CA Spectrum®

Cisco デバイス管理ガイド

CA Technologies 製品リファレンス

このドキュメントでは CA Spectrum® Infrastructure Manager （CA Spectrum）について説明します。

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: Cisco デバイス サポートの概要

このセクションには、以下のトピックが含まれています。

デバイス サポート

CA Spectrum Cisco デバイス認証により、Cisco MIB とトラップのサポート、わかりやすいデバイス識別、OneClick ビュー、Cisco 技術サポートが実現します。 CA Spectrum Cisco デバイス認証は、特定デバイスやファームウェアに対する CA Spectrum の標準機能も提供します。

デバイス ファミリ認証の例として、Catalyst、PIX Firewall、Wireless LAN Controller、Aironet などがあります。

ファームウェア ベースの認証の例には、Cisco IOS、CatOS、Unified Computing System （UCS）などがあります。

ご使用の Cisco デバイスで特定のデバイス ファミリ認証が使用できない場合は、以下のいずれかのファームウェア ベースのモデル タイプを使用します。

- Rtr_Cisco -- IOS ファームウェアを実行している Cisco ルータをモデリングします。
- SwCiscoIOS -- IOS ファームウェアを実行している Cisco スイッチをモデリングします。
- RtrCatOS -- CatOS ファームウェアを実行している Cisco ルータをモデリングします。
- SwCatOS -- CatOS ファームウェアを実行している Cisco スイッチをモデリングします。
- CiscoNXOS -- NX-OS ファームウェアを実行している Cisco Nexus デバイスをモデリングします。
- GnCiscoDev -- IOS または CatOS ファームウェアを実行していない Cisco デバイスをモデリングします。

MIB ソース

Cisco デバイス ファームウェアに応じて、シャーシとボード、またはモジュールの情報が、以下の MIB ソース内に見つかります。

OLD-CISCO-CHASSIS-MIB

Cisco は、この MIB を推奨しません。 そのため、情報は不完全な場合があります。この MIB のコンテンツを表示するには、OneClick で［Cisco シャーシ ビュー］サブビューを参照します。

CISCO-STACK-MIB

CatOS デバイスは、この MIB をサポートします。 この MIB は推奨されません。ENTITY-MIB を優先してください。 この MIB の内容を表示するには、MIB ツール ユーティリティを参照します。

注: MIB ツールの詳細については、「認定ユーザ ガイド」を参照してください。

ENTITY-MIB

この MIB には、新しいデバイス用の最新のボードまたはモジュール情報が含まれます。 ただし、旧式のデバイスを使用している場合、この MIB に情報が正しく入力されません。 この MIB の内容を表示するには、OneClick で［エンティティ ビュー］サブビューを参照します。

第 2 章: Cisco Unified Computing System

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 の概要

Cisco Unified Computing System （UCS）は、シャーシとサーバのブレードなど、連携する一連の専用デバイスから構成されています。 UCS は、動的な IT インフラストラクチャの提供と、ネットワーク、コンピューティング、および仮想化の各リソースの統合により、データ センターをサポートします。

CA Spectrum は、Cisco UCS の以下の主要コンポーネントへの可視性を提供します。

UCS マネージャ

Fabric Interconnect スイッチ上で動作している Web サービス エージェント Cisco UCS マネージャは、クライアント インタラクション用に、XML ベースの API をサポートします。

Fabric Interconnect（FI）スイッチ

- 通常、UCS 1 システム当たり 2。Cisco は冗長構成を推奨します。
- NX-OS を実行します。
- UCS マネージャをホストします。

シャーシ

1 つの UCS マネージャ当たり、最大 40 のシャーシ構成を持つ、エージェントレス、スイッチレスのブレード サーバ筐体。 各シャーシは、8 つのハーフ サイズ（横幅）のブレード、または 4 つのフル サイズ（横幅）のブレードを格納します。

ブレード

仮想ホストとして機能するサーバ プラットフォーム。

サービス プロフィール

ブレード サーバの論理ビュー。 FI スイッチ内に格納されていて、ブレード サーバの個別情報（アイデンティティとネットワーク情報）が保存されています。

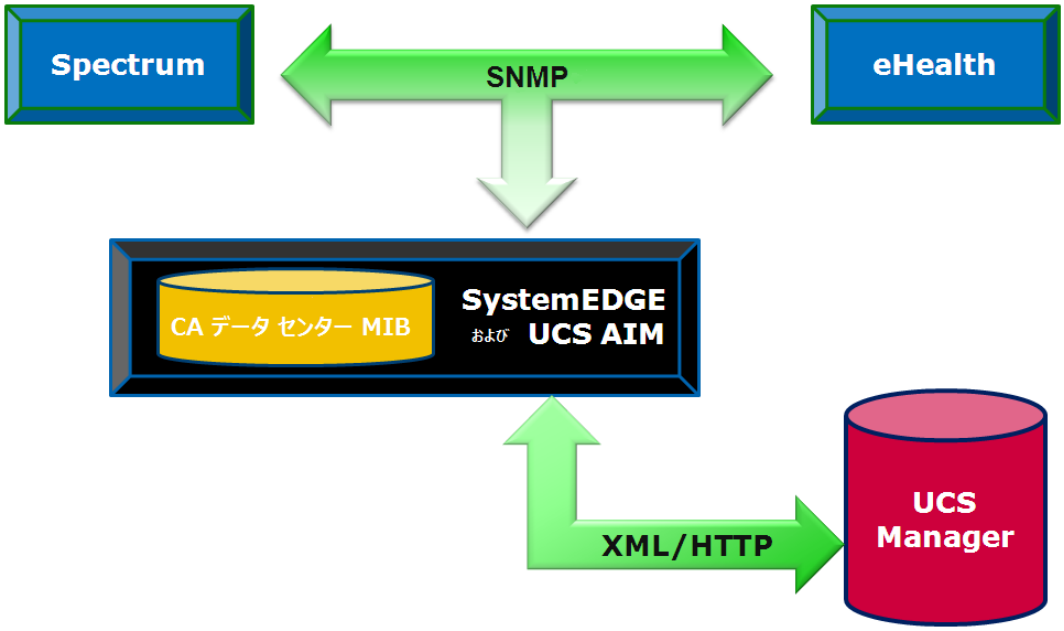
ソリューション アーキテクチャ

特殊な SystemEDGE Application Insight Module（AIM）を使うことで、Cisco UCS に対する CA Spectrum のサポートを有効にすることができます。 この AIM は、UCS 管理環境に関する情報を取得するため、UCS XML ベースの API と通信します。 その後、このデータは CA が開発した 1 組の MIB に書き込まれます。 このソリューションを移用すると、CA eHealth などの他の SNMP クライアントは AIM を活用することができます。

UCS AIM は SystemEDGE SNMP エージェントを拡張したもので、複数の UCS システムをサポートできます。 CA が開発した MIB は次のとおりです。

- 汎用データ センター MIB （CADATACENTERA）
- UCS 固有のデータ センター拡張 MIB （CACUCSEXTENSIONA）

次の図に示すように、CA Spectrum や CA eHealth などの CA 製品は、Cisco UCS の詳細情報を取得するため、SNMP を使って、UCS AIM をホストする SystemEDGE に接続します。 UCS AIM は、XML/HTTP を使って UCS マネージャに接続します。



機能

CA Spectrum UCS 認定機能には以下のものが含まれます。

- 自動デバイス ディスカバリとモデリング - UCS コンポーネントのモデルを作成し、ブレード モデルと任意の常駐 ESX ホストの間の関連性を保持します。
- 接続 - UCS システム コンポーネントの正確な物理（レイヤ 2）トポロジ マップを生成します。
- 障害管理の強化 -- 徴候的なアラームの認識と抑制、およびプロキシ管理を使った障害分離の支援を行います。
- 専用 UCS ビュー -- UCS 固有データを表示します。
- インテリジェントなトラップ転送 -- 個々の UCS コンポーネントでアラームを生成できます。
- シャーシ管理（非 UCS 固有） - CA Spectrum の豊富なシャーシ管理機能セットを活用します。

自動化されたデバイス ディスカバリとモデリング

認定では、UCS AIM をホストしている Host_SystemEDGE モデルを作成することで、UCS システム コンポーネントが自動的にモデリングされます。このモデルは Cisco UCS Manager として識別できます。 このモデルは、UCS AIM MIB が検出されると、cacucsaimApp のアプリケーション モデル タイプを作成します。次に、このアプリケーション モデルは、ファブリック インターコネクト、シャーシ、ブレード、サービス プロファイルなど、UCS システム コンポーネントを作成します。

注: ファブリック エクステンダ、電源、メディア アダプタ、インターフェースなど、すべての UCS コンポーネントがモデリングされるとは限りません。

次に、任意のブレード上にある、以前モデリングされた ESX ホストに関する検索が実行されます。 このハードウェアとソフトウェアの関係を表示できるようにするため、対応するブレードと ESX モデル間の関連付けが作成されます。

