CA Performance Management Data Aggregator

管理者ガイド

2.4

ca technologies

CA Technologies 製品リファレンス

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

- CA Performance Management Data Aggregator （Data Aggregator）
- CA Performance Management Data Collector （Data Collector）
- CA Performance Center

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: 製品管理

このセクションには、以下のトピックが含まれています。

Data Repository の自動バックアップの設定方法（単一ノードおよびクラスタ へのインストール）

Data Repository をバックアップする必要が生じる場合があります。たとえば、Data Aggregator をアップグレードする前、または cron ジョブによる自動バックアップを設定する前に Data Repository をバックアップします。Data Repository をバックアップすると、予期しない障害の場合にアクセス可能な Data Repository のコピーが用意できます。

重要: 初めて Data Repository をバックアップする際は、フル バックアップが行われます。 このフル バックアップは、存在する履歴データの量に応じて、完了までに時間がかかる場合があります。 初期バックアップが実行されると、その後にスケジュールされるバックアップは増分バックアップになります。 日単位バックアップの場合、増分バックアップには、過去 24 時間以内（たとえば、最終バックアップ後に経過した時間）に発生したデータベース アクティビティのみを含める必要があります。

フル バックアップの実行後に増分バックアップを実行するには、フル バックアップの実行時に指定したのと同じ snapshotName、および同じバックアップ ディレクトリを Vertica バックアップ スクリプトに指定します。 これらの名前を変更すると、フル バックアップが実行されます。

Vertica （データベース）は、データを格納するためのデータ ファイルを作成します。 これらのファイルは、作成後に変更されることがありません。新しいファイルが作成されると古いファイルが削除されます。 この方法により、Data Repository のバックアップに、他のコンピュータへの高速なファイル レプリケーションをサポートする標準的な rsync ユーティリティを使用できます。 rsync の詳細については、http://everythinglinux.org/rsync/ を参照してください。

Data Repository の自動バックアップを設定するには、以下の手順に従います。

1. バックアップの考慮事項を確認します (P. 11)。
2. 以下の手順のいずれかを実行します。
   - リモート ホストへの Data Repository のバックアップを設定します (P. 12)。
   - 同じホストへの Data Repository のバックアップを設定します (P. 15)。
3. Data Repository を設定します (P. 17)。

Data Repository バックアップの考慮事項

Data Repository をバックアップする前に、以下の情報を考慮します。

- Data Repository をバックアップするときは、Data Repository または Data Aggregator を停止する必要はありません。
- バックアップは、データベースのバックアップに使用する設定ファイルの指定した場所に格納されます。バックアップ ファイルが含まれるディレクトリには、そのディレクトリにバックアップされる各ノードのサブディレクトリがあります。 サブディレクトリには、バックアップ スナップショットの名前が付いたディレクトリが含まれます。 スナップショット名は設定ファイルの snapshotName オプションを使用して設定されます。
- 増分バックアップは毎日実行します。バックアップ処理には大量のリソースが必要になるため、業務時間外に実行することをお勧めします。
- Data Repository は、リモート ホストまたは同じホストにバックアップできます。

  注: 同じホストにバックアップする場合は、カタログやデータのディレクトリによって使用されるパーティションとは異なるパーティションにバックアップを保存してください。

- フル バックアップは週単位で実行します。日単位のスナップショットはフル バックアップに依存します。任意のスナップショットへのリストアは、フル バックアップの整合性に依存します。 フル バックアップに関する以下の情報を考慮します。
  - 週単位のフル バックアップそれぞれについて、.ini ファイルを 1 つ作成します。 特定のスナップショットへリストアするには、.ini ファイルが必要です。 .ini ファイルに一意の名前を付け、この .ini ファイルを初めて実行したときに、フル バックアップが実行されます。 このため、ディスク容量に注意することが大切です。 ディスク容量に余裕がない場合は、保存期間を現在の週に加えて 1 ～ 2 週間にすることを推奨します。 この解決方法には、毎週、週初めに最も古い週のバックアップを削除するという追加のメンテナンス処理が必要です。
  - /opt/vertica/bin/vbr.py -setupconfig コマンドを実行して新しい .ini ファイルを生成するか、現在の .ini ファイルのバージョンをコピーして、フル バックアップを行います。 既存の .ini ファイルを新しい .ini ファイルにコピーし、次に、新しい .ini ファイル内の「snapshotName」の値を変更します。

詳細:

Data Repository の自動バックアップの設定方法（単一ノードおよびクラスタ へのインストール） (P. 10)

リモート ホストへの Data Repository バックアップの設定（単一ノードおよびクラスタ へのインストール）

Data Repository はリモート ホストにバックアップできます。

各 Data Repository ノードが、バックアップ用に独自のリモート ホストを持つことを推奨します。 たとえば、Data Repository ノードを 3 つ持つクラスタ環境では、Data Repository ホストはそれぞれ専用のバックアップ ホストを持つ必要があります。

重要: クラスタ環境では、クラスタ ノードごとのバックアップで使用する各リモート ホストで、以下の手順を実行してください。 クラスタ内の各ノードをバックアップする必要があります。

以下の手順に従います。

1. コンソールを開き、リモート バックアップ ホストとして使用するコンピュータに root ユーザとしてログインします。
2. リモート バックアップ ホストで Vertica Linux データベース管理者ユーザを作成するには、以下のコマンドを入力します。

   ```
   useradd database_admin_user -s /bin/bash
   ```

   例：

   ```
   useradd dradmin -s /bash/bin
   ```

   注: Data Repository ホストに存在するリモート バックアップ ホストに、同じ Vertica Linux データベース管理者ユーザを作成します。 Data Repository ホストとリモート バックアップ ホストが、LDAP または Network Information Service （NIS）に接続されていないこと、および同じ Vertica Linux データベース管理者ユーザを共有していることを確認してください。
3. Vertica Linux データベース管理者ユーザを作成するには、以下のコマンドを入力します。

   ```
   passwd database_admin_user
   ```

   例：

   ```
   passwd dradmin
   ```
4. リモート バックアップ ホストに Vertica ディレクトリを作成するには、以下のコマンドを入力します。

   ```
   mkdir /opt/vertica/bin
   ```

   ```
   mkdir /opt/vertica/oss
   ```
5. Vertica ディレクトリの所有者を変更するには、以下のコマンドを入力します。

   ```
   chown -R dradmin /opt/vertica
   ```

6. リモート バックアップ ホストからログアウトします。
7. リモート バックアップ ホストの Data Repository ホストにパスワードなしの ssh を設定するには、以下の手順に従います。
   a. コンソールを開き、Vertica Linux データベース管理者ユーザとして Data Repository ホストにログインします。
   b. 以下のコマンドを入力します。

      ```
      ssh-keygen -N "" -t rsa -f ~/.ssh/id_rsa
      cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys2
      chmod 644 ~/.ssh/authorized_keys2
      ```

   c. リモート バックアップ ホストの認可されたキーのリストに Vertica Linux データベース管理者ユーザ公開鍵をコピーするには、以下のコマンドを入力します。

      ```
      ssh-copy-id -i dradmin@backuphost
      ```

   d. コンソールを開き、Vertica Linux データベース管理者ユーザとしてリモート バックアップ ホストにログインします。
   e. Data Repository ホストからリモート バックアップ ホストに Vertica rsync および python ツールをコピーするには、以下のコマンドを入力します。

      ```
      scp dradmin@<drhost>:/opt/vertica/bin/rsync /opt/vertica/bin
      scp -r dradmin@<drhost>:/opt/vertica/oss/python /opt/vertica/oss
      ```

8. リモート バックアップ ホストに新しい /opt/vertica/bin/rsync ファイル ディレクトリと /opt/vertica/oss/python ディレクトリがあることを確認します。
9. リモート バックアップ ホストにバックアップ ディレクトリを作成するには、以下のコマンドを入力します。

   ```
   mkdir backup_directory
   ```

   backup_directory

   Data Repository をバックアップするディレクトリを指定します。大量の空きスペースがあるディスク パーティション上のバックアップ ディレクトリを選択します。 これらのディレクトリにデータベース管理者ユーザによる書き込みができない場合は、chown および chmod コマンドを使用して、このユーザにディレクトリへのアクセス権を付与します。

   注: クラスタ インストールでは、データベースをバックアップする前に、バックアップ ディレクトリを作成します。 ホストごとに異なるバックアップ ディレクトリを選択できます。

例：

```
mkdir ~dradmin/backups
```

詳細:

Data Repository の自動バックアップの設定方法（単一ノードおよびクラスタ へのインストール） (P. 10)

同じホストへの Data Repository バックアップの設定（単一ノードおよびクラスタへのインストール）

Data Repository は同じホストへバックアップできます。クラスタ環境では、クラスタ内の各ノードをバックアップする必要があります。 ホストごとに異なるバックアップ ディレクトリを選択できます。

以下の手順に従います。

1. データベース管理者ユーザの Linux ユーザ アカウントとして Data Repository にログインします。

   注: クラスタ インストールでは、クラスタに含まれている 3 つのホストのいずれからでも Data Repository にログインできます。

2. データベース管理者ユーザの Linux ユーザ アカウントに、パスワードなしの ssh キーが設定されていることを確認してください。

   注: クラスタ インストールでは、クラスタに含まれている各ホストに、パスワードなしの ssh キーを設定する必要があります。

   以下の手順に従います。

   a. パスワードなしの ssh キーが設定されているかどうかを確認するため、以下のコマンドを入力します。

      ```
      ssh hostname ls
      ```

      ホスト名

      Data Repository がインストールされているホストの名前を示します。

      パスワードなしの ssh キーがセットアップされている場合、パスワード入力は要求されません。これ以外の操作は必要ありません。

b. パスワードの入力を求められる場合は、プロンプトを無視して Ctrl + C キーを押します。 パスワードなしの ssh キーを持つデータベース管理者ユーザの Linux ユーザ アカウントをセットアップするため、以下のコマンドを入力します。

```
ssh-keygen -N "" -t rsa -f ~/.ssh/id_rsa
cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys2
chmod 644 ~/.ssh/authorized_keys2
```

パスワードを求められないことを確認するには、以下のコマンドを再入力します。

```
ssh hostname ls
```

ホスト名

Data Repository がインストールされているホストの名前を示します。

重要: パスワードなしの ssh キーを設定しないと、Data Repository をバックアップできません。バックアップを同じコンピュータに保存する場合でも、パスワードなしの ssh キーをセットアップします。

3. バックアップ ディレクトリを作成するため、以下のコマンドを入力します。

```
mkdir backup_directory
```

backup_directory

Data Repository をバックアップするディレクトリを指定します。大量の空きスペースがあるディスク パーティション上のバックアップ ディレクトリを選択します。 これらのディレクトリにデータベース管理者ユーザによる書き込みができない場合は、chown および chmod コマンドを使用して、このユーザにディレクトリへのアクセス権を付与します。

注: クラスタ インストールでは、データベースをバックアップする前に、バックアップ ディレクトリを作成します。 ホストごとに異なるバックアップ ディレクトリを選択できます。

例：

```
mkdir ~dradmin/backups
```

詳細:

Data Repository の自動バックアップの設定方法（単一ノードおよびクラスタ へのインストール） (P. 10)

Data Repository の設定

自動バックアップ用の Data Repository を設定します。

以下の手順に従います。

1. データベース管理者ユーザの Linux ユーザ アカウントとして Data Repository にログインします。

   注: クラスタ インストールでは、クラスタに含まれている 3 つのホストのいずれからでも Data Repository にログインできます。 ただし、バックアップを開始する Data Repository ホストにログインすることをお勧めします。

2. 再利用可能な設定スクリプトを作成して、Data Repository のバックアップとリストアに使用するには、データベース管理者ユーザの Linux ユーザ アカウントで以下のコマンドを入力します。

   ```
   /opt/vertica/bin/vbr.py --setupconfig
   ```

   注: 設定ファイルのターゲット ディレクトリで、このコマンドを起動することをお勧めします。 データベース管理者ユーザの Linux ユーザ アカウントは、そのディレクトリへの書き込み権限を有する必要があります。

   さまざまな質問およびステートメントに対して答えるように促されます。 質問とステートメントのリストおよびそれらへの典型的な応答の説明を以下に示します。

   - Snapshot name： バックアップ スナップショット名
   - Back up vertica configurations? [y/n]： y
   - Number of restore points (1)： 7

     注: リストア ポイントを 7 に指定すると、Data Repository を最新のバックアップ、または過去 7 つの増分バックアップのいずれかにリストアできます。 リストア ポイントを 1 に設定した場合、Data Repository は最新のバックアップ、または直前の増分バックアップにのみリストアできます。 リストア ポイントの上限に到達すると、最も古いバックアップが削除されます。 リストア ポイントの数以上を保存するには、リストア ポイントを増やすか、設定ファイル内のスナップショット名を変更してください。 ただし、スナップショット名を変更すると一連の新たなフル バックアップが開始され、バックアップに必要なディスク領域が倍になります。

- Specify objects (no default)：値を指定せずに Enter キーを押して、すべてのオブジェクトがバックアップされるようにします。
- Vertica user name (dradmin)： Enter キーを押してデフォルトを受け入れます。
- Save password to avoid runtime prompt ? (n) [y/n]： y
- Password to save in vbr config file (no default)： 入力を求められた場合、パスワードを入力します。

  注: このパスワードは、Vertica 内のデータベース管理者アカウントのデータベース パスワードと一致する必要があります。
- Backup host name (no default)： バックアップ用のホスト名

  注: クラスタをバックアップしている場合、クラスタ内の各ノードに一致するホスト名の入力を求められます。 クラスタ内の各ノードをバックアップする必要があります。
- Backup directory (no default)： Data Repository のバックアップ先のディレクトリ パス

  注: クラスタをバックアップしている場合、クラスタ内の各ノードのバックアップ ディレクトリの入力を求められます。 クラスタ内の各ノードをバックアップする必要があります。
- Config file name (snapshot name.ini)： Enter キーを押してデフォルトを受け入れます。

  .ini ファイルを作成しているディレクトリに対する書き込み権限があることを必ず確認してください。.ini ファイルへのフル パスを入力しない場合、/opt/vertica/bin/vbr.py（setupconfig コマンド）を実行したディレクトリにファイルが保存されます。

  重要: 生成される設定ファイルにはクリア テキスト パスワードが含まれます。
- Change advanced settings? (n) [y/n]： n

  メッセージが表示され、vbr 設定が「スナップショット名.ini」という名前の設定ファイルに保存されたことを示します。

3. Data Repository をバックアップします。以下のコマンドを入力します。

   ```
   /opt/vertica/bin/vbr.py --task backup --config-file
   configuration_directory_path_filename
   ```

   configuration_directory_path_filename

   以前に作成した設定ファイルのディレクトリ パスおよびファイル名を指定します。 このファイルは、バックアップ ユーティリティを実行した場所（/opt/vertica/bin/vbr.py）にあります。

   例：

   ```
   /opt/vertica/bin/vbr.py --task backup --config-file
   /home/vertica/vert-db-production.ini
   ```

   ホストの信ぴょう性に関するプロンプトが表示された場合は、「はい」と回答します。

   注: クラスタ インストールでは、クラスタに含まれているホストのいずれかにのみ、この手順を実行します。

   Data Repository がバックアップされます。

4. （オプション）将来の手動バックアップに備えて Data Repository のパスワードをクリア テキストで保持しない場合は、以下の手順に従います。

   a. [Database] セクションに以下の行が存在することを確認します。

      ```
      dbPromptForPassword = True
      ```

   b. [Database] セクションから以下の行を削除します。

      ```
      dbPassword = password
      ```

   注: 自動バックアップでは、対応するパスワードが指定された dbPassword 行を設定ファイルに残しておく必要があります。dbPromptForPassword を False に設定します。

5. Data Repository の日単位の自動バックアップ（推奨します）をセットアップするには、以下の手順に従います。

   a. 任意のテキスト エディタを開いて、新しいラッパー シェル スクリプトを作成します。

b. ラッパー シェル スクリプトのコンテンツには、以下の 1 行を含める必要があります。

```
/opt/vertica/bin/vbr.py --task backup --config-file
configuration_directory_path_filename
```

configuration_directory_path_filename

以前に作成した設定ファイルのディレクトリ パスおよびファイル名を指定します。このファイルは、バックアップ ユーティリティを実行した場所（/opt/vertica/bin/vbr.py）にあります。

例：

```
  /opt/vertica/bin/vbr.py --task backup --config-file
/home/vertica/vert-db-production.ini
```

c. コンテンツを backup_script.sh という名前の新しいファイルとして、指定した場所に保存します。

例：

```
/home/vertica/backup_script.sh
```

d. 以下のコマンドを入力して、スクリプトを実行するための権限を変更します。

```
chmod 777 location_backup_script.sh/backup_script.sh
```

例：

```
chmod 777 /home/vertica/backup_script.sh
```

e. データベース管理者ユーザの Linux ユーザ アカウントで、以下のコマンドを入力します。

```
crontab -e
```

f. 作成したバックアップ スクリプトを実行する cron ジョブを追加します。

注: 毎日の混雑していない時間にスクリプトを実行する cron ジョブを作成することをお勧めします。

例：

```
00 02 * * *   /home/vertica/backup_script.sh >/tmp/backup.log  2>&1
```

この例の cron ジョブは、毎日の午前 02:00 にバックアップ スクリプトを実行します。

重要: 初めて Data Repository をバックアップする際は、フル バックアップが行われます。 このフル バックアップは、存在する履歴データの量に応じて、完了までに時間がかかる場合があります。初期バックアップが実行されると、その後にスケジュールされるバックアップは増分バックアップになります。 日単位バックアップの場合、増分バックアップには、過去 24 時間以内（たとえば、最終バックアップ後に経過した時間）に発生したデータベース アクティビティのみを含める必要があります。

Data Repository のリストア

バックアップした Data Repository をリストアできます。この手順は、データベース管理者ユーザが sudoers ファイルの一部であることを前提にしています。

注: 通常、Data Repository は、バックアップ元コンピュータにリストアされます。 しかし、Data Repository を異なるコンピュータにリストアすることも できます。 リストア先コンピュータは、Data Repository のバックアップ元コンピュータと同様に設定しておく必要があります。 クラスタ環境では、リストア先の各コンピュータは、各 Data Repository ノードのバックアップ元コンピュータと同様に設定しておく必要があります。

以下の設定は必ず同じにしてください。

- IP アドレス
- ホスト名
- カタログ ディレクトリとデータ ディレクトリ
- カタログ ディレクトリとデータ ディレクトリの権限
- Vertica Linux データベース管理者のユーザ認証情報
- データベース管理者のユーザ アカウント認証情報
- データベースのユーザ アカウント認証情報

以下の手順に従います。

1. Data Collector がインストールされているコンピュータに、root ユーザまたは特定のコマンド セットへのアクセス権を持つ sudo ユーザとしてログインし、Data Aggregator に関連付けられたすべての Data Collector ホストを停止します。コマンド プロンプト ウィンドウを開き、以下のコマンドを入力します。

   ```
   service dcmd stop
   ```

   Data Collector ホストが停止します。

2. Data Aggregator がインストールされているコンピュータに、特定のコマンド セットへのアクセス権を持つ root ユーザまたは sudo ユーザとしてログインし、Data Aggregator を停止します。 コマンド プロンプト ウィンドウを開き、以下のコマンドを入力します。

   ```
   service dadaemon stop
   ```

   注: 特定のコマンド セットへのアクセス権を持つ sudouser の作成の詳細については、「Data Aggregator インストール ガイド」を参照してください。

   Data Aggregator が停止されます。

3. Data Repository に使用するデータベース サーバに、（root ユーザではなく）データベース管理者ユーザとしてログインします。

4. 以下のコマンドを入力します。

   ```
   /opt/vertica/bin/adminTools
   ```

   ［Administration Tools］ダイアログ ボックスが表示されます。

5. ［(4) Stop Database］を選択します。

6. データベース名の隣のスペース バーを押し、［OK］を選択して Enter キーを押します。

   データベース パスワードの入力を促すプロンプトが表示されます。

7. データベース パスワードを入力し、Enter キーを押します。

   Data Repository が停止します。

   注: Data Repository が停止しない場合、［(7) Advanced Tools Menu］の［(2) Stop Vertica on Host］を選択します。

8. ［Exit］を選択して Enter キーを押します。
9. Data Repository バックアップのリストア準備を行うには、Data Repository で使用しているデータベース サーバに、データベース管理者ユーザの Linux ユーザ アカウントとしてログインします。

   Data Repository の自動バックアップを設定したとき、環境設定ファイルに 7 個のリストア ポイントを設定しました。 Data Repository は最新のバックアップ、または過去 7 個の増分バックアップのいずれかにリストアできます。
10. 以下の手順のいずれかを実行します。
    a. Data Repository を最新のバックアップへリストアするには、以下のコマンドを入力します。

       ```
       /opt/vertica/bin/vbr.py --task restore --config-file
       configuration_directory_path_filename
       ```

       configuration_directory_path_filename

       バックアップ設定手順を実行したときに作成した設定ファイルのディレクトリ パスとファイル名を指定します。 このファイルは、バックアップ ユーティリティを実行した場所（/opt/vertica/bin/vbr.py）にあります。

       例：

       ```
       /opt/vertica/bin/vbr.py --task restore --config-file
       /home/vertica/vert-db-production.ini
       ```

       注: クラスタ インストールでは、クラスタに含まれている任意のホストからリストア タスクを実行できます。
    b. Data Repository を過去 7 個の増分バックアップのいずれかにリストアするには、以下のコマンドを入力します。

       ```
       /opt/vertica/bin/vbr.py --task restore --config-file
       configuration__directory_path_filename  --archive_name
       ```

       configuration_directory_path_filename

       ファイル名および、リストアするアーカイブの特定の設定ファイルへのディレクトリ パスを示します。 この設定ファイルは、バックアップ設定手順を実行したときに作成したものです。このファイルは、バックアップ ユーティリティを実行した場所（/opt/vertica/bin/vbr.py）にあります。

archive_name

リストアするリストア ポイントの名前を示します。 リストア ポイントの設定ファイルが示すバックアップ ディレクトリに移動します。 使用可能なリストア ポイントのすべてがリスト表示されます。 リストアするリストア ポイント用のアーカイブ名を決定します。

例：

```
/opt/vertica/bin/vbr.py --task restore --config-file myconfig.ini  --archive
20131020_170018
```

注: クラスタ インストールでは、クラスタに含まれている任意のホストからリストア タスクを実行できます。

11. Data Repository がインストールされているコンピュータに、データベース管理者ユーザ（root ユーザではなく）としてログインし、Data Repository を再起動します。 コマンド プロンプトを開き、以下の手順を実行します。
    a. 以下のコマンドを入力します。

       ```
       /opt/vertica/bin/adminTools
       ```

       ［Administration Tools］ダイアログ ボックスが表示されます。
    b. ［(3) Start Database］を選択します。
    c. データベース名の隣のスペース バーを押し、［OK］を選択して Enter キーを押します。

       データベース パスワードの入力を促すプロンプトが表示されます。
    d. データベース パスワードを入力し、Enter キーを押します。

       Data Repository が起動します。
    e. ［Exit］を選択して Enter キーを押します。
12. Data Aggregator がインストールされているコンピュータに、root ユーザ、または特定のコマンド セットへのアクセス権を持つ sudo ユーザとしてログインし、Data Aggregator を再起動します。 以下のコマンドを入力します。

    ```
    /etc/init.d/dadaemon start
    ```

    Data Aggregator が起動します。

13. Data Aggregator と関連付けられている Data Collector ホストをすべて再起動します。
    a. ［管理］-［データ ソース設定］を選択し、［Data Aggregator のデータ ソース］をクリックします。
    b. ［システム ステータス］メニューから［Data Collector］をクリックします。
    c. Data Aggregator と関連付けられている Data Collector ホストをすべて選択し、［開始］をクリックします。

    Data Collector ホストが起動されます。

Data Aggregator のバックアップ

Data Aggregator をバックアップする必要が生じる場合があります。たとえば、アップグレードの前に Data Aggregator と Data Repository をバックアップします。 これらのコンポーネントをバックアップすると、予期しない失敗が起きた場合にアクセスするための、ユーザ設定およびカスタム認定のコピーが用意されます。

Data Aggregator をバックアップするときは、Data Repository、Data Collector、または Data Aggregator サービスを停止する必要はありません。

バックアップは、ユーザが指定する Data Aggregator システムまたは別のバックアップ ホスト システム上の場所に格納されます。

注: このタスクを実行するには、root または sudo 権限が必要です。

以下の手順に従います。

1. コマンド プロンプトを開きます。
2. 同一または別のバックアップ ホスト システム上の安全な場所にバックアップ ディレクトリを作成するには、以下のコマンドを使用します。

   `mkdir` *`DA_Backup`*

   DA_Backup

   バックアップ ディレクトリのディレクトリ パスおよび名前を指定します。

3. 以下のコマンドをすべて使用して、DA_Backup 内のサブディレクトリを作成します。

   ```
   mkdir DA_Backup/deploy_backup
   mkdir DA_Backup/MIBDepot_backup
   mkdir DA_Backup/CustomDeviceType_backup
   ```

4. DA 上のファイルをバックアップするには、以下のコマンドを実行します。

   - このコマンドはカスタム ベンダー認定をバックアップします。 このディレクトリから local-jms-broker.xml および README ファイルをバックアップしないでください。

     ```
     cp Data Aggregator インストール ディレクトリ
     /apache-karaf-2.3.03/deploy/im.ca.com.*.xml DA_Backup/deploy_backup
     ```

   - このコマンドは、MIBDepot ディレクトリ内のカスタム MIB をすべてバックアップします。

     ```
     cp Data Aggregator インストール ディレクトリ/apache-karaf-2.3.0/MIBDepot/*
     DA_Backup/MIBDepot_backup
     ```

   - このコマンドはカスタム デバイス サブタイプの XML ファイルをすべてバックアップします。

     ```
     cp Data Aggregator インストール ディレクトリ
     /apache-karaf-2.3.0/custom/devicetype/DeviceType.xml
     DA_Backup/CustomDeviceType_backup/
     ```

   Data Aggregator インストール ディレクトリ

   Data Aggregator インストール ディレクトリを指定します。

   デフォルト： /opt/IMDataAggregator

Data Aggregator のリストア

バックアップした Data Aggregator の情報をリストアできます。 Data Repository に問題がない場合は、Data Aggregator コンポーネントのみをリストアできます。

リストア前に Data Aggregator を停止する必要はありません。 Data Aggregator が実行中であっても、バックアップ ファイルは正しいディレクトリにドロップされます。

注: このタスクを実行するには、root または sudo 権限が必要です。

以下の手順に従います。

1. コマンド プロンプトを開きます。
2. （オプション）Data Aggregator karaf サービスが実行中でない場合、既存の Data Aggregator をアンインストールして再インストールします。
3. 以下のコマンドをすべて実行します。

   ```
   cp DA_Backup/deploy_backup/*.* Data Aggregator インストール ディレクトリ
   /apache-karaf-2.3.0/deploy/
   cp DA_Backup/MIBDepot_backup/*.* Data Aggregator インストール ディレクトリ
   /apache-karaf-2.3.0/MIBDepot/
   cp DA_Backup/CustomDeviceType_backup/*.* Data Aggregator インストール ディレクト
   リ/apache-karaf-2.3.0/custom/devicetype/
   ```

   プロンプトが表示される場合は、既存のファイルを上書きします。

   DA_Backup

   バックアップ ディレクトリのディレクトリ パスおよび名前を指定します。

   Data Aggregator インストール ディレクトリ

   Data Aggregator インストール ディレクトリを指定します。

   デフォルト： /opt/IMDataAggregator

4. Data Aggregator が CA Performance Center と自動的に同期されるまで数分かかります。Data Aggregator ホストおよび Data Collector ホスト間の接続が確立されると、Data Collector ホストはポーリングを再開します。

   Data Aggregator がリストアされます。

   注: 以前の状態に Data Collector をリストアする必要がある場合は、Data Collector をアンインストールして、再インストールすることができます。

Data Aggregator の詳細の表示

Data Aggregator が監視している、管理可能な Ping 可能デバイスの数を表示できます。

管理者は、Data Aggregator によって監視されているすべてのテナントの管理可能デバイスおよび Ping 可能デバイスの合計数を表示できます。 各テナントの個別のデバイス合計もテーブルで表示されます。

テナント管理者は、Data Aggregator によって監視されている各自のテナントの管理可能デバイスおよび Ping 可能デバイスの合計数を表示できます。

また、Data Aggregator のバージョンおよびビルド番号を表示することもできます。

以下の手順に従います。

1. 管理者として CA Performance Center を開きます。
2. ［管理］-［データ ソース設定］を選択し、［Data Aggregator のデータ ソース］をクリックします。
3. ［システム ステータス］メニューから［Data Aggregator］をクリックします。

   Data Aggregator リスト ページが表示されます。テナントごとの管理可能デバイスおよび Ping 可能デバイスの合計数が表示され、選択した Data Aggregator インストールのバージョンおよびビルド番号が表示されます。

Data Collector インストールのリストの表示

利用可能な Data Collector インストールのリストを表示して、設定の一部を変更できます。 Data Collector リストには、各 Data Collector インストールが割り当てられたテナントと IP ドメイン、およびこの Data Collector のステータスとバージョンが表示されます。 また、各 Data Collector インストールがポーリングしているデバイスとコンポーネントの数や、現在ポーリングされていないデバイスを含め、この Data Collector インスタンスに割り当てられるデバイスの総数も確認できます。

管理者は、すべてのテナントに対する Data Collector インストールのリストを確認できます。 テナント管理者は、各自のテナントに割り当てられた Data Collector インストールのみを確認できます。

以下の手順に従います。

1. 管理者として CA Performance Center を開きます。
2. ［管理］-［データ ソース設定］を選択し、［Data Aggregator のデータ ソース］をクリックします。
3. ［システム ステータス］メニューから［Data Collector］をクリックします。

   Data Collector リスト ページが開き、利用可能な Data Collector インストールのリストが表示されます。

詳細:

Data Collector インストールの管理 (P. 29)

Data Collector インストールの管理

管理者は、各 Data Collector インストールの IP ドメインおよびテナントを選択する必要があります。それぞれの Data Collector インスタンスは、1 つの IP ドメインのみに関連付けることができます。その IP ドメインと関連付けられた Data Collector インスタンスがディスカバリ リクエストを実行します。

*IP ドメイン*は、さまざまなデバイスおよびネットワークからのデータを識別する論理的なグループです。 ドメインによる監視は、IP アドレスと、それに関連する別のカスタマ ネットワークに属するインターフェースまたはアプリケーションを別々に監視することを意味します。 適切な権限と組み合わせることで、IP ドメインは単一のコンソールから監視されますが、ユーザには、自身が監視するドメインのデータのみ表示されます。

テナントは、管理対象サービス プロバイダが管理するカスタマ環境を表します。各テナント環境は独立しており、CA Performance Center の個別のインスタンスとして有効に機能します。 各インスタンスには、テナント間で共有されない複数のユーザおよび役割を含めることができます。

デフォルト テナントは、管理対象インフラストラクチャ内の管理対象サービス プロバイダ用のテナント領域を表します。 マルチテナンシーを展開していない場合は、デフォルト テナントを割り当てます。 単一のテナント環境では、デフォルト テナントはインフラストラクチャ全体の監視に使用される領域です。

以下の手順に従います。

1. 管理者として CA Performance Center を開きます。
2. ［Data Collector］ページに移動します (P. 28)。
3. リストから Data Collector インスタンスを選択します。
4. Data Collector が割り当て可能であることを確認します。［ポーリングされるアイテム数］列は、この Data Collector インスタンスに割り当てられる、ポーリングされたデバイスおよびコンポーネントの数をリスト表示します。

   重要: ポーリングされるデバイスおよびコンポーネントの数が 2 つ以上の場合、Data Collector インスタンスに対するテナントおよび IP ドメインの割り当ては変更できません。
5. ［割り当て］をクリックします。

   ［Data Collector の割り当て］ダイアログ ボックスが表示されます。
6. ドロップダウン リストから、この Data Collector インスタンスに割り当てるテナントを選択します。

   この Data Collector インスタンスが検出するすべての監視対象デバイスおよびコンポーネントは、このテナントと自動的に関連付けられます。

   デフォルト テナントを使用する場合、［デフォルト テナント］を選択します。
7. この Data Collector インスタンスと関連付ける IP ドメインを選択します。

   この Data Collector インスタンスが検出するすべての管理対象デバイスおよびコンポーネントは、この IP ドメインと自動的に関連付けられます。
8. ［保存］をクリックします。

   テナントおよび IP ドメインが Data Collector インストールに割り当てられます。

Data Collector に対する負荷の再調整

Data Collector インスタンスが監視するデバイスの数が増えるに従って、負荷が Data Collector の処理限界を超過し、過負荷状態になる可能性があります。 このリリースでは、ある過負荷状態の Data Collector インスタンスから別の Data Collector インスタンスに作業負荷を移すことができるようになりました。 Data Collector に対する負荷を再調整する方法には、以下の 2 通りがあります。

- 過負荷の Data Collector インスタンスを選択し、次に［再調整］を選択します。使用可能な別の Data Collector インスタンスを使って、自動的に負荷が再調整されます。
- デバイスをある Data Collector インスタンスから別のインスタンスに移動します。

重要: エンドユーザのパフォーマンスに影響する可能性があるため、ピーク時には、Data Collector 上の負荷の調整を行わないか、または Data Collector インスタンスから別のインスタンスに多くのアイテムを移動させないことをお勧めします。

以下の手順に従います。

1. 管理者として CA Performance Center を開きます。
2. ［管理］-［データ ソース設定］を選択し、［Data Aggregator のデータ ソース］をクリックします。
3. ［システム ステータス］メニューから［Data Collector］をクリックします。

   Data Collector インストールがそれぞれポーリングしているデバイスおよびコンポーネントの数を確認できます。 また、そのときにポーリングされていないデバイスを含め、各 Data Collector インスタンスに割り当てられるデバイスの総数も確認できます。

Data Collector に対する負荷の自動再調整

1. 再調整の対象となる Data Collector インスタンスを選択し、［再調整］をクリックします。

   注: 必ず同じ IP ドメイン内の Data Collector インスタンスを選択してください。 同じ IP ドメインに存在する Data Collector インスタンスのみ、デバイス間で負荷を再調整することができます。

2. 確認ダイアログには、選択された各 Data Collector の現在のデバイスとポーリングされたアイテム数、および結果として提案されるデバイスとポーリングされたアイテム数が表示されます。

   注: デバイスは、接続可能な Data Collector インスタンスにのみ移動できます。

3. ［はい］をクリックします。

   注: ポーリングされたアイテムの再調整を行うと、再調整されたすべてのポーリング済みアイテムに対してベースライン平均計算が再起動されます。

選択したデバイスを特定の Data Collector インスタンスに移動

1. 移動したいデバイスが入っている Data Collector インスタンスを選択します。
2. ［デバイス］テーブルで、別の Data Collector インスタンスに移動するデバイスを選択し、［デバイスの移動］をクリックします。
3. ［デバイスの選択された Data Collector への移動］ダイアログ ボックスが開きます。
4. 選択した移動対象のデバイスが入っている Data Collector インスタンスをドロップダウン リストから選択します。

   注: 選択肢には、同じ IP ドメインに存在する Data Collector インスタンスのみ含まれます。

5. ［はい］をクリックします。

   注: デバイスを移動させると、移動されたデバイスに対するベースライン平均計算が再起動されます。

非 SNMP（CAMM）データを収集する Data Collector に対する負荷分散

Data Collector インスタンスから別のインスタンスへデバイスおよびコンポーネントを移動することによる Data Collector の負荷分散は、SNMP または ICMP を介して監視されているデバイスおよびコンポーネントにのみ適用されます。CAMM を介して非 SNMP データを収集している Data Collector インスタンスでリソースの再調整が必要な場合、環境内の別のホストにデバイス パック エンジンを分散させることができます。 この再調整を実行する方法について以下に示します。

1. ローカル コントローラ（LC）を新しいサーバにインストールし、インストール時に適切なマルチ コントローラ（MC）をポイントするようにします
2. LC が新しいサーバに正常にインストールされたら、CAMM Web に 2 つの LC が表示されていることを確認します。
   a. CAMMWEB を開きます
   b. ホストをクリックします。インストールされた LC（新しいサーバ）が表示されている必要があります
3. CAMMWEB を使用して新しいサーバを選択し、マイグレートされるデバイスパック エンジンを展開します
4. MC サーバにログインし、以下に移動します：

