CA Spectrum®

ホスト システム リソース管理ユーザ ガイド

リリース 9.3

CA Technologies 製品リファレンス

このガイドは、以下の製品に関するものです。

- CA Spectrum®
- CA Spectrum® Report Manager （Report Manager）
- CA SystemEDGE （SystemEDGE）

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

ホスト システム リソース マネージャについて

ホスト リソース監視は、一致または違反する場合にイベントおよびアラームを生成するホスト リソース状態およびしきい値を定義する CA Spectrum のメカニズムです。 リソース監視の目標は、ホストのパフォーマンスおよびサービス レベル アグリーメントに影響を及ぼす可能性のある重大なリソース イベントについてネットワーク管理者にアラートすることです。

リソースを監視できるようにするため、CA Spectrum は、以下のリソース監視エージェントの管理サポートを提供します。

- CA SystemEDGE エージェント
- CA Unicenter NSM システム エージェント
- Dell OpenManage
- 富士通 ServerView エージェント（PRIMERGY サーバ用）
- HP Systems Insight Manager
- iAgent
- IBM ディレクタ
- Net-SNMP （UC Davis）
- Sun Management Center

監視エージェントに対するこのサポートによって、ネットワーク内のホスト システムにあるリソースのステータスに関連する最新情報を表示および評価できます。

ホスト システム リソース管理コンセプト

以下の用語およびコンセプトは、CA Spectrum ホスト システム リソース管理を理解および動作させるための鍵です。

アラーム状態

アラーム状態は、RFC 2790 監視ルールで指定するプロセスしきい値のことです。

設定しきい値

設定しきい値は、NSM エージェント監視ルールで指定するプロセスしきい値のことです。

ファイル システム

ファイル システムは、ホスト上の任意のデータ ストレージ システムです。

ホスト

ホストはネットワーク内の他のシステムと通信する任意のコンピュータ システムです。 このガイドで、ホストは CA Spectrum でモデリングされた任意のデバイスのことで、RFC 2790 ホスト リソース MIB、NSM エージェント ベンダー固有 MIB またはログ ファイル監視をサポートします。

ホスト リソース

ホスト リソースは、監視できるプロセス、ファイル システム、プロセッサ、メモリおよび他のホスト エレメントです。

ログ ファイル

ログ ファイルは、ホストまたはホスト アプリケーションに関するステータス情報が含まれる任意のファイルです。

監視ルール

OneClick の監視ルールでは、リソース状態変更およびリソース アクティビティしきい値と CA Spectrum アラームを関連付けることができます。

プロセス

プロセスはホスト上で実行される任意のアプリケーションです。

監視タスクの概要

このガイドは、OneClick で以下のタスクを完了するための手順を提供します。

- プロセス監視ルールを作成および管理する
- ファイル システム監視ルールを作成および管理する
- CA Spectrum グローバル コレクション コンテナに適用し、監視ルールの作成を自動化するファイル システム監視ルール セットを作成する
- ログ ファイル監視を作成する

プロセスおよびファイル システム監視ルールの作成

ホスト モデルにプロセスまたはファイル システム監視ルールを作成するときに、CA Spectrum にアラームを生成させる条件を指定します。監視ルールを作成する場合、複数の利用可能な条件を指定できます。 また、CA Spectrum が監視ルール モデルまたはホスト モデルにアラームを生成するかどうかを指定できます。

詳細情報:

プロセス監視ルールの作成 (P. 17)
ファイル システム監視ルールの作成 (P. 45)

RFC 2790 ホスト リソース MIB 監視ルール アラーム状態およびしきい値

RFC 2790 ホスト リソース MIB をサポートするホストのプロセス監視ルールには、以下のアラーム状態が含まれます。

- プロセス開始
- プロセス停止
- プロセス インスタンス数が特定の数を超える
- プロセス インスタンス数が特定の数を下回る

ファイル システム監視ルールには、以下のアラーム状態が含まれます。

- ファイル システム使用率しきい値に到達
- ファイル システムがオフライン

RFC 2790 ホスト リソース監視ルールの詳細については、「RFC 2790 プロセス監視ルール パラメータの設定 (P. 21)」を参照してください。

NSM エージェント監視ルールしきい値

以下のテーブルでは、NSM エージェントのプロセス監視ルールを指定できる設定しきい値について説明します。 利用可能なしきい値は、ホスト タイプ（UNIX または Windows）およびホスト上にあるエージェントのバージョン（3.1 または r11）の両方に依存しています。

詳細については、「NSM エージェントのプロセス監視ルール パラメータ (P. 23)」を参照してください。

	プラットフォームおよび NSM エージェント バージョン			
設定しきい値	Win r11	UNIX r11	Win 3.1	UNIX 3.1
子	X	X	X	X
CPU 使用状況	X	X	X	X
CPU 使用状況 - 長期		X		
ハンドル	X			
インスタンス	X	X	X	X
再起動	X	X		
ランタイム	X			
サイズ	X	X	X	X
スレッド	X	X	X	

ルール セットを使用した監視ルール作成の自動化

ルール セットは監視ルールのコレクションです。 グローバル コレクション コンテナに 1 つ以上のルール セットを適用し、コンテナ内のモデルに対する監視ルールの作成を自動化できます。 RFC 2790 MIB または NSM エージェントをサポートするモデルがコレクションに追加される場合、監視ルールは自動的にモデルに設定されます。 ルールはルール セット内のルールを適用する任意のプロセスまたはファイル システムに対して設定されます。

たとえば、svchost.exe プロセスの監視ルールが含まれるルール セットは、グローバル コレクションに適用されます。 コレクションは、CA Spectrum でモデリングされるホストとして Windows ホストを追加するように設定されます。svchost.exe の監視ルールは、コレクションに追加されるすべてのホスト モデルで設定されます。 一方、ホストがコレクションから削除されると、監視ルールはホストから削除されます。

グローバル コレクションと関連付けられたルール セットのルールに加えた変更は、そのルールのすべてのインスタンスに適用されます。 このタイプのルールには、ルール セットに属する（または「所有」される）インジケータがあります。 ルール セットの所有権は、ルール セット名で確認できます。 名前が、OneClick のすべての監視対象プロセス テーブルおよび監視対象ファイル システム テーブルの［ルール所有者］フィールドに表示されます。

svchost.exe 監視に対してアラーム状態を変更すると仮定します。 svchost.exe ルールで、最大プロセス数のしきい値を 10 から 12 に変更します。 その後、変更はコレクション内のすべての svchost.exe 監視ルール インスタンスに適用されます。

詳細については、「ルール セットの作成 (P. 51)」を参照してください。

ログ ファイル監視の作成について

ログ ファイル監視をサポートするエージェントは、正規表現を使用してログ ファイル テキストを検索します。 通常、システムまたはアプリケーションのエラー状態に関する情報を見つけるために、ログ ファイルを監視します。テキスト一致検出は、CA Spectrum にログ ファイル エントリが起こったデバイス上にアラームを生成させます。

詳細については、「ログ ファイルの監視 (P. 59)」を参照してください。

ホスト リソース監視およびサービス レベル アグリーメント

ホスト リソース監視では、サービス レベル アグリーメント（SLA）で定義されているネットワーク サービスに影響を及ぼす可能性のあるホスト リソースを監視します。 たとえば、プロセス監視ルールは、ウイルス保護プロセスが予期せず停止したかどうか、悪意のあるプロセスがホストで開始されたかどうかを判断できます。 ファイル システム監視ルールは、ホスト上のディスク ドライブまたは物理 RAM がストレージ容量に達したか、または近づいているかどうかを判断できます。 ビジネス サービスの実行可能性は、プロセスがホスト上で実行されているかどうか、ホストが適切なデータ ストレージ容量を提供しているかどうかに依存することがあります。

注: サービス管理システムおよび SLA の設定に関する詳細については、「Service Manager ユーザ ガイド」を参照してください。

ホスト リソースのイベントおよびアラームのレポーティング

CA Spectrum Report Manager アプリケーションでは、ホスト モデルのイベントおよびアラームについてレポートを生成できます。 アラームおよびレポートは、監視対象プロセスおよびファイル システムのしきい値違反に対して生成されます。 また、アラームはログ ファイルから解析されるエラー メッセージからも生成されます。

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

OneClick でのホスト システム リソースの管理

このセクションでは、監視ルール、ルール セットおよび監視対象ホスト リソース情報のビューを設定する作業領域を起動する方法について説明します。

注: OneClick コンソール インターフェース エレメントの詳細については、「オペレータ ガイド」を参照してください。

監視ルールの作成および管理用作業領域へのアクセス

監視エージェントをサポートするホスト モデルのコンテキストから監視ルールを作成および管理します。

次の手順に従ってください:

1. コンテンツ画面から監視ルールを作成するホストを選択します。
2. コンポーネント詳細画面の［情報］タブでシステム リソース オプションを展開します。

   実行中/監視対象プロセス セクションでは、プロセス監視ルールを作成および管理できます。 詳細については、「プロセスの監視 (P. 17)」を参照してください。

   監視対象ログおよびプロセス ログ セクションでは、ログ ファイル監視ルールを作成できます。詳細については、「ログ ファイルの監視 (P. 59)」を参照してください。

   ファイル システム セクションでは、ファイル システム監視ルールを作成できます。 詳細については、「ファイル システムの監視 (P. 45)」を参照してください。

ルール セットの作成および管理用作業領域へのアクセス

特定のホスト用に作成する監視ルールとは異なり、CA Spectrum はグローバル コレクションに別のルールを作成します。 ルール セットが適用されたグローバル コレクションに含まれている任意のホストについては、CA Spectrum はルール セットで指定するルールを作成します。 この機能は、複数の別のホスト タイプに使用する監視ルールの作成プロセスを自動化します。

コンテンツ画面のルール セットを管理します。

次の手順に従ってください:

- ［ロケータ］-［システムとアプリケーションの監視］-［すべての監視ルール］を選択します。

コンテンツ画面は、作成されたすべてのルール セットのリストを示します。

デフォルト ルールは設定されていません。 ルール セットを作成および管理し、グローバル コレクションにそれらを適用する詳細については、「監視ルール セットの使用 (P. 51)」を参照してください。

監視ルール情報の表示

OneClick では、コンポーネント詳細画面の監視対象プロセスおよびファイル システムに関する包括的な情報を表示できます。

プロセス監視ルールに関する情報を表示する方法

- ［ロケータ］-［システムとアプリケーションの監視］-［すべての監視対象プロセス］を選択します。

  注: プロセス モデルは SystemEDGE ホストのルールに対して作成されないため、SystemEDGE ホストに使用されるルールはこのビューに表示されません。

ファイル システム監視ルールに関する情報を表示する方法

- ［ロケータ］-［システムとアプリケーションの監視］-［すべての監視対象ファイル システム］を選択します。

このビューは、選択されたホストおよびホスト上の監視設定に関する情報を提供します。 ルールと関連付けられた監視エージェントは、ビューが提供する情報を決定します。

第 2 章: プロセスの監視

プロセス監視ルールは、満たされた場合に CA Spectrum にアラームを生成させる条件を指定します。 このセクションでは、プロセス監視エージェントを含むホスト モデルに対してプロセス監視ルールを設定する方法について説明します。 グローバル コレクション コンテナに含まれるモデルにプロセス監視ルールを自動的に作成する方式を設定する詳細については、「監視ルール セットの使用 (P. 51)」を参照してください。

このセクションには、以下のトピックが含まれています。

プロセス監視ルールの作成

プロセスがホスト上で実行されているかどうかにかかわらず、ホスト モデルにプロセス監視ルールを作成できます。

注: 適切な権限のあるユーザのみが、プロセス監視ルールを作成できます。詳細については、「システムとアプリケーションの監視権限 (P. 101)」を参照してください。

次の手順に従ってください:

1. コンテンツ画面で、監視ルールを作成するホスト モデルを選択します。

   このホスト デバイスの情報が、コンポーネント詳細画面に表示されます。

2. コンポーネント詳細画面の［情報］タブで、［システム リソース］-［実行中］-［監視対象プロセス］を展開します。

   このホスト タイプに利用可能なプロセス オプションが表示されます。

   注: RFC 2790 は、RFC 2790 ホスト リソース MIB をサポートするホストを示します。

3. ［実行中のプロセス］および［監視対象プロセス］の両方を展開します。

   実行中のプロセス テーブルでは、選択したホスト モデルで実行中のプロセスのリストを示します。

   監視対象プロセス テーブルは、選択したホストで作成されたプロセス監視ルールのリストを示します。

4. 選択したホスト モデルにプロセス監視ルールを作成するには、以下の*いずれか*の方式を使用します。

   - プロセスが実行中の場合、実行中のプロセス テーブルのプロセスを右クリックし、［このプロセスを監視］を選択します。
   - プロセスが実行中の場合は、実行中のプロセス テーブルに含まれていません。 監視対象プロセス テーブルの上の［追加］をクリックします。次に、定期的に実行されるが現在は実行されておらず、開始時に認識する必要のあるプロセスにプロセス監視ルールを指定できます。 たとえば、ウイルス スキャンおよびシステムの保守プロセスがいつ実行されるかを認識します。

     注: NSM エージェントの監視については、一致条件が指定された複数の別プロセスをウォッチする監視ルールを作成する場合に、この方式を使用します。 詳細については、「NSM エージェントのプロセス監視ルール パラメータ (P. 23)」を参照してください。

   ダイアログ ボックスがホスト タイプに応じて開きます。 実行中のプロセス テーブルからプロセスを選択した場合、ダイアログ ボックスにはプロセス名および他の情報が含まれます。 ［追加］オプションを使用して、ダイアログ ボックスを起動した場合、すべてのプロセス情報を提供するように指示されます。

5. プロセス監視ルール設定を設定します。

   - RFC 2790 ホスト リソース MIB をサポートするエージェントについては、「RFC 2790 プロセス監視ルール パラメータ (P. 21)」を参照してください。

- NSM エージェント バージョン 3.1 および r11 をサポートするエージェントについては、「NSM エージェント プロセス監視ルール パラメータ (P. 23)」を参照してください。
- SystemEDGE ホスト エージェントについては、「SystemEDGE ホスト プロセス監視ルール パラメータ (P. 35)」を参照してください。

6. ［OK］をクリックします。

   以下のイベントが発生します。

   - プロセス監視ルールは、監視対象プロセス テーブルに追加されます。 テーブルの列は、選択したホスト上の監視エージェント タイプに固有の事前定義済みのプロセス ID 情報を表します。 ルールは、プロセス一致選択条件を満たしているプロセスのすべての同一インスタンスに適用されます。
   - プロセス モデルは RFC 2790 および NSM エージェントのルールに対して作成されます。

   注: 監視ルールのローカル所有権は、ルールが特定のホスト用に明示的に作成されており、そのためルール セットの一部ではないことを示します。 ルール セットの詳細については、「監視ルール セットの使用 (P. 51)」を参照してください。

7. 監視対象プロセス テーブルの上にあるアラーム生成およびエージェント ポーリング オプションを、ホスト タイプに応じて指定します。

   新規プロセス監視間隔（秒）

   監視ルールがウォッチしているプロセスの新規インスタンスに対して、CA Spectrum が実行中のプロセス テーブルを検査する頻度を指定します。 プロセスの新規インスタンスが実行されていることを検出した場合、CA Spectrum は監視対象プロセス用の監視対象プロセス テーブルで［実行中の数］値を更新します。

   アラーム生成対象

   ルール違反から生じるアラームの宛先を選択します。 CA Spectrum がアラームをプロセス監視ルール モデルまたはホスト モデル上に作成することを指定できます。

   注: プロセス モデルは SystemEDGE ホスト上のルールに対して作成されないため、アラームは常に SystemEDGE ホストのホスト モデル上にあります。

エージェント ポーリング間隔（秒）

エージェントがホスト デバイスからプロセス情報を収集する頻度を指定します。 最小値は 30 秒です。

エージェント ポーリング方法

エージェントがプロセス データを収集する方法とタイミングを指定します。

無効

エージェントは（ポーリングまたは GET 要求によって）プロセス情報を取得しません。また、アラーム状態のすべてのステータス表示にパッシブまたは OK を設定します。