最後に、各 UCS システムを表すコンテナ モデルが作成されます。 これらのモデルは、SystemEDGE ホストと同じコンテナ（ユニバースなど）に常駐します。 各コンテナは、UCS システム コンポーネントの論理的トポロジのグループ化を提供します。

UCS 環境からステータスとモデリング情報を収集するために、UCS AIM MIB は定期的にポーリングされます。ポーリング間隔の設定に関する詳細については、「Cisco UCS AIM ポーリングの制御 (P. 26)」を参照してください。

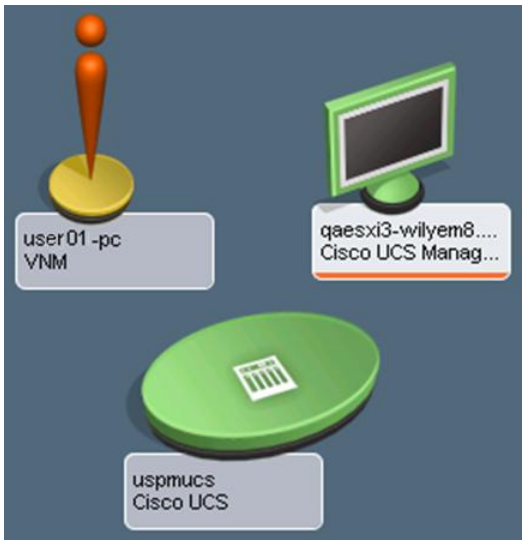
重要: 任意のランドスケープでは、UCS AIM が同じ UCS システムを監視する、複数の Host_SystemEDGE モデルをモデルリングできません。この設定は、サポートされていません。

UCS AIM をホストする Host_SystemEDGE が仮想デバイスの場合、対応する仮想テクノロジー AIM をホストする Host_SystemEDGE よりも前にモデリングを行ってください。そうでないと、仮想テクノロジーの物理ホスト コンテナの内部に UCS コンテナが誤って作成されます。 この状況は、CA Spectrum の障害分離アルゴリズムを中断させます。

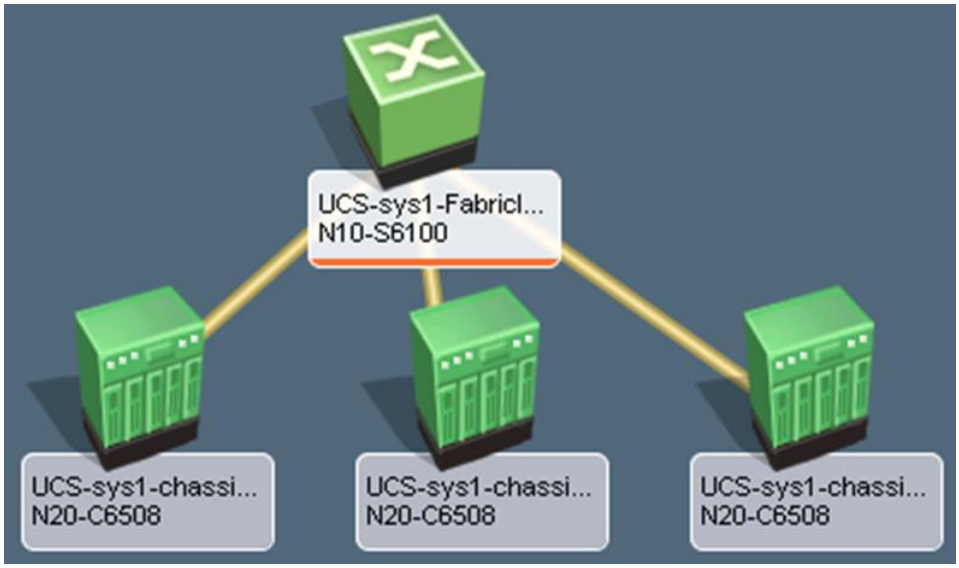
UCS コンテナ モデル

UCS コンテナを表すために、CA Spectrum は、シャーシ ロゴの付いた標準的なコンテナ アイコンを使用します。 UCS コンテナには CiscoUCSContainer というモデル タイプがあります。 各コンテナは、単一の UCS システム（最大 2 つの FI および 40 のシャーシ）のトポロジ上重要なモデルをすべて収集します。 UCS コンテナの内容は変更できません。

UCS コンテナは、次のイメージとして表示されます。



次のイメージでは、UCS Container の内容の例について説明します。



UCS Fabric Interconnect モデル

UCS Fabric Interconnect は、CA Spectrum の標準スイッチ アイコンを使用します。 このデバイスが IP アドレスまたはディスカバリによってモデリングされ、その NX-OS SNMP エージェント（デフォルトでは無効）が有効な場合、CiscoUCSFabricInterconnect というモデル タイプが作成されます。そうでない場合、UCS 自動ディスカバリによって、Ping 可能なモデルが作成されます。このモデルには、デバイス インタフェースも、アップストリーム デバイスへの接続も含まれません。 IP アドレスのモデリングは、UCS ディスカバリの後に発生する可能性があることに注意してください。その場合、Ping 可能モデルが CiscoUCSFabricInterconnect モデルに置き換えられます。

UCS Fabric Interconnect モデルは専用の UCS OneClick ビューをサポートし、UCS Fabric Interconnect のトラップとアラームのターゲット モデルです。

UCS シャーシ モデル

UCS シャーシは、CA Spectrum の標準シャーシ アイコンを使用し、CiscoUCSChassis というモデル タイプがあります。OneClick のコンポーネント詳細画面内の［インターフェース］タブは、UCS シャーシ用に拡張されます。ブレード管理を支援するため、シャーシ内のブレードが表示されます。

また UCS シャーシにより CA Spectrum の障害分離機能も拡張され、共同設置されたハードウェア リソースのアラーム相関が提供されます。

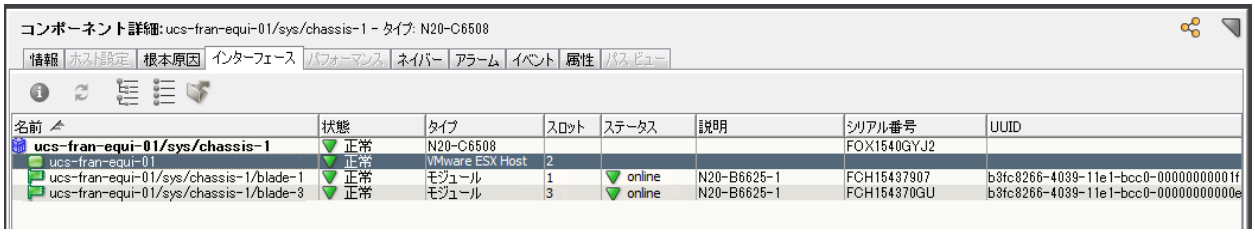
UCS シャーシ モデルは、専用 UCS OneClick ビューをサポートします。またこのモデルは、UCS シャーシのトラップとアラームのターゲット モデルです。

UCS ブレード モデル

UCS ブレードは CA Spectrum でモデリングされますが、ファブリック インターコネクト スイッチやシャーシとは異なり、親 UCS コンテナの内部にも、CA Spectrum のトポロジの他の場所にも表示されません。 ただし、各シャーシの UCS ブレードはシャーシの［インターフェース］タブにリスト表示されます。 UCS ブレードには、CiscoUCSBlade というモデル タイプがあります。

CA Spectrum は、ブレードと、そのブレード上に常駐している ESX ホストの間の関連付けを自動作成します。 この関連付けは、以前モデリングした ESX ホストの検索を実行して、UUID （Universally Unique Identifier）値を取得することで実行されます。 その後、ブレード UUID が調べられます。一致が見つかると、ESX ホスト モデルはブレード モデルと関連付けられます。 自動関連付けがサポートされているのは、ESX ホストだけです。 CA Spectrum はブレード（ハードウェア）と ESX ホスト（ソフトウェア）との関係を理解し、拡張された障害分離機能を介して、この情報を活用します。ブレードで障害が発生したため ESX ホストと通信できない場合などに、意味のあるアラーム詳細が表示されます。

関連付けが作成されると、シャーシ モデルの［インターフェース］タブで、ブレード モデルが X ホスト モデルに置き換えられます。



UCS ブレードを対応する SNMP エージェント モデルに手動で関連付け、ブレード（ハードウェア）とエージェント（ソフトウェア）との関係を表示することもできます。