   $CAMM_INSTALL/MC/repository/<OLD_SEVER_IP>/COMPONENTS directory
5. 以下を実行します：

   'cp –R ENGINE_<devicepack> $CAMM_INSTALL/MC/repository/<NEW_SEVER_IP>/COMPONENTS/'
6. マイグレートされるデバイスパックで、データ取得方法として sftp/ftp/copy を使用している場合：
   a. NEW_SERVER で以下のディレクトリを $CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<devicepack>/ に作成します
      - tmp ディレクトリ（$CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<devicepack>/tmp/input/inventory 内）
      - input ディレクトリ（$CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<devicepack>/tmp/input/performance 内）
   b. 以下のファイルを OLD_SERVER から NEW_SERVER にコピーします
      - $CAMM_INSTALL/COMPONENTS/ENGINE_<devicepack>/tmp/input/inventory/.historyFile.Inventory を $CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<devicepack>/tmp/input/inventory へ
      - $CAMM_INSTALL/COMPONENTS/ENGINE_<devicepack>/tmp/input/performance/.historyFile.Performance を $CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<devicepack>/tmp/input/performance へ

7. CAMMWEB からデバイスパックを開始します。

Data Collector を別のホストに移動する方法

Data Collector は Data Aggregator のコンポーネントです。 Data Collector を別のホスト システムに移動する操作は、ネットワーク デバイスおよびコンポーネントの再検出を実行せずにデータを保持したまま実行することができます。 たとえば、ユーザがツール管理者である場合、サーバ管理者から Data Collector を別のホストに移動するように指示される可能性があります。Data Collector では 500,000 のデバイスおよびコンポーネントをポーリングしているため、データの喪失や再検出の実行を避けたいと考えます。

Data Collector コンポーネントは、デバイス パックがインストールされている場合でも移動させることができます。

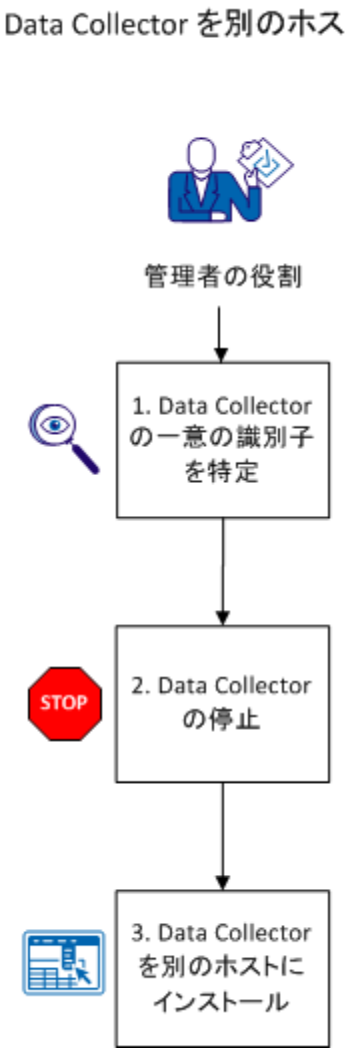
以下の点に注意してください。

- データ ロスの量は、古い Data Collector コンポーネントをシャットダウンしてから、新しい Data Collector コンポーネントを展開するまでの経過時間に等しくなります。
- 古い Data Collector コンポーネントが誤って開始された場合は、SNMP データの二重ポーリングが発生します。 Data Aggregator の karaf ログに、以下のような警告が表示されます。

  ```
  WARN  | Session Task-810 | 2013-01-02 13:52:09,062 | DCHeartBeatLog |
  ore.collector.interfaces |
        | HeartBeat message not received.  Expected: 93, Received: 255
  ```

  この問題を修正するには、古い Data Collector コンポーネントを停止またはアンインストールします。

以下の図に、Data Collector を別のホストに移動する方法を示します。



Data Collector を別のシステムに移動させるには、以下の手順に従います。

1. Data Collector の一意の識別子を決定します (P. 36)。
2. Data Collector を停止します (P. 36)。
3. （CA Mediation Manager 統合についてのみ）デバイス パックを移行します (P. 38)。
4. Data Collector を別のホストにインストールします (P. 38)。

Data Collector の一意の識別子の決定

このコンポーネントを別のホストに移動させる前に、Data Collector の一意の識別子を決定します。

以下のいずれかの方法で Data Collector ID を取得します。

- 管理者の役割を持つユーザとして CA Performance Center にログインし、以下の手順を実行します。
  a. ［管理］を選択し、メニューから Data Aggregator データ ソースを選択します。
  b. Data Aggregator 管理 UI が開きます。
  c. メニューから［システム ステータス］-［Data Collector］を選択します。
  d. 移動させる Data Collector コンポーネントを検索し、その ID をメモします。
- Web ブラウザを開き、以下の Web サービス コールを発行します。

  `http://DA_hostname:port/rest/dcms`

  DA_hostname:port

  Data Aggregator のホスト名およびポート番号を指定します。

  デフォルト ポート： 8581

  移動させる HostName および IPAddress を含む <DataCollectionMgrInfo> セクションを検索します。 <DcmID> の値をメモします。

次に、現在のホスト上の Data Collector サービスを停止します。

Data Collector の停止

Data Collector を別のホストに移動させる前に、現在のホスト上の Data Collector サービスを停止します。

以下の手順に従います。

1. この Data Collector にデバイス パックをインストール済みである場合は、以下の手順に従います。デバイス パックがインストールされていない場合は、手順 2 に進みます。

   a. 管理者の役割を持つユーザとして CA Performance Center にログインします。

   b. ［管理］を選択し、メニューから Data Aggregator データ ソースを選択します。

      Data Aggregator 管理 UI が開きます。

   c. ［監視設定］メニューから［EMS 統合プロファイル］を選択します。

   d. この Data Collector ホストに関連付けられているプロファイルを右クリックして、［停止］を選択します。 この Data Collector ホストに関連付けられるすべての EMS プロファイルに対して、この手順を実行します。

   e. このコマンドを実行して CA Mediation Manager アーティファクトをアーカイブします。

      ```
      tar -zcvf filename
      /opt/IMDataCollector/apache-karaf-{n.n.n}/MediationCenter
      ```

      filename

      アーカイブ ファイルの名前を指定します。

      注: このアーカイブ ファイルは、後で新しい Data Collector ホストに移動されます。

2. Data Collector ホストにログオンし、以下のコマンドを実行します。

   ```
   /etc/init.d/dcmd stop
   ```

3. Data Collector が停止したことを確認します。

   a. 管理者の役割を持つユーザとして CA Performance Center にログインします。

   b. ［管理］を選択し、メニューから Data Aggregator データ ソースを選択します。

   c. メニューから［システム ステータス］-［Data Collector］を選択します。

   d. Data Collector が「接続なし」のステータスを示していることを確認します。

次に、Data Collector を新しいホストにインストールします。

Data Collector の別のホストへのインストール

古いホスト上の Data Collector サービスを停止した後、Data Collector を新しいホストにインストールします。 古いホストからの Data Collector データは、以下の手順の実行中に新しいホストにエクスポートされます。

以下の手順に従います。

1. （CA Mediation Manager との統合についてのみ）デバイス パックを移行します。 古い Data Collector ホストで、*$CAMM_HOME*/tools/migratePMtoCAMM スクリプトを -t フラグで実行します。

   この手順は、ローカル コントローラがインストールされている Data Collector サーバ上でユーザがスクリプトを実行していることを前提としています。 また、別のサーバ上で CA Mediation Manager コンソールが実行されている必要があります。

注: 移行したデバイス パックは、.zip ファイルの形式で *$CAMM_HOME*/MigratedIMDevicepacks にコピーされます。 デバイス パックの移行の詳細については、「デバイス パックを移行する方法」シナリオを参照してください。

2. 新しいホスト システムにログインし、コマンド シェル セッションを開きます。
3. 以下のコマンドを実行して、以前にコピーした ID を環境変数に設定します。

   ```
   export DCM_ID=data collector id
   ```

4. **install.bin** バイナリを実行して、同じセッションから Data Collector をインストールします。
5. CA Mediation Manager LC を同じサーバにインストールします。
6. 以前にこの Data Collector 用のデバイス パックをインストールしている場合は、以下の追加の手順を実行します。
   a. このホストのローカル ディレクトリに、移行スクリプトで以前作成した ZIP ファイルをコピーします。
   b. CA Mediation Manager Web コンソールを使用して、これらのデバイス パックを展開し、開始します。

      注: 認証パックを Data Aggregator ホストに再展開する必要はありません。

注: 数回のポーリングの後、新しい Data Collector ホストによってデータが収集されていることを確認します。

ベスト プラクティスとしては、新しいホスト上でデータが収集されていることを確認したら、古い Data Collector をアンインストールし、関連付けられた EMS プロファイルを削除します。 このベスト プラクティスは任意です。

Data Collector ホストとのネットワーク切断中の Data Aggregator 設定変更

時々、ネットワークの切断の発生などにより Data Aggregator ホストおよび Data Collector ホスト間の接続が中断することがあります。 Data Aggregator および Data Collector プロセスが切断中に実行されている場合は、Data Aggregator インストールに対して設定変更ができます。 この場合、ネットワークが切断される前に存在していた設定に従って、Data Collector ホストでのポーリングが続行されます。 Data Aggregator と Data Collector ホスト間の接続が再確立されると、Data Collector は新規設定をダウンロードし、それに従ってポーリングを調整します。

たとえば、以下のいずれかの設定変更を行います。

- SNMP ベンダー認定がメトリック ファミリの値の計算に使用する式を変更します。
- 新規オペレーショナル メトリックをポーリングするためにメトリック ファミリを変更します。

Data Aggregator ホストおよび Data Collector ホスト間の接続が中断されると、変更は有効になりません。 再接続の後、Data Collector は、新規の式または新規オペレーショナル メトリックの計算に使用される、新規 SNMP MIB オブジェクトのポーリングを開始します。

Data Collector IP アドレスが変更された場合の Data Aggregator の設定

Data Collector が Data Aggregator と通信できるようにするには、Data Aggregator の IP を変更した場合に Data Collector を設定します。

注: Data Collector がホスト名を使用している場合、Data Collector を再起動するだけで、Data Collector および Data Aggregator の間の通信を維持できます。 Data Aggregator と通信するために IP アドレスを使用する場合にのみ、Data Collector を設定します。

以下の手順に従います。

1. Data Collector が実行されている場合は停止します。コマンド プロンプト ウィンドウを開き、以下のコマンドを入力します。

   ```
   /etc/init.d/dcmd stop
   ```

2. 以下のファイル内のホスト名またはアドレスを編集します。

   ```
   /opt/IMDataCollector/apache-karaf-2.3.0/etc/com.ca.im.dm.core.collector.cfg
   ```

   以下の行を編集します。

   ```
   collector-manager-da-hostname
   ```

   ファイルを保存します。

3. 以下のファイル内の IP アドレスを更新します。

   ```
   /opt/IMDataCollector/apache-karaf-2.3.0/jms/local-jms-broker.xml
   ```

4. 以下のファイルを削除します。

   ```
   /opt/IMDataCollector/apache-karaf-2.3.0/deploy/local-jms-broker.xml
   ```

5. キャッシュを削除します。 コマンド プロンプト ウィンドウを開き、以下のコマンドを入力します。

   ```
   rm -rf /opt/IMDataCollector/apache-karaf-2.3.0/data/cache/*
   ```

6. Data Collector を起動します。 コマンド プロンプト ウィンドウを開き、以下のコマンドを入力します。

   ```
   /etc/init.d/dcmd start
   ```

7. 正しいアドレスが Data Collector リストに表示されることを確認します。

   a. 管理者として CA Performance Center を開きます。

   b. ［管理］-［データ ソース設定］を選択し、［Data Aggregator のデータ ソース］をクリックします。

   c. ［システム ステータス］メニューから［Data Collector］をクリックします。

   d. 各 Data Collector の IP アドレスが「アドレス」列の下に表示されます。

   e. 各 Data Collector のステータスは「データ収集中」です。

Data Aggregator ホストが利用不可な場合の Data Collector によるポーリング済みデータのキャッシング

Data Aggregator と Data Collector ホストの間のネットワーク接続が失われることがあります。この場合、Data Collector はポーリングを続行し、ポーリングしたデータを設定可能な上限までメモリにキャッシュします。Data Aggregator ホストが利用可能になると、キャッシュされたポーリング済みデータは Data Aggregator に送信されます。

ポーリングされたデータは、「先入れ先出し」方式で処理されます。つまり、キャッシュ済みのポーリングされたデータのうち、古いものから先に Data Aggregator に送信されます。キャッシュ メモリ上限に到達すると、Data Aggregator ホストが利用可能になり、Data Aggregator ホストが、キャッシュされたデータの 9 パーセントを処理するまで、新規にポーリングされたデータは失われます。

重要: Data Aggregator が利用できない場合、Data Collector システムのメモリ使用率は著しく増加します。

メモリ ストレージの要件はさまざまで、以下の要因に依存します。

- ポーリングされるデバイスとコンポーネントの数
- ポーリング レート
- Data Aggregator ホストが利用できない場合に保持するデータ量。

キャッシュメモリ上限のデフォルト値は、最大の Data Collector プロセス メモリの最大値の半分です。 Data Collector のインストール時またはインストール後に、最大メモリ使用量が設定されます。

Data Collector が適切に動作するには、専用のメモリ容量が必要です。Data Collector が 5 分のポーリング レートで 50,000 のデバイスおよびコンポーネントをポーリングする小規模な環境では、基本操作に 2 GB のメモリが必要です。Data Collector が 5 分のポーリング レートで 500,000 のデバイスおよびコンポーネントをポーリングする大規模な環境では、基本操作に 24 GB のメモリが必要です。 残りのメモリは、ポーリングされたデータのキャッシュに使用できます。

ポーリング データのキャッシュに必要なメモリの計算

ポーリング データのキャッシュに必要なメモリの量は、以下の情報によって異なります。

- ユーザ環境の規模。
- Data Aggregator ホストが利用できない場合のデータ保存期間。

データ キャッシュに必要なメモリ量を計算するには、以下の数式を使用します。

キャッシュに必要な容量（GB）=（データをキャッシュする時間（秒）×ポーリングするアイテムの数）/（262144×平均ポーリング レート（秒））

例: 1 時間にポーリングされたデータをキャッシュするために必要なメモリの計算

- Data Collector が 5 分のポーリング レートで 50,000 のデバイスおよびコンポーネントをポーリングする小規模な環境で必要なメモリを計算します。 Data Aggregator が利用不可である間に、ポーリングされたデータを 1 時間キャッシュする場合は次のように計算します。

  キャッシュに必要な容量（GB）=（3600×50000）/（262144×300）

  キャッシュに必要な容量（GB）=2.3GB

  注: この計算は、基本の操作メモリ要件へ追加するものです。 小規模環境では基本操作に必要なメモリは 2GB です。 このため、必要なメモリ合計は 4608 M（2 GB + 2.3 GB）です。

- Data Collector が 5 分のポーリング レートで 500,000 のデバイスおよびコンポーネントをポーリングする大規模な環境で必要なメモリを計算します。 Data Aggregator が利用不可である間に、ポーリングされたデータを 1 時間分キャッシュする場合は次のように計算します。

  キャッシュに必要な容量（GB）=（3600×500000）/（262144×300）

  キャッシュに必要な容量（GB）=22.9 GB

  注: この計算は、基本の操作メモリ要件へ追加するものです。 大規模環境では基本操作に必要なメモリは 24 GB です。 このため、必要なメモリ合計は 47 GB（24 GB + 22.9 GB）です。

データ キャッシュメモリ上限の変更

Data Aggregator が利用不可能なときに Data Collector がキャッシュするデータ量を変更できます。

以下の手順に従います。

1. データキャッシュに必要なメモリ量を計算します (P. 44)。
2. データキャッシュに必要なメモリの量を書き留めます。
3. Data Collector がインストールされているコンピュータにログインします。root ユーザ、または特定のコマンド セットにアクセス可能な sudo ユーザとしてログインします。

   注: sudo ユーザの詳細については、「Data Aggregator インストール ガイド」を参照してください
4. このコマンドを使用して Data Collector を停止します。

   ```
   service dcmd stop
   ```
5. Data Collector の IM_MAX_MEM メモリ設定を変更します。
   a. *Data Collector のインストール ディレクトリ* /apache-karaf-2.3.0/jms/local-jms-broker.xml ファイルにアクセスします。
   b. IM_MAX_MEM 制限を、上で書き留めたメモリ量の 2 倍の値に変更します。書き留めた手順 : 2.この値が、システムで利用可能な RAM 容量を超えていないことを確認します。
6. Data Collector 上の JMS ブローカーのキャッシュ メモリ上限を変更します。
   a. *Data Collector のインストール ディレクトリ* /apache-karaf-2.3.0/jms/local-jms-broker.xml ファイルにアクセスします。
   b. 以下の行を見つけます。

      ```
      <memoryUsage limit="value"/>
      ```

      value

      現在のキャッシュ上限の設定です。
   c. 現在のキャッシュ上限の以前計算した値を変更し、ファイルを保存します。

7. jms/local-jms-broker.xml ファイルへの変更を Data Collector に認識させます。以下のコマンドを入力して、フェイク .lock ファイルを展開します。 フェイク .lock ファイルによって、正常でないシャットダウンがあったことが Data Collector に認識させます。

   ```
   echo `date` > /opt/IMDataCollector/apache-karaf-2.3.0/.lock
   ```

8. このコマンドを使用して Data Collector を再起動します。

   ```
   service dcmd start
   ```

   キャッシュ メモリ上限が設定されます。

Data Repository の監査プロセス

監査プロセスは、データベースを毎日午前 3:00 に監査して、Data Aggregator のデータが占める総容量を計算します。 このプロセスは、Vertica の機能（‘audit’）を使用してデータベースのサイズの概算を求めます。 データベースの概算を求める場合、一時テーブル内に保存されているデータ、削除用としてマークされていてデータベースからまだパージされていないデータ、および Vertica 監視テーブル内のデータは含まれません。

CA Technologies と Vertica との使用許諾契約には、Data Repository に保存されるデータの合計は 32 TB を超えることはできないと規定されています。

最新の監査結果を表示するには、ブラウザで以下の URL にアクセスします。

http://*hostname:port*/rest/datarepositorymaintenance/audit

この URL は XML を返します。「Current Size」タグに、Data Repository の現在のサイズがバイト単位で表示されます。

重要: 監査結果は定期的に確認してください。 32 TB より大きい値になった場合、使用許諾契約に準拠しません。 CA テクニカル サポートにお問い合わせください。

Data Repository ハートビート監視プロセス

ハートビート監視プロセスは、Data Repository が稼働しているかどうかを 10 秒ごとに確認します。 ハートビート プロセスが、データベースが動作していることを 5 分間、確認できない場合、Data Aggregator はシャットダウンします。 監査メッセージは *Data Aggregator のインストール ディレクトリ*/apache-karaf-2.3.0/shutdown.log ファイルに記録されます。

クラスタ環境では、10 秒ごとにクラスタ内のすべてのノードの可用性が継続的に確認されます。 5 分以内にノードにアクセスできない場合、CA Performance Center の Data Aggregator デバイスでイベントが生成され、ログに記録されます。 監査メッセージは *Data Aggregator のインストール ディレクトリ*/apache-karaf-2.3.0/shutdown.log ファイルに記録されます。

停止した Data Repository ノードがプライマリ ノードである場合（すべての Data Aggregator クエリはプライマリ ノードを通じて作成されます）、Data Aggregator は自動的に利用可能な次の Data Repository ノードに切り替えます。 Data Aggregator デバイスでイベントが生成され、ログに記録されます。

重要: 高可用性フェールオーバ中に発生する特定の管理機能は中断され、失敗します。1 つのポーリング サイクルが失われます。これらの機能は、Data Repository がクラスタ環境内の別のノードに接続した後でも再開しません。Data Repository がクラスタ環境内の別のノードに接続した後に実行する管理機能は、設計どおりに動作します。

クラスタ環境ですべての Data Repository ノードが停止した場合、Data Aggregator はシャットダウンします。

Data Repository との接続が失われると、Data Aggregator が収集するデータが損失する可能性があります。 Data Aggregator を再起動する前に、接続性または Data Repository の問題をすべて解決してください。 起動時に Data Repository へ接続できない場合、Data Aggregator は自動的にシャットダウンします。データの損失を最小限にとどめるため、Data Aggregator が再起動されるまで Data Collector インストールは収集を続行し、ローカルにデータを格納します。

停止したノードを復旧するには、admintools ユーティリティのメイン メニューで［Restart Vertica on Host］オプションを選択し、プロンプト メッセージの指示に従います。 停止したノード上の Vertica プロセスを再起動してネットワーク接続に成功するまで、Data Aggregator は、そのノード上のハートビートを確立しません。

選択したホストが失敗する場合、クラスタ内の別のホストを選択

Data Aggregator のインストール中に指定されたデータベース ホストがランタイムに失敗する場合、Data Aggregator は自動的にシャットダウンします。 Data Repository をクラスタ内にインストールした場合、データベース接続がクラスタ内のほかのホストをポイントするようにしてから Data Aggregator を再起動します。

以下の手順に従います。

1. Data Aggregator ホスト上の *Data Aggregator インストール ディレクトリ*/apache-karaf-2.3.0/etc/dbconnection.cfg ファイルを開きます。
2. dbconnection.cfg ファイルの以下の行を変更します。 まだ実行中の Data Repository クラスタ ホストの 1 つのホスト名または IP アドレスを参照するように行を変更します。

   ```
   dbUrl=jdbc:vertica://database server hostname:database server
   port/databasename?use35CopyFormat=true&BinaryDataTransfer=false
   ```

   database server hostname:*database server port*

   Data Aggregator のインストール時に入力した Data Repository のホスト名または IP アドレス、および Data Repository のポート番号を指定します。

   デフォルト ポート番号： 5433

   例：

   host2 がクラスタ内で稼働中であり、host2 をポイントするデータベース接続を選択した場合、更新済みの dbUrl エントリは以下の行のようになります。

   ```
   dbUrl=jdbc:vertica://host2:5433/mydatabasename?use35CopyFormat=true&BinaryDat
   aTransfer=false
   ```

3. dbconnection.cfg ファイルを保存します。

4. Data Aggregator を再起動するには、以下のコマンドを入力します

   ```
   /etc/init.d/dadaemon start
   ```

5. Data Aggregator がまだ実行中でないことを確認するには、以下のコマンドを入力します。

   ```
   Ps –ef | grep java | grep –v grep
   ```

   Data Aggregator が実行されていない場合、Data Aggregator プロセスは返されません。

   これ以降、データベース接続はクラスタ内の指定されたホストをポイントします。

Data Repository クラスタ内の複数のホストが停止した場合、Data Repository および Data Aggregator は自動的にシャットダウンします。 Data Repository クラスタが失うことができるホストは 1 つのみです。

Data Aggregator のインストール中に指定されていないクラスタ内の単一ホストがネットワークから切断されると（たとえば、ファイアウォールが配置されたり、Ethernet ケーブルが取り除かれたため）、Data Aggregator はシャットダウンします。 Data Aggregator のインストール中に Data Aggregator プロセスの自動復旧をセットアップした場合、Data Aggregator は自動的に再起動します。 オフラインであったホストが利用可能になると、そのホストはクラスタに戻ります。 admintools ユーティリティのメイン メニューで［Restart Vertica on Host］オプションを選択し、プロンプト メッセージの指示に従います。

注: Data Aggregator プロセスを自動復旧する設定の詳細については、「Data Aggregator インストール ガイド」を参照してください。

Data Aggregator のインストール中に指定されていないクラスタ内の単一ホストを、admintools ユーティリティの Advanced Menu にある「Kill Vertica Process on Host」オプションによって停止する場合、Data Aggregator の動作は続行します。 オフラインであったホストが利用可能になると、そのホストはクラスタに戻ります。 admintools ユーティリティのメイン メニューで［Restart Vertica on Host］オプションを選択し、プロンプト メッセージの指示に従います。

インストール後の Data Aggregator および Data Collector コンポーネントの最大メモリ使用量の変更（オプション）

Data Aggregator および Data Collector コンポーネントのデフォルトの最大メモリ使用量は十分ではありません。 大規模展開で効果的に実行するには、Data Aggregator および Data Collector の最大メモリ使用量を変更します。この変更は、インストール中またはインストール後に実行できます。 デフォルトでは、Data Aggregator および Data Collector のメモリ使用量は 2GB です。

重要：この手順のメモリ変更では、Data Aggregator および Data Collector が別のコンピュータにインストールされていることを前提とします。 またこの手順では、それらのコンピュータがこれらのコンポーネントのインストール専用であると仮定しています。

以下の手順に従います。

1. コンソールを開き、以下のコマンドを入力します。

   ```
   more /proc/meminfo
   ```

   合計メモリ使用率が表示されます。
2. この合計メモリをメモします。
3. 以下の手順に従って、Data Aggregator の最大メモリを変更します。
   a. *Data Aggregator インストール ディレクトリ* /apache-karaf-2.3.0/bin/setenv ファイルにアクセスします。
   b. IM_MAX_MEM=*number unit* 行を大規模展開用に変更します。

      number unit

      メモリの最大量を示します。*number* は正の整数で、*unit* は「G」または「M」です。 以前に書き留めたメモリ合計から 2 GB を引き、ここに入力します。 2 GB は、他のオペレーティング システムの操作のために予約されています。

      例： 33544320 KB - 2G = 30 GB

      IM_MAX_MEM=30G

      例：

      IM_MAX_MEM=4G
   c. ファイルを保存します。

d. 以下のコマンドを使用して Data Aggregator を再起動します。

```
service dadaemon start
```

Data Aggregator が自動的に起動し、CA Performance Center と同期されます。

e. Data Aggregator のアップグレード中にメモリ設定の変更を続けるには、/etc/DA.cfg ファイルを変更して、プロパティ「da.memory」を最新の値に更新します。

例：

```
da.memory=4G
```

4. 以下の手順に従って、すべての Data Collector ホストの最大メモリを変更します。

a. *Data Collector インストール ディレクトリ*/apache-karaf-2.3.0/bin/setenv ファイルにアクセスします。

b. IM_MAX_MEM=*number unit* 行を大規模展開用に変更します。

number unit

メモリの最大量を示します。*number* は正の整数で、*unit* は「G」または「M」です。 以前に書き留めたメモリ合計から 2 GB を引き、ここに入力します。 2 GB は、他のオペレーティング システムの操作のために予約されています。

例： 33544320 KB - 2G = 30 GB

IM_MAX_MEM=30G

例：

IM_MAX_MEM=4G

c. ファイルを保存します。

d. 次のコマンドを使って Data Aggregator ホストを再起動します。

```
service dcmd start
```

e. Data Collector のアップグレード中、メモリ設定の変更を続けるには、/opt/DCM.cfg ファイルを変更して、プロパティ「IM_MAX_MEM」を最新の値に更新します。

例：

```
IM_MAX_MEM=4G
```

メモリの最大量が大規模展開用に設定されます。

例：Data Aggregator のインストール後に Data Aggregator の最大メモリ使用量を設定

以下の例では、メモリ合計が 3354432 KB である Data Aggregator の最大メモリ使用量を設定します。

1. コンソールを開き、以下のコマンドを入力します。

   ```
   more /proc/meminfo
   ```

   以下の結果が表示されます。

   ```
   MemTotal: 33554432KB
   ```

2. 大規模展開に必要な最大メモリを計算します。

   式： 総メモリ - 2G = 大規模展開用最大メモリ

   解答： 3354432 KB - 2G = 30G

3. *Data Aggregator インストール ディレクトリ* /apache-karaf-2.3.0/bin/setenv ファイルにアクセスします。
4. IM_MAX_MEM=*number unit* 行を大規模展開用に変更します。

   IM_MAX_MEM=30G

5. ファイルを保存します。
6. Data Aggregator を再起動します。

   メモリの最大量が大規模展開用に変更されます。

インストール後の外部 ActiveMQ メモリ制限の変更（オプション）

Data Aggregator インストーラは、ApacheMQ プロセスを提供するためにシステムで必要なメモリを計算します。 ただし、このメモリ制限設定を手動で変更して、Data Aggregator システム上の ActiveMQ を調整することもできます。 たとえば、以下のような状況で設定を変更できます。

- システム メモリが変更された場合。
- Data Collector システムの数が変更された場合。
- メモリ設定を最適化する場合。
- ActiveMQ メトリックで JConsole または CA Performance Management カスタム グラフを監視した結果、ActiveMQ のパフォーマンスが低下していると判断できる場合。

以下の手順に従います。

1. 以下の設定に基づいて ActiveMQ 用のメモリの量を計算します。

   Java ヒープの最大サイズ

   この値はデフォルトでシステム メモリの 20% に設定されています。最小値は 512M です。

   Java ヒープの最小サイズの初期値

   この値は Java ヒープの最大サイズの 50% です。

   すべてのメッセージに対するメモリ上限

   この値は Java ヒープの最大サイズの 50% です。

   キュー 1 つ当たりのメモリ上限

   この値は、Data Collector インストールの個数に基づいて計算する必要があります。

   例： キュー 1 つ当たりのメモリ

   （すべてのメッセージに対するシステム メモリ）/5/（Data Collector の個数）

2. Data Aggregator がインストールされているコンピュータにログインします。 root ユーザ、または特定のコマンド セットにアクセス可能な sudo ユーザとしてログインします。

   注: sudo ユーザの詳細については、「Data Aggregator インストール ガイド」を参照してください

3. 以下のコマンドを入力して、ActiveMQ ブローカを停止します。

   ```
   /etc/init.d/activemq stop
   ```

4. ActiveMQ 用の Java ヒープ サイズを変更します。

   a. broker/apache-activemq-*version*/bin にある **activemq** ファイルにアクセスします。

   b. ACTIVEMQ_OPTS_MEMORY を定義する行を見つけます。

   c. –Xms を Java ヒープの最小サイズの初期値に変更します。

   d. –Xmx を Java ヒープの最大サイズに変更します。

   e. ファイルを保存します。

5. プロデューサ フロー コントロールに使用される ActiveMQ メモリ制限を変更します。

   a. *Data Aggregator installation directory*/broker/apache-activemq-*version*/conf ファイルにある activemq.xml ファイルにアクセスします。

   b. 以下の行を見つけ、値をすべてのメッセージに対するメモリ上限に変更します。

   ```
   <memoryUsage limit=”value”/>
   ```

   c. 以下の行を見つけ、値をキュー 1 つ当たりのメモリ上限に変更します。

   ```
   <policyEntry queue=">" producerFlowControl="true"
   memoryLimit="value"/>
   ```

   注: 詳細については、http://activemq.apache.org/producer-flow-control.html http://activemq.apache.org/producer-flow-control.html を参照してください。

6. 以下のコマンドを入力して、ActiveMQ ブローカを起動します。

   ```
   ./etc/init.d/activemq start
   ```

   新しい設定が起動されます。

データ保持の管理

Data Repository のデータ保持レートは管理可能です。 Data Repository のデフォルトのデータ保持レートは、ディスク容量を節約しつつ、ほとんどのユーザのレポート作成で利用できるように設定されています。 ポーリング済みデータは、指定されたデバイスに対してデフォルトで 5 分ごとに生成されます。このデータは製品で利用できる最も詳細なデータです。 このポーリング済みの生データは、1 時間間隔でロールアップするように設定されています。 ロールアップされたデータはポーリング値の集計値であり、より粒度の低い概要を表すビューをレポートに提供します。 日単位および週単位のロールアップは、保存に必要なディスク容量が少ないため、ポーリング済みデータや時間単位のデータより長期間保持されます。

ただし、ポーリング済みデータ、時間単位・日単位・週単位のロールアップ データを Data Repository に保持するレートは変更することができます。たとえば、ポーリング済みデータの保存期間を 30 日に変更して、ディスク容量を節約することができます。 ニーズと環境に最適なバランスを見つけてください。

注: データ保存レートの変更方法の詳細については、「REST Web サービス ガイド」を参照してください。

デフォルトで Data Repository にデータが保持される日数は以下のとおりです。

- ポーリング済みデータ： 45 日

  注: Data Aggregator の以前のリリースからこのリリースにアップグレードした場合、ポーリング済みデータの保存期間は、以前のデフォルトである 10 日から変更されません。
- 時間単位のロールアップ データ： 90 日
- 日単位のロールアップ データ： 365 日
- 週単位のロールアップ データ： 730 日

Data Repository がデータを保持できる最小の日数は以下のとおりです。

- ポーリングされたデータ： 2 日
- 時間単位のロールアップ データ： 8 日
- 日単位のロールアップ データ： 31 日
- 週単位のロールアップ データ： 366 日

第 2 章: コンポーネント サービスの再起動

このセクションには、以下のトピックが含まれています。

Data Aggregator の停止と再起動

Data Aggregator を停止して再起動する必要が生じる場合があります たとえば、Data Aggregator ホストのオペレーティング システムはアップグレードを必要とします。Data Aggregator を停止し、必要なアクションを実行して Data Aggregator を再起動します。 その後、Data Aggregator が処理を再開します。

計画された Data Aggregator のシャットダウン中に、Data Aggregator のシャットダウン前に受信されたすべてのポーリング済みデータが Data Repository に送信されます。 このポーリング済みデータは、レポートおよびその他の目的のために保持されます。

計画的に Data Aggregator を停止するとき、データ ロード、ロールアップ、およびイベントしきい値に関する以下の情報を考慮します。

- 現在のポーリング サイクル用の Data Collector コンポーネントから受信されたすべてのデータは、Data Aggregator が停止する前に処理されます。 データは失われません。
- シャットダウン時にしきい値イベントの処理が開始された場合、Data Collector コンポーネントから受信されたデータの処理は、Data Aggregator が停止する前に完了します。
- Data Aggregator が再起動すると、しきい値イベントの処理が再開します。
- シャットダウン時にロールアップ処理が開始された場合、Data Collector ホストから収集されたデータのロールアップ処理は、Data Aggregator が停止する前に完了します。
- Data Aggregator が再起動すると、ロールアップ処理が再開されます。

Data Aggregator は、Data Aggregator がインストールされているコンピュータの電源が失われた場合など、計画されていない方法でシャットダウンする場合があります。 この場合、Data Aggregator は突然停止します。 この場合は、ポーリング済みデータおよびしきい値イベント情報は失われる場合があります。Data Aggregator が再起動すると、Data Collector ホストからキューに格納されたデータのローディングが再開されます。 Data Aggregator が再起動すると、イベントしきい値の処理、およびキューに格納されたデータのロールアップ処理が再開されます。

以下の手順に従います。

1. Data Aggregator がインストールされているコンピュータにログインします。 root ユーザ、または特定のコマンド セットにアクセス可能な sudo ユーザとしてログインします。

   注: sudo ユーザの詳細については、「Data Aggregator インストール ガイド」を参照してください。

2. コマンド プロンプトを開き、以下のいずれかの手順を実行します。

   a. root ユーザとしてログインしている場合は、以下のコマンドを入力します。

      ```
      service dadaemon stop
      ```

   b. sudo ユーザとしてログインしている場合は、以下のコマンドを入力します。

      ```
      sudo service dadaemon stop
      ```

   実行中およびポーリング中であった Data Aggregator が停止すると、ポーリングは Data Collector 上で続行されます。Data Collector はポーリング済みデータをキューに入れ、後で Data Aggregator に配信します。

3. コンピュータを再配置するか、または他の管理タスクを実行します。

4. Data Aggregator がインストールされているコンピュータにログインします。 root ユーザ、または特定のコマンド セットにアクセス可能な sudo ユーザとしてログインします。

   注: Data Aggregator を sudo ユーザとしてインストールした場合は、/etc/init.d/dadaemon コマンド用の sudo コマンド エイリアスをセットアップします。 sudo コマンドを使用して dadaemon 起動スクリプトを実行します。 sudo ユーザの詳細については、「Data Aggregator インストール ガイド」を参照してください。

5. コマンド プロンプト ウィンドウを開き、以下のコマンドを入力します。

   ```
   service dadaemon start
   ```

   Data Aggregator が自動的に起動し、CA Performance Center と同期されます。

Data Aggregator が起動すると、Data Collector ホスト上のすべてのキューに格納されたデータおよびポーリング済みデータが Data Aggregator に送信されます。 キューに格納されたデータが Data Collector システムに設定されたディスク容量制限を越える場合は、最新のデータが破棄されます。結果として、ポーリング済みのレポート データには欠落部が存在します。

Data Collector の停止と再起動

Data Collector を停止し再起動する必要が生じる場合があります。 たとえば、Data Collector がインストールされているコンピュータの電源が切れたり、ロックアップしたりすることがあります。 また、そのコンピュータを移動する必要があることもあります。 この場合は、Data Collector を停止および再起動します。 オペレーティング システムのパッチをインストールする場合も、Data Collector を停止して再起動します。