ポーリング間隔およびクエリ

エージェントは、ポーリングおよび GET 要求の両方によってプロセス情報を取得します。

ポーリング間隔のみ

エージェントは、ポーリングのみによってプロセス情報を取得します。

クエリのみ

エージェントは、GET 要求のみによってプロセス情報を取得します。

プロセスの区別

ホストは、常に特定プロセスで複数のインスタンスを実行できます。Windows ホスト上の svchost.exe プロセスおよび Linux および UNIX ホスト上の nfsd プロセスは、典型的な例です。すべてのプロセス インスタンス、複数のプロセス インスタンス、または単一のプロセス インスタンスに適用されるプロセス監視ルールを作成できます。たとえば、svchost.exe のインスタンスをすべて監視すると決定した場合、パラメータまたは名前でインスタンスを区別しません。

CA Spectrum については、svchost.exe プロセス監視ルールで指定されるアラーム状態およびしきい値は、プロセスのすべてのインスタンスに適用されます。 ルールがプロセス開始および停止のアラームを指定する場合には、CA Spectrum は各インスタンスの開始および停止ごとにアラームを生成します。 つまり、CA Spectrum は監視対象プロセス テーブルのエントリ（プロセス名による）に一致する実行中のプロセス テーブルの各エントリにルールを適用します。

インスタンスまたはプロセスの同一インスタンスのグループに対してルールを作成できます。 この場合、インスタンスまたはインスタンスのグループを、監視しないインスタンスと区別する必要があります。 区別するために一意の名前、パラメータまたはその両方を使用できます。 区別オプションでは、プロセス インスタンスを区別する多くのタイプを作成できます。

プロセス監視ルール パラメータ

このセクションでは、以下のホスト タイプに使用するプロセス監視ルール パラメータについて説明します。

- RFC 2790（P. 21）
- NSM エージェント（P. 23）
- SystemEDGE ホスト（P. 35）

RFC 2790 プロセス監視ルール パラメータ

RFC 2790 の監視をサポートするホストにプロセス監視ルールを作成する場合、以下のパラメータを指定できます。

- プロセス ID、プロセス名とプロセスの区別化要因を含む
- プロセス開始/停止およびプロセス数のアラーム状態
- 監視ルールに関連付けされたプロセスの新規インスタンスに使用する実行中のプロセス テーブルのポーリング

監視情報

プロセスのすべてのインスタンスまたはプロセスの特定のインスタンスを選択して監視できます。 監視ルールで以下のパラメータを使用します。

プロセス名

ホスト モデル上のプロセスを示します。 この設定でプロセス インスタンスを区別したり、［一致パラメータ］フィールドを使用してより正確に区別することもできます。

RFC 2790 の監視をサポートするホストについては、このフィールドに入力される値を大文字と小文字で区別しません。 監視対象プロセス（RFC 2790）テーブルに表示されるときは、値は小文字に変換されます。 また、重複したエントリは許可されません。 新しいエントリが同じプロセスの名前（および指定されれば一致パラメータの値）で作成される場合、新しいエントリは既存のエントリを置換します。 変更されたすべての設定が更新されます。

一致パラメータ

同じプロセスで同一に命名されたインスタンスを区別する 1 つ以上のプロセス パラメータを指定します。パラメータを追加するか、または設定を保存する前にプロセスに含まれるパラメータを変更することができます。 この設定はプロセスの名前と共に使用され、プロセス インスタンスを区別します。 詳細については、「プロセスの区別 (P. 20)」を参照してください。

説明

プロセスのニックネームを示します。 固有名詞（たとえば、javaw.exe プロセス用に「java runtime」）よりも、プロセスの目的または機能を明確に伝える記述的な名前を提供することをお勧めします。 この設定はプロセスを区別する要因として使用されません。

アラーム設定

RFC 2790 監視ルールで以下のアラーム状態を指定できます。

プロセス数の最小値

プロセス インスタンス数が特定の値未満であるときに、CA Spectrum がアラームを生成するかどうかを指定します。 プロセス数が値以上である場合、CA Spectrum はアラームをクリアします。

プロセス数の最大値

プロセス インスタンス数が特定の値より大きいときに、CA Spectrum がアラームを生成するかどうかを指定します。プロセス数が値以下である場合、CA Spectrum はアラームをクリアします。

プロセス開始

プロセスが開始されるときに毎回、CA Spectrum がアラームを生成するかどうかを指定します。 プロセスが停止する場合、CA Spectrum はプロセス開始アラームをクリアします。

プロセス停止

プロセスが停止されるときに毎回、CA Spectrum がアラームを生成するかどうかを指定します。 プロセスが開始する場合、CA Spectrum はプロセス停止アラームをクリアします。

NSM エージェント プロセス監視ルール パラメータ

「プロセス監視ルールの作成 (P. 17)」に述べたように、プロセス監視ルールは［監視対象プロセスの追加］ダイアログ ボックスで定義されます。NSM エージェントの監視をサポートするホストにプロセス監視ルールを作成する場合、以下のパラメータを指定できます。

- プロセス監視ルール ID
- プロセス一致条件
- 設定しきい値監視オプション
- 設定しきい値
- 集約ステータス評価ポリシー、リソース クラスタ グループおよび集約違反しきい値などの詳細オプション

注: NSM エージェント バージョンおよびエージェント ホスト プラットフォームが、これらすべての設定およびこのセクションに示されているオプションへのアクセスを決定します。

すべてのプラットフォーム上にあるすべての NSM エージェント バージョンに、エージェント ポーリング間隔およびメソッドを指定できます。 詳細については、「プロセス監視ルールの作成 (P. 17)」を参照してください。

監視情報

［監視対象プロセスの追加］ダイアログ ボックスには、以下のプロセス監視ルール ID が含まれます。 利用可能な ID は、NSM エージェント バージョンおよびエージェント ホスト プラットフォームに依存しています。

監視名

監視ルール名を示します。 CA Spectrum は監視名によって同一の監視ルール設定を区別します。 この名前は一意である必要があります。

説明

監視ルール ニックネームまたは短い記述用語を示します。

以下のテーブルでは、各エージェント タイプのプロセス監視を一意に識別する属性（すなわちフィールド）について説明します。

バージョン	監視識別フィールド
Win r11	監視名 * 説明（オプション）
UNIX r11	監視名 * 説明（オプション）
Win 3.1	説明（オプション） プロセス名 * パス * ユーザ *
UNIX 3.1	プロセス名 * パラメータ * パス * ユーザ *

* プロセス監視を一意に示します。

プロセス一致条件

NSM エージェントのプロセス監視ルールを実装する前に、CA Spectrum がしきい値条件に従って評価するプロセスを識別します。 プロセスを識別するために正規表現および文字列比較を使用できます。

重要: r11 エージェントは一致条件で正規表現をサポートしますが、3.1 エージェントはワイルドカード（*）の使用のみをサポートします。

以下のテーブルでは、各タイプの NSM エージェントの条件に一致するプロセスとして使用される属性（すなわちフィールド）について説明します。

注: r11 NSM エージェントについては、一致タイプはその他すべての一致条件属性の組み合わせに適用されます。 これは他のプロセス一致フィールドの組み合わせが評価される方法を定義します。

バージョン	監視識別フィールド
Win r11	プロセス名 一致タイプ パス ユーザ
UNIX r11	プロセス名 一致タイプ パラメータ パス ユーザ
Win 3.1	プロセス名 パス ユーザ
UNIX 3.1	プロセス名 パラメータ パス ユーザ

［監視対象プロセスの追加］ダイアログ ボックスには、動作中の NSM エージェント バージョンおよびエージェント ホスト プラットフォームに応じて、以下のフィールドおよびオプションが含まれます。

プロセス名

一致させるプロセス（複数可）のテキスト パターンを示します。 リテラル文字列 ID または正規表現を使用し、テキスト検索パターンを指定できます。

注: 他のプロセス一致条件が指定されない場合、［プロセス名］フィールドの名前に一致するすべてのプロセスが監視されます。

一致タイプ

プロセス一致条件に一致する、または一致しないプロセス（複数可）を指定できます。

注: プロセス名の一致条件は、大文字と小文字を区別しません。

オプションは以下のとおりです。

正の正規表現

エージェントは、正規表現としてプロセスの名前に一致するプロセスを検索します。

負の正規表現

エージェントは、正規表現としてプロセスの名前に一致しないプロセスを検索します。

正の文字列比較

エージェントは、文字列比較としてプロセス名に一致するプロセスを検索します。

負の文字列比較

エージェントは、文字列比較としてプロセス名に一致しないプロセスを検索します。

パラメータ

一致させるプロセス引数を示します。NSM のバージョンおよび使用しているプラットフォームに応じて、リテラル文字列または正規表現としてパラメータを指定できます。

パス

一致させるプロセス（複数可）のパス名を示します。 リテラル文字列または正規表現としてパスを指定できます。

ユーザ

一致させるプロセス アカウントのユーザ名を示します。 NSM のバージョンおよび使用しているプラットフォームに応じて、リテラル文字列または正規表現としてユーザ名を指定できます。

NSM エージェントのしきい値設定

しきい値設定は、監視でウォッチされる対象を定義します。 監視ルールを作成するときに、複数のしきい値を指定できます。 たとえば、プロセスが消費する CPU 時間のみをウォッチするように監視を指定できます。 または、CPU 使用状況およびプロセスの子、スレッドおよびハンドル、さらにプロセスが再起動される頻度をウォッチするように監視を指定できます。

CA Spectrum は、警告しきい値の違反にメジャー（オレンジ）アラーム、重大しきい値の違反に重大（赤）アラームを生成します。 アラームの生成は、監視ルールの全体的なステータスに依存します。

指定できるしきい値は、ホスト プラットフォーム（Windows または UNIX）、およびホスト上で実行中の NSM エージェント バージョン（3.1 または r11）に依存しています。

以下のテーブルでは、各 NSM エージェントに利用可能なしきい値および監視オプションについて説明します。

しきい値	監視オプション プラットフォームおよびエージェント バージョン			
	Win r11	UNIX r11	Win 3.1	UNIX 3.1
子	監視せず ダウン - 警告 ダウン - 重大	監視せず ダウン - 警告 ダウン - 重大	監視せず ダウン - 警告 ダウン - 重大	監視せず 監視
CPU 使用状況	監視せず 警告のみ 重大のみ 最小値のみ 最大値のみ すべて	監視せず 警告のみ 重大のみ 最小値のみ 最大値のみ すべて	監視せず 警告のみ 重大のみ 両方	監視せず 警告のみ 重大のみ 両方
CPU 使用状況 - 長期	N/A	監視せず 警告のみ 重大のみ 最小値のみ 最大値のみ すべて	N/A	N/A

しきい値	監視オプション プラットフォームおよびエージェント バージョン			
	Win r11	UNIX r11	Win 3.1	UNIX 3.1
ハンドル	監視せず ダウン - 警告 ダウン - 重大	N/A	N/A	N/A
インスタンス	監視せず ダウン - 警告 ダウン - 重大	監視せず ダウン - 警告 ダウン - 重大	監視せず ダウン - 警告 ダウン - 重大	監視せず 監視
再起動	監視せず ダウン - 警告 ダウン - 重大	監視せず ダウン - 警告 ダウン - 重大	N/A	N/A
ランタイム	監視せず ダウン - 警告 ダウン - 重大	N/A	N/A	N/A
サイズ	監視せず 警告のみ 重大のみ 最小値のみ 最大値のみ すべて	監視せず ダウン - 警告 ダウン - 重大	監視せず 警告のみ 重大のみ 両方	監視せず 監視
スレッド	監視せず ダウン - 警告 ダウン - 重大	監視せず ダウン - 警告 ダウン - 重大	監視せず ダウン - 警告 ダウン - 重大	N/A

注: しきい値を無効にするには、特定の最小または最大値しきい値に値「-1」を指定します。 たとえば、最大しきい値ではなく最小しきい値、またはその逆に監視ウォッチを選択して指定できます。

子

監視がプロセスの子の数をウォッチするかどうかを指定します。

注: Windows のバージョン r11 については、このオプションは［リソース］-［タイプ］のドロップダウン リストにあります。

CPU 使用状況 /CPU 短期 - 使用状況 /CPU 長期 - 使用状況

監視がプロセスが使用する CPU 時間をウォッチするかどうかを指定します。

以下に使用可能なオプションの一部を示します。

警告しきい値

この値は「1」から「99」パーセントの間にすることができますが、重大しきい値のパーセントを下回る必要があります。 複数のプロセス インスタンスについては、すべてのインスタンスの最大値がこの値と比較されます。

重大しきい値

この値は「2」から「100」パーセントの間にすることができますが、警告しきい値のパーセントを超える必要があります。 複数のプロセス インスタンスについては、すべてのインスタンスの最大値がこの値と比較されます。

CPU 間隔

この値は、CPU 値を計算するための基準として使用される秒単位の合計値を定義します。 特にプロセスの CPU 使用状況（秒数）は、この間隔を参照します。 値を「0」以上の任意の値または「-1」に設定できます。

- 「-1」に設定すると、CPU 値はエージェントの開始またはプロセス監視ルールの作成から現在の時間までに使用した CPU 使用状況（秒数）として計算されます。
- CPU 間隔が現在のエージェント ポーリング間隔より大きな値に設定され、その最初の時間を経過していない場合、CPU 値は推定された値になります。
- CPU 間隔が現在のエージェント ポーリング間隔より小さな値に設定された場合、CPU 値は最後のエージェント ポーリング間隔の値の適切な割合として計算されます。
- CPU 間隔が現在のエージェント ポーリング間隔より大きな値に設定され、その時間がすでに経過している場合、CPU 値は合計を調整して（現在のポーリング間隔の値と前回のポーリング時の値の合計）計算され、この CPU 間隔の割合に基づいて重み付けされます。
- 間隔が「-1」に設定された場合、しきい値に使用される過負荷率（%）は無視されます。

最小/最大ユニット数

測定単位（秒数またはパーセント）。CPU 使用状況しきい値に使用されます。

インスタンス

監視がプロセス インスタンス数をウォッチするかどうかを指定します。

リソース

監視が以下のいずれかのリソース タイプをウォッチするかどうかを指定します。

スレッド

プロセス スレッド カウントを指定します。

ハンドル

プロセスでの各スレッドによって現在開かれているハンドルの合計数を指定します。

子

プロセスの子の数を指定します。

ランタイム

プロセスが作成されてから実行される時間（秒数）を指定します。

再起動

監視がプロセス再起動数をウォッチするかどうかを指定します。しきい値違反の再起動アラーム状態のステータスをダウンに設定するタイミングを判断するためにエージェントが使用するポリシーを決定します。

いずれかが停止または開始

プロセスが停止または開始した場合、ステータスがダウンに設定されます。

いずれかが停止

プロセスが停止した場合、ステータスがダウンに設定されます。

いずれかが開始

プロセスが開始した場合、ステータスがダウンに設定されます。

すべて停止

すべてのプロセスが停止した場合、ステータスがダウンに設定されます。

サイズ

監視がプロセスが消費するメモリ量（キロバイト単位）をウォッチするかどうかを指定します。

スレッド

監視がプロセス スレッド カウントをウォッチするかどうかを指定します。

注: Windows のバージョン r11 については、このオプションは［リソース］-［タイプ］のドロップダウン リストにあります。

監視オプション

監視オプションは、NSM エージェントが特定の設定しきい値をウォッチするかどうか、およびウォッチするしきい値タイプ（警告または重大、最小値または最大値）を指定します。

［監視対象プロセスの追加］ダイアログ ボックスの監視ドロップダウン リストには、ホスト プラットフォーム（Windows または UNIX）、NSM エージェントのバージョン（3.1 または r11）、および設定している特定のアラーム状態に応じて以下のオプションが含まれます。

監視せず

アラームなし。 エージェントはしきい値設定を無視します。

監視

重大アラーム。 エージェントは、すべてのしきい値の最小および最大値を監視します。

警告のみ

メジャー アラーム。 エージェントは、警告しきい値（最小と最大の両方）のみを評価し、プロセスのステータスを決定します。

重大のみ

重大アラーム。 エージェントは、重大しきい値（最小と最大の両方）のみを評価し、プロセスのステータスを決定します。

最小値のみ

メジャー（警告）および重大（重大）アラーム。 エージェントは、最小しきい値（警告および重大の両方）のみを評価し、プロセスのステータスを決定します。

最大値のみ

メジャー（警告）および重大（重大）アラーム。 エージェントは、最大しきい値（警告および重大の両方）のみを評価し、プロセスのステータスを決定します。

すべて

メジャー（警告）および重大（重大）アラーム。 エージェントはすべてのしきい値を評価します。

ダウン - 警告

メジャー アラーム。 リソースが悪い状態にある場合、エージェントは重大度として「警告」を使用します。 これで［ダウン-重大］違反よりも重大ではないとしてしきい値違反を指定できます。

