

CA Virtual Assurance for Infrastructure Managers

管理ガイド

リリース 12.8



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写、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 © 2013 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 ITAM)
- CA ITCM (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 Systems Performance for Infrastructure Managers
- 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	15
対象読者.....	15
関連ドキュメント.....	15
規則.....	16
 第 2 章: 概要	 19
アーキテクチャ.....	20
イメージング サービス.....	24
データベース.....	25
管理 DB.....	25
パフォーマンス DB.....	26
ユーザ インターフェース.....	26
ユーザ インターフェースへのアクセス.....	27
eHealth 統合の概要.....	28
Spectrum Infrastructure Manager 統合の概要.....	31
 第 3 章: ユーザとユーザ グループの管理	 35
ユーザ アクセス制御.....	35
Active Directory.....	36
ネイティブセキュリティ.....	37
パスワード管理.....	40
CA EEM 管理者パスワード (EiamAdmin) の変更.....	41
データベース管理者 (sa) パスワードの変更.....	42
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.....	43
Active Directory セキュリティのシステム ユーザ パスワードの変更.....	45
ユーザ グループ管理.....	46
ユーザまたはユーザ グループの検索.....	47
ユーザ グループの作成.....	47
グループへのユーザの割り当て.....	48
外部ディレクトリ ユーザ グループのユーザ グループへの割り当て.....	49
ユーザ グループ権限の設定.....	51
ユーザ グループ権限の設定.....	51
サービスに対するユーザ グループ権限の設定.....	52

コマンド スクリプトの実行権限の設定	53
外部ディレクトリのインポート	53
ユーザ グループの削除	54
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	55
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	55

第 4 章: システム パフォーマンスの管理 57

システム管理	57
ディスカバリ	59
システムの検出	60
システムの削除	61
ネットワークの検出	62
拡張ディスカバリおよび SNMP 情報	63
ネットワーク ディスカバリのキャンセル	65
ネットワークの再検出	65
ネットワークの削除	66
サービス	66
サービスの作成	66
サービスの編集	68
サービスからのサーバの削除	70
サービスの削除	70
管理対象リソースと管理対象外リソース	71
管理対象リソースの管理の停止	72
管理対象外リソースの管理	72
管理対象リソースの削除	73
SystemEDGE 機能	74
システム管理 MIB	76
状態管理モデル	79
ステートレスなモニタリング	81
管理対象モードおよび管理対象外モード	81
Application Insight Module (AIM)	82
エージェントの設定	84
モニタリング ソフトウェアの設定	86
セキュリティおよび保守	87
保守モードの有効化	87
サービス レスポンス モニタリング	89
SRM テスト	91
エージェントの視覚化	92
SystemEDGE モニタの表示	93

管理対象オブジェクト状態の表示	94
サービス レスポンス テストの表示	95
 第 5 章: SystemEDGE および Application Insight Module (AIM) の管理	97
ユーザ権限およびアクセス要件のリファレンス	97
Active Directory および Exchange Server (ADES)	98
Cisco UCS.....	99
Citrix XenDesktop.....	100
Citrix XenServer.....	101
Huawei GalaX	101
Hyper-V	102
IBM PowerHA.....	103
IBM PowerVM	104
Microsoft Cluster Server	105
Oracle Solaris ズーン.....	105
Red Hat Enterprise Virtualization.....	106
リモート展開エージェント	107
リモート モニタリング	108
SystemEDGE と Advanced Encryption	109
VMware vCenter	110
VMware vCloud.....	110
SNMP およびアクセス制御リストの設定方法	111
SNMP の整合性.....	111
グローバルおよびサーバ レベルの SNMP 設定	112
SNMPv1/v2 設定およびアクセス制御リストの設定方法	114
サーバ レベルの SNMP 設定を管理する方法	128
SNMPv3 の設定方法.....	133
イベント転送のための CA Virtual Assurance の設定.....	141
SystemEDGE および AIM の展開方法	142
概要	143
設定	146
スケーラビリティ	150
展開パッケージ.....	152
リモート展開の使用.....	169
具体的なリモート展開の使用例.....	184
展開ジョブ	192
インフラストラクチャ展開プロセス	193
ポリシーとテンプレートを使用した SystemEDGE およびサービス レスポンス モニタの設定方法.....	202
設定の概要.....	202
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	205

自動ウォッチャーを作成してシステムに適用する方法	250
ユーザ固有のメトリック（MIB 拡張）をモニタする方法.....	259
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.....	262
SRM ポリシーを作成する方法.....	266
エージェントの検出.....	267
ポリシー設定機能の一般的な使用法	267
SystemEDGE の設定モードの変更方法.....	334
要件の確認.....	335
管理対象モードおよび管理対象外モードの詳細の確認	336
SystemEDGE の現在の設定モードの確認	337
管理対象モードから管理対象外モードへの SystemEDGE の変更方法.....	338
管理対象外モードから管理対象モードへの SystemEDGE の変更方法.....	342
SystemEDGE の設定モードの確認	345

第 6 章: 仮想環境の管理 347

Cisco UCS.....	347
Cisco UCS 管理コンポーネントを設定する方法	348
Cisco UCS の管理.....	362
Citrix XenServer	384
XenServer 管理コンポーネントを設定する方法.....	385
XenServer のプロビジョニング用に Linux テンプレートを準備する方法.....	398
XenServer のプロビジョニング用に Windows テンプレートを準備する方法.....	403
VM ステータスの管理（XenServer）	407
Citrix XenServer 仮想マシンのプロビジョニング	409
Huawei GalaX	410
Huawei GalaX 管理コンポーネントを設定する方法.....	411
Virtual Private Cloud VLAN を作成する方法.....	426
Huawei SingleCLOUD 環境を管理する方法.....	438
GalaX のプロビジョニング用に Windows テンプレートを準備する方法	449
IBM PowerVM（LPAR）	454
IBM PowerVM サーバ管理の概要	455
PowerVM 管理コンポーネントを設定する方法	458
calpara.xml ファイル	475
LPAR モニタリング.....	481
IBM PowerVM の管理	483
Microsoft Hyper-V Server.....	495
Hyper-V 管理の設定方法.....	497
Hyper-V の管理	513
Red Hat Enterprise Virtualization	522

Red Hat Enterprise Virtualization 管理コンポーネントの設定方法	523
KVM のプロビジョニング用に Linux テンプレートを準備する方法	534
KVM のプロビジョニング用に Windows テンプレートを準備する方法	540
VM ステータスの管理 (KVM)	545
RHEV 仮想マシンのプロビジョニング	547
Solaris ゾーン	548
Solaris ゾーン管理コンポーネントを設定する方法	549
Solaris ゾーン管理	563
VMware vCloud	572
vCloud Director 管理コンポーネントを設定する方法	573
リモートおよびマルチインスタンスの vCloud Director のサポート	589
vCloud のフォルダ構造	590
vCloud での vApp のサポート	590
vCloud のリソース プール プロバイダとしての vCenter Server	592
vCloud 組織	593
VMware vSphere および vCenter Server	595
モニタ対象の vSphere および vCenter Server のリソース	596
vCenter Server 管理コンポーネントを設定する方法	599
vCenter Server でのユーザ スコープ認証	618
VM のデバイス管理	620
仮想マシンに対するフォールト トレランス	623
VM のホットプラグ サポート	629
仮想マシンの論理ボリューム	631
リソース割り当て	631
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	636
vApp のサポート	640
クラスタ内の vCenter Server	652
vNetwork パネル内の仮想標準スイッチおよび分散仮想スイッチ	652
VMware vCenter のプロビジョニングと一般的なユース ケース	662

第 7 章: クラスタおよび仮想デスクトップのモニタリング 685

Citrix XenDesktop 環境	685
Citrix XenDesktop 管理コンポーネント間のインタラクション	686
Citrix XenDesktop の前提条件	687
IBM PowerHA	687
IBM PowerHA 管理コンポーネント間のインタラクション	688
SSH の設定	689
ダイアログ モードの NodeCfgUtil による PowerHA AIM の設定	689
コマンド モードの NodeCfgUtil による PowerHA AIM の設定	690

CA IBM SystemEDGE PowerHA AIM トラップ	692
Microsoft Cluster Service	693
Microsoft Cluster Service 管理コンポーネントを設定する方法	694
クラスタの登録	707
クラスタの削除	708
クラスタ プロパティの変更	709
Microsoft Cluster Service の管理	710

第 8 章: エージェントレス モニタリング 713

リモート モニタリング	713
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	714
リモート モニタリングの利点	716
機能と利点	716
アーキテクチャ	719
ユース ケース シナリオ	721
設定の前提条件	723
リモート モニタ システムの設定	724
設定セットの作成	727
リモート モニタリングを使用したシステムの管理	728

第 9 章: Active Directory および Exchange Server 用の AIM のインストールおよび設定 735

はじめに	735
ADES AIM のスケーラビリティ	736
ADES AIM のインストール	737
リモート展開を使用した ADES AIM の展開	738
コマンド モードでの ADES AIM のインストール	740
Active Directory および Exchange Server のモニタリングの設定方法	742
要件	745
Active Directory および Exchange Server AIM の動作方法	746
ADES AIM のモニタリングを有効にするための環境設定	748
ドメイン サーバまたは Exchange Server のマネージャへの追加	749
マネージャへのサーバ接続の失敗	750
ADES AIM インスタンスの追加	752
AIM インスタンス接続のトラブルシューティング	753
Active Directory および Exchange Server モニタリングの検証	757
(オプション) ノード設定ユーティリティを使用した ADES AIM の設定	757
ADES AIM のアンインストール	759

トラブルシューティング	759
AIM が非アクティブで、データを収集していない	760
1 つ以上のドメインがモニタされない	761
一部のカウンタがモニタされない	761
一部のホストがモニタされない	762

第 10 章: ルールとアクションの使用 763

ルールとアクション	763
CA SDM の設定	765
CA SDM チケット ステータス設定の構成	766
ルールの設計	767
ルールの作成	767
事前定義済みアクション タイプの使用	771
カスタム アクションの作成	874
アクション シーケンスの定義	876
スケジュールの定義	877
自動化ポリシーの作成	879
ポリシーのユース ケース	880
ユース ケース: サーバをサービスに追加する	880
ユース ケース: 新規ルールをサービスに追加する	881
ユース ケース: アクションを定義する	881
データ収集の設定	882
メトリック収集に関する重要な点	882
データ センター用のデータ収集の設定	885
サーバ用のデータ収集の設定	887
仮想リソース用のデータ収集の設定	889
パフォーマンスしきい値の設定	893
メトリック フィルタの設定	894

付録 A: FIPS 140-2 の暗号化 897

FIPS の概要	897

付録 B: ツール 899

NodeCfgUtil による AIM の設定	899
NodeCfgUtil の概要	900
ダイアログ モードの NodeCfgUtil による AIMs の設定	902
コマンド モードの NodeCfgUtil による AIM の設定	906
サポート エージェント	909

付録 C: トラブルシューティング

911

Solaris ゾーン環境でのポーリング間隔設定の調整.....	913
属性にゼロの値が表示される.....	913
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.....	914
Cisco UCS フォルダが UI 内に表示されない.....	914
DB トランザクション ログサイズが予期せずに増加する.....	915
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.....	916
ドメイン サーバが使用できない.....	917
eHealth が LPAR 物理ディスクを検出しない.....	917
dpmvc virtualswitch コマンドでの空のタスク ID.....	918
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.....	918
IBM 論理パーティションの名前付け制限.....	919
AIX システム上での SystemEDGE インストーラのナビゲーションの問題.....	920
NodeCfgUtil は XenDesktop コントローラへの接続を検証できない.....	920
パフォーマンス チャートの LPAR レベルのメモリ使用率が 0 として表示される.....	921
PMM が AIM のポーリングを停止する.....	922
Solaris Lists SPARC および x86 システムへのリモートでの展開.....	922
アップグレード後の空白の [クエリ結果] タブ.....	924
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.....	925
vCenter Server のパスワードを変更するとデータ収集に失敗する.....	925
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.....	926
コンポーネントのステータス アイコンが [設定されていません] を示している.....	926
SystemEDGE のアップグレード.....	926
Microsoft SQL サーバに接続できない.....	927
製品のアップグレードがユーザ インターフェースに反映されない.....	927
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ない.....	928
ユーザ インターフェースが動作しない.....	928
vCenter Server AIM 属性にゼロが表示される.....	929
vCenter Server の接続に失敗した.....	930
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.....	933
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.....	934
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.....	934
vCenter AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される.....	936
VM 使用率の値が電源オフ後にすぐに更新されない.....	936

用語集	937
索引	955

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. 15)

[関連ドキュメント](#) (P. 15)

[規則](#) (P. 16)

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、および MIB 属性に関する詳細情報を提供します。

パフォーマンス メトリック参照

サポート対象プラットフォームのシステム パフォーマンスのモニタリングに利用可能なパフォーマンス メトリックについて説明します。

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 レスポンス 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が記載されています。

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

他のガイド、またはこのガイドの他のセクション内の情報への参照は、以下の形式で表示されます。

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 `CASYSEDGE` 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. 20)

[データベース](#) (P. 25)

[ユーザ インターフェース](#) (P. 26)

[eHealth 統合の概要](#) (P. 28)

[Spectrum Infrastructure Manager 統合の概要](#) (P. 31)

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。

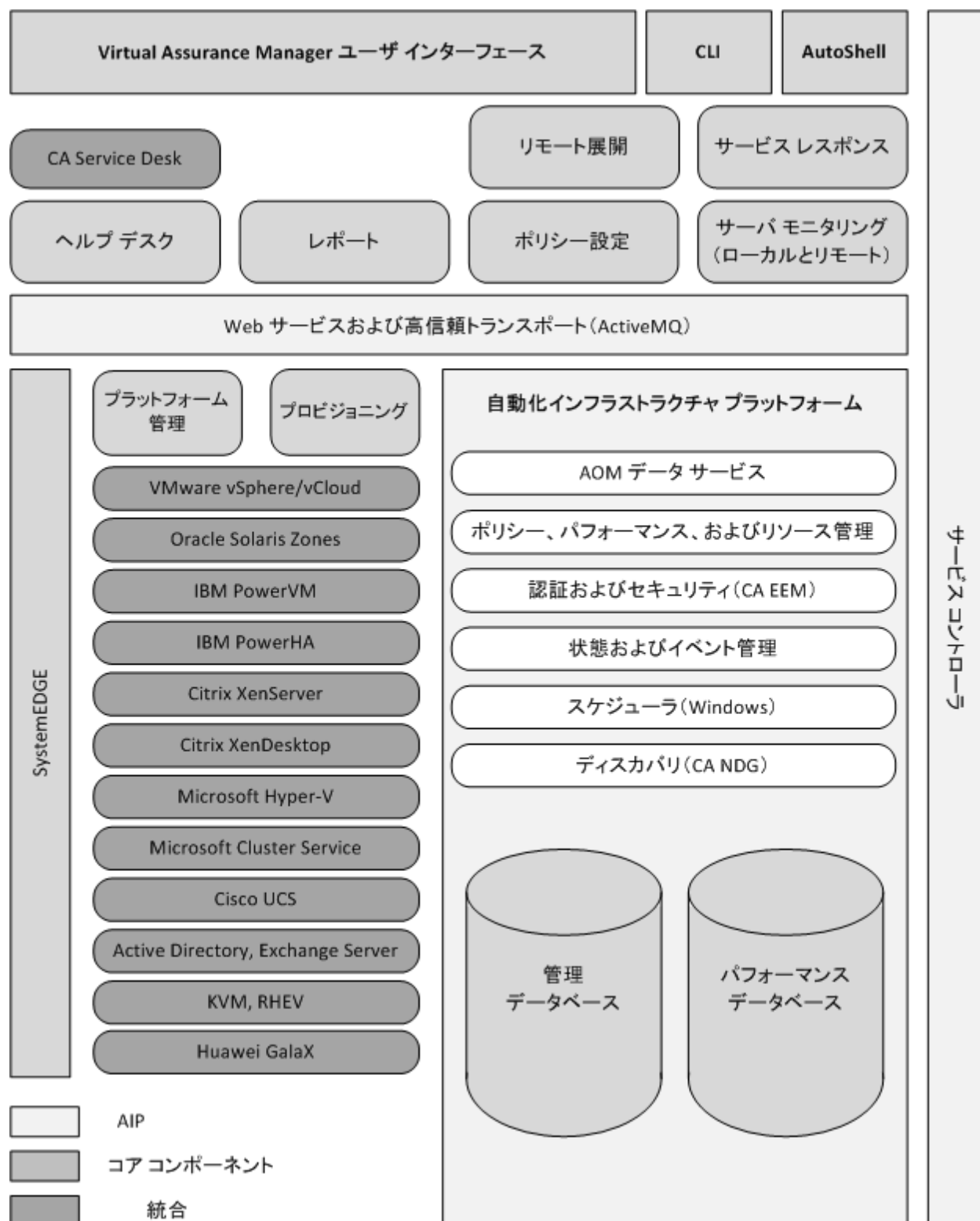
CA Virtual Assurance は以下の外部テクノロジーと統合されます。

- Cisco Unified Computing System
- Citrix XenDesktop
- Citrix XenServer
- Huawei GalaX
- IBM PowerHA
- IBM PowerVM for AIX 仮想化管理
- Microsoft Cluster Service
- 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
- Red Hat Enterprise Virtualization (RHEV)
- Solaris ゾーン仮想化管理
- 仮想マシン (VM) 管理のための VMware vCenter Server
- VMware vCloud

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 EEM
- 軽量のスタンドアロン ディスカバリ機能のための Common Discovery

以下の図は、製品アーキテクチャを示しています。



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 EEM 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に表示されるグラフやチャート、または **CA Virtual Assurance** によって生成されるレポートを通じて、データセンターのパフォーマンスをモニタできます。**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。

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。

- **VM** のプロビジョニングのための **VMware vCenter Server** 統合。
- 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いた、**VM** のプロビジョニングのための **Hyper-V** 統合。
 - 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)** との統合。
- ゾーンのプロビジョニングのための **Solaris** ゾーンの統合。
- **VM** のプロビジョニングのための **Citrix XenServer** の統合。

- VM のプロビジョニングのための VMware vCloud Director の統合。
- KVM プロビジョニングのための Red Hat Enterprise Virtualization の統合。

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。

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 -perfdb` 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。反復作業を自動化するには、AutoShell インターフェースを使用できます。

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 EEM 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。

いつでも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して高度な機能を実行できます。たとえば、ネイティブセキュリティを使用するために **CA EEM** 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。

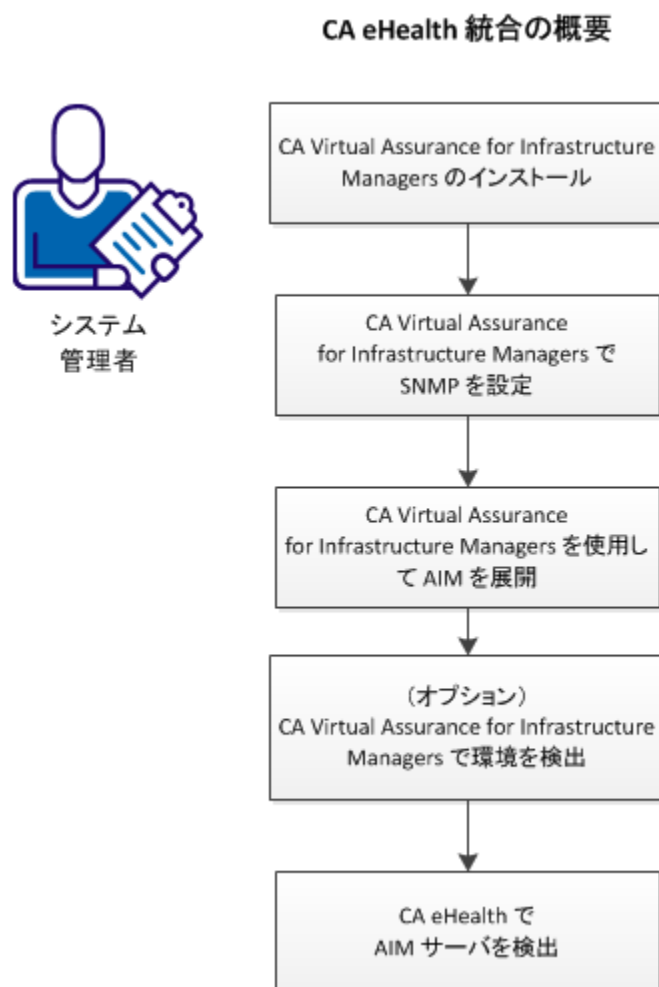
eHealth 統合の概要

システム管理者として、ユーザの物理 IT インフラストラクチャでパフォーマンス管理およびレポート用に **eHealth** を使用します。管理された物理および仮想サーバ環境にこれらの機能を拡張するとします。

CA Virtual Assurance は、**Application Insight Module (AIM)** を使用して、物理および仮想システム環境の管理とモニタを行います。

注: サポートされる環境は、**CA Virtual Assurance** および **eHealth** のバージョンによって変わります。詳細については、**eHealth** のドキュメントを参照してください。

以下の図は、システム管理者が eHealth で CA Virtual Assurance の管理対象環境をモニタできるように CA Virtual Assurance を設定する方法の概要を示しています。



1. CA Virtual Assurance をインストールします。

注: 詳細については、「CA Virtual Assurance インストール ガイド」を参照してください。

2. CA Virtual Assurance での SNMP の設定

CA Virtual Assurance の SNMP 設定が eHealth ポートの設定と一致していることを確認します。CA Virtual Assurance と eHealth が異なるネットワークにインストールされている場合は、適切なファイアウォールポートが開いていることを確認します。

注: 詳細については、「CA Virtual Assurance 管理ガイド」を参照してください。

3. CA Virtual Assurance から使用している環境に AIM を展開します。

インフラストラクチャおよび環境用の適切な AIM およびエージェント展開メソッドを使用します。

注: 詳細については、「CA Virtual Assurance 管理ガイド」を参照してください。

4. (オプション) CA Virtual Assurance で環境を検出します。

CA Virtual Assurance 内でのサーバ管理を有効にするために環境のコンポーネントを検出します。

注: 詳細については、「CA Virtual Assurance 管理ガイド」およびオンラインヘルプを参照してください。

5. eHealth で AIM サーバを検出します。

AIM は、サポートするインフラストラクチャを eHealth に公開します。

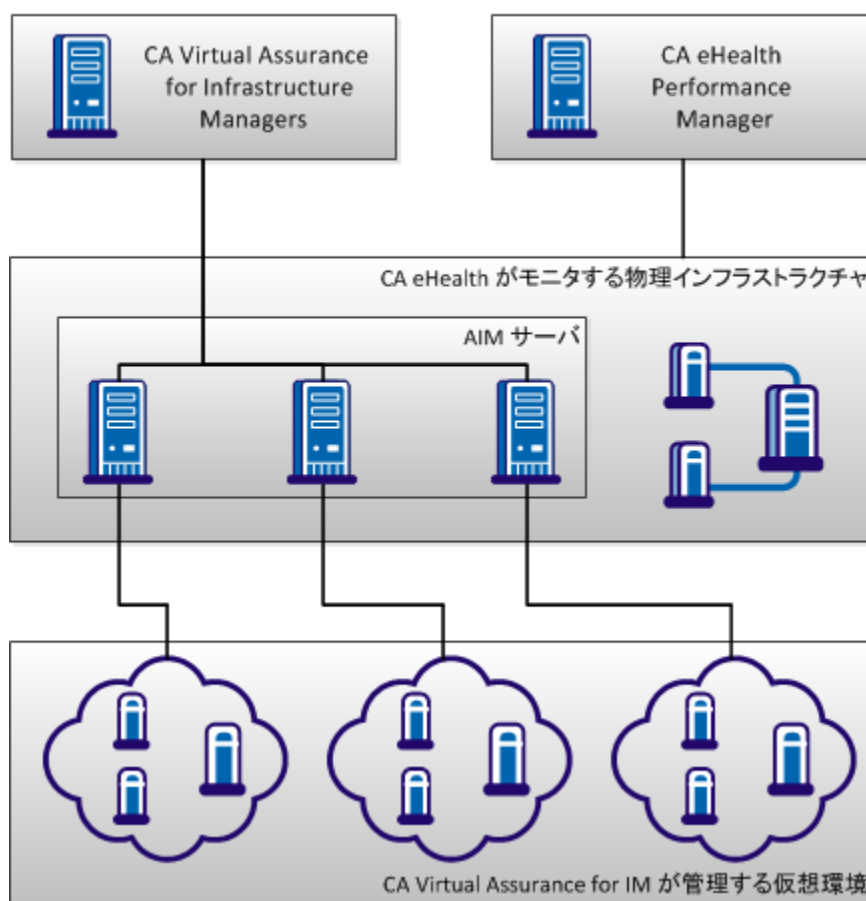
注: 詳細については、eHealth のドキュメントを参照してください。

eHealth は、検出されたインフラストラクチャをそのナビゲーションパネルに表示し、パフォーマンス ダッシュボード、および環境に存在するコンポーネントのほぼリアルタイムでのパフォーマンスと可用性のレポートを提供します。

環境のコンポーネントを管理し、CA Virtual Assurance を使用して、ポリシーベースの管理を実装します。

以下の図は、統合インフラストラクチャの概要を表しています。

統合インフラストラクチャの概要



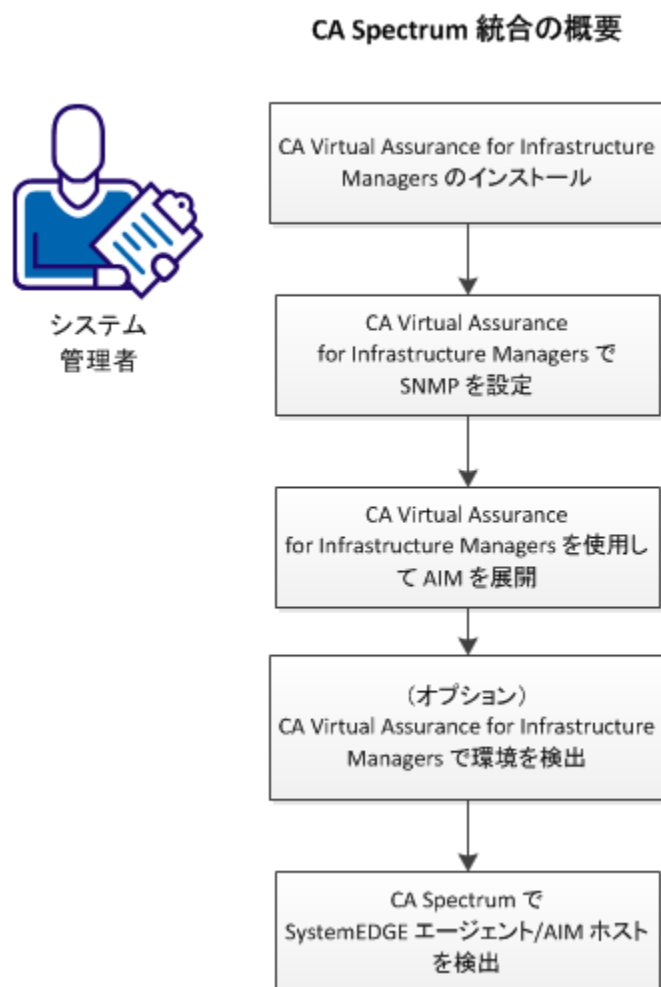
Spectrum Infrastructure Manager 統合の概要

システム管理者として、Spectrum Infrastructure Manager を使用してユーザの物理 IT インフラストラクチャを管理およびモニタし、障害を根本原因に分離します。これらの機能は、仮想環境に拡張できます。

CA Virtual Assurance は、Application Insight Module (AIM) を使用して、物理および仮想システム環境の管理とモニタを行います。

注: サポートされる環境は、CA Virtual Assurance および Spectrum Infrastructure Manager のバージョンによって変わります。詳細については、Spectrum Infrastructure Manager のドキュメントを参照してください。

以下の図は、システム管理者が Spectrum Infrastructure Manager で CA Virtual Assurance の管理対象環境をモデル化およびモニタできるように CA Virtual Assurance を設定する方法の概要を示しています。



1. CA Virtual Assurance をインストールします。

注: 詳細については、「CA Virtual Assurance インストールガイド」を参照してください。

2. CA Virtual Assurance での SNMP の設定

CA Virtual Assurance の SNMP 設定が Spectrum Infrastructure Manager ポートの設定と一致していることを確認します。CA Virtual Assurance と Spectrum Infrastructure Manager が異なるネットワークにインストールされている場合は、適切なファイアウォールポートが開いていることを確認します。

注: 詳細については、「CA Virtual Assurance 管理ガイド」を参照してください。

3. CA Virtual Assurance から使用している環境に AIM を展開します。

インフラストラクチャおよび環境用の適切な AIM およびエージェント展開メソッドを使用します。

注: 詳細については、「CA Virtual Assurance 管理ガイド」を参照してください。

4. (オプション) CA Virtual Assurance で環境を検出します。

CA Virtual Assurance 内でのサーバ管理を有効にするために環境のコンポーネントを検出します。

注: 詳細については、「CA Virtual Assurance 管理ガイド」およびオンラインヘルプを参照してください。

5. Spectrum Infrastructure Manager で SystemEDGE エージェント/AIM ホストを検出します。

AIM は、サポートするインフラストラクチャを Spectrum Infrastructure Manager に公開します。

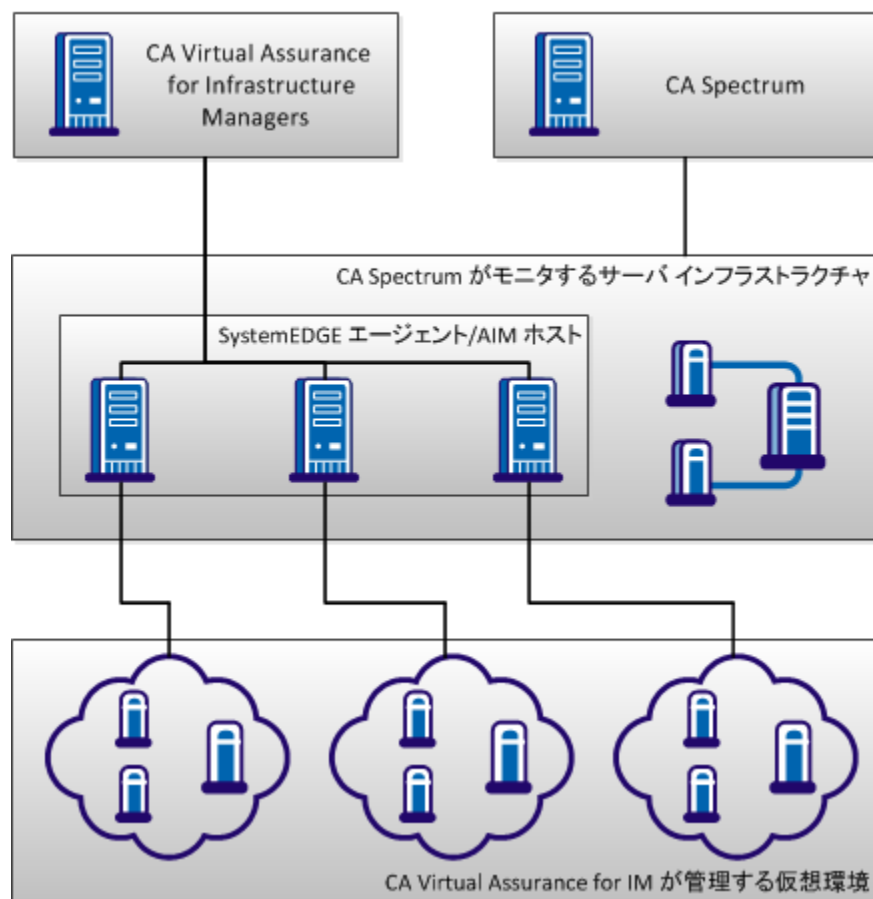
注: 詳細については、Spectrum Infrastructure Manager のドキュメントを参照してください。

Spectrum Infrastructure Manager は、検出されたインフラストラクチャをその OneClick ナビゲーションパネルに表示し、インフラストラクチャモデリング、および環境に存在するコンポーネントの可用性のレポートを提供します。

環境のコンポーネントを管理し、CA Virtual Assurance を使用して、ポリシーベースの管理を実装します。

以下の図は、統合インフラストラクチャの概要を表しています。

統合インフラストラクチャの概要



第 3 章: ユーザとユーザ グループの管理

このセクションには、以下のトピックが含まれています。

[ユーザ アクセス制御](#) (P. 35)

[パスワード管理](#) (P. 40)

[ユーザ グループ管理](#) (P. 46)

ユーザ アクセス制御

CA EEM 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 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 EEM 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 EEM 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実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 の間の通信ではセキュリティが保証されません。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 EEM が CA Virtual Assurance で動作するしくみ

CA EEM 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 EEM 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、その後の許可処理で使用できます。

許可

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、許可が制御されます。これらのポリシーは、CA Virtual Assurance に CA EEM 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 EEM 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 EEM 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 EEM 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 ユーザ インターフェース] を選択します。

CA EEM の [ログイン] ウィンドウが表示されます。

注: セキュリティ証明書リクエストを受信した場合は、それを無視して続行します。このような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 EEM 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 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 EEM ホーム ページ上の [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 EEM ホーム ページの [ホーム] タブ上の [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 [新規アプリケーション グループ] をクリックします。
[新規アプリケーション 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 EEM 管理者
- データベース sa ユーザ (SQL 認証)

CA EEM 管理者パスワード(EiamAdmin)の変更

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

CA EEM 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 ユーザ インターフェース] 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 のパスワード] 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 EEM 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 サービスをリサイクルします。

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 EEM 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 サービスをリサイクルします。

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 EEM および CA Virtual Assurance 内に **sys_service** 認証情報を格納します。後から CA EEM 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 EEM 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 ユーザ インターフェース] 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 EEM** 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** サービスをリサイクルします。
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

CA Virtual Assurance をインストールする際に Active Directory に接続するように設定すると、CA Virtual Assurance をインストールしたユーザは自動的に CA EEM 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 EEM 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 インターフェー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 ユーザ インターフェース] 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. 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 EEM 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进行を要求します。

情報を入力してコマンドを完了します。

9. CAAIPApache および CAIPTomcat サービスをリサイクルします。

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 EEM 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。

ユーザグループ管理

[ユーザグループ] ページでは、ユーザとユーザグループの認証および製品機能へのユーザアクセス制御にアクセスできます。

関連項目:

[ユーザまたはユーザグループの検索](#) (P. 47)

[ユーザグループの作成](#) (P. 47)

[グループへのユーザの割り当て](#) (P. 48)

[外部ディレクトリ ユーザグループのユーザグループへの割り当て](#) (P. 49)

[ユーザグループ権限の設定](#) (P. 51)

[ユーザグループ権限の設定](#) (P. 51)

[サービスに対するユーザグループ権限の設定](#) (P. 52)

[コマンドスクリプトの実行権限の設定](#) (P. 53)

[外部ディレクトリのインポート](#) (P. 53)

[ユーザグループの削除](#) (P. 54)

[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](#) (P. 55)

[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](#) (P. 55)

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。

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。

関連項目:

[グループへのユーザの割り当て \(P. 48\)](#)

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 \(P. 47\)](#) 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。

外部ディレクトリ ユーザ グループのユーザ グループへの割り当て

既存のアクセス権を付与するとき、外部ディレクトリから既存の **CA Virtual Assurance** ユーザ グループにユーザ グループを追加できます。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。

外部ディレクトリ ユーザ グループをユーザ グループに割り当てる方法

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] ノード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] ページ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] ペインがタブの下に表示されます。
5. [アイデンティティ] リストから [ユーザ グループ] を選択します。
ユーザの検索条件が [属性] リストに表示されます。

6. 外部ディレクトリから追加するユーザグループ名を〔値〕テキストボックスに入力し、〔検索〕をクリックします。

ユーザが検索されるか、一致するものが見つからなかったことがメッセージで通知される場合、そのユーザグループは〔利用可能なユーザ/ユーザグループ〕ペインに表示されます。ユーザグループ名は、〔利用可能なユーザ/ユーザグループ〕リストの〔グローバルグループ〕で確認できます。

7. 追加するユーザグループを〔利用可能なユーザ/ユーザグループ〕ペインから選択し、右方向矢印  をクリックします。

選択したユーザグループが〔選択したユーザ/ユーザグループ〕ペインに移動します。

8. 〔保存〕をクリックし、ユーザグループの追加を完了します。

ユーザには、関連付けられているユーザグループに割り当てられたアクセス権限がただちに付与されます。

ユーザグループ権限の設定

〔管理〕ページを使用して、サービスへのユーザグループのアクセスを制御できます。管理者権限が付与されたユーザは、すべてのサービスにアクセスできます。

注: ユーザに CA Virtual Assurance へのアクセス権を付与する場合の詳細については、「管理ガイド」を参照してください。

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、〔権限〕タブをクリックします。
〔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タブおよびアクションのチェックボックスをオンにし、〔保存〕をクリックします。
ユーザグループ権限が更新されます。

注: 特定のページからユーザグループを制限する場合は、そのページ上のすべてのアクションからも、そのユーザグループを制限します。

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。

サービスに対するユーザグループ権限の設定

サービスへのユーザグループのアクセスを制御できます。管理者権限を持つユーザは、デフォルトですべてのサービスにアクセスできます。

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. 左側のペインでユーザグループをクリックします。
4. [サービスアクセス] をクリックします。
右側のペインに、サービスが有効または無効にされているリソースが表示されます。
5. 必要に応じて、サービスアクセス権についてリソースを有効または無効にします。
6. [保存] をクリックします。
[サービスアクセス] リストが更新されます。

コマンド スクリプトの実行権限の設定

管理者ユーザを使用することによって、個別のコマンド スクリプト アクションに対するアクセス権をユーザ グループに付与するか、個別のコマンド スクリプト アクションに対するユーザのアクセス権を有効にできます。対象のコマンド スクリプト アクションは、[アクション & ルール] ページ (ポリシー) で作成済みの必要があります。

コマンド スクリプト アクションの実行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. [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。
タブが右側のペインに表示されます。
4. [権限] タブを選択します。
権限のリストと、権限を選択または選択解除するためのチェック ボックスが表示されます。
5. [ポリシー] フォルダを展開し、[コマンド スクリプトの実行] を選択して、[保存] をクリックします。
コマンド スクリプト権限が更新されます。

外部ディレクトリのインポート

ユーザ グループとしてユーザ名とパスワードの認証を提供する外部ディレクトリ サービスをインポートできます。

外部ディレクトリをインポートする方法

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。
4. [メンバシップ] を選択します。
[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から [ユーザグループ] を選択し、[値] テキストボックスに外部ディレクトリの名前または名前の一部を入力して、[検索] をクリックします。

検索が失敗すると、確認メッセージが表示されます。見つかると、見つかったユーザグループの情報が [利用可能なユーザ/ユーザグループ] セクションに設定されます。外部ディレクトリが CA Virtual Assurance にインポートされました。

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] 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。

第 4 章：システム パフォーマンスの管理

このセクションには、以下のトピックが含まれています。

[システム管理](#) (P. 57)

[ディスカバリ](#) (P. 59)

[サービス](#) (P. 66)

[管理対象リソースと管理対象外リソース](#) (P. 71)

[SystemEDGE 機能](#) (P. 74)

[サービス レスポンス モニタリング](#) (P. 89)

[エージェントの視覚化](#) (P. 92)

システム管理

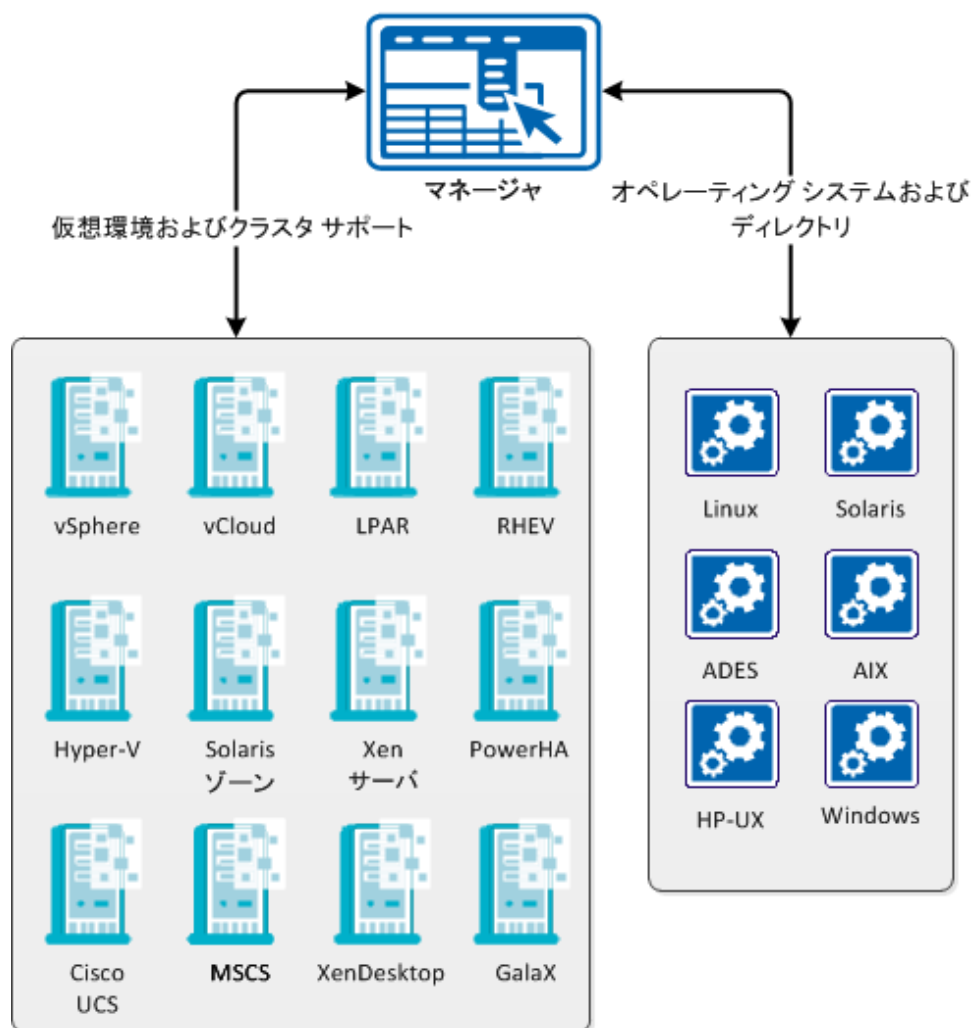
CA Virtual Assurance は、仮想環境を管理するよう設計されていますが、システム (管理対象ノード) の検出や管理も行います。CA Virtual Assurance は、管理対象ノード上の以下のオペレーティング システムをサポートしています。

- 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 Systems Performance LiteAgent

サポートされている仮想環境およびオペレーティング 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

注: SystemEDGE 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 \(P. 74\)](#)

[サービス レスポンス モニタリング \(P. 89\)](#)

[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 \(P. 714\)](#)

[エージェントの設定 \(P. 84\)](#)

[エージェントの視覚化 \(P. 92\)](#)

[セキュリティおよび保守 \(P. 87\)](#)

ディスカバリ

以前は管理対象外であったサーバまたは新たに追加されたサーバを含む、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。

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、あるいはサービスに割り当てるシステムを 1 つ指定できます。

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. [システム名] フィールドに入力して、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。

システムの削除

検出済みのシステムを削除すると、そのシステムは CA Virtual Assurance から削除されます。

システムを削除する方法

1. [リソース] - [管理] - [システムの管理] を選択します。
2. 右ペインの上部のドロップダウンメニューから、以下のいずれかを選択します。
 - ベア メタル サーバ
 - 管理対象サーバ
 - 管理対象外サーバ

検出されたシステムのリストが表示されます。

3. 削除する 1 台または複数のシステムを選択し、[アクション] ドロップダウンメニューで [削除] を選択します。

注: また、[システム] ページで [すべて削除] を選択することにより、すべてのシステムを削除できます。

確認のためのメッセージが表示されます。

4. [はい] をクリックします。

システムは [システム] ページから削除され、CA Virtual Assurance 内で検出済みシステムのリストに表示されなくなります。

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 ディスカバリ用の IP アドレスをユーザ インターフェイ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 スイープ

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。

拡張ディスカバリおよび SNMP 情報

認証情報および SNMP 情報を指定して、システムまたはネットワークを検出できます。

拡張情報を使用して検出する方法

1. [リソース] - [管理] - [ネットワークの検出] または [システムの検出] を選択します。
[ディスカバリ タイプおよびターゲットの指定] セクションが表示されます。
[ディスカバリ タイプ] セクションおよび [ディスカバリ方法] セクションに必要な詳細情報を入力し、[次へ] をクリックします。[拡張ディスカバリおよび SNMP 情報] セクションが表示されます。

2. [拡張ディスカバリ] セクションの以下のフィールドで選択および入力を行います。

拡張ディスカバリ

ディスカバリ用の拡張認証情報を指定するには、このオプションを選択します。

ディスカバリ認証情報

オプションのいずれかを選択して、認証情報を指定します。

認証情報の指定

ユーザ名およびパスワードなどの認証情報を指定するには、このオプションを選択します。

保存された認証情報の選択

[利用可能] リストから既存の保存された認証情報を選択します。

3. [SNMP 情報] セクションの以下のフィールドで選択および入力を行い、次に、[次へ] をクリックします。

SNMP デフォルトを上書きする

ディスカバリ用の SNMP デフォルトを上書きするには、このオプションを選択します。

SNMP 設定

オプションのいずれかを選択して、認証情報を指定します。

認証情報の指定

SNMP バージョンやコミュニティ文字列などの認証情報を指定するには、このオプションを選択します。

保存された認証情報の選択

[利用可能] リストから既存の保存された認証情報を選択します。

4. [終了] をクリックします。

システムまたはネットワークが検出されると、成功したことを示す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 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。

ネットワークの再検出

検出済みのネットワークにシステムが追加されるか、またはネットワークが最後のディスカバリ以降にほかの方法で変更されている場合、そのネットワークの再検出を行うことができます。

ネットワークを再検出する方法

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. 再検出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  (再検出) をクリックします。

ディスカバリがそのネットワーク上で開始されます。ディスカバリが完了すると、ネットワークに対するすべての変更（システムの追加または削除）が反映されます。

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。

サービス

既存の管理対象サーバをサービスにグループ化し、そのグループをモニタできます。

関連項目:

[サービスの作成](#) (P. 66)

[サービスの編集](#) (P. 68)

[サービスからのサーバの削除](#) (P. 70)

[サービスの削除](#) (P. 70)

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。

- 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: % " ' < > / ¥ : ` ~ ;

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。

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

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 レベルでは全体使用率メトリックのみを評価できます。

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 メニューの [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。

- 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 レベルでは全体使用率メトリックのみを評価できます。

- 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。

サービスからのサーバの削除

サーバが特定のサービスに属さないようにすることが必要な場合があります。 サービスからサーバを削除できます。

サービスからサーバを削除する方法

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] ペインで [データ センター] フォルダおよび [CA Virtual Assurance サービス] フォルダを展開します。
データ センターによって検出され、管理されているリソースが表示されます。
3. サーバを右クリックし、[管理] - [サービスから削除] を選択します。
サーバを削除するかどうかを確認するメッセージが表示されます。
4. [OK] をクリックします。
サーバはサービスから削除されます。

サービスの削除

サービスを削除すると、そのサーバ収集は削除されますが、サービス内のサーバは、CA Virtual Assurance 内で管理対象のままとなります。

サービスを削除する方法

1. [リソース] - [管理] - [サービスの管理] を選択します。
サービスのリストが、右ペイン内に表示されます。
2. サービスを選択し、[サービス] 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. [はい] をクリックします。
サービスが削除されます。

管理対象リソースと管理対象外リソース

リソース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。

重要: リソースの管理対象または管理対象外のステータスは、SystemEDGE の管理対象または管理対象外モードとは異なります。コンピュータ システムを管理対象外に設定すると、そのシステムに SystemEDGE がインストールされている場合は SystemEDGE の保守モードが有効になります。

関連項目:

[管理対象リソースの管理の停止](#) (P. 72)

[管理対象外リソースの管理](#) (P. 72)

[管理対象リソースの削除](#) (P. 73)

管理対象リソースの管理の停止

現在管理対象のサーバの管理を停止できます。

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] ペインで [データ センター] フォルダおよび [CA Virtual Assurance サービス] フォルダを展開します。
データ センターによって検出され、管理されているリソースが表示されます。
3. サーバを右クリックし、[管理] - [管理対象外] を選択します。
サーバを管理対象外にするかどうかを確認するメッセージが表示されます。
4. [OK] をクリックします。
管理対象外サーバは管理対象リソース リストに表示されません。管理対象外サーバを表示するには、[エクスプローラ] ペインで [管理対象外] フォルダを開きます。

管理対象外リソースの管理

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。

管理対象リソースの削除

管理が不要になったリソースは削除できます。

管理対象リソースを削除する方法

1. [リソース] をクリックします。
2. [リソース] ページが表示されます。
3. [エクスプローラ] ペインで[データ センター] フォルダおよび[CA Virtual Assurance サービス] フォルダを展開します。

データ センターによって検出され、管理されているリソースが表示されます。

4. サーバを右クリックし、[管理]-[システムから削除]を選択します。
削除するかどうかを確認するメッセージが表示されます。

5. [OK] をクリックします。

削除済みのサーバは、管理対象サーバリストおよび管理対象外サーバリストに表示されません。

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)
- システム管理 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)

システム管理 **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ったら、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ったら、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. 76)

[状態管理モデル](#) (P. 79)

[オブジェクト集計の設定](#) (P. 278)

[ステートレスなモニタリング](#) (P. 81)

[管理対象モードおよび管理対象外モード](#) (P. 81)

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プライベート 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。

システム管理 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。

システム管理 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。

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管理対象外モード

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 インターフェイ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。

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。

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。

Citrix XenDesktop 用の AIM

Citrix XenDesktop 環境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。

Citrix XenServer 用の AIM

Citrix XenServer 環境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。 AIM は、XML RPC を使用して XenServers と直接通信することにより、設定されているすべての XenServer とリソース プールの全体ビューを取得します。

Active Directory および Exchange Server 用の 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 Active Directory および Exchange Server 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。

Huawei GalaX 用の AIM

Huawei GalaX 環境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。

IBM PowerHA 用の AIM

IBM PowerHA（旧名称「High Availability Cluster Multiprocessing」システム）をモニタする機能を提供します。

IBM PowerVM 用の AIM (LPAR)

LPAR を含むシステム全体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。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。

KVM 用の AIM

RHEV 環境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。AIM は RHEV マネージャと通信して、マネージャに登録されるすべての KVM サーバの全体ビューを取得します。

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。

Microsoft Hyper-V 用の AIM

Microsoft Hyper-V 環境を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。

リモート モニタリング用の AIM

リモートの Windows システムをモニタする機能を提供します。リモート モニタリングは、エージェントレス モニタリングとも呼ばれます。

サービス レスpons 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。

Solaris ゾーン用の AIM

ゾーンを実行するように設定された Solaris システム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。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。

VMware vCenter Server 用の AIM

VMware vCenter Server の管理下にあるシステム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。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。

VMware vCloud Director 用の AIM

VMware vCloud Director の管理下にある仮想システム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。

関連項目

[NodeCfgUtil の概要](#) (P. 900)

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. 85)

[設定の概要](#) (P. 202)

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。

モニタリング ソフトウェアの設定

[モニタリング ソフトウェア] ページでは、個別のサーバ、サーバ グループ、またはサービス用の非ポリシー関連情報を設定できます。

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. システムまたはサービスを選択します。

3. [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. 必要に応じて設定を変更し、[適用] をクリックします。

System Description

システムの説明を定義します。

システム担当者

システムの連絡先を定義します。

システムの場所

システムの場所を定義します。

SystemEDGE ログ レベル

SystemEDGE のログ レベルを指定します。

設定が更新されます。

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. 87)

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. [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。

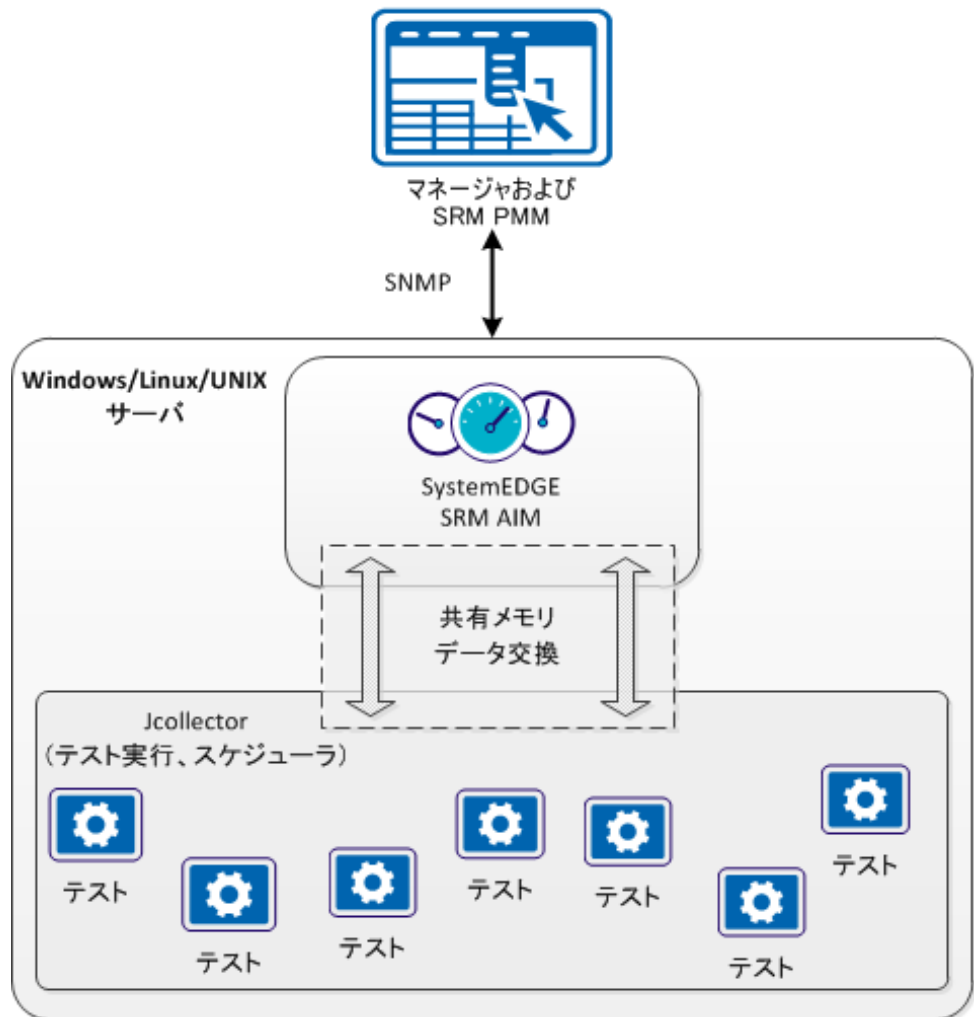
エージェントで保守モードを終了するには、[保守モード] を無効にして [適用] をクリックします。

サービス レスpons モニタリング

サービス レスpons 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、ローカルまたはリモート システムで実行される論理または物理サービスの応答を取得します。SRM は Java ベースのマルチスレッドで、複数のサーバにわたって複数のテスト設定を処理します。SRM は、事前設定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。

以下の図は、これらの関係を示しています。

サービスレスpons 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の仕様が含まれます。SRM AIM は、この設定ファイルを読み取り、テストの仕様を共有メモリ セグメントで利用できるようにします。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、それを SRM AIM にプロパゲートします。SystemEDGE は、これらの結果および関連付けられたステータス情報を CA Virtual Assurance に送信します。

サービス レスpons 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. 91)

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す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することを確認します。

DHCP

DHCP (Dynamic Host Configuration Protocol) サーバが応答して、アドレス要求に応答す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、アドレス解決要求を処理す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、また特定のテキストが Web ページ上に表示されるかどうかを確認します。

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す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 リクエストに応答す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、短いクエリを処理す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、処理す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。

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. 94)

[SystemEDGE モニタの表示](#) (P. 93)

[サービス レスポンス テストの表示](#) (P. 95)

SystemEDGE モニタの表示

CA Virtual Assurance ユーザ インターフェイスには、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. 85)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

管理対象オブジェクト状態の表示

CA Virtual Assurance ユーザ インターフェースには、管理対象システムの SystemEDGE 管理対象オブジェクトがすべて表示されます。

管理対象オブジェクト状態の表示方法

1. [リソース] をクリックし、[エクスプローラ] ツリーの適切なフォルダを展開して、SystemEDGE が実行される管理対象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。

[システム 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、保守中、破棄)
- オブジェクトクラス、インスタンス、および属性
- 現在モニタされている値、オペレータ、しきい値、およびモニタリングマシン名

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。

サービス レスポンス テストの表示

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

サービス レスポンス テストの表示方法

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、[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 テスト] ペインが表示されます。

[サービス レスポンス 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

第 5 章: SystemEDGE および Application Insight Module (AIM) の管理

この章では、環境にモニタリングソフトウェアを設定する方法について説明します。また、適切なユーザ権限と、SystemEDGE を管理対象モードまたは管理対象外モードに変更する方法の詳細についても説明します。

このセクションには、以下のトピックが含まれています。

[ユーザ権限およびアクセス要件のリファレンス \(P. 97\)](#)

[SNMP およびアクセス制御リストの設定方法 \(P. 111\)](#)

[SystemEDGE および AIM の展開方法 \(P. 142\)](#)

[ポリシーとテンプレートを使用した SystemEDGE およびサービス レスポンス モニタの設定方法 \(P. 202\)](#)

[SystemEDGE の設定モードの変更方法 \(P. 334\)](#)

ユーザ権限およびアクセス要件のリファレンス

以下のセクションでは、CA Virtual Assurance コンポーネントをインストールし、CA Virtual Assurance を使用して環境をモニタするためのアクセス要件の概要を説明します。各セクションでは、必要な通信ポートについても説明します。マネージャの分散インストールがファイアウォールをまたぐ場合は、以下のリストを使用して、必要な通信ポートが開いていることを確認できます。

このドキュメントの対象読者は以下のとおりです。

- 仮想環境を管理するために CA Virtual Assurance をインストール、設定、使用する管理者。
- 仮想環境をモニタするために CA Virtual Assurance を使用するオペレータ。

関連項目：

[Active Directory および Exchange Server \(ADES\)](#) (P. 98)
[Cisco UCS](#) (P. 99)
[Citrix XenDesktop](#) (P. 100)
[Citrix XenServer](#) (P. 101)
[Huawei GalaX](#) (P. 101)
[Hyper-V](#) (P. 102)
[IBM PowerHA](#) (P. 103)
[IBM PowerVM](#) (P. 104)
[Microsoft Cluster Server](#) (P. 105)
[Oracle Solaris ゾーン](#) (P. 105)
[Red Hat Enterprise Virtualization](#) (P. 106)
[リモート展開エージェント](#) (P. 107)
[リモート モニタリング](#) (P. 108)
[SystemEDGE と Advanced Encryption](#) (P. 109)
[VMware vCenter](#) (P. 110)
[VMware vCloud](#) (P. 110)

Active Directory および Exchange Server (ADES)

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

(Exchange 2007) ドメイン管理者または Exchange 管理者の役割が必要です。

(Exchange 2010) Exchange Organization Management の役割が必要です。

通信ポート

PowerShell ポート： 80、443、5985、5986

ADSI ポート： 3268、389

Cisco UCS

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

ブレードの電源操作、サービス プロファイルの操作、プール操作、ポリシー操作、インポート/エクスポート操作といった UCS 操作を実行するために十分な権限を持った UCS Manager のユーザ アカウントが必要です。

注: UCS ユーザ管理者権限を与えることを推奨します。

管理者権限を与えることができない場合は、UCS ユーザに以下の役割を割り当てます。

- Ext-lan-config
- Ext-san-config
- Service-profile-config
- Service-profile-config-policy
- Service-profile-ext-access
- Service-profile-network
- Service-profile-network-policy
- Service-profile-qos
- Service-profile-qos-policy
- Service-profile-security
- Service-profile-security-policy
- Service-profile-server
- Service-profile-server-oper
- Service-profile-server-policy
- Service-profile-storage

- Service-profile-storage-policy
- Operations
- Server-equipment

通信ポート

HTTP ポート : 80

HTTPS ポート : 443

Citrix XenDesktop

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

Citrix XenDesktop バージョン 5.6 では、XenDesktop で少なくとも読み取り専用の管理者の役割を持つ Active Directory アカウントが必要です。

通信ポート

WinRM ポート : 5985、5986

SNMP ポート : 161

WMI ポート : 135

Citrix XenServer

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

(XenServer 6.0 以降) 読み取り専用の役割を持つルートまたは Active Directory のサブジェクトが必要です。

通信ポート

HTTPS ポート : 443

SNMP ポート : 161

Huawei GalaX

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

Huawei GalaX モニタリングでは、管理者のユーザ認証情報と、GalaX 環境から取得した対応する p12 ファイルが必要です。

通信ポート

HTTP ポート : 8773

Hyper-V

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

ローカルの管理者アカウントが必要です。

SCVMM モニタリング

System Center Virtual Machine Monitoring (SCVMM) の管理者の役割が必要です。

通信ポート

Windows RPC エンドポイント マッパー ポート : 135

DCOM/WMI ポート : RPC エンドポイントのネゴシエーション時に動的に割り当てられます。

IBM PowerHA

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

PowerHA の監視

以下の CLI コマンドを実行する権限を持つアカウントが必要です。

- clstat
- clRGinfo -s
- cldump
- cllsnw
- cltopinfo
- cllsif
- clshowsrv -v
- vmstat

通信ポート

Secure Shell TCP ポート : 22

IBM PowerVM

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

以下の要件は、CA Virtual Assurance でモニタする既存の環境によって異なります。

ハードウェア管理コンソール(HMC)

hmcsuperadmin タスク役割アカウントが必要です。リソース役割に管理する P-Server だけが含まれるユーザを定義することを推奨します。

注: HMC モニタリングには、HMC および VIOS 設定の両方が必要です。

仮想 IO サーバ(VIOS)のモニタリング

モニタする VIOS 上の padmin ユーザアカウントが必要です。

Integrated Virtualization Manager (IVM)のモニタリング

モニタする IVM 上の padmin ユーザアカウントが必要です。

注: IVM モニタリングには IVM 設定が必要です。

通信ポート

Secure Shell TCP ポート : 22

Microsoft Cluster Server

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

ドメイン管理者アカウントまたはクラスタ ノードのローカル アカウントが必要です。ドメイン ユーザを使用する場合は、ドメイン管理者グループに属している必要があります。クラスタ ノードのローカル アカウントを使用する場合は、ユーザが管理者グループのメンバである必要があります。

重要: すべてのノードに同じクラスタ ノード ローカル認証情報をセットアップしてください。クラスタ サービスが別のノードに移動され、そのノードには別の認証情報がある場合、AIM が接続できなくなります。

通信ポート

Windows RPC エンドポイント マッパー ポート : 135

DCOM/WMI ポート : RPC エンドポイントのネゴシエーション時に動的に割り当てられます。

Oracle Solaris ゾーン

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

root ユーザによるアクセスが必要です。

通信ポート

Secure Shell TCP ポート : 22

Red Hat Enterprise Virtualization

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

スーパーユーザ権限を持つ、対応する Red Hat Enterprise Administrator の役割が必要です。

注: Microsoft Active Directory (AD) ユーザまたは Red Hat Enterprise IPA ユーザを使用できます。

通信ポート

REST API ポート : 8443

リモート展開エージェント

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

Windows へのインストール

Windows のシステム管理者権限が必要です。

Linux へのインストール

root アクセス権、あるいは sudo または pfexec の使用が必要です。

クロスプラットフォーム リモート展開

インフラストラクチャ展開 (ID) を使用します。

ID マネージャ コンポーネント

(Windows のターゲット) ターゲット マシンに Windows 共有 Admin\$ のマッピングが必要です。

(UNIX または Linux のターゲット) マネージャとターゲットの間の SSH 接続が正しく行われていることが必要です。

リモート展開 (Windows)

CIFS UDP ポート : 137 (受信/送信)

CIFS UDP ポート : 138 (受信/送信)

TCP ポート : 135

CIFS TCP ポート : 139 (受信/送信)

CIFS TCP ポート : 445 (受信/送信)

CAM UDP ポート : 4104 (受信/送信)

CAM TCP ポート : 4105 用の通信ポート

リモート展開 (UNIX、Linux)

CAM UDP ポート : 4104 (受信/送信)

Secure Shell TCP ポート : 22 (受信)

TCP ポート : 135

CAM TCP ポート : 4105 用の通信ポート

リモート モニタリング

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

リモート モニタリング

Windows Management Instrumentation (WMI) へアクセスできる認証情報が必要です。

通信ポート

Windows RPC エンドポイント マッパー ポート : 135

DCOM/WMI ポート : RPC エンドポイントのネゴシエーション時に動的に割り当てられます。

ベストプラクティスとして、リモート モニタリング システムは AD ドメインのメンバである必要があります。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 アカウントと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。

SystemEDGE と Advanced Encryption

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

Linux または UNIX へのインストール

root アクセス権または権限のないユーザ アカウント用の `sudo` 設定の使用が必要です。

モニタリング

cf ファイルを編集およびロードする権限、またはリモート設定を使用する権限。

通信ポート

UDP ポート : 161 (SNMP Get/Set 要求)、代替ポート : 1691

UDP トラップ ポート : 162 (送信)

管理対象モードの SystemEDGE は CAM を使用

CAM UDP ポート : 4104

CAM TCP ポート : 4105

VMware vCenter

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

(AIM に有効) AIM コンポーネント用の VC の読み取り専用ユーザ アクセスが必要です。

(PMM に有効) vSphere vCenter Server に対して指定される権限のセットが必要です。

重要: ユーザの役割は、実行する操作のタイプと一致する必要があります。そうでない場合は操作は実行できません。

通信ポート

HTTPS ポート : 443

VMware vCloud

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

(AIM に有効) システム管理者の役割が必要です。

(VMware WS に有効) 操作はユーザの役割に制限されています。

System Administrator@System

フル アクセスを許可します。

Organizational Access@org_name

組織レベルおよび役割の割り当ての操作に制限します。

通信ポート

REST API ポート : 8443

SNMP およびアクセス制御リストの設定方法

このセクションでは、グローバルとサーバレベルの SNMP 設定の違い、アクセス制御リストを適用する方法、および SNMP を設定してシステムを正しく検出する方法について説明します。

関連項目:

[SNMP の整合性 \(P. 111\)](#)

[グローバルおよびサーバレベルの SNMP 設定 \(P. 112\)](#)

[SNMPv1/v2 設定およびアクセス制御リストの設定方法 \(P. 114\)](#)

[サーバレベルの SNMP 設定を管理する方法 \(P. 128\)](#)

[SNMPv3 の設定方法 \(P. 133\)](#)

[イベント転送のための CA Virtual Assurance の設定 \(P. 141\)](#)

SNMP の整合性

システムおよびネットワークを正しく検出するためには、SNMP 設定に整合性があることが必要です。リモートシステム上の SystemEDGE の SNMP 設定が CA Virtual Assurance マネージャに存在しない場合は、CA Virtual Assurance でそのシステム上の必要なリソースを検出できません。CA Virtual Assurance がシステムを検出するには、少なくとも有効な読み取り専用 SNMP 認証情報が必要です。

SystemEDGE エージェントをリモートに展開し、[ポリシー設定] によってエージェントを設定する場合は、マネージャと管理対象システムの間で SNMP の整合性に関する条件が自動的に満たされます。

リモートサーバ上で SNMP 設定をローカルに設定する場合は、SNMP 設定の整合性を確認します。リモートサーバ上の SNMP 設定がマネージャ上で指定されていない場合は、CA Virtual Assurance で不足している認証情報をグローバル SNMP オブジェクトとして指定し、リモートシステムを検出します。

この章で説明する SNMP のシナリオおよび手順は、SystemEDGE エージェントが管理対象モードで実行されると仮定しています。管理対象モードでは、SystemEDGE は CA Virtual Assurance の [ポリシー設定] によって設定されます。

関連項目:

[グローバルおよびサーバレベルの SNMP 設定 \(P. 112\)](#)

グローバルおよびサーバレベルの SNMP 設定

サーバレベルまたはグローバルの SNMP 設定のようなカテゴリは、CA Virtual Assurance マネージャにのみ存在します。ポリシー設定では、これらの設定のコレクションをポリシーによって管理対象サーバに配布します。これらの SNMP 設定は、最終的にそれぞれの管理対象のターゲットサーバの `sysedge.cf` 設定ファイルに反映されます。SystemEDGE ではサーバレベルまたはグローバルの SNMP 設定を区別しません。この情報はマネージャにのみ格納されます。マネージャは、ポリシーのどのバージョンがどの管理対象サーバに適用されたかを理解しています。

必要に応じて、CA Virtual Assurance マネージャに独自のグローバルまたはサーバレベルの SNMP 設定を追加できます。

ほとんどの場合、グローバル SNMP 設定のメカニズムにより、サーバの SNMP 設定を管理する柔軟性がもたらされます。特定のケースでは、サーバレベルの SNMP 設定を使用することが必要な場合があります。ポリシー設定により、ポリシー用に SNMP 設定のコレクションを作成するときの柔軟性が高まります。必要に応じて、グローバルまたはサーバレベルの SNMP 設定を選択できます。

グローバル SNMP 設定により、リモート展開用の SystemEDGE パッケージラッパーの以下のフィールドのドロップダウンリストが入力されます。

- ポート
- 読み取りコミュニティ
- 読み取り/書き込みコミュニティ

あるいは、フィールドをインラインで編集できます。

利用可能な **SNMPv1** コミュニティ文字列はポート設定によって異なります。ポート番号を初めて選択するときには、そのポート用のドロップダウンリストに有効なコミュニティ文字列が自動的に取得されます。パッケージラッパーに認証情報が指定されていない場合は、インストーラはデフォルトでパブリックの読み取り専用文字列になります。パッケージラッパーの認証情報は、**SystemEDGE** がインストールされた時点から、管理対象サーバがポリシー設定を登録して管理対象モードに入るときまで有効です。**SystemEDGE** によってポリシーから設定がロードされます。

注: **SystemEDGE** は、インストールのために少なくとも 1 つの **SNMPv1** コミュニティを必要とします。**CA Virtual Assurance** がサーバの **SystemEDGE** を検出した後、**CA Virtual Assurance** はこれらの **SNMPv1** 設定をサーバレベルの **SNMP** 設定として扱うことができます。

[管理] - [設定] - [展開 & 設定] の以下のオプションは、パッケージラッパーの **SNMP** 設定がサーバレベルの **SNMP** 設定になるかどうかを制御します。

- **SystemEDGE** エージェントが登録されるときにサーバ固有の **SNMP** 設定を作成します。

このオプションが有効な場合、**CA Virtual Assurance** はインストール用の **SNMPv1** 設定をサーバレベルの **SNMP** 認証情報として使用します。

各リモート展開ジョブに対しては、展開プロセス中にターゲットシステムに適用されるポリシーを指定できます。特定のポリシーを指定しないと、**CA Virtual Assurance** は **SystemEDGE** のデフォルト ポリシーを使用します。複数の **SystemEDGE** ポリシーを定義している場合は、**SystemEDGE** の[ポリシー] ペインのデフォルト ポリシーを既存のポリシーのリストから決定できます。

関連項目:

[SNMPv1/v2 設定およびアクセス制御リストの設定方法](#) (P. 114)

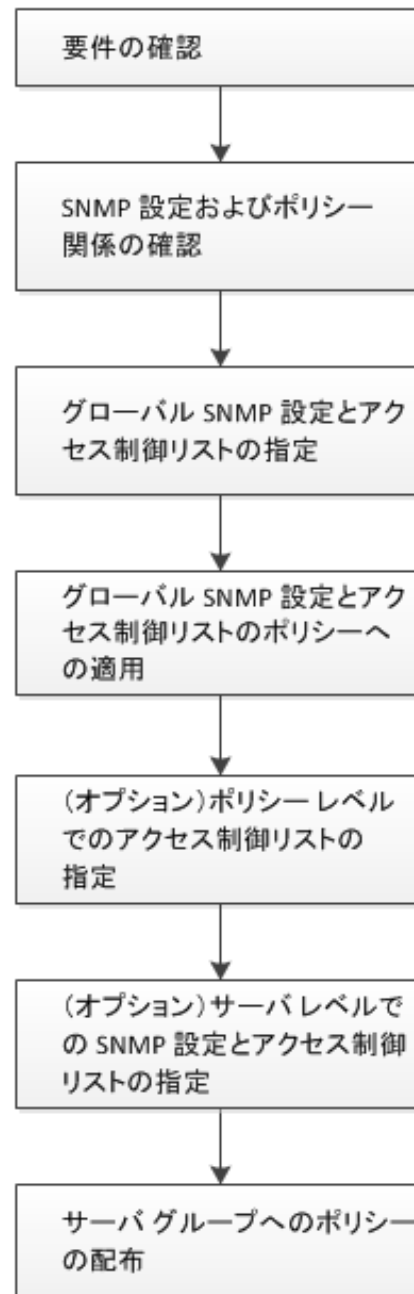
[サーバレベルの SNMP 設定を管理する方法](#) (P. 128)

[SNMPv3 の設定方法](#) (P. 133)

SNMPv1/v2 設定およびアクセス制御リストの設定方法

以下の図は、使用する環境に **SNMP** を設定するために必要なアクションの概要を示しています。この図には、一般的および例外的なケースが含まれています。例外的なケースはオプションとして図に表示されています。

SNMP 設定およびアクセス制御リストの設定方法



以下の手順に従います。

[要件の確認 \(SNMPv1/2\)](#) (P. 116)

[SNMP 設定およびポリシー関係の確認](#) (P. 117)

[グローバル SNMP 設定とアクセス制御リストの指定](#) (P. 119)

[グローバル SNMP 設定とアクセス制御リストのポリシーへの適用](#) (P. 120)

[\(オプション\) ポリシー レベルでのアクセス制御リストの指定](#) (P. 122)

[\(オプション\) サーバ レベルでの SNMP 設定とアクセス制御リストの指定](#) (P. 123)

[サーバ グループへのポリシーの配布](#) (P. 124)

[3 つのサーバ グループの例](#) (P. 125)

要件の確認(SNMPv1/2)

CA Virtual Assurance の SNMP の設定を開始する前に、以下の要件を確認します。

- TCP/IP、SNMP、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 SystemEDGE に関する基礎知識がある。
- 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。
- 管理対象ノードでモニタリング エージェント (CA SystemEDGE) 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。
- CA Virtual Assurance によって関連するシステムがすべて検出されている。
- 設定するすべてのシステムで SystemEDGE が管理対象モードで実行されている。

関連項目：

[SNMP 設定およびポリシー関係の確認](#) (P. 117)

SNMP 設定およびポリシー関係の確認

SNMPv1/v2 の SNMP 設定オブジェクトは、名前、コミュニティ文字列、操作のタイプ（読み取り専用または読み書き）、SNMP のバージョン、ポート、タイムアウト、再試行の制限、およびアクセス制御リスト（ACL）で構成されます。

ACL は、SystemEDGE が実行されている管理対象システムのグループのためのマネージャ システムのリストを指定します。CA Virtual Assurance マネージャは、ポリシー設定によって管理対象システムに SNMP 設定と ACL を配布します。これらの管理対象システムは、ACL にリストされているマネージャ システムからのみ SNMP リクエストを許可します。ACL が指定されていない場合、管理対象システムはすべてのシステムから SNMP リクエストを許可します。

ACL が定義されている場合、CA Virtual Assurance マネージャも ACL のリストに自動的に追加されます。CA Virtual Assurance マネージャには常に接続できます。

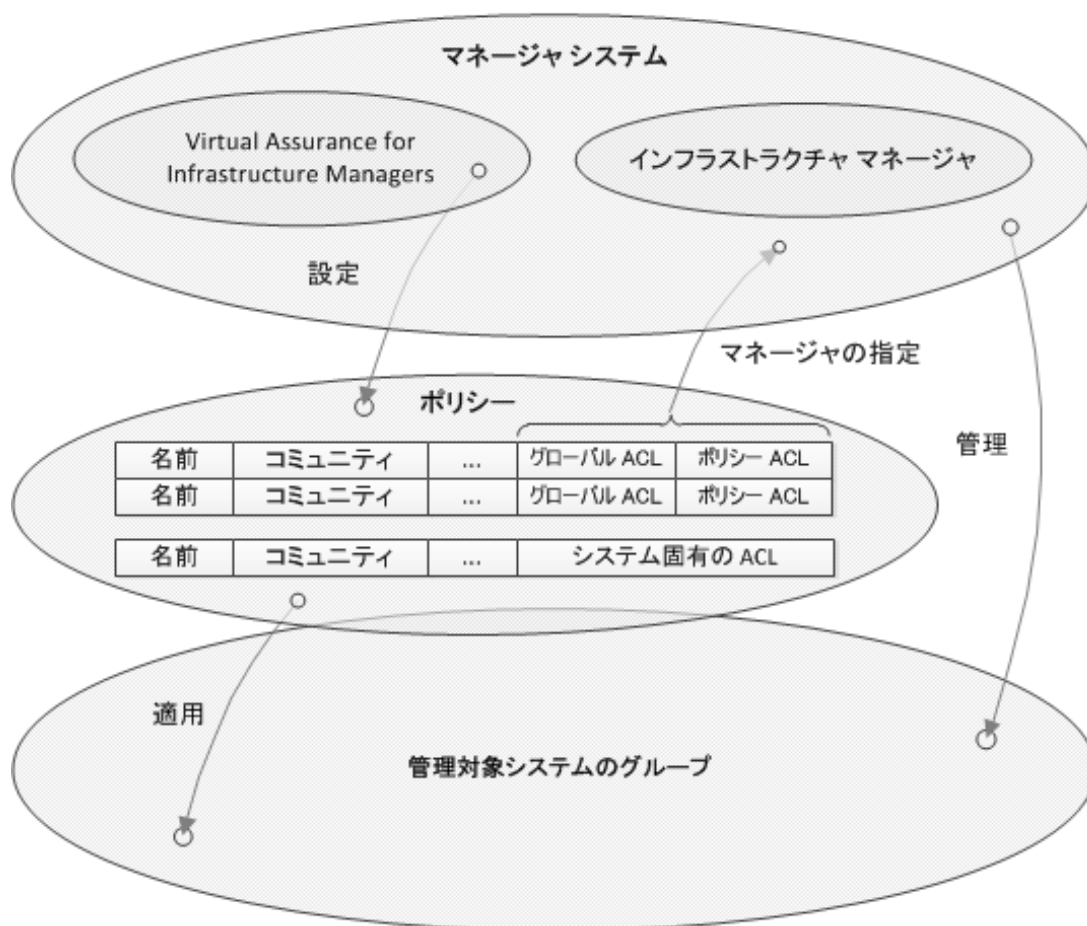
ほとんどの場合、多数またはすべてのシステムで同じ SNMP 認証情報が使用されます。これらの認証情報を適切に管理し適用するために、グローバル レベルで SNMP 認証情報および ACL を指定できます。システムを正しく検出し管理するには、マネージャ システムとエージェント システムで整合性のある SNMP 認証情報および ACL 設定が必要です。グローバル SNMP 設定オブジェクトは、[管理] - [設定] - [SNMP] で指定します。

例外的なケースでは、ACL をポリシー レベルで追加、または SNMP 認証情報と ACL をシステム レベル全体で指定できます。システム レベルで SNMP 設定を変更する場合は、影響を受ける各システムの設定を変更します。

これらの SNMP 設定だけがターゲット システムに適用され、ターゲット システムと同じポートを使用します。

以下の図は、ポリシーのアーキテクチャを示しています。

ポリシーのアーキテクチャ



SNMP 設定は、グローバル、ポリシー、またはシステム レベルで設定できます。また、これらの設定をポリシーに割り当てることができます（左上の矢印）。ポリシーは CA Virtual Assurance を使用して管理対象システムのグループに適用できます。アクセス制御リスト（ACL）では、管理対象システムのグループを管理するマネージャ システムの名前を指定します。ACL に必要なマネージャ システムをすべて追加すると、管理対象システムはこれらのマネージャからの SNMP リクエストにのみ応答します。

関連項目:

[グローバル SNMP 設定とアクセス制御リストの指定 \(P. 119\)](#)

[グローバル SNMP 設定とアクセス制御リストのポリシーへの適用 \(P. 120\)](#)

[\(オプション\) ポリシー レベルでのアクセス制御リストの指定 \(P. 122\)](#)

[\(オプション\) サーバ レベルでの SNMP 設定とアクセス制御リストの指定 \(P. 123\)](#)

[サーバ グループへのポリシーの配布 \(P. 124\)](#)

[3 つのサーバ グループの例 \(P. 125\)](#)

グローバル SNMP 設定とアクセス制御リストの指定

SystemEDGE の SNMP 認証情報のためのアクセス制御リストは、グローバル、ポリシー、およびシステム レベルで設定できます。ACL をグローバルな SNMP オブジェクトに関連付けると、システムに固有の SNMP オブジェクトへの依存性を最小限に留めることができます。

ユーザ インターフェースの [管理] - [設定] - [SNMP] を使用して、ACL をグローバル レベルで編集します。

次の手順に従ってください:

1. ユーザ インターフェースで [管理] - [SNMP] に移動します。

[SNMP 設定] ページが表示されます。

2. (オプション) SNMP 設定オブジェクトを作成するには、[アクション] - [新規] をクリックします。

[新しい SNMP 設定] ダイアログ ボックスが表示されます。SNMP 設定オブジェクトは、名前、コミュニティ文字列、操作のタイプ (読み取り専用または読み書き)、SNMP のバージョン、ポート、タイムアウト、再試行の制限、およびアクセス制御リスト (ACL) で構成されます。SNMP 設定に適用する管理対象ノードに指定されたポート番号を使用します。

3. SNMP 設定オブジェクトの作成に必要なデータを指定して、[OK] をクリックします。
4. ACL に追加する SNMP 設定オブジェクトを選択し、[編集] アイコンをクリックします。

[SNMP 設定の編集] ダイアログ ボックスと ACL のパネルが表示されます。

5. [ポリシー設定 SystemEDGE アクセス制御リスト] パネルでマネージャ システムの名前または IP アドレスを指定して、[OK] をクリックします。

特定のグローバル SNMP 設定オブジェクトのための ACL が指定されます。

そのアクセス制御リストを使用してグローバル SNMP 設定オブジェクトをポリシーに適用できます。

関連項目:

[グローバル SNMP 設定とアクセス制御リストのポリシーへの適用 \(P. 120\) \(オプション\) ポリシー レベルでのアクセス制御リストの指定 \(P. 122\) \(オプション\) サーバ レベルでの SNMP 設定とアクセス制御リストの指定 \(P. 123\) サーバグループへのポリシーの配布 \(P. 124\)](#)

グローバル SNMP 設定とアクセス制御リストのポリシーへの適用

適切な ACL を使用してグローバル SNMP 設定を完了したら、ポリシーに SNMP 設定を適用します。

次の手順に従ってください:

1. ユーザ インターフェースで [リソース] - [設定] に移動します。
[ポリシー] ページが表示されます。
2. ナビゲーション ペインで [ポリシー] - [ポリシー] - [SystemEDGE] を展開します。
[SystemEDGE] ページが表示され、利用可能なポリシーが一覧表示されます。
3. (オプション)  をクリックしてポリシーを作成します。
[新規 SystemEDGE ポリシー] ダイアログ ボックスが表示されます。
4. ポリシーの作成に必要なデータを指定して、[OK] をクリックします。

5. 1つ以上の管理対象システムに適用するポリシーを開き、[トラップ & コミュニティ] をクリックします。

[コミュニティ] ページが表示され、SNMP 設定のテーブルと以下のオプションが表示されます。

- [サーバコミュニティのみを含める]
- [サーバコミュニティおよびすべてのデフォルト コミュニティを含める] (グローバル コミュニティ)
- [カスタム選択]

注: 設定に含まれているテーブルの唯一のデフォルト (グローバル) SNMP 設定は、エージェント ポートに一致するポートを持つ設定です。

6. 3つのオプションの1つを選択し、それぞれのターゲットシステムに指定された適切なポートを持ったコミュニティが少なくとも1つあることを確認します。

最初のオプション [サーバコミュニティのみを含める] を選択する場合は、適切なサーバレベルの SNMP 設定がターゲットシステムに対して存在することを確認してください。選択できる利用可能なサーバコミュニティは一般的に以下のものです。

- サーバ読み取り
- サーバ書き込み

これらは既存のサーバレベルの読み取りおよび書き込みの認証情報を表しています。

2番目のオプションを選択する場合は、テーブルのすべてのグローバル SNMP 設定とサーバレベルの設定がターゲットシステムに適用されます。

3番目のオプションを選択する場合は、テーブルから選択された SNMP 設定だけがターゲットシステムに適用されます。このオプションでは、グローバル設定のみを選択できます。

7. [ポリシーの保存] をクリックします。

必要に応じて、適切なサーバグループにポリシーを配布したり、ポリシーまたはサーバレベルで追加の ACL を指定したりできます。

関連項目:

[\(オプション\) ポリシー レベルでのアクセス制御リストの指定 \(P. 122\)](#)
[\(オプション\) サーバ レベルでの SNMP 設定とアクセス制御リストの指定 \(P. 123\)](#)
[サーバグループへのポリシーの配布 \(P. 124\)](#)

(オプション)ポリシー レベルでのアクセス制御リストの指定

オプションのグローバル ACL を使用してグローバル SNMP 設定を指定した後、ポリシー レベルで ACL を定義できます。

次の手順に従ってください:

1. [ポリシー] ページから、テーブルの 2 番目または 3 番目のオプションを選択して、グローバル SNMP 設定に適用します。
 - [サーバコミュニティおよびすべてのデフォルト コミュニティを含める] (グローバル コミュニティ)
 - カスタム選択
2. テーブルからグローバル SNMP 設定オブジェクトを選択して、[表示] または [定義なし] リンクをクリックします。
[ACL] ダイアログ ボックスが開きます。
3. [ポリシー固有の SNMP アクセス制御リスト] フィールドにマネージャ システムの名前または IP アドレスを追加して、[OK] をクリックします。
このポリシーを適用するサーバグループのサーバは、これらのマネージャ システムからの SNMP リクエストを許可します。
4. [ポリシーの保存] をクリックします。

必要に応じて、適切なサーバグループにポリシーを配布したり、システム レベルで追加の ACL を指定したりできます。

関連項目:

[\(オプション\) サーバ レベルでの SNMP 設定とアクセス制御リストの指定 \(P. 123\)](#)
[サーバグループへのポリシーの配布 \(P. 124\)](#)

(オプション)サーバレベルでの SNMP 設定とアクセス制御リストの指定

例外的なケースでは、特定の管理対象システムに対して **SNMP** 設定およびアクセス制御リストを指定できます。

次の手順に従ってください:

1. ユーザ インターフェイスで [リソース] - [エクスプローラ] に移動します。
[エクスプローラ] ペインが表示されます。
2. [エクスプローラ] ツリーを展開し、**SNMP** 認証情報およびアクセス制御リストを指定するシステムを右クリックします。
3. ポップアップ メニューから、[ポリシー] - [**SNMP** の設定] を選択します。
[**SNMP** 設定] ダイアログ ボックスには、そのシステムに対して有効な **SNMP** 設定が一覧表示されます。
4. [追加] をクリックします。
[新しい **SNMP** 設定] ダイアログ ボックスが表示されます。
5. 名前、ポート、コミュニティ文字列、操作のタイプ（読み取り専用または読み取り/書き込み）、**SNMP** のバージョン、タイムアウト、および再試行の限度を指定します。サーバにインストールされている **SystemEDGE** のポート番号を使用します。[OK] をクリックします。
6. ダイアログ ボックスが閉じて、選択したシステムのページが表示されたら、[モニタリング ソフトウェア] - [**SNMP** アクセス制御] タブをクリックします。
指定したシステムに固有の **SNMP** コミュニティ設定が一覧表示されます。
7. [アクセス制御リスト] 列から [編集] リンクをクリックします。
システムに固有の [アクセス制御リスト] ダイアログ ボックスが表示されます。

8. [SNMP アクセス制御リスト] フィールドにマネージャ システムの名前を入力し、[OK] をクリックします。

管理対象システムは、ACL に一覧表示されたマネージャ システムからの SNMP リクエストを許可します。

9. [保存] をクリックします。

適切なサーバ グループにポリシーを配布します。

関連項目:

[サーバ グループへのポリシーの配布](#) (P. 124)

サーバ グループへのポリシーの配布

適切な ACL を使用して SNMP 設定を完了したら、ネットワーク内のシステムにポリシーを適用します。

次の手順に従ってください:

1. ユーザ インターフェースで [リソース] - [設定] に移動します。
[ポリシー] ページが表示されます。
2. ナビゲーション ペインで [ポリシー] - [ポリシー] - [SystemEDGE] を展開します。
[SystemEDGE] ページが表示され、利用可能なポリシーが一覧表示されます。
3. 以前に適切な SNMP 設定を使用して保存したポリシーを選択します。
[ポリシー] ページが表示されます。

注: [ポリシー設定] を使用して管理対象システムに既存のサーバ レベルの SNMP 設定および ACL を適用しない場合は、[サーバ コミュニティ] ペインの [サーバ 読み取り] および [サーバ 書き込み] エントリをクリアします。

- 4. [アクション] - [適用] をクリックします。
[マシンを選択] ページが表示されます。
- 5. そのポリシーを設定するシステムをすべて選択し、[適用] をクリックします。
配布ステータスを表示するか、または [ポリシー] ページに戻ることができます。
新しい設定がターゲット システムに適用されます。

関連項目:

[3 つのサーバ グループの例](#) (P. 125)

3 つのサーバ グループの例

以下の例では、3 つのサーバ グループ、グローバル SNMP 設定、およびグローバルおよびポリシー レベルで指定された ACL で構成される使用例について説明します。

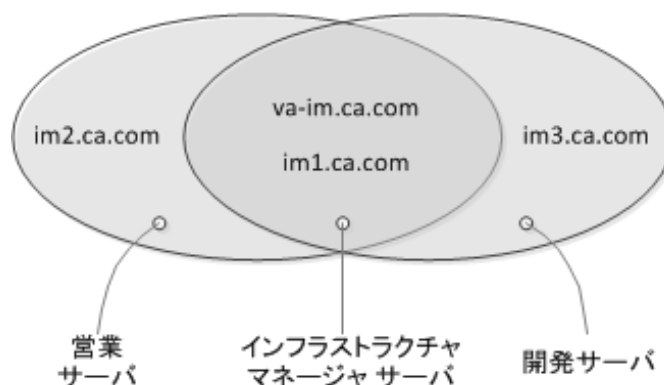
データセンターは以下のサーバ グループで構成されています。

- インフラストラクチャ マネージャ サーバ: CA Virtual Assurance システム、SQL Server システム、CA EEM システム、1 台以上の配布サーバ、3 つのインフラストラクチャ マネージャ システム (im1.ca.com、im2.ca.com、im3.ca.com)。これらのシステムは va-im.ca.com、im1.ca.com によって管理されます。
- 営業サーバ: 営業部門に属し、va-im.ca.com、im1.ca.com、im2.ca.com によって管理されるすべてのサーバ。
- 開発サーバ: 開発部門に属し、va-im.ca.com、im1.ca.com、im3.ca.com によって管理されるすべてのサーバ。

サーバグループ	グローバル コミュニティ設定	グローバル アクセス制御リスト	ポリシー レベルのアクセス制御リスト
インフラストラクチャ マネージャ サーバ	_public_	va-im.ca.com、im1.ca.com	-
	admin	va-im.ca.com、im1.ca.com	-
営業サーバ	_public_	va-im.ca.com、im1.ca.com	im2.ca.com
	admin	va-im.ca.com、im1.ca.com	im2.ca.com

開発サーバ	<code>_public_</code>	<code>va-im.ca.com</code> 、 <code>im1.ca.com</code>	<code>im3.ca.com</code>
	<code>_admin_</code>	<code>va-im.ca.com</code> 、 <code>im1.ca.com</code>	<code>im3.ca.com</code>

アクセス制御リストの関係



次の手順に従ってください:

1. [管理] - [SNMP] で以下のグローバル SNMP オブジェクトを指定します。
 - `infrastructure-read`: port 161, read-only access, community `_public_`, ACL: `va-im.ca.com`, `im1.ca.com`
 - `infrastructure-write`: port 161, read-write access, community `_admin_`, ACL: `va-im.ca.com`, `im1.ca.com`
 - `sales-read`: port 161, read-only access, community `_public_`, ACL: `va-im.ca.com`, `im1.ca.com`
 - `sales-write`: port 161, read-write access, community `_admin_`, ACL: `va-im.ca.com`, `im1.ca.com`
 - `development-read`: port 161, read-only access, community `_public_`, ACL: `va-im.ca.com`, `im1.ca.com`
 - `development-write`: port 161, read-write access, community `_admin_`, ACL: `va-im.ca.com`, `im1.ca.com`
2. デフォルト ポリシーに基づいて、`infrastructure`、`sales`、および `development` の 3 つのポリシー (各サーバグループごとに 1 つずつ) を作成します。
3. `infrastructure` ポリシーのページに切り替え、テーブルからグローバル SNMP 設定を適用する 3 番目のオプションを選択します。
 - カスタム選択

4. グローバル SNMP オブジェクトの `infrastructure-read` および `infrastructure-write` を `infrastructure` ポリシーに追加します。
5. ポリシーを保存します。
6. `sales` ポリシーのページに切り替え、テーブルからグローバル SNMP 設定を適用する 3 番目のオプションを選択します。
 - カスタム選択
7. グローバル SNMP オブジェクトの `sales-read` および `sales-write` を `sales` ポリシーに追加します。
8. `sales-read` および `sales-write` の [表示] リンクをクリックします。
対応する [ACL] ダイアログボックスが開きます。
9. `im2.ca.com` を `sales-read` および `sales-write` オブジェクトに追加して (ポリシー固有の SNMP アクセス制御リスト)、[OK] をクリックします。
10. ポリシーを保存します。
11. `development` ポリシーのページに切り替え、テーブルからグローバル SNMP 設定を適用する 3 番目のオプションを選択します。
 - カスタム選択
12. グローバル SNMP オブジェクトの `development-read` および `development-write` を `development` ポリシーに追加します。
13. `development-read` および `development-write` の [表示] リンクをクリックします。
対応する [ACL] ダイアログボックスが開きます。
14. `im3.ca.com` を `development-read` および `development-write` オブジェクトに追加して、[OK] をクリックします。
15. ポリシーを保存します。
16. 各ポリシー (`infrastructure`、`sales`、`development`) を、その関連するサーバグループに適用します。

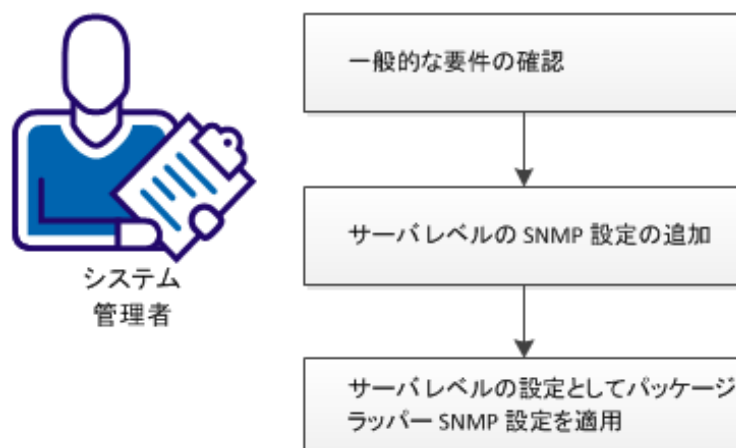
関連項目:

[SNMP 設定およびポリシー関係の確認 \(P. 117\)](#)

サーバレベルの SNMP 設定を管理する方法

以下の図は、サーバ レベルの SNMP 設定を管理するために必要なアクションの概要を示しています。

サーバレベルの SNMP 設定を管理する方法



以下の手順に従います。

[要件の確認（サーバ レベル）](#) (P. 128)

[サーバ レベルの SNMP 設定の追加](#) (P. 129)

[サーバ レベルの設定としてパッケージラッパー SNMP 設定を適用する](#) (P. 131)

要件の確認(サーバレベル)

CA Virtual Assurance のサーバ レベルの SNMP 設定の管理を開始する前に、以下の要件を確認します。

- TCP/IP、SNMP、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 SystemEDGE に関する基礎知識がある。
- 「SNMPv1/v2 設定およびアクセス制御リストの設定方法」のシナリオを確認した。
- 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。

- 管理対象ノードでモニタリング エージェント (CASystemEDGE) 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。
- CA Virtual Assurance によって関連するシステムがすべて検出されている。
- 設定するすべてのシステムで SystemEDGE が管理対象モードで実行されている。