以下の手順に従います。

1. Data Collector がインストールされているコンピュータにログインします。root ユーザ、または特定のコマンド セットにアクセス可能な sudo ユーザとしてログインします。

   注: sudo ユーザの詳細については、「Data Aggregator インストール ガイド」を参照してください。

2. コマンド プロンプトを開き、以下のいずれかの手順を実行します。

   a. root ユーザとしてログインしている場合は、以下のコマンドを入力します。

      ```
      service dcmd stop
      ```

   b. sudo ユーザとしてログインしている場合は、以下のコマンドを入力します。

      ```
      sudo service dcmd stop
      ```

   Data Collector が停止すると、進行中のポーリングはすべて停止します。ユーザはディスカバリを実行できません。

3. コンピュータを再配置するか、または他の管理タスクを実行します。

4. Data Collector がインストールされているコンピュータにログインし、Data Collector を起動します。root ユーザ、または特定のコマンド セットにアクセス可能な sudo ユーザとしてログインします。

   注: Data Collector を sudo ユーザとしてインストールした場合は、/etc/init.d/dcmd コマンド用の sudo コマンド エイリアスをセットアップします。 sudo コマンドを使用して dcmd 起動スクリプトを実行します。sudo ユーザの詳細については、「Data Aggregator インストール ガイド」を参照してください。

5. コマンド プロンプト ウィンドウを開き、以下のコマンドを入力します。

   ```
   service dcmd start
   ```

   Data Collector が再起動すると、スケジュール済みのポーリングが再開されます。ディスカバリの実行を再開できます。Data Collector は自動的に CA Performance Center と再同期されます。

詳細:

テナントの有効化 (P. 123)

Data Repository の停止と再起動

Data Repository を停止して再起動する必要が生じる場合があります。たとえば、Data Repository がインストールされているコンピュータの電源が切れたり、ロックアップしたりすることがあります。また、そのコンピュータを移動する必要があることもあります。 このような場合、Data Repository を停止して再起動します。オペレーティング システムのパッチをインストールしたり、新しいバージョンの Data Repository にアップグレードする場合は、Data Repository を停止して再起動します。

以下の手順に従います。

1. Data Aggregator がインストールされているコンピュータにログインします。 root ユーザ、または特定のコマンド セットにアクセス可能な sudo ユーザとしてログインします。

   注: sudo ユーザの詳細については、「Data Aggregator インストール ガイド」を参照してください。

2. コマンド プロンプト ウィンドウを開き、以下のコマンドを入力します。

   ```
   service dadaemon stop
   ```

3. Data Repository に使用するデータベース サーバに、（root ユーザではなく）データベース管理者ユーザとしてログインします。

4. 以下のコマンドを入力します。

   ```
   /opt/vertica/bin/adminTools
   ```

   ［Administration Tools］ダイアログ ボックスが表示されます。

5. ［(4) Stop Database］を選択します。

6. データベース名の隣のスペース バーを押し、［OK］を選択して Enter キーを押します。

   データベース パスワードの入力を促すプロンプトが表示されます。

7. データベース パスワードを入力し、Enter キーを押します。

   Data Repository が停止します。

   注: Data Repository が停止しない場合、［(7) Advanced Tools Menu］の［(2) Stop Vertica on Host］を選択します。

8. ［Exit］を選択して Enter キーを押します。

9. コンピュータを再配置するか、または他の管理タスクを実行します。
10. Data Repository に使用するデータベース サーバに、（root ユーザではなく）データベース管理者ユーザとしてログインします。
11. 以下のコマンドを入力します。

    ```
    /opt/vertica/bin/adminTools
    ```

    ［Administration Tools］ダイアログ ボックスが表示されます。
12. ［(3) Start Database］を選択します。
13. データベース名の隣のスペース バーを押し、［OK］を選択して Enter キーを押します。

    データベース パスワードの入力を促すプロンプトが表示されます。
14. データベース パスワードを入力し、Enter キーを押します。

    データベースが開始します。
15. ［(E) Exit］を選択して Enter キーを押します。
16. Data Aggregator がインストールされているコンピュータにログインし、Data Aggregator を起動します。 root ユーザ、または特定のコマンド セットにアクセス可能な sudo ユーザとしてログインします。

    Data Aggregator を sudo ユーザとしてインストールした場合は、service dadaemon コマンド用の sudo コマンド エイリアスをセットアップします。 sudo コマンドを使用して dadaemon 起動スクリプトを実行します。

    注: sudo ユーザの詳細については、「Data Aggregator インストール ガイド」を参照してください。
17. コマンド プロンプト ウィンドウを開き、以下のコマンドを入力します。

    ```
    service dadaemon start
    ```

    Data Repository が再起動します。

ActiveMQ ブローカの停止と再起動

Data Aggregator が ActiveMQ に関する問題を検出し、ブローカを正常に再起動できない場合は、Apache ActiveMQ ブローカを再起動します。 また、必要に応じて、手動でもサービスを停止して再起動できます。

以下の手順に従います。

1. コマンド ラインから以下のディレクトリを開きます。
   `cd da_install_dir/broker/apache-activemq-version/bin`

   da_install_dir

   Data Aggregator インストール ディレクトリの場所を指定します。

   apache-activemq-*version*

   Apache ActiveMQ のバージョンを指定します。

   例： apache-activemq-5.5.1b

2. 次の stop コマンドを実行します。

```
./activemq stop –jmxurl
service:jmx:rmi:///jndi/rmi://localhost:11099/jmxrmi --jmxuser
admin --jmxpassword activemq da_broker
```

–jmxurl service:jmx:rmi:///jndi/rmi://localhost:11099/jmxrmi

activemq ブローカの場所を指定します。この場所は、ユーザがポートを変更した場合、またはブローカを外部のシステムに配置した場合のみ変更されます。

注: ポート番号の変更はサポートされていますが、ブローカの外部への配置はサポートされていません。

--jmxuser admin

サービスのシャットダウンに使用するユーザ名を指定します。

デフォルト： admin

--jmxpassword activemq

サービスのシャットダウンに使用するパスワードを指定します。

デフォルト： activemq

da_broker

シャットダウンされるブローカ名を指定します。

デフォルト： da_broker

3. 以下の開始コマンドを実行します。

```
./activemq start
```

第 3 章: ユーザのネットワークの検出

このセクションには、以下のトピックが含まれています。

デバイスのディスカバリ

*ディスカバリ*とは、Data Aggregator によって IT インフラストラクチャが検出およびモデル化されるプロセスです。

ディスカバリ プロセスでは、以下の手順が実行されます。

- デバイスがどのプロトコルに応答しているかを確認します。 Data Aggregator は常に、デバイスが SNMP に応答できるかどうかを判断します。 ICMP を選択した場合は、Data Aggregator はまず、デバイスが ICMP に応答できるかどうかを判断します。 デバイスが ICMP に*応答する*場合、次に Data Aggregator はデバイスが SNMP に応答できるかどうかを判断します。デバイスが ICMP に*応答しない*場合、Data Aggregator はデバイスが SNMP に応答することを確認しません。
- 検出されたすべてのデバイスについて、デバイスを分類して適切なデバイス コレクションに追加するのに十分な最小セットの情報を取得します。

Data Aggregator でデバイスを検出するには、以下の 2 つの方法を使用できます。

- Data Aggregator で作成したディスカバリ プロファイルを使用して、インフラストラクチャ環境の特定のデバイスを検出できます。この方法でデバイスを管理するには、ディスカバリのワークフローに従います。（P. 66）
- CA Performance Center から提供されたデバイスを検出できます（P. 91）。

ディスカバリのワークフロー

以下のワークフローでは、インベントリのディスカバリを実行する際のクイック リファレンスとして使用できるベストプラクティスを説明します。

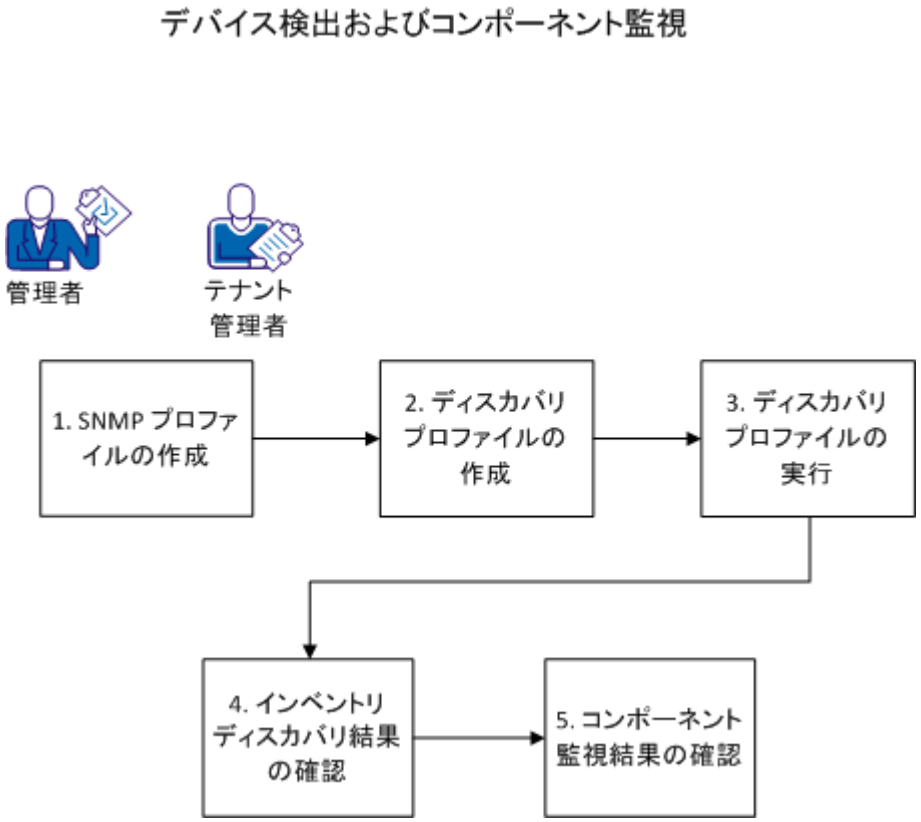
管理者の役割を持つユーザ、またはテナント管理者として、このプロセスを実行します。

1. Data Collector に、SNMP を使用するデバイス MIB テーブルのクエリを実行させる場合は、ディスカバリを実行する前に CA Performance Center で SNMP プロファイルを作成します。

   注: テナントに SNMP プロファイルを適用するには、テナント管理者の役割を持つユーザによって、テナント領域に SNMP プロファイルが作成される必要があります。 SNMP プロファイル作成の詳細については、「CA Performance Center 管理者ガイド」を参照してください。

2. Data Aggregator 管理ページから 1 つ以上のディスカバリ プロファイルを作成します（P. 76）。
3. 1 つ以上のディスカバリ プロファイルを実行します（P. 84）。ディスカバリはスケジュールするか、または手動で実行できます。
4. ディスカバリ結果を確認します。
5. コンポーネント監視結果を確認します（P. 111）。この結果を使用して、デバイスとコンポーネントの管理方法を決定します。

この図はディスカバリ プロセスを示します。



詳細情報:

デバイスのディスカバリ (P. 65)

SNMP プロファイル

SNMP プロファイルは、Data Collector に SNMP を使用するデバイス MIB テーブルのクエリの実行を許可するための必要な情報が含まれる定義です。 Data Collector は、SNMPv1、SNMPv2c および SNMPv3 をサポートするデバイスと通信できます。 コミュニティ文字列と認証情報は、CA Performance Center に格納されるときと、Data Aggregator および Data Collector に送信されるときに暗号化されます。

重要: SNMPv3 コミュニティ名を使用する場合、CA Performance Management には 8 文字より長い、任意の認証パスワードまたはプライバシー パスワードが必要です。8 文字より短いパスワードが設定されている場合、SNMPV3 プロファイルはデバイスと通信することができません。

Data Collector は、デバイスへのアクセス時に使用する認証情報を決定するために、インベントリ ディスカバリ中に SNMPv1/SNMPv2c および SNMPv3 プロファイルを使用します。 CA Performance Center は、このプロファイル リストを保持します。 それぞれのプロファイルはデバイス アクセス用にランク付けされます。 ディスカバリ中に、各プロファイルでデバイス アクセスが試行されます。 デバイスにアクセスできる最も高ランクのプロファイルが使用されます。

CA Performance Center で SNMP プロファイルを作成できます。また、SNMP プロファイル ランキングを変更できます。SNMP プロファイルの新しいランキング リストは、以下の状況で有効になります。

- 新しいデバイスが検出されます。
- 既存のデバイスは少なくとも 2 ポーリング サイクルの間、SNMP を介してアクセスすることはできなくなります。
- デバイスが使用している SNMP プロファイルは CA Performance Center から削除されます。

そうでない場合、すでに正常にポーリングされているデバイスは、SNMP プロファイルのランキング リストに加えられた変更にかかわらず、既存の SNMP プロファイルの使用を継続します。

注: SNMPv1/SNMPv2c プロファイルがデバイスにアクセスできる最も高ランクのプロファイルで、SNMPv1 と SNMPv2c の両方でデバイスにアクセスできる場合、Data Collector は SNMPv2c を使用してそのデバイスと通信します。

さまざまな SNMPv3 プロトコルが使用されるとき増加する CPU 負荷を判断するために Data Collector のテストを行いました。その結果、SNMPv1 と比較して、SHA/AES が CPU 使用率に及ぼす影響は穏当（<30 パーセント）であることがわかりました。MD5/DES、SHA/DES および SHA/3DES が CPU 使用率に及ぼす影響は大きい（>30 パーセント）ことがわかりました。

注: このテストが行われたサーバの CPU には AES 機能が組み込まれています。

ユーザが追加の CPU コアを環境に追加する場合、Data Collector は CPU 負荷のバランスをとることができます。

CA Performance Center ユーザ インターフェース内、または CA Performance Center REST Web サービスを使用して SNMP プロファイルを作成します。作成された SNMP プロファイルは直ちに Data Aggregator と同期され、インベントリ ディスカバリで利用可能になります。

注: SNMP プロファイルの作成の詳細については、「CA Performance Center 管理者ガイド」および「CA Performance Center REST Web サービス ガイド」を参照してください。

ディスカバリの実行後、［ディスカバリ履歴］ビューにアクセスして、使用される SNMP プロファイルのリストと、デバイスが応答した最も高ランクの SNMP プロファイルを参照できます。

詳細情報:

ディスカバリ結果の表示 (P. 89)

ディスカバリとポーリング

*ディスカバリ*とは、Data Aggregator によって IT インフラストラクチャが検出およびモデル化されるプロセスです。

ディスカバリ プロセスでは、以下の手順が実行されます。

- ディスカバリ プロファイルの作成時に選択したプロトコルに応じて、デバイスが応答するプロトコルを確認します。 たとえば、すべてのプロトコル（SNMP および ICMP）を選択したとすると、以下の手順が実行されます。 Data Aggregator は、デバイスが ICMP に応答できるかどうかを判断します。 次に、Data Aggregator は、デバイスが SNMP に応答できるかどうかを判断します。デバイスが ICMP に*応答しない*場合、Data Aggregator はデバイスが SNMP に応答することを確認しません。
- 検出されたすべてのデバイスについて、デバイスを分類して適切なデバイス コレクションに追加するのに十分な最小セットの情報を取得します。

インベントリ ディスカバリは、Data Aggregator がネットワーク上のデバイスを識別するプロセスです。デバイスの識別には、ディスカバリ プロファイルで指定された IP ドメイン、IP アドレス、IP 範囲、およびホスト名が使用されます。 特に、インベントリ ディスカバリは、デバイスが管理可能であるか（Ping 可能、または SNMP 対応）を識別して、分類（ルータ、スイッチなど）を特定します。 また、インベントリ ディスカバリは、ベンダー（Cisco、Juniper など）およびタイプ（7700、8200 など）を特定します。

このプロセス中に検出されたデバイスは、各デバイス コレクション メンバシップを制御するルールに従って、デフォルトのデバイス コレクションに自動的に追加されます。 CA Performance Center にカスタム デバイス コレクションを作成することもできます。その場合、同期の発生時に、対応するカスタム デバイス コレクションが Data Aggregator に作成されます。デバイスの検出*後*、初めての CA Performance Center との同期中に、カスタム コレクションに定義されたルールに基づいて、デバイスがカスタム コレクションに追加されます。

注: カスタム デバイス コレクションの作成および Data Aggregator との同期の詳細については、「*CA Performance Center 管理者ガイド*」を参照してください。

コンポーネント監視は別のプロセスです。 監視プロセスでは、CPU、メモリ、およびインターフェースなど、特定のデバイス コンポーネントに対するさまざまな運用上のデータを収集して分析します。 監視がどのように行われるかを記述している情報はすべて、デバイス コレクションに割り当てる監視プロファイル内に存在します。

監視プロファイルとデバイス コレクションの関係によって、コンポーネント監視が規定されます。 コンポーネント監視は、以下の方法でトリガできます。

- 指定されたデバイスがメンバであるデバイス コレクションに、監視プロファイルが割り当てられます。
- すでに監視プロファイルが割り当て済みのデバイス コレクションに、デバイスが追加されます。
- デバイス コレクションに割り当てられた監視プロファイルが編集され、監視する新しいメトリック ファミリが追加されます。 メトリック ファミリに関連付けられたコンポーネントは、デバイスで以前に監視されていなかった場合、監視プロファイルが関連付けられたコレクション内の各デバイスで自動的に監視されます。
- 新しいベンダー認定が、監視プロファイルでポーリングされる既存のメトリック ファミリに追加されます。
- 監視プロファイルで変更の検出レートを指定して、［自動的にメトリック ファミリを更新する］をオンにします。
- ［監視対象デバイス］ビューの［ポーリングされるメトリック ファミリ］タブにある［メトリック ファミリの更新］ボタンをクリックします。

*メトリック ファミリ*は、指定されたテクノロジーに対して収集しレポートする値のセットを定義します。 レポートがデータ ソースにかかわらず均一になるように、これらの値は正規化されます。 監視プロファイル内に含まれているとき、メトリック ファミリはその監視プロファイルと関連付けられるデバイスに対してどの値を収集する必要があるか決定します。

インベントリ ディスカバリおよびコンポーネント監視が完了した後、ポーリングが自動的に開始します。 オペレーショナル メトリックおよび設定データが、検出されたデバイスおよびその監視対象コンポーネント上でポーリングされます。 ポーリングされるオペレーショナル メトリックおよび設定データは、監視プロファイルで指定するメトリック ファミリによって異なります。 オペレーショナル メトリックはレポート用に一定間隔で収集され保持されます。 オペレーショナル メトリックの例としては、エラー率、日単位のベースライン、時間単位のベースラインおよびポートのパフォーマンスなどがあります。 設定データは、コンポーネントまたはコンポーネント設定を表したり識別したりします。

設定データの例には以下のものが含まれます。

ifNumber

デバイスのポート数を Data Aggregator に示す MIB 変数。

ifStackLastChange

インターフェース スタック テーブル上で変更が発生するかどうかを示す MIB 変数。

検出されたデバイスおよび監視対象コンポーネントは通常、CA Performance Center との同期を開始するまで最長で 5 分ほどかかります。同期の進行中に検出および監視されたデバイスおよびコンポーネントは、現在の同期が完了した後に同期されます。

詳細:

監視対象デバイスの表示 (P. 111)
変更検出を管理する方法 (P. 125)

VMware 環境でのディスカバリおよびポーリング

ネットワーク デバイスと共に、VMware 仮想マシンと ESX ホストのディスカバリおよび監視を実行できます。VMware デバイスおよびコンポーネントは物理コンポーネントのように動作しますが、これらのデバイスおよびコンポーネントのディスカバリと監視のプロセスは、vCenter からのデータ収集への対応の点で異なります。 SNMP を使用して直接 VM および ESX ホストをディスカバリすることはできますが、vCenter Server Application Insight Module （VCAIM）を使用して vCenter データを収集する場合があります。

VMware 環境で ESX ホストおよび仮想マシンのディスカバリができます。

インベントリ ディスカバリでは、Data Aggregator は、以下の方法で ESX ホストおよび仮想マシンを識別します。

- ICMP で識別
- 展開された SNMP エージェントをサーバが持つ場合、SNMP で識別
- SystemEDGE を実行しているサーバを VCAIM でディスカバリすることで識別

各 ESX ホストおよび仮想マシンは、ICMP、SNMP、および vCenter を通じて複数回識別できますが、デバイスは 1 つだけ作成されます。このデバイスは、ESX ホストまたは仮想マシンを表します。

ESX および VM デバイスが作成されると、Data Aggregator は vCenter 固有のメトリックのポーリングを開始し、SNMP エージェントによって識別される追加コンポーネントを検出してポーリングを開始できます。

メトリック データのソースによっては、VM および ESX のポーリングがデバイスに対する直接ポーリングによって行われる場合や、VCAIM のポーリングが他のデータの収集のために行われる場合があります。

デフォルトでは、Data Aggregator は VMware 環境を検出した後に、追加または削除された仮想マシン、または ESX ホスト間で vMotion が実行された仮想マシンを 15 分ごとに監視します。 また、デフォルトで、Data Aggregator は追加または削除された ESX ホストを 24 時間ごとに監視します。

ディスカバリ プロファイル

ディスカバリ プロファイルは、インベントリ ディスカバリがどのように動作するかを指定します。管理者として、CA Performance Center ユーザ インターフェースまたは Data Aggregator REST Web サービスを使用し、ディスカバリ プロファイルを管理できます。

ディスカバリ プロファイル内で、デバイスを検出する IP アドレス、IP アドレス範囲、およびホスト名を指定します。IP ドメインも指定します。作成するディスカバリ プロファイルごとに IP ドメインを 1 つだけ指定できます。新しく検出されたデバイスは、その IP ドメイン内に作成されます。

1 つの IP ドメインに複数の Data Collector ホストが展開されている場合、各 Data Collector はそのデバイスへのディスカバリ リクエストを発行します。

複数の Data Collector が同じデバイスに接続できる場合、そのデバイスを監視するために特定の Data Collector が選択されます。 この選択は、負荷分散に基づいたアルゴリズムによって決定されます。

IP ドメインは、IP アドレスが重複するテナント環境を監視するためにも必要です。 1 つのテナントは 1 つ以上の IP ドメインを持てます。 テナントの IP アドレスが重複している場合、ネットワーク内に複数の IP ドメインが必要です。 IP アドレスの重複は IP ドメインにより処理されます。

IP ドメインは CA Performance Center 内に作成されます。 はマニュアルまたは自動同期が発生するとき、Data Aggregator は新しい IP ドメインを認識します。

ディスカバリ プロセスは使用可能な Data Collector インスタンス全体にわたってデバイスの配布を試みますが、このプロセスでは、そのときに Data Collector インスタンスがどのデバイスを監視しているかは考慮されません。

注: IP ドメインの作成および同期の詳細については、「CA Performance Center 管理者ガイド」を参照してください。

ディスカバリ プロファイルには、ディスカバリ プロファイルが作成されたテナント領域内のユーザのみがアクセスできます。 「デフォルト テナント」領域に割り当てられたユーザは、「デフォルト テナント」領域に存在するディスカバリ プロファイルを使用してディスカバリを実行することができ、その結果を参照できます。

そのため、ディスカバリ プロファイルを作成する*前に*、正しいテナントでログインしており、テナントを適切に管理していることが重要です。

注: テナントの作成および管理の詳細については、「CA Performance Center 管理者ガイド」を参照してください。

詳細:

ディスカバリ プロファイルの作成 (P. 76)
ディスカバリ プロファイルの削除 (P. 84)
ディスカバリ プロファイルの編集 (P. 81)
ディスカバリ プロファイルのリストの表示 (P. 75)
IP ドメインの削除 (P. 119)

ディスカバリ プロファイルのリストの表示

SNMP および ICMP 用のディスカバリ プロファイルを使用して、ユーザ環境におけるディスカバリの動作を設定できます。

ディスカバリ プロファイルのリスト、および各リストの詳細を表示できます。 ディスカバリのステータス、およびディスカバリが最後に実行された時間を表示できます。 これらの詳細については、ネットワークがどのように検出されているか理解するのに役立ちます。

注: このタスクを実行するには、テナント管理者としてログインします。

以下の手順に従います。

1. ［管理］-［データ ソース設定］を選択し、［Data Aggregator のデータ ソース］をクリックします。
2. ［監視対象インベントリ］メニューの［ディスカバリ プロファイル］をクリックします。

   ディスカバリ プロファイル リスト ページが開き、利用可能なディスカバリ プロファイルのリストが表示されます。

詳細:

ディスカバリ プロファイルの IP 範囲 (P. 79)
ディスカバリ プロファイルの作成 (P. 76)
ディスカバリ プロファイルの削除 (P. 84)
ディスカバリ プロファイルの編集 (P. 81)
オンデマンド ディスカバリの実行 (P. 84)
ディスカバリのスケジュール (P. 86)
ディスカバリ プロファイル (P. 73)
ディスカバリ結果の表示 (P. 89)

ディスカバリ プロファイルの作成

ディスカバリ プロファイルを作成することで、ユーザ環境でのインベントリ ディスカバリの動作方法を指定できます。

このタスクを実行するには、テナント管理者としてログインします。ディスカバリ プロファイルには、ディスカバリ プロファイルが作成されたテナント領域内のユーザのみがアクセスできます。

注: テナントの詳細については、「CA Performance Center 管理者ガイド」を参照してください。

以下の手順に従います。

1. 利用可能なディスカバリ プロファイルのリストに移動します (P. 75)。
2. ［新規］をクリックします。
3. 以下の手順を実行します。
   a. ［名前］フィールドにディスカバリ プロファイルの名前を入力します。

      注: 一重引用符、二重引用符、バック スラッシュ、スラッシュおよびアンパサンドは使用できません。

   b. あらかじめ設定されたドメインのリストから IP ドメインを選択します。
4. ［IP/ホスト］タブを選択し、以下のアクションの 1 つ以上を実行します。
   - （オプション） IP アドレスの CSV ファイルを参照してインポートします。 CSV ファイルには、IPv4 アドレス、IPv6 アドレス、IPv4 アドレスの範囲、およびホスト名のカンマ区切りリストを含めることができます。 ファイルを参照して選択し、［開く］をクリックします。

     注: エイリアス名に日本語を使用するには、CSV ファイルを UTF-8 形式で保存します。

   - デバイスを検出する IP アドレス範囲を［IP アドレス範囲］フィールドに入力します。 カンマ区切り値を使用できます。

     注: ホスト名を持つデバイスからの複数の IP アドレスが IP 範囲に含まれており、かつホスト名にマップされる IP も IP 範囲に含まれている場合、インベントリ ディスカバリは常にホスト名 IP をデバイスのプライマリ IP アドレスに使用します。

- デバイスを検出する個別の IP アドレスを［IP アドレス リスト］フィールドに入力します。 カンマ区切り値を使用できます。
- ［ホスト リスト］フィールドにデバイスを検出するホスト名を入力します。 カンマ区切り値を使用できます。
- 個々の IP アドレス、IP アドレス範囲、およびホスト名のリストをクリップボードにコピーし、Ctrl+v を押してそのリストをリストビューに貼り付けます。
- IP アドレス、範囲、またはホスト名を選択し ［削除］をクリックして、IP リストからアイテムを削除します。
- ［検索］フィールドに IP アドレス、範囲、またはホスト名を入力して、IP リストでアイテムを検索します。 IP リストでアイテムの完全なリストに戻るには、X ボタンをクリックします。あるいは、キーボードの Esc キーを押します。

注: IP リスト内の IP アドレス、範囲、またはホスト名を編集するには、それをダブルクリックします。 Enter キーを押して、変更を保存します。 変更を保存せずに編集モードを終了するには Esc キーを押します。

IP アドレスやホスト名の重複がないようにします。重複が検出された場合、重複が見つかり無視されたことを示すメッセージが表示されます。

注: 一重引用符、二重引用符、バック スラッシュ、スラッシュおよびアンパサンドは使用できません。

5. （オプション）［スケジュール］タブを選択します。 このディスカバリ プロファイルの実行スケジュールを作成するには、以下の手順を実行します。
   - 日単位スケジュールを作成するには、［スケジュール間隔］ドロップダウン ボックスから［日単位］を選択します。 ディスカバリが毎日開始される時間を選択します。
   - 週単位スケジュールを作成するには、［スケジュール間隔］ドロップダウン ボックスから［週単位］を選択します。 ディスカバリを実行する日をそれぞれ選択します。 ディスカバリを開始する時間を選択します。

6. ［SNMP］タブを選択します。 すべての SNMP プロファイルを使用する場合、特別な操作は必要ありません。 すべての SNMP プロファイルはデフォルトで選択済みです。 特定の SNMP プロファイルを使用するには、［割り当て済み SNMP プロファイルの特定のリストを使用］チェック ボックスをオンにします。使用可能なプロファイルのリストから 1 つ以上の SNMP プロファイルを選択し、割り当てられたリストにそれらを移動します。 SNMP プロファイルのサブセットを使用すると、ネットワーク トラフィックを削減できます。
7. ［詳細］タブを選択して、以下の手順を実行します。
   a. （オプション）検出されたデバイスに名前を付ける優先度を変更します。 ディスカバリ中に、ディスカバリ プロファイルによって作成される任意のデバイス アイテムは、利用可能な最も優先度の高い命名規則で指定されます。 命名規則がデバイス用の MIB 内に設定されていない場合は利用できず、次に優先度の高い命名規則が試みられます。
   b. （オプション）*新しいディスカバリ プロファイル*用の名前付け順序を保存する場合は、［デフォルトとして保存］オプションを選択します。 次回、ディスカバリ プロファイルを作成したとき、名前付け順序は保存された順に自動的に表示されます。

      製品購入時のデフォルトの名前付け順序は、［システム名］、［ホスト名］、［IP アドレス］です。
   c. ディスカバリ プロセス中にデバイスが ICMP に応答できるかどうかを Data Aggregator に判断させる場合は、［ICMP を使用］を選択します。 ディスカバリ中に Ping 可能デバイスを作成するには、［Ping 可能の作成］を選択します。 Ping 可能デバイスを作成できないようにするには、［ICMP を使用］の選択を解除します。 これらのオプションが解除されていない場合、Data Aggregator は、デバイスが ICMP に応答できるかどうかを判断しません。

      選択した ICMP ディスカバリ オプションを保存する場合、［デフォルトとして保存］オプションを選択します。 次回ディスカバリ プロファイルを作成するとき、ICMP ディスカバリ オプションが自動的に選択されます。
8. ［保存］をクリックします。

ディスカバリ プロファイルが作成され、［ディスカバリ プロファイル］リストに表示されます。

詳細:

ディスカバリ プロファイルの IP 範囲 (P. 79)
ディスカバリのワークフロー (P. 66)
ディスカバリ プロファイル (P. 73)

ディスカバリ プロファイルの IP 範囲

ディスカバリ プロファイルを作成または編集するときに、IPv4 に対して検出する IP アドレス範囲を入力できます。 IPv6 アドレスの範囲のディスカバリはサポートされていません。

ディスカバリ プロファイルで IP 範囲を指定するときは、以下のルールが適用されます。

- IPv4 範囲にはワイルドカード（*）を含めることができます。 ワイルドカードは、IP オクテットの全範囲である 0-255 を表します。
- IPv4 の範囲にハイフン（-）を含めることができます。 最小 IP アドレスと最大 IP アドレスの間をハイフンでつなぐことができます。最小 IP アドレス内の IP オクテット範囲を表すためにハイフンを使用することもできます。
- 最小 IP アドレス内のオクテットでワイルドカードまたはハイフンを使用する場合、最大 IP アドレスを指定することはできません。

例: 有効な IP 範囲

- 以下の例ではどちらも、10.25.1.0 から 10.25.1.190 までのすべての IP アドレスでデバイスを検出しようとします。

  ```
  10.25.1.0-10.25.1.190
  ```

  または

  ```
  10.25.1.0-190
  ```

- 以下の例ではどちらも、10.25.0.0 から 10.25.255.255 までのすべての IP アドレスでデバイスを検出しようとします。

  ```
  10.25.*.*
  ```

  または

  ```
  10.25.0.0 - 10.25.255.255
  ```

- 以下の例ではどちらも、10.25.0.3 から 10.25.0.40 および 10.25.1.3 から 10.25.1.40 までのすべての IP アドレスでデバイスを検出しようとします。

  ```
  10.25.0-1.3-40
  ```

  または

  ```
  10.25.0.3 - 10.25.0.40, 10.25.1.3 - 10.25.1.40
  ```

- 以下の例ではどちらも、10.25.0.0 から 10.25.0.5、10.25.1.0 から 10.25.1.5 など、最大 10.25.255.0 から 10.25.255.5 までの IP アドレスすべてでデバイスを検出しようとします。

  ```
  10.25.*.0-5
  ```

  または

  ```
  10.25.0.0 - 10.25.0.5, 10.25.1.0 - 10.25.1.5 ... 10.25.255.0 - 10.25.255.5
  ```

例: 無効な IP 範囲

- 最大 IP アドレスが不完全なので、以下の例は無効です。

  ```
  10.25.1.0 - 10.23
  ```

- 最小 IP アドレス内のオクテットでハイフン(-)が使用されている場合、最大 IP アドレスは指定できないため、以下の例は無効です。

  ```
  10.25.1.0-190 - 10.25.1.255
  ```

- 最小 IP アドレス内のオクテットでワイルドカード（*）が使用されている場合、最大 IP アドレスは指定できないため、以下の例は無効です。

  ```
  10.25.*.0 - 10.25.255.255
  ```

- ワイルドカードオクテット（1*）が 10.25.10-19.0 と 10.25.10-199.0 のとちらを意味するのか不明瞭であるため、以下の例は無効です。

  ```
  10.25.1*.0
  ```

詳細:

ディスカバリ プロファイルの作成 (P. 76)
ディスカバリ プロファイルのリストの表示 (P. 75)

ディスカバリ プロファイルの編集

既存のディスカバリ プロファイルを編集できます。

注: このタスクを実行するには、テナント管理者としてログインします。

以下の手順に従います。

1. 利用可能なディスカバリ プロファイルのリストに移動します (P. 75)。
2. 編集するディスカバリ プロファイルを選択し、［編集］をクリックします。 必要に応じて、各タブのさまざまなフィールドを変更します。
3. 以下の手順を実行します。
   a. ［名前］フィールドにディスカバリ プロファイルの名前を入力します。

      注: 一重引用符、二重引用符、バック スラッシュ、スラッシュおよびアンパサンドは使用できません。

   b. あらかじめ設定されたドメインのリストから IP ドメインを選択します。

      注: このディスカバリ プロファイルですでにディスカバリを実行した場合、IP ドメインは変更できません。
4. ［IP/ホスト］タブを選択し、以下のアクションの 1 つ以上を実行します。
   - （オプション） IP アドレスの CSV ファイルを参照してインポートします。 CSV ファイルには、IPv4 アドレス、IPv6 アドレス、IPv4 アドレスの範囲、およびホスト名のカンマ区切りリストを含めることができます。 ファイルを参照して選択し、［開く］をクリックします。

     注: エイリアス名に日本語を使用するには、CSV ファイルを UTF-8 形式で保存します。

   - デバイスを検出する IP アドレス範囲を［IP アドレス範囲］フィールドに入力します。 カンマ区切り値を使用できます。

     注: ホスト名を持つデバイスからの複数の IP アドレスが IP 範囲に含まれており、かつホスト名にマップされる IP も IP 範囲に含まれている場合、インベントリ ディスカバリは常にホスト名 IP をデバイスのプライマリ IP アドレスに使用します。

- デバイスを検出する個別の IP アドレスを［IP アドレス リスト］フィールドに入力します。 カンマ区切り値を使用できます。
- ［ホスト リスト］フィールドにデバイスを検出するホスト名を入力します。 カンマ区切り値を使用できます。
- 個々の IP アドレス、IP アドレス範囲、およびホスト名のリストをクリップボードにコピーし、Ctrl+v を押してそのリストをリスト ビューに貼り付けます。
- IP アドレス、範囲、またはホスト名を選択し ［削除］をクリックして、IP リストからアイテムを削除します。
- ［検索］フィールドに IP アドレス、範囲、またはホスト名を入力して、IP リストでアイテムを検索します。 IP リストでアイテムの完全なリストに戻るには、X ボタンをクリックします。あるいは、キーボードの Esc キーを押します。

注: IP リスト内の IP アドレス、範囲、またはホスト名を編集するには、それをダブルクリックします。 Enter キーを押して、変更を保存します。 変更を保存せずに編集モードを終了するには Esc キーを押します。

IP アドレスやホスト名の重複がないようにします。重複が検出された場合、重複が見つかり無視されたことを示すメッセージが表示されます。

注: 一重引用符、二重引用符、バック スラッシュ、スラッシュおよびアンパサンドは使用できません。

5. （オプション）［スケジュール］タブを選択します。 このディスカバリ プロファイルの実行スケジュールを作成するには、以下の手順を実行します。
   - 日単位スケジュールを作成するには、［スケジュール間隔］ドロップダウン ボックスから［日単位］を選択します。 ディスカバリが毎日開始される時間を選択します。
   - 週単位スケジュールを作成するには、［スケジュール間隔］ドロップダウン ボックスから［週単位］を選択します。 ディスカバリを実行する日をそれぞれ選択します。 ディスカバリを開始する時間を選択します。