ダウン - 重大

重大アラーム。 リソースが悪い状態にある場合、エージェントは重大度として「重大」を使用します。 これで［ダウン-重大］違反よりも重大であるとしてしきい値違反を指定できます。

両方

メジャー（警告）および重大（重大）アラーム。 エージェントは、警告および重大しきい値の両方を評価し、プロセスのステータスを決定します。

詳細オプション

詳細オプションでは、監視が 2 つ以上のプロセス、プロセス リソース クラスタ グループ、および集約アラーム状態の違反しきい値をウォッチする場合、設定しきい値違反に評価ポリシーを指定できます。このしきい値が満たされた場合、プロセスのステータスを低下させ、CA Spectrum アラーム生成をトリガします。

注: 利用可能な詳細オプションは、設定しているホスト プラットフォーム（Windows または UNIX）および NSM エージェントのバージョン（3.1 または r11）に依存しています。

評価ポリシー（r11 のみ）

エージェントが複数の別プロセスをウォッチする監視用アラーム状態しきい値と比較する値をエージェントが計算する方法を指定します。また、これはしきい値違反原因リストに含まれる他のプロセスを指定します。

注: NSM エージェントのバージョン 3.1 は、ウォッチされるすべてのプロセス インスタンスの悪い値（個別ポリシー）がしきい値に準拠しているか判断するために、アラーム状態しきい値と比較します。

評価ポリシー オプションは以下のとおりです。

個別（デフォルト）

エージェントがすべてのプロセス インスタンスの悪い値（最小値/最大値）をアラーム状態しきい値と比較することを指定します。値がしきい値条件に違反する場合、原因リストには最も重大なしきい値に違反しているすべてのインスタンスが個別に含まれます。

最小

エージェントがすべてのプロセス インスタンスの悪い値（最小値）をアラーム状態しきい値と比較することを指定します。 値がしきい値条件に違反する場合、原因リストには同じ最小値を含むすべてのインスタンスが含まれます。

最大

エージェントがすべてのプロセス インスタンスの最も高い値（最大値）をアラーム状態しきい値と比較することを指定します。 値がしきい値条件に違反する場合、原因リストには同じ最大値を含むすべてのインスタンスが含まれます。

合計

エージェントがすべてのプロセス インスタンスの累積値（合計）をアラーム状態しきい値と比較することを指定します。 値がしきい値条件に違反する場合、原因リストにはすべてのインスタンスが含まれます。

平均

エージェントがすべてのプロセス インスタンスの平均値をアラーム状態しきい値と比較することを指定します。 値がしきい値条件に違反する場合、原因リストには最も重大なしきい値に違反しているすべてのインスタンスが個別に含まれます。

クラスタ リソース グループ（r11 のみ）

クラスタ リソース グループを示します。

集約違反しきい値

このオプションは、しきい値が OK 以外の状態である必要のあるエージェントのポーリング サイクルが何回続いたら、監視の集約ステータスが変更されるかを指定します。 この値は 0 より大きい必要があります。 ［集約違反しきい値］フィールドは UNIX 3.1 に利用可能ではありません。

選択したホスト モデルの監視対象プロセス テーブルの［ステータス］フィールドは、集約ステータス状態を示します。

NSM エージェントがプロセス情報を取得しない場合

プロセス監視情報を取得するための NSM エージェント サブエージェントがダウンになった場合、CA Spectrum は以下のように応答します。

- ホスト モデル上に「NSM プロセス監視エージェントが切断されました」アラームを生成する
- プロセス モデル上に抑制された APPLICATION_LOST アラーム状態をアサートする

プロセス監視サブエージェントを再起動する場合、CA Spectrum はホスト モデル上の「NSM プロセス監視エージェントが切断されました」アラームをクリアし、関連するプロセス モデル上の APPLICATION_LOST アラームをクリアします。

NSM エージェント プロセス監視ルールのステータス表示

選択したホスト モデル用の監視対象プロセス テーブルの［ステータス］フィールドは、監視の集約ステータス状態を示します。ステータス フィールドは、監視で定義される各しきい値のステータス値で最も悪い集約を表します。

しきい値が特定の連続エージェント ポーリング サイクル数を超える違反ステータスにある場合、集約ステータスは次善の状態を入力します。［集約違反しきい値］フィールドは、しきい値の違反状態が何回続いたら、集約ステータスが変更されるかを定義します。 CA Spectrum は、集約ステータスが次善の状態になるまで、違反されたしきい値のアラームを生成しません。

SystemEDGE ホスト プロセス監視ルール パラメータ

プロセス監視ルールは、［プロセス監視テーブル エントリの追加］ダイアログ ボックスで定義されます。 詳細については、「プロセス監視ルールの作成 (P. 17)」を参照してください。

SystemEDGE ホストにプロセス監視ルールを作成する場合、以下のパラメータを指定できます。

- プロセス監視ルール ID
- 設定しきい値監視オプション
- 設定しきい値
- 詳細オプション。トラップの送信および親プロセスまたは Windows サービスの監視など

注: ルールが SystemEDGE ホスト用に作成される場合、プロセス モデルは作成されません。 その結果、［ロケータ］タブのルールを検索および表示するときに、監視ルールは表示されません。

監視情報

［プロセス監視テーブル エントリの追加］ダイアログ ボックスには、以下のプロセス監視ルール ID が含まれます。

インデックス

プロセス監視エントリを一意に識別する整数値を指定します。エントリを作成するときにこのフィールドを空にするか「0」に設定した場合、未使用インデックスが自動的に選択されます。

プロセス名

一致するプロセス テキスト パターンを示します。 リテラル文字列 ID または正規表現を使用し、テキスト検索パターンを指定できます。

一致パラメータ

プロセスの名前とパラメータの両方に一致させるか、またはプロセスの名前のみに一致させるかを示します。

説明

監視ルール ニックネームまたは短い記述用語を示します。

しきい値設定

しきい値設定は、監視がウォッチする属性およびメトリックを定義します。監視ルールを作成する場合、SystemEDGE ホスト バージョンに応じて適切なしきい値を指定できます。

以下のパラメータを使用できます。

属性

監視するプロセス属性です。

演算子

現在の値としきい値を比較するために使用されるブール演算子です。［操作なし］は現在の値のみを追跡し、しきい値との比較は行いません。

しきい値

エージェントが現在の値と比較するしきい値です。 このパラメータは［演算子］パラメータで動作します。

間隔

エージェントによる連続するサンプリングの間隔（秒数）です。 値は 30 から MAXINT の間で、30 の倍数である必要があります。

サンプル タイプ

監視対象オブジェクトで実行されるサンプリング タイプです。

絶対

実際の値を測定します（例： ゲージ）。

デルタ

値の変化を測定します（例： カウンタ）。

重大度

オブジェクト状態モデルに使用する重大度です。

注: このしきい値はすべての SystemEDGE ホスト バージョンに利用可能ではありません。

オブジェクト クラス

オブジェクト状態モデルに使用するオブジェクト クラスです。

注: このしきい値はすべての SystemEDGE ホスト バージョンに利用可能ではありません。

オブジェクト属性

オブジェクト状態モデルに使用するオブジェクト属性です。

注: このしきい値はすべての SystemEDGE ホスト バージョンに利用可能ではありません。

オブジェクト インスタンス

オブジェクト状態モデルに使用するオブジェクト インスタンスです。

注: このしきい値はすべての SystemEDGE ホスト バージョンに利用可能ではありません。

アクションの実行

しきい値を超えた場合に実行されるコマンド（4096 文字までの文字列）を指定します。アクション スクリプトはホスト上に存在する必要があります。

引数の送信

アクション スクリプトまたはプログラムに対してデフォルトの引数を送信するかどうかを示します（例： トラップ タイプまたは説明フィールドなど）。

詳細オプション

詳細オプションでは、監視プロセス中に実行するアクションを指定できます。

SNMP トラップの送信

SNMP トラップを送信するかどうかを示します。

プロセス開始トラップの送信

プロセス開始トラップを送信するかどうかを示します。

プロセス開始トラップの処理

プロセス開始トラップが発生した場合に、アクション、イベントのログ記録、SNMP トラップの送信を実行するかどうかを示します。 3 つの個別のフラグを同時に設定するために便利なフラグとして動作します。

準備未完了トラップの送信

準備未完了トラップを送信するかどうかを示します。

1 回

準備未完了トラップが 1 回送信されます。

継続的

継続的に準備未完了トラップが送信されます。

プロセス クリア トラップの送信

プロセス クリア トラップを送信するかどうかを示します。

親プロセスの監視

親プロセスを監視するかどうかを示します。

Windows サービスの監視

Windows サービスを監視するかどうかを示します。

エントリの再初期化

エントリを再初期化するかどうかを示します。

イベントのログ記録

イベントをログ記録するかどうかを示します。

***x* 個のプロセスを監視**

指定された数のプロセスについて監視するかどうかを示します。

連続する *x* 個のイベントの後の違反

指定された数の連続するイベントの後にトラップを送信するかどうかを示します。

連続する *x* 個の違反トラップを許可

指定された数の連続する違反トラップを許可するかどうかを示します。

プロセス監視ルールの編集

ローカル プロセス監視ルールを編集できます。 また、ホスト モデルのコンテキスト内のルール セットによって所有されるルールを編集できます。後者の場合、変更はルールの所有権をルール セットからモデルに変換します（［ルール所有者］値を［ローカル］に変換）。

重要: ルールを編集するには、ルールが作成されたすべてのランドスケープにユーザ モデルが必要です。

次の手順に従ってください:

1. コンテンツ画面で、編集するプロセス監視ルールを含むモデルを選択します。

   このホスト デバイスの情報が、コンポーネント詳細画面に表示されます。

2. コンポーネント詳細画面の［情報］タブで、［システム リソース］-［実行中］-［監視対象プロセス］-［監視対象プロセス］を展開します。

   監視対象プロセス テーブルは、選択したモデルのプロセス監視ルールのリストを示します。

3. 編集するプロセス監視ルールを選択し、［編集］をクリックします。

   ［プロセス監視テーブル エントリの編集］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、［OK］をクリックします。

   選択されたモデルのプロセス監視ルールへの変更は、すぐに有効になります。

プロセス監視ルールの削除

ローカル監視ルールおよびホスト モデルのルール セットによって所有されるルールを削除できます。 前者の場合、プロセスの監視が停止されます。 後者の場合の削除は、ルール セットのルールによる特定のモデルに対する監視も停止されます。 ただし、ルール セットのルールの削除は一時的なものです。 ルールによって指定されるプロセス監視は、次にルール セットが更新されるときに再確立されます。 詳細については、「ルール セットの外部ルールの削除 (P. 58)」を参照してください。

プロセス監視ルールを削除する場合、CA Spectrum およびプロセス監視エージェントは、ルールで指定されるプロセスのすべての同一（区別されなかった）インスタンスの監視を停止します。 さらに、ルールはエージェント MIB から削除されます。

次の手順に従ってください:

1. コンテンツ画面で、削除するプロセス監視ルールを含むモデルを選択します。

   このホスト デバイスの情報が、コンポーネント詳細画面に表示されます。

2. コンポーネント詳細画面で、［システム リソース］-［実行中］-［監視対象プロセス］-［監視対象プロセス］を展開します。

   監視対象プロセス テーブルは、選択したモデルのプロセス監視ルールのリストを示します。

3. 削除するプロセス監視ルールを選択し、［削除］をクリックします。

   削除を確認できるプロンプトが表示されます。

4. 削除を確認します。

   プロセス監視ルールが削除されます。

   選択されたモデルのルールによって指定されたプロセス監視はすぐに停止します。

保守モード

プロセス監視が保守モードである場合、プロセスは監視されません。 プロセスの監視に関連付けられたイベントまたはアラームは生成されません。

複数の重大アプリケーションが実行されているホスト上で単一のアプリケーションがアップグレードされる場合、プロセス監視を保守モードにすると役立つ場合があります。 アップグレードされている間は、特定のアプリケーションと関連付けられたプロセスのみ保守モードに設定できます。 他のアプリケーションの監視は続行できます。

保守モードはスケジュールすることもできます。これによりプロセスのアラームに時刻を指定できます。

保守モードでは、RFC 2790 および NSM エージェントのプロセス監視のみがサポートされています。

注: ホスト デバイスが保守にある場合、そのデバイスのプロセス監視は自動的に一時停止されます。

プロセス監視を保守モードにする

プロセス監視は、いつでも保守モードにできます。 この手順では、プロセス監視を保守モードにする方法を説明します。

次の手順に従ってください:

1. コンテンツ画面で、プロセス監視を保守モードにするホスト モデルを選択します。

   注: 保守モードでは、RFC 2790 および NSM エージェントのプロセス監視のみがサポートされています。

2. コンポーネント詳細画面の［情報］タブで、該当する場合は、［システム リソース］-［実行中］-［監視対象プロセス］-［RFC 2790］を展開します。

3. プロセス監視を保守モードにする監視対象プロセスまたは監視対象プロセス (RFC 2790) テーブルから以下のいずれかの手順を実行します。

   - プロセス監視を選択し、保守モードに設定して、テーブルの上にある［保守］ボタンをクリックします。
   - プロセス監視を右クリックし、保守モードに設定して、［保守モードの切り替え］を選択します。

   これでプロセス監視は保守モードになり、アイコンは茶色に変更されます。 モードは、監視対象プロセス テーブルの［状態］列に反映されます。 アイコンがすぐに変更されない場合は、［リフレッシュ］をクリックします。

注: この同じ手順を使用して、保守モードからプロセス監視を削除できます。

プロセス監視の保守モードのスケジュール

保守スケジュールを適用することによって、プロセス監視が保守モードになる時間をスケジュールできます。 既存のスケジュールを適用、または新しいスケジュールを作成できます。 プロセス監視に複数のスケジュールを適用できます。

次の手順に従ってください:

1. ［ロケータ］-［システムとアプリケーションの監視］-［すべての監視対象プロセス］を選択します。
2. コンテンツ画面で保守スケジュールを適用するプロセス監視を選択します。

   注: 保守モードでは、RFC 2790 および NSM エージェントのプロセス監視のみがサポートされています。
3. コンポーネント詳細画面で[プロセス監視詳細]サブビューを展開し、［保守中］を検索し、［スケジュール］をクリックします。

   ［スケジュールの追加/削除］ダイアログ ボックスが表示されます。プロセス監視に適用されている保守スケジュールは、［現在のスケジュール］列に表示されます。
4. （オプション）既存のスケジュールを適用します。 ［使用可能スケジュール］列からスケジュールを選択し、左矢印をクリックし、それを［現在のスケジュール］列に移動させます。
5. ［作成］をクリックします。

   ［スケジュールの作成］ダイアログ ボックスが表示されます。
6. スケジュールの［開始日］、［開始時刻］、および［終了時刻］または［期間］のいずれかを選択します。
7. ［繰り返しのオプション］ファクタを選択します。

   注: ［繰り返しのオプション］を［なし］に設定し、一度だけの保守モード ウィンドウを作成します。
8. 説明を提供し、スケジュールを示します。
9. ［OK］をクリックします。

   ［スケジュールの作成］ダイアログ ボックスが閉じます。 新規スケジュールが、［スケジュールの追加/削除］ダイアログ ボックスの［現在のスケジュール］列に表示されます。

10. ［OK］をクリックします。

［スケジュールの追加/削除］ダイアログ ボックスが閉じます。 保守モードのスケジュール変更がプロセス監視に適用されます。 変更が［割り当てられた保守スケジュール］リストに表示されます。

デバイス モデルで保守アラームを細分化

デバイスが保守モードにある場合、デバイス上で生成される保守アラームは関連するプロセス モデルに細分化される可能性があります。 rollMMAlarmToApp 属性を TRUE に設定することにより、この継承を有効にします。 このオプションが有効な場合、アラームもデバイスと関連付けられたアプリケーション モデルに細分化されます。

注: デバイスを保守モードにする詳細については、「オペレータ ガイド」を参照してください。モデル属性を変更する詳細については、「IT インフラストラクチャのモデリング/管理 - 管理者ガイド」を参照してください。