UCS ブレード モデルは、専用 UCS ハードウェア ベースの OneClick ビューをサポートします。このビューには、以下の種類の情報が表示されます。

- CPU の負荷、メモリ、ストレージの使用率などの統計情報
- イメージ インベントリ（BIOS とファームウェア）および BIOS H/W 設定

- ブレード サーバの物理インターフェース
- サービス プロファイルの詳細

UCS ブレード モデルは、UCS ブレード トラップおよびアラーム用のターゲット モデルです。

詳細

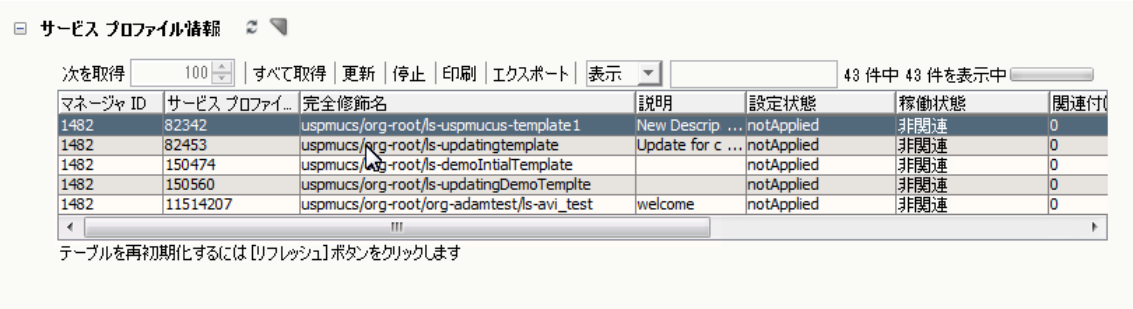
ブレード/SNMP デバイスの手動での関連付け (P. 24)

UCS サービス プロファイル モデル

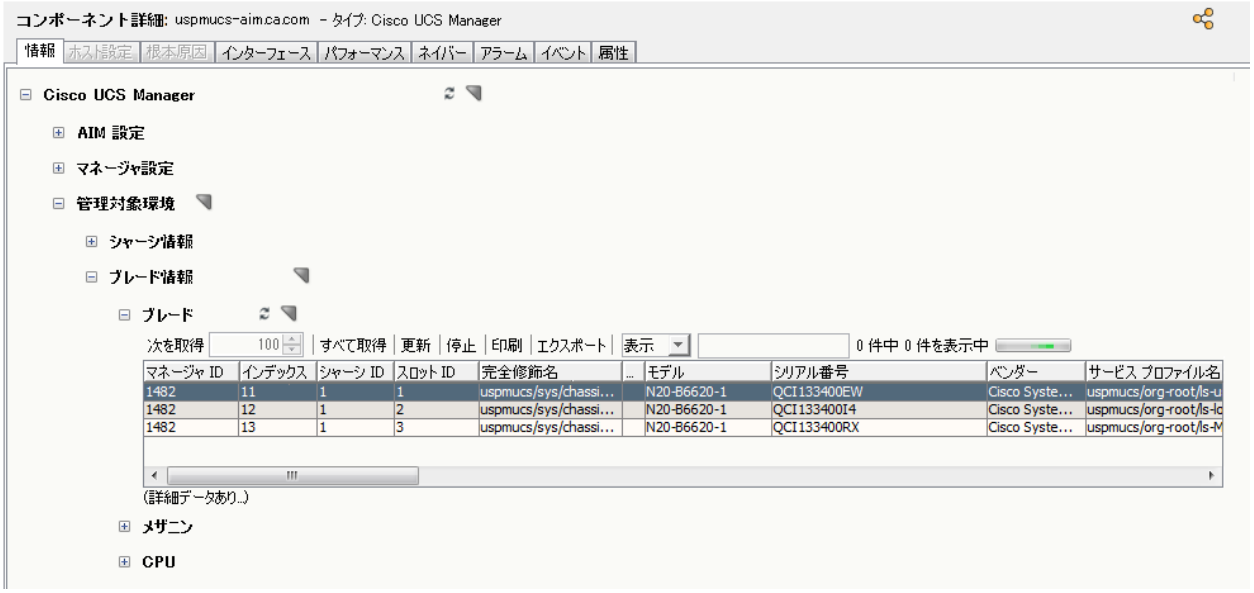
Cisco Unified Computing System でプロビジョニングされるブレード サーバは、サービス プロファイルによって指定されます。 サービス プロファイルとは、サーバおよびその LAN と SAN ネットワーク接続のソフトウェア定義です。 UCS サービス プロファイルには、CiscoUCSServiceProfile というモデル タイプがあります。

サーバ、ネットワークおよびストレージ管理者は、サービス プロファイルを作成します。 サービス プロファイルは、Cisco UCS 6100 Series Fabric Interconnects に保存されます。 サービス プロファイルをブレード サーバ上に展開する場合、UCS マネージャは、ブレード サーバ、そのネットワーク アダプタ、ファブリック エクステンダおよび Fabric Interconnect を自動設定し、サービス プロファイル内で指定された設定をサポートします。

CA Spectrum は、UCS マネージャによって定義されるサービス プロファイルごとに、モデルを作成します。 これらのモデルは、サービス プロファイル モデル クラスの検索オプションが含まれる［OneClick ロケータ］タブから表示できます。 さらにサービス プロファイル詳細も、さまざまな OneClick ビューに表示されます。 UCS AIM をホストしている Host_SystemEDGE モデル上で、［Cisco UCS マネージャ］、［管理対象環境］、および［サービス プロファイル情報］オプションをオンにします。 その後、Host_SystemEDGE が管理する UCS システムのすべてのサービス プロファイルの名前、ID、説明、関連付けられているブレード、および各種ステータスを確認できます。



また CA Spectrum は、各 UCS マネージャ シャーシにインストールされている各ブレードに関連付けられているサービス プロファイルを表示します。



UCS サービス プロファイル モデルは、UCS サービス プロファイル アラームのターゲット モデルです。

接続

UCS Fabric Interconnect モデルは、アップストリーム デバイスとシャーシ内のブレード サーバ間の境界切り替えノードを提供することで、接続に加わります。

UCS Fabric Interconnect からのアップストリーム

Fabric Interconnect インターフェースからのアップストリーム接続は、標準ブリッジ テーブルを介して実行されます。 これらの接続では、以下の手順を必要とします。

- Fabric Interconnect での、ネイティブ NX-OS SNMP エージェントの有効化
- IP アドレスまたはディスカバリによる、デバイスのモデリング

詳細

UCS Fabric Interconnect モデル (P. 14)

UCS Fabric Interconnect からのダウンストリーム

UCS Fabric Interconnect からその構成シャーシへのダウンストリーム FCoE 接続は、標準的な CA Spectrum L2 接続として表示されます。 これらの接続はプログラム的に作成されるもので、標準的なブリッジ テーブルや UCS MIB によって作成されるものではありません。

障害管理の強化

UCS 用に強化された障害管理では、次のような 2 種類のアラームが用意されています。

- 障害アラーム
  - L2 可用性に関する問題を示します。
  - 特別な相関ロジックで強化されます

- プロキシ ロスト アラーム
  - 更新された UCS 情報を、SystemEDGE UCS AIM ホストから取得できないことを示します。
  - ホスト自体のプロキシ利用不可アラームを含んでいます。

UCS の障害管理拡張機能には、シャーシ レベルおよびブレード レベルの可用性アラームと、インフラストラクチャと環境の問題を示す、トラップ生成アラームが含まれます。

UCS は、次のようなアラーム相関の利点を活用します。

- 根本原因の特定
- 無関係なアラームの抑制
- 根本原因に対する症状の関連付け
- 影響の表示

UCS アラーム相関は、シャーシ レベルと UCS システム レベルの両方で発生します。

シャーシ レベルのアラーム相関は、障害（接続切断）アラーム発生時のシャーシ、そのブレード、およびすべての SNMP ブレード エージェント モデルが含まれるドメインを使用します。 これらの各ドメイン エンティティ（つまり、シャーシ、ブレードおよび SNMP ブレード エージェント）に対して、接続が切断された場合、単一のシャーシ ダウン アラームがシャーシで生成されます。 接続切断アラームの全セットは、これと相関しています。

プロキシ ロスト アラームの場合、シャーシ レベルのアラーム相関で、シャーシとそのブレードを含む、より小さなドメインを使用します。 ここで、すべてのブレードのプロキシ ロスト アラームは、シャーシのプロキシ ロスト アラームと相関しています。

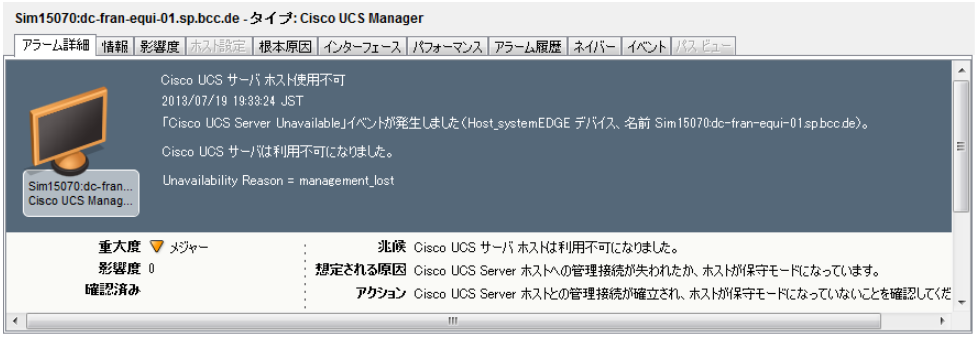
UCS System レベルのアラーム相関は、SystemEDGE ホスト、FI および子シャーシ、およびブレードを含むドメインを使用します。 CA Spectrum と SystemEDGE ホスト間で通信が切断された場合、プロキシ ロスト アラームはすべての FI、シャーシおよびブレードに存在します。プロキシ利用不可アラームは、ホストに存在します。