6. ［SNMP］タブを選択します。 すべての SNMP プロファイルを使用する場合、特別な操作は必要ありません。 すべての SNMP プロファイルはデフォルトで選択済みです。 特定の SNMP プロファイルを使用するには、［割り当て済み SNMP プロファイルの特定のリストを使用］チェック ボックスをオンにします。使用可能なプロファイルのリストから 1 つ以上の SNMP プロファイルを選択し、割り当てられたリストにそれらを移動します。 SNMP プロファイルのサブセットを使用すると、ネットワーク トラフィックを削減できます。

7. ［詳細］タブを選択して、以下の手順を実行します。

   a. （オプション）検出されたデバイスに名前を付ける優先度を変更します。 ディスカバリ中に、ディスカバリ プロファイルによって作成される任意のデバイス アイテムは、利用可能な最も優先度の高い命名規則で指定されます。 命名規則がデバイス用の MIB 内に設定されていない場合は利用できず、次に優先度の高い命名規則が試みられます。

   b. （オプション）*新しいディスカバリ プロファイル*用の名前付け順序を保存する場合は、［デフォルトとして保存］オプションを選択します。 次回、ディスカバリ プロファイルを作成したとき、名前付け順序は保存された順に自動的に表示されます。

      製品購入時のデフォルトの名前付け順序は、［システム名］、［ホスト名］、［IP アドレス］です。

   c. ディスカバリ プロセス中にデバイスが ICMP に応答できるかどうかを Data Aggregator に判断させる場合は、［ICMP を使用］を選択します。 ディスカバリ中に Ping 可能デバイスを作成するには、［Ping 可能の作成］を選択します。 Ping 可能デバイスを作成できないようにするには、［ICMP を使用］の選択を解除します。 これらのオプションが解除されていない場合、Data Aggregator は、デバイスが ICMP に応答できるかどうかを判断しません。

      選択した ICMP ディスカバリ オプションを保存する場合、［デフォルトとして保存］オプションを選択します。 次回ディスカバリ プロファイルを作成するとき、ICMP ディスカバリ オプションが自動的に選択されます。

8. ［保存］をクリックします。

ディスカバリ プロファイルはユーザの変更で更新されます。次回、このディスカバリ プロファイルを実行すると、変更が適用されます。

詳細:

トラブルシューティング： ディスカバリが開始しない (P. 193)
ディスカバリ プロファイル (P. 73)

ディスカバリ プロファイルの削除

ディスカバリ プロファイルが不要になった場合は削除できます。 たとえば、使用されなくなったり、ほかのディスカバリ プロファイルと重複していたりするディスカバリ プロファイルを削除できます。 削除されたディスカバリ プロファイルで指定されているデバイスは再検出できません。

注: このタスクを実行するには、テナント管理者としてログインします。

以下の手順に従います。

1. ディスカバリ プロファイルのリストに移動します。
2. 削除するディスカバリ プロファイルを選択し、［削除］をクリックします。

   確認ダイアログ ボックスが表示されます。
3. ［はい］をクリックします。

   ディスカバリ プロファイルが削除されます。

オンデマンド ディスカバリの実行

インベントリ ディスカバリは、ディスカバリ プロファイルに追加した情報に基づいて、ネットワークでデバイスが検出されるプロセスです。 オンデマンド ディスカバリを実行できます。

デバイス検出の試行は SNMP および ICMP プロトコルを通して行われます。デバイスがユーザが作成した SNMPv1/SNMPv2c または SNMPv3 プロファイルで SNMP には応答せず、ICMP に応答する場合、Ping 可能デバイスが作成されます。 （SNMP プロファイルは、CA Performance Center ユーザ インターフェースまたは CA Performance Center REST Web サービスのいずれかを使用して作成されます。）

このタスクはテナント管理者または管理者のどちらかとして実行できます。 管理者としてディスカバリを実行するには、ディスカバリを実行する前にデフォルト テナント ドメインに対して Data Collector を設定します。

注: SNMP プロファイルの作成および Data Aggregator との同期の詳細については、「CA Performance Center 管理者ガイド」および「CA Performance Center REST Web サービス ガイド」を参照してください。

以下の手順に従います。

1. CA Performance Center 内のディスカバリ プロファイルのリストに移動します (P. 75)。
2. ディスカバリを実行するディスカバリ プロファイルを 1 つ以上選択し、［実行］をクリックします。

   注: ディスカバリを実行できるのは、「準備完了」状態のディスカバリ プロファイルのみです。

   確認ダイアログ ボックスが表示されます。
3. ［はい］をクリックします。

   ディスカバリが開始されます。選択したディスカバリ プロファイルの［状態］列に［実行中］と表示され、［最終実行時刻］列がディスカバリの開始時刻に更新されます。

   注: ディスカバリの実行中に［完了率］列を更新するには、［リフレッシュ］をクリックします。

   確認ダイアログ ボックスが表示されます。
4. ［OK］をクリックします。

   検出されたデバイスはデバイス コレクションに追加され、コンポーネントの監視とポーリングが開始されます。ディスカバリ プロファイル ページに戻ります。

   ディスカバリが 10 分を超えてハングアップする場合はアボートされます。 ディスカバリは、新しいデバイスが 10 分以内に検出されず、さらに選択されたディスカバリ プロファイルの状態が 10 分以内に変更されなかった場合に、ハングアップしているとみなされます。 Data Aggregator デバイスで監査イベントが生成されます。

   選択したディスカバリ プロファイルの［状態］列には、デバイスの検出に成功しなかった場合は［失敗］と表示され、少なくとも 1 つのデバイスの検出に成功した場合は［部分的な失敗］と表示されます。

検出されたデバイスおよび監視対象コンポーネントは、CA Performance Center との同期に最長で 5 分間かかる場合があります。同期が完了すると、検出されたデバイスおよび監視対象コンポーネントが CA Performance Center の［インベントリ］タブに表示されます。

5. （オプション）検出されたデバイスおよび監視対象コンポーネントをすぐに CA Performance Center と同期するには、以下の手順に従います。

   a. ［管理］-［データ ソース設定］を選択し、［Data Aggregator のデータ ソース］をクリックします。

   b. ［システム ステータス］メニューから［Data Aggregator］をクリックします。

   c. ［Data Aggregator］を選択し、［再同期］ボタンをクリックします。

詳細:

ディスカバリのワークフロー (P. 66)
インターフェース フィルタを設定しアクティブにする方法 (P. 145)

ディスカバリのスケジュール

インベントリ ディスカバリは、ディスカバリ プロファイルに追加した情報に基づいて、ネットワークでデバイスが検出されるプロセスです。ディスカバリを毎日または週単位で実行するようにスケジュールできます。

注: ディスカバリ プロファイルを選択して［実行］をクリックすると、スケジュール済みディスカバリをいつでも実行できます。 ただし、ディスカバリ プロファイルでスケジュール済みディスカバリを実行している間は、そのディスカバリ プロファイルでオンデマンド ディスカバリを開始できません。

デバイス検出の試行は SNMP および ICMP プロトコルを通して行われます。デバイスがユーザが作成した SNMPv1/SNMPv2c または SNMPv3 プロファイルで SNMP には応答せず、ICMP に応答する場合、Ping 可能デバイスが作成されます。（SNMP プロファイルは、CA Performance Center ユーザ インターフェースまたは CA Performance Center REST Web サービスのいずれかを使用して作成されます。）

管理者としてディスカバリを実行するには、ディスカバリをスケジュールする前にデフォルト テナント ドメインに対して Data Collector を設定します。

注: SNMP プロファイルの作成および Data Aggregator との同期の詳細については、「CA Performance Center 管理者ガイド」および「CA Performance Center REST Web サービス ガイド」を参照してください。

以下の手順に従います。

1. CA Performance Center 内のディスカバリ プロファイルのリストに移動します (P. 75)。
2. 以下の手順のいずれかを実行します。
   - ディスカバリをスケジュールする既存のディスカバリ プロファイルを選択し、［編集］をクリックします。

     ディスカバリ プロファイルの編集ページが表示されます。
   - ［新規］をクリックして、ディスカバリをスケジュールするディスカバリ プロファイルを作成します。

     ［ディスカバリ プロファイル］ダイアログ ボックスが表示されます。
3. このディスカバリ プロファイルの実行スケジュールを作成するには、以下のいずれかの手順を実行します。
   - 日単位スケジュールを作成するには、［スケジュール間隔］ドロップダウン ボックスから［毎日実行］を選択し、毎日のディスカバリの開始時間を選択します。
   - 週単位スケジュールを作成するには、［スケジュール間隔］ドロップダウン ボックスから［毎週実行］を選択し、ディスカバリの実行日を選択して、ディスカバリの開始時間を選択します。

   注: スケジュールを削除するためには、［スケジューリング］ドロップダウン ボックスから［なし］を選択します。
4. ［保存］をクリックします。

ディスカバリがスケジュールされると、ディスカバリ プロファイルの［状態］列に［スケジュール済み］と表示され、スケジュールされた次回の実行時間が表示されます。

スケジュール済みディスカバリが開始されると、選択したディスカバリ プロファイルの［状態］列に［実行中］と表示され、［最終実行時刻］列がディスカバリの開始時間で更新されます。

注: ディスカバリの実行中に［完了率］列を更新するには、［リフレッシュ］をクリックします。

検出されたデバイスはデバイス コレクションに追加され、コンポーネントの監視とポーリングが開始されます。ディスカバリ プロファイル ページに戻ります。

ディスカバリが 10 分を超えてハングアップする場合はアボートされます。 ディスカバリは、新しいデバイスが 10 分以内に検出されず、*さらに*選択されたディスカバリ プロファイルの状態が 10 分以内に変更されなかった場合に、ハングアップしているとみなされます。 Data Aggregator デバイスで監査イベントが生成されます。

選択したディスカバリ プロファイルの［状態］列には、デバイスの検出に成功しなかった場合は［失敗］と表示され、少なくとも 1 つのデバイスの検出に成功した場合は［部分的な失敗］と表示されます。

検出されたデバイスおよび監視対象コンポーネントは、CA Performance Center との同期を開始するまで最長で 5 分かかる場合があります。 同期が完了すると、検出されたデバイスおよびコンポーネントが CA Performance Center 内の［インベントリ］タブ内に表示されます。

5. （オプション）検出されたデバイスおよびコンポーネントをすぐに CA Performance Center と同期するには、以下の手順に従います。

   a. ［管理］-［データ ソース設定］を選択し、［Data Aggregator のデータ ソース］をクリックします。

   b. ［システム ステータス］メニューから［Data Aggregator］をクリックします。

   c. ［Data Aggregator］を選択し、［再同期］ボタンをクリックします。

ディスカバリ結果の表示

特定のディスカバリ インスタンスで検出された、新しい Ping 可能（ICMP）デバイス数と管理可能（SNMP）デバイス数のサマリを表示できます。 また、これらの検出されたデバイスに関する詳細情報（IP アドレス、モデル、タイプ、ベンダー名、場所、および使用されたプロトコルなど）を表示できます。

ディスカバリ結果には、既存デバイスの検出を表示することもできます。これらの既存デバイスは、同一または異なるディスカバリ プロファイルによって以前に検出されたものです。既存デバイスを表示するには、［変更なし］フィルタを使用します。 既存デバイスの IP アドレスが異なる場合、そのデバイスは以前に検出済みであり、現在は別の IP アドレスで監視されていることを示します。

多くのデバイスは複数の IP アドレスに応答できるため、このような動作は一般的で予想されるものです。Data Aggregator は各デバイスの完全な IP アドレス セットを保持し、すべてのアドレスを CA Performance Center に渡します。

以下の手順に従います。

1. ディスカバリ プロファイルのリストを表示します (P. 75)。
2. ディスカバリ結果を表示するディスカバリ プロファイルを選択し、［履歴］ボタンをクリックします。

   注: ディスカバリが実行されていないディスカバリ プロファイルを選択すると、［履歴］ボタンは無効になります。
3. 該当する場合、ディスカバリ インスタンスを選択します。
4. （オプション）以下のいずれかのオプションを実行して、［検出されたデバイス］テーブルをフィルタします。
   - ［デバイス タイプ］フィルタ リストから表示するデバイス タイプを選択して［適用］をクリックすることにより、デバイス タイプでフィルタリングします。
   - 表示する状態を状態リストから選択し、［適用］をクリックすることにより、検出されたデバイスの状態でフィルタリングします。
   - ［デバイス タイプ］フィルタ リストおよび［状態］リストから選択して［適用］をクリックすることにより、デバイス タイプとその状態でフィルタリングします。

ディスカバリ結果が、［検出されたデバイス］テーブルに表示されます。［SNMP プロファイル］列には、デバイスが応答した SNMP プロファイルのうち、最もランクの高いものが表示されます。

具体的には、［状態］列は以下のいずれかの状態を示します。

新規

このディスカバリ プロファイルが実行されたときに初めて検出されたデバイスを示します。

変更済み

デバイス タイプが以前のディスカバリから変更されたことを示します。 たとえば、以前に検出された Ping 可能デバイスが、今回は管理可能デバイスとして検出されました。 または、管理可能デバイスのデバイス タイプが以前は「スイッチ」でしたが、現在は「ルータ」に変更されているような場合です。 ホスト名やシステムの説明など、属性のみが変更されたデバイスは、「変更済み」として分類されません。

変更なし

既存デバイスが変更されていないことを示します。 属性のみが変更された既存デバイスは、「変更なし」として分類されます。

削除済み

ディスカバリが実行された後に、デバイスが Data Aggregator から削除されたことを示します。

注: 検出された個々のデバイスが「Ping 可能」または「管理可能」として認識されない場合、「到達不可」の状態となります。ただし、Data Aggregator は、IP 範囲内で見つかった到達不可デバイスをレポートしません。

詳細:

SNMP プロファイル (P. 68)
ディスカバリのワークフロー (P. 66)

他のデータ ソースからのディスカバリ

他のデータ ソースによって CA Performance Center と同期されたデバイスを、Data Aggregator が自動的に検出するかどうかを選択できます。 Data Aggregator を登録するとき、またはデータ ソース オプションを編集するときに、このオプションを使用できます。 デフォルトでは、このオプションは無効になっています。

重要: 有効にすると、Data Aggregator は他のすべてのデータ ソースによって提供されるデバイスの検出を試行します。 この機能をデータ ソースの特定のセットに対して設定することはできません。

有効にすると、Data Aggregator はそれ以降に見つかった新しいデバイスの検出を試行します。Data Aggregator で、過去に CA Performance Center と同期されたデバイスの検出を試行する場合は、Data Aggregator データ ソースを選択して［再同期］をクリックし、［完全な再同期を実行］チェック ボックスをオンにします。

ICMP または他のサポートされるプロトコルを通じてデバイスに到達できる場合、ディスカバリの試行によって、Ping 可能または他のタイプのデバイスが Data Aggregator に作成されます。

注: このオプションを有効にした後で無効にしても、Data Aggregator は過去に検出されたデバイスの監視を続行します。

このオプションを有効にするには、CA Performance Center 内の［データ ソースの管理］ページにある［データ ソースの編集］ダイアログ ボックスで、［廃止されたアイテムの同期］チェック ボックスをオンにします。

詳細:

デバイスのディスカバリ (P. 65)

デバイス タイプの変更

Data Aggregator は、デバイス サービス情報に基づいて、管理可能デバイスをルータ、スイッチおよびサーバ タイプとして自動的に分類できます。管理可能デバイスが、ルータ、スイッチ、またはサーバとして識別されない場合、「デバイス」デバイス タイプとして分類されます。

一部の SNMP 管理可能デバイスのタイプが予定通りに識別されなかった場合、デバイス タイプを上書きできます。 デバイスの sysObjectID MIB 値を、明示的に Data Aggregator に付属している $KARAF_HOME/custom/devicetypes/DeviceTypes.xml ファイル内の正しいデバイス タイプにマップします。

注: DeviceTypes.xml ファイルには新しいデバイス タイプを追加できません。

DeviceTypes.xml ファイルには、sysObjectID を適切なデバイス タイプにマップするためのテンプレートが含まれます。 デフォルトでは、ファイルには sysObjectID からタイプへのマッピング エントリは含まれていません。 特定の sysObjectID を持つデバイス タイプを分類する場合は、テンプレートを変更して、ファイルに sysObjectID からタイプへのエントリを追加できます。sysObjectID を追加する前に、sysObjectID を追加するセクションのコメントを解除します。

注: DeviceTypes.xml ファイルの更新は、適用されるまで最大 1 分間かかる場合があります。

デバイスは複数のデバイス タイプに分類できます。 ただし、デバイスというタイプは、ほかのデバイス タイプとは相互に排他的です。たとえば、ルータ、スイッチ、サーバのデバイス タイプのうちの 1 つ以上に sysObjectID を追加し、また「デバイス」デバイス タイプにも sysObjectID を追加する場合、「デバイス」デバイス タイプはドロップされ、認識されません。

注: Data Aggregator をアップグレードした場合、DeviceTypes.xml ファイルは保持されません。 ただし、アップグレード以前に追加された設定は*保持されます*。

例: その他のデバイス タイプにデバイスの sysObjectID をマップする

以下の手順に従います。

1. $KARAF_HOME/custom/devicetypes/DeviceTypes.xml ファイルを開きます。

2. 以下の情報を入力します。

```
<DeviceType>
    <Routers>
     <sysObjectID>1.3.6.5.1.34</sysObjectID>
    </Routers>

    <Switches>
      <sysObjectID>1.3.6.5.5.3</sysObjectID>
      <sysObjectID>1.3.6.5.1.34</sysObjectID>
     </Switches>

    <Servers>
      <sysObjectID>1.3.6.5.567.1</sysObjectID>
    </Servers>

    <Device>
      <sysObjectID>1.3.6.5.49.1</sysObjectID>
    </Device>
<DeviceType>
```

3. デバイスが含まれるディスカバリ プロファイルでディスカバリを実行します。

   注: ディスカバリを再実行するまでは、DeviceTypes.xml ファイルに行った変更は、既存のデバイスに対して有効になりません。

   ディスカバリを実行すると、以下の結果が得られます。

   - sysObjectID 1.3.6.5.1.34 を持つすべてのデバイスは、ルータおよびスイッチのデバイス タイプとして分類されます。
   - sysObjectID 1.3.6.5.5.3 を持つすべてのデバイスは、スイッチのデバイス タイプとして分類されます。
   - sysObjectID 1.3.6.5.567.1 を持つすべてのデバイスは、サーバのデバイス タイプとして分類されます。
   - sysObjectID 1.3.6.5.49.1 を持つすべてのデバイスは、デバイスのデバイス タイプとして分類されます。

再ディスカバリ

実行されるディスカバリ プロファイルに、既存の監視対象デバイスの IP アドレスの 1 つまたはホスト名が含まれている場合、その監視対象デバイスが再検出されます。 特定デバイスの［詳細］タブにある［再検出］ボタンをクリックすると、監視対象デバイスを 1 つ再検出できます。

このディスカバリの結果、以下の属性セットが更新されます。

- システム名
- ホスト名
- デバイス タイプ（CA Performance Center に表示される）
- 場所
- ベンダー
- デバイスの説明
- デバイス モデル

注: デバイス属性を変更すると、デバイスが属するグループおよびデバイス コレクションが変更される場合があります。 グループおよびデバイス コレクションの変更により、監視プロファイルが追加または削除される可能性があります。

CA Performance Center インベントリまたはダッシュボード ビューでデバイス属性の変更を参照できるようになるまで、最大 5 分かかります。

第 4 章: インフラストラクチャの管理

このセクションには、以下のトピックが含まれています。

デバイスおよびコンポーネント管理ワークフローのカスタマイズ

検出されたデバイスおよび監視対象コンポーネントの管理方法をカスタマイズできます。プロファイルの変更、関連付けの変更、新しいベンダー認定の作成、およびメトリック ファミリのインポートも可能です。 たとえば、重要なインターフェースを頻繁にポーリングしたり、イベント ルールが設定されたカスタム監視プロファイルを、カスタム デバイス コレクションに適用できます。

以下のワークフローでは、カスタマイズ時のクイック リファレンスとして使用できるベストプラクティスを説明します。

管理者の役割を持つユーザとしてログインし、以下の手順を実行します。

1. ユーザのデバイスを監視するためのポーリング レートおよびメトリックをカスタマイズするために、新規の監視プロファイルを作成（またはファクトリ監視プロファイルのコピーを作成）します。
2. （オプション）カスタム監視プロファイルにイベント ルールを追加します (P. 163)。

3. （オプション）ファクトリ ベンダー認定および関連付けられたメトリック ファミリがニーズを満たさない場合は、カスタム ベンダー認定を作成して、新しいメトリック ファミリをインポートします。この手順はいつでも行うことがきます。

   注: カスタム メトリック ファミリおよびカスタム ベンダー認定の詳細については、「*Data Aggregator 自己認定ガイド*」を参照してください。

4. CA Performance Center でカスタム デバイス コレクションおよび関連付けルールを作成します。これらはその後、Data Aggregator デバイス コレクションとして使用されます。これらのデバイス コレクションを直ちに Data Aggregator と同期するか、または自動同期の発生を待つことができます。これらのデバイス コレクションへのデバイスの追加は、ディスカバリの後に手動で実行できます。

   注: MSP またはテナントの場合は、テナント管理者としてこの手順を実行します。監視対象グループの作成およびデータ ソースの同期の詳細については、「CA Performance Center 管理者ガイド」を参照してください。

5. 希望するポーリング レートが使用されるように、監視プロファイルおよびデバイス コレクションの関連付けをカスタマイズします (P. 102)。カスタム監視プロファイルを作成する場合、カスタム監視プロファイルをカスタム デバイス コレクションに関連付けて、監視プロファイルおよび関連するイベント ルールをアクティブにします。

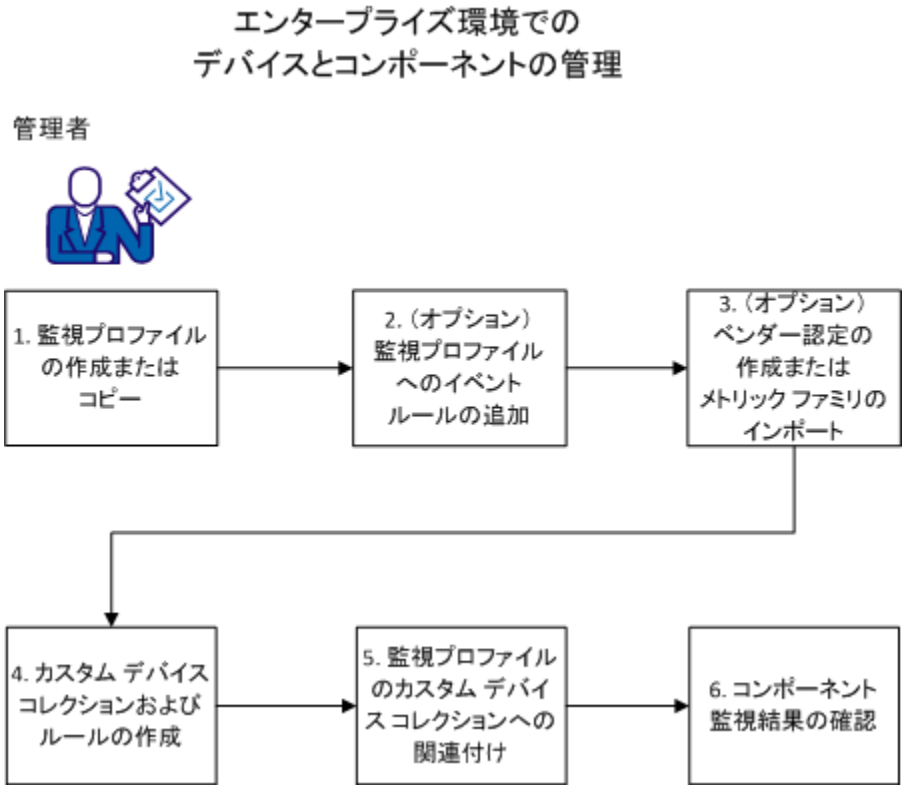
   注: MSP またはテナントの場合は、テナント管理者としてこの手順を実行します。

   カスタマイズでは、ファクトリ監視プロファイルとデバイス コレクション間の関連付けを削除したり、ファクトリ コレクションまたはカスタム デバイス コレクションのいずれかに、カスタム監視プロファイルを関連付けることもできます。

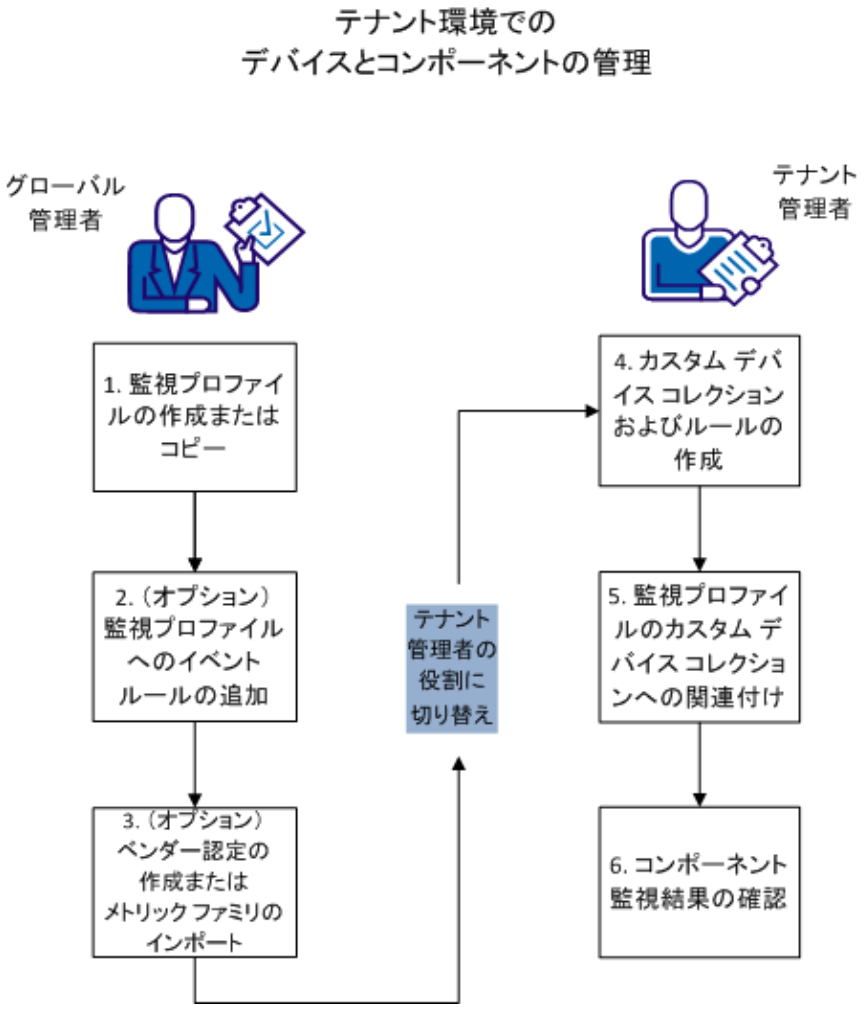
6. 新しい設定のポーリングが開始した後に、コンポーネント監視結果を確認して、必要な情報が収集されていることを確認します (P. 111)。

   注: MSP またはテナントの場合は、テナント管理者としてこの手順を実行します。

この図は、エンタープライズ環境のワークフローを示します。



この図は、テナント環境のワークフローを示します。



監視プロファイル

監視プロファイルは、デバイス コレクション内のデバイス用にどのような統計が検出されてポーリングされるか、およびポーリング速度を決定します。ファクトリ監視プロファイル一式が標準で用意されています。ファクトリ監視プロファイルは、［All Routers］デバイス コレクションなどのファクトリ デバイス コレクションに自動的に適用されます。 ファクトリ監視プロファイルは編集したりシステムから削除したりできません。しかし、デバイス コレクションから削除することや、コピーしてカスタム プロファイルを作成することが可能です。

管理者であれば、カスタマイズされた監視プロファイルを作成、編集、コピー、または削除できます。 カスタム監視プロファイルは、ユーザ インターフェース全体で利用可能になり、テナント ワークスペースで作業する MSP 管理者でも、テナントに限定されません （ただし、監視プロファイルが関連付けられるデバイス コレクションの有効範囲はテナント限定です）。 たとえば、「ゴールドサービス ルータ監視」監視プロファイルを作成してゴールド レベルのテナントすべてに対して使用できます。 ゴールド レベルのテナント*ごとに個別の*「ゴールドサービス ルータ監視」監視プロファイルを作成する必要はありません。

監視プロファイルの名前は、すべてのテナントにわたって一意である必要があります。

監視プロファイルを管理し、それらのデバイス コレクションとの関連を表示するには、CA Performance Center ユーザ インターフェースまたは Data Aggregator REST Web サービスを使用します。

ファクトリ監視プロファイルの関連付け

監視プロファイルは、ポーリングする統計を指定します。 標準で提供されるファクトリ監視プロファイルは、以下のようにデバイス コレクションと自動的に関連付けられます。

- ［Accessibility］監視プロファイルは［All Devices］デバイス コレクションと関連付けられます。
- ［Reachability］監視プロファイルは［All Devices］デバイス コレクションと関連付けられます。
- ［Router］監視プロファイルは［All Routers］デバイス コレクションと関連付けられます。
- ［Physical Server］監視プロファイルは［All Servers］デバイス コレクションと関連付けられます。
- ［Virtual Server］監視プロファイルは［All Servers］デバイス コレクションと関連付けられます。
- ［Switch］監視プロファイルは［All Switches］デバイス コレクションと関連付けられます。
- ［Microsoft Cluster Services］監視プロファイルは［All Servers］デバイス コレクションと関連付けられます。

- ［VMWare］監視プロファイルは［All VMare vCenters］デバイス コレクションと関連付けられます。
- ［VMware ESX Host］監視プロファイルは［All VMware vCenters］デバイス コレクションと関連付けられます。
- ［VMware Virtual Machine］監視プロファイルは［All VMware vCenters］デバイス コレクションと関連付けられます。

以下の監視プロファイルには、デバイス コレクションとのファクトリの関連付けがありません。 この仕様により、パフォーマンスに影響する大規模のディスカバリが回避できます。 手動でこれらの監視プロファイルをデバイス コレクションに割り当て、データを収集します。

- ネットワーク インターフェース
- レスポンス パス
- MPLS
- CBQoS

詳細:

ファクトリ デバイス コレクション (P. 105)
［All Devices］デバイス コレクション (P. 107)
［All Routers］デバイス コレクション (P. 107)
監視プロファイルのデバイス コレクションへの割り当てまたは削除 (P. 102)

監視プロファイルの表示

管理者は、監視プロファイルのリストおよびデバイス コレクションとの関連を参照できます。

- 管理者は、管理しているテナントのデバイス コレクションを参照できます。
- テナント管理者は、自身のデバイス コレクションのリストを参照できます。

この情報は、監視プロファイルおよびポーリング レートを管理する方法を決定するのに役立ち、デバイス コレクション用にどのようなレポート タイプを作成できるかがわかります。

以下の手順に従います。

1. Data Aggregator のデータ ソース用の［監視設定］メニューから［監視プロファイル］をクリックします。

   監視プロファイルのリストが表示されます。

2. 管理者であれば、システムに監視プロファイルを追加したり、監視プロファイルを選択して編集、コピー、または削除できます。 カスタムを含むすべての監視プロファイルは、グローバルです。

   注: ファクトリ監視プロファイルは編集、削除できません。カスタム監視プロファイルのみが変更できます。

3. 監視プロファイルを選択します。

4. 選択された監視プロファイルの詳細については、以下のようにタブに入力されます。

   - ［メトリック ファミリ］タブには、その特定の監視プロファイルと関連付けられたメトリック ファミリのリストが入力されます。 メトリック ファミリには、デバイスとインターフェースのポーリングに使用されるメトリックが含まれます。
   - ［イベント ルール］タブには、その特定の監視プロファイルと関連付けられたイベント ルールのリストが入力されます。 管理者であれば、ルールを割り当てたり削除することにより、イベント ルールと選択された監視プロファイルの関係を管理できます。
   - ［コレクション］タブには、その特定の監視プロファイルと関連付けられたデバイス コレクションのリストが入力されます。 テナント管理者として監視プロファイルを割り当てたり削除したりすることにより、デバイス コレクションと選択された監視プロファイルの関係を管理できます。

詳細:

トラブルシューティング： ポーリングが検出されたメトリック ファミリ上で停止する (P. 194)
デバイス再設定の自動更新 (P. 127)

監視プロファイルのデバイス コレクションへの割り当てまたは削除

管理者またはテナント管理者は、システム内の特定のデバイス コレクションと監視プロファイルの関係を追加または削除できます。 この機能により、デバイス コレクション中のデバイスとコンポーネントに関連する監視プロファイルと関連する統計のポーリングを開始または停止できます。

重要: 監視プロファイルをデバイス コレクションに割り当てるときは、多数の SNMP リクエストが発生します。これらのリクエストは、デバイスのパフォーマンスに影響を与えることがあります。 また、監視プロファイルを［All Devices］デバイス コレクションと関連付けないでください。 このような関連付けを行うと、余計な SNMP リクエストが Ping 可能デバイスに対して行われ、メトリック ファミリ サポートが断続的になる可能性があります。

たとえば、1,000 個の物理および論理インターフェースを持つルータが検出されました。 また、インターフェース監視プロファイルを作成して、その監視プロファイル上のポーリング レートを 1 分間に設定しました。 このインターフェース監視プロファイルを、ルータが含まれるデバイス コレクションに割り当てると、各インターフェースに対して 10 個の MIB オブジェクトがポーリングされます。 この設定により、応答する SNMP エージェントでは毎秒 166 個のレートで MIB オブジェクトが発生します。 この大きな SNMP 負荷は、ルータのパフォーマンスに影響を与える可能性があります。

QoS、MPLS、および IPSLA などのメトリック ファミリも、SNMP リクエストの増加に関与することがあります。 ネットワーク デバイスに対する SNMP リクエストの影響および制限事項の詳細については、ベンダーのマニュアルを参照するか、またはベンダーにお問い合わせください。

注: Data Aggregator は、複数のデバイス コレクションが監視プロファイルに割り当てられる場合に設定される、最も速いポーリング レートを使用します。 カスタム ポーリング レートを使用する場合は、デバイス コレクションと監視プロファイルのファクトリの関連付けを削除します。

以下の手順に従います。

1. Data Aggregator のデータ ソース用の［監視設定］メニューから［コレクション］をクリックします。

   コレクションのリストが表示されます。管理者は、管理しているテナントのデバイス コレクションを参照できます。テナント管理者は、自身の（テナントの）デバイス コレクションのリストを参照できます。

2. コレクションを選択し、［監視プロファイル］タブをクリックします。

   選択されたデバイス コレクションに割り当てられた監視プロファイルを示すリストが表示されます。

3. ［管理］をクリックします。

   ［監視プロファイルへのコレクションの割り当て］ダイアログ ボックスが表示されます。

4. 以下のいずれかを実行します。

   - ［利用可能な監視プロファイル］リストから 1 つ以上の監視プロファイルを選択し、［追加］をクリックします。

     選択された監視プロファイルは、［割り当てられた監視プロファイル］リストに移ります。

     監視プロファイルをデバイス コレクションに関連付けると、監視プロファイルに含まれているイベント ルールがアクティブになります。デバイス コレクション内のデバイスがイベント ルールの条件を満たすと、イベントが発生およびクリアされます。

   - ［割り当てられた監視プロファイル］リストから 1 つ以上の監視プロファイルを選択し、［削除］をクリックします。

     選択された監視プロファイルは、［利用可能な監視プロファイル］リストに移ります。

     注: 関係を削除しても監視プロファイルはシステムから削除されません。

5. ［保存］をクリックします。

   変更が保存されます。手順 2 を繰り返すことで確認できます。

詳細:

ファクトリ監視プロファイルの関連付け (P. 99)
トラブルシューティング： ポーリングが検出されたメトリック ファミリ上で停止する (P. 194)
デバイスおよびコンポーネント管理ワークフローのカスタマイズ (P. 95)
インターフェース フィルタを設定しアクティブにする方法 (P. 145)

caim--監視プロファイルポーリング フィルタの設定

フィルタリングでは、ポーリングするコンポーネント アイテムと、それらをポーリングする時間間隔を指定します。 ポーリングするコンポーネント アイテムを指定することにより、必要なコンポーネント アイテムのみを監視することができます。 *カスタム*監視プロファイルの場合は、追加フィルタを指定できます。

フィルタは、ディスカバリの実行前または実行後に追加/編集できます。 Data Aggregator はディスカバリの後にフィルタリングを適用します。 フィルタ条件に一致するコンポーネント アイテムのみがポーリングされます。 ディスカバリを実行した後でフィルタを追加または編集すると、これらのコンポーネント アイテムに関するポーリングは停止します。