プロセス モデル内部状態

CA Spectrum は、プロセス監視イベントにアラームを生成させずに、プロセス モデルの状態を維持できます。 この機能は、サービスまたはリソース内の複数の監視対象プロセス モデルを統合する場合に役立ちます。 プロセス監視ルールが違反されるごとにアラームがデバイスまたはプロセス モデル上に生成されるのではなく、サービス ポリシーが違反された場合にサービス モデル上に単一のアラームを確認できます。

この機能はデフォルトでは無効です。 EnableInternalCondition 属性の値を「Yes」に設定するには、属性エディタを使用して有効にします。 この属性は、NSM プロセス監視のデバイス モデル、および RFC 2790 プロセス監視の rfc2790App アプリケーション モデル上にあります。 この機能が有効または無効のいずれかの場合、すべての既存プロセス監視アラームは関連するプロセス モデル上でクリアされ、それらの InternalCondition 属性は「通常」に設定されます。

機能は有効で、［アラーム生成対象］オプションが「プロセス モデル」に設定された場合、プロセス監視イベントはアラームを生成しません。代わりに、プロセス モデルの InternalCondition 属性は、プロセス モデルの条件を反映すると設定されます。 この属性の値は、［ロケータ］タブのすべての監視対象プロセス テーブルにあるシステムとアプリケーションの監視の［内部状態］列に表示されます。 また、値はプロセス モデルの［属性］タブ上で見つけることができます。

［内部状態］機能が有効であるときに、プロセス モデルにログ ファイル監視をマッピングしません。 ログ ファイル監視イベントは、アラームの生成を続けます。

RFC 2790 監視をサポートするホストの場合

- 機能が有効または無効の場合
  - 影響を受けたデバイス モデルに存在するすべてのプロセス監視アラームを手動でクリアします。
  - プロセス数の条件は再度アサートされますが、プロセス開始およびプロセス停止条件は再度アサートされません。
- ［内部状態］機能がそのランドスケープのデバイス上で有効なときに、SpectroSERVER が再起動される場合、その機能を無効にして、デバイス上で再度有効する必要があります。これらのステップは、プロセス モデルの［内部状態］がプロセス監視の実際の条件で正確に同期することを確認します。

第 3 章: ファイル システムの監視

ファイル システム監視ルール（RFC 2790）は、CA Spectrum にアラームを生成させるファイル システムのアラーム状態を指定します。 ルールが作成されるホスト モデル上でこの状態が発生するときに、アラームが生成されます。

- ファイル システム使用率
- ファイル システムがオフライン

このセクションでは、特定のホスト モデルに対してファイル システム監視を設定する方法について説明します。 グローバル コレクション コンテナに含まれたモデルに対して、ファイル システム監視ルールの作成を自動化する詳細については、「監視ルール セットの使用 (P. 51)」を参照してください。

ファイル システム監視ルールの作成

ファイル システム監視ルールを作成する場合、オンラインまたはオフラインのあらゆるファイル システムを指定できます。 CA Spectrum は、ルールに対してモデルを作成します。

ファイル システム監視ルールの設定中に、CA Spectrum にアラームを生成させるアラーム状態を定義します。 アラーム状態の例には、システム使用率しきい値またはオフラインのファイル システムが含まれます。

注: 適切な権限のあるユーザのみが、ファイル システム監視ルールを作成できます。詳細については、「システムとアプリケーションの監視権限 (P. 101)」を参照してください。

次の手順に従ってください:

1. コンテンツ画面で、監視するファイル システムを含むモデルを選択します。

   このホスト デバイスの情報が、コンポーネント詳細画面に表示されます。

2. コンポーネント詳細画面で、［システム リソース］-［ファイル システム］を展開します。

   このホスト タイプ用の利用可能なファイル システム監視オプションが表示されます。

3. ［ファイル システム］（RFC 2790）および［監視対象ファイル システム］（RFC 2790）を展開します。

   ファイル システム（RFC 2790）テーブルは、選択したモデルのファイル システムのリストを示します。 監視対象ファイル システム（RFC 2790）テーブルは、選択したホスト用に作成されたファイル システム監視ルールのリストを示します。

4. 選択したモデルにファイル システム監視ルールを作成するには、以下のいずれかの方式を使用します。

   - 監視するファイル システムが利用可能な場合、ファイル システム（RFC 2790）テーブルのファイル システムを右クリックし、［このファイル システムを監視］を選択します。
   - ファイル システムが利用できないため、ファイル システム（RFC 2790）テーブルに含まれていない場合、監視対象ファイル システム（RFC 2790）テーブルの上の［追加］をクリックします。 たとえば、これでオフラインのファイル システムを認識するために指定し、それがオンラインになるのを監視できます。

   ［ファイル システム監視の追加］ダイアログ ボックスが表示されます。ファイル システム（RFC 2790）テーブルからファイル システムを選択した場合、ボックスにはファイル システム名が含まれます。

5. 設定を入力します。 利用可能な設定は以下のとおりです。

   ファイル システム名

   ファイル システムを指定します。 現在、利用可能ではないファイル システムを監視に追加した場合、名前を入力します。 利用可能なファイル システムを追加した場合、名前が自動的に入力されます。

   RFC 2790 監視をサポートするホストについては、このフィールドに入力する値は大文字と小文字を区別しません。 監視対象ファイル システム（RFC 2790）テーブルに表示されるときは、このフィールドは小文字に変換されます。 重複したエントリは許可されません。 新規エントリが同じファイル システム名で作成される場合、新規エントリは既存のエントリを置換し、変更されていた設定はすべて更新されます。

説明

ファイル システムのニックネーム（エイリアス）を指定します。

しきい値タイプ

容量の割合またはストレージの単位（バイト、キロバイト、メガバイト、ギガバイト、テラバイト）で、ファイル システム使用率しきい値を監視するかどうかを指定します。

使用率しきい値

イベント、マイナー アラーム、メジャー アラームおよび重大アラーム用のしきい値を指定します。 メトリックがしきい値を超えなくなったとき、CA Spectrum はしきい値アラームをクリアします。

オフラインの場合にアラーム

ファイルシステムがオフラインになったとき、CA Spectrum がアラームを生成するかどうかを指定します。 ファイル システムがオンラインに戻ったとき、CA Spectrum はアラームをクリアします。

6. ［OK］をクリックします。

ファイル システム監視ルールは、監視対象ファイル システム（RFC 2790）テーブルに追加されます。 CA Spectrum は、ルールで指定されたアラーム状態しきい値違反に応じてアラームを生成します。

注: 監視ルールの［ルール所有者］フィールドの値「ローカル」は、ルールが特定のホスト用に明示的に作成されているため、ルール セットの一部ではないことを示します。 ルール セットの詳細については、「監視ルール セットの使用 (P. 51)」を参照してください。

7. ［アラームの生成対象］ドロップダウン リストのルール違反から生ずるアラームの宛先を選択します。 CA Spectrum がアラームを監視ルール モデルまたはホスト モデル上に作成することを指定できます。

ファイル システム監視ルールの編集

ローカル ファイル システム監視ルールおよびホスト モデルのルール セットによって所有されるルールを編集できます。 後者の場合、変更はルールの所有権をルール セットからモデルに変換します（［ルール所有者］値を［ローカル］に変換）。 ただし、次にルール セットが更新されるときに元のルール仕様および所有権が再確立されるため、この変更および所有権変換は一時的なものです。 詳細については、「ルール セットの外部ルールの編集 (P. 57)」を参照してください。

重要: ルールを編集するには、ルールが作成されたすべてのランドスケープにユーザ モデルが必要です。

次の手順に従ってください:

1. コンテンツ画面で、編集するファイル システム監視ルールを含むモデルを選択します。

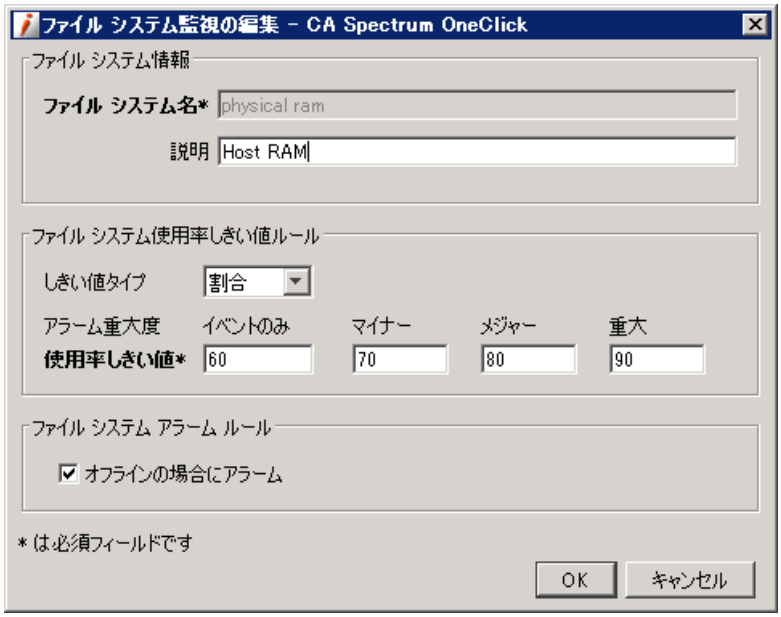
   このホスト デバイスの情報が、コンポーネント詳細画面に表示されます。

2. コンポーネント詳細画面で、［システム リソース］-［ファイル システム］-［監視対象ファイル システム］（RFC 2790）を展開します。

   監視対象ファイル システム（RFC 2790）テーブルでは、ファイル システム監視ルールのリストを示します。

3. 編集するファイル システム ルールを選択して、［編集］をクリックします。

   ［ファイル システム監視の編集］ダイアログ ボックスが表示されます。読み取り専用設定はグレー表示になります。



4. 必要に応じて設定を変更し、［OK］をクリックします。

   選択されたモデルのファイル システム監視ルールへの変更は、すぐに有効になります。

ファイル システム監視ルールの削除

ローカル ファイル システム監視ルールおよびホスト モデルのルール セットによって所有されるルールを削除できます。 前者の場合、ファイル システムの監視が停止されます。 後者の場合の削除は、ルール セットのルールによる特定のモデルに対する監視も停止されます。 ただし、次にルール セットが更新されるときにルールが再確立され、ファイル システム監視が指定されるため、ルール セットのルールの削除は一時的なものです。 詳細については、「ルール セットの外部ルールの削除 (P. 58)」を参照してください。

次の手順に従ってください:

1. コンテンツ画面で、削除するファイル システム監視ルールを含むモデルを選択します。

   このホスト デバイスの情報が、コンポーネント詳細画面に表示されます。

2. コンポーネント詳細画面で、［システム リソース］-［ファイル システム］-［監視対象ファイル システム］（RFC 2790）を展開します。

   監視対象ファイル システム（RFC 2790）テーブルでは、ファイル システム監視ルールのリストを示します。

3. 削除するファイル システム監視ルールを選択し、［削除］をクリックします。

   削除を確認できるプロンプトが表示されます。

4. 削除を確認します。

   選択されたモデルのルールによって指定されたファイル システム監視はすぐに停止します。

第 4 章: 監視ルール セットの使用

ルール セットはグローバル コレクションに適用できるプロセスおよびファイル システムのルールを監視するコレクションです。 ルール セットは、CA Spectrum でモデリングされたホストの監視を設定および管理するプロセスを自動化します。 ホスト モデルのプロセスまたはファイル システム監視ルールを作成する場合、このルールはこのホスト モデルのみに適用されます。 他のホスト モデルに同じルールを適用する場合は、各ホスト モデルに対して繰り返し同じルールを作成します。 すべてのモデルのルールを編集する場合は、ホスト モデルごとにルールの各インスタンスを変更します。 このタスクは明らかに多数のホスト モデルのホスト監視を管理する上で、面倒で非能率的な方法です。

グローバル コレクションにルール セットを適用することによって、IT インフラストラクチャ リソースを管理するより効率的な方法を活用します。ホスト モデルがコレクションに追加されると、CA Spectrum はモデルのプロセスまたはファイル システムを参照する監視ルールを作成します。 さらに、ルール セットの監視ルールが変更される場合、変更はコレクション内のすべてのホスト モデルに適用されます。 ホスト モデルがコレクションから削除される場合、モデルの監視ルールもすべて削除されます。

ルール セットの作成

ホスト プロセスおよびファイル システムの両方に使用する複数の監視ルールを含むルール セットを作成できます。また、いずれか 1 つを含むルール セットを作成できます。 グローバル コレクションに必要な数だけルール セットを適用できます。 また、複数のコレクションに同じルール セットを適用できます。

重要: ルールを複製しないように、また、矛盾するルールを実装しないように、ルール セットの実装を慎重に計画します。複製または矛盾するルールは、予期しない結果を引き起こし、トラブルシューティングを困難にする可能性があります。 また、ホスト モデルが含まれるルール セットを適用するグローバル コレクションが、ルール セット内の監視ルールに適切であることを確認します。

ルール セットを作成するときは、以下の点に留意してください。

- ルール セットは一意の名前である必要があります。
- ルール セットに含まれているルールは、グローバル コレクションに含まれるホスト モデルの同名のローカル監視ルールを優先しません。ローカル監視ルールが特定のホスト モデルに対して作成され、同名のルールを含むルールに適用されたルール セットのあるグローバル コレクションにモデルが含まれている場合、ローカル ルールは保持され、モデルに対して有効となります。

注: 適切な権限のあるユーザのみが、監視ルール セットを作成できます。詳細については、「システムとアプリケーションの監視権限 (P. 101)」を参照してください。

次の手順に従ってください:

1. ［ロケータ］-［システムとアプリケーションの監視］-［すべての監視ルール］を選択します。

   コンテンツ画面は、作成されたすべてのルール セットのリストを示します。

   デフォルトのルール セットは存在しません。

2.  （タイプ別に新しいルール セットを作成）をクリックして、動作させているエージェントに応じて、以下のいずれかのオプションを選択します。

   - RFC2790
   - NSM エージェント：
     - r11 Windows
     - r11 UNIX
     - 3.1 Windows
     - 3.1 UNIX

   ［新規ルール セット］ダイアログ ボックスが表示されます。

3. ［ルール セット名］フィールドでルール セットの名前を入力して、［OK］をクリックします。

   新規ルール セットがリストに表示されます。これでプロセス監視およびファイル システム監視設定ルールをルール セットに追加できます。さらに、グローバル コレクション コンテナにルール セットを適用できます。

監視ルールをルール セットに追加

ルール セットをグローバル コレクションに適用する前後のルール セットに、監視ルールを追加できます。

次の手順に従ってください:

1. ［ロケータ］-［システムとアプリケーションの監視］-［すべての監視ルール］を選択します。

   コンテンツ画面はルール セットのリストを示します。

   注: ルール セットがリスト表示されない場合、「ルール セットの作成 (P. 51)」で述べたように、ルールにルール セットを作成します。

2. 監視ルールを追加するルール セットを選択します。

   コンポーネント詳細画面は、ルール セットに関する情報を表示します。

3. ［情報］タブで、ルール セットに追加するルールのタイプを指定します。

   - プロセス監視ルールを追加するには、［プロセス監視ルール］を展開します。
   - ファイル システム監視ルールを追加するには、［ファイル システム監視ルール］を展開します。

     注: NSM ルール セットは、ファイル システム監視ルールをサポートしません。

   各ルール テーブルでは、ルール セットに追加されたルールのリストを示します。

4. ルールのタイプをルール セットに追加するために、［追加］をクリックします。

   ［監視対象プロセスの追加］ダイアログ ボックスまたは［ファイル システム監視の追加］ダイアログ ボックスのいずれかが表示されます。

5. 設定を行います。

   - プロセス監視ルールを設定する詳細については、「プロセス監視ルール パラメータ (P. 21)」を参照してください。
   - ファイル システム監視ルールを作成する詳細については、「ファイル システム監視ルールの作成 (P. 45)」を参照してください。

6. ［OK］をクリックします。

   ルールはルール セットに追加されます。

グローバル コレクションにルール セットを適用します

グローバル コレクションにルール セットを適用することで、監視ルールを作成するプロセスは自動化されます。 CA Spectrum は、グローバル コレクションにあるすべてのモデルに監視ルールを自動的に作成します。

