ヘルプ」を参照してください。

ダッシュボードでは、以下の RM モジュールを使用できます。

- CA SystemEDGE マシン ステータス
- CA SystemEDGE オブジェクト ステータス

第 11 章: Exchange Server および Active Directory 用 AIM

このセクションには、以下のトピックが含まれています。

[概要](#) (P. 287)

[アーキテクチャ](#) (P. 288)

[機能](#) (P. 290)

[Exchange Server および Active Directory 用 AIM のメリット](#) (P. 291)

[パフォーマンス](#) (P. 291)

[ESAD AIM のインストール](#) (P. 291)

[Exchange Server と Active Directory をモニタするための設定の適用](#) (P. 293)

[コマンド モードの NodeCfgUtil による ESAD AIM の設定](#) (P. 294)

[ダイアログ モードの NodeCfgUtil による ESAD AIM の設定](#) (P. 296)

[ESAD AIM のアンインストール](#) (P. 297)

概要

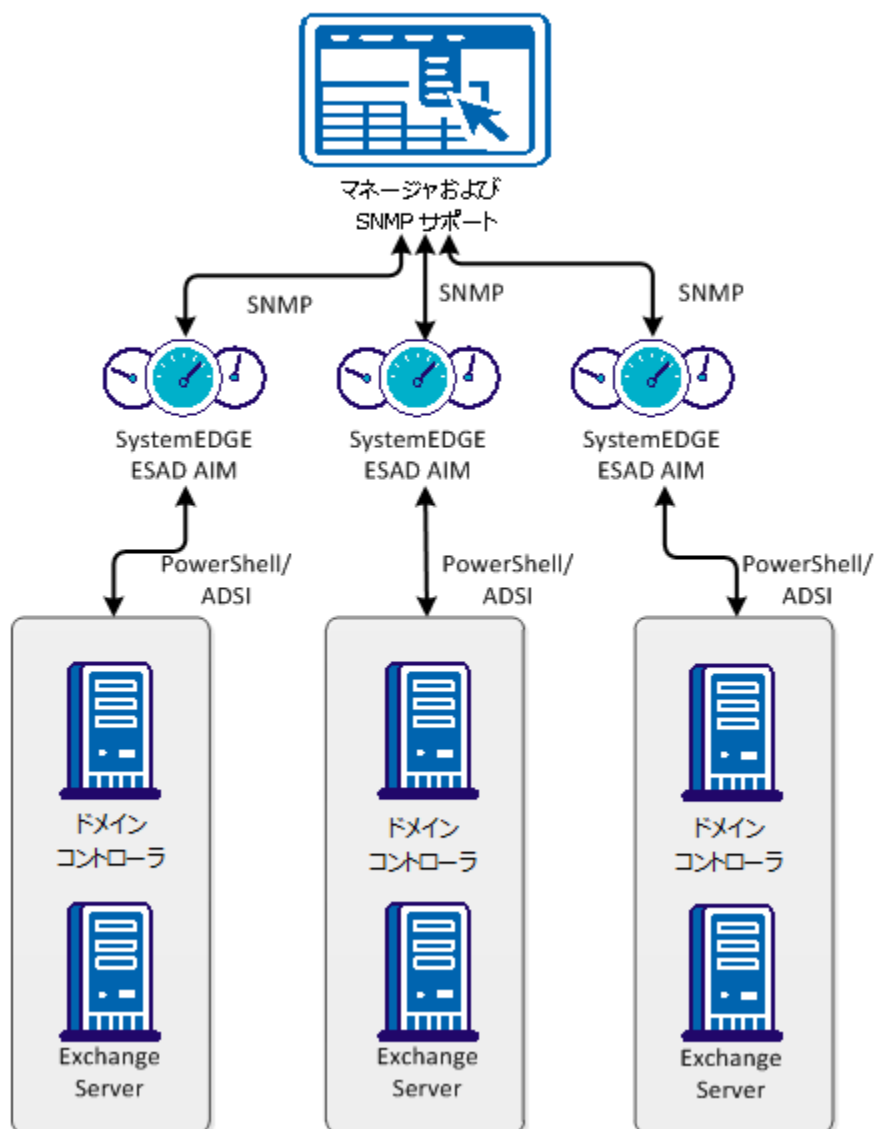
Exchange Server および Active Directory 用 AIM を使用すると、クラウドおよび社内運用の両方のインフラストラクチャにおける Exchange Server 環境と Active Directory 環境をモニタできます。この AIM は、Exchange Server 環境と Active Directory 環境の設定、およびキー パフォーマンス インジケータのモニタリングを可能にします。

アーキテクチャ

ESAD AIM は、その再使用可能な分散アーキテクチャによって、スケーラビリティとパフォーマンスの問題を解決します。

以下の図は、AIM の概要を示しています。

Active Directory および Exchange Server 管理コンポーネント間の
インタラクション



注: ESAD AIM は SystemEDGE との連携がサポートされています。CA Virtual Assurance for Infrastructure Managers では、NodeCfgUtil ユーティリティに基づいたリモート展開およびローカル設定がサポートされています。AIM をリモートでインストールするための詳細については、「CA Virtual Assurance 管理ガイド」の「リモート展開」セクションを参照してください。

機能

ESAD AIM には、ヘルス状態およびキー パフォーマンス インジケータ (KPI) のメトリックをモニタする機能が用意されています。ESAD AIM の主要な特長および機能を、以下に示します。

- メールボックス サーバのメッセージレコード マネージャ、論理ディスクの使用率、論理ディスクの読み取り/書き込み、およびメモリと CPU の使用率をモニタします。
- ハブトランスポート サーバのネットワーク遅延、キュー、およびメール配信のメトリックをモニタします。
- Active Directory のパフォーマンスおよびレプリケーションをモニタします。
- CA Virtual Assurance を通じてリモート展開をサポートします。

Exchange Server および Active Directory 用 AIM には以下のコンポーネントがあります。

ドメイン データ コレクタ

モニタ対象として特定されたドメインから設定データを収集します。

Exchange Server データ コレクタ

モニタ対象として特定された Exchange Server から設定データを収集します。

イベント コレクタ

Active Directory および Exchange Server のホストからイベント データを収集します。

ドメイン パフォーマンス データ コレクタ

モニタ対象として特定された Exchange Server からパフォーマンス データを収集します。

Exchange パフォーマンス データ コレクタ

モニタ対象として特定されたドメインからパフォーマンス データを収集します。

Exchange Server および Active Directory 用 AIM のメリット

Exchange Server および Active Directory 用 AIM を使用すると、クラウドおよび社内運用の両方のインフラストラクチャにおける Exchange Server 環境と Active Directory 環境をモニタできます。

ESAD AIM は、以下のメリットを提供します。

- Exchange Server と Active Directory をモニタするための統合されたソリューションを提供する。
- 迅速でシームレスな展開を可能にし、モニタ対象環境への侵入が少ない。
- 管理対象サーバのリソースの使用量が少ない。
- モニタ対象サーバに関するより多くの詳細データを提供する。
- 動作に必要なネットワーク帯域幅が小さい。
- より高度なスケーラビリティを提供する。

パフォーマンス

Exchange Server および Active Directory AIM からの最適なパフォーマンスを得るには、以下を実行します。

- ESAD AIM は、モニタ対象のサーバに対して地理的に近い場所に展開します。これにより、地理的に分散された Active Directory および Exchange Server 環境でのネットワーク遅延などが原因でエンドツーエンドのメトリックポーリングのパフォーマンスが低下するのを防ぐことができます。
- 最適なパフォーマンスを得るためにサーバの数に比例したポーリング間隔を設定します。

ESAD AIM のインストール

ESAD AIM をインストールするには、リモート展開を使用します。パッケージラッパーには以下のパラメータを指定します。

User

管理者ユーザの名前を指定します。

Password

そのユーザのパスワードを指定します

Domainname

ESAD AIM でモニタするドメインの名前を指定します。

Management Entity

管理対象エンティティを指定します。

0

Active Directory をモニタリングの対象にします。

1

Exchange Server をモニタリングの対象にします。

2

Active Directory および Exchange Server の両方をモニタリングの対象にします。

Management Mode

管理のオプションを指定します。

0

ドメイン全体をモニタリングの対象にします。

1

ドメインの特定のホストをモニタリングに対象にします。

Exchange Server と Active Directory をモニタするための設定の適用

Microsoft Exchange Server および Active Directory のモニタリング用に以下の設定を適用します。

前提条件:

AIM がインストールされているのと同じホストに以下のアイテムがインストールされていることを確認します。

- SystemEDGE
- Advanced Encryption
- .Net 3.5 以降のバージョン
- Windows PowerShell 2.0
- ESAD AIM および Exchange Management Tools SP3

注: Exchange Management Tools SP3 は、Exchange Server 2007 のモニタリングに必要です。

Exchange Server 上の PowerShell の設定

管理者として、Exchange Server システム上で PowerShell 設定を適用し、リモート接続および Exchange Server のモニタリングを有効にします。

次の手順に従ってください:

1. [スタート]メニューから[プログラム]-[アクセサリ]を選択して Windows PowerShell を起動します。

PowerShell コマンド プロンプトが表示されます。

2. 以下のコマンドを入力します。

```
Enable-PSRemoting
```

WinRM クイック設定メッセージが表示されます。

3. Y を指定して Set-WSManQuickConfig コマンドを実行します。

WinRM セットアップにより、リモート管理が開始され、WS-Man リクエストを受信するための WinRM リスナが作成されます。セッション設定を登録するための確認が表示されます。

4. Y を指定してセッション設定の登録を確認します。

セッション設定の登録が開始されます。

5. 以下のコマンドを入力して信頼済みホスト(trustedhosts)を設定します。

```
set-item wsman:localhost¥client¥trustedhosts -value *
```

すべてのコンピュータを **trustedhosts** リストに追加し、接続を確立します。

6. 以下の PowerShell コマンドを入力し、WinRM サービスを再開します。

```
restart-Service winrm
```

新しい **TrustedHosts** 設定および **Exchange Server** モニタリングを有効にします。

コマンド モードの NodeCfgUtil による ESAD AIM の設定

NodeCfgUtil.exe を使用して、**Exchange Server** と **Active Directory** 用の **AIM** 設定を変更できます。このユーティリティをコマンド モードで使用する場合、**AIM** 設定への管理対象ノードの追加のみが実行できます。

このコマンドの形式は、以下のとおりです。

```
nodecfgutil esad -u user -p passwd -d domainname -e entity -o option
```

esad

Exchange Server および **Active Directory** 用 **AIM** を指定します。

-u user

管理者ユーザの名前を指定します。

-p password

そのユーザのパスワードを指定します

-d domainname

ESAD AIM でモニタするドメインの名前を指定します。

-e *entity*

管理対象エンティティを指定します。

0

Active Directory をモニタリングの対象にします。

1

Exchange Server をモニタリングの対象にします。

2

Active Directory および Exchange Server の両方をモニタリングの対象にします。

-o *option*

管理のオプションを指定します。

0

ドメイン全体をモニタリングの対象にします。

1

ドメインの特定のホストをモニタリングに対象にします。

コマンドモードの NodeCfgUtil で ESAD AIM を設定する方法

1. AIM が存在するシステムでコマンドプロンプトを開きます。

コマンドプロンプトが表示されます。

2. 以下のコマンドのいずれかを入力します。

```
nodecfgutil esad -u user -p passwd -d domainname -e {0|1|2} -o {0|1}
```

Exchange Server および Active Directory に対して認証を実行し、正しい認証情報を格納します。

このユーティリティは、ESAD の環境設定ファイル (esad.cfg) を Sysedge_Install_Path¥plugins¥AIPCommon ディレクトリに書き込みます。

ダイアログ モードの NodeCfgUtil による ESAD AIM の設定

NodeCfgUtil を使用して、Exchange Server と Active Directory 用の AIM 設定を変更できます。このユーティリティをダイアログ モードで使用すると、ESAD AIM が管理するノードを設定できます。

次の手順に従ってください:

1. AIM が存在するシステムで Windows エクスプローラを開き、
`SystemEDGE_InstallPath¥plugins¥AIPCommon` ディレクトリに移動して、
`NodeCfgUtil.exe` を起動します。NodeCfgUtil で、インストールされた ESAD AIM が検出され、その後に表示されるダイアログ ボックスには、それらの AIM のみのリストが含まれます。
2. **1** を入力して、新しい管理対象ノードを追加します。

NodeCfgUtil で検出できるのは、インストールされた AIM のみです。
3. 画面上の指示に従って、設定を完了します。各ノードには、認証用の有効なユーザ名とパスワードが必要です。
4. 設定が正常に完了したら、**0** を入力して前のメニューに戻るか、またはユーティリティを終了します。

NodeCfgUtil は、ESAD の環境設定ファイル (`esad.cfg`) を `SystemEDGE_InstallPath¥plugins¥AIPCommon` ディレクトリに書き込みます。また、NodeCfgUtil ユーティリティを使用して、既存のエントリの編集または削除を実行できます。対応するダイアログ ボックスには、目的に応じた名前が付けられています。

ESAD AIM はマルチインスタンス AIM です。したがって、この手順を繰り返し、この AIM で管理するエンティティをさらに追加できます。

注: サーバ エントリを削除すると、NodeCfgUtil は、このサーバに削除のマークを付けますが、それだけではユーザ インターフェースからもデータベースからもサーバは削除されません。ユーザ インターフェースとデータベースからサーバを削除するには、AIM が実行されている Windows サーバを再検出してください。新しいディスカバリ プロセスが削除マークを検出し、対応するサーバをユーザ インターフェースとデータベースから削除します。

例

以下の例は、ESAD AIM の設定に正常に追加された mydomain に関する[管理対象ノードのインストール]ダイアログを示します。管理エンティティは **Active Directory** に設定されます。管理モードはドメイン全体に設定されます。詳細については、NodeCfgUtil コマンド モードを参照してください。管理対象モードは、NodeCfgUtil コマンド モードのオプション パラメータに相当します。

**** 管理対象ノードの選択 ****

1. Microsoft Exchange Server および Active Directory

0. 前のメニューに戻る

選択項目を入力してください: 2

Microsoft Exchange Server および Active Directory ノードの以下の情報を入力します...

(いずれかの時点で前のメニューに戻るには、Ctrl + Q キーを入力します)

1. ドメイン名: mydomain

2. ユーザ名: administrator

3. パスワード: *****

4. 管理エンティティ: 0

5. 管理モード: 0

CAAC1016 認証しています。お待ちください...

CAAC1018 認証に成功しました。

キーをどれか押してください。

ESAD AIM のアンインストール

SystemEDGE エージェントおよび ESAD AIM は、Windows の[プログラムの追加と削除]ウィンドウまたはコマンドラインを使用してアンインストールできます。アンインストーラは ESAD AIM をシステムから削除します。ユーザは、データディレクトリからコンフィギュレーション データを削除するかどうかを指定できます。

SystemEDGE または ESAD AIM を Windows の[プログラムの追加と削除]ウィンドウでアンインストールする方法

1. [スタート]-[設定]-[コントロール パネル]-[プログラムの追加と削除]を選択します。

[プログラムの追加と削除]ウィンドウが表示され、以下のコンポーネントが一覧表示されます。

- CA_SystemEDGE_ESAD

2. アンインストールの順序に従って適切なコンポーネントを右クリックし、[アンインストール]を選択します。

SystemEDGE の場合は、設定ファイルを保持するかどうかを指定するためのダイアログ ボックスが表示されます。

3. [はい]または[いいえ]をクリックします。

アンインストール プロセスのチャートを示すダイアログ ボックスが表示されます。アンインストールが完了すると、ダイアログ ボックスが閉じます。

第 12 章：シナリオおよびベスト プラクティス

このセクションには、以下のトピックが含まれています。

[vCenter Server 管理コンポーネントを設定する方法 \(P. 300\)](#)

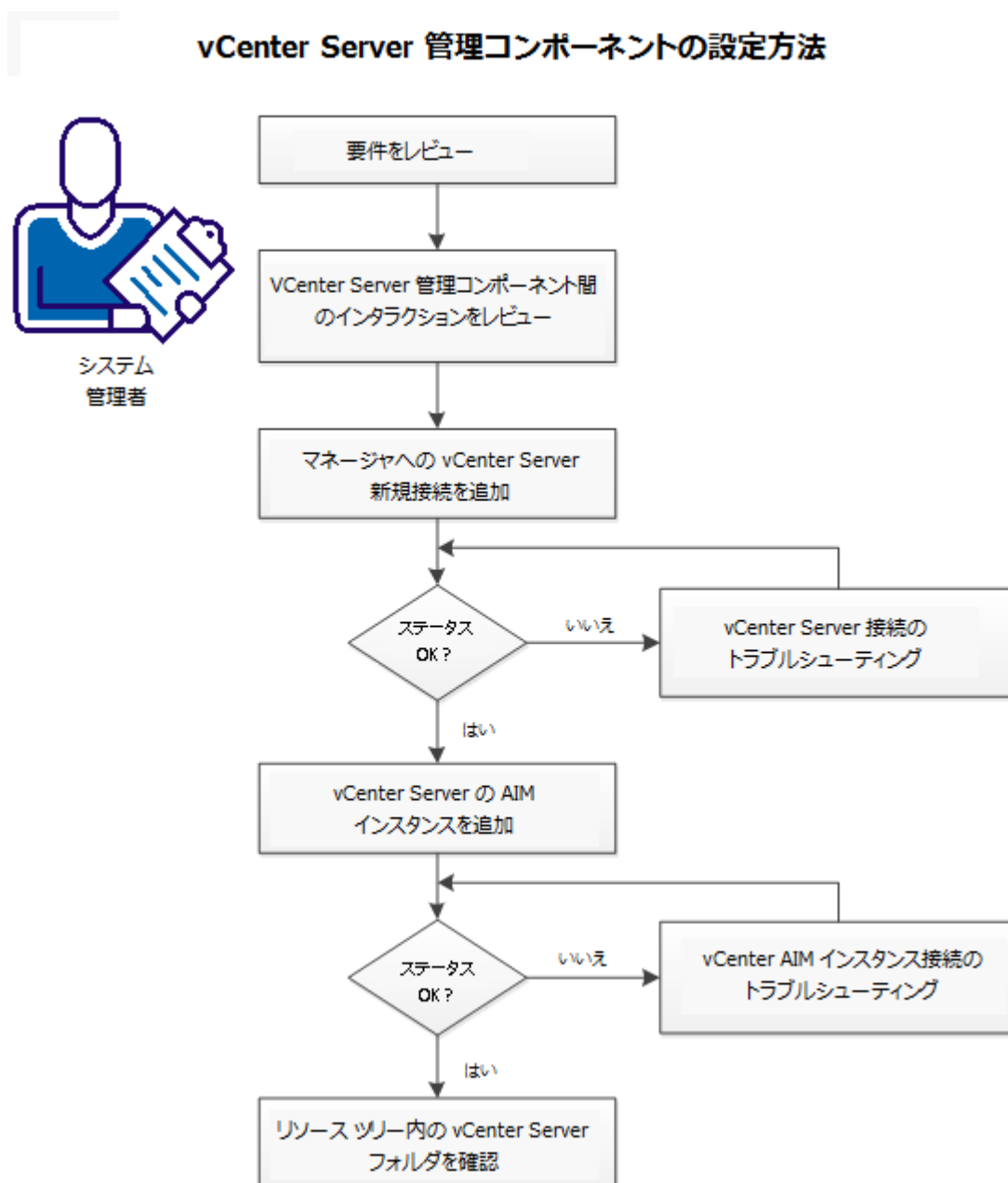
[ポリシー アクションを使ってパフォーマンスの問題を特定する方法 \(P. 317\)](#)

[スケーラビリティのベストプラクティス \(P. 321\)](#)

[ポリシーおよび階層型テンプレートをサーバに適用する方法 \(P. 337\)](#)

vCenter Server 管理コンポーネントを設定する方法

以下の図は、必要なアクションに関する概要を示しています。接続の問題が発生した場合のトラブルシューティング戦略も含まれます。



以下の手順に従います。

[確認要件](#) (P. 301)

[vCenter Server 管理コンポーネント間のインタラクションの確認](#) (P. 302)

[新しい vCenter Server 接続のマネージャへの追加](#) (P. 304)

[vCenter Server の AIM インスタンスの追加](#) (P. 309)

[リソース ツリーでの vCenter Server フォルダの表示の確認](#) (P. 316)

[vCenter Server 接続のトラブルシューティング](#) (P. 305)

[vCenter AIM インスタンス接続のトラブルシューティング](#) (P. 310)

確認要件

CA Virtual Assurance for Infrastructure Managers の vCenter Server 管理コンポーネントの設定を開始する前に、以下の要件を確認します。

- TCP/IP、SNMP、Web サービスおよび Windows Server オペレーティングシステムに精通している。
- CA Virtual Assurance、CASystemEDGE、および VMware vSphere に関する基礎知識を持っている。
- vCenter プラットフォーム管理モジュール (PMM)、vCenter Application Insight Module (AIM)、およびモニタリング エージェント (CA SystemEDGE) を含む CA Virtual Assurance マネージャ インストールにアクセスできる。
- CA Virtual Assurance ユーザ インターフェースにアクセスできる。
- 管理対象となる新しい vSphere 環境の vCenter Server にアクセスするための有効な認証情報を入手できる (ユーザ名とパスワード)。
- Web サービスを通して vSphere 環境の vCenter Server にアクセスするために使用するプロトコル (HTTP または HTTPS) およびポートを決定済みである。
デフォルト: HTTPS、ポート 443
- 新しい vSphere 環境とその vCenter Server が正しく実行されることを確認済みである。
- vCenter PMM と vCenter AIM が別々のシステムにインストールされている場合、それらのシステムでの SNMP 設定に整合性があることを確認済みである。読み取り/書き込みコミュニティ文字列および SNMP ポート番号が同一である。
- 使用するすべてのリモート vCenter AIM サーバが CA Virtual Assurance マネージャによって検出されることを確認済みである。

vCenter Server 管理コンポーネント間のインタラクションの確認

システム管理者として、CA Virtual Assurance を使って新しい VMware vSphere 環境を管理するとします。CA Virtual Assurance を使用すると、1 つ以上の vSphere 環境の物理リソースと仮想リソースを動的に管理できます。

vSphere は、1 台の vCenter Server、物理 ESXi ホスト、および ESXi ホスト上で実行される仮想インフラストラクチャから構成されます。vCenter Server は、仮想インフラストラクチャ全体を含む vSphere 環境を制御するための中心点です。このインフラストラクチャの構成要素には、データセンター、クラスタ、リソースプール、vApps、VM、仮想デバイス、仮想スイッチなどがあります。vSphere を管理するため、CA Virtual Assurance は、その vCenter プラットフォーム管理モジュール (PMM)、vCenter Application Insight Module (AIM)、および VMware vCenter Server の間にネットワーク接続を必要とします。これらのネットワーク接続を確立するには、CA Virtual Assurance vCenter Server 管理コンポーネント (つまり vCenter PMM と vCenter AIM) を設定します。

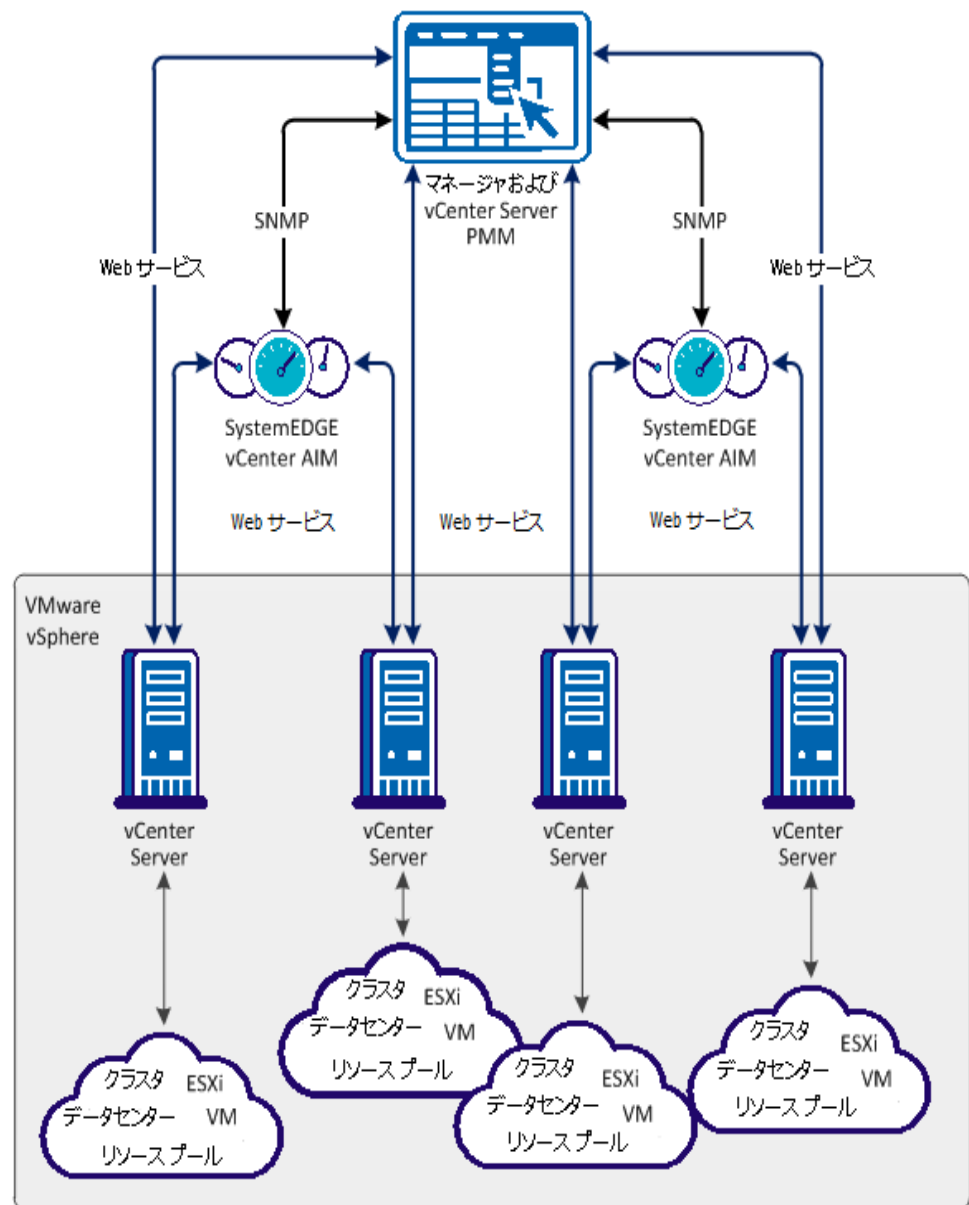
vCenter AIM は、SystemEDGE の機能範囲を拡張する SystemEDGE エージェントプラグインです。vCenter AIM によって SystemEDGE は、複数の vSphere 環境のパフォーマンスをモニタでき、モニタ対象 vSphere リソースの状態を評価できます。一般的なモニタ対象リソースは、仮想 CPU、仮想メモリ、仮想スイッチ、仮想ディスク、リソースプール、vApps などです。しきい値に基づき、SystemEDGE および vCenter AIM はモニタ対象リソースのステータスを判断し、その情報を SNMP を使用して CA Virtual Assurance マネージャにプロパゲートします。

vCenter PMM は CA Virtual Assurance マネージャのコンポーネントです。PMM には、Web サービスを使用するすべての VMware vCenter 操作のサポートと接続を提供する役割があります。PMM は、vCenter Server との接続を管理し、vSphere 関連の操作を実行します。また、vCenter AIM からデータを取得し、CA Virtual Assurance 管理データベースに入力します。典型的な操作には、VM の作成、開始、停止、クローン作成、CPU 共有の追加、削除、VM 実行時の VM へのメモリの追加などがあります。

vCenter PMM および AIM は相互に対話するので、CA Virtual Assurance は動的に複数の vSphere 環境を管理できます。CA Virtual Assurance は、AIM によって収集されたしきい値、ステータス、および値に基づいて、自動的に操作を実行できます。たとえば、CA Virtual Assurance は、VM の負荷に応じて CPU 共有を動的に追加または削除できます。