すべてのコンポーネントに対するプロキシ ロスト アラームは、ホストのプロキシ利用不可アラームと相関しています。 これらの相関は、階層的に実行されます。 プロキシ利用不可アラームはそれ自体、通信障害の理由を示すアラームに関連しています。 たとえばこのアラームは、接続切断、管理の喪失、または保守モードを示します。 次に、このトップレベルの重要アラームは、アラーム ウィンドウ内に表示されます。

根本原因の分離例

根本原因の分離は、以下の例にように行われます。

- UCS シャーシの電源が誤ってオフにされると、ブレード（およびブレード上で実行されているサービス）が影響を受けます。 そのため、すべてのブレード上の個別の接続切断アラームは、シャーシの障害を特定するシャーシ ダウンアラームと相関しています。
- CA Spectrum は、SystemEDGE ホストとの接続を失います。 そのため、すべての FI、シャーシおよびブレード上のプロキシ ロスト アラームは、ホストのプロキシ使用不可アラームと、階層的に関連付けられます。



シャーシとブレードの可用性アラーム

シャーシの可用性アラームには、シャーシ ダウンおよびブレード ステータス ダウン（シャーシ ダウンと相関関係がある）があります。

ブレードの可用性アラームには、ブレード削除およびブレード障害（ブレードは存在するが、障害状態）があります。 これらのアラームは両方とも、親シャーシ上の既存のブレード ステータス不明アラームに関連付けられています。 ブレード モデルはデフォルトでは、ブレードの交換できる有効期間は 2 時間で失効するという点に注意してください。

サービス プロファイル アラーム

サービス プロファイルの詳細をすべて表示するだけではなく、各サービス プロファイルの CA Spectrum モデルも作成します。 CA Spectrum は、積極的にサービス プロファイルの状態を監視し、各サービス プロファイルの動作状態に基づいてイベントとアラームを生成します。

トラップ生成アラーム

UCS は、トラップが生成するアラームをサポートしています。このアラームは、インフラストラクチャと環境の問題を示しています。適切な場合、識別子が使われます。 例には Blade Added、Blade Removed、Power Supply Inoperable、Temperature Warning などがあります。

専用 UCS ビュー

専用 UCS ビューは、以下のデバイス タイプ（かっこ内の項目）に対して使用できます。

- SystemEDGE ホスト（Cisco UCS Manager）

  このビューには、管理対象環境のテーブル ビューが含まれます。
- ファブリック インターコネクト（Cisco UCS スイッチ）
- シャーシ（Cisco UCS シャーシ）
- ブレード（Cisco UCS ブレード）
- サービス プロファイル（N/A）

OneClick ビューは、メモリ DIMM、メザニン カード、ファブリック インターコネクト エクステンダ、インターフェースなど、ハードウェアの詳細を表示します。

インテリジェントなトラップ転送

UCS トラップはすべて UCS AIM から生成されるため、SystemEDGE ホストから CA Spectrum に到達します。 このため、CA Spectrum は適切な UCS コンポーネントに関するイベントまたはトラップを生成するため、転送メカニズムを使用します。 コンポーネントが適切かどうかの決定は、トラップ変数値を検証することで実現されます。 該当するコンポーネントが見つからない場合、トラップ イベントは SystemEDGE ホストでアサートされます。

シャーシ管理

UCS は、豊富なシャーシ管理機能セットを活用します。CA Spectrum で使用可能な機能を以下に示します。

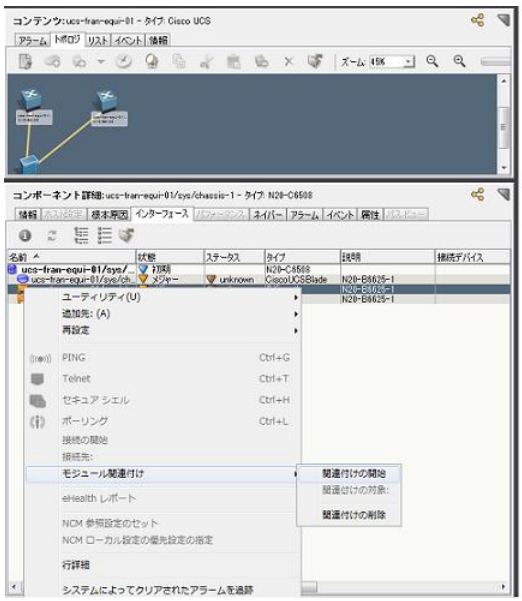
- ブレード/SNMP デバイスの手動での関連付け
- ブレードと管理対象デバイスの表示
- ロケータ検索

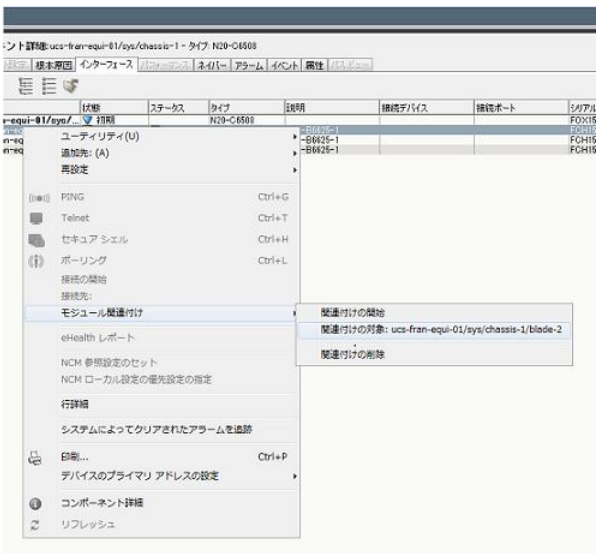
詳細については、「認定ユーザ ガイド」の「シャーシベースのサポート」を参照してください。

ブレード/SNMP デバイスの手動での関連付け

ブレード/SNMP デバイスの手動関連付けは、シャーシの 1 つのブレードを SNMP 対応のブレード エージェント モデルにバインドします。 この関連付けにより、エージェント モデルからシステム/シャーシの場所への迅速な決定が可能になります。SNMP モデルは UCS コンテナには移されませんが、シャーシの［インターフェース］タブのブレードではこの処理が実行されます。

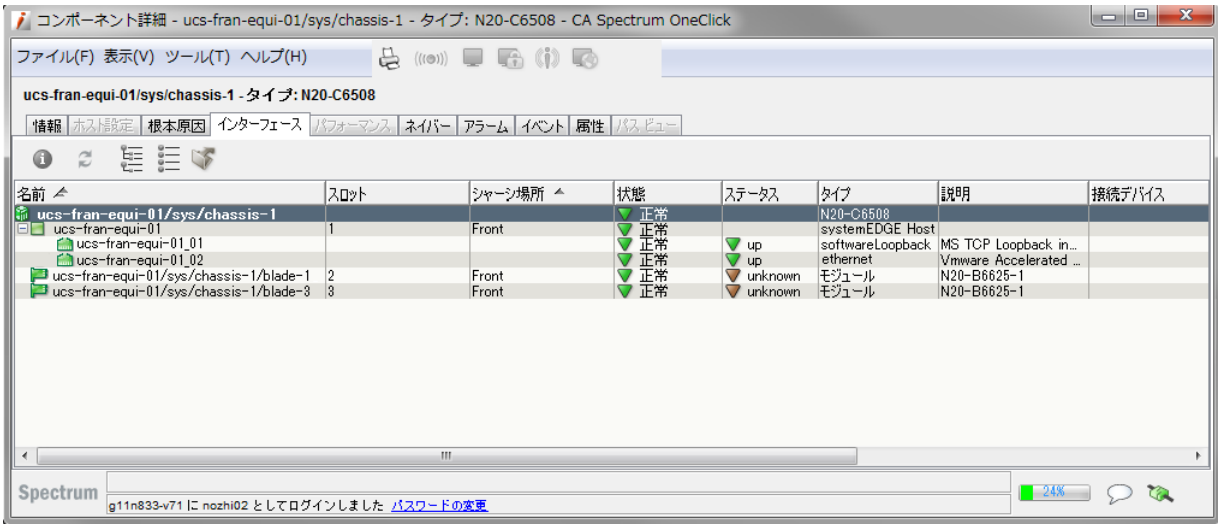
この統合を支援するため、SNMP エージェント モデルがシャーシ障害相関関係に組み込まれます。 ブレード/エージェントの関連付けによって、シャーシ ベースのロケータ検索による SNMP モデルの識別も可能になります。