サーバレベルの SNMP 設定の追加

CA Virtual Assurance は SNMP リクエストを使用して SystemEDGE からパフォーマンス メトリックを収集します。個々のサーバの SNMP 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、サブフォルダの順に展開し、設定するサーバを選択します。
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. [SNMP の設定] をクリックします。
[SNMP の設定] ダイアログ ボックスが開き、サーバ レベルの設定が表示されます。
5. 以下のいずれかのオプションを実行します。
 - リストから既存のメトリック用のチェック ボックスをオンにし、ツール アイコン (編集) をクリックして既存のエントリを変更します。
 - [追加] をクリックして、サーバ レベルで SNMP エントリを作成します。
[新しい SNMP 設定] ダイアログ ボックスが表示されます。

6. 以下のフィールドに入力して、[OK] をクリックします。

名前

定義する SNMP 認証情報を説明します。

ポート

これらの認証情報で管理するシステムで SystemEDGE 用に設定するポートを定義します。

SNMP バージョン

使用されている SNMP バージョンを指定します。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。

コミュニティ文字列 (SNMP v1/v2 用)

SNMP コミュニティ文字列を指定します。

セキュリティ ユーザ (SNMP v3 用)

定義する SNMP 認証情報のための SNMP セキュリティ ユーザを指定します。

アクセス タイプ

アクセス タイプを指定します。有効なオプションは、「読み取り専用」または「読み書き」です。

タイムアウト

通知配信の確認待機がタイムアウトするまでの時間を秒単位で指定します。

デフォルト : 10 秒

再試行の制限

タイムアウト後に通知の送信を再試行する回数を指定します。

認証 (SNMP v3 用)

使用する認証プロトコルを指定します。[タイプ] ドロップダウンリストから [MD5] または [SHA] を選択し、パスワードを指定します。

プライバシー (SNMP v3 用)

使用するプライバシープロトコルを指定します。[タイプ] ドロップダウンリストから [DES]、[AES]、または [3DES] を選択し、パスワードを指定します。

SNMP 設定が保存され、[サーバの設定] テーブルに表示されます。

サーバレベルの設定としてパッケージ ラッパー SNMP 設定を適用する

SystemEDGE でポリシー設定を登録した後、サーバレベルの SNMP 設定としてパッケージ ラッパー SNMP 設定を使用するように CA Virtual Assurance に指定することができます。これを行わないと、パッケージ ラッパー SNMP 設定は SystemEDGE がポリシー設定を登録するまでの間しか使用されません。

次の手順に従ってください:

1. [管理] - [設定] - [展開 & 設定] に移動します。

以下のオプションは、パッケージ ラッパーの SNMP 設定がサーバレベルの SNMP 設定になるかどうかを制御します。

- SystemEDGE エージェントが登録されるときにサーバ固有の SNMP 設定を作成します。

2. 要件に応じて、このオプションを有効または無効にします。

このオプションを無効にすると、パッケージ ラッパー SNMP 設定はマネージャに保存されず、配布には使用できません。

このオプションを有効にすると、パッケージ ラッパー SNMP 設定はサーバレベルの SNMP 設定として CA Virtual Assurance マネージャに保存されます。

3. [リソース] - [設定] に移動して、管理対象ノードに適用する SystemEDGE ポリシーを開きます。

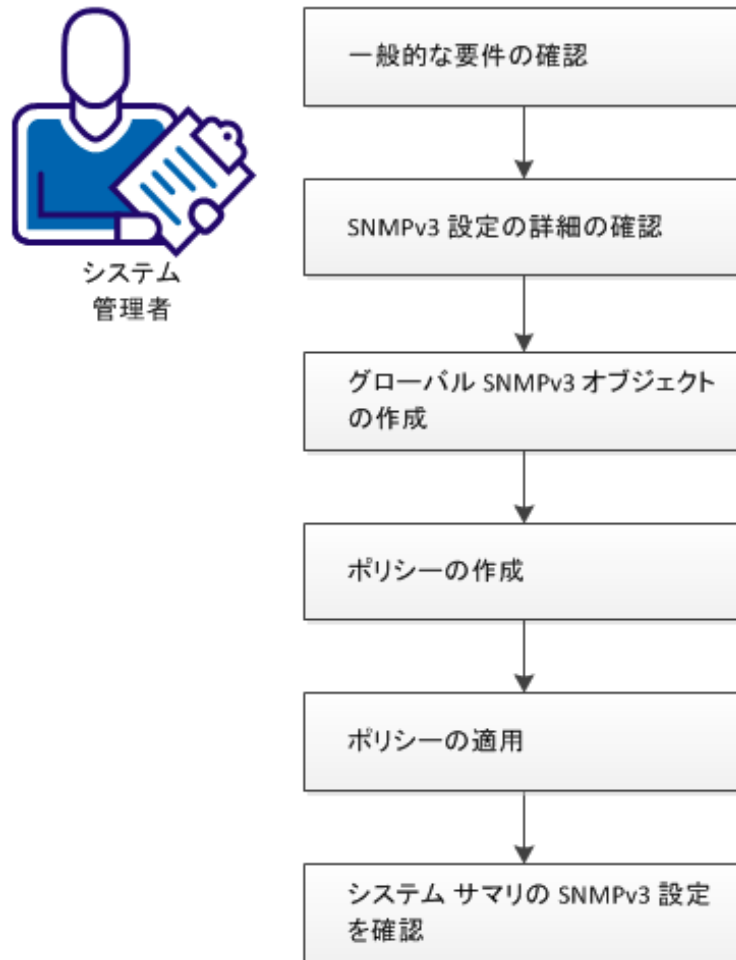
[ポリシー] ペインが表示されます。

4. [トラップ & コミュニティ] - [サーバコミュニティ] で適切なアイテムを選択します。
[サーバ読み取り] および [サーバ書き込み] は、このポリシーを適用する管理対象ノードに使用できるサーバレベルの **SNMP** 設定を表します。
5. [デフォルト コミュニティ] から適切な項目を選択します。
[デフォルト コミュニティ] はグローバル **SNMP** 設定を表します。
6. [リソース] - [展開] - [パッケージ] に移動して、**SystemEDGE** パッケージラッパーを開きます。
7. **SNMP** 認証情報を設定し、管理対象ノードへのインストール後に **SystemEDGE** エージェントに適用するポリシーを選択し、ラッパーを保存します。
8. [展開ジョブ] を作成し、管理対象ノードにそのポリシーで **SystemEDGE** パッケージを展開します。

SNMPv3 の設定方法

以下の図は、使用する環境に **SNMPv3** を設定するために必要なアクションの概要を示しています。このユースケースでは、CA Virtual Assurance の **SNMPv3** 設定について説明します。

SNMPv3 の設定方法



以下の手順に従います。

[一般的な要件の確認 \(SNMPv3\)](#) (P. 134)

[SNMPv3 設定の詳細の確認](#) (P. 135)

[グローバル SNMPv3 オブジェクトの作成](#) (P. 136)

[ポリシーの作成](#) (P. 137)

[ポリシーの適用](#) (P. 139)

[システム サマリの SNMPv3 設定を確認します。](#) (P. 140)

一般的な要件の確認(SNMPv3)

CA Virtual Assurance の SNMP の設定を開始する前に、以下の要件を確認します。

- TCP/IP、SNMP、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 SystemEDGE に関する基礎知識がある。
- 「SNMPv1/v2 設定およびアクセス制御リストの設定方法」のシナリオを確認した。
- 「サーバ レベルの SNMP 設定を管理する方法」のシナリオを確認した。
- 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。
- 管理対象ノードでモニタリング エージェント (CASystemEDGE) 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。
- CA Virtual Assurance によって関連するシステムがすべて検出されている。
- 設定するすべてのシステムで SystemEDGE が管理対象モードで実行されている。

SNMPv3 設定の詳細の確認

使用環境での CA Virtual Assurance マネージャと管理対象ノードとの間の通信に SNMPv3 を使用することを検討している場合は、以下の詳細事項を考慮してください。

- SystemEDGE は、インストールのために少なくとも 1 つの SNMPv1 コミュニティを必要とする。CA Virtual Assurance がサーバを検出した後、CA Virtual Assurance はこれらの SNMPv1 設定をサーバ固有の SNMP 設定として扱う。
- 使用するインフラストラクチャ マネージャが SNMPv3 をサポートしていることを確認する。
- グローバル SNMPv3 認証情報を作成する。
- リモート サーバに SNMPv3 設定を適用するためのポリシーを作成する。
- 純粋な SNMPv3 設定が必要な場合は、ポリシー設定でサーバ固有の SNMPv1 設定を適用しないようにする。

グローバル SNMPv3 オブジェクトの作成

特定のサーバに有効なグローバル SNMP 設定またはサーバ固有の SNMP 設定を作成できます。グローバル設定は、ポリシーによってサーバグループに適用できます。

次の手順に従ってください:

1. ユーザ インターフェースで [管理] - [SNMP] に移動します。
グローバル オブジェクト用の [SNMP 設定] ページが表示されます。
2. SNMP 設定オブジェクトを作成するには、[アクション] - [新規] をクリックします。
[新しい SNMP 設定] ダイアログ ボックスが表示されます。
3. [SNMP バージョン] を [SNMPv3] に設定します。
SNMPv3 に関連するフィールドがダイアログ ボックスに表示されます。
4. 以下のフィールドに入力して、[OK] をクリックします。

名前

定義する SNMP 認証情報の名前を指定します。

ポート

これらの認証情報で管理するシステムで SystemEDGE 用に設定するポートを定義します。

SNMP バージョン

SNMPv3 を指定します（前の手順で設定済み）。

セキュリティ ユーザ

定義する SNMP 認証情報のための SNMP セキュリティ ユーザを指定します。

アクセス タイプ

アクセス タイプを指定します。有効なオプションは、「読み取り専用」または「読み書き」です。

タイムアウト

通知配信の確認待機がタイムアウトするまでの時間を秒単位で指定します。

デフォルト : 10 秒

再試行の制限

タイムアウト後に通知の送信を再試行する回数を指定します。

認証

使用する認証プロトコルを指定します。[タイプ] ドロップダウンリストから [MD5] または [SHA] を選択し、パスワードを指定します。

プライバシー

使用するプライバシー プロトコルを指定します。[タイプ] ドロップダウンリストから [DES]、[AES]、または [3DES] を選択し、パスワードを指定します。

SNMP 設定が保存され、[サーバの設定] テーブルに表示されます。

ポリシーの作成

グローバル SNMPv3 設定が完了したら、ポリシーに SNMPv3 設定を適用します。

次の手順に従ってください:

1. ユーザ インターフェースで [リソース] - [設定] に移動します。
[ポリシー] ページが表示されます。
2. ナビゲーション ペインで [ポリシー] - [ポリシー] - [SystemEDGE] を展開します。
[SystemEDGE] ページが表示され、利用可能なポリシーが一覧表示されます。
3.  をクリックしてポリシーを作成します。
[新規 SystemEDGE ポリシー] ダイアログ ボックスが表示されます。
4. ポリシーの作成に必要なデータを指定して、[OK] をクリックします。
5. 1 つ以上の管理対象システムに適用するポリシーを開き、[トラップ & コミュニティ] をクリックします。
[コミュニティ] ページが表示され、SNMP 設定のテーブルと以下のオプションが表示されます。
 - サーバ コミュニティのみを含める
 - サーバ コミュニティおよびすべてのデフォルト コミュニティを含める
 - カスタム選択

注: 設定に含まれているテーブルの唯一のデフォルト (グローバル) SNMP 設定は、エージェント ポートに一致するポートを持つ設定です。

6. [カスタム選択] を選択します。

このオプションでは、グローバル **SNMPv3** オブジェクトのみを選択し、サーバ固有の **SNMP** 設定をすべてクリアします。

7. ターゲットシステムごとに指定された適切なポートを持つ **SNMPv3** 設定オブジェクトを少なくとも 1 つ選択し、[ポリシーの保存] をクリックします。

選択した **SNMPv3** オブジェクトは、ポリシーと関連付けられます。

8. [トラップ先] タブをクリックします。

[トラップ先] ページが表示されます。[**SNMPv3** トラップデスティネーション] を設定できます。

9. [トラップタイプ] フィールドから、[**SNMPv3** トラップ情報] または [**SNMPv3** 通知情報] (**INFORM** 要求および確認済みトラップとも呼ばれる) を選択します。

選択内容に応じて、以下のフィールドが表示されます。

デスティネーション

トラップの送信先となるホストを指定します。ホスト名または IP アドレスを指定できます。

ポート

トラップの送信先となるデスティネーション ホスト上のポート番号を指定します。

ユーザ名

トラップの送信時に使用する **SNMPv3** ユーザを指定します。

エンコーディング

トラップの送信時に使用するエンコーディングのタイプを指定します。

デフォルト : 000

このエンコーディングは **SNMPv1** のトラップ エンコーディングの設定と同様です。「**SystemEDGE ユーザガイド**」、「**SNMPv1** トラップデスティネーションの設定」も参照してください。

コンテキスト

このフィールドの値としては、*（アスタリスク）のみがサポートされています。この値は必須です。

タイムアウト

（通知のみ）通知の配信確認処理がタイムアウトするまでの待機時間を秒単位で指定します。

再試行回数

（通知のみ）タイムアウト後に通知の送信を再試行する回数を指定します。

10. これらのフィールドに入力し、[追加] をクリックします。
新しいエントリが [トラップ先] テーブルに表示されます。
最後の手順を繰り返すと、テーブルにさらにエントリを追加できます。
11. [トラップ先] のいずれかを選択し、[ポリシーの保存] をクリックします。
ポリシーが適切なトラップ先に保存されます。

適切なサーバグループにポリシーを配布できます。

ポリシーの適用

SNMPv3 設定が完了したら、ネットワーク内のシステムにポリシーを適用できます。

次の手順に従ってください:

1. ユーザインターフェースで [リソース] - [設定] に移動します。
[ポリシー] ページが表示されます。
2. ナビゲーションペインで [ポリシー] - [ポリシー] - [SystemEDGE] を展開します。
[SystemEDGE] ページが表示され、利用可能なポリシーが一覧表示されます。
3. 以前に適切な SNMPv3 設定を使用して保存したポリシーを選択します。
[ポリシー] ページが表示されます。
4. [アクション] - [適用] をクリックします。
[マシンを選択] ページが表示されます。

5. そのポリシーを設定するシステムをすべて選択し、[適用] をクリックします。

配布ステータスを表示するか、または [ポリシー] ページに戻ることができます。

新しい設定がターゲット システムに適用されます。

代替方法

リモート システムに **SystemEDGE** を展開し、**SNMPv3** 認証情報を使用する場合は、パッケージ ラッパーにポリシーを適用し、展開ジョブを実行できます。

システム サマリの SNMPv3 設定を確認します。

SNMPv3 設定がターゲット システムに正しく適用されたことを確認するには、**CA Virtual Assurance** ユーザ インターフェースの [エクスプローラ] ペインに切り替えます。

次の手順に従ってください:

1. [エクスプローラ] ペインのコンポーネント ツリーを展開します。
2. **SNMPv3** 設定を適用した管理対象システムを選択し、[サマリ] を開きます。
[マシン ステータス情報] が表示されます。
3. [アクティブな **SNMP** 認証情報] フィールドに、**SNMPv3** グローバル オブジェクトが表示されていることを確認します。

注: 管理対象サーバに純粋な **SNMPv3** 設定を適用しており、そのサーバで **SystemEDGE** のコントロール パネル (Windows のみ) を開いた場合は、コミュニティとトラップのフィールドは空です。 **SystemEDGE** のコントロール パネルには、これらのフィールドの **SNMPv1** 情報が表示されます。

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 SNMP Event Manager にイベントを転送するように製品を設定します。この処理は、次の 2 つの部分で構成されます。

1. CA Virtual Assurance のトラップまたはイベントを受信するためにイベント マネージャを設定します。
2. イベントを転送するために CA Virtual Assurance を設定します。

以下の手順では、イベントを受信するためにイベント マネージャのコンソールを設定したと想定しています。

次の手順に従ってください:

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. + (追加する) 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. [サーバ] フィールドに管理サーバの名前を入力します。
7. 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。
8. [OK] をクリックします。
確認メッセージが表示されます。
9. [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。

SystemEDGE および AIM の展開方法

このセクションでは、モニタリング ソフトウェアを正しく展開するためのジョブを設定および管理する方法について説明します。

関連項目：

[概要](#) (P. 143)

[設定](#) (P. 146)

[スケーラビリティ](#) (P. 150)

[展開パッケージ](#) (P. 152)

[リモート展開の使用](#) (P. 169)

[具体的なリモート展開の使用例](#) (P. 184)

[展開ジョブ](#) (P. 192)

[インフラストラクチャ展開プロセス](#) (P. 193)

概要

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。カスタマイズされたインストールパラメータを含む付属パッケージに基づいて展開テンプレートを作成すると同時に、そのようなテンプレートを多数の管理対象システムに展開できます。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展開方法を定義する設定を作成、編集、および削除できます。これらの設定は、「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、取り消し、およびフィルタリングが可能になり、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

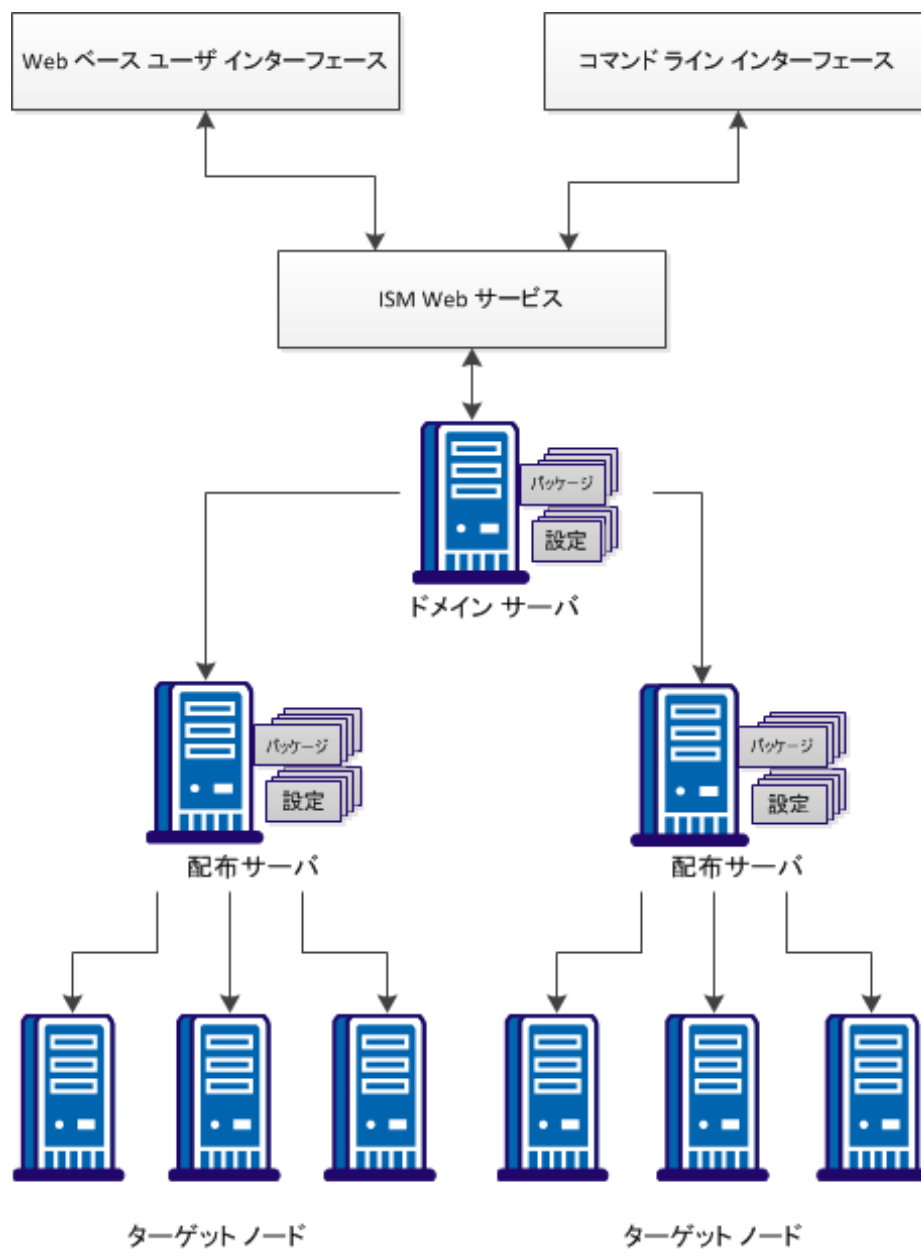
展開ジョブのステータスをクエリすることができます。

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。



パッケージについて

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。展開パッケージは、プラットフォームに固有なパッケージ ラッパーに分かれています。パッケージ ラッパーは、エージェント ソフトウェアをインストールするのに必要なインストール パラメータをカプセル化します。また、展開をサポートするすべてのプラットフォームで使用できます。

注: デフォルトのパッケージ ラッパー名がローカライズされておらず、サポートされたすべての言語で「**default**」と表示されます。カスタムのパッケージ ラッパー名はローカライズされています。

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。

設定

このセクションでは、リモート展開のユーザ インターフェース設定と配布サーバの接続に関する詳細について説明します。

関連項目:[展開ダッシュボードビュー \(P. 147\)](#)[リモート展開の検索機能の強化 \(P. 148\)](#)[ジョブステータス フィルタ \(P. 149\)](#)[配布サーバが接続するドメイン サーバの変更 \(P. 149\)](#)**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。

リモート展開の検索機能の強化

検索機能が強化されたことにより、リモート展開に関連するキーワードで検索を実行し、この結果からリモート展開操作に迅速にアクセスできるようになりました。この機能の利点は以下のとおりです。

この機能の利点は以下のとおりです。

- リモート展開コンポーネントに迅速にアクセスできる。
- サーバとサービスにリモート展開ソフトウェア パッケージを展開できる。
- リモート展開ソフトウェア パッケージおよびテンプレートを管理できる。
- 展開ジョブを迅速に作成および管理し、利用可能なパッケージおよびラッパーにアクセスできる。

次の手順に従ってください:

1. [値] フィールドにキーワード（またはワイルドカードを使用した部分的な値）を入力して、[検索] をクリックします。

例:

「展開」、「リモート」、または「リモート展開」などを指定します。

[リモート展開] リンクのリストが表示されます。

2. 適切なリモート展開操作を選択します。

リモート展開操作を実行します。

ジョブステータス フィルタ

ジョブステータス データは各ジョブに関連する詳細のみを表示するためにフィルタされます。列を並べ替えてカスタマイズすることや、1 つ以上の列によってフィルタ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] - [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. [ジョブ] をクリックします。
右側のペインにジョブの詳細が表示されます。
3. (オプション) [ジョブステータス] 列のチェック ボックスを選択/選択解除します。
カスタマイズされた列が表示されます。
4. 列のフィルタを選択/選択解除します。
フィルタの選択に基づいてジョブが表示されます。

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] ユーザー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 Distribution Server] 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ています。

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。

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。

注: 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。

展開の推奨事項：

- 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。
- 追加の配布サーバは、ターゲットのローカルの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。

注：CA Virtual Assurance スケーラビリティの詳細については、「スケーラビリティのベスト プラクティス」を参照してください。

複数の配布サーバ

リモート展開ソリューションでは、すべての展開で単一の中央サーバ（マネージャ）を使用できますが、以下の要件のいずれかを満たす場合は、中央のドメイン 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推奨します。

- 2 か所以上の地理的に離れた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、中央のドメイン サーバに接続された配布サーバを少なくとも 1 つ配置することを推奨します。

- 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、複数のサブネットにわたって論理的に分離された多数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、中央のドメインサーバに接続されています。

展開パッケージ

展開パッケージは、企業全体にわたってモニタリング用ソフトウェアをシステムに展開するために必要な要素を提供します。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。

重要: AIM は SystemEDGE および Advanced Encryption パッケージに依存します。これらのパッケージのいずれかを展開するには、SystemEDGE と Advanced Encryption がシステムにすでに存在するか、または展開ジョブに含まれている必要があります。

以下の展開パッケージが利用可能です。

Performance Agent (CA Systems Performance LiteAgent)

Windows、UNIX、または Linux のパフォーマンス メトリックをモニタおよび収集するための軽量なモニタリング エージェントを提供します。

SystemEDGE

コア SystemEDGE エージェントを提供します。

SystemEDGE ADES

Active Directory および Exchange Server 用の AIM 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

IBM PowerVM (LPAR) 用の AIM を提供します。

SystemEDGE CXEN

Citrix XenServer 用の AIM を提供します。

SystemEDGE Citrix XenDesktop

Citrix XenDesktop 用の AIM を提供します。

SystemEDGE GalaX

Huawei GalaX8800 用の AIM を提供します。

SystemEDGE Hyper-V

Microsoft Hyper-V 用の AIM を提供します。

SystemEDGE IBM PowerHA

IBM PowerHA（旧名称「Availability Cluster Multi-Processing」）用の AIM を提供します。

SystemEDGE KVM

KVM テクノロジーに基づき、RHEV（Red Hat Enterprise Virtualization）用の AIM を提供します。

SystemEDGE MSCS

Microsoft クラスタ サポート（MSCS）用の 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 Zone

Oracle Solaris ゾーン用の AIM を提供します。

SystemEDGE SRM

サービス レスポンス モニタ AIM を提供します。

SystemEDGE UCS

Cisco UCS 用の AIM を提供します。

SystemEDGE VC

VMware vCenter 用の AIM を提供します。

SystemEDGE VCLLOUD

VMware vCloud Director 用の AIM を提供します。

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、選択したソフトウェア パッケージ用に一連のデフォルト値が設定されたインストーラ パラメータが含まれます。パッケージが必須パラメータを必要とする場合は、これらのパラメータを指定し、パッケージを展開する前に設定を保存します。

パッケージのインストーラ パラメータ値を変更する必要がある場合を除き、パラメータを再度編集する必要はありません。必須パラメータを指定せずにパッケージを展開しようとすると、展開プロセスは停止されます。このようなパッケージ ラッパーは展開可能な状態ではありません。

利用可能なパッケージラッパーには、以下のパラメータが含まれます。必須パラメータは、ユーザ インターフェースで以下のように示されます。

SystemEDGE

[管理] - [設定] - [SNMP] で指定されたグローバル **SNMP** 設定によって、**SystemEDGE** パッケージラッパーの以下のフィールドのドロップダウン リストが入力されます。

- ポート
- 読み取りコミュニティ
- 読み取り/書き込みコミュニティ

あるいは、フィールドをインラインで編集できます。

利用可能なコミュニティ文字列はポート設定によって異なります。ポート番号を初めて選択するときには、そのポート用のドロップダウン リストに有効なコミュニティ文字列が自動的に取得されます。

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。

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

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。

Location

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。また、このエージェントは、このユーザのデフォルト グループを有効なグループとして使用します。

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

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。

注: [再起動の抑制] チェック ボックスは Windows パッケージでのみ利用可能です。

[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: 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。

CA SystemEDGE ADES

Windows ドメイン

モニタする Windows ドメインを指定します。

ドメイン ユーザ

ドメイン サーバまたは Exchange Server に接続するためのドメイン 管理者ユーザを指定します。

ドメイン ユーザ パスワード

ドメイン サーバまたは Exchange Server に接続するためのドメイン 管理者ユーザのパスワードを指定します。

管理エンティティ

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。

管理モード

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。

[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 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。

CA SystemEDGE AIX LPAR

LPAR ホスト

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ための IBM LPAR のホスト名を指定します。

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ための IBM LPAR のユーザ名を指定します。

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ための IBM LPAR パスワードを指定します。

CA SystemEDGE CXEN

CXEN ホスト名

Citrix XenServer の統合に使用するホスト名を指定します。

CXEN ユーザ名

Citrix XenServer の統合に使用するユーザ名を指定します。

CXEN パスワード

Citrix XenServer の統合に使用するパスワードを指定します。

[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。

CA SystemEDGE CXenDesktop

ホスト名

Citrix XenDesktop 統合に使用するホスト名を指定します。

ユーザ名

Citrix XenDesktop 統合に使用するユーザ名を指定します。

パスワード

Citrix XenDesktop 統合に使用するパスワードを指定します。

[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。

CA SystemEDGE GalaX

[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。

CA SystemEDGE PowerHA

ホスト名

IBM PowerHA 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ための PowerHA ホスト名を指定します。

ユーザ名

IBM PowerHA 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ための PowerHA ユーザ名を指定します。

パスワード

IBM PowerHA 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ための PowerHA パスワードを指定します。

ポート

PowerHA ポート番号を定義します。

デフォルト : 22

[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。

CA 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。

CA SystemEDGE KVM (RHEV)**KVM Hostname**

RHEV (Red Hat Enterprise Virtualization) に接続するためのホスト名を指定します。

KVM Username

RHEV に接続するためのユーザ名を指定します。

KVM Password

RHEV に接続するためのパスワードを指定します。

KVM Port

RHEV に接続するためのポートを指定します。

デフォルト : 8443

[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。

CA SystemEDGE MSCS**MSCS ホスト名**

クラスタに接続するためのホスト名を指定します。

MSCS ユーザ名

クラスタに接続するためのユーザ名を指定します。

MSCS パスワード

クラスタに接続するためのパスワードを指定します。

[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。

CA 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ためのユーザ名を指定します。

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ためのパスワードを指定します。

[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。

CA 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。

[信頼できない SSL の許可]チェック ボックス

未検証の証明書による 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。

[ユーザ TOS の無効化]チェック ボックス (Windows)

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。

[再起動の抑制]チェック ボックス (Windows)

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。

CA SystemEDGE Solaris ゾーン

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ための Solaris ゾーン ホスト名を指定します。

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ための Solaris ゾーン ユーザ名を指定します。

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ための Solaris ゾーン パスワードを指定します。

CA 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ための UCS ホスト名を指定します。

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ための UCS ユーザ名を指定します。

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ための UCS パスワードを指定します。

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。

[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。

CA SystemEDGE VC

ホスト名

vCenter 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ための vCenter ホスト名を指定します。

ユーザ名

vCenter 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ための vCenter ユーザ名を指定します。

パスワード

vCenter 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ための vCenter パスワードを指定します。

ポート

vCenter ポート番号を定義します。

デフォルト : 443

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。

CA SystemEDGE VCLOUD

VCLOUD ホスト名

vCloud への接続に使用するホスト名を指定します。

VCLOUD username

vCloud への接続に使用するユーザ名を指定します。

VCLOUD パスワード

vCloud への接続に使用するパスワードを指定します。

VCLOUD ポート

vCloud のポート番号を定義します。

デフォルト : 443

[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。

CA Systems Performance LiteAgent

共有パス

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

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。

関連項目

[新規パッケージ ラッパーの作成 \(P. 171\)](#)

[パッケージ ラッパーの変更 \(P. 172\)](#)

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」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%\CA¥SM¥domainserver¥Deployment¥Packages¥SM

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
│   │   ├── 5.8.0
│   │   │   ├── ENU
│   │   │   │   ├── AIX_aix
│   │   │   │   ├── HPUX_hp
│   │   │   │   ├── HPUX_ia64
│   │   │   │   ├── Linux_ia64
│   │   │   │   ├── Linux_ppc
│   │   │   │   ├── Linux_x86
│   │   │   │   ├── Solaris_sparc
│   │   │   │   ├── Solaris_x86
│   │   │   │   ├── Windows_ia64
│   │   │   │   ├── Windows_x64
│   │   │   │   └── Windows_x86
│   │   ├── CA_SystemEDGE_CXEN
│   │   ├── CA_SystemEDGE_CXENDESKTOP
│   │   ├── CA_SystemEDGE_ESAD
│   │   ├── CA_SystemEDGE_GALAX
│   │   ├── CA_SystemEDGE_HACMP
│   │   ├── CA_SystemEDGE_HyperV
│   │   ├── CA_SystemEDGE_KVM
│   │   ├── CA_SystemEDGE_LPAR
│   │   ├── CA_SystemEDGE_MSCS
│   │   ├── CA_SystemEDGE_RM
│   │   ├── CA_SystemEDGE_SRM
│   │   ├── CA_SystemEDGE_UCS
│   │   ├── CA_SystemEDGE_VCLOUD
│   │   ├── CA_SystemEDGE_Zone
│   │   └── CA_VMCAIM
```

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。

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)。

注: 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の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。

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 インターフェイスで [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 インストール要素のほか、展開可能な各パッケージは、追加のパッケージ設定ファイル `pkginfo_PLATFORM.xml` で参照されます。パッケージ設定ファイルでは、インストール パッケージと設定プロセスについて説明されています。

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。

- 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するメカニズム。
- 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の指定。
- 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。pkginfo_PLATFORM.xml と一致する名前のファイルは、ローカライズされたメッセージデータを取得するためにロードされます。

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。たとえば、以下のディレクトリを参照します。

%AllUsersProfile%¥CA¥SM¥domainserver¥Deployment¥Packages¥SM¥CA_SystemEDGE_Core¥5.7.1¥ENU

pkginfo_AIX.xml
 pkginfo_HPUX.xml
 pkginfo_Linux.xml
 pkginfo_LinuxPPC.xml
 pkginfo_Solaris_sparc.xml
 pkginfo_Solaris_x86.xml
 pkginfo_Windows.xml

リモート展開の使用

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回の操作で複数システムにモニタリングエージェントを展開できます。CA Virtual Assurance によるパッケージ展開は、セントラルインターフェースから企業全体にわたってインストールされたモニタリングソフトウェアを設定することができる、安全で信頼できるソリューションです。

展開の制限

展開を実行する前に、以下の制限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します。**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。

注: インストールの詳細については、「**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。

注: 展開のサポートの詳細については、「**CA Virtual Assurance 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。

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 システムで利用可能な 1 つ以上のパッケージを指定します。**展開タスク**は、ターゲット システム上でのソフトウェア パッケージの個別の展開を表します。展開ジョブ レポートにより、展開ジョブのステータスをクエリできます。

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。ジョブの開始後、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。

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 ラッパーのコピー

パッケージ ラッパーは、コピーし、必要に応じてそのプロパティを編集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] - [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] が表示されます。
2. [パッケージ]、パッケージの特定の種類、およびプラットフォームを展開します。
3. 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。

4. ラッパー名を右クリックします。[コピー]を選択します。[アクション] ドロップダウンメニューから [コピー] を選択することもできます。

[コピー] ダイアログ ボックスが表示されます。

5. パッケージ ラッパーの名前と任意の説明を入力し、[OK] をクリックします。

新しいパッケージ ラッパーが [展開] ペインに表示されます。

6. 必要に応じてプロパティを編集し、[保存] をクリックします。

新しいパッケージ ラッパーが左ペインに表示されます。

パッケージ ラッパーの削除

必要なくなったパッケージ ラッパーは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] - [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] が表示されます。
2. [パッケージ]、パッケージの特定の種類、およびプラットフォームを展開します。
3. 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。

4. ラッパー名を右クリックします。[削除]を選択します。[アクション]ドロップダウンメニューから[削除]を選択することもできます。
警告メッセージが表示されます。
5. [はい] をクリックして削除を確定します。
パッケージラッパーが削除されます。

パッケージラッパーの名前変更

パッケージラッパーの名前は変更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] - [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] が表示されます。
2. [パッケージ]、パッケージの特定の種類、およびプラットフォームを展開します。
3. 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。
4. ラッパー名を右クリックします。
5. [名前の変更]を選択します。[アクション]ドロップダウンメニューから[名前の変更]を選択することもできます。
[名前の変更] ダイアログボックスが表示されます。
6. 新しい名前を入力し、[OK] をクリックします。
パッケージラッパーの名前が変更されます。

展開ジョブの作成

システムにエージェントを展開するには、展開ジョブを作成します。展開ジョブには、展開パッケージを適切なシステムに適切なタイミングで配信するために、CA Virtual Assurance にとって必要な詳細が含まれます。

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] が表示されます。

2. [管理対象リソース] ペインで [ジョブ] フォルダを右クリックし、[新規ジョブの作成] を選択します。 [ジョブ] フォルダを選択し、[ジョブステータス] ツールバーの [+] (新規) をクリックする方法もあります。
[ジョブセットアップ] ページが表示されます。
3. [ジョブ名] ペインで名前を入力し、オプションで、ベースにする既存のテンプレートを選擇して、[次へ] をクリックします。
[パッケージ選擇] ページが表示されます。
4. プラットフォームと、展開するパッケージを選択します。
5. (オプション) [詳細] タブをクリックします。
[パッケージラッパー詳細] ダイアログボックスが表示され、パッケージプロパティをインラインで編集できます。 パッケージラッパーが不完全または無効な状態であっても、フィールドがインライン編集によって修正できる場合。
 - a. [編集] をクリックし、パッケージラッパーのプロパティを変更します。
 - b. [保存] をクリックし、[OK] をクリックします。
パッケージラッパーのプロパティが更新されます。
6. 下矢印をクリックしてパッケージラッパーをジョブに追加し、[次へ] をクリックします。
[マシン選擇] ページが表示されます。
7. 展開先のシステムを選択し、[次へ] をクリックします。環境内に多数のサーバがある場合、すべてのサーバを一覧表示するには、一定数のエントリを含むページが複数必要になることがあります。ページでサーバを選択し、次のページにスクロールしても、前のページで行った選擇内容は有効なままです。
[選擇済みマシン] ページが表示されます。
8. [認証情報の設定] をクリックし、接続を確立するために必要なシステム認証情報を設定して、[次へ] をクリックします。
注: ドメイン認証情報を使って Windows ターゲット システムに展開する場合は、「DOMAIN¥ユーザ名」の形式を使用する必要があります。
詳細設定ページが表示されます。
9. (オプション) 展開を管理する配布サーバを設定します。設定しない場合は、自動的に選擇されます。

10. ジョブのスケジュール オプションを選択します。

即時配布

新しい展開ジョブを作成した直後にジョブを開始します。即時配布はデフォルト オプションです。

時差配布

特定の時間にパッケージを配布します。

スケジュール済み配布

将来の特定の時間に展開をスケジュールします。

11. (オプション) 以前に同じ展開インフラストラクチャを使ってパッケージをシステムに正常に展開したことがある場合は、再度そのインフラストラクチャを強制的に実行することができます。
12. [次へ] をクリックします。
[サマリ] ページが表示されます。
13. ジョブの詳細を確認し、[展開] をクリックします。
展開ジョブが作成されます。

注: 作成したジョブはテンプレートとして保存できます。将来のジョブで簡単に再利用できるように、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ます。

展開前の読み取り/書き込みコミュニティの指定

SystemEDGE のモニタリング機能と管理機能をフルに活用するには、SystemEDGE エージェントのための有効な読み取り/書き込みコミュニティを指定する必要があります。読み取り/書き込みコミュニティ文字列は、展開の前に、SystemEDGE のリモート展開パッケージ ラッパー内で設定できます。

展開前の読み取り/書き込みコミュニティの指定

1. [リソース] - [展開] を選択します。
2. [展開] ペインを開きます。
利用可能な展開グループが表示されます。
3. [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。
4. [読み取り/書き込みコミュニティ] フィールドで読み取り/書き込みパラメータを指定し、[保存] をクリックします。

注: ユーザ インターフェイスでスペース文字またはセミコロン (;) を含むコミュニティ文字列を指定すると、エージェントは正しく機能しません。

関連項目:

[サーバ レベルの SNMP 設定の追加](#) (P. 129)

[マシンへのポリシーの適用](#) (P. 327)

インストール後の読み取り/書き込みコミュニティの指定

SystemEDGE のモニタリング機能と管理機能をフルに活用するには、SystemEDGE エージェントのための有効な読み取り/書き込みコミュニティを指定する必要があります。SystemEDGE エージェントをすでに展開している場合、インストール後に読み取り/書き込みコミュニティ文字列を追加できます。これは、複数システムのモニタおよび管理に使用できるグローバル **SNMP** エントリを作成することにより、またはサーバ固有 **SNMP** エントリを作成することにより、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. [サーバ固有 **SNMP** 設定のみを含める] を選択します。
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。

グローバル **SNMP** エントリを作成する方法

1. [管理] をクリックします。
[管理] ページが表示されます。
2. [設定] をクリックします。
[設定] ページが表示されます。
3. [SNMP] をクリックします。
4. リストで、編集する **SNMP** 設定のチェック ボックスをオンにし、ツールアイコン (編集) をクリックします。
[SNMP 設定の編集] ダイアログ ボックスが表示されます。
5. [アクセス タイプ] ドロップダウン リストから [読み書き] を選択し、[コミュニティ文字列] フィールドにパラメータを指定して、[OK] をクリックします。

6. [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。
7. [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。
8. [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。
9. [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。
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、「マシンへのポリシーの適用」を参照してください。

関連項目:

[サーバレベルの SNMP 設定の追加 \(P. 129\)](#)

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] タブには、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。

注: [ジョブステータス] ペインで、フィルタを選択して特定のジョブタスクをフィルタできます。

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] が表示されます。

2. [ジョブ] フォルダをクリックします。
[ジョブ ステータス] ページが表示されます。
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] をクリックしてタスクの拡張情報を表示します。
タスク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

タスクに関する一般情報を表示します。

メッセージ

タスク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。

例：

- 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

アクション

問題を修正するため取るアクションを表示します。

展開ジョブの再サブミット

失敗した、または部分的に失敗した展開ジョブは、再サブミット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] - [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] が表示されます。
2. [ジョブ] フォルダをクリックします。
[ジョブ ステータス] ページが表示されます。
3. 再サブミット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. [アクション] をクリックし、[再サブミット] を選択します。
[パッケージ選択] 画面に展開ウィザードが表示されます。
5. 展開する希望のパッケージ ラッパーを選択し、[次へ] をクリックします。
[選択済みマシン] ページが表示されます。
6. (オプション) 展開したくないマシンを削除します。
注: すべてのパッケージが以前正常に展開されたマシンは選択されません。
7. [認証情報の設定] をクリックし、選択したすべてのマシンの認証情報を適宜変更します。オプションで、再起動ジョブからマシンを削除し、[次へ] をクリックします。
詳細設定ページが表示されます。

8. (オプション) ジョブのスケジュール オプションを変更します。

即時配布

新しい展開ジョブを作成した直後にジョブを開始します。即時配布はデフォルト オプションです。

時差配布

特定の時間にパッケージを配布します。

スケジュール済み配布

将来の特定の時間に展開をスケジュールします。

9. すべてのパッケージ (以前展開に成功したパッケージを含む) を強制的に展開するには、[以前展開されていたパッケージの再展開] を選択し、[次へ] をクリックします。

[サマリ] ページが表示されます。

10. ジョブの詳細を確認し、[展開] をクリックします。

ジョブが再サブミットされます。

展開済みパッケージの表示

[モニタリング ソフトウェア] ページでは、単一のマシンまたは複数のマシンに展開したパッケージのリストを表示できます。

展開済みのパッケージを表示する方法

1. [リソース] を選択します。

[エクスプローラ] ペインが表示されます。

2. システムまたはサービスを選択します。

[サマリ] ページが表示されます。

3. [モニタリング ソフトウェア] - [展開] を選択します。

[展開履歴] ページが開き、マシンの全展開ジョブのリストが示されます。テーブルには、選択したシステムの全展開ジョブの詳細が表示されます。

- タスク ID
- ジョブ ID

- ターゲット
- パッケージ
- プラットフォーム
- ラッパー
- ラッパー バージョン
- 開始者
- 開始時刻
- 終了時刻
- ステータス
- 拡張ステータス

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

注: 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。

具体的なリモート展開の使用例

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ースで [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する必要があります。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ースで [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。

SystemEDGE エージェント ポートの再設定

SystemEDGE エージェント ポートは、標準（デフォルト）ポート 161 から 1691 に再設定できます。たとえば、デフォルト ポート 161 上で MIB-II エージェントを実装する Microsoft SNMP サービスをインストールすることができます。sysedge.cf ファイルを編集する方法は、エージェント ポートを再設定するためのサポートされている方法ではありません。ポートの変更は、エージェントの再インストールによって実行する必要があります。これは、別のポートを指定するリモート展開を使用して、エージェントを再展開することにより実行できます。Windows システムの場合、SystemEDGE コントロール パネル アプレットを使用して、エージェントを再設定することもできます。

コントロール パネルでの SystemEDGE エージェントの再設定

1. [スタート] - [コントロール パネル] をクリックして、[プログラムの追加と削除] を選択します。さらに、リスト内の SystemEDGE Core を選択して、[変更] をクリックします。

SystemEDGE セットアップ ウィザードが開きます。

2. [次へ] をクリックします。

[再インストール タイプ] ページが表示されます。

3. [再インストール] を選択し、[次へ] をクリックします。

[アプリケーション設定] ページが開き、インストール文書設定を変更できます。

4. [次へ] をクリックします。

[SystemEDGE SNMP ポート番号] ページが開きます。

5. SystemEDGE ポート番号 1691 を指定し [次へ] をクリックします。

6. 設定を確認し、[再インストール] をクリックします。

SystemEDGE エージェントはポート番号 1691 を使用するよう再設定されます。

リモート展開/ポリシー設定を使用する SystemEDGE エージェント ポートの再設定

1. 「[展開ジョブの作成](#) (P. 174)」の章にある手順に従ってください。ウィザードの手順 5 で、「以前展開されていたパッケージの再展開」を選択します。

注: 再インストールでは、ポート番号以外のすべての指定されたインストールパラメータは無視されます。

ポートを変更するためにエージェントを再インストールした後、正しいコミュニティ文字列でエージェントが設定されていることを確認するために、管理者はいくつかの手順を手動で実行する必要があります。

2. 以下のいずれかを実行します。

サーバ用のサーバ固有 SNMP エントリを作成する。

1. CA Virtual Assurance UI で [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、Machine_Name を選択します。

Machine_Name が選択されます。

2. Machine_Name を右クリックし、[ポリシー] - [SNMP の設定] を選択します。

[SNMP 設定] ページが表示されます。

3. [追加] をクリックして、必要なポートに新しいエントリを作成します。

[新しい SNMP 設定] ページが表示されます。

4. 必要な詳細を入力して、[OK] をクリックします。

サーバ用に、サーバ固有の SNMP エントリが作成されます。

グローバル SNMP 設定が存在し、ポリシーを更新することを確認する。

CA Virtual Assurance の UI で、[管理] - [SNMP] にナビゲートし、必要なポートの新しいエントリを追加します。設定が正しければ、[リソース] タブに移動して [設定] ペインを開き、ポリシーを選択してポリシーを編集します。次に、[トラップ & コミュニティ] - [コミュニティ] をクリックし、中央のオプション [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] を選択します。[ポリシーの保存] をクリックして、ポリシーを保存します。この時点で、[システムにポリシーを適用](#) (P. 327) する必要があります。エージェントマシン上で SystemEDGE コントロールパネルアプレットを使用して、エージェントによって使用されるコミュニティ文字列を確認できます。

注: 詳細については、「Administration Guide」の「Deploying/Installing SystemEDGE Agents Using Custom Ports」を参照してください。

関連項目:

[サーバレベルの SNMP 設定の追加](#) (P. 129)

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 *
```

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。「**id**」および「**sh**」のパスが **/usr/bin/id** または **/bin/sh** とは異なる場合は、設定エントリのパスを適切に調整してください。

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」プロファイルを付与できます。

```
usermod -P "Primary Administrator" {user}
```

- **/etc/user_attr** ファイル内のエントリを手動で追加することで、すべての非ローカルユーザに「プライマリ管理者」プロファイルを付与できます。

```
user::::type=normal;profiles=Primary Administrator
```


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に対する書き込みコミュニティの設定は必須ではありませんが、以下の情報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** を使用するようエージェントを設定することもできます。

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

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、最初に展開ジョブを作成します。展開ジョブには、展開パッケージを適切なシステムにスケジュールされた時間で配信するために、CA Virtual Assurance にとって必要な詳細が含まれます。いくつかの場所からアクセス可能なリモート展開ジョブウィザードを使用して、新規ジョブを作成できます。以下のいずれかの方法を選択します。

- ダッシュボードの [クイック起動] パネルにある [ジョブの展開] リンクを使用する
- [リソース] - [展開] タブの [ジョブ] パネルから [+] (新規) ボタンを使用する
- [リソース] - [エクスプローラ] タブにある管理対象ノードのコンテキストメニューを使用する
- [リソース] - [エクスプローラ] タブにある現在選択されている管理対象ノードの [モニタリング ソフトウェア] - [展開] タブから [+] (新規) ボタンを使用する

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。

IP Address

ジョブを展開するインターフェースの IP アドレスを指定します。システムに複数の IP アドレスがある場合は、管理プロパティを持つ IP アドレスをデフォルトとして設定します。

注: 管理プロパティが有効になっていない IP アドレスは選択できません。

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。将来のジョブで簡単に再利用できるように、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。

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. 195)

[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. 198)

[IDManager が使用する転送パッケージのプロトコル](#) (P. 198)

[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. 199)

[Windows での展開プライマ インストール](#) (P. 199)

[Linux または UNIX での展開プライマ インストール](#) (P. 200)

[展開管理証明書のプライマ インストールへの提供](#) (P. 200)

[Windows 上の展開管理証明書](#) (P. 200)

[Linux または UNIX 上の展開管理証明書](#) (P. 201)

[Linux の Compatibility Library](#) (P. 201)

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 システムの機能によってのみ実行できます。このインストールは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。**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 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、使用される共有名は **ADMIN\$** です。**IDManager** 設定オプションはデフォルトの共有名を制御します。このメカニズムは、**Windows** ベースの環境で実行している展開マネージャからのみ使用可能です。**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 コンピュータ上でファイアウォールを実行している場合は、以下の条件が満たされることを確認します。

- SSH ポート (22) は展開マネージャからの接続を許可するために有効にされます
- 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ます

注: 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. 188)」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 を使用するよう設定します。SSH を設定するには、`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します。

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と、ステータスが「プライマ 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するなど、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、許可された展開を実行する前に、有効な認証情報を入力します。

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します。展開リクエスト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ます。

デフォルトの共有 : ADMIN\$

- 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する必要があります。

関連項目

[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 \(P. 188\)](#)

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。

32 ビット Windows で有効

```
%PROGRAMFILES%\CA\SC\IDMgrApi\packages\private\idprimer\Windows_x86
```

64 ビット Windows で有効

```
%PROGRAMFILES(X86)%\CA\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 installidp
```

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 32 ビット ライブラリ 依存関係が存在することを前提としています。IDPrimer をインストールするには、これらの 32 ビット ライブラリが Linux ホスト上に存在している必要があります。

ほとんどの 32 ビットの Linux ディストリビューションでは、デフォルトですでにインストールされています。64 ビットの Linux の依存関係を満たすには、以下のコマンドを実行します。

- RedHat、CentOS、SuSE（32 ビットおよび 64 ビット OS）で有効：

```
yum install libstdc++.i686
```

このコマンドは、glibc、libstdc++、nss-softokn-freebl および libgcc の合計 4 つの RPM パッケージにインストールされます。

- Debian（64 ビット）で有効：

```
apt-get install ia32-libs
```

このコマンドは必須の 32 ビット ライブラリ（libc、libstd++、libgcc）をインストールします。

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 サプライヤのサポート Web サイトを参照してください。

関連項目：

[インフラストラクチャ展開プロセス \(P. 193\)](#)

ポリシーとテンプレートを使用した SystemEDGE およびサービス レスpons モニタの設定方法

このセクションでは、制御の中心点である CA Virtual Assurance から、環境内のモニタリング ソフトウェアを管理する方法について説明します。

関連項目：

[設定の概要 \(P. 202\)](#)

[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 \(P. 205\)](#)

[自動ウォッチャーを作成してシステムに適用する方法 \(P. 250\)](#)

[ユーザ固有のメトリック（MIB 拡張）をモニタする方法 \(P. 259\)](#)

[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 \(P. 262\)](#)

[SRM ポリシーを作成する方法 \(P. 266\)](#)

[エージェントの検出 \(P. 267\)](#)

[ポリシー設定機能の一般的な使用法 \(P. 267\)](#)

設定の概要

CA Virtual Assurance ユーザ インターフェースから一元化された [ポリシー 設定] 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、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. 268)

[SRM ポリシーを作成する方法](#) (P. 266)

[マシンへのポリシーの適用](#) (P. 327)

[ポリシー適用の進捗状況の確認](#) (P. 329)

[適用されるポリシーの設定と表示](#) (P. 330)

[エージェント ポリシーのダッシュボード ビュー](#) (P. 204)

[ユーザ固有のメトリック \(MIB 拡張\) をモニタする方法](#) (P. 259)

[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. 262)

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、ポリシー設定で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。

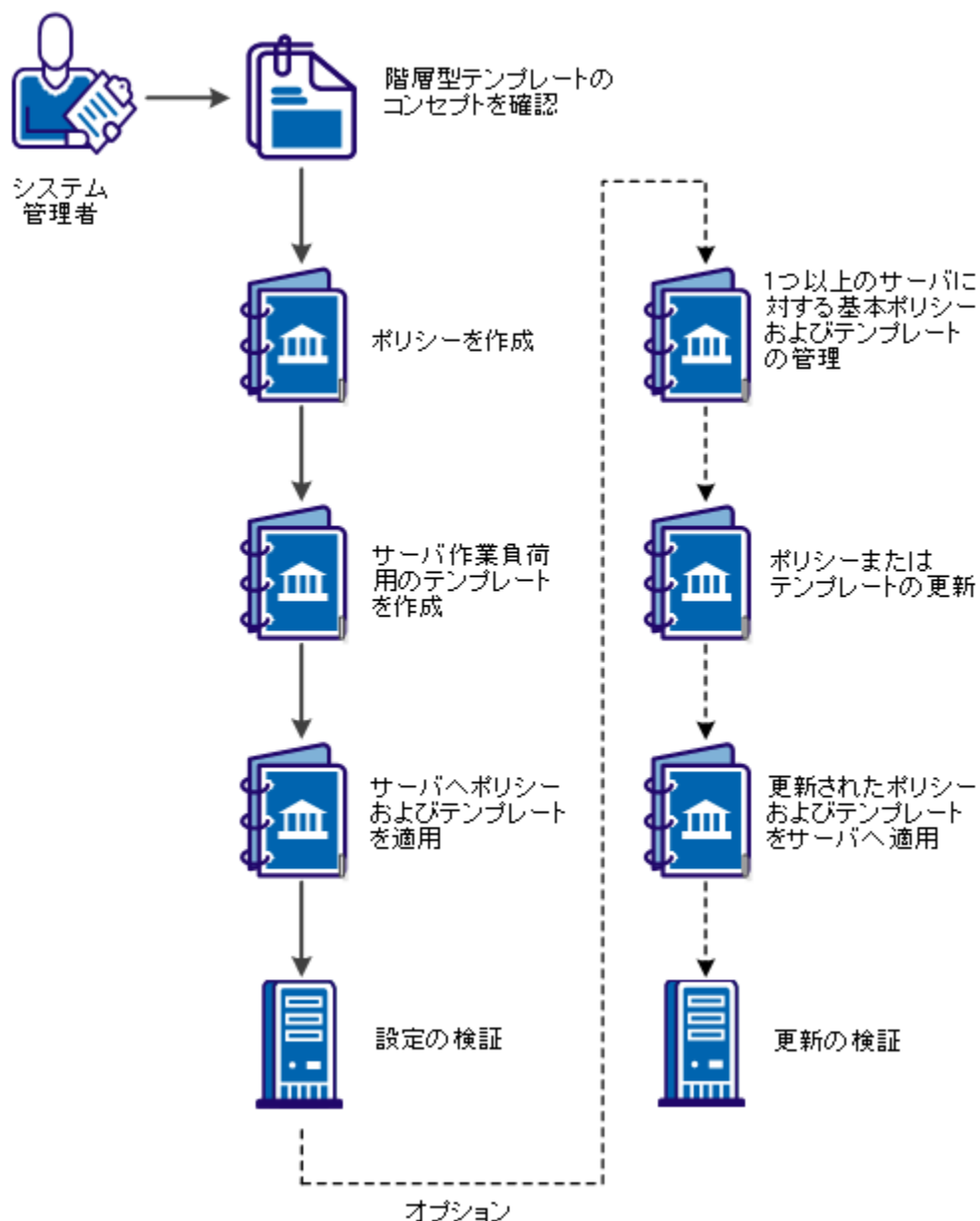
標準以外のポリシーを持つマシン

適用されたポリシーに対する標準以外の変更が含まれるシステムが表示されます。

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



以下の手順に従います。

[階層型テンプレートの概念](#) (P. 207)

[ポリシーの作成](#) (P. 210)

[サーバワークロード用のテンプレートの作成](#) (P. 224)

[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](#) (P. 244)

[\(オプション\) サーバのベース ポリシーおよびテンプレートの管理](#) (P. 246)

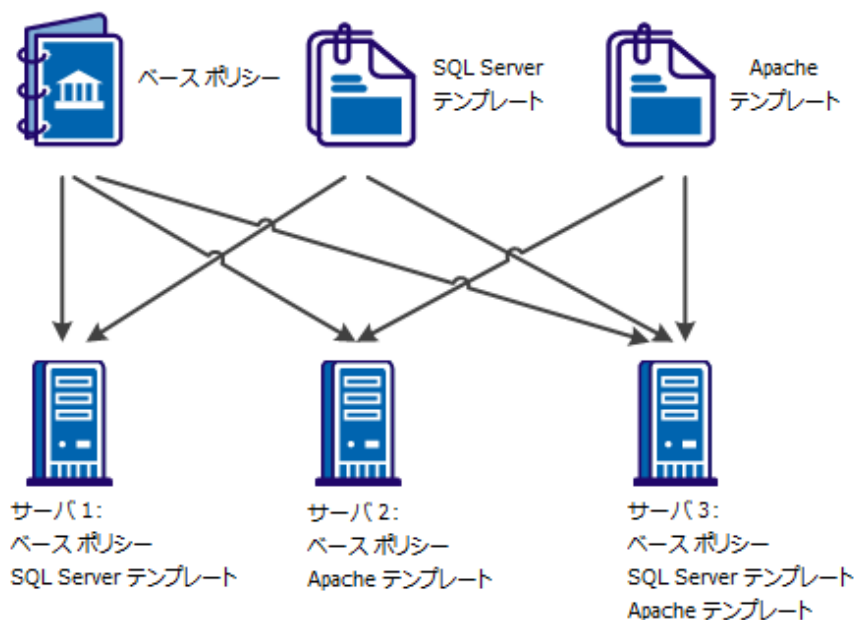
[\(オプション\) ポリシーまたはテンプレートの更新](#) (P. 244)

[\(オプション\) 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](#) (P. 248)

階層型テンプレートの概念

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。

すぐに使用できるテンプレート

すぐに使用できるテンプレートを管理対象ノードに適用できます。管理対象ノードに対するテンプレート設定を使用してポリシーを設定します。テンプレートは以下のオペレーティング システムに利用可能です。

すべてのオペレーティング システム用:

- CPU Utilization - Autowatch

- Swap Capacity

Windows の場合:

- App Monitoring - CA eTrust Antivirus

- Process Crash

- System Errors

- System Processes

- User Activity

- Windows Services - Autowatch

UNIX (AIX、HPUnix、Linux、Solaris) :

- System Messages

- System Processes

- User Activity

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。

関連項目:

[SystemEDGE ポリシーのコピー \(P. 268\)](#)

[SystemEDGE ポリシーの名前変更 \(P. 269\)](#)

[SystemEDGE ポリシーの削除 \(P. 269\)](#)

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

システム管理 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、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 (ディスクのプロンプ)
- 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 \(P. 218\)](#)」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 \(P. 278\)](#)

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 \(P. 271\)](#)

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 \(P. 225\)](#)」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 \(P. 239\)](#)」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. 226)
 - [プロセス モニタの作成](#) (P. 229)
 - [ログ ファイル モニタの作成](#) (P. 231)
 - [Windows イベント モニタの作成](#) (P. 233)
 - [履歴モニタの作成](#) (P. 235)
 - [プロセス グループ モニタの作成](#) (P. 237)
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。

関連項目:

[しきい値モニタの定義 \(P. 290\)](#)

[プロセス モニタの定義 \(P. 293\)](#)

[ログ ファイル モニタの定義 \(P. 295\)](#)

[Windows イベント モニタの定義 \(P. 297\)](#)

[履歴モニタの定義 \(P. 299\)](#)

[プロセス グループ モニタの定義 \(P. 301\)](#)

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ったと、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。

開始時刻

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。

停止時刻

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ったら、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=1.3.6.1.4.1.546.1.1.7.1.14`) 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。

開始時刻

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。

停止時刻

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 \(P. 240\)](#)」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。

(オプション)テンプレートまたはポリシーからのモニタのインデックス再作成

[しきい値]、[プロセス]、[ログ ファイル]、[Windows イベント]、[履歴]、および [プロセス グループ] タブのモニタには、インデックスを再作成することができます。インデックスの再作成によって、既存のインデックスに連続する値が割り当てられます。

注: モニタにインデックスを再作成すると、将来のインデックスが次の論理的なベース インデックスから開始されるようになります。

モニタにインデックスを再作成するには、以下を考慮します。

- モニタが存在することを確認します。

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. [モニタ] タブをクリックします。
[サマリ] ページが開き、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、[アクション]をクリックして、[再インデックス付け] を選択します。

新しいベース インデックスのダイアログ ボックスが表示されます。

5. ベース インデックスとして数値を入力します。

例：1000

6. [インデックスを連続させます] を選択します。

[インデックスを連続させます]

[インデックスを連続させます] オプションを選択して、既存のインデックスが連続するようにします。

例：1001、1002、1003、1004 など。

注: このオプションを選択しないと、インデックス間の欠番は保持されます。

例：1001、1010、1020、1030 など。

7. [OK] をクリックしてインデックスの再作成を確定します。

モニタにインデックスが再作成されます。

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 1 つまたは複数選択します。

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。

(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 \(P. 225\)](#)」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 \(P. 243\)](#)」を参照してください。
2. [MIB 拡張を定義 \(P. 239\)](#) します。
3. [SystemEDGE ポリシー制御設定を定義 \(P. 211\)](#) します。
ポリシーまたはテンプレートが更新されます。

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]

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します。

[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]

システムにポリシーまたはテンプレートを適用します。

4. (ポリシーの場合のオプション) [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。

- ポリシーの期限切れバージョンを実行しているマシン
- ポリシー例外が適用されているマシン
- ポリシーの現在のバージョンを実行しているマシン
- このポリシーに対して設定エラーがあるマシン

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 (手動でマシンを選択)] を選択して、[マシンを選択] ペインにポリシーを再割り当てするマシンを手動で追加します。

5. (テンプレートの場合のオプション) [このテンプレートを実行しているマシンを更新] タブから、以下のいずれかを選択します。

[既存のマシン] で、以下のいずれかのオプションを選択します。

- このテンプレートを適用してすべてのマシンを更新
- このテンプレートの最新の変更が適用されていないマシンのみを更新
- テンプレートが正常に適用されていないマシンのみを更新
- 詳細 (手動でマシンを選択)
- マシンからこのテンプレートを削除

6. (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。
7. [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。
8. 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. 225)」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. 243)」を参照してください。
2. [MIB 拡張を定義](#) (P. 239) します。
3. [SystemEDGE ポリシー制御設定を定義](#) (P. 211) 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。

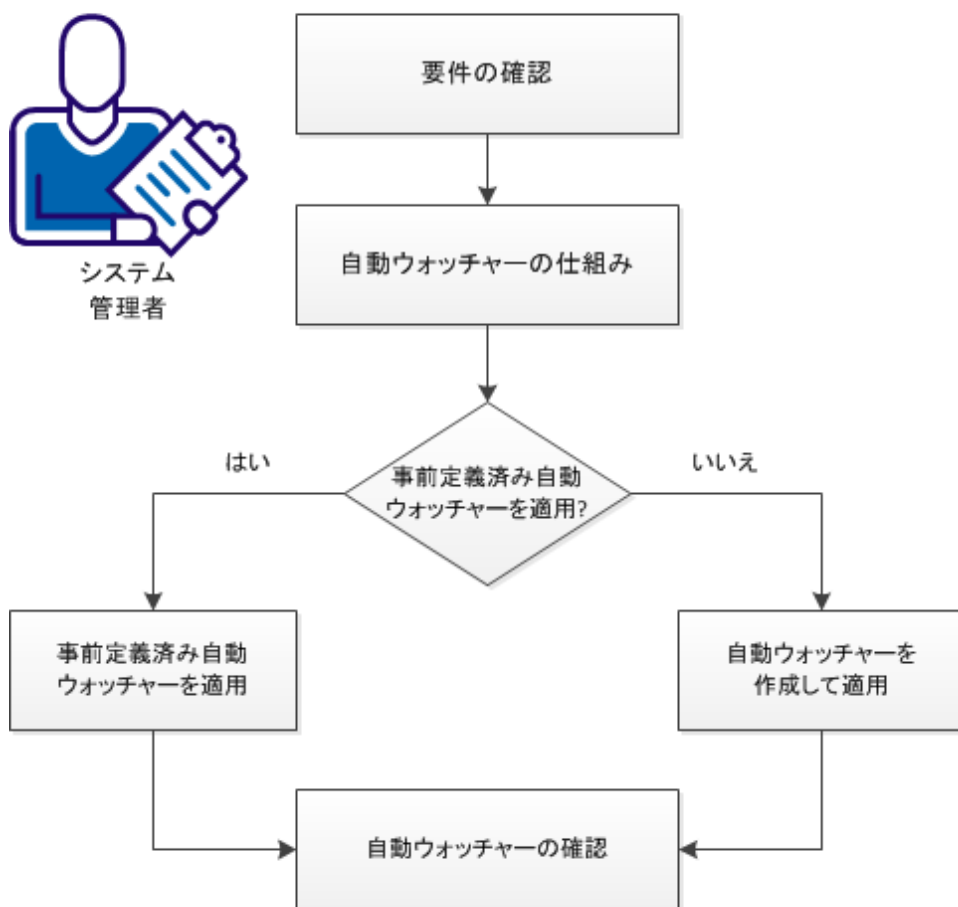
自動ウォッチャーを作成してシステムに適用する方法

このシナリオでは、システム管理者が自動ウォッチャーを使用して、管理対象システムのリソースを動的にモニタする方法について説明します。

管理対象システムに追加および削除されるリソースの検出に、自動ウォッチャーを使用できます。リソースが追加される場合、自動ウォッチャーは対応するモニタを作成します。リソースが削除される場合、自動ウォッチャーは「消失アクション」を実行します。

以下の図は、管理対象システムに自動ウォッチャーを作成して適用する方法の概要を示しています。

自動ウォッチャーを作成してシステムに適用する方法



以下の手順に従います。

[要件の確認 \(P. 251\)](#)

[自動ウォッチャーの仕組み \(P. 252\)](#)

[事前定義済み自動ウォッチャーの適用 \(P. 256\)](#)

[自動ウォッチャーの作成とシステムへの適用 \(P. 257\)](#)

[自動ウォッチャーの確認 \(P. 258\)](#)

要件の確認

SystemEDGE 用の自動ウォッチャーを作成する前に、以下の要件を確認します。

- TCP/IP および SNMP に精通している。
- CA Virtual Assurance および SystemEDGE に関する基礎知識がある。
- CA Virtual Assurance ユーザ インターフェースにアクセスできる。
- 影響を受ける SystemEDGE エージェントが管理対象モードで実行されていることを確認する。

関連項目：

[事前定義済み自動ウォッチャーの適用 \(P. 256\)](#)

[自動ウォッチャーの作成とシステムへの適用 \(P. 257\)](#)

自動ウォッチャーの仕組み

自動ウォッチャーは、自動ウォッチャーがモニタを作成するリソースの名前に一致するパターンとして正規表現を使用して、定期的なディスカバリプロセスを実行します。自動ウォッチャーを使用すると、新しいリソースがオンラインになるときに、これらに対するモニタを **SystemEDGE** で自動的に作成できます。自動ウォッチャーは予約済みのインデックス範囲（1000000 ～ 1999999）でモニタを作成します。

リソースが非表示になるとき、**SystemEDGE** は **CA Virtual Assurance** にトラップを送信し、自動ウォッチャーで設定した「消失アクション」を適用します。モニタ対象のリソースが消失する場合には、「消失アクション」によってモニタを削除したり、リソースのステータスを以下の特定のステータスに設定したりすることができます。

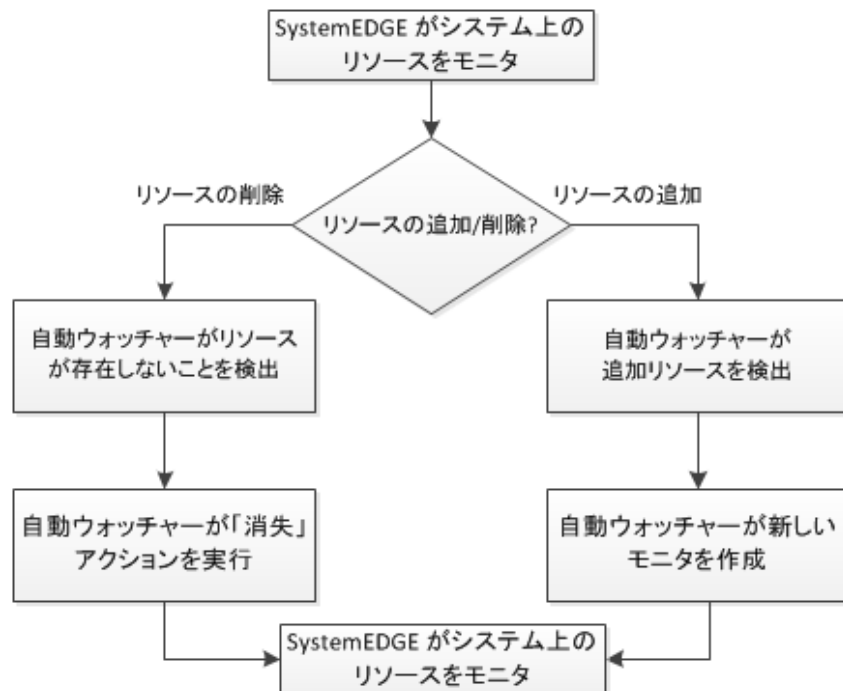
「OK」、「警告」、「マイナー」、「メジャー」、「重大」、「稼働中」、「ダウン」。

自動ウォッチャーを使用すると、管理対象システムに存在するリソースを知らなくても、柔軟にポリシーや階層型テンプレートを作成できます。リソースには、デバイス、サービス、管理対象システムで実行されるプロセスを指定できます。

使用できる自動ウォッチャーのタイプは以下のとおりです。

- 汎用自動ウォッチャー：デバイス、インターフェース、ファイルシステム、ファイルなど、管理対象システムのさまざまなリソース用のモニタを作成します。
- プロセスとサービスの自動ウォッチャー：管理対象システムで実行されるプロセスとサービス用のモニタを作成します。

自動ウォッチャーのプロセス ワークフロー



消失アクションを設定するときには、以下のガイドラインを使用できます。

- 消失するリソースがシステムの健全性に影響する場合は、対応するリソースのステータスを重大な状態に変更する消失アクションを設定できます。
- 消失するリソースがシステムの健全性に影響しない場合は、対応するモニタを削除する消失アクションを設定できます。

関連項目：

[汎用自動ウォッチャー](#) (P. 254)

[プロセスとサービスの自動ウォッチャー](#) (P. 254)

汎用自動ウォッチャー

汎用自動ウォッチャーでは、デバイス、インターフェース、ファイルシステム、ファイルなど、管理対象システムのさまざまなリソース用のモニタを作成できます。

汎用自動ウォッチャーの例としては、以下のものがあります。

- 検出されたすべてのデバイスの容量
- 検出されたすべてのディスクのディスク サービス時間
- すべての `cmd` プロセスの常駐セット サイズ
- すべてのトンネル ネットワーク インターフェースの稼働ステータス
- すべてのデバイスのデバイス ステータス

関連項目:

[自動ウォッチャーの仕組み](#) (P. 252)

プロセスとサービスの自動ウォッチャー

プロセスとサービスのモニタを動的に作成するには、プロセスとサービスの自動ウォッチャーを使用します。

サービス自動ウォッチャーは、自動ウォッチャーの条件（サービス名、開始タイプなど）にサービスが一致した場合に、プロセス テーブルに複数のサービス モニタを作成します。たとえば、インストールされている SQL サービスで開始タイプが「自動」であるものをすべてモニタできます。

プロセス自動ウォッチャーは、以下の 2 つの方法でプロセス モニタを作成します。

- プロセス名を使用 (デフォルト) - プロセス名が 自動ウォッチャーの条件に一致する場合。

たとえば、プロセス名が「sql」または「svchost」であるという条件にプロセスが一致するときに、プロセス モニタを作成します。 自動ウォッチャーによって作成されたプロセス モニタは、PID に関係なく、一致するプロセスで現在管理対象システムで実行されているものを追跡します。

 - 自動ウォッチャーによって作成されたプロセス モニタの定義は、手動で作成されたプロセス モニタと同じです。
 - 同じ名前で引数が異なるプロセスのセットを個別に管理できます。たとえば、「java.exe」などです。
 - 関連するプロセスのセットに対するモニタを作成できます。
- PID の使用 - PID が 自動ウォッチャーの条件に一致する場合。 自動ウォッチャーでは、ユーザ インターフェースで PID フラグを使用してモニタ プロセスを有効にするか、または sysedge.cf ファイルで監視フラグ 0x1000 を指定します。

自動ウォッチャーによって作成された各モニタは、一致するプロセスのインスタンスをすべて追跡します。

 - プロセスの特定のインスタンス用のモニタを作成します。
 - ほかと区別するための引数を使用せず、複数のプロセスのインスタンスをモニタします。

関連項目:

[自動ウォッチャーの仕組み](#) (P. 252)

事前定義済み自動ウォッチャーの適用

ポリシー設定では、テンプレートで事前定義済みの自動ウォッチャーと以下の SystemEDGE のデフォルト ポリシーを提供します。

- CPU Utilization (OS 非依存テンプレート)
- CA ARCserve (Windows テンプレート)
- Windows Services (Windows テンプレート)
- Microsoft Exchange (Windows テンプレート)
- All Filesystems (SystemEDGE デフォルト ポリシー)
- All Disks (SystemEDGE デフォルト ポリシー)

事前定義済み自動ウォッチャーを使用できるかどうかを確認します。

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] または [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。

[利用可能ポリシー] ペインまたは [テンプレート リスト] が開き、事前定義済みの自動ウォッチャーが表示されます。

2. [利用可能ポリシー] ペインまたは [テンプレート リスト] で、事前定義済みの自動ウォッチャーをクリックします。

自動ウォッチャーの [詳細] ペインが表示されます。

3. [アクション] - [適用] をクリックします。

[マシン選択] ページが表示されます。

4. 適切なシステムを選択して、[適用] をクリックします。

自動ウォッチャーが選択したシステムの SystemEDGE 設定に追加されます。

SystemEDGE は、自動ウォッチャーの設定に基づいてモニタを自動的に作成します。

注：管理対象外モードの SystemEDGE の場合は、sysedge.cf ファイルで自動ウォッチャーを指定します。SystemEDGE を管理対象モードに変更すると、SystemEDGE が CA Virtual Assurance に登録する前に定義された自動ウォッチャーをポリシーへインポートできます。

関連項目:

[自動ウォッチャーの作成とシステムへの適用](#) (P. 257)

自動ウォッチャーの作成とシステムへの適用

管理対象モードの SystemEDGE では、ポリシーまたはテンプレートで自動ウォッチャーを指定できます。一元化された設定により、すべてのサーバにわたって一貫性のあるモニタリングを実行できます。ポリシーまたはテンプレートで自動ウォッチャーを設定し、管理対象システム上のリソースをモニタするために自動ウォッチャーを適用します。

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、[ポリシー] または [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。
[利用可能ポリシー] ペインまたは [テンプレート リスト] が表示されます。
2. ポリシーまたはテンプレートを開き、[自動ウォッチャー] をクリックします。
[汎用自動ウォッチャー] ペインが表示されます。
3. プロセスまたはサービスの自動ウォッチャーを追加する場合は、[プロセス/サービス] タブを選択します。
4. ツールバーの  (追加) をクリックします。
自動ウォッチャーの [詳細] ペインが表示されます。
5. 必要な値を指定して、[保存] をクリックします。
自動ウォッチャーが保存されます。
6. [アクション] - [適用] をクリックします。
[マシン選択] ページが表示されます。

7. 適切なシステムを選択して、[適用] をクリックします。

自動ウォッチャーが選択したシステムの SystemEDGE 設定に追加されます。

SystemEDGE は、自動ウォッチャーの設定に基づいてモニタを自動的に作成します。

注: 管理対象外モードの SystemEDGE の場合は、sysedge.cf ファイルで自動ウォッチャーを指定します。SystemEDGE を管理対象モードに変更すると、SystemEDGE が CA Virtual Assurance に登録する前に定義された自動ウォッチャーをポリシーへインポートできます。

関連項目:

[自動ウォッチャーの確認](#) (P. 258)

自動ウォッチャーの確認

CA Virtual Assurance のユーザ インターフェイスで、自動ウォッチャーによってリソースに対応するモニタが作成されたかどうかを確認できます。自動ウォッチャーは予約済みのインデックス範囲 (1000000 ~ 1999999) でモニタを作成します。

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] ペインで [データ センター] フォルダおよび [CA Virtual Assurance サービス] フォルダを展開します。
データ センターによって検出され、管理されているリソースが表示されます。
3. 対応するモニタを確認するリソースを選択します。
選択したリソースの [クイック スタート] タスクが表示されます。
4. [環境設定] タブをクリックします。
[セルフ モニタ] ページ表示され、予約済みのインデックス範囲で自動ウォッチャーが作成したモニタが表示されます。

関連項目:

[自動ウォッチャーの仕組み](#) (P. 252)

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。

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。Windows パフォーマンス オブジェクトおよびカウンタで使用する名前は、perfmon.exe 内の名前と一致する必要があります。

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 [リソース] タブをクリックし、[設定] ペインを開き、[ポリシー] ツリーを展開して、適切なサブカテゴリをクリックします。

[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. [追加] フィールドに以下のデータを追加します。

例：

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。

注：ポリシーを作成する際に、オブジェクトとカウンタのカスタム エントリを指定できます。同じメトリックは、別のポリシーを作成する際に将来使用するために保存されます。
 - 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. [+] (新規) をクリックして、モニタを作成します。
[しきい値モニタの詳細: 新規] ペインが表示されます。

- c. 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任意の文字列で定義します（たとえば「**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。

開始時刻

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。

停止時刻

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。

- d. [保存] をクリックします。

モニタがポリシーに追加されます。

3. [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。

- a. 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。

- b. [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、[エクスプローラ] - [サマリ] の下にある [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。

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pons] をクリックします。

[サービス レスpons] 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pons 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。
5. テストのしきい値を定義します。
6. [制御設定を定義します](#) (P. 316)。
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。

エージェントの検出

エージェントに複数の NIC（ネットワーク インターフェース コントローラ）がある場合は、ポリシー設定によってそのエージェントの名前またはアドレスがすべて検出されます。不要な名前やアドレスが検出されないようにするために、ポリシー設定ではジョブを展開する管理名またはアドレスでエージェントを検出する機能をサポートしています。

注: システムはエージェントのリストを 30 分ごとにリフレッシュします。

次の手順に従ってください:

1. CA Virtual Assurance アプリケーションにログインし、[リソース] タブをクリックします。
2. [エクスプローラ] タブから、[ドメイン サーバ] を右クリックし、[ポリシー] - [SystemEDGE] - [エージェントの検出] を選択します。
確認ダイアログ ボックスが表示されます。
3. [OK] をクリックします。

注: リストを表示するには、[モニタリング ソフトウェア] タブをクリックし、[ポリシー] タブをクリックします。管理名またはアドレスを持つ利用可能なエージェントのリストが表示されます。

ポリシー設定機能の一般的な使用法

このセクションでは、一般的なポリシー設定機能について説明します。

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。
5. [制御設定を定義します](#) (P. 271)。
6. [SNMP 設定を定義します](#) (P. 219)。
7. MIB 拡張を定義します。
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。

SystemEDGE ポリシーのコピー

既存の SystemEDGE ポリシーはコピー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. コピーするポリシーを [利用可能ポリシー] テーブルから選択し、[アクション] をクリックして、[コピー] を選択します。[設定] ペインでポリシーを右クリックし、[コピー] を選択することもできます。
[コピー] ダイアログ ボックスが表示されます。
3. ポリシーの新しい名前を入力し、[OK] をクリックします。
ポリシーがコピーされ、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。
ポリシーが保存されます。

SystemEDGE ポリシーの名前変更

既存の SystemEDGE ポリシーの名前は変更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. 名前を変更するポリシーを [利用可能ポリシー] テーブルから選択し、[アクション] をクリックして、[名前の変更] を選択します。[設定] ペインでポリシーを右クリックし、[名前の変更] を選択することもできます。
[名前の変更] ダイアログ ボックスが表示されます。
注: ポリシーが使用中の場合は、ポリシー名を変更できないことを示すエラー メッセージが表示されます。
3. ポリシーの新しい名前を入力し、[OK] をクリックします。
確認のメッセージが表示され、ポリシーの名前が変更されたことが通知されます。
4. [ポリシーの保存] をクリックします。
ポリシーが保存されます。

SystemEDGE ポリシーの削除

既存の SystemEDGE ポリシーを削除できます。

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] テーブルで削除するポリシーを選択し、[アクション] をクリックして、[削除] を選択します。[設定] ペインでポリシーを右クリックし、[削除] を選択することもできます。

注: ポリシーが使用されている場合、ポリシーを削除できないことを示すエラー メッセージが表示されます。

警告メッセージが表示されます。

3. [OK] をクリックして削除を確認します。

確認メッセージが表示されます。ポリシーは削除されます。

ポリシーへの SystemEDGE 設定のインポート

SystemEDGE を最新バージョンにアップグレードした後、以前の SystemEDGE 設定をインポートし、SystemEDGE ポリシーに変換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] 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. [インポート] をクリックします。

[SystemEDGE エージェント マシン] ウィンドウが表示されます。

4. SystemEDGE 設定をインポートする元のコンピュータを選択し、[OK] をクリックします。

注: マシン リストには、元の設定ファイルからアップグレードされたすべてのマシンと、定義されたモニタが表示されます。SystemEDGE 5.x が検出され、ポリシー設定に登録されると、コンピュータがリストに表示されます。コンピュータがリストに表示されない場合は、SystemEDGE の以前のバージョン レベルでモニタが定義されているかどうか、および [ポリシー設定] で設定が行われているかどうかを確認します。

5. [新規 SystemEDGE ポリシー] ダイアログ ボックスで名前および説明 (任意) を入力し、[OK] をクリックしてインポート プロセスを完了します。

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。

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

システム管理 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 (ディスクのプロンプ)
- 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 \(P. 278\)](#)」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 \(P. 278\)](#)

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 \(P. 271\)](#)

新しい SystemEDGE モニタリング テンプレートの定義

SystemEDGE はさまざまなポリシーを使って設定することができます。[モニタリング テンプレート] では、複数のポリシーを設定し、共有サーバ上の同じエージェントに配信できます。

[モニタリング テンプレート] ページでは、特定のサーバまたはサーバグループに適用されたポリシーを表示および更新できます。SystemEDGE モニタリング テンプレート（階層型テンプレート）を作成してポリシーにインポートできます。これによって複数のポリシーでモニタを再利用できるようになり、モニタを何回もセットアップする必要がありません。

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。

[SystemEDGE] 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任意の説明、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。テンプレートにモニタを追加する方法については、「[SystemEDGE ポリシーへのモニタの追加](#) (P. 289)」を参照してください。
4. [テンプレートの保存] をクリックします。
テンプレートが保存されます。

関連項目:

[階層型テンプレート](#) (P. 281)

[SystemEDGE ポリシーへのモニタリング テンプレートのインポート](#) (P. 284)

[SystemEDGE モニタリング テンプレートのコピー](#) (P. 285)

[SystemEDGE モニタリング テンプレートの変更](#) (P. 285)

[SystemEDGE モニタリング テンプレートの名前変更](#) (P. 286)

[SystemEDGE モニタリング テンプレートの削除](#) (P. 286)

[モニタリング テンプレート適用の進捗状況の確認](#) (P. 287)

[マシンへのテンプレートの適用](#) (P. 287)

[階層型テンプレート](#) (P. 281)

[SystemEDGE モニタリング テンプレートの変更](#) (P. 285)

[SystemEDGE モニタリング テンプレートの名前変更](#) (P. 286)

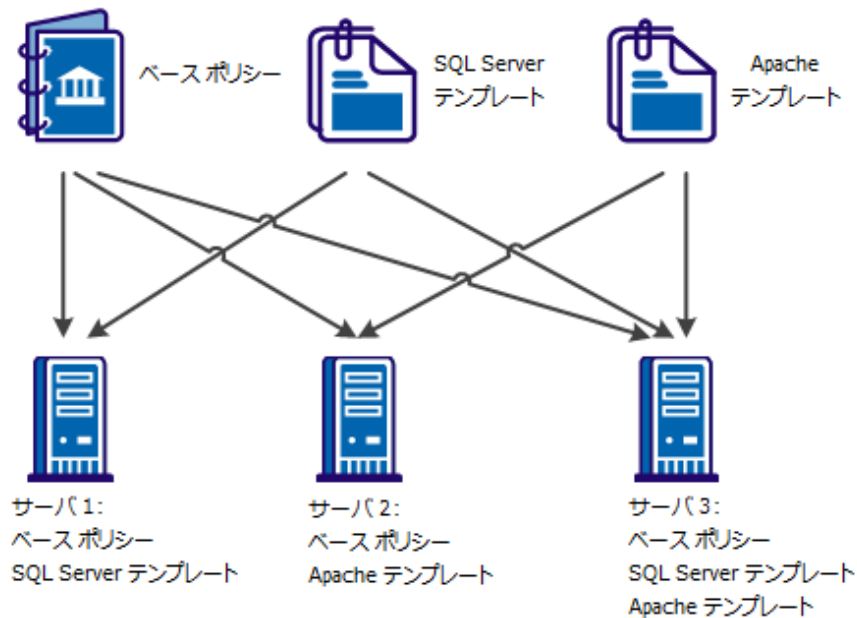
[モニタリング テンプレート適用の進捗状況の確認](#) (P. 287)

[マシンへのテンプレートの適用](#) (P. 287)

階層型テンプレート

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せら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。

すぐに使用できるテンプレート

すぐに使用できるテンプレートを管理対象ノードに適用できます。管理対象ノードに対するテンプレート設定を使用してポリシーを設定します。テンプレートは以下のオペレーティング システムに利用可能です。

すべてのオペレーティング システム用:

- CPU Utilization - Autowatch

- Swap Capacity

Windows の場合:

- App Monitoring - CA eTrust Antivirus

- Process Crash

- System Errors

- System Processes

- User Activity

- Windows Services - Autowatch

UNIX (AIX、HPUnix、Linux、Solaris) :

- System Messages

- System Processes

- User Activity

SystemEDGE ポリシーへのモニタリング テンプレートのインポート

SystemEDGE ポリシーへモニタリング テンプレートをインポートできます。これは、1 回の操作ですべてのシステムの既存のポリシーを一貫したポリシーに置換します。

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. [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. [アクション] をクリックし、[インポート] を選択します。
テンプレートのインポート ウィザードが表示されます。
5. [システム タイプ] を選択し、インポートするモニタリング テンプレートをドロップダウン リストから選択します。
6. (オプション) インポートされたモニタごとに新しいベース インデックスを定義します。
7. ドロップダウン リストから [競合の解決オプション] を選択し、[次へ] をクリックします。
[競合の解決] ページが表示されます。
8. 任意のモニタ競合を調査し、インデックスを調整して、[次へ] をクリックします。
[サマリ] ページが表示されます。
9. インポートされるモニタを調査し、[終了] をクリックしてインポート プロセスを完了します。
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。

SystemEDGE モニタリング テンプレートのコピー

既存の SystemEDGE モニタリング テンプレートはコピー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] を展開して [SystemEDGE] をクリックします。
[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. コピーするモニタリング テンプレートを選択し、[アクション] をクリックして、[コピー] を選択します。[設定] ペインでモニタリング テンプレートを右クリックし、[コピー] を選択することもできます。
[コピー] ダイアログ ボックスが表示されます。
3. モニタリング テンプレートの新しい名前を入力し、[OK] をクリックします。
モニタリング テンプレートがコピーされ、右側のペインに設定画面が表示されます。

SystemEDGE モニタリング テンプレートの変更

SystemEDGE モニタリング テンプレートは変更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] を展開して [SystemEDGE] をクリックします。
[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. [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、変更するモニタを選択します。
[編集] ダイアログ ボックスが表示されます。

5. 必要に応じて設定を変更し、[保存] をクリックします。
6. (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。
7. [保存] をクリックします。

モニタリング テンプレートが保存されます。

SystemEDGE モニタリング テンプレートの名前変更

既存の SystemEDGE モニタリング テンプレートの名前は変更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] を展開して [SystemEDGE] をクリックします。
[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. 名前を変更するモニタリング テンプレートを選択し、[アクション] をクリックして、[名前の変更] を選択します。[設定] ペインでモニタリング テンプレートを右クリックし、[名前の変更] を選択することもできます。
[名前の変更] ダイアログ ボックスが表示されます。
3. モニタリング テンプレートの新しい名前を入力し、[OK] をクリックします。

モニタリング テンプレートの名前が変更され、右側のペインに設定画面が表示されます。

SystemEDGE モニタリング テンプレートの削除

必要のなくなった既存の SystemEDGE モニタリング テンプレートは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] を展開して [SystemEDGE] をクリックします。
[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. [管理対象マシン] タブをクリックします。
[サマリ] ページが開き、テンプレートに適用された管理対象マシンのリストが表示されます。
3. 削除するモニタリング テンプレートを選択し、[削除] アイコンをクリックします。
確認メッセージが表示されます。
4. [OK] をクリックして削除を確定します。
モニタリング テンプレートが削除されます。

モニタリング テンプレート適用の進捗状況の確認

モニタリング テンプレート適用操作の進捗状況は、個々のテンプレートについて詳細なレベルで確認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] 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. [管理対象マシン] タブをクリックします。
[管理対象マシン] ページが開き、設定ステータスの表示が可能なモニタリング テンプレートを現在実行しているマシンのリストが表示されます。
4. (オプション) [設定の表示] をクリックします。
[SystemEDGE 設定] ペインが開き、ポリシーとテンプレート、およびエージェントに対して配信された設定ファイルを表示できます。

マシンへのテンプレートの適用

モニタリング テンプレートを更新したら、企業全体でそれを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、[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] で、以下のいずれかのオプションを選択します。
 - このテンプレートを適用してすべてのマシンを更新
 - このテンプレートの最新の変更が適用されていないマシンのみを更新
 - テンプレートが正常に適用されていないマシンのみを更新
 - 詳細 (手動でマシンを選択)
 - マシンからこのテンプレートを削除
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。
テンプレートの適用が開始されます。

テンプレートへの SystemEDGE 設定のインポート

SystemEDGE を最新バージョンにアップグレードした後、以前の SystemEDGE 設定をインポートし、SystemEDGE モニタリング テンプレートに変換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] を展開して [SystemEDGE] をクリックします。
[利用可能な SystemEDGE モニタリング テンプレート] ページが表示されます。
2. [利用可能な SystemEDGE モニタリング テンプレート] ツールバーで [+] (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. [インポート] をクリックします。
[SystemEDGE エージェント マシン] ウィンドウが表示されます。
4. SystemEDGE 設定をインポートする元のコンピュータを選択し、[OK] をクリックします。

注: マシン リストには、元の設定ファイルからアップグレードされたすべてのマシンと、定義されたモニタが表示されます。SystemEDGE 5.x が検出され、ポリシー設定に登録されると、コンピュータがリストに表示されます。コンピュータがリストに表示されない場合は、SystemEDGE の以前のバージョン レベルでモニタが定義されているかどうか、および [ポリシー設定] で設定が行われているかどうかを確認します。
5. [新規 SystemEDGE モニタリング テンプレート] ダイアログ ボックスで名前および説明 (任意) を入力し、[OK] をクリックしてインポート プロセスを完了します。
6. [テンプレートの保存] をクリックします。
テンプレートが保存されます。

SystemEDGE ポリシーへのモニタの追加

SystemEDGE ポリシーにはモニタを追加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. [モニタ] をクリックし、追加するモニタを選択します。
 - [しきい値モニタの定義](#) (P. 290)
 - [プロセス モニタの定義](#) (P. 293)
 - [ログ ファイル モニタの定義](#) (P. 295)
 - [Windows イベント モニタの定義](#) (P. 297)
 - [履歴モニタの定義](#) (P. 299)
 - [プロセス グループ モニタの定義](#) (P. 301)
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. [ポリシーの保存] をクリックします。

モニタがポリシーにロードされ、ポリシーが保存されます。

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

関連項目:

[しきい値モニタの定義](#) (P. 290)
[プロセス モニタの定義](#) (P. 293)
[ログ ファイル モニタの定義](#) (P. 295)
[Windows イベント モニタの定義](#) (P. 297)
[履歴モニタの定義](#) (P. 299)
[プロセス グループ モニタの定義](#) (P. 301)

しきい値モニタの定義

SystemEDGE ポリシーのしきい値設定は定義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. [モニタ] 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。ドロップダウン リストの値は、利用可能な MIB テーブルです。

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。これは任意の文字列です（FileSystems など）。

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。ドロップダウン リストの値は、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です。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。これは任意の文字列です (SysVol_C など)。

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。

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

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. [ポリシーの保存] をクリックします。
しきい値モニタがポリシーにロードされます。

プロセス モニタの定義

SystemEDGE ポリシーのプロセス設定は定義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. [モニタ] 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。これは任意の文字列です（Process など）。

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。ドロップダウン リストの値は、プロセス モニタリングに利用可能な属性です。

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（MemUsedPercent 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。これは任意の文字列です（ApacheServer など）。

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。

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

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. [ポリシーの保存] 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 モニタの定義

SystemEDGE ポリシーのログ ファイル設定は定義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. [モニタ] 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。

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

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. 「ポリシーの保存」 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 モニタの定義

SystemEDGE ポリシーの Windows イベント設定は定義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. 「モニタ」 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。

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

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. 〔ポリシーの保存〕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。

履歴モニタの定義

SystemEDGE ポリシーの履歴設定は定義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. 〔モニタ〕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。 ドロップダウン リストの値は、利用可能な MIB テーブルです。

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。 ドロップダウン リストの値は、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です。 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、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、この履歴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。

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。

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

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. [ポリシーの保存] 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 モニタの定義

SystemEDGE ポリシーのプロセス グループ設定は定義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. [モニタ] 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、照合に使用する正規表現です (オプション設定から独立しています)。プロセスを名前で、それぞれ照合します。

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。

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

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. 〔ポリシーの保存〕 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。

SystemEDGE ポリシー内のモニタの表示

SystemEDGE ポリシーに含まれているモニタは表示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. 〔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。モニタリングクラスのサブタブをクリックすると、ポリシーに含まれている他のモニタを表示できます。

関連項目

[SystemEDGE ポリシー内のモニタの変更 \(P. 304\)](#)

[SystemEDGE ポリシーからのモニタの削除 \(P. 305\)](#)

SystemEDGE ポリシー内のモニタのコピー

SystemEDGE ポリシー内のモニタはコピー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. [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、コピーするモニタを選択します。
5. [アクション] をクリックし、[コピー] を選択します。
[編集] ダイアログ ボックスが表示されます。
6. 必要に応じて設定を変更し、[保存] をクリックします。
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。
ポリシーが保存されます。

SystemEDGE ポリシー内のモニタの変更

SystemEDGE ポリシー内のモニタは変更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. [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、変更するモニタを選択します。
5. [アクション] をクリックし、[変更] を選択します。
[編集] ダイアログ ボックスが表示されます。
6. 必要に応じて設定を変更し、[保存] をクリックします。
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。
ポリシーが保存されます。

SystemEDGE ポリシーからのモニタの削除

SystemEDGE ポリシー内のモニタは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、[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. [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。
ポリシーが保存されます。

SystemEDGE ポリシー内の既存テンプレートの変更

既存のモニタリング テンプレートは、変更して SystemEDGE ポリシーにインポート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. [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. [アクション] をクリックし、[インポート] を選択します。
テンプレートのインポート ウィザードが表示されます。
5. 必要な情報を使ってモニタリング テンプレートを更新します。
6. [システム タイプ] を選択し、インポートする更新済みのモニタリング テンプレートをドロップダウン リストから選択します。
7. (オプション) インポートされたモニタごとに新しいベース インデックスを定義します。
8. [競合の解決オプション] で [既存のモニタをインポートされるエンティティに置換します] を選択し、[次へ] をクリックします。
[競合の解決] ページが表示されます。
9. 任意のモニタ競合を調査し、インデックスを調整して、[次へ] をクリックします。
[サマリ] ページが表示されます。
10. インポートされるモニタを調査し、[終了] をクリックしてインポート プロセスを完了します。

11. [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。
12. [アクション] ドロップダウン リストから [適用] を選択します。
保存したポリシーが希望のマシンに適用されます。

新しい SRM ポリシーの定義

SRM ポリシーを作成することで、実行するテスト、モニタするしきい値、基本設定、およびエージェントの実行方法とモニタ対象を制御する他の設定を定義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 [サービス レスpons] 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。
[新規サービス レスpons 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。
ポリシーが保存されます。

関連項目:

[SRM ポリシーのコピー](#) (P. 307)

[SRM ポリシーの名前変更](#) (P. 308)

[SRM ポリシーの削除](#) (P. 309)