以下の図は、4 台の vCenter Server によって表される 4 つの vSphere 環境例において、影響を受けるコンポーネントのインタラクションを示しています。通常、vCenter PMM およびそのマルチインスタンス サポートを含む各 vCenter AIM は、複数の vCenter Server に接続できます。図中に示される接続では制限が指定されていません。必要なネットワーク接続は、TCP/IP、SNMP、および Web サービスに基づきます。

vCenter Server 管理コンポーネント間のインタラクション



CA Virtual Assurance コンポーネントを正常に設定すると、CA Virtual Assurance は新しい vSphere 環境を検出します。デイスカバリに成功すると、vSphere 環境の vCenter Server およびその仮想インフラストラクチャが、CA Virtual Assurance [エクスプローラ] ペインのリソース ツリーに表示されます。管理者は、新しい vSphere 環境を管理できます。

新しい vCenter Server 接続のマネージャへの追加

CA Virtual Assurance ユーザ インターフェースの[管理]タブを使用して、vCenter Server 接続を追加できます。

次の手順に従ってください:

1. [スタート]メニューから CA Virtual Assurance ユーザ インターフェースを開きます。[管理]、[設定]をクリックします。
[設定]ページが表示されます。
2. 左側のペインの[プロビジョニング]セクションから[vCenter Server]を選択します。
右側のペインがリフレッシュされ、管理対象の vCenter Server、関連付けられている vCenter AIM サーバ、および vCenter Server AIM インスタンスが表示されます。
3. [vCenter Server] ペイン ツールバーの  (追加) をクリックします。
[新しい vCenter Server] ダイアログ ボックスが表示されます。
4. 必要な接続データ(サーバ名、ユーザ、パスワード、プロトコル、ポート)を入力し、[管理ステータス] (チェック ボックス) をオンにして、[OK] をクリックします。

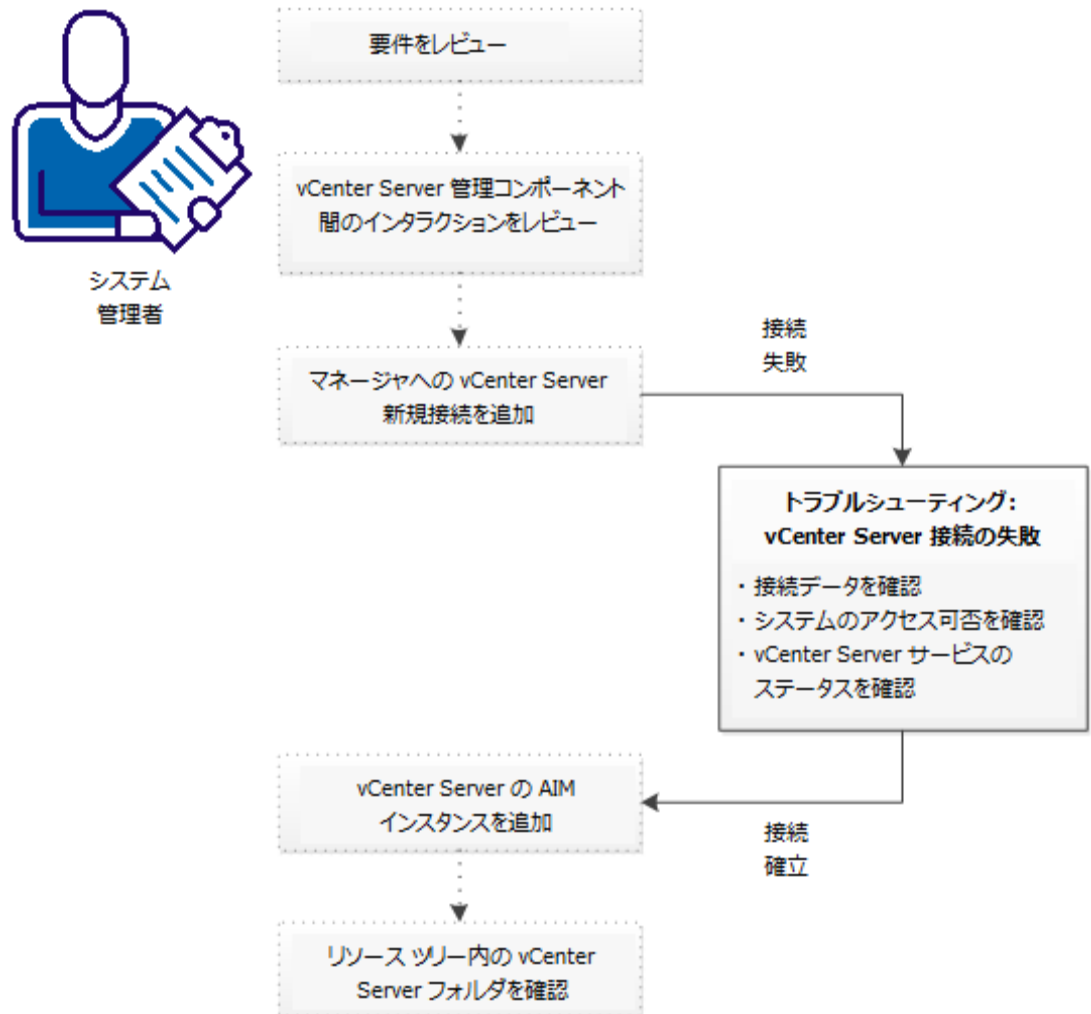
ネットワーク接続が正常に確立されている場合、右上の[vCenter Server] ペインに vCenter Server が緑のステータス アイコンを使って追加されます。CA Virtual Assurance によって vCenter Server が自動的に検出されます。

接続に失敗した場合、[検証が失敗しました] ダイアログ ボックスが表示されます。[はい] をクリックすると、CA Virtual Assurance によって vCenter Server が赤のステータス アイコンを使ってリストに追加されます。[いいえ] をクリックすると、何も追加されません。接続のトラブルシューティングについては、「[vCenter Server 接続のトラブルシューティング \(P. 305\)](#)」を参照してください。

vCenter Server 接続のトラブルシューティング

vCenter Server 接続に失敗しました。以下の図に示されたトラブルシューティング情報に従ってください。

vCenter Server 接続のトラブルシューティング方法



トラブルシューティング: vCenter Server 接続の失敗

症状:

[管理]-[設定]で新しい vCenter Server 接続を追加した後、vCenter Server への接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- vCenter Server の接続に使用されたデータ(サーバ名、ユーザ、パスワード、プロトコル、ポート)が今でも有効かどうかを確認します。必要な場合は、接続データを更新します。
- vCenter Server システムが実行されており、アクセス可能であるかどうかを確認します。
- vCenter Server システム上で VMware 管理サービスが正常に動作しているかどうかを確認します。

vCenter Server の接続データを更新する方法

1. 失敗した接続に関連付けられた  (追加)または  (編集)をクリックします。

[新しい vCenter Server]または[vCenter Server の編集]ダイアログ ボックスが表示されます。

2. 有効なサーバ名、ユーザ、パスワード、プロトコル、およびポートを追加します。[管理ステータス]を有効にして[OK]をクリックします。

接続データが更新されます。

3. 右上角の  (検証)をクリックして新しい設定を検証します。

vCenter Server への接続を確立できない場合は、次の手順に進みます。

vCenter Server システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Virtual Assurance マネージャシステムでコマンドプロンプトを開き、以下のコマンドを実行します。

```
nslookup <vCenter Server Name>  
ping <IP Address of vCenter Server>
```

2. vCenter Server に有効な DNS エントリおよび IP アドレスがあることをコマンドの出力で確認します。

vCenter Server が DNS 内にない場合は、CA Virtual Assurance マネージャシステムの Windows ホストファイルに vCenter Server を追加します。手順 3 に進みます。

vCenter Server が DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%\system32\drivers\etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

```
ipaddress <vCenter Server Name>
```

正しい IP アドレスと vCenter Server の名前を入力します。例:

```
192.168.50.50 myvCenter
```

4. 右上角の  (検証) をクリックします。

vCenter Server の認証情報と接続データが正しく、vCenter Server に対して ping を実行できる場合は、接続がまだ失敗する可能性があります。この場合は、vCenter Server に問題がある可能性があります。vCenter Server への接続を確立できない場合は、次の手順に進みます。

vCenter Server システム上で VMware 管理サービスが正常に動作しているかどうかを確認する方法

1. vCenter Server システムにアクセスする方法を vSphere の管理者に問い合わせます。
2. vCenter Server システムにログインし、[スタート]メニューから[管理ツール]-[サービス]を開きます。
[サービス]ウィンドウが表示されます。
3. *VMware VirtualCenter Server* サービスを選択します。サービスを開始または再開します。
4. CA Virtual Assurance ユーザ インターフェースに移動し、マネージャシステムの[vCenter Server]ペインの右上角にある  (検証)をクリックします。

CA Virtual Assurance によって vCenter Server の接続が検証されます。

vCenter Server への接続が失敗する場合は、このシナリオの要件に従って集めたデータがまだ有効であることを確認してください。

vSphere の管理者または VMware のサポート担当者と協力して、vCenter Server の接続の問題を解決します。

vCenter Server の AIM インスタンスの追加

CA Virtual Assurance マネージャに新しい vCenter Server 接続を追加した後、新しい vCenter Server を管理するための vCenter AIM インスタンスを追加します。その後、vCenter Server、ESX サーバ、VM など、そのすべての物理および仮想コンポーネントを含む vSphere 環境全体が CA Virtual Assurance によって検出されます。

次の手順に従ってください：

1. [スタート]メニューから CA Virtual Assurance ユーザ インターフェイスを開きます。[管理]、[設定]をクリックします。

[設定]ページが表示されます。

2. 左側のペインの[プロビジョニング]セクションから[vCenter Server]を選択します。

右側のペインがリフレッシュされ、管理対象の vCenter Server、関連付けられている vCenter AIM サーバ、および管理対象 vCenter Server の AIM インスタンスが表示されます。

3. [vCenter AIM サーバ]ペイン ツールバーの  (追加)をクリックします。

[新しい vCenter AIM サーバ] ダイアログ ボックスが表示されます。

4. [vCenter AIM サーバ] ドロップダウンリストを開きます。

検出された vCenter AIM サーバのリストが表示されます。vCenter AIM をローカル システムにインストールしている場合は、ローカル システムの名前もリストに表示されます。

5. ドロップダウンリストから vCenter AIM サーバを選択します。

[vCenter Server]ペインに一覧表示された vCenter Server が[vCenter Server]ドロップダウンリストに入力されます。つまり、管理できる vCenter Server は、CA Virtual Assurance マネージャで有効な接続が確立されているものに限られます。

6. 管理する vCenter Server を選択し、[OK]をクリックします。

選択した vCenter Server の新しい AIM インスタンスが追加されます。インスタンスがエラー状態または停止状態にない場合、CA Virtual Assurance は関連付けられている vSphere 環境の検出を開始します。ディスカバリプロセスが完了したら、vSphere の仮想および物理リソースの管理を開始できます。

vCenter AIM インスタンス接続のトラブルシューティング

vCenter AIM 接続が準備未完了のステータスにあります。以下のいずれかのステータスアイコンが表示されます。

 ディスカバリが進行中 - プラットフォーム マネージャによってすべてのデータが同期されるまで待機します。

 複数のインスタンス - このインスタンスは複数の AIM によって管理されています。重複するインスタンスを削除します。

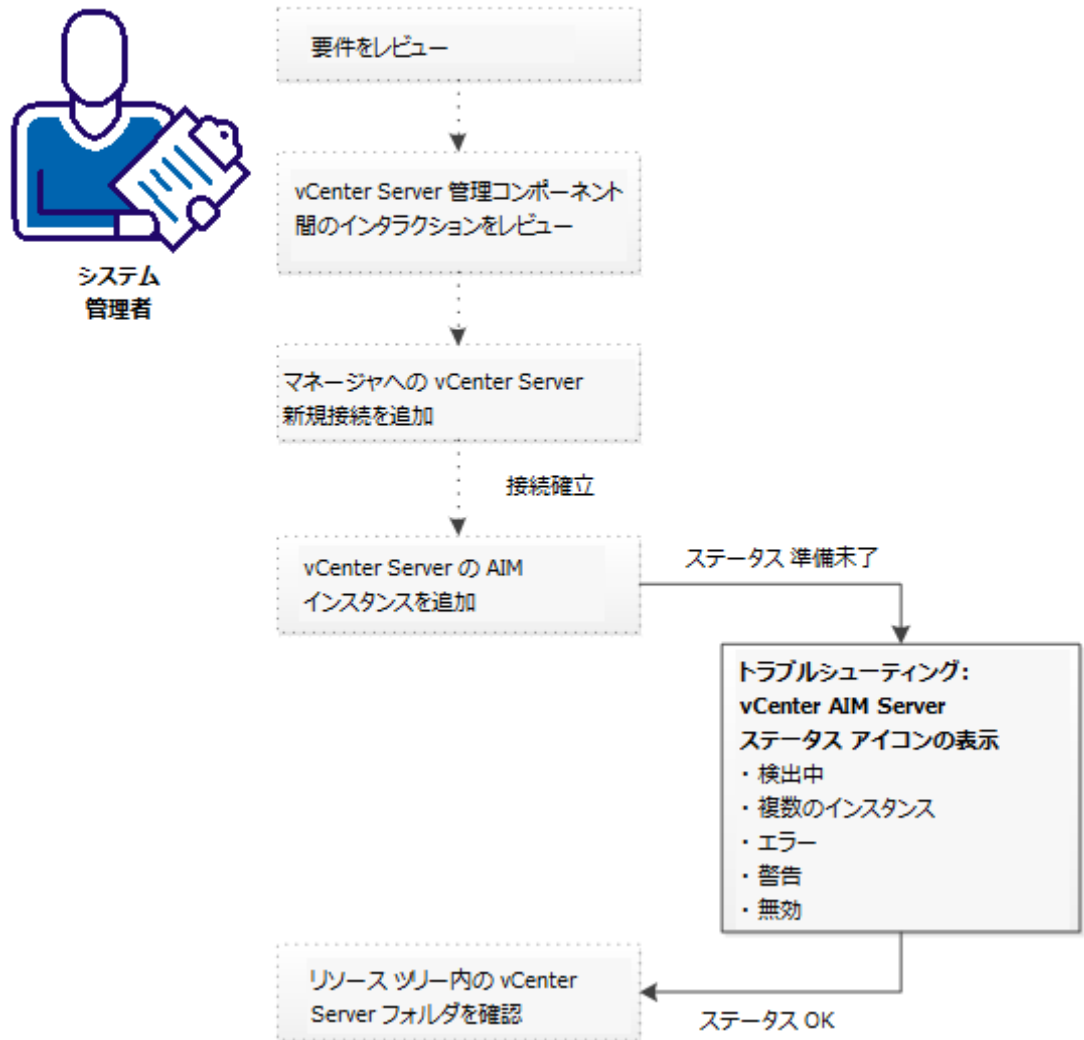
 エラー - AIM に接続できません。ネットワーク接続を確認してください。

 警告 - AIM 上の一部のインスタンスがまだエラー状態にあります。

 無効 - このインスタンスは管理されていません。

以下の図に示されたトラブルシューティング情報に従ってください。

vCenter AIM インスタンス接続のトラブルシューティング方法



トラブルシューティング: vCenter AIM インスタンス ステータス アイコンが「ディスクバリが進行中」を示している

症状:

[管理]-[設定]で vCenter Server に対して vCenter Server AIM インスタンスを追加した後、ステータス アイコンに  (ディスクバリが進行中)が表示されます。

解決方法:

vSphere 環境のディスクバリ プロセスが完了するまで待機します。ディスクバリ期間は、vSphere 内の仮想および物理リソースに関連する管理対象オブジェクトの量に依存します。アイコンの上にカーソルを置くと、未処理のディスクバリ要求の数を示すツールヒントが表示されます。ディスクバリ ジョブが完了すると、CA Virtual Assurance は vCenter Server フォルダをリソース ツリーに追加します。これで、vSphere とその仮想インフラストラクチャ全体の管理を開始できます。

トラブルシューティング: vCenter AIM インスタンス ステータス アイコンが複数のインスタンスを示している

症状:

[管理]-[設定]で vCenter Server に対して vCenter Server AIM インスタンスを追加した後、ステータス アイコンに  (複数の AIM がこのインスタンスを管理している)が表示されます。

解決方法:

CA Virtual Assurance マネージャが 1 つの vCenter AIM インスタンスのみを使用して各 vCenter Server を管理していることを確認します。CA Virtual Assurance マネージャが複数の AIM インスタンスを使用して vCenter Server を管理している場合は、管理上の問題が発生します。CA Virtual Assurance は関連付けられた vCenter Server のモニタリングを停止します。

どの AIM インスタンスを使用して vCenter Server を管理するかを決定し、[vCenter AIM サーバ] ペインから他のインスタンスを削除してください。

次の手順に従ってください:

1. 削除する AIM インスタンスを選択し、 (削除)をクリックします。
[項目の削除]ダイアログ ボックスが表示されます。
2. [はい]をクリックします。

マネージャと AIM インスタンスの間で一意的な関係が確立するまで、他の複数のインスタンスに対して上記の手順を繰り返します。

トラブルシューティング: vCenter AIM インスタンス ステータス アイコンがエラーを示している

症状:

[管理]-[設定]で vCenter Server に対して vCenter Server AIM インスタンスを追加した後、ステータス アイコンに  (エラー)が表示されます。AIM に接続できません。

解決方法:

vCenter AIM への接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- vCenter AIM サーバがアクセス可能であるかどうかを確認します。
- SystemEDGE が実行されているかどうかを確認します。必要な場合は、SystemEDGE を開始または再開します。

vCenter AIM サーバシステムがアクセス可能かどうかを確認する方法

1. CA Virtual Assurance マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

```
ping servername
```

2. vCenter AIM サーバに有効な DNS エントリおよび IP アドレスがあることをコマンドの出力で確認します。

vCenter AIM サーバが DNS 内にはない場合は、CA Virtual Assurance マネージャ システムの Windows ホスト ファイルに vCenter AIM サーバを追加します。手順 3 に進みます。

vCenter Server が DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%\system32\drivers\etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

```
ipaddress servername
```

正しい IP アドレスと vCenter AIM サーバの名前を入力します。例:

```
192.168.50.51 myvCenterAIM
```

4. [vCenter AIM サーバ] ペインの右上角の  (検証)をクリックします。

エラー ステータスが変わらない場合は、次の手順に進みます。

SystemEDGE が実行されているかどうかを確認する方法

1. vCenter AIM サーバにログインし、%windir%\Program Files\CA\SystemEdge\bin ディレクトリから sysedge.cpl を実行します。

SystemEDGE コントロール パネルが開き、SystemEDGE の実行状態が表示されます。
2. SystemEDGE を開始または再開します。

SystemEDGE が実行されていることが SystemEDGE コントロール パネルに表示されるまで待機します。
3. CA Virtual Assurance ユーザ インターフェースに移動し、マネージャ システムの[vCenter AIM サーバ]ペインの右上角にある  (検証) をクリックします。

CA Virtual Assurance によって vCenter AIM サーバの接続が検証されます。

エラー ステータスが変わらない場合は、このシナリオの要件に従って集めたデータがまだ有効であることを確認してください。

トラブルシューティング: vCenter AIM インスタンス ステータス アイコンが警告を示している

症状:

[管理]-[設定]で vCenter Server に対して vCenter Server AIM インスタンスを追加した後、ステータス アイコンに  (警告) が表示されます。AIM 上の他のインスタンスがまだエラー状態です。

解決方法:

関連付けられたインスタンスに、特定の必要なアクションはありません。同じ AIM 上の他のインスタンスがエラー ステータスであることを通知する警告が表示されます。他のインスタンスの問題が解決されると、警告が表示されなくなります。AIM の 1 つ以上のインスタンスがエラー状態であれば、AIM の他のすべてのインスタンスが警告状態として表示されます。

トラブルシューティング: vCenter AIM インスタンス ステータス アイコンが無効を示している

症状:

CA Virtual Assurance がネットワーク内の vCenter AIM インスタンスを検出した後、いくつかのインスタンスのステータス アイコン  (無効)が表示されます。この vCenter AIM インスタンスは管理されていません。

このステータスは、CA Virtual Assurance が以下の関係を持つ vCenter AIM を検出した場合に表示されます。

- CA Virtual Assurance マネージャへの接続が有効であるが管理対象外の状態である vCenter Server 用に vCenter AIM が設定されている。
- [vCenter Server] ペインで設定されていない vCenter Server に AIM が接続されている。

解決方法:

AIM インスタンスのステータスを「準備完了」に変更するには、以下のいずれかを実行します。

- 欠落している vCenter Server から CA Virtual Assurance マネージャへの接続を追加します。
- 既存の vCenter Server 接続を編集し、その管理ステータスを「有効」に変更します。

リソース ツリーでの vCenter Server フォルダの表示の確認

新しい vCenter Server は、設定およびディスカバリに成功すると、[リソース]-[エクスプローラ]ペインの[VMware vCenter Server]フォルダに示されます。

次の手順に従ってください:

1. [リソース]-[エクスプローラ]をクリックします。

リソース ツリーが表示されます。

2. [VMware vCenter Server]を展開します。

管理対象の vCenter Server が表示されます。

3. 新しい vCenter Server エントリを展開します。

管理対象の vSphere インフラストラクチャが表示されます (VMware データセンター、ESX サーバ、リソース プール、VM など)。

CA Virtual Assurance は、追加された vSphere 環境とその仮想インフラストラクチャを管理する準備が整いました。

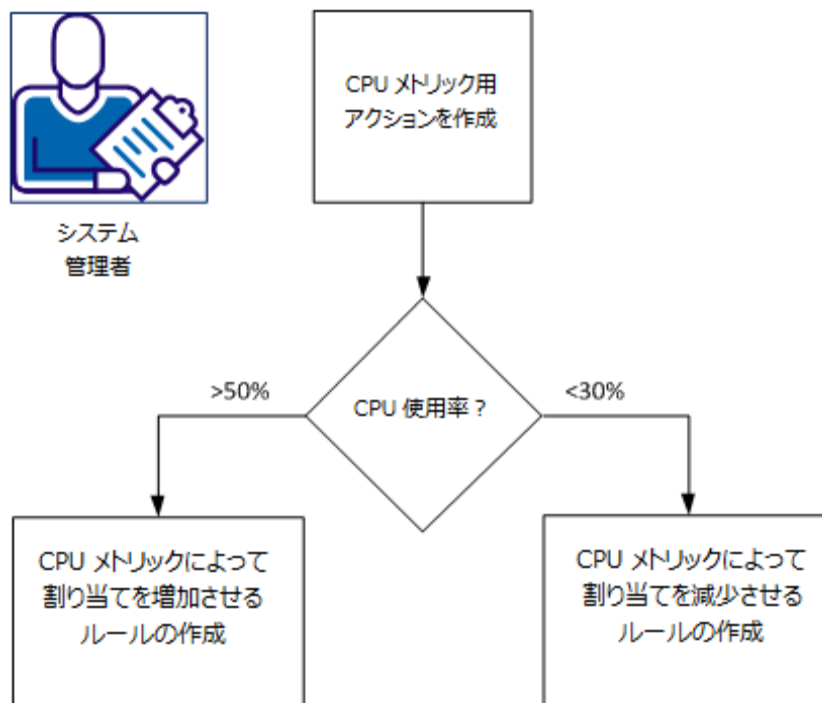
ポリシー アクションを使ってパフォーマンスの問題を特定する方法

このシナリオでは、システム管理者がパフォーマンスの問題を特定し、動的に対処する方法について説明します。この情報は、管理対象 vCenter 環境のリソース共有の割り当てを最適化するシステム管理者を対象にしています。

