構成と管理
OnCommand Insight

NetApp
October 24, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/oncommand-insight/config-admin/opening-insight.html on October 24, 2024. Always check docs.netapp.com for the latest.

目次

構成と管理 . . . 1
- Insightをセットアップしています . . . 1
- Insightセキュリティ . . . 97
- スマートカードおよび証明書によるログインのサポート . . . 123
- Data Warehouseでスマートカードおよび証明書によるログインを設定しています . . . 133
- スマートカードおよび証明書によるログインのためのCognosの設定（OnCommand Insight 7.3.10以降） . . . 134
- CognosおよびDWHのCA署名SSL証明書のインポート（Insight 7.3.10以降） . . . 136
- SSL証明書のインポート . . . 138
- ビジネスエンティティ階層 . . . 141
- アノテーションの定義 . . . 144
- アセットを照会しています . . . 160
- Insightデータソース管理 . . . 167
- デバイス解決 . . . 274
- Insightのメンテナンス . . . 293
- 環境の監視 . . . 317
- OCI Data Collectorのサポートマトリックス . . . 347

構成と管理

Insightをセットアップしています

Insightをセットアップするには、Insightのライセンスをアクティブ化し、データソースをセットアップし、ユーザと通知を定義し、バックアップを有効にして、必要な高度な設定手順を実行する必要があります。

OnCommand Insight システムをインストールしたら、次のセットアップタスクを実行する必要があります。

- Insightのライセンスをインストールします。
- Insightでデータソースを設定します。
- ユーザアカウントを設定します。
- Eメールを設定します。
- 必要に応じて、SNMP、Eメール、またはsyslogの通知を定義します。
- Insightデータベースの自動週次バックアップを有効にします。
- アノテーションやしきい値の定義など、必要な高度な設定手順を実行します。

Web UIへのアクセス

OnCommand Insight をインストールしたら、ライセンスをインストールし、環境を監視するようにInsightをセットアップする必要があります。そのためには、Webブラウザを使用してInsight Web UIにアクセスします。

手順

1. 次のいずれかを実行します。

   - InsightサーバでInsightを開きます。

     ```
     https://fqdn
     ```

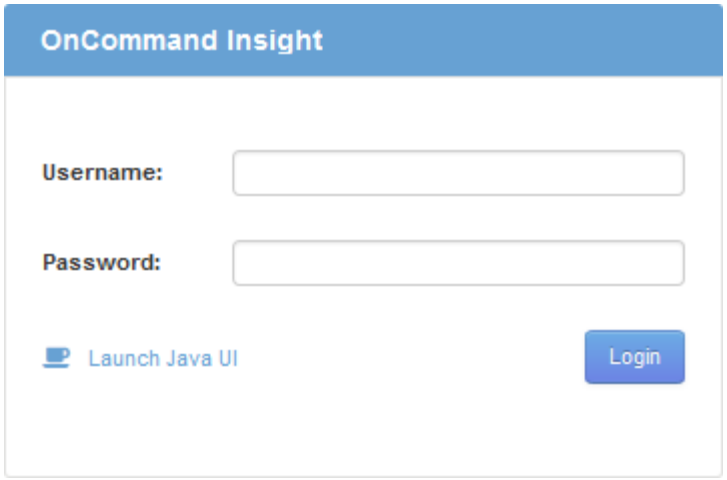
   - その他の場所からInsightを開きます。

     ```
     https://fqdn:port
     ```

     ポート番号には、443またはInsight Serverのインストール時に設定した別のポートを指定します。URLで指定しない場合、ポート番号はデフォルトで443になります。

   OnCommand Insight ダイアログボックスが表示されま

す。



2. ユーザー名とパスワードを入力し、* Login *をクリックします。

   ライセンスがインストールされている場合は、データソースのセットアップページが表示されます。

   Insightのブラウザセッションが30分間アクティブでないとタイムアウトになり、システムから自動的にログアウトされます。セキュリティを強化するために、Insightからログアウトしたあとにブラウザを閉じることを推奨します。

Insightのライセンスをインストールします

Insightのライセンスキーが格納されたライセンスファイルをネットアップから受け取ったら、セットアップ機能を使用してすべてのライセンスを同時にインストールできます。

このタスクについて

Insightのライセンスキーはに格納されます `.txt` または `.lcn` ファイル。

手順

1. ライセンスファイルをテキストエディタで開き、テキストをコピーします。
2. ブラウザでInsightを開きます。
3. Insightのツールバーで、*[Admin]*をクリックします。
4. [設定]*をクリックします。
5. [ライセンス]タブをクリックします。
6. ［ * ライセンスの更新 * ］ をクリックします。
7. ライセンスキーのテキストを* License *テキストボックスにコピーします。
8. [更新（最も一般的な）]*操作を選択します。
9. [保存（ Save ）] をクリックします。
10. Insightの消費ライセンスモデルを使用している場合は、セクションの[使用状況情報をネットアップに送信する]*チェックボックスをオンにする必要があります。プロキシが適切に設定され、環境に応じて有効に

なっている必要があります。

完了後

ライセンスをインストールしたら、次の設定作業を実行できます。

- データソースを設定します。
- OnCommand Insight ユーザアカウントを作成します。

OnCommand Insight ライセンス

OnCommand Insight は、Insight Serverで特定の機能を有効にするライセンスで動作します。

- * 発見 *

  Discoverは、インベントリをサポートするInsightの基本ライセンスです。OnCommand Insight を使用するにはDiscoverライセンスが必要です。また、DiscoverライセンスをAssure、Perform、またはPlanの少なくとも1つのライセンスと組み合わせて使用する必要があります。

- 保証

  Assureライセンスは、グローバルパスポリシーやSANパスポリシー、違反管理などの保証機能をサポートします。脆弱性を表示および管理するには、Assureライセンスも必要です。

- 実行

  Performは、アセットページ、ダッシュボードウィジェット、クエリなどでのパフォーマンス監視、およびパフォーマンスポリシーや違反の管理をサポートするライセンスです。

- 計画

  Planライセンスは、リソースの使用状況や割り当てなどの計画機能をサポートします。

- * Host Utilization Pack *

  Host Utilizationライセンスは、ホストおよび仮想マシンでのファイルシステムの使用をサポートします。

- レポートオーサリング

  Report Authoringライセンスでは、レポートの作成者を追加できます。このライセンスにはPlanライセンスが必要です。

OnCommand Insight モジュールのライセンスは、年間または無期限で提供されます。

- Discover、Assure、Plan、Performモジュールの監視対象容量（テラバイト）
- Host Utilizationパックのホスト数
- Report Authoringに必要なCognos Pro-Authorsの追加単位数

ライセンスキーは、顧客ごとに生成される一意の文字列のセットです。ライセンスキーは、OnCommand Insight の担当者から入手できます。

インストールされているライセンスによって、ソフトウェアで使用できる次のオプションが制御されます。

- * 発見 *

  インベントリの取得と管理（基盤）

  変更を監視し、インベントリポリシーを管理します

- 保証

  SANパスのポリシーや違反を表示および管理します

  脆弱性を確認および管理します

  タスクと移行を表示および管理します

- 計画

  リクエストを表示および管理します

  保留中のタスクを表示および管理します

  リザベーション違反を表示および管理します

  ポートバランス違反を表示および管理します

- 実行

  パフォーマンスデータ（ダッシュボードウィジェット、アセットページ、クエリのデータなど）を監視します

  パフォーマンスポリシーや違反を表示および管理します

次の表に、adminユーザとadmin以外のユーザについて、Performライセンスがある場合とない場合に使用できる機能の詳細を示します。

機能（admin）	Performライセンスあり	Performライセンスなし
アプリケーション	はい。	パフォーマンスデータやグラフはありません
仮想マシン	はい。	パフォーマンスデータやグラフはありません
ハイパーバイザー	はい。	パフォーマンスデータやグラフはありません
ホスト	はい。	パフォーマンスデータやグラフはありません

データストア	はい。	パフォーマンスデータやグラフはありません
VMDK です	はい。	パフォーマンスデータやグラフはありません
内部ボリューム	はい。	パフォーマンスデータやグラフはありません
ボリューム	はい。	パフォーマンスデータやグラフはありません
ストレージプール	はい。	パフォーマンスデータやグラフはありません
ディスク	はい。	パフォーマンスデータやグラフはありません
ストレージ	はい。	パフォーマンスデータやグラフはありません
ストレージノード	はい。	パフォーマンスデータやグラフはありません
ファブリック	はい。	パフォーマンスデータやグラフはありません
スイッチポート	はい。	パフォーマンスデータやグラフはありません。「Port Errors」には「N/A」と表示されます。
ストレージポート	はい。	はい。
NPVポート	はい。	パフォーマンスデータやグラフはありません
スイッチ	はい。	パフォーマンスデータやグラフはありません
NPVスイッチ	はい。	パフォーマンスデータやグラフはありません
qtree	はい。	パフォーマンスデータやグラフはありません

クォータ	はい。	パフォーマンスデータやグラフはありません
パス	はい。	パフォーマンスデータやグラフはありません
ゾーン	はい。	パフォーマンスデータやグラフはありません
ゾーンメンバー	はい。	パフォーマンスデータやグラフはありません
汎用デバイス	はい。	パフォーマンスデータやグラフはありません
テープ	はい。	パフォーマンスデータやグラフはありません
マスキング	はい。	パフォーマンスデータやグラフはありません
iSCSIセッション	はい。	パフォーマンスデータやグラフはありません
ICSIネットワークポータル	はい。	パフォーマンスデータやグラフはありません
検索	はい。	はい。
管理	はい。	はい。
ダッシュボード	はい。	はい。
ウィジェット	はい。	一部使用可（アセット、クエリ、管理の各ウィジェットのみ使用可能）
違反ダッシュボード	はい。	非表示
アセットダッシュボード	はい。	一部使用可（ストレージIOPSとVM IOPSのウィジェットは非表示）
パフォーマンスポリシーの管理	はい。	非表示

アノテーションを管理します	はい。	はい。
アノテーションルールを管理します	はい。	はい。
アプリケーションを管理します	はい。	はい。
クエリ	はい。	はい。
ビジネスエンティティの管理	はい。	はい。

フィーチャー（Feature ）	ユーザ- Performライセンスあり	ゲスト- Performライセンスあり	ユーザ- Performライセンスなし	ゲスト- Performライセンスなし
アセットダッシュボード	はい。	はい。	一部使用可（ストレージIOPSとVM IOPSのウィジェットは非表示）	一部使用可（ストレージIOPSとVM IOPSのウィジェットは非表示）
カスタムダッシュボード	表示のみ（作成、編集、保存のオプションはありません）	表示のみ（作成、編集、保存のオプションはありません）	表示のみ（作成、編集、保存のオプションはありません）	表示のみ（作成、編集、保存のオプションはありません）
パフォーマンスポリシーの管理	はい。	非表示	非表示	非表示
アノテーションを管理します	はい。	非表示	はい。	非表示
アプリケーションを管理します	はい。	非表示	はい。	非表示
ビジネスエンティティの管理	はい。	非表示	はい。	非表示
クエリ	はい。	表示と編集のみ（保存オプションなし）	はい。	表示と編集のみ（保存オプションなし）

ユーザアカウントの設定と管理

ユーザアカウント、ユーザ認証、およびユーザ許可は、Microsoft Active Directory（バージョン2または3）LDAP（Lightweight Directory Access Protocol）サーバ、または内部OnCommand Insight ユーザデータベースのいずれかの方法で定義および管理できます。ユーザごとに異なるユーザアカウントを設定することで、アクセス権、個 々 の設定、およびアカウンタビリティを制御できます。この操作には、管理者権限を持つアカ

ウントを使用してください。

作業を開始する前に

次の作業を完了しておきます。

- OnCommand Insight ライセンスをインストールします。
- 各ユーザに一意のユーザ名を割り当てます。
- 使用するパスワードを決定します。
- 正しいユーザロールを割り当てます。

LDAP証明書をインポートする際に、を使用して_server.keystore_and/or_server.trustore_passwordsを変更した場合は"securityadmin"、SANscreen証明書をインポートする前に_ldap_serviceを再起動してください。

セキュリティのベストプラクティスでは、管理者がホストオペレーティングシステムを設定して、管理者以外のユーザや標準ユーザが対話的にログインできないようにすることを推奨しています。

手順

1. ブラウザでInsightを開きます。
2. Insightのツールバーで、*[Admin]*をクリックします。
3. [設定]*をクリックします。
4. [ユーザー]タブを選択します。
5. 新しいユーザを作成するには、**[Actions]***ボタンをクリックし、[Add user]*を選択します。

   [名前]、[パスワード]、[電子メール]のいずれかのアドレスを入力し、[管理者]、[ユーザ]、[ゲスト]のいずれかのユーザを選択します。

6. ユーザーの情報を変更するには、リストからユーザーを選択し、ユーザー概要 の右側にある*ユーザーアカウントの編集*記号をクリックします。
7. OnCommand Insight システムからユーザを削除するには、リストからユーザを選択し、ユーザ概要 の右側にある*[ユーザアカウントの削除]*をクリックします。

結果

ユーザがOnCommand Insight にログインすると、LDAPが有効になっている場合、サーバは最初にLDAPによる認証を試みます。ユーザがLDAPサーバで見つからない場合、OnCommand Insight はローカルのInsightデータベースで検索します。

Insightのユーザロール

各ユーザアカウントには、3つの可能な権限レベルのいずれかが割り当てられます。

- Guestを使用すると、Insightにログインしてさまざまなページを表示できます。

- ユーザはゲストレベルのすべての権限に加え、ポリシーの定義や汎用デバイスの識別など、Insightの処理へのアクセスを許可します。Userアカウントタイプでは、データソースの処理を実行したり、自分以外のユーザアカウントを追加または編集したりすることはできません。
- 管理者は、新しいユーザの追加やデータソースの管理など、あらゆる処理を実行できます。

*ベストプラクティス：*管理者権限を持つユーザーの数を制限するには、ユーザーまたはゲストのほとんどのアカウントを作成します。

LDAP用の**Insight**の設定

OnCommand Insight は、Lightweight Directory Access Protocol（LDAP）設定を使用して、社内のLDAPドメインで設定する必要があります。

LDAPまたはSecure LDAP（LDAPS）で使用するようにInsightを設定する前に、社内環境でのActive Directoryの設定をメモしておいてください。Insightの設定は、組織のLDAPドメイン設定と一致している必要があります。InsightをLDAPで使用するように設定する前に、以下の概念を確認し、LDAPドメイン管理者に問い合わせて、環境で使用する適切な属性を確認してください。

すべてのSecure Active Directory（LDAPS）ユーザに対して、ADサーバ名は証明書で定義されているとおりに正確に使用する必要があります。セキュアADログインにIPアドレスを使用することはできません。

を使用して_server.keystore_and/or_server.trustore_passwordsを変更した場合は"securityadmin"、SANscreen証明書をインポートする前に_ldap_serviceを再起動してください。

OnCommand Insight は、Microsoft Active DirectoryサーバまたはAzure AD経由でLDAPとLDAPSをサポートしています。その他のLDAP実装でも動作する可能性がありますが、Insightでは確認されていません。これらのマニュアルの手順は、Microsoft Active Directoryバージョン2または3 LDAP（Lightweight Directory Access Protocol）を使用していることを前提としています。

ユーザープリンシパル名属性：

Insightでは、LDAPのUser PrincipalName属性（userPrincipalName）をユーザ名属性として使用します。ユーザープリンシパル名は、Active Directory(AD)フォレスト内でグローバルに一意であることが保証されていますが、多くの大規模な組織では、ユーザーのプリンシパル名がすぐにはわかりません。組織では、プライマリユーザー名に[ユーザープリンシパル名]属性の代わりに使用することがあります。