SRM ポリシーのコピー

既存の SRM ポリシーはコピー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 [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. コピーするポリシーを [利用可能ポリシー] テーブルから選択し、[アクション] をクリックして、[コピー] を選択します。[設定] ペインでポリシーを右クリックし、[コピー] を選択することもできます。
[コピー] ダイアログ ボックスが表示されます。
3. ポリシーの新しい名前を入力し、[OK] をクリックします。
ポリシーがコピーされ、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。
ポリシーが保存されます。

SRM ポリシーの名前変更

既存の SRM ポリシーの名前は変更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 [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. 名前を変更するポリシーを [利用可能ポリシー] テーブルから選択し、[アクション] をクリックして、[名前の変更] を選択します。[設定] ペインでポリシーを右クリックし、[名前の変更] を選択することもできます。
[名前の変更] ダイアログ ボックスが表示されます。
注： ポリシーが使用中の場合は、ポリシー名を変更できないことを示すエラー メッセージが表示されます。
3. ポリシーの新しい名前を入力し、[OK] をクリックします。
確認のメッセージが表示され、ポリシーの名前が変更されたことが通知されます。
4. [ポリシーの保存] をクリックします。
ポリシーが保存されます。

SRM ポリシーの削除

既存の SRM ポリシーは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、[ポリシー] を展開して [サービス レスpons] 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. 削除するポリシーを [利用可能ポリシー] テーブルから選択し、[アクション] をクリックして、[コピー] を選択します。[設定] ペインでポリシーを右クリックし、[削除] を選択することもできます。
注: ポリシーが使用中の場合は、ポリシーを削除できないことを示すエラー メッセージが表示されます。
3. 警告メッセージが表示されます。[OK] をクリックして削除を確認します。
4. [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。

SRM ポリシーへのテストの追加

SRM ポリシーにはテストを追加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 [サービス レスpons] 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. [テスト] をクリックし、[テスト モニタ] ツールバーの [+] (新規) をクリックします。
[新規] ダイアログ ボックスが表示されます。
4. [テスト名] フィールドに、テストの一意の名前を入力します。この名前は 64 文字以下にしてください。テスト名では大文字と小文字が区別されます。
5. (オプション) テストの説明を入力します。

6. (オプション) テスト クラスを定義します。
7. [テスト タイプ] リストで、希望のテスト タイプをクリックします。

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す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することを確認します。

DHCP

DHCP (Dynamic Host Configuration Protocol) サーバが応答して、アドレス要求に応答することを確認します。

DNS

解決要求に対応するためにドメイン名システム サーバがホスト名を処理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、また特定のテキストが Web ページ上に表示されるかどうかを確認します。

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す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 リクエストに応答す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、短いクエリを処理す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、処理す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。

注: 各テスト タイプの詳細と定義については、「SRM ユーザ ガイド」を参照してください。

8. [テスト間隔] フィールドにテストの間隔 (秒単位) を指定します。間隔は、30 秒の倍数にする必要があります。このオプションは、テストのパフォーマンスを調整するために使用します。
 9. [テスト タイムアウト] フィールドにテストがタイムアウトする時間 (秒単位) を指定します。テスト間隔より短く、テストの実行にかかる時間より長い数値を選択してください。
 10. [ポーリング間隔] リストから以下のいずれかを選択して、ポーリング間隔を設定します。
 - 通常
 - オフ
 - 低速
- 注: 詳細については、「SRM ユーザ ガイド」を参照してください。
11. (オプション) [履歴データの保持] チェック ボックスをオンにします。
 12. [保存] をクリックすると、ポリシーにテストが追加されます。
テストが保存されます。
 13. (オプション) 追加するテストごとに同じ手順を繰り返します。
 14. [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:

[SRM テストの変更](#) (P. 312)

[SRM ポリシーへのしきい値定義の追加](#) (P. 314)

[SRM しきい値定義の変更](#) (P. 315)

[SRM 制御設定の定義](#) (P. 316)

SRM テストの変更

既存の SRM テストは変更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 [サービス レスpons] 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. 変更するテストが含まれるポリシーを [利用可能ポリシー] テーブルから選択します。
[サマリ] ページが表示されます。
3. [テスト] タブをクリックします。
[テスト モニタ] ページが表示されます。
4. 変更するテストを選択し、[アクション] をクリックして、[変更] を選択します。
[編集] ダイアログ ボックスが表示されます。
5. 必要に応じてテストを変更し、[保存] をクリックします。
テストが更新されます。
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。

SRM テストのコピー

既存の SRM テストはコピー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 [サービス レスpons] 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. コピーするテストが含まれるポリシーを [利用可能ポリシー] テーブルから選択します。
[サマリ] ページが表示されます。
3. [テスト] タブをクリックします。
[テスト モニタ] ページが表示されます。
4. コピーするテストを選択し、[アクション] をクリックして、[コピー] を選択します。
コピー ダイアログ ボックスが表示されます。
5. SRM テスト名を入力します。
SRM テストがコピーされます。

SRM テストの削除

既存の SRM テストは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、[ポリシー] を展開して [サービス レスpons] 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. 削除するテストが含まれるポリシーを [利用可能ポリシー] テーブルから選択します。
[サマリ] ページが表示されます。
3. [テスト] タブをクリックします。
[テスト モニタ] ページが表示されます。
4. 削除するテストを選択し、[アクション] をクリックして、[削除] を選択します。
5. アクションを確認します。
SRM テストが削除されます。

SRM ポリシーへのしきい値定義の追加

SRM ポリシーにはしきい値定義を追加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 [サービス レスpons] 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. [しきい値] タブをクリックし、[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] ダイアログ ボックスが表示されます。

4. 以下のしきい値モニタ設定を行います。

名前

しきい値モニタ名を定義します。

属性

使用する属性を指定します。

演算子

使用する演算子を指定します。

警告値

使用する警告値を定義します。

マイナー値

使用するマイナー値を定義します。

メジャー値

使用するメジャー値を定義します。

重大値

使用する重大値を定義します。

致命的値

使用する致命的値を定義します。

5. [保存]をクリックすると、ポリシーにしきい値定義が追加されます。
しきい値定義が保存されます。
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。

SRM しきい値定義の変更

既存の SRM しきい値定義は変更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 [サービス レスpons] 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. 変更するしきい値定義が含まれるポリシーを[利用可能ポリシー]テーブルから選択します。
[サマリ] ページが表示されます。
3. [しきい値] タブをクリックします。
[しきい値モニタ] ページが表示されます。
4. 変更するしきい値定義を選択し、[アクション]をクリックして、[変更]を選択します。
[編集] ダイアログ ボックスが表示されます。
5. 必要に応じてしきい値定義を変更し、[保存]をクリックします。
しきい値定義が更新されます。
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。

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pons] 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。

新しい SRM テスト定義テンプレートの定義

SRM テスト定義テンプレートは、作成してポリシーにインポートすることができます。これによって複数のポリシーでテストを再利用できるようになり、テストを何回もセットアップする必要がありません。

新しい SRM テスト定義テンプレートを定義する方法

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 [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] ページが表示されます。
2. [テストテンプレート リスト] ツールバーの [+] (新規) をクリックします。
[新規サービス レスポンス テスト定義テンプレート] ダイアログボックスが表示されます。
3. テスト定義テンプレートの名前と任意の説明、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。
テスト定義テンプレートが作成され、[サマリ] ページが表示されます。テンプレートにテストを追加する方法については、「SRM (309P.) ポリシーへのテストの追加」を参照してください。
4. [テンプレートの保存] をクリックします。
テンプレートが保存されます。

関連項目:

[SRM ポリシーへのテスト定義テンプレートのインポート](#) (P. 319)

[SRM テスト定義テンプレートの変更](#) (P. 320)

[SRM テスト定義テンプレートのコピー](#) (P. 320)

[SRM テスト定義テンプレートの名前変更](#) (P. 321)

[SRM テスト定義テンプレートの削除](#) (P. 322)

SRM ポリシーへのテスト定義テンプレートのインポート

テスト定義テンプレートは **SRM** ポリシーにインポート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. [テスト] 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テスト モニタのリストが表示されます。
4. [アクション] をクリックし、[インポート] を選択します。
テンプレートのインポート ウィザードが表示されます。
5. インポートするテスト テンプレートをドロップダウン リストから選択します。
6. (オプション) インポートする各テスト定義の新しいベース インデックスを定義します。
7. ドロップダウン リストから [競合の解決オプション] を選択し、[次へ] をクリックします。
[競合の解決] ページが表示されます。
8. テスト定義の競合を確認し、インデックスの調整を行います。次に、インポートすべきでないテスト定義を選択解除し、[次へ] をクリックします。
[サマリ] ページが表示されます。
9. インポートするテスト定義を確認し、[終了] をクリックしてインポート プロセスを完了します。
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。

SRM テスト定義テンプレートの変更

SRM テスト定義テンプレートは変更することができます。

SRM テスト定義テンプレートを変更する方法

1. [設定] ペインを開いて[モニタリング テンプレート]を展開します。
次に、[サービス レスポンス]をクリックし、[テスト定義テンプレート]を展開します。
テスト テンプレートを含むテスト テンプレート リストが表示されます。
2. 変更するサービス レスポンス テスト テンプレートを選択します。
テスト テンプレートの [サマリ] ページが表示されます。
3. [テスト] タブをクリックし、変更するテスト モニタを選択します。
次に、[アクション] をクリックし、[変更] を選択します。
[編集] ダイアログ ボックスが表示されます。
4. 必要に応じて設定を変更し、[保存] をクリックします。
5. [テンプレートの保存] をクリックします。
テンプレートが保存されます。

SRM テスト定義テンプレートのコピー

SRM テスト定義テンプレートはコピーすることができます。

SRM テスト定義テンプレートのコピーする方法

1. [設定] ペインを開いて[モニタリング テンプレート]を展開します。
次に、[サービス レスポンス]をクリックし、[テスト定義テンプレート]を展開します。
テスト テンプレートを含むテスト テンプレート リストが表示されます。
2. コピーするサービス レスポンス テスト テンプレートを選択します。
テスト テンプレートの [サマリ] ページが表示されます。

3. [テスト] タブをクリックし、コピーするテストを選択します。次に、[アクション] をクリックし、[コピー] を選択します。[設定] ペインでテストテンプレートを右クリックし、[コピー] を選択する方法もあります。

[コピー] ダイアログ ボックスが表示されます。

4. テスト定義テンプレートの新しい名前を入力し、[OK] をクリックします。

テスト定義テンプレートがコピーされ、テスト テンプレート リストに表示されます。

SRM テスト定義テンプレートの名前変更

SRM テスト定義テンプレートの名前は変更することができます。

SRM テスト定義テンプレートを名前変更する方法

1. [設定] ペインを開いて[モニタリング テンプレート]を展開します。次に、[サービス レスpons] をクリックし、[テスト定義テンプレート] を展開します。

テスト テンプレートを含むテスト テンプレート リストが表示されます。

2. 名前を変更するサービス レスpons テスト テンプレートを選択します。

テスト テンプレートの [サマリ] ページが表示されます。

3. [テスト] タブをクリックし、名前を変更するテストを選択します。次に、[アクション] をクリックし、[名前の変更] を選択します。[設定] ペインでテストテンプレートを右クリックし、[名前の変更] を選択することもできます。

[名前の変更] ダイアログ ボックスが表示されます。

4. テスト定義テンプレートの新しい名前を入力し、[OK] をクリックします。

確認のメッセージが表示され、テスト定義テンプレートの名前が変更されたことが通知されます。

SRM テスト定義テンプレートの削除

SRM テスト定義テンプレートは削除することができます。

SRM テスト定義テンプレートを削除する方法

1. [設定] ペインを開いて[モニタリング テンプレート]を展開します。次に、[サービス レスpons]をクリックし、[テスト定義テンプレート]を展開します。
テスト テンプレートを含むテスト テンプレート リストが表示されます。
2. 削除するサービス レスpons テスト テンプレートを選択します。
テスト テンプレートの [サマリ] ページが表示されます。
3. [テスト] タブをクリックし、削除するテストを選択します。次に、[アクション] をクリックし、[削除] を選択します。[設定] ペインでテスト テンプレートを右クリックし、[削除] を選択することもできます。
警告メッセージが表示されます。
4. [OK] をクリックして削除を確定します。
確認メッセージが表示されます。これで、テスト テンプレートは削除されます。

新しい SRM しきい値定義テンプレートの定義

SRM しきい値定義テンプレートは、作成してポリシーにインポートすることができます。これによって複数のポリシーでしきい値を再利用できるようになり、しきい値を何回もセットアップする必要がありません。

新しい SRM しきい値定義テンプレートを定義する方法

1. [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、[サービス レスpons] をクリックします。
[サービス レスpons] ページが表示されます。
2. [しきい値テンプレート リスト] ツールバーの [+] (新規) をクリックします。
[新規サービス レスpons しきい値定義テンプレート] ダイアログ ボックスが表示されます。

3. しきい値定義テンプレートの名前と任意の説明、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。
しきい値定義テンプレートが作成され、[サマリ] ページが表示されます。テンプレートにしきい値定義を追加する方法については、「SRM (314P.)ポリシーへのしきい値定義の追加」を参照してください。
4. [テンプレートの保存] をクリックします。
テンプレートが保存されます。

関連項目:

[SRM ポリシーへのしきい値定義テンプレートのインポート \(P. 323\)](#)

[SRM しきい値定義テンプレートの変更 \(P. 324\)](#)

[SRM しきい値定義テンプレートのコピー \(P. 325\)](#)

[SRM しきい値定義テンプレートの名前変更 \(P. 325\)](#)

[SRM しきい値定義テンプレートの削除 \(P. 326\)](#)

SRM ポリシーへのしきい値定義テンプレートのインポート

しきい値定義テンプレートは SRM ポリシーにインポート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. [しきい値] 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しきい値モニタのリストが表示されます。
4. [アクション] をクリックし、[インポート] を選択します。
テンプレートのインポート ウィザードが表示されます。

5. インポートするしきい値テンプレートをドロップダウン リストから選択します。
6. インデックス競合の処理方法を選択し、[次へ] をクリックします。
[競合の解決] ページが表示されます。
7. しきい値定義の競合を確認し、しきい値定義名の調整を行います。次に、インポートすべきでないしきい値定義を選択解除し、[次へ] をクリックします。
[サマリ] ページが表示されます。
8. インポートするしきい値定義を確認し、[終了] をクリックしてインポート プロセスを完了します。
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。

SRM しきい値定義テンプレートの変更

SRM しきい値定義テンプレートは変更することができます。

SRM しきい値定義テンプレートを変更する方法

1. [設定] ペインを開いて[モニタリング テンプレート]を展開します。次に、[サービス レスpons]をクリックし、[テスト定義テンプレート]を展開します。
しきい値テンプレートを含むしきい値テンプレート リストが表示されます。
2. 変更するサービス レスponsしきい値テンプレートを選択します。
テスト テンプレートの [サマリ] ページが表示されます。
3. [しきい値] をクリックし、変更するしきい値モニタを選択します。次に、[アクション] をクリックし、[変更] を選択します。
[しきい値モニタの詳細] ダイアログ ボックスが表示されます。
4. 必要に応じて設定を変更し、[保存] をクリックします。
5. [テンプレートの保存] をクリックします。
テンプレートが保存されます。

SRM しきい値定義テンプレートのコピー

SRM しきい値定義テンプレートはコピーすることができます。

SRM しきい値定義テンプレートをコピーする方法

1. [設定] ペインを開いて[モニタリング テンプレート]を展開します。次に、[サービス レスpons]をクリックし、[テスト定義テンプレート]を展開します。
しきい値テンプレートを含むしきい値テンプレート リストが表示されます。
2. コピーするサービス レスponsしきい値テンプレートを選択します。
しきい値テンプレートの [サマリ] ページが表示されます。
3. [しきい値] タブをクリックし、コピーするしきい値モニタを選択します。次に、[アクション]をクリックし、[コピー]を選択します。
[設定] ペインでモニタリング テンプレートを右クリックし、[コピー]を選択することもできます。
[コピー] ダイアログ ボックスが表示されます。
4. しきい値定義テンプレートの新しい名前を入力し、[OK] をクリックします。
しきい値定義テンプレートがコピーされ、しきい値テンプレート リストに表示されます。

SRM しきい値定義テンプレートの名前変更

SRM しきい値定義テンプレートの名前は変更することができます。

SRM しきい値定義テンプレートの名前を変更する方法

1. [設定] ペインを開いて[モニタリング テンプレート]を展開します。次に、[サービス レスpons]をクリックし、[テスト定義テンプレート]を展開します。
しきい値テンプレートを含むしきい値テンプレート リストが表示されます。
2. 名前を変更するサービス レスponsしきい値テンプレートを選択します。
しきい値テンプレートの [サマリ] ページが表示されます。

3. [しきい値] タブをクリックし、名前を変更するしきい値モニタを選択します。次に、[アクション] をクリックし、[名前の変更] を選択します。[設定] ペインでテスト テンプレート を右クリックし、[名前の変更] を選択することもできます。

[名前の変更] ダイアログ ボックスが表示されます。

4. しきい値定義テンプレートの新しい名前を入力し、[OK] をクリックします。

確認のメッセージが表示され、しきい値定義テンプレートの名前が変更されたことが通知されます。

SRM しきい値定義テンプレートの削除

SRM しきい値定義テンプレートは削除することができます。

SRM しきい値定義テンプレートを削除する方法

1. [設定] ペインを開いて[モニタリング テンプレート] を展開します。次に、[サービス レスpons] をクリックし、[テスト定義テンプレート] を展開します。

しきい値テンプレートを含むしきい値テンプレート リストが表示されます。

2. 削除するサービス レスpons しきい値テンプレートを選択します。

しきい値テンプレートの [サマリ] ページが表示されます。

3. [しきい値] タブをクリックし、削除するしきい値モニタを選択します。次に、[アクション] をクリックし、[削除] を選択します。[設定] ペインでモニタリング テンプレート を右クリックし、[削除] を選択することもできます。

警告メッセージが表示されます。

4. [OK] をクリックして削除を確定します。

確認メッセージが表示されます。しきい値テンプレートが削除されます。

既存の SRM 設定のインポート

既存の Service Availability (SA) 2.0 AIM を SRM 3.1.0 にアップグレードした後、前の SA 2.0 設定をインポートし、それを SRM 3.1.0 ポリシーに変換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 [サービス レスpons] 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。
[新規サービス レスpons ポリシー] ダイアログ ボックスが表示されます。
3. [インポート] をクリックし、ポリシーのインポート元のマシンをリストから選択して、[OK] をクリックします。
4. 名前と任意の説明を入力し、[OK] をクリックすると、インポートプロセスは完了します。
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ます。新規ポリシーは、自動エージェント ウォーム スタート後に実装されます。

以下のいずれかが該当する場合は、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。
 - ポリシーの期限切れバージョンを実行しているマシン
 - ポリシー例外が適用されているマシン
 - ポリシーの現在のバージョンを実行しているマシン
 - このポリシーに対して設定エラーがあるマシン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 (手動でマシンを選択)] を選択して、[マシンを選択] ペインにポリシーを再割り当てするマシンを手動で追加します。

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pons] 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
- 最後のポリシーまたはテンプレートの適用以降の例外を表示します。
- 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] のいずれかの状態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
- テンプレートの一括削除

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:

選択したポリシーをサービス グループに適用する場合には、ポリシーを適用するマシンを選択するオプションがあります。

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。

[既存の設定を選択されたテンプレートで置換します]

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、選択したテンプレートをすべてのマシンに適用します。

[選択されたテンプレートを既存の設定に追加します]

選択したテンプレートを追加します。選択したテンプレートのいずれかがマシン設定の一部としてすでに適用されている場合は、それらのテンプレートが再適用されます。

テンプレートの一括削除

マシンに適用されている既存のテンプレートを削除します。

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。

ポリシーを以前のバージョンに戻す

ポリシーは以前のバージョンに戻すことができます。

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. [バージョン] タブをクリックします。
[バージョン] ページが表示されます。
4. リストアするバージョンをテーブルから選択し、[最新のバージョンにする] をクリックします。
確認のメッセージが表示されます。[OK] をクリックします。ポリシーの新しいバージョンが作成され、サマリ ページが表示されます。
5. (オプション) バージョンの新しいコピーを作成することができます。
[利用可能ポリシー] テーブルからバージョンを選択し、[コピー] をクリックします。
[コピー] ダイアログ ボックスが表示されます。
6. ポリシーの新しい名前を入力し、[OK] をクリックします。
ポリシーがコピーされ、[設定] ペインのポリシー ツリーに追加されます。新しいコピーのサマリ ページが表示されます。
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。

新規インスタンスのデフォルト ポリシーの指定

検出されたすべての新しいインスタンスについて、単一のデフォルト ポリシーを設定することができます。SystemEDGE または SRM のインストール中または展開中にポリシーを指定しなかった場合、または指定したポリシーが利用可能でない場合、デフォルト ポリシーが配信されます。

デフォルト ポリシーを指定する方法

1. [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。

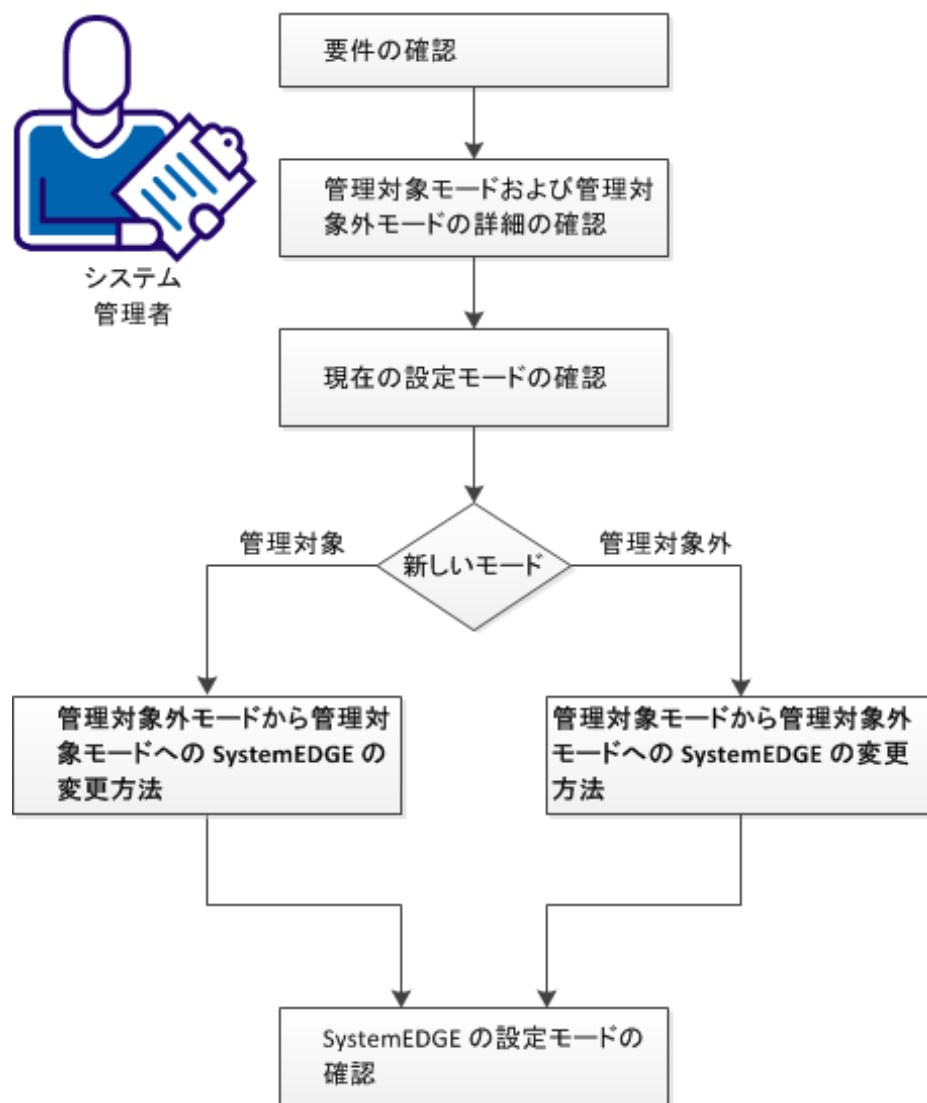
2. [デフォルト ポリシー] セクションで、使用するポリシーを [デフォルト ポリシー] ドロップダウン リストから選択し、[適用] をクリックします。

デフォルト ポリシーが適用されます。

SystemEDGE の設定モードの変更方法

SystemEDGE の設定モードの変更が必要になる場合があります。以下の図は、設定モードを変更するために必要なアクションの概要を示しています。

SystemEDGE の設定モードの変更方法



以下の手順に従います。

[要件の確認 \(P. 335\)](#)

[管理対象モードおよび管理対象外モードの詳細の確認 \(P. 336\)](#)

[SystemEDGE の現在の設定モードの確認 \(P. 337\)](#)

[管理対象モードから管理対象外モードへの SystemEDGE の変更方法 \(P. 338\)](#)

[管理対象外モードから管理対象モードへの SystemEDGE の変更方法 \(P. 342\)](#)

[SystemEDGE の設定モードの確認 \(P. 345\)](#)

要件の確認

SystemEDGE の設定モードを変更する前に、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 SystemEDGE に関する基礎知識がある。
- 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。
- 管理対象ノードでモニタリング エージェント (CASystemEDGE) 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。
- CA Virtual Assurance によって関連するシステムがすべて検出されている。

管理対象モードおよび管理対象外モードの詳細の確認

以下の用語を確認してください。このシナリオでは、管理対象外モードおよび管理対象モードという用語は、SystemEDGE の設定で使用しています。

管理対象外モード

特定のサーバの SystemEDGE 設定は CA Virtual Assurance のポリシー設定によって管理されません。sysedge.cf ファイルを編集して、設定を変更することができます。

管理モード

特定のサーバの SystemEDGE 設定は CA Virtual Assurance のポリシー設定によって管理されます。CA Virtual Assurance マネージャの[ポリシー設定]で SystemEDGE の設定を指定し、これをネットワーク内の適切なサーバに配布します。sysedge.cf ファイルをローカルで編集すると、その変更は次のポリシー配布の際に CA Virtual Assurance によって上書きされます。

SystemEDGE の設定モードに影響する以下の場合を考慮します。

- 製品メディアから一般的な SystemEDGE インストールを実行する場合、SystemEDGE はインストール後に管理対象外モードで実行されるよう設定されます。
- 製品メディアからカスタマイズした SystemEDGE インストールを実行する場合、管理対象モードを使用するようマネージャ システムを設定できます。マネージャ システムを指定して、CA Virtual Assurance によってインストール後に SystemEDGE が検出された場合、SystemEDGE はポリシー設定に自動的に登録され、管理対象モードで実行されます。
- リモート展開を使用して SystemEDGE をリモート システムにインストールする場合、展開ジョブで SystemEDGE の設定モードを指定できます。デフォルト値は管理対象モードです。

重要： [エクスプローラ] ペインには、管理対象と管理対象外のフォルダが表示されます。ここには、CA Virtual Assurance によってポーリングされるサーバ（管理対象）と、ポーリングされないサーバ（管理対象外）が一覧表示されます。このプロパティは、SystemEDGE 設定の管理対象モードまたは管理対象外モードとは異なります。 [エクスプローラ] ペインのサーバの管理対象または管理対象外のステータスは、SystemEDGE の設定モードには影響しません。SystemEDGE 設定ファイルの特定のエントリは、SystemEDGE の設定モードを示します。

SystemEDGE の現在の設定モードの確認

以下の手順では、SystemEDGE の設定モードを確認する方法について説明します。

以下の用語がこれらのユース ケース全体で使用されます。

静的な sysedge.cf ファイル

インストーラによって導入されるファイルを示します。このファイルは *Installed_Dir*¥SystemEDGE¥config ディレクトリに置かれます。

デフォルト：

Windows：C:¥Program Files¥CA¥SystemEDGE¥config

UNIX/Linux：/opt/CA/SystemEDGE/config

動的な sysedge.cf ファイル

現行の SystemEDGE 設定ファイルを示します。このファイルは *Data_Dir*¥port<number> ディレクトリに置かれます。

デフォルト：

Windows：C:¥Users¥Public¥CA¥SystemEDGE¥port161

UNIX/Linux：/opt/CA/SystemEDGE/config/port161

次の手順に従ってください：

1. SystemEDGE の設定モードを確認するサーバにログインします。
2. SystemEDGE の「data」ディレクトリに移動して、port<number>ディレクトリを開きます。Windows の場合は、SystemEDGE のコントロールパネルから data ディレクトリの sysedge.cf ファイルを開くことができます。

注：「data」ディレクトリにある動的な sysedge.cf ファイルは、「config」ディレクトリにある静的な sysedge.cf ファイルとは異なります。

3. port<number>ディレクトリにある動的な sysedge.cf ファイルを開きます。

SystemEDGE が管理対象モードで実行される場合、最初の行には制御値 (ctrl_value) を指定します。

例：

```
ctrl_value 0x9e30d00e
```

```
# Generated file - DO NOT EDIT
```

```
#
```

```
# Configuration file generated on 2012:03:27 05:37
```

```
#
```

```
# Generated from default.generic.0.prof
```

```
#
```

```
version 5.7
```

SystemEDGE が管理対象外モードで実行される場合、最初の行にはバージョンを指定します。

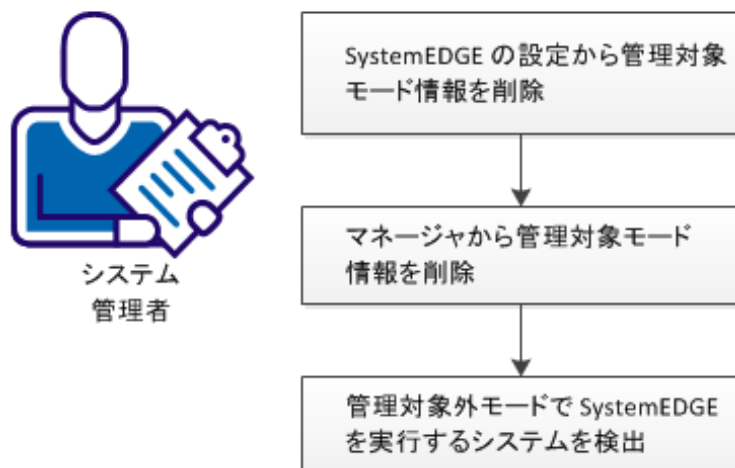
例：

```
version 5.7
```

管理対象モードから管理対象外モードへの SystemEDGE の変更方法

以下の図は、管理対象外モードに変更するために必要なアクションの概要を示しています。

管理対象モードから管理対象外モードへの SystemEDGE の変更方法



以下の手順に従います。

[SystemEDGE の設定からの管理対象モードの情報の削除 \(P. 339\)](#)

[マネージャからの管理対象モードの情報の削除 \(P. 340\)](#)

[管理対象外モードで SystemEDGE を実行するシステムの検出 \(P. 341\)](#)

SystemEDGE の設定からの管理対象モードの情報の削除

以下の手順では、特定のサーバの SystemEDGE の設定から管理対象モードの情報を削除する方法について説明します。

次の手順に従ってください:

1. SystemEDGE の設定モードを変更するサーバにログインします。
2. 便利な場所に以下のバックアップディレクトリを作成します。
`data.backup`
`config.backup`
3. 通常の方法で SystemEDGE を停止します。
4. SystemEDGE の「data」ディレクトリに移動して、`port<number>` ディレクトリを開きます。デフォルトのディレクトリは `port161` です。
ディレクトリの内容が一覧表示されます。
5. `data.backup` ディレクトリに以下のファイルを移動させて、`port<number>` ディレクトリに表示されないようにします。
`.sysedge.id`
`sysedge.cf`
6. SystemEDGE の「config」ディレクトリに移動します。
ディレクトリの内容が一覧表示されます。
7. `config.backup` ディレクトリに以下のファイルをコピーします。
`sysedge.cf`
8. 「config」ディレクトリに移動して、テキストエディタで `sysedge.cf` ファイルを開き、ファイルの末尾までスクロールします。

9. 以下の行を削除します。

```
manager_name <hostname of the manager>
```

10. ファイルを保存して、SystemEDGE を起動します。

SystemEDGE によって「data」ディレクトリに管理対象モードの情報のない `sysedge.cf` ファイルが作成されます。

マネージャからの管理対象モードの情報の削除

以下の手順では、特定のサーバの SystemEDGE の設定から管理対象モードの情報を削除する方法について説明します。

次の手順に従ってください:

1. CA Virtual Assurance のユーザ インターフェースにログインし、[管理] に移動します。
[リソース] タブが開き、[エクスプローラ] ペインが表示されます。
2. SystemEDGE の設定を変更するサーバの名前を [検索] フィールドへ入力し、 (検索) をクリックします。
[検索] ウィンドウが開き、検索結果が表示されます。
3. 検索結果のいずれかをクリックします。
該当サーバの [リソース] ページが開き、[クイック スタート] パネルが表示されます。
4. [システムから削除] をクリックします。
該当サーバが [エクスプローラ] ペインに表示されなくなります。管理対象モードの情報を含めて、サーバに関連するすべてのオブジェクトがマネージャから削除されます。

管理対象外モードで SystemEDGE を実行するシステムの検出

以下の手順では、管理対象外モードで実行されているサーバを再検出する方法について説明します。

次の手順に従ってください:

1. CA Virtual Assurance のユーザ インターフェイスにログインし、[管理] に移動します。

[リソース] タブが開き、[エクスプローラ] ペインが表示されます。

2. [データ センター] を右クリックして、[管理] - [検出] - [サーバ] を選択します。

[検出] ウィンドウが開きます。

3. 前の手順で削除したサーバの名前を入力し、[終了] クリックします。

CA Virtual Assurance によって、SystemEDGE が管理対象外モードで実行されているサーバが検出されます。

CA Virtual Assurance で検出が完了すると、検出されたサーバの SystemEDGE は [ポリシー設定] に登録されていないことが確認できます。SystemEDGE は管理対象外モードで実行されています。

4. [エクスプローラ] ペインのサーバ名をダブルクリックします。

該当サーバの [リソース] ページが表示されます。

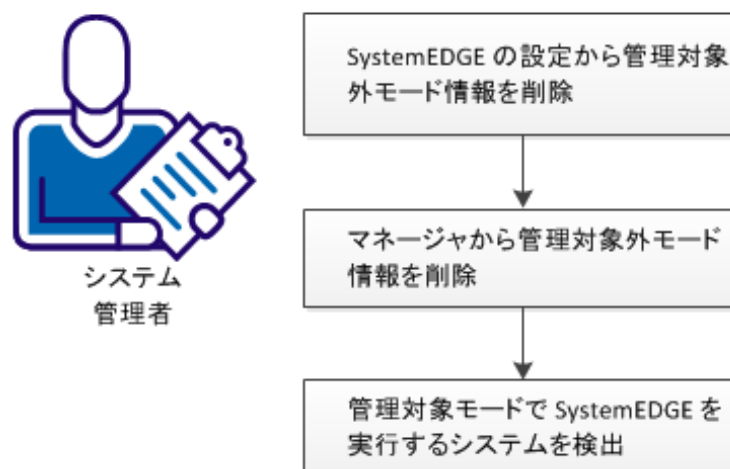
5. [サマリ] タブに切り替えて、CA Virtual Assurance よってサーバが正しく検出されたことを確認します。必要に応じて、CA Virtual Assurance がサーバのモニタリングに使用している別の SNMP コミュニティを選択できます。

これで、sysedge.cf 設定ファイルを編集して該当サーバの SystemEDGE を設定できるようになります。

管理対象外モードから管理対象モードへの SystemEDGE の変更方法

以下の図は、管理対象モードに変更するために必要なアクションの概要を示しています。

管理対象外モードから管理対象モードへの SystemEDGE の変更方法



以下の手順に従います。

[SystemEDGE の設定からの管理対象外モードの情報の削除](#) (P. 342)
[マネージャからの管理対象外モードの情報の削除](#) (P. 343)
[管理対象モードで SystemEDGE を実行するシステムの検出](#) (P. 344)

SystemEDGE の設定からの管理対象外モードの情報の削除

以下の手順では、特定のサーバの SystemEDGE の設定から管理対象外モードの情報を削除して、サーバを管理対象モードに変更できるよう準備する方法について説明します。

次の手順に従ってください:

1. SystemEDGE の設定モードを変更するサーバにログインします。
2. 便利な場所に以下のバックアップディレクトリを作成します。

```
data.backup  
config.backup
```

3. 通常の方法で SystemEDGE を停止します。

4. SystemEDGE の「data」ディレクトリに移動して、port<number>ディレクトリを開きます。デフォルトのディレクトリは port161 です。

ディレクトリの内容が一覧表示されます。

5. data.backup ディレクトリに以下のファイルを移動させて、port<number>ディレクトリに表示されないようにします。

sysedge.cf

6. SystemEDGE の「config」ディレクトリに移動します。

ディレクトリの内容が一覧表示されます。

7. config.backup ディレクトリに以下のファイルをコピーします。

sysedge.cf

8. 「config」ディレクトリに移動して、テキストエディタで sysedge.cf ファイルを開き、ファイルの末尾までスクロールします。

9. 以下の行を追加します。

manager_name <hostname of the manager>

10. ファイルを保存して、SystemEDGE を起動します。

SystemEDGE によって「data」ディレクトリに sysedge.cf ファイルが作成されます。

マネージャからの管理対象外モードの情報の削除

以下の手順では、特定のサーバの SystemEDGE の設定から管理対象外モードの情報を削除する方法について説明します。

次の手順に従ってください:

1. CA Virtual Assurance のユーザインターフェースにログインし、[管理] に移動します。

[リソース] タブが開き、[エクスプローラ] ペインが表示されます。

2. SystemEDGE の設定を変更するサーバの名前を [検索] フィールドへ入力し、 (検索) をクリックします。

[検索] ウィンドウが開き、検索結果が表示されます。

3. 検索結果のいずれかをクリックします。
該当サーバの [リソース] ページが開き、[クイック スタート] パネルが表示されます。
4. [システムから削除] をクリックします。
該当サーバが [エクスプローラ] ペインに表示されなくなります。サーバに関連するすべてのオブジェクトがマネージャから削除されます。

管理対象モードで SystemEDGE を実行するシステムの検出

以下の手順では、管理対象モードで SystemEDGE を実行するサーバを再検出する方法について説明します。

次の手順に従ってください:

1. CA Virtual Assurance のユーザ インターフェイスにログインし、[管理] に移動します。
[リソース] タブが開き、[エクスプローラ] ペインが表示されます。
2. [データ センター] を右クリックして、[管理] - [検出] - [サーバ] を選択します。
[検出] ウィンドウが開きます。
3. 前の手順で削除したサーバの名前を入力し、[終了] をクリックします。
CA Virtual Assurance によってサーバが検出されます。
CA Virtual Assurance で検出が完了すると、検出されたサーバの SystemEDGE が [ポリシー設定] に登録されていることが確認できます。SystemEDGE は管理対象モードで実行されています。
4. [エクスプローラ] ペインのサーバ名をダブルクリックします。
該当サーバの [リソース] ページが表示されます。
5. [サマリ] タブに切り替えて、CA Virtual Assurance によってサーバが正しく検出されたことを確認します。必要に応じて、CA Virtual Assurance がサーバのモニタリングに使用している別の SNMP コミュニティを選択できます。

SystemEDGE の設定モードの確認

基本的には、「[現在の設定モードの確認 \(P. 337\)](#)」の手順を繰り返すことができます。

SystemEDGE が管理対象外モードで実行される場合、「data」ディレクトリの動的な sysedge.cf ファイルの最初の行にはバージョンを指定します。

例

リリース 5.7.1

SystemEDGE が管理対象モードで実行される場合、最初の行には制御値 (ctrl_value) を指定します。

例

```
ctrl_value 0x9e30d00e

# Generated file - DO NOT EDIT
#
# Configuration file generated on 2012:03:27 05:37
#
# Generated from default.generic.0.prof
#
リリース 5.7.1
```

ディスカバリ プロセス中に、動的な sysedge.cf ファイルの末尾にメタ情報が追加されています。

例

```
template data_directory <path>
data_directory "C:¥Users¥Public¥CA¥SystemEDGE¥"
template default_port CA Portal
default_port 161
template manager_name <name>
manager_name manager_server.mycompany.com
template manager_policy_name <policy>
manager_policy_name default.generic
template manager_policy_version <version>
manager_policy_version 1
```

関連項目:

[SystemEDGE の現在の設定モードの確認 \(P. 337\)](#)

第 6 章：仮想環境の管理

このセクションには、以下のトピックが含まれています。

[Cisco UCS](#) (P. 347)
[Citrix XenServer](#) (P. 384)
[Huawei GalaX](#) (P. 410)
[IBM PowerVM \(LPAR\)](#) (P. 454)
[Microsoft Hyper-V Server](#) (P. 495)
[Red Hat Enterprise Virtualization](#) (P. 522)
[Solaris ゾーン](#) (P. 548)
[VMware vCloud](#) (P. 572)
[VMware vSphere および vCenter Server](#) (P. 595)

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、ネットワーキング、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。

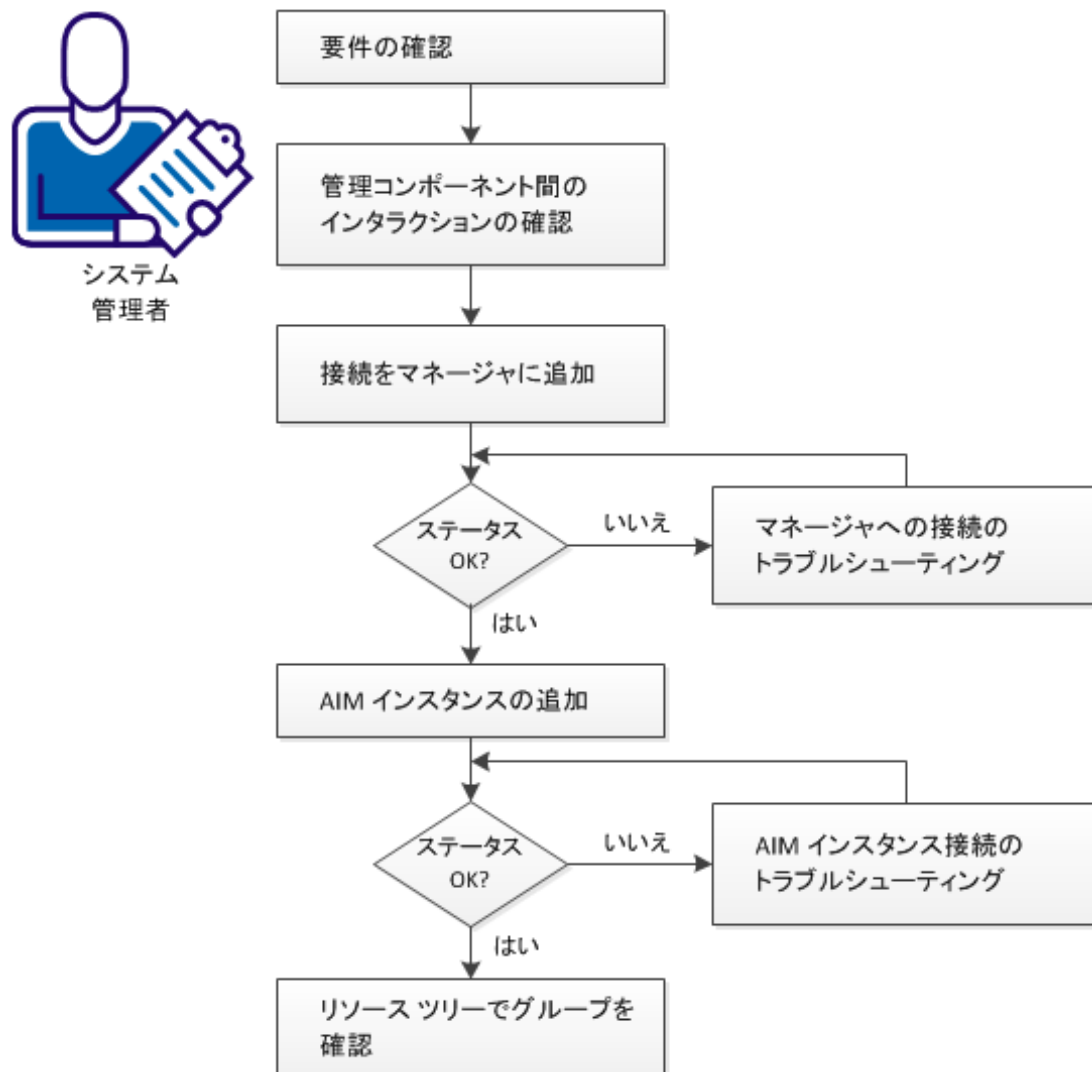
関連項目:

[Cisco UCS 管理コンポーネントを設定する方法](#) (P. 348)
[Cisco UCS の管理](#) (P. 362)

Cisco UCS 管理コンポーネントを設定する方法

以下の図は、管理コンポーネントを設定するために必要なアクションの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。

管理コンポーネントの設定方法



スイッチ上で実行される Cisco UCS Manager は、ネットワーキング、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。

以下の手順に従います。

[要件の確認 \(P. 349\)](#)

[Cisco UCS 管理コンポーネント間のインタラクション \(P. 351\)](#)

[マネージャへの Cisco UCS の追加 \(P. 353\)](#)

[サーバへのマネージャの接続が失敗する \(P. 354\)](#)

[UCS AIM サーバの登録 \(P. 356\)](#)

[AIM インスタンス接続のトラブルシューティング \(P. 357\)](#)

[リソース ツリーでの Cisco UCS の確認 \(P. 361\)](#)

要件の確認

CA Virtual Assurance の管理コンポーネントを設定する前に、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 および SystemEDGE に精通している。
- 以下を含む CA Virtual Assurance マネージャ インストールにアクセスできる。
 - プラットフォーム管理モジュール (PMM)
 - Application Insight Module (AIM)
 - モニタリング エージェント (SystemEDGE)
- CA Virtual Assurance ユーザ インターフェイスにアクセスできる。
- 管理対象となる環境のサーバ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 サービスを通して使用する環境のサーバ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

- 使用する環境にあるサーバが正常に実行されていることを確認済みである。
- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM 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。
- 使用するリモート 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。

関連項目:

[Cisco UCS サーバ](#) (P. 350)

Cisco UCS サーバ

Cisco UCS 管理に対する以下の条件を確認します。

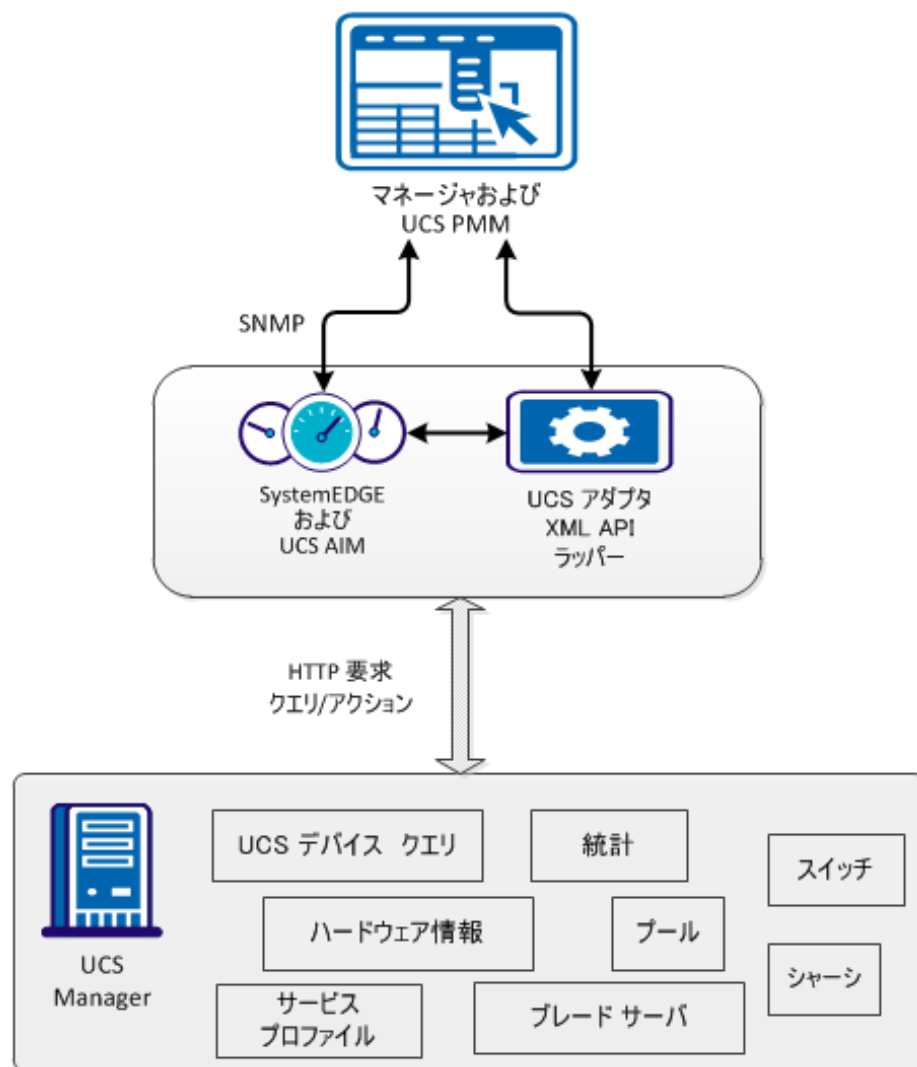
- Cisco Java ユーザインターフェースを起動して Cisco UCS Manager が実行されていることを確認します。Cisco Java ユーザインターフェースを起動するリンクは http://<UCS_Manager_name> または https://<UCS_Manager_name> です。

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 でハードウェア、統計、プール (UUID、MAC、WWPN、WWNN) 、および UCS Manager 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



この図は、Cisco UCS の統合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。

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。

マネージャへの Cisco UCS の追加

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。

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 [Cisco UCS] を選択します。
3. [Cisco UCS] ペインのツールバーで  (追加) をクリックします。
[Cisco Unified Computing System サーバの追加] ダイアログ ボックスが表示されます。
4. 必要な接続データ (サーバ名、ユーザ、パスワード、ポート) を入力し、優先 AIM を指定して、[管理ステータス] (チェック ボックス) をオンにします。
5. 必要なサーバ識別情報を入力して、[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は、右上のペインにサーバが緑のステータス アイコンを使って追加されます。

注: 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 によってサーバが赤のステータス 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。

サーバへのマネージャの接続が失敗する

症状:

「管理」 - 「設定」でサーバ接続を追加した後に、サーバ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。

- サーバへの接続に使用したデータが現在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。
- サーバ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。
- 接続に必要なすべてのサービスが、サーバシステム上で正しく実行されているかどうかを確認します。

サーバ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。
2. 接続の詳細を追加し、「管理ステータス」を有効にし、「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。
サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ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 <Server Name>  
ping <IP Address of Server>
```

2. サーバに有効な DNS エントリおよび IP アドレスが設定されているかどうかを調べるには、これらのコマンドの出力を確認します。

サーバが DNS で見つからない場合は、CA Virtual Assurance マネージャ システム上にある Windows の hosts ファイルにサーバを追加します。手順 3 に進みます。

サーバが DNS で見つかった場合は、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 <Server Name>
```

正しい IP アドレスとサーバ名を入力してファイルを保存します。例：

```
192.168.50.50 myServer
```

4. CA Virtual Assurance ユーザ インターフェイスで、[管理] タブの [設定] に移動して、[サーバ] ペインの右上角にある  (検証) をクリックします。

サーバの認証情報と接続データが正しく、サーバに対して ping を実行できる場合でも、接続に失敗することがあります。このような場合は、サーバに問題がある可能性があります。サーバへの接続を確立できない場合は、次の手順に進みます。

接続に必要なすべてのサービスが、サーバシステム上で正しく実行されているかどうかを確認する方法

1. サーバにアクセスするために、システム管理者に問い合わせます。
2. サーバシステムにログインします。
3. 接続に必要なすべてのサービスが正しく実行されているかどうかを確認します。
4. 必要に応じて、サービスを開始または再起動します。
5. **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 [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 によってサーバ接続が検証されます。

サーバ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収集したデータが正しいことを確認してください。

管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

UCS AIM サーバの登録

CA Virtual Assurance マネージャに **Cisco UCS** コンポーネントを追加した後、**Cisco UCS** 環境を管理するために、ユーザ インターフェースの [管理] ページを使用して **AIM** インスタンスを追加します。

次の手順に従ってください:

1. [スタート] メニューから **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 [Cisco UCS] を選択します。
3. [UCS AIM サーバ] ペイン ツールバーの  (追加) をクリックします。
[Cisco Unified Computing System AIM サーバの追加] ダイアログ ボックスが表示されます。
4. ドロップダウン リストから [UCS AIM サーバ] を選択します。
UCS AIM サーバのリストが表示されます。

5. ドロップダウンリストから [Cisco UCS サーバ] を選択します。

[Cisco UCS] ペインに一覧表示されたサーバが [Cisco UCS サーバ] ドロップダウンリストに入力されます。管理できる UCS サーバは、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。

注: AIM がリモートシステムに存在している場合、CA Virtual Assurance でこのシステムを最初に検出する必要があります。検出後、AIM サーバがドロップダウンリストに表示されます。

6. [OK] をクリックします。

選択したサーバの新しい AIM インスタンスが登録されます。

注: 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、Cisco UCS 環境の管理を開始できます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータスアイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

[管理] - [設定] でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  (ディスカバリが進行中) が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。ディスカバリにかかる時間は、環境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数によって異なります。アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Virtual Assurance はサーバフォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

[管理] - [設定] で AIM インスタンスを追加した後、ステータス アイコンに  (ポーリングなし) が表示されます。

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。このアイコンは、CA Virtual Assurance マネージャがこの AIM をポーリングしないこと表します。この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。別の AIM を使用したい場合は、[管理] - [設定] - [プロビジョニング] で優先 AIM を設定できます。サーバエントリの [編集] をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

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 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:

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。

- 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。

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. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

AIM サーバが 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 AIM サーバを追加します。手順 3 に進みます。

サーバが 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 AIM サーバの名前を入力します。例:

```
192.168.50.51 myAIM
```

4. [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. 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 [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 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、収集したデータがこのシナリオの要件に従っていることを確認してください。

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 AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン  (無効) が表示されます。この 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 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サーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

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。

- 欠落しているサーバから CA Virtual Assurance マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、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 Cisco UCS の確認

設定および検出に成功すると、新たに検出されたリソースが [リソース] - [エクスプローラ] ペインの対応するグループに表示されます。

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] ペインを開きます。
2. Cisco UCS グループを展開します。

管理対象の Cisco UCS リソースが表示されます。

CA Virtual Assurance で、設定された Cisco UCS 環境を管理する準備が整いました。

Cisco UCS の管理

CA Virtual Assurance と Cisco UCS の統合により、一元化されたユーザ インターフェースから UCS スイッチ、シャーシ、およびブレードを管理することができます。スイッチ上で実行される UCS Manager は、UCS リソースを表示し、クローン作成、スナップショット、電源操作などの管理操作を実行できる場所になります。

このセクションでは、[リソース] ページから Cisco UCS リソースに対して実行できるリソース管理操作について説明します。[リソース] ページには、以下の UCS オブジェクトに関する基本情報が表示されます。

- Cisco UCS サーバ
- UCS Manager サーバ
- シャーシ
- ブレード サーバ
- Fabric Interconnect
- 組織

[サマリ] ページでは、オブジェクトに関連付けられている情報を見ることができます（たとえば、シャーシサマリではそのブレードを表示でき、ブレードサマリではそのストレージを表示できます）。また、リソースに関連付けられているイベントを見ることができます。

[詳細] ページを利用できる場合は、その他のリソース情報（システム プロパティ、ソフトウェア、ハードウェア、パフォーマンスなど）を見ることができます。ここで自動化ソースを割り当てた後、デフォルトのアクセス プロファイルと管理プロファイルがシステムに対して自動的に作成され、ディスカバリが実行されます。

リソース管理タスクを実行するための、他のページを表示できる場合もあります。[エクスプローラ] ペイン内のオブジェクトを右クリックして表示されるメニューを使って UCS 管理タスクを実行することもできます。

関連項目:

[一元化されたサービス プロファイルを使用する方法](#) (P. 363)

[サービス プロファイル](#) (P. 365)

[ポート プロファイルを管理する方法](#) (P. 368)

[SNMP データ ポーラーの設定](#) (P. 371)

[サービス ポーラーの設定](#) (P. 372)

[Cisco UCS リソースの表示](#) (P. 373)

[サービス プロファイルとブレードの関連付け](#) (P. 374)

[UCS Manager 設定のバックアップ](#) (P. 375)

[vNIC テンプレート](#) (P. 376)

[UCS 組織](#) (P. 376)

[UCS プール](#) (P. 377)

[UCS のアクションタイプ](#) (P. 381)

[UCS トラップ管理](#) (P. 381)

[ブレード電源アクションの作成](#) (P. 382)

[UCS サーバの削除](#) (P. 383)

[UCS AIM の削除](#) (P. 383)

一元化されたサービス プロファイルを使用する方法

CA Virtual Assurance 管理 DB 内に存在するセントラル サービス プロファイルは、複数の UCS ドメインにわたって設定情報を管理する効率的な方法を提供します。CA Virtual Assurance ユーザ インターフェースを使用して、UCS Manager から 管理 DB にサービス プロファイルをインポートするか、管理 DB 内にセントラル サービス プロファイルを作成します。

管理 DB から、任意の UCS Manager にセントラル サービス プロファイルをエクスポートできます。

セントラル サービス プロファイルの管理

リソース ページからセントラル サービス プロファイルを管理できます。エクスプローラのペインで **[Cisco UCS サーバ]** を選択し、右側のペインの **[セントラル サービス プロファイル]** をクリックしてアクセスします。

UCS Manager からサービス プロファイルをインポートするには

1. 白の三角形（インポート）のアイコンをクリックします。
2. **[サービス プロファイルのインポート]** ダイアログ ボックスを使用して、**[UCS Manager]** を選択します。**[リフレッシュ]** をクリックしてサービス プロファイル リストを取り込み、**[すべてのサービス プロファイルのインポート]** を選択するか、またはリストから **1** つ以上の値を選択します。インポート後に **UCS Manager** からインポートされたプロファイルを削除するには、**[ソース サービス プロファイルの削除]** を選択します。
3. **[OK]** をクリックします。
選択したサービス プロファイルは **管理 DB** にインポートされます。

管理 DB でセントラル サービス プロファイルを作成または更新する方法

1. **[+]**（作成）アイコンをクリックするか、またはセントラル サービス プロファイルを選択してツール（編集）アイコンをクリックします。
2. ウィザード ページを使用して、セントラル サービス プロファイルを作成または更新します。

注: 管理 DB 内にサービス プロファイルを作成する場合、プールおよびポリシーは指定できません。これらの情報は参照専用です。これらの情報は、セントラル サービス プロファイルを **UCS Manager** にエクスポートした後に指定できます。

3. サービス プロファイルが作成または更新されたら、**[終了]** をクリックします。

UCS Manager にサービス プロファイルをエクスポートするには

1. **1** つ以上のセントラル サービス プロファイルを選択します。
2. 青の三角形（エクスポート）のアイコンをクリックします。
[サービス プロファイルのエクスポート] ダイアログ ボックスが表示されます。

3. [利用可能な UCS Manager] リストで、1 つの UCS Manager を選択し、右方向矢印をクリックして、[選択された UCS Manager] リストに転送します。すべてを転送するには、二重の右方向矢印をクリックします。
4. [OK] をクリックします。

注: プールとポリシーはエクスポートされないため、ターゲットの UCS Manager 上にすでに存在している必要があります。

管理 DB からサービス プロファイルを削除するには

1. 削除するサービス プロファイルを選択します。
2. [-] (削除) アイコンをクリックします。

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。

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。

ポートプロファイルを管理する方法

CA Virtual Assurance を使用してポートプロファイルを管理するには、以下の手順に従います。

1. プラグインをエクスポートします。

Cisco UCS Manager と vCenter 間の通信を確立するには、ターゲットの vCenter 内に拡張 XML ファイルを以下のとおり生成およびインストールします。

- vCenter 4.0 の場合、複数の拡張ファイルが必要です。
- vCenter 4.0 update 1 以上の場合、Cisco UCS Manager から 1 つの拡張ファイルをエクスポートします。

必要なファイルがエクスポートされたら、vSphere Client を使用してそれらのファイルを新規プラグインとして vCenter にインポートします。これは、UCS Manager と vCenter の組み合わせごとに一度ずつ必要になります。Cisco UCS Manager では、別の UCS Manager からエクスポートされたファイルを使用することはできません。

2. .vib ファイルを ESX サーバにエクスポートします。

ESX のバージョンに応じて、適切な .vib ファイル コンポーネントを Cisco Nexus 1000V Virtual Ethernet Module ソフトウェアからインストールすることによって、ESX サーバを設定します。このパッケージ (Cisco および VMware による共同設計) により、VMware 仮想インフラストラクチャと完全に統合される分散仮想スイッチ ソリューションが有効になります。

3. [ポートプロファイル ネットワーク トポロジの作成](#) (P. 370)
4. [ポートプロファイルとポートプロファイルクライアントの作成](#) (P. 370)

ポートプロファイル ネットワークトポロジの作成

ポートプロファイルを VMware にプッシュするには、Cisco UCS Manager に vCenter、データセンター、DVS フォルダ、DVS、およびプロファイルクライアントオブジェクトが定義されている必要があります。これらのオブジェクトのトポロジは VMware のトポロジと一致する必要があります。CA Virtual Assurance では、必要なトポロジを作成できます。

次の手順に従ってください:

1. [リソース] をクリックし、[エクスプローラ] ペインを開きます。
2. エクスプローラ ツリーで UCS Manager を右クリックし、[VMware] をクリックして、[vCenter のレイアウト] ダイアログ ボックスを開きます。
3. vCenter を展開し、vCenter、データセンター、DVS フォルダ、DVS、またはプロファイルクライアントオブジェクトを強調表示します。
4. [アクション] ドロップダウン メニューで [新規作成] を選択します。
5. 必須情報を入力し、[終了] をクリックします。DVS パネル上の [有効] を選択すると、関連付けられたポートプロファイルが vCenter に自動的にプッシュされます。

vCenter、データセンター、DVS フォルダ、DVS、またはプロファイルクライアントオブジェクトが追加されます。

注: このダイアログ ボックスを使用してトポロジオブジェクトを削除するには、[アクション] ドロップダウンリストの [削除] をクリックします。

ポートプロファイルとポートプロファイル クライアントの作成

CA Virtual Assurance vCenter の [レイアウト] ダイアログ ボックスを使用して、ポートプロファイルおよびポートプロファイル クライアントを作成することができます。

次の手順に従ってください：

1. エクスプローラ ツリーで **UCS Manager** を右クリックし、[VMware] をクリックして、[vCenter のレイアウト] ダイアログ ボックスを開きます。
2. ポートプロファイルを作成する場合は [ポートプロファイル] をハイライトし、ポートプロファイル クライアントを作成する場合は既存のポートプロファイル をハイライトします。
3. [アクション] ドロップダウン メニューで [新規作成] を選択します。
4. 必須情報を入力し、[OK] をクリックします。

ポートプロファイルまたはポートプロファイル クライアントが作成されます。

注： この手順を使用して、ポートプロファイルおよびポートプロファイル クライアントを編集または削除することもできます。既存のポートプロファイルまたはポートプロファイル クライアントをハイライトして、[アクション] ドロップダウン リストの [編集] または [削除] を選択します。

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. `¥conf¥caucsconf.cfg` 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。

Cisco UCS リソースの表示

「リソース」ページでは、**UCS** オブジェクト ツリーのすべてのレベルの **UCS** リソースを表示できます。たとえば、以下のオブジェクトを検査して情報を確認できます。

- Cisco UCS サーバ - カテゴリおよびブレード割り当てごとの **UCS** リソース、およびインポートされたサービス プロファイル
 - 一元化されたサービス プロファイル - **UCS Manager** の割り当て、インポート、およびエクスポート
 - **UCS Manager** - Fabric Interconnect、シャーシ、および組織
 - シャーシ - マウントされているブレードの数、ファンの数（およびそれらのステータス）、および入力/出力モジュール
 - ブレードサーバ - ブレードの数、電源がオンかオフか、サービス プロファイルに関連付けられているかどうか、および **OS** ホスト名
- 注: **OS** ホストを参照するには「エクスプローラ」ツリーのブレードを展開します。ブレードの **OS** ホスト名が表示されるのは、プロビジョニングとディスクバリが完了した後です。
- 個別のブレード - マザーボード、CPU、メモリ、およびストレージを含めて高いレベルのインベントリ
 - Fabric Interconnect - 高いレベルのハードウェアおよびファン
 - 組織 - プール、サービス プロファイル、およびサービス プロファイル テンプレート

Cisco UCS リソースを表示する方法

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. Cisco UCS リソースを検索し選択します。
右側のペインに、「リソース」ページが表示されます。

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。

UCS Manager 設定のバックアップ

CA Virtual Assurance は、以下に示すタイプの UCS Manager 設定情報のバックアップをサポートします。

- すべての状態
- すべての設定
- システム設定
- 論理設定

エクスポート/インポート機能を使用すると、Cisco UCS 機能をエミュレートし、バックアップジョブを作成および再実行できるようになります。

UCS Manager の設定をエクスポートする方法

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. Cisco UCS Manager を選択します。
右側のペインに UCS Manager ページが表示されます。
4. [エクスポート/インポート] をクリックします。
[エクスポート/インポート] ページが表示されます。
5. [エクスポート ジョブ] セクションで、[+]（作成）をクリックします。
[バックアップ操作の作成] ダイアログ ボックスが表示されます。
6. エクスポート情報を入力し、[OK] をクリックします。
エクスポートジョブが開始され、[エクスポート] リストに表示されます。

UCS Manager の設定をインポートする方法

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. Cisco UCS Manager を選択します。
右側のペインに **UCS Manager** ページが表示されます。
4. [エクスポート/インポート] をクリックします。
[エクスポート/インポート] ページが表示されます。
5. [インポート ジョブ] セクションで、[+]（作成）をクリックします。
[バックアップ操作の作成] ダイアログ ボックスが表示されます。
6. インポート情報を入力し、[OK] をクリックします。
インポート ジョブが開始され、[インポート] リストに表示されます。

vNIC テンプレート

CA Virtual Assurance は、vNIC テンプレートの作成および管理をサポートします。サービス プロファイルまたは VM のいずれかとしてテンプレートターゲットを指定できます。

vNIC テンプレートを作成するには、サービス プロファイル ウィザードで [vNIC Template を使用] を選択し、[vNIC テンプレートの作成] ダイアログ ボックスを開きます。また、[エクスプローラ] ペインで UCS 組織を右クリックします。

UCS 組織

関連する UCS リソースを組織でグループ化して、プール、サービス プロファイル、およびサービス プロファイル テンプレートのネスト階層を作成することで、UCS リソース管理を行うことができます。組織とサブ組織は作成および削除できます。

関連項目：

[サブ組織の作成](#) (P. 377)

サブ組織の作成

UCS ルート ツリー上には、組織またはサブ組織を作成できます。

組織を追加する方法

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。
ルートに移動するか、ルートを開いてサブ組織をクリックします。
3. ルートまたはサブ組織を右クリックし、[管理] - [サブ組織の作成] を選択します。
4. 新しいサブ組織を作成するには、[サブ組織の作成] ダイアログ ボックスを使用します。
サブ組織が作成されます。

UCS プール

CA Virtual Assurance では、UCS リソースをさらに効率的に管理するためのプールを作成できます。

注: プール範囲の競合が発生した場合は、警告が表示されます。

利用可能なプールのタイプは、以下のとおりです。

- 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

WWNN プールと WWPN プールは、リモートストレージ (SAN) を使用するためのブレードの設定に使用できます。

関連項目:

[UCS プールの表示](#) (P. 378)

[UCS プールの作成](#) (P. 379)

[UCS プールの名前変更](#) (P. 380)

[UCS プールの削除](#) (P. 381)

UCS プールの表示

[リソース] ページでは、UCS プールを表示できます。

UCS プールを表示する方法

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. UCS 組織ツリーの最上位にあるルートをクリックし、希望の組織に移動します。
4. [サマリ] をクリックします。
[サマリ] ページが表示されます。
5. [コンポーネント] セクションのドロップダウン メニューでプール タイプをクリックします。
6. 表示するプールを選択し、ツール (表示) アイコンをクリックします。
7. プール リストに戻るには、[キャンセル] をクリックします。

UCS プールの作成

UCS リソースをさらに効率的に管理するため、[リソース] ページでは UCS プールを作成できます。

リソース プールを作成する方法

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. UCS 組織ツリーの最上位にあるルートをクリックし、希望の組織に移動します。
4. [サマリ] をクリックします。
[サマリ] ページが表示されます。
5. [コンポーネント] セクションのドロップダウン メニューでプール タイプをクリックします。
6. [+] (新規プールの追加) ボタンをクリックします。
[プールの作成] ダイアログ ボックスが表示されます。
7. ダイアログ ボックスを使って定義を完成させます。
プールがプール リストに追加されます。

注: [クイック スタート] メニューをカスタマイズして機能を提供できます。

UCS プールの名前変更

[リソース] ページでは、UCS プールの変更できます。

UCS プールの変更する方法

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. UCS 組織ツリーの最上位にあるルートをクリックし、希望の組織に移動します。
4. [サマリ] をクリックします。
[サマリ] ページが表示されます。
5. [コンポーネント] セクションのドロップダウン メニューでプール タイプをクリックします。
6. 名前を変更するプールを選択します。
7. 二重矢印アイコン (>>) をクリックします。
[プールの名前変更] ダイアログ ボックスが表示されます。
8. ダイアログ ボックスを使ってプールの名前を変更します。
リスト内のプールの名前が変更されます。

UCS プールの削除

[リソース] ページでは、UCS プールを削除できます。

UCS プールを削除する方法

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. UCS 組織ツリーの最上位にあるルートをクリックし、希望の組織に移動します。
4. [サマリ] をクリックします。
[サマリ] ページが表示されます。
5. [コンポーネント] セクションのドロップダウンメニューでプールタイプをクリックします。
6. 削除するプールを選択します。
7. [-] (削除) アイコンをクリックします。
削除の確認が表示されます。
8. [はい] をクリックします。
プールが削除されます。

UCS のアクションタイプ

Cisco UCS リソースは、CA Virtual Assurance のアクションタイプを使用して新しいアクションを作成することができます。これらのアクションは、割り当てられたルール条件が満たされた場合に、UCS の電源投入、リソースの割り当て、およびその他の操作を自動化します。また、これらのアクションが特定の時間に実行されるようにスケジュールすることもできます。

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。

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。

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] をクリックします。
[Cisco UCS] 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. サーバのツールバーで [-] (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。
サーバが削除されます。

UCS AIM の削除

ユーザ インターフェースの [管理] ページでは、UCS AIM 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] をクリックします。
[Cisco UCS] ページが表示されます。
3. 削除する UCS AIM サーバを選択します。
4. サーバのツールバーで [-] (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。
UCS AIM サーバが削除されます。

Citrix XenServer

Citrix XenServer は、仮想化されたサーバおよびクライアント オペレーティング システムにベア メタルに近い仮想化パフォーマンスを提供する仮想化プラットフォームです。XenServer は Xen ハイパーバイザを使用して、それがインストールされているサーバを仮想化し、各サーバが保証されたパフォーマンスで同時に複数の仮想マシン (VM) をホストできるようにします。XenServer には、XenServer ホストの物理および仮想リソースを管理するための独自のオペレーティング システムがあるため、特定のオペレーティング システムを必要としません。XenServer では、Linux と Windows のゲスト オペレーティング システムをサポートしています。

XenServer リソースは、以下の 3 つのレベルで管理できます。

ホスト管理

XenServer ホストオブジェクトは、XenServer とその VM が実行される物理ホストを表します。XenServer ホストはスタンドアロン ホストとすることも、XenServer プールと関連付けることもできます。保守モードでは、XenServer ホストで利用可能な仮想および物理リソースのモニタ、仮想ディスク イメージが含まれるストレージ リポジトリの管理、タスクの管理、または XenServer ホストの実行を行えます。

リソース プール管理

リソース プールは最大で 16 台の XenServer ホストを接続したグループです。リソース プール内の XenServer ホストは、共有ストレージと動的に制御されるメモリ、CPU、およびネットワーク リソースを組み合わせて、VM が実行されるオペレーティング環境を提供します。プール内での XenServer ホストのメンバシップまたは役割を管理したり、高可用性を確保するために XenServer にプール メンバのヘルス状態をモニタさせたりすることができます。必要に応じて、プール ホスト間で VM のライブ マイグレーションを行って、ダウンタイムを回避できます。

仮想マシンの管理

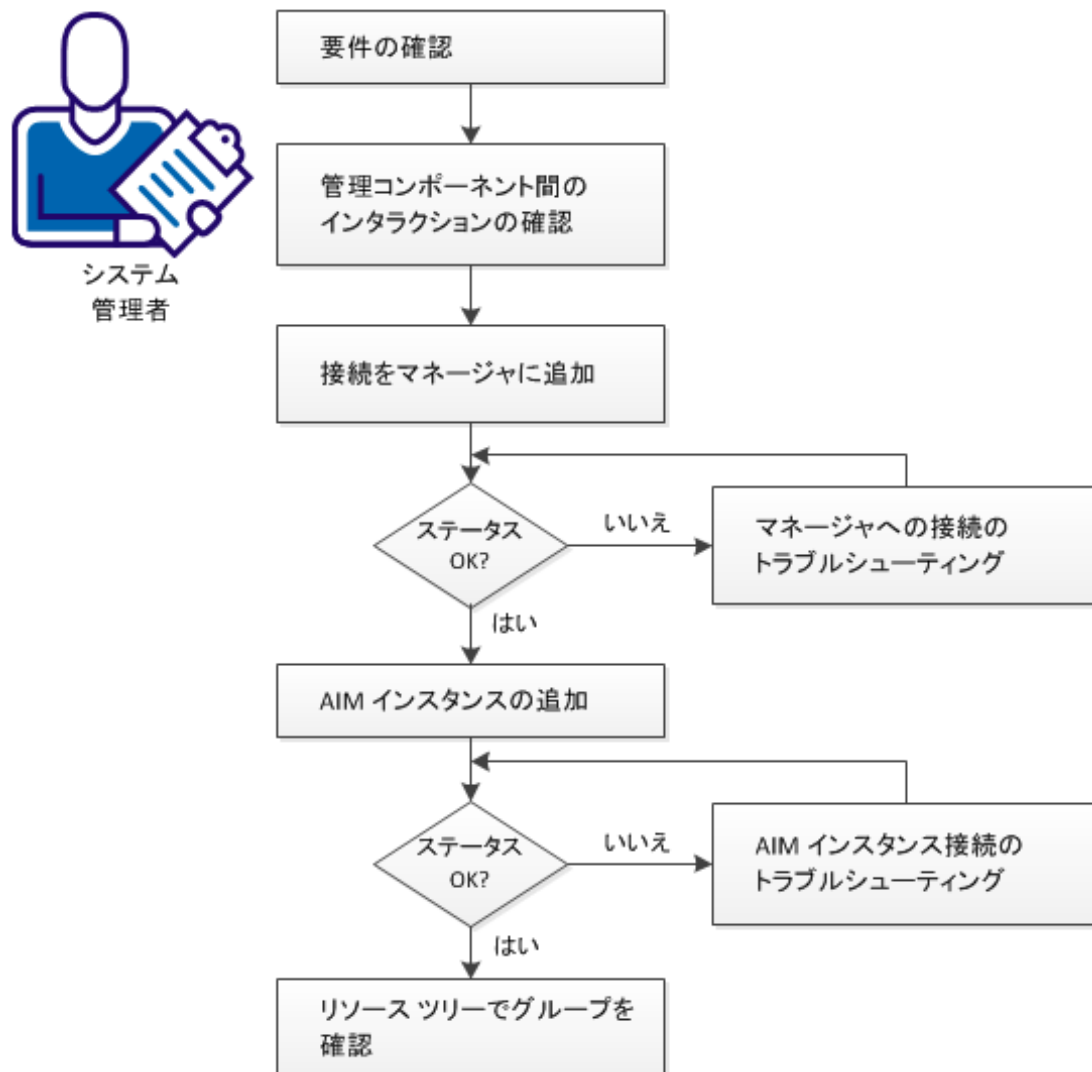
VM 管理レベルで、以下のタスクを実行できます。

- VM の制御 (検出、開始、中断、シャットダウン、ディスクから削除)
- VM の管理 (クローン)

XenServer 管理コンポーネントを設定する方法

以下の図は、管理コンポーネントを設定するために必要なアクションの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。

管理コンポーネントの設定方法



以下の手順に従います。

[要件の確認](#) (P. 386)

[Citrix XenServer 管理コンポーネント間のインタラクション](#) (P. 388)

[マネージャへの Citrix XenServer 接続の追加](#) (P. 389)

[マネージャへのサーバ接続の失敗 \(Citrix XenServer\)](#) (P. 390)

[検出された Citrix XenServer AIM インスタンスの追加](#) (P. 392)

[AIM インスタンス接続のトラブルシューティング](#) (P. 394)

[リソース ツリーでの Citrix XenServer グループの確認](#) (P. 397)

要件の確認

CA Virtual Assurance の管理コンポーネントを設定する前に、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 および SystemEDGE に精通している。
- 以下を含む CA Virtual Assurance マネージャ インストールにアクセスできる。
 - プラットフォーム管理モジュール (PMM)
 - Application Insight Module (AIM)
 - モニタリング エージェント (SystemEDGE)
- CA Virtual Assurance ユーザ インターフェースにアクセスできる。
- 管理対象となる環境のサーバ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 サービスを通して使用する環境のサーバ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
- 使用する環境にあるサーバが正常に実行されていることを確認済みである。

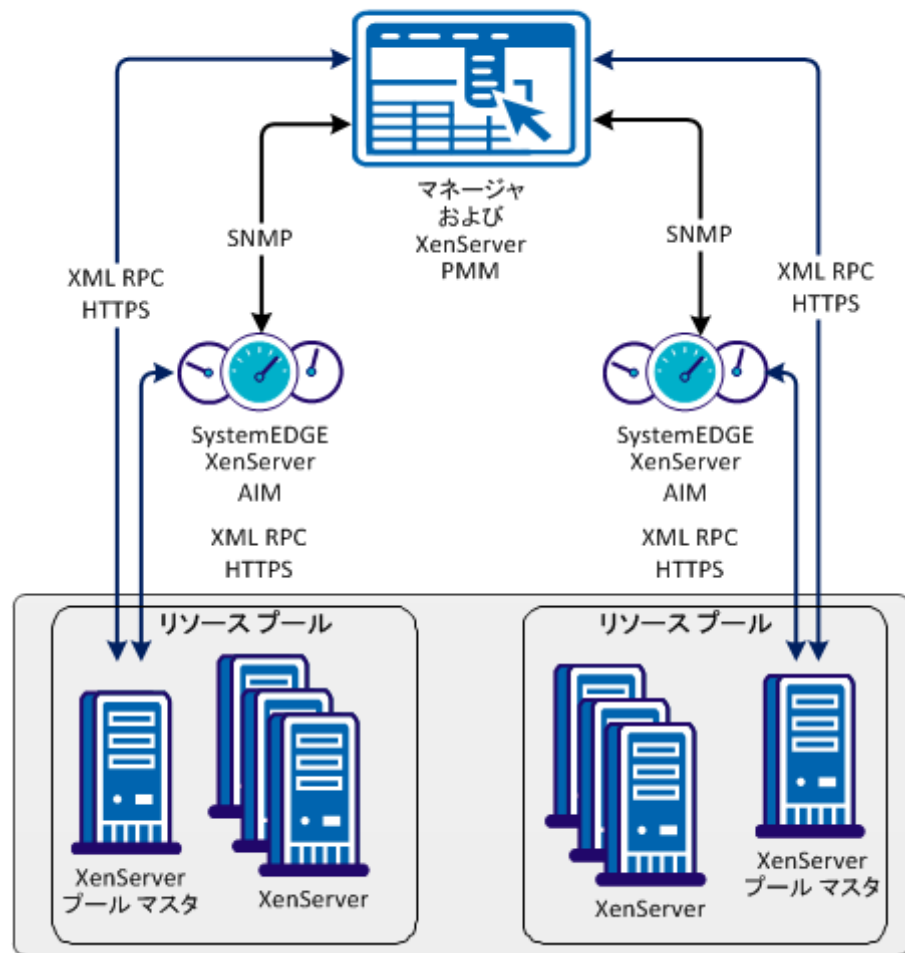
- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM のシステムでの SNMP 設定に整合性があることを確認済みである。読み取り/書き込みコミュニティ文字列および SNMP ポート番号が同一である。
- 使用するリモート AIM サーバが CA Virtual Assurance マネージャによって検出されることを確認済みである。

Citrix XenServer 管理コンポーネント間のインタラクション

Citrix XenServer AIM はマルチインスタンスのリモート AIM として実装されます。CA Citrix XenServer AIM は、複数のスタンドアロン Citrix XenServer および Citrix XenServer リソース プールをリモートでモニタできます。Citrix XenServer AIM は x86 および x64 モジュールとして実装されます。

Citrix XenServer 用の管理 API は XML RPC に基づいています。Citrix XenServer のリソース プールの場合、すべての XML RPC 通信は AIM、PMM、およびプール マスタ間にもみ発生します。

XenServer 管理コンポーネント間のインタラクション



マネージャへの Citrix XenServer 接続の追加

CA Virtual Assurance ユーザ インターフェースの [管理] タブを使用して、Citrix XenServer 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 [Citrix XenServer] を選択します。
3. [登録済み Citrix XenServer] ペイン ツールバーの  (追加) をクリックします。
[Citrix XenServer の追加] 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、ユーザ名、パスワード、リソース プールの UUID) を入力し、優先 AIM を指定して、[管理ステータス] (チェック ボックス) を有効にします。

重要: [登録済み Citrix XenServer] ヘッダー マスタが追加されていることを確認してください。

5. [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、右上のペインにサーバ追加され、緑のステータス アイコンが表示されます。 **CA Virtual Assurance** によって **Citrix XenServer** システム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** によってサーバがリストに追加され、接続の失敗を示す赤のステータス アイコンが表示されます。 [いいえ] をクリックすると、何も追加されません。

マネージャへのサーバ接続の失敗 (Citrix XenServer)

症状:

「管理」 - 「設定」でサーバ接続を追加した後に、サーバ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。

- サーバへの接続に使用したデータが現在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。
- サーバ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。
- サーバシステム上で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。

サーバ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。
2. 接続の詳細を追加し、「管理ステータス」を有効にし、「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。
サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ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 <Server Name>
ping <IP Address of Server>
```

2. サーバに有効な DNS エントリおよび IP アドレスが設定されていることをコマンドの出力で確認します。

サーバが DNS で見つからない場合は、CA Virtual Assurance マネージャ システム上にある Windows の hosts ファイルにサーバを追加します。手順 3 に進みます。

サーバが DNS で見つかった場合は、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 <Server Name>
```

正しい IP アドレスとサーバの名前を入力します。例：

```
192.168.50.50 myServer
```

4. 右上角の （検証）をクリックします。

サーバの認証情報と接続データが正しく、サーバに対して ping を実行できる場合でも、接続に失敗することがあります。このような場合は、サーバに問題がある可能性があります。サーバへの接続を確立できない場合は、次の手順に進みます。

サーバシステム上で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. サーバシステムにアクセスする方法を管理者に問い合わせます。
2. サーバシステムにログインし、`xsconsole` コマンドを実行します。
サービス コントロール コンソールが起動します。
3. サービスのステータスを確認し、報告された問題を解決します。
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 [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 によってサーバ接続が検証されます。

サーバ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収集したデータが現在も有効であることを確認してください。

管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

検出された Citrix XenServer AIM インスタンスの追加

CA Virtual Assurance マネージャに Citrix XenServer 接続を追加した後、Citrix XenServer を管理するための AIM インスタンスを追加します。

次の手順に従ってください:

1. [スタート] メニューから **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 [Citrix XenServer] を選択します。

3. [検出された Citrix XenServer AIM インスタンス] ペイン ツールバーの  (追加) をクリックします。

[Citrix XenServer AIM の追加] ダイアログ ボックスが表示されます。

4. ドロップダウン リストから [Citrix XenServer AIM サーバ] を選択します。

検出された XenServer AIM サーバのリストが表示されます。XenServer 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 [Citrix XenServer] を選択します。

[登録済み Citrix XenServer] ペインに一覧表示された XenServer が [XenServer] ドロップダウン リストに入力されます。管理できる XenServer 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。

注: AIM がリモート システムに存在している場合、CA Virtual Assurance でこのシステムを最初に検出する必要があります。検出後、AIM サーバがドロップダウン リストに表示されます。

6. [OK] をクリックします。

選択したサーバの新しい 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、Citrix XenServer 環境の管理を開始できます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

[管理] - [設定] でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  (ディスカバリが進行中) が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。ディスカバリにかかる時間は、環境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数によって異なります。アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Virtual Assurance はサーバフォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

〔管理〕 - 〔設定〕 で AIM インスタンスを追加した後、ステータス アイコンに  (ポーリングなし) が表示されます。

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。このアイコンは、CA Virtual Assurance マネージャがこの AIM をポーリングしないこと表します。この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。別の AIM を使用したい場合は、〔管理〕 - 〔設定〕 - 〔プロビジョニング〕 で優先 AIM を設定できます。サーバエントリの〔編集〕をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

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 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:

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。

- 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。

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. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

AIM サーバが 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 AIM サーバを追加します。手順 3 に進みます。

サーバが 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 AIM サーバの名前を入力します。例：

```
192.168.50.51 myAIM
```

4. [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. 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 [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 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、収集したデータがこのシナリオの要件に従っていることを確認してください。

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 AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン （無効）が表示されます。この 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 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サーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

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。

- 欠落しているサーバから CA Virtual Assurance マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、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 Citrix XenServer グループの確認

設定および検出に成功すると、新たに検出されたリソースが [リソース] - [エクスプローラ] ペインの対応するグループに表示されます。

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] ペインを開きます。
2. Citrix XenServer グループを展開します。
管理対象の Citrix リソース プールが表示されます。
3. リソース プールのエントリを展開します。
管理対象 Citrix XenServer が表示されます。

CA Virtual Assurance で、設定された Citrix XenServer 環境を管理する準備が整いました。

XenServer のプロビジョニング用に Linux テンプレートを準備する方法

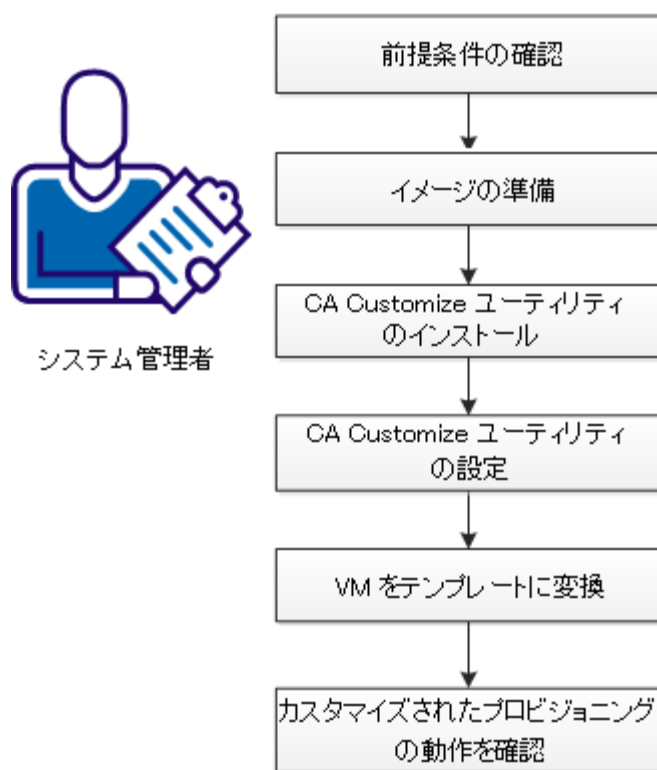
CA Virtual Assurance は、以下のオペレーティング システムを実行する新しい仮想マシン (VM) のカスタマイズされたプロビジョニングをサポートします。

- Red Hat Enterprise Server 6.0
- SUSE Linux Enterprise Server 11

カスタマイズ オプションには、ホスト名、パスワード、ドメイン、またはネットワーク設定が含まれます。

以下の図は、システム管理者が VM のプロビジョニング用に Linux テンプレートを準備する方法を示しています。

VM のプロビジョニング用に Linux テンプレートを準備する方法



以下の手順に従います。

[カスタマイズされた VM プロビジョニングの前提条件](#) (P. 399)

[Linux イメージの準備 \(XenServer\)](#) (P. 399)

[CA Customize ユーティリティのインストール](#) (P. 400)

[CA Customize ユーティリティの設定](#) (P. 401)

[VM をテンプレートに変換](#) (P. 402)

[カスタマイズされたプロビジョニングの動作](#) (P. 402)

カスタマイズされた VM プロビジョニングの前提条件

Linux ゲストをカスタマイズするには、ファイル システムまたはコンソールへの直接アクセスが必要です。

XenServer 環境が以下の前提条件に適合することを確認します。

- リソース プール内の各 XenServer で、SSH または SFTP アクセスを有効にしておく必要があります。

Linux イメージの準備 (XenServer)

Linux オペレーティング システムが含まれるテンプレートを作成するときには、この手順に従ってイメージを準備します。一部の手順は Linux ディストリビューションによって異なる場合があります。

次の手順に従ってください:

1. Linux オペレーティング システムを新しい仮想マシンにゼロからインストールします。
2. Citrix XenServer 用の XenTools を仮想マシンにインストールします。
3. ユーザ アカウント、ポリシー、アプリケーション、ホット フィックスなど、新しい仮想マシンに追加するカスタマイズを適用します。

この Linux イメージは、CA Customize ユーティリティを使用してさらにカスタマイズできます。

CA Customize ユーティリティのインストール

CA Customize ユーティリティを使用すると、CA Virtual Assurance で仮想マシンの設定を外部から変更できます。このゲストユーティリティは、OSの開始時に CD ドライブをモニタします。特別な ISO が接続されると、以下のアクションが実行されます。

1. コマンドセットによってゲストがカスタマイズされます。
2. ゲストシステムはカスタマイズ済みとしてマークされます。
この状態がリセットされるまで、システムはこれ以上変更できなくなります。
3. システムが停止し、カスタマイズが成功したことを示します。

ca-customize ゲストユーティリティを正しくインストールする方法

1. このユーティリティを以下で見つけます。
 - Red Hat Enterprise Server 6.0 の場合
`<InstallationRoot>%Utilities%\linuxCustomization%\rh6`
 - SUSE Linux Enterprise Server 11 の場合
`<InstallationRoot>%Utilities%\linuxCustomization%\sles11`
2. この実行可能ファイルを、準備する VM のハードドライブの以下の場所に移動します。
`/usr/bin/ca-customize`
3. (オプション) サポートされていない他のゲストシステムをサポートするには、ユーザ独自の `ca-customize` スクリプトを指定します。
4. `ca-customize` ユーティリティの実行可能ビットを有効にします。
`chmod 755 /usr/bin/ca-customize`

CA Customize ユーティリティの設定

Linux プロビジョニング用のテンプレートをセットアップできます。ゲストをカスタマイズするには、利用可能なスクリプトを使用します。また、ユーザ独自のスクリプトを使用して詳細なセットアップを行うこともできます。

次の手順に従ってください:

1. ネットワークがカスタマイズのプロセスに影響しないように、ネットワーク インターフェースを無効にします。

注: ネットワークはカスタマイズ中に自動的に有効化されます。

2. 必要に応じて、`/etc/ca-customize.conf` ファイルを使用して、デフォルトの CDROM デバイス名を上書きします。

`CD_DEVICE=/dev/cdrom`

CD ドライブに使用するデバイス名を定義します。

デフォルト: `/dev/cdrom`

3. ブートプロセスの最後に自動起動をセットアップします。

- (SUSE Linux の場合) `/etc/init.d/after.local` ファイルを作成または変更します。

```
#!/bin/bash
[ -e /etc/ca-customized ] || /usr/bin/ca-customize
```

- (Red Hat Linux の場合) 以下の行を `/etc/rc.local` ファイルに追加します。

```
[ -e /etc/ca-customized ] || /usr/bin/ca-customize
```

4. システムをシャットダウンします。

VM をテンプレートに変換

テンプレートを使用すると、カスタマイズした仮想マシンをいくつでも作成できます。

次の手順に従ってください:

1. VM をシャットダウンします。
2. 準備したイメージを XenServer テンプレートに変換するには、XenCenter を使用します。

テンプレートが CA Virtual Assurance に表示され、プロビジョニングのカスタマイズに使用できるようになります。

これらの手順の実行後、新規テンプレートを使用して任意の数のカスタマイズされた仮想マシンを新しく作成することができます。

カスタマイズされたプロビジョニングの動作

以下の手順は、カスタマイズされた VM プロビジョニングのワークフローを表します。

1. プラットフォーム管理サービスは新しい Linux VM をプロビジョニングします。
2. プラットフォーム管理サービスは、カスタマイズ パラメータを使用して新しい ISO を準備し、新しい VM に添付します。
3. プラットフォーム管理サービスは VM を開始します。
4. VM はカスタマイズ ISO が添付されていることを検出します。VM はカスタマイズ変更を適用します。
5. カスタマイズが成功すると、VM はシャットダウンします。PMM は VM の停止を検出します。プラットフォーム管理サービスは再度 VM を開始し、プロビジョニングを完了します。
6. カスタマイズが失敗すると、VM は停止しません。プラットフォーム管理サービスは以下のアクションを実行します。
 - a. プロビジョニングの失敗を返します
 - b. プロビジョニング ジョブを例外状態に設定します

カスタマイズ ログ

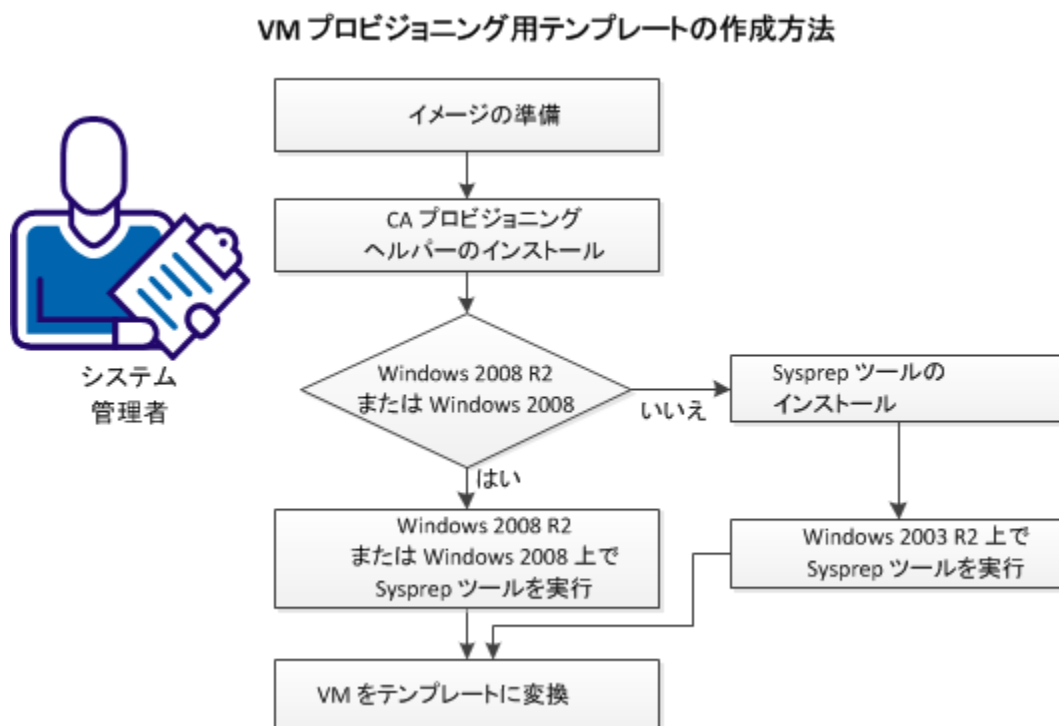
成功したカスタマイズは、`/etc/ca-customized` ファイルに格納されます。このファイルには、カスタマイズ変更のリストが含まれます。

カスタマイズに失敗すると、ログが `/etc/ca-customized.tmp` ファイルに格納されます。

XenServer のプロビジョニング用に Windows テンプレートを準備する方法

CA Virtual Assurance では、Windows 2003 R2 Server (32 ビット/64 ビット)、Windows 2008 (32 ビット/64 ビット) または Windows 2008 R2 Server (64 ビット) を実行する新しい仮想マシン (VM) でのプロビジョニングのカスタマイズをサポートしています。カスタマイズ オプションには多数の設定があります。たとえば、組み込みの管理者アカウントのパスワード、コンピュータ名、およびネットワーク設定を変更できます。

以下の図は、システム管理者が XenServer のプロビジョニング用に Windows テンプレートを準備する方法を示しています。



次の手順に従ってください:

1. [Windows イメージを準備します](#) (P. 404)。
2. [CA プロビジョニング ヘルパーをインストールします。](#) (P. 405)
3. (Windows 2003 R2 で有効) [Sysprep ツールをインストールします](#) (P. 405)。
4. 使用するオペレーティング システムに応じて、以下のアクションのいずれかを選択します。
 - [Windows 2003 R2 で Sysprep ツールを実行する。](#) (P. 405)
 - [Windows 2008 または Windows 2008 R2 で Sysprep ツールを実行する。](#) (P. 406)
5. [VM を XenCenter のテンプレートに変換します](#) (P. 406)。

Windows イメージの準備

Windows オペレーティング システムが含まれるテンプレートを作成するときには、この手順に従って、イメージを準備します。テンプレートをカスタマイズするには、CA Virtual Assurance のプロビジョニング操作を有効にする手順に従ってください。一部の手順は Windows のバージョンによって異なります。

次の手順に従ってください:

1. Windows オペレーティング システムを新しい仮想マシンにゼロからインストールします。
2. Citrix XenServer 用の XenTools を仮想マシンにインストールします。
3. ユーザ アカウント、ポリシー、アプリケーション、ホット フィックスなど、新しい仮想マシンに適用したいカスタマイズを適用します。
4. (Windows 2003 で有効) 組み込みの管理者アカウントのパスワードを空白にします。

注: 管理者パスワードが空でないと、プロビジョニングの際に SysPrep で新しいパスワードを設定できず、既存のパスワードが残ります。

XenServer 環境の前提条件

XenServer 環境が以下の前提条件に適合することを確認します。

- リソース プール内の各 XenServer で、SSH または SFTP アクセスを有効にしておく必要があります。

CA プロビジョニング ヘルパーのインストール

CA プロビジョニング ヘルパーは、CA Virtual Assurance で仮想マシンの設定を外部から変更できるようにするものです。

次の手順に従ってください:

1. <InstallationRoot>\Utilities\Sysprep\CAProvisioningHelper.exe でこのユーティリティを見つけます。
2. 準備する VM のハード ドライブの任意の場所に、この実行可能ファイルを移動します。
3. コマンド ラインから CA プロビジョニング ヘルパーを 1 回実行します。

Sysprep ツール

Microsoft は、設定されている Windows インストールを一般化、フリーズ、およびシャットダウンするための Sysprep ツールを提供しています。以下のセクションでは、Windows 2003 R2 および Windows 2008 R2 用の Sysprep ツールを使用する方法の詳細について説明します。

Sysprep ツールを Windows 2003 R2 にインストールして実行する

Windows 2003 では、Sysprep ツールはデフォルトではインストールされませんが、Windows インストール CD-ROM に収録されています。

Sysprep ツールのインストール

Windows インストール CD-ROM から Sysprep ツールをインストールします。

Windows 2003 R2 での Sysprep ツールの実行

Sysprep ツールのインストールを設定した後、Sysprep ツールを実行します。

次の手順に従ってください:

1. 以下の CAB ファイルを探して開きます。
`%SUPPORT%\TOOLS\%DEPLOY.CAB`
2. CAB ファイルに含まれるファイルをすべて選択し、%SystemDrive%\Sysprep (通常は C:\Sysprep) にコピーします。
 注: ディレクトリ名は変更しないでください。
3. Sysprep ディレクトリに移動して、以下を実行します。
`sysprep -quiet -reseal -mini -forcshutdown`

Windows 2008 R2 での Sysprep ツールの実行

通常の Windows インストールプロセスでは、Sysprep プロセスを実行するためのすべてのファイルがインストールされます。Windows インストールを設定した後、以下の手順を実行します。

1. Windows Server 2008 R2 用の Windows 自動インストールキット (WAIK) を使用して、有効な XML 応答ファイルを作成します。WAIK は Microsoft の Web サイトから入手できます。

注: このプロビジョニングでは、ダミーの自動応答ファイルが必要で、これがないとシャットダウンできません。応答ファイルの内容はプロビジョニングプロセスによって置換されるため、どのようなものでもかまいません。ただし、ファイルは Sysprep に固有の XML スキーマに従う必要があります。

2. 作成された XML ファイルに「sysprep.xml」と名前を付け、これを以下の Sysprep ディレクトリに置きます。

`%SystemRoot%\system32\sysprep`

3. 以下のコマンドを実行します。

`sysprep /generalize /oobe /shutdown /unattend:sysprep.xml`

VM を XenCenter のテンプレートへ変換

テンプレートを使用すると、カスタマイズした仮想マシンをいくつでも作成できます。

次の手順に従ってください:

1. 仮想マシンをシャットダウンします。
2. 準備したイメージを XenServer テンプレートに変換するには、XenCenter を使用します。

テンプレートが CA Virtual Assurance に表示され、プロビジョニングのカスタマイズに使用できるようになります。

VM ステータスの管理 (XenServer)

仮想マシンのステータスを制御するには、以下のいずれかの操作を行います。

- 検出
 - サーバ
 - ネットワーク
- 開始
- 中断
- シャットダウン
- ディスクから削除

VM ステータスを制御する方法

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. VM を右クリックし、[管理] を選択して、以下のいずれかのオプションを選択します。

検出

サーバまたはネットワークを検出します。

開始

指定された XenServer ホスト上の VM を開始します。

中断

指定された XenServer ホストで実行されている VM を中断して、その現在の状態を保存します。VM を再開するまで、すべてのアクティビティが中断されます。

シャットダウン

指定された XenServer ホストで実行されている VM をシャットダウンします。

ディスクから削除

ディスクから VM を削除します。

対応するウィザードが表示されます。

3. 必要な情報を入力して、次の手順に進みます。

4. サブミットします。

ステータス操作が実行され、確認のメッセージが表示されます。インターフェースをリフレッシュして、最新の **VM** ステータスを表示します。操作の結果を確認するイベントが表示されます。

Citrix XenServer 仮想マシンのプロビジョニング

以下の手順を実行することで、仮想マシンをプロビジョニングできます。
VM のプロビジョニング用の **Windows** テンプレートを準備してください。

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. Citrix XenServer グループを右クリックし、[プロビジョニング] - [Citrix XenServer 仮想マシンのプロビジョニング] を選択します。
プロビジョニング ウィザードが表示されます。
3. 必要な情報を入力します。

VM 名

新しい VM 名を定義します。

テンプレート

Windows プロビジョニング テンプレートを指定します。

管理者パスワード

新しい VM の管理者パスワードを定義します。

製品のアクティベーション キー

Windows 2003 のアクティベーション キーを定義します。

フル ネーム

VM のフル ネームを定義します。

4. (オプション) 追加情報 (ワークグループ、メモリ、CPU、VM ホスト、組織) を指定します。静的 IP アドレスを使用する場合は、DHCP を無効にし、IP アドレス、マスク、およびデフォルト ゲートウェイを指定します。

注: メモリと CPU の設定は、使用する Windows プロビジョニング テンプレートによって異なります。

5. サブミットします。
確認メッセージが表示されます。
6. [ジョブ] パネルをリフレッシュして、進捗状況を表示します。
操作の結果を確認するイベントが表示されます。

Huawei GalaX

Huawei GalaX には以下のプラットフォームが含まれます。

仮想化インフラストラクチャ プラットフォーム

コンピューティング、ストレージ、ネットワークなどの物理リソースを、集中管理、柔軟なスケジュール設定、動的割り当てが可能な仮想リソースに仮想化します。仮想化インフラストラクチャは、クラウドコンピューティング ベースのデータ センターを構築するために使用される重要なプラットフォームです。

クラウドコンピューティング インフラストラクチャ プラットフォーム

仮想化インフラストラクチャ プラットフォームによって提供された仮想リソースをカプセル化および管理します。キャリアや企業がデータ センター OMM 機能を構築するのを支援します。管理機能にはリソース管理、イメージ管理、課金管理、スケジュール管理、およびユーザ管理が含まれます。

操作および保守管理 (OMM) プラットフォーム

OMM ユーザのための統合 OMM インターフェースを提供します。OMM ユーザは、Web インターフェースによって SingleCLOUD OMM System にリモートからアクセスできます。ユーザは、リソース管理、リソース モニタリング、およびリソース統計レポートなどの操作を実行できます。

関連項目：

[Huawei GalaX 管理コンポーネントを設定する方法](#) (P. 411)

[Virtual Private Cloud VLAN を作成する方法](#) (P. 426)

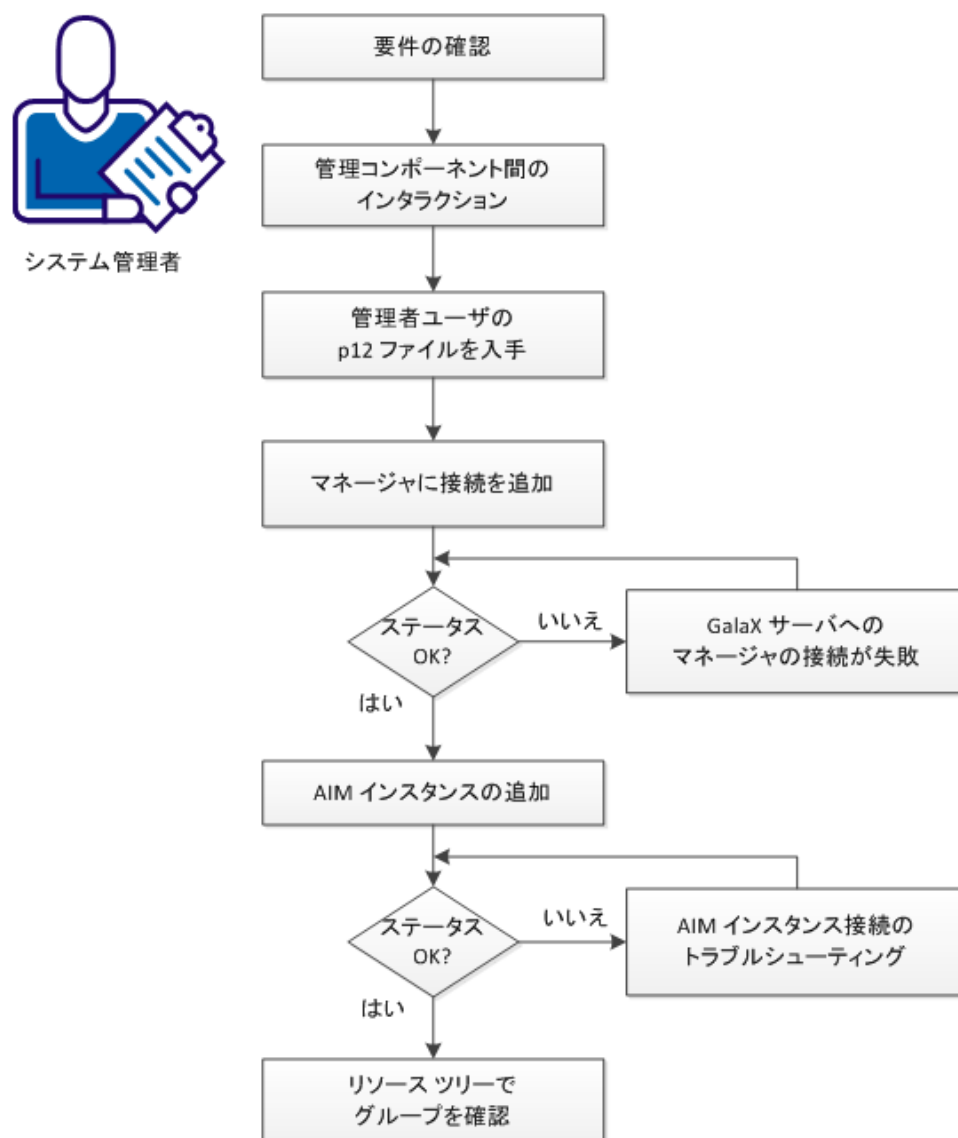
[Huawei SingleCLOUD 環境を管理する方法](#) (P. 438)

[GalaX のプロビジョニング用に Windows テンプレートを準備する方法](#) (P. 449)

Huawei GalaX 管理コンポーネントを設定する方法

システム管理者として、ユーザの Huawei GalaX 環境に接続し、そのパフォーマンスをモニタするように CA Virtual Assurance を設定できます。

GalaX 管理コンポーネントの設定方法



以下の手順に従います。

[要件の確認 \(P. 412\)](#)

[Huawei GalaX 管理コンポーネント間のインタラクションの確認 \(P. 413\)](#)

[管理者ユーザ p12 ファイルの取得 \(P. 415\)](#)

[新しい GalaX 接続のマネージャへの追加 \(P. 417\)](#)

[GalaX サーバへのマネージャの接続が失敗する \(P. 418\)](#)

[GalaX サーバの AIM インスタンスの追加 \(P. 421\)](#)

[リソース ツリーでの Huawei GalaX の確認 \(P. 422\)](#)

[AIM インスタンス接続のトラブルシューティング \(P. 422\)](#)

要件の確認

CA Virtual Assurance の管理コンポーネントを設定する前に、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 および SystemEDGE に精通している。
- 以下を含む CA Virtual Assurance マネージャ インストールにアクセスできる。
 - プラットフォーム管理モジュール (PMM)
 - Application Insight Module (AIM)
 - モニタリング エージェント (SystemEDGE)
- CA Virtual Assurance ユーザ インターフェースにアクセスできる。
- 管理対象となる環境のサーバ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 サービスを通して使用する環境のサーバにアクセスするために使用するポートを決定済みである。
デフォルトの HTTP ポート : 8773。
- 使用する環境にあるサーバが正常に実行されていることを確認済みである。

- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM 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。
- 使用するリモート 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。

Huawei GalaX 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 Huawei GalaX 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 GalaX 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。Huawei GalaX は、1 つ以上の Computing Resource Managers (CRM) と通信する Elastic Service Controller (ESC) から構成されます。CRM は複数の Computing Node Agents (CNA) と通信します。

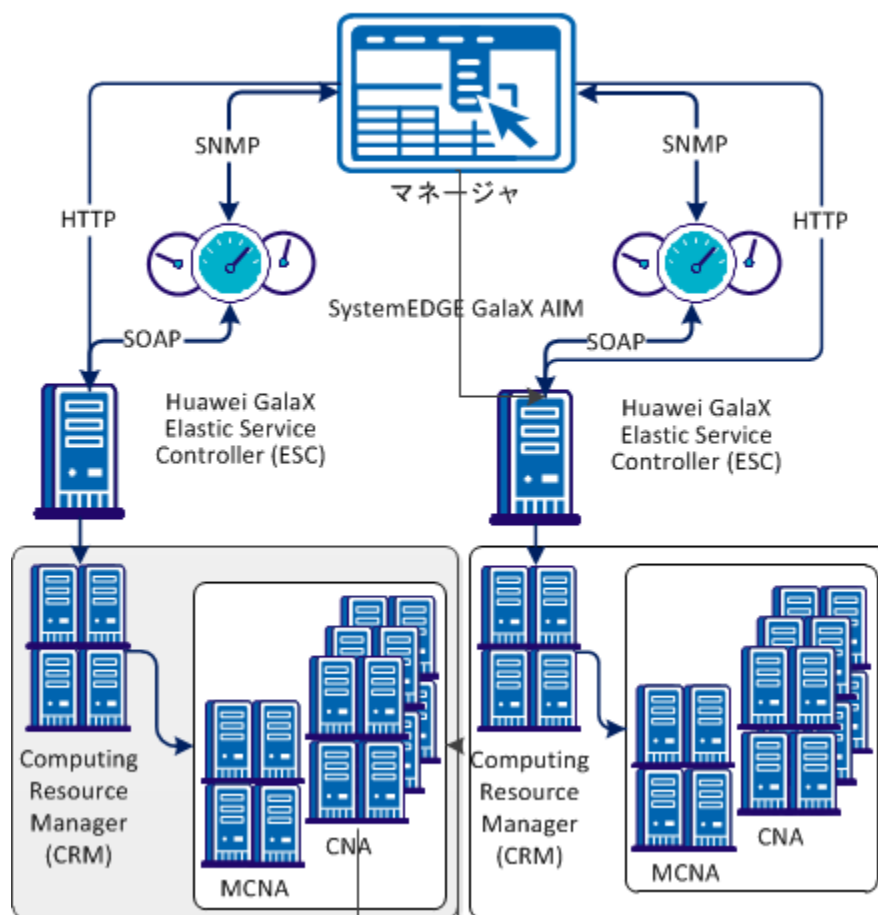
GalaX を管理するため、CA Virtual Assurance は、その GalaX プラットフォーム管理モジュール (PMM)、GalaX Application Insight Module (AIM)、および Elastic Service Controller (ESC) の間にネットワーク接続を必要とします。これらのネットワーク接続を確立するには、CA Virtual Assurance GalaX 管理コンポーネント (つまり GalaX PMM と GalaX AIM) を設定します。

GalaX 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。GalaX AIM によって SystemEDGE は、複数の GalaX 環境のパフォーマンスをモニタでき、モニタ対象 GalaX リソースの状態を評価できます。しきい値に基づき、SystemEDGE および 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。

GalaX PMM は CA Virtual Assurance マネージャのコンポーネントです。PMM には、SOAP を使用するすべての Huawei GalaX 操作のサポートと接続を提供する役割があります。PMM は、Computing Resource Manager との接続を管理し、GalaX 関連の操作を実行します。また、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。

以下の図は、2つの GalaX ESC 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、GalaX PMM およびそのマルチインスタンス サポートを含む各 GalaX AIM は、複数の Elastic Service Controller 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 SOAP に基づきます。

Huawei GalaX 管理コンポーネント間のインタラクション



管理者ユーザ p12 ファイルの取得

CA Virtual Assurance UI で操作を実行するには、GalaX 環境から管理者ユーザ p12 ファイルを取得します。p12 ファイルでは、GalaX 環境を設定、モニタ、および管理するための管理者権限が提供されます。

p12 証明書ファイルは、GalaX のインストール中に生成されます。証明書ファイルはグローバルに一意であり、特定の Elastic Service Controller (ESC) API に対してのみ有効です。特定の証明書ファイルを使用して異なる GalaX ESC サーバにアクセスすることはできません。

以下の手順を実行する前に、お使いの GalaX ESC サーバの IP アドレス、および、root ユーザのパスワードを確認してください。

次の手順に従ってください:

1. p12 ファイルの生成に使用するパスワードを指定します。
このパスワードは、CA Virtual Assurance マネージャと GalaX ESC サーバの間の接続を設定する際にも必要になります。
2. root を使用して GalaX ESC サーバにログインします。
3. ターミナル ウィンドウを開き、以下のコマンドを実行します。

```
cd /opt/eucalyptus/.euca
```

このディレクトリには証明書ファイルが含まれています。

4. デジタル署名された証明書ファイルおよび秘密鍵証明書ファイルの名前を取得するには、ls コマンドを実行します。

ファイル名の形式は、以下のようになります。

- デジタル署名された証明書ファイル: euca2-admin-*-cert.pem
- 秘密鍵証明書ファイル: euca2-admin-*-pk.pem

5. 以下のコマンドを実行します。

```
openssl pkcs12 -export -in <デジタル署名された証明書ファイル> -out admin.p12 -inkey  
<秘密鍵証明書ファイル>
```

例:

```
openssl pkcs12 -export -in euca2-admin-109f9d47-cert.pem -out admin.p12 -inkey  
euca2-admin-109f9d47-pk.pem
```

6. システムにプロンプトが表示されます： "Enter Export Password"
7. 手順 1 で指定したパスワードを入力します。

システムによって、要求された **admin.p12** 証明書ファイルが
/opt/eucalyptus/.euca ディレクトリに生成されます。

8. **CA Virtual Assurance** マネージャが存在するサーバに **admin.p12** ファイルをコピーします。ディレクトリは、サーバ上の任意のディレクトリを使用できます。 **admin.p12** ファイルを **Windows** システムにコピーするには、**WinSCP** などのツールを使用することができます。
9. これで、**CA Virtual Assurance** マネージャと **GalaX ESC** サーバの間の接続を確立するために **admin.p12** ファイルとパスワードを使用できるようになりました。

新しい GalaX 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、GalaX 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 [Huawei SingleCLOUD] 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 GalaX サーバおよび関連する GalaX AIM サーバが表示されます。
3. [GalaX 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 GalaX サーバ] 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 (ユーザ名、サーバ、ポート、P12 ファイルパス、およびパスワード) を入力し [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 [GalaX Server] ペインに GalaX 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 GalaX サーバ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 GalaX サーバが赤のステータス 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。

GalaX サーバへのマネージャの接続が失敗する

症状:

「管理」 - 「設定」でサーバ接続を追加した後に、サーバ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。

- サーバへの接続に使用したデータが現在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。
- サーバシステムが実行されており、アクセス可能であることを確認します。
- CA Virtual Assurance サーバと GalaX サーバ間の時間差が 5 分未満であることを確認します。
- 接続に必要なサービスがサーバ上で正しく実行されていることを確認します。

サーバ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。
2. 接続の詳細を追加し、「管理ステータス」を有効にし、「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。
サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ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 <Server Name>
ping <IP Address of Server>
```

2. サーバに有効な DNS エントリおよび IP アドレスが設定されているかどうかを調べるには、これらのコマンドの出力を確認します。

サーバが DNS で見つからない場合は、CA Virtual Assurance マネージャ システム上にある Windows の hosts ファイルにサーバを追加します。手順 3 に進みます。

サーバが DNS で見つかった場合は、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 <Server Name>
```

正しい IP アドレスとサーバ名を入力してファイルを保存します。例：

```
192.168.50.50 myServer
```

4. CA Virtual Assurance ユーザ インターフェースで、[管理] タブの [設定] に移動して、[サーバ] ペインの右上角にある  (検証) をクリックします。

サーバの認証情報と接続データが正しく、サーバに対して ping を実行できる場合でも、接続に失敗することがあります。このような場合は、サーバに問題がある可能性があります。サーバへの接続を確立できない場合は、次の手順に進みます。

CA Virtual Assurance サーバと GalaX サーバ間の時間差が 5 分未満であるかどうかを確認する方法

1. GalaX サーバにアクセスするために、システム管理者に問い合わせます。
2. GalaX サーバのシステム時間を確認します。
3. CA Virtual Assurance マネージャ システムのシステム時間を確認します。
4. システムの時間差が 5 分を超える場合は、時間設定を適切に更新します。

接続に必要なすべてのサービスが、サーバシステム上で正しく実行されているかどうかを確認する方法

1. GalaX サーバにログインします。
2. 接続に必要なサービスが正しく実行されていることを確認します。
3. 必要に応じて、サービスを開始または再起動します。
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 [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 によってサーバ接続が検証されます。

サーバ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収集したデータが正しいことを確認してください。

管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

GalaX サーバの AIM インスタンスの追加

CA Virtual Assurance マネージャに新しい GalaX 接続を追加した後、新しい GalaX サーバを管理するための GalaX AIM インスタンスを追加します。その後、そのすべての物理および仮想コンポーネントを含む Huawei GalaX 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 [Huawei SingleCLOUD] 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 GalaX サーバおよび関連する GalaX AIM サーバが表示されます。
3. [GalaX 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 GalaX AIM サーバ] ダイアログ ボックスが表示されます。
4. [GalaX AIM サーバ] ドロップダウン リストを開きます。
検出された GalaX AIM サーバのリストが表示されます。
5. ドロップダウン リストから [GalaX AIM サーバ] を選択します。
[GalaX サーバ] ペインに一覧表示された GalaX サーバが [GalaX サーバ] ドロップダウン リストに入力されます。管理できる GalaX サーバは、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。
注: AIM がリモート システムに常駐している場合、AIM サーバがドロップダウン リスト内に表示されるように、最初に CA Virtual Assurance によってシステムが検出される必要があります。
6. 管理する GalaX サーバを選択し、[OK] をクリックします。
選択した GalaX サーバの新しい 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でない場合、CA Virtual Assurance は関連付けられている Huawei GalaX 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、Huawei GalaX の仮想および物理リソースの管理を開始できます。

リソース ツリーでの Huawei GalaX の確認

設定および検出に成功すると、新たに検出されたリソースが [リソース] - [エクスプローラ] ペインの対応するグループに表示されます。

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] ペインを開きます。
2. Huawei SingleCLOUD グループを展開します。

Huawei GalaX リソースが表示されます。

CA Virtual Assurance で、設定された Huawei GalaX 環境を管理する準備が整いました。リソースのステータスとプロパティをモニタできます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

[管理] - [設定] でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  (ディスカバリが進行中) が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。ディスカバリにかかる時間は、環境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数によって異なります。アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Virtual Assurance はサーバフォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

[管理] - [設定] で AIM インスタンスを追加した後、ステータス アイコンに  (ポーリングなし) が表示されます。

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。このアイコンは、CA Virtual Assurance マネージャがこの AIM をポーリングしないこと表します。この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。別の AIM を使用したい場合は、[管理] - [設定] - [プロビジョニング] で優先 AIM を設定できます。サーバエントリの [編集] をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

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 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:

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。

- 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。

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. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

AIM サーバが 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 AIM サーバを追加します。手順 3 に進みます。

サーバが 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 AIM サーバの名前を入力します。例:

```
192.168.50.51 myAIM
```

4. [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. 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 [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 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、収集したデータがこのシナリオの要件に従っていることを確認してください。

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 AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン  (無効) が表示されます。この 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 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サーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

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。

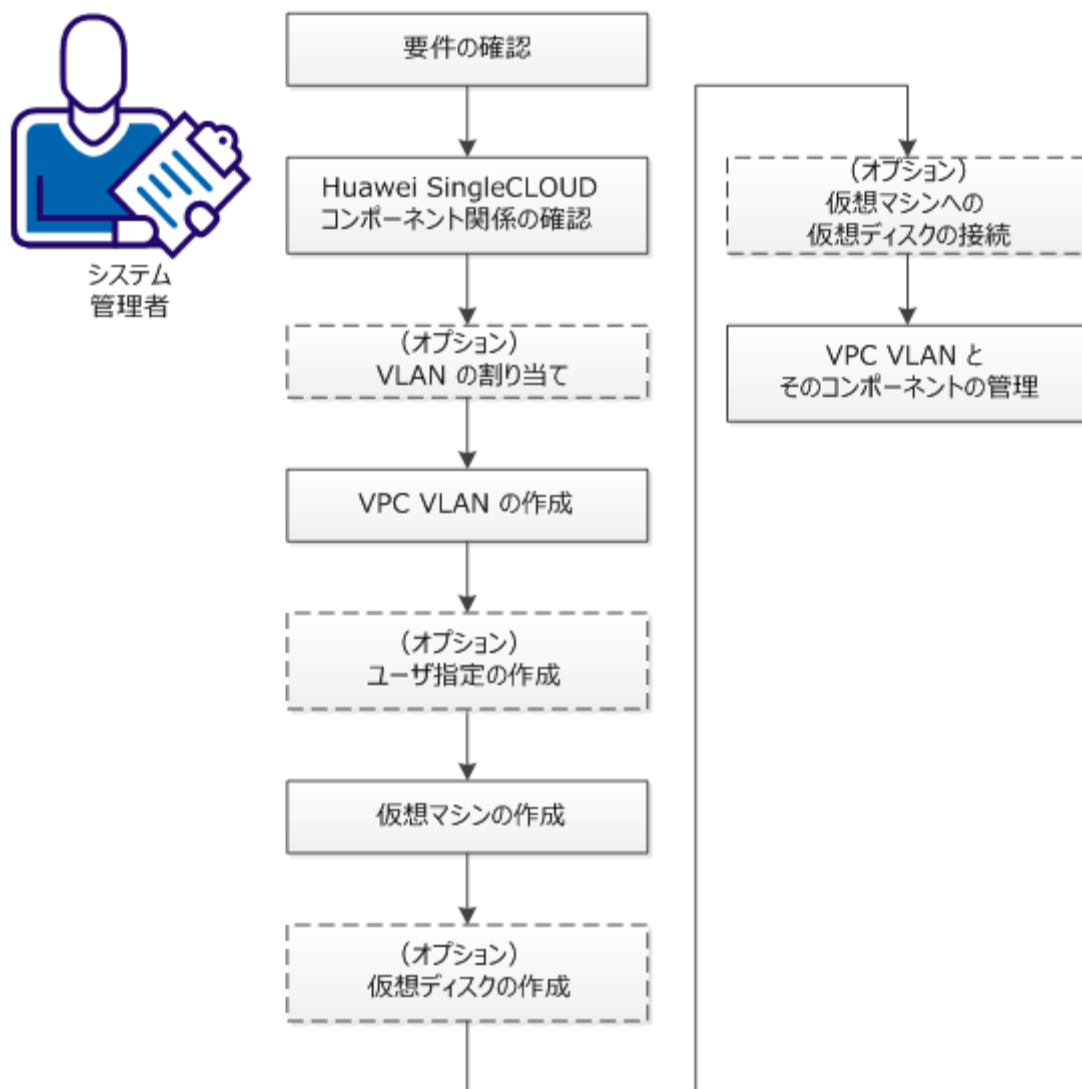
- 欠落しているサーバから CA Virtual Assurance マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、その管理ステータスを「有効」に変更します。

Virtual Private Cloud VLAN を作成する方法

システム管理者として GalaX 環境の関連する仮想マシンと仮想ディスクで Virtual Private Cloud を作成するとします。 *Virtual Private Cloud* (VPC) は、複数の仮想マシンおよび関連する仮想ディスクを備えた Huawei SingleCLOUD ユーザのためのプライベート ローカル ネットワークです。 CA Virtual Assurance が GalaX 環境をすでに検出しているため（「[要件の確認](#) (P. 429)」を参照）、CA Virtual Assurance ユーザ インターフェースは必要な VPC VLAN リソースを作成するためのインフラストラクチャを提供します。

以下の図は、VPC VLAN の作成方法に関する必要な手順を示しています。

VPC VLAN の作成方法



以下の手順に従います。

[要件の確認](#) (P. 429)

[Huawei SingleCLOUD コンポーネント関係の確認](#) (P. 430)

[\(オプション\) VLAN の割り当て](#) (P. 432)

[VPC VLAN の作成](#) (P. 433)

[\(オプション\) ユーザ指定の作成](#) (P. 433)

[仮想マシンの作成](#) (P. 434)

[\(オプション\) 仮想ディスクの作成](#) (P. 436)

[\(オプション\) 仮想マシンへの仮想ディスクの接続](#) (P. 437)

[VPC VLAN とそのコンポーネントの管理](#) (P. 437)

要件の確認

CA Virtual Assurance で Huawei SingleCLOUD インスタンスをセットアップする前に、以下の前提条件を確認します。

- Huawei GalaX 環境に精通していること。
- CA Virtual Assurance ユーザ インターフェース、およびリソースをプロビジョニングする方法に精通していること。
- モニタリング ソフトウェア (SystemEDGE) の展開および設定に精通していること。
- CA Virtual Assurance がインストールされており、CA Virtual Assurance ユーザ インターフェースにアクセスできること。
- Huawei GalaX 環境が利用可能で、実行されていること。
- コンピューティング クラスタのサーバ (仮想マシン用) およびストレージクラスタ (仮想ディスク用) が Huawei GalaX 環境で利用可能であること。
- 仮想マシンに適用するオペレーティング システムのイメージが Huawei GalaX 環境で利用可能であること。
- CA Virtual Assurance と Huawei GalaX サーバの間の接続が確立されていること。
- GalaX AIM が Huawei GalaX サーバをモニタするように設定されていること。
- ユーザ VLAN プールおよび VPC VLAN プール用のサーバが利用可能であること。
- CA Virtual Assurance が Huawei GalaX サーバとその関連リソース (クラスタ、ストレージクラスタ、仮想マシンなど) を検出していること。
- 共有ディスクには Microsoft Cluster Service (MSCS) が必要です。

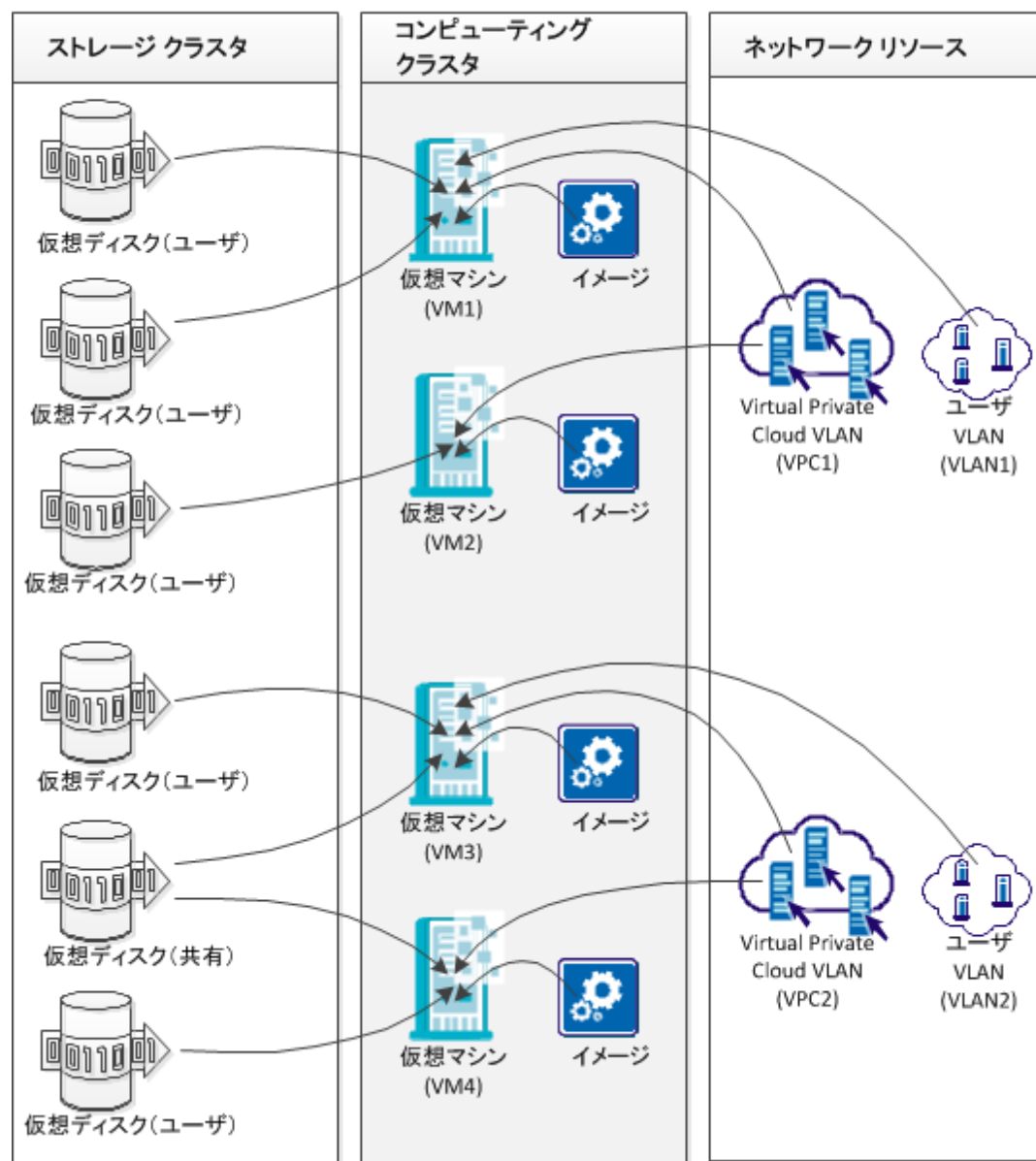
Huawei SingleCLOUD コンポーネント関係の確認

Huawei GalaX 環境は Huawei SingleCLOUD ソリューションの一部で、クラウドサービスプロバイダまたは企業顧客のクラウドコンピューティングデータセンター向けに設計されています。

Huawei SingleCLOUD ソリューションは階層状のアーキテクチャから構成されます。物理層およびネットワーク層のデバイスはソリューションへ統合されます。クラスタ、分散ストレージ、NAS ストレージ、および仮想化の技術に基づいて、これらの統合されたデバイスはストレージ、コンピューティング、およびネットワークサービスを上層のサービスに提供します。CA Virtual Assurance 内の Huawei SingleCLOUD インスタンスには、お使いの Huawei GalaX 環境を管理、モニタするために必要なインフラストラクチャが含まれます。Huawei GalaX 環境は、クラスタおよびそれらに関連するリソースから構成されます。

以下の図は、CA Virtual Assurance によって管理できる SingleCLOUD ソリューションの GalaX コンポーネントおよびこれらのコンポーネント間の依存関係を示します。

Huawei SingleCLOUD GalaX コンポーネントおよびそれらの関係



最初に、クラウド内の仮想マシンとそのユーザへの **VLAN** アクセスを提供する **VPC VLAN** を作成します。必要に応じて、ユーザ **VLAN** を仮想マシンに追加できます。コンピューティング クラスタ内の仮想マシンには、適切なイメージ、および仮想マシンが属する **VPC VLAN** が必要です。イメージには、この仮想マシン用のオペレーティング システムおよびアプリケーションが含まれます。

その後、ストレージクラスタで仮想ディスクを作成し、これらのディスクを適切な仮想マシンに接続して、ユーザに固有のデータを格納することができます。ユーザディスクと共有ディスクという 2 つのタイプの仮想ディスクがサポートされています。ユーザディスクには仮想マシンとの 1 対 1 の関係があります。また、共有ディスクには一対多数の関係がありえます。共有ディスクには **Microsoft Cluster Service (MSCS)** サポートが必要です。

(オプション) VLAN の割り当て

Virtual Private Cloud オブジェクトが **VLAN** を必要とするため、最初に **VLAN** を割り当てます。

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] - [リソース] をクリックします。
[エクスプローラ] ツリーが開きます。
2. **Huawei SingleCLOUD** フォルダを展開し、適切な **SingleCLOUD** サーバを選択します。
右側のペインがリフレッシュされ、[リソース管理] および [ネットワーク管理] タブが表示されます。
3. [ネットワーク管理] - [VLAN] をクリックします。
既存の **VLAN** オブジェクトのリストが表示されます。
4. [VLAN] ペインのツールバーで  (追加) をクリックします。
[VLAN の割り当て] ダイアログ ボックスが表示されます。
5. **VLAN** 名を指定し、ドロップダウン メニューからクラスタを選択し、方法 (自動または手動入力) を指定して、[OK] をクリックします。
VLAN が割り当てられます。

VPC VLAN の作成

VPC は、いくつかの仮想マシンおよび関連する仮想ディスクを備えたクラウドユーザのためのプライベート ローカル ネットワークとして機能します。

次の手順に従ってください:

1. [スタート] メニューから **CA Virtual Assurance** ユーザ インターフェースを開きます。 [管理] - [リソース] をクリックします。
[エクスプローラ] ツリーが開きます。
2. **Huawei SingleCLOUD** フォルダを展開し、適切な **SingleCLOUD** サーバを選択します。
右側のペインがリフレッシュされ、[リソース管理] および [ネットワーク管理] タブが表示されます。
3. [ネットワーク管理] - [VPC] をクリックします。
既存の **VPC** インスタンスのリストが表示されます。
4. [VPC] ペインのツールバーで  (追加) をクリックします。
[VPC の作成] ダイアログ ボックスが表示されます。
5. **VPC** 名を指定し、ドロップダウンメニューからクラスタを選択し、(自動的にまたはリストから手動で) **VLAN** を割り当てて、[OK] をクリックします。
VPC インスタンスが作成されます。

(オプション) ユーザ指定の作成

ユーザ指定は、仮想マシンを作成するために使用可能な **CPU**、メモリ、およびシステム ボリューム サイズに対する 1 セットの設定値です。

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] - [リソース] をクリックします。
エクスプローラのツリーが開きます。
2. **Huawei SingleCLOUD** フォルダを展開し、適切な **SingleCLOUD** サーバを選択します。
右側のペインがリフレッシュされ、[リソース管理] および [ネットワーク管理] タブが表示されます。

3. [リソース管理] - [ユーザ指定] をクリックします。
既存のユーザ指定のリストが表示されます。
4. [ユーザ指定] ペインのツールバーで  (追加) をクリックします。
[ユーザ指定の作成] ダイアログ ボックスが表示されます。
5. CPU、メモリおよびシステム ボリューム サイズのユーザ指定の名前および値を指定します。 [OK] をクリックします。
ユーザ指定が作成されます。

仮想マシンの作成

仮想マシンには、システム ボリューム、CPU、メモリおよびディスク空き領域の設定用のイメージ、VPC および NIC 仕様が必要です。

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] - [リソース] をクリックします。
[エクスプローラ] ツリーが開きます。
2. Huawei SingleCLOUD フォルダを展開し、適切なコンピューティング クラスタを右クリックします。
ポップアップ メニューが表示されます。
3. [管理] - [テンプレートから VM を作成] を選択します。
[VM の作成] ダイアログ ボックスが開きます。
4. 以下のパラメータを指定して、[OK] をクリックします。
 - VM 数
 - VM Name
 - Image ID
 - ユーザ指定または CPU、メモリ、ディスク領域
 - VPC VLAN
 - (オプション) 追加のネットワーク インターフェース コントローラ (NIC)

- サービス品質 (QoS) の設定

- メモリ予約
- CPU 予約
- CPU 制限
- 高可用性
- NIC 速度制限

CA Virtual Assurance は指定された仮想マシンを作成します。仮想マシンは、割り当てられた VPC VLAN に属します。仮想マシンのリストを取得するには、[コンピューティング クラスタ] パネルの [詳細] タブを開きます。

以下のダイアログ ボックスには追加の説明が必要です。

メモリ予約

仮想マシンに割り当てられる物理メモリの最小の割合を指定します。予約はパーセント (%) で定義され、値は 0 ~ 100 % を割り当てることができます。

例：メモリを 2 GB に設定し、予約を 25 % に設定した場合、システムにより、仮想マシンに 512 MB 以上が確保されます。

CPU 予約

この仮想マシンに予約される物理 CPU パフォーマンスの割合の最小値を指定します。予約はパーセント (%) で定義され、値は 0、50、または 100 % を割り当てることができます。

例：予約を 50 % に設定した場合、システムにより、各 CPU コアの CPU 時間は 50 % 以上が確保されます。

CPU 制限

この仮想マシンが割り当てることができる CPU パフォーマンスの最大のパーセンテージを指定します。

注：制限の値は、予約用にしていた値以上である必要があります。

(オプション) 仮想ディスクの作成

仮想ディスクはユーザ固有のデータを格納するためのもので、仮想マシンに接続されています。

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] - [リソース] をクリックします。
[エクスプローラ] ツリーが開きます。
2. **Huawei SingleCLOUD** フォルダを展開し、適切なストレージクラスタを右クリックします。
ポップアップ メニューが表示されます。
3. [管理] - [ディスクの作成] を選択します。
[ディスクの作成] ダイアログ ボックスが表示されます。
4. 以下のパラメータを指定して、[OK] をクリックします。
 - ディスク名
 - ディスク タイプ (ユーザ ディスクまたは共有ディスク)。ユーザ ディスクは 1 つの仮想マシンに接続できます。共有ディスクは複数の仮想マシンに接続できます。
 - 動的な割り当て (通常またはシンプロビジョニング)
シンプロビジョニングには IP SAN デバイス サポートが必要です。
 - ディスク サイズ (GB)
 - 仮想ディスクの説明

CA Virtual Assurance は仮想ディスクを作成します。仮想ディスクのリストを取得するには、[ストレージクラスタ] パネルの [詳細] タブを開きます。

(オプション) 仮想マシンへの仮想ディスクの接続

指定された仮想ディスク タイプに従って、1つの仮想マシンにユーザ ディスクを、複数の仮想マシンに共有ディスクを接続することができます。

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] - [リソース] をクリックします。
[エクスプローラ] ツリーが開きます。
2. **Huawei SingleCLOUD** フォルダを展開し、適切なストレージ クラスタを選択します。
[ストレージ クラスタ] パネルが表示され、指定された仮想ディスク がリスト表示されます。
3. 接続する仮想ディスクを選択し、 接続アイコンをクリックします。
利用可能な仮想ディスクのリストが表示されます。
4. 適切な仮想マシンを選択し、[OK] をクリックします。
仮想ディスクが接続されます。

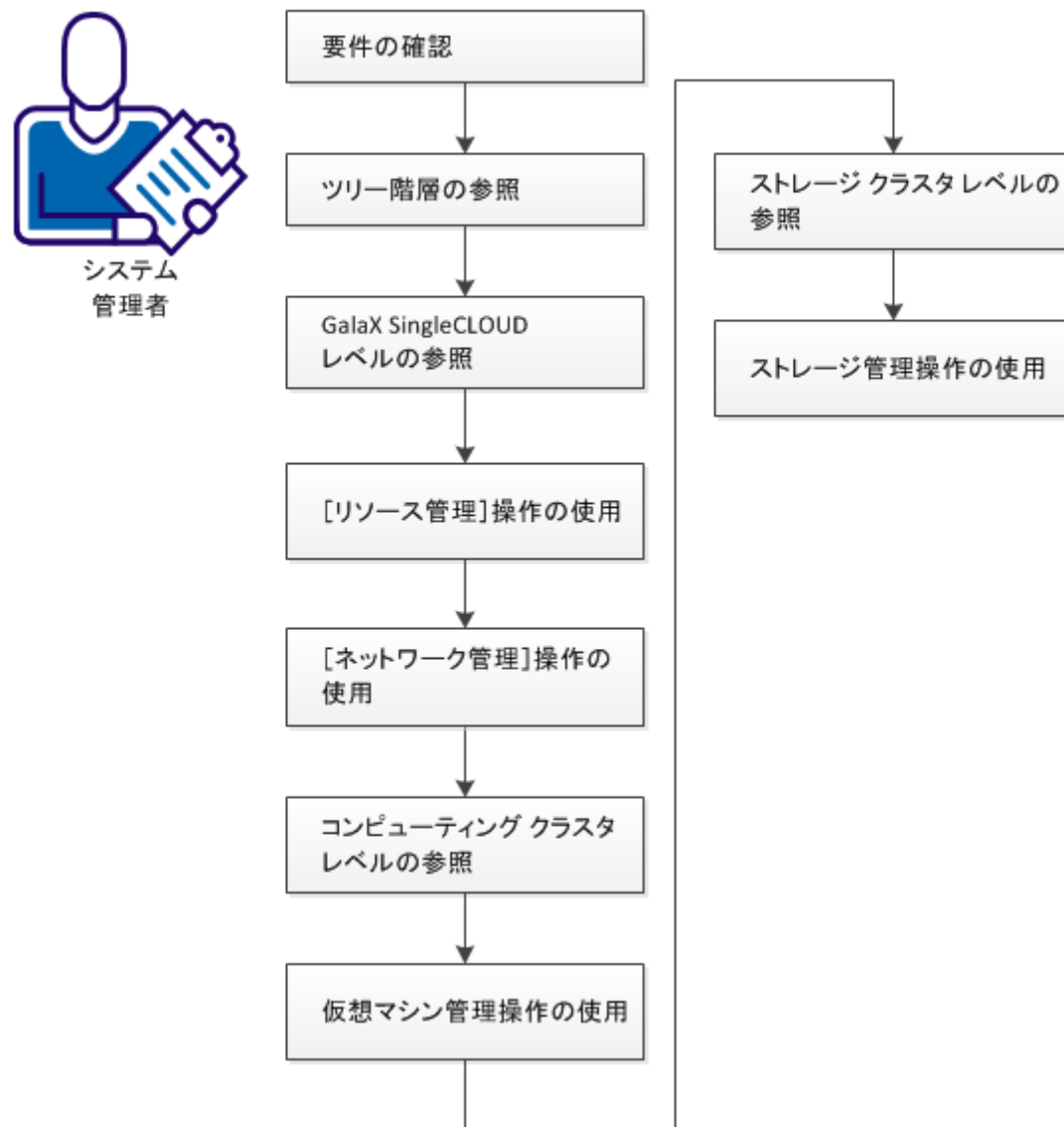
VPC VLAN とそのコンポーネントの管理

通信に **VLAN** を使用する仮想ディスクが接続された仮想マシンが指定されているとします。これらのリソースは、**CA Virtual Assurance** によって管理できる **Virtual Private Cloud** に属します。

Huawei SingleCLOUD 環境を管理する方法

ユーザ インターフェースの大部分が見たとおりの内容であるため、このシナリオは Huawei SingleCLOUD 環境のオブジェクト階層を検索し、関連する管理機能を参照するためのガイドラインです。

Huawei SingleCLOUD 環境を管理する方法



以下の手順に従います。

[要件の確認](#) (P. 440)

[ツリー階層の参照](#) (P. 441)

[GalaX SingleCLOUD サーバ レベルの参照](#) (P. 442)

[\[リソース管理\] 操作の使用](#) (P. 442)

[\[ネットワーク管理\] 操作の使用](#) (P. 443)

[コンピューティング クラスタ レベルの参照](#) (P. 443)

[仮想マシン管理操作の使用](#) (P. 444)

[ストレージ クラスタ レベルの参照](#) (P. 448)

[ストレージ管理操作の使用](#) (P. 449)

要件の確認

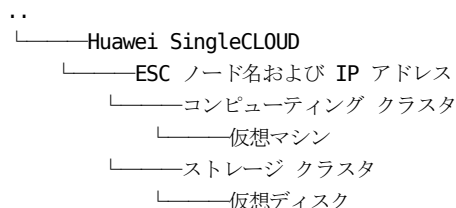
CA Virtual Assurance 内の Huawei SingleCLOUD インスタンスを管理する前に、以下の前提条件を確認します。

- Huawei GalaX 環境に精通していること。
- CA Virtual Assurance ユーザ インターフェース、およびリソースをプロビジョニングする方法に精通していること。
- モニタリング ソフトウェア (SystemEDGE) の展開および設定に精通していること。
- CA Virtual Assurance がインストールされており、CA Virtual Assurance ユーザ インターフェースにアクセスできること。
- Huawei GalaX 環境が利用可能で、実行されていること。
- コンピューティング クラスタのサーバ (仮想マシン用) およびストレージクラスタ (仮想ディスク用) が Huawei GalaX 環境で利用可能であること。
- 仮想マシンに適用するオペレーティング システムのイメージが Huawei GalaX 環境で利用可能であること。
- CA Virtual Assurance と Huawei GalaX サーバの間の接続が確立されていること。
- GalaX AIM が Huawei GalaX サーバをモニタするように設定されていること。
- ユーザ VLAN プールおよび VPC VLAN プール用のサーバが利用可能であること。
- CA Virtual Assurance が Huawei GalaX サーバとその関連リソース (クラスタ、ストレージクラスタ、仮想マシンなど) を検出していること。
- 仮想マシンを備えた Virtual Private Cloud が利用可能である。

ツリー階層の参照

SingleCLOUD vCloud フォルダは、最上位のサービス レベルを表します。SingleCLOUD サービスは 1 つ以上の Elastic Service Controller (ESC) から構成されます。各 ESC は、仮想マシンと仮想ディスクを備えた複数のコンピューティング クラスタおよびストレージ クラスタを制御できます。

以下の図は、SingleCLOUD vCloud フォルダのオブジェクト階層を表しています。



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] - [リソース] をクリックします。
[エクスプローラ] ツリーが開きます。
2. Huawei SingleCLOUD フォルダを展開します。
 - Huawei SingleCLOUD イベントのリストを開くには、Huawei SingleCLOUD オブジェクトを選択します。
 - リソース管理とネットワーク管理にアクセスするには、ESC ノードを選択します。
 - 利用可能な仮想マシンのリストを取得するか、または仮想マシンを作成するには、コンピューティング クラスタを選択します。
 - 利用可能な仮想ディスクのリストを取得するか、または仮想ディスクを作成するには、ストレージ クラスタを選択します。

GalaX SingleCLOUD サーバレベルの参照

GalaX SingleCLOUD は、ツリー階層内の 2 番目のレベルに存在します。

次の手順に従ってください:

1. [スタート] メニューから **CA Virtual Assurance** ユーザ インターフェースを開きます。 [管理] - [リソース] をクリックします。
エクスプローラのツリーが開きます。
2. Huawei SingleCLOUD フォルダを展開します。
フォルダ階層が表示されます。
3. ESC ノードを選択します。
[リソース管理] および [ネットワーク管理] タブが表示されます。
 - スナップショット、イメージ、およびユーザ指定には [リソース管理] を使用します。
 - VPC VLAN およびユーザ VLAN には [ネットワーク管理] を使用します。

[リソース管理]操作の使用

ユーザ インターフェースは、[リソース管理] タブ下で以下の操作を提供します。

- スナップショットとそれらのプロパティの表示
- 仮想マシンへのスナップショットのリストア
- スナップショットの削除
- イメージとそれらのプロパティの表示
- ユーザ指定とそれらのプロパティの表示
- ユーザ指定の作成
- ユーザ指定の編集
- ユーザ指定の削除

使用方法とダイアログ ボックスから内容がわかるようになっています。
必要な場合、ツールヒントを表示させるためにアイコン上にカーソルを移動することができます。

[ネットワーク管理]操作の使用

ユーザインターフェースは、[リソース管理] タブ下で以下の操作を提供します。

- VPC VLAN の作成
- VPC VLAN およびそれらのプロパティの表示
- VPC VLAN の削除
- ユーザ VLAN の割り当て
- ユーザ VLAN の削除

使用方法とダイアログボックスから内容がわかるようになっています。必要な場合、ツールヒントを表示させるためにアイコン上にカーソルを移動することができます。

コンピューティング クラスタレベルの参照

コンピューティング クラスタはツリー階層内の 3 番目のレベルに存在します。

次の手順に従ってください:

1. [スタート] メニューから **CA Virtual Assurance** ユーザインターフェースを開きます。[管理] - [リソース] をクリックします。
エクスプローラのツリーが開きます。
2. **Huawei SingleCLOUD** フォルダを展開します。
フォルダ階層が表示されます。
3. コンピューティング クラスタを選択するか展開します。
使用可能な仮想マシンのリストが表示されます。
4. コンピューティング クラスタを右クリックして、仮想マシンを作成します。
システム ボリューム (リソース管理) 用のディスクとオペレーティング システムを含むイメージ、**VPC VLAN**、ユーザ指定 (オプション)、**ユーザ VLAN** (オプション) が必要です。
5. 仮想マシン管理操作を実行する仮想マシンを右クリックします。
適用不可の操作は利用できなくなっています。

仮想マシン管理操作の使用

ユーザが仮想マシンを右クリックするときに、ユーザ インターフェースは、仮想マシン用の管理操作を提供します。使用方法とダイアログ ボックスから内容がわかるようになっています。

- VM の削除
- VM の再起動
- VM の電源オン
- VM の電源オフ
- VM のセーフ再起動（オペレーティング システムのシャットダウン）
- VM のセーフ電源オフ（オペレーティング システムのシャットダウン）
- VM のハイバネート
- VM の始動
- VM 名の変更
- 初期パスワードの表示
- ブート順序の設定
- スナップショットのロールバック
- VM スナップショットの作成

以下の管理操作には、追加の説明が必要です。

- CPU 設定および QoS の変更
- メモリ設定および QoS の変更
- VNC ログイン
- ツールのマウント/マウント解除

CPU 設定および QoS の変更

以下の値を指定します。

CPU 数

仮想マシンに割り当てられる CPU コアの数指定します。仮想マシンに割り当てることができる CPU コアの最大数は、8 です。

例：この数値を 5 に設定した場合、5 つの CPU コアが仮想マシンに対して利用可能になります。

予約

この仮想マシンに予約される物理 CPU パフォーマンスの割合の最小値を指定します。予約はパーセント（%）で定義され、値は 0、50、または 100 % を割り当てることができます。

例：予約を 50 % に設定した場合、システムにより、各 CPU コアの CPU 時間は 50 % 以上が確保されます。

制限

この仮想マシンが割り当てることができる CPU パフォーマンスの最大のパーセンテージを指定します。

注：制限の値は、予約用にしていた値以上である必要があります。

メモリ設定および QoS の変更

以下の値を指定します。

メモリ

仮想マシンに割り当てるメモリの量を指定します。メモリは、512 MB ～ 256 GB の範囲でメガバイト（MB）で定義されます。

例：メモリを 512 MB に設定した場合、仮想マシンに割り当てることができるメモリの最大値は 512 MB になります。

予約

仮想マシンに割り当てられる物理メモリの最小の割合を指定します。予約はパーセント（%）で定義され、値は 0 ～ 100 % を割り当てることができます。

例：メモリを 2 GB に設定し、予約を 25 % に設定した場合、システムにより、仮想マシンに 512 MB 以上が確保されます。

VNC ログイン

VNC を使用して VM にアクセスできるようにするには、VNC ログインでの初期設定が必要です。VncViewer.jar をダウンロードし、それを CA Virtual Assurance マネージャ システムにインストールします。

次の手順に従ってください:

1. CA Virtual Assurance マネージャ サーバにログインし、ユーザ インターフェイスを開きます。エクスプローラ ツリーを展開し、Huawei SingleCloud VM を右クリックして、[管理] - [VNC ログイン] を選択します。

手順を示すメッセージが表示されます。

2. CA Virtual Assurance マネージャ サーバから ESC または OMM サーバに接続し、以下のディレクトリから VncViewer.jar をダウンロードします。

`/opt/omm/oms/webapps/oms/business/resourcemanage/virtualresources`

3. 再度 [VNC ログイン] をクリックします。

メッセージ ダイアログ ボックスが開きます。

4. ダイアログ ボックスのメッセージをクリックします。

[ファイルのアップロード] ダイアログ ボックスが表示されます。

5. [参照] をクリックし、ダウンロードされた VncViewer.jar ファイルに移動して、[開く] をクリックします。

[ファイルパス] がダイアログ ボックスに表示されます。

6. [OK] をクリックします。

CA Virtual Assurance は、VncViewer.jar を以下にアップロードします。

`Install_Path¥product¥tomcat¥webapps¥UI directory.`

VNC ビューアが自動的に開き、VM に接続します。

この手順を完了すると、VNC ログインが利用可能になり、お使いの環境内の任意の Huawei SingleCloud VM にリモートでアクセスできるようになります。

ツールのマウント/マウント解除

機能を最大限に利用するには、SingleCloud ツールを VM にインストールします。

次の手順に従ってください：

1. CA Virtual Assurance マネージャ サーバにログインし、ユーザ インターフェースを開きます。エクスプローラ ツリーを展開し、VM を右クリックして、[管理] - [ツールのマウント/マウント解除] を選択します。

CA Virtual Assurance のダイアログ ボックスに、現在の VM ステータスおよび SingleCloud ツールのステータスが表示されます。

2. SingleCloud ツール ステータスを変更してマウント/マウント解除するには、[OK] をクリックします。
3. SingleCLOUD ツールを VM に正常にマウントした後、PV ドライバをインストールします。VM が Linux OS 上で実行されている場合は、VM を再起動して、PV ドライバをインストールします。

リソース割り当てのベスト プラクティス

Huawei SingleCLOUD 環境で仮想マシンに適したリソース割り当て設定（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。

- 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の環境の変更を行う場合、予約によって指定した CPU またはメモリの量は変わりません。
- 仮想マシンの予約を指定するときに、すべてのリソースをコミットしないでください。予約量がシステム容量の限界に近くなると、予約の変更が著しく困難になるため、未予約の部分が適宜残るようにしてください。

ストレージ クラスタレベルの参照

ストレージ クラスタはツリー階層内の 3 番目のレベルに存在します。

次の手順に従ってください:

1. [スタート] メニューから **CA Virtual Assurance** ユーザ インターフェースを開きます。 [管理] - [リソース] をクリックします。
エクスプローラのツリーが開きます。
2. **Huawei SingleCLOUD** フォルダを展開します。
フォルダ階層が表示されます。
3. ストレージ クラスタを展開します。
使用可能な仮想ディスクのリストが表示されます。
4. ストレージ クラスタを右クリックして、仮想ディスクを作成します。
以下のダイアログ ボックスには追加の説明が必要です。

ディスクタイプ: ユーザ ディスク

1 つの仮想マシンに接続できます。

ディスクタイプ: 共有ディスク

複数の仮想マシンに接続できます。

動的な割り当て: シン プロビジョニング

指定されたディスク領域を予約しますが、その領域にデータを格納する必要が生じるまでは、ディスクの予約領域全体を完全には確保しません。シン プロビジョニングの仮想ディスクのサイズは、格納されるデータの量に応じて増加します。

シン プロビジョニングによりデータストアの超過割り当てが可能になり、予約済みであっても使用されていないディスク領域を最小化することにより、格納に使用できる領域を増加させることができます。

5. [エクスプローラ] ツリーで仮想ディスクを右クリックし、仮想ディスク管理操作を実行します。
仮想ディスクの詳細を表示するか、または仮想ディスクを削除できます。

ストレージ管理操作の使用

ユーザが仮想マシンを右クリックするときに、ユーザ インターフェースは、仮想マシン用の管理操作を提供します。使用方法とダイアログ ボックスから内容がわかるようになっています。

- 仮想ディスクの削除
- 仮想ディスクの詳細の表示
- 仮想ディスクのイベントを表示する仮想ディスクの選択

利用可能な仮想ディスクのリストを開くにはストレージ クラスタを選択します。以下の操作を使用できます。

- 仮想ディスクの接続 
- 仮想ディスクの接続解除 
- 仮想ディスクの削除 

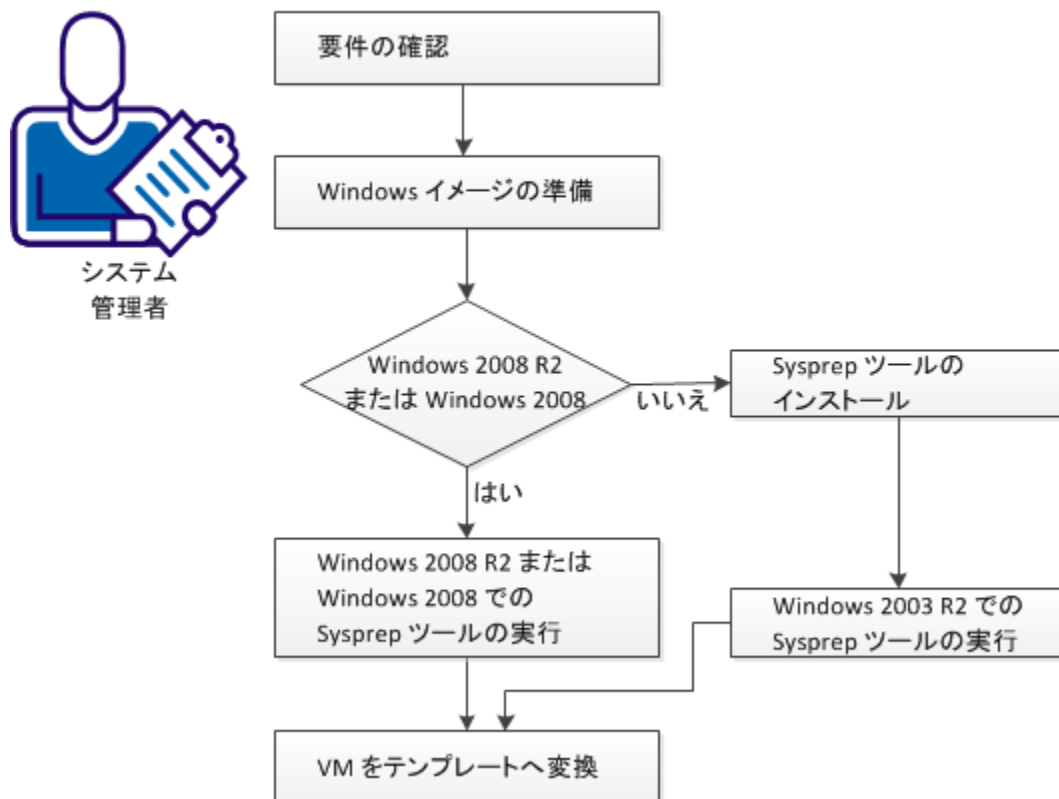
使用方法は意味がわかるようになっています。必要な場合、ツールヒントを表示させるためにアイコン上にカーソルを移動することができます。

GalaX のプロビジョニング用に Windows テンプレートを準備する方法

CA Virtual Assurance では、Windows 2003 R2 Server (32 ビット/64 ビット)、Windows 2008 (32 ビット/64 ビット) または Windows 2008 R2 Server (64 ビット) を実行する新しい仮想マシン (VM) でのプロビジョニングのカスタマイズをサポートしています。カスタマイズ オプションには多数の設定があります。たとえば、組み込みの管理者アカウントのパスワード、コンピュータ名、およびネットワーク設定を変更できます。

以下の図は、システム管理者が GalaX のプロビジョニング用に Windows テンプレートを準備する方法を示しています。

VM のプロビジョニング用にテンプレートを作成する方法



Microsoft sysprep ツールでは、設定されている Windows インストールを一般化、フリーズ、およびシャットダウンが可能です。以下のセクションでは、Windows 2003 R2 および Windows 2008 R2 用の Sysprep ツールを使用する方法の詳細について説明します。

Windows 2003 では、Sysprep ツールはデフォルトではインストールされませんが、Windows インストール CD-ROM に収録されています。

以下の手順に従います。

[要件の確認 \(P. 451\)](#)

[Windows イメージの準備 \(P. 452\)](#)

[Windows 2003 R2 での Sysprep ツールの実行 \(P. 452\)](#)

[Windows 2008 R2 での Sysprep ツールの実行 \(P. 453\)](#)

[VM を GalaX のテンプレートへ変換 \(P. 453\)](#)

[プロビジョニングされた仮想マシンの使用 \(P. 454\)](#)

要件の確認

CA Virtual Assurance での仮想マシン プロビジョニング用テンプレートを作成する前に、以下の前提条件を確認します。

- Huawei GalaX 環境に精通していること。
- CA Virtual Assurance ユーザ インターフェース、およびリソースをプロビジョニングする方法に精通していること。
- CA Virtual Assurance がインストールされており、CA Virtual Assurance ユーザ インターフェースにアクセスできること。
- Huawei GalaX 環境が利用可能で、実行されていること。
- コンピューティング クラスタのサーバ（仮想マシン用）およびストレージクラスタ（仮想ディスク用）が Huawei GalaX 環境で利用可能であること。
- ユーザ VLAN プールおよび VPC VLAN プール用のサーバが利用可能であること。
- CA Virtual Assurance が Huawei GalaX サーバとその関連リソース（クラスタ、ストレージクラスタ、仮想マシンなど）を検出していること。

Windows イメージの準備

Windows オペレーティング システムが含まれるテンプレートを作成する際には、この手順に従って、イメージを準備します。テンプレートをカスタマイズするには、**CA Virtual Assurance** のプロビジョニング操作を有効にする手順に従ってください。一部の手順は **Windows** のバージョンによって異なります。

次の手順に従ってください:

1. Windows オペレーティング システムを新しい仮想マシンにゼロからインストールします。
2. 仮想マシンに SingleCloud ツールをインストールします。
3. ユーザ アカウント、ポリシー、アプリケーション、ホット フィックスなど、新しい仮想マシンに適用したいカスタマイズを適用します。

Windows 2003 R2 での Sysprep ツールの実行

Sysprep ツールのインストールを設定した後、Sysprep ツールを実行します。

次の手順に従ってください:

1. 以下の CAB ファイルを探して開きます。
`¥SUPPORT¥TOOLS¥DEPLOY.CAB`
2. CAB ファイルに含まれるファイルをすべて選択し、`%SystemDrive%¥Sysprep` (通常は `C:¥Sysprep`) にコピーします。

注: ディレクトリ名は変更しないでください。

3. Sysprep ディレクトリに移動して、以下を実行します。

```
sysprep -quiet -reseal -mini -forceshutdown
```


Windows 2008 R2 での Sysprep ツールの実行

通常の Windows セットアップでは、Sysprep プロセスを実行するためのすべてのファイルがインストールされます。Windows インストールを設定した後、以下の手順を実行します。

1. 以下のディレクトリに移動します。

`C:\Windows\system32\sysprep`

2. 以下のコマンドを実行します。

`sysprep /generalize /shutdown`

`sysprep` コマンドはインストール用イメージを準備し、仮想マシンをシャットダウンします。`generalize` パラメータは、コンピュータ名、ログファイル、リストアポイント、およびハードウェア固有情報などの一意のシステム情報をすべて削除します。

VM を GalaX のテンプレートへ変換

`sysprep` コマンドが仮想マシンをシャットダウンした後、テンプレートを作成するために SingleCloud ユーザインターフェースに移動します。

次の手順に従ってください:

1. SingleCloud ユーザインターフェースにログインします。
2. [VM] タブをクリックし、`sysprep` で準備した仮想マシンを選択します。
3. 仮想マシンを右クリックし、[イメージのエクスポート] を選択します。

[イメージのエクスポート] ダイアログボックスが表示されます。

4. ファイル名を指定し、[イメージタイプ] を「ゴースト」に設定して [OK] をクリックします。

仮想マシンはゴーストイメージとして保存されます。

5. SingleCloud ユーザインターフェースでゴーストイメージを登録します。

ゴーストイメージをプロビジョニング用のテンプレートとして使用できるようになりました。

プロビジョニングされた仮想マシンの使用

前の[シナリオ \(P. 449\)](#)に従って作成されたテンプレートを使用すると、プロビジョニングされた仮想マシンの動作が以下のようになります。

プロビジョニングされた仮想マシンを最初に起動する際、起動プロセスは、ロケール設定、製品キー、EULAなどのユーザ入力を待機し、この特定のマシン用のホスト名の指定が可能になります。

仮想マシンにアクセスするには、VNC が利用可能であることを確認します。

IBM PowerVM (LPAR)

IBM PowerVM システムは、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 システム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 システム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 プラットフォーム管理モジュール (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

IBM PowerVM サーバ管理の概要

CA Virtual Assurance の CA IBM PowerVM コンポーネントでは、IBM PowerVM リソースをモニタおよび管理できます。モニタおよび管理されるリソースには以下のタイプがあります。

- ハードウェア管理コンソール (HMC)
- Integrated Virtualization Manager (IVM)
- 仮想 IO サーバ (VIOS)
- 管理対象システム (POWER サーバ)
- 論理パーティション (LPAR)

ハードウェア管理コンソール (HMC) は、IBM PowerVM システム上で管理タスクを実行するために使用す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 システム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。

Integrated Virtualization Manager (IVM) は仮想 I/O サーバ (VIOS) の機能拡張で、単一の POWER システムを管理できます。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。

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、その仮想化機能をほかの 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。

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 はネットワーク内で別々のシステムとして通信します。

IBM PowerVM リソースを管理するには、HMC/IVM サーバと仮想 I/O サーバに SSH アクセス認証情報を提供します。

CA Virtual Assurance の[管理]-[設定]-[プロビジョニング]-[IBM PowerVM]グループを使用して、PowerVM リソースを管理するよう CA Virtual Assurance を設定できます。

以下のパネルを使用できます。

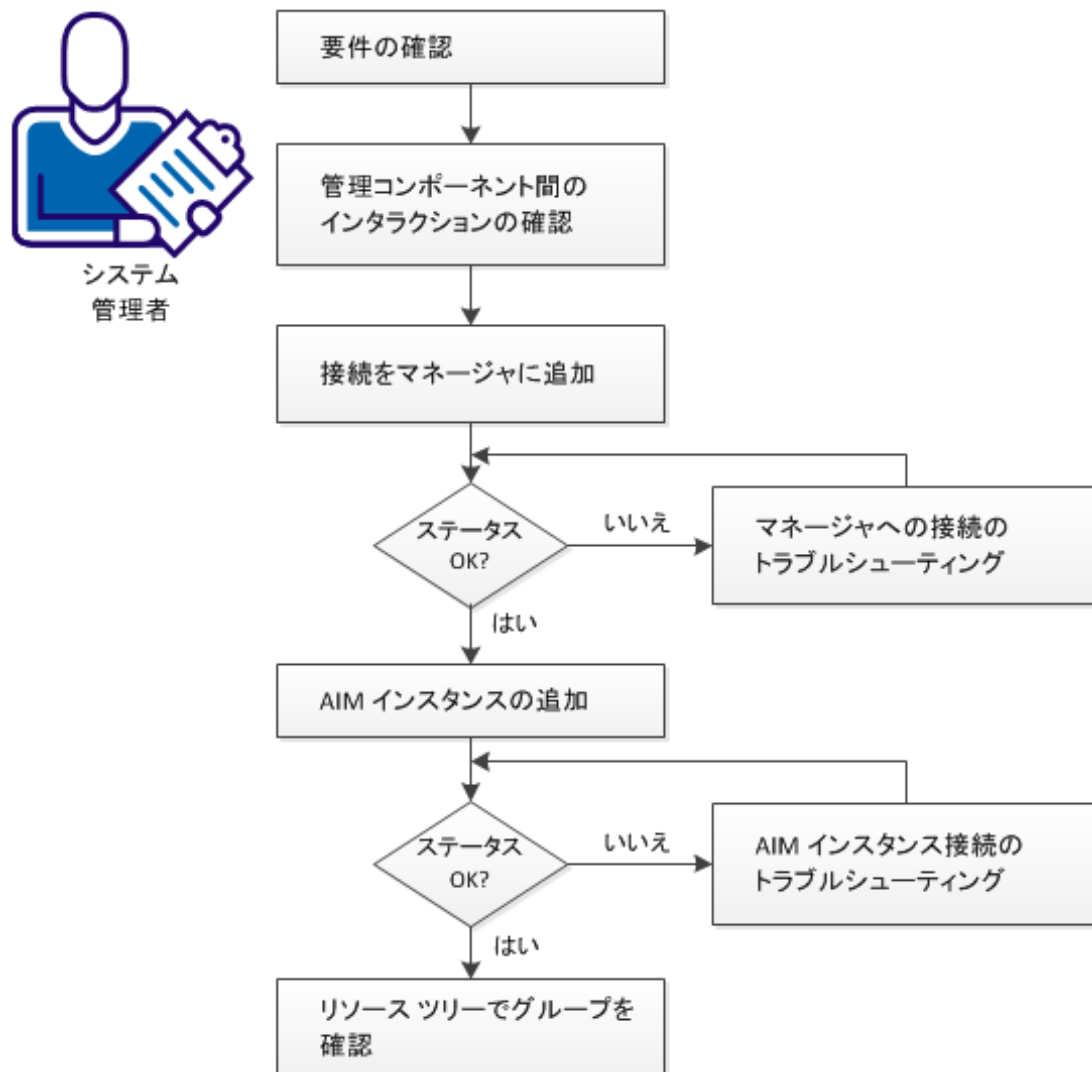
- HMC/IVM サーバ
- 仮想 I/O サーバ
- LPAR AIM サーバ

LPAR AIM サーバは、SystemEDGE および LPAR AIM が実行されるシステムです。LPAR AIM は、ローカル CA Virtual Assurance マネージャ システムまたはリモート Windows サーバ上で実行できます。LPAR AIM はマルチインスタンス AIM で、複数の HMC または IVM に接続できます。AIM が HMC または IVM サーバの管理を開始すると、この HMC または IVM サーバに接続されている P-Server が AIM によってすべて検出および管理されます。

PowerVM 管理コンポーネントを設定する方法

以下の図は、管理コンポーネントを設定するために必要なアクションの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。

管理コンポーネントの設定方法



以下の手順に従います。

[要件の確認 \(P. 459\)](#)

[AIX LPAR 管理コンポーネント間のインタラクション \(P. 461\)](#)

[HMC または IVM サーバ接続のマネージャへの追加 \(P. 465\)](#)

[サーバへのマネージャの接続が失敗する \(P. 466\)](#)

[LPAR AIM インスタンスの追加 \(P. 468\)](#)

[AIM インスタンス接続のトラブルシューティング \(P. 471\)](#)

[リソース ツリーでグループを確認する \(P. 474\)](#)

要件の確認

CA Virtual Assurance の管理コンポーネントを設定する前に、以下の要件を確認します。

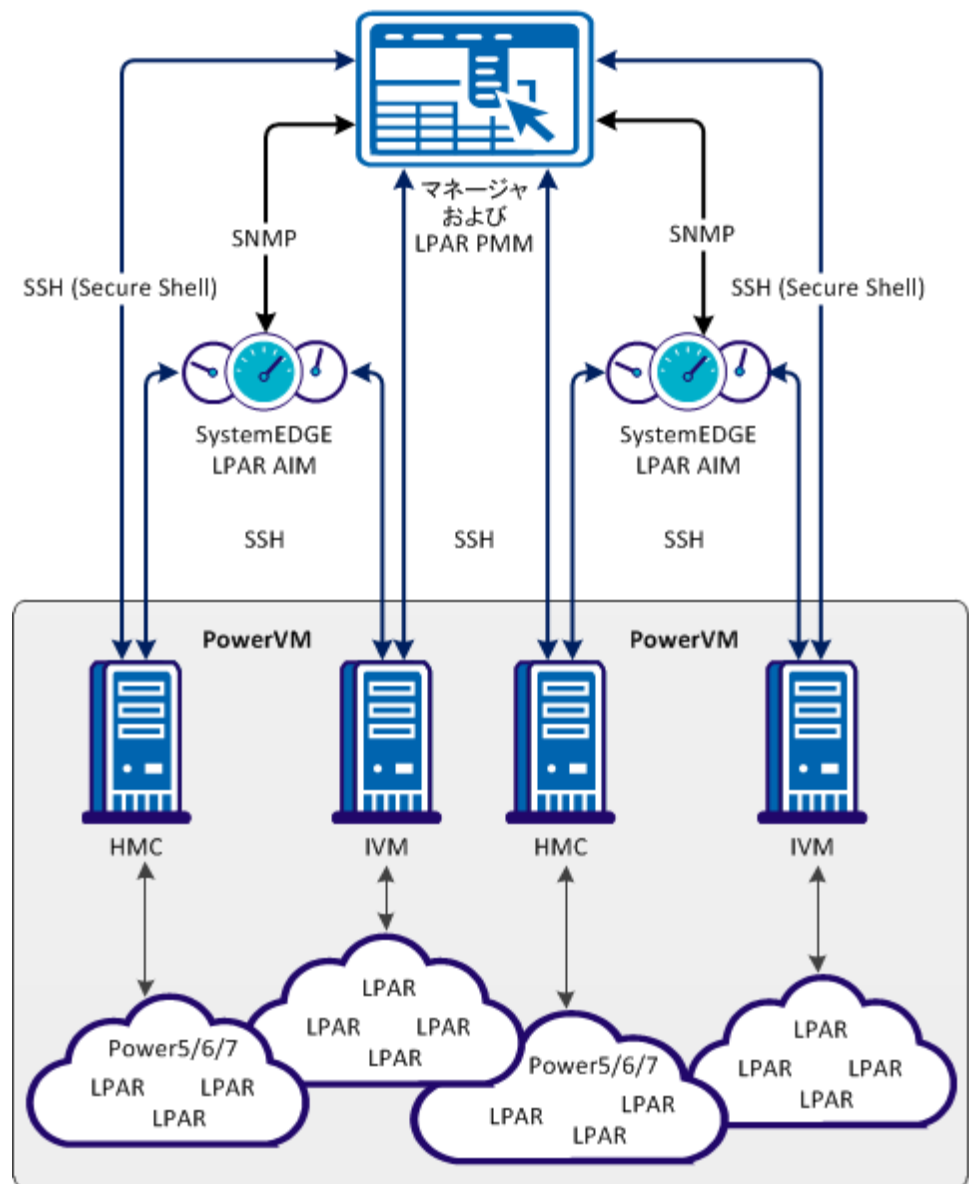
- TCP/IP、SNMP、Web サービスおよび Windows Server オペレーティングシステムに精通している。
- CA Virtual Assurance および SystemEDGE に精通している。
- 以下を含む CA Virtual Assurance マネージャ インストールにアクセスできる。
 - プラットフォーム管理モジュール (PMM)
 - Application Insight Module (AIM)
 - モニタリング エージェント (SystemEDGE)
- CA Virtual Assurance ユーザ インターフェースにアクセスできる。
- 管理対象となる環境のサーバ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 サービスを通して使用する環境のサーバ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
- 使用する環境にあるサーバが正常に実行されていることを確認済みである。

- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM 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。
- 使用するリモート 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。

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 管理コンポーネント間のインタラクション



インストールの後、必要な HMC/IVM および仮想 I/O サーバに接続情報を追加して、環境を設定します。以下のいずれかの方法を使用します。

- ユーザインターフェースの [管理] タブ
- 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。

IBM PowerVM 設定の使用例

以下の使用例では、[管理] タブにおける管理対象の PowerVM 環境の LPAR AIM インスタンス エントリの扱いについて説明します。

- HMC サーバおよび LPAR AIM インスタンスを追加します。

AIM は以下を検出します。

- HMC と関連付けられている Power システム。
- Power システムと関連付けられている仮想 I/O サーバ。HMC を追加するときに指定したデフォルトの VIOS 認証情報が適用されている AIM。

重要: HMC サーバ用のデフォルトの VIOS 認証情報を指定しない場合は、[仮想 I/O サーバ] パネルで各 VIOS の VIOS 認証情報を指定して、検出された VIOS を設定します。デフォルトの VIOS 認証情報が特定の VIOS に適用されない場合は、[仮想 I/O サーバ] パネルの認証情報を上書きできます。

- 優先 AIM

2 つの AIM で 1 つの HMC を管理できます。2 番目の AIM が追加されると、これは冗長 AIM になります、最初に追加された AIM は優先 AIM になります。冗長 AIM の下の HMC のステータスは中断になります。このステータスは、HMC が優先 AIM によって管理されていることを反映しています。優先 AIM は [HMC/IVM サーバ] パネルで変更できます。

- デュアル HMC 機能は、1 台の Power システムを 2 台の HMC サーバと関連付ける設定をサポートしています。

P-Server および関連付けられた HMC サーバは、1 まとまりの管理エンティティで、1 つの AIM によって管理する必要があります。デュアル HMC の設定では、1 つの AIM のスコープでのみサポートされています。たとえば、ある Power システム (P1) を、2 台の HMC サーバ (HMC1 および HMC2) に接続します。両方の HMC サーバは 1 つの AIM (AIM1) によって管理されます。

- デュアル HMC によるフェールオーバー

優先 HMC に障害が発生した場合、冗長 HMC がシステムの管理を自動的に開始します。冗長 HMC が現在の HMC になります。ただし、優先 HMC が利用可能になっても、現在の HMC は変更されません。優先 HMC によって再度システムを管理するには、[管理] - [設定] タブにある [LPAR AIM サーバ] パネルで現在の HMC を変更します。

注: 優先 HMC に障害が発生すると、冗長 HMC によってシステムが管理されます。フェールオーバー後、システムに対する現在の HMC は手動で変更できます。

- デフォルトの VIOS 認証情報に正しくない仮想 I/O サーバ認証情報は指定できません。

ユーザ インターフェイスに、操作の失敗を示すメッセージが表示されます。正しくない仮想 I/O サーバ認証情報を適用しようとすると (🔒)、仮想 I/O サーバの状態は「認証失敗」に変わります。接続の問題により、管理対象システム インスタンスの状態は「VIOS 待ち」から「期限切れ」に変わります。

- 仮想 I/O サーバなしで管理対象システム インスタンスを追加します。

管理対象システム インスタンスが「準備完了」の状態ではインスタンステーブルに表示されません。

- P-server を管理対象システムに追加します。

新しい P-server および VIOS は自動的に検出されます。VIOS 認証情報がデフォルトの VIOS 認証情報と同じである場合、設定は必要ありません。VIOS 認証情報がデフォルト VIOS 認証情報と同一でない場合は、AIM インスタンスに VIOS 認証情報を設定します (🔒)。

- 「設定が無効」状態の仮想 I/O サーバを管理対象システムから削除します。

LPAR AIM は、対応するレコードをインスタンス テーブルから削除し、管理対象システムの状態は「準備完了」に変わります。

- 「準備完了」状態の仮想 I/O サーバを管理対象システムから削除します。

LPAR AIM は、対応するレコードをインスタンス テーブルから削除します。

- 1 つまたは 2 つの仮想 I/O サーバを含む管理対象システム インスタンスを削除します。

管理対象システム インスタンスおよび関連付けられた仮想 I/O サーバのエントリが、インスタンス テーブルに表示されなくなります。

- IBM PowerVM 管理ペインでは、ステータス情報がアイコンとツールヒントによって表示されます。

詳細なツールヒントは、警告およびエラーのアイコンの上にカーソルを置くと表示されます。

以下のアイコンが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

HMC または IVM サーバ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、HMC または IVM サーバ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 [IBM PowerVM] 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 HMC サーバ、IVM サーバ、関連付けられている仮想 I/O サーバ、および LPAR AIM サーバが表示されます。

3. [HMC/IVM 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 HMC/IVM サーバ] 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) を入力し、優先 AIM を指定して、[管理ステータス] (チェック ボックス) をオンにします。

注: 指定された HMC または IVM サーバに対して複数の AIM インスタンスを指定した場合にのみ、優先 AIM フィールドがアクティブになります。

5. (オプション) 仮想 I/O サーバのデフォルト認証情報を指定します。

仮想 I/O サーバのデフォルト認証情報は、新しく検出された仮想 I/O サーバに適用されます。

重要: HMC サーバ用のデフォルトの VIOS 認証情報を指定しない場合は、[仮想 I/O サーバ] パネルで各 VIOS の VIOS 認証情報を指定して、検出された VIOS を設定します。デフォルトの VIOS 認証情報が特定の VIOS に適用されない場合は、[仮想 I/O サーバ] パネルの認証情報を上書きできます。

6. [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 [HMC/IVM サーバ] ペインにサーバが緑のステータス アイコンを使って追加されます。CA Virtual Assurance によって HMC/IVM サーバ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 によってサーバがリストに追加され、接続の失敗を示す赤のステータス アイコンが表示されます。[いいえ] をクリックすると、何も追加されません。

サーバへのマネージャの接続が失敗する

症状:

[管理] - [設定] でサーバ接続を追加した後に、サーバ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。

- サーバへの接続に使用したデータが現在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。
- サーバ 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。
- 接続に必要なすべてのサービスが、サーバ システム上で正しく実行されているかどうかを確認します。

サーバ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。
2. 接続の詳細を追加し、[管理ステータス] を有効にし、[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。

サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ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 <Server Name>
ping <IP Address of Server>
```

2. サーバに有効な DNS エントリおよび IP アドレスが設定されているかどうかを調べるには、これらのコマンドの出力を確認します。

サーバが DNS で見つからない場合は、CA Virtual Assurance マネージャ システム上にある Windows の hosts ファイルにサーバを追加します。手順 3 に進みます。

サーバが DNS で見つかった場合は、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 <Server Name>
```

正しい IP アドレスとサーバ名を入力してファイルを保存します。例：

```
192.168.50.50 myServer
```

4. CA Virtual Assurance ユーザ インターフェイスで、[管理] タブの [設定] に移動して、[サーバ] ペインの右上角にある  (検証) をクリックします。

サーバの認証情報と接続データが正しく、サーバに対して ping を実行できる場合でも、接続に失敗することがあります。このような場合は、サーバに問題がある可能性があります。サーバへの接続を確立できない場合は、次の手順に進みます。

接続に必要なすべてのサービスが、サーバシステム上で正しく実行されているかどうかを確認する方法

1. サーバにアクセスするために、システム管理者に問い合わせます。
2. サーバシステムにログインします。
3. 接続に必要なすべてのサービスが正しく実行されているかどうかを確認します。
4. 必要に応じて、サービスを開始または再起動します。
5. **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 [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 によってサーバ接続が検証されます。

サーバ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収集したデータが正しいことを確認してください。

管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

LPAR AIM インスタンスの追加

CA Virtual Assurance マネージャに **HMC** または **IVM** サーバ接続を追加した後、新しいサーバを管理するための **AIM** インスタンスを追加します。その後、**CA Virtual Assurance** によって **PowerVM** 環境が検出されます。

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 [IBM PowerVM] 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 **HMC** サーバ、**IVM** サーバ、関連付けられている仮想 I/O サーバ、および **LPAR AIM** サーバが表示されます。

3. [LPAR 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 LPAR AIM サーバ] ダイアログ ボックスが表示されます。

4. ドロップダウン リストから [LPAR AIM サーバ] を選択します。

検出された LPAR AIM サーバのリストが表示されます。LPAR 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 [HMC または IVM サーバ] を選択します。

[HMC/IVM サーバ] ペインに一覧表示された HMC または IVM サーバが [HMC/IVM サーバ] ドロップダウン リストに入力されます。管理できる HMC または IVM サーバは、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。

注: AIM がリモート システムに存在している場合、CA Virtual Assurance でこのシステムを最初に検出する必要があります。検出後、AIM サーバがドロップダウン リストに表示されます。

6. [OK] をクリックします。

選択したサーバの新しい 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 PowerVM 環境の検出を開始します。

- 各 HMC サーバについては、AIM はすべての Power システムと仮想 I/O サーバを検出します。
- 各 IVM サーバについては、AIM は IVM が管理する Power システムを検出します。

ディスカバリ プロセスが完了したら、PowerVM 環境の管理を開始できます。

[管理] タブには、AIM が検出したすべての Power システムと VIO サーバの集計された状態が表示されます。これらの個別の設定状態を表示するには、[管理対象システムを表示] () アイコンをクリックします。

管理対象 Power システムの優先 HMC の変更

Power システムでデュアル HMC を使用する場合は、優先 HMC を変更できます。

重要: 1 つの LPAR AIM でプライマリと冗長用の HMC サーバの両方を管理していることを確認します。

次の手順に従ってください:

1. [スタート] メニューから 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 [IBM PowerVM] 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 HMC サーバ、IVM サーバ、関連付けられている仮想 I/O サーバ、および LPAR AIM サーバが表示されます。

3. HMC サーバと関連付けられている  (管理対象/VIO サーバを設定) をクリックします。

[IBM PowerVM] ダイアログ ボックスに管理対象/VIO サーバが表示されます。

4. [アクション] 行の下にある  (優先 HMC を切り替えます) をクリックして確認します。

冗長 HMC が優先 HMC として設定されます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

[管理] - [設定] でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  (ディスカバリが進行中) が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。ディスカバリにかかる時間は、環境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数によって異なります。アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Virtual Assurance はサーバフォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

〔管理〕 - 〔設定〕 で AIM インスタンスを追加した後、ステータス アイコンに  (ポーリングなし) が表示されます。

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。このアイコンは、CA Virtual Assurance マネージャがこの AIM をポーリングしないこと表します。この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。別の AIM を使用したい場合は、〔管理〕 - 〔設定〕 - 〔プロビジョニング〕 で優先 AIM を設定できます。サーバエントリの〔編集〕をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

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 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:

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。

- 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。

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. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

AIM サーバが 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 AIM サーバを追加します。手順 3 に進みます。

サーバが 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 AIM サーバの名前を入力します。例：

```
192.168.50.51 myAIM
```

4. [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. 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 [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 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、収集したデータがこのシナリオの要件に従っていることを確認してください。

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 AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン  (無効) が表示されます。この 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 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サーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

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。

- 欠落しているサーバから CA Virtual Assurance マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、その管理ステータスを「有効」に変更します。

リソース ツリーでグループを確認する

設定および検出に成功すると、新たに検出されたリソースが [リソース] - [エクスプローラ] ペインの対応するグループに表示されます。

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] ペインを開きます。
2. IBM PowerVM グループを展開します。
管理対象の HMC および IVM サーバが表示されます。
3. [HMC または IVM サーバ] エントリを展開します。
管理対象システムが表示されます。

CA Virtual Assurance で、追加された PowerVM 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。

calpara.xml ファイル

calpara.xml ファイルの主な目的は、永続データやデフォルト値などの LPAR AIM の設定データを格納することです。モニタリングの設定は、特定の環境に合わせて調整できます。

このドキュメントは、XML 形式に精通しているシステム管理者を対象としています。このファイルを変更するときには、十分に注意してください。calpara.xml ファイルを変更するには、SystemEDGE を終了し、ファイルを変更した後に SystemEDGE を再起動します。

重要: モニタリングのしきい値、遅延、または重大度の調整が必要な場合は、デフォルト値のみを変更します。ポーリンググループと DisableOutOfDate の設定は、CA サポートから指示された場合にのみ変更してください。

calpara.xml ファイルは以下の場所にあります。

```
<SystemEDGE_InstallDir>%plugins%calpara%calpara.xml
```

永続データ

永続データは AIM が次に開始するときに利用できます。このデータは AIM の存続期間中に変更でき、SNMP の SET 要求を使用してユーザが設定することができます。

以下に永続データの例を示します。

- インスタンス
- システム
- パーティション
- スロット
- ポーリンググループ

インスタンス

インスタンス テーブル (IparAimInstanceTable) に設定されている各インスタンスについては、以下の例のようなセクションが格納されます。

```
<ManagedInstance>
  <InstIndex>7</InstIndex>
  <SerialNr>1010101</SerialNr>
  <ServerName>vios1.company.com</ServerName>
  <ServerType>vios</ServerType>
  <RowStatus>1</RowStatus>
</ManagedInstance>
```

ServerType

サーバタイプとして、hmc、vios、または ivm のいずれかを指定します。

RowStatus

ステータスを active (1) または notInService (2) として指定します。

システム

システム テーブル (IparAimStatSysTable) に設定されている管理対象の Power システムについては、以下の例のようなセクションが関連する ManagedInstance セクション内に格納されます。

```
<System>
  <MonitorIndices>530091,530092,530093,530094,530095</MonitorIndices>
</System>
```

MonitorIndices

Power システムの動作ステータス、CPU、およびメモリの使用状況をモニタするために AIM が作成した SystemEDGE モニタのインデックスを格納します。

注: 今後 AIM で Power システムを管理しない場合は、対応するモニタが削除されます。

パーティション

パーティションテーブル (lparAimStatLPTable) 内の管理対象の各論理パーティションについては、以下の例のような 4 つの対応するエントリが関連する ManagedInstance セクション内の Partitions セクションに格納されます。

```
<Partitions>
...
  <LparIndex>7</LparIndex>
  <LparId>7</LparId>
  <LparName>LPAR12345</LparName>
  <MonitorIndices>530141,530142,530143,530144,530145</MonitorIndices>
...
</Partitions>
```

注: 今後 AIM で Power システムを管理しない場合は、対応するモニタが削除されます。

スロット

スロットテーブル (lparAimStatSlotTable) 内の各物理スロットについては、以下の例のような 4 つの対応するエントリが関連する ManagedInstance セクション内の Slots セクションに格納されます。

```
<Slots>
...
  <SlotIndex>3</SlotIndex>
  <DRCName>U787B.001.DNFFF77-P1-C3</DRCName>
  <DRCIndex>553713666</DRCIndex>
  <SlotName>C3</SlotName>
...
</Slots>
```

LPAR AIM では、このデータを使用して、スロットに関係する変更を起動直後に検出します。これによって対応する SNMP トラップが送信される可能性があります。

ポーリング グループ

ポーリング グループは、関連する一連のコマンドであり、すべて同じポーリング間隔で実行されます。ポーリング テーブル (IparAimPollTable) 内の各ポーリング グループについては、それぞれのポーリング グループセクションに対応する 3 つのエントリが格納されます。以下の例は、基本ポーリング グループを示しています。

```
<Basic>
  <PollDefault>5</PollDefault>
  <PollSpecific>30,30</PollSpecific>
  <PollInstances>4,6</PollInstances>
</Basic>
```

PollDefault

デフォルト ポーリング間隔 (分単位) を格納し、すべてのインスタンスに適用します。ただし、**PollInstances** に一覧表示されるインスタンス (インスタンスのインデックスのリスト) は除きます。

PollSpecific

PollInstances に格納されたインスタンスのリストに 1 対 1 で対応させて適用するポーリング間隔 (分単位) のリストを格納します。

注: PollSpecific と PollInstances は最初は空です。

デフォルト値

以下のセクションでは、calpara.xml ファイルに格納される遅延、しきい値、重大度を指定するデフォルト値について説明します。これらは、AIM によって SystemEDGE モニタを作成するときに使用されます。

重要: デフォルト値は AIM の存続期間中に変更できず、ユーザが設定することもできません。

```
<LowestPollInterval>5</LowestPollInterval>
<DisableOutOfDate>0</DisableOutOfDate>
<MonitorIndexStart>530001</MonitorIndexStart>
<SysAliveSev>fatal</SysAliveSev>
<CpuLagValue>3</CpuLagValue>
<CpuThresh1Val>95</CpuThresh1Val>
<CpuThresh1Sev>warning</CpuThresh1Sev>
<CpuThresh2Val>98</CpuThresh2Val>
<CpuThresh2Sev>critical</CpuThresh2Sev>
<MemLagValue>2</MemLagValue>
```

```

<MemThresh1Val>95</MemThresh1Val>
<MemThresh1Sev>warning</MemThresh1Sev>
<MemThresh2Val>98</MemThresh2Val>
<MemThresh2Sev>critical</MemThresh2Sev>

```

LowestPollInterval

許可されている最短のポーリング間隔（分単位）を格納します。

DisableOutOfDate

データ ステータス（lparAimInstDataStatus） outOfDate を除外するかどうかを指定します。

注: コマンド実行が失敗した場合に、outOfDate(7) になったデータ ステータスを無効にするには、この変数を 1 に設定します。

デフォルト: 0

MonitorIndexStart

AIM がスタートアップ後に作成する最初の SystemEDGE モニタのインデックスを指定します。

注: 新しいモニタを作成する場合、AIM は常に、等しいかより大きい、次に空いているインデックスを検索します。

SysAliveSev

Power システムまたは論理パーティションの動作ステータスをモニタするために AIM が作成する SystemEDGE モニタの重大度を指定します。

有効な値: ok、warning、minor、major、critical、fatal。

注: この値を変更しても、既存のモニタに影響はありません。

CpuThresh1Val と CpuThresh2Val

Power システムまたは論理パーティションの CPU 使用率をモニタするために AIM が作成する 2 つの SystemEDGE モニタのしきい値を指定します。