グローバル コレクションにルール セットを適用するときに、以下の事実を考慮します。

- グローバル コレクションからモデルを削除する場合、ルール セットによって指定される監視ルールはすべてモデルから削除されます。
- グローバル コレクションに含まれている特定のモデルのルール セットからルールを編集する場合、ルールの所有権はローカルの所有権に変更されます。ルールはルール セットのルールと関連付けられた状態ではなくなり、特定のモデルのみに適用されます。
- グローバル コレクションと関連付けられたルール セット、またはルール セットに関連付けられたグローバル コレクションを削除する場合、ルール セットによって指定されるルールはコレクションのモデルから削除されます。

次の手順に従ってください:

1. ［ロケータ］-［システムとアプリケーションの監視］-［すべての監視ルール］を選択します。

   コンテンツ画面はルール セットのリストを示します。

   注: ルール セットがリスト表示されない場合は、「ルール セットの作成 (P. 51)」で述べたように、ルール セットを作成します。

2. グローバル コレクションに適用するルール セットまたはセットを右クリックし、［グローバル コレクションの適用/削除］を選択します。

   ［ルール セットに対するコレクションの適用/削除］ダイアログ ボックスが表示されます。

   ダイアログ ボックスの左側にリスト表示されるすべてのグローバル コレクションが、選択したルール セットに現在適用されています。右側にリスト表示されるグローバル コレクションは適用されていません。

3. ［非適用先］リストで、ルール セットを適用するグローバル コレクションをダブルクリックします。

   選択されたグローバル コレクションは、［適用先］リストに移動されます。

   注: 複数のルール セットにグローバル コレクションを同時に適用できません。

4. （オプション）ダイアログ ボックスで［OK］をクリックする場合、ルール セットにすでに適用されているグローバル コレクションまたはコレクションを再適用するために、［再適用］のチェック ボックスをオンにします。

5. ［OK］をクリックし、変更を適用します。

   注: ダイアログ ボックスで加えた変更のみが適用されます。［再適用］のチェック ボックスをオンにしていない場合、［適用先］リストにすでに表示されているグローバル コレクションは再適用されません。

   選択したルール セットの［情報］タブの［適用されるグローバル コレクション リスト］は、それが適用されるグローバル コレクションを表示します。

グローバル コレクションからルール セットを削除

グローバル コレクションからルール セットを削除するときに、CA Spectrum はグローバル コレクションのすべてのモデルからルール セットの監視ルールを削除します。

次の手順に従ってください:

1. ［ロケータ］-［システムとアプリケーションの監視］-［すべての監視ルール］を選択します。

   コンテンツ画面はルール セットのリストを示します。

2. グローバル コレクションを削除するルール セットまたはセットを右クリックし、［グローバル コレクションの適用/削除］を選択します。

   ［ルール セットに対するコレクションの適用/削除］ダイアログ ボックスが表示されます。

   注: ［結果］タブ ツールバーで  をクリックし、このダイアログ ボックスを起動することもできます。

ダイアログ ボックスの左側にリスト表示されるすべてのグローバル コレクションが、選択したルール セットに現在適用されています。右側にリスト表示されるグローバル コレクションは適用されていません。

3. ［適用先］リストで、ルール セットから削除するグローバル コレクションをダブルクリックします。

   選択されたグローバル コレクションは、［非適用先］リストに移動されます。

   注: 複数のルール セットからグローバル コレクションを同時に削除できません。

4. （オプション）ダイアログ ボックスで［OK］をクリックする場合、ルール セットにすでに適用されているグローバル コレクションまたはコレクションを再適用するために、［再適用］のチェック ボックスをオンにします。

5. ［OK］をクリックし、変更を適用します。

   注: ダイアログ ボックスで加えた変更のみが適用されます。［再適用］のチェック ボックスをオンにしていない場合、［適用先］リストにすでに表示されているグローバル コレクションは再適用されません。

   選択したルール セットの［情報］タブの［適用されるグローバル コレクション リスト］は更新されます。 削除したグローバル コレクションまたはコレクションは表示されなくなります。

ルール セットのルールの編集

グローバル コレクションに適用されるルール セットのルールを編集する場合、修正されたルール設定はグローバル コレクションのすべてのモデルに展開されます。

重要: ルールを編集するには、ルールが作成されたすべてのランドスケープにユーザ モデルが必要です。

次の手順に従ってください:

1. ［ロケータ］-［システムとアプリケーションの監視］-［すべての監視ルール］を選択します。

   コンテンツ画面はルール セットのリストを示します。

2. 編集するルールを含むルール セットを選択します。

   コンポーネント詳細画面は、ルール セットに関する情報を表示します。

3. コンポーネント詳細画面で、編集するルールのタイプをプロセス監視ルールまたはファイル システム監視ルールのいずれかで指定します。

   各ルール タイプ テーブルでは、ルール セットに含まれているルールのリストを示します。

4. ルールを選択して、［編集］をクリックします。

   ［編集］ダイアログ ボックスが表示されます。

   注: 一部の設定は編集に使用できません。

5. 設定を編集し、［OK］をクリックします。

   変更される設定はすぐに有効になります。

ルール セットの外部ルールの編集

ある状況下では、ルールがグローバル コレクションに適用されたルール セットに属していても、グローバル コレクションの特定モデルの監視ルールを変更する場合があります。その後、変更はグローバル コレクションのすべてのモデルに適用されるため、ルール セットのルールに適用する変更を加えたくない場合があります。 ただし、それでもコレクションにモデルを保持する必要があります。

この場合、ルールをモデル用のローカル バージョンに変換します。 この結果を得るには、ルール セットの特定の外部モデルのコンテキストからこのルールを変更できます。

ルール セットからルールを削除

グローバル コレクションに適用されるルール セットからルールを削除する場合、ルールはグローバル コレクションのすべてのモデルから削除されます。

次の手順に従ってください:

1. ［ロケータ］-［システムとアプリケーションの監視］-［すべての監視ルール］を選択します。

   コンテンツ画面はルール セットのリストを示します。

2. 削除するルールを含むルール セットを選択します。

   コンポーネント詳細画面は、ルール セットに関する情報を表示します。

3. コンポーネント詳細画面で、ルール セットから削除するルールのタイプをプロセス監視ルールまたはファイル システム監視ルールのいずれかで指定します。

   各ルール テーブルでは、ルール セットに含まれているルールのリストを示します。

4. ルールを選択して、［削除］をクリックします。

   ルールはルール セットおよびそのルール テーブルから削除されます。

ルール セットの外部ルールの削除

ある状況下では、ルールがグローバル コレクションに適用されたルール セットに属していても、グローバル コレクションの特定モデルのルールを削除する場合があります。 ルール セットのルールが削除されないように、グローバル コレクションのすべてのモデルでルールを削除する場合があります。 ただし、それでもコレクションにモデルを保持する必要があります。

この場合、ルール セットの特定の外部モデルのコンテキストからこのルールを削除します。 ただし、ルール セットとグローバル コレクションとの関連付けが更新されると、削除されたルールはモデルに対して再作成されます。

ルール セットの削除

グローバル コレクションに適用されるルール セットを削除する場合、ルール セットのルールはすべてコレクションのモデルから削除されます。

次の手順に従ってください:

1. ［ロケータ］-［システムとアプリケーションの監視］-［すべての監視ルール］を選択します。

   コンテンツ画面は利用可能なすべてのルール セットのリストを示します。

2. 削除するルール セットを選択して、［削除］をクリックします。

第 5 章: ログ ファイルの監視

この章では、以下のエージェント用に OneClick でログ ファイル監視を設定する方法について説明します。

- iAgent
- CA SystemEDGE エージェント
- CA Unicenter NSM エージェント

この章では、iAgent syslog サーバ監視および CA Spectrum に転送するトラップを設定する方法について説明します。

ログ ファイル監視を設定するには、以下のタスクを必要とします。

- トラップおよびイベント生成を開始する条件を指定する。 指定する情報のタイプがログ ファイルで検出された場合、トラップおよびイベントが生成されます。
- （オプション）ログ ファイルと監視対象プロセス モデルとの関連付けを指定する。その後、イベントはプロセス モデルへのログ ファイル エントリに対応して生成されます。 イベントはプロセス ホスト モデル上ではなくプロセス モデル上で生成されます。

ログ ファイル監視プロセスについて

ネットワーク上のさまざまなデバイスは、iAgent、SystemEDGE エージェントまたは NSM サーバ上のログ ファイルにデータを送信するように設定できます。 また、これらのサーバのうちの 1 つにあるアプリケーションは、ログ ファイルにデータを送信できます。 いずれの場合も、エージェントはログ ファイルを監視し、ログ ファイル エントリのコンテンツに基づいて SNMP トラップを生成するように設定できます。

ログ ファイル監視は指定する情報のタイプのログ ファイルを検出および解析するテキスト パターン一致システムの設定を含んでいます。 次に、監視エージェントは解析されたテキストに関するデータを含む CA Spectrum にトラップを送信します。次に、このデータは CA Spectrum イベントにマッピングされ、アラームはエージェント モデル、デバイスまたはデバイスが関連するプロセス上にアサートされます。 また、イベント条件ルールを使用し、CA Spectrum が「ログ ファイル内のテキスト一致」イベントからより詳細なイベントおよびオプションのアラームを作成するように設定できます。 その結果、インフラストラクチャで発生している、将来的な問題または実際の問題を示すイベントの通知を受信します。詳細については、「Event Configuration User Guide」を参照してください。

監視しているログ ファイルの構文は、ログ ファイルのタイプおよびログ ファイルに送信されるデータに依存しています。 アプリケーション ログ ファイルが監視しているアプリケーションに直接一致しているため、特別なログ ファイル構文は必要ありません。 ただし、CA Spectrum は別に他のデバイスからデータを収集した他のログ ファイルを処理します。 そのため、これらのログ ファイル エントリは特定の構文条件に一致する必要があります。

監視するログ ファイルのタイプにかかわらず、複数のデバイスから複数のアプリケーションへのエントリが含まれるアプリケーション ログ ファイルまたは syslog ファイルのどちらであっても、監視する情報のタイプを識別する（または解析する）正規表現を定義する必要があります。 正規表現構文は、エージェントのタイプと互換性が必要です。 一致するテキストが見つかると、監視エージェントは一致するテキストが含まれる CA Spectrum にトラップを送信します。 CA Spectrum は、ホスト モデルにアサートされるイベントにトラップを関連付けます。

注: 正規表現の定義に関する詳細については、「イベント設定ユーザ ガイド」を参照してください。

「Syslog ファイル一致を処理する CA Spectrum の設定 (P. 74)」では、トラップを生成する情報で文字列のログ ファイルを監視するためにエージェントを設定する方法について説明します。

注: iAgent は、iAgent サーバに存在するログ ファイルのみを監視できます。これはマッピングされたネットワーク ドライブ上のログ ファイルを監視できません。

詳細情報:

ログ ファイル構文 (P. 61)

ログ ファイル構文

アプリケーション ログまたは他のデバイスからデータを受信する Syslog ファイルなどのログ ファイルを監視できます。 アプリケーション ログを監視するログ ファイルに特別な構文は必要ありません。 ただし、CA Spectrum が適切なデバイス モデルに関するトラップ情報をアサートするには、ネットワーク上のデバイスから情報を受信するログ ファイルは以下の形式が必要です。その形式は BSD Syslog および Cisco IOS 形式に基づいています。

<MessagePrefix>%<MessageHeader><Additional_Information>

<MessagePrefix>

メッセージの日時およびエントリに含まれる情報のソースの IP アドレスまたはホスト名が含まれています。 プレフィックス内に挿入された他の情報がある場合がありますが、そこにはこれら 2 つの情報が含まれている必要があります。

注: ホスト名を使用してソースを識別する場合、myhost.ca.com または myhost の形式となります。

<MessageHeader>

形式は *<A>-<B>-* である必要があります。

<A>

任意の数の大文字の英字、アンダースコアまたは文字列「Aprisma」が含まれます。

<B>

任意の数の大文字の英字、数字またはアンダースコアが含まれます。

<C>

任意の数の大文字の英字、アンダースコアまたはダッシュ記号が含まれます。

<Additional_Information>

あらゆるデータを含めることができます。

一般的に、この構文は以下のタイプのログ ファイルで見つけることができます。

- Cisco または Riverstone デバイスからの Solaris syslog ファイル エントリ。
- 前述の*<MessageHeader>* 形式を使用する別のタイプのデバイスからの Solaris syslog ファイル エントリ。
- Cisco または Riverstone デバイスからの Kiwi syslog ファイル エントリ。
- 前述の*<MessageHeader>* 形式を使用する別のタイプのデバイスからの Kiwi syslog ファイル エントリ。
- CA ログ ファイル。

注: CA Spectrum が Agent トラップを処理するように設定する詳細については、「Syslog ファイル一致を処理する CA Spectrum の設定 (P. 74)」を参照してください。

詳細情報:

ログ ファイル監視プロセスについて (P. 59)

iAgent ホストのログ ファイル監視の作成

以下の手順では、iAgent ホスト エージェントのログ ファイル監視を設定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. コンテンツ画面で、監視するログ ファイルを含むモデルを選択します。

   このホスト デバイスの情報が、コンポーネント詳細画面に表示されます。

2. コンポーネント詳細画面の［情報］タブで、［システム リソース］-［監視対象ログおよびプロセス ログ-［監視対象ログ］を展開します。

   監視対象ログ リストが表示されます。

   注: 一部のリスト フィールドはエージェント固有です。

3. 監視対象ログ リストで［追加］をクリックします。

   エージェント用の［ログ ファイル監視の追加］ダイアログ ボックスが表示されます。

4. 必要に応じてログ ファイル監視設定を設定します。特に以下の必須およびオプションの設定に注意してください。

   ログ ファイル名

   監視対象ログ ファイルを示します。

   正規表現

   ログ ファイルで解析するテキスト パターンを示します。

   注: 正規表現の定義に関する詳細については、「イベント設定ユーザ ガイド」を参照してください。

   説明

   他のユーザに監視の目的を示します。

   一致時にトラップを送信/トラップの送信

   正規表現が一致するテキスト パターンを検出した場合、エージェントが CA Spectrum にトラップを送信するかどうかを指定します。

5. ［OK］をクリックします。

   監視設定は監視対象ログ リストに追加され、監視はすぐに開始されます。

NSM エージェントのログ ファイル監視

OneClick で NSM エージェントのログ ファイル監視およびファイル監視を設定できます。 以下の定義は、これら 2 つの監視の違いを説明します。

NSM ログ ファイル監視

NSM ログ ファイル監視は、特定のパターンのファイルでコンテンツをウォッチします。

NSM ファイル監視

NSM ファイル監視は、単にファイルの有無をウォッチします。

NSM エージェント ログ ファイル監視では、以下のタスクを実行できます。

- NSM エージェントのファイル監視の編集および表示
- NSM エージェントのログ監視の編集および表示
- NSM エージェントのファイルおよびログ監視のステータス変更の表示

OneClick を使用した NSM エージェントのログ ファイル監視の設定

OneClick を使用して、NSM ホスト エージェントのログ ファイル監視を設定できます。

次の手順に従ってください:

1. コンテンツ画面で、監視するログ ファイルを含むモデルを選択します。

   このホスト デバイスの情報が、コンポーネント詳細画面に表示されます。

2. コンポーネント詳細画面の［情報］タブで、［システム リソース］-［監視対象ログおよびファイル］-［監視対象ログ］を展開します。

   監視対象ログ リストが表示されます。

3. 監視対象ログ リストで［追加］をクリックします。

   ［ログ ファイル監視の追加］ダイアログ ボックスが表示されます。

4. 必要に応じてログ ファイル監視設定を設定します。以下のオプションを使用できます。

   監視名

   このログ ファイル監視の名前を示します。

   ファイル名

   監視するログ ファイルのフル パスおよびファイル名（またはワイルドカードを使用したファイル名）を示します。

   一致パターン

   指定された正規表現がファイルで見つかる場合、監視を DOWN 状態にします。

   不一致パターン

   指定された正規表現がファイルで見つからない場合、監視を DOWN 状態にします。

一致パターンの切り替え

指定された正規表現がファイルで見つかった場合、監視を UP 状態にします。 このフィールドは、ステータス ポリシーが toggled または toggledEOF の場合のみ利用可能です。

不一致パターンの切り替え

指定された正規表現がファイルで見つからない場合、監視を UP 状態にします。このフィールドは、ステータス ポリシーが toggled または toggledEOF の場合のみ利用可能です。