次に'ユーザープリンシパル名属性フィールドの代替値を示します

- * sAMAccountName *

  このユーザー属性は、Windows 2000 NT以前のレガシーユーザー名です。これは、ほとんどのユーザーが個人用Windowsマシンにログインするのに慣れているものです。これは、ADフォレスト全体でグローバルに一意であることが保証されていません。

  sAMAccountNameは'ユーザープリンシパル名属性では大文字と小文字が区別されます

- メール

  MS Exchangeを使用するAD環境では、この属性はエンドユーザーのプライマリ電子メールアドレスで

す。これは、userPrincipalName属性とは異なり、ADフォレスト全体でグローバルに一意である必要があります（エンドユーザーにも馴染みがあります）。メール属性は、MS Exchange以外のほとんどの環境には存在しません。

- 紹介

  LDAPリファーラルは、要求されたオブジェクト（より正確には、 オブジェクトが存在するディレクトリツリーのセクションを保持せず、オブジェクトを保持する可能性が高い場所をクライアントに与えます。次に、クライアントはこのリファーラルをドメインコントローラのDNS検索のベースとして使用します。理想的には、リファーラルは常にオブジェクトを保持するドメインコントローラを参照する。ただし、参照先ドメインコントローラが別のリファーラルを生成することは可能ですが、通常はオブジェクトが存在しないことを検出してクライアントに通知するのに時間はかかりません。

通常、ユーザプリンシパル名よりもsAMAccountNameが推奨されます。sAMAccountNameは、ドメイン内で一意です（ただし、ドメインフォレスト内で一意ではない場合もあります）が、通常、ログインに使用するドメインユーザの文字列です（例：*NetApp\username*）。識別名はフォレスト内で一意の名前ですが、通常はユーザによって認識されません。

同じドメインのWindowsシステム部分では、いつでもコマンドプロンプトを開き、setと入力して適切なドメイン名(USERDOMAIN=)を検索できます。OCIログイン名はになります `USERDOMAIN\sAMAccountName`。

ドメイン名* mydomain.x.y.z.com *には、を使用します `DC=x,DC=y,DC=z,DC=com` をクリックします。

- ポート * ：

LDAPのデフォルトポートは389、LDAPSのデフォルトポートは636です

LDAPSの一般的なURL： `ldaps://<ldap_server_host_name>:636`

ログは次の場所にあります。`\\<install directory>\SANscreen\wildfly\standalone\log\ldap.log`

デフォルトでは、次のフィールドに値が表示されます。Active Directory環境でこれらの変更が発生した場合は、InsightのLDAP設定で変更してください。

ロール属性
所属グループ
Mail属性
メール
Distinguished Name属性
distinguishedName

リファーラル
ついて来い

グループ：

OnCommand Insight サーバとDWHサーバで異なるアクセスロールを持つユーザを認証するには、Active Directoryでグループを作成し、OnCommand Insight サーバとDWHサーバでそれらのグループ名を入力する必要があります。以下のグループ名は一例です。InsightでLDAP用に設定する名前は、Active Directory環境用に設定した名前と一致している必要があります。

Insight Groupの略	例
Insight Server管理者グループ	insight.server.admins
Insight管理者グループ	insight.admins
Insightユーザグループ	insight.users
Insightゲストグループ	インサイトゲスト
Reporting Administrator Groupの略	insight.report.admins
Reporting Pro Authorsグループ	insight.report.proauthors
レポート作成者グループ	insight.report.business.authors
レポートコンシューマグループ	洞察力レポートビジネス消費者
レポート受信者グループ	インサイトレポート受信者

LDAPを使用したユーザ定義の設定

LDAPサーバからのユーザ認証と許可にOnCommand Insight （OCI）を設定するには、LDAPサーバでOnCommand Insight サーバ管理者として定義されている必要があります。

作業を開始する前に

LDAPドメインでInsight用に設定されているユーザとグループの属性を確認しておく必要があります。

すべてのSecure Active Directory（LDAPS）ユーザに対して、ADサーバ名は証明書で定義されているとおりに正確に使用する必要があります。セキュアADログインにIPアドレスを使用することはできません。

を使用して_server.keystore_and/or_server.trustore_passwordsを変更した場合は"securityadmin"、SANscreen証明書をインポートする前に_ldap_serviceを再起動してください。

このタスクについて

OnCommand Insight は、Microsoft Active Directoryサーバを介したLDAPとLDAPSをサポートしています。その他のLDAP実装でも動作する可能性がありますが、Insightでは確認されていません。この手順 は、Microsoft Active Directoryバージョン2または3のLDAP（Lightweight Directory Access Protocol）を使用していることを前提としています。

LDAPユーザは、ローカルで定義されたユーザとともに* Admin *>メニューのSetup [Users]リストに表示されます。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [設定]*をクリックします。
3. [ユーザー]タブをクリックします。
4. [LDAP]セクションまでスクロールします。
5. [LDAPを有効にする]*をクリックして、LDAPユーザの認証と許可を許可します。
6. 次のフィールドに入力します。

   ◦ `LDAP servers`：Insightでは、LDAP URLをカンマで区切ったリストを使用できます。LDAPプロトコルを検証せずに、指定されたURLに接続しようとします。

   LDAP証明書をインポートするには、*[証明書]*をクリックし、証明書ファイルを自動的にインポートするか、手動で検索します。

   LDAPサーバの識別に使用するIPアドレスまたはDNS名は、通常次の形式で入力します。

   ```
   ldap://<ldap-server-address>:port
   ```

   または、デフォルトのポートを使用している場合：

   ```
   ldap://<ldap-server-address>
   ```

   + このフィールドに複数のLDAPサーバを入力する場合は、各エントリで正しいポート番号が使用されていることを確認してください。

   ◦ `User name`：LDAPサーバでディレクトリ検索クエリを許可されたユーザのクレデンシャルを入力します。

   ◦ `Password`：上記のユーザのパスワードを入力します。LDAPサーバでこのパスワードを確認するには、*[検証]*をクリックします。

7. このLDAPユーザをより正確に定義する場合は、*[詳細を表示]*をクリックし、表示された属性のフィールドに入力します。

   これらの設定は、LDAPドメインで設定されている属性と一致する必要があります。これらのフィールドに入力する値が不明な場合は、Active Directory管理者に確認してください。

   - 管理者グループ

     Insight管理者の権限を持つユーザのLDAPグループ。デフォルトはです `insight.admins`。

   - ユーザーグループ

     Insightユーザの権限を持つユーザのLDAPグループ。デフォルトはです `insight.users`。

   - ゲストグループ

     Insight Guest権限を持つユーザのLDAPグループ。デフォルトはです `insight.guests`。

   - サーバー管理者グループ

     Insight Server管理者権限を持つユーザーのLDAPグループ。デフォルトはです `insight.server.admins`。

   - タイムアウト

     タイムアウトするまでにLDAPサーバからの応答を待機する時間（ミリ秒）。デフォルトは2、000です。これはすべてのケースで適切なため、変更しないでください。

   - ドメイン

     OnCommand Insight がLDAPユーザの検索を開始するLDAPノード。通常、これは組織のトップレベルドメインです。例：

     ```
     DC=<enterprise>,DC=com
     ```

   - ユーザープリンシパル名属性

     LDAPサーバ内の各ユーザを識別する属性。デフォルトはです `userPrincipalName`世界的にユニークなものですOnCommand Insight は、この属性の内容を上記で指定したユーザ名と照合しようとします。

   - ロール属性

     指定したグループ内でのユーザの適合性を識別するLDAP属性。デフォルトはです `memberOf`。

   - メール属性

     ユーザのEメールアドレスを識別するLDAP属性。デフォルトはです `mail`。これは、OnCommand Insight から利用可能なレポートをサブスクライブする場合に便利です。Insightでは、各ユーザが初めてログインしたときにユーザのEメールアドレスが取得され、それ以降は検索されません。

LDAPサーバでユーザのEメールアドレスが変更された場合は、Insightでそのアドレスを更新してください。

- 識別名属性

  ユーザの識別名を識別するLDAP属性。デフォルトはです `distinguishedName`。

8. [保存（ Save ）] をクリックします。

ユーザパスワードの変更

管理者権限を持つユーザは、ローカルサーバで定義されている任意のOnCommand Insight ユーザアカウントのパスワードを変更できます。

作業を開始する前に

次の項目を完了しておく必要があります。

- 変更するユーザアカウントにログインしたユーザへの通知。
- この変更後に使用する新しいパスワード。

このタスクについて

この方法を使用する場合、LDAPで検証されるユーザのパスワードは変更できません。

手順

1. 管理者権限でログインします。
2. Insightのツールバーで、*[Admin]*をクリックします。
3. [設定]*をクリックします。
4. [ユーザー]タブをクリックします。
5. 変更するユーザアカウントが表示されている行を探します。
6. ユーザー情報の右側にある*[ユーザーアカウントの編集]*をクリックします。
7. 新しい*パスワード*を入力し、確認フィールドにもう一度入力します。
8. [保存（ Save ）] をクリックします。

ユーザー定義の編集

管理者権限を持つユーザは、ユーザアカウントを編集して、OnCommand Insight またはDWHおよびレポート機能用のEメールアドレスやロールを変更できます。

作業を開始する前に

変更が必要なユーザアカウントのタイプ（OnCommand Insight 、DWH、またはその組み合わせ）を決定します。

このタスクについて

LDAPユーザについては、この方法でのみEメールアドレスを変更できます。

手順

1. 管理者権限でログインします。
2. Insightのツールバーで、*[Admin]*をクリックします。
3. [設定]*をクリックします。
4. [ユーザー]タブをクリックします。
5. 変更するユーザアカウントが表示されている行を探します。
6. ユーザ情報の右側にある*[ユーザアカウントの編集]*アイコンをクリックします。
7. 必要な変更を行います。
8. [保存（ Save ）] をクリックします。

ユーザアカウントの削除

管理者権限を持つユーザは、ユーザアカウントが使用されなくなった場合（ローカルユーザ定義の場合）、または次回ユーザがログインしたとき（LDAPユーザの場合）にOnCommand Insight にユーザ情報の再検出を強制する場合（LDAPユーザの場合）に、ユーザアカウントを削除できます。

手順

1. 管理者権限でOnCommand Insight にログインします。
2. Insightのツールバーで、*[Admin]*をクリックします。
3. [設定]*をクリックします。
4. [ユーザー]タブをクリックします。
5. 削除するユーザアカウントが表示されている行を探します。
6. ユーザー情報の右側にある*ユーザーアカウントの削除*"* x *"アイコンをクリックします。
7. [保存（ Save ）] をクリックします。

ログイン警告メッセージの設定

OnCommand Insight を使用すると、管理者はユーザーのログイン時に表示されるカスタムテキストメッセージを設定できます。

手順

1. OnCommand Insight サーバでメッセージを設定するには、次の手順を実行します。
   a. メニュー[Admin][Troubleshooting]>[Advanced Troubleshooting]>[Advanced Settings]に移動します
   b. テキスト領域にログインメッセージを入力します。

c. [Client displays login warning message]*チェックボックスをクリックします。

d. [保存（ Save ）] をクリックします。

このメッセージは、すべてのユーザのログイン時に表示されます。

2. Data Warehouse（DWH）およびReporting（Cognos）でメッセージを設定するには、次の手順を実行します。

a. に移動し、[ログイン警告]*タブをクリックします。

b. テキスト領域にログインメッセージを入力します。

c. [保存（ Save ）] をクリックします。

このメッセージは、DWHおよびCognos Reportingにすべてのユーザがログインすると表示されます。

securityadminツール

OnCommand Insightには、Insight環境を高度なセキュリティで運用できる機能が用意されています。これらの機能には、暗号化、パスワードハッシュ、およびパスワードを暗号化および復号化する内部ユーザパスワードとキーペアを変更する機能が含まれます。これらの機能は、* SecurityAdmin Tool *を使用して、Insight環境内のすべてのサーバで管理できます。

SecurityAdminツールとは

セキュリティ管理ツールでは、ボルトの内容を変更したり、OnCommand Insightのインストール環境を調整したりすることができます。

SecurityAdminツールの主な用途は、セキュリティ設定（ボルトなど）およびパスワードの*バックアップ*および*リストア*です。たとえば、Local Acquisition Unitにバックアップを作成してRemote Acquisition Unitにリストアすることで、環境全体でパスワードの調整が可能になります。また、環境内に複数のOnCommand Insight Serverがある場合は、サーバーボルトのバックアップを作成し、パスワードを同じにするために他のサーバーに復元することもできます。これらは、SecurityAdminを使用して環境内で一貫性を確保する方法のほんの2つの例です。

OnCommand Insightデータベースをバックアップする場合は、必ず*ボルト*をバックアップすることを強くお勧めします。これを行わないと、アクセスが失われる可能性があります。

このツールには、*インタラクティブ*モードと*コマンドライン*モードの両方が用意されています。

SecurityAdmin Toolの多くの操作では、ボルトの内容が変更され、インストールも変更されます。これにより、ボルトとインストールの同期が維持されます。

例えば、

- ユーザのパスワードを変更すると、SANscreen .Usersテーブル内のユーザのエントリが新しいハッシュで更新されます。
- MySQLユーザーのパスワードを変更すると、適切なSQLステートメントが実行され、MySQLインスタンスのユーザーのパスワードが更新されます。

状況によっては、インストールに複数の変更が加えられることがあります。

- DWH MySQLユーザを変更すると、MySQLデータベースのパスワードが更新されるだけでなく、ODBCの複数のレジストリエントリも更新されます。

以降のセクションでは、これらの変更を「調整された変更」という用語で説明します。

実行モード

- 通常/デフォルト動作- SANscreenサーバサービスが実行されている必要があります

  デフォルトの実行モードでは、SecurityAdminツールは* SANscreenサーバーサービス*を実行している必要があります。サーバは認証に使用され、サーバを呼び出すことで、インストールに対する多くの調整された変更が行われます。

- 直接操作- SANscreenサーバサービスが実行中または停止している可能性があります。

  OCIサーバまたはDWHのインストール環境でツールを実行する場合は、「直接」モードでも実行できます。このモードでは、データベースを使用して認証と調整された変更が実行されます。Serverサービスは使用されません。

  動作は通常モードと同じですが、次の例外があります。

- ドメイン管理者以外のユーザに対してのみ認証がサポートされます。（パスワードとロールがLDAPではなくデータベースに存在するユーザ）。
- 「キーの置換」操作はサポートされていません。
- バックアップリストアの再暗号化手順はスキップされます。
- リカバリモードこのツールは、サーバーとデータベースの両方にアクセスできない場合でも実行できます（例えば、ボルト内のルートパスワードが正しくないため）。

  このモードで実行すると、認証ができないため、インストールに対して調整された変更を伴う操作は実行できません。

  リカバリモードは、次の目的で使用できます。

- どのボールトエントリが間違っているかを判断する（検証操作を使用）
- 間違ったrootパスワードを正しい値に置き換えます。（パスワードは変更されません。ユーザは現在のパスワードを入力する必要があります）。

> ボルト内のルートパスワードが正しくなく、パスワードが不明で、正しいルートパスワードを持つボルトのバックアップが存在しない場合、SecurityAdmin Toolを使用してインストールを復元することはできません。インストールを回復する唯一の方法は、に記載されている手順に従ってMySQLインスタンスのパスワードをリセットすることです https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html。リセット手順を実行した後、correct-stored-password操作を使用して新しいパスワードをボルトに入力します。

コマンド

制限されていないコマンド

無制限のコマンドは、インストールに対して調整された変更を行います（信頼ストアを除く）。制限のないコマンドは、ユーザ認証なしで実行できます。

コマンド	説明
バックアップ-ヴォールト	ボルトを含むzipファイルを作成します。ボールトファイルへの相対パスは、インストールルートを基準としたボールトパスと一致します。 • wildfly/standalone/configuration/vault/* • acq/conf/vault/* OnCommand Insightデータベースをバックアップする場合は、必ずヴォールトをバックアップすることを強く推奨します。
check-for-default-keys	ボルトのキーが7.3.16より前のインスタンスで使用されていたデフォルトボルトのキーと一致するかどうかを確認します。
correct-stored-password	ボルトに保存されている（正しくない）パスワードを、ユーザーが知っている正しいパスワードに置き換えます。 これは、ボルトとインストールが一貫していない場合に使用できます。インストール時に実際のパスワードが変更されることはありません。
	change-trust-store-password信頼ストアに使用するパスワードを変更し、新しいパスワードをボルトに保存します。信頼ストアの現在のパスワードは「既知」である必要があります。
verify-keystore	ボルトの値が正しいかどうかを確認します。 • OCIユーザの場合、パスワードのハッシュがデータベース内の値と一致しているか • MySQLユーザの場合、データベースに接続できますか • キーストアの場合、キーストアをロードし、キー（存在する場合）を読み取ることができますか？
リストキー	ボルト内のエントリを一覧表示します（保存されている値は表示されません）。