値の範囲: 0 ～ 100。

注: この値を変更しても、既存のモニタに影響はありません。

CpuThresh1Sev と CpuThresh2Sev

Power システムまたは論理パーティションの CPU 使用率をモニタするために AIM が作成する 2 つの SystemEDGE モニタの重大度を指定します。

有効な値： ok、warning、minor、major、critical、fatal。

注： この値を変更しても、既存のモニタに影響はありません。

MemThresh1Val と MemThresh2Val

Power システムまたは論理パーティションのメモリ使用率をモニタするために AIM が作成する 2 つの SystemEDGE モニタのしきい値を指定します。

値の範囲： 0 ～ 100。

注： この値を変更しても、既存のモニタに影響はありません。

MemThresh1Sev と MemThresh2Sev

Power システムまたは論理パーティションのメモリ使用率をモニタするために AIM が作成する 2 つの SystemEDGE モニタの重大度を指定します。

有効な値： ok、warning、minor、major、critical、fatal。

注： この値を変更しても、既存のモニタに影響はありません。

CpuLagValue と MemLagValue

Power システムまたは論理パーティションの CPU とメモリ使用率をモニタするために AIM が作成する SystemEDGE モニタの遅延値を指定します。遅延値には、モニタがその数に到達するとステータスが変わる連続するポーリング間隔（基本ポーリンググループ）の数を指定します。

注： この値を変更しても、既存のモニタに影響はありません。

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://System:Serial Number/Total	Alive	critical	ok
530002	lparAimStatSys CPUUsage PerMil.1	CPU	lpar://System:Serial Number/Total	PercentUsed	warning	ok
530003	lparAimStatSys CPUUsage PerMil.1	CPU	lpar://System:Serial Number/Total	PercentUsed	minor	ok

mon Index	monOID	mon ObjClass	monObjInstance	mon ObjAttribute	mon Severity	mon CurrState
530004	IparAimStatSys MemoryUsage PerMil.1	Memory	Ipar://System:Serial Number/Total	PercentUsed	warning	warning
530005	IparAimStatSys MemoryUsage PerMil.1	Memory	Ipar://System:Serial Number/Total	PercentUsed	minor	minor
530006	IparAimStatLP Status.1.1	System	Ipar://System:Serial Number/Ipar01/Tota l	Alive	critical	critical
530007	IparAimStatLPCPU Usage.1.1	CPU	Ipar://System:Serial Number/Ipar01/Tota l	PercentUsed	warning	ok
530008	IparAimStatLPCPU Usage.1.1	CPU	Ipar://System:Serial Number/Ipar01/Tota l	PercentUsed	minor	ok
530009	IparAimStatLP MemoryUsage.1.1	Memory	Ipar://System:Serial Number/Ipar01/Tota l	PercentUsed	warning	ok
530010	IparAimStatLP MemoryUsage.1.1	Memory	Ipar://System:Serial Number/Ipar01/Tota l	PercentUsed	minor	ok
530011	IparAimStatLP Status.1.2	System	Ipar://System:Serial Number/Ipar02/Tota l	Alive	critical	critical
530012	IparAimStatLPCPU Usage.1.2	CPU	Ipar://System:Serial Number/Ipar02/Tota l	PercentUsed	warning	ok
530013	IparAimStatLPCPU Usage.1.2	CPU	Ipar://System:Serial Number/Ipar02/Tota l	PercentUsed	minor	ok
530014	IparAimStatLP Memory Usage.1.2	Memory	Ipar://System:Serial Number/Ipar02/Tota l	PercentUsed	warning	ok

IBM PowerVM の管理

このセクションでは、[リソース] ページから実行できる IBM PowerVM の管理操作について説明します。

[リソース] ページでは、イベントを表示し LPAR に対して管理操作を実行できます。[エクスプローラ] ペインで [IBM PowerVM] グループを展開すると、以下のオブジェクトが一覧表示されます。

- HMC/IVM サーバ
- PowerVM システム
- 論理パーティション (LPAR)

リソース サマリおよびイベントの表示

CA Virtual Assurance では、右側のペインに [サマリ] が表示されます。[サマリ] ページには、オブジェクト階層の以下のレベルのリソース プロパティが表示されます。

- PowerVM Server
- LPAR

[パフォーマンス チャート] ペインには、利用可能なメトリックおよびオプションで使用率が表示されます。パフォーマンス チャートを適切に表示するには、フィルタ設定を使用します。

- CPU
- メモリ
- その他のメトリック

[一般情報] ペインには、以下のプロパティが含まれます。

- 名前、アイテム タイプ、タイプ (pSeries)
- CPU とメモリの数量特性
- LPAR および利用可能な処理装置の数
- シリアル番号

[概要] ペインには、以下の情報が表示されます。

- CPU 状態
- メモリ状態
- 稼働状態
- ヘルス状態
- プロパゲートされたヘルス状態
- 収集エンジンの状態

[サマリ] タブでは、オブジェクトに関連付けられた情報（メモリ合計、オペレーティング システム、CPU の数、IP アドレス、CPU とメモリの全体的な使用率、リソースに関連付けられたイベントなど）を表示できます。しきい値制限を設定するには、[使用方法] パネルの [設定] タブをクリックします。

論理パーティションの電源ステータスの制御

論理パーティションのステータスを制御するには、以下のいずれかの操作を行います。

- アクティブ化
- 再起動
- シャットダウン
- 削除

これらの操作はいずれも、1 つ以上の論理パーティションに対して同時に実行できます。

次の手順に従ってください:

1. [エクスプローラ] ペインでステータス処理を実行する管理対象マシンを選択します。
2. パーティションを右クリックし、[管理] を選択します。[クイックスタート] をクリックし、電源制御の関連するリンクをクリックする方法もあります。以下のいずれかを選択します。

アクティブ化

現在電源オフまたは中断になっている、選択された論理パーティションをアクティブ化します。

再起動

ゲスト オペレーティング システムをシャットダウンし、再起動します。

シャットダウン

選択された論理パーティションをシャットダウンします。現在電源がオンになっている論理パーティションのみ、シャットダウンすることができます。

削除

選択された論理パーティションを完全に削除します。論理パーティションは、シャットダウンされている場合のみ削除できます。

確認ダイアログ ボックスが開きます。

3. [OK] をクリックします。

ステータス操作が実行され、確認のメッセージが表示されます。インターフェースをリフレッシュすると、新しい論理パーティションステータスが表示されます。操作の結果を確認するイベントが表示されます。

論理パーティションのアクティブ化

論理パーティションをアクティブ化して、パーティションにリソースをコミットし、インストールされたオペレーティングシステムを開始することができます。パーティションをアクティブ化できるのは、パーティションが実行されていないときのみです。

論理パーティションをアクティブ化する方法

1. [エクスプローラ] ペイン上でパーティションを右クリックし、[管理] - [アクティブ化] を選択します。

[論理パーティションのアクティブ化] ダイアログ ボックスが表示されます。

2. 以下のフィールドに入力し、[OK] をクリックします。

プロファイル

パーティションのアクティブ化に使用するパーティション プロファイルを指定します。

キー ロック

キー ロック位置を指定します。キー ロックは、システムに許可される電源オン モードと電源オフ モードを設定します。CA Virtual Assurance は、以下の有効なキーロック モードをサポートします。

上書きしない

LPAR は、選択されたプロファイル内に指定されたキーロック モードを使用します。

通常

LPAR が通常の設定で起動されます。日常的なタスクの実行には、ほぼ例外なく、このオプションを使用します。

手動

キー ロック位置を [手動] に設定する場合は、セキュリティへの影響を考慮してください。

起動モード

起動モードを指定します。選択されたプロファイル内に指定されたものとは異なる起動モードを使用する場合のみ、起動モードを選択し、[アクティブ化] チェック ボックスをオンにします。パーティションプロファイルをアクティブ化するときに、他の方法を指定しない限り、システムは、この起動モードを使用して、論理パーティション上でオペレーティングシステムを開始します。CA Virtual Assurance は、以下の有効な起動モードをサポートします。

上書きしない

LPAR は、選択されたプロファイル内に指定された起動モードを使用します。

通常

LPAR が通常の設定で起動されます。日常的なタスクの実行には、ほぼ例外なく、このオプションを使用します。

ファームウェアを開く

LPAR が起動されると、ファームウェア プロンプトが開かれます。このオプションは、デバッグ情報を追加で取得するために、サービスマンが使用します。

- パーティションの [イベント] タブをクリックします。
操作の結果を確認するイベントが表示されます。

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

- [リソース] をクリックします。
- [エクスプローラ] ペインで [IBM PowerVM] グループを右クリックし、[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. プロセッサユニットの一部または専用のプロセッサ、および最小、希望、最大のプロセッサユニットを割り当てるかどうかを指定します。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。

[仮想ディスク] 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 バックリング デバイスを追加するには、[SCSI デバイス] テーブル上の [+]（新規バックリング 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。

注: NPIV をサポートする物理ファイバチャネル ポートを選択すると、パーティションに対して仮想ファイバチャネル サーバアダプタと仮想ファイバチャネル クライアント アダプタが作成されます。

13. [次へ] をクリックします。

[サマリ] ページが表示されます。

14. 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。

論理パーティションの削除

不要になったパーティションを管理対象システムから削除できます。論理パーティションを削除すると、すべてのハードウェアリソースはプライマリパーティションに返されます。電源がオフのパーティションのみを削除できます。

論理パーティションをアクティブ化する方法

1. [エクスプローラ] ペインでパーティションを右クリックし、[管理] - [削除] を選択します。

確認ダイアログボックスが開きます。

2. [OK] をクリックします。

要求がサブミットされたことを確認するメッセージが表示されます。

3. パーティションの [サマリ] タブをクリックします。

操作の結果を確認するイベントが表示されます。パーティションの電源がオフになっていないと、削除は失敗します。削除が成功した場合、インターフェースをリフレッシュすると、パーティションは [エクスプローラ] ペインに表示されなくなります。

論理パーティションの再起動

すでに実行されているパーティションを再起動できます。パーティションを再起動すると、パーティションはシャットダウンされ、オペレーティングシステムが再度開始されます。

注: 論理パーティションを再起動するには、論理パーティションが [実行中] または [ファームウェアを開く] 状態である必要があります。

論理パーティションを再起動する方法

1. [エクスプローラ] ペイン上でパーティションを右クリックし、[管理] - [再起動] を選択します。
[論理パーティションの再起動] ダイアログ ボックスが表示されます。
2. [タイプ] ドロップダウン リストを使用して、以下のいずれかの再起動タイプを選択し、[OK] をクリックします。

即時

論理パーティションをすぐにシャットダウンします。HMC/IVM はすべてのアクティブなジョブを即座に終了します。アクティブなジョブ内で実行されていたプログラムでは、ジョブクリーンアップを実行できません。データが部分的に更新されていた場合、このオプションは望ましくない結果を引き起こすことがあります。このオプションは、制御されたシャットダウンが成功しなかった場合のみ使用してください。

OS のシャットダウン

論理パーティションに対してシャットダウン コマンドを発行することにより、論理パーティションを通常どおりシャットダウンします。この操作中に、論理パーティションは、必要なすべてのシャットダウン アクティビティを実行します。このオプションは AIX 論理パーティションにのみ使用できます。

OS のシャットダウン即時

論理パーティションに対してシャットダウン -F コマンドを発行することにより、論理パーティションを即座にシャットダウンします。この操作中に、論理パーティションは、メッセージを他のユーザおよびシャットダウン アクティビティにバイパスします。このオプションは AIX 論理パーティションにのみ使用できます。

3. パーティションの [サマリ] タブをクリックします。
操作の結果を確認するイベントが表示されます。

論理パーティションのシャットダウン

パーティションをシャットダウンすると、オペレーティング システムがシャットダウンされます。パーティションをシャットダウンするには、パーティションが [実行中] または [ファームウェアを開く] 状態である必要があります。

論理パーティションをシャットダウンする方法

1. [エクスプローラ] ペイン上でパーティションを右クリックし、[管理] - [シャットダウン] を選択します。
[論理パーティションのシャットダウン] ページが表示されます。
2. [タイプ] ドロップダウン リストを使用して、以下のいずれかのシャットダウン タイプを選択し、[OK] をクリックします。

即時

論理パーティションをすぐにシャットダウンします。HMC/IVM はすべてのアクティブなジョブを即座に終了します。アクティブなジョブ内で実行されていたプログラムでは、ジョブ クリーンアップを実行できません。データが部分的に更新されていた場合、このオプションは望ましくない結果を引き起こすことがあります。このオプションは、制御されたシャットダウンが成功しなかった場合のみ使用してください。

OS のシャットダウン

論理パーティションに対してシャットダウン コマンドを発行することにより、論理パーティションを通常どおりシャットダウンします。この操作中に、論理パーティションは、必要なすべてのシャットダウン アクティビティを実行します。このオプションは AIX 論理パーティションにのみ使用できます。

OS のシャットダウン即時

論理パーティションに対してシャットダウン -F コマンドを発行することにより、論理パーティションを即座にシャットダウンします。この操作中に、論理パーティションは、メッセージを他のユーザおよびシャットダウン アクティビティにバイパスします。このオプションは AIX 論理パーティションにのみ使用できます。

3. パーティションの [サマリ] タブをクリックします。

操作の結果を確認するイベントが表示されます。

CPU とメモリの設定

仮想マシンに割り当てるメモリ共有を設定して、その割り当てリソースを調整することができます。この操作が成功するためには、リソースを追加するときに、適切な量の未割り当てのメモリ共有または CPU 共有が利用可能である必要があります。メモリ共有または CPU 共有で許可される最小または最大の値が存在する場合、リソース割り当てを変更するときは常にこの制限内にとどめる必要があります。[リソース] タブの [クイック スタート] リンクを使用すると、VM の CPU とメモリの割り当てを編集できます。特定の VM リソース割り当てアクションでは、作成およびスケジュールポリシーを使用することもできます。

重要: CPU およびメモリの追加または削除などの動的 LPAR 操作の場合は、各 LPAR システムに AIX バージョン 5.2、5.3、または 6.0 以上をインストールします。あるいは、LPAR システム上で AIX リソース制御デーモン IBM.DRM を実行します。

CPU の設定

VM の CPU 割り当てを設定する方法

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. [エクスプローラ] ペインで仮想マシンを探して右クリックし、[設定] - [プロセッサの設定...] を選択します。
[プロセッサ リソース割り当ての設定] ダイアログ ボックスが表示されます。
3. 以下の調整タイプの中から 1 つ選択します。

動的調整

実行中の VM を更新します。

プロファイルの更新

アクティブなプロファイルを更新します。プロファイルの変更を反映するには、VM を再起動する必要があります。

動的調整およびプロファイル更新

実行中の VM とアクティブなプロファイルの両方を更新します。

4. 対応するフィールドを編集し、[OK] をクリックします。
確認メッセージが表示されます。

メモリの設定

VM のメモリ割り当てを設定する方法

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. [エクスプローラ] ペインで仮想マシンを探して右クリックし、[設定] - [メモリの設定...] を選択します。
[メモリ リソース割り当ての設定] ダイアログ ボックスが表示されます。
3. 以下の調整タイプの中から 1 つ選択します。

動的調整

実行中の VM を更新します。

プロファイルの更新

アクティブなプロファイルを更新します。プロファイルの変更を反映するには、VM を再起動する必要があります。

動的調整およびプロファイル更新

実行中の VM とアクティブなプロファイルの両方を更新します。

4. 対応するフィールドを編集し、[OK] をクリックします。
確認メッセージが表示されます。

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。

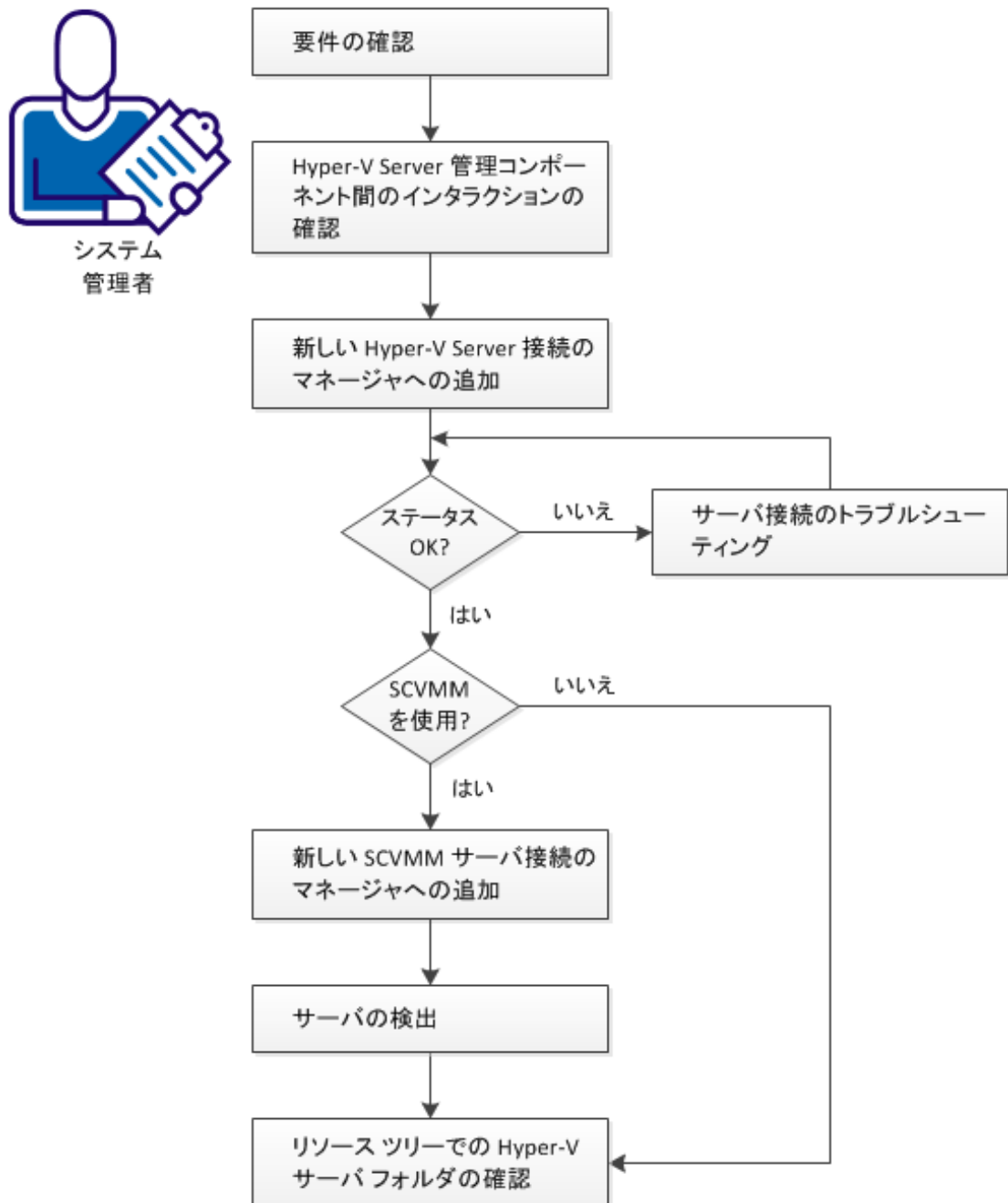
仮想マシン

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 管理の設定方法

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。図には、接続の問題のトラブルシューティング戦略が含まれます。

Hyper-V Server 管理コンポーネントを設定する方法



以下の手順に従います。

[Hyper-V の要件の確認 \(P. 498\)](#)

[Microsoft Hyper-V を使用するために必要な設定の適用 \(P. 499\)](#)

[新しい Hyper-V Server 接続のマネージャへの追加 \(P. 502\)](#)

[\(オプション\) CA Virtual Assurance マネージャへの SCVMM 管理インスタンスの追加 \(P. 505\)](#)

[サーバの検出 \(P. 511\)](#)

[リソース ツリーでの Hyper-V Server フォルダの確認 \(P. 512\)](#)

Hyper-V の要件の確認

CA Virtual Assurance の Hyper-V 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、CA SystemEDGE、および Hyper-V Server に関する基礎知識がある。
- Hyper-V プラットフォーム管理モジュール (PMM)、Hyper-V 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。
- Hyper-V AIM が Hyper-V Server にインストールされていることを確認する。
- 管理対象となる Hyper-V 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)。
- Hyper-V Server が正しく実行されることを確認済みである。
- CA Virtual Assurance マネージャと Hyper-V Server の SNMP 設定に整合性があることを確認する。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 Hyper-V Server 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。

関連項目:

[Microsoft Hyper-V を使用するために必要な設定の適用](#) (P. 499)
[Hyper-V Server 管理コンポーネント間のインタラクション](#) (P. 500)
[新しい Hyper-V Server 接続のマネージャへの追加](#) (P. 502)
[\(オプション\) CA Virtual Assurance マネージャへの SCVMM 管理インスタンスの追加](#) (P. 505)
[サーバの検出](#) (P. 511)
[リソース ツリーでの Hyper-V Server フォルダの確認](#) (P. 512)

Microsoft Hyper-V を使用するために必要な設定の適用

前提条件を確認し、Microsoft Hyper-V 管理用の以下の設定を適用します。

Microsoft Hyper-V を使用するために必要な設定を適用する方法

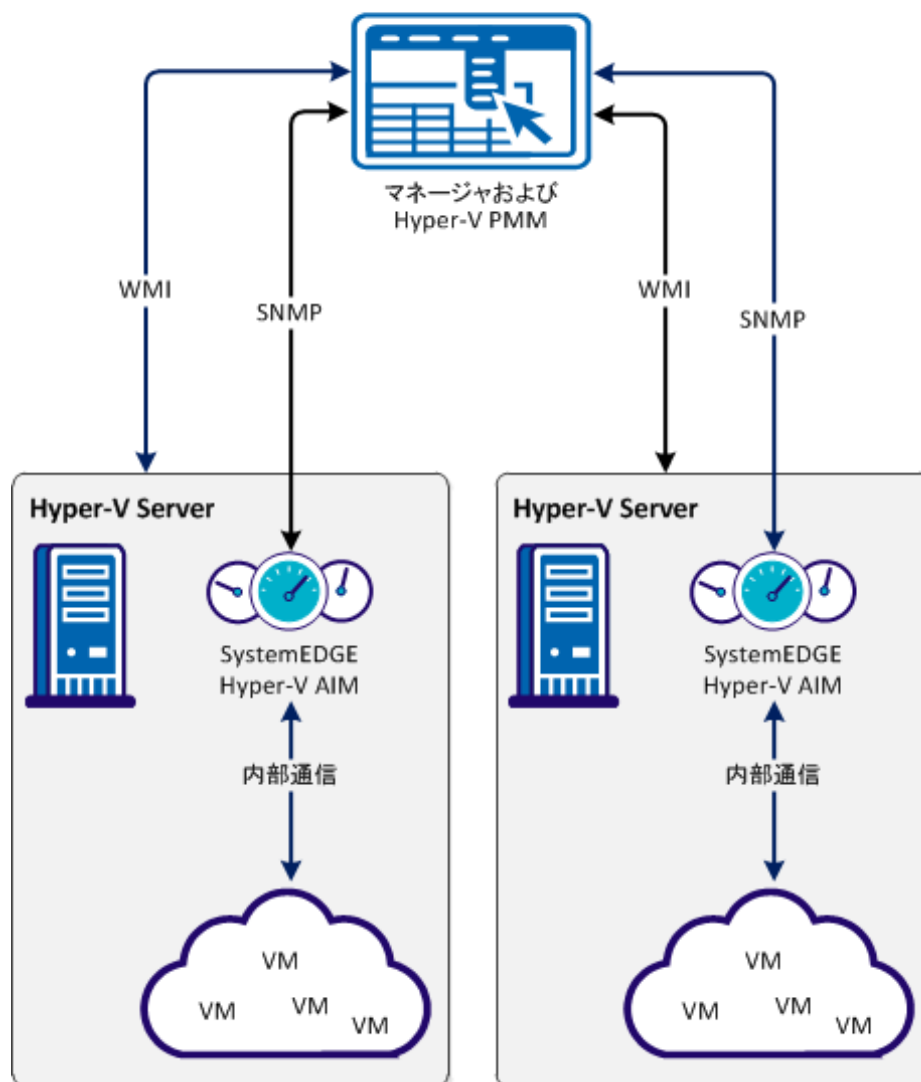
1. SystemEDGE、Advanced Encryption、および Hyper-V AIM が Hyper-V Server にインストールされていることを確認します。各管理対象 Hyper-V Server に割り当てることができる AIM は 1 つだけです。
2. Hyper-V Server 上でローカルのユーザ アクセス制御 (UAC) を無効にします。
3. 以下のレジストリ値を設定してネットワーク UAC を無効にします。
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy,1 (REG_DWORD)
4. コマンドプロンプトから以下のコマンドを実行して、リモート WMI ファイアウォール例外を有効にします。

```
netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)" new enable=yes
```
5. サーバ アクセス用の管理コンポーネントで設定されたユーザが「Distributed COM Users」グループのメンバであることを確認します。

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 管理に参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



接続情報を追加して、Hyper-V 管理を設定できます。以下のいずれかの方法を使用します。

- ユーザインターフェースの [管理] タブ
- AIM サーバ上の NodeCfgUtil.exe ユーティリティ

関連項目：

[新しい Hyper-V Server 接続のマネージャへの追加 \(P. 502\)](#)

[\(オプション\) CA Virtual Assurance マネージャへの SCVMM 管理インスタンスの追加 \(P. 505\)](#)

[サーバの検出 \(P. 511\)](#)

[リソース ツリーでの Hyper-V Server フォルダの確認 \(P. 512\)](#)

新しい Hyper-V 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、Hyper-V 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 [Hyper-V 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 Hyper-V Server が表示されます。
3. [Hyper-V Server] ペイン ツールバーの  (追加) をクリックします。
[新しい Hyper-V 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) を入力し、[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 [Hyper-V Server] ペインに Hyper-V 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 Hyper-V 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 Hyper-V 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、[Hyper-V サーバ接続のトラブルシューティング](#) (P. 503)を参照してください。

関連項目:

[\(オプション\) CA Virtual Assurance マネージャへの SCVMM 管理インスタンスの追加](#) (P. 505)

[サーバの検出](#) (P. 511)

[リソース ツリーでの Hyper-V Server フォルダの確認](#) (P. 512)

[Hyper-V サーバ接続の失敗](#) (P. 503)

Hyper-V サーバ接続の失敗

症状:

〔管理〕-〔設定〕で新しい Hyper-V Server 接続を追加した後、Hyper-V 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。

- Hyper-V Server の接続に使用したデータ（サーバ名、ユーザ、パスワード）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。
- Hyper-V 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。

Hyper-V 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 Hyper-V Server〕または〔Hyper-V 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、およびパスワードを追加します。〔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。

Hyper-V Server への接続を確立できない場合は、次の手順に進みます。

Hyper-V 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 <Hyper-V Server Name>
ping <IP Address of Hyper-V Server>
```

2. Hyper-V 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。

Hyper-V 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 Hyper-V Server を追加します。手順 3 に進みます。

Hyper-V 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 <Hyper-V Server Name>
```

正しい IP アドレスと Hyper-V Server の名前を入力します。例：

```
192.168.50.50 myHyper-V
```

4. 右上角の  (検証) をクリックします。

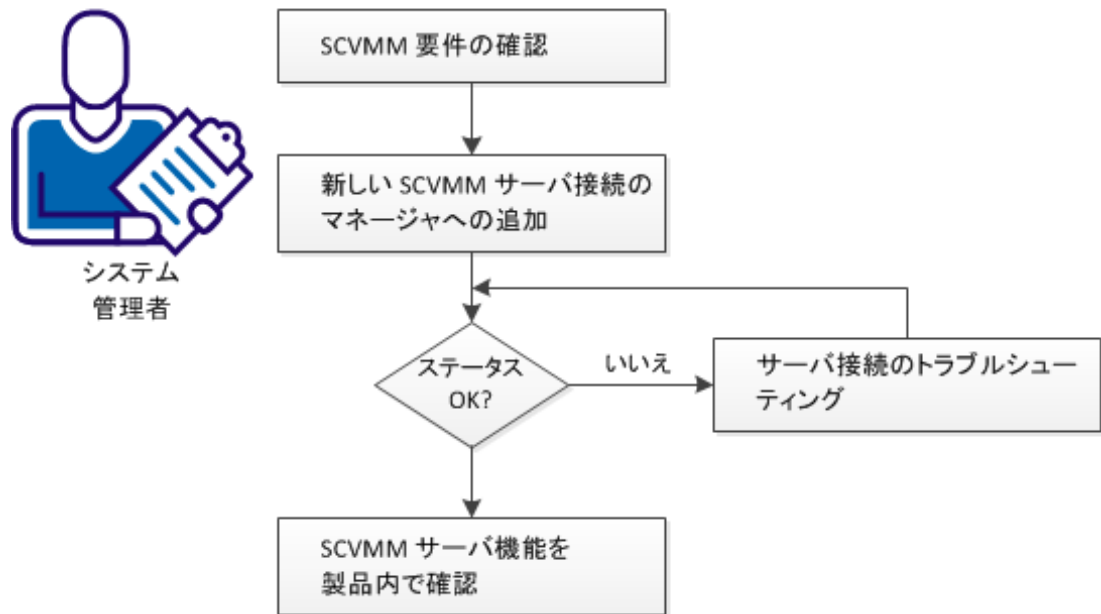
Hyper-V Server への接続が失敗する場合は、このシナリオの要件に従って集めたデータがまだ有効であることを確認してください。

Hyper-V の管理者または VMware のサポート担当者と協力して、Hyper-V Server の接続の問題を解決します。

(オプション) CA Virtual Assurance マネージャへの SCVMM 管理インスタンスの追加

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。

新しい SCVMM サーバ接続の マネージャへの追加



以下の手順に従います。

[Microsoft SCVMM を使用するために必要な設定の適用](#) (P. 506)

[新しい SCVMM サーバ接続のマネージャへの追加](#) (P. 508)

[SCVMM サーバ接続の失敗](#) (P. 509)

Microsoft SCVMM を使用するために必要な設定の適用

CA Virtual Assurance はオプションで、Hyper-V のプロビジョニングのために Microsoft System Center Virtual Machine Manager (SCVMM) と統合できます。Hyper-V のモニタリングと管理に SCVMM は必要ありません。SCVMM の代わりに、VM プロビジョニング用のローカルテンプレート (Hyper-V Server にバインド) を使用することもできます。

オプションの SCVMM 統合を使用するときは、以下の前提条件を確認し、必要な設定を適用します。

Microsoft SCVMM を使用するために必要な設定を適用する方法

1. SCVMM サーバ、VM プロビジョニング用の Hyper-V ターゲットホストの全候補、および Hyper-V PMM を実行している CA Virtual Assurance マネージャが、同じ Active Directory ドメインのメンバであることを確認します。
2. CA Virtual Assurance と SCVMM で、VM プロビジョニング用の Hyper-V ターゲットホストが設定されていることを確認します。CA Virtual Assurance は SCVMM のディスカバリを行いません。
3. SCVMM で Windows Remote Management (WinRM) が設定されていることを確認します。

4. WinRM を設定するには、SCVMM サーバのコマンドラインで以下のコマンドを実行します。

```
winrm quickconfig
```

5. SCVMM サーバでの WinRM の基本設定に加えて、暗号化されない HTTP を許可するか、HTTPS を有効にします。

暗号化されない HTTP トラフィックを許可するには、以下のコマンドを実行します。

```
winrm set winrm/config/service @{AllowUnencrypted="true"}
```

HTTPS を有効にするには、SCVMM サーバ用の SSL 証明書を取得、インストールして、以下のコマンドを実行します。

```
winrm quickconfig -transport:https
```

SCVMM サーバ上でリモート シェル用の割り当て管理のパラメータ設定が不適切であると、環境内での SCVMM サーバの予想使用率によっては、VM プロビジョニングに失敗する可能性があります。関係のあるパラメータは以下のとおりです。

MaxShellsPerUser

ユーザ当たりのシェルの最大数を指定します。

デフォルト : 5

MaxConcurrentUsers

シェルを開くことができる同時ユーザの最大数を指定します。

デフォルト : 5

一度に複数のプロビジョニング ジョブを見込んでいる場合、SCVMM サーバ上のパラメータ設定は以下のように増やすことができます。

```
winrm set winrm/config/winrs @{MaxShellsPerUser="数値"}  
winrm set winrm/config/winrs @{MaxConcurrentUsers="数値"}
```

例

```
winrm set winrm/config/winrs @{MaxShellsPerUser="30"}  
winrm set winrm/config/winrs @{MaxConcurrentUsers="10"}
```

Microsoft が提供している「[Quota Management for Remote Shells](#)」 (英語) の記事も参照してください。

新しい SCVMM サーバ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、SCVMM 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 [SCVMM サーバ] 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 SCVMM サーバが表示されます。
3. [SCVMM 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 SCVMM サーバ] 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) を入力し、[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 [SCVMM Server] ペインに SCVMM 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 SCVMM サーバ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 SCVMM サーバが赤のステータス 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、[SCVMM サーバ接続のトラブルシューティング](#) (P. 509)を参照してください。

SCVMM サーバ接続の失敗

症状:

〔管理〕 - 〔設定〕 で新しい SCVMM サーバ接続を追加した後、SCVMM サーバ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。

- SCVMM サーバの接続に使用したデータ（サーバ名、ユーザ、パスワード）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。
- SCVMM サーバ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。

SCVMM サーバ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 SCVMM サーバ〕 または 〔SCVMM サーバの編集〕 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、およびパスワードを追加します。〔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。

SCVMM サーバへの接続を確立できない場合は、次の手順に進みます。

SCVMM サーバ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 <SCVMM Server Name>  
ping <IP Address of SCVMM Server>
```

2. SCVMM 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。

SCVMM サーバが 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 SCVMM サーバを追加します。手順 3 に進みます。

SCVMM サーバが 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 <SCVMM Server Name>
```

正しい IP アドレスと SCVMM サーバの名前を入力します。例：

```
192.168.50.50 mySCVMM
```

4. 右上角の  (検証) をクリックします。

SCVMM サーバ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。

SCVMM の管理者または Microsoft のサポート担当者と協力して、SCVMM サーバの接続の問題を解決します。

サーバの検出

CA Virtual Assurance マネージャに新しい Hyper-V サーバ接続とオプションの SCVMM 接続を追加した後、Hyper-V Server と SCVMM サーバを検出します。その後、そのすべての仮想コンポーネントを含む Hyper-V 環境全体が CA Virtual Assurance によって検出されます。

CA Virtual Assurance マネージャと、Hyper-V Server および SCVMM サーバの SNMP 認証情報に整合性があることを確認します。必要な場合は、SNMP 設定をそれに応じて更新します。

次の手順に従ってください:

1. [スタート] メニューから CA Virtual Assurance ユーザ インターフェースを開きます。[リソース] - [データ センター] をクリックします。
[データ センター] ページが表示されます。
2. 右側のペインにある [クイック スタート] から、[システムの検出] をクリックします。
右側のペインがリフレッシュされ、[システムの検出] ウィザードが表示されます。
3. 必要なデータを入力し、[終了] をクリックします。
CA Virtual Assurance によってシステムが検出されます。

関連項目:

[リソース ツリーでの Hyper-V Server フォルダの確認 \(P. 512\)](#)

リソース ツリーでの Hyper-V Server フォルダの確認

新しい Hyper-v Server は、設定およびディスクバリエーションに成功すると、[リソース] - [エクスプローラ] ペインの [Hyper-V Server] フォルダに表示されます。

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. [Hyper-V Server] を展開します。
管理対象の Hyper-V Server が表示されます。
3. 新しい Hyper-V Server エントリを展開します。
管理対象の Hyper-V インフラストラクチャが表示されます。

CA Virtual Assurance で、追加された Hyper-V 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。

Hyper-V の管理

Hyper-V Server では、Hyper-V サーバおよび仮想マシンを管理できます。Hyper-V Server は、すべての仮想リソースを表示し、開始、停止、削除などの管理操作を実行できる一元的な場所です。

このセクションでは、[リソース] ページから Hyper-V Server リソースに対して実行できるリソース管理操作について説明します。[リソース] ページでは、以下のオブジェクトに関する基本情報と詳細情報を表示できます。

- Hyper-V Server
- 仮想マシン

[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。次に、いずれか 1 つの Hyper-V リソースを選択し、そのリソースの [サマリ] をクリックします。

[サマリ] ページでは、そのオブジェクトに関連付けられている情報 (Hyper-V Server や、Hyper-V サーバ上の仮想マシン上の仮想マシンなど)、およびリソースに関連付けられているイベントを表示できます。

[詳細] ページでは、リソースの他の詳細情報 (システム プロパティ、ソフトウェア、ハードウェア、パフォーマンスなど) を見ることができます。

[エクスプローラ] ペインのメニューを右クリックすると、管理とポリシーのタスクを実行することができます。

関連項目

[VM ステータスの管理 \(Hyper-V\)](#) (P. 516)

[仮想マシンの削除](#) (P. 517)

[仮想マシン名の変更](#) (P. 518)

[アクションとルールを作成](#) (P. 518)

[起動とシャットダウンのアクションの編集](#) (P. 519)

[VM の CPU およびメモリの割り当ての編集](#) (P. 521)

[Hyper-V 管理アクション](#) (P. 522)

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。.

関連項目

[マシンのプロビジョニング : Microsoft Hyper-V \(P. 850\)](#)

VM ステータスの管理(Hyper-V)

以下のいずれかの VM 操作の実行により Hyper-V Server 仮想マシンのステータスを制御できます。

- 開始
- 停止
- 一時停止
- 再起動
- シャットダウン
- 保存

これらの操作は、複数の VM で同時に実行できます。

VM ステータスを制御する方法

1. [エクスプローラ] ペインでステータス処理を実行する仮想マシンを選択します。
2. VM を右クリックし、[管理] を選択します。[クイック スタート] をクリックし、電源制御の関連するリンクをクリックする方法もあります。以下のいずれかを選択します。

開始

仮想マシンを開始し、ゲスト オペレーティング システムを起動します。現在電源がオフになっているか、中断されている仮想マシンのみ、電源をオンにすることができます。

停止

仮想マシンを電源オフします。現在電源がオンになっているか、中断されている仮想マシンのみ、電源をオフにすることができます。

一時停止

仮想マシンを中断し、現在の状態を保存します。マシンを再開するまで、すべてのアクティビティが中断されます。

再起動

ゲスト オペレーティング システムをシャットダウンし、再起動します。

シャットダウン

ゲスト オペレーティング システムをシャットダウンします。現在電源がオンになっている仮想マシンのみ、シャットダウンすることができます。

保存

仮想マシンの現在のステータスを保存します。このオプションは、他のプラットフォームでの [中断] に似ています。

確認ダイアログ ボックスが開きます。

3. [OK] をクリックします。

ステータス操作が実行され、確認のメッセージが表示されます。インターフェースをリフレッシュして、最新の VM ステータスを表示します。操作の結果を確認するイベントが表示されます。

仮想マシンの削除

Hyper-V Server から仮想マシンを削除すると、仮想マシンは仮想ディスクから削除されます。

仮想マシンを削除する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックし、[管理] - [削除] を選択します。

[Hyper-V VM の削除] ダイアログ ボックスが、追加のコンポーネントを削除するオプションと共に表示されます。

3. [OK] をクリックします。

要求のサブミットを確認するメッセージが表示されます。

4. 仮想マシンの [サマリ] タブをクリックします。

処理の結果を確認するイベントが表示されます。成功すると、その仮想マシンが仮想ディスクから削除され、インターフェースをリフレッシュした後、[エクスプローラ] ペインに表示されなくなります。

注: 電源オフの状態にある VM のみを削除できます。その状態でないと、削除リンクは無効になります。

仮想マシン名の変更

Hyper-V Server から既存の仮想マシンの名前を変更できます。

仮想マシンの名前を変更する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックし、[管理] - [名前の変更] を選択します。
[VM の名前変更] ダイアログ ボックスが表示されます。
3. 新しい VM 名を入力して、[OK] をクリックします。
要求のサブミットを確認するメッセージが表示されます。
4. 仮想マシンの [サマリ] タブをクリックします。

アクションとルールの作成

仮想マシンなど、さまざまなタイプのリソースの既定のポリシーに基づいて、アクションおよびルールを作成できます。

仮想マシンのアクションおよびルールを作成する方法

1. [リソース] - [エクスプローラ] - [データ センター] を選択します。
2. [ポリシー] タブおよび [アクション] サブタブを開きます。
3. [+] (追加) をクリックして、新しいアクションを作成します。
4. ドロップダウン メニューから適切な項目を選択し、ユーザ インターフェイス内の手順に従ってアクションを作成します。
5. [ルール] サブタブを選択し、[+] (追加) をクリックして新しいルールを作成します。

[ルール/テンプレートの特典および評価] ダイアログ ボックスが表示されます。

ウィザードに従って、作成プロセスを進めます。利用可能なアクションのリストからアクションをこのルールに割り当てます。

アクションとルールの詳細については、「[アクションの作成 \(P. 771\)](#)」および「ルールの作成」を参照してください。

起動とシャットダウンのアクションの編集

仮想マシンを起動およびシャットダウンするアクションを編集できます。

起動とシャットダウンのアクションを編集する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックし、[設定] - [起動とシャットダウンのアクション] を選択します。
[起動とシャットダウンのアクション] ダイアログ ボックスが表示されます。
3. [起動とシャットダウンのアクション] ダイアログ ボックスには以下のフィールドが含まれます。

アクション開始

Hyper-V Server の開始時に実行するアクションを指定します。 ドロップダウン リストから、以下のいずれかを選択します。

- 常に
Hyper-V Server の開始時に常に VM を開始します。
- 自動
VM が実行モードでシャットダウンした場合、Hyper-V Server が開始するときに、VM を自動的に開始します。
- なし
Hyper-V Server の開始時に VM を開始しません。

開始遅延

Hyper-V Server の開始後に VM を開始する遅延時間（数秒）を調整します。

シャットダウン アクション

仮想マシンのシャットダウン時に実行するアクションを指定します。ドロップダウン リストから、以下のいずれかを選択します。

- オフ
Hyper-V Server のシャットダウン前に VM をオフにします。
- 保存

Hyper-V Server のシャット ダウン前に VM を保存（中断）します。

- シャットダウン

Hyper-V Server のシャット ダウン前に VM をシャットダウンします。

復旧アクション

Hyper-V Server で障害が発生したときに仮想マシンの以前の詳細を回復するためのアクションを指定します。 ドロップダウン リストから、以下のいずれかを選択します。

- なし

サーバ障害発生後の Hyper-V Server の開始時に特別なアクションを行いません。

- 再起動

VM サーバが失敗した後に Hyper-V Server が開始するとき、VM を再起動します。

- 元に戻す

サーバ障害発生後の Hyper-V Server の開始時に、最新のスナップショットを使って VM を元に戻します。

4. すべての詳細を編集した後、[OK] をクリックします。確認メッセージが表示されます。

VM の CPU およびメモリの割り当ての編集

仮想マシンに割り当てられている CPU 数とメモリ共有を編集して、割り当てられているリソースを調整できます。リソースを追加する場合、適切な量の割り当てられていないメモリと CPU 共有が利用できる必要があります。メモリまたは CPU 共有で許可される最小値および最大値が存在する場合は、リソース割り当ての変更は、これらの制限内で行う必要があります。

特定の VM リソース割り当てアクションを使用して、ポリシーの作成およびスケジュールを行うこともできます。

VM の CPU およびメモリの割り当てを編集する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックし、[設定] - [リソース割り当て] - [CPU およびメモリ] を選択します。
[CPU およびメモリ リソース割り当て] ダイアログ ボックスが表示されます。
3. CPU の数、予約済み CPU パーセンテージ、および CPU 制限のパーセンテージを調節します。
4. 仮想マシンに割り当てられているメモリ共有を調節し、すべての詳細を編集した後、[OK] をクリックします。
確認メッセージが表示されます。

Hyper-V 管理アクション

以下のアクションタイプを Hyper-V Server で使用できます。

- [マシンの削除](#) (P. 818)
- [マシン状態の変更](#) (P. 783)
- [電源の設定](#) (P. 800)
- [CPU/メモリの設定](#) (P. 789)

割り当てられたルール基準が満たされるときに、Hyper-V Server の起動オプションとシャットダウン オプションの設定、および他の操作を自動化する新規アクションを作成するためにこれらのアクションタイプを使用できます。これらのアクションが特定の時刻に行われるようにスケジュールすることもできます。

自動化ポリシーを作成するアクションおよびルールの使用の詳細については、「ポリシー」の章を参照してください。

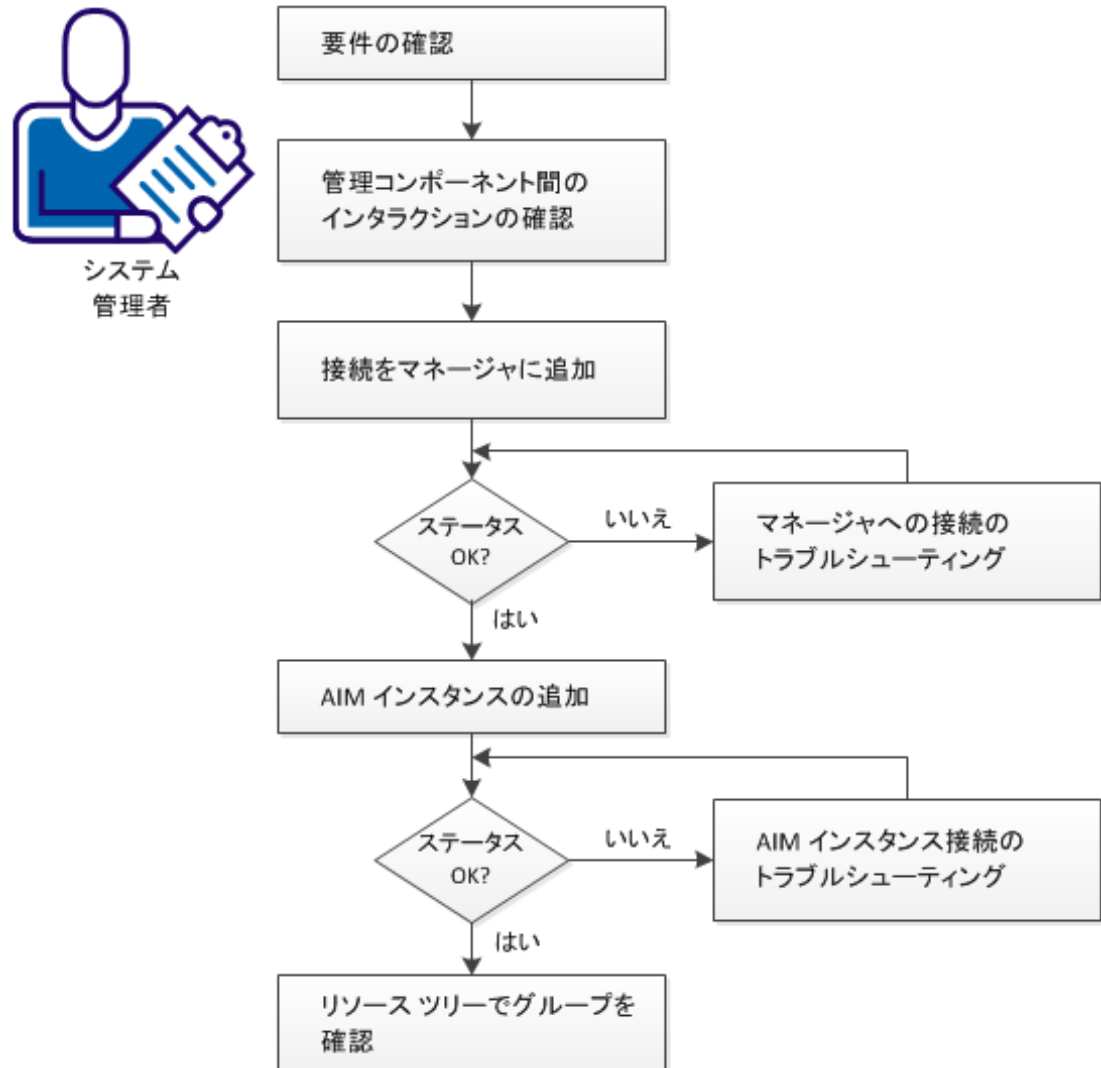
Red Hat Enterprise Virtualization

CA Virtual Assurance では、カーネルベースの仮想マシン サポートが導入されました。カーネルベースの仮想マシン(KVM)は Linux カーネル用のハードウェア支援型仮想化インフラストラクチャです。CA KVM AIM はマルチインスタンスのリモート AIM として実装されます。CA KVM AIM は RHEV モニタリングを有効にします。Red Hat Enterprise Red Hat Enterprise Virtualization (RHEV) は KVM ハイパーバイザに基づいたエンタープライズ仮想化製品です。

Red Hat Enterprise Virtualization 管理コンポーネントの設定方法

以下の図は、管理コンポーネントを設定するために必要なアクションの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。

管理コンポーネントの設定方法



以下の手順に従います。

[要件の確認](#) (P. 524)

[RHEV 管理コンポーネント間のインタラクション](#) (P. 525)

[マネージャへの Red Hat Enterprise Virtualization 接続の追加](#) (P. 526)

[サーバへのマネージャの接続が失敗する](#) (P. 527)

[検出された Red Hat Enterprise Virtualization AIM インスタンスの追加](#) (P. 529)

[AIM インスタンス接続のトラブルシューティング](#) (P. 530)

[リソース ツリーでの Red Hat Enterprise Virtualization グループの確認](#) (P. 534)

要件の確認

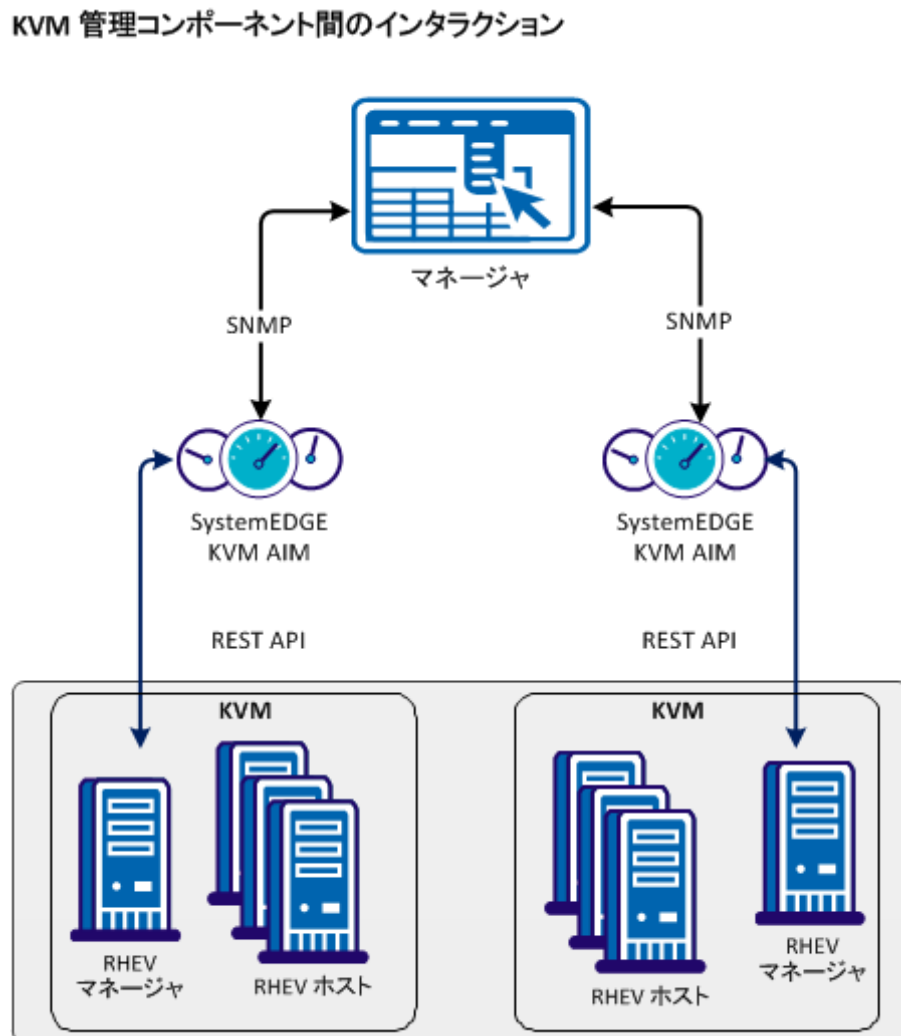
CA Virtual Assurance の管理コンポーネントを設定する前に、以下の要件を確認します。

- 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 および SystemEDGE に精通している。
- 以下を含む CA Virtual Assurance マネージャ インストールにアクセスできる。
 - プラットフォーム管理モジュール (PMM)
 - Application Insight Module (AIM)
 - モニタリング エージェント (SystemEDGE)
- CA Virtual Assurance ユーザ インターフェースにアクセスできる。
- 管理対象となる環境のサーバ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 サービスを通して使用する環境のサーバ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
- 使用する環境にあるサーバが正常に実行されていることを確認済みである。

- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM 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。
- 使用するリモート 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。

RHEV 管理コンポーネント間のインタラクション

以下の図は、RHEV モニタリング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 KVM AIM は、同じ Windows Server 上で実行します。AIM は REST API を使用して、1 つ以上の RHEV マネージャと通信します。



マネージャへの Red Hat Enterprise Virtualization 接続の追加

CA Virtual Assurance ユーザ インターフェースの [管理] タブを使用して、Red Hat Enterprise Virtualization 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. 左ペインの [プロビジョニング] セクションから **Red Hat Enterprise Virtualization** を選択します。
3. [登録された Red Hat Enterprise Virtualization サーバ] ペイン ツールバー上の  (追加) をクリックします。
[Red Hat Enterprise Virtualization サーバの追加] ダイアログ ボックスが表示されます。
4. 必要な接続データ (サーバ名、ユーザ、パスワード、ISO ライブラリ認証情報、ポート) を入力し、優先の AIM を指定し、[管理ステータス] (チェック ボックス) を有効にします。

注: ISO ライブラリには、プロビジョニング用の ISO イメージが含まれています。 ISO イメージがない場合、プロビジョニングは動作しません。

5. [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、右上のペインにサーバ追加され、緑のステータス アイコンが表示されます。

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** によってサーバがリストに追加され、接続の失敗を示す赤のステータス アイコンが表示されます。 [いいえ] をクリックすると、何も追加されません。

サーバへのマネージャの接続が失敗する

症状:

「管理」 - 「設定」でサーバ接続を追加した後に、サーバ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。

- サーバへの接続に使用したデータが現在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。
- サーバ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。
- 接続に必要なすべてのサービスが、サーバシステム上で正しく実行されているかどうかを確認します。

サーバ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。
2. 接続の詳細を追加し、「管理ステータス」を有効にし、「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。
サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ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 <Server Name>
ping <IP Address of Server>
```

2. サーバに有効な DNS エントリおよび IP アドレスが設定されているかどうかを調べるには、これらのコマンドの出力を確認します。

サーバが DNS で見つからない場合は、CA Virtual Assurance マネージャ システム上にある Windows の `hosts` ファイルにサーバを追加します。手順 3 に進みます。

サーバが DNS で見つかった場合は、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 <Server Name>
```

正しい IP アドレスとサーバ名を入力してファイルを保存します。例：

```
192.168.50.50 myServer
```

4. CA Virtual Assurance ユーザ インターフェイスで、[管理] タブの [設定] に移動して、[サーバ] ペインの右上角にある  (検証) をクリックします。

サーバの認証情報と接続データが正しく、サーバに対して `ping` を実行できる場合でも、接続に失敗することがあります。このような場合は、サーバに問題がある可能性があります。サーバへの接続を確立できない場合は、次の手順に進みます。

接続に必要なすべてのサービスが、サーバシステム上で正しく実行されているかどうかを確認する方法

1. サーバにアクセスするために、システム管理者に問い合わせます。
2. サーバシステムにログインします。
3. 接続に必要なすべてのサービスが正しく実行されているかどうかを確認します。
4. 必要に応じて、サービスを開始または再起動します。
5. **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 [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 によってサーバ接続が検証されます。

サーバ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収集したデータが正しいことを確認してください。

管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

検出された Red Hat Enterprise Virtualization AIM インスタンスの追加

Red Hat Enterprise Virtualization 接続を **CA Virtual Assurance** マネージャに追加した後、Red Hat Enterprise Virtualization 環境を管理するために AIM インスタンスを追加します。

次の手順に従ってください:

1. [スタート] メニューから **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. 左ペインの [プロビジョニング] セクションから Red Hat Enterprise Virtualization を選択します。

3. [検出された Red Hat Enterprise Virtualization AIM インスタンス] ペイン ツールバー上の  (追加) をクリックします。
[Red Hat Enterprise Virtualization AIM インスタンスの追加] ダイアログ ボックスが表示されます。
4. ドロップダウン リストから [RHEV AIM サーバ] を選択します。
検出された RHEV AIM サーバのリストが表示されます。
5. ドロップダウン リストから [RHEV サーバ] を選択します。
[登録された Red Hat Enterprise Virtualization サーバ] ペインに一覧表示された RHEV サーバが [RHEV サーバ] ドロップダウン リストに入力されます。管理できる RHEV サーバは、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。
注: AIM がリモートシステムに存在している場合、CA Virtual Assurance でこのシステムを最初に検出する必要があります。検出後、AIM サーバがドロップダウン リストに表示されます。
6. [OK] をクリックします。
選択したサーバの新しい 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、Red Hat Enterprise Virtualization 環境の管理を開始できます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

[管理] - [設定] でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  (ディスカバリが進行中) が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。ディスカバリにかかる時間は、環境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数によって異なります。アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Virtual Assurance はサーバフォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

[管理] - [設定] で AIM インスタンスを追加した後、ステータス アイコンに  (ポーリングなし) が表示されます。

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。このアイコンは、CA Virtual Assurance マネージャがこの AIM をポーリングしないこと表します。この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。別の AIM を使用したい場合は、[管理] - [設定] - [プロビジョニング] で優先 AIM を設定できます。サーバエントリの [編集] をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

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 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:

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。

- 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。

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. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

AIM サーバが 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 AIM サーバを追加します。手順 3 に進みます。

サーバが 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 AIM サーバの名前を入力します。例:

```
192.168.50.51 myAIM
```

4. [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. 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 [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 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、収集したデータがこのシナリオの要件に従っていることを確認してください。

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 AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン  (無効) が表示されます。この 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 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サーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

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。

- 欠落しているサーバから CA Virtual Assurance マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、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 Red Hat Enterprise Virtualization グループの確認

設定および検出に成功すると、新たに検出されたリソースが [リソース] - [エクスプローラ] ペインの対応するグループに表示されます。

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] ペインを開きます。
2. Red Hat Enterprise Virtualization グループを展開します。

管理対象の Red Hat Enterprise Virtualization リソースが表示されます。

これで、CA Virtual Assurance は、設定された Red Hat Enterprise Virtualization 環境を管理できる状態になります。

KVM のプロビジョニング用に Linux テンプレートを準備する方法

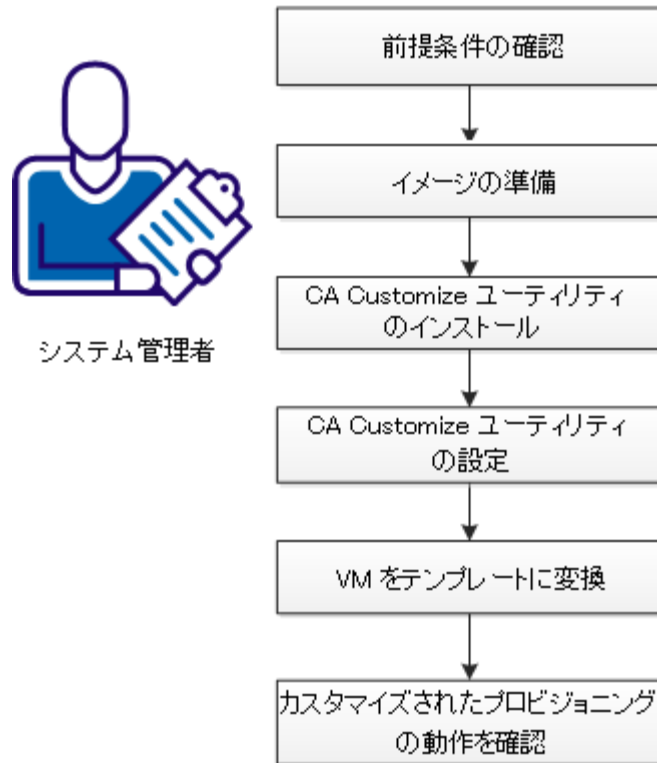
CA Virtual Assurance は、以下のオペレーティング システムを実行する新しい仮想マシン (VM) のカスタマイズされたプロビジョニングをサポートします。

- Red Hat Enterprise Server 6.0
- SUSE Linux Enterprise Server 11

カスタマイズ オプションには、ホスト名、パスワード、ドメイン、またはネットワーク設定が含まれます。

以下の図は、システム管理者が VM のプロビジョニング用に Linux テンプレートを準備する方法を示しています。

VM のプロビジョニング用に Linux テンプレートを準備する方法



以下の手順に従います。

[カスタマイズされた VM プロビジョニングの前提条件](#) (P. 536)

[Linux イメージの準備 \(KVM\)](#) (P. 536)

[CA Customize ユーティリティのインストール](#) (P. 537)

[CA Customize ユーティリティの設定](#) (P. 538)

[VM をテンプレートに変換](#) (P. 539)

[カスタマイズされたプロビジョニングの動作](#) (P. 539)

カスタマイズされた VM プロビジョニングの前提条件

Linux ゲストをカスタマイズするには、ファイル システムまたはコンソールへの直接アクセスが必要です。

RHEV 環境が以下の前提条件に適合することを確認します。

- 各 RHEV データ センターが、RHEV マネージャ システム上でローカル ISO ライブラリを使用している。
- 各マシンで SFTP アクセスが有効になっている。
- RHEV マネージャで SSH アクセスが有効になっている。

Linux イメージの準備 (KVM)

Linux オペレーティング システムが含まれるテンプレートを作成するときには、この手順に従ってイメージを準備します。一部の手順は Linux ディストリビューションによって異なる場合があります。

次の手順に従ってください:

1. Linux オペレーティング システムを新しい仮想マシンにゼロからインストールします。
2. 仮想マシン内で RHEV Guest Tools をインストールします。
3. ユーザ アカウント、ポリシー、アプリケーション、ホット フィックスなど、新しい仮想マシンに追加するカスタマイズを適用します。

この Linux イメージは、CA Customize ユーティリティを使用してさらにカスタマイズできます。

CA Customize ユーティリティのインストール

CA Customize ユーティリティを使用すると、CA Virtual Assurance で仮想マシンの設定を外部から変更できます。このゲストユーティリティは、OS の開始時に CD ドライブをモニタします。特別な ISO が接続されると、以下のアクションが実行されます。

1. コマンドセットによってゲストがカスタマイズされます。
2. ゲストシステムはカスタマイズ済みとしてマークされます。
この状態がリセットされるまで、システムはこれ以上変更できなくなります。
3. システムが停止し、カスタマイズが成功したことを示します。

ca-customize ゲストユーティリティを正しくインストールする方法

1. このユーティリティを以下で見つけます。
 - Red Hat Enterprise Server 6.0 の場合
`<InstallationRoot>%Utilities%\linuxCustomization%\rh6`
 - SUSE Linux Enterprise Server 11 の場合
`<InstallationRoot>%Utilities%\linuxCustomization%\sles11`
2. この実行可能ファイルを、準備する VM のハードドライブの以下の場所に移動します。
`/usr/bin/ca-customize`
3. (オプション) サポートされていない他のゲストシステムをサポートするには、ユーザ独自の `ca-customize` スクリプトを指定します。
4. `ca-customize` ユーティリティの実行可能ビットを有効にします。
`chmod 755 /usr/bin/ca-customize`

CA Customize ユーティリティの設定

Linux プロビジョニング用のテンプレートをセットアップできます。ゲストをカスタマイズするには、利用可能なスクリプトを使用します。また、ユーザ独自のスクリプトを使用して詳細なセットアップを行うこともできます。

次の手順に従ってください:

1. ネットワークがカスタマイズのプロセスに影響しないように、ネットワーク インターフェースを無効にします。

注: ネットワークはカスタマイズ中に自動的に有効化されます。

2. 必要に応じて、`/etc/ca-customize.conf` ファイルを使用して、デフォルトの CDROM デバイス名を上書きします。

`CD_DEVICE=/dev/cdrom`

CD ドライブに使用するデバイス名を定義します。

デフォルト: `/dev/cdrom`

3. ブート プロセスの最後に自動起動をセットアップします。

- (SUSE Linux の場合) `/etc/init.d/after.local` ファイルを作成または変更します。

```
#!/bin/bash  
[ -e /etc/ca-customized ] || /usr/bin/ca-customize
```

- (Red Hat Linux の場合) 以下の行を `/etc/rc.local` ファイルに追加します。

```
[ -e /etc/ca-customized ] || /usr/bin/ca-customize
```

4. システムをシャットダウンします。

VM をテンプレートに変換

テンプレートを使用すると、カスタマイズした仮想マシンをいくつでも作成できます。

次の手順に従ってください:

1. VM をシャットダウンします。
2. シャットダウンした仮想マシンを RHEV テンプレートに変換するには、RHEV Administration Portal を使用します。

テンプレートが CA Virtual Assurance に表示され、プロビジョニングのカスタマイズに使用できるようになります。

これらの手順の実行後、新規テンプレートを使用して任意の数のカスタマイズされた仮想マシンを新しく作成することができます。

カスタマイズされたプロビジョニングの動作

以下の手順は、カスタマイズされた VM プロビジョニングのワークフローを表します。

1. プラットフォーム管理サービスは新しい Linux VM をプロビジョニングします。
2. プラットフォーム管理サービスは、カスタマイズ パラメータを使用して新しい ISO を準備し、新しい VM に添付します。
3. プラットフォーム管理サービスは VM を開始します。
4. VM はカスタマイズ ISO が添付されていることを検出します。VM はカスタマイズ変更を適用します。
5. カスタマイズが成功すると、VM はシャットダウンします。PMM は VM の停止を検出します。プラットフォーム管理サービスは再度 VM を開始し、プロビジョニングを完了します。
6. カスタマイズが失敗すると、VM は停止しません。プラットフォーム管理サービスは以下のアクションを実行します。
 - a. プロビジョニングの失敗を返します
 - b. プロビジョニング ジョブを例外状態に設定します

カスタマイズ ログ

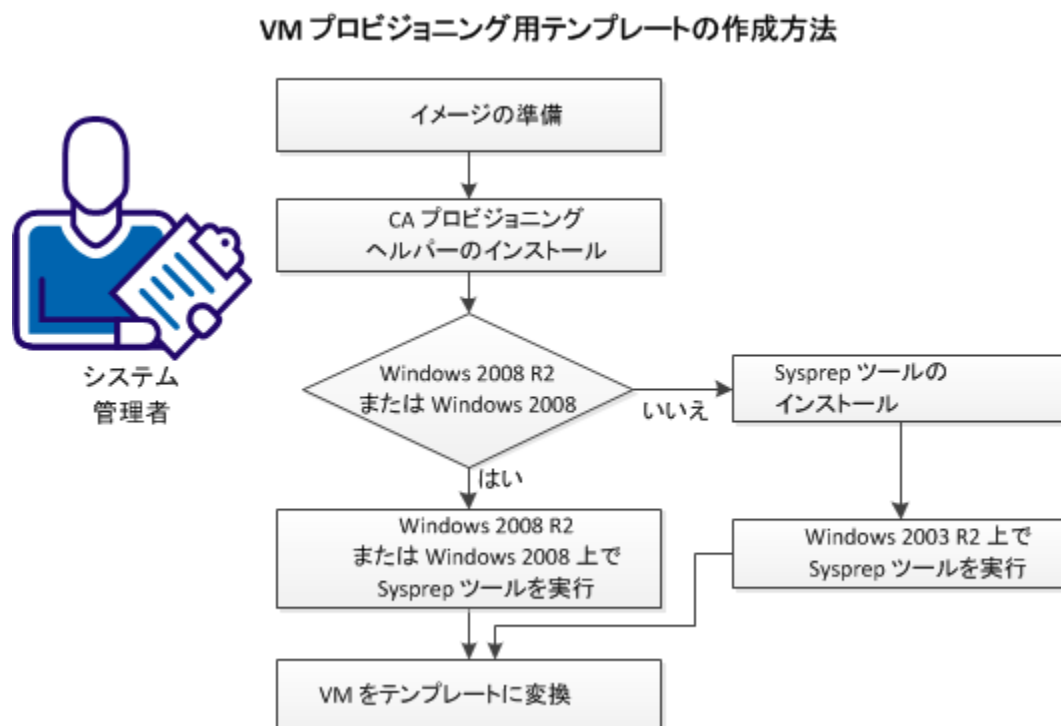
成功したカスタマイズは、`/etc/ca-customized` ファイルに格納されます。このファイルには、カスタマイズ変更のリストが含まれます。

カスタマイズに失敗すると、ログが `/etc/ca-customized.tmp` ファイルに格納されます。

KVM のプロビジョニング用に Windows テンプレートを準備する方法

CA Virtual Assurance では、Windows 2003 R2 Server (32 ビット/64 ビット)、Windows 2008 (32 ビット/64 ビット) または Windows 2008 R2 Server (64 ビット) を実行する新しい仮想マシン (VM) でのプロビジョニングのカスタマイズをサポートしています。カスタマイズ オプションには多数の設定があります。たとえば、組み込みの管理者アカウントのパスワード、コンピュータ名、およびネットワーク設定を変更できます。

以下の図は、システム管理者が KVM のプロビジョニング用に Windows テンプレートを準備する方法を示しています。



次の手順に従ってください:

1. [イメージを準備します。](#) (P. 542)
2. [CA プロビジョニング ヘルパーをインストールします。](#) (P. 405)
3. (Windows 2003 R2 で有効) [Sysprep ツールをインストールします](#) (P. 405)。
4. 使用するオペレーティング システムに応じて、以下のアクションのいずれかを選択します。
 - [Windows 2003 R2 で Sysprep ツールを実行する。](#) (P. 405)
 - [Windows 2008 R2 上で Sysprep ツールを実行する。](#) (P. 406)
5. [VM をテンプレートに変換します。](#) (P. 544)

RHEV 環境の前提条件

RHEV 環境が以下の前提条件に適合することを確認します。

- 各 RHEV データ センターが、RHEV マネージャ システム上でローカル ISO ライブラリを使用している。
- 各マシンで SFTP アクセスが有効になっている。
- RHEV マネージャで SSH アクセスが有効になっている。

Windows イメージの準備

Windows オペレーティング システムが含まれるテンプレートを作成する際には、この手順に従って、イメージを準備します。テンプレートをカスタマイズするには、**CA Virtual Assurance** のプロビジョニング操作を有効にする手順に従ってください。一部の手順は **Windows** のバージョンによって異なります。

次の手順に従ってください:

1. **Windows** オペレーティング システムを新しい仮想マシンにゼロからインストールします。
2. 仮想マシン内で **RHEV Guest Tools** をインストールします。
3. ユーザ アカウント、ポリシー、アプリケーション、ホット フィックスなど、新しい仮想マシンに適用したいカスタマイズを適用します。
4. (**Windows 2003** で有効) 組み込みの管理者アカウントのパスワードを空白にします。

注: 管理者パスワードが空でないと、プロビジョニングの際に **SysPrep** で新しいパスワードを設定できず、既存のパスワードが残ります。

CA プロビジョニング ヘルパーのインストール

CA プロビジョニング ヘルパーは、**CA Virtual Assurance** で仮想マシンの設定を外部から変更できるようにするものです。

次の手順に従ってください:

1. `<InstallationRoot>\Utilities\Sysprep\CAProvisioningHelper.exe` でこのユーティリティを見つけます。
2. 準備する VM のハード ドライブの任意の場所に、この実行可能ファイルを移動します。
3. コマンド ラインから **CA プロビジョニング ヘルパー** を 1 回実行します。

Sysprep ツールのインストール

Windows インストール CD-ROM から **Sysprep** ツールをインストールします。

Sysprep ツール

Microsoft は、設定されている Windows インストールを一般化、フリーズ、およびシャットダウンするための Sysprep ツールを提供しています。以下のセクションでは、Windows 2003 R2 および Windows 2008 R2 用の Sysprep ツールを使用する方法の詳細について説明します。

Windows 2003 R2 での Sysprep ツールの実行

Sysprep ツールのインストールを設定した後、Sysprep ツールを実行します。

次の手順に従ってください:

1. 以下の CAB ファイルを探して開きます。

`%SUPPORT%TOOLS%DEPLOY.CAB`

2. CAB ファイルに含まれるファイルをすべて選択し、%SystemDrive%¥Sysprep（通常は C:¥Sysprep）にコピーします。

注: ディレクトリ名は変更しないでください。

3. Sysprep ディレクトリに移動して、以下を実行します。

```
sysprep -quiet -reseal -mini -forcshutdown
```

Windows 2008 R2 での Sysprep ツールの実行

通常の Windows インストールプロセスでは、SysPrep プロセスを実行するためのすべてのファイルがインストールされます。Windows インストールを設定した後、以下の手順を実行します。

1. Windows Server 2008 R2 用の Windows 自動インストールキット (WAIK) を使用して、有効な XML 応答ファイルを作成します。WAIK は Microsoft の Web サイトから入手できます。

注: このプロビジョニングでは、ダミーの自動応答ファイルが必要で、これがないとシャットダウンできません。応答ファイルの内容はプロビジョニングプロセスによって置換されるため、どのようなものでもかまいません。ただし、ファイルは SysPrep に固有の XML スキーマに従う必要があります。

2. 作成された XML ファイルに「sysprep.xml」と名前を付け、これを以下の Sysprep ディレクトリに置きます。

```
%SystemRoot%\system32\sysprep
```

3. 以下のコマンドを実行します。

```
sysprep /generalize /oobe /shutdown /unattend:sysprep.xml
```

VM を RHEV のテンプレートへ変換

シャットダウンした仮想マシンを RHEV テンプレートに変換するには、RHEV Administration Portal を使用します。

テンプレートが CA Virtual Assurance に表示され、プロビジョニングのカスタマイズに使用できるようになります。

これらの手順の実行後、新規テンプレートを使用して任意の数のカスタマイズされた仮想マシンを新しく作成することができます。

VM ステータスの管理 (KVM)

仮想マシンのステータスを制御するには、以下のいずれかの操作を行います。

- 検出
 - サーバ
 - ネットワーク
- 開始
- 中断
- シャットダウン
- 破棄

VM ステータスを制御する方法

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. VM を右クリックし、[管理] を選択して、以下のいずれかのオプションを選択します。

検出

サーバまたはネットワークを検出します。

開始

指定された RHEV ホスト上の VM を開始します。

中断

指定された RHEV ホストで実行されている VM を中断して、その現在の状態を保存します。VM を再開するまで、すべてのアクティビティが中断されます。

シャットダウン

指定された RHEV ホストで実行されている VM をシャットダウンします。

破棄

VM を削除します。

対応するウィザードが表示されます。

3. 必要な情報を入力して、次の手順に進みます。

4. サブミットします。

ステータス操作が実行され、確認のメッセージが表示されます。インターフェースをリフレッシュして、最新の **VM** ステータスを表示します。操作の結果を確認するイベントが表示されます。

RHEV 仮想マシンのプロビジョニング

以下の手順を実行することで、仮想マシンをプロビジョニングできます。
VM のプロビジョニング用の **Windows** テンプレートを準備してください。

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. **Red Hat Enterprise Virtualization** グループを右クリックし、[プロビジョニング] - [RHEV 仮想マシンのプロビジョニング] を選択します。
プロビジョニング ウィザードが表示されます。
3. 必要な情報を入力します。

VM 名

新しい VM 名を定義します。

テンプレート

Windows プロビジョニング テンプレートを指定します。

管理者パスワード

新しい VM の管理者パスワードを定義します。

製品のアクティベーション キー

Windows 2003 のアクティベーション キーを定義します。

フルネーム

VM のフルネームを定義します。

4. (オプション) 追加情報 (ワークグループ、メモリ、CPU、VM ホスト、組織) を指定します。静的 IP アドレスを使用する場合は、DHCP を無効にし、IP アドレス、マスク、およびデフォルトゲートウェイを指定します。

注: メモリと CPU の設定は、使用する Windows プロビジョニング テンプレートによって異なります。

5. サブミットします。
確認メッセージが表示されます。
6. [ジョブ] パネルをリフレッシュして、進捗状況を表示します。
操作の結果を確認するイベントが表示されます。

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、プロセスがほか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。

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。

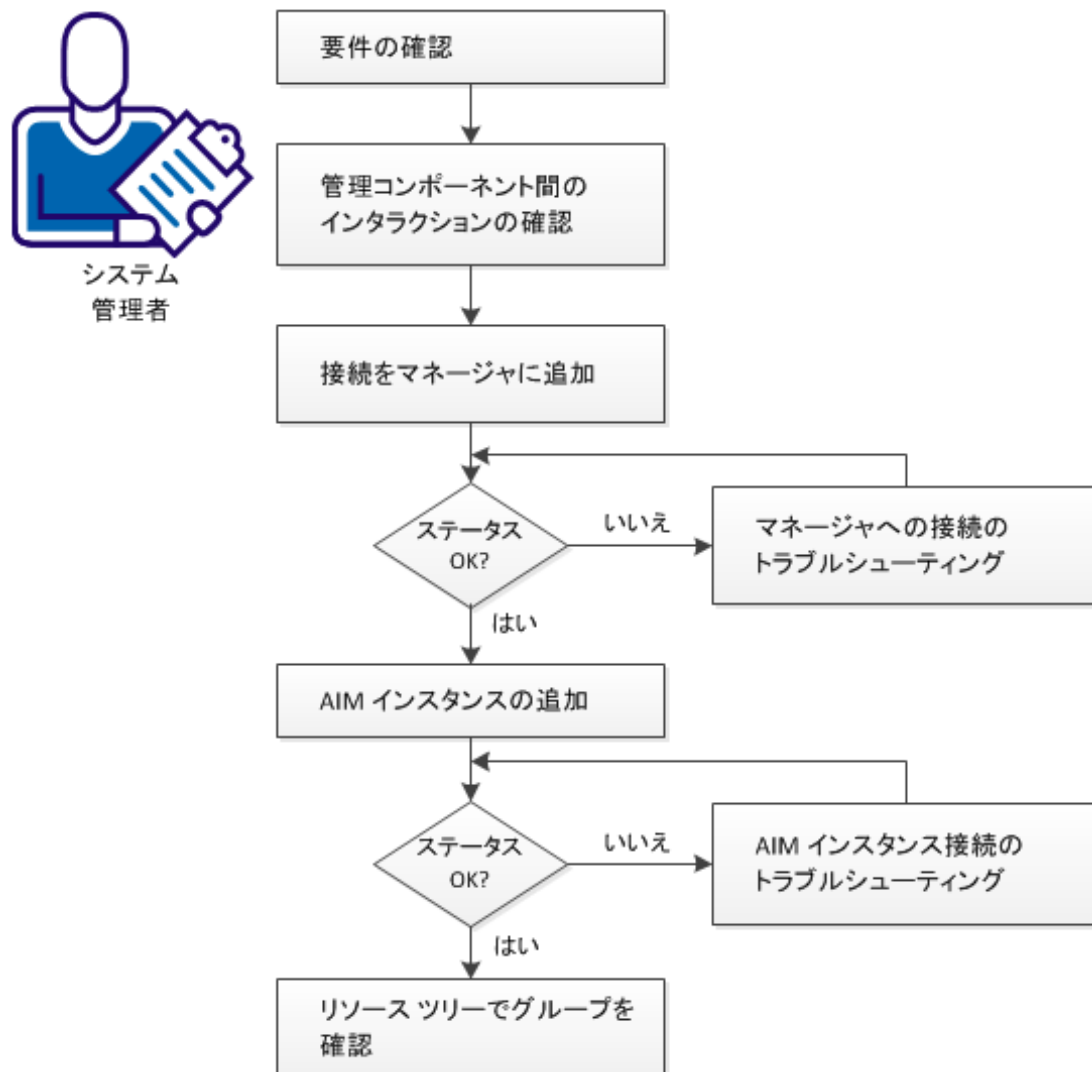
Solaris ゾーン リソース プール管理

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を設定する方法

以下の図は、管理コンポーネントを設定するために必要なアクションの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。

管理コンポーネントの設定方法



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。

以下の手順に従います。

[要件の確認 \(P. 550\)](#)

[Solaris ゾーン管理コンポーネント間のインタラクション \(P. 553\)](#)

[マネージャへの Solaris ゾーン接続の追加 \(P. 554\)](#)

[サーバへのマネージャの接続が失敗する \(P. 555\)](#)

[ゾーン AIM サーバの追加 \(P. 558\)](#)

[AIM インスタンス接続のトラブルシューティング \(P. 559\)](#)

[リソース ツリーでの Solaris ゾーン グループの確認 \(P. 562\)](#)

要件の確認

CA Virtual Assurance の管理コンポーネントを設定する前に、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 および SystemEDGE に精通している。
- 以下を含む CA Virtual Assurance マネージャ インストールにアクセスできる。
 - プラットフォーム管理モジュール (PMM)
 - Application Insight Module (AIM)
 - モニタリング エージェント (SystemEDGE)
- CA Virtual Assurance ユーザ インターフェースにアクセスできる。
- 管理対象となる環境のサーバ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 サービスを通して使用する環境のサーバ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
- 使用する環境にあるサーバが正常に実行されていることを確認済みである。

- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM 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。
- 使用するリモート 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。

関連項目:

[Solaris ゾーン管理の要件](#) (P. 552)

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

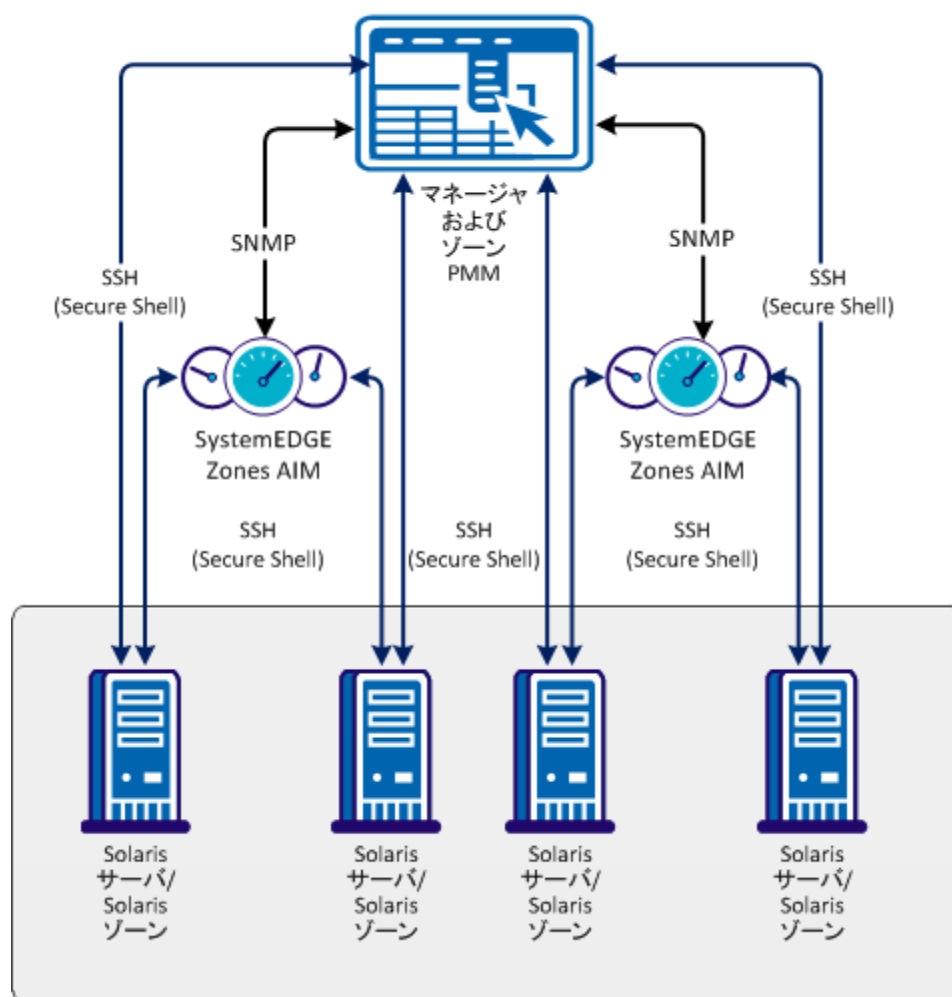
Solaris ゾーン AIM が存在する管理対象ノード上で、ユーザ インターフェースまたは **NodeCfgUtil.exe** ユーティリティを使用して、設定時に **CA Virtual Assurance** に対するこのユーザ名および対応するパスワードを追加します。

[エクスプローラ] - [管理] - [リソース プールの作成] からリソース プールを作成して、Solaris ゾーン サーバ上のゾーン、プロジェクト、およびアプリケーションにリソースを割り当てます。ゾーンにはゾーン作成中にリソースを割り当てます。

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 ゾーン管理に関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、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。

マネージャへの Solaris ゾーン接続の追加

CA Virtual Assurance ユーザ インターフェースの [管理] タブを使用して、Solaris ゾーン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 [Solaris ゾーン] を選択します。
3. [Solaris ゾーン サーバ] ペイン ツールバーの  (追加) をクリックします。
[Solaris ゾーン サーバ] 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、ポート) を入力し、優先 AIM を指定して、[管理ステータス] (チェック ボックス) をオンにします。
5. [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は、右上のペインにサーバが緑のステータス アイコンを使って追加されます。

注: 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 によってサーバが赤のステータス 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。

サーバへのマネージャの接続が失敗する

症状:

「管理」 - 「設定」でサーバ接続を追加した後に、サーバ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。

- サーバへの接続に使用したデータが現在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。
- サーバ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。
- 接続に必要なすべてのサービスが、サーバシステム上で正しく実行されているかどうかを確認します。

サーバ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。
2. 接続の詳細を追加し、「管理ステータス」を有効にし、「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。
サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ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 <Server Name>  
ping <IP Address of Server>
```

2. サーバに有効な DNS エントリおよび IP アドレスが設定されているかどうかを調べるには、これらのコマンドの出力を確認します。

サーバが DNS で見つからない場合は、CA Virtual Assurance マネージャシステム上にある Windows の hosts ファイルにサーバを追加します。手順 3 に進みます。

サーバが DNS で見つかった場合は、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 <Server Name>
```

正しい IP アドレスとサーバ名を入力してファイルを保存します。例：

```
192.168.50.50 myServer
```

4. CA Virtual Assurance ユーザインターフェースで、[管理] タブの [設定] に移動して、[サーバ] ペインの右上角にある  (検証) をクリックします。

サーバの認証情報と接続データが正しく、サーバに対して ping を実行できる場合でも、接続に失敗することがあります。このような場合は、サーバに問題がある可能性があります。サーバへの接続を確立できない場合は、次の手順に進みます。

接続に必要なすべてのサービスが、サーバシステム上で正しく実行されているかどうかを確認する方法

1. サーバにアクセスするために、システム管理者に問い合わせます。
2. サーバシステムにログインします。
3. 接続に必要なすべてのサービスが正しく実行されているかどうかを確認します。
4. 必要に応じて、サービスを開始または再起動します。
5. **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 [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 によってサーバ接続が検証されます。

サーバ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収集したデータが正しいことを確認してください。

管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

ゾーン AIM サーバの追加

CA Virtual Assurance マネージャに Solaris ゾーン接続を追加した後、Solaris ゾーン環境を管理するための AIM インスタンスを追加します。

次の手順に従ってください:

1. [スタート] メニューから **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 [Solaris ゾーン] を選択します。
3. [ゾーン AIM サーバ] ペイン ツールバーの  (追加) をクリックします。
[新しいゾーン AIM サーバ] ダイアログ ボックスが表示されます。
4. ドロップダウン リストから [AIM サーバ] を選択します。
[ゾーン サーバ] ペインに一覧表示されたゾーン サーバが [インスタンス] ドロップダウン リストに入力されます。管理できるゾーン サーバは、**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。

注: AIM がリモート システムに存在している場合、**CA Virtual Assurance** でこのシステムを最初に検出する必要があります。 検出後、AIM サーバがドロップダウン リストに表示されます。

5. ドロップダウン リストから [インスタンス] を選択し、[OK] をクリックします。

選択したサーバの新しい AIM インスタンスが追加されます。

これで、AIM サーバ上の AIM は指定されたゾーン サーバからデータを収集するように設定されました。 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、Solaris ゾーン環境の管理を開始できます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

[管理] - [設定] でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  (ディスカバリが進行中) が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。ディスカバリにかかる時間は、環境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数によって異なります。アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Virtual Assurance はサーバフォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

〔管理〕 - 〔設定〕 で AIM インスタンスを追加した後、ステータス アイコンに  (ポーリングなし) が表示されます。

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。このアイコンは、CA Virtual Assurance マネージャがこの AIM をポーリングしないこと表します。この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。別の AIM を使用したい場合は、〔管理〕 - 〔設定〕 - 〔プロビジョニング〕 で優先 AIM を設定できます。サーバエントリの〔編集〕をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

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 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:

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。

- 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。

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. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

AIM サーバが 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 AIM サーバを追加します。手順 3 に進みます。

サーバが 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 AIM サーバの名前を入力します。例：

```
192.168.50.51 myAIM
```

4. [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. 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 [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 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、収集したデータがこのシナリオの要件に従っていることを確認してください。

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 AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン  (無効) が表示されます。この 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 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サーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

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。

- 欠落しているサーバから CA Virtual Assurance マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、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 Solaris ゾーン グループの確認

設定および検出に成功すると、新たに検出されたリソースが [リソース] - [エクスプローラ] ペインの対応するグループに表示されます。

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] ペインを開きます。
2. Solaris ゾーン グループを展開します。

管理対象の Solaris ゾーン リソースが表示されます。

CA Virtual Assurance で、設定された Solaris ゾーン環境を管理する準備が整いました。

Solaris ゾーン管理

Solaris ゾーン サーバは、ゾーンによって隔離された環境でアプリケーションを実行することで、各アプリケーションが物理的に別々のコンピュータ上で実行されているように見せることができます。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。

このセクションでは、Solaris ゾーンのリソースに対して [リソース] ページから実行できる管理操作について説明します。[リソース] ページでは、以下のオブジェクトに関する基本情報と詳細情報を表示できます。

- Solaris ゾーン サーバ
- Solaris ゾーン

[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。次に、いずれか 1 つのリソースを選択し、そのリソースの [サマリ] をクリックします。[サマリ] ページでは、リソースに関連付けられている情報 (Solaris ゾーン サーバ上のゾーン、リソース プール、ディスクや、ゾーン上のネットワーク インターフェースとプロジェクトなど)、またはリソースに関連付けられているイベントを見ることができます。

注: [使用方法] パネルの [設定] ボタンを使ってアラートを [正常] として選択すると、CPU またはメモリが重大または警告の状態になった場合でも、ゾーンは正常状態 (緑色) で表示されます。同様に、アラートを [警告] として選択すると、ゾーンは常に警告状態で表示されます。

コンポーネント ツリーには、ゾーンによって使用されるリソース プールだけが表示されます。非アクティブなリソース プールは、このパネルに一覧表示されません。

[詳細] ページでは、リソースの他の詳細情報 (システム プロパティ、ソフトウェア、ハードウェア、パフォーマンスなど) を見ることができます。

リソース管理タスクを実行するための、他のページが表示される場合もあります。[エクスプローラ] ペインのメニューを右クリックすると、管理とポリシーのタスクを実行することもできます。

関連項目

[リソース プールの作成](#) (P. 567)

[ゾーン ステータスの制御](#) (P. 568)

[ゾーンのクローン作成](#) (P. 570)

[ゾーンの削除](#) (P. 571)

[利用可能な Solaris ゾーン アクション](#) (P. 571)

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]、[ルート全体]、[ブランド化] のどれ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時、ゾーンを自動的に再起動するかどうかを定義します。

リソース プールの作成

Solaris ゾーン サーバ上のゾーン、プロジェクト、およびアプリケーションにリソースを割り当てるときに使用するリソース プールは作成することができます。作成したリソース プールは、ゾーン作成中にゾーンに割り当てることができます。

リソース プールを作成する方法

1. [エクスプローラ] ペインで Solaris ゾーン サーバを右クリックし、[管理]、[リソース プールの作成] を選択します。
[リソース プールの作成] ダイアログ ボックスが表示されます。
2. 以下のフィールドに入力し、[OK] をクリックします。

名前

リソース プールの名前を指定します。

最小 CPU 共有

プールにとって常に必要な CPU 共有の最小数を指定します。

最大 CPU 共有

プールで利用できる CPU 共有の最大数を指定します。

プロセッサ設定名

プールのプロセッサ設定名を指定します。

スケジューラタイプ

リソースの割り当て時に使用するスケジューリングのタイプを指定します。作業負荷の重要度（プロジェクトまたはタスクについて指定された CPU 共有の数）に基づいてリソースを割り当てるためにフェア シェア スケジューリングを使用するには、[FSS - フェア シェア スケジュール] を選択します。

プールが作成され、確認のメッセージが表示されます。

3. プールを作成したゾーン サーバの [サマリ] タブをクリックし、[表示] ドロップダウン リストから [リソース プール] を選択して、プールが作成されたことを確認します。

ゾーン ステータスの制御

ゾーンのステータスを制御するために、停止、再起動、開始、およびアンインストールの操作を実行することができます。これらの操作を、グローバルゾーンまたはインストールされた状態のゾーンに対して実行することはできません。

ゾーン ステータスを制御する方法

1. [エクスプローラ] ペインでゾーンを右クリックし、[管理] および以下のいずれかのオプションを選択します。

開始

ゾーンを開始し、実行状態に置きます。インストールされた状態のゾーンのみ開始できます。

停止

インストールされた状態にリセットすることで、ゾーンを停止します。ゾーンを停止すると、すべてのプロセスが停止し、ネットワーク インターフェースが削除されます。また、ゾーンの既存のアプリケーション環境と仮想プラットフォームを削除するための他の操作が実行されます。ゾーンを停止した後は、同じゾーンを開始して環境を再初期化する必要があります。現在実行されているゾーンのみ停止できます。

再起動

ゾーンを停止し、再起動します。現在実行されているゾーンのみ再起動できます。ゾーンを再起動すると、サーバによって新しいゾーン ID が割り当てられます。

削除

ゾーンを削除します。詳細については、「ゾーンの削除」を参照してください。

インストール

ネイティブまたはブランド化のゾーンをインストールします。インストールが完了すると、ゾーンは設定された状態に入ります。ゾーンをインストールするときは、ブランド化ゾーンのアーカイブパスを求めるダイアログボックスが開きます。ネイティブゾーンをインストールする場合は、このフィールドを空のままにします。ブランド化ゾーンの場合には、アーカイブパスを入力します。

注: アーカイブ パス パラメータを入力しないでブランド化ゾーンをインストールしようとしたり、アーカイブ パス パラメータを入力してネイティブ ゾーンをインストールしようとしたりすると、エラー メッセージが表示されます。

アンインストール

ゾーンのルート ファイル システム下にあるファイルをすべてアンインストールします。現在実行されていない（インストールされた状態）ゾーンのみアンインストールできます。ゾーンを削除するには、事前にゾーンをアンインストールする必要があります。

クローン

ゾーンのクローンを作成します。詳細については、「ゾーンのクローン作成」を参照してください。

確認ダイアログ ボックスが開きます。

2. [OK] をクリックします。

要求がサブミットされたことを確認するメッセージが表示されます。

3. ゾーン ホストの [サマリ] タブをクリックします。

操作の結果を確認するイベントが表示されます。

注: 現在の操作が進行中で、まだ完了していない場合、ゾーン ステータスは未完了と表示されます。

関連項目

[ゾーンの削除](#) (P. 571)

[ゾーンのクローン作成](#) (P. 570)

ゾーンのクローン作成

ゾーンのクローン作成では、既存のゾーンからデータをコピーすることで、新しいゾーンを設定およびインストールできます。クローン作成の対象となるゾーンは、クローン操作を行えるように停止する必要があります。この操作を、グローバルゾーンや、設定された状態または実行中の状態にあるゾーンに対して実行することはできません。

ゾーンのクローンを作成する方法

1. [エクスプローラ] ペインでゾーンを右クリックし、[管理]-[クローン] を選択します。

[クローン作成] ペインが表示されます。

2. [ターゲット] ペインの以下のフィールドに入力し、[クローン] をクリックします。

名前

クローン作成される情報のコピー先となるゾーンの名前を指定します。

パス

クローン作成される情報のコピー先となるゾーンのファイルパスを指定します。

確認メッセージが表示されます。

3. ゾーンホストの [サマリ] タブをクリックします。

操作の結果を確認するイベントが、ダッシュボードに表示されます。操作が完了すると、クローン作成されたゾーンは、その親ホストの [エクスプローラ] ペインに表示されます。