ブレードと管理対象デバイスの表示

関連する SNMP デバイスを含めることで、拡張された［インターフェース］タブには、シャーシのブレードと管理対象デバイスが表示されます。



ロケータ検索

シャーシ ベースの検索は、［ロケータ］タブのシャーシ ノードの下に一覧表示されます。 これらの検索により、シャーシとそのコンポーネントを迅速に特定できます。

検索には以下のものが含まれます。

- すべてのシャーシ
- すべてのシャーシ管理対象デバイス
- すべてのモジュール
- 管理対象デバイス - シャーシ名
- モジュール - シャーシ名

Cisco UCS AIM ポーリングの制御

ネットワークの問題のトラブルシューティングまたは Cisco UCS Manager のパフォーマンスのチューニングを行う場合、Cisco UCS AIM（cacucsaimApp）ポーリング レートを変更して頻度を増減してください。Cisco UCS AIM アプリケーション モデルで Poll_Interval 属性を設定することにより、ポーリング レートを設定できます。

次の手順に従ってください:

1. OneClick を開き、［ナビゲーション］ペインの［ロケータ］を選択します。
2. ［アプリケーション モデル］を展開し、［デバイス IP アドレス］をダブルクリックします。

   ［検索］ダイアログ ボックスが表示されます。
3. ［デバイス IP アドレス］フィールドに Cisco UCS Manager の IP アドレスを入力し、［OK］をクリックします。

   Cisco UCS Manager のアプリケーション モデルの一覧がコンテンツ画面に表示されます。
4. cacucsaimApp アプリケーション モデルを選択します。

   アプリケーション モデルの詳細がコンポーネント詳細画面に表示されます。
5. ［コンポーネント詳細］ペイン内の［情報］を選択します。
6. ［CA Spectrum モデリング情報］を展開します。
7. ［ポーリング間隔（秒）］フィールドの［設定］をクリックし、新しい値を入力し、Enter キーを押します。

   注: ［ポーリング間隔］値を任意の数から 0 に変更すると［ポーリング］フィールドも［オフ］に設定され、UCS AIM ポーリングが無効になります。［ポーリング間隔］を 0 に設定し、［ポーリング］フィールドを［オン］に設定した場合、UCS AIM ポーリングは、Cisco UCS Manager デバイスに対して設定されているポーリング間隔を使用して続行されます。

   Cisco UCS AIM ポーリング レートが設定されました。

第 3 章: Cisco Catalyst

Cisco Catalyst デバイス サポート

CA Spectrum は複数の拡張認証で、Catalyst デバイス ファミリ 1200、1400、1900、2820、3000、3200、4000、4500、5000、および 6500 をサポートします。

Catalyst 2900 および Catalyst 3500 デバイス ファミリについては、特定の拡張認証は、サポート対象の MIB セットに依存します。

CA Spectrum は Catalyst 2900 シリーズ デバイスを次のようにモデリングします。

- HubCat29xx モデル タイプは、IOS ファームウェアを実行し、CISCO-C2900-MIB をサポートする Catalyst 2900 シリーズ スイッチをモデリングします。
- SwCiscoIOS モデル タイプは、IOS ファームウェアを実行しているけれども、CISCO-C2900-MIB をサポートしない Catalyst 2900 シリーズ スイッチをモデリングします。Catalyst 2970 および Catalyst 2948g デバイスは、このカテゴリに分類されます。
- SwCat4xxx モデル タイプは、CatOS ファームウェアを実行する Catalyst 2900 シリーズ スイッチをモデリングします。

CA Spectrum は、Catalyst 3500 シリーズ デバイスを次のようにモデリングします。

- HubCat29xx モデル タイプは、IOS ファームウェアを実行し、CISCO-C2900-MIB をサポートする Catalyst 3500 シリーズ スイッチをモデリングします。
- SwCiscoIOS モデル タイプは、IOS ファームウェアを実行しているけれども、CISCO-C2900-MIB をサポートしない Catalyst 3500 シリーズ スイッチをモデリングします。 Catalyst 3550 シリーズは、このカテゴリに分類されます。

Cisco Catalyst ボード障害分離機能の概要

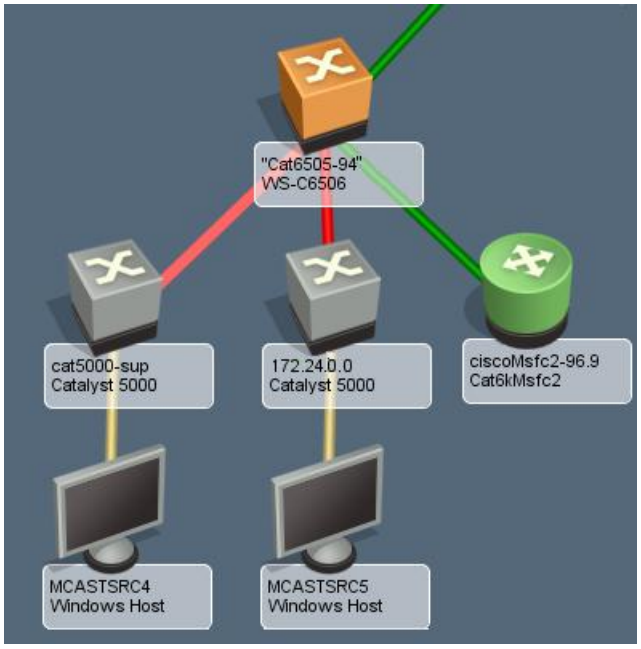
CA Spectrum は、取り外されているボードや障害が発生したボードをサポートします。

従来の障害分離シナリオでは、シャーシベースのデバイス内のボードで障害が発生すると、CA Spectrum はすべてのダウンストリーム デバイス-モデルに関して重大なアラームを生成します。 障害が発生したボードを含んでいるデバイス モデルでは、通常状態が保持されます。 ただしこの動作では、実際にどのデバイスで障害が発生したかはわかりません。

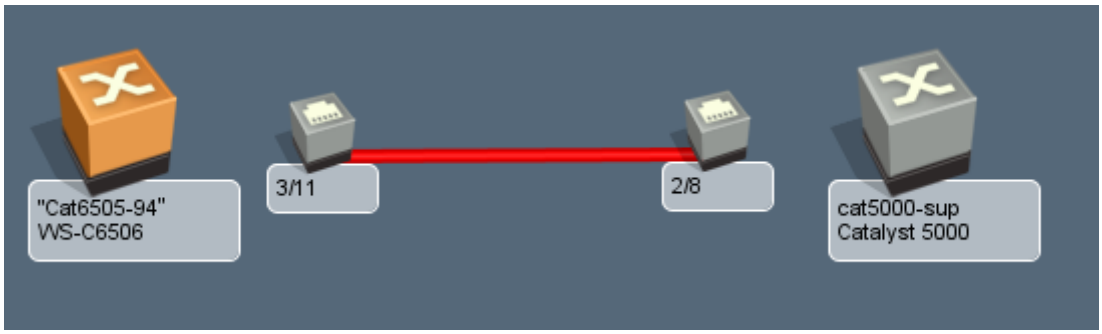
同じシナリオでも、CISCO-STACK-MIB をサポートする Catalyst シャーシベースのデバイスでは、ダウンストリーム デバイス モデルを抑制する障害分離機能が拡張され、障害が発生したボードが装着されたデバイス モデルに関して重大なアラームが生成されます。またボード モデルに関する重大なアラームも生成されます。 そのボード モデルに関連付けられているポートも抑制されるため、どのデバイスに障害があるかだけでなく、障害が発生したボードも明確にわかります。

ダウンストリーム デバイスがある Catalyst デバイスの例

次の例では、接続されたデバイスで［Enable Live Links］を TRUE に設定します。 Catalyst ボードをプルすると、そのボードを介してポートに接続されているデバイスはダウンします。 このイベントが発生すると、CA Spectrum による障害の原因の特定がトリガされます。この例では、2 つのダウンストリーム スイッチおよびホストが影響を受けています。