注: このタスクを実行するには、管理者としてログインする必要があります。

以下の手順に従います。

1. リスト内に作成した監視プロファイルを選択します。

   選択した監視プロファイルの詳細が右側のペインに表示されます。デフォルトでは［メトリック ファミリ］タブが選択されます。

2. リスト内のメトリック ファミリの名前をクリックします。

   ペインの下部にある［フィルタの編集］ボタンと［フィルタのクリア］ボタンが使用できるようになります。

3. ［フィルタの編集］ボタンをクリックします。

   ［フィルタ式］ダイアログ ボックスが表示されます。

4. 既存の AND 条件をクリックし、ダイアログ ボックスの右側のロジック ボタンをクリックします。

5. 属性および操作を選択し、条件値を入力します。

6. ［条件の追加］ボタンをクリックします。

   作成した条件がフィルタ式に追加されます。

7. 追加の条件があれば作成します。

   ［条件の追加］ボタンをクリックして、各条件を追加します。

8. ［保存］ボタンをクリックします。フィルタ式が保存され、選択した［メトリック ファミリ］に割り当てられます。

注: コンポーネント アイテムと、これに割り当てられたフィルタを表示すると、フィルタが割り当てられていない各コンポーネント アイテムの隣にはアスタリスク（*）が表示されます。

ファクトリ デバイス コレクション

Data Aggregator および CA Performance Center は、*デバイス コレクション*と呼ばれる、監視対象デバイスの論理グループ化の概念をサポートしています。

Data Aggregator システムでデータを素早く取得し、製品をテストできるように、複数のファクトリ デバイス コレクションが標準で提供されています。 ディスカバリ中に検出されるデバイスは、タイプに応じてこれらのデバイス コレクションに追加されます。たとえば、ルータは［All Routers］ファクトリ デバイス コレクションに追加されます。 同期の際に、これらの監視対象デバイスは、CA Performance Center 内の対応するデバイス コレクションに追加されます。

次に、ファクトリ監視プロファイルが自動的にファクトリ デバイス コレクションに適用され、ユーザの介在なしに直ちにデータを収集できます。このデータが収集されると、データに対してレポートを実行して、ネットワークの状態をより詳細に把握することができます。

以下のファクトリ デバイス コレクションが用意されています。

- All Devices（P. 107）
- All Routers（P. 107）
- All Servers（P. 108）
- All Switches（P. 108）
- All Manageable Devices（P. 108）
- All ESX Hosts（P. 109）
- All Virtual Machines（P. 109）
- All VMware vCenters（P. 110）

注: ファクトリ デバイス コレクションは、主にラボまたはデモ環境で使用するためのものです。 実稼働環境では、詳細な制御および最適なデータ収集を行うためのカスタム デバイス コレクションを設計して設定することを推奨します。

［監視設定］メニューにアクセスし、デバイス コレクションのリストおよび、それぞれに適用される監視プロファイルを参照します。管理者は、管理しているテナントのデバイス コレクションを参照できます。 テナント管理者は、自身のデバイス コレクションのリストを参照できます。

詳細:

ファクトリ監視プロファイルの関連付け (P. 99)
トラブルシューティング： ポーリングが検出されたメトリック ファミリ上で停止する (P. 194)
カスタム デバイス コレクション (P. 110)

[All Devices]デバイス コレクション

［All Devices］デバイス コレクションはファクトリ デバイス コレクションです。ディスカバリ中に検出される、管理可能で Ping 可能なデバイスは、自動的に［All Devices］デバイス コレクションに追加されます。 アクセス不可能なデバイスは、［All Devices］デバイス コレクションに含まれません。

重要: 監視プロファイルを［All Devices］デバイス コレクションと関連付けないでください。このような関連付けを行うと、余計な SNMP リクエストが Ping 可能デバイスに対して行われ、メトリック ファミリ サポートが断続的になる可能性があります。

詳細:

ファクトリ デバイス コレクション (P. 105)
ファクトリ監視プロファイルの関連付け (P. 99)

[All Routers]デバイス コレクション

［All Routers］デバイス コレクションはファクトリ デバイス コレクションです。 ディスカバリ中に検出されるルータは、自動的に［All Routers］デバイス コレクションに追加されます。

注: ルータは、［All Routers］デバイス コレクションおよび［All Switches］デバイス コレクションの両方に表示されることがあります。

詳細:

ファクトリ デバイス コレクション (P. 105)
ファクトリ監視プロファイルの関連付け (P. 99)

[All Servers]デバイス コレクション

［All Servers］デバイス コレクションはファクトリ デバイス コレクションです。 ディスカバリ中に検出される物理サーバおよび仮想サーバ（ホスト）は、自動的に［All Servers］デバイス コレクションに追加されます。ルータやスイッチなどのネットワーク デバイスは［All Servers］デバイス コレクションに含まれません。

詳細:

ファクトリ デバイス コレクション (P. 105)
ファクトリ監視プロファイルの関連付け (P. 99)

[All Servers]デバイス コレクション

［All Switches］デバイス コレクションはファクトリ デバイス コレクションです。 ディスカバリ中に検出されるルータは、自動的に［All Switches］デバイス コレクションに追加されます。

注: スイッチは、［All Routers］デバイス コレクションおよび［All Switches］デバイス コレクションの両方に表示されることがあります。

詳細:

ファクトリ デバイス コレクション (P. 105)
ファクトリ監視プロファイルの関連付け (P. 99)

[All Manageable Devices]デバイス コレクション

［All Manageable Devices］デバイス コレクションはファクトリ デバイス コレクションです。 管理可能デバイスは詳細なパフォーマンス統計を収集し、SNMP などのプロトコルで監視されます。 ディスカバリ中に検出される管理可能なデバイスは、自動的に［All Manageable Devices］デバイス コレクションに追加されます。

Ping 可能デバイスは可用性についての監視のみができ、追加のパフォーマンス メトリックは提供されません。したがって、Ping 可能デバイスは［All Manageable Devices］デバイス コレクションに含まれていません。

注: 管理可能デバイスは、［All Devices］デバイス コレクションおよび、［All Manageable Devices］デバイス コレクションの両方に表示されることがあります。

詳細:

ファクトリ デバイス コレクション (P. 105)

［All ESX Hosts］デバイス コレクション

［All ESX Hosts］デバイス コレクションはファクトリ デバイス コレクションです。ディスカバリ中に検出される ESX ホストは、自動的に［All ESX Hosts］デバイス コレクションに追加されます。

詳細:

ファクトリ デバイス コレクション (P. 105)
ファクトリ監視プロファイルの関連付け (P. 99)

［All Virtual Machines］デバイス コレクション

［All Virtual Machines］デバイス コレクションはファクトリ デバイス コレクションです。ディスカバリ中に検出される VMware 仮想マシンは、自動的に［All Virtual Machines］デバイス コレクションに追加されます。

詳細:

ファクトリ デバイス コレクション (P. 105)
ファクトリ監視プロファイルの関連付け (P. 99)

[All VMware vCenters]デバイス コレクション

［All VMware vCenters］デバイス コレクションはファクトリ デバイス コレクションです。ディスカバリ中に検出される、VCAIM と共に systemEdge を実行しているすべてのサーバは、自動的に［All VMware vCenters］デバイス コレクションに追加されます。

詳細:

ファクトリ デバイス コレクション (P. 105)
ファクトリ監視プロファイルの関連付け (P. 99)

カスタム デバイス コレクション

ファクトリ デバイス コレクションは、主にラボまたはデモ環境で使用するためのものです。 実稼働環境では、詳細な制御および最適なデータ収集を行うためのカスタム デバイス コレクションを設計して設定することを推奨します。 たとえば、関連付けられているプロファイルを監視しているほかのデバイス コレクションからデバイスの関連付けを解除して、ポーリングを無効にすることができます。 監視プロファイルを（［All Routers］などの）ファクトリ デバイス コレクションに関連付けている場合は、単一デバイスのポーリングを停止することはできません。 ファクトリ デバイス コレクションからデバイスを削除することができないため、ポーリングを無効化するかわりに、監視プロファイルの関連付けを解除します。 その後で、同じポーリング ポリシーを適用したいデバイスを含むカスタム デバイス コレクションを作成します。 監視プロファイル（またはカスタム監視プロファイル）をそれらのカスタム デバイス コレクションに関連付けて、ポーリングを開始します。

CA Performance Center でカスタム デバイス コレクションを作成し、次に、すぐに Data Aggregator で同期するか、自動同期を待機します。同期では、Data Aggregator がデバイス監視で使用する、対応するデバイス コレクションを作成します。

注: カスタム デバイス コレクションの作成および Data Aggregator との同期の詳細については、「*CA Performance Center 管理者ガイド*」を参照してください。

［監視設定］メニューにアクセスし、デバイス コレクションのリストおよび、それぞれに適用される監視プロファイルを参照します。管理者は、管理しているテナントのデバイス コレクションを参照できます。 テナント管理者は、自身のデバイス コレクションのリストを参照できます。

詳細情報:

ファクトリ デバイス コレクション (P. 105)

監視対象デバイスの表示

監視対象デバイスの詳細とともに、これらのデバイスとデバイス コレクション、コンポーネント、監視プロファイル、メトリックとの関連を表示できます。 また、フィルタ レポートも表示できます。 この情報は、どの監視プロファイルがデバイス コンポーネントのポーリングに使用されているかなどのコンテキスト情報を参照するのに役立ちます。

注: 一部の機能には管理者権限が必要です。

監視対象デバイスは、管理可能または Ping 可能（アクセス可能で管理不可）です。アクセス不可能なデバイスは監視対象デバイスではありません。監視対象デバイスのコンポーネントは［ポーリングされるメトリック ファミリ］タブで表示できます。

以下の手順に従います。

1. Data Aggregator データ ソースの［監視対象インベントリ］メニューから［監視対象デバイス］をクリックします。

   ［ツリー表示］タブが表示されます。

2. ドロップダウン リストから［コレクション別デバイス］または［監視プロファイル別デバイス］を選択し、対応するツリー表示から特定のデバイスを選択します。

   注: あるいは、［検索］タブを選択し、ホスト名、デバイス名または IP アドレスで検索します。 名前の一部または IP アドレスを入力すると、部分一致するデバイスのリストが返されます。 ワイルドカードと正規表現はサポートされていません。

［詳細］タブには、選択された監視対象デバイスの詳細が表示されます。 確認できる詳細には、デバイスの IP アドレス、関連する SNMP プロファイル、デバイスのステータスなどがあります。IP アドレス、Data Collector ホスト、SNMP プロファイル、デバイスの SNMP バージョンを編集することもできます。

デバイスの IP アドレスを編集する方法には次の 2 通りがあります。

- ［IP アドレス］フィールドを編集し、［保存］をクリックします。
- ［IP アドレス]テーブルの IP アドレスを右クリックし、［この IP をデバイスのプライマリ IP として設定］を選択して、［保存］をクリックします。

注: このビューには管理可能デバイスに関する情報が他にも表示されています。

（オプション）［再検出］をクリックして、デバイスを再検出します。このディスカバリの結果、以下の属性セットが更新されます。

- システム名
- ホスト名
- デバイス タイプ（CA Performance Center に表示）
- 場所
- ベンダー
- デバイスの説明
- デバイス モデル

注: デバイス属性を変更すると、デバイスが属するグループおよびデバイス コレクションが変更される場合があります。グループおよびデバイス コレクションの変更により、監視プロファイルが追加または削除される可能性があります。

デバイスが再検出されたことを確認するには、再検出がトリガしたイベントを探します。イベントを表示するには、CA Performance Center の［ダッシュボード］メニューをクリックし、［操作の表示］の下の［イベントの表示］を選択します。

3. （オプション） 設定更新に対してコンポーネントを再設定するには、メトリック ファミリを選択し、［メトリック ファミリの更新］をクリックします。たとえば、サーバのディスク ドライブを追加する場合、設定更新を再検出するために［メトリック ファミリの更新］ボタンを使用できます。 この設定更新により、ディスク コンポーネントが作成されます。

4. 別のタブを選択します。

   - ［ポーリングされるメトリック ファミリ］タブには、デバイス上でポーリングされるメトリック ファミリの合計セットと、そのポーリング レートが表示されます。 この合計セットは、デバイス上のすべての監視プロファイルを集約したものです。 また、このタブには、デバイスがメトリック ファミリをサポートするかどうかが示されます。

     所定のメトリック ファミリの［コンポーネント］テーブルには、以前に検出されたメトリック ファミリ コンポーネント用のコンポーネントのポーリング ステータスが表示されます。 以下のいずれかが［ステータス］列に表示されます。

     アクティブ

     コンポーネントがポーリングされていることを示します。

     非アクティブ

     デバイスのメトリック ファミリが監視されなくなったため、コンポーネントでのポーリングが停止したことを示します。

     廃棄済み

     コンポーネントが物理デバイスに存在しなくなったことを示します。 コンポーネントへのポーリングは停止されます。 レポート目的で履歴データを表示できます。デフォルトでは、廃棄済みのコンポーネントは CA Performance Center と同期されません。 このオプションを有効にするには、CA Performance Center 内の［データ ソースの管理］ページにある［データ ソースの編集］ダイアログ ボックスで、［廃止されたアイテムの同期］チェック ボックスをオンにします。

     （オプション） 設定更新に対してコンポーネントを再設定するには、メトリック ファミリを選択し、［メトリック ファミリの更新］をクリックします。 たとえば、サーバのディスク ドライブを追加する場合、設定更新を再検出するために［メトリック ファミリの更新］ボタンを使用できます。 この設定更新により、ディスク コンポーネントが作成されます。

- ［しきい値プロファイル］タブには、選択したデバイスが属するグループを通じてそのデバイスに適用されるしきい値プロファイルが表示されます。
- ［監視プロファイル］タブでは、デバイス コレクションを選択して、関連するプロファイル名を参照できます。 説明を参照するには、プロファイルの上にマウス ポインタを置きます。
- ［メトリック］タブには、このデバイスがサポートするメトリックのリストが入力されています。 詳細を表示するメトリック ファミリを選択します。 サポートしているベンダー認定、ベンダー ソース（SNMP ベンダー認定である場合、MIB テーブル ソースが表示されます）、および各メトリックを計算するために使用される式が表示されます。
- ［フィルタ レポート］タブには、コンポーネント監視中に使用されたインターフェース フィルタ条件が表示されます。 またこのタブには、デバイスで識別されたすべてのインターフェースのレポートと、これらが指定したフィルタ条件と一致したかどうかが表示されます。 カスタム監視プロファイルのルールを変更する場合、［インターフェース フィルタ条件］ペインにはこの変更が反映されません。 監視プロファイルとグループの関連付けを解除する場合、［インターフェース フィルタ条件］ペインにはこの変更が反映されません。 フィルタ条件および監視プロファイルに対して行った変更に基づいてインターフェースをフィルタするために、デバイスを再検出します。

詳細情報:

ディスカバリとポーリング (P. 69)
デバイス再設定の手動更新 (P. 129)
インターフェース フィルタのクリア (P. 147)
トラブルシューティング： ポーリングが検出されたメトリック ファミリ上で停止する (P. 194)
インターフェース フィルタを設定しアクティブにする方法 (P. 145)

デバイスの削除

検出されたデバイスを削除できます。 たとえば、監視を停止する場合に検出されたデバイスを削除します。

デバイスを削除すると、以下の結果が発生します。

- 関連付けられたデバイス コンポーネントがすべて削除されます。
- 削除されたデバイスおよびデバイス コンポーネント上の履歴データにアクセスできなくなります。

注: 既存のディスカバリ プロファイルを再実行すると、削除されたデバイスを再検出できます。

以下の手順に従います。

1. Data Aggregator データ ソース用の［監視対象インベントリ］メニューから［監視対象デバイス］をクリックします。

   ［ツリー表示］タブが表示されます。

2. ［検索］タブを選択します。

   注: ページ上部のグローバル検索ボックスを使用しないでください。

3. 削除する監視対象デバイスを検索するには、ローカルの［検索］ボックスにテキストを入力します。ホスト名、デバイス名、または IP アドレスによって検索できます。部分的な一致を含むデバイスのリストを返すために、名前の一部または IP アドレスを入力できます。

   注: ワイルドカードと正規表現はサポートされていません。

   一致するデバイスのリストが返されます。

4. 以下の手順のいずれかを実行します。

   - 削除する監視対象デバイス（1 つまたは複数）を選択し、［削除］をクリックします。
   - 結果リスト内のデバイスをすべて削除するには、［名前］列の横にあるチェック ボックスをオンにして、［削除］をクリックします。

   確認ダイアログ ボックスが表示されます。

5. ［はい］をクリックし、削除を確定します。

   デバイスは削除され、［監視対象デバイス］インベントリ内に表示されなくなります。別のデータ ソースがこれらのデバイスを管理していない場合、Data Aggregator が次回に CA Performance Center と同期すると、そのデバイスは［インベントリ］ビューに表示されなくなり、グループ メンバから削除されます。

監視対象デバイスのプライマリ IP アドレスの変更

監視対象デバイスのプライマリ IP アドレスを変更できます。

以下の手順に従います。

1. Data Aggregator データ ソースの［監視対象インベントリ］メニューから［監視対象デバイス］をクリックします。

   ［ツリー表示］タブが表示されます。

2. ドロップダウン リストから［コレクション別デバイス］または［監視プロファイル別デバイス］を選択し、対応するツリー表示から特定のデバイスを選択します。

   注: あるいは、［検索］タブを選択し、ホスト名、デバイス名または IP アドレスで検索します。 名前の一部または IP アドレスを入力すると、部分一致するデバイスのリストが返されます。 ワイルドカードと正規表現はサポートされていません。

3. プライマリ IP アドレスを変更するには、以下のいずれかの手順を実行します。

   - ［IP アドレス］フィールドを編集し、［保存］をクリックします。
   - ［IP アドレス]テーブルの IP アドレスを右クリックし、［この IP をデバイスのプライマリ IP として設定］を選択して、［保存］をクリックします。

   プライマリ IP アドレスが変更されます。

廃止されたコンポーネントの削除

Data Aggregator には、廃止されたコンポーネントを削除するためのスクリプトが含まれます。 廃止されたコンポーネントとは、物理デバイスに存在しなくなったコンポーネントです。 廃止されたコンポーネントが多すぎると、ユーザ インターフェースのパフォーマンスに影響を与える場合があります。 廃止されたコンポーネントを削除するために、このスクリプトの使用方法を説明します。

注: 廃止されたコンポーネントの削除を自動化するには、「*Data Aggregator REST Web サービスを使用した管理ガイド*」を参照してください。

以下の手順に従います。

1. コマンドプロンプトを開き、/opt/IMDataAggregator/scripts ディレクトリにアクセスします。
2. 廃止されたコンポーネントを削除するスクリプトを呼び出すには、以下のコマンドを入力します。

   ```
   ./remove_retired_items.sh
   ```

   スクリプト パラメータのリストと説明が表示されます。

例: 廃止されたコンポーネントの総数を返す

1. 以下のコマンドを入力します。

   ```
   ./remove_retired_items.sh -h host_name
   ```

   -h *host_name*

   接続する Data Aggregator ホスト名を指定します。

   廃止されたコンポーネントの総数が表示されます。
2. （オプション）廃止されたコンポーネントの*名前*のリストを返すには、数字の「1」を入力します。
3. （オプション）廃止されたコンポーネントをすべて削除するには、数字の「1」を入力します。

例: 特定の条件で、廃止されたコンポーネントのリストをフィルタリングする

1. 廃止されたコンポーネントを削除するスクリプトを呼び出すには、以下のコマンドを入力します。

   ```
   ./remove_retired_items.sh
   ```

   スクリプト パラメータのリストと説明が表示されます。
2. 特定の条件で廃止されたコンポーネントを削除します。
   - 複数の Data Collector インスタンスがインストールされている場合、IP アドレスが重複している可能性があります。 廃止されたコンポーネントを IP アドレスによってフィルタリングするには、以下の手順に従います。
     a. 以下のコマンドを入力します。

        ```
        ./remove_retired_items.sh -h host_name -a device_IP_address
        ```

     b. **注**: IP アドレスの範囲は入力できません。

c. （オプション）廃止されたコンポーネントの*名前*のリストを返すには、数字の「1」を入力します。

d. （オプション）廃止されたコンポーネントをすべて削除するには、数字の「1」を入力します。

- 廃止されたコンポーネントの経過期間（経過日数内）によって削除するには、以下のコマンドを入力します。

  ```
  ./remove_retired_items.sh -h host_name -t
  filter_by_days_old_from_current_time
  ```

  たとえば、以下のコマンドは、廃止されてからの日数が、現在の時刻から数えて 10 日未満であるコンポーネントを削除します。

  ```
  ./remove_retired_items.sh -h host_name -t 10
  ```

例: 多数の廃止コンポーネントの削除

廃止されたコンポーネントの数が 100,000 を超えている場合、そのすべてを容易に削除できます。

- 廃止されたコンポーネントの数が 100,000 を超えている場合に、そのすべてを確認するには、以下のコマンドを入力します。

  ```
  ./remove_retired_items.sh -h host_name –o ouputfile
  ```

  -o *outputfile*

  すべての廃止コンポーネントの出力です。 出力は .csv ファイルです。

  たとえば、以下のコマンドは、すべての廃止されたコンポーネントのリストを出力します。 .csv ファイル形式には、デバイス アイテム ID、デバイス表示名、廃止されたコンポーネント ID、および廃止されたコンポーネント表示名が含まれます。

  ```
  ./remove_retired_items.sh -h my_host_name –o myretired.csv
  ```

- 廃止されたコンポーネントの数が 100,000 を超えている場合にそのすべてを削除し、.csv ファイルに情報を記録するには、以下のコマンドを入力します。

  ```
  ./remove_retired_items.sh -h host_name –o ouputfile –c Yes
  ```

  -o *outputfile*

  すべての廃止コンポーネントの出力です。 出力は .csv ファイルです。

  –c Yes

  廃止されたすべてのコンポーネントの削除を確定します。

  たとえば、以下のコマンドは廃止されたすべてのコンポーネントを削除します。

  ```
  ./remove_retired_items.sh -h my_host_name –o myretired.csv –c Yes
  ```

廃止されたコンポーネントの削除について、さらに詳しく説明します。

- 廃止コンポーネントを IP ドメイン名または IP ドメイン ID によってフィルタリングする場合も、特定の IP アドレスを指定すると正しい結果が返されます。
- フィルタ条件によって返される廃止コンポーネントの数が多すぎる場合、REST インターフェースは応答を返しません。その他のフィルタリング オプションを使用して、返される結果の範囲を絞ります。フィルタ条件の詳細については、http://*hostname*:*port*/rest/retired/xsd/filterselect.xsd を参照してください。

IP ドメインの削除

IP ドメインを削除できます。 たとえば、2 つ以上のドメインをマージするときに IP ドメインを削除できます。 また、テストの目的で使用した IP ドメインを削除できます。 IP ドメインを削除すると、関連付けられているデバイスおよびデバイス コンポーネントはすべて削除されます。また、IP ドメインを削除すると、その IP ドメインと関連付けられたディスカバリ プロファイルが無効になります。

CA Performance Center 内の IP ドメインを削除します。 IP ドメインを削除した後、削除を Data Aggregator と同期することも、または自動同期が発生するのを待つこともできます。

注: IP ドメインの削除および同期の詳細については、「CA Performance Center 管理者ガイド」を参照してください。

一度 IP ドメインが削除されたことが Data Aggregator で認識されると、以下の処理が行われます。

- 削除された IP ドメインと関連付けられるデバイスおよびデバイス コンポーネントがすべて削除されます。
- 削除された IP ドメインに関連付けられた Data Collector が停止します。ステータスには［データ収集なし］と表示されます。

  注: Data Collector がダウンしているときに IP ドメインを削除できます。Data Collector が再稼働すると、*Data Collector のインストール ディレクトリ*/apache-karaf-2.3.0/shutdown.log ファイルにエラー メッセージが表示され、すぐに Data Collector がシャットダウンします。
- 削除された IP ドメインを指定するディスカバリ プロファイルはすべて無効になり、実行できません。 状態は［データ収集なし］になります。削除された IP ドメインで実行中のディスカバリはすべてアボートされます。

  注: 無効な状態のディスカバリ プロファイルを「準備完了」状態に戻すことができます。そのためには、デバイスを検出する有効な IP ドメインを指定します。
- 監査イベントはそれぞれの削除されたデバイスに関連付けられたテナント アイテムで生成されます。

詳細情報:

ディスカバリ プロファイル (P. 73)

テナントの削除

テナントを削除できます。 たとえば、ユーザが管理対象サービス プロバイダ（MSP）の場合、テナントが顧客でなくなったときにテナントを削除できます。テナントを削除すると、テナントに関連付けられたデバイス、デバイス コンポーネント、IP ドメイン、SNMP プロファイル、およびディスカバリ プロファイルがすべて削除されます。

注: デフォルト テナントは削除できません。

CA Performance Center 内のテナントを削除します。テナントを削除した後、手動で削除を Data Aggregator と同期することも、または自動同期が発生するのを待つこともできます。

注: テナントの削除および同期の詳細については、「CA Performance Center 管理者ガイド」を参照してください。

一度テナントが削除されたことが Data Aggregator によって認識されると、以下のイベントが実行されます。

- 削除されたテナントに関連付けられたすべてのデバイス、デバイス コンポーネント、IP ドメイン、SNMP プロファイル、およびディスカバリ プロファイルが削除されます。
- 削除されたデバイスおよびデバイス コンポーネント上のポーリングが停止します。
- 削除されたデバイスおよびデバイス コンポーネント上の履歴データにアクセスできなくなります。
- 削除された各テナントの Data Aggregator デバイス上で監査イベントが生成されます。
- 削除されたデバイス、およびその削除されたコンポーネントのしきい値イベントがすべて削除されます。

注: Data Collector がダウンしているときに、テナントを削除できます。Data Collector が再稼働すると、*Data Collector のインストール ディレクトリ*/apache-karaf-2.3.0/shutdown.log ファイルにエラー メッセージが表示され、すぐに Data Collector がシャットダウンします。

テナントの無効化

テナントを無効にできます。 たとえば、ユーザが管理対象サービス プロバイダ（MSP）の場合、テナント インフラストラクチャのアクティブな監視を停止するときに、テナントを無効にできます。

注: このタスクを実行するには、管理者としてログインする必要があります。

CA Performance Center 内のテナントを無効にします。テナントを無効にした後、無効化を Data Aggregator と同期することも、または自動同期が発生するのを待つこともできます。

注: テナントの無効化の詳細については、「CA Performance Center 管理者ガイド」を参照してください。

テナントが無効化されたことが Data Aggregator によって認識されると、以下の結果が発生します。

- Data Aggregator システムは、無効にしたテナントと関連付けられている Data Collector ホストをすべて停止します。Data Collector ホストには、［データ収集なし］のステータスが表示されます。 （テナントを再度有効にする場合は、Data Collector ホストを手動で再起動する必要があります。）

  注: 無効なテナントに対するすべての新規 Data Collector インストールについては、［データ収集なし］ステータスが表示されます。 テナントが再度有効になった場合にのみ、ディスカバリが許可されます。
- 無効化されたテナントに関連付けられたすべてのデバイス、デバイス コンポーネント、IP ドメイン、SNMP プロファイル、およびディスカバリ プロファイルは引き続き存在します。
- 無効化されたテナントに代わって監視されているデバイスおよびコンポーネントに対し、ポーリングが停止されます。
- テナント用のデバイスおよびコンポーネントの履歴データはアクセス可能なままです。
- 無効化されたテナントと関連付けられたディスカバリ プロファイルは無効になり実行できません。ディスカバリ プロファイルは［テナント無効］の状態になります。

- ディスカバリの実行中に対象のディスカバリ プロファイルが無効になると、そのディスカバリはアボートされます。
- 無効化されたテナントの Data Aggregator デバイスで監査イベントが生成されます。

詳細情報:

テナントの有効化 (P. 123)

テナントの有効化

以前に無効にしたテナントを有効にできます。 たとえば、ユーザが管理対象サービス プロバイダ（MSP）の場合、テナント インフラストラクチャのアクティブな監視を再開するときに、テナントを有効にできます。

注: このタスクを実行するには、管理者としてログインする必要があります。

CA Performance Center 内のテナントを有効にします。テナントを有効にした後、以下のアクションを実行します。

1. アクティブ化を Data Aggregator と同期することも、または自動同期が発生するのを待つこともできます。

   注: テナントの有効化の詳細については、「CA Performance Center 管理者ガイド」を参照してください。

   以下の結果が生じます。

   - テナントが有効化されたことが Data Aggregator によって認識されます。
   - 有効化されたテナントと関連付けられたディスカバリ プロファイルが有効になります。 ディスカバリ プロファイルに現在の状態が表示されます。
   - テナントの Data Aggregator デバイスで監査イベントが生成されます。
2. テナントと関連付けられている Data Collector ホストをすべて手動で再起動します (P. 59)。

以下の結果が生じます。

- 有効化されたテナントに代わって監視されているデバイスおよびコンポーネントに対し、ポーリングが再起動されます。
- 有効化されたテナントと関連付けられたディスカバリ プロファイルを実行できます。

詳細情報:

テナントの無効化 (P. 122)
トラブルシューティング： ディスカバリが開始しない (P. 193)

デバイスの再設定

デバイス コンポーネントを最新状態に維持するため、Data Aggregator でデバイスの再設定変更を監視し、自動または手動で更新することができます。デバイス再設定には、物理デバイス コンポーネントへの変更、およびソフトウェアの設定変更（プロトコルの監視レスポンス パス テストなど）が含まれます。Data Aggregator は、両タイプの再設定の監視に同じメソッドを使用します。

再設定の変更の追加例には、以下のものがあります。

- デバイスにボードを追加し、デバイスのポートを増設する。
- 検出されたデバイスにメモリ、CPU、物理インターフェース、または任意のメトリック ファミリを追加する。
- 仮想スイッチを再設定する。
- ルーティング プロトコルに検出されたデバイスが含まれるようにデバイスの設定を変更する。

変更が検出されると、Data Aggregator は再設定イベントを生成し、メトリック ファミリの表示を更新してデバイス コンポーネントの変更を反映できます。 再設定イベントを確認するには、［ダッシュボード］-［操作］-［イベントの表示］を選択します。

Data Aggregator で変更検出がどのように動作しているかを理解しておくと、環境内の監視デバイスを再設定するにあたり最適なオプションを選択するのに役立ちます。 たとえば、変更検出を監視する頻度を設定できます。

詳細情報:

変更検出を管理する方法 (P. 125)

変更検出を管理する方法

変更検出の管理を計画すると、ニーズに応じて、Data Aggregator による環境内のデバイス再設定の検出および監視を確実に実行することができます。Data Aggregator を最初にセットアップして新しいデバイスを検出する際に、デバイスの再設定をあらかじめ計画することができます。または、デバイスが検出された後に、これらのオプションをいつでも編集できます。

ユーザの行う選択は以下に基づきます。

- 変更の可能性。
- 予想される変更の頻度。
- 古いデータをどこまで許容するか。

メトリック ファミリには、CPU など、まれに再設定を監視する必要のあるものがあります。一方で、仮想システムなど、より動的なメトリック ファミリについては、より頻繁なレートを選択します。

変更検出を設定するための基本的なプロセスは次のとおりです。

1. *カスタム*監視プロファイルを作成または編集します（ファクトリ監視プロファイルをコピーし、そのコピーを編集することもできます）。
2. 監視プロファイルで、［変更検出の有効化］を選択し、［変更検出の設定］の検出レートを設定します。

   ［変更検出の設定］の［検出レート］オプションは、Data Aggregator が変更をチェックする頻度を設定するために使用されます。検出のレートは、分単位または時間単位で設定できます。デフォルトでは、レートは 24 時間に設定されています。

   注: メトリック ファミリが変更される頻度、および監視プロファイルが適用されるデバイスの数を考慮します。設定変更の検出が必要以上に頻繁に行われないようにする必要があります。

3. Data Aggregator でのメトリック ファミリの表示を更新します。

   変更の検出レートを設定した後、Data Aggregator 設定の修正にはメトリック ファミリの自動更新または手動更新の 2 つのオプションがあります。 このオプションはメトリック ファミリを更新しません。 代わりに、正しいコンポーネント セットが監視されていることを確認して、メトリック ファミリの表示を更新します。

   - ［自動的にメトリック ファミリを更新する］オプション（デフォルトの選択）をオンにするということは、再設定が検出された場合にユーザが介在する必要はないということです。Data Aggregator は自動的にすべての新しいコンポーネントの監視を開始し、再設定イベントが発生すると、検出されなくなったすべてのコンポーネントを削除します。

     ［イベントの表示］ダッシュボードを表示して、再設定イベントを参照します。

     - デバイスのコンポーネントが変更された場合、関連するデバイス上でイベントが生成されます。このイベントは、コンポーネントの変更が検出され、短期間で適用されることを示します。
     - コンポーネントの調整が適用された後、別のイベントが生成されます。このイベントは、追加、廃棄、および未変更のコンポーネント数を示します。

   - ［自動的にメトリック ファミリを更新する］オプションをオフにするということは、Data Aggregator は新しいコンポーネントの自動監視を開始することも、古いコンポーネントを削除することもないということです。

     ［イベントの表示］ダッシュボードを表示して、再設定イベントを参照します。

     - デバイスのコンポーネントが変更された場合、関連するデバイス上でイベントが生成されます。このイベントは、コンポーネントの変更が発生したが、調整が発生しなかったことを示します。

     再設定の変更を適用するには、デバイスの［ポーリングされるメトリック ファミリ］ページにある［メトリック ファミリの更新］ボタンを手動でクリックします。

4. 監視プロファイルをアクティブにするには、カスタム監視プロファイルをデバイス コレクションに割り当てます。

例:

- ご使用の環境で大規模なメンテナンスが行われていることが分かっている場合は、主要メンテナンスが終了するまで、自動更新をオフにすることができます。 小規模な通常の変更については、自動更新の機能を有効にしておくと、Data Aggregator を最新の状態に保つことができます。
- 監視プロファイルは、デバイスが含まれるデバイス コレクションに割り当てられます。 個別に監視することが望ましい特殊デバイスがある場合、この特殊デバイス用のカスタム デバイス コレクションを作成し、目的の変更検出を設定したカスタム監視プロファイルを割り当てます。 たとえば、重要なコア ルータ デバイス コレクションを作成し、変更検出を一時間ごとに実行するカスタム監視プロファイルを割り当てることにより、重要なコア ルータを他のルータより頻繁にモニタすることができます。 そのほかのルータは、（変更検出なしの）ファクトリ監視プロファイル、または変更検出頻度を低く設定したカスタム監視プロファイルを使用して、［All Routers］デバイス コレクションに含めたままにすることができます。

詳細:

ディスカバリとポーリング (P. 69)
デバイス再設定の手動更新 (P. 129)
デバイス再設定の自動更新 (P. 127)

デバイス再設定の自動更新

検出されたデバイスに対する再設定の変更は、そのデバイスに関連付けられているメトリック ファミリに影響します。 デバイス再設定が自動更新されるように、メトリック ファミリが割り当てられている監視プロファイルで設定できます。この設定は監視プロファイルに含まれるすべてのメトリック ファミリに適用されます。 このオプションはカスタム監視プロファイルの作成時にデフォルトで設定されていますが、いつでも編集することができます。 この手順では、以前に選択解除された既存のカスタム監視プロファイルで［自動的にメトリック ファミリを更新する］オプションを設定する方法について説明します。

メトリック ファミリが更新されると、Data Aggregator にデバイス設定が正確に表示されます。 生成するレポートにも正確な情報が反映されます。

以下の手順に従います。

1. すべての監視プロファイルのリストに移動します。
2. 自動で更新する監視プロファイルを選択し、［編集］をクリックします。
3. ［変更検出の有効化］を選択し、次に以下の手順に従います。
   - ［変更検出の設定］の［レート］をゼロより大きい値に設定します。

     注: メトリック ファミリが変更される頻度、および監視プロファイルが適用されるデバイスの数を考慮します。 設定変更の検出が必要以上に頻繁に行われないようにする必要があります。
   - ［自動的にメトリック ファミリを更新する］を選択します。
   - ［保存］をクリックします。

   この監視プロファイルに関連付けられているデバイスの設定変更を行うと、デバイス設定は自動的に更新されます。

   デバイス設定が更新されると、Data Aggregator が以下の手順を行います。

   - 監視対象デバイス上でイベントを生成します。
   - 新規コンポーネントが識別および作成されます。
   - 存在しなくなったコンポーネントが識別され、廃止されます。

     注: デフォルトでは、廃止されたコンポーネントは CA Performance Center と同期されません。 このオプションを有効にするには、CA Performance Center 内の［データ ソースの管理］ページにある［データ ソースの編集］ダイアログ ボックスで、［廃止されたアイテムの同期］チェック ボックスをオンにします。
   - 前回のディスカバリから変更された既存のコンポーネントが識別されます。 該当する場合は、［名前］列が変更されます。

     注: 履歴データにはアクセス可能で、レポートも生成できます。

詳細:

変更検出を管理する方法 (P. 125)