ポリシー アクションによって、VM リソースが特定され、CPU 割り当てが動的に調整されます。共有は、複数の VM 間でリソース競合が発生した場合に、どの VM がリソースを取得するかを決定します。共有を使用することによって、CPU リソースの動的な割り当てが可能になります。各 VM には、指定された数の共有が割り当てられます。VM に割り当てられるリソースの量は、利用可能な共有の総数に対するその共有の割合によって異なります。割り当ては、ESX サーバホスト上の CPU リソースの現在の使用率に基づいて、動的に変化します。

VM の CPU 使用率が 50 パーセントを超える場合、CPU 共有の割り当ては動的に増加されます。CPU 使用率が 30 パーセント未満の場合、CPU 共有の割り当ては動的に減少されます。ポリシー コンポーネントは、問題のある仮想マシンを特定するだけでなく、ビジネスの継続性を維持する動的アクションの実行を支援します。ポリシー アクションは、リソースを必要とする仮想マシンにリソースを割り当て、リソースの必要がなくなったときに割り当てを解除するのに役立ちます。

パフォーマンスの問題を特定するためのポリシー アクションの使用方法



ポリシー アクションを使ってパフォーマンスの問題を特定して対処するには、以下の手順に従います。

1. [CPU メトリックのアクションを作成します。](#) (P. 319)
2. CPU 使用率が 50 パーセントを超える場合は、[CPU メトリックによって割り当てを増加させるルールを作成](#) (P. 320)します。
3. CPU 使用率が 30 パーセント未満の場合は、[CPU メトリックによって割り当てを減少させるルールを作成](#) (P. 320)します。

CPU メトリックのアクションの作成

システム管理を自動化するためのポリシーの作成に使用できるルールおよびアクションの作成は、ポリシーによって提供されます。デフォルト ライブラリに含まれないアクションに対してはカスタム アクションを作成できます。

次の手順に従ってください:

1. [リソース]をクリックします。
[リソース]ページが表示されます。
2. [エクスプローラ]ペインを開きます。
利用可能なグループ、サービス、およびシステムが表示されます。
3. [ポリシー]をクリックし、次に、[アクション]をクリックします。
[アクション]ページが表示されます。
4. 新しいアクションを追加するには、右上のバーの[+]をクリックします。
5. アクションの名前を入力します。
6. [カテゴリ]ドロップダウンリストから[リソース設定]を選択します。
7. [タイプ]ドロップダウンリストから[共有の設定]を選択します。
8. 任意の VC サーバ上の任意の VM にこのアクションを適用するには、[VC サーバ] フィールドでエントリを「%VCServer%」のままにします。
9. [VC データ センター] フィールドで、エントリを「%DATACENTER%」のままにします。
10. [ターゲット VM マシン]フィールドで、エントリを「%VMNAME%」のままにします。
11. [操作]ドロップダウンリストから[CPU の設定]を選択し、[値]に「10000」を入力します。
数は任意です。また、共有値は標準値に設定されます。
注: 使用する値を大きくまたは小さくすると、それに応じて共有の割り当ても増減します。
12. 変更の承認が必要な場合は、[ヘルプ デスク承認]を有効にします。
アクションが作成されると、イベント コンソールにメッセージが表示されます。
CAAP4521 ポリシー: アクション <アクション名> が作成されました。

CPU メトリックによって割り当てを増加させるルールの作成

CPU メトリックによって CPU 割り当てを増加させるルールを作成すると、使用率がしきい値を超えたときに動的なリソース割り当てを実行するのに役立ちます。

次の手順に従ってください:

1. [リソース]タブをクリックし、[ポリシー]-[ルール]をクリックします。
2. 新しいルールを追加するには、右上のバーの[+]をクリックします。
3. ルールの名前を入力し、[次へ]をクリックします。
4. ルールの[アクションの選択]リストからアクションを選択し、[次へ]をクリックします。
5. CPU 使用率が 50 パーセントを超えた場合に VM の CPU 共有を増加させる、メトリックベースのルールを入力します。

CPU メトリックによって割り当てを減少させるルールの作成

CPU メトリックによって割り当てを減少させるルールの作成

次の手順に従ってください:

1. [リソース]タブをクリックし、[ポリシー]-[ルール]をクリックします。
2. 新しいルールを追加するには、右上のバーの[+]をクリックします。
3. ルールの名前を入力します。
4. ルールの[アクションの選択]リストからアクションを選択します。
5. CPU 使用率が 30 パーセント未満の場合に VM の CPU 共有を減少させる、メトリックベースのルールを入力します。

スケーラビリティのベスト プラクティス

このセクションでは、CA Virtual Assurance の展開に関するベストプラクティスおよび推奨事項について説明します。このドキュメントの目的は、実稼働環境内に CA Virtual Assurance をロールアウトする場合に必要な作業、特に次の項目を計画する作業を支援することです。

- VMware 環境のモニタリングおよび CA Virtual Assurance 管理
- SystemEDGE およびほかのモニタリング ソフトウェアの展開
- SystemEDGE の初期および継続的な設定

以下のセクションが含まれています。

1. [リモート展開およびポリシー設定の概要](#) (P. 321)
2. [ハードウェアの仕様](#) (P. 323)
3. [データベースに関する考慮事項](#) (P. 323)
4. [ネットワークに関する考慮事項](#) (P. 324)
5. [スケーラビリティに関する推奨事項および制限事項](#) (P. 324)
6. [シナリオに関する使用事例](#) (P. 331)

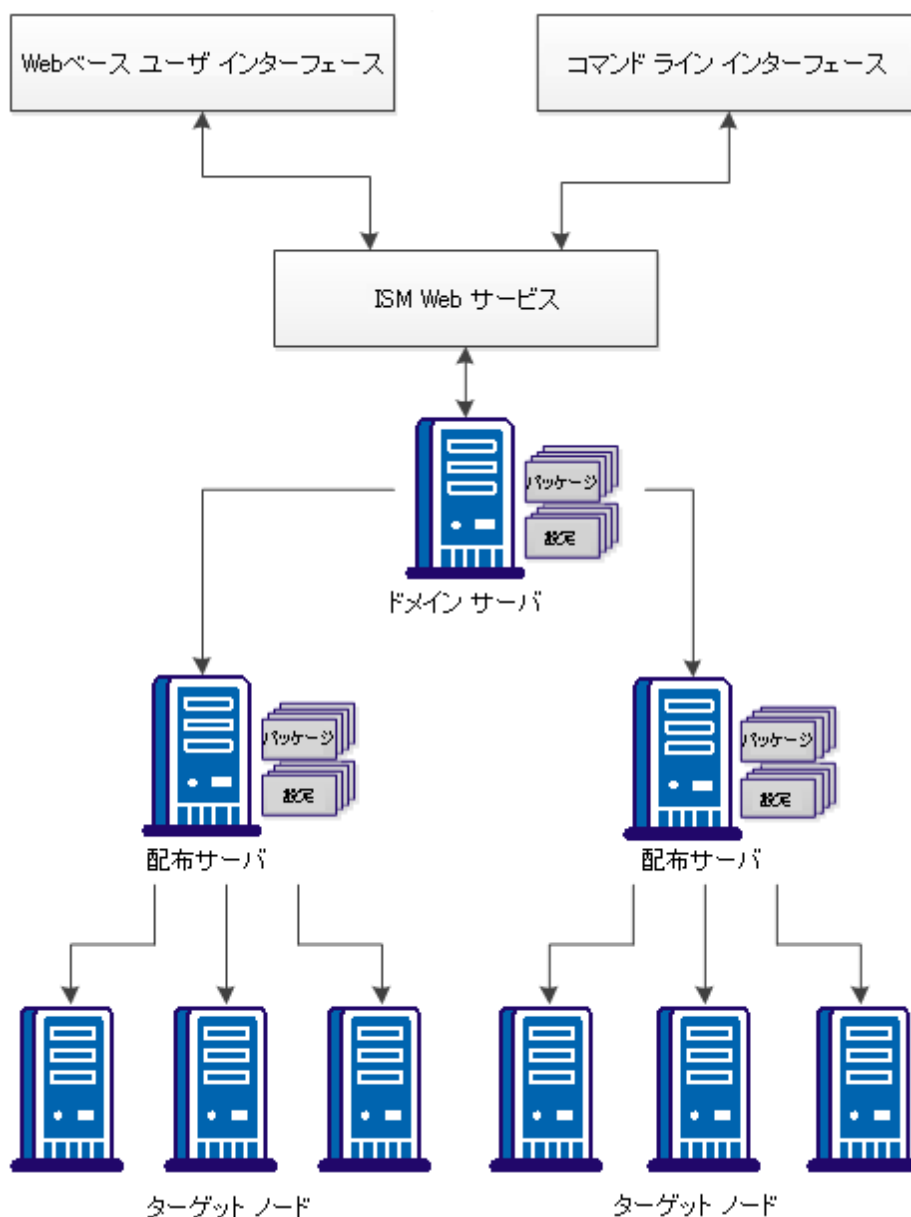
リモート展開およびポリシー設定の概要

CA Virtual Assurance は、SystemEDGE エージェントをすべての管理対象システムにリモート展開するための包括的なソリューションを提供します。カスタマイズ済みのインストール パラメータを含む提供パッケージに基づいて展開テンプレートを作成し、これらのテンプレートを多数の管理対象システムに同時に展開できます。

さらに、CA Virtual Assurance は、すべての管理対象システム上で実行している SystemEDGE エージェントの設定を継続的に行うための包括的なソリューションを提供します。ポリシー設定は、ポリシーのライブラリを作成する機能を提供します。これらのポリシーは、SystemEDGE および SRM AIM を実行する 1 つ以上のシステムに適用されます。ポリシー設定によって管理されたエージェントがインストールされると、そのエージェントは自動的にポリシーを要求します。このため、エージェントは、制御され、一貫したセットのポリシーを実行します。その後、エージェントは、エージェントが実行しているポリシー、またはエージェントがメンバであるサービスに基づいて、個別に更新できます。

リモート展開およびポリシー設定は、ドメイン サーバおよび配布サーバの技術を共有します。この技術は、スケーラビリティが高く、複数のデータセンターにわたって配布することを可能にするソリューションを提供します。

以下の図は、リモート展開およびポリシー設定のコンポーネントの基本的なアーキテクチャを示します。



ハードウェアの仕様

このセクションでは、CA Virtual Assurance の大規模実装のためのハードウェア 最小仕様をリスト表示します。より大規模な実装においては、管理サーバの仕様の拡張を考慮してください。

- ドメイン サーバ: 2.6 GHz の Dual-Core プロセッサ、4 GB の RAM、100 GB の ディスク。
- 配布サーバ: 1 GHz のシングル コア/プロセッサ/仮想プロセッサ、2 GB の RAM、100 GB のディスク、100 Mb/秒イーサネット。
- VC AIM モニタリング サーバ: 2.6 GHz の Dual Core プロセッサ、4 GB の RAM、100 GB のディスク。

注: CPU とメモリの使用率は、最大 50 パーセントに抑える必要があります。

- ターゲット システム: 1 GHz のシングル コア/プロセッサ/仮想プロセッサ、512 MB の RAM、2 GB のディスク、100 Mb/秒イーサネット x 1

データベースに関する考慮事項

管理対象の環境が拡大するほど、発生するデータベース アクティビティも増えることが予想されます。製品のデータベースは、製品の使用状況に基づいてサイズが大きくなります。メンテナンスの実施内容によっては、30 GB 以上が消費される可能性があります。データ保持については、一般的なルールに従うことをお勧めします。つまり、モニタ対象環境内のマシン 1000 台ごとにポーリング間隔を 300 秒増やします。

注: データベース専用のスタンドアロン システムを使用すると、パフォーマンスを改善できます。データベースをネットワーク上の他の Virtual Assurance for Infrastructure Managers コンポーネントの近く(同一サブネット上など)に配置すれば、レスポンス時間が向上します。

ネットワークに関する考慮事項

CA Virtual Assurance のロールアウトを計画する場合には、ネットワーク接続の品質を検討して、管理コンポーネントを配置する場所を決定します。以下の項目が、ソリューションのスケーラビリティおよび効率に影響を及ぼします。

- ネットワーク品質: 品質が低いと、データの損失が発生し、結果としてレスポンスの遅延、または接続障害を引き起こします。
- ネットワーク帯域幅: 帯域幅が低いと、コンポーネント間でのデータ転送速度が制限されます。
- ネットワーク遅延: ネットワーク遅延が大きいと、帯域幅が低い場合と同様に、データ転送率が制限されます。
- DNS: 適切に設定されていない DNS では、モニタリング エージェントの展開および継続的な設定作業に支障が発生します。

管理コンポーネント間には、少なくとも 100 Mb/秒のネットワークリンクを使用することを推奨します。特にリモート DB を使用するときには、強く推奨します。ネットワーク速度が 100 Mb/秒未満の場合は、別の配布サーバをターゲットシステムと連結して導入することを検討します。

スケーラビリティに関する推奨事項

このセクションでは、スケーラビリティに関する推奨事項および制限事項について説明します。

以下の情報について検討します。

- [VMware 環境のモニタリング](#) (P. 325)
- [VMware 環境の CA Virtual Assurance 管理](#) (P. 327)
- [リモート展開およびポリシー設定に関する推奨事項](#) (P. 329)
- [ドメイン サーバに関する推奨事項](#) (P. 331)
- [配布サーバに関する推奨事項](#) (P. 331)
- [スケーラビリティに関する使用事例](#) (P. 331)

vCenter AIM モニタリングの推奨事項

SystemEDGE エージェントには、初期化時にオプションの *Application Insight Module (AIM)* をロードできるプラグイン アーキテクチャが備わっています。AIM は SystemEDGE エージェントの機能拡張です。たとえば、vCenter AIM により、SystemEDGE は VMware vCenter Server を介して vSphere 環境を管理できます。

vCenter AIM (Application Insight Module) は、SystemEDGE フレームワーク内にインプリメントされたプラグブル コンポーネントです。そのため、これによって発行されるデータは複数の SNMP マネージャから利用可能です。CA Virtual Assurance マネージャ、eHealth、および Spectrum IM などの製品はこのデータをレバレッジできます。

このコンポーネントが CA Virtual Assurance マネージャの外部で利用される可能性があるため、スケーラビリティ推奨事項はそれぞれ別に指定されます。スケーラビリティ推奨事項については、主として 2 つの考慮事項があります。

vCenter AIM モニタリングに対する一般的な推奨事項

vCenter AIM モニタリングにおけるスケーラビリティ制限について、一般的な推奨事項を以下に示します。

- VM の最大数 (概算) : $240,000 / (x + 6)$
- オブジェクトの最大数 (概算) : $2,000,000 / (x + 6)$

x は AIM に対する SNMP ポーリングの 1 時間あたりの回数です。

モニタ対象オブジェクトに関するスケーラビリティ制限

一般的に、スケーラビリティの制限においては CPU 使用率が主な考慮事項となります。vCenter AIM モニタリングについては、CPU 使用率に影響を及ぼす 3 つの主要因を考慮します。

- モニタ対象である vCenter Server が動的であること。

vCenter Server のアクティビティレベルは CPU 消費に影響を及ぼします。以下のスケーラビリティ推奨事項では、モニタ対象である vCenter Server の平均的なアクティビティレベルを想定しています。

- SNMP マネージャの数、およびそれらの SNMP マネージャのポーリング間隔。

vCenter AIM のポーリングを行う SNMP マネージャの数が多く、あるいはポーリング間隔が短い場合、CPU 消費は増加します。

- VM 数に関するオブジェクト数の比率。

オブジェクトは、vCenter AIM によってモニタされる vSphere の任意の要素です。たとえば、vCenter AIM は、データストア、仮想ディスク、物理ネットワーク インターフェースコントローラ、仮想スイッチ、SCSI コントローラ、ESX ホスト ハードウェア センサなどをモニタします。オブジェクトの数は CPU の使用率に直接影響があります。vCenter AIM キャッシュを維持する必要があり、さらにこのデータのパブリッシュに追加のオーバーヘッドが必要となるためです。現実のシステムでは、通常、指定された vCenter 内の仮想マシンより 6 ～ 11 倍も多くのオブジェクトがあります。

先行する要因に基づき、vCenter AIM をモニタする単一の SNMP マネージャでポーリング間隔が 10 分の場合、VM 数の制限は約 20000 になります。

モニタ対象サーバに関するスケーラビリティ制限

vCenter AIM は複数の vCenter Server 環境で機能します。実際、vCenter AIM のフレームワークは、vCenter Server あたりの VM の数が減少すると、CPU 使用率もわずかに減少します。たとえば、それぞれ 2000 の VM を持つ 3 つの vCenter Server の CPU 使用率は、6000 の VM を持つ 1 つの vCenter Server の CPU 使用率より低くなります。

そのため、vCenter AIM 応答性がスケーラビリティの制限となる点があります。一般的に、vCenter AIM は最大 10 の vCenter Server をモニタできます。

CA Virtual Assurance vCenter 管理の推奨事項

VA-IM マネージャには、vCenter データのモニタおよび発行だけでなく、多くの機能があります。履歴データの格納と管理、vCenter に対するアクティブな操作、vCenter データに基づく自動ポリシーの実行、レポート機能などです。そのため、vCenter AIM より多くのリソースが必要となることが多く、主なデータ収集メカニズムとして使用されます。

仮想マシンに関する vCenter 管理の制限

CA Virtual Assurance マネージャの大部分は単一のプロセス空間内に存在しているため、多くの場合、オペレーティング システムの制限がスケーラビリティにおける主な問題となります。以下の制限要因を考慮してください。

- 利用可能なメモリ: 管理対象オブジェクトの数が増加すると、データのキャッシュおよびメッセージング処理に必要とされるメモリの量が急激に増加します。マネージャのメモリを 8GB 以上に増加させることを推奨します。
- 利用可能な CPU: CA Virtual Assurance マネージャは、特に急速な環境変化または初期起動において、大量の CPU リソースを必要とします。自動プロセスの応答性を向上させるため、ある程度大規模な管理対象環境については、追加 CPU (3.2 GHz 以上)を準備することを推奨します。
- オペレーティング システムの制限: CA Virtual Assurance マネージャの多くは単一のプロセス空間内に存在します。その結果、32 ビット オペレーティング システムのメモリアドレス空間は、システム メモリの空き容量がまだ残っている場合にも使い尽くされる可能性があります。この問題を回避するには、ある程度の規模の管理対象環境については、64 ビットのプロセッサおよびオペレーティング システムを使用することを推奨します。

例:

以下の例は、CA Virtual Assurance マネージャの要件およびスケーラビリティ制限の推奨事項を提供します。

- 最小要件 (32 ビット、2.6GHz の CPU、4GB の RAM、100GB のディスク)
スケーラビリティ制限: 2500 のコンピュータ システム (VM および ESX ホスト)
- 推奨されるシステム (64 ビット プロセッサおよびオペレーティング システム、3.2GHz CPU、8GB の RAM、100GB ディスク)
スケーラビリティ制限: 8000 のコンピュータ システム (VM および ESX ホスト)

初期ディスカバリでのパフォーマンスの考慮事項

管理対象とする vCenter 環境の初期ディスカバリおよびデータベースロードの実行には、時間がかかる場合があります。このプロセスでは、以下が行われます。

1. vCenter AIM が vCenter 環境全体を解析し、マネージャに結果を発行します。
2. CA Virtual Assurance マネージャは vCenter AIM から発行されたデータを取得し、処理用に内部キャッシュを作成します。
3. 内部キャッシュは現在の CA Virtual Assurance マネージャ データベースの内容と同期され、現在データベース内にないコンピュータシステムについての検出が実行されます。

vCenter サーバの初期管理中、データベースにはコンピュータシステムがないため、これらのオブジェクトはすべて検出され、作成されます。初期ディスカバリの完了に必要な予測時間を考慮してください。ベースライン テストに基づく平均スループット: 毎分 8 ～ 9 のコンピュータシステム

例:

以下の例は、環境のサイズ、および、初期ディスカバリの完了に必要なと予想される時間を提供します。

- 2,500 のコンピュータシステム - 約 5 時間
- 8,000 のコンピュータシステム - 約 15 時間

この初期取り込み中は、CPU 使用率が高い状態が長く続きます。

注: 初期ディスカバリプロセスには多大な時間がかかります。ただし、初期ディスカバリは製品の使用において 1 度だけ実行されます。vCenter AIM および CA Virtual Assurance 内部キャッシュのプロセスは、これらのプロセスが再起動されるたびに実行されますが、ずっと短時間で完了します。たとえば、vCenter AIM によって通常 2500 のコンピュータシステムが発行され、CA Virtual Assurance マネージャによって完全にキャッシュされますが、かかる時間は約 5 分です。

リモート展開およびポリシー設定に関する推奨事項

リモート展開およびポリシー設定の作業を効率化するために、以下の観点および推奨事項を検討します。

- ターゲット マシンの数

最適なパフォーマンスのためには、1 つのバッチでの展開ジョブ サイズを 500 のターゲット マシンに制限します。

- 配布サーバの数

複数の配布サーバを使用すると、展開のスループットが向上します。

- 展開パッケージ サイズ

展開ソフトウェア パッケージのサイズが小さいほど、スループットが良くなります。推奨される数は、すべての管理対象サーバに SystemEDGE および Advanced Encryption が必要であると想定したものです。

注: 典型的なパッケージ サイズは 10MB ~ 20MB です。

- ネットワークの品質および速度

配布サーバとターゲット マシンの間で、低い帯域幅のネットワークが使用されており、多量のパケット損失および大きな遅延が発生している場合は、展開と設定の作業の効率と信頼性が低下します。

- ターゲット システムにモニタリング ソフトウェアをロールアウトする時間スケール

連結した展開サーバを使用して、モニタリング ソフトウェアの展開を時間的にずらして実行します。こうすることで、ネットワーク インフラストラクチャの負荷が軽減されます。負荷の軽減は、複数のジョブの作成、またはソリューションに組み込まれている時差配布の機能を使用して達成できます。

モニタリング ソフトウェアを短時間で展開する必要がある場合、環境内により多くの配布サーバを展開することを推奨します。

- (ポリシー設定による) エージェント再設定の頻度

典型的なネットワーク環境での **SystemEDGE** エージェントの再設定には、約 30 秒に加え、1 エージェントにつき 2 ～ 10 秒かかることが予想されます。エージェントを頻繁に再設定する必要がある場合、環境内により多くの配布サーバを展開することを推奨します。

- 複数のサイトに存在するターゲットシステムの地理的分布

ターゲットシステムが複数のサイトに分散されている場合、各サイトに配布サーバを展開することを推奨します。このことは、リモートデータセンターが遅いリンク(100Mb/秒より遅い)、または信頼性の低いリンクを使用する場合、特に推奨されます。ローカル配布サーバを展開することにより、展開および設定の要求がすべてオンサイトの配布サーバを介して送信できます。これにより、中央とリモートサイトの間のトラフィックが軽減されます。

- 通信ポート

リモート展開およびポリシー設定では、ドメインサーバから配布サーバへの通信と、配布サーバからエージェントへの通信に、**CA-Messaging** による通信を使用します。**CA-Messaging** はポート 4104 (UDP) および 4105 (TCP) を使用して通信します。ファイアウォールで保護されているリモートサイトの場合、サイトに配布サーバを配置することにより、すべての **CA-Messaging** 通信をポイントツーポイントとしてセットアップできます。

注: エージェント ディスカバリおよび継続的なモニタリングについては、**SNMP** 通信 (通常ポート 161) が使用されます。管理対象システムからマネージャへの直通通信用にこのポートを開きます。

- ポリシー設定のポリシーおよびテンプレートの管理

お使いの環境内のさまざまなワークロードに基づいて、モニタリング要件をテンプレートにまとめることを推奨します。ポリシーまたはテンプレートあたり最大 1000 のモニタを使用してください。システムに適用するテンプレートの数は任意ですが、テンプレートの数を 1 システムにつき 100 に制限することを推奨します。

- サービスメンバシップ

設定操作を容易にするために、1 サービスにつき約 500 サーバを上限としてサーバをサービスにまとめることを推奨します。1 つのサーバを複数のサービスのメンバとすることが可能であるため、異なるワークロードごとに複数のサービスを作成することを推奨します。こうすると、テンプレートをサービスに直接適用できます。

ドメイン サーバに関する推奨事項

展開および設定ドメイン サーバ(ドメイン サーバ)は、展開とポリシー設定の全操作を管理および制御します。

ターゲットシステムの数が 10000 を超過する場合、CA Virtual Assurance の複数のインスタンスを実行することを推奨します。

配布サーバに関する推奨事項

展開および設定配布(スケーラビリティ)サーバは、展開とポリシー設定の操作を効率的かつタイムリーに行うことを支援します。

CA Virtual Assurance マネージャをインストールしたら、リモート展開およびポリシー設定をロールアウトするための次の手順は、配布サーバの数を検討することです。

展開操作では、典型的な 100 Mb/秒ネットワーク環境で、2000 のターゲットシステムごとに 1 台の配布サーバを使用することを推奨します。

SystemEDGE エージェントがリモート展開を使用せずに展開されている場合(すなわち、ポリシー設定のみが使用されている場合)、3000 のターゲットシステムごとに 1 台の配布サーバを使用することができます。

重要: 大規模な展開操作を行う前に、各配布サーバにつき少なくとも 1 つのシステムへのテスト展開を実行することを推奨します。より大規模な展開で失敗が発生しないことを確認するために、配布サーバを使用して、あらゆるパッケージを展開することを推奨します。

スケーラビリティに関する使用事例

このセクションでは、典型的な実稼働環境を表す使用事例を提供します。これらの事例をお使いの環境と比較し、最も近いものについての推奨事項に従ってください。

部門のデータセンター

この使用事例では、**1000** のシステムをモニタリングする必要があります。すべてのシステムが **1** つのデータセンター内に配置されています。すべてのシステムが、ファイアウォール内の **1** つの場所にあります。また、コンピュータ間の通信には、高速のリンクが使用されています。