制限されたコマンド

インストールに対して調整された変更を行う非表示のコマンドでは、認証が必要です。

コマンド	説明

restore-vault-backup	現在のボルトを、指定したボルトバックアップファイルに含まれているボルトで置き換えます。 すべての連携アクションを実行して、リストアされたボルトのパスワードと一致するようにインストールを更新します。 • OCI通信ユーザのパスワードを更新する • MySQLユーザのパスワード（rootを含む）を更新する • キーストアごとに、キーストアのパスワードが「既知」の場合は、復元されたボルトのパスワードを使用してキーストアを更新します。 通常モードで実行すると、はインスタンスから各暗号化された値を読み取り、現在のボールトの暗号化サービスを使用して復号化し、復元されたボールトの暗号化サービスを使用して再暗号化し、再暗号化された値を保存します。
synchronize-with-vault	すべての連携アクションを実行して、リストアされたボルトのユーザーパスワードと一致するようにインストールを更新します。 • OCI通信ユーザのパスワードを更新します。 • MySQLユーザのパスワード（rootを含む）を更新します。
パスワードの変更	ボルトのパスワードを変更し、調整された操作を実行します。
キーの置換	新しい空のボールト（既存のボールトとは異なるキーを持つ）を作成します。次に、現在のボルトから新しいボルトにエントリをコピーします。次に、インスタンスから各暗号化された値を読み取り、現在のボールトの暗号化サービスを使用して復号化し、復元されたボールトの暗号化サービスを使用して再暗号化し、再暗号化された値を保存します。

連携されたアクション

サーバーボールト

_internal	データベースのユーザのパスワードハッシュの更新
取得	データベースのユーザのパスワードハッシュの更新 取得ボールトが存在する場合は、取得ボールトのエントリも更新します。
dwh_internalの略	データベースのユーザのパスワードハッシュの更新
cognos_adminをクリックします	データベースのユーザのパスワードハッシュの更新 DWHおよびWindowsの場合は、SANscreen /cognos/analytics/configuration/SANscreenAP.propertiesを更新して、cognos.adminプロパティをパスワードに設定します。

ルート	SQLを実行してMySQLインスタンスのユーザパスワードを更新
在庫	SQLを実行してMySQLインスタンスのユーザパスワードを更新
DWH	SQLを実行してMySQLインスタンスのユーザパスワードを更新 DWHおよびWindowsの場合は、Windowsレジストリを更新して、次のODBC関連エントリを新しいパスワードに設定します。 • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\DWH_CAPACITY\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\DWH_CAPACITY_Efficiency\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\odbc\odbc.ini\dwh_fs_util\pwd • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\odbc\odbc.ini\dwh_inventory\pwd • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\DWH_PERFORMANCE\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\DWH_PORTS\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\odbc\odbc.ini\dwh_sa\pwd • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\odbc\odbc.ini\dwh_cloud_cost\pwd
誰だ	SQLを実行してMySQLインスタンスのユーザパスワードを更新
ホスト	SQLを実行してMySQLインスタンスのユーザパスワードを更新
キーストアパスワード	キーストアを新しいパスワード-wildfly/standalone/configuration/server.keystoreで書き換えます。
信頼ストアのパスワード	キーストアを新しいパスワード-wildfly/standalone/configuration/server.trustoreで書き換えます。
キーパスワード	キーストアを新しいパスワード-wildfly/standalone/configuration/sso.jksで書き換えます。

cognos_archive	なし

Acquisition Vault

取得	なし
信頼ストアのパスワード	キーストアを新しいパスワード（存在する場合）で書き換えます。 -acq/conf/cert/client.keystore

Security Adminツールの実行**-**コマンドライン

コマンドラインモードでSAツールを実行する構文は次のとおりです。

```
securityadmin [-s | -au] [-db] [-lu <user> [-lp <password>]] <additional-
options>

where

-s                      selects server vault
-au                     selects acquisition vault

-db                     selects direct operation mode

-lu <user>              user for authentication
-lp <password>          password for authentication
<addition-options>      specifies command and command arguments as
described below
```

注：

- コマンドラインに「-i」オプションがない場合があります（対話モードが選択されるため）。
- 「-s」および「-au」オプションの場合：
  - 「-s」はRAUでは使用できません
  - DWHでは「-au」は使用できません
  - どちらも存在しない場合は、
    - サーバーボルトは、サーバー（Server）、DWH、およびデュアル（Dual）で選択されています。
    - RAUで収集ボールトが選択されている
- ユーザ認証には-luオプションと-lpオプションを使用します。
  - <user>が指定され、<password>が指定されていない場合は、ユーザにパスワードの入力を求められます。
  - <user>を指定せず、認証が必要な場合は、<user>と<password>の両方の入力を求められます。

『コマンド・

コマンド	使用法
correct-stored-password	`securityadmin [-s`

-au] [-db] -pt <key> [<value>]
 	
`where`
 	
-pt specifies the command ("put") <key> is the key <value> is the value. If not present, user will be prompted for value
 	
` `
	バックアップ-ヴォールト

`securityadmin [-s`	-au] [-db] -b [<backup-dir>] where -b specified command <backup-dir> is the output directory. If not present, default location of SANscreen/backup/vault is used The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip ` `
バックアップ-ヴォールト	`securityadmin [-s`
-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file ` `	リストキー

`securityadmin [-s`	-au] [-db] -l where -l specified command ``
チェックキー	`securityadmin [-s`
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys ``	verify-keystore（サーバ）

`securityadmin [-s] [-db] -v`
 	
`where`
 	
`-v specified command`
	アップグレード

`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -u where -u specified command For server vault, if -lu is not present, then authentication will be performed for <user> =_internal and <password> = _internal's password from vault. For acquisition vault, if -lu is not present, then no authentication will be attempted ``

キーの置換	`securityadmin [-s`
-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command ``	restore-vault-backup
`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file> where -r specified command <backup-file> the backup file location ``

change-password（サーバ）	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-un <user> entry ("user") name to update`
	`-p <password> new password. If <password not supplied, user will be prompted.`
	`-sh for mySQL user, use strong hash`

change - acquisitionユーザ（acquisition）のパスワード	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-p <password> new password. If <password not supplied, user will be prompted.`

change-password for truststore -_password （acquisition）	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -utp -p [<password>]`
	
	`where`
	
	`-utp specified command ("update-truststore-password")`
	`-p <password> new password. If <password not supplied, user will be prompted.`

synchronize-with-vault（サーバー）	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>`
	
	`where`
	
	`-sv specified command`

Security Admin Toolの実行-インタラクティブモード

インタラクティブ-メインメニュー

SAツールを対話型モードで実行するには、次のコマンドを入力します。

```
 securityadmin -i
```

サーバまたはデュアルインストールの場合は、`SecurityAdmin`によってサーバまたは`Local Acquisition Unit`のどちらかを選択するように求められます。

ServerおよびAcquisition Unitノードが検出されました。セキュリティを再設定する必要があるノードを選択します。

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

DWHでは、[Server]が自動的に選択されます。リモートAUでは、「Acquisition Unit」が自動的に選択されます。

Interactive Server：rootパスワードのリカバリ

サーバーモードでは、SecurityAdminツールは最初に保存されているルートパスワードが正しいことを確認します。そうでない場合、ツールはrootパスワードの回復画面を表示します。

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

オプション1を選択すると、正しいパスワードの入力を求められます。

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
```

正しいパスワードを入力すると、次のように表示されます。

```
 Password verified.  Vault updated
```

ENTERキーを押すと、サーバーの無制限メニューが表示されます。

間違ったパスワードを入力すると、次のメッセージが表示されます。

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
```

ENTERキーを押すと、リカバリメニューに戻ります。

オプション2を選択すると、正しいパスワードを読み取るバックアップファイルの名前の入力を求めるプロンプトが表示されます。

```
 Enter Backup File Location:
```

バックアップのパスワードが正しい場合は、次のように表示されます。

```
 Password verified.  Vault updated
```

ENTERキーを押すと、サーバーの無制限メニューが表示されます。

バックアップのパスワードが正しくない場合、次のメッセージが表示されます。

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
```
ENTERキーを押すと、リカバリメニューに戻ります。

Interactive-Server:正しいパスワード

「正しいパスワード」アクションは、ボルトに保存されているパスワードを変更し、インストールで必要とされる実際のパスワードと一致させるために使用されます。このコマンドは、securityadminツール以外によってインストールに変更が加えられた場合に便利です。たとえば、次のようなもの

- SQLユーザのパスワードがMySQLに直接アクセスして変更されました。
- キーストアが置き換えられたか、キーストアのパスワードがkeytoolを使用して変更されました。
- OCIデータベースがリストアされ、そのデータベースの内部ユーザ用に異なるパスワードが設定されている

「Correct Password」では、最初に正しい値を保存するパスワードを選択するように求められます。

```
Replace incorrect stored password with correct password.  (Does not change
the required password)
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

修正するエントリを選択すると、値の指定方法を求めるプロンプトが表示されます。

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

オプション1を選択すると、正しいパスワードの入力を求められます。

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
```

正しいパスワードを入力すると、次のように表示されます。

```
 Password verified.  Vault updated
```

ENTERキーを押すと、サーバーの無制限メニューに戻ります。

間違ったパスワードを入力すると、次のメッセージが表示されます。

```
Password verification failed - {additional information}
Vault entry not updated.
```

ENTERキーを押すと、サーバーの無制限メニューに戻ります。

オプション2を選択すると、正しいパスワードを読み取るバックアップファイルの名前の入力を求めるプロンプトが表示されます。

```
 Enter Backup File Location:
```

バックアップのパスワードが正しい場合は、次のように表示されます。

```
 Password verified.  Vault updated
```

ENTERキーを押すと、サーバーの無制限メニューが表示されます。

バックアップのパスワードが正しくない場合、次のメッセージが表示されます。

```
Password verification failed - {additional information}
Vault entry not updated.
```

ENTERキーを押すと、サーバーの無制限メニューが表示されます。

対話型サーバ：ボールトの内容の確認

ボルトの内容を確認（Verify Vault Contents）では、以前のバージョンのOCIで配布されたデフォルトのボルトと一致するキーがボルトにあるかどうかがチェックされ、ボルト内の各値がインストール環境と一致するかどうかがチェックされます。

各キーの結果は次のとおりです。

OK	ボルトの値が正しい

未チェック	この値はインストールに対してチェックできません
不良	値がインストール環境と一致しません
不明	想定されるエントリがありません。

```
Encryption keys secure: unique, non-default encryption keys detected

             cognos_admin: OK
                    hosts: OK
             dwh_internal: OK
                inventory: OK
                  dwhuser: OK
        keystore_password: OK
                      dwh: OK
      truststore_password: OK
                     root: OK
                _internal: OK
          cognos_internal: Not Checked
             key_password: OK
              acquisition: OK
           cognos_archive: Not Checked
 cognos_keystore_password: Missing


Press enter to continue
```

対話型サーバ：バックアップ

Backupは、バックアップzipファイルを保存するディレクトリの入力を求めます。ディレクトリがすでに存在している必要があり、ファイル名はServerSecurityBackup-yyyy-mm-dd-hh-mm.zipになります。

```
Enter backup directory location [C:\Program Files\SANscreen\backup\vault]
:

Backup Succeeded!   Backup File: C:\Program
Files\SANscreen\backup\vault\ServerSecurityBackup-2024-08-09-12-02.zip
```

対話型サーバ：ログイン

ログインアクションは、ユーザを認証し、インストールを変更する操作にアクセスするために使用されます。ユーザには管理Privilegesが必要です。サーバで実行する場合は、任意の管理者ユーザを使用できます。直接モードで実行する場合は、LDAPユーザではなくローカルユーザである必要があります。

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

または

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:
```

パスワードが正しく、ユーザが管理者ユーザである場合は、制限されたメニューが表示されます。

パスワードが正しくない場合は、次のメッセージが表示されます。

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:

Login Failed!
```

ユーザが管理者でない場合は、次のメッセージが表示されます。

```
Authenticating via server. Enter user and password

UserName: user

Password:

User 'user' does not have 'admin' role!
```

Interactive-Server:制限付きメニュー

ユーザーがログインすると、ツールに制限付きメニューが表示されます。

```
Logged in as: admin
Select Action:

2 - Change Password

3 - Verify Vault Contents

4 - Backup

5 - Restore

6 - Change Encryption Keys

7 - Fix installation to match vault

9 - Exit

Enter your choice:
```

Interactive-Server:パスワードの変更

「パスワードの変更」アクションは、インストールパスワードを新しい値に変更するために使用します。

[パスワードの変更]をクリックすると、最初に変更するパスワードを選択するように求められます。

```
Change Password
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

ユーザがMySQLユーザの場合、修正するエントリを選択すると、パスワードを強力にハッシュするかどうかを確認するメッセージが表示されます。

```
MySQL supports SHA-1 and SHA-256 password hashes. SHA-256 is stronger but
requires all clients use SSL connections

Use strong password hash? (Y/n): y
```

次に、新しいパスワードの入力を求められます。

```
New Password for '{user}':
If the password is empty, the operation is cancelled.

Password is empty - cancelling operation
```

空でないパスワードを入力すると、パスワードの確認を求めるプロンプトが表示されます。

```
New Password for '{user}':

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

変更に失敗すると、エラーまたは例外が表示されます。

対話型サーバ：リストア

Interactive Server：暗号化キーの変更

暗号化キーの変更アクションは、ボールトエントリの暗号化に使用される暗号化キーを置き換え、ボールトの暗号化サービスに使用される暗号化キーを置き換えます。暗号化サービスのキーが変更されるため、データベース内の暗号化された値は再暗号化されます。これらの値は、現在のキーで読み取られ、復号化され、新しいキーで暗号化され、データベースに保存されます。

サーバは一部のデータベースコンテンツに対して再暗号化処理を提供するため、ダイレクトモードではこのアクションはサポートされていません。

```
Replace encryption key with new key and update encrypted database values

Confirm (y/N): y

Change Encryption Keys succeeded! Restart 'Server' Service!
```

インタラクティブサーバー:インストールの修正

[インストールの修正]アクションを実行すると、インストールが更新されます。securityadminツールを使用して変更可能なすべてのインストールパスワード（rootを除く）は、ボルト内のパスワードに設定されます。

- OCIの内部ユーザのパスワードが更新されます。
- root以外のMySQLユーザのパスワードが更新されます。
- キーストアのパスワードが更新されます。