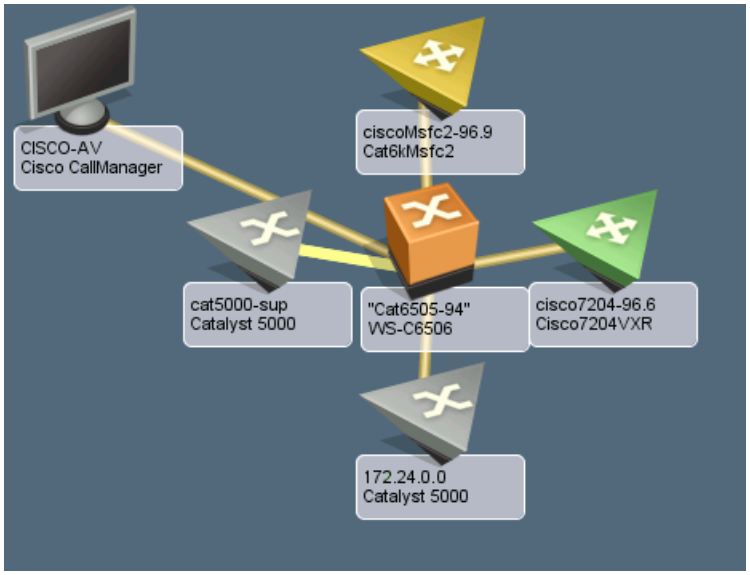


以下の図は、［リンク情報］ビューを示しています。［リンク情報］ビューは、アラームの根本原因を表示します。

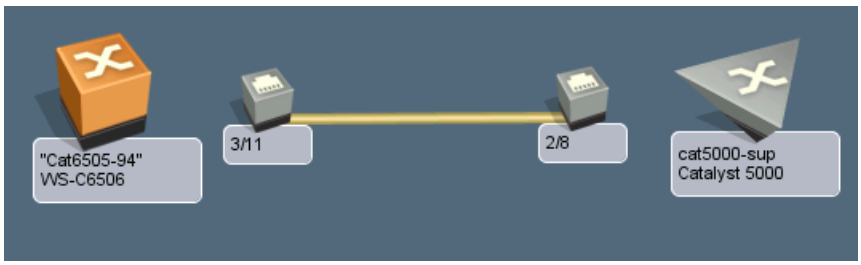


ダウンストリーム デバイスがある Catalyst デバイスの例

以下の例では、接続されたデバイスで［Enable Live Links］を FALSE に設定します。 Catalyst ボードを引き出すと、トラップを受信し、そのボードを介してポートに接続されているデバイスはダウンします。 このイベントが発生すると、CA Spectrum による障害の原因の特定がトリガされます。この例では、2 つのダウンストリーム スイッチ（オフページ参照）およびホスト（ビュー内にはない）が影響を受けています。

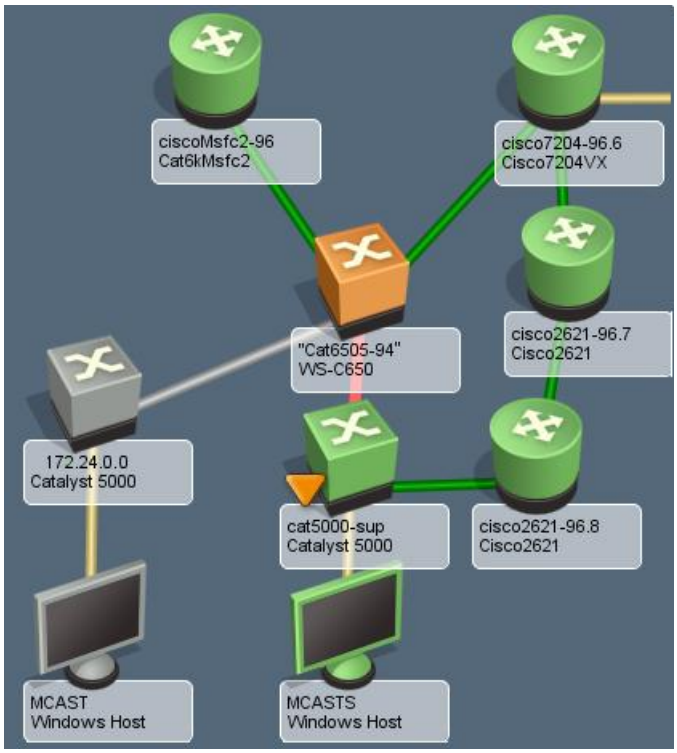


以下の図は、［リンク情報］ビューを示しています。［リンク情報］ビューは、アラームの根本原因を表示します。



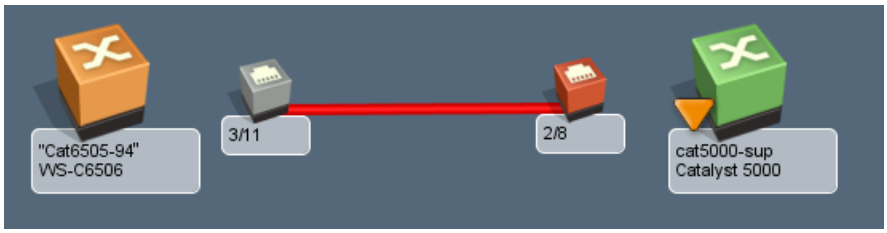
複数の管理パスを備えたダウンストリーム デバイスを持つ Catalyst の例

次の例では、接続されたデバイスで［Enable Live Links］を TRUE に設定します。 Catalyst ボードをプルすると、そのボードを介してポートに接続されているデバイスはダウンします。 このイベントが発生すると、CA Spectrum による障害の原因の特定がトリガされます。 この例では、1 つのダウンストリーム スイッチおよびホストが影響を受けています。



注: 2 番目の管理パスを備えたスイッチは接続を確立したまま、ポートにアラームを発行します。

以下の図は、［リンク情報］ビューを示しています。［リンク情報］ビューは、アラームの根本原因を表示します。



第 4 章: Cisco 技術サポート

このセクションには、以下のトピックが含まれています。

ルータ冗長性

CISCO-HSRP-MIB では、Cisco IOS 専用の Hot Standby Router Protocol（HSRP）を管理できます。

HSRP を使用すると、実際には最初のホップ ルータで障害が発生した場合でも、ホストは見かけ上、単一のルータを使用して、接続を維持しているように見えます。 複数のルータが、このプロトコルに参加します。 複数のルータが協調して、仮想 IP アドレスとして認識されている静的 IP アドレスを持つ単一の仮想ルータをシミュレートします。 終了ホストは、仮想ルータにパケットを転送します。

パケットを転送するルータは、アクティブ ルータとして認識されます。アクティブ ルータで障害が発生すると、スタンバイ ルータがアクティブ ルータと入れ替わります。 HSRP は、参加するルータ上の IP アドレスを使用して、アクティブ ルータとスタンバイ ルータを確定するためのメカニズムを提供します。 アクティブ ルータで障害が発生すると、スタンバイ ルータはホストの接続を大きく損なうことなく、処理を引き継ぎます。

HSRP グループ モデリング

CA Spectrum は、検出されたホット スタンバイ ルータ プロトコル（HSRP）グループごとにモデルを作成します。 CA Spectrum は仮想 IP アドレスによって、これらのモデルを識別します。 この仮想 IP アドレスが、HSRP グループのアクティブ ルータの [冗長除外アドレス] に追加されます。HSRP グループの各モデルは、HSRP グループ内のアクティブ ルータとスタンバイ ルータを認識します。

OneClick は、以下のルータ冗長性スポットライト メソッドを使用して、HSRP グループ メンバシップを表示します。

エクスプローラ検索

必要に応じて、アクティブ ラベルとスタンバイ ラベルを使って、HSRP グループ メンバを強調表示するビューを提供します。［エクスプローラ］タブ内のコンテナを選択し、コンテンツ パネルの［トポロジ］タブを選択し、スポットライト アイコンをクリックし、［ルータ冗長性］を選択できます。

ロケータ検索

HSRP グループ モデルの使用可能な検索を表示します。［ロケータ］タブ内の［ルータ冗長性］ディレクトリを開くことができます。各モデルに対して、コンテンツ画面には、HSRP グループ モデルに関する情報（仮想 IP、グループ ID、およびグループ メンバシップ）が表示されます。

HSRP グループ:メンバシップ

CA Spectrum は状態とメンバシップの変更がないか、各ホット スタンバイ ルータ プロトコル（HSRP）グループを監視します。CA Spectrum は、アクティブなルータ デバイス モデルのポーリング間隔を使用して、アクティブなルータの HSRP グループ テーブルをポーリングします。CA Spectrum は、デバイスが送信する状態変更トラップにも応答します。

ルータのフェールオーバが発生すると、HSRP グループ モデルでメジャー アラームがアサートされます。これは、スタンバイ ルータが使用できなくなり、ルータの冗長性が失われたことを意味します。新しいスタンバイ ルータが検出された場合、CA Spectrum はこのアラームをクリアします。

注: グループ モデル用の［情報］タブは、［レポート選択変更］設定を提供します。この設定を有効にすると、新しいアクティブ ルータが選択されるたびに、CA Spectrum はアラームを生成します。CA Spectrum はこのアラームをクリアしません。

HSRPMode 属性の状態の変更

ネットワーク パフォーマンスの低下を防ぐために、HSRP 展開で実行されているネットワーク デバイスに対する SNMP 要求ボリュームのボリュームの制限 HSRPMode 属性の状態を、以下の 3 つの状態のいずれかに設定できます。

オフ

HSRP テーブルはポーリングされません。

パッシブ

HSRP テーブルは、アクティブになった時点で 1 回ポーリングされます。そうでない場合、CA Spectrum はこの情報を更新するため、トラップからの更新に依存します。