ゾーンの削除

グローバル ゾーン以外のゾーンは Solaris ゾーン サーバから削除できます。ゾーンを削除するには、事前にゾーンをシャット ダウンする必要があります。

インストールされた状態のゾーンに対して削除操作を実行すると、ゾーンは最初にアンインストールされてから削除されます。他の状態にある（実行中など）ゾーンに対して削除操作を実行すると、エラー メッセージが表示されます。

ゾーンを削除する方法

1. [エクスプローラ] ペインでゾーンを右クリックし、[管理]、[削除] を選択します。

確認ダイアログ ボックスが開きます。

2. [OK] をクリックします。

削除を確認するメッセージが表示されます。

3. ゾーンホストの [サマリ] タブをクリックします。

操作の結果を確認するイベントが表示されます。操作が完了すると、削除したゾーンは[エクスプローラ]ペインに表示されなくなります。

利用可能な Solaris ゾーン アクション

Solaris ゾーンで利用できるアクション タイプを以下に示します。

- [ゾーン マシンのクローン作成](#) (P. 785)
- [ゾーン マシンの削除](#) (P. 820)
- [ゾーン マシンのプロビジョニング](#) (P. 854)

このようなアクション タイプを使用して、割り当てたルール条件が満たされたときにゾーン操作を自動化する新しいアクションを作成できます。また、これらのアクションが特定の時間に実行されるようにスケジュールすることもできます。

アクションとルールを使って自動化ポリシーを作成する方法の詳細については、「ポリシー」の章を参照してください。

VMware vCloud

VMware vCloud Director では、仮想インフラストラクチャ リソースを仮想データ センターへプールして、ユーザにそれらを公開することにより、安全なマルチテナント クラウドを構築できます。**CA Virtual Assurance** では **VMware vCloud Director** の管理をサポートしています。

vCloud Director のリソースは、仮想マシンを実行するための **CPU**、メモリ、ストレージ、**vNetwork** 分散スイッチなどの **vSphere** リソースの基盤によって異なります。これらの基盤となる **vSphere** リソースを使用して、**vCloud** で仮想マシンと **vApp** を作成できます。

vCloud 組織は、ユーザ、グループ、および計算リソースのコレクションを表す管理の 1 単位です。対応する仮想データセンターは必要な計算リソースを提供します。ユーザは組織レベルでの認証後、仮想マシンまたは **vApp** を作成、使用、管理できます。

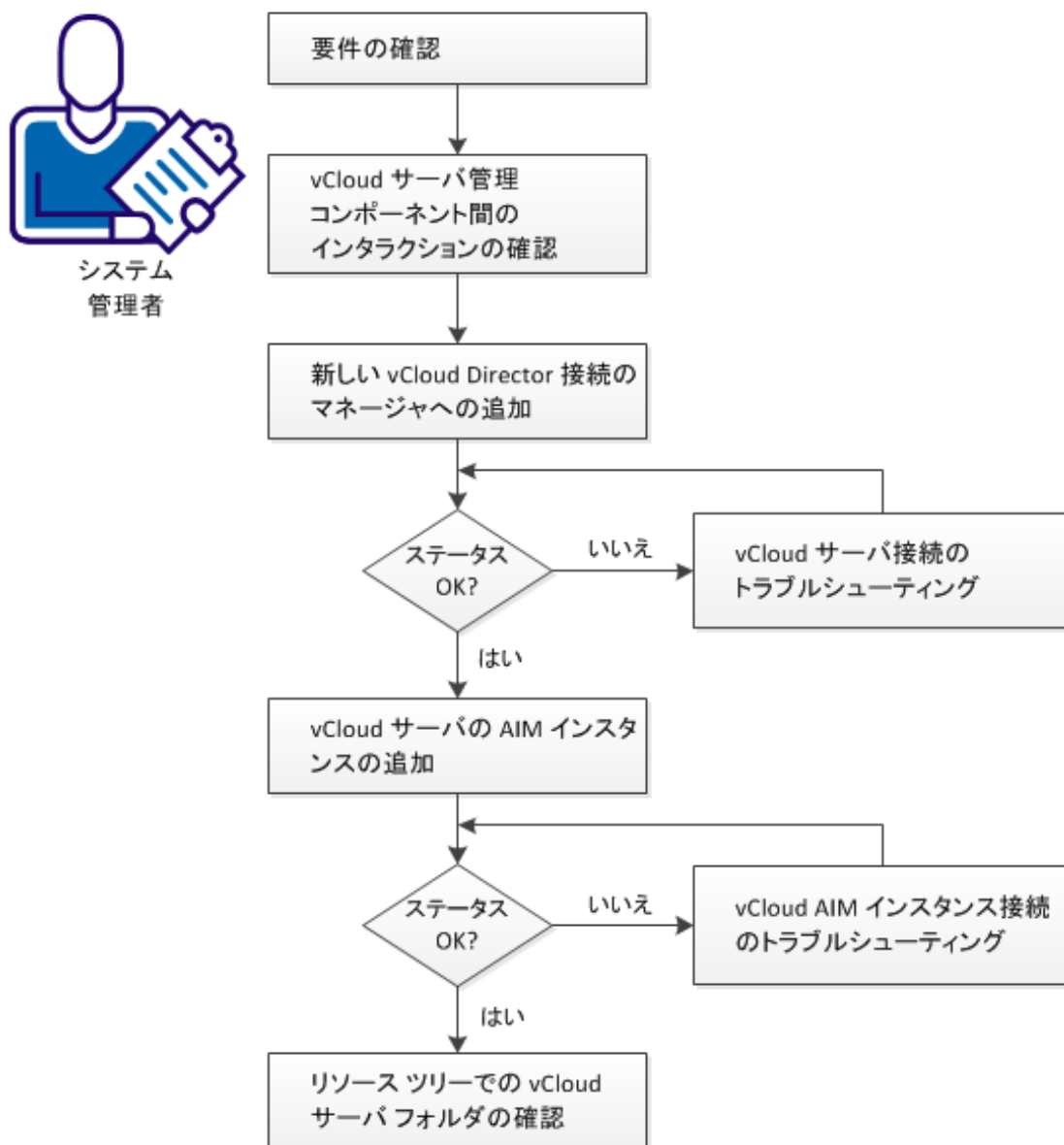
仮想データセンター (vDC) は、**vCloud 組織**に仮想計算リソースを提供します。仮想システムのプロビジョニング、実行、および仮想データセンターへの格納を行えます。**vCloud 組織**は複数の仮想データセンターを持つことができます。

組織は、**vApp** テンプレートおよびメディア ファイルを格納するためにカタログを提供します。組織のメンバは、独自の **vApp** を作成するためにカタログで **vApp** テンプレートおよびメディア ファイルを使用できます。

vCloud Director 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。

vCloud サーバ管理コンポーネントを設定する方法



以下の手順に従います。

[vCloud の要件の確認 \(P. 574\)](#)
[vCloud 管理コンポーネント間のインタラクション \(P. 576\)](#)
[vCloud Director 接続のマネージャへの追加 \(P. 578\)](#)
[vCloud サーバ接続のトラブルシューティング \(P. 579\)](#)
[vCloud サーバ接続の失敗 \(P. 580\)](#)
[vCloud サーバの AIM インスタンスの追加 \(P. 582\)](#)
[vCloud AIM インスタンス接続のトラブルシューティング \(P. 584\)](#)
[リソース ツリーでの VMware vCloud フォルダの確認 \(P. 589\)](#)

vCloud の要件の確認

CA Virtual Assurance の vCloud Director 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、VMware vSphere、および VMware vCloud に関する基礎知識がある。
- VMware プラットフォーム管理モジュール (PMM)、vCloud 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 vCloud Director サーバ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 vCloud Director 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
- vSphere 環境とその vCloud Director が正しく実行されることを確認済みである。
- VMware PMM と vCloud 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 vCloud 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。

関連項目：

[vCloud Director 接続のマネージャへの追加](#) (P. 578)

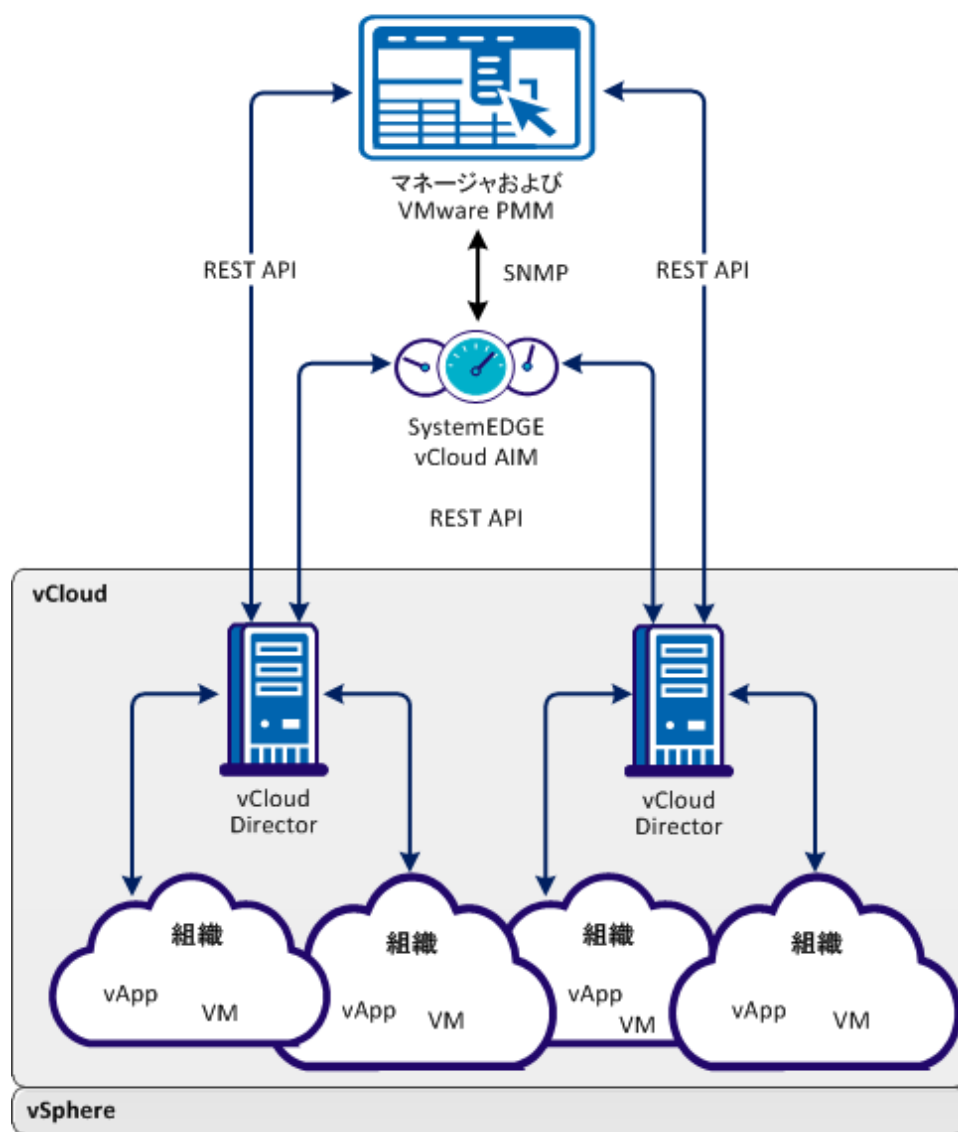
[vCloud サーバの AIM インスタンスの追加](#) (P. 582)

[リソース ツリーでの VMware vCloud フォルダの確認](#) (P. 589)

vCloud 管理コンポーネント間のインタラクション

以下の図は、vCloud Director 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 vCloud AIM は、同じ Windows サーバ上で実行します。この AIM は、1 つ以上のリモート vCloud Director サーバと通信して、仮想環境を管理します。vCloud AIM はデータを収集し、vCloud Director と関連付けられている仮想リソースをすべて表示します。基盤となる vSphere 環境は、仮想マシンおよび vApp を実行するためのリソースを提供します。

vCloud Director 管理コンポーネント間のインタラクション



vCloud の管理は、ユーザ インターフェースの [管理] タブで設定できます。

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。

vCloud Director 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、vCloud Director 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 [vCloud サーバ] 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 vCloud サーバ、関連付けられている vCloud AIM サーバ、および vCloud サーバ AIM インスタンスが表示されます。

3. [vCloud サーバ] ペイン ツールバーの  (追加) をクリックします。

[vCloud サーバの追加] ダイアログ ボックスが表示されます。

4. 必要な接続データ (サーバ名、ユーザ名、パスワード、プロトコル、ポート) を入力し、優先 AIM を指定し、[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。

ユーザ名を指定するときには、ユーザ役割およびアクセス レベルを考慮するために以下の構文を使用できます。

- システム管理者 (フルアクセス) : `administrator@System`
- 組織レベルおよび役割の割り当ての操作に制限 (組織によるアクセス) : `username@organization_name`

ネットワーク接続が正常に確立されている場合、右上の [vCloud サーバ] ペインに vCloud サーバが緑のステータス アイコンを使って追加されます。 **CA Virtual Assurance** によって vCloud サーバ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 vCloud サーバが赤のステータス 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、[「vCloud サーバ接続のトラブルシューティング \(P. 579\)」](#) を参照してください。

関連項目:

[vCloud サーバの AIM インスタンスの追加 \(P. 582\)](#)

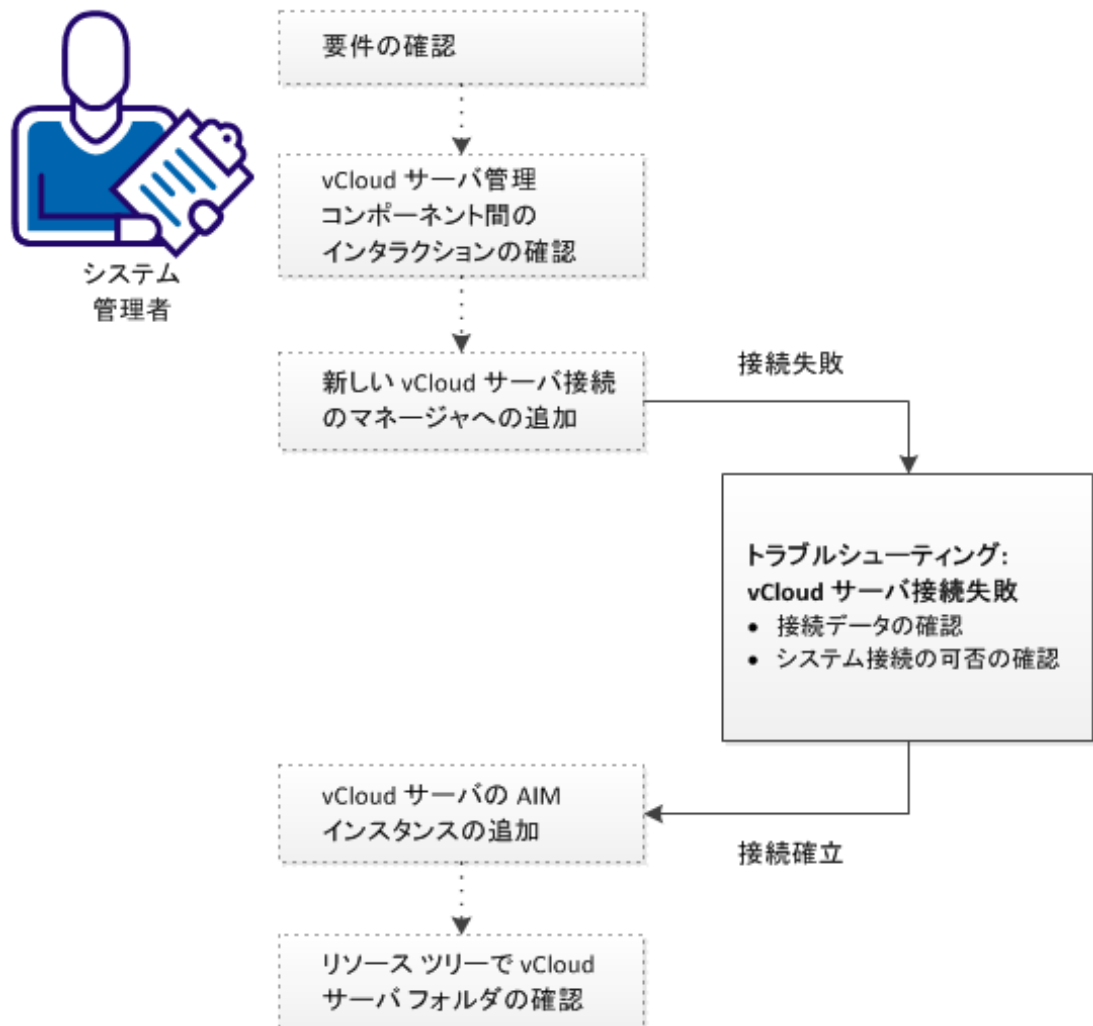
[リソース ツリーでの VMware vCloud フォルダの確認 \(P. 589\)](#)

[vCloud サーバ接続のトラブルシューティング \(P. 579\)](#)

vCloud サーバ接続のトラブルシューティング

vCloud サーバ接続に失敗しました。以下の図に示すトラブルシューティング情報に従ってください。

vCloud サーバ接続のトラブルシューティング方法



以下の手順に従います。

[vCloud サーバ接続の失敗 \(P. 580\)](#)

[vCloud サーバの AIM インスタンスの追加 \(P. 582\)](#)

[リソース ツリーでの VMware vCloud フォルダの確認 \(P. 589\)](#)

vCloud サーバ接続の失敗

症状:

[管理] - [設定] で新しい vCloud サーバ接続を追加した後、vCloud サーバ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。

- vCloud サーバの接続に使用したデータ（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。
- vCloud サーバ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。

vCloud サーバ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。

[vCloud サーバの追加] または [vCloud サーバの編集] 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。優先 AIM を指定します。[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。

vCloud サーバへの接続を確立できない場合は、次の手順に進みます。

vCloud サーバ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 <vCloud Server Name>  
ping <IP Address of vCloud Server>
```

2. vCloud 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。

vCloud サーバが 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 vCloud サーバを追加します。手順 3 に進みます。

vCloud サーバが 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 <vCloud Server Name>
```

正しい IP アドレスと vCloud サーバの名前を入力します。例：

```
192.168.50.50 myvCloud
```

4. 右上角の  (検証) をクリックします。

vCloud サーバ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。

vCloud の管理者または VMware のサポート担当者と協力して、vCloud サーバの接続の問題を解決します。

vCloud サーバの AIM インスタンスの追加

CA Virtual Assurance マネージャに新しい vCloud サーバ接続を追加した後、新しい vCloud サーバを管理するための vCloud AIM インスタンスを追加します。その後、組織、vApp、VM など、そのすべての仮想コンポーネントを含む vCloud 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 [vCloud サーバ] 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 vCloud サーバ、関連付けられている vCloud AIM サーバ、および管理対象の vCloud サーバの AIM インスタンスが表示されます。

3. [vCloud AIM サーバ] ペイン ツールバーの  (追加) をクリックします。

[vCloud AIM サーバの追加] ダイアログ ボックスが表示されます。

4. [vCloud AIM サーバ] ドロップダウン リストを開きます。

検出された vCloud AIM サーバのリストが表示されます。vCloud 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 vCloud AIM サーバを選択します。

[vCloud サーバ] ペインに一覧表示された vCloud サーバが [vCloud サーバ] 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 vCloud サーバは、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 vCloud サーバを選択し、[OK] をクリックします。

選択した vCloud サーバの新しい 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 vCloud 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、vCloud の仮想リソースの管理を開始できます。

関連項目:

[リソース ツリーでの VMware vCloud フォルダの確認 \(P. 589\)](#)

[vCloud AIM インスタンス接続のトラブルシューティング \(P. 584\)](#)

vCloud AIM インスタンス接続のトラブルシューティング

vCloud 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。

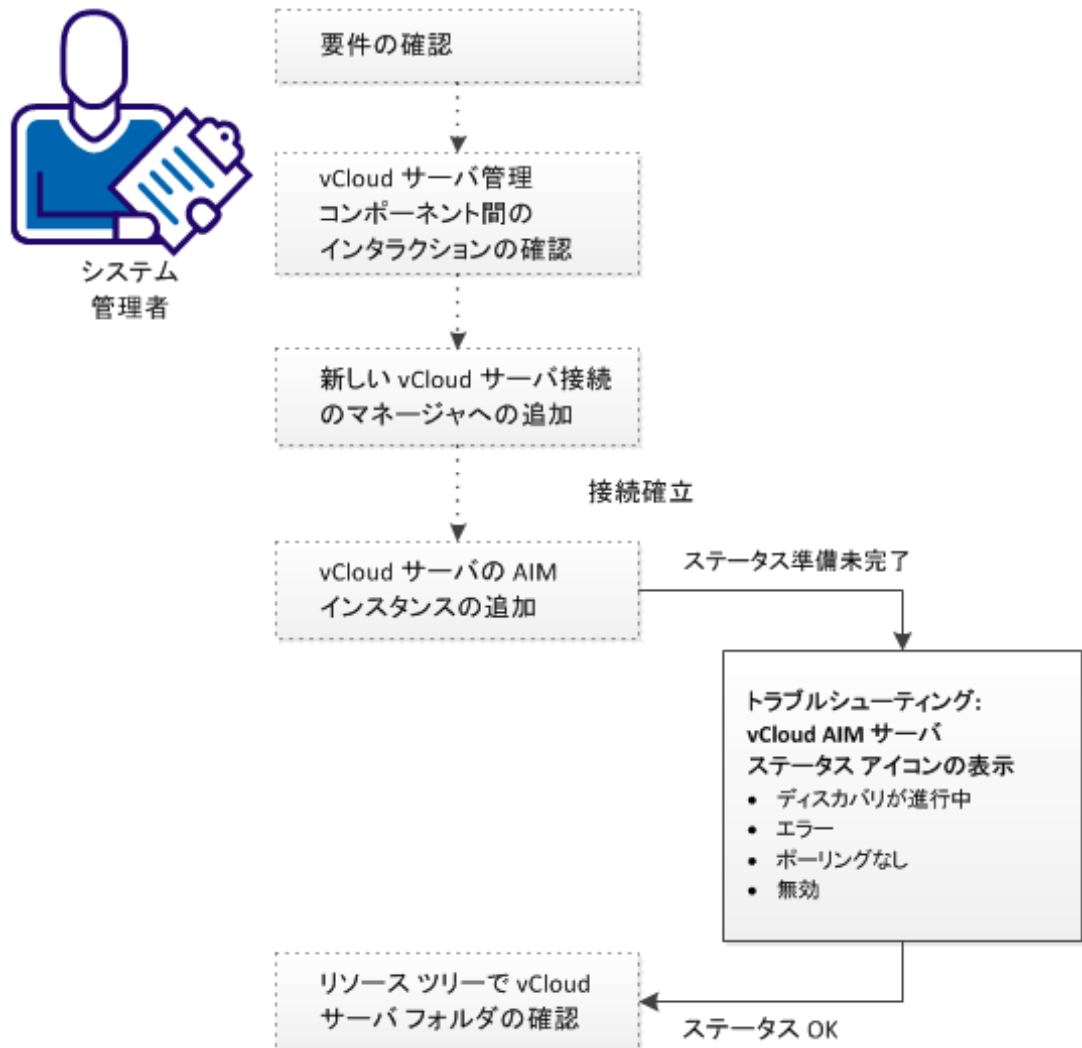
 エラー - AIM に接続できません。 ネットワーク接続を確認してください。

 ポーリングなし - CA Virtual Assurance マネージャはこの AIM インスタンスをポーリングしません。

 無効 - このインスタンスは管理されていません。

以下の図に示すトラブルシューティング情報に従ってください。

vCloud AIM インスタンス接続のトラブルシューティング方法



関連項目:

[vCloud AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される \(P. 586\)](#)

[vCloud 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 \(P. 586\)](#)

[vCloud AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される \(P. 588\)](#)

[vCloud 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 \(P. 588\)](#)

vCloud AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

〔管理〕 - 〔設定〕 で vCloud サーバに対して vCloud AIM インスタンスを追加した後、ステータス アイコンに  (ディスカバリが進行中) が表示されます。

解決方法:

vCloud 環境のディスカバリ プロセスが完了するまで待機します。ディスカバリにかかる時間は、vCloud 内の仮想リソースに関連する管理対象オブジェクトの数によって異なります。アイコンの上にカーソルを置くと、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Virtual Assurance は vCloud サーバ フォルダをリソース ツリーに追加します。これで、vCloud 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。

vCloud 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 vCloud サーバに対して vCloud 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:

vCloud 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。

- vCloud 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。

vCloud 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. vCloud 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。

vCloud AIM サーバが 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 vCloud AIM サーバを追加します。手順 3 に進みます。

vCloud サーバが 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 vCloud AIM サーバの名前を入力します。例：

```
192.168.50.51 myvCloudAIM
```

4. [vCloud 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. vCloud 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 [vCloud 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 vCloud 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。

vCloud AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

[管理] - [設定] で vCloud Director に対して vCloud AIM インスタンスを追加した後、ステータス アイコンに  (ポーリングなし) が表示されます。

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。このアイコンは、CA Virtual Assurance マネージャがこの AIM をポーリングしないこと表します。この AIM は優先 AIM ではありません。

特定の vCloud Director を管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。別の AIM を使用したい場合は、[管理] - [設定] - [プロビジョニング] で優先 AIM を設定できます。サーバエントリの [編集] をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

vCloud 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 vCloud AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン  (無効) が表示されます。この vCloud 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 vCloud 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 vCloud サーバ用に vCloud AIM が設定されている。
- [vCloud サーバ] ペインで設定されていない vCloud サーバに 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 vCloud サーバから CA Virtual Assurance マネージャへの接続を追加します。
- 既存の vCloud サーバ接続を編集し、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 VMware vCloud フォルダの確認

新しい vCloud サーバは、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 vCloud] 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 vCloud] を展開します。

管理対象の vCloud Director サーバが表示されます。

3. 新しい vCloud Director サーバ エントリを展開します。

管理対象の vCloud インフラストラクチャが表示されます (組織、vApp、VM など)。

CA Virtual Assurance で、追加された vCloud 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。

リモートおよびマルチインスタンスの vCloud Director のサポート

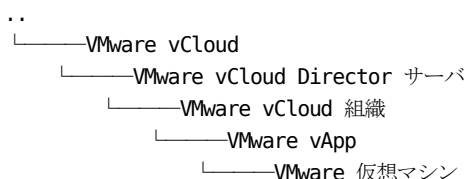
vCloud AIM は 1 つ以上のリモート vCloud Director インスタンスと通信します。ただし、複数のリモート vCloud AIM を持つ CA Virtual Assurance マネージャを使用して複数の vCloud Director 環境を管理する場合は、以下を考慮してください。

それぞれの vCloud Director は、設定時に指定した優先 vCloud AIM の 1 つと一意に関連付けられます。優先 AIM の設定は、複数の AIM で 1 つの vCloud Director を管理する場合に、どの AIM をポーリングに使用するかを示します。

vCloud のフォルダ構造

vCloud Director サーバへの接続が正しく設定されると、CA Virtual Assurance によって、組織、vApp、および仮想マシンから構成される vCloud Director 環境が検出されます。ディスカバリが完了すると、VMware vCloud フォルダが [リソース] タブの [エクスプローラ] ペインに表示されます。フォルダを展開して、vCloud 環境を管理することができます。

以下の図は、VMware vCloud フォルダの下のオブジェクト階層を表しています。



VMware vCloud フォルダは、最上位のサービス レベルを表します。vCloud サービスは、複数の VMware vCloud Director サーバで構成できます。それぞれの vCloud Director には、通常は vApp と仮想マシンを持つ複数の組織があります。

組織レベルでは、カタログに保存されたテンプレートに基づいて vApp をプロビジョニングできます。

vCloud での vApp のサポート

vApp の概念は、vCloud 環境と vSphere 環境で類似しています。どちらも、単一のエンティティとして操作できるアプリケーション オブジェクトを表しています。通常、vApp には複数の VM が含まれています。それぞれの VM には、エンドユーザに提供する vApp アプリケーションまたはサービスを実行するという独自の目的があります。vApp で実行される操作は、vApp のすべての VM でも実行されます。たとえばどちらのタイプも、vApp 内のすべての VM の起動および停止順序を定義し、vApp 内のすべての VM が使用できる CPU とメモリのリソース制限を定義します。

vCloud 内の vApp の目的は、アプリケーションまたはサービスをテンプレートとして 1 度定義して、組織カタログによってそれを複数の組織からアクセスできるようにすることです。vCloud はデータを vCloud データベースに保存します。これは vCenter Server データベースとは異なります。

重要: vCloud で定義した VM を vCenter Server から直接操作しないでください。この操作によって、vCloud データベースが実際に定義された VM と同期できなくなる場合があります。CA Virtual Assurance は、データベースが非同期にならないように、vCloud および vCenter Server の下に表示される VM に対する操作を制限しています。

vCloud vApp と vSphere vApp の相違点

- vCloud vApp には、ネスト階層のための機能がありません。vSphere vApp にはほかの vApp およびリソース プールを含めることができます。
- vCloud では、CPU とメモリのリソース制限は仮想データセンター (vDC) によって定義されます。また、vApp はこれらの仮想データセンターのいずれかにマップされます。

vSphere では、vApp のリソース制限は vApp 自体によって定義されます。

- vCloud vApp には、さまざまな vCenter Server および ESX ホストで定義された VM を含めることができます。

vSphere vApp の VM は、特定のデータセンターおよびクラスタの VM に制限されています。

- vCloud vApp はリース制限があります。vApp のランタイムとストレージの制限を定義できます。ランタイム制限に到達すると、vCloud vApp は使用できなくなります。ストレージ制限に到達すると、vApp は組織のリース ポリシーに応じて vCloud から削除されるか、期限切れ項目フォルダに移動されます。

vSphere vApp は、ユーザが手動で削除するまで残ります。

- vCloud vApp は vApp テンプレートから作成されます。vApp テンプレートは、vCenter Server から VM をインポートするか、OVF パッケージをインポートすることで作成されます。vApp は、テンプレートを作成した組織のクラウドにテンプレートを展開することによって作成されます。展開後、その他の VM は vApp へ移動させることができます。

vSphere vApp は、CPU とメモリのリソースに必要な制限を加えて vApp を定義することで作成されます。その後、vApp が定義されたデータセンター用の VM は、vApp へ移動させることができます。

vCloud のリソース プール プロバイダとしての vCenter Server

vCenter Server の役割を設定して、vCloud のリソース プール プロバイダとして機能させることができます。この場合、vCenter Server は、vCloud が VM を作成するための計算リソースとメモリ リソースを提供します。このリソース プールは、プロバイダ vDC として vCloud に表示されます。

この設定によって、このリソース プールの VM が、vCenter オブジェクト階層および vCloud オブジェクト階層の CA Virtual Assurance [エクスプローラ] ペインに表示されます。そのような VM の [サマリ] パネルの vCloud の下には、vCenter Server の下に表示されるのと同じ情報が表示されます。

- パフォーマンス チャート
- 一般情報
- 概要 (モニタ対象リソースのステータス情報)
- CPU とメモリの使用率 (しきい値の設定は vCenter Server のみでサポートされます)
- ディスク使用率

これらの VM に適用できる操作セットは、vCloud および vCenter Server 環境の両方で制限されます。操作セットを制限することで、vCenter と vCloud が同期されない問題を回避できます。たとえば、その VM の親 vApp が vCloud で実行中の場合、vCenter Server 下の VM の電源はオフにできません。そのような VM の電源をオフにするには、最初に vCloud 内の vApp の電源をオフにします。

有効な VM 操作を以下に示します。

- モニタリング ソフトウェアの展開
- 自動化ルール管理
- サーバメトリック収集の設定
- しきい値の設定

VM が作成された vCloud に vCenter Server への接続がない場合、[サマリ] ペインには以下の情報のみが表示されます。

- アイテム タイプ
- 名前
- 稼働ステータス

vCloud 組織

vCloud 組織は、ユーザ、グループ、および計算リソースのコレクションに対する管理の 1 単位です。組織は、vApp テンプレートおよびメディア ファイルを格納するためにカタログを提供します。組織のメンバは、独自の vApp を作成するためにカタログで vApp テンプレートおよびメディア ファイルを使用できます。

仮想データセンター (vDC) は、vCloud 組織に仮想計算リソースを提供します。仮想システムのプロビジョニング、実行、および仮想データセンターへの格納を行えます。vCloud 組織は複数の仮想データセンターを持つことができます。

テンプレートからの vApp のプロビジョニング

vCloud 組織のレベルでは、カタログに保存されるテンプレートから vApp をプロビジョニングできます。

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. VMware vCloud フォルダを展開します。
vCloud フォルダの構造が表示されます。
4. 組織オブジェクトを右クリックします。
[プロビジョニング] ポップアップメニューが表示されます。
5. [テンプレートからの vApp のプロビジョニング] をクリックします。
[テンプレートからの新規 vApp のプロビジョニング] ダイアログボックスが表示されます。
6. [名前]、[vApp テンプレート]、[展開リリース]、および [ストレージリリース] を指定します。[OK] をクリックします。

CA Virtual Assurance によって組織内に vApp が作成されます。

vCloud の vApp に対する操作

vCloud 組織のレベルでは、カタログに保存されるテンプレートから vApp をプロビジョニングできます。

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. VMware vCloud フォルダを展開します。
vCloud フォルダの構造が表示されます。
4. vApp オブジェクトを右クリックします。
[管理] ポップアップメニューが表示されます。
5. 以下のいずれかの操作を選択します。

vApp の電源オン

vCloud vApp の電源をオンにします。

vApp の電源オフ

vCloud vApp の電源をオフにします。

vApp のリセット

vCloud vApp をリセットします。

vApp の中断

vCloud vApp を中断します。

vApp の再開

vCloud vApp を再開します。

vApp のクローン作成

既存の vApp から vCloud vApp を作成します。

vApp の移動

vCloud vApp を別の仮想データセンターに移動します。

vApp の削除

vCloud vApp を削除します。

vApp リースの変更

展開およびストレージ リースを変更します。

必要なパラメータ値を指定して、[OK] をクリックします。

6. [イベント] をクリックして、vApp の新規ステータスを確認します。
イベントのリストが表示されます。

VMware vSphere および vCenter Server

CA Virtual Assurance は、VMware vSphere および vCenter Server の仮想環境を管理します。vCenter Server は、vSphere 環境にアクセスするために CA Virtual Assurance および vCenter AIM が使用する主要コンポーネントです。SystemEDGE と vCenter 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。

CA Virtual Assurance 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。マネージャは、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 AIM は、Web サービスを使用して 1 つ以上のリモート vCenter Server インスタンスと通信します。AIM は SNMP を使用してマネージャと通信します。vCenter Server の管理に複数の vCenter AIM を利用できる場合、設定時に任意の vCenter AIM を指定できます。または、マネージャに選択させることもできます。

注: eHealth、Spectrum Infrastructure Manager 環境で CA Virtual Assurance マネージャを使用せずに vCenter 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。

モニタ対象の vSphere および vCenter Server のリソース

vCenter AIM は、vSphere 環境のコンポーネント間の論理的および物理的関係を検出します。AIM は、仮想化された環境全体を視覚化し、以下のリソース タイプやプロパティを管理します。

データセンター

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。

データストア

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。

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。

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。

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。

リソース プール

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。

vApp

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** を使用します。 **Open Virtualization Format (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 上での操作は vApp 内のすべての VM にプロパゲートされます。

vCenter Server

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。

仮想ディスク

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

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。

VMware クラスタ/高可用性/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。

vNetwork Distributed Switch

ホストからデータセンター レベルまでの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。

vNetwork Standard Switch

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。

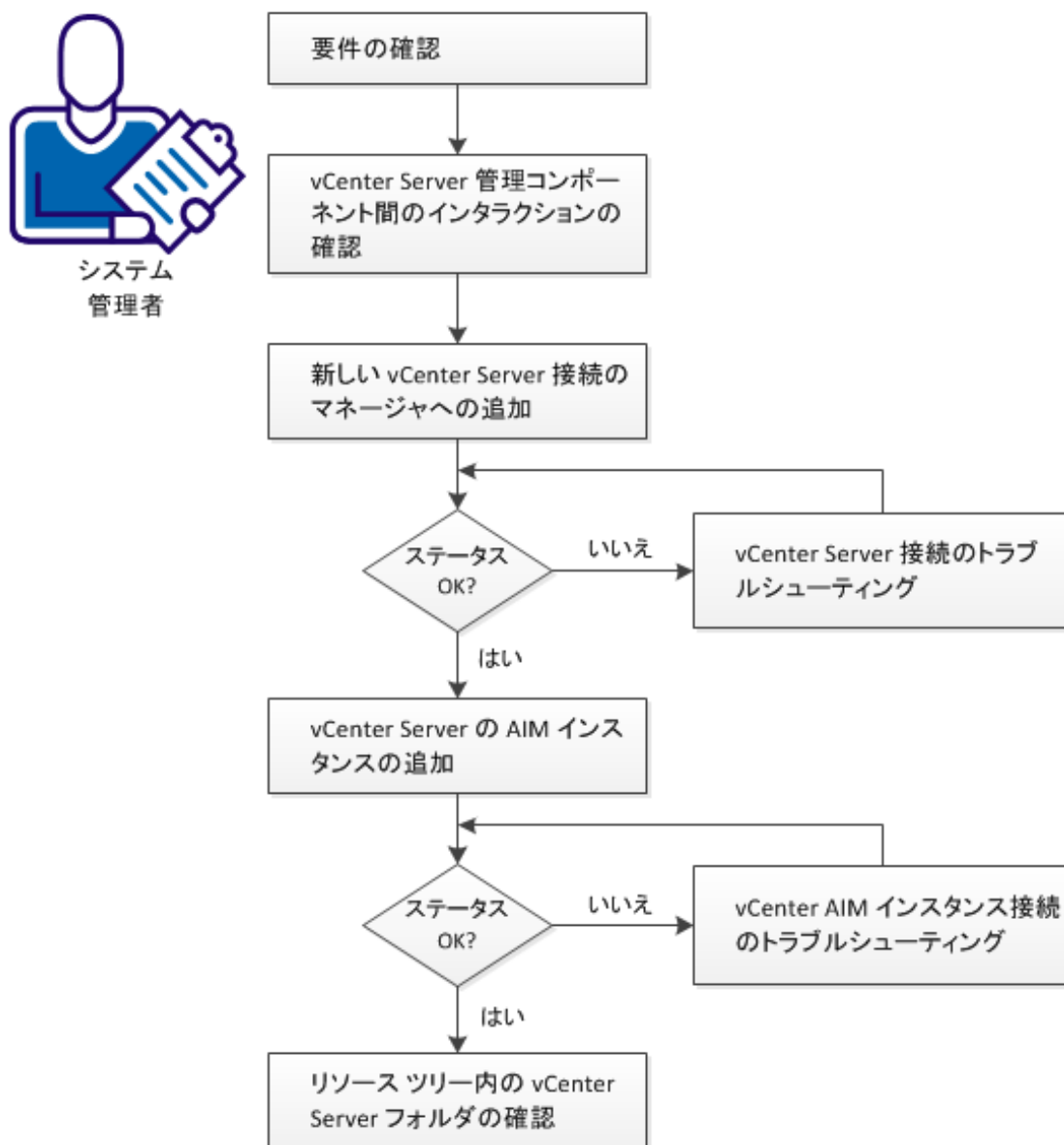
仮想 NIC

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は固有の MAC アドレスと 1 つ以上の IP アドレスを持ち、標準的なイーサネットプロトコルに応答します。

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。

vCenter Server 管理コンポーネントを設定する方法



以下の手順に従います。

[要件の確認 \(P. 600\)](#)

[vCenter Server 管理コンポーネント間のインタラクションの確認 \(P. 601\)](#)

[新しい vCenter Server 接続のマネージャへの追加 \(P. 605\)](#)

[vCenter Server 接続のトラブルシューティング \(P. 606\)](#)

[vCenter Server の AIM インスタンスの追加 \(P. 610\)](#)

[vCenter AIM インスタンス接続のトラブルシューティング \(P. 612\)](#)

[リソース ツリーでの vCenter Server フォルダの表示の確認 \(P. 618\)](#)

要件の確認

CA Virtual Assurance 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。
- VMware 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たことを確認済みである。

関連項目：

[vCenter Server 管理コンポーネント間のインタラクションの確認 \(P. 601\)](#)

[新しい vCenter Server 接続のマネージャへの追加 \(P. 605\)](#)

[vCenter Server の AIM インスタンスの追加 \(P. 610\)](#)

[リソース ツリーでの vCenter Server フォルダの表示の確認 \(P. 618\)](#)

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。

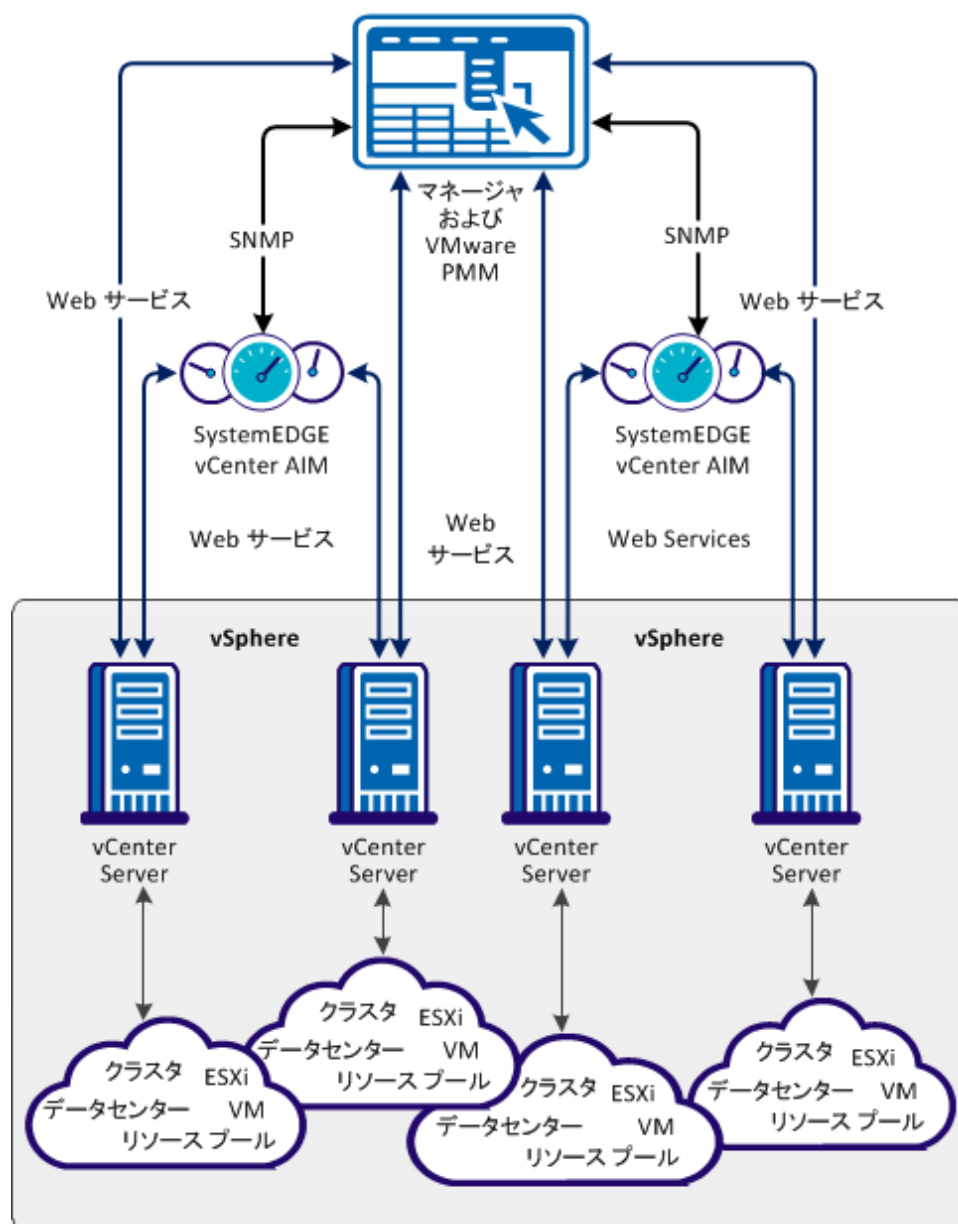
vCenter AIM は、SystemEDGE の機能範囲を拡張する SystemEDGE エージェントプラグインです。vCenter AIM によって SystemEDGE は、複数の vSphere 環境のパフォーマンスをモニタでき、モニタ対象 vSphere リソースの状態を評価できます。一般的なモニタ対象リソースは、仮想 CPU、仮想メモリ、仮想スイッチ、仮想ディスク、リソースプール、vApp、およびその他の仮想リソースです。しきい値に基づき、SystemEDGE および vCenter AIM はモニタ対象リソースのステータスを判断し、その情報を SNMP を使用して CA Virtual 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。検出に成功すると、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 の[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。

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:

[新しい vCenter Server 接続のマネージャへの追加](#) (P. 605)

[vCenter Server の AIM インスタンスの追加](#) (P. 610)

[リソース ツリーでの vCenter Server フォルダの表示の確認](#) (P. 618)

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、優先 AIM を指定し、[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 \(P. 606\)」](#)を参照してください。

関連項目:

[vCenter Server の AIM インスタンスの追加 \(P. 610\)](#)

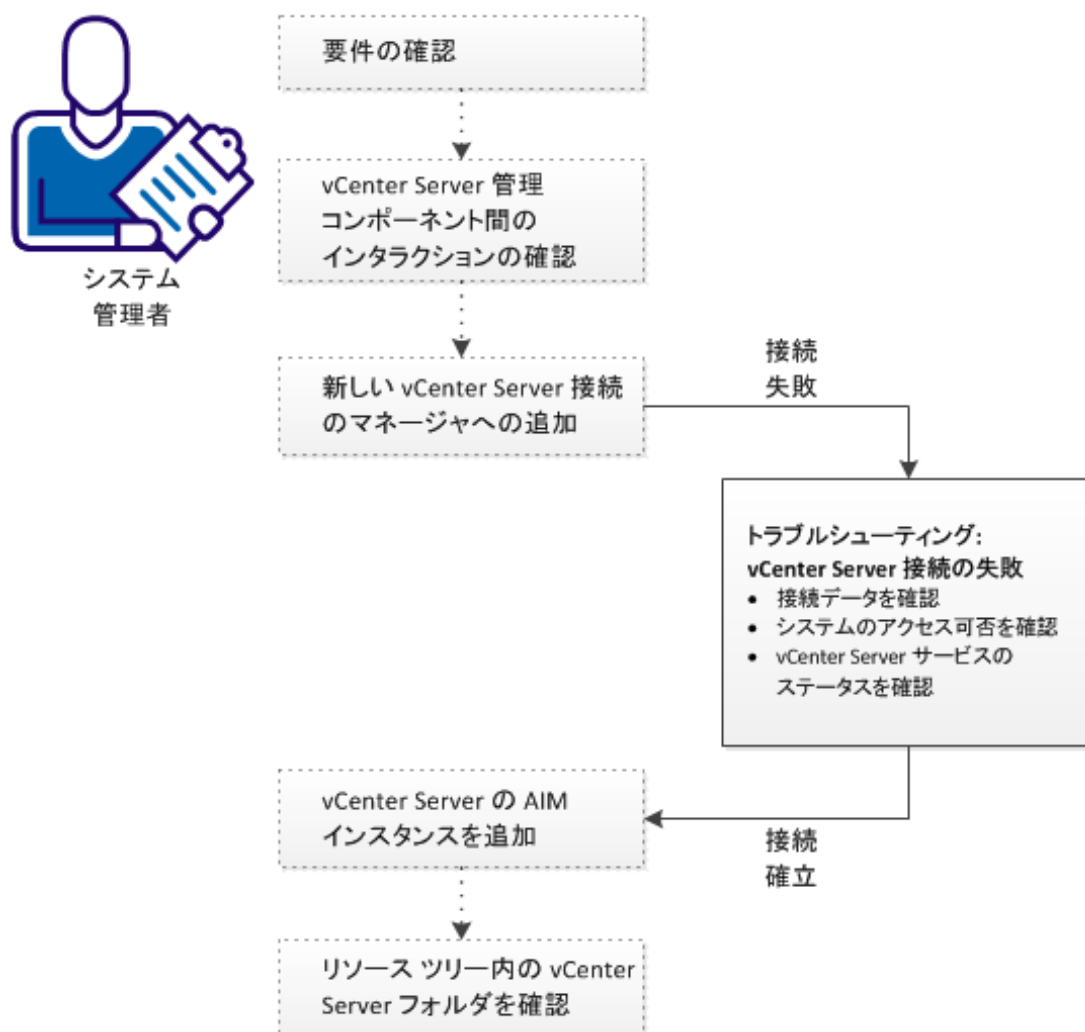
[リソース ツリーでの vCenter Server フォルダの表示の確認 \(P. 618\)](#)

[vCenter Server 接続のトラブルシューティング \(P. 606\)](#)

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。以下の図に示す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



以下の手順に従います。

[vCenter Server の接続に失敗した](#) (P. 607)

[vCenter Server の AIM インスタンスの追加](#) (P. 610)

[リソース ツリーでの vCenter Server フォルダの表示の確認](#) (P. 618)

vCenter Server の接続に失敗した

症状:

「管理」 - 「設定」で 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、その他の仮想コンポーネントなど、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。

関連項目:

[リソース ツリーでの vCenter Server フォルダの表示の確認 \(P. 618\)](#)

[vCenter AIM インスタンス接続のトラブルシューティング \(P. 612\)](#)

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。

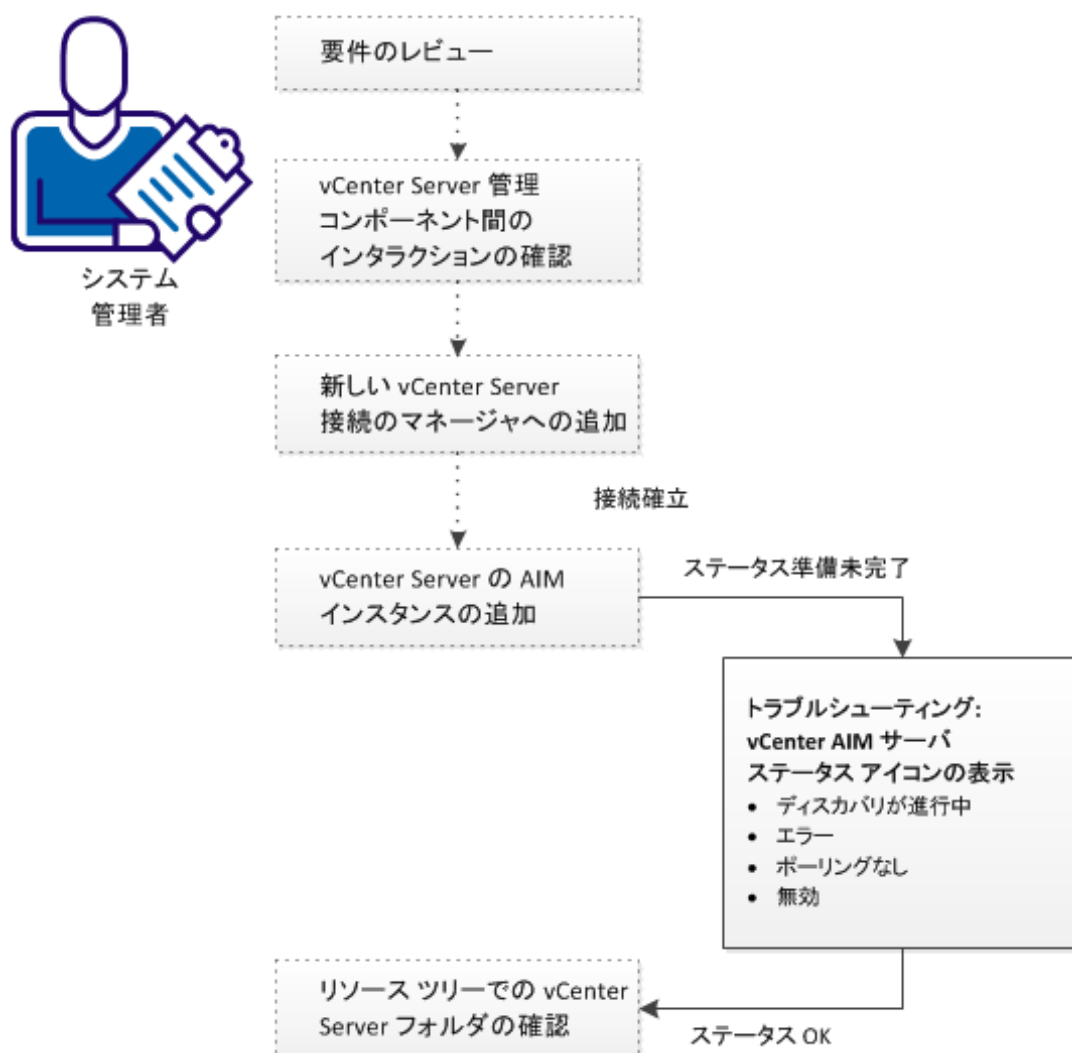
 エラー - AIM に接続できません。 ネットワーク接続を確認してください。

 ポーリングなし - CA Virtual Assurance マネージャはこの AIM インスタンスをポーリングしません。

 無効 - このインスタンスは管理されていません。

以下の図に示す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



関連項目:

[vCenter AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される \(P. 614\)](#)

[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 \(P. 614\)](#)

[vCenter AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される \(P. 616\)](#)

[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 \(P. 616\)](#)

vCenter AIM インスタンスのステータス アイコンに「ディスカバリが進行中」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  (ディスカバリが進行中) が表示されます。

解決方法:

vSphere 環境のディスカバリ プロセスが完了するまで待機します。ディスカバリにかかる時間は、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数によって異なります。アイコンの上にカーソルを置くと、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ 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 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「ポーリングなし」が表示される

症状:

「管理」 - 「設定」 で vCenter Server に対して vCenter AIM インスタンスを追加した後、ステータス アイコンに （ポーリングなし）が表示されます。

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。このアイコンは、CA Virtual Assurance マネージャがこの AIM をポーリングしないこと表します。この AIM は優先 AIM ではありません。

特定の vCenter Server を管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。別の AIM を使用したい場合は、「管理」 - 「設定」 - 「プロビジョニング」 で優先 AIM を設定できます。サーバエントリの「編集」をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

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についてステータス 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「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。

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] フォルダに表示されます。

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。

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、`Install_Path¥productname¥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、
Install_Path¥productname¥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>
```

```
  ...
```

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」ページを参照）。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、完全インストールと適切な vCenter Server 設定に準じています。

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）。

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

仮想ディスクの追加または削除

VM に対して仮想ディスクの動的な追加または削除を行うことができます。以下のディスクを追加できます。

- 同じまたは別のデータストアからの新しいディスク
- データストアからの既存ディスク
- 別のデータストアからの既存ディスクの追加

仮想ディスクを追加する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックするか、[クイック スタート] タブをクリックし、[新しいディスクの追加] を選択します。
[新しいディスクの追加] ダイアログ ボックスが表示されます。
4. 必要に応じて新しいディスクの詳細を入力します。
確認のためのメッセージが表示されます。
5. [OK] をクリックします。
新しいディスクの追加を確認するメッセージが表示されます。

仮想ディスクを削除する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックするか、[クイック スタート] タブをクリックし、[ディスクの削除] を選択します。
[ディスクの削除] ダイアログ ボックスが表示されます。

4. ハードドライブおよびデータを削除するかどうかを選択します。
確認のためのメッセージが表示されます。
5. [OK] をクリックします。
ディスクの削除を確認するメッセージが表示されます。

仮想ネットワーク インターフェースの追加または削除

既存の VM に対して仮想ネットワーク インターフェースの動的な追加または削除を行うことができます。

仮想ネットワーク インターフェースを追加する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックするか、[クイック スタート] タブをクリックし、[新しい仮想ネットワーク インターフェースの追加] を選択します。
[新しい仮想ネットワーク インターフェースの追加] ダイアログ ボックスが表示されます。
4. 新しいネットワーク インターフェースの詳細を入力します。
確認のためのメッセージが表示されます。
5. [OK] をクリックします。
新しいカードの追加を確認するメッセージが表示されます。

仮想ネットワーク インターフェースを削除する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックするか、
[クイック スタート] タブをクリックし、[仮想ネットワーク インターフェースの削除] を選択します。
[仮想ネットワーク インターフェースの削除] ダイアログ ボックスが表示されます。
4. 削除する NIC を選択します。
確認のためのメッセージが表示されます。
5. [OK] をクリックします。
ネットワーク インターフェースの削除を確認するメッセージが表示されます。

仮想マシンに対する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

仮想マシン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。

保護されている

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。

フォールトトレランスのモニタ

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。

フォールトトレランスのプロパティをモニタする方法

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. [VMware vCenter Server] フォルダおよび ESX サーバオブジェクトを展開します。
VM のリストが表示されます。
4. (オプション) ESX ホストを選択します。
[サマリ] タブに以下の FT 属性が表示されます。

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

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

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

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

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。

5. （オプション）VM を選択します。

[サマリ] タブに以下の FT プロパティが表示されます。

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。

保護されている

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。

フォールトトレランスの管理

VM のフォールトトレランスプロパティは制御することができます。

VM のフォールトトレランスプロパティを管理する方法

1. [エクスプローラ] ペインで VM を選択します。

右側に [一般情報] ペインが表示され、VM のフォールトトレランスステータスが示されます。

2. VM を右クリックし、[管理] を選択して、ドロップダウンメニューからアクションを 1 つ選択します。フォールトトレランスの管理に利用できるアクションを以下に示します。

- フォールトトレランスをオフ
- フォールトトレランスの有効化
- フォールトトレランスの無効化
- セカンダリ VM のマイグレート

3. 選択したアクションについて、情報を入力し、内容を確認します。

確認のメッセージが表示されます。

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。

vCPU の動的な追加または削除

プロビジョニングされた VM に対して CPU の動的な追加または削除を行うことができます。ホットプラグが VM に有効な場合、実行時に vCPU を動的に追加できます。

CA Virtual Assurance は以下の VM プロパティを検証します。

- ESX ライセンス (ESX レベル)
- サポートされる最大 vCPU 数 (ESX レベル)
- ホットプラグが有効 (VM レベル)

例

- ESX ライセンスが許可する CPU が 8 個 (Enterprise Plus)、最大サポート vCPU が 8 個、およびホットプラグが無効な場合、1、2、4、8 個の CPU を追加できます。
- ESX ライセンスが許可する CPU が 8 個 (Enterprise Plus)、最大サポート vCPU が 8 個、およびホットプラグが有効な場合、1、2、3、4、5、6、7、8 個の CPU を追加できます。

vCPU を追加する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックするか、[クイック スタート] タブをクリックし、[vCPU の追加/削除] を選択します。
[vCPU の変更] ダイアログ ボックスが表示されます。
4. 必要に応じて CPU の数を調節します。
確認のためのメッセージが表示されます。
5. [OK] をクリックします。
変更を確認するメッセージが表示されます。

注: vCPU を削除するには、仮想マシンをオフにする必要があります。

メモリの動的な追加または削除

プロビジョニングされた **VM** に対してメモリの動的な追加または削除を行うことができます。ホットプラグが **VM** に有効な場合、実行時にメモリを動的に追加できます。

メモリを追加する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックするか、[クイック スタート] タブをクリックし、[メモリの追加/削除] を選択します。
[仮想メモリの変更] ダイアログ ボックスが表示されます。
 4. 必要に応じてメモリの数を調節します。
確認のためのメッセージが表示されます。
 5. [OK] をクリックします。
変更を確認するメッセージが表示されます。
- 注: メモリを削除するには、**VM** をオフにする必要があります。

仮想マシンの論理ボリューム

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。

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ができません。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ができません。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に、すべてのリソースをコミットしないでください。予約する量がすべてのシステム容量の限界に近づく、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るため、予約しない部分が適切に残るように計画してください。
- 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。

VM の CPU およびメモリの割り当ての編集

仮想マシンに割り当てられている CPU 数とメモリ共有を編集して、割り当てられているリソースを調整できます。リソースを追加する場合、適切な量の割り当てられていないメモリと CPU 共有が利用できる必要があります。メモリまたは CPU 共有で許可される最小値および最大値が存在する場合は、リソース割り当ての変更は、これらの制限内で行う必要があります。

特定の VM リソース割り当てアクションを使用して、ポリシーの作成およびスケジュールを行うこともできます。

VM の CPU およびメモリの割り当てを編集する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックし、[設定] - [リソース割り当て] を選択します。
[リソース割り当て] セクションが表示されます。
3. 仮想マシンに割り当てられている CPU の数とメモリ共有を調節し、編集した各値の [保存] をクリックします。
確認メッセージが表示されます。

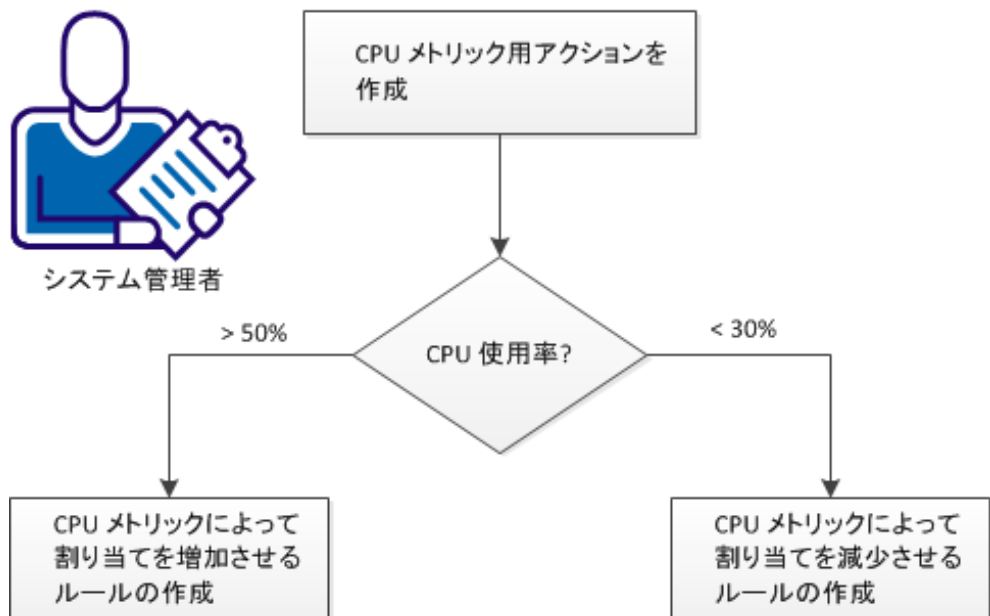
ポリシー アクションを使ってパフォーマンスの問題を特定する方法

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。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を実行できるようにします。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します。

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. 638)
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. 639) 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. 639) 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. 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を作成

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が実行されます。

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、[ポリシー] - [ルール] をクリックします。
2. 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を作成

CPU メトリックによって割り当てを減少させるルールを作成します。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。

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. 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 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。

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** を使用します。**Open Virtualization Format (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** 上での操作は **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。

vApp は、ホストおよびクラスタ レベルに表示されます。

CA Virtual Assurance vApp レベルで以下の管理操作をサポートします。

- 検出
 - サーバ
 - ネットワーク
 - vCenter Server
- サービスのキャプチャ
- 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
- 並べ替え順序の編集

CA Virtual Assurance は、vApp に対する以下のプロビジョニング操作をサポートします。

- VMware VM のプロビジョニング
- VMware vApp のプロビジョニング

VMware vApp のプロビジョニング

vApp は、ESX ホストまたはクラスタ レベルに、または既存のリソース プールまたは vApp の一部として直接作成できます。

次の手順に従ってください:

1. [エクスプローラ] ペインのホストまたはクラスタ レベルから、ESX ホストまたはクラスタを右クリックします。
ポップアップ メニューが表示されます。
2. [プロビジョニング] - [VMware vApp のプロビジョニング] を選択します。
[vApp の新規作成] ダイアログ ボックスが表示されます。
3. 以下のフィールドで値を指定して、[OK] をクリックします。

名前

vApp を識別します。

CPU 共有

親ホスト、リソース プール、または vApp の合計 CPU リソースに関して、この vApp 用の CPU 共有を指定します。親が同じ vApp は、予約と制限によって制約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。適切な相対値を表す共有の数を指定します。

たとえば、ホスト上に vApp1 と vApp2 があり、各々に 1000 CPU 共有が割り当てられていると仮定します。相対値が等しいので、vApp はそれぞれ、親ホストの 50 パーセントの CPU 時間を使用できます。vApp1 に 2000 CPU 共有、vApp2 に 1000 CPU 共有が割り当てられている場合、相対値が等しくありません。共有の総数は 3000 で、1000 の共有は 33.3 パーセントを表し、2000 の共有は 66.6 パーセントを表します。したがって、vApp2 は CPU の 66.6 パーセントを、vApp2 は 33.3 パーセントを使用できます。

CPU 予約

この vApp に保証される CPU 割り当てを指定します。

CPU 無制限

[CPU 制限] の設定を無効にします。実際の制限は、利用可能な物理リソースに設定されるようになります。

CPU 制限

この vApp に割り当てる CPU の上限を指定します。通常、デフォルトを受け入れることができます。

メモリ共有

親リソース プールまたは vApp のメモリ合計リソースに関して、この vApp 用のメモリ共有を指定します。親が同じ vApp は、予約と制限によって制約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。適切な相対値を表す共有の数を指定します。

たとえば、ホスト上に vApp1 と vApp2 があり、各々に 1000 メモリ共有が割り当てられていると仮定します。相対値が等しいので、vApp はそれぞれ、親ホストの 50 パーセントのメモリを使用できます。vApp1 に 2000 メモリ共有、vApp2 に 1000 メモリ共有が割り当てられている場合、相対値が等しくありません。共有の総数は 3000 で、1000 の共有は 33.3 パーセントを表し、2000 の共有は 66.6 パーセントを表します。したがって、vApp2 はメモリの 66.6 パーセントを、vApp2 は 33.3 パーセントを使用できます。

メモリ予約

この vApp に保証されるメモリ割り当てを指定します。

メモリ無制限

[メモリ制限] の設定を無効にします。実際の制限は、利用可能な物理リソースに設定されるようになります。

メモリ制限

この vApp に割り当てるメモリの上限を指定します。通常、デフォルトを受け入れることができます。

新しい vApp が [エクスプローラ] ペインに表示されます。

vApp のクローン作成

仮想マシンのクローンを作成する方法に類似した方法で vApp のクローンを作成できます。

次の手順に従ってください:

1. [エクスプローラ] ペインのホストまたはクラスター レベルで、クローンの作成元となる vApp を選択します。
2. vApp を右クリックします。
ポップアップ メニューが表示されます。
3. [管理] - [vApp のクローン作成] を選択します。
[vApp のクローン作成] ダイアログ ボックスが表示されます。
4. 以下のフィールドで値を指定して、[OK] をクリックします。

名前

新規にクローン作成される vApp を識別します。

場所

適切な場所を指定します。ポップアップ メニュー上に表示されるオブジェクトを展開し、場所を選択します。

データストア

ドロップダウン メニューからの適切なデータストアを指定します。
新規にクローン作成された vApp が、[エクスプローラ] ペインに表示されます。

その他の vApp 操作

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

- 電源オン
- 電源オフ
- 中断
- VMware vCenter からの削除
- VMware vCenter からの登録解除

次の手順に従ってください:

1. [エクスプローラ] ペインでホストまたはクラスターレベルから、適切な vApp を選択します。
2. vApp を右クリックします。
ポップアップメニューが表示されます。
3. [管理] を選択し、実行する操作をクリックします。
確認ダイアログボックスが開きます。
4. [OK] をクリックします。

CA Virtual Assurance によって、選択された操作が実行されます。

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。

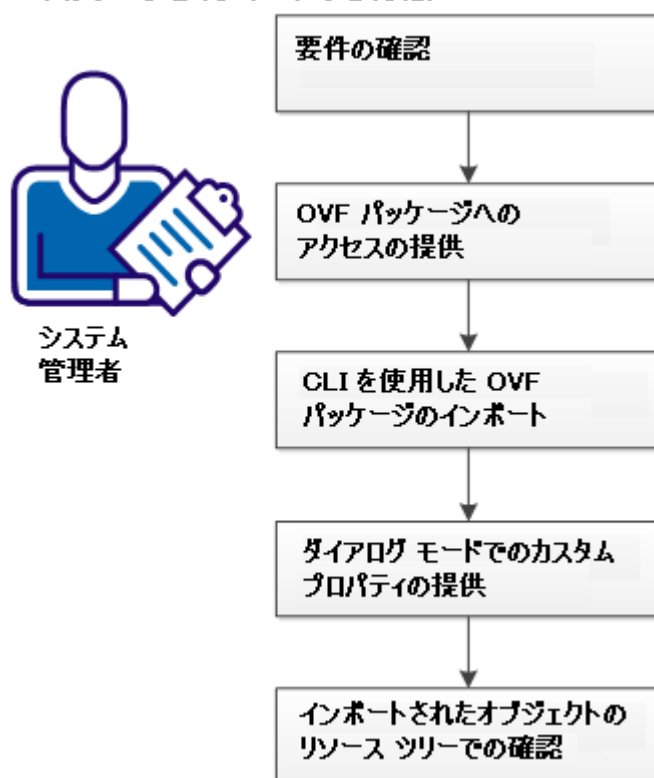
CA Virtual Assurance を使用した OVF パッケージのインポート方法

このシナリオは、CA Virtual Assurance を使用した OVF パッケージのインポートに関する情報を提供します。この情報は、システム管理者が OVF パッケージをインポートし、これらの OVF パッケージで指定される vApps を展開するのを支援するために提供されます。

Open Virtualization Format (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。

以下の図は、OVF パッケージをインポートする手順を説明します。

OVF パッケージをインポートする方法



以下の手順に従います。

[要件の確認 \(P. 648\)](#)

[OVF パッケージへのアクセスの提供 \(P. 648\)](#)

[dpmovf import コマンド -- OVF パッケージのインポート \(P. 649\)](#)

[ダイアログモードでのカスタム プロパティの提供 \(P. 651\)](#)

[インポートされたオブジェクトのリソース ツリーでの確認 \(P. 652\)](#)

要件の確認

また、以下の要件も確認してください。

- CA Virtual Assurance ユーザ インターフェースにアクセスできる。
- ターゲット 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。
- 管理者として CMD ウィンドウを開始できること、および、dpmovf.exe ファイルがコンピュータにインストールされていることを確認済みである。

関連項目：

[vCenter Server 管理コンポーネント間のインタラクションの確認 \(P. 601\)](#)

[新しい vCenter Server 接続のマネージャへの追加 \(P. 605\)](#)

[vCenter Server の AIM インスタンスの追加 \(P. 610\)](#)

[リソース ツリーでの vCenter Server フォルダの表示の確認 \(P. 618\)](#)

OVF パッケージへのアクセスの提供

CA Virtual Assurance から OVF パッケージにアクセスできるようにするには、以下のいずれかのタスクを実行します。

- マネージャ上で、OVF パッケージがある場所にドライブをマップします。
- OVF パッケージをマネージャ上にコピーします。

dpmovf import コマンド -- OVF パッケージのインポート

dpmovf import コマンドは OVF パッケージをインポートし、VM または vApps を作成します。-properties 属性を使用すると、カスタム プロパティ ファイルを提供できます。カスタム プロパティ ファイルを使用すると、OVF パッケージで定義されているカスタム プロパティを指定できます。カスタム プロパティ ファイルには、プロパティ キーおよび対応するプロパティ値のリストが含まれます。

注: カスタム プロパティ ファイルがない場合は、properties.txt ファイルが作業ディレクトリに作成されます。デフォルトディレクトリは CA¥ProductName¥bin です。

このコマンドの形式は、以下のとおりです。

```
dpmovf import
-host vCenter_server
-user user_name
-password user_password
-name VM_VApp_name
-path OVF_file_path
-datacenter data_center
-datastore data_store
-resourcepool resource_pool
[-locale iso639value]
[-properties properties_file]
```

-host vCenter_server

vCenter Server ホストの名前を指定します。

-user user_name

ログインするユーザ名を指定します。

-password user_passsword

ログインするユーザのパスワードを指定します。

-name VM_VApp_name

VM または vApp の名前を指定します。

-path OVF_file_path

OVF ファイルパスを指定します。

-datacenter data_center

データ センター名を指定します。

-datastore *data_store*

データ ストアを指定します。

-resourcepool *resource_pool*

リソース プールを指定します。

-locale *iso639value*

(オプション) デフォルトの英語出力より優先させるロケールを、ISO 639_3166 の組み合わせ (たとえばフランス語の場合は **fr_FR**) で指定します。コマンドプロンプトのロケールを使用する場合は「**native**」を指定します。

-properties *properties_file*

(オプション) カスタム プロパティ ファイルパスを指定します。

例: CA Virtual Assurance を使用した、CA プラットフォーム用の OVF ファイルのインポート

この例では、CA プラットフォーム OVF パッケージをインポートし、vApp および VM を作成します。CA プラットフォーム OVF ファイルは **CA Platform_v1_0_0_92c.ovf**、ファイルの場所は **D:¥OVF¥CA_Platform** です。ユーザ名は **user123** です。vApp の以下の属性が指定されています: **my_datastore**、**my_datacenter**、および **my_resourcepool**。カスタム プロパティは **custom_properties.txt** ファイルで提供されます。

```
dpmovf import -path "D:¥OVF¥CA_Platform¥CA Platform_v1_0_0_92c.ovf" -name
"My_CA_Platform" -host my_host.company.com -user user123 -locale en-US -datastore
"my_datastore" -datacenter "my_datacenter" -resourcepool "my_resourcepool"
-properties "custom_properties.txt"
```

ダイアログ モードでのカスタム プロパティの提供

OVF ファイルにカスタム プロパティが含まれる場合、ダイアログ モードでカスタム プロパティを編集できます。カスタム プロパティ ファイルを指定すると、ダイアログ モードでカスタム プロパティ ファイルを上書きできます。

注: カスタム プロパティ ファイルがない場合は、`properties.txt` ファイルが作業ディレクトリに作成されます。デフォルト ディレクトリは `CA¥ProductName¥bin` です。

次の手順に従ってください:

1. 編集するカスタム プロパティのカスタム プロパティ番号を入力します。
2. カスタム プロパティの値を入力します。
3. 提供または編集するすべてのカスタム プロパティに対して、手順 1 ～ 2 を繰り返します。
4. 以下のいずれかのオプションを入力します。

r

プロパティ ファイルを読み取ります。

w

プロパティ ファイル内のプロパティすべてを上書きします。

c

インポート コマンドを実行します。

注: 提供されたプロパティの一部は、条件が満たされているか、あるいは提供された値が有効かどうかを確認するために検証されます。

CA Virtual Assurance は vCenter に OVF を展開し、OVF ファイルで指定される vApps および VM が参照可能です。

インポートされたオブジェクトのリソース ツリーでの確認

vApps と VM をインポートした後、追加されたインスタンスは [VMware vCenter Server] フォルダのリソース エクスプローラ ペインに一覧表示されます。

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] ペインを開きます。
2. [VMware vCenter Server] を展開します。

インポートされたオブジェクトが表示されます。

OVF ファイルで指定された vApps が vCenter 環境にインポートされています。CA Virtual Assurance では、vSphere 環境に追加された vApps および VM を管理する準備ができています。

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。

vNetwork パネル内の仮想標準スイッチおよび分散仮想スイッチ

vNetwork パネルは、VMware データセンター レベルおよび ESX ホスト レベルのユーザ インターフェースで利用できます。VMware データセンター レベルでは、vNetwork は、そのデータセンターの分散仮想スイッチを示します。ESX ホスト レベルでは、vNetwork は、関連付けられた分散仮想スイッチおよび仮想標準スイッチを示します。

関連項目:

[vNetwork 標準スイッチ \(vSwitch\)](#) (P. 653)

[分散仮想スイッチ](#) (P. 653)

[プロパティ](#) (P. 655)

[アクション](#) (P. 659)

[イベントによる分散仮想スイッチのモニタリング](#) (P. 661)

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 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。

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。

仮想標準スイッチ オブジェクトを展開すると、関連付けられたポートおよびポート グループを参照できます。

- ポート グループには、そのポート グループを使用する関連 VM が含まれます。

分散仮想スイッチ

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。

分散仮想スイッチは、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。分散仮想スイッチは、これらのホストに対して同じスイッチ（同じ名前、同じネットワーク ポリシー）とポート 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 は一貫したネットワーク設定を維持できます。

各分散仮想スイッチは、vNetwork Standard Switch と同様、VM が使用できるネットワーク ハブです。分散仮想スイッチは、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。

分散仮想ポート グループ（dvPort グループ）は、分散仮想スイッチと関連付けられたポート グループであり、各メンバ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、分散仮想スイッチを介してネットワークに接続する方法を定義します。

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、分散仮想スイッチによるネットワークへのアクセスに、VM が ESX または ESXi ホスト上のどの物理 NIC を使用するかを定義します。

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。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witchのマニュアルを参照してください。

注: Cisco Nexus 1000V スwitch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witchに影響しないことを確認してください。

分散仮想スイッチ オブジェクトを展開すると、関連付けられたポートグループおよびアップリンク グループを参照できます。

- ポート グループには、そのポート グループを使用する関連付けられた VM が含まれます。
- [アップリンク グループ] には、物理アップリンク アダプタがリスト表示されます。

プロパティ

[プロパティ] ペインには、仮想標準スイッチまたは分散仮想スイッチのプロパティが表示されます。

ポリシー

以下のリストに、仮想標準スイッチまたは分散仮想スイッチ用のデフォルト ポリシー（有効化されているポリシー）を示します。

プロミスキャス モード

ポート上ですべてのトラフィックを見られるかどうかを示します。

MAC アドレス変更

MAC（Media Access Control）アドレスを変更できるかどうかを示します。

偽造された送信

MAC アドレスが仮想ネットワーク アダプタの MAC アドレスと異なるかどうかを示します。

トラフィックシェイピング

ポート上でトラフィックシェイパが有効かどうかを示します。

平均帯域幅

ポートでシェイピングが有効な場合、平均帯域幅をビット/秒で示します。

ピーク帯域幅

ポートでトラフィックシェイピングが有効な場合、バースト時のピーク帯域幅をビット/秒で示します。

バースト サイズ

ポートでシェイピングが有効な場合、許可される最大バーストサイズをバイト単位で示します。

ネットワーク障害検出

ネットワーク障害検出が有効かどうかを示します。有効な値は以下のとおりです。

- false (1)
- true (2)

スイッチの通知

リンクが失敗した場合に、物理スイッチに通知するかどうかを指定します。

フォールバック

フォールバックが有効かどうかを示します。

ポリシー受信フレーム

受信フレームにチーミング ポリシーが適用されるかどうかを示します。

アクティブなアダプタ

負荷分散に使用されるアクティブなネットワーク アダプタのリストを表示します。

スタンバイアダプタ

フェールオーバーに使用されるスタンバイ ネットワーク アダプタのリストを表示します。

vSwitch のプロパティ

以下の vSwitch プロパティから、ポート番号の特性がわかります。

ポート数

分散仮想スイッチまたは仮想標準スイッチの現在のポート数を示します。

ポートの最大数

分散仮想スイッチのポートの最大数を示します。

注: 分散仮想スイッチの場合、この情報は **VMware** データセンター レベルでのみ利用できます。 **ESX** ホスト レベルでは利用できません。

ポート グループのプロパティ

以下のポート グループ プロパティが **VLAN ID** を示します。

VLAN ID

ポート グループの **VLAN ID** を示します。

ポートのプロパティ

以下のプロパティがポート特性を指定します。

VLAN ID

ポートの VLAN ID を示します。

タイプ

ポートのタイプ (VMkernel ポート、サービス ポートなど) を示します。

ネットワークのプロパティ

以下のプロパティが、仮想スイッチのネットワーク特性を指定します。

- IPv4 アドレス
- IPv6 アドレス
- MAC アドレス

仮想マシン数

以下の値は、ポート グループと関連付けられた VM に関する統計情報を提供します。

- 電源オン
- 電源オフ
- 中断
- 不明

アクション

仮想標準スイッチと分散仮想スイッチの管理に適切なアクションを使用します。以下のアクションを使用できます。

- vSwitch の追加
- vSwitch の更新
- vSwitch の削除
- ポート グループの追加
- ポート グループの更新
- ポート グループの削除
- ポート グループの名前変更

これらのアクションを適用しようとする、ダイアログ ボックスが表示され、必要な情報の入力を求められます。表示される可能性のあるフィールドは、以下のとおりです。

スイッチ名

操作を実行するスイッチの名前を指定します。

NIC

(オプション) ESX ホスト メンバと関連付けられた物理 NIC のリストを指定します。

アップリンクポート名

(オプション) 使用するアップリンク ポート名のリストを指定します。

ポートの最大数

(オプション) 分散仮想スイッチのポートの最大数を指定します。

バインドタイプ

(オプション) ポート グループのバインド タイプを指定します。有効な値は以下のとおりです。

earlyBinding

VM がポートグループにバインドする際にポートを割り当てます。このバインディング タイプは、接続性の常時確保に有効ですが、ポートが永続的に予約されます。デフォルトはこのバインディング タイプです。

lateBinding

VM の電源がオンで NIC の状態が接続済みの場合、VM にポートを割り当てます。このバインディング タイプは、VM の電源がオフになるか、NIC が切断されると、ポートを割り当て直します。

LateBinding は vCenter で設定できます。

ephemeral

VM の電源がオンで NIC の状態が接続済みの場合、VM にポートを割り当てます。このバインディング タイプは、VM の電源がオフになるか、NIC が切断されると、ポートを割り当て直します。

ephemeral バインディングは、ESX ホストと vCenter で設定できます。

ポート数

(オプション) ポート グループのポートの数を指定します。

ポートグループ名

ポート グループ名を指定します。

新しいポートグループ名

新しいポート グループ名を指定します。

LAN ID *vlanid*

(オプション) 仮想ポート グループの操作に使用する整数値 (*vlanid*) を指定します。

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。

VMware vCenter のプロビジョニングと一般的なユース ケース

このセクションでは、仮想リソースをプロビジョニングする方法と一般的なユース ケースについて説明します。

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 インターフェー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。

仮想マシンのクローン作成

仮想マシンのクローンを作成することによって、同じ仮想マシン ファームのいかなる場所にも配置できる仮想マシンのコピーを作成できます。また、クローンを作成するときに、ゲスト オペレーティング システムをカスタマイズできます。仮想マシンが電源オフの状態にあるときのみ、仮想マシンのクローンを作成できます。

仮想マシンのクローンを作成する方法

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. [エクスプローラ] ペインでクローン作成する仮想マシンを見つけて右クリックし、[管理] - [クローン作成] を選択します。
[クローン作成] ペインが表示されます。
3. 以下のフィールドに入力し、[クローン] をクリックします。

名前

VM クローン名を指定します。

データストア

クローン作成された VM を格納するデータストアを指定します。データストアはソース VM と同じファーム内にある必要があります。

カスタム仕様

使用するゲスト オペレーティング システム仕様を指定します。デフォルトまたはカスタマイズを選択できます。

デスティネーション リソース プール

クローン作成された VM がリソースを取得するプールを指定します。

要求のサブミットを確認するメッセージが表示されます。

4. 仮想マシンの [サマリ] タブをクリックします。
処理を確認するイベントが表示されることを確認します。処理が完了すると、クローンが [エクスプローラ] ペインに表示されます。

VM ステータスの管理(VMware)

以下のいずれかの VM 操作の実行により vCenter Server 仮想マシンのステータスを制御できます。

- 電源オン
- 電源オフ
- 中断
- リセット
- シャットダウン

これらの操作は、複数の VM で同時に実行できます。

VM ステータスを制御する方法

1. [エクスプローラ] ペインでステータス処理を実行する仮想マシンを選択します。
2. VM を右クリックし、[管理] を選択します。[クイック スタート] をクリックし、電源制御の関連するリンクをクリックする方法もあります。以下のいずれかを選択します。

電源オン

仮想マシンを開始し、ゲスト オペレーティング システムを起動します。現在電源がオフになっているか、中断されている仮想マシンのみ、電源をオンにすることができます。

電源オフ

仮想マシンを電源オフします。現在電源がオンになっているか、中断されている仮想マシンのみ、電源をオフにすることができます。

中断

仮想マシンを中断し、現在の状態を保存します。マシンを再開するまで、すべてのアクティビティが中断されます。

リセット

ゲスト オペレーティング システムをシャットダウンし、再起動します。

シャットダウン

ゲスト オペレーティング システムをシャットダウンします。現在電源がオンになっている仮想マシンのみ、シャットダウンすることができます。

確認ダイアログ ボックスが開きます。

3. [OK] をクリックします。

ステータス操作が実行され、確認のメッセージが表示されます。インターフェースをリフレッシュして、最新の **VM** ステータスを表示します。操作の結果を確認するイベントが表示されます。

次のアイコンが **VM** ステータスを示します。



VM が重大な状態であることを示します。



VM が警告の状態であることを示します。



VM が正常な状態であることを示します。



VM が不明な状態であることを示します。

テンプレートの仮想マシンへの変換

仮想マシン テンプレートを仮想マシンに変換できます。テンプレートから変換された VM は、そのテンプレートの名前と設定を使用します。

テンプレートを仮想マシンに変換する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックし、[管理] - [VM に変換] を選択します。
[変換] ページが表示されます。
3. 仮想マシンの ESX サーバおよびリソース プールを選択し、[変換] をクリックします。
要求のサブミットを確認するメッセージが表示されます。
4. 仮想マシン テンプレートの [サマリ] タブをクリックします。
処理を確認するイベントが表示されることを確認します。処理が完了した後、インターフェースをリフレッシュすると、テンプレートが [エクスプローラ] ペインに仮想マシンとして表示されます。

仮想マシンをテンプレートに変換します

電源オフした仮想マシンをテンプレートに変換して、他の仮想マシンのベースとしてその仮想マシンの設定を使用できます。

仮想マシンをテンプレートに変換する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックし、[管理] - [テンプレートに変換] を選択します。
確認ダイアログ ボックスが開きます。
3. [OK] をクリックします。
要求のサブミットを確認するメッセージが表示されます。
4. 仮想マシンの [サマリ] タブをクリックします。
処理を確認するイベントが表示されることを確認します。処理が完了した後、インターフェースをリフレッシュすると、仮想マシンが [エクスプローラ] ペインにテンプレートとして表示されます。

スナップショットの作成

後で同じ状態に戻ることができるように、スナップショットを作成して、仮想マシンの現在の状態を保存します。スナップショットは、メモリ内容、設定、および仮想ディスク状態を含め、仮想マシン全体の状態を保存します。電源オン、電源オフ、または中断されている仮想マシンのスナップショットを作成できます。

スナップショットを作成する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックし、[管理] - [スナップショット] を選択します。
[スナップショット] ペインが表示されます。
3. [アクション] ドロップダウン メニューから [新規] を選択します。
[新しいスナップショットの作成] ダイアログ ボックスが表示されます。
4. スナップショット名および説明を入力して、メモリのキャプチャを有効にするべきかどうかを指定し、[OK] をクリックします。
確認メッセージが表示されます。
5. 仮想マシンの [サマリ] をクリックします。
6. 処理を確認するイベントが表示されることを確認します。
処理が完了すると、スナップショットが [スナップショット] ペインに表示されます。

スナップショットの削除

必要がなくなったスナップショットを削除できます。

スナップショットを削除する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックし、[管理] - [スナップショット] を選択します。
[スナップショット] ペインが表示され、その仮想マシンの既存のすべてのスナップショットが表示されます。
3. スナップショットを選択し、[アクション] ドロップダウン メニューから [削除] を選択します。
確認ダイアログ ボックスが開きます。
4. [OK] をクリックします。
要求のサブミットを確認するメッセージが表示されます。
5. 仮想マシンの [サマリ] タブをクリックします。
処理を確認するイベントが表示されることを確認します。処理が完了した後、スナップショットが [スナップショット] ペインに表示されなくなります。

すべてのスナップショットの削除

1回の操作で、1つの仮想マシンの既存のスナップショットをすべて削除できます。

すべてのスナップショットを削除する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックし、[管理] - [スナップショット] を選択します。
[スナップショット] ペインが表示され、その仮想マシンの既存のすべてのスナップショットが表示されます。
3. [アクション] ドロップダウンメニューから [すべて削除] を選択します。
確認ダイアログ ボックスが開きます。
4. [OK] をクリックします。
確認メッセージが表示されます。
5. 仮想マシンの [サマリ] をクリックします。
処理を確認するイベントが表示されることを確認します。処理が完了した後、すべてのスナップショットが [スナップショット] ペインに表示されなくなります。

仮想マシンの削除

VMware vCenter Server から仮想マシンを削除すると、仮想マシンは仮想ディスクから削除されます。

仮想マシンを削除する方法

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. [エクスプローラ]ペインで仮想マシンを見つけて右クリックし、[管理] - [vCenter Server から削除] を選択します。
確認ダイアログ ボックスが開きます。
3. [OK] をクリックします。
要求のサブミットを確認するメッセージが表示されます。
4. 仮想マシンの [サマリ] タブをクリックします。
処理の結果を確認するイベントが表示されます。成功すると、その仮想マシンが仮想ディスクから削除され、インターフェースをリフレッシュした後、[エクスプローラ] ペインに表示されなくなります。

仮想マシンのテンプレートからの展開

テンプレートの設定を使用して、テンプレートから新しい仮想マシンを作成および展開できます。

テンプレートから仮想マシンを展開する方法

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. すべての必須フィールドを指定し、適切な VC テンプレートを選択します。
[次へ] をクリックします。
3. 残りの手順を実行して、仮想マシン用の仮想ハードウェアを指定します。[終了] をクリックします。
要求のサブミットを確認するメッセージが表示されます。
4. 処理を確認するイベントが表示されることを確認します。
処理が完了した後、インターフェースをリフレッシュすると、新しい仮想マシンが [エクスプローラ] ペインに表示されます。

クラスタ サービスの管理

VMware vCenter クラスタ上の以下のサービスのステータスを制御できます。

HA

ホストで障害が発生したときの、自動マイグレーションおよび VM の再起動を可能にします。

DRS

リソースのコレクションとしてホストを管理できます。必要に応じて、DRS のサービスは、VM をホストに、リソースを VM にマイグレートします。

Cluster Services を管理する方法

1. [エクスプローラ] ペイン上の VMware vCenter クラスタを選択します。
[概要] ペインが右側に表示され、HA サービスおよび DRS サービスのステータスを表示します。
2. ドロップダウン メニューから [有効] または [無効] を選択します。
サービスのステータスが変更されます。

仮想マシンのマイグレート

仮想マシンをマイグレートして、別の ESX ホストにその仮想マシンを移動できます。電源オフのマシンをマイグレートできます。または、VMotion を備えたマシン上では電源オンのマシンをマイグレートできます。中断されている仮想マシンはマイグレートできません。

仮想マシンをマイグレートする方法

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. [エクスプローラ] ペインでマイグレートする仮想マシンを見つけて右クリックし、[管理] - [マイグレート] を選択します。
[マイグレート] ペインが表示されます。
3. 仮想マシンのデスティネーション ESX サーバおよびリソース プールを入力し、[マイグレート] をクリックします。
注: VM データストア/ディスクが 2 つの ESX ホスト間で共有される場合のみ、ESX ホスト間の VM マイグレーションがサポートされます。
確認メッセージが表示されます。
4. 仮想マシンの [サマリ] タブをクリックします。
処理を確認するイベントが表示されることを確認します。処理が完了した後、仮想マシンが [エクスプローラ] ペインのマイグレートされた場所に表示されます。

仮想マシンのモニタ

VM のステータスとプロパティは詳細にモニタすることができます。

仮想マシンをモニタする方法

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. [VMware vCenter Server] フォルダおよび ESX サーバ オブジェクトを展開します。
VM リストが表示されます。
4. [サマリ] タブをクリックします。

右側のペインに、一般情報、FT プロパティ、概要、CPU とメモリの使用率、ディスク使用率（論理ボリューム）、およびイベントが表示されます。

[概要] パネルに示されるディスク状態は、仮想ディスクの仮想ハードウェア状態を表しています。この状態は **SystemEDGE** によって計算され、**vCenter AIM** 内に設定されたモニタに基づいています。この情報は、1 秒あたりの読み取り数/書き込み数という観点から見た、仮想ディスクの真のパフォーマンス データに基づいています。

[ディスク使用率] パネルに示されるディスク状態は、ゲストオペレーティングシステムの観点から見た論理ボリュームの使用率を表しています。この状態は **SystemEDGE** によって計算され、**vCenter AIM** 内に設定されたモニタに基づいています。VM とゲストオペレーティングシステムが動作している場合のみ、この情報が有効になります。

[一般情報] パネルには、VM の接続状態に関する詳細が示されます。接続状態の有効な値は以下のとおりです。

- 未接続
- 接続済み
- 孤立

孤立の接続状態は、クラスタがフェールオーバーしている状況で発生する場合があります。仮想マシンが孤立状態であるとマークされるとき、[概要] セクションに反映される状態は、孤立状態になる前に収集されたデータに基づいています。

ESX サーバのモニタ

ESX サーバのステータスとプロパティは詳細にモニタすることができます。

ESX サーバをモニタする方法

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. [VMware vCenter Server] フォルダを展開し、ESX サーバを選択します。
4. [サマリ] タブをクリックします。
右側のペインに、一般情報、FT 属性、概要、CPU とメモリの使用率、使用状況、およびイベントが表示されます。
5. [vNetwork] タブをクリックします。
右側のペインに、関連付けられている仮想標準スイッチ (vSwitch) および分散仮想スイッチ (vDS) のリストが表示されます。
6. リストから仮想スイッチを選択します。
右側のペインに、仮想スイッチのプロパティが表示されます。

スナップショットに戻す

スナップショットに戻すと、スナップショットを作成したときの正確な状態に仮想マシンが戻されます。

スナップショットに戻す方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックし、[管理] - [スナップショット] を選択します。
[スナップショット] ペインが表示され、その仮想マシンの既存のすべてのスナップショットが表示されます。
3. スナップショットを選択し、[アクション] ドロップダウン メニューから [元に戻す] を選択します。
確認ダイアログ ボックスが開きます。
4. [OK] をクリックします。
確認メッセージが表示されます。
5. 仮想マシンの [サマリ] タブをクリックします。
処理を確認するイベントが表示されることを確認します。

仮想マシンの登録解除

vCenter Server から仮想マシンを登録解除すると、仮想マシンはそのまま存在しますが、VMware vCenter Server インベントリからは削除されます。

仮想マシンを登録解除する方法

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. [エクスプローラ] ペインで仮想マシンを見つけて右クリックし、[管理] - [vCenter Server からの登録解除] を選択します。
確認ダイアログ ボックスが開きます。
4. [OK] をクリックします。
要求のサブミットを確認するメッセージが表示されます。
5. 仮想マシンの [サマリ] タブをクリックします。
処理の結果を確認するイベントが表示されます。成功すると、仮想マシンは vCenter インベントリから削除されます。

vCenter の自動化とポリシー アクション

以下のアクション タイプを VMware vCenter Server で使用できます。

- [ディスクの追加](#) (P. 777)
- [ネットワーク インターフェースの追加](#) (P. 779)
- [共有の設定](#) (P. 807)
- [CPU/メモリの設定](#) (P. 791)
- [電源の設定](#) (P. 803)
- [テンプレートの仮想マシンへの変換](#) (P. 809)
- [仮想マシンのテンプレートへの変換](#) (P. 811)
- [マシンの削除](#) (P. 822)
- [VM スナップショットの管理](#) (P. 831)
- [CPU の変更](#) (P. 841)
- [メモリの変更](#) (P. 843)
- [マシンのプロビジョニング](#) (P. 858)
- [ディスクの削除](#) (P. 861)
- [ネットワーク インターフェースの削除](#) (P. 863)
- [マシンをマイグレート](#) (P. 839)

割り当てられたルール基準が満たされるときに、vCenter の電源、リソース割り当て、および他の操作を自動化する新規アクションを作成するためにこれらのアクション タイプを使用できます。また、これらのアクションが特定の時間に実行されるようにスケジュールすることもできます。

自動化ポリシーを作成するアクションおよびルールの使用の詳細については、「ポリシー」を参照してください。

カスタム仕様の表示

カスタム仕様は、仮想マシン上で使用しているゲスト オペレーティング システムのカスタム バージョンです。現在のカスタム仕様、最後の更新の日付、および現在のバージョン番号をすべて表示できます。

カスタム仕様を表示する方法

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. VMware vCenter Server を検索して選択します。
右側のペインに [サーバ] ページが表示されます。
3. [設定] タブをクリックし、[カスタマイズの仕様] サブメニューを選択します。
[カスタマイズの仕様] セクションが表示されて、既存のカスタマイズ仕様が表示されます。

一般情報の表示

CA Virtual Assurance は、右側のペイン内で [一般情報] を表示し、オブジェクト階層内の以下のレベルでリソース プロパティを提供します。

- vCenter Server
- ESX Server
- リソース プール
- VM

リソース プロパティには、以下のカテゴリに関する情報が含まれます。

- 名前、アイテム タイプ、バージョン
- CPU とメモリの数量特性
- VM 数とリソース プール数
- リソースの現在のモード

さらに、CA Virtual Assurance には接続状態、電源状態、および VM レベルについてのフォールト トレランス情報が表示されます。

有効なフォールトトレランスステータスの値は以下のとおりです。

- フォールトトレラントでない
- 保護されている
- 保護されていない (起動中)
- 保護されていない (セカンダリ VM が必要)
- 保護されていない (無効)
- 保護されていない (VM が実行されていない)

セカンダリの場所の値は以下のとおりです。

- 利用不可
- セカンダリ CPU 合計使用率
- セカンダリ メモリ合計

[一般情報] パネルには、フォールトトレランスが設定されているかどうか、バージョン、およびサポートされている FT VM のさまざまな数量に関する詳細が表示されます。その数量には、以下が含まれます。

- プライマリ VM の合計
- セカンダリ VM の合計
- 電源オン プライマリ VM
- 電源オン セカンダリ VM

[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。

関連項目

[ESX サーバのモニタ](#) (P. 679)

[仮想マシンのモニタ](#) (P. 678)

第 7 章：クラスタおよび仮想デスクトップの 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。

[Citrix XenDesktop 環境](#) (P. 685)

[IBM PowerHA](#) (P. 687)

[Microsoft Cluster Service](#) (P. 693)

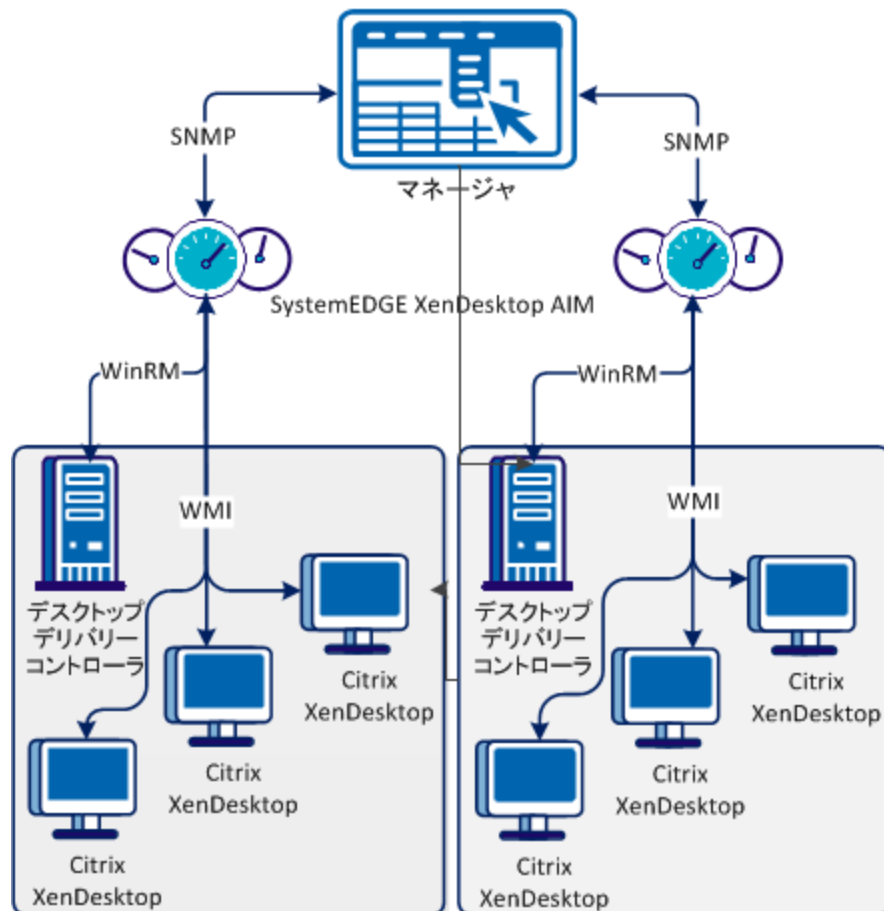
Citrix XenDesktop 環境

CA Virtual Assurance は Citrix XenDesktop 環境をリモートでモニタします。
Citrix XenDesktop AIM は統計データを提供し、Citrix XenDesktop 環境内の問題の検出を容易にします。

Citrix XenDesktop 管理コンポーネント間のインタラクション

以下の図は、Citrix XenDesktop 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 XenDesktop AIM が稼働する Windows サーバです。XenDesktop AIM と Citrix XenDesktop コントローラとの間の通信には、Windows リモート管理 (WinRM) を使用します。XenDesktop AIM とユーザの環境内の Citrix XenDesktop の間の通信には、WMI を使用します。CA Virtual Assurance は複数の Citrix XenDesktop コントローラに接続でき、Citrix XenDesktop 環境全体を把握することができます。

Citrix XenDesktop 管理コンポーネント間のインタラクション



Citrix XenDesktop コントローラの必要な接続情報を追加するには、以下の方法を使用します。

- 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。

XenDesktop AIM は設定ファイルをポーリングし、Citrix XenDesktop コントローラを介して、あるいは Citrix XenDesktop から直接、Citrix XenDesktop 環境のモニタリングを開始します。

Citrix XenDesktop の前提条件

- XenDesktop AIM のインストールには、以下の一覧表示された前提条件が必要です。

注: Windows Management Framework の詳細については、Microsoft サポート技術情報の記事 968929 を参照してください。

信頼済みホストリストへのマシン名の追加

Citrix XenDesktop が別のドメイン内にある場合は、AIM マシン上の WinRM サービス用に、マシン名を信頼済みホスト設定に追加します。

以下のコマンドを使用します。