```
Fix installation - update installation passwords to match values in vault

Confirm:  (y/N): y

Installation update succeeded! Restart 'Server' Service.
```

最初の更新に失敗した時点でアクションが停止し、エラーまたは例外が表示されます。

Insight Serverでセキュリティを管理する

。 `securityadmin` ツールを使用すると、Insight Serverでセキュリティオプションを管理できます。セキュリティの管理には、パスワードの変更、新しいキーの生成、作成したセキュリティ設定の保存とリストア、デフォルト設定への設定のリストアが含まれます。

このタスクについて

を使用します `securityadmin` セキュリティ管理ツール：

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

詳細については、のドキュメントを参照してください"securityadmin"。

Local Acquisition Unit上のセキュリティの管理

。 `securityadmin` ツールを使用すると、Local Acquisition User（LAU；ローカル収集ユーザ）のセキュリティオプションを管理できます。セキュリティの管理には、キーとパスワードの管理、作成したセキュリティ設定の保存とリストア、またはデフォルト設定への設定のリストアが含まれます。

作業を開始する前に

が必要です `admin` セキュリティ設定タスクを実行するための権限。

このタスクについて

を使用します `securityadmin` セキュリティ管理ツール：

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

詳細については、手順を参照して"securityadminツール"ください。

RAUでのセキュリティの管理

。 `securityadmin` ツールを使用すると、RAUのセキュリティオプションを管理できま

す。場合によっては、ヴォールト設定のバックアップやリストア、暗号化キーの変更、Acquisition Unitのパスワードの更新が必要になることがあります。

このタスクについて

を使用します `securityadmin` セキュリティ管理ツール：

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

LAU / RAUのセキュリティ設定を更新する1つのシナリオは、サーバでそのユーザのパスワードが変更されたときに「acquisition」ユーザのパスワードを更新することです。LAUおよびすべてのRAUは、サーバとの通信にサーバ「acquisition」ユーザのパスワードと同じパスワードを使用します。

「acquisition」ユーザが存在するのはInsight Serverだけです。RAUまたはLAUは、サーバに接続するときにそのユーザとしてログインします。

詳細については、手順を参照して"securityadminツール"ください。

Data Warehouseでセキュリティを管理する

。 `securityadmin` ツールを使用すると、Data Warehouseサーバのセキュリティオプションを管理できます。セキュリティの管理には、DWHサーバで内部ユーザの内部パスワードを更新したり、セキュリティ設定のバックアップを作成したり、設定をデフォルトの設定にリストアしたりする作業があります。

このタスクについて

を使用します `securityadmin` セキュリティ管理ツール：

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

詳細については、のドキュメントを参照してください"securityadmin"。

OnCommand Insight の内部ユーザのパスワードを変更しています

セキュリティポリシーによっては、OnCommand Insight 環境でパスワードの変更が必要になる場合があります。1台のサーバのパスワードの一部は、環境内の別のサーバに存在するため、両方のサーバでパスワードを変更する必要があります。たとえば、Insight Serverでユーザのパスワード「inventory」を変更する場合は、そのInsight Server用に設定されたData Warehouse Server Connectorでユーザのパスワード「inventory」と一致している必要があります。

作業を開始する前に

パスワードを変更する前に、ユーザアカウントの依存関係を理解しておく必要があります。必要なすべてのサーバでパスワードを更新しないと、Insightコンポーネント間の通信に失敗します。

このタスクについて

次の表に、Insight Serverの内部ユーザパスワードと、依存するパスワードが新しいパスワードと一致する必要があるInsightコンポーネントを示します。

Insight Serverのパスワード	必要な変更
_internal	
取得	愛称はラオ
dwh_internalの略	Data Warehouse
ホスト	
在庫	Data Warehouse
ルート	

次の表に、Data Warehouseの内部ユーザパスワードと、依存するパスワードが新しいパスワードと一致する必要があるInsightコンポーネントを示します。

Data Warehouseのパスワード	必要な変更
cognos_adminをクリックします	
DWH	
dwh_internal（Server Connectorの設定UIを使用して変更）	Insightサーバ
誰だ	
ホスト	
インベントリ（Server Connector設定UIを使用して変更）	Insightサーバ
ルート	

- DWHサーバ接続設定UIでのパスワードの変更*

次の表に、LAUのユーザパスワードと、依存するパスワードが新しいパスワードと一致する必要があるInsightコンポーネントを示します。

LAUパスワード	必要な変更
取得	Insight Server、RAU

Server Connection Configuration UIを使用して「**inventory**」パスワードと「**dwh_internal**」パスワードを変更します

「inventory」または「dwh_internal」のパスワードをInsight Serverと同じパスワードに変更する必要がある場合は、Data Warehouse UIを使用します。

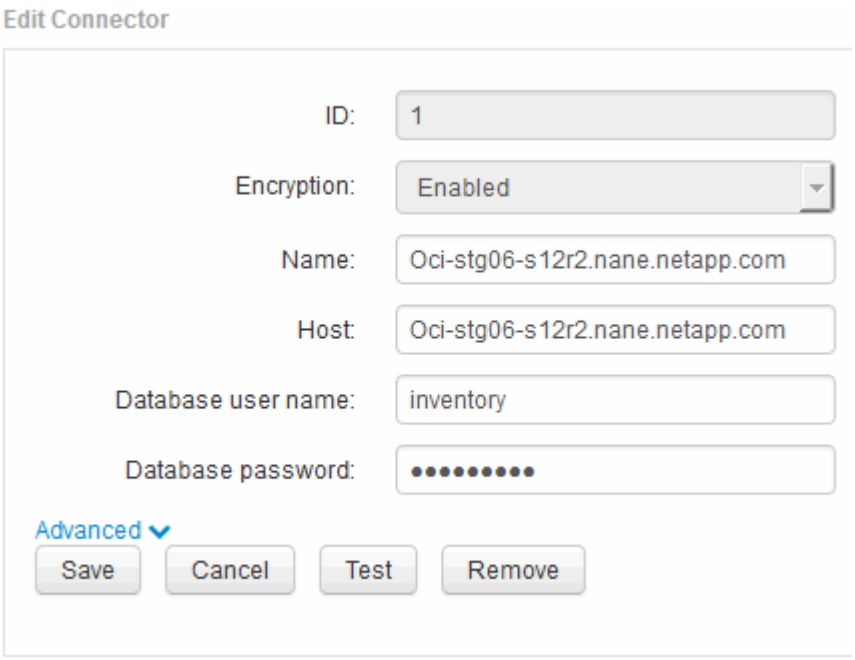
作業を開始する前に

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。

手順

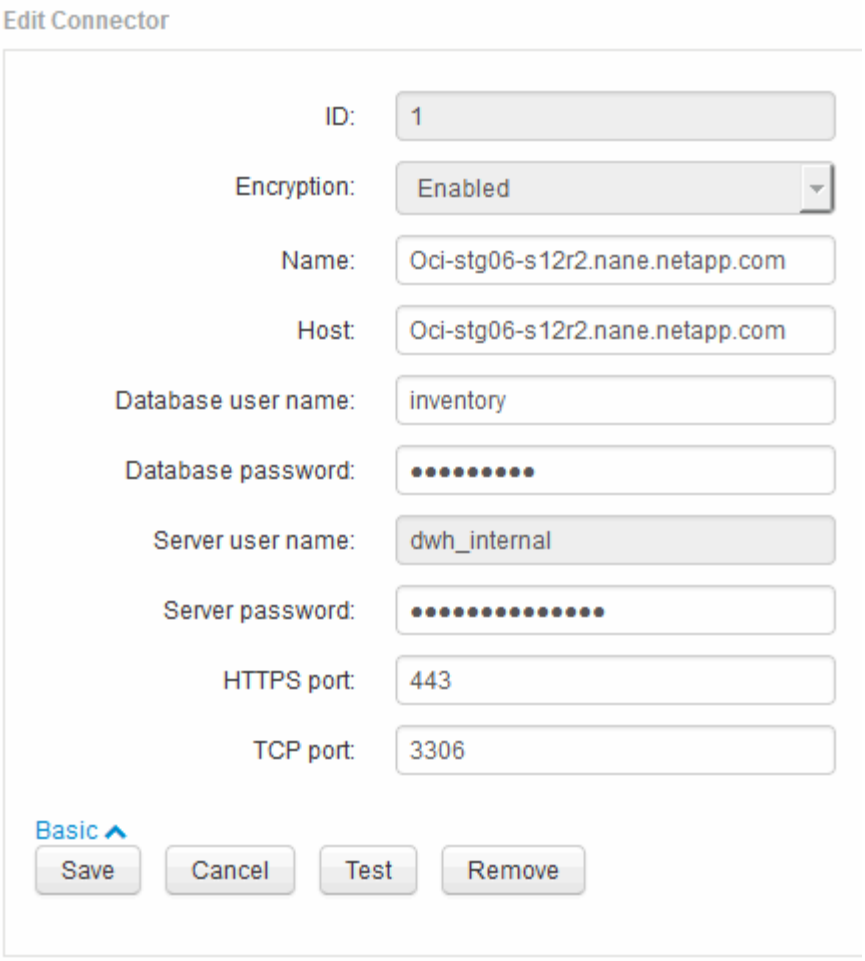
1. Data Warehouseポータルにログインします https://hostname/dwhhostnameは、OnCommand Insight Data Warehouseがインストールされているシステムの名前です。
2. 左側のナビゲーションペインで、*[コネクタ]*をクリックします。

   [Edit Connector]（コネクタの編集）*画面が表示されます。



3. 「* Database password *」フィールドに新しい「`inventory`」パスワードを入力します。
4. [保存（ Save ）] をクリックします。
5. 「`dwh_internal`」パスワードを変更するには、*[詳細設定]*をクリックします

   [Edit Connector Advanced]画面が表示されます。



6. 新しいパスワードを* Server password *フィールドに入力します。
7. [保存] をクリックします .

ODBC Administrationツールを使用した**DWH**パスワードの変更

Insight ServerでDWHユーザのパスワードをで変更した場合は、Data Warehouseサーバでもパスワードを変更する必要があります。ODBC Data Source Administratorツールを使用して、Data Warehouseのパスワードを変更します。

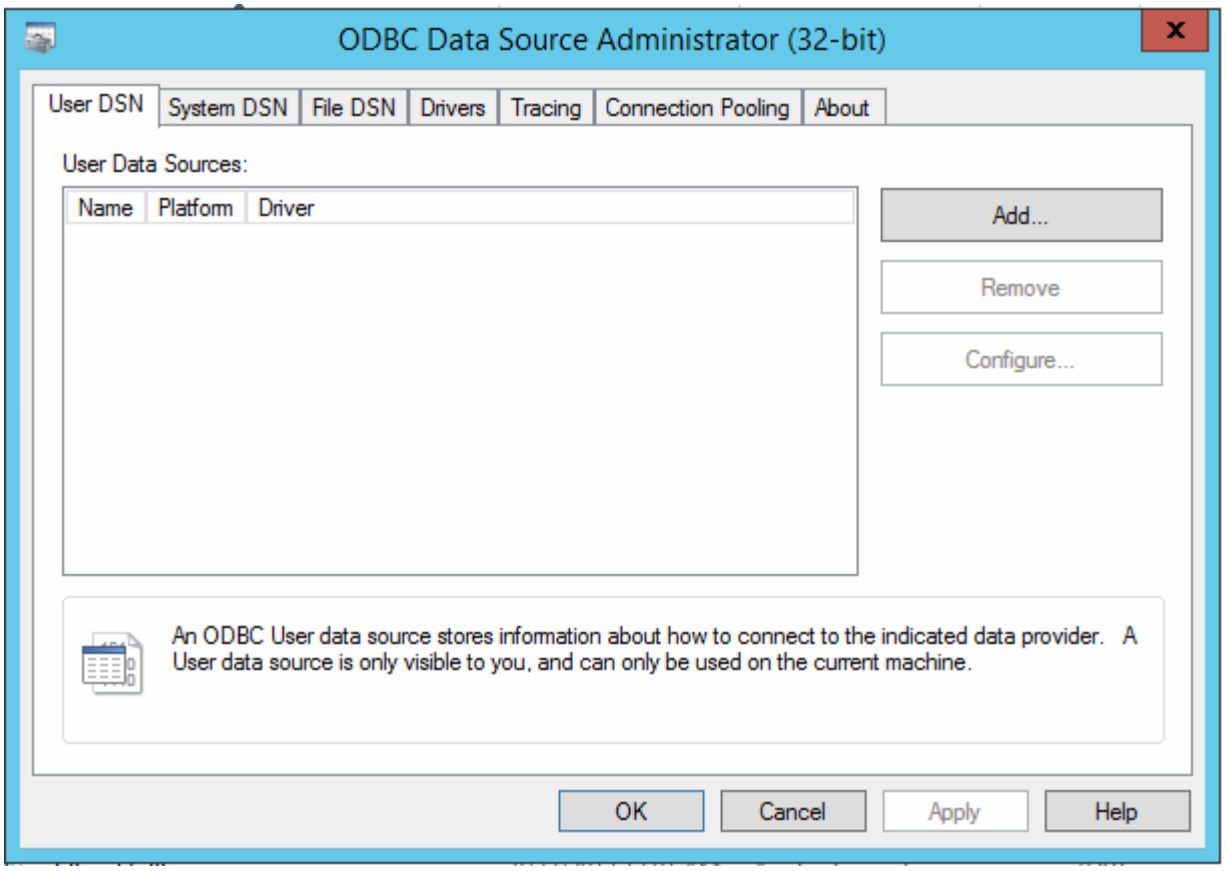
作業を開始する前に

管理者権限があるアカウントを使用してData Warehouseサーバへのリモートログインを実行する必要があります。

手順

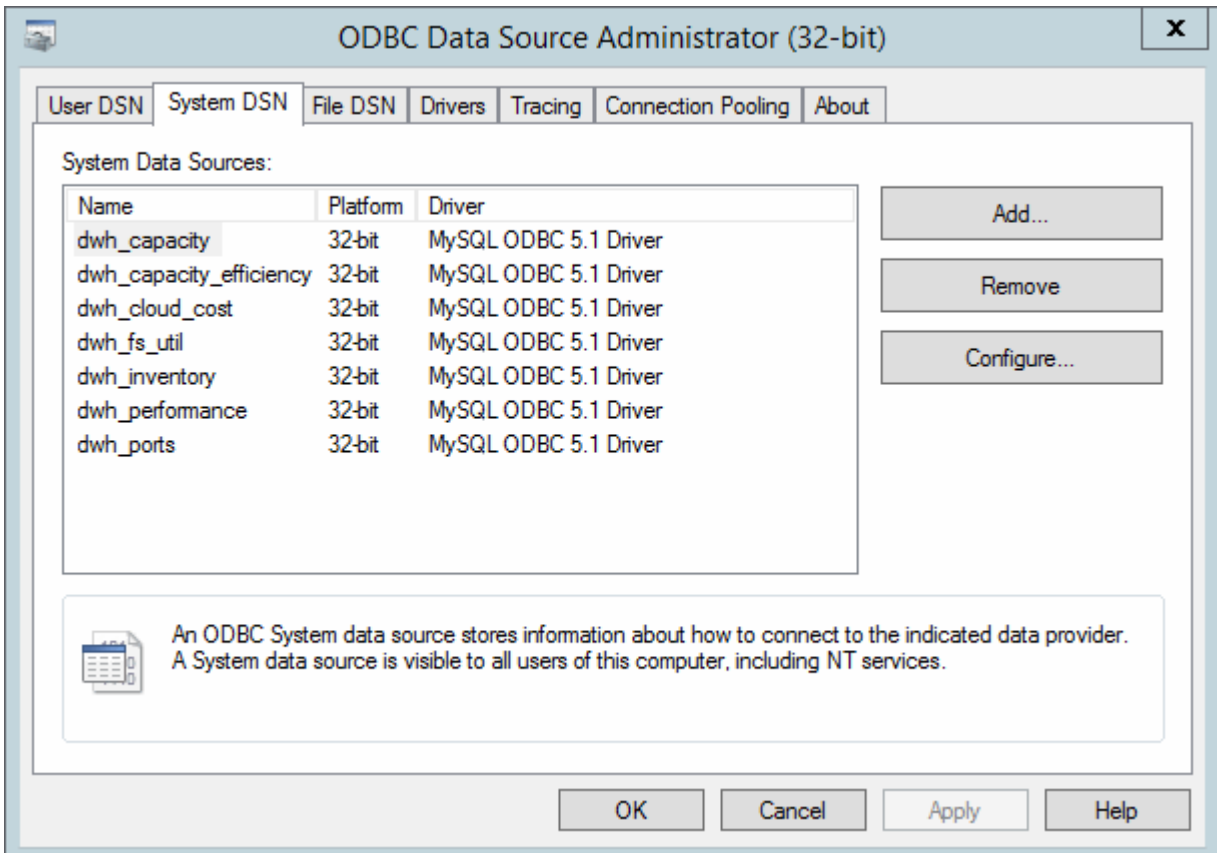
1. Data Warehouseをホストしているサーバへのリモートログインを実行します。
2. ODBC Administrationツールにアクセスします `C:\Windows\SysWOW64\odbcad32.exe`

   [ODBC Data Source Administrator]画面が表示されます。



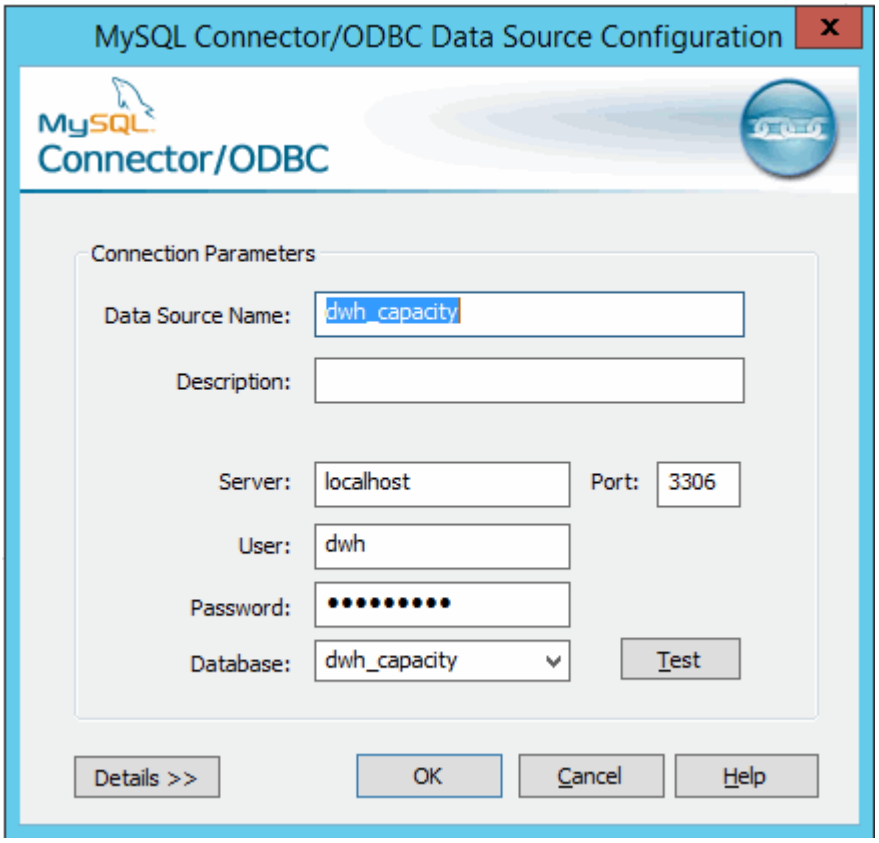
3. [システムDSN]*をクリックします

   システムデータソースが表示されます。



4. リストからOnCommand Insight データソースを選択します。
5. [設定]*をクリックします

   [Data Source Configuration]画面が表示されます。



6. [パスワード]*フィールドに新しいパスワードを入力します。

スマートカードおよび証明書によるログインのサポート

OnCommand Insight では、Insightサーバにログインするユーザの認証にスマートカード（CAC）と証明書を使用できます。これらの機能を有効にするには、システムを設定する必要があります。

CACと証明書をサポートするようにシステムを設定した後、OnCommand Insight の新しいセッションに移動すると、ブラウザにネイティブダイアログが表示され、選択する個人証明書のリストが表示されます。これらの証明書は、OnCommand Insight サーバによって信頼されたCAによって発行された個人証明書のセットに基づいてフィルタリングされます。ほとんどの場合、単一の選択があります。既定では、選択肢が1つしかない場合、Internet Explorerはこのダイアログをスキップします。

CACユーザの場合、スマートカードには複数の証明書が含まれており、信頼されたCAに一致できる証明書は1つだけです。のCAC証明書 `identification` を使用する必要があります。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "WindowsホストにインストールされているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

スマートカードおよび証明書によるログイン用にホストを設定しています

スマートカード（CAC）および証明書によるログインをサポートするには、OnCommand Insight ホストの設定を変更する必要があります。

作業を開始する前に

- システムでLDAPが有効になっている必要があります。
- LDAP `User principal account name` 属性は、ユーザのIDを含むLDAPフィールドと一致する必要があります。

を使用して_server.keystore_and/or_server.trustore_passwordsを変更した場合は"securityadmin"、SANscreen証明書をインポートする前に_ldap_serviceを再起動してください。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "WindowsホストにインストールされているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

手順

1. を使用します `regedit` でレジストリ値を変更するユーティリティ

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java：

a. jvm_optionを変更します DclientAuth=false 終了： DclientAuth=true.

2. キーストアファイルをバックアップします。 C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore
3. コマンドプロンプトを開き、を指定します Run as administrator
4. 自己生成証明書を削除します。 C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore
5. 新しい証明書を生成します。 C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"
6. 証明書署名要求（CSR）を生成します。 C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"
7. 手順6でCSRが返されたら、証明書をインポートし、Base-64形式でエクスポートしてに保存します "C:\temp" named servername.cer。
8. キーストアから証明書を抽出します。C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12
9. p12ファイルから秘密鍵を抽出します。 openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"
10. 手順7でエクスポートしたBase-64証明書を秘密鍵とマージします。 openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"
11. マージした証明書をキーストアにインポートします。 C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"
12. ルート証明書をインポートします。 C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"
13. ルート証明書をserver.trustoreにインポートします。 C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"
14. 中間証明書をインポートします。 C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program