アクティブ

HSRP テーブルはパッシブ処理に加えて、ポーリング間隔ごと、ポーリングされます。

次の手順に従ってください:

1. ［ロケータ］タブから［アプリケーション モデル］を展開します。
2. ［名前］を選択します。

   ［検索］ダイアログ ボックスが表示されます。
3. ［検索］ダイアログ ボックスで、［モデル タイプ］名前テキスト ボックスに「CiscoHSRPApp」と入力します。

   CiscoHSRPApp デバイスのすべてのリストが表示されます。
4. リスト内のすべてのデバイスを選択して右クリックし、［ユーティリティ］、［属性エディタ］と選択します。

   ［属性エディタ］ダイアログ ボックスが表示されます。
5. 左ペインで［ユーザ定義］を展開し、［ハイパーリンクの追加］をクリックします。

   ［属性セレクタ］ダイアログ ボックスが表示されます。

6. ［フィルタ］テキスト ボックスに「HSRPMode」と入力し、［OK］をクリックします。

   HSRPMode 属性が［ユーザ定義］に追加されます。

7. HSRPMode を選択し、右矢印をクリックして、右ペインに移動します。

   右ペインで HSRPMode 属性の状態を設定できるようになります。

8. 左ペインで［SNMP 通信］を展開して［*ポーリング間隔（秒）*］を選択し、右矢印をクリックして右ペインに移動します。

   これで右ペインで［ポーリング間隔］に値を設定できます。

9. 右ペインで［変更なし］をオフにして、［ポーリング間隔］の値を設定します。HSRPMode の状態をオフ、パッシブ、アクティブのいずれかに設定します。

HSRPMode の状態が変更され、ランドスケープ内のすべてのデバイス モデルでポーリング間隔の値が変更されました。

SNMPv3 デバイス ディスカバリ

VLAN を構成している Cisco スイッチ上で SNMPv3 デバイスを検出した場合、community_string@VLAN_ID フォーマットを使用して、各 VLAN のブリッジ情報にインデックスを付けることはできません。 コンテキストを代わりに作成します。

CA Spectrum がブリッジ情報を読み取るには、次のフォーマットを使って、これらのコンテキストを作成します。

```
vlan-<VLAN_ID>
```

例: SNMP v3 ユーザの作成

この例では CA Spectrum が読み取り可能なフォーマットを使って、SNMPv3 ユーザ コンテキストを作成します。

（有効化） `set snmp user <level1-vlan> nonvolatile`

（出力） `Snmp user was set to level1-vlan authProt no-auth  privProt no-priv`

例: SNMP グループの作成

この例では、CA Spectrum が読み取り可能なフォーマットを使って、SNMP グループ コンテキストを作成します。

（有効化） set snmp group <v3-level1-vlan> user <level1-vlan> security-model v3 nonvolatile

（出力） Snmp group was set to v3-level1-vlan user level1-vlan and version v3, nonvolatile.

例: SNMP アクセス グループの作成

この例では、CA Spectrum が読み取り可能なフォーマットを使って、SNMP アクセス グループ コンテキストを作成します。

（有効化） set snmp access <v3-level1-vlan> security-model v3 noauthentication read <defaultUserView> write <defaultUserView> notify <defaultUserView> nonvolatile

（出力） Snmp access group was set to v3-level1-vlan version v3 level noauthentication, readview defaultUserView, writeview defaultUserView, notifyview defaultUserView context match: exact, nonvolatile.

（有効化） set snmp access <v3-level1-vlan> security-model v3 noauthentication read <defaultUserView> write <defaultUserView> notify <defaultUserView> context <vlan> prefix nonvolatile

（出力） Snmp access group was set to v3-level1-vlan version v3 level noauthentication, readview defaultUserView, writeview defaultUserView, notifyview defaultUserView context: vlan, context match: prefix, nonvolatile.

Syslog トラップのサポート

システム メッセージ ログ（syslog）プロトコルでは、Cisco デバイスからネットワーク管理ソフトウェアへテキスト メッセージを送信できます。テキスト メッセージは、SNMP トラップとして CA Spectrum Event マネージャに送信されます。 Syslog トラップ サポートにより、ルータ デバイスはテキスト メッセージを識別し、必要に応じてアラートへのエスカレーションを実行することができます。Syslog トラップ サポートにより、Cisco Router モデルのアイコンで、アラーム重大度情報を通知することもできます。

Cisco デバイス アイコンによって示されたようなアラームが発生すると、CA Spectrum アラーム重大度と syslog メッセージがアラーム ログに表示されます。

syslog メッセージは、重大度に基づいて、0 ～ 7 の範囲に分類されます（最も重大が 0、最も軽微が 7）。アラームは、アラーム ログに表示されます。これらのアラームは Cisco デバイス モデルに関連付けられているため、対応するモデル アイコンがアラームの重大度に応じて、色と点滅を変更します。

以下の表に、重大度コードとその説明のリストを示します。

重大度	説明
0	緊急 -- システムが使用不可能
1	アラート -- 即時のアクションが必要
2	重大 -- 重大な状態
3	エラー -- エラー状態
4	警告 -- 警告の状況
5	通知 -- 正常だが、注意が必要な状態
6	情報 -- 情報メッセージのみ
7	デバッグ -- デバッグ中にのみ表示されるメッセージ

次の表は、syslog メッセージの重大度を CA Spectrum アラームの重大度にマッピングします。

アラーム重大度	色
0 または 1	レッド
2 ～ 3	オレンジ
4	イエロー

アラーム重大度が 5 ～ 7 のメッセージは、重要性が低いため、アラームを生成しません。機能（ハードウェア デバイス、プロトコル、またはモジュールかシステムソフト）は、メッセージをリスト表示します。

機能コードは、メッセージが参照する機能の略語です。 機能は、特定のハードウェア デバイスの場合もあれば、プロトコルやソフトウェアの場合もあります。 各機能内では、メッセージは重大度別に最高（0）から最低（7）にリスト表示されます。 *ニーモニック*は、メッセージを一意に識別する大文字の文字列です。

各メッセージの後に、説明および推奨されるアクションが表示されます。システムが運用可能な状態の場合に限り、メッセージが表示されます。次の行は、syslog メッセージの例です。

01/01/2001,18:31:15:SYS-5-MOD_INSERT:Module 5 has been inserted.

このメッセージは、以下のように解釈されます。

- 01/01/2001、18:31:15 が、エラーの発生日時（この情報は、システム ログ メッセージング用に設定されている場合のみ表示されます）
- SYS は機能タイプです。
- 5 は重大度レベルで、通常だが注意が必要な状態を意味します。
- MOD_INSERT は、メッセージを一意に識別するニーモニックです。
- 「Module 5 has been inserted （モジュール 5 が挿入されました）」は状況を説明するメッセージ テキストです。

システム メッセージ ログ（syslog）プログラムは、システム メッセージをログ ファイルに保存するか、メッセージを他のデバイスに転送します。Syslog ソフトウェアでは、以下の機能を実行できます。

- 監視とトラブルシューティングを目的としたログ情報の保存
- ログ情報のタイプおよび送信先の選択

デフォルトでは、スイッチは、正常だが注意が必要なシステムメッセージを内部バッファに記録し、そのメッセージをシステム コンソールに送信します。 機能の種類と重大度レベルに基づいて、システム メッセージの保存方法を指定できます。 リアルタイムでのデバッグと管理を向上させるため、メッセージにタイムスタンプを付けることができます。

CA Spectrum への Syslog トラップ マッピングの追加

CA Spectrum には、Cisco syslog トラップを CA Spectrum イベントにマッピングするために SpectroSERVER が使用する 3 つのテキスト ファイルが含まれます。

次の表は、syslog テキスト ファイルを示しています。

デバイス syslog メッセージ	テキスト ファイル
Cisco Router	<$SPECROOT>/SS/CsVendor/Cisco_Router/Rtr.txt
Catalyst Switch	<$SPECROOT>/SS/CsVendor/Ctron_CAT/Switch.txt
Cisco PIX	<$SPECROOT>/SS/CsVendor/CiscoPIX/Pix.txt

これらのテキスト ファイルの各行には、syslog メッセージを CA Spectrum イベントにマッピングするための情報が記載されます。 行には以下の形式があります（各フィールドで、1 文字のスペースが区切り文字です）。

<機能> <重大度> <ニーモニック> <イベント コード>

次の手順に従ってください:

1. 前の情報を含む行をファイルに追加します。

   たとえば、Cisco ルータ用の %SPE-3-SM_DOWNLOAD_FAILED syslog メッセージのサポートを追加するには、以下の行を Rtr.txt ファイルに追加します： SPE 3 SM_DOWNLOAD_FAILED 0xffff0001。 ここで 0xffff0001 は選択する任意のコードです。