```
set-Item wsman:%localhost%\client%\trustedhosts machine_dnsname  
machine_dnsname
```

XenDesktop AIM が接続するコンピュータの完全な DNS 名のリストを指定します。

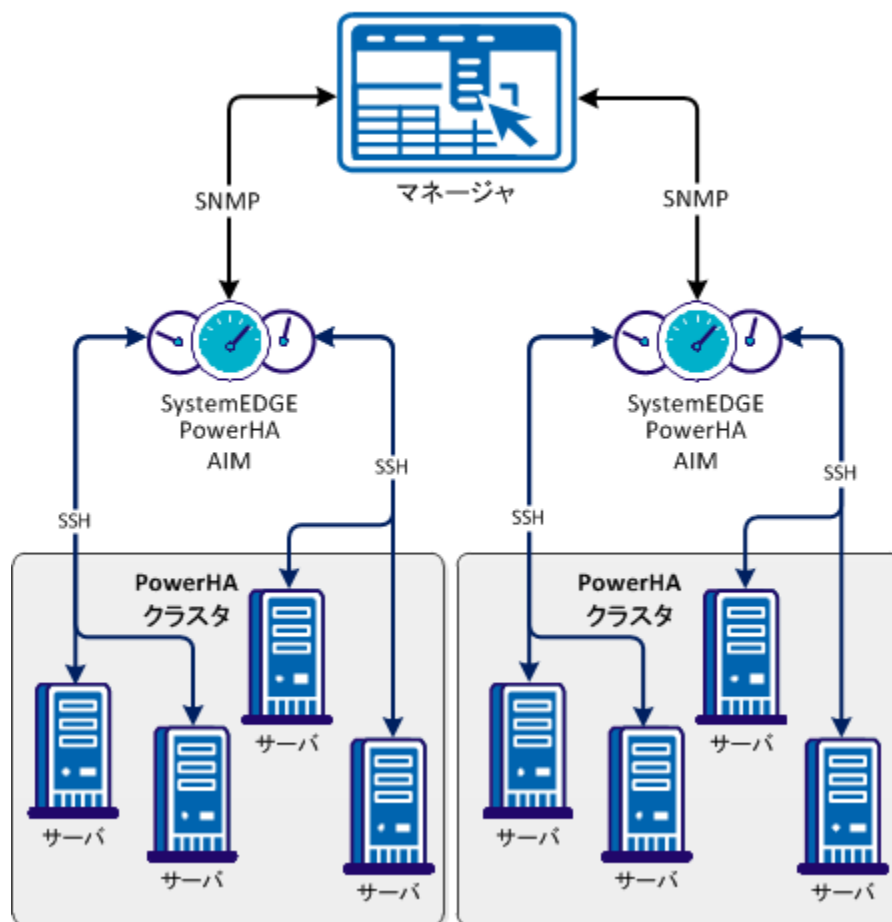
IBM PowerHA

CA Virtual Assurance は、IBM PowerHA（旧名称「High Availability Cluster Multiprocessing（HACMP）」）をモニタします。CA Virtual Assurance はクラスタをリモートでモニタし、障害を検出して、クラスタ内のアラートやその他の環境の問題に関する詳細を提供します。

IBM PowerHA 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 PowerHA に関与する管理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 PowerHA AIM が稼働する Windows サーバです。AIM と PowerHA クラスタの間の通信では、SSH（Secure Shell）が使用されます。CA Virtual Assurance は複数のクラスタに接続できるため、CA Virtual Assurance では IBM PowerHA 環境全体のビューが取得できます。

PowerHA 管理コンポーネント間のインタラクション



必要な各 IBM PowerHA クラスタに要求される接続情報を追加するには、以下の方法を使用します。

■ 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。PowerHA AIM は設定ファイルをポーリングし、マスタ ノードを通じて IBM PowerHA 環境のモニタリングを開始します。

SSH の設定

クラスタ ノードをモニタするには、リモート アクセス用の SSH を設定します。

次の手順に従ってください:

1. クラスタ (ノード) 上に SSH デーモンをインストールして実行します。
2. SSH 接続を許可するようにローカル ファイアウォールを設定します。

ダイアログ モードの NodeCfgUtil による PowerHA AIM の設定

NodeCfgUtil.exe は、AIM 設定を変更するために使用できるユーティリティです。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。

次の手順に従ってください:

1. AIM がインストールされているコンピュータで管理者としてログインし、Windows エクスプローラを開きます。
2. *SystemEDGE_InstallPath¥plugins¥AIPCommon* ディレクトリに変更し、*NodeCfgUtil.exe* を起動します。

NodeCfgUtil によって、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 ボックスに一覧表示されます。

3. 1 を入力して、新しい管理対象ノードを追加します。

4. 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。
5. 設定が完了したら、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、PowerHA の設定ファイル (hacmp.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。

例

以下の例は、PowerHA AIM の設定に正常に追加された *mycluster* に関する [管理対象ノードのインストール] ダイアログ ボックスを示します。PowerHA AIM はマルチインスタンス AIM です。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. IBM PowerHA
0. 前のメニューに戻る
*****
選択項目を入力してください: 2
IBM PowerHA 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. クラスタ名: mycluster
2. ユーザ名: administrator
3. パスワード: *****
4. ポート [デフォルトは 22]:
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...
```

コマンド モードの NodeCfgUtil による PowerHA AIM の設定

NodeCfgUtil.exe は、AIM 設定を変更するために使用できるユーティリティです。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 管理者として実行してください。

このコマンドの形式は、以下のとおりです。

- (1) `nodecfgutil -help`
- (2) `nodecfgutil powerha -u user -p password -h cluster_name [-t port]`

-help

コンソールに関する使用情報が表示されます。

powerha

仮想環境または物理環境を指定します。

-u user/usercertificate

管理者ユーザの名前またはユーザ証明書をそれぞれ指定します。

-p password

そのユーザのパスワードを指定します

-h cluster_name

クラスタの名前を指定します。

-t port

(オプション) ポート番号を指定します。

デフォルト : 22

次の手順に従ってください:

1. AIM がインストールされてい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 powerha -u user -p password -h cluster_name [-t port]`

(1) コンソールに関する使用情報が表示されます。

(2) IBM PowerHA 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、IBM PowerHA の設定ファイル (`hacmp.cfg`) を `SystemEDGE_Install\path¥plugins¥AIPCommon` ディレクトリに書き込みます。

CA IBM SystemEDGE PowerHA AIM トラップ

CA SystemEDGE PowerHA AIM トラップ タイプ

CA SystemEDGE PowerHA AIM トラップ タイプのリストを以下に示します。
varbind の詳細については、MIB ファイルを参照してください。

hacmpAimInstanceAddedTrap

新しいインスタンスまたはサーバが追加されるとトラップを送信します。

トラップ ID : 165800

hacmpAimInstanceRemovedTrap

インスタンスまたはサーバが削除されるとトラップを送信します。

トラップ ID : 165801

hacmpAimInstanceDataStatusChanged

インスタンスまたはサーバデータ ステータスが変更されるとトラップを送信します。

トラップ ID : 165802

hacmpAimNodeAddedTrap

ノードが追加されるとトラップを送信します。

トラップ ID : 165803

hacmpAimNodeRemovedTrap

ノードが削除されるとトラップを送信します。

トラップ ID : 165804

hacmpAimResourceGroupAddedTrap

リソース グループが追加されるとトラップを送信します。

トラップ ID : 165805

hacmpAimResourceGroupRemovedTrap

リソース グループが削除されるとトラップを送信します。

トラップ ID : 165806

hacmpAimResourceGroupMigration

リソース グループがマイグレートされるとトラップを送信します。

トラップ ID : 165807

hacmpAimResourceAddedTrap

インスタンスまたはサーバ リソースが追加されるとトラップを送信します。

トラップ ID : 165808

hacmpAimResourceRemovedTrap

リソースが削除されるとトラップを送信します。

トラップ ID : 165809

Microsoft Cluster Service

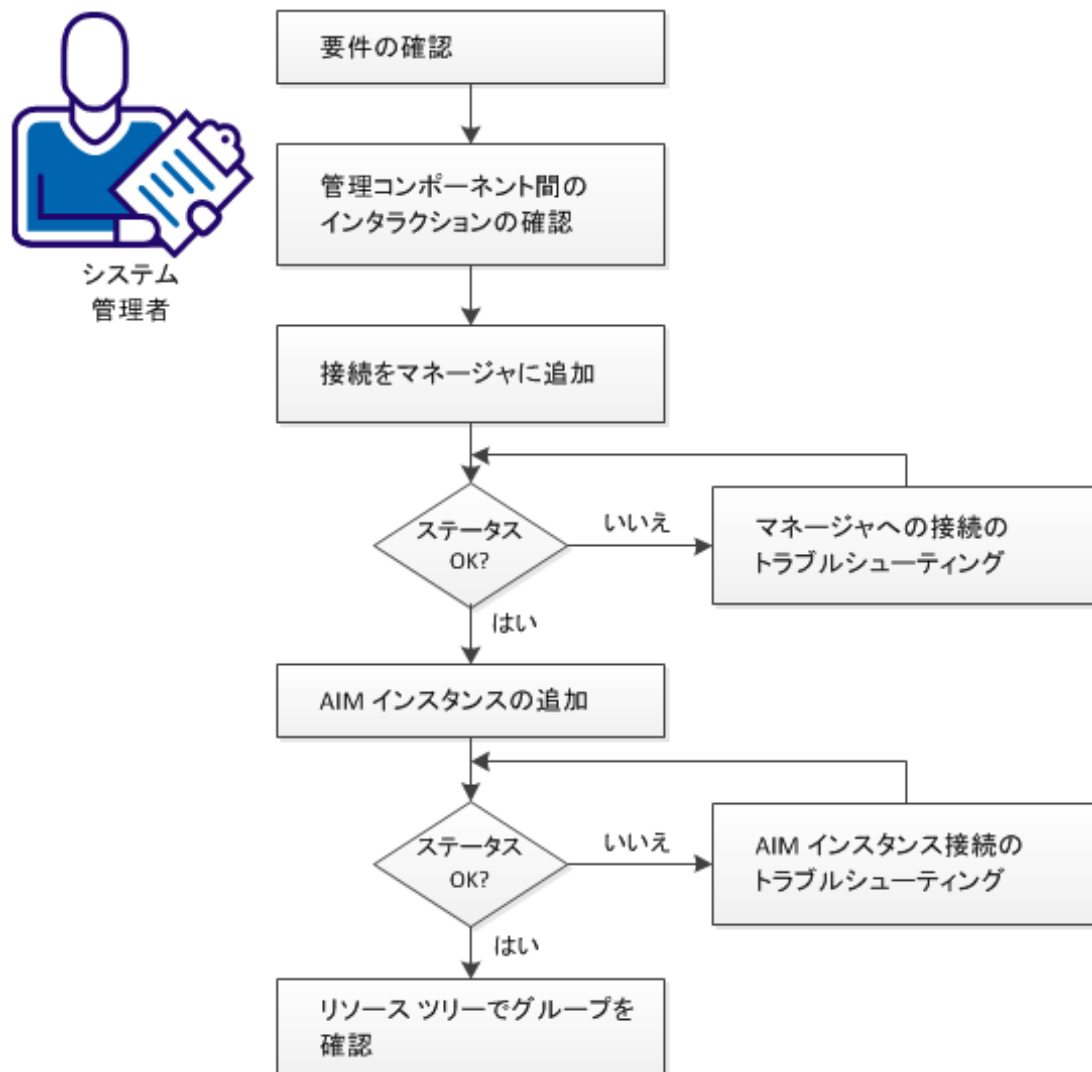
Microsoft Cluster Service (MSCS) は 2 つ以上のサーバを一緒に接続し、それらが単一のコンピュータとしてクライアントに表示されるようにします。クラスタ化によって、フェイルセーフアプリケーションを保有することができます。**Microsoft SQL Server** のようなクラスタ対応アプリケーションは一度にノード上で実行されます。そのノードがダウンした場合、別のノードがサービスを引き継ぎます。クラスタ化によって、アプリケーションが絶えず稼働されていることを確認することができます。

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 Cluster Service 管理コンポーネントを設定する方法

以下の図は、管理コンポーネントを設定するために必要なアクションの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。

管理コンポーネントの設定方法



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、アプリケーションを常に稼働させることができます。

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。

以下の手順に従います。

[要件の確認 \(P. 695\)](#)

[MSCS 管理コンポーネント間のインタラクション \(P. 697\)](#)

[マネージャへの Microsoft Cluster Service の追加 \(P. 699\)](#)

[サーバへのマネージャの接続が失敗する \(P. 700\)](#)

[検出された MSCS AIM インスタンスの追加 \(P. 702\)](#)

[AIM インスタンス接続のトラブルシューティング \(P. 703\)](#)

[リソース ツリーでの Microsoft Cluster Service の確認 \(P. 707\)](#)

要件の確認

CA Virtual Assurance の管理コンポーネントを設定する前に、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 および SystemEDGE に精通している。
- 以下を含む CA Virtual Assurance マネージャ インストールにアクセスできる。
 - プラットフォーム管理モジュール (PMM)
 - Application Insight Module (AIM)
 - モニタリング エージェント (SystemEDGE)
- CA Virtual Assurance ユーザ インターフェースにアクセスできる。
- 管理対象となる環境のサーバ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 サービスを通して使用する環境のサーバ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
- 使用する環境にあるサーバが正常に実行されていることを確認済みである。
- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM 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。
- 使用するリモート 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。

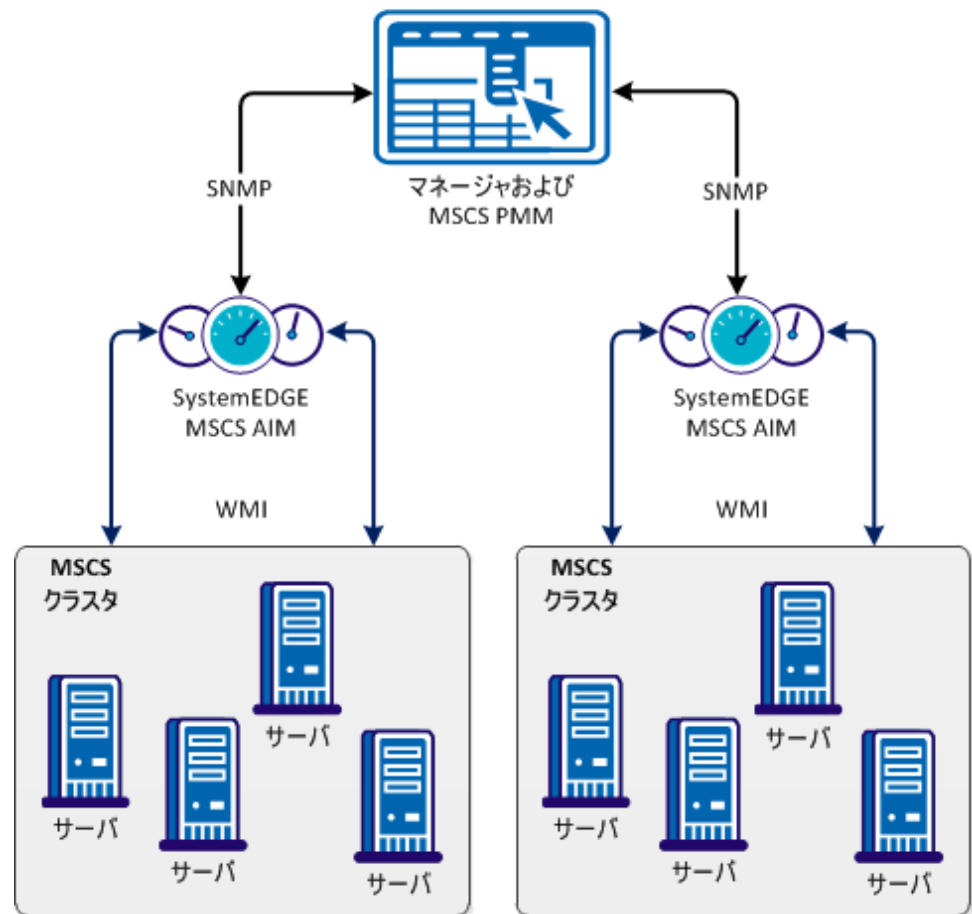
MSCS 管理コンポーネント間のインタラクション

以下の図は、**MSCS** モニタリング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 **MSCS AIM** は、同じ **Windows Server** 上で実行します。

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。

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。

MSCS 管理コンポーネント間のインタラクション



マネージャへの Microsoft Cluster Service 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、Microsoft クラスタを追加できます。

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 [Microsoft Cluster Services] を選択します。
3. [Microsoft Cluster Service] ペイン ツールバーの  (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. 必要な接続データ (サーバ名、ユーザ、パスワード、ポート) を入力し、優先 AIM を指定して、[管理ステータス] を有効にします。
5. [OK] をクリックします。

Microsoft クラスタが登録されます。

ネットワーク接続が正常に確立されている場合、右上のペインにサーバ追加され、緑のステータス アイコンが表示されます。

注: 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 によってサーバがリストに追加され、接続の失敗を示す赤のステータス アイコンが表示されます。 [いいえ] をクリックすると、何も追加されません。

サーバへのマネージャの接続が失敗する

症状:

「管理」 - 「設定」でサーバ接続を追加した後に、サーバ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。

- サーバへの接続に使用したデータが現在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。
- サーバ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。
- 接続に必要なすべてのサービスが、サーバシステム上で正しく実行されているかどうかを確認します。

サーバ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。
2. 接続の詳細を追加し、「管理ステータス」を有効にし、「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。
サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ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 <Server Name>
ping <IP Address of Server>
```

2. サーバに有効な DNS エントリおよび IP アドレスが設定されているかどうかを調べるには、これらのコマンドの出力を確認します。

サーバが DNS で見つからない場合は、CA Virtual Assurance マネージャ システム上にある Windows の hosts ファイルにサーバを追加します。手順 3 に進みます。

サーバが DNS で見つかった場合は、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 <Server Name>
```

正しい IP アドレスとサーバ名を入力してファイルを保存します。例：

```
192.168.50.50 myServer
```

4. CA Virtual Assurance ユーザ インターフェイスで、[管理] タブの [設定] に移動して、[サーバ] ペインの右上角にある  (検証) をクリックします。

サーバの認証情報と接続データが正しく、サーバに対して ping を実行できる場合でも、接続に失敗することがあります。このような場合は、サーバに問題がある可能性があります。サーバへの接続を確立できない場合は、次の手順に進みます。

接続に必要なすべてのサービスが、サーバシステム上で正しく実行されているかどうかを確認する方法

1. サーバにアクセスするために、システム管理者に問い合わせます。
2. サーバシステムにログインします。
3. 接続に必要なすべてのサービスが正しく実行されているかどうかを確認します。
4. 必要に応じて、サービスを開始または再起動します。
5. **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 [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 によってサーバ接続が検証されます。

サーバ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収集したデータが正しいことを確認してください。

管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

検出された MSCS AIM インスタンスの追加

CA Virtual Assurance マネージャに Microsoft Cluster Service 接続を追加した後、Microsoft Cluster Service 環境を管理するための AIM インスタンスを追加します。

次の手順に従ってください:

1. [スタート] メニューから **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 [Microsoft Cluster Service] を選択します。

3. [検出された Microsoft クラスタ AIM インスタンス] ペイン ツールバーの  (追加) をクリックします。

[クラスタ AIM インスタンスの追加] が表示されます。

4. ドロップダウン リストから [AIM ホスト] を選択します。

検出された AIM ホストのリストが表示されます。

5. ドロップダウン リストから [登録済みクラスタ] を選択します。

CA Virtual Assurance は、[登録済み Microsoft クラスタ] ペインに一覧表示されたクラスタ名が [登録済みクラスタ] ドロップダウン リストに入力されます。管理できるクラスタは、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。

注: AIM がリモート システムに存在している場合、CA Virtual Assurance でこのシステムを最初に検出する必要があります。検出後、AIM サーバがドロップダウン リストに表示されます。

6. [OK] をクリックします。

選択したクラスタの新しい 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、Microsoft Cluster Service 環境の管理を開始できます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

[管理] - [設定] でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  (ディスカバリが進行中) が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。ディスカバリにかかる時間は、環境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数によって異なります。アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Virtual Assurance はサーバフォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

[管理] - [設定] で AIM インスタンスを追加した後、ステータス アイコンに  (ポーリングなし) が表示されます。

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。このアイコンは、CA Virtual Assurance マネージャがこの AIM をポーリングしないこと表します。この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。別の AIM を使用したい場合は、[管理] - [設定] - [プロビジョニング] で優先 AIM を設定できます。サーバエントリの [編集] をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

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 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:

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。

- AIM サーバがアクセス可能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。

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. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

AIM サーバが 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 AIM サーバを追加します。手順 3 に進みます。

サーバが 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 AIM サーバの名前を入力します。例:

```
192.168.50.51 myAIM
```

4. [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. 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 [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 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、収集したデータがこのシナリオの要件に従っていることを確認してください。

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 AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン  (無効) が表示されます。この 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 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サーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

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。

- 欠落しているサーバから CA Virtual Assurance マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、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 Microsoft Cluster Service の確認

設定および検出に成功すると、新たに検出されたリソースが [リソース] - [エクスプローラ] ペインの対応するグループに表示されます。

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] ペインを開きます。
2. MSCS グループを展開します。

MSCS リソースが表示されます。

CA Virtual Assurance で、設定された MSCS 環境を管理する準備が整いました。MSCS リソースのステータスとプロパティをモニタできます。

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 Cluster Services] をクリックします。
[Microsoft Cluster Services] 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。

次の手順に従ってください:

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 Cluster Services] をクリックします。
[Microsoft Cluster Services] ページが表示されます。
3. [登録済み Microsoft クラスタ] セクションで、削除するクラスタを選択します。
4. [登録済み Microsoft クラスタ] ツールバー上で「-」（削除）をクリックします。
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 Cluster Services」をクリックします。
「Microsoft Cluster Services」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。

Microsoft Cluster Service の管理

Microsoft Cluster Service の管理では、Microsoft のクラスタ、サービスとアプリケーション、およびノードを管理できます。Microsoft Cluster Service は、すべてのクラスタを表示して管理操作を実行するための一元的な場所です。

このセクションでは、[リソース] ページから Microsoft クラスタ リソースに対して実行できる管理操作について説明します。[リソース] ページでは、以下のオブジェクトに関する基本情報と詳細情報を表示できます。

- Microsoft クラスタ
- サービスとアプリケーション
- ノード

[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。次に、いずれか 1 つのクラスタ リソースを選択し、そのリソースの [サマリ] をクリックします。

[サマリ] ページでは、オブジェクトに関連付けられている情報と、リソースに関連付けられているイベントを見ることができます。

Microsoft Cluster Service のモニタ

MS クラスタ リソースのステータスとプロパティは詳細にモニタすることができます。

クラスタリソースをモニタする方法

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. [Microsoft Cluster Service] フォルダを展開し、クラスタ オブジェクトをクリックします。

クラスタ ノードおよびサービス オブジェクトのリストが表示されます。

4. [サービスとアプリケーション] オブジェクトをクリックします。
サービスのリストが表示されます。

5. サービス オブジェクトをクリックします。

右側のペインに、一般情報、リソース、およびイベントが表示されます。

[一般情報] パネルには、サービス名、ステータス、および所属先クラスタの名前が表示されます。

[リソース] パネルの [概要] タブには、リソース名、タイプ、ステータスなどのリソース詳細が表示されます。 [リソース] パネルの [プライベート プロパティ] タブには、各リソースのプライベート プロパティが表示されます。

[イベント] パネルには、最新のイベントが表示されます。

第 8 章: エージェントレス モニタリング

CA Virtual Assurance は、サポートされた仮想環境（Hyper-V を除く）および Windows システム（リモート モニタリング）のエージェントレス モニタリングを提供します。

このセクションには、以下のトピックが含まれています。

[リモート モニタリング](#) (P. 713)

リモート モニタリング

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。

関連項目:

[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](#) (P. 714)

[リモート モニタリングの利点](#) (P. 716)

[機能と利点](#) (P. 716)

[アーキテクチャ](#) (P. 719)

[ユース ケース シナリオ](#) (P. 721)

[設定の前提条件](#) (P. 723)

[リモート モニタ システムの設定](#) (P. 724)

[設定セットの作成](#) (P. 727)

[リモート モニタリングを使用したシステムの管理](#) (P. 728)

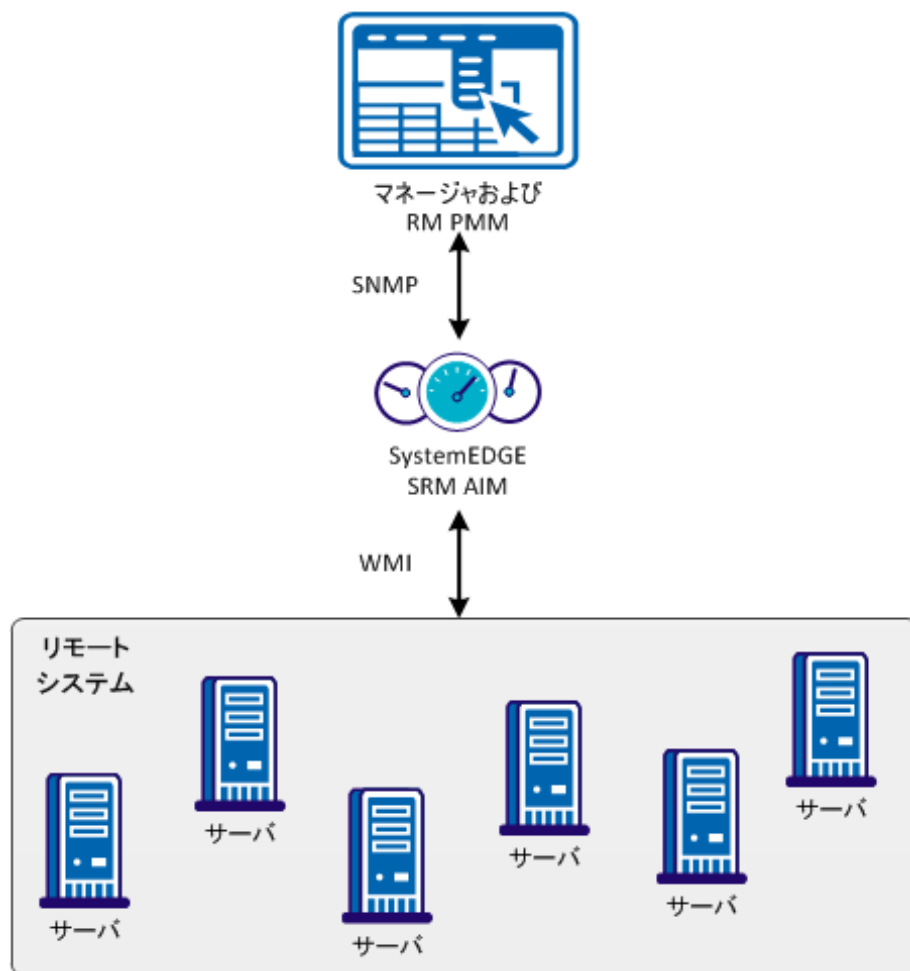
リモート モニタリング コンポーネント間のインタラクション

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（ポート 135）を実行することにより、Windows システム情報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）。

以下の図は、これらの関係を示しています。

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



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、eHealth、および Spectrum のマネージャから容易にアクセスできます。

自動化

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。

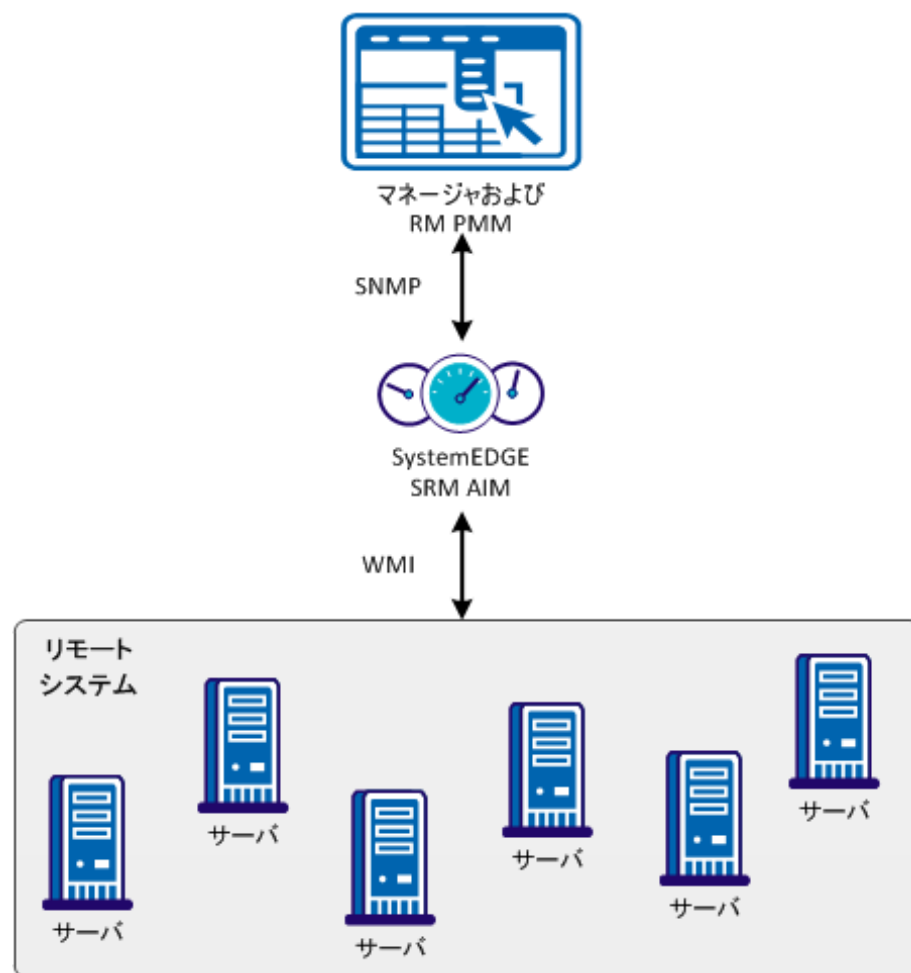
アーキテクチャ

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

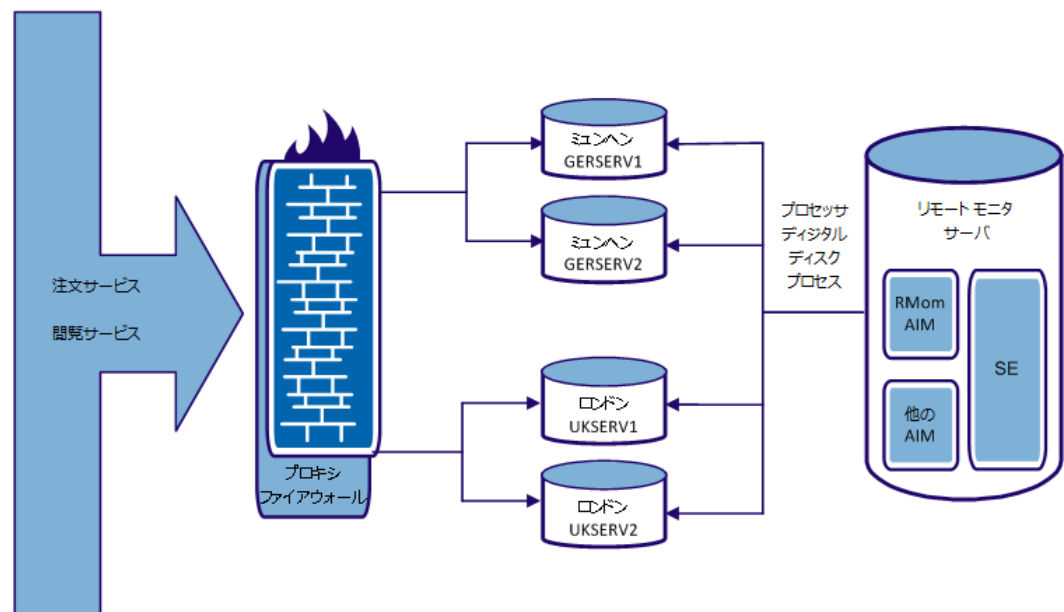


ユースケースシナリオ

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	order browse
GERSERV2	order
UKSERV1	order browse
UKSERV2	browse

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: 固定ポートの使用方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。

- デフォルト
- 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	デフォルト
Disk_PercentIdle	デフォルト
Event_SystemErrors	デフォルト
FSys_FreeMB	デフォルト
FSys_FreeMBDecrease	デフォルト
Mem_PercentUsed	デフォルト
Net_MACAddress	デフォルト
Net_MACIndex	デフォルト
Net_QueueLength	デフォルト
Proc_PercentCPU	デフォルト
Proc_PercentMemory	デフォルト
Srvc_StoppedAuto	デフォルト
Sys_LastBootTime	デフォルト
Sys_LastLocalTime	デフォルト
Sys_OSInfo	デフォルト
Sys_PhysMemKB	デフォルト
Disk_ReadPerSec	extended
Disk_WritePerSec	extended
Disk_QueueLength	extended
Mem_FreeMB	extended
Mem_FreePages	extended
Mem_NonPagedMB_3GB	extended

メトリック	設定セット
Mem_PagedMB	extended
Mem_PagedMB_3GB	extended
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、「Performance Metrics Reference」を参照してください。

設定セットの作成

リモート モニタリングには、変更すべきでない、すぐに使用できる設定セットが複数用意されています。自分のニーズに合ったカスタム設定セットを作成するには、[設定セット] ページを使用します。

設定セットを作成する方法

1. [+]（新規作成）をクリックします。
[個別設定セットの詳細] ペインが表示されます。
2. 新しい設定セットの名前と説明を入力し、新しいセットに含める設定セットを強調表示します（複数のエントリを強調表示するには、Ctrl キーを押しながら選択します）。
3. [保存] をクリックします。
新しい設定セットが [設定セット] リストに追加されます。

注: [アクション] ドロップダウンリストを使用すると、カスタム設定セットのクローン作成および削除もできます。

リモート モニタリング メトリックのサポート

CA Virtual Assurance はメトリックを収集し、デフォルト設定セット内の RM メトリックの固定セットに基づいてレポートを生成します。

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
- Svc_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

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

モニタリング対象のリモートシステムの追加

リモートでモニタするシステムのシステム情報を入力するには、[システム] ページを使用します。

システムを追加する方法

1. [+]（新規作成）をクリックします。
[新規作成] ペインが表示されます。
2. リモートでモニタするシステムの名前を [RM システム名] フィールドに入力し、以下の設定を編集します（必要に応じて）。

RM システム名

RM システムの名前を指定します。ユーザ インターフェースを使用して、FQDN 表記法でのみ RM システム名を入力する必要があります（「vm1234.ca.com」など）。「rmonwatch」ユーティリティを使用すると、RM システムをショート ネームまたは IP アドレスで指定することもできます。

ステータス

システムがアクティブまたは保守中のどちらであるかを指定します。

プロトコル

プロトコルが DCOM または SOAP のどちらかであることを指定します。

最大インスタンス

システムに対する任意のクエリによってインスタンス テーブル内に作成されるインスタンスの最大数を指定します。

認証情報

リモート システムのユーザ認証情報を指定します。

設定セット

リモート システムで収集される設定セット（またはメトリックのグループ）を指定します。

3. [保存] をクリックします。
リモートでモニタするシステムのリストにシステムが追加されます。

クエリ結果の表示

RM システムに関連付けられたクエリ結果を表示するには、[クエリ] ページを使用します。

[クエリ] ページでは、以下のアクションを実行できます。

- クエリの結果と設定の詳細を表示する（クエリ テーブルでクエリを強調表示し、[結果] または [設定] を選択します）。
- システム、ステータス、設定セット、または特定のクエリに基づいてクエリ結果をフィルタする（双眼鏡のアイコンでクエリ フィルタの表示/非表示を切り替えます）。
- クエリ テーブルに表示される情報を管理する（列見出しをクリックすると、列を昇順または降順で並べ替えたり、列を追加または削除したりできます）。

認証情報設定の管理

RM システムに関連付けられた個々の認証情報設定を管理するには、[認証情報] ページを使用します。

[認証情報] ページでは、以下のアクションを実行できます。

- 認証情報を追加する（[+]（新規作成）アイコンを使用し、[個別認証情報の詳細] ペインで設定を入力して、[保存] をクリックします）。
- 認証情報を削除する（既存の認証情報を強調表示し、[-] アイコンをクリックします）。
- 認証情報を編集する（既存の認証情報を強調表示し、[個別認証情報の詳細] ペインで設定を更新して、[保存] をクリックします）。

設定エントリの管理

クエリに関連付けられた設定を表示および管理するには、[設定エントリ] ページを使用します。

設定を表示または管理する方法

1. [設定エントリ] テーブル内のクエリを強調表示します。フィルタの表示/非表示アイコン（双眼鏡）を使用すると、設定セット、重大度、クエリ クラス、およびエスカレーション重大度のエントリにフィルタを適用できます。

[個別設定エントリの詳細] ペインが表示されます。

2. 以下の値を表示または更新し、[保存] をクリックします。

インデックス

設定セット内の設定エントリに対して一意のインデックスを指定します。

クエリ名

クエリの名前を指定します（「.」記号は使用できません）。

同じクエリ名を別の設定セット内に使用することもできます。ただし、システムに複数の設定セットを適用するときは、すべてのクエリ名が一意であることを確認してください。修飾子を固定エントリに設定した場合、クエリ名を変更することはできません。

説明

設定エントリの説明を指定します。

間隔

連続して行われるクエリ実行とモニタ評価の間隔を秒単位で指定します（値は 30 秒の倍数である必要があります）。

クエリ クラス

設定エントリのクエリ クラスを指定します。

クエリ スコープ

クエリに適用するスコープを指定します。

クエリ プロパティ

クエリ クラスのプロパティを指定します。

設定セット

設定セットの名前を指定します（「,」を使用しないでください）。

クエリ依存

あるクエリ（Q2）が別のクエリ（Q1）に依存することを指定します。つまり、Q2 は Q1 の結果に基づいてのみ作成されます。

修飾子

設定済みのクエリとモニタに関連する追加情報を指定します。

可能な値は、以下のとおりです。

- エントリは削除できず、クエリ名は変更できません（固定エントリ）
- クエリは 1 回のみ実行されます（少なくとも 1 回成功）
- クエリは、失敗するとそれ以上実行されません
- クエリ テーブルにクエリが表示されません
- 結果はインスタンスごとに表示されます
- 結果は現在の値の代わりに以前の値を示します
- 結果は増加デルタ値を示します
- 結果は減少デルタ値を示します
- 同じオブジェクト データと重大度を持つモニタを **AND** 関係として集計

クエリ合計

合計参照として適用するクエリ クラスのプロパティを指定します。

クエリスケール

プロパティ値に適用するスケールを指定します（*100、/1024、/1024*100 など）。このスケールは、クエリ テーブルでのクエリ スケールのデフォルトとして使用されます。クエリ プロパティの値は、結果属性に保存される前に、スケールによって乗算または除算されます。

クエリ インスタンス

インスタンス テーブルでインスタンスの名前付けに使用するクエリ クラスのプロパティを指定します。

条件

結果属性値を、しきい値およびエスカレーションしきい値と比較するための条件を指定します。

しきい値

結果属性値と比較するしきい値を指定します。

重大度

しきい値条件が満たされる場合に、SysEDGE オブジェクト状態モデルに使用する重大度を指定します。

オブジェクト クラス

SysEDGE オブジェクト状態モデルに使用するクラス名を指定します（「*」を使用しないでください）。

オブジェクト インスタンス

SysEDGE オブジェクト状態モデルに使用するインスタンス名を指定します（「*」を使用しないでください）。

オブジェクト 属性

SysEDGE オブジェクト状態モデルに使用する属性名を指定します（「*」を使用しないでください）。

遅延

SysEDGE オブジェクト状態モデルの状態変化が起きるために、しきい値（エスカレーション）条件が満たされる必要のある回数を指定します。

エスカレーション デルタ

エスカレーション条件を示すのに必要なしきい値との差分を指定します。

エスカレーション 重大度

エスカレーション条件が満たされる場合に、SysEDGE オブジェクト状態モデルに使用する重大度を指定します。

結果

SysEDGE モニタを使ってモニタするクエリ テーブルまたはインスタンス テーブル内のクエリの結果属性を指定します。

すべての変更が反映されるように、設定は更新されます。

第 9 章: Active Directory および Exchange Server 用の AIM のインストールおよび設定

このセクションには、以下のトピックが含まれています。

[はじめに](#) (P. 735)

[ADES AIM のスケーラビリティ](#) (P. 736)

[ADES AIM のインストール](#) (P. 737)

[Active Directory および Exchange Server のモニタリングの設定方法 \(オプション\) ノード設定ユーティリティを使用した ADES AIM の設定](#) (P. 757)

[ADES AIM のアンインストール](#) (P. 759)

[トラブルシューティング](#) (P. 759)

はじめに

Active Directory および Exchange Server (ADES) AIM では、Active Directory および Exchange Server 環境のヘルス状態およびキー パフォーマンス インジケータ (KPI) メトリックをモニタできます。ADES AIM には、以下の機能があります。

- 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、メール配信メトリック、論理ディスク使用率、および論理ディスク読み取り/書き込みをモニタします。
- アクティブ ディレクトリのパフォーマンス、レプリケーション、論理ディスク使用率、および論理ディスク読み取り/書き込みをモニタします。

ADES AIM は、モニタリングのために以下のデータを収集します。

- Active Directory と Exchange Server の設定データ
- Active Directory と Exchange Server のパフォーマンス データ

ADES AIM のスケーラビリティ

ADES AIM の展開を計画する場合、インフラストラクチャのサイジングおよびシステム パフォーマンスに影響を及ぼす以下のキー ファクタを考慮します。

- オペレーティング システムおよびその他のアプリケーションが使用するメモリを除き、ADES AIM が利用可能なメモリ
 - 1 GB の空きメモリがあるホストは 20 のホスト（2 台の Active Directory ホストと 18 台の Exchange ホスト）をモニタできます。
 - 2 GB の空きメモリがあるホストは 40 のホスト（6 台の Active Directory ホストと 34 台の Exchange ホスト）をモニタできます。
 - 3 GB の空きメモリがあるホストは 60 のホスト（10 台の Active Directory ホストと 50 台の Exchange ホスト）をモニタできます。
- 環境の地理的分布
 - ADES AIM が地理的に近い場所にある場合、環境の検出とポーリングにかかる時間が短縮されます。
 - 大きな遅延や多量のパケット損失は、AIM が必要なすべてのデータを取得できない原因となります。

注: サイジング情報は展開要件の概算であり、最終的なものではありません。サイジング情報はモニタリング環境によって異なります。

ADES AIM のインストール

ADES AIM をインストールするために以下のタスクを完了します。

1. CA SystemEDGE r11.6 エージェントおよび CA Advanced Encryption r11.6 をインストールします。
2. 以下のいずれかの方法を使用して、ADES AIM をインストールします。
 - CA Virtual Assurance リモート展開によって展開します。
 - コマンドモードによって手動でインストールします。
3. 以下の内容をモニタするドメインを指定して、ADES AIM を設定します。

注:

- ADES Manager と CA Spectrum を併用する場合は、ADES AIM ホストを管理するホストに SpectroSERVER をインストールしないでください。また、ADES AIM は SystemEDGE ホストにインストールされている唯一の AIM である必要があります。
- 他のドメインと信頼関係を持つドメインのいずれかのメンバサーバである Windows ホスト上に SystemEDGE および ADES AIM をインストールします。
- SystemEDGE エージェントおよび ADES AIM ホストには、Active Directory や Exchange Server の役割は設定できません。

リモート展開を使用した ADES AIM の展開

CA Virtual Assurance リモート展開を使用して、ADES AIM をホストにインストールするソフトウェア ジョブを作成します。

次の手順に従ってください：

1. CA Virtual Assurance アプリケーションにログインし、管理ビューに移動します。
2. [リソース] タブで、ADES AIM を展開するホストを検索します。
3. ジョブを作成し、プラットフォーム タイプとして **Windows** を選択します。利用可能なラッパー パッケージが表示されます。

ジョブの作成時に、ラッパー パッケージで以下のパラメータを指定します。

ユーザ

完全修飾ドメイン名 (FQDN) なしのドメイン管理者の名前を定義します。たとえば、**adminuser** と指定します。

パスワード

ユーザのパスワードを指定します。

ドメイン名

ADES AIM を介してモニタするドメインの名前を定義します。FQDN を入力します。

管理エンティティ

テクノロジーに基づき、管理するホストを指定します。

0

Active Directory ホストのみをモニタします。

1

Exchange Server ホストのみをモニタします。

2

Active Directory ホストと Exchange Server ホストの両方をモニタします。

管理モード

管理するホストを指定します。

0

管理エンティティで定義されるドメイン内のすべてのホストを自動的に検出してモニタします（ドメインベースの管理）。

注: 子ドメインのホストは自動的にモニタされません。

1

ドメイン内のホストをすべて検出しますが、マネージャによって設定されているホストのみをモニタします（ホストベースの管理）。

4. 必要なパッケージを選択し、ホストに展開します。

[ジョブ] パネルでジョブ ステータスを確認します。ジョブが失敗した場合は、再度パッケージを展開します。

注: 詳細については、「[SystemEDGE および AIM の展開方法 \(P. 142\)](#)」を参照してください。

コマンド モードでの ADES AIM のインストール

コマンド モードでのインストールでは、リモート展開を使用せずに、ホストに ADES AIM をインストールします。

注: ADES AIM をインストールする前に、CASystemEDGE r11.6 および CA Advanced Encryption r11.6 がホストにインストールされていることを確認してください。

次の手順に従ってください：

1. *DVD1¥Installers¥Windows¥Data¥SysMan* に移動して、以下の ZIP ファイルをローカルディスクにコピーします。
 - CA_SystemEDGE_ESAD-Windows.zip
 - CA_SystemEDGE_ESAD-Windows-metadata.zip
2. コピーした ZIP ファイルをローカルディスクに解凍します。解凍した場所で、以下のファイルが利用可能になります。
 - caesadaimx64.msi
 - ca-setup.exe
 - ca-setup.dat
3. コマンドプロンプトウィンドウを開き、*Extracted_Path¥CA_SystemEDGE_ESAD¥5.8.0¥ENU¥Windows_x64* に移動します。
4. ca-setup.exe を実行して、ADES AIM をインストールします。コマンドのフォーマットは、以下のとおりです。

```
ca-setup EULA_ACCEPTED="[yes|no]"
CASE_ESAD_DOMAIN_NAME="domain_name"
CASE_ESAD_DOMAIN_USER_NAME="username@fqdn"
CASE_ESAD_DOMAIN_PWD="password"
CASE_ESAD_MANAGEMENT_ENTITY="[0|1|2]"
CASE_ESAD_MANAGEMENT_MODE="[0|1]"
EULA_ACCEPTED="[yes|no]"
```

ライセンスが許可されるかどうかを指定します。

```
CASE_ESAD_DOMAIN_NAME="fully_qualified_domain_name"
```

ADES AIM を介してモニタするドメインの完全修飾名を指定します。

```
CASE_ESAD_DOMAIN_USER_NAME="username@fqdn"
```


ドメイン管理者権限および Exchange Organization Administrator 権限、または Organization Management 権限を持つユーザの名前を指定します。

`CASE_ESAD_DOMAIN_PWD="password"`

ユーザのパスワードを指定します。

`CASE_ESAD_MANAGEMENT_ENTITY="[0|1|2]"`

テクノロジーに基づき、管理するホストを指定します。

0

Active Directory ホストのみをモニタします。

1

Exchange Server ホストのみをモニタします。

2

Active Directory ホストと Exchange Server ホストの両方をモニタします。

`CASE_ESAD_MANAGEMENT_MODE="[0|1]"`

管理するホストを指定します。

0

管理エンティティで定義されるドメイン内のすべてのホストを自動的に検出してモニタします（ドメインベースの管理）。

注: 子ドメインのホストは自動的にモニタされません。

1

ドメイン内のホストをすべて検出しますが、マネージャによって設定されているホストのみをモニタします（ホストベースの管理）。

5. SystemEDGE サービスを再起動して、ADES AIM を実行します。

例

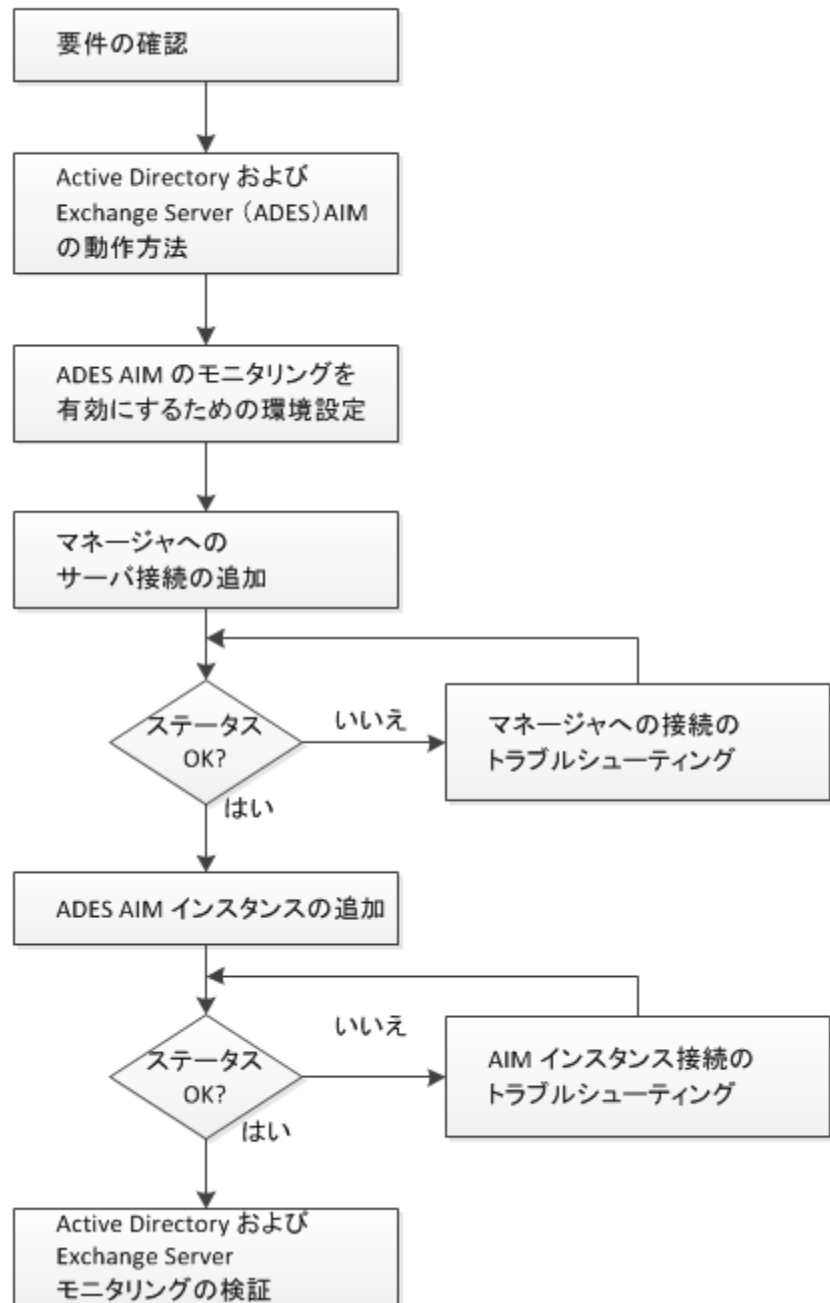
以下の例は、ADES AIM をホストにインストールし、ドメイン mydomain.com をモニタする方法を示しています。

```
ca-setup EULA_ACCEPTED="yes"
CASE_ESAD_DOMAIN_NAME="mydomain.com"
CASE_ESAD_DOMAIN_USER_NAME="adminuser@mydomain.com"
CASE_ESAD_DOMAIN_PWD="domainpass123" CASE_ESAD_MANAGEMENT_ENTITY="2"
CASE_ESAD_MANAGEMENT_MODE="0"
```

Active Directory および Exchange Server のモニタリングの設定方法

以下の図は、管理コンポーネントを設定するために必要なアクションの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。

Active Directory および Exchange Server のモニタリングの設定方法



以下の手順に従います。

[要件](#) (P. 745)

[Active Directory および Exchange Server AIM の動作方法](#) (P. 746)

[ADES AIM のモニタリングを有効にするための環境設定](#) (P. 748)

[ドメインサーバまたは Exchange Server のマネージャへの追加](#) (P. 749)

[マネージャへのサーバ接続の失敗](#) (P. 750)

[ADES AIM インスタンスの追加](#) (P. 752)

[AIM インスタンス接続のトラブルシューティング](#) (P. 753)

[Active Directory および Exchange Server モニタリングの検証](#) (P. 757)

要件

以下の前提条件が ADES AIM をインストールおよび設定するのに必要です。

一般的な要件

- CA Virtual Assurance を使用してサーバを検出し、パッケージを展開するための知識。
- 必要な権限
 - リモート展開用の権限を持つユーザ アカウント。
 - 手動インストール用のホスト上のローカル管理者権限を持つユーザ アカウント。
 - ドメインをモニタリングするためのドメイン管理者権限と Exchange Organization Administrator 権限、または Exchange Organization Management 権限。

注：ドメイン管理者権限と Exchange Organization Administrator 権限が同じユーザに割り当てられていることを確認します。

ソフトウェア要件

- ADES AIM ホストがサポートされているオペレーティング環境
 - Windows Server 2008 SP2
 - Windows 2008 R2 SP2 x64
- サポートされているドメイン コントローラの動作環境：
 - Windows 2008
 - Windows 2008 R2
- サポートされている Exchange Server バージョン：
 - Exchange 2007 SP3
 - Exchange 2010 SP2

注：

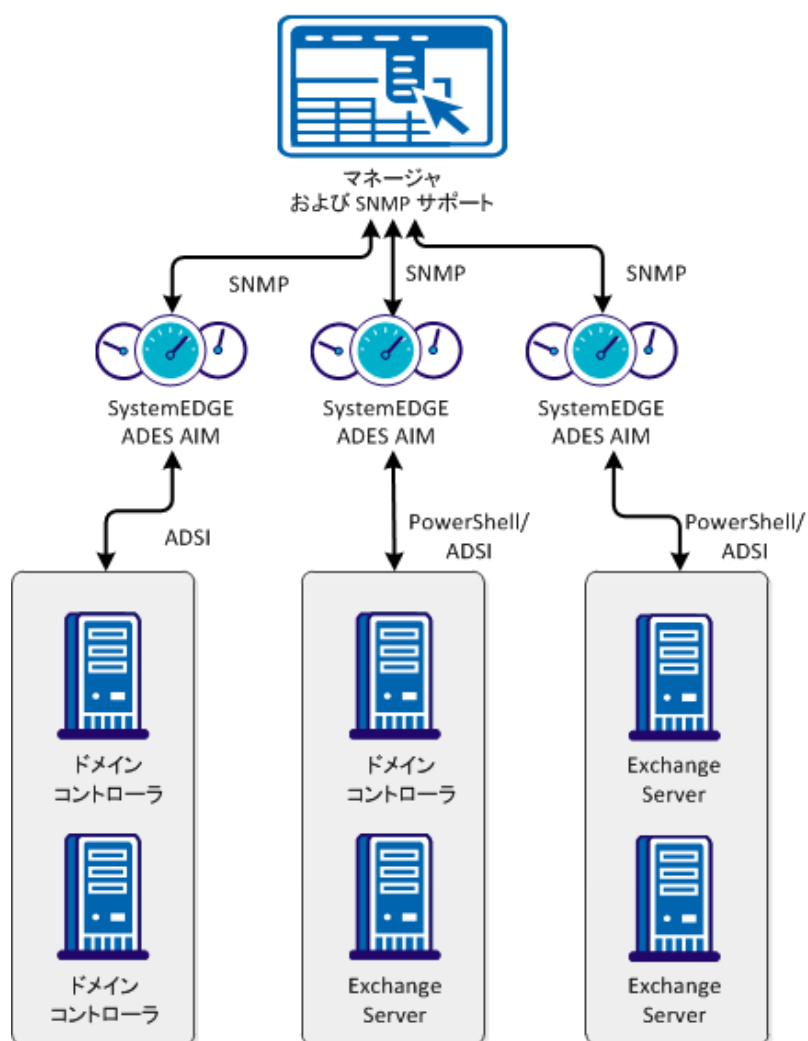
- Exchange 2003 ホストのモニタリングはサポートされていません。
- フォレスト間での Exchange 2007 ホストのモニタリングはサポートされていません。
- 必要なアプリケーション

- .Net 3.5 以降のバージョン
- Windows PowerShell 2.0
- Exchange 2007 ホストをモニタリングするための Exchange 2007 Management Tools SP3
- CA SystemEDGE リリース r11.6 および CA Advanced Encryption r11.6

Active Directory および Exchange Server AIM の動作方法

以下の図は、ADES AIM のアーキテクチャを示しています。

Active Directory および Exchange Server の管理コンポーネント間のインタラクション



以下のプロセスでは、ADES AIM の仕組みについて説明します。

1. ADES AIM はドメイン コントローラを検索してホストを検出します。
ADES AIM は、以下に関する情報を収集します。
 - ドメイン コントローラやグローバル カタログなどの **Active Directory** サーバの役割。
 - ハブ トランスポート、メールボックス、およびクライアント アクセス サーバなどの **Exchange Server** の役割。

注: ユニファイド メッセージングおよびエッジ トランスポートの役割は、モニタリングに対してはサポートされていません。
2. ホストが検出されると、AIM は以下からデータを収集するメッセージを送信します。
 - ドメイン コントローラ (ADSI コールを使用)
 - Exchange Server (PowerShell コマンドを使用)
3. AIM はデータを受信し、SystemEDGE エージェントについて MIB テーブルを更新します。
4. CA eHealth や CA Spectrum などのマネージャは、SystemEDGE ホストにポーリングして、表示するデータを収集します。
5. AIM は管理対象ホスト (モニタリング用に設定されている **Active Directory** と **Exchange Server** ホスト) に継続的にポーリングして、その MIB テーブルを更新します。

ADES AIM のモニタリングを有効にするための環境設定

Exchange ホスト上で PowerShell 設定を適用して、ADES AIM がドメインをモニタできるようにします。

注: モニタリングを開始する前に、すべての Exchange Server を設定します。

次の手順に従ってください：

1. [スタート] - [プログラム] - [アクセサリ] - [Windows PowerShell] - [Windows PowerShell (x86)] を選択します。

Windows PowerShell コマンドプロンプトが表示されます。

2. 以下のコマンドを実行して、WinRM サービスを介してホストをリモートで管理できるようにします。

Enable-PSRemoting

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。

3. 以下のコマンドを実行して、信頼されたホストのリストにホストを追加します。

Set-Item WSMan:Localhost¥Client¥TrustedHosts -Value * -Force

4. 以下のコマンドを実行して、WinRM サービスを再開します。

Restart-Service WinRM

TrustedHosts 設定が更新され、Exchange Server のモニタリングが利用可能になります。

ドメイン サーバまたは Exchange Server のマネージャへの追加

ユーザ インターフェースを使用して、Microsoft Active Directory ドメイン コントローラまたは Exchange Server の接続をマネージャに追加できます。

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. 左ペインの [プロビジョニング] セクションから [Microsoft Active Directory および Exchange Server] を選択します。
3. [サーバ] ペイン ツールバーの  (追加) をクリックします。
[サーバの追加] ダイアログ ボックスが表示されます。
4. 必要な接続データ (サーバ名、ユーザ、パスワード、モード、テクノロジー) を入力し、優先 AIM を指定して、[管理ステータス] を有効にします。
5. [OK] をクリックします。

CA Virtual Assurance はサブミットされた接続データを検証し、サーバへの接続を確立しようとします。

ネットワーク接続が正常に確立されている場合は、右上のペインにサーバが緑のステータス アイコンを使って追加されます。

注: 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 によってサーバがリストに追加され、接続の失敗を示す赤のステータス アイコンが表示されます。 [いいえ] をクリックすると、何も追加されません。

マネージャへのサーバ接続の失敗

症状:

[管理] - [設定] でサーバ接続を追加した後、サーバ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。

- サーバの接続に使用したデータ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。
- サーバ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。
- サーバシステム上で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。

サーバ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。
2. 接続の詳細を追加し、[管理ステータス] を有効にし、[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。
サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ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 <Server Name>
ping <IP Address of Server>
```

2. 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。

サーバが 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 ファイルにサーバを追加します。手順 3 に進みます。

サーバが 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 <Server Name>
```

正しい IP アドレスとサーバの名前を入力します。例：

```
192.168.50.50 myServer
```

4. 右上角の （検証）をクリックします。

サーバの認証情報と接続データが正しく、サーバに対して 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、サーバに問題がある可能性があります。サーバへの接続を確立できない場合は、次の手順に進みます。

サーバシステム上で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. サーバシステムにアクセスする方法を管理者に問い合わせます。
2. サーバ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. サービスを選択し、その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 [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 によってサーバの接続が検証されます。

サーバ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有効であることを確認してください。

管理者またはサポート担当者と協力して、サーバの接続の問題を解決します。

ADES AIM インスタンスの追加

Active Directory および Exchange Server の接続を CA Virtual Assurance マネージャに追加した後、環境を管理するために AIM インスタンスを追加します。

次の手順に従ってください:

1. [スタート] メニューから **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. 左ペインの [プロビジョニング] セクションから [Microsoft Active Directory および Exchange Server] を選択します。

3. [AIM サーバ] ペイン ツールバーの  (追加) をクリックします。
[AIM サーバの追加] ダイアログ ボックスが表示されます。

4. ドロップダウン リストから [AIM ホスト] を選択します。
検出された AIM ホストのリストが表示されます。

5. ドロップダウン リストからサーバを選択します。

CA Virtual Assurance によって、[サーバ] ペインに一覧表示されたサーバ名がサーバ ドロップダウン リストに入力されます。管理できるサーバは、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。

注: AIM がリモートシステムに存在している場合、CA Virtual Assurance でこのシステムを最初に検出する必要があります。検出後、AIM サーバがドロップダウン リストに表示されます。

6. [OK] をクリックします。

選択したサーバの新しい 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環境の検出を開始します。ディスカバリ プロセスが完了すると、Active Directory および Exchange Server の環境のモニタリングを開始できます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

[管理] - [設定] でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  (ディスカバリが進行中) が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。ディスカバリにかかる時間は、環境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数によって異なります。アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Virtual Assurance はサーバフォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

[管理] - [設定] で AIM インスタンスを追加した後、ステータス アイコンに  (ポーリングなし) が表示されます。

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。このアイコンは、CA Virtual Assurance マネージャがこの AIM をポーリングしないこと表します。この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。別の AIM を使用したい場合は、[管理] - [設定] - [プロビジョニング] で優先 AIM を設定できます。サーバエントリの [編集] をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

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 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:

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。

- 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。

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. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

AIM サーバが 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 AIM サーバを追加します。手順 3 に進みます。

サーバが 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 AIM サーバの名前を入力します。例:

```
192.168.50.51 myAIM
```

4. [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. 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 [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 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、収集したデータがこのシナリオの要件に従っていることを確認してください。

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 AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン  (無効) が表示されます。この 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 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サーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

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。

- 欠落しているサーバから CA Virtual Assurance マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、その管理ステータスを「有効」に変更します。

Active Directory および Exchange Server モニタリングの検証

設定が正常に実行された後、CA Virtual Assurance は Active Directory および Exchange Server のモニタリングを開始します。Active Directory および Exchange Server のイベントをユーザ インターフェイスでモニタします。

(オプション)ノード設定ユーティリティを使用した ADES AIM の設定

ユーザ インターフェイスの代わりに NodeCfgUtil を使用して ADES AIM を設定する方法もあります。ADES AIM を設定することで、ADES AIM で管理する 1 つ以上のドメインを追加、変更、または削除できます。NodeCfgUtil は、ADES AIM の設定ファイル (esad.cfg) を作成します。このファイルは、`SystemEDGE_InstallPath¥plugins¥AIPCommon` ディレクトリにあります。

次の手順に従ってください：

1. 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ます。
2. NodeCfgUtil.exe を起動します。
3. 選択に応じてオプションを入力します。ドメインの追加、変更、または削除ができます。たとえば、「1」を入力して新しい管理対象ノードを追加します。
4. [管理対象ノードの選択]画面内の ADES AIM に対応する数を入力します。たとえば、「1」を入力して ADES AIM を選択します。
5. 画面上の指示に従って、設定を完了します。各ドメインには、認証用の有効なユーザ名とパスワード、および適切な管理エンティティと管理モードが必要です。
6. 設定が完了したら、「0」を入力して設定を保存し、ユーティリティを終了します。
7. SystemEDGE サービスを再起動して、変更を適用します。

例

以下の例は、ADES AIM の設定に正常に追加された mydomain.net に関する [管理対象ノードのインストール] ダイアログ ボックスを示しています。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ベースで設定されます。

**** 管理対象ノードの選択 ****

1. Microsoft Active Directory および Exchange Server

0. 前のメニューに戻る

選択項目を入力してください: 1

Microsoft Active Directory および Exchange Server 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 (FQDN) : mydomain.com

2. ユーザ名 (例: adminuser@domain.com) : administrator@mydomain.com

3. パスワード: *****

4. 管理エンティティ (0: AD のみ、1: Exchange のみ、2: AD と Exchange の両方) : 0

5. 管理モード: (0: ドメイン ベース/自動、1: ホスト ベース/手動) : 0

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。 . . .

ADES AIM のアンインストール

エージェントをアンインストールすると、エージェントおよびその関連する設定データがホストから削除されます。

次の手順に従ってください：

1. SystemEDGE コントロール パネルを使用して、SystemEDGE プロセスを停止します。
2. [スタート] - [コントロール パネル] - [プログラム] - [プログラムと機能] を選択します。

[プログラムのアンインストールまたは変更] ウィンドウが開きます。

3. Exchange Server および Active Directory コンポーネント用の CA AIM を右クリックし、[アンインストール] を選択します。

確認メッセージが表示されます。

4. [はい] をクリックします。

ADES AIM コンポーネントが削除されます。ADES AIM コンポーネントが [追加/削除] コントロール パネルに表示されていないことを確認します。

トラブルシューティング

関連項目：

[AIM が非アクティブで、データを収集していない \(P. 760\)](#)

[1 つ以上のドメインがモニタされない \(P. 761\)](#)

[一部のカウンタがモニタされない \(P. 761\)](#)

[一部のホストがモニタされない \(P. 762\)](#)

AIM が非アクティブで、データを収集していない

症状

AIM が非アクティブになっていて、データを収集できません。

解決策

以下を確認してください。

- `caesadaim.exe` プロセスが実行中である。
- 設定済みのすべてのドメインに対して、AIM ディレクトリ内にドメインのログ ファイルが作成されている。

プロセスが実行中でないか、ログ ファイルが作成されていない場合は、SystemEDGE サービスを再起動します。

SystemEDGE サービスを再起動しても AIM が実行されない場合は、以下の要件を確認して適切な処置を行います。

- AIM ホストに .NET 3.5 SP1 Framework がインストールされている。
- AIM と同じホストに Exchange Management Tools 2007 SP3 がインストールされている（ドメインに Exchange 2007 Server が 1 台以上含まれている場合）。

1 つ以上のドメインがモニタされない

症状

ADES AIM が 1 つ以上のドメインをモニタしません。

解決策

- ADES AIM フォルダに、モニタ対象の各ドメインのログ ファイルが `domain_AIM.log` という名前で作成されていることを確認します。ログ ファイルが作成されていない場合は、`nodecfgutil.exe` を使用したモニタリングの対象としてドメインが設定されていることを確認します。
- ドメインのログ ファイルが作成されている場合は、ログ ファイルを開き、以下のエラー メッセージを探します。

The specified domain does not exist or cannot be contacted.

このメッセージがログ ファイルに含まれている場合は、ADES AIM ホストとドメイン コントローラ間の通信がブロックされていないことを確認します。ドメイン コントローラが ADES AIM ホストからアクセス可能な場合は、CA Spectrum で AIM のディスカバリを開始します。

一部のカウンタがモニタされない

症状

一部のパフォーマンス カウンタがモニタされません。

解決策

ADES AIM で検出を再度開始して、カウンタが存在しないホスト上にカウンタを作成します。

注: 特定の設定に対して表示されるパフォーマンス カウンタは、必要な設定またはインスタンスがホストで利用可能な場合にのみモニタされます。

一部のホストがモニタされない

症状

ドメイン内の **Active Directory** ホストおよび **Exchange Server** ホストでモニタされていないものがあります。

解決策

以下の設定を確認してください。

- AIM がドメイン モードまたはホスト モードで設定されている。

注: ホスト モードでは、ユニバーサル ホスト テーブルにあるホストごとに、**CA Spectrum** または **MIB** ブラウザを使用して管理ステータスを変更します。

- AIM が **Active Directory** ホストのみ、または **Exchange Server** ホストのみをモニタするように管理エンティティで設定されている。**ADES AIM** が両方のテクノロジーをモニタするように、**NodeCfgUtil** を使用して、ドメインの [管理エンティティ] オプションの値を **2** に変更します。

第 10 章：ルールとアクションの使用

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. 763)

[ポリシーのユース ケース](#) (P. 880)

[データ収集の設定](#) (P. 882)

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、「Performance Metrics Reference」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マ 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。

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、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。

事前定義済みアクションタイプのリスト

このセクションでは、ポリシー ルールのアクションを作成するのに利用できる、以下の事前定義済みアクションタイプについて説明します。

ディスクの追加: VMware vCenter

ディスクの追加アクション タイプでは、仮想マシンにディスクを追加できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Virtual Center

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

データセンター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。ドロップダウン リストから 1 つ選択します。

仮想マシン

ディスクの追加先となる仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。

データストア

選択した VM の ESX サーバに関連付けられているデータストアの名前を指定します。ドロップダウン リストから 1 つ選択します。

ドライブ サイズ

追加ディスクのサイズを指定します。値を入力し、ドロップダウン リストから [MB] または [GB] を選択します。

SCSI コントローラ

追加ディスクの作成に使用する SCSI コントローラを指定します。ドロップダウン リストから 1 つ選択します。

[シンプロビジョニング]チェック ボックス

シンプロビジョニングを有効にするかどうかを指定します。

ディスク モード

ディスク モードを指定します。ドロップダウン リストから、以下のいずれかを選択します。

- 永続
- 独立永続
- 独立非永続

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウン リストから有効なチケット タイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウン リストからテンプレートを選択します。選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

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。

ネットワーク インターフェースの追加: VMware vCenter

ネットワーク インターフェースの追加アクション タイプを使用すると、仮想マシンに仮想 NIC を追加できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Virtual Center

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

データセンター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。ドロップダウン リストから 1 つ選択します。

仮想マシン

仮想 NIC の追加先となる仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。

デバイス タイプ

デバイス タイプを指定します。ドロップダウン リストから 1 つ選択します。

ネットワーク

選択した VM の ESX サーバに関連付けられているネットワークを指定します。ドロップダウン リストから 1 つ選択します。

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。

MAC アドレス

(オプション) MAC アドレスを指定します。MAC アドレスが自動生成されるようにしたい場合は、フィールドを空白のままにします。

[ウェイク オン ラン]チェック ボックス

仮想 NIC の LAN 上でのウェイクアップを設定するかどうかを指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウン リストから有効なチケット タイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウン リストからテンプレートを選択します。選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

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。

サーバをサービスに追加

サーバをサービスに追加アクション タイプでは、既存のサービスにサーバを追加できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

サービス名

サービスの名前を指定します。

サーバリスト(カンマで区切られたリスト)

サービスに追加するサーバのリストを指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

マシン状態の変更: Microsoft Hyper-V

マシン状態の変更アクション タイプでは、Hyper-V 環境内の仮想マシンの状態変更を制御します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Hyper-V ホスト

Hyper-V Server が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

Hyper-V VM 名

状態を変更する仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。

状態

仮想マシンの希望する状態を指定します。ドロップダウン リストから、以下のいずれかを選択します。

- 電源オフ
- シャットダウン
- 保存
- 中断
- 開始

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

マシンのクローン作成: Solaris ゾーン

Solaris ゾーン マシンのクローン作成アクションタイプでは、既存のゾーンからデータをコピーすることにより、新しいゾーンを設定およびインストールします。この操作を、グローバルゾーンまたはインストールされた状態のゾーンに対して実行することはできません。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

ゾーン ホスト

クローン作成するゾーンが含まれる Solaris ゾーン ホストを定義します。

ゾーン

クローン作成するゾーンを定義します。イベント メッセージから抽出されたテキストを使用できます。

名前

新しいゾーンの名前を定義します。自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

パス

新しいゾーンのインストール パスを定義します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウン リストから有効なチケット タイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウン リストからテンプレートを選択します。選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

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。

CPU/メモリの設定: IBM LPAR

CPU/メモリの設定アクション タイプでは、**IBM LPAR** 環境内の仮想マシンに割り当てる **CPU** リソースとメモリ リソースに対して制限を設定できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

HMC/IVM 名

選択したパーティションが存在する管理対象サーバに関連付けられた HMC/IVM を指定します。

システム名

仮想マシンが存在する **IBM LPAR** のデータ センターの名前を指定します。ドロップダウン リストから 1 つ選択します。

パーティション名

パーティションの一意の名前を表示します。

プロファイル名

選択した **LPAR** の既存のプロファイル名を指定します。

オペレーション

実行する操作を指定します。ドロップダウン リストから、以下のいずれかを選択します。

- メモリ ユニットの追加
- メモリ ユニットの削除
- プロセッサの追加
- プロセッサの削除

プロセッサ

追加または削除するプロセッサの数を指定します。

調整タイプ

調整タイプを指定します。 オプションを 1 つ選択します。

- 動的調整のみ
- 動的調整およびプロファイル更新

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

CPU/メモリの設定: Microsoft Hyper-V

CPU/メモリの設定アクションタイプでは、Hyper-V 環境内の仮想マシンに割り当てる CPU 共有とメモリ共有の数を制御します。

アクション定義の [詳細] セクションには、以下のフィールドがあります。

Hyper-V ホスト

Hyper-V Server が常駐するサーバの名前を指定します。ドロップダウンリストから 1 つ選択します。

Hyper-V VM 名

状態を変更する仮想マシンの名前を指定します。ドロップダウンリストから 1 つ選択します。

CPU 割り当て

仮想マシンの CPU 割り当てを指定します。ドロップダウンリストから、以下のいずれかを調整します。

- CPU 数
- CPU 予約 %
- CPU の重み
- CPU 制限 %
- 現在の CPUID

メモリ割り当て

仮想マシンに割り当てるメモリ共有を指定します（メガバイト）。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

CPU/メモリの設定: VMware vCenter

CPU/メモリの設定アクションタイプでは、CPU リソースとメモリ リソースに対して制限を設定できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウンリストから 1 つ選択します。

VC データ センター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。ドロップダウンリストから 1 つ選択します。

ターゲット VM マシン

リソース調整の対象となる仮想マシンの名前を指定します。ドロップダウンリストから 1 つ選択します。あるいは、自動生成されるテキストや、イベントメッセージから抽出されるテキストを使用できます。

操作

実行する操作を指定します。ドロップダウン リストから、以下のいずれかを選択します。

- CPU 制限の設定
- メモリ制限の設定
- CPU 予約の設定
- メモリ予約の設定

MHz、MB

選択した操作について適切な値を入力します。

[無制限]チェック ボックス

選択した操作においてリソースを無制限に使用することを許可します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウン リストから有効なチケット タイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウン リストからテンプレートを選択します。選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

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。

電源の設定: Cisco UCS

このアクションタイプでは、UCS ブレードサーバ用の電源管理アクションを設定できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

UCS Manager

UCS Manager の名前を指定します。

UCS シャーシ

UCS シャーシの名前を指定します

UCS ブレード

UCS ブレードの名前を指定します

電源操作

ドロップダウンリストから操作を選択します。

サイクル即時

ただちにブレードの電源をオンにしてオフにします。

サイクル待機

ブレードの電源を入れ直し、すべてのアプリケーションにシャットダウンを通知します。

ハードリセット即時

ブレードの電源を入れ直します（ブレードの電源プラグを抜くのと似た作用です）。

ハードリセット待機

ブレードの電源をオフにします。電源をオフにする前に、ブレードによってすべてのアプリケーションにシャットダウンが通知されます。

ソフトシャットダウン

ブレードをシャットダウンします。シャットダウンする前に、ブレードによってすべてのアプリケーションにシャットダウンが通知されます。

シャットダウン

ブレードをただちにシャットダウンします。

起動

ブレードを起動します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

電源の設定: IBM LPAR

LPAR 電源の設定アクション タイプでは、LPAR の電源設定を制御します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

HMC/IVM 名

選択したパーティションが存在する管理対象サーバに関連付けられた HMC/IVM を指定します。

システム名

仮想マシンが存在する IBM LPAR のデータ センターの名前を指定します。ドロップダウンリストから 1 つ選択します。

パーティション名

制御するパーティション名を指定します。

操作

実行する電源操作を指定します。[アクティブ化]を選択する場合は、[操作オプション] セクション内の以下のフィールドに入力します。

パーティション プロファイル

電源設定のアクティブ化に使用するパーティション プロファイルを指定します。

キー ロック

パーティション プロファイル内のキー ロック モードを指定します。キー ロックによって、システムで許可される電源オンと電源オフのモードが確立されます。キー ロックは、**manual** または **normal** のいずれかです。セキュリティ上の理由により、キー ロック位置を **manual** に設定することは推奨されません。

起動モード

パーティションプロファイル内の起動モードを指定します。パーティションプロファイルをアクティブ化するときには別の方法を指定する場合を除き、この起動モードを使って論理パーティション上のオペレーティングシステムが起動されます。CA Virtual Assurance は以下の有効な起動モードをサポートしています。

normal

論理パーティションを **normal** として開始します。（多くの日常的なタスクを実行するには、このオプションを使用します）。

open_firmware

論理パーティションを起動して **Open Firmware** のプロンプトを表示します。サービス担当者は、このオプションを使って追加のデバッグ情報を取得します。

[シャットダウン] を選択する場合は、[操作オプション] セクション内の以下のフィールドに入力します。

遅延

遅延のあるシャットダウンシーケンスを使用して、論理パーティションをシャットダウンします。このシーケンスでは、ジョブを終了し、ディスクにデータを書き込むための論理パーティション時間が考慮されます。論理パーティションは、事前定義された時間内にシャットダウンできない場合、異常終了します。次の再起動は通常より時間がかかる場合があります。

即時

論理パーティションをただちにシャットダウンします。HMC はアクティブなすべてのジョブをただちに終了します。そのようなジョブで実行されているプログラムは、いかなるジョブのクリーンアップも許可されません。データが部分的に更新されている場合、このオプションを使用すると好ましくない結果になる可能性があります。このオプションを使用するのは、制御されたシャットダウン試行が失敗した後だけにしてください。

OS のシャットダウン

論理パーティションに対して **shutdown** コマンドを発行することによって、論理パーティションを通常どおりにシャットダウンします。この操作中、論理パーティションは必要なシャットダウンアクティビティをすべて実行します。このオプションは AIX 論理パーティションでのみ利用できます。

OS のシャットダウン即時

論理パーティションに対して **shutdown -F** コマンドを発行することによって、論理パーティションをただちにシャットダウンします。この操作中、論理パーティションは他のユーザおよび他のシャットダウン アクティビティへのメッセージをバイパスします。このオプションは AIX 論理パーティションでのみ利用できます。

[再起動] を選択する場合は、[操作オプション] セクションから 1 つのオプションを選択します。

パーティション プロファイル

パーティションの再起動に使用するパーティション プロファイルを指定します。

即時

論理パーティションをただちにシャットダウンします。HMC はアクティブなすべてのジョブをただちに終了します。そのようなジョブで実行されているプログラムは、いかなるジョブのクリーンアップも許可されません。データが部分的に更新されている場合、このオプションを使用すると好ましくない結果になります。このオプションを使用するのは、制御されたシャットダウン試行が失敗した後だけにしてください。

OS のシャットダウン

論理パーティションに対して **shutdown** コマンドを発行することによって、論理パーティションを通常どおりにシャットダウンします。この操作中、論理パーティションは必要なシャットダウンアクティビティをすべて実行します。このオプションは AIX 論理パーティションでのみ利用できます。

OS のシャットダウン即時

論理パーティションに対して **shutdown -F** コマンドを発行することによって、論理パーティションをただちにシャットダウンします。この操作中、論理パーティションは他のユーザおよび他のシャットダウン アクティビティへのメッセージをバイパスします。このオプションは AIX 論理パーティションでのみ利用できます。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

電源の設定 : Microsoft Hyper-V

電源の設定アクションタイプでは、Hyper-V 環境内にある仮想マシンの起動とシャットダウンを制御します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Hyper-V ホスト

Hyper-V Server が常駐するサーバの名前を指定します。ドロップダウンリストから 1 つ選択します。

Hyper-V VM 名

状態を変更する仮想マシンの名前を指定します。ドロップダウンリストから 1 つ選択します。

アクション開始

Hyper-V Server の開始時に実行するアクションを指定します。ドロップダウンリストから、以下のいずれかを選択します。

- 常に
Hyper-V Server の開始時に常に VM を開始します。
- 自動
Hyper-V Server の開始時に自動的に VM を開始します。
- なし
Hyper-V Server の開始時に VM を開始しません。

開始遅延

Hyper-V Server の開始後に VM を開始する遅延時間（数秒）を調整します。ドロップダウンリストから 1 つ選択します。

シャットダウン アクション

仮想マシンのシャットダウン時に実行するアクションを指定します。ドロップダウンリストから、以下のいずれかを選択します。

- オフ
Hyper-V Server のシャットダウン前に VM をオフにします。
- 保存
Hyper-V Server のシャットダウン前に VM を保存（中断）します。
- シャットダウン

Hyper-V Server のシャット ダウン前に VM をシャットダウンします。

復旧アクション

Hyper-V Server で障害が発生したときに仮想マシンの以前の詳細を回復するためのアクションを指定します。 ドロップダウン リストから、以下のいずれかを選択します。

- なし
サーバ障害発生後の Hyper-V Server の開始時に特別なアクションを行いません。
- 再起動
サーバ障害発生後の Hyper-V Server の開始時に VM を再起動します。
- 元に戻す
サーバ障害発生後の Hyper-V Server の開始時に、最新のスナップショットを使って VM を元に戻します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

電源の設定: VMware vCenter/vApp 電源の調整

電源の設定アクションタイプは、VMware vCenter 環境内の仮想マシンおよび vApp の電源設定を制御します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウンリストから 1 つ選択します。

VC データ センター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。ドロップダウンリストから 1 つ選択します。

VM/vAPP

ターゲット タイプ (VM または vApp) を指定するラジオ ボタン。

ターゲット

電源調整の対象となる仮想マシンまたは vApp の名前を指定します。ドロップダウンリストから 1 つ選択します。あるいは、自動生成されるテキストや、イベントメッセージから抽出されるテキストを使用できます。

電源操作

実行する電源操作を指定します。ドロップダウンリストから、以下のいずれかを選択します。

- VC 電源オン
- VC 電源オフ
- VC 電源リセット
- VC 電源中断
- VC 電源シャットダウン
- vApp の電源オン
- vApp の電源オフ
- vApp の中断

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウン リストから有効なチケット タイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウン リストからテンプレートを選択します。選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

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。

サービス プロファイルの設定: Cisco UCS

[サービス プロファイルの設定] アクション タイプでは、サービス プロファイルの UCS ブレード サーバへの関連付け、関連付け解除、またはフェールオーバーを実行できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

UCS マネージャ

UCS Manager の名前を指定します。

UCS Chassis

Cisco UCS シャーシの名前を指定します。

UCS ブレード

Cisco UCS ブレードの名前を指定します。

サービス プロファイル

サービス プロファイルの名前を指定します。

プロファイル操作

ドロップダウン リストからプロファイルを選択します。

関連付け

サービス プロファイルをブレードに関連付けます。

関連付け解除

ブレードからサービス プロファイルを関連付け解除します。

フェールオーバー

このオプションを使用すると、サービス プロファイルに対してチェック ボックスが表示されます。このチェックボックスをオンにすると、サービス プロファイルは次に利用可能なブレードに自動的にフェールオーバーされるようになります。デフォルトでは、チェック ボックスはオンになっています。また、シャーシおよびブレードのドロップダウンは両方とも無効になっています。

特定のサービス プロファイルのフェールオーバー用にシャーシとブレードを指定したい場合は、チェック ボックスをオフにします。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウン リストから有効なチケット タイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウン リストからテンプレートを選択します。選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

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。

共有の設定: VMware vCenter

共有の設定アクションタイプでは、VMware vCenter 環境内にある仮想マシンの CPU 共有とメモリ共有を制御します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウンリストから 1 つ選択します。

VC データ センター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。ドロップダウン リストから 1 つ選択します。

ターゲット VM マシン

共有調整の対象となる仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。あるいは、自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

操作

実行する操作を指定します。ドロップダウン リストから、以下のいずれかを選択します。

- CPU の設定
- CPU の追加
- CPU の削除
- メモリ の設定
- メモリ の追加
- メモリ の削除

値

選択した操作について適切な値を入力します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウン リストから有効なチケット タイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウン リストからテンプレートを選択します。選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

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。

テンプレートを VM に変換: VMware vCenter

[テンプレートを VM に変換] アクション タイプを使用すると、テンプレートを仮想マシンに変換できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

VC データ センター

VM が配置されているデータ センターを指定します。ドロップダウン リストから 1 つ選択します。

VC 計算リソース

VM が作成されるクラスタまたは VMware ESX ホストを指定します。ドロップダウン リストから 1 つ選択します。

VC ESX サーバ

VM が常駐する VMware ESX サーバを指定します。ドロップダウン リストから 1 つ選択します。

VC リソース プール

クローン作成用の VM の選択元となるリソース プールの名前を指定します。ドロップダウン リストから 1 つ選択します。

VC テンプレート

変換対象のテンプレートの名前を指定します。ドロップダウン リストから 1 つ選択します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

VM をテンプレートに変換: VMware vCenter

VM をテンプレートに変換アクションタイプでは、電源がオフの仮想マシンをテンプレートに変換できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウンリストから 1 つ選択します。

VC データ センター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。ドロップダウン リストから 1 つ選択します。

VC 仮想マシン

変換対象の仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択するか、イベント メッセージから抽出されるテキストを使用します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

イベントの作成

イベントの作成アクションタイプでは、システム ディスカバリ、システム削除、複数システムのディスカバリ、システム管理ステータスの変更などのイベントを作成できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

イベントステータス

イベントのステータスを指定します。

イベントコンポーネント

イベントに関係のあるコンポーネント名を指定します。

イベントメッセージ

イベントが生成されたというメッセージを指定します。

イベントソース

イベントのソースを指定します。

イベントターゲット

イベントのターゲットを指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

レポートの作成

[レポートの作成] アクションタイプを使用すると、自動的にレポートを作成できます。このアクションをスケジュールして、レポートが定期的に作成されるようにすることができます。このアクションタイプも[レポート] タブから作成できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

レポートタイプ

作成されるレポートのタイプを指定します。利用可能なレポートタイプおよび関連する作成オプションの説明については、「レポート」を参照してください。

生成されたレポートは、[スケジュール済みレポート]フォルダの[レポート] タブで表示できます。

サービスの作成

サービスの作成アクション タイプでは、モニタ対象のサーバを構成して、ビジネス ニーズで要求されるリソースが反映された論理サービスへと変えることができます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

サービス名

サービスの名前を指定します。

サーバリスト(カンマで区切られたリスト)

利用可能なサーバのリストを指定します。

下限しきい値

サービス全体の下限しきい値を指定します。

上限しきい値

サービス全体の上限しきい値を指定します。

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。条件が 1 回満たされたときにトリガすべきアクションもあれば、条件が何回も満たされて永続的な問題の可能性が示されて初めてトリガすべきアクションもあります。

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。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウン リストから有効なチケット タイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウン リストからテンプレートを選択します。選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

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。

マシンの削除: IBM LPAR

LPAR マシンの削除アクション タイプでは、指定した LPAR を削除できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

HMC/IVM 名

選択したパーティションが存在する管理対象サーバに関連付けられた HMC/IVM を指定します。

システム名

仮想マシンが存在する IBM LPAR のデータ センターの名前を指定します。ドロップダウン リストから 1 つ選択します。

パーティション名

削除するパーティション名を定義します。

注: このアクションの場合、削除するパーティションの電源をオフにする必要があります。このアクションによって、論理パーティションと、パーティション プロファイルに格納された設定データが消去されます。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

マシンの削除: Microsoft Hyper-V

Hyper-V VM の削除アクション タイプでは、Hyper-V Server 環境から仮想マシンを削除します。

アクション定義の [詳細] セクションには、以下のフィールドがあります。

Hyper-V ホスト

Hyper-V Server が常駐するホストの名前を指定します。ドロップダウン リストから 1 つ選択します。

Hyper-V VM 名

削除する仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。

付属のリソース

削除する仮想マシンに付属するリソースを指定します。削除するリソースを選択します。

- ハード ドライブ
- フロッピー ドライブ
- DVD/ISO イメージ

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

マシンの削除: Solaris ゾーン

Solaris ゾーン マシンの削除アクションタイプでは、Solaris ゾーン ホストからゾーンを削除します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

ゾーン ホスト

削除するゾーンが含まれる Solaris ゾーン ホストを定義します。

ゾーン

削除するゾーンを定義します。自動生成されるテキストや、イベントメッセージから抽出されるテキストを使用できます。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

マシンの削除: VMware vCenter

vCenter VM の削除アクション タイプでは、VMware vCenter Server 環境から仮想マシンを削除します。

アクション定義の [詳細] セクションには、以下のフィールドがあります。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

VC データ センター

仮想マシンが常駐するデータ センターの名前を指定します。ドロップダウン リストから 1 つ選択します。選択したデータ センターは、そのデータ センターに関連付けられた VM の名前と共に、[ターゲット VM マシン] ドロップダウン リストに入力されます。

ターゲット VM マシン

削除する仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

名前でホストを検出

名前でホストを検出アクションタイプでは、指定のホスト名を使ってホストを検出できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

ホスト名

ホスト名を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

ネットワークの検出

ネットワークの検出アクションタイプでは、ドメイン内で利用できるネットワークを検出できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

ネットワーク ID

検出するネットワーク ID を指定します。

ネットワーク名

検出するネットワーク名を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

分散スイッチの管理: VMware vCenter

分散仮想スイッチを管理するには、このアクション タイプを使用します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

操作

以下のいずれか 1 つの操作を選択します。

- ポート グループの追加
- ポート グループの削除
- ポート グループの更新

Virtual Center

vCenter Server を指定します。 ドロップダウン リストから 1 つ選択します。

仮想スイッチ

管理する仮想スイッチを指定します。 ドロップダウン リストから 1 つ選択します。

ポートグループ

ポート グループ名を指定します。 ドロップダウン リストから 1 つ選択します。

バインドタイプ(オプション)

以下のバインド タイプのいずれかを選択します。

earlyBinding

VM がポートグループにバインドする際にポートを割り当てます。このバインディング タイプは、接続性の常時確保に有効ですが、ポートが永続的に予約されます。 デフォルトはこのバインディング タイプです。

lateBinding

VM の電源がオンで NIC の状態が接続済みの場合、VM にポートを割り当てます。 このバインディング タイプは、VM の電源がオフになるか、NIC が切断されると、ポートを割り当て直します。

LateBinding は vCenter で設定できます。

ephemeral

VM の電源がオンで NIC の状態が接続済みの場合、VM にポートを割り当てます。このバインディングタイプは、VM の電源がオフになるか、NIC が切断されると、ポートを割り当て直します。
ephemeral バインディングは、ESX ホストと vCenter で設定できません。

VLAN ID (オプション)