```
Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file
"C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"
```

すべての中間証明書について、この手順を繰り返します。

15. この例と一致するようにLDAPでドメインを指定します。
16. サーバを再起動します。

スマートカードおよび証明書によるログインをサポートするようにクライアントを設定しています

クライアントマシンでスマートカードを使用し、証明書によるログインを有効にするには、ミドルウェアを使用し、ブラウザを変更する必要があります。スマート・カードをすでに使用しているお客様は、クライアント・マシンに追加の変更を加える必要はありません。

作業を開始する前に

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "Windowsホストにインストールされ ているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

このタスクについて

一般的なクライアント設定要件は次のとおりです。

- ActivClientなどのスマートカードミドルウェアのインストール（を参照）
- IEブラウザの変更（を参照
- Firefoxブラウザの変更（を参照

Linuxサーバでの**CAC**の有効化

Linux OnCommand Insight サーバでCACを有効にするには、いくつかの変更が必要です。

ルートCAを信頼ストアにインポートする必要があります。

手順

1. に移動します `/opt/netapp/oci/conf/`
2. 編集 `wildfly.properties` をクリックし、の値を変更します `CLIENT_AUTH_ENABLED` 「True」へ
3. 以下にある「ルート証明書」をインポートします。
   `/opt/netapp/oci/wildfly/standalone/configuration/server.truststore`
4. サーバを再起動します

Data Warehouseでスマートカードおよび証明書によるログインを設定しています

スマートカード（CAC）および証明書によるログインをサポートするには、OnCommand Insight データウェアハウスの設定を変更する必要があります。

作業を開始する前に

- システムでLDAPが有効になっている必要があります。
- LDAP `User principal account name` 属性は、ユーザの政府機関ID番号を含むLDAPフィールドと一致する必要があります。

  政府発行のCACに保存される共通名（CN）は、通常次の形式になります。 `first.last.ID`。一部のLDAPフィールド（など） `sAMAccountName`この形式は長すぎます。これらのフィールドの場合、OnCommand Insight はCNからID番号だけを抽出します。

を使用して_server.keystore_and/or_server.trustore_passwordsを変更した場合は"securityadmin"、SANscreen証明書をインポートする前に_ldap_serviceを再起動してください。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "WindowsホストにインストールされているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

手順

1. regeditを使用して、のレジストリ値を変更します
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

a. jvm_optionを変更します `-DclientAuth=false` 終了： `-DclientAuth=true`。

Linuxの場合は、を変更します `clientAuth` のパラメータ `/opt/netapp/oci/scripts/wildfly.server`

2. Data Warehouse TrustoreにCertificate Authority（CA；認証局）を追加します。
   a. コマンドウィンドウで、に進みます `..\SANscreen\wildfly\standalone\configuration`。
   b. ユーティリティを使用し `keytool`て、信頼できるCAのリストを表示します `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>`。+ server_trustoreのパスワードの設定または変更の詳細については、ドキュメントを参照してください"securityadmin"。

      各行の最初の単語はCAエイリアスを示します。

   c. 必要に応じて、CA証明書ファイル（通常は）を指定します `.pem` ファイル。Data Warehouseの信頼済みCAにお客様のCAを含めるには、に進みます `..\SANscreen\wildfly\standalone\configuration` およびを使用します `keytool` インポートコマンド： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      my_aliasは通常、でCAを簡単に識別できるエイリアスです`keytool -list` 操作。

3. OnCommand Insight サーバで、を実行します `wildfly/standalone/configuration/standalone-full.xml` でverify-clientを「requested」に更新して、ファイルを変更する必要があります `/subsystem=undertow/server=default-server/https-listener=default-https`CACを有効にします。Insight Serverにログインし、該当するコマンドを実行します。

OS	スクリプト
Windows の場合	<install dir> を参照してください\enableCACforRemoteEJB.bat
Linux の場合	/opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB.sh

   スクリプトの実行後、wildflyサーバのリロードが完了するまで待ってから、次の手順に進みます。

4. OnCommand Insight サーバを再起動します。

スマートカードおよび証明書によるログインのための**Cognos**の設定（**OnCommand Insight 7.3.10**以降）

Cognosサーバでスマートカード（CAC）および証明書によるログインをサポートするには、OnCommand Insight Data Warehouseの設定を変更する必要があります。

作業を開始する前に

この手順 は、OnCommand Insight 7.3.10以降を実行しているシステム用です。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "Windowsホストにインストールされ ているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

手順

1. Cognos TrustoreにCertificate Authority（CA；認証局）を追加します。
   a. コマンドウィンドウで、に進みます `..\SANscreen\cognos\analytics\configuration\certs\`
   b. ユーティリティを使用し `keytool`て、信頼できるCAのリストを表示します。'..\..\IBM-JRE\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>

      各行の最初の単語はCAエイリアスを示します。
   c. 適切なファイルが存在しない場合は、CA証明書ファイル（通常は）を指定します `.pem` ファイル。
   d. OnCommand Insight の信頼済みCAに顧客のCAを含めるには、に進みます `..\SANscreen\cognos\analytics\configuration\certs\`。
   e. を使用します `keytool` をインポートするユーティリティ `.pem` ファイル： `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias`は通常、操作でCAを簡単に識別できるエイリアスです`keytool -list`。
   f. パスワードの入力を求められたら、_/ SANscreen /bin/cognos_info.dat_ファイルからパスワードを入力します。
   g. 回答 `yes` 証明書を信頼するように求められたら、
2. CACモードをイネーブルにするには、次の手順を実行します。
   a. 次の手順に従って、CACログアウトページを設定します。
      - Cognosポータルにログオンします（ユーザはシステム管理者グループ（cognos_admin）に属している必要があります）。
      - （7.3.10および7.3.11の場合のみ）[管理]→[構成]→[システム]→[セキュリティ]をクリックします
      - （7.3.10および7.3.11の場合のみ）Logout Redirect URL-> Applyに対してcacLogout.htmlと入力します
      - ブラウザを閉じます。

b. 実行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. IBM Cognosサービスを開始します。Cognosサービスが開始されるまで待ちます。

3. CACモードを無効にするには、次の手順を実行します。

a. 実行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. IBM Cognosサービスを開始します。Cognosサービスが開始されるまで待ちます。

c. （7.3.10および7.3.11の場合のみ）次の手順に従って、CACログアウトページの設定を解除します。

- Cognosポータルにログオンします（ユーザはシステム管理者グループ（cognos_admin）に属している必要があります）。
- [管理]→[設定]→[システム]→[セキュリティ]をクリックします
- Logout Redirect URL-> Applyに対してcacLogout.htmlと入力します
- ブラウザを閉じます。

Cognosおよび**DWH**の**CA**署名**SSL**証明書のインポート（**Insight 7.3.10**以降）

SSL証明書を追加して、Data WarehouseおよびCognos環境の認証と暗号化を強化することができます。

作業を開始する前に

この手順 は、OnCommand Insight 7.3.10以降を実行しているシステム用です。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "Windowsホストにインストールされ ているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

このタスクについて

この手順 を実行するには、admin権限が必要です。

手順

1. IBM Cognos Configurationツールを使用してCognosを停止します。Cognosを閉じます。
2. のバックアップを作成します `..\SANScreen\cognos\analytics\configuration` および `..\SANScreen\cognos\analytics\temp\cam\freshness` フォルダ。

3. Cognosから証明書暗号化要求を生成します。Admin CMDウィンドウで、次のコマンドを実行します。
   a. CD “`\Program Files\sanscreen\cognos\analytics\bin`”
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d “CN=server.domain.com,O=NETAPP,C=US” -H “server.domain.com” -I “ipaddress”`です。注意:ここで-Hと-Iはdnsやipaddressのようなサブジェクトの代替名を追加します。
   c. <password>の場合は、_/ SANscreen /bin/cognos_info.dat_ファイルのパスワードを使用します。
4. を開きます `c:\temp\encryptRequest.csr` ファイルを作成し、生成されたコンテンツをコピーします。
5. encryptRequest.csrコンテンツを入力し、CA署名ポータルを使用して証明書を生成します。
6. PKCS7形式を使用してルート証明書を含め、チェーン証明書をダウンロードします

   FQDNの.p7bファイルがダウンロードされます
7. CAから.p7b形式の証明書を取得します。Cognos Webサーバの証明書としてマークする名前を使用します。
8. ThirdPartyCertificateTool.batはチェーン全体をインポートできないため、すべての証明書をエクスポートするには複数の手順が必要です。チェーンを次のように個別にエクスポートして分割します。
   a. "`Crypto Shell Extensions`"の.p7b証明書を開きます。
   b. 左側のペインで「証明書」を参照します。
   c. ルートCA > All Tasks > Exportを右クリックします。
   d. Base64出力を選択します。
   e. ルート証明書として識別するファイル名を入力します。
   f. 手順8aから8eを繰り返して、すべての証明書を.cerファイルに個別にエクスポートします。
   g. ファイルにmediateX.cerとcognos.cerという名前を付けます。
9. CA証明書が1つしかない場合は、この手順を無視します。それ以外の場合は、root.cerとintermediateX.cerの両方を1つのファイルにマージします。
   a. メモ帳でroot.cerを開き、内容をコピーします。
   b. メモ帳を使用してintermediate.cerを開き、9aのコンテンツを追加します（最初に中間、次にルート）。
   c. ファイルをchain.cerとして保存します。
10. Admin CMDプロンプトを使用して、Cognosキーストアに証明書をインポートします。
    a. cd「Program Files\SANscreen\cognos\analytics\bin`」
    b. ThirdPartyCertificateTool.bat - java：local -i -T -r c：\temp\root.cer
    c. ThirdPartyCertificateTool.bat - java：local -i -T -r c：\temp\intermediate.cer
    d. ThirdPartyCertificateTool.bat - java：local -i -e -r c：\temp\cognos.cer -t c：\temp\chain.cer
11. [IBM Cognos Configuration]を開きます。
    a. [Local Configuration]→[Security]→[Cryptography]→[Cognos]を選択します
    b. 「サードパーティCAを使用しますか？」を変更します。 Trueに設定します。
    c. 設定を保存します。

d. Cognosを再起動します

12. Admin CMDプロンプトを使用して、最新のCognos証明書をcognos.crtにエクスポートします。
    a. CD "`C：\Program Files\SANscreen"
    b. java\bin\keytool.exe -exportcert -file c：\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password>-alias encryption
    c. <password>の場合は、_/ SANscreen /bin/cognos_info.dat_ファイルのパスワードを使用します。
13. DWHサーバのtrustoreをにバックアップしま す`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. Admin CMDプロンプトウィンドウを使用して、「c：\temp\cognos.crt」をDWH trustoreにインポートし、CognosとDWHの間のSSL通信を確立します。
    a. CD "`C：\Program Files\SANscreen"
    b. java\bin\keytool.exe -importcert -file c：\temp\cognos.crt -keystore wildfly\standalone\configuration\server.trustore -storepass <password>-alias cognos3rdca
    c. <password>の場合は、_/ SANscreen /bin/cognos_info.dat_ファイルのパスワードを使用します。
15. SANscreen サービスを再起動します。
16. DWHのバックアップを実行して、DWHがCognosと通信していることを確認します。
17. 次の手順は、「sl certificate」のみを変更し、デフォルトのCognos証明書を変更しない場合でも実行する必要があります。そうしないと、新しいSANscreen 証明書についてCognosから苦情が表示されたり、DWHバックアップを作成できない可能性があります。
    a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`
    b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass <password> -alias "ssl certificate"`
    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

    通常、これらの手順はCognos証明書のインポートプロセスの一環として実行します（を参照） "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

SSL証明書のインポート

SSL証明書を追加して強化された認証と暗号化を有効にすると、OnCommand Insight 環境のセキュリティを強化できます。

作業を開始する前に

システムが最小必要ビットレベル（1024ビット）を満たしていることを確認する必要があります。

このタスクについて

アップグレードの前にボルトをバックアップすることを強くお勧めします。

ボルトとパスワードの管理の詳細については、手順を参照してください"securityadminツール"。

手順