2. イベントとアラームに対して、イベント形式ファイルと想定される原因ファイルを作成します。

   この場合、Eventffff0001 と Probffff0001 を作成します。 これらのファイルに、任意のテキストを入力できます。 以下の変数データはイベント メッセージから読み取って、イベント形式ファイルにひゅつりょくで来ます。

   {S 1} - 機能
   {T T1_210017 2} - 重大度
   {S 3} - ニーモニック
   {S 4} - メッセージ

3. イベントからアラームへのマッピングを追加します。 前の例を使用して、次の行を追加します。

   0xffff0001 E 50 A 2,0xffff0001

   注: Rtr.txt ファイルと同じディレクトリ内に EventDisp ファイルを保存する必要があります。

   SpectroSERVER がこの syslog トラップを受信すると、オレンジのアラームが生成されます。

注: SpectroSERVER の実行中、この設定を実行できます。 SpectroSERVER は 1 分ごとに、*.txt ファイルへの変更がないか確認します。

syslog メッセージ フィルタ

Cisco Syslog メッセージ フィルタ OneClick ビューでは、不要な syslog メッセージをフィルタできます。 syslog メッセージをフィルタすることで、不要なアラームやイベントがブロックされます。 SS/CsVendor/SYSLOG には、別のフィルタ カテゴリに対応する 8 つのファイルが含まれます。 ニーモニックが属するフィルタ カテゴリを選択するには、必要な SS/CsVendor/SYSLOG ファイルにニーモニックを移動します。

以下のテーブルは、SS/CsVendor/SYSLOG ファイルと対応するフィルタを示します。

ファイル	対応するフィルタ
Syslog0	Protocol_Filter
Syslog1	System_Filter
Syslog2	Environment_Filter

ファイル	対応するフィルタ
Syslog3	Software_Filter
Syslog4	Security_Filter
Syslog5	Hardware_Configuration_Filter
Syslog6	Connection_Configuration_Filter
Syslog7	PIX_Firewall_Filter

注: ニーモニックは、任意のフィルタと置き換え可能です。

以下のフィルタがあります。

Protocol_Filter

Syslog0 ファイルに影響します。 このフィルタを True に設定すると、プロトコルを処理するすべての syslog メッセージがフィルタされます。 BGP、OSPF、SNMP、SPANTREE などがその例です。

System_Filter

Syslog1 ファイルに影響します。 このフィルタを True に設定すると、システムを処理するすべての syslog メッセージがフィルタされます。 CBUS、MEMSCAN などがその例です。

Environment_Filter

Syslog2 ファイルの内容に影響します。 このフィルタを True に設定すると、環境変数を処理するすべての syslog メッセージがフィルタ除外されます。 LCFE、LCGE などがその例です。

Software_Filter

Syslog3 ファイルの内容に影響します。 このフィルタを True に設定すると、内部ソフトウェアを処理するすべての syslog メッセージがフィルタ除外されます。 PARSER、RSP、GRPGE などがその例です。

Security_Filter

Syslog4 ファイルの内容に影響します。 このフィルタを True に設定すると、システムのセキュリティを処理するすべての syslog メッセージがフィルタ除外されます。 RADIUS、SECURITY などがその例です。

Hardware_Configuration_Filter

Syslog5 ファイルの内容に影響します。 このフィルタを True に設定すると、デバイスのハードウェア コンフィギュレーションを処理するすべての syslog メッセージがフィルタ除外されます。IOCARD、MODEM、DIALSHELF などがその例です。

Connection_Configuration_Filter

Syslog6 ファイルの内容に影響します。 このフィルタを True に設定すると、デバイスの接続設定を処理するすべての syslog メッセージがフィルタ除外されます。 MROUTE、ISDN、X25 などがその例です。

Pix_Firewall_Filter

Syslog7 ファイルの内容に影響します。 このフィルタを True に設定すると、Cisco PIX Firewall デバイスを処理するすべての syslog メッセージがフィルタ除外されます。

トンネル インターフェース モデリング

CA Spectrum は、CISCO-IPSEC-FLOW-MONITOR-MIB および CISCO-IPSEC-MIB をサポートする Cisco デバイスに対して、IPSec トンネル インターフェース管理をサポートします。 これらの MIB は Cisco ファームウェア バージョン 12.1 (4) 以降で使用できます。

CA Spectrum は、以下の IPSEC VPN 管理機能をサポートします。

- トンネル インターフェースのモデリング（サイト間）
- 自動接続マッピング
- インターフェース モデル識別
- インターフェース モデル エージング
- リンク ダウン トラップ相関
- トンネル インターフェースのステータス監視

以下の属性が IPSEC VPN 管理を制御します。

- CreateTunnelLIf
- Interface_Polling_Interval

CreateTunneLIf の設定

CreateTunnelLIf 属性は、トンネル インターフェース モデルが、デバイスで定義される各 IPSec トンネル用に作成されたどうかを示します。 この属性が TRUE の場合、インターフェース再設定中に、CA Spectrum が外部テーブルを読み取ることを指定します。 これらの外部テーブルは、トンネル インターフェースが提供する値定義します。 CA Spectrum は、関連する物理インターフェースのサブインターフェースとして、適切なトンネル インターフェース モデルを作成します。

次の手順に従ってください:

1. ［ロケータ］タブに移動し、［アプリケーション モデル］フォルダを展開し、［デバイス IP アドレス］をダブルクリックします。

   ［検索］ダイアログ ボックスが表示されます。

2. 設定する Cisco IPSec-対応デバイスの IP アドレスを入力し、［OK］をクリックします。

   デバイスがコンテンツ画面に表示されます。

3. コンテンツ画面で CiscIPSecExtAp デバイスを選択します。
4. コンポーネント詳細画面で［属性］タブをクリックします。
5. 左ペインで CreateTunneLIf を選択し、右矢印ボタンをクリックして右ペインに移動します。
6. 右ペイン内の CreateTunneLIf をダブルクリックして、値を変更します。

   注: CreateTunneLIf を No に設定すると、Cisco IPSec トンネル モデリングが無効になります。

Interface_Polling_Interval の設定

Interface_Polling_Interval 属性は、トンネル テーブル ポーリング間隔を秒単位で定義します。この属性を 0 に設定すると、テーブルはポーリングされません。

次の手順に従ってください:

1. ［ロケータ］タブに移動し、［アプリケーション モデル］フォルダを展開し、［デバイス IP アドレス］をダブルクリックします。

   ［検索］ダイアログ ボックスが表示されます。

2. 設定する Cisco IPSec-対応デバイスの IP アドレスを入力し、［OK］をクリックします。

   デバイスがコンテンツ画面に表示されます。

3. コンテンツ画面でデバイスを選択します。
4. コンポーネント詳細画面で［属性］タブをクリックします。
5. 左ペインの Interface_Polling_Interval を選択し、右矢印ボタンをクリックして、右ペインに移動します。
6. 右ペイン内の Interface_Polling_Interval をダブルクリックして、値を変更します。

VLAN インデックスのサポート

CA Spectrum は、VLAN インデックス コミュニティ文字列が特定の Cisco デバイスでサポートされているかどうかテストできます。 VLAN インデックス コミュニティ文字列は、認証失敗トラップを防止します。

Cisco デバイスが VLAN インデックス コミュニティ文字列をサポートしている場合、VLANIndexingSupported （0x4a0037）属性値は Supported 1 に設定されます。

Cisco デバイスが VLAN インデックス コミュニティ文字列をサポートしない場合、VLANIndexingSupported （0x4a0037）属性値は、列挙 NotSupported 0 に設定されます。 さらに、VLAN インデックス読み取りは作成されません。 この設定により、認証失敗トラップが生成されるのを防ぎます。

デバイスの VLAN 情報が不足しているために Cisco デバイスがテストされなかった場合は、デバイスをテストします。 そのデバイスでディスカバリを実行するか、VLANIndexingSupported （0x4a0037）属性値を Test 2 に設定して、VLAN オーバレイを有効にします。

VLAN インデックス コミュニティ文字列がサポートするように、デバイスの設定が変更された場合は、属性エディタを使って、そのデバイスの Transparnt_App モデルに関する VLANIndexingSupported（0x4a0037）の属性値を変更します。

第 5 章: CiscoWorks 統合

このセクションには、以下のトピックが含まれています。

CiscoWorks の概要

CA Spectrum r9.2.1 を使用すると、CA Spectrum は、Cisco の CiscoWorks アプリケーションとシームレスに統合します。 CiscoWorks は、Cisco デバイスを管理するために強力なツールを提供します。

Cisco デバイスを選択して、CiscoWorks の［デバイス センター］ページで直接起動できるようになりました。

CiscoWorks 統合

［OneClick 管理］Web ページは、［CiscoWorks 設定］ページへのアクセスを提供します。 このページでは、CiscoWorks Web サーバ名およびポートを設定し、devman/config ディレクトリ内の ciscoworks-config.xml ファイルというファイルに、この情報を保存できます。 サーバ名が設定ファイルで設定される場合にのみ、メニュー ピックが作成されます。