この環境の推奨事項は以下のとおりです。

- コンポーネントのインストール

すべての **CA Virtual Assurance** マネージャ コンポーネントは、同じシステムにインストールできます。

- 初期展開

すべてのターゲット ノードにモニタリング ソフトウェアを展開するために **2** つのジョブを作成します。ネットワークの負荷にもよりますが、**SystemEDGE** (および必要な場合 **Advanced Encryption**) の初期展開を完了するのに、**8 ～ 12** 時間を必要とします。

リモートシステムへの展開が完了すると、**CA Virtual Assurance** マネージャは **SystemEDGE** を検出します。ポリシー設定は各エージェントに初期ポリシーを配信します。初期ポリシーの配信は、ジョブ完了の約 **8** 時間後に完了することが予想されます。

- サービス メンバシップ

保守を容易にするために、管理対象のサーバを、**1** サービス当たり **200** サーバを目安として、サービスにまとめます。サービスは、ビジネス機能、ネットワークトポロジ、または他の要件に応じてまとめることができます。

- ポリシーの適用

必要な場合は、**1** 回の操作で、すべてのモニタ対象システムにポリシーを適用できます。

複数のデータ センター

この使用事例では、複数のデータ センターに配置された 10000 のシステムが管理されています。各データ センターのシステム数は 500 ～ 2500 の範囲でさまざまです。データ センターは、複数の場所に地理的に分散しています。データ センター間は、100 Mb/秒未満の専用線でリンクされています。システムはさまざまなワークロードを実行し、多くの異なる部門 (アプリケーション所有者) によって管理されています。

この環境の推奨事項は以下のとおりです。

■ コンポーネントのインストール

専用サーバに CA Virtual Assurance マネージャ コンポーネントをインストールします。このサーバはその最小サポート要件を満たす必要があります。しかし、少なくとも 8 GB の RAM を備えた Quad-Core サーバが推奨されます。

上位の仕様 (Quad-Core プロセッサと 8 GB の RAM) を備えた個別の専用サーバにデータベースをインストールすることを推奨します。

リモート データ センターをサポートするために、各データ センター内に 1 つの配布サーバをインストールすることを推奨します。2000 を超えるサーバが配置されているデータ センターについては、配布サーバを追加して配置することが推奨されます。各配布サーバは、ポリシー設定のためにのみ使用される場合は、最大 3000 サーバに拡張することができます。

■ 初期展開

複数の配布サーバを使用した展開を計画する場合に考慮すべき関連要因を以下に示します。

- 可能な場合は、単一の展開ジョブ サイズを最大 500 のターゲットシステムに制限します。
- 最も近い配布サーバが展開操作のために選択されることを確認します。
- 同時展開は単一の配布サーバ内でサポートされていますが、複数の配布サーバが使用される場合に限定することを推奨します。4 台の配布サーバを用意することにより、各配布サーバで展開するマシンを 500 台にすることができます。
- 同じ配布サーバを使用して同時展開を実行する場合は、ジョブごとに異なるターゲット マシンが展開されることを確認します。
- 複数のパッケージが多くのシステムに配信される場合、パッケージ配信を複数のジョブに分割することを考慮します。たとえば、SystemEDGE および Advanced Encryption を先に展開します。

- 大規模な展開中に失敗が発生する場合は、すべての前提条件を確認してから[ジョブの再サブミット]を使用して展開を再試行します。
- 将来の操作に備えて、展開をテンプレートとして保存することを推奨します。

- サービスメンバシップ

保守を容易にするために、管理対象のサーバを、1 サービス当たり最大 500 サーバを目安として、サービスにまとめます。リモートデータセンターについては、データセンターのサイズに応じて、それぞれに 1 つ以上のサービスを作成することを推奨します。

複数の部門が特定のシステムを使用している場合、各部門による管理を容易にするために、それらのシステムを複数のサービスに追加できます。

- ポリシーの適用

この使用事例では、サーバはさまざまなワークロードを実行します。そのため、ベースポリシーには制御設定のみが含まれるようにすることを推奨します。モニタリング要件に基づいて複数のテンプレートを作成し、個別のモニタリング設定を保持します。その後、これらのテンプレートは、手動でシステムを選択することにより、またはサービスにテンプレートを適用することにより、必要なシステムに適用できます。

モニタリング要件を複数のテンプレートに分割すると、必要なシステムに必要なテンプレートを個別に適用できます。システムを手動で選択するか、またはサービスにテンプレートを適用します。テンプレートの適用は、2000 ～ 2500 のシステムに分けて行うことを推奨します。

ベースポリシーを変更する必要がある場合、2000 ～ 2500 のシステムに分けてポリシーを適用することを推奨します。

注: テンプレートを使用する場合、テンプレートまたはポリシーの各配信において、すべての割り当て済みテンプレートがベースポリシーにマージされます。次の手順は、結果の設定のエージェントへの配信です。そのため、複数のテンプレートがシステムに適用される場合、配信時間がわずかに長くなる場合があります。

大規模な環境

この事例では、約 **21000** のエージェントが管理されています。これらのエージェントは **3** つのデータセンターに配置されており、各データセンターには **2000** ～ **10000** のターゲットが存在します。データセンターは分散されていますが、高速のリンクで接続されています。管理対象システムは大部分が仮想化されており、さまざまなワークロードを実行し、必要に応じて再プロビジョニングされます。

この環境の推奨事項を以下に示します。

■ コンポーネントのインストール

各データセンターで **CA Virtual Assurance** のインスタンスを実行し、各インスタンスが最大 **10000** のシステムを管理することを強く推奨します。

各データセンターでは、専用サーバに **CA Virtual Assurance** マネージャコンポーネントをインストールすることを推奨します。このサーバはその最小サポート要件を満たす必要があります。さらに、**RAM** を **8 GB** に増強することを推奨します。

8 GB の **RAM** を備えた個別の専用サーバにデータベースをインストールすることを推奨します。

CA Virtual Assurance を単一のインスタンスで運用する必要がある場合は、**Quad-Core** プロセッサと **16 GB** の **RAM** を備えたマネージャサーバとデータベースサーバを使用することを推奨します。

リモート展開およびポリシー設定の操作をサポートするために、各データセンターに **1** つの配布サーバをインストールすることを推奨します。**3** つの配布サーバの内の **1** つはマネージャシステムにインストールします。

■ 初期展開

この使用事例では、データセンターに **1** つの配布サーバが追加されています。セットアップ時の **1** つの相違を除いて、前のシナリオで強調されたすべての要因が、このシナリオにも等しく適用されます。

■ サービスメンバシップ

保守を容易にするために、管理対象のサーバを、**1** サービス当たり **500** サーバを目安として、複数のサービスに分割することを推奨します。

■ ポリシーの適用

ベースポリシーを、制御設定と「ベース OS」モニタに制限することを推奨します。異なる複数のイメージが仮想マシンのベースとして使用されている場合、ベースポリシーを各 OS イメージについて作成することができます。登録時にこのポリシーを要求するように SystemEDGE が設定されていることを確認してください。

アプリケーションに固有のモニタについては、個別のモニタリング要件に基づいてテンプレートを作成します。テンプレート間のインデックス競合を回避するために、各アプリケーションに「インデックス範囲」を事前に定義することを推奨します。あるいは、ベースポリシーを、「制御設定」セクションで「インデックスの競合を自動的に解決する」に設定できます。

モニタリング要件を複数のテンプレートに分割すると、必要なシステムに必要なテンプレートを個別に適用できます。手動でシステムを選択するか、またはサービスにテンプレートを適用することによって、個別に適用できます。テンプレートの適用は、2000 ～ 2500 のシステムに分けて行うことを推奨します。

ベースポリシーを変更する必要がある場合、2000 ～ 2500 のシステムに分けてポリシーを適用することを推奨します。

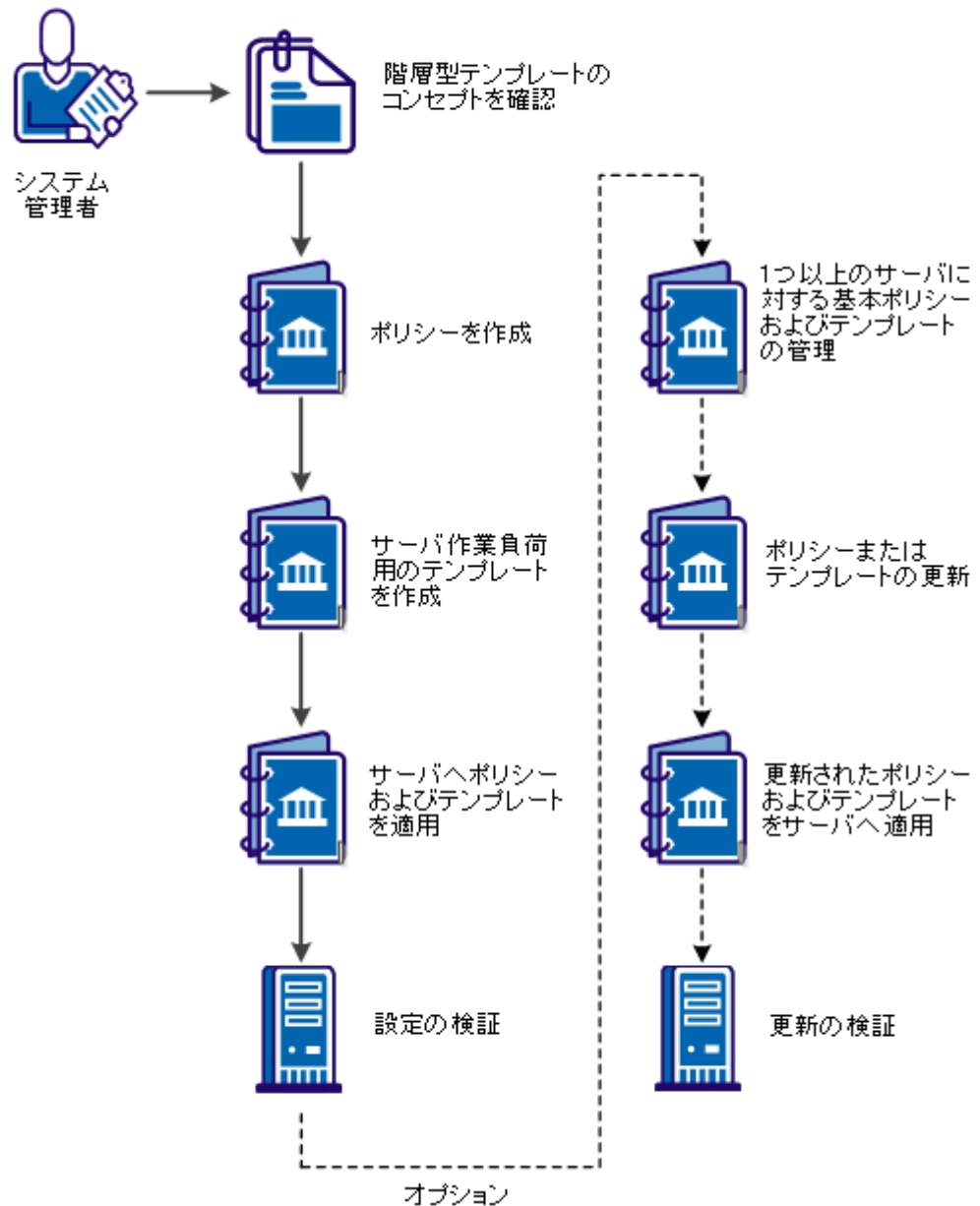
注: テンプレートを使用する場合、テンプレートまたはポリシーの各配信において、すべての割り当て済みテンプレートがベースポリシーにマージされます。次の手順は、結果の設定のエージェントへの配信です。そのため、複数のテンプレートがシステムに適用される場合、配信時間がわずかに長くなる場合があります。

重要: CA Virtual Assurance の複数インスタンスが展開されており、作成されたポリシーを異なるインスタンス間で共有したい場合は、CA サポートにお問い合わせください。CA サポートは、CA Virtual Assurance インスタンス間でのポリシーおよびテンプレートのエクスポートおよびインポートに関して支援できます。

ポリシーおよび階層型テンプレートをサーバに適用する方法

ベース ポリシーを作成し、そのポリシーにテンプレートを階層として追加することにより、CA Virtual Assurance ユーザ インターフェースから SystemEDGE エージェント モニタリングを制御できます。以下の図では、ベース ポリシーと階層型テンプレートの使用方法を示しています。

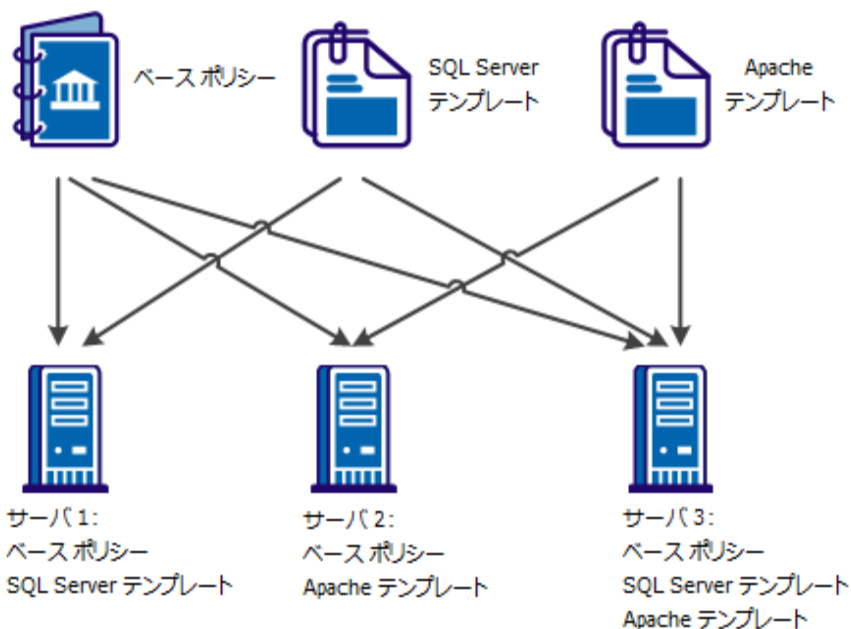
サーバへのポリシーおよび階層型テンプレートの適用



階層型テンプレートとの概念

企業では、サーバまたはサーバグループによって処理されるワークロードは異なります。サーバまたはサーバグループによって処理されるワークロードに固有の複数のポリシーを作成することができます。ポリシーを容易に作成できるようにするために、テンプレートを使用してアプリケーション固有のモニタを作成します。ベースポリシーと階層型テンプレートが組み合わされて設定ファイルが形成され、モニタするサーバに適用されます。階層型テンプレートは、追加または削除することができます。テンプレート更新はサーバに直接適用できます。ベースポリシーを変更したり、更新されたテンプレートをベースポリシーに再インポートしたりする必要はありません。

例：ベース ポリシーおよびテンプレートをサーバに適用



階層型ポリシーは、以下のシナリオで使用できます。

異種アプリケーション

異なるセットのアプリケーションを実行するサーバごとにテンプレートのライブラリを作成します。各サーバにテンプレート更新を直接適用できます。

動的な環境

サーバの負荷は、動的な環境で頻繁に変化します。階層型テンプレートを使用して、モニタを論理グループに分離します。負荷の変化に基づいて、論理グループを直接システムに適用したり、システムから削除したりできます。

共有サーバ

企業セットアップでは、サーバは複数の部門間で共有されます。各部門は共有サーバ上のアプリケーションを管理し、モニタします。階層型テンプレートを使用することにより、テンプレートの個別の管理および各部門のシステムへの適用を行うことができます。

アプリケーションの保守

モニタリングは複数のテンプレートに分割できます。サーバでは、使用していないアプリケーションのテンプレートを削除でき、システムの他の部分のモニタリングに影響することはありません。

ポリシーの作成

エージェントのモニタリングを制御するため、モニタ、MIB 拡張、トラップ & コミュニティ、および制御設定のセットを定義するベース ポリシーを作成します。

トラップ & コミュニティと制御設定の中の共通設定はポリシーのみに利用可能です。階層型テンプレートを使用する場合、共通設定はベース ポリシー内に指定されます。

次の手順に従ってください:

1. [リソース] タブをクリックして[設定] ペインを開き、[ポリシー] を展開して [SystemEDGE] をクリックします。
[利用可能ポリシー] ページが表示されます。
2. [利用可能ポリシー] ツールバーの[+] (新規) をクリックします。
[新規 SystemEDGE ポリシー] ダイアログ ボックスが表示されます。

3. ポリシーの名前と任意の説明、システムタイプ、および既存のポリシーをベースにするかどうかを入力し、[OK]をクリックします。

ポリシーが作成され、右側のペインに設定画面が表示されます。

4. [ポリシーの保存]をクリックします。

ポリシーが作成および保存されます。

注: 必要に応じて、既存のデフォルトポリシーをベースポリシーとして使用することができます。

SystemEDGE ポリシー制御設定の定義

SystemEDGE ポリシー コントロール設定を使用して、以下のエージェント動作を制御できます。

- セキュリティ設定
- SNMP の設定
- MIB テーブルへのデータのロード
- UNIX の設定
- パフォーマンス モニタリングの設定

これらの共通コントロール設定は、ベースポリシーに追加することで特定のサーバワークロード設定から分離することができます。

ポリシーに定義されたコントロール設定は、この設定でモニタするすべてのシステムに適用することができます。

次の手順に従ってください:

1. [リソース]タブをクリックして[設定]ペインを開き、[ポリシー]を展開して[SystemEDGE]をクリックします。

[利用可能ポリシー]ページが表示されます。

2. [利用可能ポリシー]テーブルでポリシーを選択します。

ポリシーの[サマリ]ページが表示されます。

3. [制御設定]をクリックします。
[コントロール]ページが表示されます。
4. (オプション)[デフォルトを使用]をクリックします。
デフォルトの選択ペインが表示されます。デフォルトの設定を変更できます。
5. 以下の制御設定を行います。

SNMP

以下の基本的な SNMP プロパティを定義できます。

バインド アドレス

エージェントがバインドし、受信 SNMP リクエストをリスンするインターフェースを指定します。有効なアドレスは IPv4 または IPv6 のアドレスです。

注: 対応するデフォルトのポートはインストール中に指定します。

バインド ポート

SNMP トラップを送信するために、エージェントがバインドするトラップ ポートを指定します。bind_address が指定されていない場合、エージェントは利用可能なすべての UDP アドレスにバインドします。

デフォルト: システムによって選択されたポート

IP ファミリ

エージェントの通信方法 (IPv4 のみ、IPv6 のみ、またはその両方) を指定します。デフォルトでは、エージェントは、IPv4、IPv6 の順に使用を試行します。

FIPS モード

FIPS 準拠の暗号化を使用するように、エージェントを指定します。CA eTrust 公開鍵インフラストラクチャ ライブラリを有効にするには、[非 FIPS モード]を選択します。この方法が失敗する場合は、内部の最低限のセキュリティソリューションにフォールバックします。FIPS 準拠の暗号化を有効にするには、[FIPS 共存モード]を選択します。この方法が失敗する場合は、CA eTrust 公開鍵インフラストラクチャ ライブラリにフォールバックします。これらが失敗した場合は、[FIPS のみのモード]を選択して、RSA BSAFE Crypto-C Micro Edition FIPS 準拠ライブラリを有効にし、暗号化を実行しません。

デフォルト: 非 FIPS モード

トラップ ソース

トラップを送信するために使用されるソースアドレスを指定します。有効なアドレスは IPv4 アドレス、IPv6 アドレス、またはホスト名です。

デフォルト: エージェントのホスト名

セキュリティ設定

以下のセキュリティ基本設定を定義できます。

認証トラップ

エージェントが認識できないという、コミュニティ名を備えた SNMP メッセージをエージェントが受信した場合に、認証失敗トラップを送信します。

デフォルト: 無効

プロセス セット

プロセステーブルおよび Running Software テーブルで、エージェントシステム上で実行されているプロセスや他のソフトウェアにアクセスできます。これらのテーブルで SNMP セットを許可すると、セキュリティの問題が発生する場合があります。

リモート シェル グループ

管理システムは、リモートシェルグループを使用して、エージェントシステム上でシェル スクリプトおよびプログラムを実行するようにエージェントに対してリモートから指示できます。このタイプの情報が漏えいすると、潜在的なセキュリティリスクが発生する可能性があります。

実行アクション

しきい値違反が発生したときに、モニタリング テーブルを使用したアクション コマンドの実行を有効にします。アクション コマンドおよびスクリプトを実行する機能が原因で、セキュリティ上の問題が発生する可能性があります。

MIB テーブルへのデータのロード

Systems Management MIB の以下のテーブルに入力します。

- プロセス テーブル
- ユーザ グループ テーブル
- Who テーブル
- トラップ コミュニティ テーブル
- ミラー テーブルのモニタ
- ミラー テーブルを集計
- トップ プロセス テーブル

各テーブルには、MIB で公開可能な機密情報か、ディスク領域を節約するために無効にできる重要でない情報のいずれかが含まれています。デフォルト設定では、プロセス テーブルを除くすべてのテーブルにデータをロードできます。

その他

以下のその他の設定を定義できます。

SNMP を使用してエージェントが更新されるのを許可

SNMP SET を使用したエージェントの更新を許可します (書き込みコミュニティの削除など)。エージェント上で SNMP SET を許可すると、この方式でのあらゆる更新において、SNMP SET 変更の通知が送信されます。また、これらの更新により、システムのポリシー詳細の表示時に例外が発生します。

マネージャに設定の更新を通知

エージェントが処理する **SNMP** 設定リクエストすべてについて、エージェントによるマネージャへの通知送信を可能にします。

ウォーム スタートのディスカバリ

ウォーム スタート設定が更新されるたびに、すべてのデバイスでエージェントが再検出されます。デバイスが多数あるシステムを管理している場合、ウォーム スタートのたびにディスカバリが実行されると、非常に多くの時間とリソースを消費する場合があります。

Perl 互換正規表現を使用

Perl 互換正規表現 (PCRE) を使用すると、正規表現をサポートするモニタを定義するときに **i18n** 互換の正規表現を指定できます。正規表現の例には、ログ ファイル、プロセス、プロセスグループ、**Windows** サービスおよび **Windows** イベントがあります。また、このオプションを使用して、より複雑な正規表現を作成できます。このオプションは、**SystemEDGE** エージェント **5.1.0** 以降のバージョンで提供されています。

インデックスの競合を自動的に解決する

インデックスの競合を解決できるようにします。すべてのシステムに階層型テンプレートを適用するとき、インデックスはテンプレート内に追加されたモニタに割り当てられます。割り当てられたインデックスがベース ポリシーまたは別のテンプレート内の既存のインデックスと競合する場合、このオプションは一意のインデックス値を再割り当てします。

注: ベース ポリシー内に含まれるインデックスは、配信された設定で常に維持されます。このオプションが無効な場合、競合するインデックスを解決できません。ただし、システムに階層型テンプレートを適用するとき、競合するインデックスは、競合するインデックスが発生した階層型テンプレート上にエラーとして表示されます。

履歴パフォーマンス モニタリング

パフォーマンス キューブ **AIM** に対して以下の設定を定義できます。パフォーマンス キューブ **AIM** では、履歴パフォーマンスを管理するための履歴情報を **Systems Performance** キューブに収集します。

収集間隔

履歴テーブルからパフォーマンス キューブに情報を収集する頻度を指定します。

インデックス範囲の開始

インデックスの予約済み範囲の開始を指定します。デフォルトでは、エージェントはこの範囲でパフォーマンスキューブ データを収集するための履歴コントロール エントリを作成します。この予約済み範囲は、SRM (サービスレスポンス モニタリング) がパフォーマンスデータを収集するよう設定されている場合などに使用されます。

インデックス範囲の終了

インデックスの予約済み範囲の開始を指定します。デフォルトでは、エージェントはこの範囲でパフォーマンスキューブ データを収集するための履歴コントロール エントリを作成します。この予約済み範囲は、SRM (サービスレスポンス モニタリング) がパフォーマンスデータを収集するよう設定されている場合などに使用されます。

UNIX 制御設定

UNIX システム上で実行されるエージェントに対して、以下の設定を定義できます。

サブプログラム グループ

サブプログラムを実行するルート以外のグループ名を指定します。

サブプログラム ユーザ

サブプログラムを実行するルート以外のユーザ名を指定します。

Linux Freemem を含む

空きメモリの計算に、システム バッファ、ディスク キャッシュ メモリ、またはその両方を含めるかどうかを指定します。

システム デバイスのクエリ

以下のシステム デバイス メトリックのクエリを有効にできます。

- シリアル デバイス ステータス
- フロッピー ディスク ステータス
- ディスク サイズ、容量、説明、およびその他のプロパティ(ディスクのプロープ)
- NFS ファイル システム ステータス
- HP-UX グラフィックス ステータス

これらのメトリックに対してクエリを実行すると、潜在的なエージェントブロックに関する問題が発生する可能性があります。デフォルト設定では、シリアル デバイス ステータスおよび NFS ファイル システム ステータスに対するクエリのみが有効になっています。

6. [プラグイン]をクリックします。

[プラグイン]ペインが表示されます。このペインで、エージェントを使用してロードする AIM を指定します。

7. 以下のいずれかを実行します。

- [利用可能なすべてのプラグインをロードします]を選択して、エージェントシステムで利用可能なすべての AIM をロードします。
- [テーブルで選択されたプラグインをロードします]を選択します。
- [外部プラグイン]ツールバーの[+] (新規)をクリックし、外部プラグインテーブルに AIM を追加します。

注: 利用可能な AIM の詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

AIM ロードが設定されます。

8. [モニタを集計]をクリックします。

[「オブジェクト集計の設定 \(P. 347\)」](#)の説明に従って、モニタの集計を設定します。

制御設定が定義されます。

9. [ポリシーの保存]をクリックします。

ポリシーが保存されます。

関連項目:

[オブジェクト集計の設定](#) (P. 122)

オブジェクト集計の設定

デフォルトでは、**SystemEDGE** がモニタを集計し、オブジェクト クラス、インスタンス、および属性プロパティに同じ値を含む管理対象オブジェクトを生成します。たとえば、**SysHealth** のクラス、**CPU** のインスタンス、および **SysTime** の属性を備えたすべてのモニタが組み合わされ、集計管理対象オブジェクトとなります。

SystemEDGE ポリシーを定義するときに、より高いレベルでオブジェクトを集計するよう、エージェントを設定できます。また、オブジェクト集計および状態管理モデルに関連するエージェント動作の他の側面も設定できます。

次の手順に従ってください:

1. [リソース] タブをクリックして [設定] ペインを開き、[ポリシー] を展開して [SystemEDGE] をクリックします。

[利用可能ポリシー] ページが表示されます。

2. [利用可能ポリシー] テーブルでポリシーを選択します。

ポリシーの [サマリ] ページが表示されます。

3. [制御設定] をクリックします。

[コントロール] ページが表示されます。

4. [モニタを集計] をクリックします。

[モニタを集計] ページが表示されます。

5. 集計レベルを指定するチェック ボックスを 1 つ以上、オンにします。

これらはデフォルトより高い集計レベルを表し、最も高いレベルでは 1 つの最上位エージェントオブジェクトにすべてのモニタを集計できます。集計レベルを指定すると、指定したレベルまでステータスをプロパゲートする層構造のオブジェクトアーキテクチャを作成できます。

6. 以下の追加設定を設定して、[ポリシーの保存]をクリックします。

すべての集計済みモニタのレガシートラップを送信します。

管理対象オブジェクトを形成するすべてのモニタのレガシートラップを送信するかどうかを指定します。デフォルトでは、オブジェクト内の他のモニタでしきい値違反が発生しても、エージェントは、最も重大度の高いモニタの状態変更トラップを送信するのみです。

すべての集計済みモニタのコマンドを実行します。

管理対象オブジェクトを形成するすべてのモニタのアクション コマンドを実行するかどうかを指定します。デフォルトでは、オブジェクト内の他のモニタでしきい値違反が発生しても、エージェントは、最も重大度の高いモニタのアクション コマンドを実行するのみです。

集計設定が設定されます。変更を有効にするには、ポリシーを適用または再適用します。

関連項目：

[SystemEDGE ポリシー制御設定の定義 \(P. 181\)](#)

トラップとコミュニティの定義

SNMP 設定では、エージェントが使用するコミュニティ、およびエージェントがトラップを送信する宛先を定義します。

次の手順に従ってください：

1. [リソース]タブをクリックして[設定]ペインを開き、[ポリシー]を展開して[SystemEDGE]をクリックします。
[利用可能ポリシー]ページが表示されます。
2. [利用可能ポリシー]テーブルでポリシーを選択します。
ポリシーの[サマリ]ページが表示されます。
3. [トラップ & コミュニティ]タブをクリックします。
[コミュニティ]ページが表示されます。

4. 以下のいずれかを選択して[アクション]をクリックし、[適用]を選択します。
- サーバ固有 SNMP 設定のみを含める
 - サーバ固有 SNMP 設定およびすべてのデフォルト設定を含める
 - [サーバ固有 SNMP 設定および選択されたデフォルト設定を含める]を選択します。

[SNMP 設定]が更新され、[コミュニティ]テーブル内のコミュニティ ページに以下が表示されます。

名前

コミュニティ文字列の名前を指定します。

ポート

SNMP のポートを指定します。

SNMP バージョン

コミュニティが使用する SNMP バージョンを指定します。

アクセス権

コミュニティが、読み書きまたは読み取り専用のいずれの権限を持つかを指定します。

注: 少なくとも 1 つの読み取り専用コミュニティと、1 つの読み書きコミュニティを追加してください。

コミュニティ/ユーザ

コミュニティ名を指定します。

認証プロトコル

SNMPv3 データを認証するプロトコルを指定します。

プライバシープロトコル

SNMPv3 データを認証するプロトコルを指定します。

アクセス制御リスト

IP アドレスのスペース区切りリストを指定して、コミュニティの使用をこれらのアドレスのみに制限します。リストを空にしておくと、エージェントは、関連付けられたコミュニティ名を使用するあらゆるシステムに対してアクセス権を付与します。アクセスリストは、**SNMPv1** を使用するコミュニティについてのみ有効です。

注: **SNMPv2c** および **SNMPv3** のアクセスリストの定義の詳細については、「**SystemEDGE ユーザ ガイド**」を参照してください。

5. (オプション) 必要に応じて、他のコミュニティを追加、更新、または削除します。
6. [ポリシーの保存]をクリックします。
ポリシーが保存されます。
7. [トラップ先]をクリックします。
[トラップ先]ページが表示されます。
8. 以下のコントロールを使用して、トラップ先を定義し、[追加]をクリックします。

トラップ タイプ

SNMP バージョンに応じて、送信するトラップのタイプを指定します。

デスティネーション

トラップを送信する IPv4 アドレスまたは IPv6 アドレスを指定します。

ポート

トラップを送信する UDP ポートを指定します。

コミュニティ

トラップで送信されるコミュニティ名を指定します。

エンコーディング

(オプション)トラップ内の[制御設定]ペインの[トラップ ソース]フィールドで定義したソース アドレスを含める方法を指定します。このパラメータはトラップ ソースが IPv6 アドレスに変換される場合に重要です。3 桁の XYZ の形式(先頭の未使用桁をゼロで埋める)でエンコーディング パラメータを入力します。

デフォルト: 000

X

4 バイトの IPv4 ソース アドレス フィールド(SNMPv1 トラップのみ)の拡張を制御します。16 バイトの IPv6 アドレスを含めるのに、ソース アドレス フィールドを拡張しない場合は 0 を入力し、ソース アドレス フィールドを拡張する場合は 1 を入力します。

Y、Z

トラップの varbind (Y) または UDP パケット(Z、SNMPv1 トラップのみ)にソース情報を含めるかどうかを制御します。これらの桁に以下のいずれかを入力します。

0: トラップの varbind または外部 UDP パケットは変更されません。

1: varbind またはパケットに trap_source パラメータ(IPv4/IPv6 アドレスまたはホスト名)をそのまま含めます。

2: trap_source パラメータを、可能であれば IPv4 アドレスとして(続いて IPv6 アドレス、ホスト名の順に試行)含めます。

3: trap_source パラメータを、可能であれば IPv6 アドレスとして(続いて IPv4 アドレス、ホスト名の順に試行)含めます。

4: trap_source パラメータを、可能であればホスト名として(続いて IPv4、IPv6 の順に試行)含めます。

5: 2 の優先順位に従い、ホスト名を含めます。

6: 3 の優先順位に従い、ホスト名を含めます。

7: 1 の優先順位に従い、ホスト名を含めます(trap_source が IPv6 アドレスの場合)。

トラップ ソース

(オプション)トラップ ソースとして使用する IPv4 アドレス、IPv6 アドレス、またはホスト名を指定します。

デフォルト: グローバルトラップ

トラップ先が[定義済みトラップ先]テーブルに表示されます。

9. (オプション) 必要に応じて、他のトラップ先を追加、更新、または削除します。
10. [ポリシーの保存]をクリックします。
ポリシーが保存されます。

注: 詳細については、「[SystemEDGE ユーザ ガイド](#)」を参照してください。

サーバワークロード用のテンプレートの作成

サーバのワークロードに固有のテンプレートを作成します。モニタと MIB 拡張を指定できます。

次の手順に従ってください:

1. [リソース]タブをクリックして[設定]ペインを開き、[モニタリング テンプレート]を展開して[SystemEDGE]をクリックします。
[テンプレートリスト]ページが表示されます。
2. [テンプレートリスト]ツールバーの[+] (新規)をクリックします。
[新規 SystemEDGE モニタリング テンプレート]ダイアログ ボックスが表示されます。
3. テンプレートの名前と説明(説明はオプションです)、システムタイプ、および既存のテンプレートをベースにするかどうかを入力し、[OK]をクリックします。
テンプレートが作成され、[サマリ]ページが表示されます。
4. テンプレートは、モニタおよび MIB 拡張のコレクションです。テンプレートにモニタを追加する方法については、「[テンプレートまたはポリシーへのモニタの追加 \(P. 353\)](#)」を参照してください。テンプレートに MIB 拡張を追加するには、「[MIB 拡張の定義 \(P. 366\)](#)」を参照してください。
5. [テンプレートの保存]をクリックします。
テンプレートが作成および保存されます。

テンプレートまたはポリシーへのモニタの追加

サーバまたはサーバグループによって処理されるワークロードに固有のテンプレートに、モニタを追加します。以下の手順は、ポリシーへのモニタの追加の場合と似ています。

次の手順に従ってください:

1. [リソース]タブをクリックして[設定]ペインを開き、[モニタリング テンプレート]および適切なサブカテゴリを展開します。

[テンプレートリスト]ページが表示されます。

2. [テンプレートリスト]内のテンプレートを選択します。

テンプレートの[サマリ]ページが表示されます。

3. [モニタ]をクリックし、追加するモニタを選択します。

モニタを作成するために、以下のモニタに対するしきい値と重大度の値を指定する設定を定義します。

- [しきい値モニタの作成](#) (P. 354)
- [プロセス モニタの作成](#) (P. 356)
- [ログ ファイル モニタの作成](#) (P. 359)
- [Windows イベント モニタの作成](#) (P. 361)
- [履歴モニタの作成](#) (P. 362)
- [プロセスグループ モニタの作成](#) (P. 364)

4. (オプション) 追加するモニタごとに同じ手順を繰り返します。

5. [保存]をクリックします。

モニタがポリシーまたはテンプレートにロードされます。

しきい値モニタの作成

エージェントが、指定したしきい値に対して、サーバまたはサーバグループをモニタすることを可能にするしきい値モニタを作成します。しきい値違反が発生すると、エージェントがトラップを送信します。

次の手順に従ってください:

1. [リソース]タブをクリックして[設定]ペインを開き、[モニタリング テンプレート]および適切なサブカテゴリを展開します。
[テンプレートリスト]ページが表示されます。
2. [テンプレートリスト]内のテンプレートを選択します。
テンプレートの[サマリ]ページが表示されます。
3. [モニタ]タブをクリックします。
[サマリ]ページが開き、ポリシーによって管理されるモニタのリストが表示されます。
4. [しきい値]をクリックします。
[しきい値モニタ]ページが表示されます。
5. [しきい値モニタ]ツールバーの[+] (新規)をクリックします。
[しきい値モニタの詳細: 新規]ペインが表示されます。
6. 以下のしきい値設定を行います。

インデックス

使用するテーブル インデックスを定義します。

プラットフォーム

プラットフォームを指定します。

説明

オプションの説明を定義します。

オブジェクト クラス

モニタするオブジェクト クラスを指定します。値は利用可能な MIB テーブルを参照します。

オブジェクト クラス名

オブジェクト状態モデルに使用するオブジェクト クラス名を定義します。値は任意の文字列(たとえば FileSystems)です。

オブジェクト属性

モニタするオブジェクト属性を指定します。値は、オブジェクトクラスとして選択されたテーブルの利用可能な属性を参照します。属性(たとえば `devCapacity = 1.3.6.1.4.1.546.1.1.1.7.1.14`)は、このしきい値モニタでモニタする MIB オブジェクト(OID)の初期部分を指定します。

オブジェクト属性名

オブジェクト状態モデルに使用するオブジェクト属性名を定義します。これは任意の文字列です(PercentUsed など)。

オブジェクト インスタンス

モニタするオブジェクト インスタンスを指定します。この値、たとえば、デバイス テーブル(devTable)内の 3 番目の行をモニタするための .3 は、このしきい値モニタでモニタする MIB オブジェクト(OID)のインデックス部分を指定します。いくつかのオブジェクトクラスについては、インスタンス自体の名前を指定できます(たとえば .3 の代わりに C:、または UNIX マシンで /var)。

オブジェクト インスタンス名

オブジェクト状態モデルに使用するオブジェクト インスタンス名を定義します。値は任意の文字列(たとえば SysVol_C)です。

間隔

モニタの評価間隔を 30 秒の倍数で定義します。

[しきい値設定] ページで、以下の設定を定義できます。

重大度

オブジェクト状態モデルで使用する重大度を指定します。

演算子

使用する演算子を指定します。

値

使用する値を定義します。

サンプル タイプ

使用するサンプル タイプを指定します。

[保守ウィンドウ]ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

[オプション設定]サブタブで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

7. [保存]をクリックします。

[しきい値モニタ]設定が保存されます。

8. [テンプレートの保存]をクリックします。

しきい値モニタがテンプレートにロードされます。

プロセス モニタの作成

エージェントが、指定したしきい値に対してプロセス、サービス、またはプロセス テーブル オブジェクトをモニタできるようにするプロセス モニタを作成します。しきい値違反が発生するか、プロセスの状態(実行中または停止中)が変化すると、エージェントはトラップを送信します。

次の手順に従ってください:

1. [リソース]タブをクリックして[設定]ペインを開き、[モニタリング テンプレート]および適切なサブカテゴリを展開します。

[テンプレートリスト]ページが表示されます。

2. [テンプレートリスト]内のテンプレートを選択します。

テンプレートの[サマリ]ページが表示されます。

3. [モニタ]タブをクリックします。

[サマリ]ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. プロセスをクリックします。
[プロセス モニタ]ページが表示されます。
5. [プロセス モニタ]ツールバーの[+] (新規)をクリックします。
[プロセス モニタの詳細: 新規]ダイアログ ボックスが表示されます。
6. 以下のプロセス設定を行います。

インデックス

使用するテーブル インデックスを定義します。

プラットフォーム

プラットフォームを指定します。

説明

オプションの説明を定義します。

オブジェクト クラス名

オブジェクト状態モデルに使用するオブジェクト クラス名を指定します。
値は任意の文字列(たとえば `Process`)です。

オブジェクト属性

モニタするオブジェクト属性を指定します。値は、プロセス モニタリング
で利用できる属性を定義します。

オブジェクト属性名

オブジェクト状態モデルに使用するオブジェクト属性名を定義します。
値は任意の文字列(たとえば `MemUsedPercent`)です。

オブジェクト インスタンス

モニタするオブジェクト インスタンスを指定します。これは、名前による
一致処理、または名前による **Windows** サービスの一致処理に使用さ
れる正規表現(オプションの設定に依存します)です。パターンは一意
に単一のプロセス(サービス)と一致する必要があります。引数を含むこ
とができます(オプション設定を参照してください)。

オブジェクト インスタンス名

オブジェクト状態モデルに使用するオブジェクト インスタンス名を指定
します。値は任意の文字列(たとえば `ApacheServer`)です。

間隔

モニタの評価間隔を 30 秒の倍数で定義します。

[しきい値設定] ページで、以下の設定を定義できます。

重大度

オブジェクト状態モデルで使用する重大度を指定します。

演算子

使用する演算子を指定します。

値

使用する値を定義します。

サンプル タイプ

使用するサンプル タイプを指定します。

[保守ウィンドウ] ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

[オプション設定] サブタブで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

7. [保存] をクリックします。
[プロセス モニタ] 設定が保存されます。
8. [テンプレートの保存] をクリックします。
プロセス モニタがポリシーにロードされます。

ログ ファイル モニタの作成

エージェントがすべての UTF-8 エンコードされたシステムまたはアプリケーションのログ ファイルを、正規表現として指定されている文字列を検索することによってモニタできるようにする、ログ ファイル モニタを作成します。一致する行が見つかると、エージェントがトラップを送信します。

次の手順に従ってください:

1. [リソース]タブをクリックして[設定]ペインを開き、[モニタリング テンプレート]および適切なサブカテゴリを展開します。
[テンプレートリスト]ページが表示されます。
2. [テンプレートリスト]内のテンプレートを選択します。
テンプレートの[サマリ]ページが表示されます。
3. [モニタ]タブをクリックします。
[サマリ]ページが開き、ポリシーによって管理されるモニタのリストが表示されます。
4. [ログ ファイル]をクリックします。
[ログ ファイル モニタ]ページが表示されます。
5. [ログ ファイル モニタ]ツールバーの[+] (新規)をクリックします。
[ログ ファイルの詳細: 新規]ダイアログ ボックスが表示されます。
6. 以下のプロセス設定を行います。

インデックス

使用するテーブル インデックスを定義します。

モニタ タイプ

使用するモニタ タイプを指定します。

プラットフォーム

プラットフォームを指定します。

説明

オプションの説明を定義します。

ログ ファイル/ディレクトリ名

モニタするファイルまたはディレクトリのパスを定義します。

検索フィルタ

検索フィルタを指定します。

間隔

モニタ評価間隔を分単位で定義します。

重大度

一致したときのモニタの重要度を指定します。

[保守ウィンドウ]ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

[オプション設定]ページで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

7. [保存]をクリックします。

[ログ ファイル モニタ]設定が保存されます。

8. [テンプレートの保存]をクリックします。

ログ ファイル モニタがポリシーにロードされます。

Windows イベント モニタの作成

エージェントが別のフィルタ(イベントソース)を使用して、Windows イベント ログ エントリをモニタできるようにする Windows イベント モニタを作成します。一致する行が見つかり、エージェントがトラップを送信します。

次の手順に従ってください:

1. [リソース]タブをクリックして[設定]ペインを開き、[モニタリング テンプレート]および適切なサブカテゴリを展開します。
[テンプレートリスト]ページが表示されます。
2. [テンプレートリスト]内のテンプレートを選択します。
テンプレートの[サマリ]ページが表示されます。
3. [モニタ]タブをクリックします。
[サマリ]ページが開き、ポリシーによって管理されるモニタのリストが表示されます。
4. [Windows イベント]をクリックします。
[Windows イベント モニタ]ページが表示されます。
5. [Windows イベント モニタ]ツールバーの[+] (新規)をクリックします。
[Windows イベントの詳細: 新規]ダイアログ ボックスが表示されます。
6. 以下のプロセス設定を行います。

インデックス

使用するテーブル インデックスを定義します。

プラットフォーム

プラットフォームを指定します。

説明

オプションの説明を定義します。

イベント ログ

読み取るイベント ログを指定します。

イベント タイプ

モニタするイベント タイプを指定します。

ソース フィルタ

使用するソース フィルタを定義します。

説明フィルタ

使用する説明フィルタを定義します。

重大度

一致したときのモニタの重要度を指定します。

[保守ウィンドウ]サブタブで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

[オプション設定]サブタブで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

7. [保存]をクリックします。

[Windows イベント モニタ]設定が保存されます。

8. [テンプレートの保存]をクリックします。

Windows イベント モニタがポリシーにロードされます。

履歴モニタの作成

エージェントがマネージャ側ベースラインおよび傾向分析用の履歴データを収集できるようにする履歴モニタを作成します。エージェントはメトリックを使用して、特定の期間中の平均システム パフォーマンスの図を提供します。

次の手順に従ってください:

1. [リソース]タブをクリックして[設定]ペインを開き、[モニタリング テンプレート]および適切なサブカテゴリを展開します。
[テンプレートリスト]ページが表示されます。
2. [テンプレートリスト]内のテンプレートを選択します。
テンプレートの[サマリ]ページが表示されます。

3. [モニタ]タブをクリックします。
[サマリ]ページが開き、ポリシーによって管理されるモニタのリストが表示されます。
4. [履歴]をクリックします。
[履歴モニタ]ページが表示されます。
5. [履歴モニタ]ツールバーの[+] (新規)をクリックします。
[履歴詳細: 新規]ダイアログ ボックスが表示されます。
6. 以下のプロセス設定を行います。

インデックス

使用するテーブル インデックスを定義します。

プラットフォーム

プラットフォームを指定します。

説明

オプションの説明を定義します。

オブジェクト クラス

モニタするオブジェクトを指定します。値は利用可能な MIB テーブル値を参照します。

オブジェクト属性

モニタするオブジェクト属性を指定します。値は、オブジェクトクラスとして選択されたテーブルの利用可能な属性を参照します。属性(たとえば devCapacity=1.3.6.1.4.1.546.1.1.1.7.1.14)は、この履歴エントリを使用してモニタするための MIB オブジェクト(OID)の初期部分を指定します。

オブジェクト インスタンス

モニタするオブジェクト インスタンスを定義します。この値(たとえば、0.3 はデバイス テーブル(devTable)の 3 行目をモニタします)は、この履歴エントリでモニタする MIB オブジェクトのインデックス部分(OID)を指定します。

間隔

収集間隔を 30 秒の倍数で定義します。

バケット

収集するサンプル数を定義します。

[パフォーマンス キューブに追加]チェック ボックス

このエントリのパフォーマンス キューブ データを収集するかどうかを指定します。

[保守ウィンドウ]ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

7. [保存]をクリックします。
[履歴モニタ]設定が保存されます。
8. [テンプレートの保存]をクリックします。
履歴モニタがポリシーにロードされます。

プロセス グループ モニタの作成

エージェントがプロセスのグループを定義し、そのグループの変更をモニタできるようにするプロセスグループ モニタを定義します。プロセスグループが変化すると、エージェントはトラップを送信します。

次の手順に従ってください:

1. [リソース]タブをクリックして[設定]ペインを開き、[モニタリング テンプレート]および適切なサブカテゴリを展開します。
[テンプレートリスト]ページが表示されます。
2. [テンプレートリスト]内のテンプレートを選択します。
テンプレートの[サマリ]ページが表示されます。

3. [モニタ]タブをクリックします。
[サマリ]ページが開き、ポリシーによって管理されるモニタのリストが表示されます。
4. [プロセスグループ]をクリックします。
[履歴モニタ]ページが表示されます。
5. [プロセスグループ モニタ]ツールバーの[+] (新規)をクリックします。
[プロセスグループ詳細: 新規]ダイアログ ボックスが表示されます。
6. 以下のプロセス設定を行います。

インデックス

使用するテーブル インデックスを定義します。

プラットフォーム

プラットフォームを指定します。

説明

オプションの説明を定義します。

プロセス名

プロセス名を定義します。これは、名前による一致処理、に使用される正規表現(オプションの設定に依存します)です。

間隔

モニタの評価間隔を 30 秒の倍数で定義します。

ユーザ名

任意のプロセス名正規表現に加えて、モニタするユーザ名を定義します。

グループ名

任意のプロセス名正規表現に加えて、モニタするグループ名を定義します。

重大度

グループ変更に関する、モニタの重要性を指定します。

[保守ウィンドウ]ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

[オプション設定]ページで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

7. [保存]をクリックします。

[プロセス グループ モニタ]設定が保存されます。

8. [テンプレートの保存]をクリックします。

プロセス グループ モニタがポリシーにロードされます。

MIB 拡張の定義

MIB 拡張を定義すると、ローカル ファイル操作では利用できない機能が利用できるようになります。ポリシー設定機能により、フィールド名、および、オブジェクトタイプなどのキー プロパティのリストが提供されます。

ポリシーまたはモニタリング テンプレートを設定する場合に[MIB 拡張] タブをクリックすると、以下のオブジェクトが追加できます。

- MIB 拡張
- Windows パフォーマンス
- Windows レジストリ

注: テンプレートまたはポリシーに MIB 拡張を追加するには、「[テンプレートまたはポリシーへの MIB 拡張の追加 \(P. 367\)](#)」を参照します。テンプレート内の MIB 拡張は、モニタされたシステムに MIB 拡張を直接適用することを目的としてサポートされています。ポリシー内で使用するための MIB 拡張は、ポリシー内に直接作成する必要があります。

テンプレートまたはポリシーへの MIB 拡張の追加

ポリシー設定機能を使用して、テンプレートまたはポリシー用の MIB 拡張を定義します。

次の手順に従ってください:

1. [リソース]タブをクリックして[設定]ペインを開き、[モニタリング テンプレート]または[ポリシー]を展開します。
2. [テンプレートリスト]または[利用可能ポリシー]ページから、テンプレートまたはポリシーの名前をクリックします。
[サマリ]ページが表示されます。
3. [MIB 拡張]タブをクリックします。
[MIB 拡張]ページが表示されます。
4. 以下のコントロールを使用して、MIB 拡張属性を定義し、[追加]をクリックします。

インデックス

属性リーフ番号を定義します。

タイプ

属性タイプを指定します。

拡張コマンド

実行するスクリプトまたはバイナリのフル パスまたは名前 (パラメータを含む) を定義します。

アクセス権

属性アクセス権限を指定します。

5. [Windows パフォーマンス]タブをクリックします。
[Windows パフォーマンス]ペインが表示されます。
6. 以下のコントロールを使用して、Windows パフォーマンス属性を定義し、[追加]をクリックします。

インデックス

属性リーフ番号を定義します。

タイプ

属性タイプを指定します。

オブジェクト

パフォーマンスレジストリ オブジェクトを指定します。

カウンタ

パフォーマンスレジストリ カウンタを指定します。

インスタンス

パフォーマンスレジストリ インスタンスを定義します。

7. [Windows レジストリ] タブをクリックします。
[Windows レジストリ] ペインが表示されます。
8. 以下のコントロールを使用して、Windows レジストリ 属性を定義し、[追加] をクリックします。

インデックス

属性リーフ番号を定義します。

タイプ

属性タイプを指定します。

キー

HKEY_LOCAL_MACHINE にレジストリ キーを定義します。

値

属性値を定義します。

注: 詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

9. [テンプレートまたはポリシーの保存] または Policy をクリックします。
設定が保存されます。

テンプレートまたはポリシーからのモニタの削除

テンプレートまたはポリシーからモニタを削除することができます。

次の手順に従ってください:

1. [リソース] タブをクリックして [設定] ペインを開き、[モニタリング テンプレート] または [ポリシー] を展開します。
2. [テンプレートリスト] または [利用可能ポリシー] ページから、テンプレートまたはポリシーの名前をクリックします。
[サマリ] ページが表示されます。