開始

開始文字位置です。

終了

終了文字位置です。

ステータス ポリシー

監視がファイルを処理する方法を定義します。 以下のオプションを使用できます。

poll

各ポーリングの初めに、監視ステータスを UP に設定します。 一致した場合、状態は DOWN に変更されます。 ファイル全体が読み取られた場合、それが新しい監視でない限り、ファイルは前回の読み取り場所からスキャンされます。

historical

一致が発生するときに、監視ステータスを DOWN に設定し、ステータスはログ ファイルの有効期間に DOWN のままです。 そのため、ログ ファイルは再度作成されます。 ファイル全体が読み取られた場合、それが新しい監視でない限り、ファイルは前回の読み取り場所からスキャンされます。

startFromPreviousRead

一致が発生するときに、監視ステータスを DOWN に設定し、リセットするまでステータスは DOWN のままです。 ファイルは前回の読み取り場所からスキャンされます。

toggled

履歴属性と同様に DOWN パターンを指定できます。また、UP パターン（一致および不一致パターンの切り替え属性で形成）も指定でき、UP に状態を戻す変更と比較されます。 ファイルは前回の読み取り場所からスキャンされます。

firstLineOnly

ファイルの最初の行のみを読み取ります。 監視ステータスは、各ポーリングの初めに UP に設定されます。 一致が見つかる場合、状態は DOWN に変更されます。

pollEOF

各ポーリングの初めに、監視ステータスを UP に設定します。 一致が見つかる場合、状態は DOWN に変更されます。 ファイルの最後から読み取りが開始された場合、それが新しい監視でない限り、ファイルは前回の読み取り場所からスキャンされます。

startFromPreviousReadEOF

一致が発生するときに、監視ステータスを DOWN に設定し、リセットするまでステータスは DOWN のままです。 ファイルの最後から読み取りが開始された場合、それが新しい監視でない限り、ファイルは前回の読み取り場所からスキャンされます。

toggledEOF

履歴属性と同様に DOWN パターンを指定できます。また、UP パターン（一致および不一致パターンの切り替え属性で形成）も指定でき、UP に状態を戻す変更と比較されます。 ファイルの最後から読み取りが開始された場合、それが新しい監視でない限り、ファイルは前回の読み取り場所からスキャンされます。

rescan

ファイル長が増加している場合、ファイルを先頭から再スキャンします。 ファイルが 10 KB を超える場合、監視を「不明」に設定します。

監視ステータス

トラップ送信に一致しない場合も、監視のステータス側を無効にできます。 以下のオプションを使用できます。

downCritical

設定されたとおり状態変更が動作し、重大アラートが発生されることを示します。

doNotMonitor

ログ ファイルが監視されていますが、状態は常に UP であることを示します。

downWarning

設定されたとおり状態変更が動作し、警告アラートが発生されることを示します。

トラップ送信ポリシー

監視ステータス トラップに適用されるポリシーを定義します。 以下のオプションを使用できます。

never

状態変更がトラップを送信させないことを示します。

once

監視状態が変更される場合のみ、状態変更トラップが送信されることを示します。

perPoll

状態は変更されないが、一致条件が最後のポーリング以降に発生する場合、状態変更トラップがポーリングごとに送信されことを示します。

each

状態変更トラップがエージェントが一致を見つけるごとに送信されることを示します。切り替え属性については、監視がダウンした場合、切り替えパターンは検索される次の一致になります。 この結果、後続のダウン パターンは一致しません。

一致トラップ ポリシー

一致トラップに適用されるポリシーを定義します。 以下のオプションを使用できます。

send

見つかった一致ごとにトラップを送信します。切り替え属性については、監視がダウンした場合、切り替えパターンは検索される次の一致になります。この結果、ステータス監視がオフにされない限り、後続のダウン パターンは一致しません。

doNotSend

一致が見つかるごとにトラップは送信されません。

履歴ポリシー

トラップ詳細を履歴テーブルに格納するかどうか定義します。 以下のオプションを使用できます。

generateHistory

ステータス トラップが履歴テーブルに記録されることを示します。

noGenerateHistory

ステータス トラップが履歴テーブルに記録されないことを示します。

5. ［OK］をクリックします。

監視設定は監視対象ログ リストに追加されます。監視はすぐに開始されます。

OneClick を使用した NSM エージェントのファイル監視の設定

OneClick を使用して、NSM ホスト エージェントのログ ファイル監視を設定できます。

次の手順に従ってください:

1. コンテンツ画面で、監視するファイルを含むモデルを選択します。

   このホスト デバイスの情報が、コンポーネント詳細画面に表示されます。

2. コンポーネント詳細画面の［情報］タブで、［システム リソース］-［監視対象ログおよびファイル］-［監視対象ファイル］を展開します。

   監視対象ファイル リストが表示されます。

3. 監視対象ファイル リストで［追加］をクリックします。

   ［ファイル監視の追加］ダイアログ ボックスが表示されます。

4. ファイル監視設定を設定します。特に以下の必須およびオプションの設定に注意してください。

   監視名

   ファイル監視の名前を示します。

   ファイル名

   この監視がウォッチするファイルの名前を示します。

   ファイルあり

   ファイルが存在するかどうかを示します。

   トラップ送信ポリシー

   NSM エージェントがトラップを送信する頻度を指定します。 以下の設定を使用できます。

   never

   トラップを送信しません。

   once

   状態が変化した場合にのみ、トラップを送信します。

   perPoll

   状態がダウンの場合の各ポーリングでステータス トラップを送信します。

   履歴ポリシー

   履歴ポリシー設定の詳細については、「OneClick を使用した NSM エージェントのログ ファイル監視の設定 (P. 64)」を参照してください。

5. ［OK］をクリックします。

   監視設定は監視対象ファイル リストに追加され、監視はすぐに開始されます。

SystemEDGE ホストのログ ファイル監視の作成

OneClick を使用して、SystemEDGE ホスト エージェントのログ ファイル監視を設定できます。

次の手順に従ってください:

1. コンテンツ画面で、監視するログ ファイルを含むモデルを選択します。

   このホスト デバイスの情報が、コンポーネント詳細画面に表示されます。

2. コンポーネント詳細画面の［情報］タブで、［システム リソース］-［監視対象ログおよびプロセス ログ-［監視対象ログ］を展開します。

   監視対象ログ リストが表示されます。

3. 監視対象ログ リストで［追加］をクリックします。

   エージェント用の［ログ ファイル監視の追加］ダイアログ ボックスが表示されます。

4. 必要に応じてログ ファイル監視設定を設定します。

   ログ ファイル名またはディレクトリ名

   監視タイプに応じて、監視対象ログ ファイルまたはディレクトリを示します。

   監視タイプ

   ログ ファイルまたはディレクトリを監視するかどうかを示します。

   ファイル

   ログ ファイルが監視されることを示します。

   ディレクトリ

   ディレクトリが監視されることを示します。また、再帰的に監視するかどうか、およびシンボリック リンクをたどるかどうかを指定することもできます。

   説明

   （オプション）たとえば、監視の目的を示す簡単な説明です。

   間隔

   ログ ファイルの連続するスキャンの間隔（分単位）です。

重大度

この監視エントリに使用する重大度です。

ファイルの解析

ログ ファイルで一致させる正規表現です（256 文字まで）。 値は ed(1) に定義されているとおり、有効な文字列である必要があります

一致しない

ログ ファイルを解析するときに論理オペレータ NOT を適用するかどうかを示します。

アクションの実行

一致検索の後に実行されるコマンドを指定する文字列です（4096 文字まで）。 アクション スクリプトはホスト上に存在する必要があります。

引数の送信

アクション スクリプトまたはプログラムに対してデフォルトの引数を送信するかどうかを示します（例： トラップ タイプまたは説明フィールドなど）。

SNMP トラップの送信

正規表現が一致するテキスト パターンを検出した場合、エージェントが CA Spectrum にトラップを送信するかどうかを指定します。

準備未完了トラップの送信

準備未完了トラップを送信するかどうかを示します。

1 回

準備未完了トラップが 1 回送信されます。

継続的

継続的に準備未完了トラップが送信されます。

エントリの再初期化

エントリを再初期化するかどうかを示します。

連続する *x* 個の一致の後の違反

指定された数の連続する一致が発生した後に、トラップを送信するかどうかを示します。

イベントのログ記録

イベントをログ記録するかどうかを指定します。

5. ［OK］をクリックします。

監視設定は監視対象ログ リストに追加され、監視はすぐに開始されます。

ログとプロセスのマッピング

CA Spectrum は、解析されたログ ファイル エントリがホスト モデル以外を参照するプロセスにイベントを生成できます。 このようなイベントを設定するには、ホスト モデルのプロセス監視ルールがプロセスを参照することを確認します。 また、プロセスに関連するエントリが含まれるログ ファイルとプロセスを関連付けます。 プロセス監視ルールの詳細については、「プロセス監視 (P. 17)」を参照してください。

RFC 2790 エージェントおよび SystemEDGE ホスト用のマッピングの指定

OneClick を使用して、RFC 2790 エージェントのプロセスに対してログのマッピングを指定できます。

次の手順に従ってください:

1. コンテンツ画面で、監視するログ ファイルを含むモデルを選択します。

   このホスト デバイスの情報が、コンポーネント詳細画面に表示されます。

2. コンポーネント詳細画面で、［システム リソース］-［監視対象ログおよびプロセス ログ］-［監視対象プロセス ログ ファイルのマッピング］を展開します。

   監視対象のプロセス ログ ファイルのマッピング リストが表示されます。

3. 監視対象のプロセス ログ ファイルのマッピング リストの［追加］をクリックします。

   ［ログとプロセスのマッピングの追加］ダイアログ ボックスが表示されます。

4. 以下のデータを入力します。

   ログ ファイル名

   監視するログ ファイルです。

   プロセス名

   プロセス監視ルールで指定されるプロセスです。

5. ［OK］をクリックします。

   マッピングは、監視対象のプロセス ログ ファイルのマッピング リストに追加されます。プロセスに関するテキストがログ ファイルから解析される場合は常に、CA Spectrum は監視対象プロセス モデルにイベントを生成します。

NSM r11 エージェントのマッピング

OneClick を使用して、NSM r11 エージェントのプロセスに対してログのマッピングを指定できます。

注: NSM 3.1 エージェントのマッピングは作成できません。

次の手順に従ってください:

1. コンテンツ画面で、監視するログ ファイルを含むモデルを選択します。

   このホスト デバイスの情報が、コンポーネント詳細画面に表示されます。

2. コンポーネント詳細画面で、［システム リソース］-［監視対象ログおよびファイル］-［監視対象プロセス ログ ファイルのマッピング］を展開します。

   監視対象のプロセス ログ ファイルのマッピング リストが表示されます。

3. 監視対象のプロセス ログ ファイルのマッピング リストの［追加］をクリックします。

   ［ログとプロセスのマッピングの追加］ダイアログ ボックスが表示されます。

4. 以下のデータを入力します。

   ログ ファイル名

   ログ ファイルの名前。

   監視名

   プロセス監視の名前。 この値は、多くの場合、プロセス監視ルールでプロセスに指定される名前と異なります。

5. ［OK］をクリックします。

   マッピングは、監視対象のプロセス ログ ファイルのマッピング リストに追加されます。プロセスに関するテキストがログ ファイルから解析される場合は常に、CA Spectrum は監視対象プロセス モデルにイベントを生成します。

監視対象ログおよびプロセス ログ マッピング設定の管理

OneClick を使用して、監視対象ログおよびプロセス ログ ファイル マッピング設定を編集および削除できます。

- 監視対象ログおよびプロセス ログ ファイル マッピング設定を編集するには、変更する設定エントリを選択し、設定エントリ リストの［編集］をクリックし、エントリを編集して、［OK］をクリックします。

  注: アクティブな監視エントリは編集できません。 アクティブ状態にある監視エントリを編集するには、エントリの状態を notInService(2) または notReady(3) に変更します。 SET コマンドを使用して、MIB ツールでこのタスクを実行できます。

- 監視対象ログおよびプロセス ログ ファイル マッピング設定を削除するには、削除する設定エントリを選択し、設定エントリ リストの［削除］をクリックし、［OK］をクリックします。

Syslog ファイル一致を処理する CA Spectrum の設定

CA Spectrum を設定して、iAgent、SystemEDGE および NSM エージェントから syslog ファイル一致を処理できます。

トラップ処理の概要

ログ ファイル エントリのコンテンツに基づいてエージェントが生成する各トラップに OID があります。この OID は、エージェントの AlertMap ファイルのトラップ マッピングに基づいて CA Spectrum のイベント 0x3e00009 を生成します。 このイベントはモデルにアサートされます。

各ログ ファイル エントリ（255 文字まで）で一致した行、およびトラップを生成したログ ファイル名は、トラップ情報の一部として送信されます。CA Spectrum は、トラップ データを解析し、ログ ファイル エントリの元のソースを判断します。 このソースは、IP アドレス、ホスト名、CA Spectrum モデル ハンドルまたはアプリケーション ログ ファイル名の場合があります。

IP アドレス、ホスト名またはモデル ハンドルを含むトラップの処理

IP アドレス、ホスト名またはモデル ハンドルがログ ファイル エントリのソースとして抽出されている場合、CA Spectrum は IP アドレス、ホスト名またはモデル ハンドルに一致するデバイス モデルを検索し、このモデルにイベントをアサートできます。 ログ ファイル エントリが「ログ ファイル構文 (P. 61)」に述べられた構文に一致する場合、デバイス モデルにアサートされたイベントを有益なものにするために、ParseMap ファイルを作成し、このイベントおよびコンテンツをカスタマイズできます。

注: CA Spectrum には多くの ParseMap ファイルが含まれます。常に 1 つ作成する必要はありません。

ParseMap ファイルが作成されない場合、デバイス モデルにルーティングされたイベントは、エージェントのモードにアサートされたイベントと同じです。

ParseMap ファイルの作成

ParseMap ファイルは、受信トラップで情報と関連付けられるイベントを指定します。 さらに、ParseMap ファイルでは、イベント変数として使用されるログ ファイル エントリ テキストの部分を指定できます。イベント ルールと共にこれらの変数を使用し、イベントを処理できます。

注: イベント処理およびイベント ルールに関する詳細については、「イベント設定ユーザ ガイド」を参照してください。

「ログ ファイル構文」で述べたように、ログ ファイル エントリには以下のコンポーネントが含まれます。

<MessagePrefix>%<MessageHeader><Additional_Information>

CA Spectrum は、名前がログ ファイル エントリの *<MessageHeader>* のテキストに一致する ParseMap ファイルを検索することにより、トラップを処理する ParseMap ファイルを識別します。 以下のログがログ ファイル エントリの例です。

```
2004-2-19 11:19:14 Local7.Info 172.19.38.36 Feb 19 09:14:50

%SNMP-I-SENT_TRAP、通知リンク アップを 192.168.32.44 に送信
```

エントリの *<MessageHeader>* 部分は SNMP-I-SENT_TRAP です。 そのため、CA Spectrum は SNMP-I-SENT_TRAP という名前の ParseMap ファイルを検索します。 トラップを生成するために設定する一意の *<MessageHeader>* を含むログ エントリごとに、ParseMap ファイルを作成します。

注: 多くの ParseMap ファイルが CA Spectrum で使用可能です。次のディレクトリで見つけることができます: *<$SPECROOT>*/SS/CsVendor/ParseMaps。

次の手順に従ってください:

1. 任意のテキスト エディタを使用して、新規テキスト ファイルを作成します。

   テキスト ファイルは編集できます。

2. テキスト ファイルの最初の行で、生成するイベントの新規イベント ファイル名を入力します。イベント ファイル名は Eventffff から始まり、xxxx で終了する必要があります。x は任意の有効な 16 進数です。

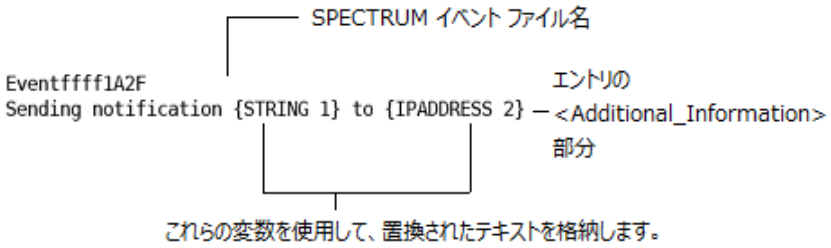
   たとえば、Eventffff1A2F および Eventffff1234 は有効なイベント ファイル名であり、Event012za8b は無効です。