1. 元のキーストアファイルのコピーを作成します。 `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old`
2. キーストアの内容を表示します。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   キーストアの内容が表示されます。キーストアには少なくとも1つの証明書が必要です。 `"ssl certificate"`。
3. を削除します `"ssl certificate"`： `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. 新しいキーを生成します。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. 名と姓の入力を求められたら、使用するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を入力します。
   b. 組織および組織構造に関する次の情報を入力します。
      - Country：ISOの2文字の国の略語（USなど）
      - State or Province：組織の本社がある都道府県の名前（例：Massachusetts）
      - Locality：組織の本社がある市区町村の名前（例：Waltham）
      - Organizational name：ドメイン名を所有する組織の名前（例：NetApp）
      - Organizational unit name：証明書を使用する部門またはグループの名前（Supportなど）
      - Domain Name/Common Name：サーバのDNSルックアップに使用されるFQDN（例：www.example.com）。システムから次のような情報が返されます。 `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
   c. 入力するコマンド `Yes` Common Name（CN；共通名）がFQDNになっている場合。
   d. キーのパスワードの入力を求められたら、パスワードを入力するか、Enterキーを押して既存のキーストアパスワードを使用します。
5. 証明書要求ファイルを生成します。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -alias "ssl certificate" -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr`

   。 `c:\localhost.csr` fileは、新しく生成される証明書要求ファイルです。

6. を送信します `c:\localhost.csr` を承認のためにCertificate Authority（CA；認証局）に送信します。

   証明書要求ファイルが承認されたら、で証明書を返す必要があります `.der` の形式で入力しファイルがとして返される場合と返されない場合があります `.der` ファイル。デフォルトのファイル形式はです `.cer` Microsoft CAサービスの場合。

   ほとんどの組織のCAは、ルートCAを含む信頼チェーンモデルを使用しています。ルートCAは、多くの場合オフラインです。中間CAと呼ばれる少数の子CAの証明書にのみ署名しています。

   公開鍵（証明書）は、信頼チェーン全体（OnCommand Insight サーバの証明書に署名したCAの証明書、およびその署名CAから組織のルートCAまでのすべての証明書）を取得する必要があります。

   組織によっては、署名要求を送信すると、次のいずれかが送信される場合があります。

   - 署名済み証明書と信頼チェーン内のすべてのパブリック証明書を含むPKCS12ファイル
   - A `.zip` 個 々 のファイル（署名済み証明書を含む）および信頼チェーン内のすべてのパブリック証明書を含むファイル
   - 署名済み証明書のみ

     パブリック証明書を入手する必要があります。

7. server.keystoreの承認済み証明書をインポートします。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   a. プロンプトが表示されたら、キーストアのパスワードを入力します。

      次のメッセージが表示されます。 `Certificate reply was installed in keystore`

8. server.trustoreの承認済み証明書をインポートします。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"`

   a. プロンプトが表示されたら、trustoreパスワードを入力します。

      次のメッセージが表示されます。 `Certificate reply was installed in trustore`

9. を編集します `SANscreen\wildfly\standalone\configuration\standalone-full.xml` ファイル：

   次のエイリアス文字列を置き換えます。 `alias="cbc-oci-02.muccbc.hq.netapp.com"`。例：

   ```
   <keystore path="server.keystore" relative-to="jboss.server.config.dir"
   keystore-password="${VAULT::HttpsRealm::keystore_password::1}" alias="cbc-oci-
   02.muccbc.hq.netapp.com" key-
   password="${VAULT::HttpsRealm::key_password::1}"/>
   ```

10. SANscreen サーバサービスを再起動します。

    Insightが起動したら、鍵のアイコンをクリックして、システムにインストールされている証明書を表示で

きます。

「Issued To」の情報が「Issued By」の情報と一致する証明書が表示された場合、まだ自己署名証明書がインストールされています。Insightのインストーラで生成される自己署名証明書の有効期限は100年です。

この手順 でデジタル証明書に関する警告が削除されることを保証することはできません。ネットアップでは、エンドユーザのワークステーションの設定方法を制御できません。次のシナリオを検討してください。

- Microsoft Internet ExplorerとGoogle Chromeは、どちらもWindowsでMicrosoftのネイティブ証明書機能を使用します。

  つまり、Active Directory管理者が組織のCA証明書をエンドユーザーの証明書トラスストアにプッシュすると、OnCommand Insight の自己署名証明書が内部CAインフラストラクチャによって署名された証明書に置き換えられたときに、これらのブラウザのユーザーに証明書の警告が表示されなくなります。

- JavaおよびMozilla Firefoxには独自の証明書ストアがあります。

  システム管理者がこれらのアプリケーションの信頼された証明書ストアにCA証明書を自動で取り込んでいない場合、自己署名証明書が置き換えられても、信頼されていない証明書が原因で、Firefoxブラウザで証明書に関する警告が引き続き生成されることがあります。組織の証明書チェーンをtrustoreにインストールすることは、追加の要件です。

Insightデータベースの週次バックアップの設定

データを保護するために、Insightデータベースの自動週次バックアップを設定することができます。これらの自動バックアップでは、指定したバックアップディレクトリ内のファイルが上書きされます。

このタスクについて

ベストプラクティス：OCIデータベースの週次バックアップを設定する場合は、そのサーバで障害が発生した場合に備えて、Insightで使用しているサーバとは別のサーバにバックアップを保存する必要があります。週次バックアップではディレクトリ内のファイルが上書きされるため、週次バックアップディレクトリに手動バックアップを保存しないでください。

バックアップファイルには次の内容が含まれます。

- インベントリデータ
- 最大7日分のパフォーマンスデータ

手順

1. Insightのツールバーで、* Admin > Setup *をクリックします。
2. [バックアップとアーカイブ]*タブをクリックします。
3. [Weekly Backup]セクションで、*[Enable weekly backup]*を選択します。
4. バックアップ先*へのパスを入力します。これは、ローカルのInsight Server上のに配置することも、Insight Serverからアクセスできるリモートサーバ上に配置することもできます。

バックアップの場所の設定はバックアップ自体に含まれているため、別のシステムにバックアップをリストアする場合は、新しいシステムではバックアップフォルダの場所が無効である可能性があることに注意してください。バックアップのリストア後に、バックアップの場所の設定を再確認してください。

5. [Cleanup]*オプションを選択して、バックアップを2つまたは5つ保持します。
6. [保存（ Save ）] をクリックします。

結果

- Admin > Troubleshooting *に移動して、オンデマンドバックアップを作成することもできます。

バックアップに含まれるもの

週次バックアップとオンデマンドバックアップは、トラブルシューティングや移行に使用できます。

週次バックアップまたはオンデマンドバックアップには、次のものが含まれます。

- インベントリデータ
- パフォーマンスデータ（バックアップに含めることを選択した場合）
- データソースとデータソースの設定
- 統合パック
- Remote Acquisition Unitの略
- ASUP /プロキシの設定
- バックアップの場所の設定
- アーカイブ場所の設定
- 通知設定
- ユーザ
- パフォーマンスポリシー
- ビジネスエンティティとアプリケーション
- デバイス解決のルールと設定
- ダッシュボードとウィジェット
- カスタマイズされたアセットページのダッシュボードとウィジェット
- クエリ
- アノテーションとアノテーションルール

週次バックアップには、次のものは含まれません。

- セキュリティツールの設定/ヴォールト情報（別のCLIプロセスでバックアップ）
- ログ（オンデマンドで.zipファイルに保存可能）

- パフォーマンスデータ（バックアップに含めることを選択していない場合）
- ライセンス

パフォーマンスデータをバックアップに含めることを選択した場合は、直近7日間のデータがバックアップされます。残りのデータは、その機能を有効にしている場合はアーカイブに保存されます。

パフォーマンスデータのアーカイブ

OnCommand Insight 7.3では、パフォーマンスデータを毎日アーカイブする機能が導入されています。これは、構成および限られたパフォーマンスデータのバックアップを補完するものです。

OnCommand Insight には、最大90日分のパフォーマンスデータと違反データが保持されます。ただし、そのデータのバックアップを作成する場合は、最新の情報のみがバックアップに含まれます。アーカイブを使用すると、残りのパフォーマンスデータを保存し、必要に応じてロードできます。

アーカイブの場所を設定してアーカイブをアクティブ化すると、1日に1回、すべてのオブジェクトの前日のパフォーマンスデータがアーカイブの場所にアーカイブされます。毎日のアーカイブは、アーカイブフォルダ内の別のファイルに保存されます。アーカイブはバックグラウンドで実行され、Insightが実行されているかぎり継続されます。

最新の90日分のアーカイブが保持されます。90日を経過したアーカイブファイルは、新しいアーカイブファイルが作成されると削除されます。

パフォーマンスアーカイブの有効化

パフォーマンスデータのアーカイブを有効にするには、次の手順を実行します。

手順

1. ツールバーで、* Admin > Setup *をクリックします。
2. [バックアップとアーカイブ]*タブを選択します。
3. [Performance Archive]セクションで、[**Enable performance archive]がオンになっていることを確認します。
4. 有効なアーカイブの場所を指定してください。

   Insightのインストールフォルダにフォルダを指定することはできません。

   ベストプラクティス：アーカイブ用にInsightのバックアップ先と同じフォルダを指定しないでください。
5. [保存（ Save ）] をクリックします。

   アーカイブプロセスはバックグラウンドで処理されるため、Insightの他のアクティビティに影響はありません。

パフォーマンスアーカイブをロードしています

パフォーマンスデータアーカイブをロードするには、次の手順を実行します。

作業を開始する前に

パフォーマンスデータアーカイブをロードする前に、有効な週次バックアップまたは手動バックアップをリストアする必要があります。

手順

1. ツールバーで、* Admin > Troubleshooting *をクリックします。
2. [リストア]セクションの*で、[ロード]*をクリックします。

> アーカイブのロードはバックグラウンドで処理されます。アーカイブされた各日のパフォーマンスデータがInsightに読み込まれるため、フルアーカイブのロードには時間がかかることがあります。アーカイブロードのステータスは、このページのアーカイブセクションに表示されます。

Eメールを設定しています

OnCommand Insight Serverで登録したレポートをEメールで配信したり、トラブルシューティング用のサポート情報をネットアップテクニカルサポートに転送したりできるように、Eメールシステムにアクセスするように OnCommand Insight を設定する必要があります。

Eメール設定の前提条件

EメールシステムにアクセスするようにOnCommand Insight を設定するには、（SMTPまたはExchange）メールサーバを識別するためのホスト名またはIPアドレスを検出し、OnCommand Insight レポート用のEメールアカウントを割り当てる必要があります。

メール管理者に、OnCommand Insight 用のメールアカウントを作成するよう依頼してください。次の情報が必要です。

- 組織で使用されているメールサーバ（SMTPまたはExchange）を識別するホスト名またはIPアドレス。この情報は、メールを読むために使用するアプリケーションで確認できます。たとえば、Microsoft Outlook では、アカウント設定を表示してサーバーの名前を確認できます。[ツール]-[電子メールアカウント]-[既存の電子メールアカウントの表示または変更]。
- OnCommand Insight が定期的にレポートを送信するメールアカウントの名前。アカウントは、組織内の有効なEメールアドレスである必要があります。（ほとんどのメールシステムは、有効なユーザから送信されない限り、メッセージを送信しません）。 メールサーバでメールを送信するためにユーザ名とパスワードが必要な場合は、システム管理者にこの情報を入手してください。

Insight用のEメールを設定しています

Insightのレポートをユーザのメールアカウントで受信する場合は、Eメールサーバでこ

の機能を有効にする必要があります。

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Notifications]*を選択します。
2. ページの* Eメール*セクションまでスクロールします。
3. [サーバ]ボックスに、組織内のSMTPサーバの名前を入力します。このサーバは、ホスト名またはIPアドレス（_nnn.nnn.nnn.nnn_format）を使用して識別されます。

   ホスト名を指定する場合は、DNSを介して名前を解決できることを確認してください。
4. [ユーザー名]ボックスにユーザー名を入力します。
5. [パスワード]*ボックスに、Eメールサーバにアクセスするためのパスワードを入力します。このパスワードは、SMTPサーバがパスワードで保護されている場合にのみ必要です。これは、メールを読むためのアプリケーションへのログインに使用するパスワードと同じです。パスワードが必要な場合は、確認のためにもう一度入力する必要があります。
6. [送信者のEメール]ボックスに、すべてのOnCommand Insight レポートの送信者として識別される送信者のEメールアカウントを入力します。

   このアカウントは、組織内の有効なEメールアカウントである必要があります。
7. [電子メール署名]ボックスに、送信するすべての電子メールに挿入するテキストを入力します。
8. [Recipients]ボックスで、をクリックします をクリックして、Eメールアドレスを入力し、* OK *をクリックします。

   Eメールアドレスを編集するには、アドレスを選択し、をクリックします 。Eメールアドレスを削除するには、アドレスを選択してをクリックします 。
9. 指定した受信者にテストEメールを送信するには、をクリックします 。
10. [保存（ Save ）] をクリックします。

SNMP通知の設定

OnCommand Insight では、設定およびグローバルパスポリシーの変更および違反に関するSNMP通知がサポートされます。SNMP通知は、たとえばデータソースのしきい値を超えたときに送信されます。

作業を開始する前に

次の作業が完了している必要があります。

- イベントのタイプごとにトラップを統合するサーバのIPアドレスを特定します。

  この情報を取得するには、システム管理者に問い合わせる必要があります。
- イベントのタイプごとに、指定したマシンがSNMPトラップを取得する際に使用するポート番号を識別します。

  SNMPトラップのデフォルトポートは162です。

- サイトでMIBをコンパイルします。

  独自のMIBには、OnCommand Insight トラップをサポートするインストールソフトウェアが付属しています。NetApp MIBは、すべての標準的なSNMP管理ソフトウェアと互換性があり、Insightサーバのにあります `<install dir>\SANscreen\MIBS\sanscreen.mib`。

手順

1. をクリックし、[通知]*を選択します。
2. ページの*[SNMP]*セクションまでスクロールします。
3. をクリックし、[Add trap source]*を選択します。
4. [SNMPトラップ受信者の追加]*ダイアログボックスで、次の値を入力します。
   - * IP *

     OnCommand Insight がSNMPトラップメッセージを送信するIPアドレス。
   - * ポート *

     OnCommand Insight がSNMPトラップメッセージを送信するポート番号。
   - コミュニティストリング

     SNMPトラップメッセージには「public」を使用します。
5. [保存（ Save ）] をクリックします。

syslogファシリティのイネーブル化