3. [モニタ]タブをクリックします。
[サマリ]ページが開き、ポリシーによって管理されるモニタのリストが表示されます。
 4. 適切なモニタ タブをクリックし、削除するモニタを選択します。
 5. [アクション]をクリックし、[削除]を選択します。
警告メッセージが表示されます。
 6. [OK]をクリックして削除を確定します。
 7. (オプション) 追加するモニタごとに同じ手順を繰り返します。
 8. [ポリシーの保存]をクリックします。
モニタがポリシーから削除されます。
- 注:** サーバまたはサーバグループによって使用されているテンプレート、またはテンプレートを持つポリシーは、削除できません。

ポリシーとテンプレートのサーバへの適用と設定の確認

テンプレートを作成した後、企業全体のサーバまたはサーバグループに、テンプレートを持つポリシーを直接適用できます。

次の手順に従ってください:

1. [利用可能ポリシー]テーブル内のポリシーを選択するか、または[テンプレートリスト]からテンプレートを選択します。
ポリシーまたはテンプレートの[サマリ]ページが表示されます。
2. [管理対象マシン]タブを選択します。
管理対象マシンのリストが表示されます。
3. [アクション]をクリックし、[適用]を選択します。
ポリシーを適用するシステムを選択するためのタブが表示されます。[このポリシー/テンプレートを実行しているマシンを更新]タブでは、すでにポリシーまたはテンプレートを実行しているシステムにポリシーを適用できます。[このポリシー/テンプレートを実行していないマシンに適用]タブでは、システムにポリシーまたはテンプレートを適用できます。

4. (オプション) [このポリシー/テンプレートを実行しているマシンを更新] タブから、以下のいずれかを実行します。
 - 現在ポリシーまたはテンプレートを実行しているすべてのシステム上でポリシーまたはテンプレートを展開するには、[このポリシー/テンプレートを]を使用してすべてのマシンを更新]を選択します。このオプションは、グローバルに適用する設定の変更を行った場合に便利です。
 - 以下の条件のいずれかを満たすシステムのみを更新するには、[選択したマシン グループを更新]を選択します。
 - 期限切れバージョンのポリシーまたはテンプレートを実行している。
 - 例外が発生した。
 - 現在のバージョンのポリシーを実行している。これらのオプションのいずれかを選択します。例外は、適用されるポリシーまたはテンプレート内に示されていないエージェントにユーザがポイント設定変更を適用すると発生します。
 - [詳細]を選択し、ポリシーまたはテンプレートを再適用するシステムを [マシンを選択] ペインで手動で選択します。
5. (オプション) [このポリシー/テンプレートを実行していないマシンに適用] タブから、ポリシーまたはテンプレートを適用するシステムを選択します。
6. [ポリシーの適用]または[テンプレートの適用]をクリックします。
適用が開始されます。
7. サーバが予期したように動作するかどうかを確認します。必要な場合、更新されたポリシーとテンプレートを更新および適用できます。

(オプション)サーバのベース ポリシーおよびテンプレートの管理

1 つまたは複数のサーバ用のテンプレートおよびベース ポリシーを管理します。現在のベース ポリシーの置換、テンプレートの追加、テンプレートの削除などを実行できます。

次の手順に従ってください:

1. [リソース]タブをクリックし、[エクスプローラ]ペインを開き、ポリシー設定を変更するサーバを選択します。

サーバのリソース ページが表示されます。

2. [モニタリング ソフトウェア]-[ポリシー]を選択します。

ポリシー、およびサーバに適用されているテンプレートのリストが表示されます。

3. このサーバの現在のベース ポリシーを別の使用可能なベース ポリシーで置き換えるには、 (ポリシーの変更)をクリックします。

[ポリシーの変更]ダイアログ ボックスが表示され、利用可能なベース ポリシーがすべて示されます。

4. 適切なポリシーを選択して[適用]をクリックします。

選択されたサーバに新しいベース ポリシーが適用されました。ポリシーのステータスは[配信が要求されました]から[配信]、[設定完了]に変更されます。

5. 選択されたサーバの設定に対してテンプレートを追加または削除するには、 (テンプレートの変更)をクリックします。

[テンプレートの変更]ダイアログ ボックスが表示され、利用可能なテンプレートが左ペインに、適用されているテンプレートが右ペインに示されます。

6. 追加または削除するテンプレートを選択し、矢印を使用して割り当てを行い、[適用]をクリックします。

テンプレートの新しいセットが設定に適用されました。テンプレートのステータスは[配信が要求されました]から[配信]、[設定完了]に変更されます。

新しい設定が適用されました。

複数のサーバをグループとして管理することもできます。

次の手順に従ってください:

1. サーバのグループを指定するサービスをデータセンター レベルで作成します。
新しいサービスが[エクスプローラ]ペインに表示されます。
2. サービスを選択します。
サービス ページが表示されます。
3. [モニタリング ソフトウェア]-[ポリシー]を選択します。
ポリシー、およびサーバに適用されているテンプレートのリストが表示されます。
以降の手順は単一のサーバの場合と同じです。
4. 設定を完成します。

(オプション)ポリシーまたはテンプレートの更新

必要に応じて、ポリシーやテンプレートに対してモニタを追加または削除し、ポリシーやテンプレートを更新することができます。更新手順は作成プロセスに似ています。

次の手順に従ってください:

1. サーバワークロードに固有のモニタを追加するか削除します。テンプレートまたはポリシーにモニタを追加する方法については、「[テンプレートまたはポリシーへのモニタの追加](#) (P. 353)」を参照してください。ポリシーからモニタを削除するには、「[テンプレートまたはポリシーからのモニタの削除](#) (P. 368)」を参照してください。
2. [MIB 拡張を定義](#) (P. 366)します。
3. [SystemEDGE ポリシー制御設定を定義](#) (P. 340)します。
ポリシーまたはテンプレートが更新されます。

(オプション)サーバへのポリシー/テンプレート更新の適用と更新の確認

テンプレートを更新した後、企業全体のサーバまたはサーバグループにテンプレート更新を直接適用します。

次の手順に従ってください:

1. [リソース]タブをクリックして[設定]ペインを開き、[モニタリング テンプレート]を展開して[SystemEDGE]を選択します。
[サマリ]ページには SystemEDGE モニタリング テンプレートのリストが表示されます。
2. テンプレート名を選択します。
[サマリ]ページが開き、テンプレート情報が示されます。
3. [アクション]をクリックし、[適用]を選択します。
モニタリング テンプレートを適用するマシンを選択するためのタブが表示されます。[このテンプレートを実行しているマシンを更新]タブでは、すでにテンプレートを使用しているマシンにモニタリング テンプレートを適用できます。[このテンプレートを実行していないマシンに適用]タブでは、テンプレートをまったく使用していないマシンにモニタリング テンプレートを適用できます。
4. (オプション)[既存のマシン]の下での[このテンプレートを実行しているマシンを更新]タブ オプションでマシンを選択します。
5. (オプション)[選択したマシン]の下で、テンプレートが再適用されるマシンを選択します。
6. (オプション)テンプレートを適用するマシンを[このテンプレートを実行していないマシンに適用]タブから選択します。

7. [適用]をクリックします。

テンプレート アプリケーションが起動され、[ステータスの表示]リンクが表示されます。

8. [ステータスの表示]リンクをクリックして、**SystemEDGE** モニタリング テンプレート更新がサーバに適用されていることを確認します。

SystemEDGE モニタリング テンプレート更新が適用されたサーバのリストを表示するページが開きます。

階層型テンプレートの更新がサーバまたはサーバグループに正常に適用されました。

9. サーバが予期したように動作するかどうかを確認します。必要な場合、更新されたポリシーとテンプレートを再度更新および適用できます。

付録 A: FIPS 140-2 の暗号化

このセクションには、以下のトピックが含まれています。

[FIPS の概要](#) (P. 375)

FIPS の概要

連邦情報処理標準(FIPS) 140-2 は、製品が暗号化に使用すべき暗号のライブラリおよびアルゴリズムのセキュリティ標準です。FIPS 140-2 の暗号化は、CA 製品のコンポーネント間、および CA 製品とサードパーティ製品間におけるすべての機密データの通信に影響を与えます。FIPS 140-2 は、取り扱い注意ではあるが機密扱いではないデータを保護するセキュリティシステムの中で暗号アルゴリズムを使用するための要件を規定しています。

CA Virtual Assurance では、米国政府が採用している高度暗号化標準(AES)を使用します。CA Virtual Assurance には、RSA Crypto-J v3.5 および Crypto-C ME v2.0 暗号ライブラリが組み込まれています。これらは、FIPS 140-2 の暗号モジュール セキュリティ要件を満たしていることが確認されています。

付録 B: トラブルシューティング

このセクションには、以下のトピックが含まれています。

[Solaris ゾーン環境でのポーリング間隔設定の調整 \(P. 378\)](#)

[属性にゼロの値が表示される \(P. 378\)](#)

[ブラウザにイベントの連続するスペースが表示されない \(P. 378\)](#)

[CA NSM が Windows でトラップの受信に失敗する \(P. 379\)](#)

[Cisco UCS フォルダが UI 内に表示されない \(P. 379\)](#)

[DB トランザクション ログ サイズが予期せずに増加する \(P. 380\)](#)

[廃止された Solaris ゾーン AIM 属性で常に N/A またはゼロが表示される \(P. 380\)](#)

[dpmvc virtualswitch コマンドでの空のタスク ID \(P. 381\)](#)

[ローカル モニタとリモート モニタに同じ値が表示されない \(P. 381\)](#)

[Solaris Lists SPARC および x86 システムへのリモートでの展開 \(P. 382\)](#)

[PMM が AIM のポーリングを停止する \(P. 383\)](#)

[vCenter Server を削除すると、別の管理対象 vCenter Server のオブジェクトが非表示になる \(P. 384\)](#)

[vCenter Server のパスワードを変更するとデータ収集に失敗する \(P. 384\)](#)

[モニタされたシステムがダウンしている場合は Solaris ゾーン AIM がリセットされる \(P. 385\)](#)

[Microsoft SQL サーバに接続できない \(P. 385\)](#)

[SystemEDGE のアップグレード \(P. 385\)](#)

[プロビジョニング画面およびポリシー画面でユーザ インターフェースが応答しません \(P. 386\)](#)

[vCenter Server AIM 属性にゼロが表示される \(P. 386\)](#)

[vCenter Server の接続に失敗した \(P. 387\)](#)

[vCenter AIM インスタンスのステータス アイコンに「無効」が表示される \(P. 390\)](#)

[vCenter AIM インスタンスのステータス アイコンに「ディスクバリが進行中」が表示される \(P. 391\)](#)

[vCenter AIM インスタンスのステータス アイコンに「エラー」が表示される \(P. 391\)](#)

[vCenter AIM インスタンスのステータス アイコンに「複数インスタンス」が表示される \(P. 393\)](#)

[vCenter AIM インスタンスのステータス アイコンに「警告」が表示される \(P. 394\)](#)

[VM 使用率の値が電源オフ後にすぐに更新されない \(P. 394\)](#)

[アップグレード後の空白の \[クエリ結果\] タブ \(P. 395\)](#)

Solaris ゾーン環境でのポーリング間隔設定の調整

症状:

Solaris ゾーン環境でポーリング間隔の設定を調整する方法がわかりません。

解決方法:

システムとゾーンの数が増加する場合は、Solaris ゾーン AIM のポーリング間隔を増加させます。たとえば、ホストとゾーンの数が増える場合は、デフォルトのポーリング間隔を 240 に設定します。

属性にゼロの値が表示される

症状:

属性にゼロの値が表示される

解決方法:

値が 1 よりも小さい場合、SystemEDGE は値を切り捨ててゼロにします。

注: zoneAimStatHostDiskSvc MIB 属性には、常にゼロの値が表示されます。

ブラウザにイベントの連続するスペースが表示されない

症状:

ブラウザにイベント説明の複数の連続するスペース文字が表示されません。

解決方法:

追加のスペースは HTML 仕様に準拠して切り詰められるので、ブラウザには複数の連続するスペースが表示されません。ブラウザからイベントを切り取ってルールに貼り付ける場合はイベント説明が異なる場合があるため、注意を要します。

CA NSM が Windows でトラップの受信に失敗する

症状:

CA Virtual Assurance から数日間トラップを受信した後で、NSM Event Console は [イベントコンソール ログ] でのトラップの表示を停止します。問題は Windows SNMP トラップ サービスにあります。WinSNMP アプリケーションは、Windows Server 2003 ベースコンピュータ上でサードパーティのセキュリティスキャンソフトウェアプログラムを実行すると、応答を停止します。

解決方法:

この問題を解決するには、Microsoft Support Web サイト <http://support.microsoft.com/kb/931565> で KB の記事を参照してください。

Cisco UCS フォルダが UI 内に表示されない

症状:

Cisco UCS サービスの製品インストールを設定した後で、Cisco UCS フォルダがユーザ インターフェースに表示されません。

解決方法:

UCS AIM が設定されているサーバで[サービス]を開いて SystemEDGE が実行されていることを確認します。SystemEDGE サービスが停止している場合は、それを再起動します。nodecfgutil.exe を開始して UCS Manager ノードのアクセス情報を確認します。MIB ブラウザを使用して UCS Manager からのデータポーリングを確認します。UCS アクセス情報が入力されていない場合は、追加情報を sysedge ログで確認します。

DB トランザクション ログ サイズが予期せず増加する

症状:

多数の管理対象オブジェクト、設定変更およびメトリック データ収集アクティビティがあるデータ センターでは、管理データベースおよびパフォーマンス データベースのログが予期せず増加する場合があります。この問題は制限のあるリソースを使用する環境ではディスク領域を低下させる原因となる場合があります。

解決方法:

この問題を解決するには、Microsoft Support Web サイト <http://support.microsoft.com/kb/873235> で KB の記事を参照してください。

トランザクション ログ ファイル、aom2.ldf および dpm.ldf は、デフォルト Microsoft SQL Server インストールのディレクトリ C:\Program Files\Microsoft SQL Server\...\MSSQL\Data にあります。

注: データベース ログ ファイルのサイズが縮小される場合は、Apache のサービスを再起動してパフォーマンスを改善してください。

廃止された Solaris ゾーン AIM 属性で常に N/A またはゼロが表示される

症状:

Solaris ゾーン AIM MIB のいくつかの値に常に N/A またはゼロが表示されます。

解決方法:

Solaris ゾーン AIM のこれらの MIB 属性は廃止され、下位互換性のために残されています。廃止された MIB 属性は以下のとおりです。

- zoneAimStatHostDiskMode
- zoneAimStatProcessorSetContainerList
- zoneAimStatProcessorSetResourcepoolId
- zoneAimStatProcessorSetResourcePoolIdList
- zoneAimStatProcessorSetResourcepoolName
- zoneAimStatProjectFSSEnabled
- zoneAimStatResourcePoolContainerList

dpmvc virtualswitch コマンドでの空のタスク ID

症状:

dpmvc virtualswitch コマンドを実行すると、空のタスク ID が表示されます。

解決方法:

この操作は非同期で実行されず、結果はただちに返されます。ただし、PMM はこの操作をタスク化された操作として扱います。そのため、応答にはタスク ID が含まれますが、それは常に空の文字列("")です。

たとえば CLI から以下のコマンドを実行すると、空のタスク ID が表示されます。

```
dpmvc virtualswitch -vs_add -vc_server MYVC5 -switch_name XYZ  
-esx_host_name MYESX -ws_user admin -ws_password ca_admin
```

CLI の出力

```
...  
SC URL: https://VASManager/aip/sc  
VC URL: https://VASManager:443/aip/vc  
Task ID:  
Command execution successful
```

dpmvc faulttolerance や dpmvc distributedswitch などのほかのコマンドは非同期に実行され、タスク ID が表示されます。

ローカル モニタとリモート モニタに同じ値が表示されない

症状:

ローカル モニタとリモート モニタに、同じ属性の同じ値が同時に表示されません。

解決方法:

ローカルおよびリモートのモニタリングをシームレスに行うために、モニタ対象オブジェクトの名前が同一に選択されています。ただし、使用される API は異なり、別の値を返す可能性があります。

リモート マシン上の SystemEDGE は、サーバ上で RM AIM から独立して実行され、それらのポーリング スケジューラの開始ポイントは同期できません。

モニタされるメトリックは非常に不安定です。たとえば、2 つのサンプルが異なる可能性が高くなります。

Solaris Lists SPARC および x86 システムへのリモートでの展開

症状:

Deployment UI にリスト表示されたコンピュータは、通常展開している選択済みオペレーティング環境にフィルタされます。ただし、以下の状況の場合は、リストされている選択済みオペレーティング環境以外のコンピュータを表示できます。

- Solaris x86 または Solaris SPARC サーバのいずれかに展開した場合、リスト表示されたサーバは、ターゲット オペレーティング環境として Solaris x86 または Solaris SPARC を選択したかどうかにかかわらず、すべての Solaris アーキテクチャ向けです。
- 分類されていない任意のコンピュータに展開した場合。

解決方法:

展開が正常に行われるように、ターゲットコンピュータが選択済みのエージェントアーキテクチャと一致することを確認します。リスト表示されたすべてのコンピュータを選択して続行すると、展開は一致するアーキテクチャでは成功し、一致しないアーキテクチャでは失敗します。

PMM が AIM のポーリングを停止する

症状:

PMM が AIM (AIM の全インスタンス) のポーリングを停止し、CAAM6504 メッセージを送信します。また、UI の[管理]タブ、AIM パネルでは、影響のあるインスタンスが「重大」と表示されます。

ポーリングは、複数のインスタンスをモニタする Cisco UCS、Microsoft クラスタ、IBM LPAR、および Solaris ゾーンの AIM について停止されます。

その理由は、PMM が AIM のポーリングを継続できないためです。そのような状態で AIM を再起動しても、影響のあるインスタンスのデータは MIB に入力されません。PMM はこれ以上データを取得できないと判断し、管理データベースから削除します。

解決方法:

- インスタンスが準備完了状態でない理由を確認します。以下の事項をチェックできます。
 - 無効または期限切れの認証情報
 - ネットワーク接続
 - サーバに関するハードウェアの問題
- 対応するプラットフォームの[管理]タブでインスタンスを無効にします (Cisco UCS では利用できません)。
- AIM からインスタンスを削除します。

vCenter Server を削除すると、別の管理対象 vCenter Server のオブジェクトが非表示になる

症状:

vCenter Server を管理から削除すると、別の管理対象 vCenter Server のオブジェクトが予期せず非表示になります。

解決方法:

製品管理の問題を回避するには、別の vCenter Server を管理している VM に vCenter AIM をインストールしないでください。その VM に関連付けられている vCenter のモニタリングと管理を CA Virtual Assurance から削除すると、AIM を実行している VM システムを含め、vCenter に関連付けられているオブジェクトが削除されます。

vCenter Server のパスワードを変更するとデータ収集に失敗する

症状:

VMware vCenter Server と通信するために CA Virtual Assurance が使用しているユーザの VMware vCenter Server パスワードをリセットした後で、データ収集が機能しません。

解決方法:

新しいパスワードで vCenter AIM 設定を更新します。パスワードは、ユーザインターフェースの[管理]タブ、または vCenter AIM が実行されているサーバの NodeCfgUtil から更新できます。

モニタされたシステムがダウンしている場合は Solaris ゾーン AIM がリセットされる

症状:

モニタされたシステムがダウンしている場合は Solaris ゾーン AIM がリセットされます。

解決方法:

モニタされたシステムのうちの 1 つがダウンしている間に、AIM をリセットした場合、AIM は各ポーリング間隔でそのシステムをポーリングします。AIM はシステムが再度稼働するまで、プロパティを更新しません。

Microsoft SQL サーバに接続できない

症状:

Microsoft SQL Server 2005 および 2008 (評価版) への認証情報を認証する試行は、製品インストール中に失敗します。エラー メッセージ[MSSQL への接続を確立できませんでした]が表示されます。

解決方法:

この問題は、TCP/IP が評価版ではデフォルトで無効になるために発生します。TCP/IP を有効にします。

SystemEDGE のアップグレード

症状:

SystemEDGE を 5.6.0 にアップグレードしたとき、旧 CA Virtual Assurance リリースの AIM が実行できません。

解決方法:

Advanced Encryption および全 AIM を CA Virtual Assurance 12.6 レベルにアップグレードします。SystemEDGE 5.6.0 は、旧 CA Virtual Assurance リリースの AIM をロードできません。

プロビジョニング画面およびポリシー画面でユーザ インターフェースが応答しません

症状:

プロビジョニング ページまたはポリシー ページを表示しているときにデータベース サーバが再起動すると、ユーザ インターフェースは空白になるかまたは反応がありません。

解決方法:

CA Virtual Assurance ユーザ インターフェースからログアウトして再度ログインします。

vCenter Server AIM 属性にゼロが表示される

症状:

vCenter Server 属性にゼロが表示されます。

解決方法:

以下のオブジェクト値は、vCenter Server AIM がローカル vCenter Server インスタンスにインストールされている場合にのみ取得できます。AIM がリモートである場合は、これらのパラメータにゼロ (0) が表示されます。

- vmvcAimStatServerCPUUsage [1.3.6.1.4.1.546.16.52.2.2.12.0]
- vmvcAimStatServerMemUsage [1.3.6.1.4.1.546.16.52.2.2.17.0]
- vmvcAimStatServerTotalPhysMem [1.3.6.1.4.1.546.16.52.2.2.18.0]
- vmvcAimStatServerUsedPhysMem [1.3.6.1.4.1.546.16.52.2.2.19.0]

vCenter Server の接続に失敗した

症状:

[管理]-[設定]で新しい vCenter Server 接続を追加した後、vCenter Server への接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- vCenter Server の接続に使用されたデータ(サーバ名、ユーザ、パスワード、プロトコル、ポート)が今でも有効かどうかを確認します。必要な場合は、接続データを更新します。
- vCenter Server システムが実行されており、アクセス可能であるかどうかを確認します。
- vCenter Server システム上で VMware 管理サービスが正常に動作しているかどうかを確認します。

vCenter Server の接続データを更新する方法

1. 失敗した接続に関連付けられた  (追加) または  (編集) をクリックします。

[新しい vCenter Server] または [vCenter Server の編集] ダイアログ ボックスが表示されます。

2. 有効なサーバ名、ユーザ、パスワード、プロトコル、およびポートを追加します。[管理ステータス] を有効にして [OK] をクリックします。

接続データが更新されます。

3. 右上の  (検証) をクリックして新しい設定を検証します。

vCenter Server への接続を確立できない場合は、次の手順に進みます。

vCenter Server システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Virtual Assurance マネージャシステムでコマンドプロンプトを開き、以下のコマンドを実行します。

```
nslookup <vCenter Server Name>  
ping <IP Address of vCenter Server>
```

2. vCenter Server に有効な DNS エントリおよび IP アドレスがあることをコマンドの出力で確認します。

vCenter Server が DNS 内にはない場合は、CA Virtual Assurance マネージャシステムの Windows ホストファイルに vCenter Server を追加します。手順 3 に進みます。

vCenter Server が DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%\system32\drivers\etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

```
ipaddress <vCenter Server Name>
```

正しい IP アドレスと vCenter Server の名前を入力します。例：

```
192.168.50.50 myvCenter
```

4. 右上角の  (検証) をクリックします。

vCenter Server の認証情報と接続データが正しく、vCenter Server に対して ping を実行できる場合は、接続がまだ失敗する可能性があります。この場合は、vCenter Server に問題がある可能性があります。vCenter Server への接続を確立できない場合は、次の手順に進みます。

vCenter Server システム上で VMware 管理サービスが正常に動作しているかどうかを確認する方法

1. vCenter Server システムにアクセスする方法を vSphere の管理者に問い合わせます。
2. vCenter Server システムにログインし、[スタート]メニューから[管理ツール]-[サービス]を開きます。
[サービス]ウィンドウが表示されます。
3. *VMware VirtualCenter Server* サービスを選択します。サービスを開始または再開します。
4. CA Virtual Assurance ユーザ インターフェースに移動し、マネージャシステムの[vCenter Server]ペインの右上角にある  (検証)をクリックします。

CA Virtual Assurance によって vCenter Server の接続が検証されます。

vCenter Server への接続が失敗する場合は、このシナリオの要件に従って集めたデータがまだ有効であることを確認してください。

vSphere の管理者または VMware のサポート担当者と協力して、vCenter Server の接続の問題を解決します。

vCenter AIM インスタンスのステータス アイコンに「無効」が表示される

症状:

CA Virtual Assurance がネットワーク内の vCenter AIM インスタンスを検出した後、いくつかのインスタンスのステータス アイコン  (無効)が表示されます。この vCenter AIM インスタンスは管理されていません。

このステータスは、CA Virtual Assurance が以下の関係を持つ vCenter AIM を検出した場合に表示されます。

- CA Virtual Assurance マネージャへの接続が有効であるが管理対象外の状態である vCenter Server 用に vCenter AIM が設定されている。
- [vCenter Server] ペインで設定されていない vCenter Server に AIM が接続されている。

解決方法:

AIM インスタンスのステータスを「準備完了」に変更するには、以下のいずれかを実行します。

- 欠落している vCenter Server から CA Virtual Assurance マネージャへの接続を追加します。
- 既存の vCenter Server 接続を編集し、その管理ステータスを「有効」に変更します。

vCenter AIM インスタンスのステータス アイコンに「ディスクバリが進行中」が表示される

症状:

[管理]-[設定]で vCenter Server に対して vCenter Server AIM インスタンスを追加した後、ステータス アイコンに  (ディスクバリが進行中)が表示されます。

解決方法:

vSphere 環境のディスクバリ プロセスが完了するまで待機します。ディスクバリ 期間中は、vSphere 内の仮想および物理リソースに関連する管理対象オブジェクトの量に依存します。アイコンの上にカーソルを置くと、未処理のディスクバリ要求の数を示すツールヒントが表示されます。ディスクバリ ジョブが完了すると、CA Virtual Assurance は vCenter Server フォルダをリソース ツリーに追加します。これで、vSphere とその仮想インフラストラクチャ全体の管理を開始できます。

vCenter AIM インスタンスのステータス アイコンに「エラー」が表示される

症状:

[管理]-[設定]で vCenter Server に対して vCenter Server AIM インスタンスを追加した後、ステータス アイコンに  (エラー)が表示されます。AIM に接続できません。

解決方法:

vCenter AIM への接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- vCenter AIM サーバがアクセス可能であるかどうかを確認します。
- SystemEDGE が実行されているかどうかを確認します。必要な場合は、SystemEDGE を開始または再開します。

vCenter AIM サーバシステムがアクセス可能かどうかを確認する方法

1. CA Virtual Assurance マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

```
ping servername
```

2. vCenter AIM サーバに有効な DNS エントリおよび IP アドレスがあることをコマンドの出力で確認します。

vCenter AIM サーバが DNS 内にはない場合は、CA Virtual Assurance マネージャ システムの Windows ホスト ファイルに vCenter AIM サーバを追加します。手順 3 に進みます。

vCenter Server が DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%\system32\drivers\etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

```
ipaddress servername
```

正しい IP アドレスと vCenter AIM サーバの名前を入力します。例：

```
192.168.50.51 myvCenterAIM
```

4. [vCenter AIM サーバ] ペインの右上角の  (検証) をクリックします。

エラー ステータスが変わらない場合は、次の手順に進みます。

SystemEDGE が実行されているかどうかを確認する方法

1. vCenter AIM サーバにログインし、%windir%\Program Files\CA\SystemEdge\bin ディレクトリから sysedge.cpl を実行します。

SystemEDGE コントロール パネルが開き、SystemEDGE の実行状態が表示されます。

2. SystemEDGE を開始または再開します。

SystemEDGE が実行されていることが SystemEDGE コントロール パネルに表示されるまで待機します。

3. CA Virtual Assurance ユーザ インターフェースに移動し、マネージャ システムの[vCenter AIM サーバ] ペインの右上角にある  (検証) をクリックします。

CA Virtual Assurance によって vCenter AIM サーバの接続が検証されます。

エラー ステータスが変わらない場合は、このシナリオの要件に従って集めたデータがまだ有効であることを確認してください。

vCenter AIM インスタンスのステータス アイコンに「複数インスタンス」が表示される

症状:

[管理]-[設定]で vCenter Server に対して vCenter Server AIM インスタンスを追加した後、ステータス アイコンに  (複数の AIM がこのインスタンスを管理している)が表示されます。

解決方法:

CA Virtual Assurance マネージャが 1 つの vCenter AIM インスタンスのみを使用して各 vCenter Server を管理していることを確認します。CA Virtual Assurance マネージャが複数の AIM インスタンスを使用して vCenter Server を管理している場合は、管理上の問題が発生します。CA Virtual Assurance は関連付けられた vCenter Server のモニタリングを停止します。

どの AIM インスタンスを使用して vCenter Server を管理するかを決定し、[vCenter AIM サーバ] ペインから他のインスタンスを削除してください。

次の手順に従ってください:

1. 削除する AIM インスタンスを選択し、 (削除)をクリックします。
[項目の削除]ダイアログ ボックスが表示されます。
2. [はい]をクリックします。

マネージャと AIM インスタンスの間で一意的な関係が確立するまで、他の複数のインスタンスに対して上記の手順を繰り返します。

vCenter AIM インスタンスのステータス アイコンに「警告」が表示される

症状:

[管理]-[設定]で vCenter Server に対して vCenter Server AIM インスタンスを追加した後、ステータス アイコンに  (警告)が表示されます。AIM 上の他のインスタンスがまだエラー状態です。

解決方法:

関連付けられたインスタンスに、特定の必要なアクションはありません。同じ AIM 上の他のインスタンスがエラー ステータスであることを通知する警告が表示されます。他のインスタンスの問題が解決されると、警告が表示されなくなります。AIM の 1 つ以上のインスタンスがエラー状態であれば、AIM の他のすべてのインスタンスが警告状態として表示されます。

VM 使用率の値が電源オフ後にすぐに更新されない

症状:

VM 使用率の値が電源オフ後にすぐに更新されません。

解決方法:

VM の電源が切られた後で、使用率の値は次の正常なポーリングまで 0 にドロップしません。ポーリングには最大 5 分かかります。これはデフォルトのデータ収集および記録間隔です。

アップグレード後の空白の[クエリ結果]タブ

症状:

アップグレード後、リモート モニタリング クエリ結果に空白の値が表示されます。

解決方法:

システムの追加時、RM PMM には、FQDN (Fully Qualified Domain Name、完全修飾ドメイン名) 表記法に準拠しているリモート システム名が必要です。ただし、RM AIM では既存のシステムが FQDN でない名前のまま残されます。この名前の不一致が原因となって、空白のクエリ結果が表示されます。この名前の不一致は、以下のように修正できます。

アップグレード前の変換

- リフレッシュ UI にログインし、リモート モニタリングから FQDN でないシステムをすべて削除します。

関連付けられたシステム、クエリ、インスタンス、およびモニタが、両方のマネージャ(データベース)、および RM AIM プラグインを持つ SystemEDGE エージェントからすべて削除されます。

- FQDN 表記法を使用してこれらのシステムを再度追加し、同じ設定セットを指定して、関連付けられたクエリ、インスタンス、およびモニタを再作成します。
- アップグレードを実行します。

アップグレード後の変換

- SystemEDGE エージェント マシンにログインし、Refresh RM AIM プラグインを実行します。
- 現在のリモート モニタリング設定が含まれる rmonwbem.cf ファイルをデータディレクトリパスで検索し、このファイルのコピーを作成します。たとえば、rmonwbem-upgrade.cf として保存します。
- リフレッシュ UI にログインし、リモート モニタリングから FQDN でないシステムをすべて削除します。

関連付けられたシステム、クエリ、インスタンス、およびモニタが、両方のマネージャ(データベース)、および RM AIM エージェント マシンからすべて削除されます。

- ここでアップグレードを実行します。エージェント マシンで、`rmonwbem-upgrade.cf` を入力ファイルとして指定して `rmonwatch add` コマンドを実行します。この処理により、すべてのシステムおよび関連付けられたクエリ、インスタンス、およびモニタが **FQDN** 表記法で再度追加されます。

注: アップグレード後の変換方法には、システムを自動的に再度追加し、UI からシステムを設定できる長所があります。

アップグレード変換の後には、クエリ結果に値が表示されます。

用語集

Hyper-V は、Windows Server 2008 R2 用の Microsoft ハイパーバイザベースのサーバ仮想化テクノロジーです。複数の独立した仮想マシン (VM) が 1 台の物理サーバ上で実行され、Windows や Linux などの複数の異なるオペレーティングシステムを実行できます。

Application Insight Module、AIM

SystemEDGE エージェントには、初期化時にオプションの *Application Insight Module (AIM)* をロードできるプラグインアーキテクチャが備わっています。AIM は SystemEDGE エージェントの機能拡張です。たとえば、vCenter AIM により、SystemEDGE は VMware vCenter Server を介して vSphere 環境を管理できます。

AutoShell

AutoShell を使用すると、複雑な反復タスクや管理タスクを自動化できる、コマンドラインとスクリプトの環境が得られます。*AutoShell* は、プログラミング言語ではなく、スクリプト言語とコマンドラインシェルを組み合わせたものです。

AutoShell は、標準化されたスクリプト言語 ECMA-Script (JavaScript) をベースにしています。JavaScript は一般に Web ページで使われるスクリプト言語として知られていますが、必ずしもブラウザで実行される必要はありません。このスタンドアロンのスクリプト言語を使用して、オブジェクト指向、XML、および正規表現処理に対するサポートを実装できます。*AutoShell* では、Mozilla Spidermonkey JavaScript インタプリタの事前定義済みバージョンを使用します。これにより、Mozilla Firefox Web ブラウザにも JavaScript 機能が提供されます。

Autoshell Loadable Module、ALM

Autoshell Loadable Module (ALM) は *AutoShell* コアの拡張です。インストール時に選択された CA Virtual Assurance のコンポーネントに応じて、必要な ALM が自動的にインストールされます。たとえば、ALM により、LPAR、Solaris ゴースト、vCenter Server などのプラットフォームを *AutoShell* を通じて管理できます。

Cisco Nexus 1000V スイッチ

Cisco Nexus 1000V スイッチは、VMware vSphere 環境で実行できる分散仮想スイッチです。*Cisco Nexus 1000V* スイッチは、仮想イーサネット モジュール (VEM) および仮想スーパーバイザ モジュール (VSM) から構成されます。VEM は、*Cisco Nexus 1000V* スイッチに関連付けられた各 ESX ホストまたは ESXi ホスト上で、VMware vSwitch に置き換わるもので、ハイパーバイザ カーネル内のモジュールとして実行されます。VSM は、複数の VEM を 1 つの論理スイッチとして制御し、ESX ホストまたは ESXi ホスト上の VM 内で実行されます。詳細については、<http://www.cisco.com/go/1000vdocs> で *Cisco Nexus 1000V* スイッチのドキュメントを参照してください。

CA Virtual Assurance VM プロビジョニングでは、VMware vNetwork Distributed Switch および *Cisco Nexus 1000V* スイッチをサポートしています。

Cisco Unified Computing System (UCS)

Cisco Unified Computing System (UCS) は、データ センター ハードウェアと仮想化サービスを提供します。

cmdlet

cmdlet はコマンドの一種ですが、行の先頭が余白以外の文字で始まる必要があります。この制限のため、スタンドアロンでしか使用できず、より幅広く使用される JavaScript 式には含めることができません。特に、*rvalue* (代入演算子の右端のオペランド) として使用することはできません。

? は、AutoShell *cmdlet* の一例です。

CPU 共有 (VMware)

共有は自然数として指定され、各仮想マシン間の相対値を示します。

共有の指定は、階層で同じ親を持つ仮想マシン、*vApp*、またはリソース プールに関してのみ意味をなします。仮想マシンに共有を割り当てるときには、オンになっている他の仮想マシンに相対する、その仮想マシンの優先度を常に指定します。

たとえば、競合が発生すると、2000 の共有を持つ仮想マシンには、1000 の共有を持つ仮想マシンよりも多くの CPU 時間が割り当てられます。共有は他の共有に相対して設定されます。このため、共有の値ではなく相対的な大きさが意味を持ちます。1000、2000、3000 の共有の値を持つ 3 台の仮想マシンは、1、2、3 の共有の値を持つ 3 台の仮想マシンと同じように動作します。任意の数スキーム (1、2、3 や 1000、2000、3000 など) を使用できます。

Dell EqualLogic

Dell EqualLogic は、仮想サーバ用の仮想ストレージを使用するための、仮想化された iSCSI SAN ソリューションで構成されます。

dvPort グループ (VMware)

各 VMware vNetwork Distributed Switch には、1 つ以上の *dvPort* グループが割り当てられています。*dvPort* グループは、共通の設定で複数のポートをグループ化し、ラベル付きネットワークに接続する VM に安定したポイントを提供します。一意のネットワークラベルによって、各 *dvPort* グループが識別されます。ネットワークラベルは現在のデータセンターで一意です。

dvPort グループによって、vNetwork Distributed Switch の各メンバポート用にポート設定オプションが指定されます。また、*dvPort* グループによって、ネットワークへの接続方法が定義されます。

dvUplink ポート (VMware)

分散仮想アップリンク (*dvUplinks*) は、ESX ホストの物理 NIC (vmnics) の抽象化レベルを提供します。各物理 NIC は 1 つの *dvUplink* にマップされます。

VMware vNetwork Distributed Switch に関連付けられた各ホストでは、各物理 NIC (アップリンク) が 1 つのアップリンクポートを介して vNetwork Distributed Switch に割り当てられます。

ESAD AIM

Exchange Server および Active Directory 用 AIM を使用すると、クラウドおよび社内運用の両方のインフラストラクチャにおける Exchange Server 環境と Active Directory 環境をモニタできます。この AIM は、ES 環境と AD 環境の設定、およびキー パフォーマンス インジケータのモニタリングを可能にします。

ESX/ESXi ホスト (VMware)

ESX または *ESXi* ホストは、ESX または *ESXi* サーバ仮想化ソフトウェアを使用して仮想マシンを実行する物理コンピュータです。ホストによって、仮想マシンが使用する CPU とメモリのリソースが提供され、仮想マシンはストレージとネットワーク接続へのアクセスが可能になります。

funclet

funclet は、オプションの句、文字列化などが含まれた構文のような、冗長なコマンドを管理します。*funclet* は、通常、*cmdlet* のように、1 行内に単独で使用されます。*funclet* は、より広範囲な式の一部として処理できる値を返すことができます。

I18n (国際化)

I18N (国際化) とは、ソフトウェア製品で複数の言語、時間と日付の形式、数字の書式 (小数点の記号や桁区切り) などの表記規則を扱えるように、製品に改良を加えることです。CA Virtual Assurance では UTF-8 エンコーディングを使用して、入力データと出力データで言語固有の文字を表示します (ドイツ語の ü (ウムラウト)、フランス語の è (アクサングラーブ)、日本語文字など)。

Integrated Virtualization Manager (IVM、LPAR)

Integrated Virtualization Manager (IVM)は仮想 I/O サーバ (VIOS)の機能拡張で、単一の POWER Server を管理できます。IVM では、LPAR を作成し管理できます。IVM では、VIOS 機能の管理を可能にし、Web ベースユーザ インターフェースを提供します。

Internet Small Computer Systems Interface、iSCSI

iSCSI は、イントラネット上のデータ転送を円滑化し、長距離にまたがるストレージを管理するのに使用されます。iSCSI は SCSI コマンドを IP パケット内にカプセル化します。この IP パケットが他の IP パケットと同様にネットワーク上でルーティングされます。IP パケットがデスティネーションに到達すると、iSCSI デバイスはパケットのカプセル化を解除し、SCSI コマンドを解釈します。

L10n (ローカライゼーション)

L10N (ローカライゼーション)とは、すでに国際化されているソフトウェアに対して特定の言語を実装することです。

MIB オブジェクト、MIB 属性

MIB オブジェクトは、1 つ以上のリソース オブジェクトまたはデータ項目を表す MIB に定義されたエンティティです。MIB オブジェクトにはグループ、テーブルおよび個別の属性が含まれます。また、それらは管理情報の構造 (SMI) に従って定義される必要があります。

NetApp ファイラ

NetApp ファイラは、ディスク ストレージ デバイスの一種で、ファイルシステムを所有および制御します。また、ネットワーク経由でファイルとディレクトリをホストに表示します。

Network Installation Manager (NIM) (LPAR)

Network Installation Manager (NIM)は、LPAR および個々のサーバで AIX イメージをインストール、保守するための集中管理ポイントです。NIM によって、そのようなインスタンスのインストールも容易になります。インストール元が、同じマスタ イメージ、異なるイメージ、インストール メディア、または該当インスタンスの以前の mksysb であれ、すべて同じです。インスタンスは、それ自体が LPAR であるか、物理サーバ上にあるかに関係なく、OS イメージを参照します。

onTap

onTap フレームワークは、無償提供されているサービス指向の Web アプリケーション フレームワークです。

POWER プロセッサ (LPAR)

RISC ベースの **POWER** プロセッサは、IBM サーバ、ミニコンピュータ、ワークステーション、およびスーパー コンピュータの多くで CPU として採用されています。

SNMPv3

SNMPv3 は以下の 3 つの通信のレベルがあるプロトコルです。

noAuthNoPriv: メッセージにユーザ名が伴うという点で **SNMPv1** と **SNMPv2** をミラーリングします。送信者と受信者の間に一貫性がある必要があります。

AuthNoPriv: 一貫したユーザ名およびパスワードを使用します。

AuthPriv: メッセージの本体を暗号化するユーザ名、パスワードおよび暗号化キーを使用します。

UCS

「Cisco Unified Computing System (UCS)」を参照してください。

UCS マネージャ

UCS ハードウェア (スイッチ、シャーシ、およびブレード) を管理するソフトウェア モジュール

vApp (VMware)

vApp は、VM の集合を 1 つの単位として扱う特殊なリソース プールです。vApp は Open Virtualization Format (OVF) を使用します。OVF は、多層アプリケーションのすべてのコンポーネントと、アプリケーションに関連付けられた運用ポリシーおよびサービスレベルを規定し、カプセル化するための標準です。CA Virtual Assurance は vApp 上で操作を実行できます。vApp 上の操作は vApp 内のすべての VM にプロパゲートされます。

vCenter Server (VMware)

VMware **vCenter Server** は、仮想 vSphere 環境の設定、プロビジョニング、および管理を集中管理する場所を提供します。vCenter Server は、Microsoft Windows サーバおよび Linux サーバ上でサービスとして実行されます。

vCenter Server エージェント (VMware)

VMware **vCenter Server** エージェントは、ESX サーバを vCenter Server と接続します。

vCenter Server データベース (VMware)

VMware vCenter Server データベースには、VirtualCenter によって管理される物理サーバ、リソースプール、データセンター、および仮想マシンに関する永続的な情報が格納されます。

vNetwork Distributed Switch、vDS (VMware)

VMware vNetwork Distributed Switch は、ホストからデータセンター レベルに仮想スイッチの設定を抽象化します。vNetwork Distributed Switch は、そのスイッチに関連付けられているデータセンター内のすべてのホストにおいて、単一の仮想スイッチとして動作します。vNetwork Distributed Switch は、分散ポートグループから構成されます。これは、標準的なスイッチ上のポートグループと同様に設定されていますが、複数のホストにわたっています。これらのプロパティは複数のホスト間でマイグレートされるため、仮想マシンで一貫したネットワーク設定を維持できます。

各 vNetwork Distributed Switch は、vNetwork Standard Switch と同様、VM が使用できるネットワーク ハブです。vNetwork Distributed Switch は、VM 間のトラフィックを内部的に転送したり、物理 NIC (アップリンク アダプタ) に接続することで外部ネットワークにリンクしたりすることができます。詳細については、<http://pubs.vmware.com> で vNetwork Distributed Switch のドキュメントを参照してください。

CA Virtual Assurance VM プロビジョニングでは、VMware vNetwork 分散スイッチおよび Cisco Nexus 1000V スイッチがサポートされます。vNetwork パネル、AutoShell、または CLI コマンドを介して分散仮想スイッチを管理できます。

vNetwork Standard Switch、vSwitch (VMware)

CA Virtual Assurance では、抽象化されたネットワーク デバイスである Standard vSwitch のポリシーとプロパティを管理します。VMware vNetwork Standard Switch (vSwitch) は、単一のホスト、およびそのホスト上の仮想マシンで動作し、標準スイッチに接続させることができます。

vSwitch で、VM 間のトラフィックを内部的にルーティングして、外部ネットワークにリンクできます。vSwitch では、複数のネットワーク アダプタの帯域幅を組み合わせ、通信トラフィックを分散します。vSwitch は物理 NIC フェールオーバーを処理することができます。

仮想 I/O サーバ、VIOS (LPAR)

仮想 I/O サーバ (VIOS) は、すべての物理 I/O リソースを所有するように設定された特別な論理パーティションで、その仮想化機能を他の LPAR に提供します。LPAR は、仮想 I/O サーバを介して仮想デバイスとしてディスク、ネットワーク、および光学デバイスにアクセスします。仮想化されたリソースを持つ PowerVM システムには、それぞれ仮想 I/O サーバがあります。

仮想 NIC (VMware)

仮想 NIC は、仮想マシンの仮想イーサネット アダプタです。ゲストオペレーティング システムは、仮想イーサネット アダプタが物理イーサネット アダプタであるかのように、デバイスドライバを介して仮想イーサネット アダプタと通信します。仮想イーサネット アダプタは固有の MAC アドレスと 1 つ以上の IP アドレスを持ち、物理 NIC のように標準的なイーサネット プロトコルに応答します。

仮想スイッチ (VMware)

仮想スイッチは、物理スイッチと同じように動作します。各 ESX サーバには、ポート グループを通じて仮想マシンに接続する固有の仮想スイッチがあります。これらの仮想スイッチには、ESX サーバの物理イーサネット アダプタへのアップリンク接続もあります。仮想マシンは、仮想スイッチ アップリンクに接続された物理イーサネット アダプタを通じて外界と通信します。

仮想ディスク (VMware)

仮想ディスクは、仮想ゲスト オペレーティング システム内のディスクドライブを定義します。仮想ディスクは、ローカル ホストまたはリモート ファイル システム上にある特定のファイルまたはファイルのセットです。これは、オペレーティング システム内の物理ディスクドライブと同じように動作します。

仮想マシン、VM (VMware)

仮想マシン (VM) は、物理コンピュータと同じように、オペレーティング システム およびアプリケーションを実行するソフトウェア ベースのコンピュータです。物理ホストのリソースが仮想マシンによって、作業負荷に応じて動的に消費されます。仮想マシンは柔軟性の高いコンピューティング ユニットであるため、展開には、データ センター、クラスタ、クラウド コンピューティング、テスト環境、デスクトップ、ノート PC など、さまざまな環境が含まれます。一番の強みは、データ センターにあります。仮想マシンはデータセンターでサーバ統合、作業負荷の最適化、およびエネルギー効率の向上のために使用されます。

仮想マシン ハードウェア バージョン 7 (VMware)

仮想マシン ハードウェア バージョン 7 は、VMware 社の仮想ハードウェア生成を指定するもので、vSphere で作成される VM のデフォルトです。CPU やメモリなどのホットプラグをサポートします。VM でホットプラグが有効になっている場合、CA Virtual Assurance も CPU とメモリのホットプラグをサポートします。

注: VMware 仮想マシン ハードウェア バージョン 7 の詳細については、VMware 社のドキュメントを参照してください。

簡易ネットワーク管理プロトコル(SNMP: Simple Network Management Protocol)

簡易ネットワーク管理プロトコル(SNMP)はインターネットの標準的な管理プロトコルです。SNMP 管理アプリケーションおよびエージェントは、get 要求、set 要求、get-next 要求、get レスポンス、およびトラップ PDU を使用して互いと通信します。MIB は、ネットワークとシステムのリソースおよびアプリケーションの履歴を管理し、それらが交換するデータを定義します。

管理情報ベース(MIB)

管理情報ベース(MIB)はリソースのプロパティを説明するデータストアです。MIB には ASN.1 で書き込まれます。これは管理基準によって指定された言語で、SNMP MIB を定義するために OSI の管理情報の構造(SMI) 基準に準拠しています。

共有メモリ(Solaris)

共有メモリは、プロジェクト内で実行されるプロセスで使用可能なメモリの合計量を定義します。

クラスタ

クラスタとは、2 台以上の独立したコンピュータ システムが連携して 1 つのエンティティとして機能するものです。並列処理、負荷分散、およびフォールトトレランスではクラスタ化を行います。

グローバルゾーン(Solaris)

グローバルゾーンは、すべての Solaris システムに含まれているゾーンです。非グローバルゾーンがシステムに存在する場合、システムおよびシステムの全体管理のデフォルトゾーンはグローバルゾーンになります。

軽量プロセス、LWP (Solaris)

軽量プロセス(LWP)は、Solaris 10 カーネル スレッド モデルに属します。LWP によって、カーネル スレッドとユーザ スレッドが関連付けられ、ユーザ スレッドの実行コンテキストが形成されます。Solaris 10 カーネルでは、カーネル サービスとカーネル タスクがカーネル スレッドとして実行されます。ユーザ スレッドが作成されると、関連付けられた LWP とカーネル スレッドも作成され、ユーザ スレッドにリンクされます。リソース管理によって、LWP の境界を設定できます。

コンテナ(Solaris)

Solaris コンテナは、アプリケーションの完全なランタイム環境を提供します。リソース管理と Solaris ゾーンはコンテナの一部です。

サービス プロファイル

Cisco UCS ハードウェアに関する一連の構成情報(インターフェース、ファブリック接続、ネットワークとサーバの ID など)。

シャーシ (UCS)

Cisco UCS スイッチおよびブレードを格納するハードウェア フレーム

ストレージ エリア ネットワーク、SAN

ストレージ エリア ネットワーク (SAN) は、リモート コンピュータ ストレージ デバイスをサーバに接続するためのアーキテクチャです。リモート デバイスがオペレーティング システムにローカルに接続されているように表示されます。

正規表現

正規表現とは、照合に使用するテキスト パターンです。プレーン テキストと特殊文字の組み合わせを含む文字列を使って、必要とされる種類の一致を指定します。

ゾーン (Solaris)

Solaris ゾーンは、Solaris 10 システムでセットアップできる、仮想化されたオペレーティング システム環境を定義します。ゾーンはオペレーティング システム サービスを仮想化し、隔離され、セキュリティで保護された環境をアプリケーションに提供します。各 Solaris システムには、システムのデフォルトゾーンであるグローバルゾーンが含まれます。たとえば、グローバル以外のゾーンは、作成、削除、変更、停止、または再起動が可能です。

タイムシェア スケジューラ、TS (Solaris)

タイムシェア スケジューラ (TS) は、すべてのプロセスに対して、利用可能な CPU の均等なアクセスを提供するスケジューラ クラスを指定します。これによって、優先度に基づいて CPU 時間が割り当てられます。

タスク (Solaris)

タスクは、一定期間における 1 セットの作業を表します。個々のタスクは 1 つのプロジェクトに関連付けられます。

データストア (VMware)

データストアは、データセンター内の基本要素である物理ストレージリソースの組み合わせを仮想的に表現したものです。これらの物理ストレージリソースとして提供できるのは、サーバ上のローカル ディスクや SAN ディスク アレイなどです。

データセンター (VMware)

データセンターは、ホスト、仮想マシン、リソース プール、またはクラスタのコンテナとして機能します。仮想設定が特定の部門の要件を満たしていれば、データセンターは、地理的な地域や個別のビジネス機能などの組織構造を表すことができます。また、データセンターを使用して、テスト用の分離された仮想環境を構築したり、環境を組織したりすることができます。

動的再構成コネクタ インデックス、DRC インデックス (LPAR)