デバイス再設定の手動更新

検出されたデバイスに対する再設定の変更は、そのデバイスに関連付けられているメトリック ファミリに影響します。 関連付けられている監視プロファイルで［自動的にメトリック ファミリを更新する］オプションが選択されていない場合、デバイス再設定を手動で更新できます。 この場合、イベント ログを表示してメトリック ファミリを更新する再設定イベントを識別します。

メトリック ファミリが更新されると、Data Aggregator にデバイス設定が正確に表示されます。 生成するレポートにも正確な情報が反映されます。

以下の手順に従います。

1. メトリック ファミリを更新する再設定イベントを識別するために、イベント ログを表示します。（P. 168）
2. Data Aggregator データ ソースの［監視対象インベントリ］メニューから［監視対象デバイス］をクリックします。

   ［ツリー表示］タブが開きます。
3. ドロップダウン リストから［コレクション別デバイス］を選択し、対応するツリー表示から更新された監視対象デバイスを選択します。

   ［ポーリングされるメトリック ファミリ］タブには、デバイスと関連付けられた統合監視プロファイルが表示されます。デバイスが持つ統合監視プロファイルは 1 つのみです。 統合監視プロファイルにはそれぞれ、デバイス上でポーリング可能なすべてのメトリック ファミリ、およびデバイスがメトリック ファミリをサポートしているかどうかが一覧表示されます。

4. 設定を更新するメトリック ファミリを選択し、［メトリック ファミリの更新］をクリックします。

   デバイス設定が更新され、Data Aggregator によって以下の手順が実行されます。

   - 監視対象デバイス上でイベントを生成します。
   - 新規コンポーネントが識別および作成されます。
   - 存在しなくなったコンポーネントが識別され、廃止されます。

     注: デフォルトでは、廃止されたコンポーネントは CA Performance Center と同期されません。 このオプションを有効にするには、CA Performance Center 内の［データ ソースの管理］ページにある［データ ソースの編集］ダイアログ ボックスで、［廃止されたアイテムの同期］チェック ボックスをオンにします。
   - 前回のディスカバリから変更された既存のコンポーネントが識別されます。 該当する場合は、［名前］列が変更されます。

     注: 履歴データにはアクセス可能で、レポートも生成できます。

詳細:

監視対象デバイスの表示 (P. 111)
変更検出を管理する方法 (P. 125)

第 5 章: インターフェースの管理

このセクションには、以下のトピックが含まれています。

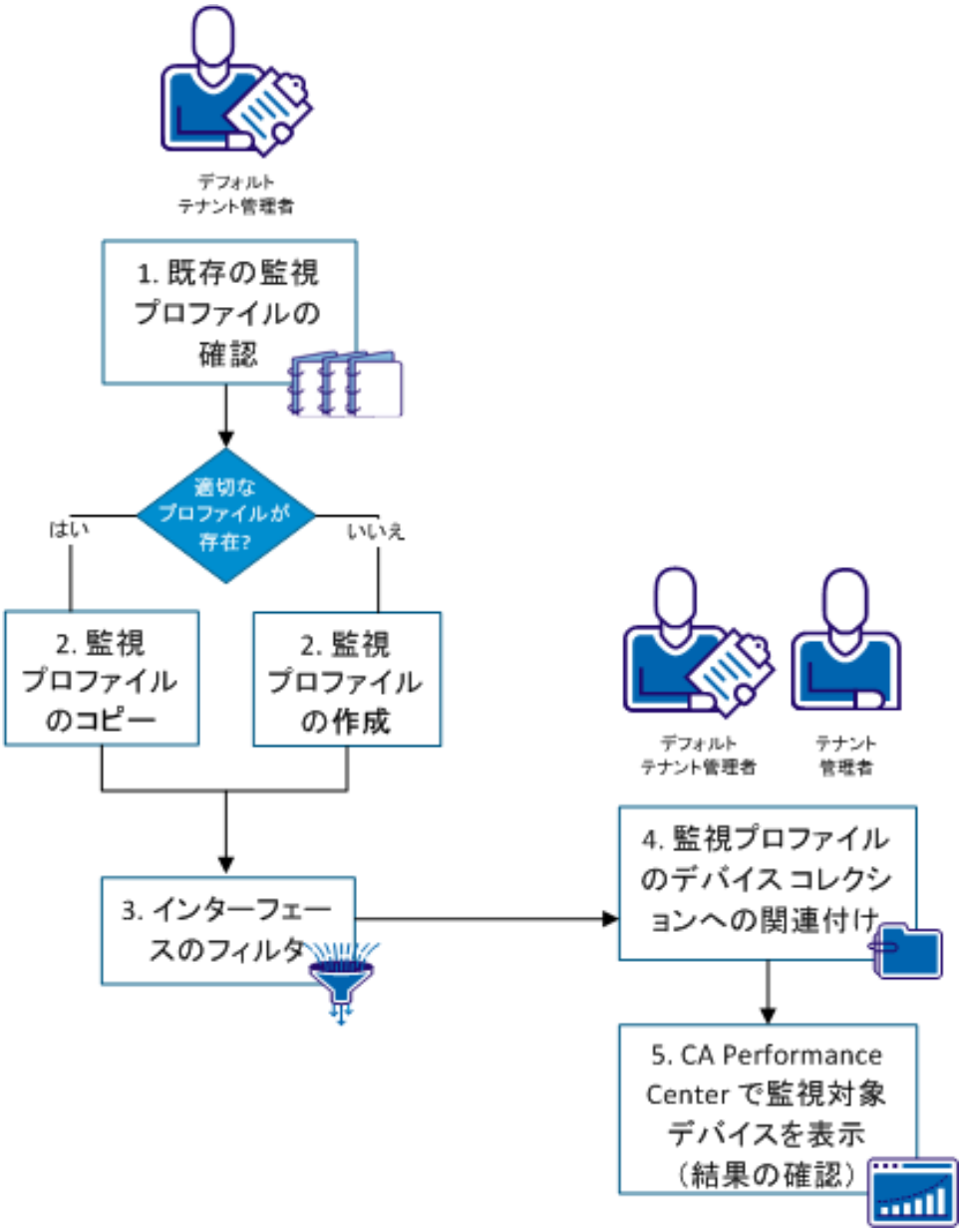
重要なインターフェースを通常のインターフェースよりも高速にポーリングする方法

管理者は、パフォーマンス管理システムの全体的なパフォーマンスを最大化する一方で、最も重要なシステムに関する最新のデータを必要としています。このような目標を達成する 1 つの方法は、重要なインターフェースのみを高いレートでポーリングし、通常のインターフェースは標準または低いレートでポーリングすることです。 異なるレートでポーリングを実行するには、監視プロファイルに関連付けられたインターフェース メトリック ファミリ上でフィルタを使用します。 インターフェースの高速ポーリングを必要な対象にのみ実行することで、ネットワーク システムの状態を十分に監視しつつ、余分なネットワーク トラフィックやパフォーマンス管理システムの負荷を軽減できます。

たとえば、データ センターのアクセス スイッチが、多数のアプリケーション サーバを 2 つの集約スイッチのみへ接続しています。 これらの集約スイッチをサポートするインターフェースを、より高いレートでポーリングすることにしました。これらのリンクは、接続された他のすべてのスイッチへのネットワーク トラフィックをサポートするため、非常に重要です。しかし、すべてのインターフェースを高いレートでポーリングすると、余分なネットワーク トラフィックが発生し、システム リソースを消費して、さらにはネットワーク パフォーマンス問題を引き起こす可能性があります。 ネットワーク運用チームおよびエンジニアリング チームと共に検討した結果、配置されたサーバ間を接続するインターフェースについては、通常のポーリング レートで十分であるという結論になりました。 別のポーリング レートを適用するには、インターフェースに 2 つの監視プロファイルを実装します。

注: 監視プロファイルに適用されるイベント ルールがイベントをトリガした場合、メトリック ファミリで設定したフィルタは無視されます。

以下の図では、監視プロファイルを設定してさまざまなレートでインターフェースをポーリングする方法について説明します。



手順
既存の監視プロファイルを表示します (P. 133)。
ファクトリの［Network Interface］監視プロファイルをコピーします (P. 134)。
［インターフェース］メトリック ファミリ上でフィルタを設定します (P. 137)。
監視プロファイルをデバイス コレクションに関連付けます (P. 140)。
監視対象デバイスを表示して結果を確認します (P. 141)。

注: 監視プロファイルがデバイス コレクションおよびメトリック ファミリとどのように連携して動作するかの詳細については、「*Data Aggregator 概要ガイド*」を参照してください。

監視プロファイルの表示

CA Performance Center 管理者として、重要なインターフェースをできるだけ頻繁にポーリングする必要があります。 ただし、そのような高速レートですべてのインターフェースをポーリングして発生する余分なネットワーク トラフィックを最小限に抑える必要もあります。そこで、インターフェース用に、通常のポーリングおよび高速ポーリングを実行する 2 つの監視プロファイルを作成します。

監視プロファイルを作成する前に、既存の監視プロファイルを確認して、ニーズに一致するプロファイルを見つけます。

以下の手順に従います。

1. Data Aggregator データ ソースの［監視設定］メニューから［監視プロファイル］をクリックします。

   監視プロファイルのリストが表示されます。

2. 監視プロファイルを選択します。

   選択した監視プロファイルの詳細が、以下のタブに表示されます。

   - ［メトリック ファミリ］タブ -- 特定の監視プロファイルに関連付けられたメトリック ファミリのリストが表示されます。 メトリック ファミリには、デバイスとコンポーネントのポーリングに使用されるメトリックが含まれます。
   - ［コレクション］タブ -- 特定の監視プロファイルに関連付けられたデバイス コレクションのリストが表示されます。

詳細:

トラブルシューティング： ポーリングが検出されたメトリック ファミリ上で停止する (P. 194)

ファクトリ監視プロファイルのコピー

CA Performance Center 管理者として、ファクトリの「Network Interface」監視プロファイルがニーズに一致しており、わずかな変更を加えるだけでよいことが分かりました。 そのため、コピーを作成して、より高速なポーリング レートで重要なインターフェースのみをポーリングするために使用します。

注: このタスクを実行するには、管理者としてログインする必要があります。

以下の手順に従います。

1. CA Performance Center 内の監視プロファイルすべてのリストに移動します (P. 133)。
2. 「Network Interface」監視プロファイルを選択して、[コピー]をクリックします。

   注: ファクトリ監視プロファイルを編集および削除することはできません。カスタムを含むすべての監視プロファイルは、グローバルです。

   [監視プロファイルの作成/編集] ダイアログ ボックスが表示されます。
3. 監視プロファイルに以下の情報を入力します。
   - **名前：** Uplink Interfaces
   - **説明**（オプション）：すべての重要なアップリンク デバイスのインターフェースのパフォーマンスを監視する。
   - **SNMP ポーリング レート：** 1 分

   注: プロファイルの名前を変更することを推奨します。 すべてのテナントにわたって名前を一意にする必要があります。

ポーリング レートに関する以下の情報を考慮します。

- ポーリング レートが変更されると、新規のポーリング レートが有効になるまで最大 2 サイクル必要です。 既存デバイスのポーリングに 60 分レートが使用されている場合、デフォルトの時間範囲が［過去 1 時間］のダッシュボード ビューには、［表示するデータがありません］というメッセージが表示されます。 ダッシュボード設定を前の時間に変更すると、以前のデータを参照できます。ただし、新しいポーリング サイクルが完了するまで、ビューには最新のデータは表示されません。
- ポーリング レートが異なる複数の監視プロファイルにインターフェースが割り当てられている場合、そのインターフェースに対するポーリングは、もっとも高速な割り当て済みのレートで実行されます。

4. ［変更検出の設定］のレートの値は 24 時間のままにします。

変更の検出レートに関する以下の情報を考慮します。

- 変更の検出レートは、デバイス上のいずれかのコンポーネントが再設定されたかどうかを、Data Aggregator が確認する頻度です。変更には、新しいコンポーネントの作成や、既存コンポーネントの廃止が含まれます。

  注: メトリック ファミリで指定された照合アルゴリズムは、監視対象にする設定変更を定義します。 変更の検出とデバイス再設定の動作についての詳細は、「Data Aggregator 管理者ガイド」を参照してください。
- ［変更検出の設定］の［検出レート］オプションは、Data Aggregator が変更をチェックする頻度を設定するために使用されます。 検出のレートは、分単位または時間単位で設定できます。 デフォルトでは、レートは 24 時間に設定されています。
- 変更の検出は、デバイスのコレクションに関連付けられた監視プロファイルすべてに対して指定された最速のレートで実行されます。

5. ［自動的にメトリック ファミリを更新する］チェック ボックスをオンにしておきます。

   このオプションは、変更または再設定が検出されたときの Data Aggregator のレスポンスを制御します。このオプションを選択すると、Data Aggregator は自動的に新規コンポーネントの監視を開始し、廃棄されたコンポーネントの監視を停止します。 このオプションが選択されていない場合、以下のようにコンポーネントの監視を手動で制御できます。

   a. ［イベントの表示］ダッシュボードを手動で確認して、設定イベントを見つけます。

   b. Data Aggregator の［管理］メニューから［監視対象デバイス］-［ポーリングされるメトリック ファミリ］ビューに移動します。

   c. 適切なメトリック ファミリを選択し、［メトリック ファミリの更新］をクリックして、Data Aggregator が最新のデバイス再設定を取得できるようにします。

   注: インターフェース フィルタが適用されると、Data Aggregator は再設定後にフィルタ条件を通過するインターフェースのみを監視します。

6. ［選択されたメトリック ファミリ］リスト内に［インターフェース］メトリック ファミリのみを残します。

7. ［保存］をクリックします。

   コピーされた監視プロファイルが、［監視プロファイル］リストに追加されます。ただし、この監視プロファイルはデバイス コレクションに割り当てるまでアクティブではありません。

詳細:

ディスカバリとポーリング (P. 69)
イベントの表示 (P. 168)
変更検出を管理する方法 (P. 125)
トラブルシューティング： ポーリングが検出されたメトリック ファミリ上で停止する (P. 194)
ディスカバリのワークフロー (P. 66)
インターフェース フィルタを設定しアクティブにする方法 (P. 145)

インターフェース フィルタの設定

デフォルトでは、ファクトリの［Network Interface］監視プロファイルには、管理目的でダウン中のインターフェースのモデリングを防ぐためのフィルタが含まれます。 フィルタリングによって、監視対象のインターフェースの数を減らすことで、不要なデータ収集とネットワーク トラフィックを減らすことができます。

管理用に稼働中のインターフェースをポーリングするだけでなく、最も重要なインターフェースをさらに頻繁にポーリングする必要が生じることがあります。 これらのインターフェースのみを区別して高速にポーリングするには、カスタム監視プロファイルに関連付けられたインターフェース フィルタに別のフィルタ条件を追加します。 この 2 番目のフィルタ条件では、説明に「uplink」が含まれるインターフェースのみを検索して、重要なインターフェースを区別します。

注: このタスクを実行するには、管理者としてログインする必要があります。

以下の手順に従います。

1. ［監視プロファイル］ページからインターフェース監視プロファイル（「Uplink Interfaces」という名前）を選択します (P. 134)。
2. ［メトリック ファミリ］タブで［インターフェース］メトリック ファミリの行をクリックし、［フィルタの編集］をクリックします。

   注: メトリック ファミリ名はメトリック ファミリの定義に移動するリンクであるため、直接クリックしないでください。 代わりにメトリック ファミリ名の行をクリックして、［フィルタの編集］オプションをアクティブにします。
3. ［条件の追加］ボタンをクリックします。

   注: 複数の条件は "and" 操作で結合されます。 すなわち、このフィルタに適合するには、すべての条件を満たす必要があります。
4. フィルタ条件に以下のオプションを設定して、［保存］をクリックします。
   - 属性： 説明
   - 操作： 指定の語句を含む
   - フィルタ値： uplink

   注:［フィルタ値］フィールドでは、大文字と小文字が区別されます。

フィルタリングに使用できる追加の属性については、以下の詳細を考慮してください。

- ［速度（イン）］と［速度（アウト）］では、テキスト フィールドで小数を使用して（1.544 など）、bps、Kbps、Mbps、または Gbps の単位を指定できます。
- タイプ（すなわち ifType）設定の詳細については、次の iana Web サイトを参照してください。
  http://www.iana.org/assignments/ianaiftype-mib
  http://www.iana.org/assignments/ianaiftype-mib。
- ［説明］と［エイリアス］では、［一致する （正規表現）］または［一致しない （正規表現）］操作を選択する場合のみ、フィルタに正規表現を使用できます。

変更を保存すると、フィルタ条件が［メトリック ファミリ］タブに表示されます。 この監視プロファイルを適切なコレクションに適用して、選択したインターフェースのポーリングを開始できるようになりました。

注: Data Aggregator はディスカバリ後にフィルタリングを適用します。 フィルタ条件に一致しないインターフェース アイテムはポーリングされません。 ディスカバリの実行*後*にインターフェース フィルタを追加または編集すると、これらのアイテム上のポーリングは停止します。 これらのインターフェース アイテムは、CA Performance Center ダッシュボードおよびデータ ビューに表示*されません*。

インターフェース フィルタおよび複数の監視プロファイルの考慮事項

複数の監視プロファイルがデバイス コレクションに割り当てられると、フィルター一致基準は「or」ルールに従います。 したがって、Data Aggregator は、グループ内の監視プロファイルのいずれかの条件を満たすインターフェースをすべて監視します。

監視プロファイルの中には、フィルタを持つものもあれば、持たないものもあります。 さらに、これらの監視プロファイルでは異なるポーリング レートを指定できます。 この場合、Data Aggregator は、いずれかの監視プロファイルに一致するインターフェースを監視しますが、ポーリング レートは異なる場合があります。 インターフェースに複数の監視プロファイルが適用される場合、Data Aggregator は一度インターフェースをポーリングし、次に最も速いポーリング レートでインターフェースをポーリングします。

- 監視プロファイル 1 -- フィルタ： 説明に「X」を含む、ポーリング レート： 1 分
- 監視プロファイル 2 -- フィルタ： なし、ポーリング レート： 5 分
- 監視プロファイル 3 -- フィルタ： 説明に「Y」を含む、ポーリング レート： 10 分

この例では、監視プロファイル 1 に一致するインターフェースは毎分ポーリングされます。他のすべてのインターフェースは 5 分ごとにポーリングされます。監視プロファイル 3 に一致するインターフェースは、フィルタを含まない監視プロファイル 2 にも一致します。 最も速いポーリング レートが適用されるため、10 分間隔でポーリングされるインターフェースはありません。

このように、1 つの監視プロファイルにフィルタがない場合、多くのインターフェースで、必要とされるよりも頻繁にポーリングが実行されることがあります。 そのため、フィルタを設定したら、他の監視プロファイルとの関連付けを削除して、指定したフィルタに一致するコンポーネントのみが監視されることを確認してください。

監視プロファイルのデバイス コレクションへの割り当て

管理者またはテナント管理者として、ポーリングを開始するために、新しい［Uplink Interfaces］監視プロファイルをデバイス コレクションに関連付けます。 この場合、プロファイルを「Switches」デバイス コレクションと関連付けます。「Switches」デバイス コレクションは、「Network Interfaces」ファクトリ監視プロファイルに関連付けられているのと同じデバイス コレクションです。 ポーリング レートは、このデバイス コレクション内のインターフェースに以下のように適用されます。

- 高速ポーリング： ［Uplink Interfaces］監視プロファイルのフィルタ条件を満たすインターフェース。
- 通常ポーリング： 「Network Interface」監視プロファイルによって検出された他のすべてのインターフェース。

重要: すべてのカスタム監視プロファイルはグローバルであり、テナント管理者が参照できます。 ただし、監視プロファイルと特定のデバイス コレクションとの関連付けは、範囲をテナントに限定できます。

以下の手順に従います。

1. Data Aggregator データ ソースの［監視設定］メニューから［コレクション］をクリックします。

   デバイス コレクションのリストが表示されます。管理者は、管理しているテナントのデバイス コレクションを参照できます。テナント管理者は、自身の（テナントの）デバイス コレクションのリストを参照できます。

2. ［All Switches］デバイス コレクションを選択し、［監視プロファイル］タブをクリックします。

   選択されたデバイス コレクションに関連付けられた監視プロファイルがリスト表示されます。［ネットワーク インターフェース］デバイス コレクションは、このリストに存在します。

3. ［管理］をクリックします。

   ［監視プロファイルへのコレクションの割り当て］ダイアログ ボックスが表示されます。

4. ［Uplink Interfaces］監視プロファイルを選択して、［追加］をクリックします。

   選択された監視プロファイルは、［割り当てられた監視プロファイル］リストに移動します。

5. ［保存］をクリックします。

   変更内容が保存されます。

詳細:

ファクトリ監視プロファイルの関連付け (P. 99)
トラブルシューティング： ポーリングが検出されたメトリック ファミリ上で停止する (P. 194)
ディスカバリのワークフロー (P. 66)
インターフェース フィルタを設定しアクティブにする方法 (P. 145)

監視対象デバイスの表示と結果の確認

監視プロファイルのセットアップ後に、監視対象デバイスとフィルタ レポートを確認して、重要なデバイスのみが高速なレートでポーリングされていることを確認します。 この情報は、どの監視プロファイルがデバイス コンポーネントのポーリングに使用されているかなどのコンテキスト情報を参照するのに役立ちます。 結果を確認することで、必要なポーリング結果を得るためにどのような調整が必要であるかを特定することができます。

注: 監視対象デバイスは、管理可能デバイスおよび Ping 可能（アクセス可能だが管理不可）デバイスです。 アクセス不可能なデバイスは監視対象デバイスではありません。 監視対象デバイスのコンポーネントは［ポーリングされるメトリック ファミリ］タブで表示できます。

以下の手順に従います。

1. オンデマンド ディスカバリを実行します。

   注: ディスカバリ プロファイルが自動的に実行される場合、スケジュールされた次回のディスカバリを待つことができます。ディスカバリ管理の詳細については、「Data Aggregator 管理者ガイド」を参照してください。

2. Data Aggregator データ ソースの［監視対象インベントリ］メニューから［監視対象デバイス］をクリックします。

3. ドロップダウン リストから以下のオプションの 1 つを選択して、集約スイッチ デバイスの 1 つを対応するツリー ビューに配置します。

   - コレクション別デバイス -- デバイスは［All Switches］デバイス コレクションの下に表示されます。
   - 監視プロファイル別デバイス -- 重要なインターフェースが［Uplink Interfaces］監視プロファイルの［デバイス］の下に表示されます。

   注: あるいは、［検索］タブを選択し、ホスト名、デバイス名または IP アドレスで検索します。 部分的な一致を含むデバイスのリストを返すために、名前の一部または IP アドレスを入力できます。 ワイルドカードと正規表現はサポートされていません。

   ［ポーリングされるメトリック ファミリ］タブには、スイッチ デバイスと関連付けられた統合監視プロファイルが表示されます。 デバイスが持つ統合監視プロファイルは 1 つのみです。 それぞれの統合監視プロファイルには、デバイス上でポーリングされるすべてのメトリック ファミリ、およびデバイスがメトリック ファミリをサポートしているかどうかが一覧表示されます。

4. ［インターフェース］メトリック ファミリを選択します。

   インターフェース メトリック ファミリのコンポーネント テーブルには、検出されたインターフェース コンポーネントに対して、以下のポーリング ステータスの 1 つが表示されます。

   アクティブ

   コンポーネントがポーリングされていることを示します。

   非アクティブ

   デバイスのメトリック ファミリが監視されなくなったため、コンポーネントでのポーリングが停止したことを示します。

   廃棄済み

   コンポーネントが物理デバイスに存在しなくなったことを示します。 コンポーネントへのポーリングは停止されます。 レポート目的で履歴データを表示できます。 デフォルトでは、廃棄済みのコンポーネントは CA Performance Center と同期されません。 このオプションを有効にするには、CA Performance Center 内の［データ ソースの管理］ページにある［データ ソースの編集］ダイアログ ボックスで、［廃止されたアイテムの同期］チェック ボックスをオンにします。

   フィルタ済み（インターフェース コンポーネントのみ）

   コンポーネントがフィルタ条件に適合せず、コンポーネントに対するポーリングが停止していることを示します。

   注: フィルタ済みのインターフェースは、CA Performance Center ダッシュボードおよびデータ ビューに表示されません。

5. （オプション）［インターフェース］メトリック ファミリを選択して、［メトリック ファミリの更新］をクリックします。

   設定更新がある場合、Data Aggregator によってコンポーネントが再設定されます。 たとえば、サーバのディスク ドライブを追加する場合、設定更新を再検出するために［メトリック ファミリの更新］ボタンを使用できます。 この設定更新により、ディスク コンポーネントが作成されます。

6. ［フィルタ レポート］タブをクリックし、以下の手順に従います。

   a. ほかのインターフェース監視プロファイルそれぞれに対するフィルタを参照し、フィルタするのと同じデバイス コレクションを監視しているかどうかを確認します。

   b. ほかの［インターフェース］監視プロファイルと、ユーザのフィルタ条件をブロックするデバイス コレクションとの関係をすべて削除します (P. 102)。 たとえば、新規の［インターフェース］監視プロファイルが［All Routers］デバイス コレクションと関連付けられる場合、*ほかの*［インターフェース］監視プロファイルと［All Routers］デバイス コレクションの関係を削除します。

   c. 別のディスカバリを実行し、更新されたフィルタ レポートを確認して、新規のフィルタ条件がアクティブであることを確認します。 不要な監視プロファイルが含まれていることをフィルタ レポートが示す場合は、必要なインターフェースのみを監視している状態になるまで、前の手順を繰り返します。

   ［フィルタ レポート］タブには、コンポーネント監視中に使用されたインターフェース フィルタ条件が表示されます。 またこのタブには、デバイスで識別されたすべてのインターフェースのレポートと、これらが指定したフィルタ条件と一致したかどうかが表示されます。

   注: カスタム監視プロファイルのルールを変更する場合、［インターフェース フィルタ条件］ペインにはこの変更が反映されません。監視プロファイルとグループの関連付けを解除する場合、［インターフェース フィルタ条件］ペインにはこの変更が反映されません。フィルタ条件および監視プロファイルに対して行った変更に基づいてインターフェースをフィルタするために、デバイスを再検出します。

詳細情報:

ディスカバリとポーリング (P. 69)
デバイス再設定の手動更新 (P. 129)
インターフェース フィルタのクリア (P. 147)
トラブルシューティング： ポーリングが検出されたメトリック ファミリ上で停止する (P. 194)
インターフェース フィルタを設定しアクティブにする方法 (P. 145)

インターフェース フィルタを設定しアクティブにする方法

デフォルトでは、監視プロファイルには、管理目的でダウン中のインターフェースのモデリングを防ぐフィルタが含まれています。

フィルタリングにより、監視されるメトリック ファミリの数を減らし、不要なデータ収集を減少させることができます。 カスタム監視プロファイルの場合は、メトリック ファミリに追加フィルタを指定できます。

注: 監視プロファイルに適用されるイベント ルールがイベントをトリガした場合、メトリック ファミリで設定したフィルタは無視されます。

複数のインターフェース監視プロファイルがデバイス コレクションに割り当てられる場合、条件に一致するフィルタは「or」ルールに従います。この場合、一方のフィルタ条件に一致するインターフェースが監視されます。

メトリック ファミリ フィルタは、ディスカバリの実行前または実行後に追加/編集できます。 Data Aggregator はディスカバリの後にフィルタリングを適用します。 フィルタ条件に一致するコンポーネント アイテムのみがポーリングされます。 ディスカバリの実行後にメトリック ファミリ フィルタを追加または編集すると、これらのメトリック ファミリに対するポーリングは停止します。 これらのメトリック ファミリは、CA Performance Center ダッシュボードおよびデータ ビューには表示されません。

注: このタスクを実行するには、管理者としてログインする必要があります。

メトリック ファミリ フィルタを設定してアクティブにするには、以下の手順に従います。

1. カスタム監視プロファイルが存在しない場合は、新規に作成するか、またはプロファイルをコピーしてカスタマイズされたプロファイルを作成します。 ファクトリ監視プロファイル用のフィルタは編集したり設定したりできません。
2. ［監視プロファイル］ページでカスタム監視プロファイルを選択します。［メトリック ファミリ］タブでメトリック ファミリの行をクリックし、［フィルタの編集］をクリックしてフィルタ条件を編集します。

注: メトリック ファミリ名はメトリック ファミリの定義に移動するリンクであるため、直接クリックしないでください。 代わりに、メトリック ファミリ名が見つかった行をクリックし、［フィルタの編集］オプションをアクティブにします。

- ［フィルタ値］フィールドでは、大文字と小文字が区別されます。
- ［速度（イン）］と［速度（アウト）］では、テキスト フィールドで小数を使用して「1.544」のように Mbps 値を指定できます。
- タイプ設定の詳細については、次の iana Web サイトを参照してください。 http://www.iana.org/assignments/ianaiftype-mib http://www.iana.org/assignments/ianaiftype-mib。

変更を保存すると、［メトリック ファミリ］タブにフィルタ条件が表示されます。

3. 監視プロファイルをデバイス コレクションに関連付けます (P. 102)。
4. ディスカバリを実行 (P. 84) し、次に、［監視対象デバイス］ページのフィルタ レポートを確認します (P. 111)。 各監視プロファイルのフィルタを参照し、フィルタするのと同じデバイス コレクションを監視しているかどうかを確認します。
5. ほかの監視プロファイルと、ユーザのフィルタ条件をブロックするデバイス コレクションとの関係をすべて削除します (P. 102)。 たとえば、インターフェース監視プロファイルが［すべてのルータ］デバイス コレクションと関連付けられている場合があります。 この場合は、*他の*監視プロファイルと［すべてのルータ］デバイス コレクションとの関係を削除します。
6. 更新されたフィルタ レポートを確認して、新規フィルタ条件がアクティブであることを確認します。 不要な監視プロファイルが含まれていることをフィルタ レポートが示す場合は、前の手順を繰り返します。 最終的に、不要な監視プロファイルは含まれなくなり、監視の必要があるメトリック ファミリのみを監視できます。

インターフェース フィルタのクリア

インターフェース フィルタをカスタム監視プロファイルと共に使用し、監視対象のインターフェースの数を減らせます。 カスタム監視プロファイルと関連付けられたすべてのデバイス コレクションのデータを収集する場合、インターフェース フィルタをクリアできます。

注: このタスクを実行するには、管理者としてログインする必要があります。

以下の手順に従います。

1. 監視プロファイルのリストに移動します。
2. ネットワーク インターフェースを監視するカスタム監視プロファイルをリストから選択します。

   ［メトリック ファミリ］タブが入力されます。
3. ［インターフェース］メトリック ファミリを選択し、［フィルタのクリア］をクリックします。

   注: このオプションが有効になるのは、フィルタ セットを含む［インターフェース］メトリック ファミリを選択した場合のみです。

   確認ダイアログ ボックスが表示されます。
4. ［はい］をクリックします。

   変更が保存され、［メトリック ファミリ］タブのフィルタ ステータスにアスタリスク（*）が表示され、フィルタが設定されていないことを示します。 フィルタは、次回のスケジュール済みディスカバリ（または、手動でディスカバリを実行できます）に適用されます。

詳細情報:

監視対象デバイスの表示 (P. 111)

インターフェース コンポーネントの命名規則

インターフェース ベンダー認定または High Speed インターフェース ベンダー認定によって支持されているインターフェース コンポーネントの命名規則は、以下のロジックに基づいています。

- ifName 属性が存在し、値が指定されている場合、インターフェースはこの値を名前として使用します。
- ifName 属性が存在*しない*か、または値が指定されて*いない*場合、インターフェースは ifDescr の値を名前として使用します。

注: ［インターフェース］メトリック ファミリを新しく認定すると、インターフェース名に異なる表示を使用できます。

インターフェース使用率の計算

Data Aggregator では、使用率の計算で適切な値が使用されるように、任意のインターフェースの速度（イン）値および速度（アウト）値を上書きできます。 たとえば、帯域幅コマンドを使用して、ルーティングの決定に影響を与えるルータ インターフェースの ifSpeedIn および ifSpeedOut を設定することができます。この場合、使用率が正しく計算されるように Data Aggregator で上書き速度を指定します。

データ転送速度は、デバイス上で設定することで実際に利用可能な値よりも高い値や低い値に変更できます。 したがって、インターフェースに対して実行される使用率の計算は、この帯域幅の操作によって不正確に見える場合があります。 インターフェース使用率が正しく計算されるようにするには、Data Aggregator 内のインターフェースに上書き速度を指定します。

インターフェースの速度（イン）値と速度（アウト）値の上書き

デフォルトで使用率の計算に使用されるのは、インターフェースを構成するデバイスからレポートされる速度（イン）値および速度（アウト）値です。ただし、これらの速度値は上書きできます。これによって、インターフェース使用率のレポートをより正確なものにできます。

以下の手順に従います。

1. Data Aggregator データ ソース用の［監視対象インベントリ］メニューから［監視対象デバイス］をクリックします。

   ［ツリー表示］タブが表示されます。

2. ドロップダウン リストから［コレクション別デバイス］または［監視プロファイル別デバイス］を選択します。インターフェースの速度（イン）値と速度（アウト）値を上書きするデバイスを選択し、［ポーリングされるメトリック ファミリ］タブで適切なインターフェース メトリック ファミリを選択します。

   デバイス上で監視されるインターフェース コンポーネントが、インターフェース コンポーネント テーブルに表示されます。

3. 速度（イン）値と速度（アウト）値を上書きするインターフェース コンポーネントを選択して、［編集］をクリックします。

   ［インターフェースの編集］ダイアログ ボックスが表示されます。このダイアログ ボックスには、デフォルトで検出された［速度（イン）］値および［速度（アウト）］値が表示されます。

4. ［速度（イン）］と［速度（アウト）］の値を 1 秒あたりのビット数で入力し、［保存］をクリックします。

   注:［クリア］-［保存］をクリックすると、上書き値を削除できます。これにより、このインターフェースに対する CA Performance Center の帯域幅使用率グラフでは、デバイスがレポートする速度値を使用して、使用率が表示されます。インターフェース上で、速度の上書き値が削除されたことを示すイベントが生成されます。 このイベントは、CA Performance Center の［イベントの表示］ダッシュボードで確認できます。

   ダイアログ ボックスが閉じます。インターフェース上の上書きされた［速度（イン）］および［速度（アウト）］の値が、インターフェース コンポーネント テーブルにアスタリスク付きで表示されます。

インターフェース上で、［速度（イン）］値および［速度（アウト）］値が上書きされたことを示すイベントが生成されます。このイベントは、CA Performance Center の［イベントの表示］ダッシュボードで確認できます。

これにより、このインターフェースに対する CA Performance Center の帯域幅使用率グラフでは、指定された速度値を使用して、使用率が表示されます。

第 6 章: イベント

このセクションには、以下のトピックが含まれています。

イベント パフォーマンスのガイドライン

以下の設定を使用して、イベント パフォーマンスの検証とベンチマークが実行されました。

- 50 万のポーリング対象アイテムが存在する「中規模」の実稼働システム（システム規模の仕様を参照）で推奨される仕様を完全に満たしているシステム。
- 10 個のイベント ルールが、ポーリング対象アイテムで使用されている 7 つの監視プロファイルに適用されています。
  - 1 つのイベント ルールは、ポーリング対象アイテムの最大 33 パーセントを構成するメトリック ファミリ上で 1 分間隔で評価されています。
  - 1 つのイベント ルールは、ポーリング対象アイテムの最大 33 パーセントを構成するメトリック ファミリ上で 15 分間隔で評価されています。
  - 残りのルールは、5 分間隔でポーリングされている残りのアイテムの一部に適用されました。
  - イベント ルールは、4 つのメトリック ファミリに均等に振り分けられました。
  - 各ルールには、1 つの固定条件と 1 つの標準偏差条件があります。

- 6 つのイベント ルールには、5 分の期間と 15 分のウィンドウがあります。
- 4 つのイベント ルールには、15 分の期間と 60 分のウィンドウがあります。

注: パフォーマンスを最適化するには、同じメトリック ファミリに対するイベント ルールを含む監視プロファイルの数を最小にします。たとえば、1 つの監視プロファイルに［インターフェース］メトリック ファミリに対する 10 個のルールが含まれる場合は、10 個の監視プロファイルに［インターフェース］メトリック ファミリに対する 1 個のルールが含まれる場合よりも、パフォーマンスは向上します。いずれも同一のデバイス セットに適用されることを前提とします。

- 10 万のポーリング対象アイテムには、さまざまな数のイベント ルールが関連付けられています。
- 5 つの Data Collector システムがあり、各システムは約 1/5 のアイテムをポーリングしてします。