OnCommand Insight 違反、パフォーマンスアラート、および監査メッセージのログの場所を特定し、ロギングプロセスをアクティブ化できます。

作業を開始する前に

- システムログを格納するサーバのIPアドレスが必要です。
- メッセージを記録するプログラムのタイプ（local1やuserなど）に対応するファシリティレベルを把握しておく必要があります。

このタスクについて

syslogには、次のタイプの情報が含まれます。

- 違反メッセージ
- パフォーマンスアラート
- 必要に応じて、監査ログメッセージ

syslogでは次の単位が使用されます。

- 利用率の指標：割合
- トラフィックの指標：MB
- トラフィックレート：MB/秒

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Notifications]*を選択します。
2. ページの* Syslog *セクションまで下にスクロールします。
3. [Enable syslog]チェックボックスをオンにします。
4. 必要に応じて、*監査を送信*チェックボックスをオンにします。新しい監査ログメッセージは[Audit]ページに表示されるだけでなく、syslogに送信されます。既存の監査ログメッセージはsyslogには送信されず、新しく生成されたログメッセージのみが送信されます。
5. [**Server**]フィールドに、ログサーバのIPアドレスを入力します。

   カスタムポートを指定するには、サーバIPの末尾にコロンの後に追加します（例：server:port）。portを指定しない場合は、デフォルトのsyslogポートである514が使用されます。
6. [**Facility**]フィールドで、メッセージを記録するプログラムのタイプに対応するファシリティレベルを選択します。
7. [保存（ Save ）] をクリックします。

Insightの**syslog**の内容

サーバでsyslogを有効にして、利用率やトラフィックのデータを含むInsight違反やパフォーマンスアラートメッセージを収集することができます。

メッセージタイプ

Insightのsyslogには、次の3種類のメッセージが表示されます。

- SANパス違反
- 一般的な違反
- パフォーマンスアラート

提供されるデータ

違反の説明には、関連する要素、イベントの時刻、違反の相対的な重大度または優先度が含まれます。

パフォーマンスアラートには次のデータが含まれます。

- 利用率
- トラフィックタイプ
- トラフィックレート（MB）

パフォーマンスと品質管理の違反通知の設定

OnCommand Insight では、パフォーマンスや品質管理の違反の通知がサポートされます。これらの違反に関する通知は、デフォルトではInsightから送信されません。違反が発生した場合に、Eメールを送信するか、syslogサーバにsyslogメッセージを送信するか、SNMP通知を送信するようにInsightを設定する必要があります。

作業を開始する前に

違反の送信方法をEメール、syslog、およびSNMPで設定しておく必要があります。

手順

1. **>**[通知]*をクリックします。
2. [イベント]をクリックします。
3. または**[Assure Violations events]***セクションで、目的の通知方法（ Eメール*、* syslog 、または SNMP ）のリストをクリックし、違反の重大度レベル（ Warning and above または Critical *）を選択します。
4. [保存（ Save ）] をクリックします。

システムレベルのイベント通知の設定

OnCommand Insight では、Acquisition Unitの障害やデータソースのエラーなど、システムレベルのイベントの通知がサポートされます。通知を受信するには、これらのイベントが発生したときにEメールを送信するようにInsightを設定する必要があります。

作業を開始する前に

- Admin **>** Notifications **>** Sending Methods *で通知を受信するEメール受信者を設定しておく必要があります。

手順

1. **>**[通知]*をクリックします。
2. [イベント]をクリックします。
3. **[Email]**セクションで、通知の重大度レベル（ Warning and above または Critical ）を選択します。システムレベルのイベントの通知を受信しない場合は、[Do not send]*を選択します。
4. [保存（ Save ）] をクリックします。
5. アラート自体を設定するには、**[**管理**]**>*[システムアラート]*をクリックします。
6. 新しいアラートを追加するには、**+**追加*をクリックし、一意の*名前*を指定します。右側のアイコンをクリックして[編集]*既存のアラートを編集することもできます。
7. アラートを送信する*イベントタイプ*を選択します（例：*Acquisition Unit Failure*）。
8. 選択した時間間隔で選択したタイプの重複イベントに関する通知を停止するには、*スヌーズ*間隔を選択します。_never_を選択すると、イベントが発生しなくなるまで1分に1回通知が繰り返し送信されます。
9. イベント通知の[Severity]*（[Warning]または[Critical]）を選択します。

10. Eメール通知はデフォルトでグローバルEメール受信者リストに送信されます。または、表示されたリンクをクリックしてグローバルリストを上書きし、特定の受信者に通知を送信できます。
11. [Save]をクリックしてアラートを追加します。

ASUPの処理を設定しています

すべてのネットアップ製品には、お客様に最大限のサポートを提供する自動化機能が搭載されています。自動サポート（ASUP）は、事前に定義された特定の情報をカスタマーサポートに定期的に送信します。ネットアップに転送する情報と送信頻度を制御できます。

作業を開始する前に

データを送信する前に、データを転送するようにOnCommand Insight を設定する必要があります。

このタスクについて

ASUPデータはHTTPSプロトコルを使用して転送されます。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [設定]*をクリックします。
3. [ASUPとプロキシ]*タブをクリックします。
4. セクションで、[ASUPを有効にする]*を選択してASUP機能をアクティブ化します。
5. 会社情報を変更する場合は、次のフィールドを更新します。
   - 会社名
   - サイト名
   - 送信対象：ログ、設定データ、パフォーマンスデータ
6. [接続のテスト]*をクリックして、指定した接続が機能することを確認します。
7. [保存（ Save ）] をクリックします。
8. [* Proxy*]セクションで、* Enable Proxy*を選択し、プロキシ*ホスト*、ポート、および* user *情報を指定します。
9. [接続のテスト]*をクリックして、指定したプロキシが動作することを確認します。
10. [保存（ Save ）] をクリックします。

AutoSupport （ASUP）パッケージの内容

AutoSupport パッケージには、データベースのバックアップと拡張情報が含まれています。

AutoSupport パッケージには次のものが含まれています。

- インベントリデータ
- パフォーマンスデータ（ASUPに含めることを選択した場合）
- データソースとデータソースの設定
- 統合パック
- Remote Acquisition Unitの略
- ASUP /プロキシの設定
- バックアップの場所の設定
- アーカイブ場所の設定
- 通知設定
- ユーザ
- パフォーマンスポリシー
- ビジネスエンティティとアプリケーション
- デバイス解決のルールと設定
- ダッシュボードとウィジェット
- カスタマイズされたアセットページのダッシュボードとウィジェット
- クエリ
- アノテーションとアノテーションルール
- ログ
- ライセンス
- 取得/データソースのステータス
- MySQLのステータス
- システム情報

AutoSupport パッケージには、次のものは含まれません。

- セキュリティツールの設定/ヴォールト情報（別のCLIプロセスでバックアップ）
- パフォーマンスデータ（ASUPに含めることを選択しなかった場合）

ASUPにパフォーマンスデータを含めることを選択した場合は、直近7日間のデータが含まれます。残りのデータは、その機能を有効にしている場合はアーカイブに保存されます。アーカイブデータはASUPに含まれません。

アプリケーションの定義

環境で実行されている特定のアプリケーションに関連するデータを追跡するには、それらのアプリケーションを定義する必要があります。

作業を開始する前に

アプリケーションをビジネスエンティティに関連付ける場合は、ビジネスエンティティを作成しておく必要があります。

このタスクについて

アプリケーションを関連付けることができるアセットは、ホスト、仮想マシン、ボリューム、内部ボリューム、 qtree 、 共有、ハイパーバイザー：

手順

1. OnCommand Insight Web UIにログインします。
2. をクリックし、[アプリケーション]*を選択します。

   アプリケーションを定義すると、[アプリケーション]ページにアプリケーションの名前と優先度、およびアプリケーションに関連付けられているビジネスエンティティ（該当する場合）が表示されます。

3. [追加（ Add ）] をクリックします。

   [アプリケーションの追加]ダイアログボックスが表示されます。

4. [名前]ボックスにアプリケーションの一意の名前を入力します。
5. [優先度]*をクリックし、環境内のアプリケーションの優先度（[重大]、[高]、[中]、[低]）を選択します。
6. このアプリケーションを特定のビジネスエンティティで使用する場合は、*[Business Entity]*をクリックし、リストからエンティティを選択します。
7. オプション：ボリューム共有を使用しない場合は、*[Validate volume sharing]*ボックスをオフにします。

   これにはAssureライセンスが必要です。この値は、クラスタ内の同じボリュームに各ホストがアクセスできるようにする場合に設定します。たとえば、高可用性クラスタのホストは、フェイルオーバーを可能にするために同じボリュームにマスクする必要があることがよくありますが、無関係なアプリケーションのホストは通常、同じ物理ボリュームにアクセスする必要はありません。また、セキュリティ上の理由から、関係のないアプリケーションによる同じ物理ボリュームへのアクセスを明示的に禁止するように規制ポリシーで規定されている場合があります。

8. [保存（ Save ）] をクリックします。

   [Applications]ページにアプリケーションが表示されます。アプリケーションの名前をクリックすると、そのアプリケーションのアセットページが表示されます。

完了後

アプリケーションを定義したら、ホスト、仮想マシン、ボリューム、内部ボリューム、またはハイパーバイザーのアセットページに移動して、アプリケーションをアセットに割り当てることができます。

アセットへのアプリケーションの割り当て

ビジネスエンティティの有無に関係なくアプリケーションを定義したら、それらのアプリケーションをアセットに関連付けることができます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法で、アプリケーションを適用するアセット（ホスト、仮想マシン、ボリューム、または内部ボリューム）を選択します。
   - をクリックし、[アセットダッシュボード]*を選択してアセットをクリックします。
   - をクリックします ツールバーの*[アセットの検索]*ボックスを表示するには、アセットの名前を入力し、リストからアセットを選択します。
3. アセットページの*セクションで、アセットに現在割り当てられているアプリケーションの名前（割り当てられているアプリケーションがない場合は[None]*と表示されます）にカーソルを合わせ、をクリックします （アプリケーションの編集）。

   選択したアセットで使用可能なアプリケーションのリストが表示されます。アセットに現在関連付けられているアプリケーションの前にチェックマークが表示されます。
4. [検索]ボックスにアプリケーション名を入力してフィルタリングするか、リストを下にスクロールします。
5. アセットに関連付けるアプリケーションを選択します。

   ホスト、仮想マシン、および内部ボリュームには複数のアプリケーションを割り当てることができますが、ボリュームに割り当てることができるアプリケーションは1つだけです。
6. をクリックします をクリックして、選択したアプリケーションをアセットに割り当てます。

   [User Data]セクションにアプリケーション名が表示されます。アプリケーションがビジネスエンティティに関連付けられている場合は、ビジネスエンティティの名前もこのセクションに表示されます。

アプリケーションの編集

必要に応じて、アプリケーションの優先度、アプリケーションに関連付けられているビジネスエンティティ、ボリューム共有のステータスを変更できます。

手順

1. OnCommand Insight Web UIにログインします。
2. をクリックし、[アプリケーション]*を選択します。
3. 編集するアプリケーションにカーソルを合わせ、をクリックします 。

   [アプリケーションの編集]ダイアログボックスが表示されます。
4. 次のいずれかを実行します。
   - [優先度]*をクリックし、別の優先度を選択します。

     アプリケーションの名前は変更できません。
   - をクリックし、アプリケーションを関連付ける別のビジネスエンティティを選択するか、[なし]*を選択してアプリケーションとビジネスエンティティの関連付けを解除します。

◦ [ボリューム共有の検証]*をクリックして選択を解除または選択します。

このオプションは、Assureライセンスがある場合にのみ使用できます。

5. [保存（ Save ）] をクリックします。

アプリケーションの削除

環境のニーズを満たせなくなったアプリケーションを削除することもできます。

手順

1. Insight Web UIにログインします。
2. をクリックし、[アプリケーション]*を選択します。
3. 削除するアプリケーションにカーソルを合わせ、をクリックします 。

   アプリケーションを削除するかどうかを確認する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。

ビジネスエンティティ階層

ビジネスエンティティを定義して、環境のデータをより細かく追跡し、レポートすることができます。

OnCommand Insight では、ビジネスエンティティ階層に次のレベルが含まれます。

- *テナント*は、主にサービスプロバイダがリソースをお客様（ネットアップなど）に関連付けるために使用します。
- *基幹業務（LOB）*は、データストレージなど、社内の基幹業務または製品ラインです。
- *ビジネスユニット*は、法務部門やマーケティング部門などの従来のビジネスユニットを表します。
- *プロジェクト*は、多くの場合、容量チャージバックが必要なビジネスユニット内の特定のプロジェクトを識別するために使用されます。たとえば、法務部門の場合は「Patents」、マーケティング部門の場合は「Sales Events」のようになります。レベル名にはスペースを含めることができます。

企業階層の設計では、すべてのレベルを使用する必要はありません。

ビジネスエンティティ階層の設計

企業構造の要素と、ビジネスエンティティで何を表す必要があるかを理解する必要があります。これは、それらがOnCommand Insight データベースで固定構造になるためです。次の情報を使用してビジネスエンティティをセットアップできます。これらのカテゴリのデータを収集するために、すべての階層レベルを使用する必要はないことに注意してください。

手順

1. ビジネスエンティティ階層の各レベルを調べて、そのレベルを会社のビジネスエンティティ階層に含める必要があるかどうかを判断します。
   - *テナント*レベルは、会社がISPで、顧客のリソース使用状況を追跡する場合に必要です。
   - *さまざまな製品ラインのデータを追跡する必要がある場合は、基幹業務（LOB）*が階層に必要です。
   - *部門ごとにデータを追跡する必要がある場合は、ビジネスユニット*が必要です。この階層レベルは、1つの部門が使用するリソースと、他の部門が使用しないリソースを分離するのに役立ちます。
   - *プロジェクト*レベルは、部門内の特殊な作業に使用できます。このデータは、企業や部門内の他のプロジェクトと比較して、個別のプロジェクトのテクノロジニーズを特定、定義、および監視するのに役立ちます。
2. 各ビジネスエンティティとそのエンティティ内のすべてのレベルの名前を示すグラフを作成します。
3. 階層内の名前をチェックして、OnCommand Insight のビューやレポートでわかりやすい名前になっていることを確認します。
4. 各ビジネスエンティティに関連付けられているアプリケーションをすべて特定します。

ビジネスエンティティを作成しています

会社のビジネスエンティティ階層を設計したら、アプリケーションをセットアップし、ビジネスエンティティをアプリケーションに関連付けることができます。このプロセスにより、OnCommand Insight データベースにビジネスエンティティ構造が作成されます。

このタスクについて

アプリケーションとビジネスエンティティの関連付けはオプションですが、これを推奨します。

手順

1. Insight Web UIにログインします。
2. をクリックし、[ビジネスエンティティ]*を選択します。

   [Business Entities]ページが表示されます。
3. をクリックします

新しいエンティティの構築を開始します。

   [ビジネスエンティティの追加]*ダイアログボックスが表示されます。
4. 各エンティティレベル（テナント、基幹業務、ビジネスユニット、プロジェクト）について、次のいずれかを実行できます。
   - エンティティレベルリストをクリックし、値を選択します。
   - 新しい値を入力し、Enterキーを押します。
   - ビジネスエンティティにエンティティレベルを使用しない場合は、エンティティレベルの値をN/Aのままにします。
5. [保存（ Save ）] をクリックします。

アセットへのビジネスエンティティの割り当て

ビジネスエンティティをアセット（ホスト、ポート、ストレージ、スイッチ、仮想マシン、 ビジネスエンティティをアプリケーションに関連付けずにqtree、共有、ボリューム、または内部ボリューム）を割り当てることができます。ただし、ビジネスエンティティに関連するアプリケーションにアセットが関連付けられている場合は、アセットにビジネスエンティティが自動的に割り当てられます。

作業を開始する前に

ビジネスエンティティを作成しておく必要があります。

このタスクについて