物理システム ユニットの各スロットには、**DRC** インデックスが割り当てられています。展開プロセスで **LPAR** を実際に作成するには、この番号が必要になります。管理コンソール (**HMC** または **IVM**) およびシステムは、このインデックスを使用してシステム上の各スロットを一意に識別します。ユニットに電源を投入するまで、**DRC** インデックスはスロットに割り当てられません。

トラップ

トラップは、エージェントとリソースのイベントの管理アプリケーションに通知するために、1 つ以上の管理者へ **SNMP** エージェントが送信できる非請求メッセージです。**SNMP** トラップは一般的 (**SNMP** エージェントのすべてのタイプに共通) であるか、または企業に固有 (それを送信するエージェントに一意) です。

ハードウェア管理コンソール、HMC (LPAR)

ハードウェア管理コンソール (**HMC**) は、**IBM POWER Server** 上で管理タスクを実行するために使用される外部アプライアンスです。**HMC** は、リソースをパーティションに動的に割り当てるなど、論理パーティションを作成または変更するのに使用できます。**HMC** は **POWER Server** のサーバファームウェア層と通信し、大規模 **PowerVM** 環境での単一制御ポイントを提供します。

非グローバルゾーン (Solaris)

非グローバルゾーンは、**Solaris** オペレーティング システムの単一インスタンスに、仮想化されたオペレーティング システム環境を提供します。**Solaris** ゾーンソフトウェア パーティション テクノロジーによって、オペレーティング システム サービスが仮想化されます。

ファイバ チャネル、FC

ファイバ チャネルは、コンピュータ デバイス間でデータを転送するための、標準化されたギガビット速度テクノロジーです。ファイバ チャネルは、コンピュータサーバを共有ストレージ デバイスに接続したり、ストレージコントローラとストレージドライブを相互接続したりするのに特に適しています。

フェアシェアスケジューラ、FSS (Solaris)

フェアシェアスケジューラ (**FSS**) は、共有に基づいて **CPU** 時間を割り当てるスケジューラクラスを指定します。共有では、プロジェクトに割り当てられるシステムの **CPU** リソースの割合が定義されます。

フォールトトレランス、FT (VMware)

VMware vSphere では、高可用性(HA)のために設定されたクラスタに定義された VM 上でフォールトトレランス(FT)を有効にすることができます。フォールトトレランスは、クラスタ内の別の ESX サーバ上でセカンダリ VM を作成します。セカンダリ VM は、ワークロードを実行しているプライマリ VM とのロックステップモードで作動します。障害が発生した場合は、セカンダリ VM が、すぐに障害発生時点からワークロードの実行を引き継ぎます。CA Virtual Assurance は、クラスタ内のプライマリおよびセカンダリ VM を検出して管理します。

プラットフォーム管理モジュール(PMM)

プラットフォーム管理モジュール(PMM)は、対応する環境用の接続および運用上のサポートを提供する Web サービスです。サポートされる環境には、たとえば、VMware vSphere、Microsoft Hyper-V、IBM PowerVM、Solaris ゾーン、Cisco UCS、Microsoft Cluster Service などがあります。PMM は、これらの環境のサーバとの接続を管理し、環境関連の操作を実行し、対応する AIM からデータを取得し、CA Virtual Assurance 管理データベースに格納します。

ブレード(UCS)

Cisco UCS シャーシに接続されているサーバ

プロジェクト(Solaris)

プロジェクトは、ホストに関連付けられたコンテナを定義します。プロジェクトは抽象化レイヤの 1 つで、物理システムリソースの収集の構成と管理に役立ちます。

プロジェクトはタスクの集合であり、タスクはプロセスの集合です。login、cron、newtask、setproject、または su コマンドによって新しいセッションが開かれると、プロジェクト内で新しいタスクが開始されます。各プロセスは 1 つのタスクのみに属し、各タスクは 1 つのプロジェクトのみに属します。

プロジェクトとタスクは、Solaris 10 オペレーティングシステム内の作業負荷を識別するのに使用される基本エンティティです。プロジェクトは 1 セットのユーザおよび 1 セットのグループに関連付けられます。ユーザとグループは、自身がメンバであるプロジェクトのコンテキストでプロセスを実行でき、複数のプロジェクトのメンバになることもできます。プロジェクトは、リソースの使用を制限できる基本エンティティです。タスクは、プロセスが関連付けられるエンティティで、プロジェクトは 1 セットのタスクに関連付けられます。

プロセッサ セット、pset (Solaris)

プロセッサ セットは、CPU の非結合グループを定義します。各プロセッサ セットに、ゼロ個以上のプロセッサを含めることができます。プロセッサ セットは、リソースプール設定内のリソース要素の 1 つです。

ポーリング間隔

*ポーリング間隔*とは、リソースグループに対して連続的に行うポーリングの間隔時間です。

ホストバスアダプタ、HBA

ホストバスアダプタ(*HBA*)は、ストレージエリアネットワーク(*SAN*)にホストを接続するインターフェースカードです。

ポリシーに基づく設定

*ポリシーに基づく設定*を使用すると、1回の操作で、管理対象のマシンのセットに展開できるエージェント設定ポリシーを作成できます。

文字列化

*文字列化*とは、一連の文字を取得して、適切な JavaScript リテラル文字列に変換することを指します。

リソース管理 (Solaris)

Solaris ゾーンの*リソース管理*は、作業負荷に対して特定リソースの消費に制限を定義することで、直接セットアップすることができます。作業負荷は、アプリケーションまたはアプリケーションのグループのすべてのプロセスを集約したものです。

リソース管理は、`zonecfg (1M)`に記述された `zonecfg` コマンドによって、`/etc/project` ファイルまたはゾーンの設定に格納されます。

リソース プール (Solaris)

リソース プールは、システムリソースをパーティション分割するための設定メカニズムを定義します。リソース プールとは、パーティション分割できるリソースグループ間の関連付けです。

リソース プール (VMware)

リソース プールは、単一ホストまたはクラスタの物理的なコンピューティングリソースとメモリリソースのパーティションを定義します。任意のリソース プールを小さくパーティション分割することで、特定のグループや特定の目的のためにリソースを分割して割り当てることができます。また、リソース プールを階層的に構成して、ネストすることもできます。

論理パーティション、LPAR

論理パーティション(LPAR)は、独立したシステムとして仮想化される、ハードウェアリソースのサブセットです。物理システムは複数の LPAR に分割でき、それぞれの LPAR が個別のオペレーティングシステムとアプリケーションを提供します。論理パーティションの数は、システムのハードウェア構成によって異なります。LPAR は通常、データベースや Web サーバなどの異なる環境で使用されます。LPAR は、ネットワーク内で独立したシステムとして通信を行います。

論理メモリブロック、LMB (LPAR)

論理メモリブロック(LMB)は、LPAR に割り当てられる物理メモリと論理メモリの粒度を指定します(256 MB など)。

索引

(

- (オプション) サーバのベース ポリシーおよびテンプレートの管理 - 371
- (オプション) サーバへのポリシー/テンプレート更新の適用と更新の確認 - 373
- (オプション) ポリシーまたはテンプレートの更新 - 372

A

- Active Directory - 24
- Active Directory セキュリティのシステム ユーザパスワードの変更 - 33
- Active Directory でのセキュリティ上の考慮事項 - 24
- AIX LPAR 管理コンポーネント間のインタラクション - 96
- Application Insight Module (AIM) - 62
- Application Insight Module、AIM - 397
- AutoShell - 397
- Autoshell Loadable Module、ALM - 397

C

- CA EEM ユーザ インターフェースへのアクセス - 26
- CA EEM ユーザの作成 - 27
- CA Embedded Entitlements Manager が CA Virtual Assurance で動作するしくみ - 25
- CA Embedded Entitlements Manager 管理者パスワード(EiamAdmin)の変更 - 29
- CA NSM が Windows でトラップの受信に失敗する - 379
- CA SDM の設定 - 143
- CA SDM チケットステータス設定の構成 - 144
- CA Technologies 製品リファレンス - 3
- CA Virtual Assurance vCenter 管理の推奨事項 - 327
- CA Virtual Assurance インフラストラクチャを自動展開するための前提条件 - 253

CA への連絡先 - 3

Cisco Nexus 1000V スイッチ - 398

Cisco UCS - 104

Cisco UCS 管理コンポーネント間のインタラクション - 105

Cisco UCS の概要 - 106

Cisco UCS フォルダが UI 内に表示されない - 379

Cisco UCS マネージャ サーバの追加 - 107

Cisco Unified Computing System (UCS) - 398
cmdlet - 398

CPU 共有 (VMware) - 398

CPU メトリックによって割り当てを減少させる
ルールの作成 - 320

CPU メトリックによって割り当てを増加させる
ルールの作成 - 320

CPU メトリックのアクションの作成 - 319

D

DB トランザクション ログ サイズが预期せずに増加する - 380

Dell EqualLogic - 398

dpmvc virtualswitch コマンドでの空のタスク ID - 381

dvPort グループ (VMware) - 399

dvUplink ポート (VMware) - 399

E

ESAD AIM - 399

ESAD AIM のアンインストール - 297

ESAD AIM のインストール - 291

ESX/ESXi ホスト (VMware) - 399

ESX ホストのフォールトトレランス属性 - 83

Exchange Server および Active Directory 用 AIM - 287

Exchange Server および Active Directory 用 AIM
のメリット - 291

Exchange Server と Active Directory をモニタするための設定の適用 - 293

F

FIPS 140-2 の暗号化 - 375

FIPS の概要 - 375

funclet - 399

H

Hyper-V Server 管理コンポーネント間のインタラクション - 93

I

I18n (国際化) - 399

IBM AIX コンピュータの論理パーティションの追加 - 217

IBM PowerVM (LPAR) - 94

IDManager が使用する転送パッケージのプロトコル - 256

Integrated Virtualization Manager (IVM、LPAR) - 400

internet Small Computer Systems Interface、iSCSI - 400

IPv6 アドレスを使用したインフラストラクチャ展開に関する注意事項 - 255

L

L10n (ローカライゼーション) - 400

Linux の Compatibility Library - 259

Linux または UNIX 上の展開管理証明書 - 258

Linux または UNIX での展開プライマ インストール - 257

LPAR 管理の要件 - 54

LPAR モニタリング - 98

M

MIB オブジェクト、MIB 属性 - 400

MIB 拡張の定義 - 192, 366

Microsoft Cluster Service - 100

Microsoft Hyper-V Server - 92

Microsoft SQL サーバに接続できない - 385

Microsoft クラスタの概要 - 101

N

NetApp ファイラ - 400

Network Installation Manager (NIM) (LPAR) - 400

O

onTap - 400

P

PMM が AIM のポーリングを停止する - 383

POWER プロセッサ (LPAR) - 401

S

SNMP Trap Receiver - 263

SNMP V3 エンジン ID - 59

SNMPv3 - 401

SNMP データ ポーラーの設定 - 110

SNMP トラップ レシーバ設定ファイル - 264

SNMP 用の Windows の設定 - 57

Solaris Lists SPARC および x86 システムへのリモートでの展開 - 382

Solaris ゾーン - 90

Solaris ゾーン環境でのポーリング間隔設定の調整 - 378

Solaris ゾーン管理コンポーネント間のインタラクション - 91

Solaris ゾーン管理の要件 - 54

Solaris ゾーンの追加 - 215

SRM 制御設定の定義 - 194

SRM テスト - 130

SRM テストの表示 - 137

SRM ポリシーを作成する方法 - 192

sysedge.cf ファイルの編集による SNMPv1 トラップの設定 - 55

SystemEDGE AIM - 126

SystemEDGE トラップの転送 - 269

SystemEDGE のアップグレード - 385

SystemEDGE ポリシーを作成する方法 - 180

SystemEDGE ポリシー制御設定の定義 - 181, 340

SystemEDGE モニタの表示 - 136

SystemEDGE 機能 - 116

U

UCS - 401

UCS AIM サーバの登録 - 108

UCS サーバの削除 - 109

UCS トラップ管理 - 111

UCS マネージャ - 401

V

vApp (VMware) - 401

vApp のサポート - 80

vCenter AIM インスタンス接続のトラブルシューティング - 310

vCenter AIM インスタンスのステータスアイコンに「エラー」が表示される - 391

vCenter AIM インスタンスのステータスアイコンに「警告」が表示される - 394

vCenter AIM インスタンスのステータスアイコンに「ディスクバリが進行中」が表示される - 391

vCenter AIM インスタンスのステータスアイコンに「複数インスタンス」が表示される - 393

vCenter AIM インスタンスのステータスアイコンに「無効」が表示される - 390

vCenter AIM モニタリングに対する一般的な推奨事項 - 325

vCenter AIM モニタリングの推奨事項 - 325

vCenter Server AIM 属性にゼロが表示される - 386

vCenter Server (VMware) - 401

vCenter Server エージェント (VMware) - 401

vCenter Server 管理コンポーネント間のインタラクション - 75

vCenter Server 管理コンポーネント間のインタラクションの確認 - 302

vCenter Server 管理コンポーネントを設定する方法 - 300

vCenter Server 接続のトラブルシューティング - 305

vCenter Server データベース (VMware) - 402

vCenter Server でのユーザスコープ認証 - 39

vCenter Server の AIM インスタンスの追加 - 309

vCenter Server の接続に失敗した - 387

vCenter Server のパスワードを変更するとデータ収集に失敗する - 384

vCenter Server を削除すると、別の管理対象 vCenter Server のオブジェクトが非表示になる - 384

VMware vCenter Server - 74

VMware vCenter Server アーキテクチャ - 84

VMware vCenter および vSphere ユーザ権限 - 206

VMware vCenter プロビジョニング - 206

VM 使用率の値が電源オフ後にすぐに更新されない - 394

VM での論理ボリューム管理 - 84

VM のデバイス管理 - 77

VM のフォールトトレランスプロパティ - 83

VM のホットプラグ サポート - 77

vNetwork Distributed Switch、vDS (VMware) - 402

vNetwork Standard Switch、vSwitch (VMware) - 402

vNetwork 標準スイッチ (vSwitch) - 77

W

Windows 上の展開管理証明書 - 258

Windows イベント モニタの作成 - 361

Windows での展開プライマ インストール - 257

あ

アーキテクチャ - 17, 277, 288

アクションシーケンスの定義 - 155

アクションタイプ - 151

アクセス制御 - 276

新しい vCenter Server 接続のマネージャへの追加 - 304

アップグレード後の空白の[クエリ結果]タブ - 395

イベント転送 - 56
イベントによる vApp のモニタリング - 81
イベントによる分散仮想スイッチのモニタリング - 79
イベント転送のための CA Virtual Assurance の設定 - 58
イメージング サービス - 205
インフラストラクチャ展開プライマ ソフトウェアの手動インストール - 256
インフラストラクチャ展開プロセス - 251
エージェントの視覚化 - 134
エージェントの設定 - 133
エージェント ポリシーのダッシュボード ビュー - 200
エージェントレスのモニタ対象システム - 274
オートメーション - 277
オブジェクト集計の設定 - 122, 347

か

階層型テンプレートの概念 - 338
回復力 - 276
外部ディレクトリ ユーザのためのタスク - 34
概要 - 17, 273, 287
書き込みコミュニティを含まないエージェント設定 - 238
確認要件 - 301
カスタム ポートを使用した SystemEDGE エージェントの展開/インストール - 229
カスタム アクションの作成 - 153
仮想 I/O サーバ、VIOS (LPAR) - 402
仮想 NIC (VMware) - 403
仮想スイッチ (VMware) - 403
仮想ディスク (VMware) - 403
仮想マシン (Hyper-V Server) の追加 - 214
仮想マシン (vCenter Server) の追加 - 211
仮想マシン、VM (VMware) - 403
仮想マシンに関する vCenter 管理の制限 - 327
仮想マシン ハードウェア バージョン 7 (VMware) - 403
仮想リソース用のデータ収集の設定 - 167

簡易ネットワーク管理プロトコル (SNMP: Simple Network Management Protocol) - 404
環境管理の設定要件 - 43
環境の検出 - 44
監査証跡 - 224
管理 DB - 20
管理情報ベース (MIB) - 404
管理対象オブジェクト状態の表示 - 135
管理対象の仮想環境 - 72
管理対象モードおよびレガシー モード - 125
管理ポリシー - 141
関連ドキュメント - 13
規則 - 14
機能 - 290
機能と利点 - 274
共有メモリ (Solaris) - 404
クラスタ - 404
クラスタ内の vCenter Server - 81
クラスタの削除 - 102
クラスタの登録 - 102
クラスタ プロパティの変更 - 103
グループへのユーザの割り当て - 35
グローバル ゾーン (Solaris) - 404
軽量プロセス、LWP (Solaris) - 404
コマンド モードの NodeCfgUtil による AIM の設定 - 49
コマンド モードの NodeCfgUtil による ESAD AIM の設定 - 294
コンテナ (Solaris) - 404

さ

サーバ用のデータ収集の設定 - 165
サーバワークロード用のテンプレートの作成 - 352
サービスの作成 - 68
サービスの編集 - 70
サービス プロファイル - 112, 176, 404
サービス プロファイルとブレードの関連付け - 178
サービス プロファイルの作成または更新を実行する方法 - 113, 177

サービス ポーラーの設定 - 111
サービスレスポンス モニタリング - 128
視覚化 - 275
しきい値定義 - 193
しきい値モニタの作成 - 354
システム管理 - 114
システム管理 MIB - 118
システムの検出 - 64
事前定義済みアクション タイプの使用 - 149
自動化ポリシーの作成 - 145
シナリオおよびベストプラクティス - 299
シャーシ(UCS) - 405
重要業績評価指標 メトリック - 275
状態管理モデル - 121
初期ディスクカバリでのパフォーマンスの考慮事項 - 328
新規パッケージ ラッパーの作成 - 238
スケーラビリティ - 224, 276
スケーラビリティに関する使用事例 - 331
スケーラビリティに関する推奨事項 - 324
スケーラビリティのベストプラクティス - 321
スケジュールの定義 - 156
ステートレスなモニタリング - 124
ストレージ エリア ネットワーク、SAN - 405
正規表現 - 405
セキュリティおよび保守 - 138
設定 - 275
設定の前提条件 - 281
ゾーン (Solaris) - 405
属性にゼロの値が表示される - 378

た

ダイアログ モードの NodeCfgUtil による AIM の設定 - 46
ダイアログ モードの NodeCfgUtil による ESAD AIM の設定 - 296
大規模な環境 - 335
対象読者 - 13
タイムシェア スケジューラ、TS (Solaris) - 405
タスク (Solaris) - 405
ダッシュボード ステータス ビュー - 137

追加プロビジョニング情報 - 219
ディスクカバリ - 43
データ収集の設定 - 160
データストア (VMware) - 405
データセンター (VMware) - 405
データセンター用のデータ収集の設定 - 164
データベース - 20
データベース管理者 (sa) パスワードの変更 - 30
データベースに関する考慮事項 - 323
適用されるポリシーの設定と表示 - 198
テスト定義 - 193
デフォルト パッケージ ラッパー - 236
デフォルト ユーザ グループの作成 - 28
展開管理証明書のプライマ インストールへの提供 - 258
展開コンポーネント - 222
展開ジョブ - 247
展開ジョブのステータスの追跡 - 248
展開ダッシュボード ビュー - 250
展開認証情報の制限 - 226
展開のサイジング キー ファクタ - 228
展開の制限 - 225
展開パッケージ - 234
展開パッケージ設定ファイル - 233
展開パッケージ ライブラリ - 230
展開パッケージ ライブラリの保守 - 232
展開履歴の表示 - 249
テンプレートまたはポリシーからのモニタの削除 - 368
テンプレートまたはポリシーへの MIB 拡張の追加 - 367
テンプレートまたはポリシーへのモニタの追加 - 353
統合 - 276
動的再構成コネクタ インデックス、DRC インデックス (LPAR) - 406
ドメイン サーバに関する推奨事項 - 331
トラップ - 406
トラップとコミュニティの定義 - 188, 348
トラップの管理 - 263
トラブルシューティング - 377

トラブルシューティング: vCenter AIM インスタンスステータスアイコンがエラーを示している - 313

トラブルシューティング: vCenter AIM インスタンスステータスアイコンが警告を示している - 314

トラブルシューティング: vCenter AIM インスタンスステータスアイコンが「ディスクバリエーションが進行中」を示している - 312

トラブルシューティング: vCenter AIM インスタンスステータスアイコンが複数のインスタンスを示している - 312

トラブルシューティング: vCenter AIM インスタンスステータスアイコンが無効を示している - 315

トラブルシューティング: vCenter Server 接続の失敗 - 306

な

名前を変更した vCenter Server の管理 - 53

ネイティブ セキュリティ - 25

ネイティブ セキュリティのシステム ユーザ パスワードの変更 - 31

ネットワーク ディスカバリのキャンセル - 67

ネットワークに関する考慮事項 - 324

ネットワークの検出 - 65

ネットワークの削除 - 67

は

ハードウェア管理コンソール、HMC (LPAR) - 406

ハードウェアの仕様 - 323

廃止された Solaris ゾーン AIM 属性で常に N/A またはゼロが表示される - 380

配布サーバが接続するドメインサーバの変更 - 223

配布サーバに関する推奨事項 - 331

はじめに - 13

パスワード管理 - 29

パッケージフィルタ - 233

パッケージラッパーの変更 - 239

パフォーマンス - 291

パフォーマンス DB - 21

パフォーマンスしきい値の設定 - 170

非グローバルゾーン (Solaris) - 406

非特権ユーザ アカウントを使用した UNIX/Linux へのリモート展開 - 227

ファイアウォール ソフトウェアを実行している Windows Vista™、Windows 2008、および Windows XP コンピュータへの展開 - 261

ファイバ チャネル、FC - 406

フェア シェア スケジューラ、FSS (Solaris) - 406

フォールトトレランス - 82

フォールトトレランス、FT (VMware) - 407

フォールトトレランスの要件 - 82

複数の vCenter AIM の管理 - 51

複数のデータセンター - 333

複数の配布サーバの使用 - 223

複数のマルチインスタンス AIM の使用 - 114

部門のデータセンター - 332

ブラウザにイベントの連続するスペースが表示されない - 378

プラットフォーム管理モジュール (PMM) - 407

ブレード (UCS) - 407

ブレード電源アクションの作成 - 175

プロジェクト (Solaris) - 407

プロセスグループ モニタの作成 - 364

プロセス モニタの作成 - 356

プロセッサ セット、pset (Solaris) - 407

プロビジョニング画面およびポリシー画面で ユーザ インターフェースが応答しません - 386

プロビジョニング リソース - 205

分散仮想スイッチ (DVS) - 78

ポイントエージェント設定の実行 - 133

ポーリング間隔 - 408

保守モードの有効化 - 138

ホストバス アダプタ、HBA - 408

ポリシー アクションを使ってパフォーマンスの問題を特定する方法 - 317

ポリシーおよび階層型テンプレートをサーバに適用する方法 - 337

ポリシー設定 - 178

ポリシー適用の進捗状況の確認 - 197

ポリシーとテンプレートのサーバへの適用と設定の確認 - 369

ポリシーに基づく設定 - 408

ポリシーの UCS アクション タイプ - 174

ポリシーの作成 - 339

ポリシーのユース ケース - 158

ま

マシンへのポリシーの適用 - 196

マネージャ コンポーネント - 61

メトリック収集に関する重要な点 - 161

メトリックフィルタの設定 - 171

文字列化 - 408

モニタされたシステムがダウンしている場合は Solaris ゾーン AIM がリセットされる - 385

モニタ対象オブジェクトに関するスケーラビリティ制限 - 326

モニタ対象サーバに関するスケーラビリティ制限 - 326

モニタ定義 - 180

モニタの設定 - 63

や

ユーザ グループからのユーザまたはユーザ グループの削除 - 36

ユーザ アクセス制御 - 23

ユーザ インターフェース - 21

ユーザ インターフェースへのアクセス - 22

ユーザ グループ権限の設定 - 37

ユーザ グループに対するサービスへのアクセス権の割り当て - 37

ユーザ グループの削除 - 38

ユーザ グループの作成 - 34

ユーザの管理 - 23

ユーザまたはユーザ グループの検索 - 38

ユース ケース: アクションを定義する - 159

ユース ケース: サーバをサービスに追加する - 158

ユース ケース: 新規ルールをサービスに追加する - 159

ユース ケース シナリオ - 279

ら

リソース管理 (Solaris) - 408

リソース ツリーでの vCenter Server フォルダの表示の確認 - 316

リソースの管理 - 61, 68

リソースの検出 - 64

リソースの設定 - 43

リソース プール (Solaris) - 408

リソース プール (VMware) - 408

リソース割り当て - 86

リソース割り当ての共有 - 87

リソース割り当ての制限 - 88

リソース割り当てのベスト プラクティス - 89

リソース割り当ての予約 - 88

リモートおよびマルチインスタンスの vCenter Server サポート - 76

リモート設定および展開 - 126

リモート展開 - 220

リモート展開アーキテクチャ - 221

リモート展開およびポリシー設定に関する推奨事項 - 329

リモート展開およびポリシー設定の概要 - 321

リモート モニタ システムの設定 - 282

リモート モニタリング - 132, 273

リモート モニタリングの利点 - 273

リモート モニタリング メトリックの収集エンジンとレポートのサポート - 285

リモート モニタリングを使用したシステムの管理 - 285

履歴モニタの作成 - 362

ルールとアクション - 141

ルールの作成 - 146

ルールの設計 - 144

例: 特定の Windows パフォーマンスレジストリのメトリックをモニタする方法 - 203

例: ユーザ固有のメトリック (MIB 拡張) をモニタする方法 - 201

レポート - 271

レポートの可用性 - 271

レポートの実行 - 271

ローカル モニタとリモート モニタに同じ値が表示されない - 381

ログ ファイル モニタの作成 - 359

論理パーティション、LPAR - 409

論理メモリブロック、LMB (LPAR) - 409