3. テキスト ファイルに新しい行を追加します (Enter キーを押します)。

4. ログ ファイル エントリの *<Additional_Information>* 部分としてこの行を使用します。 イベント変数としてこのテキストの部分を指定し、イベント ルールを含むイベントを処理するために使用できます。

   データ タイプおよび整数を使用して、変数を指定します。有効なデータ タイプは、STRING、STRINGNOWS、INTEGER および IPADDRESS です。重要な情報については、「文字列データ タイプ使用ガイドライン (P. 78)」を参照してください。

以下のイメージでは、前のセクションで示されたログ エントリに有効な ParseMap ファイルについて説明します。変数 1 は、Uplink を文字列として格納します。変数 2 は、192.168.32.44 を IP アドレスとして格納します。



5. テキスト ファイルを *<$SPECROOT>*/SS/CsVendor/ParseMaps ディレクトリに保存します。 このテキスト ファイルの名前は、ログ ファイル エントリの *<MessageHeader>* 部分に一致する必要があります。 この例で、ファイル名は SNMP-I-SENT_TRAP です。

   注: ファイル名にファイル拡張子を含めません。

   ParseMap ファイルの最初の 2 行のみが処理されます。後続の行に含まれる情報は処理されませんが、情報として含めることができます。

詳細情報:

ログ ファイル構文 (P. 61)

ParseMap ファイルの例

以下の行のシーケンスは、SYS-0-MOD_TEMPMAJORFAIL という名前の CA Spectrum を提供する ParseMap ファイルの例です。 ParseMap ファイルは次のディレクトリで見つけることができます : *<$SPECROOT>*/SS/CsVendor/ParseMaps。

```
Event04bd1522

モジュール {STRING 1} メジャー温度しきい値を超えました

%SYS-0-MOD_TEMPMAJORFAIL: モジュール {STRING} メジャー温度しきい値を超えました
```

これは一致した syslog ファイルを示します。

```
Jul 28 10:56:42 [10.253.9.11.2.45] 7931: *Jul 28 10:50:47.271:
%SYS-0-MOD_TEMPMAJORFAIL: モジュール 100 メジャー温度しきい値を超えました
```

これはエージェントがトラップを生成しても、IP アドレス 10.253.9.11 のモデルに生成されるイベント Event04bd1522 を発生させません。

文字列データ タイプ使用ガイドライン

このセクションは、ParseMap ファイルでの文字列データ タイプの使用に関する重要な情報を提供します。

有効な文字列データ タイプ

「ParseMap ファイルの作成」で示されたとおり、以下のデータ タイプが変数に使用できます。

STRING

すべての文字列の文字が、次のリテラル、データ タイプまたは文字列の最後まで一致します。

STRINGNOWS

すべての文字列の文字が、次のスペース、リテラル、データ タイプまたは文字列の最後まで一致します。

INTEGER

任意の正の整数値に一致します。

IPADDRESS

任意の有効な IPv4 アドレスに一致します。

STRING 変数の空白

空白は STRING 変数の定義に有効な文字であるため、常に認識可能なパターンを含む複数の STRING トークンを区切ります。

たとえば、以下の ParseMap は*有効な*エントリです。

```
{STRING 1}, {STRING 2}
```

```
{STRING 1} {IPADDRESS 2} {STRING 3}
```

```
{STRING 1} リテラル テキスト {STRING 2}
```

```
{STRINGNOWS 1} {STRING 2}
```

ただし、結果として生じる正規表現があいまいになるため、これらのエントリは含めません。

```
{STRING 1}{STRING 2}

{STRING 2} {STRING 2}
```

イベント形式ファイルの作成

ParseMap ファイルで指定するイベント コードごとに、個別のイベント形式ファイルが必要です。 イベントがアサートされる場合、イベント形式ファイルのテキストがイベント ログに表示されます。 イベント形式ファイルを作成しているときに、イベント メッセージ テキストから生ずるイベントについてトラブルシュータが受信する情報の多くに留意してください。

テキスト エディタを使用してイベント形式ファイルを作成し、次のディレクトリにファイルを配置します： *<$SPECROOT>*/SG-Support/CsEvFormat。*<xxxxxxxx>* が ParseMap ファイルのイベントに与えられるイベント コードである場合、イベント形式ファイルは Event*<xxxxxxxx>* と命名される必要があります。たとえば、イベント コードが 0xffff1A2F のイベントがある場合、CA Spectrum は Eventffff1A2F という名前のイベント形式ファイルを使用します。

イベント メッセージのテキストを有益なものにするには、イベントの ParseMap ファイルに割り当てられた変数、およびすべてのイベント形式ファイルに利用可能なビルトイン変数を使用できます。

注: 利用可能なビルトイン変数を含めて、イベント形式ファイルを作成するための完全な手順については、「イベント設定ユーザ ガイド」を参照してください。

例: イベント形式ファイル

ParseMap ファイルによって生成されたイベントには、以下のイベント形式ファイルを使用します。

IP アドレスの変数は、データ タイプ O （オクテット）、および ParseMap ファイルから割り当てられる変数 1 を使用して挿入されます。デバイス名の変数は、データ タイプ s （文字列）、および ParseMap ファイルから割り当てられる変数 2 を使用して挿入されます。 ビルトイン変数 {d "%w- %d %m-, %Y - %T"}、{m}、{t}、および {e} は、イベントの日付、モデル名、モデル タイプ名、およびイベント ID を示します。

```
{d "%w- %d %m-, %Y - %T"} デバイス {m} のタイプ {t} が問題を報告しました。

IP アドレスは {S 1}、デバイス名は {S 2} です。 - (イベント [{e}])
```

イベントに基づいてアラームを生成

ParseMap ファイルで作成されたイベントの詳細な処理を指定できます。イベントに基づいてアラームを生成、またはイベント ルールの一部としてイベントを使用できます。 これを行うには、このイベントをアサートでき、各モデル タイプの EventDisp ファイルで適切なイベント処理を指定できるすべてのモデル タイプを決定します。 イベントが各モデル タイプに対して同じ方法で処理されるようにする場合、グローバル EventDisp ファイルのイベント処理を指定できます。

アラームがイベントに基づいて作成されるように指定している場合、アラームがアサートされると、OneClick コンソールに表示される想定される原因ファイルを作成します。

注: EventDisp および想定される原因ファイルの詳細については、「イベント設定ユーザ ガイド」を参照してください。

SpectroSERVER への変更の適用

新規または更新されたイベント形式および ParseMap ファイルをアクティブにするには、SpectroSERVER への変更を適用します。 これは、イベント設定エディタに示された更新コマンドを使用するか、コマンド ライン インターフェースを使用するか、SpectroSERVER を停止して再起動することによって実行できます。 これらの各方法に関する詳細については、「イベント設定ユーザ ガイド」を参照してください。

エージェント モデルへのイベント転送の有効化

エージェントのモデルを設定し、リモート ランドスケープ上のモデルにイベントを転送できます。 モデルの SBG_AlertForwardingEnabled (0x3dc000c) 属性を TRUE に設定します。

第 6 章: アプリケーション監視

SystemEDGE Application Insight Module（AIM）

SystemEDGE エージェントは、初期化されるときに Application Insight Module （AIM）をロードできるプラグイン アーキテクチャを備えています。 これらの AIM は、アプリケーション固有の意味的知識をサポートするために、拡張可能で柔軟な手法を提供します。

CA Spectrum は以下の AIM をサポートします。

- Apache Web サーバ
- Microsoft IIS
- DB2、Oracle、SQL Server および Sybase 用の CA Insight DPM

注: SystemEDGE AIM は、選択された SystemEDGE エージェントに対してコンポーネント詳細画面の［情報］タブから利用可能です。

さらに、CA Spectrum は Insight AIM によるトラップで送信されるアラームを報告します。 各 Insight AIM はそのタイプに一意のトラップを送信し、これで Insight AIM エージェント タイプを区別できます。 また、アラームごとの詳細情報には、データベース名、アラーム タイプおよびアラームの説明が含まれます。

Insight AIM アラーム タイプはエージェント タイプにより変化し、広範囲の通知条件をカバーします。これらの AIM アラームは CA Spectrum の他のアラームと全く変わらず、同じテーブルに表示され、同じ機能を提供します。

Apache Web サーバ

Apache 用の AIM では、Apache Web サーバのヘルスおよび可用性を監視できます。

このモジュールは SystemEDGE エージェントで動作し、以下の情報を提供します。

- Web サーバが受信している「ヒット」数。 毎日のボリュームを追跡でき、異常なトラフィック レベルまたはサービス拒否攻撃をウォッチする監視ポイントを設定できます。
- Web ログ ファイルおよび Web サーバ ファイルが消費しているスペースの量。
- アイドル サービスおよびアクティブなプロセス。 Apache Web サーバ プロセスがアイドル サービスを効果的に監視しているかを測定できます。アイドル サービス数が低すぎる場合は警告が表示され、また、アクティブなプロセス数を監視できます。
- Apache Web サーバが使用しているシステム リソース（CPU およびメモリ）の割合。
- Web サーバのボトルネックが CPU、メモリ、ディスクまたはネットワークに関連付けられるかどうか。

Microsoft IIS

Microsoft IIS 用の AIM は、Microsoft IIS アプリケーションおよびシステム リソースでのその使用を監視するために必要な情報を提供します。

このモジュールは SystemEDGE エージェントで動作し、以下のタスクを実行できます。

- Microsoft IIS およびそのサービス（Web、FTP、SMTP および NNTP）の可用性を監視する。
- 失敗したサービスを自動的に再起動する。
- CPU （中央演算処理装置）使用率、ディスク領域、メモリなどのシステム リソースで Microsoft IIS が重大なレベルを消費し始めたかどうかを判断する。
- Web、FTP、SMTP、および NNTP サービス全体で、セキュリティ、システム、およびアプリケーション イベントのログを監視する。
- Web 404（ページが見つかりません）エラーおよび ASP スクリプト エラーなど、アクティブ サーバ ページ （ASP）、CGI （Common Gateway Interface）、およびインターネット サーバ アプリケーション プログラム インターフェース（ISAPI）アプリケーション拡張ページ全体のエラー統計を検出します。

CA Insight DPM

Insight AIM は、リアルタイムの管理および長期トレンドや容量の計画のために、DBMS タイプのパフォーマンス、設定、可用性およびヘルスに関する重要な情報を提供します。

Insight AIM は、サポートされる各 DBMS タイプに固有の変数を含む管理情報ベース（MIB）が実装されています。 以下の DBMS タイプをサポートしています。

- DB2
- Oracle
- SQL Server
- Sybase

第 7 章: CA Unicenter NSM エージェント

このセクションには、以下のトピックが含まれています。

CA Unicenter NSM エージェントの概要

CA Spectrum 管理モジュール SM-CAI1000 は、OneClick インターフェースからの CA Unicenter NSM エージェントを管理するために CA Spectrum でサポートされます。 この管理モジュールは、NSM エージェントの CA Unicenter バージョン r11 および 3.1 に対して、以下の CA Spectrum 機能を提供します。

- CA Spectrum は、NSM エージェント ホストに一意のデバイス モデル タイプを提供します。 このサポートでは、NSM エージェントおよび CA Spectrum 内のそれらのホスト デバイスの管理を可能にします。
- OneClick インターフェースには、NSM エージェントによって収集されたシステム情報が表示され、NSM エージェント ホスト上のプロセス、ログ ファイルおよびファイル監視を設定できます。

  注: プロセス監視は CA Spectrum のモデルです。そのため、監視モデルのアラーム状態を設定し、監視モデル イベント上のレポートおよび CA Spectrum Report Manager アプリケーションを含むアラームを生成し、CA Spectrum サービス レベル アグリーメント管理設定に監視モデルを組み込むことができます。

  NSM エージェントのプロセス監視機能の詳細については、「プロセス監視 (P. 17)」を参照してください。

  NSM エージェントのログ ファイルおよびファイル監視機能の詳細については、「NSM エージェントのログ ファイル監視の作成 (P. 63)」を参照してください。

- CA Spectrum は、NSM エージェント トラップの受信によってイベントおよびアラームを生成します。

- CA Spectrum は、NSM エージェント ホスト デバイスのベンダー固有インターフェースに詳細を提供します。
- CA Spectrum は、OneClick 内のエージェント ダッシュボードなどの CA Unicenter Web 管理インターフェース用に起動ポイントを提供します。

NSM エージェントのサポート

CA Spectrum 管理モジュール SM-CAI1000 は、以下のテーブルでリスト表示される CA Unicenter NSM r11 および NSM 3.1 システム エージェントをサポートします。

NSM r11 システム エージェント	NSM 3.1 システム エージェント
UNIX システム エージェント（caiUxsA2）	UNIX システム エージェント（caiUxOs）
Windows システム エージェント（caiWinA3）	Windows システム エージェント（caiW2kOs）
Active Directory サービス エージェント（caiAdsA2）	Active Directory サービス エージェント（caiAdsA2）
ログ エージェント（caiLogA2）	ログ エージェント（caiLogA2）
パフォーマンス エージェント（hpxAgent）	パフォーマンス エージェント（hpxAgent）

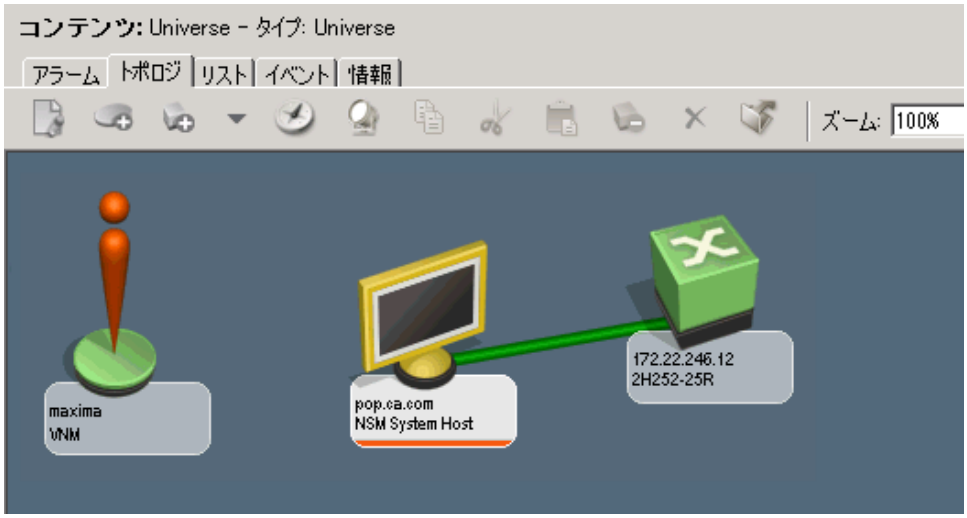
以下のテーブルは、サポートされる NSM エージェントや Unicenter バージョン、および CA Spectrum モデル タイプによって、さらに詳細な情報を提供します。

注: UNIX モデル タイプ（Host_NSMSysUnix）も、Solaris および Linux エージェントをモデリングするために使用できます。

Unicenter バージョンおよびエージェント プラットフォーム	説明	CA Spectrum のモデル タイプ
UNIX システム エージェント（caiUxsA2）	NSM r11 の Unix、Solaris および Linux エージェント サポートを提供する	Host_NSMSysUnix
Windows システム エージェント（caiWinA3）	NSM r11 の Windows エージェント サポートを提供する	Host_NSMSysWin

Unicenter バージョンおよびエージェント プラットフォーム	説明	CA Spectrum のモデル タイプ
UNIX システム エージェント（caiUxOs）	NSM 3.1 の Unix エージェント サポートを提供する	Host_NSMv3SysUnix
Windows システム エージェント（caiW2kOs）	NSM 3.1 の Windows エージェント サポートを提供する	Host_NSMv3SysWin

以下のイメージは、OneClick の［トポロジ］タブでモデリングされた NSM エージェント ホストの例を示したものです。



NSM MIB サポート

CA Spectrum は、CA Unicenter NSM エージェント管理モジュールを含む CA のベンダー固有 Unicenter NSM MIB をサポートします。NSM エージェント MIB 情報の詳細については、「CA Unicenter ネットワークおよびシステム管理 MIB リファレンス」ドキュメントを参照してください。