イベント処理を監視する方法

処理するイベントの数が多すぎるかどうかを判断するには、Data Aggregator 内のいくつかの重要業績評価指標（KPI）を監視する必要があります。 Data Aggregator でのイベント処理は、バッチ形式で実行されます。たとえば、大きなアイテム グループに対して、イベントは一度に評価および生成されます。このため、Data Aggregator システムの健全性を評価するために、Data Aggregator システムの自己監視メカニズムを通じて追跡されたさまざまなメトリックが使用されました。 これらの重要なメトリックを表示するには、カスタムの［IM デバイス マルチトレンド］ビューをダッシュボードに追加します。 ［**Data Aggregator イベント計算時間**］メトリック ファミリから以下のメトリックを使用して、ダッシュボードを編集します。

- **イベント プロセス キュー サイズ** - イベント処理キューのサイズを表示します。 0、1、または 2 の定数値は、このシステムが健全な状態にあり、現在のイベント処理を維持できることを示します。 2 を超える定数値は、このシステムが現在のイベント処理による負荷を維持できるものの、処理が遅延する（現在のポーリング サイクルより古いポーリングを処理する状態になる）可能性があることを示します。 待ち行列サイズが回復する（減少傾向に転じる）ことなく増加していくと、イベント処理が遅延し、ご使用のシステムに問題が発生する可能性があります。
- 以下の 2 つのメトリックは互いに相補的な関係にあります。
  - **クリア イベント数** - レポート間隔のウィンドウでクリアされたイベントの数。
  - **作成イベント数** - レポート間隔のウィンドウで発生したイベントの数。

  多数のイベントが連続して発生またはクリアされると、イベント マネージャ データベースに影響を与える可能性があります。

  これらの 2 つのメトリックの合計が、5 分のポーリング サイクルで 900 イベントを超えると、中規模システムで推奨されている 1 秒あたり 2 ～ 3 イベントという生成レートを超過します。 イベントの生成/クリアは、5 分のポーリング サイクルで 900 イベントを大幅に超過しても許容されます。

- **処理済みイベント ルール評価数** - イベント ルール評価は、1 つのアイテムに対する単一のイベント ルールの評価です。 このメトリックは、イベント ルールの合計を追跡し、それらのルールが適用されるアイテムの数を掛け合わせたものです。 評価数が高いほど、システムの処理量は増加します。 ただし、すべての評価が同等に作成されるわけではありません。たとえば、多くの固定条件や多くの標準偏差条件を含む、長い期間とウィンドウを使用した評価は、少ない固定条件を含む、短い期間とウィンドウを使用した評価よりも処理の負荷が大きくなります。 そのため、実行可能な評価数は、使用するイベント ルールに応じて増減します。

  テスト環境では、先に説明したように、5 分のポーリング サイクルで評価数が 15 万を超えるとシステムに問題が発生する可能性があることが分かりました。

- **イベント計算の合計時間** - このメトリック ファミリのイベント処理にかかった合計時間。 この値がレポート間隔のウィンドウの秒数を超えると、その時点でイベント処理が遅延してバックログが発生したことを示します。

これらのメトリックすべての時間変動を監視することで、ご使用のシステムのイベント パフォーマンスが正常かどうかを判断できます。 さらに、Data Aggregator システム上の Karaf ログにデータベース エラーやその他のエラーが含まれる場合、システムの負荷を示している可能性があります。一般的に、これらの自己監視メトリックは安定した値である必要があります。 ただし、夜間（デフォルトでは UTC の午前 2 時から 4 時の間）には、一部のデータベース ジョブが集中的に実行されて、自己監視メトリックの値が変動する場合があります。 メトリックが安定状態に戻れば、システムは健全な状態にあると判断できます（ただし、システムがビジーである時間帯には、イベントが遅延する可能性があります）。

ルールを変更する際は、あらかじめイベント処理を少しずつ有効にして、システムの健全性を判断することをお勧めします。 また、各変更の後には、システムの健全性を 24 時間監視することをお勧めします。イベント処理が昼間は安定しているように見えても、夜間に実行される処理に影響を受ける可能性があるためです。

しきい値を超えた場合の対処法

しきい値を超えた場合は、以下の手順に従って対処します。

1. イベント ルールを 1 つずつオフにします。 1 つのルールをオフにしたら、別のルールをオフにする前に、パフォーマンスを確認します。
2. ポーリングされているアイテムの数を減らします。
3. アイテムをポーリングしているイベント ルールを持つ監視プロファイルの数を減らします。
4. これらの手順を行ってもパフォーマンスが改善しない場合は、CA サポートまでお問い合わせください。

パフォーマンス管理イベント

イベント ルールを使用して、2 種類のパフォーマンス管理イベントを定義できます。 監視プロファイルにイベント ルールを追加します。

しきい値超過時間イベント

観測されたメトリックが、あるウィンドウ時間内の指定期間に設定された固定値と異なる場合、定数（固定値）ルールによってトリガされます。

例：

5 分間隔でポーリングする間、指定された 10 分のウィンドウ時間のうち 5 分間、帯域幅の使用率が 80 パーセントを超えるとイベントを生成するように、イベント ルールを定義できます。

標準からの偏差イベント

観測されたメトリックが、あるウィンドウ時間内の指定期間に「標準」と見なされる範囲にない場合、標準偏差ルールによってトリガされます。「標準」は、計算されたベースライン平均に基づきます。 はじめに限定された情報が収集されると、毎日の同じ時間に対するベースライン平均が計算されます。 より多くのデータが利用可能になると、Data Aggregator は平均の計算方法を、同じ曜日の同一時間における時間平均に切り替えます。

例：

5 分間隔でポーリングする間に、指定された 10 分のウィンドウ時間のうち 5 分間、帯域幅の使用率が同じ曜日の同一時間で計算された時間平均から 1 標準偏差を超えるとイベントを生成するように、イベントルールを定義できます。

ベースライン平均

収集されたポーリング データの量に応じて、ベースライン平均は 2 つの方法で計算されます。

- はじめは、同一時間（曜日に関係なく）の時間平均の平均値。
- 十分なデータが収集されると、同じ曜日の同一時間における時間平均の平均値。

ベースライン平均は、選択された監視対象メトリックの過去のパフォーマンスを表し、現在のパフォーマンスを評価するために役立ちます。 ベースライン平均および関連する標準偏差は、1 時間ごとに継続的に計算されます。 標準偏差により、ベースライン平均の計算に含まれる母集団データにどれだけの変動が存在するかを示す統計指標が提供されます。

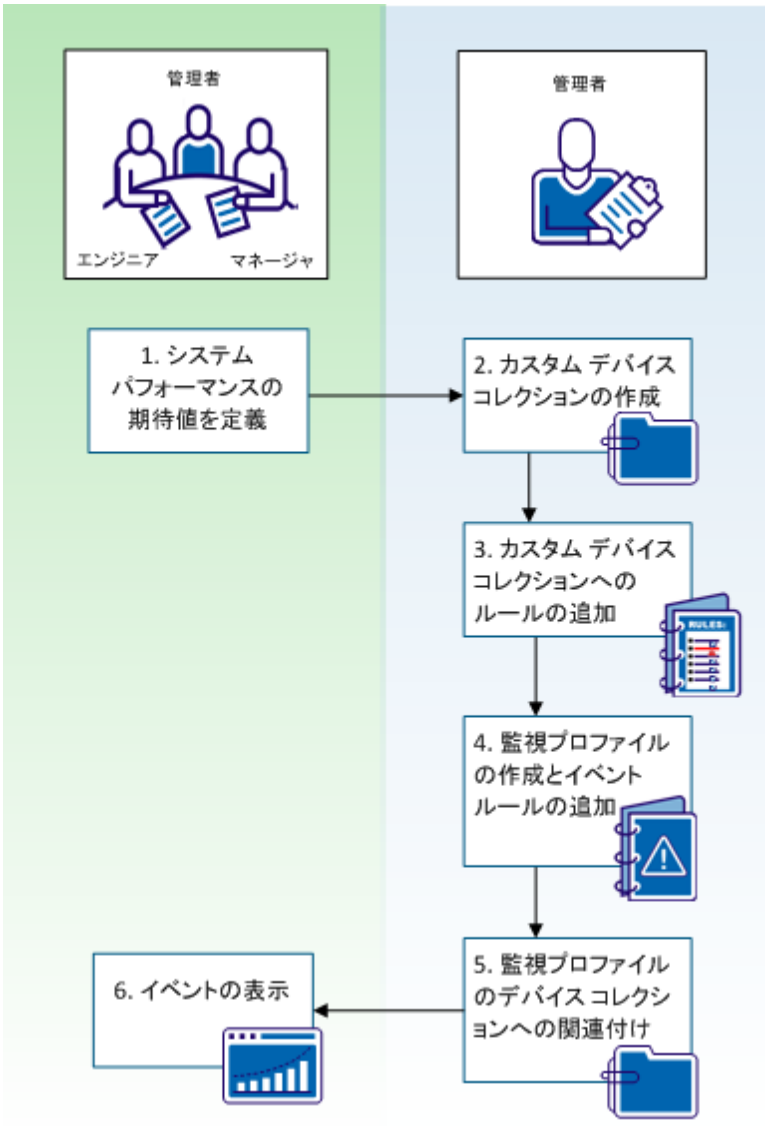
Data Aggregator では、ウィンドウ時間内の指定期間における「標準」は、計算されたベースライン平均に基づいて決定されます。

イベントを使用してデバイス パフォーマンスを監視する方法

管理者（運用センター管理者など）およびエンジニア（IT オペレータまたは IT アーキテクトなど）は、システムの健全性に関する継続的な情報を必要としています。 ツール管理者と協力して Data Aggregator を設定し、正常なパフォーマンス期待値から逸脱するデバイスに対してイベントを生成するようにします。 これらのイベントは、ネットワークの健全性をプロアクティブに監視し、必要に応じてパフォーマンス上の問題を修正する解決策を講じるために役立ちます。

たとえば、最近、効率を改善するために組織内のいくつかの重要なビジネス アプリケーションが仮想化されました。 IT アーキテクトと運用センター管理者は、これらの仮想サーバを監視して、仮想化アプリケーションの負荷を処理できるようにしたいと考えています。 ツール管理者は監視プロファイルを作成し、使用率が過剰な CPU、および仮想メモリの問題を見つけるためのイベント ルールを、仮想デバイスのコレクションに追加します。 Data Aggregator は、各デバイスのポーリング後に、コレクション内のすべてのデバイスを自動的に評価します。 デバイスがイベント ルール条件を満たすと、必要に応じて Data Aggregator はイベントを発生させるか、またはクリアします。

以下の図に、イベントを自動生成して、デバイス パフォーマンス問題の監視に役立てる方法を示します。



図のように、ツール管理者はエンジニアおよびマネージャと協力して、デバイス セットに対するパフォーマンス期待値を定義します。 その後、管理者は、カスタム デバイス コレクションの作成、監視プロファイルの作成、およびイベント ルールの監視プロファイルへの割り当てを決定します。 デバイスの監視を開始するため、管理者は、イベント ルールが割り当てられた監視プロファイルをカスタム デバイス コレクションに関連付けます。 CA Performance Center がイベントを生成すると、管理者、エンジニア、およびマネージャは、そのイベントを CA Performance Center で確認できます。

手順
カスタム デバイス コレクションを作成します (P. 161)。
カスタム デバイス コレクションにルールを追加します (P. 162)。
監視プロファイルを作成して、イベント ルールを追加します (P. 163)。
監視プロファイルをカスタム デバイス コレクションに割り当てます (P. 167)。
イベントを表示します (P. 168)。

イベント ルールを持つ監視メトリック

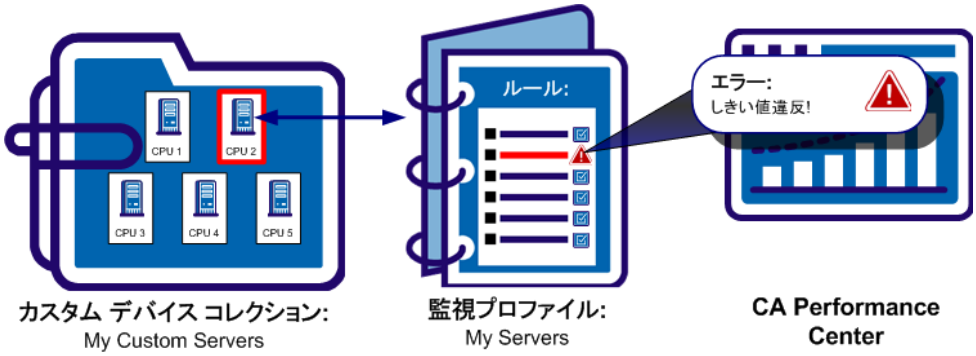
イベントは、ネットワーク環境の健全性およびステータスの監視に役立つ情報を提供します。 さらに、CA Spectrum と統合することで、イベントを使用して、イベント メッセージ内のデータに基づくプロセスを自動化することもできます。

Data Aggregator では、監視プロファイルを使用してイベントを処理します。監視プロファイルにはイベント ルールのセットを含めることができます。（メトリック ファミリからの）メトリックを使用して、これらのルールは、監視対象の条件を定義します。

イベント ルールを実装するには、監視プロファイルを デバイス コレクションに関連付けます。

重要: *監視プロセスの開始および停止で重要なのはデバイス コレクションです。*Data Aggregator で監視プロファイルを使用するには、少なくとも 1 つのデバイス コレクションに監視プロファイルを割り当てる必要があります。

Data Aggregator は直ちに、監視プロファイル内のルールを対象デバイス コレクションのデバイスに適用します。 これらのデバイスに対してポーリングされたメトリック値を使用して、必要に応じてイベント ルールによりイベントがトリガおよびクリアされます。



イベントは CA Performance Center ダッシュボードに表示されます。

注: Data Aggregator で処理およびロギングされたイベントから、CA Spectrum の表示アラームを生成できます。 詳細については、CA Spectrum のドキュメントを参照してください。

カスタム デバイス コレクションの作成

Data Aggregator のツール管理者として、仮想サーバの新規グループのパフォーマンスを監視するリクエストを受け取ります。IT アーキテクトと運用センター管理者は、CPU 使用率とメモリ使用率を追跡する必要があります。 これらの仮想サーバは重要なアプリケーションをホストしているため、そのステータスが頻繁に更新されることが必要です。

注: ネットワーク上ですでに最初のディスカバリが実行され、いくつかの仮想サーバを検出済みであると想定しています。

仮想サーバ用に標準で提供されるファクトリ デバイス コレクションは存在しないので、はじめに、検出された仮想サーバをグループ化するカスタム デバイス コレクションを作成することにします。カスタム デバイス コレクションを作成するには、最初に CA Performance Center でカスタム デバイス コレクションを作成します。 自動同期によって、対応するデバイス コレクションが Data Aggregator に作成されます。

以下の手順に従います。

1. 管理者の役割を持つユーザとして CA Performance Center にログインします。
2. ［管理］-［カスタム設定］-［グループ］を選択します。

   ［グループの管理］ダイアログ ボックスが表示されます。
3. 監視対象コレクションを右クリックし、［新規グループの追加］を選択します。

   ［グループの追加］ダイアログ ボックスが表示されます。デフォルトでは［新規］タブが選択されています。
4. 以下のパラメータの値を入力します。

   グループ名

   グループの名前を指定します。この例では、グループに「仮想サーバ」という名前を付けます。

   注: グループ名には特殊文字（/、&、¥、%）を使用しないでください。

   説明

   （オプション）グループの識別を容易にします。
5. ［保存］をクリックします。

「仮想サーバ」グループが、監視対象グループ ツリーに表示されます。Data Aggregator との自動同期が発生するのを待ちます。同期中に、Data Aggregator はデバイス監視用の対応するデバイス コレクションを作成します。 同期が開始するまで最大で 5 分かかる場合があります。

カスタム デバイス コレクションへのルールの追加

ネットワークとシステムは常に変化します。 デバイス コレクションは自動的に更新され、検出されたデバイスが含まれます。ただし、カスタム デバイス コレクションを最新に保つことは難しい場合があります。 そのため、ルールを使用してカスタム デバイス コレクションにデバイスを追加することができます。 ルール仕様に適合するデバイスが新しく検出されると、デバイス コレクションに追加されます。 同様に、ルール要件を満たさないか監視対象でなくなった場合、そのデバイスは削除されます。

さまざまな条件に基づいてグループの内容を自動的に入力し、更新するには、グループ ルールをグループに追加します。 この場合、検出された仮想サーバを最新の状態に保つには、［仮想サーバ］カスタム デバイス コレクションにグループ ルールを追加します。 このシナリオでは、仮想マシンの IP アドレスが指定された範囲内にあると想定しています。

以下の手順に従います。

1. CA Performance Center メイン メニューから［管理］-［カスタム設定］を選択して、［グループ］をクリックします。

   ［グループの管理］ダイアログ ボックスが表示されます。

2. グループ ツリーに入力するグループを選択します。

   注: 手動でグループに直接追加されたデバイスは、［グループ プロパティ］ペイン内に直接アイテムとして表示されます。 管理対象デバイスの子であるという理由でグループに追加されたコンポーネントは、［グループ プロパティ］ペイン内に継承されたアイテムとして表示されます。

3. ［ルール］タブをクリックして、［ルールの追加］をクリックします。

   ［ルールの追加］ダイアログ ボックスが表示されます。

4. ［ルール名］フィールドにルール名を入力します。

5. ［追加］リストからデバイスを選択します。

6. ［条件の追加］をクリックします。

   ドロップダウン リストの行とフィールドが表示されます。

7. 以下のアクションを実行します。

   - 最初のリストで、デバイス アドレスを選択します。
   - 2 番目のリストで、一致の方法として［指定の範囲内にある］を選択します。
   - 3 番目のリストで、開始 IP アドレスと終了 IP アドレスを入力して、仮想マシンの IP アドレスを見つける範囲を指定します。

8. ［プレビュー結果］をクリックし、必要なデバイスが新規ルールに含まれていることを確認します。

   結果が［グループ ルール プレビュー］ウィンドウに表示されます。各デバイス タイプを展開して、追加された特定のデバイスを参照できます。

9. ［保存］をクリックするか、または［ルールの保存と実行］をクリックします。

   - ［保存］- ルールを実行せずに保存します。グループは次のグローバル同期中に入力されます。グローバル同期は、約 5 分ごとに発生します。
   - ［ルールの保存と実行］- ルールを保存し、グループをすぐに入力します。

監視プロファイルの作成とイベント ルールの追加

［仮想サーバ］カスタム デバイス コレクション内の仮想サーバのパフォーマンス監視プロセスをセットアップするには、はじめに監視プロファイルを作成し、その監視プロファイルにイベント ルールを追加します。

標準で提供されるファクトリ 監視プロファイルには、イベント ルールは含まれません。また、ファクトリ監視プロファイルを変更してイベント ルールを追加することはできません。 既存の監視プロファイルをコピーし、一部を変更した類似のプロファイルを作成するためのベースとして使用します。 カスタム監視プロファイルに加える変更は、イベント ルールを追加することです。

IT アーキテクトおよび運用センター管理者と協力して、監視プロファイルを作成し、以下のイベント ルールを追加することにします。

- 以下のような VMware メモリ使用率のルールを追加します。
  - 900 秒（15 分）の期間内に、メモリ使用率が 300 秒（5 分）間、80 パーセントを超える場合に違反が発生します。
  - 900 秒の期間内に、メモリ使用率が 300 秒間、75 パーセント以下になる場合に違反がクリアされます。
- 以下のような VMware CPU 使用率ルールを追加します。
  - 以下の条件を*両方*とも満たすときに違反が発生します。
    - 条件 1： CPU 使用率が 70 パーセントを超える。
    - 条件 2： CPU 使用率が 1 つの標準偏差を超える。
  - 900 秒の期間内に、これらの条件が 300 秒間、発生します。

以下の手順に従います。

1. ［管理］-［データ ソース設定］を選択し、［Data Aggregator のデータ ソース］をクリックします。
2. Data Aggregator 管理ページの［監視設定］メニューから［監視プロファイル］をクリックします。

   監視プロファイルのリストが表示されます。
3. ［Virtual Server］監視プロファイルを選択して、［コピー］をクリックします。

   ［監視プロファイルの作成/編集］ダイアログ ボックスが表示されます。
4. 監視プロファイルの名前を「カスタム仮想サーバ」に変更します。
5. ［保存］をクリックします。

   コピーされた監視プロファイルが、［監視プロファイル］リストに追加されます。
6. 「カスタム仮想サーバ」監視プロファイルを選択します。
7. ［イベント ルール］タブをクリックします。
8. VMware メモリ使用率イベント ルールを以下のように作成します。
   a. ［新規］をクリックします。

b. 新規イベント ルールに以下の値を入力します。

- **名前：** VirtualMemUsageTooHigh
- **説明（オプション）：** VMware メモリ使用率
- **メトリック ファミリ：** VMWare 仮想マシン
- **期間**： 300

  注: この例では、デバイスがデフォルト レートの 300 秒でポーリングされると想定しています。［期間］の値は、違反しきい値とクリアしきい値で使用されます。

- **ウィンドウ**： 900

  注:［ウィンドウ］の値は、違反しきい値とクリアしきい値で使用されます。

- **重大度：** メジャー

c. ［これらの条件をすべて満たすと違反が発生します］セクションで、以下の値を選択します。

- **メトリック：** VM メモリ使用率
- **演算子：** 次より大きい
- **値：** 80
- **条件タイプ：** 固定値

d. ［違反のクリア条件］セクションで、以下の値を選択します。

- **演算子：** 次より小さいか等しい
- **値：** 75

e. ［保存］をクリックします。

9. ［イベント ルール］タブをクリックします。
10. 複数の条件を持つ VMware CPU 使用率イベント ルールを、以下のように作成します。

a. ［イベント ルール］グループ ボックス内の［新規］をクリックします。

b. 新規イベント ルールに以下の値を入力します。

- **名前：** VMwareCpuUtil
- **説明（オプション）：** VMware CPU 使用率

- **メトリック ファミリ：** VMWare 仮想マシン
- **期間**： 300
- **ウィンドウ**： 900
- **重大度：** メジャー

c. ［これらの条件をすべて満たすと違反が発生します］セクションで、以下の値を選択します。

- **メトリック：** CPU 使用率
- **演算子：** 次より大きい
- **値：** 70
- **条件タイプ：** 固定値

d. ［条件の追加］をクリックします。

e. ［これらの条件をすべて満たすと違反が発生します］セクションで、以下の値を選択します。

- **メトリック：** CPU 使用率
- **演算子：** 次より大きい
- **値：** 1
- **条件タイプ：** 標準偏差

注: 複数条件のイベント ルールは、1 つのメトリック ファミリ内のメトリックに限定されます。 この例では、メトリック ファミリが Data Aggregator ですでに使用可能であると想定しています。 カスタム メトリック ファミリを作成する方法の詳細については、「Data Aggregator 自己認定ガイド」を参照してください。

複数の条件を定義すると、いずれかの条件が true でなくなったときにクリア イベントが発行されます。

重要: メトリック ファミリの監視を開始してから Data Aggregator でベースラインが毎時間計算されるまで、最大で 48 時間かかることがあります。 ベースライン データは標準偏差ルールに必要です。

11. ［保存］をクリックします。

イベント ルールが保存されます。 イベント ルールは「カスタム仮想サーバ」監視プロファイル内のメトリック ファミリにフィルタされ、定義したすべてのルールが評価されることを保証します。

監視プロファイルのカスタム デバイス コレクションへの割り当て

「カスタム仮想サーバ」監視プロファイルを作成して、重要なビジネス アプリケーションを実行中の仮想マシンを監視するイベント ルールを追加しました。 仮想デバイスの監視を開始して、イベント ルールをアクティブにするには、［マイ監視サーバ］監視プロファイルを［仮想サーバ］カスタム デバイス コレクションに割り当てます。

重要: *監視プロセスの開始および停止で重要なのはデバイス コレクションです。*Data Aggregator で監視プロファイルを使用するには、少なくとも 1 つのデバイス コレクションに監視プロファイルを割り当てる必要があります。

以下の手順に従います。

1. Data Aggregator 管理ページの［監視設定］メニューから［コレクション］をクリックします。

   デバイス コレクションのリストが表示されます。

2. ［仮想サーバ］デバイス コレクションを選択し、［監視プロファイル］タブをクリックします。

   選択されたデバイス コレクションに割り当てられた監視プロファイルがリスト表示されます。 このリストは空になっています。

3. ［管理］をクリックします。

   ［監視プロファイルへのコレクションの割り当て］ダイアログ ボックスが表示されます。

4. ［利用可能な監視プロファイル］リストから「マイ仮想サーバ」監視プロファイルを選択して、［追加］をクリックします。

   監視プロファイルは、［割り当てられた監視プロファイル］リストに移動します。

5. ［保存］をクリックします。

   Data Aggregator は、監視プロファイルおよびイベント ルールを使用して、このデバイス コレクションの監視を開始します。 生成されたイベントは、［イベントの表示］ダッシュボードに表示されます。

イベントの表示

CA Performance Center は、［イベント］ビューと呼ばれるレポートにイベントを表示します。 最新のイベントが最初に表示されます。 最も適切なイベント データを表示するには、イベント レポートの内容を制御します。レポート内容を制御する機能には、時間制御およびソートとフィルタの機能が含まれます。

例:

- 追跡の設定変更 - カスタム監視プロファイルで［自動的にメトリック ファミリを更新する］オプションを選択しなかった場合、設定変更のイベント ログ ファイルを参照してから手動で［監視対象デバイス］-［ポーリングされるメトリック ファミリ］-［メトリック ファミリの更新］をクリックし、Data Aggregator がデバイスの再設定を確実に取得するようにする必要があります。
- パフォーマンス問題のトラブルシューティング - 特定のサーバでパフォーマンス問題のトラブルシューティングをするには、サーバの IP アドレスでイベントをフィルタリングします。［イベント］ビューは、イベントの完全なリストをフィルタリングすることで、選択したサーバのイベントのみを表示します。

イベントを表示するには、CA Performance Center の［ダッシュボード］メニューをクリックし、［操作の表示］の下の［イベントの表示］を選択します。

［イベント］ビューが表示されます。 テーブルに選択したタイム フレーム内に発生したイベントが表示され、直近のイベントが先頭にリストされます。

注: 上記イベントの詳細については、「*CA Performance Center オペレータ ガイド*」および CA Performance Center オンライン ヘルプを参照してください。

イベント マネージャからの通知を設定する方法

Data Aggregator からイベント マネージャに送信されたイベントに対して通知を設定できます。 受信イベントは、通知条件に設定した状態に対して評価されます。 条件を満たす場合のみ、イベント マネージャは通知アクションを実行します。 イベントが通知をトリガしない場合、このイベントはイベント リストに表示されたままになります。

通知の作成/編集ウィザードでは、以下の通知タイプが利用可能です。

トラップ

CA Spectrum など、環境内の障害管理システムまたはネットワーク管理システム（NMS）にトラップ通知を送信します。複数の送信先をサポートします。 最初の送信先は必須です。

カスタマのシステムに互換性を提供するために、通知ウィザードでは 2 種類の MIB が利用可能です。

サポートされる役割： 管理者の役割を持つユーザがトラップ通知を設定できます。

電子メール

イベントが発生するかクリアされたときに、1 人以上の受信者に電子メール通知を送信します。 電子メールによって提供されるリンクから、アラームをトリガしたデバイスまたはコンポーネントのコンテキスト ページを参照できます。

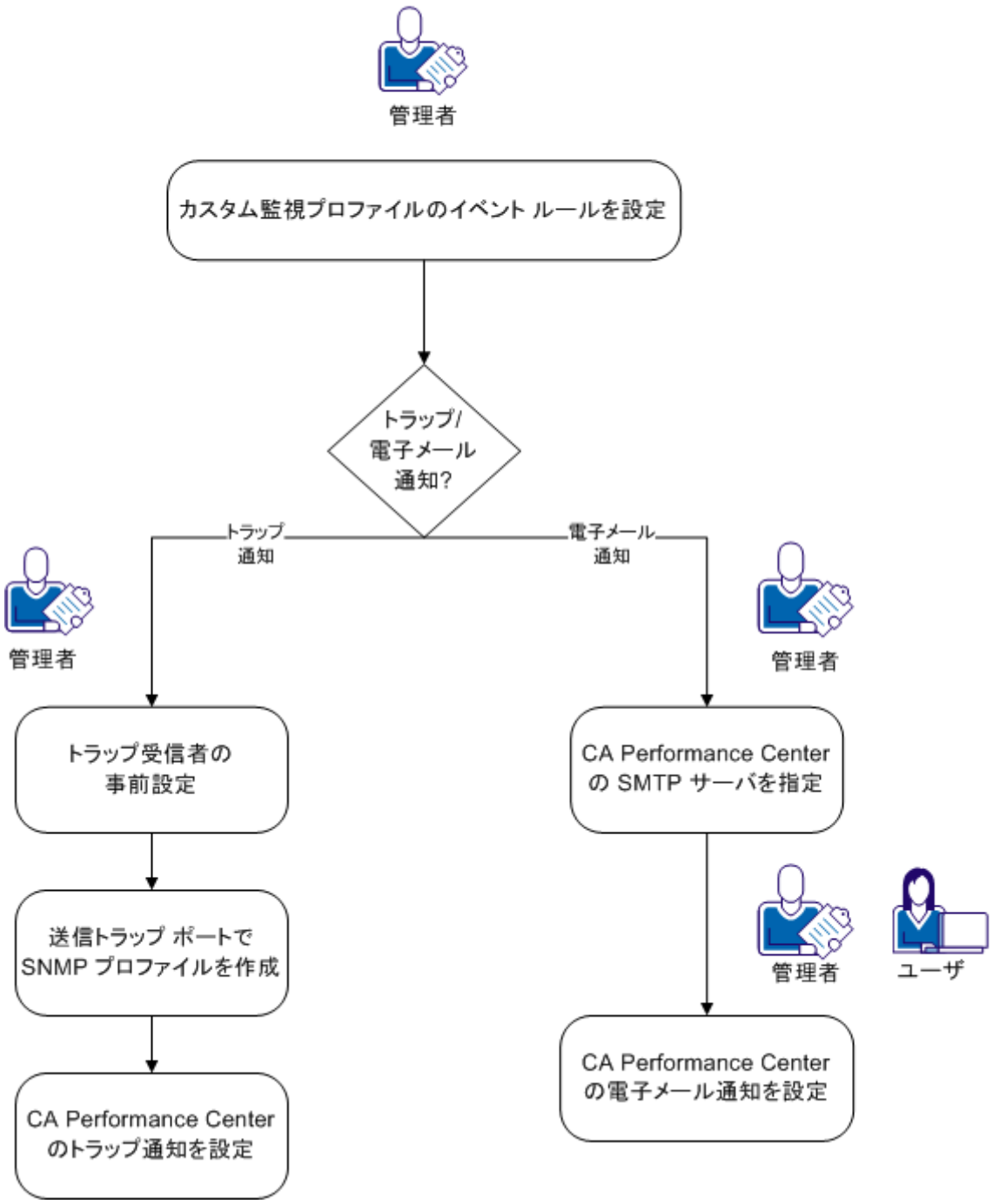
サポートされる役割： 通知の作成の役割を持つユーザが電子メール通知を設定できます。

ユーザが設定および受信するのは、アクセス権があるグループ内のデバイスに対するイベントの通知のみです。

以下の情報を考慮します。

- 通知はユーザに固有です。他のユーザが作成した通知は参照できません。
- 通知オプションが表示されるのは、イベント マネージャが有効であり、同期済みの［利用可能］状態にある場合のみです。
- イベント通知を削除するアクションは、実際のイベントまたは将来のイベントに影響しません。

以下の図に、イベント通知設定のワークフローを示します。



トラップ通知または電子メール通知は、以下の手順を使用して設定できます。

1. Data Aggregator データ ソース管理ページで、監視プロファイルの［イベント ルール］タブのイベント ルールを設定します。
2. （トラップのみ）トラップ受信者はトラップを受信するように事前の設定が必要です。 各送信先では、SNMP コミュニティおよび IPV4 送信先に関する独自の設定を行うことができます。 トラップ形式の詳細については、トラップ受信者に対応する NMS ドキュメントを参照してください。
3. （トラップのみ）通知を作成する前に、送信トラップ ポート（通常は 162）で SNMP プロファイルを作成します。
4. （電子メールのみ）CA Performance Center の［管理］-［システム設定］メニューから［電子メール サーバ］を選択して、SMTP サーバを設定します。
5. 以下の*いずれか*の操作を実行します。
   - （管理者） CA Performance Center で［管理］-［通知］を選択して通知を作成します。 トラップ通知の場合は、手順 2 で作成した SNMP プロファイルを選択します。

     注: デフォルト テナント管理者は、実際のユーザ コンテキストで作業することで、テナント管理者またはテナント ユーザ用の通知を作成できます。 テナント管理者またはテナント ユーザとしてログインします。 または、デフォルト テナント管理者はテナントを管理してユーザのプロキシを実行し、テナント範囲の通知を作成することができます。
   - （ユーザ） CA Performance Center の［マイ設定］-［通知］を選択して、電子メール通知を作成します。

   注: 管理者はイベント マネージャ API を使用して通知を管理することもできます。 次の URL を使用して、イベント マネージャ ホスト上のドキュメント インターフェースにアクセスします :
   http://*hostname:*8281/EventManager/webservice/notifications/documentation

イベント タイプ

CA Performance Management で作成された各イベントにはイベント タイプの情報が含まれており、イベント サブタイプの情報が含まれることもあります。 この情報は、CA Performance Management がイベントを適切に処理し、ユーザにインフラストラクチャのステータスやヘルスについての情報を提供し続けるために役立ちます。

CA Performance Management で提供されている標準イベント タイプには、以下の情報が含まれます。

- ポーリング イベント - ポーリングまたはポーリング データの分析の結果であるイベントに適用されます
- トラップ イベント - トラップ入力の結果であるイベントに適用されます
- しきい値イベント - デバイス上のしきい値違反によってトリガされるイベントに適用されます
- 再設定の変更 - 作成、破棄、変更されたデバイスに適用されます
- 不明イベント - 不明なタイプのイベントを示します
- すべて - イベント エンジンにサブミットされたすべてのイベントについてサブスクライバに通知する、特殊なワイルドカード イベント タイプを指します

イベント タイプはイベントの作成時に自動的に割り当てられます。 ただし、CA Performance Management では、一貫したイベント管理に役立てるために、カスタム イベント タイプの定義ができます。 カスタム イベント タイプを使用して、ユーザの一意なネットワーク環境に適用するイベント ファミリを定義します。 イベント タイプを作成する場合は、そのタイプに必要な属性を決定します。 これにより、単一のイベント タイプのすべてのイベントが、一貫して同じ情報を提供します。

カスタム イベント タイプを作成した後、これらの未加工のイベントをカスタム イベント タイプにマップするためのイベントの正規化ルールを設定します。 正規化されたイベントでは、イベントの処理方法を定義すると、ベンダーおよびバージョンの違いを無視することができます。 したがって、CA Performance Management はより具体的なユーザの管理ニーズに合わせて正規化されたイベントを処理できます。

注: イベントの詳細については、「*CA Performance Center オペレータ ガイド*」を参照してください。

第 7 章: レポート

このセクションには、以下のトピックが含まれています。

ビューの使用方法

ビューおよびレポートは論理ワークフローで使用できます。論理ワークフローでは、企業全体を見て問題を特定した後に、デバイスやコンポーネントにドリル ダウンして問題を切り分けることができます。 トラブルシューティングが必要なシステムまたはアプリケーションがわかっている場合は、デバイスおよびコンポーネントに直接移動できます。 キャパシティ計画や、ネットワークの健全性に関する月単位レポートに対して、ビュー内の情報を使用して潜在的な問題を事前に特定することもできます。

注: データをポーリングしてから、データがビューおよびレポートに表示される間に遅延が発生することがあります。 データのロード エラーが発生した場合、Data Aggregator デバイスにメッセージが記録されます。

以下のタイプのビューおよびレポートが利用可能です。

ダッシュボード

ポーリング済みデータを有意な情報として参照し、企業全体のトップデバイスのレポートを生成することができる、ビューのセットが含まれます。 ダッシュボードを開くには、［ダッシュボード］を選択し、次にリストから特定のダッシュボードを選択します。 必要に応じて、デバイス、さらにデバイス コンポーネントにドリルダウンできます。

デバイス ビュー

指定されたデバイスに対するデフォルト ビューのセットとして、ポーリング済みデータを表示します。デバイスからのデータ ビューを表示するには、ダッシュボードからドリルダウンするか、または［インベントリ］-［デバイス］で特定のデバイスを選択します。 パフォーマンス カテゴリでデバイス コンテキスト ビューを参照するタブを選択します。

デバイス コンポーネント ビュー

デバイス コンポーネントに関する 1 つのレポートに、複数のビューを同時に表示します。 デバイス コンポーネント ページを表示するには、デバイス ビューからドリルダウンするか、または［インベントリ］-［デバイス コンポーネント］を選択し、コンポーネントを選択します。