仮想ポート グループの操作に使用される整数値を指定します。

ポート数(オプション)

ポート グループのポートの数を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウン リストから有効なチケット タイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウン リストからテンプレートを選択します。選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

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。

フォールトトレランスの管理: VMware vCenter

フォールトトレランスを管理するには、このアクションタイプを使用します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

操作

指定した VM について以下のいずれかの操作を選択します。

- 電源オン
- 電源オフ
- 有効
- 無効
- セカンダリ VM のマイグレート

Virtual Center

vCenter Server のホスト名を指定します。ドロップダウンリストから 1 つ選択します。

データセンター

VM が属するデータセンターを指定します。ドロップダウンリストから 1 つ選択します。

仮想マシン

フォールトトレラント VM を指定します。ドロップダウンリストから 1 つ選択します。

セカンダリホスト

セカンダリ VM が常駐する ESX サーバを指定します。ドロップダウンリストから 1 つ選択します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

VM スナップショットの管理: VMware vCenter

VM スナップショットの管理アクションタイプでは、指定したターゲットシステム上の仮想マシン スナップショットを作成する、元に戻す、または削除することができます。

注: ESXi ホストを vCenter から削除した後に再度追加したために VM スナップショットの管理アクションが失敗する場合は、対応するスナップショットを再度選択し、アクションを保存してください。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Operation

以下のいずれかのアクションを指定します。

- 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作成] を選択する場合は、以下のフィールドに入力します。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。 ドロップダウン リストからサーバを選択します。

データ センター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。 ドロップダウン リストからデータ センターを選択します。

仮想マシン

スナップショットを作成する仮想マシンの名前を指定します。 ドロップダウン リストから仮想マシンを選択します。あるいは、自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

名前

作成する仮想マシン スナップショットの名前を定義します。 自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

説明

(オプション) 仮想マシン スナップショットについて説明します。

[メモリのキャプチャ]チェック ボックス

(オプション) スナップショットの一部としてのシステム実行メモリを使ってスナップショットを作成するかどうかを指定します。

[スナップショットに戻す] を選択する場合は、以下のフィールドに入力します。

VC サーバ

vCenter が常駐するサーバの名前を指定します。ドロップダウン リストからサーバを選択します。

データ センター

仮想マシンが常駐する vCenter 内のデータ センターの名前を指定します。ドロップダウン リストからデータ センターを選択します。

仮想マシン

スナップショットを元に戻す仮想マシンの名前を指定します。ドロップダウン リストから仮想マシンを選択します。

名前

元に戻す仮想マシン スナップショットの名前を定義します。

名前を入力するか、双眼鏡のアイコンをクリックし、表示されるダイアログ ボックスで元に戻すスナップショットを選択します。

ID

元に戻す仮想マシン スナップショットの ID を定義します。

注: スナップショットを元に戻すには名前または ID のいずれかを使用します。両方は必要ありません。1 つの仮想マシンについて同じ名前のスナップショットが複数ある場合は、ID が必要です。

[スナップショットの削除] を選択する場合は、以下のフィールドに入力します。

VC サーバ

vCenter が常駐するサーバの名前を指定します。ドロップダウン リストからサーバを選択します。

データ センター

仮想マシンが常駐する vCenter 内のデータ センターの名前を指定します。ドロップダウン リストからデータ センターを選択します。

仮想マシン

スナップショットを削除する仮想マシンの名前を指定します。ドロップダウン リストから仮想マシンを選択します。

名前

削除する仮想マシン スナップショット名を定義します。

名前を入力するか、双眼鏡のアイコンをクリックし、表示されるダイアログ ボックスで削除するスナップショットを選択します。

ID

削除する仮想マシン スナップショットの ID を定義します。

注: スナップショットを削除するには名前または ID のいずれかを使用します。両方は必要ありません。1 つの仮想マシンについて同じ名前のスナップショットが複数ある場合は、ID が必要です。

[子の削除]チェック ボックス

(オプション) スナップショットのすべての子を削除するかどうかを指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

仮想スイッチの管理: VMware vCenter

仮想スイッチを管理するには、このアクションタイプを使用します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

操作

以下のいずれか 1 つの操作を選択します。

- ポート グループの追加
- ポート グループの削除
- ポート グループの更新

Virtual Center

vCenter Server を指定します。ドロップダウン リストから 1 つ選択します。

データセンター

データセンターを指定します。ドロップダウン リストから 1 つ選択します。

ESX サーバ

仮想スイッチが属する ESX サーバを指定します。ドロップダウン リストから 1 つ選択します。

仮想スイッチ

管理する仮想スイッチを指定します。ドロップダウン リストから 1 つ選択します。

ポートグループ

ポート グループ名を指定します。ドロップダウン リストから 1 つ選択します。

VLAN ID (オプション)

仮想ポート グループの操作に使用される整数値を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

Windows サービスの管理

Windows サービスの管理アクションタイプは、AutoShell コマンドラインおよびスクリプト環境を使用して Windows サービスを制御します。

アクションの定義の [詳細] セクションには、以下のフィールドが含まれます。

操作オプション

サービスで実行される操作を指定します。

注: クエリ サービス操作が返す Windows サービス ステータスは %STDOUT% パラメータからのみ取得できます。イベント テーブルからは利用できません。このパラメータはアクション シーケンスで実行されるアクションでのみ有効です。

注: 以下の動作は Windows で直接実行されたサービス管理と異なります。

- サービスが「停止済み」のステータスであっても、[サービスの再起動] 操作を実行できます。サービス ステータスは「開始済み」に変更されます。
- サービスが「開始済み」のステータスのときに [サービスの無効化] 操作を実行すると、サービスは無効になります。また、そのステータスは「停止済み」に変わります。

ホスト名

サービスが実行されるコンピュータの名前を定義します。

ユーザ名

ユーザ名を定義します。

パスワード

パスワードを定義します。確認のためパスワードを再入力します。

サービス名

操作の対象となるサービスの名前を定義します。名前を入力するか、イベント メッセージから抽出されるテキストを使用します。

注: Windows でサービスの [プロパティ] ダイアログ ボックスを開いて、サービス名を確認します。[コンピュータの管理] ウィンドウに表示される表示名と混同しないでください。

「サービス スタートアップ タイプの変更」を選択した場合は、以下のフィールドに入力します。

スタートアップ タイプ

サービスに設定されるスタートアップ タイプを指定します。オプションには「自動」、「手動」、「無効」があります。「起動」オプションは、デバイス ドライバがブート ロードによってロードされることを意味します。「システム」オプションは、デバイス ドライバがカーネル初期化中に開始されることを意味します。

「サービス依存関係の変更」を選択した場合は、以下のフィールドに入力します。

依存関係

サービスを開始できる前に実行されている必要がある依存関係（他のサービス、システム ドライバ、またはロード オーダー グループ）を定義します。複数の依存関係を定義する場合は、スラッシュでそれらを区切ります。

「サービス アカウントの変更」を選択した場合は、以下のフィールドに入力します。

ローカル システム アカウント/このアカウント

サービスがログインするアカウントを指定します。**LocalSystem** アカウントを使用するか、またはここでアカウントを定義します。

マシンをマイグレート: VMware vCenter

vCenter VMotion のマイグレーションアクションタイプでは、VMware VMotion を使用して仮想マシンをマイグレートします。この操作を行うには VMware ESX サーバを正しく設定する必要があります。また、ターゲット コンピュータ上には VMotion ライセンスが配置されている必要があります。

アクション定義の [詳細] セクションには、以下のフィールドがあります。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

ソース データ センター

ソース仮想マシンが常駐するデータ センターの名前を指定します。ドロップダウン リストから 1 つ選択します。

ソース仮想マシン

ソース VM として使用するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

[デスティネーション ESX サーバ]

マイグレーションのターゲットとなる ESX サーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

注: ESX ホスト間で VM のマイグレーションがサポートされるのは、2 つの ESX ホスト間で VM データストア/ディスクが共有される場合のみです。

デスティネーション リソース プール

使用するリソース プールの名前を指定します。ドロップダウン リストから 1 つ選択します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウン リストから有効なチケット タイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウン リストからテンプレートを選択します。選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

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。

CPU の変更: VMware vCenter

CPU の変更アクション タイプでは、仮想マシンに割り当てる CPU の数を変更できます。

アクション定義の [詳細] セクションには、以下のフィールドがあります。

Virtual Center

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

データセンター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。ドロップダウン リストから 1 つ選択します。

仮想マシン

CPU 変更の対象となる仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。

CPU

VM に割り当てる CPU の数を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

メモリの変更: VMware vCenter

メモリの変更アクションタイプでは、仮想マシンのメモリ割り当てを変更できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Virtual Center

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウンリストから 1 つ選択します。

データセンター

仮想マシンが常駐する VMware vCenter 内のデータセンターの名前を指定します。ドロップダウンリストから 1 つ選択します。

仮想マシン

CPU 変更の対象となる仮想マシンの名前を指定します。ドロップダウンリストから 1 つ選択します。

メモリ

VM に割り当てるメモリの量を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

ヘルプデスク チケットのオープン

ヘルプデスク チケットのオープン アクション タイプでは、ヘルプデスク チケットを開くのに使用するプロパティを定義できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

サマリ

チケットの詳細を端的に示します。

説明

チケットについて説明します。

エンティティ

(オプション) ヘルプ デスク システムで既知の設定項目とチケットとを一致させるために使用するサーバまたはサービスの名前を定義します。設定項目のホスト名とエンティティ名が同じである場合、チケットはその設定項目と関連付けられます。

タイプ

チケットのタイプを指定します。

テンプレート

チケットのテンプレートを指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウン リストから有効なチケット タイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウン リストからテンプレートを選択します。選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

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。

マシンのプロビジョニング: IBM LPAR

このアクション タイプは **LPAR** をプロビジョニングします。

[ビルド パーティション] セクションには、以下のフィールドが含まれます。

HMC/IVM 名

選択したパーティションが存在する管理対象サーバに関連付けられた **HMC/IVM** を指定します。

システム名

仮想マシンが存在する **IBM LPAR** のデータ センターの名前を指定します。ドロップダウン リストから **1** つ選択します。

パーティション名

イメージ作成用のパーティションの名前を定義します。

プロファイル名

選択した **LPAR** の既存プロファイルの名前を定義します。

[メモリ設定] セクションには、以下のフィールドが含まれます。

インストール済みメモリ

インストール済みのメモリが識別されます。

利用可能なメモリ

インストール済みのメモリが識別されます。

最小

最小メモリ量を指定します。

希望

希望するメモリ量を指定します。

最大

最大メモリ量を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

[プロセッサ] セクションには、以下のフィールドがあります。

処理モード

処理モードを指定します。

以下のオプションから選択します。

- 部分的プロセッサ ユニット（共有）
- 全プロセッサ（専用）

利用可能なユニット

利用可能なプロセッサユニットが識別されます。

最小

最小プロセッサユニットを指定します。

希望

希望するプロセッサユニットを指定します。

最大

最大プロセッサユニットを指定します。

I/O コンポーネント

LPAR に関連付ける I/O コンポーネントを指定します。

I/O プール

I/O プールを追加、削除、および変更できます。

最大仮想アダプタ

仮想アダプタの最大数を定義します。

仮想アダプタ

仮想アダプタの数が識別されます。

仮想シリアル アダプタ

仮想シリアルアダプタを追加、削除、および変更できます。

仮想イーサネット アダプタ

仮想イーサネット アダプタを追加、削除、および変更します。

仮想 SCSI アダプタ

仮想 SCSI アダプタを追加、削除、および変更できます。

プロビジョニング プロセスはクライアント コンピュータ上で開始され、ジョブが正常に完了すると確認のメッセージによって通知されます。

マシンのプロビジョニング: Microsoft Hyper-V

Hyper-V VM のプロビジョニング アクション タイプでは、VM を作成およびインストールします。以下のパラメータを指定します。

アクション定義の [詳細] セクションの先頭ページには、以下のフィールドがあります。

SCVMM サーバ

Microsoft System Center Virtual Machine Manager (SCVMM) ライブラリサーバを指定します。ドロップダウン リストから 1 つ選択します。

Hyper-V Server

Hyper-V サーバを指定します。ドロップダウン リストから 1 つ選択します。

テンプレート

テンプレートを指定します。ドロップダウン リストから 1 つ選択します。

デスティネーション パス

作成する VM のデスティネーション パスを指定します (テンプレートを格納)。ドロップダウン リストから 1 つ選択します。

VM 名

VM の名前を指定します。

VM の開始

作成した VM を自動的に開始します。デフォルトでは、新しい VM は電源オフの状態です。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

[次へ] をクリックして表示される 5 番目のページの [詳細] セクションには以下のフィールドがあります。

ハードウェア プロファイル

Microsoft System Center Virtual Machine Manager (SCVMM) ライブラリサーバによって定義されるハードウェア プロファイルの名前を指定します。

仮想プロセッサ

VM に割り当てる仮想プロセッサの数を指定します。

デフォルト : 1

メモリ

作成する VM の RAM メモリをメガバイト (MB) 単位で指定します。

デフォルト : 1024

[次へ] をクリックして表示される 3 番目のページの [詳細] セクションには以下のフィールドがあります。

ゲスト OS プロファイル

(オプション) **Microsoft System Center Virtual Machine Manager (SCVMM)** ライブラリ サーバによって定義されるゲスト オペレーティング システム プロファイルの名前を指定します。このパラメータは、**SCVMM** ライブラリ サーバに格納されているオペレーティング システム構成設定を上書きします。**SCVMM** 統合を使って **VM** のプロビジョニングを行う場合、このパラメータが有効になります。

製品キー

(オプション) **VM** 用の **Windows** 製品アクティベーション キーを指定します。このパラメータをサポートするには、**Sysprep** ツールを使って作成した **Windows** イメージが必要です。このオプションはコマンドの非同期実行では無効になります。

フル ネーム

新しい **VM** にインストールする **Windows** イメージ (**Sysprep** ツールを使って作成) のユーザ名を指定します。

組織

(オプション) 新しい **VM** にインストールする **Windows** イメージ (**Sysprep** ツールを使って作成) の組織名を指定します。このパラメータをサポートするには、**Sysprep** ツールを使って作成した **Windows** イメージが必要です。このオプションはコマンドの非同期実行では無効になります。

管理者パスワード

(オプション) このオプションは **VM** 用のデフォルト管理者アカウント パスワードを設定するのに使用します。このパラメータをサポートするには、**Sysprep** ツールを使って作成した **Windows** イメージが必要です。このパラメータは非同期実行では無視されます。

注: このオプションを正常に設定するには、**Sysprep** ツールを使って作成する **Windows Server** 管理者パスワードを空に設定します。

ワークグループに参加

VM について作成したいワークグループを指定します。ドメインとワークグループの指定は相互に排他的です。

ドメインに参加

VM のドメイン名を指定します。ドメインとワークグループの指定は相互に排他的です。

ドメイン ユーザ

デフォルトの **Administrators** グループの一員として作成するドメイン ユーザ名を指定します。

ドメイン ユーザ パスワード

デフォルトの **Administrators** グループの一員として作成するドメイン ユーザ アカウントのパスワードを指定します。

[次へ] をクリックして表示される 4 番目のページの [詳細] セクションには以下のフィールドがあります。

DHCP の使用

VM のネットワーク インターフェースで **DHCP** を有効にするオプションを指定します。テンプレート イメージに複数のネットワーク アダプタがある場合、**DHCP** は最初のインターフェースでオンになります。有効にした場合、他のネットワーク パラメータにはアクセスできなくなります。

IP アドレス

VM に割り当てる静的な **IPv4** アドレスを指定します。

ネットワーク マスク

VM に割り当てるサブネット マスクを指定します。

デフォルト ゲートウェイ

VM のデフォルト ゲートウェイを指定します。

DNS Server

VM に対して設定する **DNS** サーバを指定します。

IP メトリック

(オプション) VM に対して設定するインターフェース メトリックを指定します。このオプションは、**-ip4addr** オプションと共に使用します。インターフェース名を **-ip4addr** オプションに指定する場合、このオプションにも同じインターフェース名を使用する必要があります。このパラメータをサポートするには、**Sysprep** ツールを使って作成した **Windows** イメージが必要です。このオプションはコマンドの非同期実行では無効になります。

デフォルト : 1

マシンのプロビジョニング : Solaris ゾーン

Solaris ゾーン マシンのプロビジョニング アクション タイプでは、ゾーンを作成およびインストールします。**Solaris** ゾーン ホスト、ゾーン名、ゾーン タイプ、および他のゾーン プロパティを指定します。作成したゾーンは自動的にインストールされます。

アクション定義の [詳細] セクションの先頭ページには、以下のフィールドがあります。

ホスト

ゾーンを作成する **Solaris** ゾーン ホストを定義します。

名前

ゾーン名を定義します。自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

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]、[ルート全体]、[ブランド化] のどれ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

(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。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

[次へ] をクリックして表示される 5 番目のページの [詳細] セクションには以下のフィールドがあります。

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

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

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時、ゾーンを自動的に再起動するかどうかを定義します。

マシンのプロビジョニング: VMware vCenter

vCenter マシンのプロビジョニングアクションタイプでは、仮想マシン (VM) をプロビジョニングできます。テンプレート、およびテンプレートと連携するターゲット vCenter 仕様が必要です。VM のプロビジョニングに関するサービスルールが存在する場合、新しい VM は、ルールの作成対象となったサービス内に配置されます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

VC サーバ

vCenter が常駐するサーバの名前を指定します。ドロップダウンリストから 1 つ選択します。

VC データセンター

マシンをプロビジョニングするデータセンターの名前を指定します。ドロップダウンリストから 1 つ選択します。

VC 計算リソース

計算リソースが常駐するサーバの名前を指定します。ドロップダウンリストから 1 つ選択します。

VC ESX サーバ

プロビジョニングされた VM のターゲットとなる VMware ESX サーバの名前を指定します。ドロップダウンリストから 1 つ選択します。

VC データストア

使用するデータストアの名前を指定します。ドロップダウンリストから 1 つ選択します。

VC ターゲットの場所

VC ターゲットの場所を指定します。ドロップダウンリストから 1 つ選択します。

ホスト名/VM 名

使用する名前または VC 名を仕様内から選びます。ドロップダウンリストから 1 つ選択します。あるいは、自動生成されるテキストや、イベントメッセージから抽出されるテキストを使用できます。

ユーザ名

仕様にアクセスするユーザ名認証情報を指定します。

パスワード

仕様にアクセスするためのパスワードを指定します。

VC 仮想マシン

利用可能な VC 仮想マシンのうち、どれを使用するかを指定します。選択した場合は、ドロップダウン リストから 1 つをクリックします。

VC テンプレート

利用可能な VC テンプレートのうち、どれを使用するかを指定します。クリックした場合は、事前に作成済みのソフトウェア パッケージ グループのうちの 1 つをドロップダウン リストから選択します。

NIC (VC テンプレート)

VC テンプレートによって使用されるネットワーク インターフェース カードの数を指定します。

VC 仕様

使用する VC 仕様の名前を指定します。ドロップダウン リストから 1 つ選択します。

NIC (VC 仕様)

VC 仕様によって使用されるネットワーク インターフェース カードの数を指定します。

OS システム タイプ

プロビジョニングされた VM のオペレーティング システムのタイプを表示します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

メモリ

VM に割り当てるメモリの量をメガバイト単位で指定します。

仮想プロセッサ

VM に割り当てる仮想プロセッサの数を指定します。

データストア

(オプション) ハードディスクを追加作成するストレージデータストアを指定します。

ドライブ サイズ

(オプション) 追加のハードドライブのサイズを指定します。

SCSI コントローラ

(オプション) ハードドライブの追加作成に使用する SCSI コントローラを指定します。

ネットワーク管理

ネットワーク接続設定を変更できます。

グローバル NIC 設定

DNS 検索サフィックスを追加できます。

ディスクの削除: VMware vCenter

ディスクの削除アクション タイプでは、仮想マシンからディスクを削除できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Virtual Center

VMware vCenter が存在するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

データセンター

仮想マシンが存在する VMware vCenter 内のデータ センターの名前を指定します。ドロップダウン リストから 1 つ選択します。

仮想マシン

ディスクを追加する仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。

ハードドライブ

削除するディスクを指定します。ドロップダウン リストから 1 つ選択します。

[ディスク ファイルの削除]チェック ボックス

ディスク データを削除するかどうかを指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

ネットワーク インターフェースの削除: VMware vCenter

ネットワーク インターフェースの削除アクション タイプでは、仮想マシンから仮想 NIC を削除できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Virtual Center

VMware vCenter が存在するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

データセンター

仮想マシンが存在する VMware vCenter 内のデータ センターの名前を指定します。ドロップダウン リストから 1 つ選択します。

仮想マシン

仮想 NIC を削除する仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。

ネットワーク インターフェース

削除する仮想 NIC を指定します。ドロップダウン リストから 1 つ選択します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

サーバをサービスから削除

サーバをサービスから削除アクション タイプでは、既存のサービスからサーバを削除できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

サービス

サービスの名前を指定します。

サーバリスト(カンマで区切られたリスト)

サービスから削除するサーバのリストを指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

アクションの実行

アクションの実行アクション タイプでは、アクションを実行できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

アクション名

アクションを指定します。

イベントソース

アクションのソースを指定します。

イベントメッセージ

イベント メッセージを指定します。

ルール名

アクションのルールを指定します。

サーバ名

アクションのサーバを指定します。

サービス名

アクションのサービスを指定します。

プロパゲート

-service_name オプションで指定されたサービス内のすべてのサーバ
に対して、アクションを実行するように指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に
選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

アクション シーケンスの実行

アクション シーケンスの実行アクションタイプでは、1つのルールに複数のアクションを選択し、定義したシーケンスでそれらのアクションを実行できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

中断の場合再起動

アクション シーケンスが中断された場合、そのアクション シーケンスを再起動します。アクションは中断されたポイントからは再開されません。シーケンスが先頭に戻って開始されます。

アクション シーケンス

アクションと条件を1行、または複数行選択できます。[アクション シーケンス]を選択すると、ドロップダウンリストが有効になります。ドロップダウンリストを選択しない場合、テキストがテーブルセルに表示されます。

シーケンス

アクションのシーケンスを指定します。

注: 条件が満たされずにアクション シーケンスが終了した場合、デフォルトではリターンコード -1 が返されます。

アクション

アクション名を指定します。ドロップダウンリスト内の利用可能なアクションからアクションを選択できます。

条件名

次に実行されるアクションを決定する条件を指定します。独自のカスタム条件を作成するか、または以下のいずれかの事前定義済み条件を使用できます。

- 失敗時
- 成功時

注: 条件は作成された順序で評価されます。

次の手順

条件の結果に基づいて実行する次のアクションを指定します。

続行

条件が **true** と評価された場合に、続行して次のアクションへ進みます。

終了 (RC=0)

条件が **true** と評価された場合に、シーケンスを終了し、ログにコード 0 を返します。

RC を返して終了 (RC= アクション RC)

条件が **true** と評価された場合に、アクション シーケンスを終了し、アクションのリターン コードを返します。

アボート (RC=-1)

条件が **true** と評価された場合に、アクション シーケンスを停止し、ログにコード -1 を返します。

移動

条件が **true** と評価された場合に、指定されたアクション シーケンス番号に進みます。

アクションの追加

テーブルに新しいアクションを追加し、新しいシーケンス番号を自動的に生成します。

条件の追加

アクションに新しい条件を追加します。

削除

選択された行を削除し、シーケンス番号を更新します。行には、アクションまたは条件を含めることができます。この機能により、アクション全体を削除せずに、アクションの条件を削除できます。

保存

アクション シーケンスを保存します。

注: シーケンスの最後のアクションで [次の手順] が [続行] に設定されている場合、設定は [Exit w/RC] (RC= アクション RC) に自動的に変更されます。また、シーケンスの最後のアクションの [次の手順] が変更されたことが、情報メッセージによって通知されます。

コマンド スクリプトの実行

コマンドスクリプトの実行アクションタイプでは、スクリプトを使用して、コマンドを処理したサーバから外部コマンドを実行できます。たとえば、[開始] ページからコマンドが実行される場合、コマンドを実行する **Windows** スケジューラと同じサーバ上にターゲット コマンドが存在する必要があります。ルール評価の結果としてコマンドが実行される場合、ジョブの実行後、アクションが **Windows** スケジューラ サーバをホストしているコンピュータ上で実行されます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

コマンドライン

実行するコマンドまたは代替文字列を指定します。あるいは、自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

ヘルス状態の設定

ルールヘルス状態の設定アクションタイプは、ルールのヘルス状態を[警告]、[マイナー]、[メジャー]、[重大]のいずれかに設定できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

ヘルス状態

以下のいずれかのアクションを指定します。

- 警告
- マイナー
- メジャー
- 重大

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

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。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

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

ドロップダウンリストから有効なチケットタイプを選択します。設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

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。

テンプレート

チケットを作成するために使用するテンプレートを指定します。ドロップダウンリストからテンプレートを選択します。選択されたチケットタイプに応じて、フォームは対応する値で入力されます。

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。

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. + (追加する) 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

代替キーに一意的な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。複数の代替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 シーケンスに分かりやすい名前を入力し、[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。

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。

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 \(P. 880\)](#)

[ユース ケース：新規ルールをサービスに追加する \(P. 881\)](#)

[ユース ケース：アクションを定義する \(P. 881\)](#)

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 インターフェー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

データ センターでの以下のようなデータ収集の方法を制御できます。

- メトリック収集の時間間隔
- メトリックを収集するシステム（フィルタリング）
- 各サーバで収集するメトリック
- データの経過期間とデータの有効期限（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. 882)

[データ センター用のデータ収集の設定](#) (P. 885)

[サーバ用のデータ収集の設定](#) (P. 887)

[仮想リソース用のデータ収集の設定](#) (P. 889)

[パフォーマンスしきい値の設定](#) (P. 893)

[メトリック フィルタの設定](#) (P. 894)

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 Systems Performance LiteAgent 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。

基本システム メトリックを収集する任意のサーバに CA Systems Performance LiteAgent または SystemEDGE エージェントをインストールします。 SystemEDGE エージェントが存在する場合、CA Systems Performance LiteAgent は必要ありません。必要な場合は、製品のユーザ インターフェイスを使用して 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使用率が計算されますか。全体使用率とは、CA Virtual Assurance によって管理されたサーバに関して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。

注: 全体使用率の計算に新しいメトリックを含めるには、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] を選択します。このメトリックを含めると、CA Virtual Assurance は、サーバの状態を評価するときに最新の結果を表示します。

- メトリック評価によって全体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。サーバが追加されると、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くても、CA Virtual Assurance がサーバの状態に悪影響を与えることはありません。データの欠如は、サーバの重大度に反映されません。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 データが収集されているかどうかを判定できます。ただし、収集されたデータが使用可能かどうかをより迅速に判定するための手段が必要な場合や、パフォーマンス データが重大である場合があります。この場合は、パフォーマンス データを収集できない場合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 を設定します。パフォーマンス データが使用できないシステムを容易に識別できるようにするには、CA Virtual Assurance *install_path*\conf ディレクトリにある *caaipconf.cfg* ファイルを変更します。このファイルをテキスト エディタで開き、以下のようにヘルス状態のプロパティの場所を見つけます。

```
<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>
```

CA Virtual Assurance は、XML 要素の値で囲まれた値を 5 または 10（それぞれ、[OK] または [警告] を示します）などのサポートされているほかの値のいずれかに変更します。これらの変更には、パフォーマンス データを収集できない場合の目的の状態が反映されます。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で表示されます。

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、「Performance Metrics Reference」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

注: モニタ対象環境の 1000 台のマシンごとに、データ記録間隔を 300 秒増加させることを推奨します。

[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 : 10 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。

最大 : 365

デフォルト : 365

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

注: モニタ対象環境の 1000 台のマシンごとに、データ記録間隔を 300 秒増加させることを推奨します。

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。

最大 : 365

デフォルト : 365

[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 : 10 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。

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 PowerVM Server
- 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

注: モニタ対象環境の 1000 台のマシンごとに、データ記録間隔を 300 秒増加させることを推奨します。

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。

最大 : 365

デフォルト : 365

[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 : 10 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%

[全体使用率の計算用を含める]

選択したメトリックを全体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。

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

CA Virtual Assurance がフィルタによってデフォルトで指定されたメトリックを収集するかどうかを指定します。メトリック フィルタがデフォルトとして設定されていない場合、CA Virtual Assurance は指定されたメトリックを自動的に収集しません。

[全体使用率の計算用を含める]

選択したメトリックを全体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。

[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。

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. 897)

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-CME 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: ツール

このセクションには、以下のトピックが含まれています。

[NodeCfgUtil による AIM の設定](#) (P. 899)

[サポート エージェント](#) (P. 909)

NodeCfgUtil による AIM の設定

Node Config Utility を使用すると、CA Virtual Assurance ユーザ インターフェイスを使用せずに、SystemEDGE AIM を設定できます。

このセクションでは、このユーティリティのダイアログ モードおよびコマンド モードについて説明します。

関連項目：

[NodeCfgUtil の概要](#) (P. 900)

[ダイアログ モードの NodeCfgUtil による AIMs の設定](#) (P. 902)

[コマンド モードの NodeCfgUtil による AIM の設定](#) (P. 906)

NodeCfgUtil の概要

AIM を設定して仮想環境を検出するには、以下のいずれかのアクションを実行します。

- ユーザインターフェースから [管理] タブを開いて [設定] - [プロビジョニング] に移動し、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。

- 仮想環境またはクラスタへのアクセス用に指定されたユーザには、リモートアクセスを許可する権限が必要です。
- 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。
- Citrix XenServer AIM は、プールマスタまたはスタンドアロンの Citrix XenServer にのみ接続できます。そうしないと、AIM が動作しません。
- VMware 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。
- VM の仮想化を最適化するには、対応するシステム ツールを VM にインストールします。多くの機能は、これらのツールがインストールされている場合にのみ使用できます。ユーザの環境に応じて、以下のシステム ツールを使用します。
 - (VMware の場合) VMware ツール
 - (XenServer の場合) XenTools
 - (RHEV の場合) RHEV Guest Tools

注: 対応するシステム ツールの詳細については、サードパーティのドキュメントを参照してください。

AIM サーバからサポートされる環境を検出する方法

1. 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。
2. 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、ファイル（zone.cfg、vc.cfg など）内の AIM ごとにデータを格納します。

3. マネージャ サーバでユーザ インターフェースを開き、[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。
4. 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。

5. 以下のいずれかのアクションを選択します。

- 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 ボックスが開きます。

6. 管理する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 がディスカバリ 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 \(P. 599\)](#)

ダイアログ モードの NodeCfgUtil による AIMs の設定

NodeCfgUtil.exe を使用して、IBM PowerVM、IBM PowerHA、Solaris ゾーン、VMware vCenter、VMware vCloud、Microsoft クラスタ、Cisco UCS、Citrix XenServer、Citrix XenDesktop、RHEV、Active Directory および Exchange Server (ADES)、および Huawei GalaX 用の AIM 設定を変更できます。このユーティリティは、対応する AIM の設定ファイルを `sysedge_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。

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 管理者として実行してください。

次の手順に従ってください:

1. AIM がインストールされているコンピュータで管理者としてログインし、Windows エクスプローラを開きます。
 2. `SystemEDGE_InstallPath¥plugins¥AIPCommon` ディレクトリに変更し、NodeCfgUtil.exe を起動します。
- NodeCfgUtil によって、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 ボックスに一覧表示されます。
3. 1 を入力して、新しい管理対象ノードを追加します。
 4. 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。

設定が完了したら、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)、vCloud Director (vcloud.cfg)、Microsoft クラスタ (mscs.cfg)、Citrix XenServer (cxen.cfg)、UCS (ucs.cfg)、PowerVM (lpar.cfg)、PowerHA (hacmp.cfg)、RHEV (kvm.cfg)、Huawei GalaX (galaxa.cfg)、Citrix XenDesktop (xendesktop.cfg)、または ADES (esad.cfg) 用の設定ファイルを書き込みます。

注: 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。

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。

***** メイン メニュー *****

1. 管理対象ノードのインストール
2. 管理対象ノードの変更
3. 管理対象ノードの削除
0. 終了

選択項目を入力してください:

**** 管理対象ノードの選択 ****

1. IBM PowerVM
2. Oracle Solaris ゾーン
3. Citrix XenServer
4. VMware vCenter
5. Cisco UCS
6. Microsoft Cluster Service
7. Microsoft Active Directory および Exchange Server
8. IBM PowerHA
9. VMware vCloud Director
10. Red Hat Enterprise Virtualization
11. Huawei GalaX
12. Citrix XenDesktop
0. 前のメニューに戻る

選択項目を入力してください: 4

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、ADES 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 ボックスを示します。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。ADES 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 Cluster Service
2. Microsoft Active Directory および Exchange Server
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 Active Directory および Exchange Server 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...

以下の例は、LPAR AIM の設定に正常に追加された HMC1 サーバ用の「管理対象システム」ダイアログボックスを示します。AIM が HMC サーバに関連したすべての仮想 I/O サーバを検出した後、それらのサーバは NodeCfgUtil に表示されるため、各サーバを変更してその認証情報を指定できます。AIM は、完全に設定された最初の VIO サーバの認証情報を、まだ設定されていないすべての VIO サーバのデフォルト認証情報として使用します。そのため、すべての VIO サーバが認証情報を共有している場合は、1 つの VIO サーバのみの認証情報を指定すれば十分です。そうでない場合は、各 VIO サーバに異なる認証情報を設定する必要があります。AIM は現在、HMC サーバを管理できる状態です。

```
**** 管理対象ノードの選択 ****
1. IBM PowerVM
0. 前のメニューに戻る
*****
選択項目を入力してください: 1
既存のエントリのリスト...
1. hmc: HMC1.company.com
2. vio: ibm101.company.com
変更するエントリを選択します (前のメニューに戻るには 0 を選択します) : 2
IBM LPAR 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: ibm101
2. ユーザ名: admin
3. パスワード: *****

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。
CAAC1024 ノードが正常に変更されました。

キーをどれか押してください...
```

以下の例は、GalaX AIM の設定に正常に追加された *mycluster* に関する「管理対象ノードのインストール」ダイアログボックスを示します。詳細については、NodeCfgUtil コマンドモードを参照してください。GalaX 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: Huawei Galax8800 コンポーネントを設定するには、証明書ファイル名を指定する必要があります。

```
**** 管理対象ノードの選択 ****
1. Huawei GalaX
0. 前のメニューに戻る
*****
選択項目を入力してください: 1
```

GalaX HACMP 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 : `myserver`
2. 証明書ファイル名 : `certificatename123.p12`
3. パスワード : `*****`
4. ポート [default =8773]:
5. プロトコル [default =http]:

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 PowerVM、IBM PowerHA、Solaris ゾーン、VMware vCenter、VMware vCloud、Microsoft クラスタ、Cisco UCS、Citrix XenServer、Citrix XenDesktop、RHEV、Active Directory および Exchange Server (ADES)、および Huawei GalaX 用の AIM 設定を変更できます。このユーティリティは、対応する AIM の設定ファイルを `sysedge_Install\path\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。

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 管理者として実行してください。

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|mcs} -u user -p password -h {pvmname|hostname|cluster_name}`
- (3) `nodecfgutil {vc|ucs} -u user -p password -h hostname -t port -c protocol`
- (4) `nodecfgutil ades -u user -p passwd -d domainname -e entity -o option`
- (5) `nodecfgutil {xen|vcloud|xenserver} -u user -p passwd -h hostname`
- (6) `nodecfgutil {powerha|kvm} -u user -p password -h {cluster_name|hostname} [-t port]`
- (7) `nodecfgutil galax -u usercertificate -p password -h hostname [-t port] [-c protocol]`

-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|ades|xen|vcloud|powerha|kvm|galax|xendesktop

仮想環境または物理環境を指定します。

-u *user|usercertificate*

管理者ユーザの名前またはユーザ証明書をそれぞれ指定します。

-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*

ADES 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*

クラスタの名前を指定します。

-t *port*

（オプション）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。

次の手順に従ってください:

1. AIM がインストールされてい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|cluster_name}`

(3) `nodecfgutil {vc|ucs} -u user -p password -h hostname -t port -c protocol`

(4) `nodecfgutil ades -u user -p passwd -d domainname -e entity -o option`

(5) `nodecfgutil {xen|vcloud|xenserver} -u user -p passwd -h hostname`

(6) `nodecfgutil {powerha|kvm} -u user -p password -h {cluster_name|hostname} [-t port]`

(7) `nodecfgutil galax -u usercertificate -p password -h hostname [-t port] [-c protocol]`

- (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、IBM PowerVM、または MSCS に対して渡された認証情報を認証および格納します。
- (3) 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。
- (4) Active Directory および Exchange Server (ADES) に対して認証を実行し、正しい認証情報を格納します。
- (5) Citrix XenServer、Citrix XenDesktop、または VMware vCloud に対して認証を実行し、正しい認証情報を格納します。
- (6) IBM PowerHA または Red Hat Enterprise Virtualization (KVM) に対して認証を実行し、正しい認証情報を格納します。
- (7) HUAWEI Galax に対して認証を実行し、正しい認証情報とユーザ証明書を格納します。

サポート エージェント

サポート エージェントは診断情報を収集します。サポート エージェントにアクセスするには、以下のアドレスを使用します。

`http://<Manager Server>:8556`

ユーザ インターフェースは説明がなくてもわかりやすく、以下の情報を提供します。

- システムの重要な部分のパフォーマンス メトリック
- 詳細な Web サービス使用率統計
- ログ ファイル モニタリング
- 長時間の SQL クエリ

付録 C: 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 \(P. 913\)](#)

[属性にゼロの値が表示される \(P. 913\)](#)

[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 \(P. 914\)](#)

[Cisco UCS フォルダが UI 内に表示されない \(P. 914\)](#)

[DB トランザクション ログ サイズが予想せずに増加する \(P. 915\)](#)

[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 \(P. 916\)](#)

[ドメインサーバが使用できない \(P. 917\)](#)

[eHealth が LPAR 物理ディスクを検出しない \(P. 917\)](#)

[dpmvc virtualswitch コマンドでの空のタスク ID \(P. 918\)](#)

[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 \(P. 918\)](#)

[IBM 論理パーティションの名前付け制限 \(P. 919\)](#)

[AIX システム上での SystemEDGE インストーラのナビゲーションの問題 \(P. 920\)](#)

[NodeCfgUtil は XenDesktop コントローラへの接続を検証できない \(P. 920\)](#)

[パフォーマンス チャートの LPAR レベルのメモリ使用率が 0 として表示される \(P. 921\)](#)

[PMM が AIM のポーリングを停止する \(P. 922\)](#)

[Solaris Lists SPARC および x86 システムへのリモートでの展開 \(P. 922\)](#)

[アップグレード後の空白の \[クエリ結果\] タブ \(P. 924\)](#)

[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 \(P. 925\)](#)

[vCenter Server のパスワードを変更するとデータ収集に失敗する \(P. 925\)](#)

[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 \(P. 926\)](#)

[コンポーネントのステータス アイコンが \[設定されていません\] を示している \(P. 926\)](#)

[SystemEDGE のアップグレード \(P. 926\)](#)

[Microsoft SQL サーバに接続できない \(P. 927\)](#)

[製品のアップグレードがユーザ インターフェイスに反映されない \(P. 927\)](#)

[プロビジョニング画面およびポリシー画面でユーザ インターフェイスが応答しない \(P. 928\)](#)

[ユーザ インターフェイスが動作しない \(P. 928\)](#)

[vCenter Server AIM 属性にゼロが表示される \(P. 929\)](#)

[vCenter Server の接続に失敗した \(P. 930\)](#)

[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 \(P. 933\)](#)

[vCenter AIM インスタンスのステータス アイコンに「ディスクバリエーションが進行中」が表示される \(P. 934\)](#)

[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 \(P. 934\)](#)

[vCenter AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される \(P. 936\)](#)

[VM 使用率の値が電源オフ後にすぐに更新されない \(P. 936\)](#)

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 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 仕様に依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。

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 サイズが予期せずに増加する

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に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 サポートの Web サイトにある、完全なトランザクション ログのトラブルシューティングについての KB 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

ドメイン サーバが使用できない

症状：

ドメイン サーバが使用できないか、停止されたか、機能していないか、または要求を処理しておらず、サービス コントローラ (SC) はこのコンポーネントが稼働中であることを示しています。

解決方法：

この動作は、データベース接続の失敗または AIM パスワードの期限切れのために発生し、ポリシー設定およびリモート展開コンポーネントの動作に影響を与える可能性があります。サポート サービスの Web サービス (ISM) をモニタすると、ドメイン サーバの機能が定期的にモニタされます。ISM によって予期しない動作が識別されると、ユーザには「CA SM ドメイン サービスはダウンしているか応答していません」というメッセージでステータスの変更が通知されます。

このステータスは、以下のコマンドでモニタできます。

```
Caaipscutil /status /id=ISM /user=<ユーザ> /password=<パスワード>
```

インフラストラクチャの状態および機能を確認するために、[管理] パネルにはドメイン サーバのステータスが示されます。

eHealth が LPAR 物理ディスクを検出しない

症状：

eHealth が、リリース 12.8 LPAR AIM の LPAR 物理ディスクを検出しません。

解決方法：

リリース 12.8 LPAR AIM を使用している場合は、eHealth を以下のバージョンにアップグレードします。

- eHealth 6.2.2.10 以前を使用している場合は、6.2.2 D11
- eHealth 6.3.0.05 以前を使用している場合は、6.3.0.06 以降

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 モニタで、同じ属性に同じ値が表示されません。

解決方法:

シームレスなローカルおよびリモート モニタリングでは、同一のモニタ対象オブジェクト名を選択できます。ただし、異なる API では異なる値を返す場合があります。

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。モニタ対象メトリックは非常に変化しやすいため、サンプルが異なる可能性があります。

IBM 論理パーティションの名前付け制限

症状:

論理パーティションの名前を指定しても、CA Virtual Assurance によってその名前がサポートされません。

解決方法:

IBM の LPAR 作成リクエストに使用する LPAR の名前は、大文字と小文字が区別されます。一方この製品では、名前の大文字小文字のみが異なる場合、同じ PowerVM サーバ内での 2 つの論理パーティションの管理がサポートされません。たとえば、以下の LPAR 名は PowerServer1 ではサポートされません。

LPAR1 と lpar1

モニタのオブジェクトインスタンス内でエンティティの区切り文字として使用されるため、LPAR 名に '/' という文字を含むことはできません。 '/' という文字によって、あいまいなモニタ オブジェクトインスタンスが生成されます。たとえば、'lpar/blue' という LPAR 名はサポートされません。

AIX システム上での SystemEDGE インストーラのナビゲーションの問題

症状:

AIX 6.1 および 7.1 に SystemEDGE をインストールすると、lsm (UNIX インストーラ) テキスト ユーザ インターフェースのナビゲーションが動作しません。この問題は、Advanced Encryption および SRM AIM でも発生します。

解決方法:

他の UNIX オペレーティング システムおよび古い AIX バージョン上での場合と異なり、TERM が (通常の) xterm の値に設定されていると、AIX 6.1 および 7.1 上では lsm テキスト ユーザ インターフェースのナビゲーションが機能しません。Java ベースのグラフィカル lsm UI を使用すると、この問題は発生しません。

回避策としては、インストールを開始する前に TERM を別の値 (たとえば vt100) に設定し、[+] および [-] キーを使用してナビゲートするか、または、(PuTTY の場合のみ) アプリケーション カーソル キー モードを無効にするよう設定します。

NodeCfgUtil は XenDesktop コントローラへの接続を検証できない

症状:

NodeCfgUtil は、XenDesktop コントローラへの接続を検証できません。

解決方法:

XenDesktop AIM がインストールされているマシンに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。

- Microsoft .NET Framework 4.0
- Windows Management Framework Core (Windows PowerShell 2.0、Windows Remote Management (WinRM) 2.0)

パフォーマンス チャートの LPAR レベルのメモリ使用率が 0 として表示される

症状:

LPAR レベルのメモリ使用率をモニタすると、パフォーマンス チャートに 0 と表示される

解決方法:

メモリが共有モードで使用されている、つまり、メモリが仮想化されている場合、プラットフォームはメモリ使用率のメトリックのみを提供します。専用メモリについては、使用率のメトリックを収集できないため、使用率の値としてチャートには 0 が表示されます。

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 PowerVM、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。

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。

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。

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。

コンポーネントのステータス アイコンが[設定されていません]を示している

症状:

CA Virtual Assurance によってコンポーネントがインストールされた後、このコンポーネントのステータス アイコンが （「設定されていません」）を示しています。このステータスは、CA Virtual Assurance が、未設定のサーバに接続されているコンポーネントを登録した場合に表示されます。

解決方法:

このコンポーネントのステータスを「準備完了」に変更するには、不足しているサーバ接続の設定および検証を追加します。

SystemEDGE のアップグレード

症状:

SystemEDGE を r11.6 にアップグレードすると、以前の CA Virtual Assurance リリースの AIM が実行されません。

解決方法:

Advanced Encryption およびすべての AIM を CA Virtual Assurance リリース 12.8 にアップグレードします。SystemEDGE r11.6 は、以前の CA Virtual Assurance リリースの AIM をロードしません。

Microsoft SQL サーバに接続できない

症状:

Microsoft SQL Server（評価版）への認証情報を認証する試行が、製品の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。

製品のアップグレードがユーザ インターフェイスに反映されない

症状:

CA Virtual Assurance を新バージョンにアップグレードしたのに、ユーザ インターフェイスに反映されない。

解決方法:

アップグレード後、アップグレード前と同じブラウザ インスタンスを使用している場合、ユーザ インターフェイスに新しいバージョンが反映されない可能性があります。ブラウザ セッションを閉じて新たに開き、ブラウザのキャッシュをクリアして、ユーザ インターフェイスにログインします。

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ない

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。

ユーザ インターフェースが動作しない

症状:

Windows 認証を使用してリモートの SQL Server を使用すると、ユーザ インターフェースが正常に動作しません。

解決方法:

インストール中に、適切なドメイン ユーザを追加し、「サービスとしてログオン」権限を付与するように指示されます。このドメイン ユーザ アカウントに対して、CAAIPTOMCAT、CAAIAPACHE、および CA SM Domain Server サービスが設定されていることを確認します。サービスを再設定しなかった場合、CA Virtual Assurance ユーザ インターフェースは機能しません（ダッシュボードが空であるか、機能が動作しない）。

これらの条件は SQL Server 認証では必要ありません。

次の手順に従ってください:

1. [コントロールパネル] の [管理ツール] から [サービス] ダイアログ ボックスを開きます。
使用可能なサービスのリストが表示されます。
2. CA SM ドメイン サーバ、CAAIPACHE サービス、および CAAIPTOMCAT サービスの [プロパティ] ダイアログ ボックスを開きます。
3. 各ダイアログ ボックスの [ログイン] タブに移動し、[以下のアカウント] を選択します。次に、参照できる有効な認証情報 (ドメイン ユーザ アカウント) を入力します。
4. このドメイン ユーザ アカウントを両方のシステム (マネージャ サーバとデータベース サーバ) のローカル Administrators グループに追加します。
5. このドメイン ユーザ アカウントを SQL Server の sysadmin (または dbcreator 以上) のサーバ役割に追加します。

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 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 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についてステータス 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「ディスカバリが進行中」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  (ディスカバリが進行中) が表示されます。

解決方法:

vSphere 環境のディスカバリ プロセスが完了するまで待機します。ディスカバリにかかる時間は、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数によって異なります。アイコンの上にカーソルを置くと、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ 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 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「ポーリングなし」が表示される

症状:

〔管理〕 - 〔設定〕 で vCenter Server に対して vCenter AIM インスタンスを追加した後、ステータス アイコンに  (ポーリングなし) が表示されます。

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。このアイコンは、CA Virtual Assurance マネージャがこの AIM をポーリングしないこと表します。この AIM は優先 AIM ではありません。

特定の vCenter Server を管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。別の AIM を使用したい場合は、〔管理〕 - 〔設定〕 - 〔プロビジョニング〕 で優先 AIM を設定できます。サーバエントリの〔編集〕をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

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。

用語集

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 ページで使用す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 ゾーン、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 キャップ

cpu キャップは、ゾーン用の CPU リソースの量を制限します。

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。

Elastic Service Controller (ESC)

Elastic Service Controller (ESC) は、仮想リソース、コンピューティング、ストレージ、および他のサービスの集中管理を提供する Huawei コントローラです。

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。

Huawei SingleCLOUD

Huawei SingleCLOUD はクラウドコンピューティングデータセンター用のクラウドサービスソリューションです。

Hyper-V

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。

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 (アクサングルーブ)、日本語文字など)。

IBM High Availability Cluster Multiprocessing (HACMP)

IBM High Availability Cluster Multiprocessing (HACMP) は、IBM System p プラットフォームの AIX UNIX および Linux 上に高可用性クラスタを構築するためのソリューションです。

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 システムを管理できます。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。

Multiple Shared-Processor Pools (MSPP)

Multiple Shared-Processor Pools (MSPP) は、Power6 以降のサーバでサポートされている機能です。この機能により、複数のプロセッサプールの作成が可能になり、CPU リソースの割り当てがより柔軟になります。

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。

Open Virtualization Format (OVF)

Open Virtualization Format (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。

P12 ファイル

P12 ファイルは、秘密鍵をその証明書と共に格納するアーカイブ ファイルです。P12 ファイルは、Huawei GalaX 環境で使用されます。

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。

Red Hat Enterprise Virtualization

Red Hat Enterprise Virtualization (RHEV) は KVM ハイパーバイザに基づいたエンタープライズ仮想化製品です。

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** を使用します。**Open Virtualization Format (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** 上での操作は **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。

vCloud Director (VMware)

VMware **vCloud Director** では、仮想インフラストラクチャ リソースを仮想データセンターへプールして、ユーザにそれらを公開することにより、安全なマルチテナント クラウドを構築できます。

vCloud Director のリソースは、仮想マシンを実行するための CPU、メモリ、ストレージ、vNetwork 分散スイッチなどの vSphere リソースの基盤によって異なります。これらの基盤となる vSphere リソースを使用して、vCloud で仮想マシンと vApp を作成できます。

vCloud 組織 (VMware)

*vCloud 組織*は、ユーザ、グループ、および計算リソースのコレクションを表す管理の 1 単位です。対応する仮想データセンターは必要な計算リソースを提供します。ユーザは組織レベルでの認証後、仮想マシンまたは vApp を作成、使用、管理できます。

Virtual Private Cloud (VPC)

Virtual Private Cloud (VPC) は、複数の仮想マシンおよび関連する仮想ディスクを備えた Huawei SingleCLOUD ユーザのためのプライベート ローカル ネットワークです。

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。

XenCenter (XenServer)

XenCenter は XenServer 環境を管理する Windows クライアントアプリケーションです。ネットワークを介して XenServer ホストに接続できるリモート Windows コンピュータにインストールする必要がありますが、XenServer ホストと同じシステム上で実行することはできません。

XenMotion (XenServer)

XenMotion は、リソース プール内の VM のライブ マイグレーションの機能を提供します。

XenServer ホスト (XenServer)

XenServer ホストオブジェクトは、XenServer とその VM が実行される物理ホストを表します。XenServer ホストはスタンドアロン ホストとすることも、XenServer プールと関連付けることもできます。

アクセス制御リスト

アクセス制御リスト (ACL) は、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。

カーネルベースの仮想マシン (KVM)

カーネルベースの仮想マシン (KVM) は Linux カーネル用のハードウェア支援型仮想化インフラストラクチャです。

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、その仮想化機能をほかの 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。仮想化された入出力デバイスを備えた各 PowerVM システムには、1 つ以上の仮想 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。

仮想ディスク イメージ、VDI (XenServer)

仮想ディスク イメージ (VDI) は、VMに提供される仮想ディスクのディスク上の表現です。VDIはXenServer内の仮想化されたストレージの基本単位です。

仮想データセンター、vDC (VMware)

仮想データセンター (vDC) は、vCloud 組織に仮想計算リソースを提供します。仮想システムのプロビジョニング、実行、および仮想データセンターへの格納を行えます。vCloud 組織は複数の仮想データセンターを持つことができます。

仮想ネットワーク インターフェース、VIF (XenServer)

仮想ネットワーク インターフェース (VIF) オブジェクトは、VMとネットワーク オブジェクトの間の接続を表します。VIF オブジェクトには、名前と説明、グローバルに一意的なUUIDがあり、接続先のネットワークおよびVMを指定します。VMが起動すると、作成する必要があるネットワーク デバイスを決定するためにVIF オブジェクトに対してクエリが実行されます。

仮想ブロック デバイス、VBD (XenServer)

仮想ブロック デバイス (VBD) オブジェクトは、仮想マシン (VM) と仮想ディスク イメージ (VDI) の間の接続を表します。VM が起動すると、接続するディスク イメージを決定するためにその VBD オブジェクトに対してクエリが実行されます。

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、VM (XenServer)

仮想マシン (VM) は、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。VM はテンプレートから作成されます。テンプレートには、特定の VM をインスタンス化するためのさまざまな設定がすべて含まれています。

XenServer には基本テンプレートセットが用意されています。これには、OS ベンダーのインストール CD を起動したり、ネットワーク リポジトリからインストールを実行できる汎用 raw VM や、完全に事前設定された OS インスタンスがあります。XenServer では、Linux と Windows のゲスト オペレーティング システムをサポートしています。

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。

仮想ローカルエリア ネットワーク、VLAN (XenServer)

仮想ローカルエリア ネットワーク (VLAN) では、単一の物理ネットワークが複数の論理ネットワークをサポートできます。XenServer で VLAN を使用するには、ホストの NIC を VLAN トランク ポートに接続する必要があります。

カタログ (VMware)

組織は、vApp テンプレートおよびメディア ファイルを格納するためにカタログを提供します。組織のメンバは、独自の vApp を作成するためにカタログで vApp テンプレートおよびメディア ファイルを使用できます。

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

上限のある論理パーティション (LPAR)

上限のある論理パーティションは、割り当てられたプロセッサユニットを超えるプロセッサ能力を使用できない論理パーティションです。上限のあるパーティションには最大容量が割り当てられていて、容量が超過しないように、また物理システム全体の動作に影響を与えないようになっています。

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。

ストレージ リポジトリ、SR (XenServer)

ストレージ リポジトリ (SR) は、仮想ディスク イメージ (VDI) が格納される特定のストレージ ターゲットを表します。ストレージ ハードウェアへのインターフェースでは、多くの SR タイプで VDI をサポートできます。

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。

デュアル HMC (LPAR)

デュアル HMC は、高可用性を提供する冗長なハードウェア管理コンソール (HMC) 管理システムです。

テンプレート (XenServer)

テンプレートは、*is_a_template* パラメータが **true** に設定されている VM です。テンプレートには、特定の VM をインスタンス化するためのさまざまな設定がすべて含まれています。XenServer には基本テンプレートセットが付属しています。これには、OS ベンダーのインストール CD を起動したり、ネットワーク リポジトリからインストールを実行できる汎用 raw VM や、完全に事前設定された OS インスタンスがあります。XenServer を使用すると、VM を作成し、特定のニーズに合わせて標準的な形式で設定して、将来の展開でできるようにテンプレートとしてそのコピーを保存できます。

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**) 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。

ネットワーク オブジェクト (XenServer)

各 **XenServer** ホストには、仮想イーサネット スイッチである **ネットワーク オブジェクト** が 1つ以上あります。ネットワーク オブジェクトには、名前と説明、グローバルに一意の **UUID**、および接続先の仮想および物理ネットワーク インターフェース (**VIF** と **PIF**) のコレクションがあります。特定のネットワーク オブジェクトに接続されている **VM** およびホスト オブジェクトは、互いにネットワーク パケットを送信できます。

PIF との関連付けのないネットワークは、**内部ネットワーク** と見なされ、**XenServer** ホスト上の **VM** 間の接続のみを提供し、外部との接続はできません。**PIF** との関連付けがあるネットワークは、**外部ネットワーク** と見なされ、**VIF** とネットワークに接続された **PIF** の間のブリッジを提供します。

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 PowerVM** システム上で管理タスクを実行するために使用す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** システム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。

複数の仮想 I/O サーバ

複数の仮想 I/O サーバを使用すると、クライアント パーティションのダウンタイムのない仮想 I/O サーバ メンテナンスを可能にすることによってアプリケーションの可用性を向上させる機能が提供されます。

物理ネットワーク インターフェース、PIF (XenServer)

物理ネットワーク インターフェース (PIF) オブジェクトは、XenServer ホスト上の物理ネットワーク インターフェースを表します。PIF オブジェクトには、名前と説明、グローバルに一意の UUID、PIF オブジェクトが表す NIC のパラメータがあり、接続先のネットワークおよびサーバを指定します。PIF オブジェクトは物理インターフェースおよび VLAN の両方を抽象化します。

物理ブロック デバイス、PBD (XenServer)

物理ブロック デバイス (PBD) オブジェクトは、ホストとストレージ リポジトリ オブジェクトの間の接続を表します。PBD には、指定されたストレージ ターゲットに接続し、対話するために使用されるデバイス設定 フィールドが格納されます。

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。

プロセッサ プール (LPAR)

プロセッサ プールは異なる論理パーティション間で共有することができる物理プロセッサのセットです。

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。

ポリシーベースの設定

ポリシーベースの設定を使用すると、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。

ユニバーサル一意識別子、UUID

ユニバーサル一意識別子 (UUID) は、情報を一意に識別するために分散システムで使用される ID 標準です。情報が単一のデータベースに格納されている場合、UUID で情報にラベル付けすると、ID の競合が制限されます。

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。

リソース プール、オーバーコミット (XenServer)

リソース プールは、複数の XenServer ホスト インストールで構成され、VM をホストできる単一の管理対象エンティティにバインドされます。リソース プールを共有ストレージと組み合わせると、VM を十分なメモリを備えた XenServer ホスト上で起動し、XenServer ホスト間で動的に移動できます (XenMotion)。

リソース プール内で現在実行されている VM が、ユーザ定義の障害回数後にほかのホスト上で再起動できない場合、リソース プールはオーバーコミット状態です。XenServer は、リソース プール内の複数のホストに任意の時点で障害が発生した場合に対処するためのフェールオーバープランを動的に保持します。高可用性 (HA) 設定の一部として定義されている値を許容するホストの障害により、サービスを中断せずに許容される障害の回数が決まります。プランを利用できない場合、プールはオーバーコミットされていると見なされます。プランは、VM のライフサイクル操作および移動に基づいて動的に再計算されます。

リソース プール マスタ (XenServer)

リソース プールには、リソース プール マスタと呼ばれる物理ノードが少なくとも 1 つあります。既存のプールに参加するほかの物理ノードは、メンバと表されます。マスタ ノードのみが、XenCenter と CLI によって使用される管理インターフェースを提供します。必要に応じて、マスタは、個々のメンバにプール外からコマンドまたはリクエストを転送します。

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)。

割り当てプール容量 (LPAR)

共有プロセッサ プールの割り当てプール容量は、プロセッサ プールのパーティション グループが使用できる保証プロセッサ容量を定義します。

索引

(

- (オプション) CA Virtual Assurance マネージャへの SCVMM 管理インスタンスの追加 - 505
- (オプション) VLAN の割り当て - 432
- (オプション) 仮想ディスクの作成 - 436
- (オプション) 仮想マシンへの仮想ディスクの接続 - 437
- (オプション) サーバレベルでの SNMP 設定とアクセス制御リストの指定 - 123
- (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 - 246
- (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 - 248
- (オプション) テンプレートまたはポリシーからのモニタのインデックス再作成 - 242
- (オプション) ノード設定ユーティリティを使用した ADES AIM の設定 - 757
- (オプション) ポリシーまたはテンプレートの更新 - 244, 248
- (オプション) ポリシー レベルでのアクセス制御リストの指定 - 122
- (オプション) ユーザ指定の作成 - 433

1

- 1 つ以上のドメインがモニタされない - 761

3

- 3 つのサーバグループの例 - 125

A

- Active Directory - 36
- Active Directory および Exchange Server AIM の動作方法 - 746
- Active Directory および Exchange Server (ADES) - 98
- Active Directory および Exchange Server のモニタリングの設定方法 - 742

Active Directory および Exchange Server モニタリングの検証 - 757

Active Directory および Exchange Server 用の AIM のインストールおよび設定 - 735

Active Directory セキュリティのシステム ユーザパスワードの変更 - 45

Active Directory でのセキュリティ上の考慮事項 - 36

ADES AIM インスタンスの追加 - 752

ADES AIM のアンインストール - 759

ADES AIM のインストール - 737

ADES AIM のスケーラビリティ - 736

ADES AIM のモニタリングを有効にするための環境設定 - 748

AIM インスタンス接続のトラブルシューティング - 357, 394, 422, 471, 530, 559, 703, 753

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 - 359, 395, 424, 472, 532, 560, 705, 755

AIM インスタンスのステータス アイコンに「ディスクバリエーションが進行中」が表示される - 358, 394, 423, 471, 531, 559, 704, 754

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される - 358, 395, 423, 472, 531, 560, 704, 754

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 - 360, 397, 425, 474, 533, 562, 706, 756

AIM が非アクティブで、データを収集していない - 760

AIX LPAR 管理コンポーネント間のインタラクション - 461

AIX システム上での SystemEDGE インストーラのナビゲーションの問題 - 920

Application Insight Module (AIM) - 82

Application Insight Module、AIM - 937

AutoShell - 937

Autoshell Loadable Module、ALM - 937

C

- CA Customize ユーティリティのインストール - 400, 537
- CA Customize ユーティリティの設定 - 401, 538
- CA EEM が CA Virtual Assurance で動作するしくみ - 37
- CA EEM 管理者パスワード(EiamAdmin)の変更 - 41
- CA EEM ユーザ インターフェースへのアクセス - 38
- CA EEM ユーザの作成 - 38
- CA IBM SystemEDGE PowerHA AIM トラップ - 692
- CA SDM の設定 - 765
- CA SDM チケット ステータス設定の構成 - 766
- CA SystemEDGE PowerHA AIM トラップ タイプ - 692
- CA Technologies 製品リファレンス - 3
- 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 - 195
- CA Virtual Assurance を使用した OVF パッケージのインポート方法 - 647
- calpara.xml ファイル - 475
- CA プロビジョニング ヘルパーのインストール - 405, 542
- CA への連絡先 - 3
- Cisco Nexus 1000V スイッチ - 938
- Cisco UCS - 99, 347
- Cisco UCS 管理コンポーネント間のインタラクション - 351
- Cisco UCS 管理コンポーネントを設定する方法 - 348
- Cisco UCS サーバ - 350
- Cisco UCS の管理 - 362
- Cisco UCS フォルダが UI 内に表示されない - 914
- Cisco UCS リソースの表示 - 373
- Cisco Unified Computing System (UCS) - 938
- Citrix XenDesktop - 100
- Citrix XenDesktop 環境 - 685

- Citrix XenDesktop 管理コンポーネント間のインタラクション - 686
- Citrix XenDesktop の前提条件 - 687
- Citrix XenServer - 101, 384
- Citrix XenServer 仮想マシンのプロビジョニング - 409
- Citrix XenServer 管理コンポーネント間のインタラクション - 388
- cmdlet - 938
- CPU/メモリの設定: IBM LPAR - 786
- CPU/メモリの設定: Microsoft Hyper-V - 789
- CPU/メモリの設定: VMware vCenter - 791
- cpu キャップ - 938
- CPU 共有 (VMware) - 938
- CPU とメモリの設定 - 494
- CPU の設定 - 494
- CPU の変更: VMware vCenter - 841
- 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 - 639
- 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 - 639
- CPU メトリックのアクションの作成 - 638

D

- DB トランザクション ログ サイズが予期せずに増加する - 915
- Dell EqualLogic - 939
- dpmovf import コマンド -- OVF パッケージのインポート - 649
- dpmvc virtualswitch コマンドでの空のタスク ID - 918
- dvPort グループ (VMware) - 939
- dvUplink ポート (VMware) - 939

E

- eHealth が LPAR 物理ディスクを検出しない - 917
- eHealth 統合の概要 - 28
- Elastic Service Controller (ESC) - 939
- ESX/ESXi ホスト (VMware) - 940
- ESX サーバのモニタ - 679
- ESX ホストのフォールトトレランス属性 - 626

F

FIPS 140-2 の暗号化 - 897

FIPS の概要 - 897

funclet - 940

G

GalaX SingleCLOUD サーバレベルの参照 - 442

GalaX サーバの AIM インスタンスの追加 - 421

GalaX サーバへのマネージャの接続が失敗する - 418

GalaX のプロビジョニング用に Windows テンプレートを準備する方法 - 449

H

HMC または IVM サーバ接続のマネージャへの追加 - 465

Huawei GalaX - 101, 410

Huawei GalaX 管理コンポーネント間のインタラクションの確認 - 413

Huawei GalaX 管理コンポーネントを設定する方法 - 411

Huawei SingleCLOUD - 940

Huawei SingleCLOUD 環境を管理する方法 - 438

Huawei SingleCLOUD コンポーネント関係の確認 - 430

Hyper-V - 102, 940

Hyper-V Server 管理コンポーネント間のインタラクション - 500

Hyper-V 管理アクション - 522

Hyper-V 管理の設定方法 - 497

Hyper-V サーバ接続の失敗 - 503

Hyper-V の管理 - 513

Hyper-V の要件の確認 - 498

I

I18n (国際化) - 940

IBM AIX コンピュータの論理パーティションの追加 - 487

IBM High Availability Cluster Multiprocessing (HACMP) - 940

IBM PowerHA - 103, 687

IBM PowerHA 管理コンポーネント間のインタラクション - 688

IBM PowerVM - 104

IBM PowerVM (LPAR) - 454

IBM PowerVM サーバ管理の概要 - 455

IBM PowerVM 設定の使用例 - 462

IBM PowerVM の管理 - 483

IBM 論理パーティションの名前付け制限 - 919

IDManager が使用する転送パッケージのプロトコル - 198

Integrated Virtualization Manager (IVM、LPAR) - 940

internet Small Computer Systems Interface、iSCSI - 941

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 - 198

K

KVM のプロビジョニング用に Linux テンプレートを準備する方法 - 534

KVM のプロビジョニング用に Windows テンプレートを準備する方法 - 540

L

L10n (ローカライゼーション) - 941

Linux イメージの準備 (KVM) - 536

Linux イメージの準備 (XenServer) - 399

Linux の Compatibility Library - 201

Linux または UNIX 上の展開管理証明書 - 201

Linux または UNIX での展開プライマインストール - 200

LPAR AIM インスタンスの追加 - 468

LPAR モニタリング - 481

M

MIB オブジェクト、MIB 属性 - 941

MIB 拡張の定義 - 239

Microsoft Cluster Server - 105

Microsoft Cluster Service - 693

Microsoft Cluster Service 管理コンポーネントを
設定する方法 - 694
Microsoft Cluster Service の管理 - 710
Microsoft Cluster Service のモニタ - 711
Microsoft Hyper-V Server - 495
Microsoft Hyper-V を使用するために必要な設
定の適用 - 499
Microsoft SCVMM を使用するために必要な設
定の適用 - 506
Microsoft SQL サーバに接続できない - 927
MSCS 管理コンポーネント間のインタラクション -
697
Multiple Shared-Processor Pools (MSPP) - 941

N

NetApp ファイラ - 941
Network Installation Manager (NIM) (LPAR)
- 941
NodeCfgUtil による AIM の設定 - 899
NodeCfgUtil の概要 - 900
NodeCfgUtil は XenDesktop コントローラへの接
続を検証できない - 920

O

onTap - 941
Open Virtualization Format (OVF) - 942
Oracle Solaris ゾーン - 105
OVF パッケージへのアクセスの提供 - 648

P

P12 ファイル - 942
PMM が AIM のポーリングを停止する - 922
PowerVM 管理コンポーネントを設定する方法 -
458
POWER プロセッサ (LPAR) - 942

R

Red Hat Enterprise Virtualization - 106, 522, 942
Red Hat Enterprise Virtualization 管理コンポー
ネントの設定方法 - 523
RHEV 仮想マシンのプロビジョニング - 547

RHEV 環境の前提条件 - 541
RHEV 管理コンポーネント間のインタラクション -
525

S

SCVMM サーバ接続の失敗 - 509
SNMPv1/v2 設定およびアクセス制御リストの設
定方法 - 114
SNMPv3 - 942
SNMPv3 設定の詳細の確認 - 135
SNMPv3 の設定方法 - 133
SNMP およびアクセス制御リストの設定方法 -
111
SNMP 設定およびポリシー関係の確認 - 117
SNMP データポーターの設定 - 371
SNMP の整合性 - 111
Solaris Lists SPARC および x86 システムへのリ
モートでの展開 - 922
Solaris ゾーン - 548
Solaris ゾーン環境でのポーリング間隔設定の
調整 - 913
Solaris ゾーン管理 - 563
Solaris ゾーン管理コンポーネント間のインタ
クション - 553
Solaris ゾーン管理コンポーネントを設定する方
法 - 549
Solaris ゾーン管理の要件 - 552
Solaris ゾーンの追加 - 564
Spectrum Infrastructure Manager 統合の概要 -
31
SRM しきい値定義テンプレートのコピー - 325
SRM しきい値定義テンプレートの削除 - 326
SRM しきい値定義テンプレートの名前変更 -
325
SRM しきい値定義テンプレートの変更 - 324
SRM しきい値定義の変更 - 315
SRM 制御設定の定義 - 316
SRM テスト - 91
SRM テスト定義テンプレートのコピー - 320
SRM テスト定義テンプレートの削除 - 322
SRM テスト定義テンプレートの名前変更 - 321
SRM テスト定義テンプレートの変更 - 320

SRM テストのコピー - 313
SRM テストの削除 - 314
SRM テストの変更 - 312
SRM ポリシーのコピー - 307
SRM ポリシーの削除 - 309
SRM ポリシーの名前変更 - 308
SRM ポリシーへのしきい値定義テンプレートの
インポート - 323
SRM ポリシーへのしきい値定義の追加 - 314
SRM ポリシーへのテスト定義テンプレートのイ
ンポート - 319
SRM ポリシーへのテストの追加 - 309
SRM ポリシーを作成する方法 - 266
SSH の設定 - 689
Sysprep ツール - 405, 543
Sysprep ツールのインストール - 405, 542
Sysprep ツールを Windows 2003 R2 にインスト
ールして実行する - 405
SystemEDGE エージェント ポートの再設定 - 185
SystemEDGE および AIM の展開方法 - 142
SystemEDGE および Application Insight Module
(AIM) の管理 - 97
SystemEDGE のアップグレード - 926
SystemEDGE の現在の設定モードの確認 - 337
SystemEDGE の設定からの管理対象モードの
情報の削除 - 339
SystemEDGE の設定からの管理対象外モード
の情報の削除 - 342
SystemEDGE の設定モードの確認 - 345
SystemEDGE の設定モードの変更方法 - 334
SystemEDGE ポリシーからのモニタの削除 - 305
SystemEDGE ポリシーのコピー - 268
SystemEDGE ポリシーの削除 - 269
SystemEDGE ポリシーの名前変更 - 269
SystemEDGE ポリシーへのモニタの追加 - 289
SystemEDGE ポリシーへのモニタリング テンプ
レートのインポート - 284
SystemEDGE ポリシーを作成する方法 - 268
SystemEDGE ポリシー制御設定の定義 - 211,
271
SystemEDGE ポリシー内のモニタのコピー - 304
SystemEDGE ポリシー内のモニタの表示 - 303

SystemEDGE ポリシー内のモニタの変更 - 304
SystemEDGE ポリシー内の既存テンプレートの
変更 - 306
SystemEDGE モニタの表示 - 93
SystemEDGE モニタリング テンプレートのコピー
- 285
SystemEDGE モニタリング テンプレートの削除 -
286
SystemEDGE モニタリング テンプレートの変更 -
285
SystemEDGE モニタリング テンプレートの名前
変更 - 286
SystemEDGE 機能 - 74
SystemEDGE と Advanced Encryption - 109

U

UCS - 942
UCS AIM サーバの登録 - 356
UCS AIM の削除 - 383
UCS Manager 設定のバックアップ - 375
UCS サーバの削除 - 383
UCS 組織 - 376
UCS トラップ管理 - 381
UCS のアクション タイプ - 381
UCS プール - 377
UCS プールの削除 - 381
UCS プールの作成 - 379
UCS プールの名前変更 - 380
UCS プールの表示 - 378
UCS マネージャ - 942

V

vApp (VMware) - 942
vApp のクローン作成 - 644
vApp のサポート - 640
vCenter AIM インスタンス接続のトラブルシュー
ティング - 612
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 - 614, 934
vCenter AIM インスタンスのステータス アイコン
に「ディスクバリエーションが進行中」が表示される -
614, 934

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 - 617

vCenter AIM インスタンスのステータス アイコン
に「ポーリングなし」が表示される - 616, 936

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 - 616, 933

vCenter Server AIM 属性にゼロが表示される -
929

vCenter Server (VMware) - 943

vCenter Server エージェント (VMware) - 943

vCenter Server 管理コンポーネント間のインタラ
クションの確認 - 601

vCenter Server 管理コンポーネントを設定する
方法 - 599

vCenter Server 接続のトラブルシューティング -
606

vCenter Server データベース (VMware) - 943

vCenter Server でのユーザ スコープ認証 - 618

vCenter Server の AIM インスタンスの追加 -
610

vCenter Server の接続に失敗した - 607, 930

vCenter Server のパスワードを変更するとデー
タ収集に失敗する - 925

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 - 925

vCenter の自動化とポリシー アクション - 682

vCloud AIM インスタンス接続のトラブルシュー
ティング - 584

vCloud 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 - 586

vCloud AIM インスタンスのステータス アイコン
に「ディスクバリエーションが進行中」が表示される -
586

vCloud AIM インスタンスのステータス アイコン
に「ポーリングなし」が表示される - 588

vCloud 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 - 588

vCloud Director (VMware) - 943

vCloud Director 管理コンポーネントを設定する
方法 - 573

vCloud Director 接続のマネージャへの追加 -
578

vCloud 管理コンポーネント間のインタラクション
- 576

vCloud サーバ接続の失敗 - 580

vCloud サーバ接続のトラブルシューティング -
579

vCloud サーバの AIM インスタンスの追加 - 582

vCloud 組織 - 593

vCloud 組織 (VMware) - 943

vCloud での vApp のサポート - 590

vCloud の vApp に対する操作 - 594

vCloud のフォルダ構造 - 590

vCloud の要件の確認 - 574

vCloud のリソース プール プロバイダとしての
vCenter Server - 592

vCPU の動的な追加または削除 - 630

Virtual Private Cloud VLAN を作成する方法 -
426

Virtual Private Cloud (VPC) - 943

VMware vApp のプロビジョニング - 642

VMware vCenter - 110

VMware vCenter のプロビジョニングと一般的な
ユース ケース - 662

VMware vCloud - 110, 572

VMware vSphere および vCenter Server - 595

VM 使用率の値が電源オフ後にすぐに更新さ
れない - 936

VM ステータスの管理 (Hyper-V) - 516

VM ステータスの管理 (KVM) - 545

VM ステータスの管理 (VMware) - 667

VM ステータスの管理 (XenServer) - 407

VM スナップショットの管理: VMware vCenter -
831

VM の CPU およびメモリの割り当ての編集 -
521, 635

VM のデバイス管理 - 620

VM のホットプラグ サポート - 629

VM を GalaX のテンプレートへ変換 - 453

VM を RHEV のテンプレートへ変換 - 544

VM を XenCenter のテンプレートへ変換 - 406

VM をテンプレートに変換 - 402, 539

VM をテンプレートに変換: VMware vCenter - 811
vNetwork Distributed Switch、vDS (VMware) - 944
vNetwork Standard Switch、vSwitch (VMware) - 944
vNetwork パネル内の仮想標準スイッチおよび分散仮想スイッチ - 652
vNetwork 標準スイッチ(vSwitch) - 653
vNIC テンプレート - 376
VPC VLAN とそのコンポーネントの管理 - 437
VPC VLAN の作成 - 433
vSwitch のプロパティ - 657

W

Windows 2003 R2 での Sysprep ツールの実行 - 405, 452, 543
Windows 2008 R2 での Sysprep ツールの実行 - 406, 453, 544
Windows 上の展開管理証明書 - 200
Windows イベント モニタの作成 - 233
Windows イベント モニタの定義 - 297
Windows イメージの準備 - 404, 452, 542
Windows サービスの管理 - 837
Windows での展開プライマ インストール - 199

X

XenCenter (XenServer) - 944
XenMotion (XenServer) - 944
XenServer 環境の前提条件 - 404
XenServer 管理コンポーネントを設定する方法 - 385
XenServer のプロビジョニング用に Linux テンプレートを準備する方法 - 398
XenServer のプロビジョニング用に Windows テンプレートを準備する方法 - 403
XenServer ホスト (XenServer) - 945

あ

アーキテクチャ - 20, 719
アクション - 659

アクション シーケンスの実行 - 869
アクション シーケンスの定義 - 876
アクション タイプ - 774
アクションとルールの作成 - 518
アクションの実行 - 867
アクセス制御 - 718
アクセス制御リスト - 945
新しい GalaX 接続のマネージャへの追加 - 417
新しい Hyper-V Server 接続のマネージャへの追加 - 502
新しい SCVMM サーバ接続のマネージャへの追加 - 508
新しい SRM しきい値定義テンプレートの定義 - 322
新しい SRM テスト定義テンプレートの定義 - 318
新しい SRM ポリシーの定義 - 307
新しい vCenter Server 接続のマネージャへの追加 - 605
アップグレード後の空白の[クエリ結果]タブ - 924
一元化されたサービス プロファイルを使用する方法 - 363
一部のカウンタがモニタされない - 761
一部のホストがモニタされない - 762
一般情報の表示 - 683
一般的な要件の確認(SNMPv3) - 134
イベントによる vApp のモニタリング - 645
イベントによる分散仮想スイッチのモニタリング - 661
イベントの作成 - 813
イベント転送のための CA Virtual Assurance の設定 - 141
イメージング サービス - 24
インスタンス - 476
インストール後の読み取り/書き込みコミュニティの指定 - 178
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 - 199
インフラストラクチャ展開プロセス - 193
インポートされたオブジェクトのリソース ツリーでの確認 - 652

永続データ - 475
エージェントの検出 - 267
エージェントの視覚化 - 92
エージェントの設定 - 84
エージェントポリシーのダッシュボードビュー - 204
エージェントレスのモニタ対象システム - 717
エージェントレス モニタリング - 713
オブジェクト集計の設定 - 218, 278

か

カーネルベースの仮想マシン (KVM) - 945
階層型テンプレート - 281
階層型テンプレートの概念 - 207
回復力 - 718
外部ディレクトリのインポート - 53
外部ディレクトリ ユーザ グループのユーザグループへの割り当て - 49
概要 - 19, 143
書き込みコミュニティを含まないエージェント設定 - 189
拡張ディスクバリエーションおよび SNMP 情報 - 63
カスタマイズされた VM プロビジョニングの前提条件 - 399, 536
カスタマイズされたプロビジョニングの動作 - 402, 539
カスタマイズ ログ - 403, 540
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 - 184
カスタム アクションの作成 - 874
カスタム仕様の表示 - 683
仮想 I/O サーバ、VIOS (LPAR) - 945
仮想 NIC (VMware) - 945
仮想環境の管理 - 347
仮想スイッチ (VMware) - 945
仮想スイッチの管理: VMware vCenter - 835
仮想ディスク (VMware) - 946
仮想ディスク イメージ、VDI (XenServer) - 946
仮想ディスクの追加または削除 - 621
仮想データセンター、vDC (VMware) - 946

仮想ネットワーク インターフェース、VIF (XenServer) - 946
仮想ネットワーク インターフェースの追加または削除 - 622
仮想ブロック デバイス、VBD (XenServer) - 946
仮想マシン (Hyper-V Server) の追加 - 514
仮想マシン (vCenter Server) の追加 - 662
仮想マシン、VM (VMware) - 946
仮想マシン、VM (XenServer) - 947
仮想マシン管理操作の使用 - 444
仮想マシン数 - 658
仮想マシンに対するフォールトトレランス - 623
仮想マシンのクローン作成 - 666
仮想マシンの削除 - 517, 674
仮想マシンの作成 - 434
仮想マシンのテンプレートからの展開 - 675
仮想マシンの登録解除 - 681
仮想マシンのフォールトトレランス プロパティ - 625
仮想マシンのマイグレート - 677
仮想マシンのモニタ - 678
仮想マシンの論理ボリューム - 631
仮想マシン ハードウェア バージョン 7 (VMware) - 947
仮想マシン名の変更 - 518
仮想マシンをテンプレートに変換します - 670
仮想リソース用のデータ収集の設定 - 889
仮想ローカルエリア ネットワーク、VLAN (XenServer) - 947
カタログ (VMware) - 947
簡易ネットワーク管理プロトコル (SNMP : Simple Network Management Protocol) - 947
監査証跡 - 170
管理 DB - 25
管理者ユーザ p12 ファイルの取得 - 415
管理情報ベース (MIB) - 948
管理対象 Power システムの優先 HMC の変更 - 470
管理対象オブジェクト状態の表示 - 94
管理対象外リソースの管理 - 72
管理対象モードおよび管理対象外モード - 81

管理対象モードおよび管理対象外モードの詳細の確認 - 336
管理対象リソースと管理対象外リソース - 71
管理対象リソースの管理の停止 - 72
管理対象リソースの削除 - 73
関連ドキュメント - 15
規則 - 16
起動とシャットダウンのアクションの編集 - 519
機能と利点 - 716
共有の設定: VMware vCenter - 807
共有メモリ (Solaris) - 948
クエリ結果の表示 - 730
具体的なリモート展開の使用例 - 184
クラスタ - 948
クラスタおよび仮想デスクトップのモニタリング - 685
クラスタサービスの管理 - 676
クラスタ内の vCenter Server - 652
クラスタの削除 - 708
クラスタの登録 - 707
クラスタプロパティの変更 - 709
グループへのユーザの割り当て - 48
グローバル SNMPv3 オブジェクトの作成 - 136
グローバル SNMP 設定とアクセス制御リストの指定 - 119
グローバル SNMP 設定とアクセス制御リストのポリシーへの適用 - 120
グローバルおよびサーバレベルの SNMP 設定 - 112
グローバルゾーン (Solaris) - 948
軽量プロセス、LWP (Solaris) - 948
検出された Citrix XenServer AIM インスタンスの追加 - 392
検出された MSCS AIM インスタンスの追加 - 702
検出された Red Hat Enterprise Virtualization AIM インスタンスの追加 - 529
コマンドスクリプトの実行 - 871
コマンドスクリプトの実行権限の設定 - 53
コマンドモードでの ADES AIM のインストール - 740

コマンドモードの NodeCfgUtil による AIM の設定 - 906
コマンドモードの NodeCfgUtil による PowerHA AIM の設定 - 690
コンテナ (Solaris) - 948
コンピューティング クラスタレベルの参照 - 443
コンポーネントのステータス アイコンが[設定されていません]を示している - 926

さ

サーバグループへのポリシーの配布 - 124
サーバの検出 - 511
サーバへのマネージャの接続が失敗する - 354, 466, 527, 555, 700
サーバ用のデータ収集の設定 - 887
サーバレベルの SNMP 設定の追加 - 129
サーバレベルの SNMP 設定を管理する方法 - 128
サーバレベルの設定としてパッケージラッパ - SNMP 設定を適用する - 131
サーバワークロード用のテンプレートの作成 - 224
サーバをサービスから削除 - 865
サーバをサービスに追加 - 781
サービス - 66
サービスからのサーバの削除 - 70
サービスに対するユーザグループ権限の設定 - 52
サービスの削除 - 70
サービスの作成 - 66, 815
サービスの編集 - 68
サービスプロファイル - 365, 948
サービスプロファイルとブレードの関連付け - 367, 374
サービスプロファイルの作成また更新を実行する方法 - 366
サービスプロファイルの設定: Cisco UCS - 805
サービスポラーの設定 - 372
サービスレスポンステストの表示 - 95
サービスレスポンスモニタリング - 89
サブ組織の作成 - 377
サポートエージェント - 909

視覚化 - 717
しきい値モニタの作成 - 226
しきい値モニタの定義 - 290
システム - 476
システム管理 - 57
システム管理 MIB - 76
システム サマリの SNMPv3 設定を確認します。
- 140
システムの検出 - 60
システムの削除 - 61
システム パフォーマンスの管理 - 57
事前定義済みアクション タイプの使用 - 771
事前定義済みアクション タイプのリスト - 776
事前定義済み自動ウォッチャーの適用 - 256
自動ウォッチャーの確認 - 258
自動ウォッチャーの作成とシステムへの適用 -
257
自動ウォッチャーの仕組み - 252
自動ウォッチャーを作成してシステムに適用す
る方法 - 250
自動化 - 719
自動化ポリシーの作成 - 879
シャーシ (UCS) - 948
重要業績評価指標メトリック - 717
上限のある論理パーティション (LPAR) - 949
状態管理モデル - 79
ジョブステータス フィルタ - 149
新規インスタンスのデフォルト ポリシーの指定
- 333
新規パッケージ ラッパーの作成 - 171
信頼済みホストリストへのマシン名の追加 -
687
スケーラビリティ - 150, 719
スケジュールの定義 - 877
ステートレスなモニタリング - 81
ストレージエリア ネットワーク、SAN - 949
ストレージ管理操作の使用 - 449
ストレージ クラスタレベルの参照 - 448
ストレージ リポジトリ、SR (XenServer) -
949
スナップショットに戻す - 680
スナップショットの削除 - 672

スナップショットの作成 - 671
すべてのスナップショットの削除 - 673
スロット - 477
正規表現 - 949
製品のアップグレードがユーザ インターフェー
スに反映されない - 927
セキュリティおよび保守 - 87
設定 - 146, 718
設定エントリの管理 - 730
設定セットの作成 - 727
設定の概要 - 202
設定の前提条件 - 723
セントラル サービス プロファイルの管理 - 364
ゾーン (Solaris) - 949
ゾーン AIM サーバの追加 - 558
ゾーン ステータスの制御 - 568
ゾーンのクローン作成 - 570
ゾーンの削除 - 571
属性にゼロの値が表示される - 913
その他の vApp 操作 - 645

た

ダイアログ モードでのカスタム プロパティの提
供 - 651
ダイアログ モードの NodeCfgUtil による AIMs
の設定 - 902
ダイアログ モードの NodeCfgUtil による
PowerHA AIM の設定 - 689
対象読者 - 15
タイムシェア スケジューラ、TS (Solaris) -
949
タスク (Solaris) - 949
ツール - 899
ツリー階層の参照 - 441
ディスクバリ - 59
ディスクの削除: VMware vCenter - 861
ディスクの追加: VMware vCenter - 777
データ収集の設定 - 882
データストア (VMware) - 950
データセンター (VMware) - 950
データ センター用のデータ収集の設定 - 885

データベース - 25
データベース管理者 (sa) パスワードの変更 - 42
適用されるポリシーの設定と表示 - 330
デフォルト値 - 478
デフォルト パッケージ ラッパー - 153
デフォルト ユーザ グループの作成 - 39
デュアル HMC (LPAR) - 950
展開管理証明書のプライマ インストールへの提供 - 200
展開コンポーネント - 146
展開ジョブ - 192
展開ジョブの再サブミット - 181
展開ジョブの作成 - 174
展開ジョブのステータスの追跡 - 179
展開済みパッケージの表示 - 182
展開ダッシュボード ビュー - 147
展開認証情報の制限 - 170
展開のサイジング キー ファクタ - 150
展開の制限 - 170
展開パッケージ - 152
展開パッケージ設定ファイル - 168
展開パッケージ ライブラリ - 165
展開前の読み取り/書き込みコミュニティの指定 - 177
展開履歴の表示 - 183
電源の設定: Cisco UCS - 793
電源の設定: IBM LPAR - 795
電源の設定: Microsoft Hyper-V - 800
電源の設定: VMware vCenter/vApp 電源の調整 - 803
テンプレート (XenServer) - 950
テンプレートからの vApp のプロビジョニング - 593
テンプレートの仮想マシンへの変換 - 669
テンプレートへの SystemEDGE 設定のインポート - 288
テンプレートまたはポリシーからのモニタの削除 - 243
テンプレートまたはポリシーへの MIB 拡張の追加 - 240

テンプレートまたはポリシーへのモニタの追加 - 225
テンプレートを VM に変換: VMware vCenter - 809
統合 - 719
動的再構成コネクタ インデックス、DRC インデックス (LPAR) - 950
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 - 262
ドメイン サーバが使用できない - 917
ドメイン サーバまたは Exchange Server のマネージャへの追加 - 749
トラップ - 951
トラップとコミュニティの定義 - 219
トラブルシューティング - 759, 911

な

名前でホストを検出 - 823
認証情報設定の管理 - 730
ネイティブ セキュリティ - 37
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 - 43
ネットワーク インターフェースの削除: VMware vCenter - 863
ネットワーク インターフェースの追加: VMware vCenter - 779
ネットワーク オブジェクト (XenServer) - 951
[ネットワーク管理]操作の使用 - 443
ネットワーク ディスカバリのキャンセル - 65
ネットワークの検出 - 62, 825
ネットワークの再検出 - 65
ネットワークの削除 - 66
ネットワークのプロパティ - 658

は

パーティション - 477
ハードウェア管理コンソール、HMC (LPAR) - 951
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 - 916

配布サーバが接続するドメイン サーバの変更 - 149
はじめに - 15, 735
パスワード管理 - 40
パッケージについて - 145
パッケージフィルタ - 168
パッケージラッパーのコピー - 173
パッケージラッパーの削除 - 173
パッケージラッパーの名前変更 - 174
パッケージラッパーの変更 - 172
パフォーマンス DB - 26
パフォーマンスしきい値の設定 - 893
パフォーマンス チャートの LPAR レベルのメモリ 使用率が 0 として表示される - 921
汎用自動ウォッチャー - 254
非グローバルゾーン (Solaris) - 951
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 - 188
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 - 190
ファイバ チャネル、FC - 951
フェア シェア スケジューラ、FSS (Solaris) - 952
フォールトトレランス、FT (VMware) - 952
フォールトトレランスの管理 - 629
フォールトトレランスの管理: VMware vCenter - 829
フォールトトレランスのモニタ - 627
フォールトトレランスの要件 - 624
複数の仮想 I/O サーバ - 952
複数の配布サーバ - 151
物理ネットワーク インターフェース、PIF (XenServer) - 952
物理ブロック デバイス、PBD (XenServer) - 952
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 - 914
プラットフォーム管理モジュール (PMM) - 952
ブレード (UCS) - 953
ブレード電源アクションの作成 - 382

プロジェクト (Solaris) - 953
プロセス グループ モニタの作成 - 237
プロセス グループ モニタの定義 - 301
プロセスとサービスの自動ウォッチャー - 254
プロセス モニタの作成 - 229
プロセス モニタの定義 - 293
プロセッサ セット、pset (Solaris) - 953
プロセッサ プール (LPAR) - 953
プロパティ - 655
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ない - 928
プロビジョニングされた仮想マシンの使用 - 454
分散仮想スイッチ - 653
分散スイッチの管理: VMware vCenter - 827
ヘルス状態の設定 - 873
ヘルプデスク チケットのオープン - 845
ポイント エージェント設定の実行 - 85
ポート グループのプロパティ - 657
ポートのプロパティ - 658
ポート プロファイルとポート プロファイル クライアントの作成 - 370
ポート プロファイル ネットワークトポロジの作成 - 369
ポート プロファイルを管理する方法 - 368
ポーリング間隔 - 953
ポーリング グループ - 478
保守モードの有効化 - 87
ホスト バス アダプタ、HBA - 953
ポリシー - 656
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 - 636
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 - 205
ポリシー設定機能の一般的な使用法 - 267
ポリシー適用の進捗状況の確認 - 329
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 - 244
ポリシーとテンプレートを使用した SystemEDGE およびサービス レスポンス モニタの設定方法 - 202
ポリシーの作成 - 137, 210

ポリシーの適用 - 139
ポリシーのユース ケース - 880
ポリシーベースの設定 - 953
ポリシーへの SystemEDGE 設定のインポート - 270
ポリシーを以前のバージョンに戻す - 332

ま

マシン状態の変更: Microsoft Hyper-V - 783
マシンのクローン作成: Solaris ゾーン - 785
マシンの削除: IBM LPAR - 816
マシンの削除: Microsoft Hyper-V - 818
マシンの削除: Solaris ゾーン - 820
マシンの削除: VMware vCenter - 822
マシンのプロビジョニング: IBM LPAR - 846
マシンのプロビジョニング: Microsoft Hyper-V - 850
マシンのプロビジョニング: Solaris ゾーン - 854
マシンのプロビジョニング: VMware vCenter - 858
マシンへのテンプレートの適用 - 287
マシンへのポリシーの適用 - 327
マシンをマイグレート: VMware vCenter - 839
マネージャからの管理対象外モードの情報の削除 - 343
マネージャからの管理対象モードの情報の削除 - 340
マネージャへの Cisco UCS の追加 - 353
マネージャへの Citrix XenServer 接続の追加 - 389
マネージャへの Microsoft Cluster Service の追加 - 699
マネージャへの Red Hat Enterprise Virtualization 接続の追加 - 526
マネージャへの Solaris ゾーン接続の追加 - 554
マネージャへのサーバ接続の失敗 - 750
マネージャへのサーバ接続の失敗 (Citrix XenServer) - 390
メトリック収集に関する重要な点 - 882
メトリックフィルタの設定 - 894
メモリの設定 - 495
メモリの動的な追加または削除 - 631

メモリの変更: VMware vCenter - 843
文字列化 - 954
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 - 926
モニタ対象の vSphere および vCenter Server のリソース - 596
モニタリング ソフトウェアの設定 - 86
モニタリング対象のリモートシステムの追加 - 729
モニタリング テンプレート適用の進捗状況の確認 - 287

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 - 55
ユーザ アクセス制御 - 35
ユーザ インターフェース - 26
ユーザ インターフェースが動作しない - 928
ユーザ インターフェースへのアクセス - 27
ユーザ グループ管理 - 46
ユーザ グループ権限の設定 - 51
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 - 55
ユーザ グループの削除 - 54
ユーザ グループの作成 - 47
ユーザ権限およびアクセス要件のリファレンス - 97
ユーザ固有のメトリック (MIB 拡張) をモニタする方法 - 259
ユーザとユーザ グループの管理 - 35
ユーザまたはユーザ グループの検索 - 47
ユース ケース: アクションを定義する - 881
ユース ケース: サーバをサービスに追加する - 880
ユース ケース: 新規ルールをサービスに追加する - 881
ユース ケース シナリオ - 721
ユニバーサル一意識別子、UUID - 954
要件 - 745
要件の確認 - 251, 335, 349, 386, 412, 429, 440, 451, 459, 524, 550, 600, 648, 695
要件の確認 (SNMPv1/2) - 116

要件の確認(サーバレベル) - 128

ら

リソース管理 (Solaris) - 954
[リソース管理]操作の使用 - 442
リソース サマリおよびイベントの表示 - 483
リソース ツリーでグループを確認する - 474
リソース ツリーでの Cisco UCS の確認 - 361
リソース ツリーでの Citrix XenServer グループ
の確認 - 397
リソース ツリーでの Huawei GalaX の確認 - 422
リソース ツリーでの Hyper-V Server フォルダの
確認 - 512
リソース ツリーでの Microsoft Cluster Service
の確認 - 707
リソース ツリーでの Red Hat Enterprise
Virtualization グループの確認 - 534
リソース ツリーでの Solaris ゾーン グループの
確認 - 562
リソース ツリーでの vCenter Server フォルダの
表示の確認 - 618
リソース ツリーでの VMware vCloud フォルダの
確認 - 589
リソース プール (Solaris) - 954
リソース プール (VMware) - 954
リソース プール、オーバーコミット
(XenServer) - 954
リソース プールの作成 - 567
リソース プール マスタ (XenServer) - 955
リソース 割り当て - 631
リソース 割り当ての共有 - 632
リソース 割り当ての制限 - 633
リソース 割り当てのベスト プラクティス - 447,
634
リソース 割り当ての予約 - 633
リモート および マルチインスタンスの vCloud
Director のサポート - 589
リモート 展開 アーキテクチャ - 144
リモート 展開 の検索機能の強化 - 148
リモート 展開 の使用 - 169
リモート 展開 を使用した ADES AIM の展開 - 738

リモート モニタ システム の設定 - 724
リモート モニタリング - 108, 713
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 - 714
リモート モニタリング の利点 - 716
リモート モニタリング メトリックのサポート - 727
リモート モニタリング を使用したシステムの管
理 - 728
リモート 展開 エージェント - 107
利用可能な Solaris ゾーン アクション - 571
履歴 モニタ の作成 - 235
履歴 モニタ の定義 - 299
ルール と アクション - 763
ルール と アクション の使用 - 763
ルールの作成 - 767
ルールの設計 - 767
レポートの作成 - 814
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 - 918
ログ ファイル モニタ の作成 - 231
ログ ファイル モニタ の定義 - 295
論理 パーティション、LPAR - 955
論理 パーティション のアクティブ化 - 486
論理 パーティション の再起動 - 492
論理 パーティション の削除 - 491
論理 パーティション のシャットダウン - 493
論理 メモリ ブロック、LMB (LPAR) - 955

わ

割り当て プール 容量 (LPAR) - 955