NSM MIB：

- caiUxsA2
- caiWinA3
- caiLogA2
- caiAdsA2
- hpxAgent
- caiUxOs
- caiW2kOs

CA Spectrum での NSM エージェントのモデリング

NSM エージェントは CA Spectrum ディスカバリを使用して、自動的に検出およびモデリングできます。または、手動でモデリングすることもできます。CA Spectrum で NSM エージェントをモデリングする場合、以下のファクタを考慮してください。

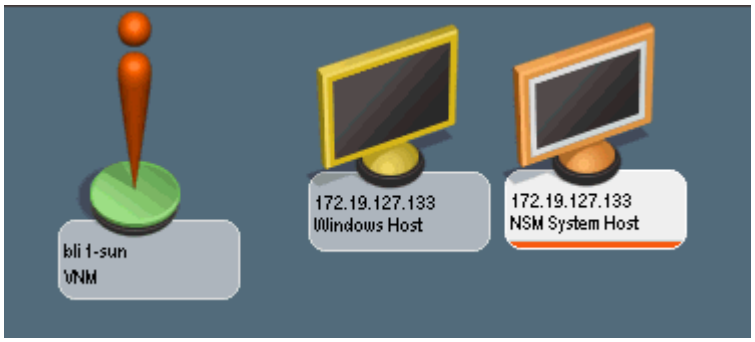
- 追加の SNMP エージェントを実行する NSM エージェント ホスト
- NSM Web ポータルにアクセスするためのモデリングの考慮事項

注: モデリングの詳細については、「IT インフラストラクチャのモデリング/管理 - 管理者ガイド」を参照してください。

追加の SNMP エージェントを実行する NSM エージェント ホスト

CA Spectrum で NSM エージェントをモデリングおよび管理する場合、ホスト デバイス上で実行されているその他のエージェントを認識します。また、ディスカバリ中に CA Spectrum によって検出およびモデリングすることもできます。これは NSM エージェントが、標準的な SNMP ポート 161 ではなく、デフォルトの SNMP 通信用 UDP ポート 6665 を使用するためです。

たとえば、Windows ワークステーションがポート 6665 にバインドされた NSM エージェント、およびポート 161 にバインドされた Microsoft SNMP エージェントを実行している場合、CA Spectrum はデバイス（NSM システム ホスト デバイス モデルおよび Windows ホスト デバイス モデル）に 2 つのモデルを作成します。以下のイメージに示されているとおりです。



このシナリオでは、以下の理由で貧弱なパフォーマンスを作成する場合があります。

- CA Spectrum での不必要な重複したモデル。
- ネットワークおよび CA Spectrum パフォーマンスを軽減できる冗長 SNMP トラフィックおよびポーリング。
- パフォーマンス データを提供している複数の管理があるため、エージェント ホスト マシンのパフォーマンスの縮小。

このシナリオを回避する方法

- ディスカバリおよびモデリングの前に、システムを管理するために使用するエージェント以外のすべての管理エージェントを停止および削除します。このクリーンアップは、同じホストに対して CA Spectrum に複数のモデルを作成および管理しないようにします。
- 任意のホスト システム上で複数のエージェントを実行する必要のある場合、CA Spectrum で管理するエージェントのみを手動でモデリングすることを検討します。

NSM Web ポータルにアクセスするためのモデリングの考慮事項

NSM Web ポータルおよび OneClick でのレポート起動ポイントにアクセスするには、IP アドレスではなくネーム サービスを使用して、CA Spectrum の NSM エージェントを最初にモデリングする必要があります。

注: OneClick でデバイスをモデリングする詳細については、「IT インフラストラクチャのモデリング/管理 - 管理者ガイド」を参照してください。

NSM エージェント ホストがネーム サービスの代わりに IP によってすでにモデリングされている場合は常に、モデルを削除し、CA Spectrum モデル名を設定し、手動でエージェントを再モデリングできます。

手動でエージェントを再モデリングする方法

1. ［トポロジ］タブで IP の名前を付けられた NSM エージェント デバイス モデルを右クリックし、［削除］をクリックします。

   モデルは CA Spectrum から削除されます。

2. トポロジ ビューで［VNM］アイコンを右クリックし、［コンポーネント詳細］をクリックします。

   ［コンポーネント詳細］ウィンドウが VNM のコンテキストで表示されます。

3. VNM の［コンポーネント詳細］ウィンドウの［情報］タブで、［SpectroSERVER コントロール］サブビューを展開します。

4. VNM の［モデル ネーミング順序］を変更するために［順序の設定］をクリックします。

   ［順序の設定］ダイアログ ボックスが表示されます。

5. ネーム サービスを選択し、上矢印ボタンを使用してリストの上部に移動させ、［OK］をクリックします。

   ［順序の設定］ダイアログ ボックスが閉じます。

6. OneClick トポロジ ビューで、IP ボタンによる新規モデルの作成を使用して、NSM エージェント ホストを再モデリングします。

   新規 NSM エージェント モデルはデバイスのネーム サービスで命名されます。

CA Spectrum の NSM エージェント インターフェース サポート

NSM エージェントは標準的な MIB-II インターフェース テーブルをサポートしませんが、代わりに関連する CA MIB で定義されたベンダー固有インターフェース テーブルを使用します。 この動作のために、NSM エージェント管理モジュールは、ベンダー固有 NSM NIB オブジェクトに基づいたインターフェース サポートを提供するために設計されています。 以下のテーブルは、MIB-2 属性および対応するベンダー固有 NSM MIB オブジェクトの相関を提供します。

MIB-2 属性	NSM r11 Windows OS エージェント（caiWinA3）属性	NSM 3.1 Windows OS エージェント（caiW2kOs）属性	NSM r11 Unix OS エージェント（caiUxsA2）属性	NSM 3.1 Unix OS エージェント（caiUxOs）属性
ifIndex	winEHIfIndex	w2kEHIfIndex	uxsEHIfIndex	ux3EHIfIndex
ifType	winEHIfType	w2kEHIfType	uxsEHIfType	ux3EHIfType
ifSpeed	winEHIfSpeed	w2kEHIfSpeed	uxsEHIfSpeed	ux3EHIfSpeed
ifPhysAddress	winEHIfPhysAddress	w2kEHIfPhysAddress	uxsEHIfPhysAddres	ux3EHIfPhysAddress
ifDescr	winEHIfDescr	w2kEHIfDescr	uxsEHIfDescr	ux3EHIfDescr
IpAdEntAddr	winEHIfIpAdEntAddr	w2kEHIfIpAdEntAddr	uxsEHIfIpAdEntAddr	ux3EHIfIpAdEntAddr
ifAdminStatus	winEHIfAdminStatus	w2kEHIfAdminStatus	uxsEHIfAdminStatus	ux3EHIfAdminStatus
ifOperStatus	ifOperStatus	w2kEHIfOperStatus	uxsEHIfOperStatus	ux3EHIfOperStatus
ifLastChange	winEHIfLastChange	w2kEHIfLastChange	uxsEHIfLastChange	ux3EHIfLastChange

NSM エージェント情報の表示

CA Spectrum OneClick は、NSM システム エージェントが収集する情報の可視性を提供します。システム リソース サブビュー セクションのプロセス、ログ ファイルおよびファイル監視を設定できます。 他のビューでは、ベンダー固有 MIB 値から利用可能な読み取り専用情報を提供します。

OneClick の NSM エージェント情報にアクセスできます。 この手順では、ディスカバリまたは手動のモデリングのいずれかで、ネットワークに NSM エージェントをすでにモデリングしたと仮定します。

次の手順に従ってください:

1. ［トポロジ］タブでモデリングされた［NSM エージェント デバイス］アイコンを選択します。

   コンポーネント詳細画面は、選択された NSM エージェント モデルの［情報］タブを表示します。

2. システム リソース サブビューを展開します。

   NSM エージェント固有の情報が表示されます。

詳細情報:

CA Spectrum での NSM エージェントのモデリング (P. 90)

NSM エージェント ダッシュボードおよびパフォーマンス レポート

CA Unicenter NSM エージェント管理モジュールは、NSM エージェント ダッシュボードおよびパフォーマンス レポーティングに使用する OneClick 起動ポイントを提供します。 OneClick 管理ページから利用可能な NSM 設定ユーティリティを使用して、起動ポイントを設定します。

注: 起動ポイントへのアクセスには、IP アドレスではなくデバイス名によって CA Spectrum の NSM エージェントをモデリングする必要があります。

OneClick の NSM 起動ポイントには以下のものが含まれます。

- NSM エージェント ダッシュボード
- NSM パフォーマンス レポート

NSM ユーザ インターフェースを起動する CA Spectrum の設定

CA Spectrum からの Unicenter NSM ダッシュボードおよびレポート サーバのコンテキストに応じた起動を有効にするには、OneClick Web サーバ上の環境に値を設定します。 OneClick 管理ページで NSM 設定ページを使用して、値を設定します。

CA Spectrum は、*<Install Area>*/custom/topo/config/ ディレクトリで、デフォルトの *<Install Area>*/tomcat/webapps/spectrum/WEB-INF/topo/config/nsm-system-config.xml ファイルのカスタマイズされたバージョンに設定値を保存します。 アップグレードする場合、このディレクトリは上書きされないため、NSM 設定値は保持されます。

Unicenter NSM ダッシュボードを起動するために、カスタム値を設定できます。

次の手順に従ってください:

1. OneClick ホーム ページで［管理］をクリックします。

   ［管理ページ］が開きます。

2. 左側のパネルで［NSM 設定］をクリックします。

   ［NSM 設定］ウィンドウが開きます。

3. 必要に応じてフィールドにデータを入力します。

   NSM ダッシュボード サーバ名

   NSM ダッシュボード サーバ（server.domain.extension）を示します。

   NSM ダッシュボード サーバ ポート

   デフォルト値は、9090 です。

   NSM レポート サーバ

   NSM レポート サーバ（server.domain.extension）を示します。

   NSM レポート ポート

   デフォルト値は、9090 です。

4. ［保存］をクリックします。

5. 変更を有効にするには、実行中の OneClick クライアントを再起動します。

   カスタム値が設定されます。

エージェント ダッシュボードの起動

エージェント ダッシュボードを起動するには、OneClick トポロジ ビューの NSM エージェント デバイス モデルを右クリックし、起動する NSM エージェント ダッシュボードを選択します。

Unicenter ダッシュボード Web インターフェースが開きます。

パフォーマンス レポーティングの起動

OneClick は、NSM モデルの各タイプにパフォーマンス レポーティング メニューの選択を提供します。 NSM デバイス モデルを右クリックして、パフォーマンス レポーティング メニューの選択は利用可能です。 このメニューの選択で、Unicenter WRS ベースのシステム パフォーマンス レポートを起動します。

OneClick から起動される NSM パフォーマンス レポーティングについては、以下の各条件が真である必要がある。

- hpxAgent は NSM エージェント ホストにインストールされる必要がある。
- 接続が必要な WRS には、システム パフォーマンス レポーティングをインストールされている必要がある。
- また、WRS は任意のホスト サーバにデータを供給するために接続される必要がある。
- 「NSM ユーザ インターフェースを起動する CA Spectrum OneClick の設定 (P. 95)」で述べたように、OneClick は設定される必要がある。

レポーティング Web インターフェースを起動するには、NSM ホストを表す NSM エージェント デバイス モデルを右クリックし、[NSM パフォーマンス レポート] をクリックします。

Unicenter Web レポーティング サーバ インターフェースが開きます。

Trap-to-Alarm マッピング

CA Unicenter NSM エージェント管理モジュールは、CA Spectrum イベントおよびアラーム処理に NSM エージェント トラップを統合します。

CA Spectrum は、システムおよびパフォーマンス エージェントを含め、NSM エージェントによって送信されるトラップを処理します。 受信された警告または重大の状態を含む各 NSM システムまたはパフォーマンス エージェント トラップについては、CA Spectrum は以下のテーブルで示されるアラームを生成します。 CA Spectrum が関連する OK トラップを受信する場合、CA Spectrum は対応するアラームをクリアします。

CA Spectrum が受信する NSM トラップ	生成された CA Spectrum アラーム
警告トラップ	マイナー アラーム
重大トラップ	メジャー アラーム

トラップ処理は NSM エージェント モデル タイプに基づいています。各モデル タイプは、以下のテーブルで概説されるとおり、複数のエージェントのトラップを処理します。

モデル タイプ	エージェントのために処理するトラップ
Host_NSMSysUnix	caiUxsA2 caiLogA2 hpxAgent
Host_NSMSysWin	caiWinA3 caiLogA2 caiAdsA2 hpxAgent
Host_NSMv3SysUnix	caiUxOs caiLogA2 hpxAgent
Host_NSMv3SysWin	caiW2kOs caiLogA2 caiAdsA2 hpxAgent

イベント コードおよび想定される原因ファイル ID の範囲

以下のテーブルでは、NSM エージェント MIB に対するイベント コードおよび想定される原因ファイル ID のリストを示します。

NSM エージェント MIB	関連する CA Spectrum イベント コードおよび想定される原因ファイルの範囲
caiUxsA2	Event04ef0000 - Event04ef00e9 Prob04ef0002 - Prob04ef00e3
caiWinA3	Event04ef1000 - Event04ef10c7 Prob04ef1002 - Event04ef10c1
caiLogA2	Event04ef2000 - Event04ef2010 Prob04ef2002 - Prob04ef200e
caiAdsA2	Event04ef3000 - Event04ef3042 Prob04ef3002 - Prob04ef303e
hpxAgent	Event04ef4000 - Event04ef4008 Prob04ef4002 - Prob04ef4006
caiUxOs	Event04ef5000 - Event04ef5069 Prob04ef5002 - Prob04ef5067
caiW2kOs	Event04ef6000 - Event04ef6099 Prob04ef6002 - Prob04ef6095

CA Spectrum の NSM システム エージェント ステータス

NSM エージェント モデルのステータスを最新に保つには、CA Spectrum はデバイス ポーリング間隔に従って、定期的に 2 つの NSM システム エージェント MIB 属性をポーリングします。 デフォルトの間隔は、5 分（300 秒）です。

注: ポーリング間隔を変更する詳細については、「IT インフラストラクチャのモデリング/管理 - 管理者ガイド」を参照してください。

ポーリングされた属性は、任意の NSM システム エージェント ホスト上の警告または重大リソースの数を示します。 一方の属性は、NSM システム エージェントのリソース警告の合計数を表します。また、もう一方の属性は、重大リソースの合計数を表します。 任意の NSM システム エージェントの警告または重大リソースの数が 0 より大きい場合、CA Spectrum は適切なアラームを作成します。 属性の値がゼロの場合、このアラームはクリアされます。 以下のテーブルでは、サポートされる各モデル タイプに対してポーリングされた属性および生成されたアラームを示します。

モデル タイプ	ポーリングされた属性	リソース警告の合計数がゼロより大きい場合に生成されるイベント / マイナー アラーム ID	重大リソースの合計値がゼロより大きい場合に生成されるイベント / メジャー アラーム ID
Host_NSMSysUnix	uxsA2StatusGeneralTotalWarn uxsA2StatusGeneralTotalCrit	0x04ef00ea	0x04ef00ec
Host_NSMSysWin	winA3StatusGeneralTotalWarn winA3StatusGeneralTotalCrit	0x04ef10c8	0x04ef10ca
Host_NSMv3SysUnix	uxsStatusGeneral TotalWarning uxsStatusGeneral TotalCritical	0x04ef506a	0x04ef506c
Host_NSMv3SysWin	w2kStatusGeneral TotalWarn w2kStatusGeneral TotalCrit	0x04ef609a	0x04ef609c

注: ポーリングされたときに、リソース警告の合計数または重大リソースの合計値がそれぞれゼロである場合、これらのアラームはクリアされます。

付録 A: システムとアプリケーションの監視権限

このセクションでは、OneClick ユーザに対するシステムおよびアプリケーション監視に関連する権限のリストを示します。

注: 権限を設定する詳細については、「管理者ガイド」を参照してください。

システムとアプリケーションの監視

システムとアプリケーションの監視権限へのアクセスを制御します。この権限を選択解除すると、自動的に以下の権限を選択解除します。

ルール セットの管理

ユーザが監視ルール セットを作成することを可能にします。

ファイル システムの監視

ユーザがファイル システム監視ルールを作成することを可能にします。

プロセスの監視

ユーザがプロセス監視ルールを作成することを可能にします。