注: ダッシュボードおよびビューのカスタマイズの詳細については、CA Performance Center のオンライン ヘルプを参照してください。

ビューにデータが表示されない場合、ビューから［監視対象デバイス］ページに直接ドリルダウンして、問題のトラブルシューティングを行います。［**設定**］ボタンを選択し、［**デバイス管理**］をクリックします。 このオプションには、「**ビューから DA 管理ページへのドリル イン**」という役割の権限が必要です。この権限は任意のユーザに割り当てることができます。グローバル管理者には、デフォルトでこの役割の権限があります。

ベースライン平均

収集されたポーリング データの量に応じて、ベースライン平均は 2 つの方法で計算されます。

- はじめは、同一時間（曜日に関係なく）の時間平均の平均値。
- 十分なデータが収集されると、同じ曜日の同一時間における時間平均の平均値。

ベースライン平均は、選択された監視対象メトリックの過去のパフォーマンスを表し、現在のパフォーマンスを評価するために役立ちます。 ベースライン平均および関連する標準偏差は、1 時間ごとに継続的に計算されます。 標準偏差により、ベースライン平均の計算に含まれる母集団データにどれだけの変動が存在するかを示す統計指標が提供されます。

Data Aggregator では、ウィンドウ時間内の指定期間における「標準」は、計算されたベースライン平均に基づいて決定されます。

95 パーセンタイル

パーセンタイルとは、一定パーセントの観察結果がそれ未満の値になる変数の値です。 たとえば、95 パーセンタイルでは、95 パーセントの観察結果がこの値（またはスコア）未満になります。

*95 パーセンタイル モニタリング*は帯域幅に関係します。 この統計はデータ スループットを測定するのに役立ちます。それは、この統計が、帯域幅の影響を受けやすいアプリケーション用の監視対象リンクに必要なキャパシティをより正確に反映するからです。 95 パーセンタイルは、95 パーセントの時間、帯域幅使用率がこの値未満であることを意味します。残りの 5 パーセントの時間、帯域幅使用率はこの値より上です。キャパシティ計画を実行するために 95 パーセンタイルを使用する場合、監視対象デバイスに対するポーリング間隔を、少なくとも 1 分間隔に設定することを推奨します。

95 パーセンタイルは、ロールアップおよびレポートのために計算されます。

*ロールアップ*はメトリック値が集計されるプロセスです。 時間単位のロールアップでは、メトリックに対する 1 分、5 分、15 分、30 分、および 60 分ポーリング値が 1 時間ごとに集計されます。 日単位のロールアップでは、時間単位のメトリック値が日に 1 度集計されます。週単位のロールアップでは、日単位のメトリック値が週に 1 度集計されます。

標準偏差

*標準偏差*は、平均（平均値、または期待値）からの変動がどれだけあるかを示します。 標準偏差が低いのは、データポイントが平均値に非常に近い傾向があることを示しています。 標準偏差が高いのは、データポイントが幅広い値の範囲に広がっていることを示します。

標準偏差は、ロールアップ、およびイベントとレポート生成のために計算されます。

*ロールアップ*はメトリック値が集計されるプロセスです。 時間単位のロールアップでは、メトリックに対する 1 分、5 分、15 分、30 分、および 60 分ポーリング値が 1 時間ごとに集計されます。 日単位のロールアップでは、時間単位のメトリック値が日に 1 度集計されます。週単位のロールアップでは、日単位のメトリック値が週に 1 度集計されます。

最小値および最大値

最小値および最大値はロールアップおよびレポートのために計算されます。 これらの値から、所定の時間間隔におけるパフォーマンスの上限および下限を観察できます。

*ロールアップ*はメトリック値が集計されるプロセスです。 時間単位のロールアップでは、メトリックに対する 1 分、5 分、15 分、30 分、および 60 分ポーリング値が 1 時間ごとに集計されます。 日単位のロールアップでは、時間単位のメトリック値が日に 1 度集計されます。週単位のロールアップでは、日単位のメトリック値が週に 1 度集計されます。

時間単位のロールアップ

- 最小： ポーリングされた値の最小値。
- 最大： ポーリングされた値の最大値。

日単位のロールアップ

- 最小： 時間単位の最小値の最小値。
- 最大： 時間単位の最大値の最大値。

週単位およびそれ以上のロールアップ：

- 最小： 日単位の最小値の最小値。
- 最大： 日単位の最大値の最大値。

5 分間隔レポート

- 最小： ポーリングされた値の最小値。
- 最大： ポーリングされた値の最大値。

1 時間間隔レポート

- 最小： 時間単位の最小値の最小値。
- 最大： 時間単位の最大値の最大値。

1 日間隔レポート

- 最小： 日単位の最小値の最小値。
- 最大： 日単位の最大値の最大値。

付録 A: 計算

このセクションには、以下のトピックが含まれています。

ベースライン平均の計算

はじめに、限られた量のデータが収集されると、過去のすべての曜日の同一時間に対するベースライン平均が計算されます。 たとえば、2 日間の履歴の後に、午前 9:00 ～ 10:00 の期間のベースライン平均値が、連続した 2 日間における同一期間の時間単位ロールアップを平均して計算されます。

最終的に、より多くのデータが利用可能になると、計算方法が自動的に切り替わり、Data Aggregator は利用可能な過去の同じ曜日における時間単位のサンプルを平均して「標準」を確立します。 この方法では、使用率の曜日パターンを考慮に入れます。 この方法によって、「標準」のすぐれた概算値が作成され、誤った違反や誤検出イベントが生成される回数を減らすことができます。 上記と同じ例で、3 週間の履歴の後、ベースライン平均は、過去 3 週間に含まれる 3 回の月曜日の午前 9:00 ～ 10:00 の時間単位ロールアップを平均して計算されます。

注: デフォルトでは、この自動切り替えが発生するのは、過去 12 週間に、同じ曜日の同一時間におけるデータ サンプルが少なくとも 3 つ利用できる場合です。 必要な数のデータ ポイントが利用できなくなると、Data Aggregator は自動的に毎日の同一時間の計算方法に切り替わります。これらのデフォルト設定は設定可能です。 これらのデフォルト設定の変更に関する詳細については、「Data Aggregator REST Web サービス ガイド」を参照してください。

ベースライン平均は、イベントとレポート生成のために計算されます。

例: CPU 使用率について、同一時間の平均および母標準偏差を計算

以下の例では、月曜日、火曜日、および水曜日の午前 2:00 に 3 つのデータポイントがあるとき、特定のデバイスの CPU 使用率について、「同一時間」の平均および母標準偏差がどのように計算されるかを示します。

以下の手順に従います。

1. 3 つのデータ ポイントを収集します。

   曜日： 月曜日 火曜日 水曜日

   平均 CPU 使用率： 76 65 10

2. 母平均を計算します。

   母平均の計算式を以下に示します。

   母平均 = 母集団のデータポイント値の合計/データポイント数。

   この例の式を以下に示します。

   （76+65+10）/3

   母平均 = 50.33

3. 各データポイントの母平均からの差分を計算します。

   この例での差分は次のとおりです。

   25.67 14.67 -40.33

4. データポイントごとの差分の二乗を計算します。

   この例での二乗は次のとおりです。

   658.78 215.11 1,626.778

5. 二乗の合計を計算します。

   この例での二乗の合計は 2,500.67 です。

6. 二乗の合計値を母集団のデータポイント数で割った値を計算します。

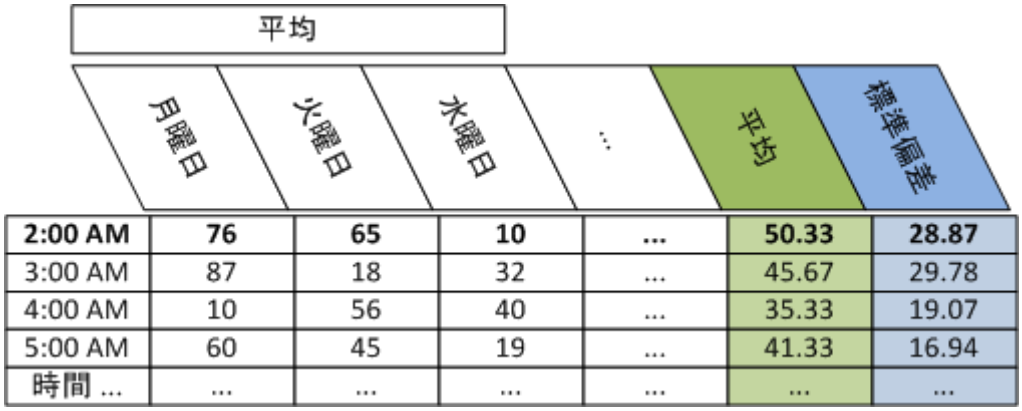
   この例での結果は 833.56 です。

7. 母平均からのデータポイント値の差分を二乗した値の合計の平方根を計算します。

   この例での平方根は 28.87 です。

   この例での標準偏差は 28.87 です。

以下の表に、曜日ごとの使用率データの時間平均、時間平均の平均値、および同一時間の時間平均の母標準偏差を示します。



2:00 AM	**76**	**65**	**10**	**...**	**50.33**	**28.87**
3:00 AM	87	18	32	...	45.67	29.78
4:00 AM	10	56	40	...	35.33	19.07
5:00 AM	60	45	19	...	41.33	16.94
時間 ...	...	...	...	...	...	...

例: CPU 使用率について、同じ曜日の同一時間における平均および母標準偏差を計算

以下の例では、3 つの月曜日の午前 2:00 に 3 つのデータ ポイントがあるとき、特定のデバイスの CPU 使用率について、平均および母標準偏差がどのように計算されるかを示します。

以下の手順に従います。

1. 3 つのデータ ポイントを収集します。

   月曜日： 1 2 3

   平均 CPU 使用率： 76 4 6

2. 母平均を計算します。

   母平均の計算式を以下に示します。

   母平均 = 母集団のデータポイント値の合計/データポイント数。

   この例の式を以下に示します。

   （76+4+6）/3

   母平均 = 28.67

3. 各データポイントの母平均からの差分を計算します。

   この例での差分は次のとおりです。

   47.33　　-24.67　　-22.67

4. データポイントごとの差分の二乗を計算します。

   この例での二乗は次のとおりです。

   2,240.44　　608.44　　513.78

5. 二乗の合計を計算します。

   この例での二乗の合計は 3,362.67 です。

6. 二乗の合計値を母集団のデータポイント数で割った値を計算します。

   この例での結果は 1,120.89 です。

7. 母平均からのデータ ポイント値の差分を二乗した値の合計の平方根を計算します。

   この例での平方根は 33.48 です。

   この例での標準偏差は 33.48 です。

以下の表に、曜日ごとの使用率データの時間平均、時間平均の平均値、および同じ曜日の同一時間における時間平均の母標準偏差を示します。

	平均							
	週 1		週 2		週 3		月曜日	
	月曜日	...	月曜日	...	月曜日	...	平均	標準偏差
2:00 AM	**76**	**...**	**4**	**...**	**6**	**...**	**28.67**	**33.48**
3:00 AM	87	...	71	...	56	...	71.33	12.66
4:00 AM	10	...	27	...	58	...	31.67	19.87
5:00 AM	60	...	3	...	32	...	31.67	23.27
時間 ...	...	...	...	...	...	...	...	...

例: CPU 使用率について、同じ曜日の同一時間における平均および母標準偏差を使用した標準からの偏差

Data Aggregator は 5 分間隔で CPU 使用率データをポーリングしていると仮定します。CPU 使用率が、単一の 5 分ポーリング間隔の平均から 1 標準偏差を超えるとイベントを生成するように、イベント ルールを定義します。

この例では、イベント ルールの期間およびウィンドウは共に 5 分に設定されています。

イベントが発生したときの計算式を以下に示します。

CPU 使用率 = 平均値 + 1（標準偏差値）

したがって、月曜日の午前 2:00 における、過去の同じ曜日の同一時間からの平均値と標準偏差値を代入します。

CPU 使用率 = 28.67 + 1（33.48）

CPU 使用率 = 62.15

その結果、月曜日の午前 1:05 ～ 午前 2:00 の間に、単一の 5 分ポーリング間隔で CPU 使用率が 62.15 を超えると、イベントが発生します。このイベントは、CPU 使用率がそのタイムフレームの標準から逸脱したことを示します。

例: トレンド グラフ ビューで CPU 使用率イベントを確認

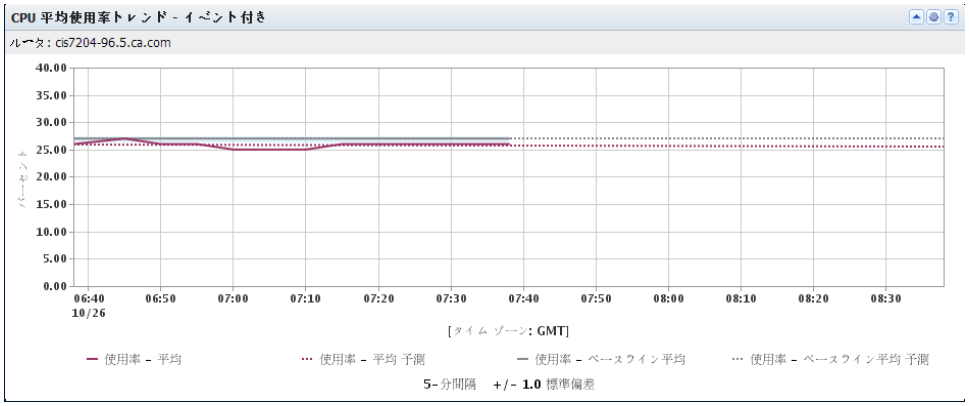
Data Aggregator は 5 分間隔で CPU 使用率データをポーリングしていると仮定します。この例では、ビジネス上重要なサーバの 1 つが予想レベルよりも低い CPU 使用率になったときにアラートを受け取るようにします。CPU 使用率が、単一の 5 分ポーリング間隔の平均から 1 標準偏差ぶん下回るときにイベントを生成するように、イベント ルールを定義します。

説明のために、月曜日の午前 12:00 から日曜日の午前 12:00 までの CPU 使用率が 50 パーセントであると仮定します。 日曜日の午前 12:00 から月曜日の午前 12:00 までに、CPU 使用率は 10 パーセントに低下します。 ユーザはこの使用率の低下を予想しています。ただし、Data Aggregator がベースライン平均の計算を開始すると、CPU 使用率が 10 パーセントに低下したときにイベントが発生します。 CPU 使用率が 50 パーセントに戻ると、イベントはクリアされます。 誤ったイベントが発生する理由は、はじめに限られた量のデータが収集されると、毎日の同一時間に対するベースライン平均が計算され、異なる曜日での使用率の違いが考慮されていないためです。 Data Aggregator は、CPU 使用率が常に 50 パーセントであると予想しています。

3 週間後に、同じ曜日の同一時間におけるデータ サンプルが 3 つ利用できるようになると、ベースライン平均の計算方法が変更されます。 Data Aggregator は、同じ曜日の時間単位のサンプルを平均して、「標準」の値を確立します。 これにより、Data Aggregator は、日曜日の午前 12:00 から月曜日の午前 12:00 の間の CPU 使用率が 10 パーセントであると予想するようになります。毎週日曜日の午前 12:00 に発生していた誤ったイベントは、発生しなくなりました。

以下のビューは、はじめに、毎日の同一時間に対するベースライン平均が計算されていることを示します。 より多くのデータが利用可能になると、計算方法が自動的に切り替わります。 Data Aggregator は、同じ曜日の時間単位のサンプルを平均します。

このビューは、計算方法の切り替えが行われると、誤ったイベントが発生しなくなることも示しています。



95 パーセンタイル計算

95 パーセンタイルは、ロールアップ、およびイベントとレポート生成のために計算されます。

ロールアップ

- 時間単位のロールアップでは、95 パーセンタイルはポーリングされた値の継続的なパーセンタイルとして計算されます。
- 日単位のロールアップでは、95 パーセンタイルは時間単位の 95 パーセンタイルの継続的なパーセンタイルとして計算されます。
- 週単位およびそれ以上のロールアップでは、95 パーセンタイルは、日単位の 95 の継続的なパーセンタイルとして計算されます。

レポート

- 間隔が 1 日未満のとき、95 パーセンタイルは、ポーリングされた値の継続的なパーセンタイルとして計算されます。
- 間隔が 1 日以上のとき、95 パーセンタイルは 95 の 95 として計算されます。

例: 95 パーセンタイルの計算

以下の例では、1 時間の計算および 5 分のポーリング サイクルとして、95 パーセンタイルの計算法を示します。

以下の手順に従います。

1. 5 分のポーリング サイクルで 1 時間分のデータを収集します。

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

   30 10 20 70 60 30 80 10 90 20 70 50

   並べ替え

   10 10 20 20 30 30 50 60 70 70 80 90

2. 行番号（RN）、フロア行番号（FRN）およびシーリング行番号（CRN）値を計算します。

   RN、FRN および CRN の計算式を以下に示します。

   - RN = 1+((N-1)*P)

     N

     収集された、ポーリングされた値の数を表します。

     P

     パーセンタイル値を表します。

   - FRN = floor(RN)

     FRN

     RN 以下で最大の整数を表します。

   - CRN = ceiling(RN)

     CRN

     RN 以上で最小の整数を表します。

   この例の式は以下のように表されます。

   ```
   RN = 1+((12-1)*0.95) = 11.45
   FRN = floor(RN) = 11
   CRN = ceiling(RN) = 12
   ```

3. 95 パーセンタイルの計算

   95 パーセンタイルの計算式を以下に示します。

   ```
   if (CRN = FRN = RN) then
   （RN の行からの式の値）
   else
   （FRN の行に対する式の値） + （RN - FRN） * （CRN 行値 - FRN 行値）
   ```

   この例の式を以下に示します。

   ```
   (80) + (11.45 - 11)*(90-80) = 84.5000
   ```

   この例の 95 パーセンタイルは 84.5000 です。

標準偏差の計算

標準偏差は、ロールアップ、およびイベントとレポート生成のために計算されます。

ロールアップ

- 時間単位のロールアップについては、標準偏差はポーリングされた値に対して計算されます。
- 日単位のロールアップについては、標準偏差は時間単位の平均に対して計算されます。
- 週単位およびそれ以上のロールアップについては、標準偏差は日単位の平均に対して計算されます。

イベント

- 標準偏差により、ベースライン平均の計算に含まれる母集団データにどれだけの変動が存在するかを示す統計指標が提供されます。

レポート

- 時間単位のレポートについては、標準偏差はポーリングされた値に対して計算されます。
- 日単位のレポートについては、標準偏差は時間単位の平均に対して計算されます。
- 週単位およびそれ以上のレポートについては、標準偏差は日単位の平均に対して計算されます。

例: 人口の標準偏差を計算します。

以下の例では、与えられた 12 ポイントのデータで、人口の標準偏差の計算法を示します。

*人口*は、観察される場合だけでなく潜在的に観察可能な場合を含めた、1 組の潜在的な値を参照します。

この標準偏差を計算する式は次のとおりです。

母集団の偏差 = (((X - 母平均)/データポイント数) の合計) の平方根

X

母集団のデータポイントの値です。

以下の手順に従います。

1. 12 ポイントのデータを収集します。

   1　2　3　4　5　6　7　8　9　10　11　12

   30　10　20　70　60　30　80　10　90　20　70　50

2. 母平均を計算します。

   母平均 = 母集団のデータポイント値の合計/データポイント数。

   この例の母平均は 45 です。

3. 各データポイントの母平均からの差分を計算します。

   この例での差分は次のとおりです。

   -15　-35　-25　25　15　-15　35　-35　45　-25　25　5

4. データポイントごとの差分の二乗を計算します。

   この例での二乗は次のとおりです。

   225　1225　625　625　225　225　1225　1225　2025　625　625　25

5. 二乗の合計を計算します。

   この例の二乗の合計は 8900 です。

6. 二乗の合計値を母集団のデータポイント数で割った値を計算します。

   この例の合計値は 741.6666667 です。

7. 母平均からのデータポイント値の差分を二乗した値の合計の平方根を計算します。

   この例での平方根は 27.23355773 です。

   この例の標準偏差は 27.23355773 です。

合計の計算

カウンタ メトリックは、ロールアップ、およびイベントとレポート生成のために計算されます。 カウンタ メトリックでは、一定期間内のすべてのサンプルの合計が計算されます。 複合トレンド ビュー タイプの動的トレンド ビューに含まれるすべてのアイテムの合計を計算する場合、ビューで選択されたアイテムすべての値の合計が計算されます。 一方、一定期間内のすべてのサンプルの平均を計算する場合は、ゲージ メトリック タイプを使用します。

例: 合計の計算

以下の例では、1 時間の計算および 5 分のポーリング サイクルとして、合計の計算法を示します。

以下の手順に従います。

1. 5 分のポーリング サイクルで 1 時間分のデータを収集します。

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

   40 10 30 60 70 20 50 20 80 30 40 60

2. 12 件のサンプルの合計を計算します。

   この例の合計は 510 です。

ゲージ メトリック タイプおよびカウンタ メトリック タイプの集計の場合は、ビュー内のアイテム/グループすべての値の合計または平均を計算することになります。 集計された多数のアイテムに対してゲージを計算する場合は、アイテムの個々の平均が加算されます。 その平均の合計をアイテムの数で割ってゲージを求めます。 同様に、カウンタは、集計される各アイテムの個別の合計値を取得し、個別の合計をすべて加算して合計を求めます。

例: カウンタ メトリックおよびゲージ メトリック

ルータの下のすべてのインターフェースのカウンタ メトリックを計算すると、スループット ビットを表示できます。 すべてのインターフェースの使用率を参照するには、ゲージ メトリックを計算します。

最小値および最大値

最小値および最大値はロールアップおよびレポートのために計算されます。 これらの値から、所定の時間間隔におけるパフォーマンスの上限および下限を観察できます。

*ロールアップ*はメトリック値が集計されるプロセスです。 時間単位のロールアップでは、メトリックに対する 1 分、5 分、15 分、30 分、および 60 分ポーリング値が 1 時間ごとに集計されます。 日単位のロールアップでは、時間単位のメトリック値が日に 1 度集計されます。週単位のロールアップでは、日単位のメトリック値が週に 1 度集計されます。

時間単位のロールアップ

- 最小： ポーリングされた値の最小値。
- 最大： ポーリングされた値の最大値。

日単位のロールアップ

- 最小： 時間単位の最小値の最小値。
- 最大： 時間単位の最大値の最大値。

週単位およびそれ以上のロールアップ：

- 最小： 日単位の最小値の最小値。
- 最大： 日単位の最大値の最大値。

5 分間隔レポート

- 最小： ポーリングされた値の最小値。
- 最大： ポーリングされた値の最大値。

1 時間間隔レポート

- 最小： 時間単位の最小値の最小値。
- 最大： 時間単位の最大値の最大値。

1 日間隔レポート

- 最小： 日単位の最小値の最小値。
- 最大： 日単位の最大値の最大値。

付録 B: トラブルシューティング

このセクションには、以下のトピックが含まれています。

トラブルシューティング : ディスカバリが開始しない

問題の状況:

ディスカバリ プロファイルを選択し、ディスカバリを実行するために［実行］をクリックしましたが、ディスカバリが開始しないか、または［実行］ボタンが無効です。

解決方法:

ディスカバリが失敗したり、［実行］ボタンが無効だったりする場合に考えられる理由には、以下のようなものがあります。

- 以前にディスカバリ プロファイルで指定された IP ドメインが削除されています。 ディスカバリ プロファイルを IP ドメインに割り当てます。
- 選択したディスカバリ プロファイルに指定されている IP ドメインに、Data Collector がインストールされていません。

  注: Data Collector ホストのインストールの詳細については、「Data Aggregator インストール ガイド」を参照してください。

- 選択したディスカバリ プロファイルに指定されている IP ドメインに、1 つ以上の Data Collector ホストがインストールされています。 ただし、IP ドメインにインストールされている Data Collector ホストはすべて停止しています。 Data Collector ホストを起動します。
- テナントが非アクティブにされます。テナントをアクティブにします。

詳細情報:

ディスカバリ プロファイルの編集 (P. 81)
テナントの有効化 (P. 123)

トラブルシューティング : ポーリングが検出されたメトリック ファミリ上で停止する

問題の状況:

監視対象デバイス ページからデバイスを選択すると、そのデバイスでサポートされているメトリック ファミリがポーリングを停止したことがわかりました。 そのメトリック ファミリのポーリングを停止するつもりはありませんでした。

解決方法:

以下のプロセスに従って、なぜポーリングが停止したかを確認し、その原因を解決する適切な手順を実行します。

1. 監視プロファイルが定義され、目的とするメトリック ファミリのポーリングをするように設定されていることを確認します (P. 100)。

   この要件がまだ満たされていない場合は、目的のメトリック ファミリが定義された監視プロファイルを作成または編集します。

2. デバイスがデバイス コレクションと関連付けられていることを確認します (P. 105)。

   デバイスがデバイス コレクションと関連付けられていない場合、デバイスをデバイス コレクションに追加します。

   注: デバイス コレクションへのデバイス追加の詳細については、「*CA Performance Center 管理者ガイド*」を参照してください。

3. 監視プロファイルがデバイス コレクションとデバイスに関連付けられていることを確認します (P. 100)。

   監視プロファイルが関連付けられていない場合、監視プロファイルとデバイス コレクションの間に関係を作成します (P. 102)。

ポーリングを再開するため、これらのアクションの 1 つを完了したら、［監視対象デバイス］ページでデバイスを選択し、以下を確認します。

- ［ポーリングされるメトリック ファミリ］タブのメトリック ファミリのステータスが変更されました。
- インターフェース コンポーネント テーブル内のステータスが［アクティブ］に変更されました。

既存デバイスのポーリングは自動的に再開します。

新しいデバイスは以下のいずれかの方法で検出できます。

- ［監視対象デバイス］ページでポーリングされるメトリック ファミリを選択し、［メトリック ファミリの更新］をクリックします (P. 111)。
- 自動ディスカバリを［True］に設定した状態で、そのメトリック ファミリの監視プロファイルで［変更の検出レート］を設定します。

トラブルシューティング：ポーリングが停止したというイベント メッセージ

問題の状況：

「ポーリングが停止した」というイベントがイベント リストに表示されました。 なぜですか。

解決方法：

デフォルトでは、Data Aggregator は SNMP ポーリングを制御し、デバイスに対するポーリング リクエストが多くなりすぎないようにします。 ポーリング トラフィックを制御する 1 つの方法は、SNMP タイムアウトしきい値です。 デフォルトのしきい値は 15 です。 そのため、15 以上の SNMP リクエストがタイムアウトすると、現在のポーリング サイクルの残りの間、ポーリングが一時停止されます。 イベントが生成され、その状況がユーザに通知されます。

注: 各ポーリング サイクルの最初の時点でポーリングが再開されます。 5 分間のポーリング サイクルの間にポーリング タイムアウトが発生しない場合、「クリア」イベントが生成されます。

トラブルシューティング：重要性の高いデバイスに対してポーリングが完了しない

問題の状況：

監視する必要がある重要なデバイスがありますが、単一のポーリング サイクルでポーリングを完了できません。 時々ネットワーク トラフィックの量が多すぎて、デバイスが動作を完全に停止することがあります。 このデバイスは重要性が高いため、このデバイスを確実にポーリングして高いパフォーマンスを確保する必要があるのですが、どうしたら良いでしょうか。

解決方法:

ポーリングはデバイスの監視に不可欠です。 しかし、ポーリングが多すぎると、ネットワーク トラフィックの量が多くなりすぎる可能性があり、デバイスを正常に監視できなくなることがあります。 ネットワーク トラフィックの量が多すぎて重要なデバイスに悪影響を及ぼしている場合、デバイスに対する全体のトラフィックを減らすために以下の手順を試行できます。

- 監視プロファイルを調整して、不要なメトリック ファミリをポーリングから削除します。
- 監視プロファイルにフィルタを適用し、ポーリングされるインターフェースの数を減らします。
- 監視プロファイルを調整し、ポーリングの頻度を減らします（たとえば、SNMP ポーリング レートをデフォルトの 5 分から 15 分に変更します）。
- SNMP トラフィックしきい値を調整し、一度にデバイスに送信される SNMP リクエストの数を減らします。
- 現在のポーリング サイクルにおいてポーリングを一時停止させる ポーリング タイムアウトしきい値を制御する SNMP タイムアウトしきい値を調整します。

トラブルシューティング : Data Aggregator の予期しないシャットダウン

問題の状況:

Data Aggregator が予期せずシャットダウンします。

解決方法:

Data Repository との接続が失われると、Data Aggregator はシャットダウンします。 Data Repository との接続が失われると、*Data Aggregator のインストール ディレクトリ*/apache-karaf-2.3.0/shutdown.log ファイルに監査メッセージが記録されます。

注: *Data Aggregator インストール ディレクトリ* /apache-karaf-2.1.3/shutdown_details.log には、Data Aggregator と Data Repository の間のハートビート メッセージ、および Data Aggregator のシャットダウンがデバッグ目的で記録されます。

Data Repository の接続性またはその他の問題を解決するには、以下の手順に従います。

1. Data Repository プロセスが実行中であることを確認します。 以下のアクションを実行します。
   a. Data Repository に使用するデータベース サーバに、(root ユーザではなく) データベース管理者ユーザとしてログインします。
   b. 以下のコマンドを入力します。

      ```
      /opt/vertica/bin/adminTools
      ```

      ［Administration Tools］ダイアログ ボックスが表示されます。
   c. ［(1) View Database Cluster State］を選択します。

      表示されるウィンドウで、次の状態である必要があります:「Host : ALL」、「State : UP」
2. Data Repository が実行中でない場合は、以下の手順に従って起動します。
   a. Data Repository に使用するデータベース サーバにログインします。
   b. 以下のコマンドを入力します。

      ```
      /opt/vertica/bin/adminTools
      ```

      ［Administration Tools］ダイアログ ボックスが表示されます。
   c. ［(3) Start Database］を選択します。
   d. データベース名の隣のスペース バーを押し、［OK］を選択して Enter キーを押します。

      データベース パスワードの入力を促すプロンプトが表示されます。
   e. データベース パスワードを入力し、Enter キーを押します。

      Data Repository データベースが起動します。

      注: ユーザ名またはパスワードのエラーにより接続できないというエラー メッセージが表示される場合、Data Aggregator が Data Repository から切断された原因はデータベース パスワードの変更である可能性があります。
   f. ［(E) Exit］を選択して Enter キーを押します。

      Data Repository が起動しない場合は、CA テクニカル サポートまでお問い合わせください。

3. Data Repository が実行中の場合は、ネットワーク遅延など、ネットワーク接続の問題が発生しています。 ネットワーク接続の問題に対処してください。
4. Data Aggregator が再実行されたら、Data Aggregator プロセスの自動復旧をセットアップします。

   注: Data Aggregator プロセスを自動復旧する設定の詳細については、「Data Aggregator インストール ガイド」を参照してください。

トラブルシューティング : Data Repository をバックアップできない

問題の状況:

Data Repository をバックアップするために vbr.py スクリプトを実行すると、「Another vbr instance is already running」というメッセージが表示されます。

解決方法:

このメッセージは、いくつかの理由（たとえば、パスワードなし ssh が正しくセットアップされていないなど）で、以前のバックアップ試行が失敗したことを示します。

Data Repository のバックアップを再試行するには、以下の手順に従います。

1. バックアップする Data Repository がインストールされているコンピュータから、/tmp/.initiator.mutex ファイルを削除します。

   通常、次のスケジュール済みバックアップが発生します。

トラブルシューティング : 複数の SNMP デバイスで侵入アラームがトリガされる

問題の状況:

制限されたファイアウォール設定（DMZ ネットワークなど）の背後に、多数の SNMP デバイスを配置しています。セキュリティ上の理由で、これらの SNMP デバイスには異なるコミュニティ文字列が設定されています。それぞれの異なるコミュニティ文字列に対して SNMP プロファイルを定義しましたが、侵入アラームを受け取り、CA Performance Center からログアウトされました。

解決方法:

デバイスに対する正しい SNMP プロファイルを特定するために、CA Performance Center はすべての SNMP プロファイルを試行します。 この動作によって侵入アラームがトリガされ、CA Performance Center からログアウトされる可能性があります。

この問題を解決するには、以下の手順に従います。

1. 重要な SNMP デバイス用に個別のディスカバリ プロファイルを作成します。
2. 正しいコミュニティ文字列を含む SNMP プロファイルを、ディスカバリ プロファイルに割り当てます。
3. 重要な SNMP デバイスのそれぞれに対して、手順 1 と 2 を繰り返します。

ディスカバリが実行されると、割り当てられた SNMP プロファイルのみが使用されます。

用語集

95 パーセンタイル モニタリング

*95 パーセンタイル モニタリング*は帯域幅に関係します。 この統計はデータ スループットを測定するのに役立ちます。それは、この統計が、帯域幅の影響を受けやすいアプリケーション用の監視対象リンクに必要なキャパシティをより正確に反映するからです。 95 パーセンタイルは、95 パーセントの時間、帯域幅使用率がこの値未満であることを意味します。残りの 5 パーセントの時間、帯域幅使用率はこの値より上です。

Data Collector

Data Collector は、データ収集を調整し、レポートおよびイベント分析に使用されるデータをアクティブにポーリングします。 オペレーショナル メトリックと設定データは、検出されたデバイスおよびその監視対象コンポーネント上でポーリングされます。収集されたデータは Data Aggregator を通して渡され、Data Repository に格納されます。

アイテム

アイテムは、Data Aggregator が監視するデバイス、コンポーネント、またはインターフェースです。

監視プロファイル

*監視プロファイル*はデバイスのコレクションに関連付けられ、ポーリングするための情報およびポーリング レートを指定します。 これらのパラメータはデバイス コレクション内の各デバイスに適用されます。ルータ、スイッチおよびサーバなどのデバイスのタイプに基づいて取り揃えたデフォルトの監視プロファイルが用意されています。
監視プロファイルには、関連デバイス コレクション内の各デバイス アイテムに適用されるイベント ルールも含まれています。 ルール評価は、デバイス コレクション内の各デバイス アイテム、およびイベント ルールに指定した各メトリックに対して行われます。 これらのルール評価によって、発生イベントまたはクリア イベントが生成されます。 その後、これらのイベントは、CA Performance Center、CA Spectrum、および CA Performance Center Notifier のイベント マネージャに送信され、さらに処理されます。

ディスカバリ プロファイル

*ディスカバリ プロファイル*では、インベントリ ディスカバリがどのように動作するか、また、デバイスの特定に使用される IP アドレス、IP アドレス範囲、およびホスト名などを指定します。

デバイス コレクション

*デバイス コレクション*は、サーバやルータなどの監視対象デバイスの論理グループです。

標準偏差

*標準偏差*は、平均（平均値、または期待値）からの変動がどれだけあるかを示します。 標準偏差が低いのは、データポイントが平均値に非常に近い傾向があることを示しています。 標準偏差が高いのは、データポイントが幅広い値の範囲に広がっていることを示します。

ファクトリ

Data Aggregator の「*ファクトリ*」という語は、CA Technologies が提供するアイテムを表し、多くの場合は製品にインストールされています。 たとえば、Data Aggregator はファクトリ ベンダー認定、監視プロファイルなどを提供します。 すぐに使用できるこれらのアイテムによって、Data Aggregator はインストールしてすぐに操作することができます。これらは、同じアイテムのカスタム バージョンの作成またはインポートの例としても使用できます。ほとんどの場合、Data Aggregator ユーザはこれらのファクトリ アイテムを編集できません。

ベースライン平均

収集されたポーリング データの量に応じて、ベースライン平均は 2 つの方法で計算されます。

- はじめは、同一時間（曜日に関係なく）の時間平均の平均値。
- 十分なデータが収集されると、同じ曜日の同一時間における時間平均の平均値。

ベースライン平均は、選択された監視対象メトリックの過去のパフォーマンスを表し、現在のパフォーマンスを評価するために役立ちます。 ベースライン平均および関連する標準偏差は、1 時間ごとに継続的に計算されます。 標準偏差により、ベースライン平均の計算に含まれる母集団データにどれだけの変動が存在するかを示す統計指標が提供されます。

Data Aggregator では、ウィンドウ時間内の指定期間における「標準」は、計算されたベースライン平均に基づいて決定されます。

メトリック ファミリ

*メトリック ファミリ*は、指定されたテクノロジーに対して収集しレポートする値のセットを定義します。 レポートがデータ ソースにかかわらず均一になるように、これらの値は正規化されます。 監視プロファイル内に含まれているとき、メトリック ファミリはその監視プロファイルと関連付けられるデバイスに対してどの値を収集する必要があるか決定します。

ロールアップ

*ロールアップ*はメトリック値が集計されるプロセスです。 時間単位のロールアップでは、メトリックに対する 1 分、5 分、15 分、30 分、および 60 分ポーリング値が 1 時間ごとに集計されます。 日単位のロールアップでは、時間単位のメトリック値が日に 1 度集計されます。週単位のロールアップでは、日単位のメトリック値が週に 1 度集計されます。