ビジネスエンティティはアセットに直接割り当てることができますが、アセットにアプリケーションを割り当ててから、ビジネスエンティティをアセットに割り当てることを推奨します。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法で、ビジネスエンティティを適用するアセットを選択します。
   - [Assets Dashboard]でアセットをクリックします。
   - をクリックします ツールバーの*[アセットの検索]*ボックスを表示するには、アセットの名前を入力し、リストからアセットを選択します。
3. アセットページの*セクションで、[Business Entities]の横にある[None]*にカーソルを合わせ、をクリックします 。

   使用可能なビジネスエンティティのリストが表示されます。

4. [検索]*ボックスに入力してリストをフィルタするか、リストを下にスクロールしてリストからビジネスエンティティを選択します。

   選択したビジネスエンティティがアプリケーションに関連付けられている場合は、アプリケーション名が表示されます。この場合、ビジネスエンティティ名の横に「データベース」という単語が表示されます。エンティティをアセットに対してのみ保持し、関連付けられているアプリケーションを保持しない場合は、アプリケーションの割り当てを手動で上書きできます。

5. ビジネスエンティティから派生したアプリケーションを上書きするには、アプリケーション名にカーソルを合わせ、をクリックします をクリックし、別のビジネスエンティティを選択し、リストから別のアプリケーションを選択します。

複数のアセットに対するビジネスエンティティの割り当てまたは削除

ビジネスエンティティを手動で割り当てたり削除したりする代わりに、クエリを使用して複数のアセットに対して割り当てたり削除したりすることができます。

作業を開始する前に

目的のアセットに追加するビジネスエンティティを作成しておく必要があります。

手順

1. 新しいクエリを作成するか、既存のクエリを開きます。
2. 必要に応じて、ビジネスエンティティを追加するアセットでフィルタを適用します。
3. リストから目的のアセットを選択するか、をクリックします をクリックして*すべて*を選択します。

   [アクション]*ボタンが表示されます。

4. 選択したアセットにビジネスエンティティを追加するには、をクリックします

。選択したアセットタイプにビジネスエンティティを割り当てることができる場合は、*[ビジネスエンティティの追加]*を選択するメニューが表示されます。これを選択します。
5. リストから目的のビジネスエンティティを選択し、*[保存]*をクリックします。

   新しいビジネスエンティティを割り当てると、アセットにすでに割り当てられているビジネスエンティティよりも優先されます。アプリケーションをアセットに割り当てると、割り当てられているビジネスエンティティも同じ方法で上書きされます。ビジネスエンティティをアセットとして割り当てると、そのアセットに割り当てられているアプリケーションよりも優先される可能性があります。

6. アセットに割り当てられているビジネスエンティティを削除するには、をクリックします

をクリックし、*[Remove Business Entity]*を選択します。
7. リストから目的のビジネスエンティティを選択し、*[削除]*をクリックします。

アノテーションの定義

OnCommand Insight でのデータの追跡方法を企業の要件に合わせてカスタマイズする場合は、アノテーションによってデータの全体像を定義できます。たとえば、アセットの耐用年数、データセンター、建物の場所、ストレージ階層、ボリューム、 および内部ボリュームのサービスレベル。

手順

1. 環境のデータを関連付ける必要がある業界固有の用語をリストします。
2. 環境データを関連付ける必要がある企業用語（ビジネスエンティティを使用してまだ追跡されていない用語）をリストします。
3. 使用できるデフォルトのアノテーションタイプがないかどうかを特定します。
4. 作成する必要があるカスタムアノテーションを特定します。

アノテーションを使用した環境の監視

企業の要件に合わせてデータを追跡するようにOnCommand Insight をカスタマイズする場合は、_annotations_という特殊なメモを定義してアセットに割り当てることができます。たとえば、アセットの終了日、データセンター、建物の場所、ストレージ階層、ボリュームのサービスレベルなどの情報をアノテートできます。

環境の監視にアノテーションを使用すると、次の作業に役立ちます。

- すべてのアノテーションタイプの定義を作成または編集します。
- アセットページを表示し、各アセットを 1 つ以上のアノテーションに関連付ける。

  たとえば、リースしているアセットのリース期限が 2 カ月以内の場合、終了日のアノテーションを適用すると、これにより、他のユーザがそのアセットを長期間使用できないようにすることができます。
- ルールを作成して、同じタイプの複数のアセットにアノテーションを自動的に適用する。
- アノテーションインポートユーティリティを使用してアノテーションをインポートする。
- アノテーションに基づいてアセットをフィルタする。
- アノテーションに基づいてレポートにデータをグループ化し、レポートを生成する。

  レポートの詳細については、OnCommand Insight レポートガイド_を参照してください。

アノテーションタイプの管理

OnCommand Insight には、アセットのライフサイクル（開始日や終了日）、建物やデータセンターの場所、階層など、カスタマイズしてレポートに表示できるデフォルトのアノテーションタイプがいくつか用意されています。デフォルトのアノテーションタイプの値を定義することも、独自のカスタムアノテーションタイプを作成することもできます。これらの値は後で編集できます。

デフォルトのアノテーションタイプ

OnCommandInsightには、デフォルトのアノテーションタイプがいくつか用意されています。これらのアノテーションを使用して、データをフィルタまたはグループ化したり、データレポートをフィルタリングしたりできます。

次のようなデフォルトのアノテーションタイプをアセットに関連付けることができます。

- アセットのライフサイクル：開始日、停止日、終了日など
- デバイスの場所の情報。データセンター、建物、フロアなど
- 品質（階層）、接続デバイス（スイッチレベル）、サービスレベルなどのアセットの分類
- ステータス（ホット（高利用率）など）

次の表に、デフォルトのアノテーションタイプを示します。これらのアノテーションの名前は必要に応じて編集できます。

アノテーションタイプ	説明	を入力します
エイリアス	リソースのフレンドリ名。	テキスト（ Text ）
誕生日	デバイスがオンラインになった日付、またはオンラインになる予定の日付。	日付

建物	ホスト、ストレージ、スイッチ、およびテープリソースの物理的な場所。	リスト
市区町村	ホスト、ストレージ、スイッチ、およびテープリソースが配置されている自治体。	リスト
コンピュートリソースグループ	Host and VM File Systemsデータソースで使用されるグループ割り当て。	リスト
大陸	ホスト、ストレージ、スイッチ、およびテープリソースの地理的な場所。	リスト
国名	ホスト、ストレージ、スイッチ、およびテープリソースが配置されている国。	リスト
データセンター	リソースの物理的な場所。ホスト、ストレージアレイ、スイッチ、およびテープで使用できます。	リスト
直接接続	ストレージリソースがホストに直接接続されているかどうか（[Yes]または[No]）を示します。	ブール値
サポート終了	リースの期限が切れた場合やハードウェアが撤去される場合など、デバイスがオフラインになる日付。	日付
ファブリックエイリアス	ファブリックのフレンドリ名。	テキスト（ Text ）
床	建物のフロア上のデバイスの場所。ホスト、ストレージアレイ、スイッチ、およびテープに対して設定できます。	リスト
ホット	定期的に頻繁に使用されている、または容量のしきい値に達しているデバイス。	ブール値
注	リソースに関連付けるコメント。	テキスト（ Text ）

ラック	リソースが配置されているラック。	テキスト（ Text ）
部屋	ホスト、ストレージ、スイッチ、およびテープリソースが配置されている建物内の部屋。	リスト
SAN	ネットワークの論理パーティション。ホスト、ストレージアレイ、テープ、スイッチ、アプリケーションで使用できます。	リスト
サービスレベル	リソースに割り当てることができる一連のサポート対象サービスレベル。内部ボリューム、 qtree 、およびボリュームの番号付きのオプションのリストが用意されています。サービスレベルを編集して、各レベルのパフォーマンスポリシーを設定できます。	リスト
都道府県	リソースが配置されている都道府県。	リスト
日没	そのデバイスに新しい割り当てを実行できないしきい値。計画的な移行や保留中のネットワークの変更に役立ちます。	日付
スイッチレベル	スイッチのカテゴリを設定するための事前定義されたオプションが含まれています。通常、これらの指定はデバイスの寿命の間維持されますが、必要に応じて編集できます。スイッチに対してのみ設定できます。	リスト
階層	を使用すると、環境内のさまざまなサービスレベルを定義できます。階層では、必要な速度などのレベルを定義できます（例： Gold や Silver ）。この機能は、内部ボリューム、 qtree 、ストレージアレイ、ストレージプール、およびボリュームに対してのみ使用できます。	リスト

違反の重大度	違反（ホストポートの欠落や冗長性の欠如など）のランク（例：Major ）。重要度の高い順に階層化されています。	リスト

エイリアス、データセンター、ホット、サービスレベル、サンセット、 スイッチレベル、サービスレベル、階層、および違反の重大度はシステムレベルのアノテーションであり、削除や名前変更はできません。変更できるのは割り当てられている値のみです。

アノテーションの割り当て方法

アノテーションは、手動またはアノテーションルールを使用して自動で割り当てることができます。また、OnCommand Insight では、アセットの取得時と継承時に一部のアノテーションが自動的に割り当てられます。アセットに割り当てたアノテーションは、アセットページの[User Data]セクションに表示されます。

アノテーションは次の方法で割り当てられます。

- アセットにアノテーションを手動で割り当てることができます。

  アノテーションがアセットに直接割り当てられている場合、そのアノテーションはアセットページに通常のテキストとして表示されます。手動で割り当てたアノテーションは、継承またはアノテーションルールで割り当てられたアノテーションよりも常に優先されます。

- アノテーションルールを作成して、同じタイプのアセットにアノテーションを自動的に割り当てることができます。

  ルールに基づいてアノテーションが割り当てられている場合、Insightのアセットページのアノテーション名の横にルール名が表示されます。

- Insightでは、階層レベルがストレージ階層モデルに自動的に関連付けられるため、アセットを取得したときにリソースにストレージのアノテーションをすばやく割り当てることができます。

  特定のストレージリソースは、事前定義された階層（階層1と階層2）に自動的に関連付けられます。たとえば、Symmetrixストレージ階層はSymmetrixおよびVMAXファミリーに基づいており、階層1に関連付けられています。デフォルト値は、階層の要件に合わせて変更できます。Insightによって割り当てられたアノテーション（階層など）については、アセットページでアノテーションの名前にカーソルを合わせると「システム定義」と表示されます。

- 一部のリソース（アセットの子）では、事前定義された階層のアノテーションをアセット（親）から取得できます。

  たとえば、ストレージにアノテーションを割り当てた場合、そのストレージに属するすべてのストレージプール、内部ボリューム、ボリューム、qtree、および共有に階層のアノテーションが適用されます。ストレージの内部ボリュームに別のアノテーションを適用すると、それ以降はすべてのボリューム、qtree、および共有にアノテーションが適用されます。アセットページのアノテーション名の横に「データベース」と表示されます。

アノテーションにコストを関連付ける

コスト関連のレポートを実行する前に、システムレベルのService Level、Switch Level、およびTierのアノテーションにコストを関連付ける必要があります。これにより、本番環境での実際の使用状況やレプリケートされた容量に基づいて、ストレージユーザへのチャージバックが可能になります。たとえば、階層レベルとしてGoldとSilverを設定し、Gold階層にSilver階層よりも高いコストを割り当てることができます。

手順

1. InsightWeb UIにログインします。
2. [管理]をクリックし、*[アノテーション]*を選択します。

   [Annotation]ページが表示されます。
3. Service Level、Switch Level、またはTierのアノテーションにカーソルを合わせ、をクリックします 。

   [Edit Annotation]ダイアログボックスが表示されます。
4. [コスト]フィールドに既存のレベルの値を入力します。

   TierアノテーションにはAuto TierとService Levelアノテーションの値が設定されており、Object Storageの値は削除できません。
5. をクリックします

をクリックしてレベルを追加します。
6. 完了したら、*[保存]*をクリックします。

カスタムアノテーションの作成

アノテーションを使用すると、ビジネスニーズに合わせて、ビジネス固有のカスタムデータをアセットに追加できます。OnCommand Insight には一連のデフォルトアノテーションが用意されていますが、別の方法でデータを表示することもできます。カスタムアノテーションのデータは、スイッチのメーカー、ポートの数、パフォーマンス統計など、すでに収集されたデバイスの補足データになります。アノテーションを使用して追加したデータはInsightで検出されません。

手順

1. Insight Web UIにログインします。
2. をクリックし、[アノテーション]*を選択します。

   アノテーションページにアノテーションのリストが表示されます。
3. をクリックします

。

   [注釈の追加]*ダイアログボックスが表示されます。
4. * Name *および*概要 *フィールドに名前と概要 を入力します。

これらのフィールドには、 255 文字まで入力できます。

アノテーション名の先頭または末尾にドットが付いています。 はサポートされていません。

5. * タイプ * をクリックし、このアノテーションで使用できるデータのタイプを表す次のオプションのいずれかを選択します。

   - ブール値

     これにより、yesとnoの選択肢を含むドロップダウンリストが作成されますたとえば、"`DirectAttached""アノテーションはブール型です。

   - 日付

     これにより、日付を保持するフィールドが作成されます。たとえば、アノテーションで日付を指定する場合は、このオプションを選択します。

   - リスト

     これにより、次のいずれかが作成されます。

     - 固定のドロップダウンリスト

       このアノテーションタイプをデバイスに割り当てるときにユーザがリストに値を追加することはできません。

     - 可変のドロップダウンリスト

       このリストの作成時に*[Add new values on the fly]*オプションを選択した場合、他のユーザがこのアノテーションタイプをデバイスに割り当てているときに、リストに値を追加できます。

   - 番号

     これにより、アノテーションを割り当てるユーザが数値を入力できるフィールドが作成されます。たとえば、アノテーションタイプが「floor」の場合は、「Value Type」として「number」を選択してフロア番号を入力できます。

   - テキスト（ Text ）

     これにより、自由形式のテキストを使用できるフィールドが作成されます。たとえば、アノテーションタイプとして「Language」と入力し、値タイプとして「Text」を選択し、言語を値として入力します。

     タイプを設定して変更を保存したあとで、アノテーションのタイプを変更することはできません。タイプを変更する必要がある場合は、アノテーションを削除して新規に作成する必要があります。

6. 注釈タイプとして[***List**]を選択した場合は、次の手順を実行します。

   a. アセットページでアノテーションの値を追加して柔軟なリストを作成できるようにするには、「 * オンザフライで新しい値を追加」を選択します。

たとえば、アセットページで、 Detroit 、 Tampa 、および Boston の値が設定された City アノテーションをアセットに割り当てているとします。「 * オンザフライで新しい値を追加」オプションを選択した場合は、「アノテーション」ページに移動して値を追加する代わりに、アセットページでサンフランシスコやシカゴなどの都市に直接値を追加できます。このオプションを選択しないと、アノテーションの適用時に新しいアノテーション値を追加できません。これにより固定リストが作成されます。

b. 値と名前を*値*および*概要 *フィールドに入力します。

c. をクリックします

をクリックして値を追加します。

d. をクリックします 値を削除します。

7. [保存（ Save ）] をクリックします。

アノテーションがアノテーションページのリストに表示されます。

◦ 関連情報 *

"ユーザーデータのインポートとエクスポート"

アセットへのアノテーションの手動割り当て

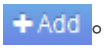
アセットにアノテーションを割り当てると、アセットをビジネスに関連付けてソート、グループ化、レポートするのに役立ちます。アノテーションルールを使用して特定のタイプのアセットにアノテーションを自動的に割り当てることができますが、アセットページで個 々 のアセットにアノテーションを割り当てることができます。

作業を開始する前に

割り当てるアノテーションを作成しておく必要があります。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法で、アノテーションを適用するアセットを選択します。
   ◦ [Assets Dashboard]でアセットをクリックします。
   ◦ をクリックします ツールバーの*[アセットの検索]*ボックスを表示するには、アセットのタイプまたは名前を入力し、表示されるリストからアセットを選択します。

   アセットページが表示されます。
3. アセットページの*[User Data]*セクションで、をクリックします 

。

[注釈の追加] ダイアログボックスが表示されます。
4. [注釈（Annotation）]*をクリックし、リストから注釈を選択します。
5. [値]*をクリックし、選択したアノテーションのタイプに応じて次のいずれかを実行します。
   ◦ アノテーションタイプがリスト、日付、またはブーリアンの場合は、値をリストから選択します。

◦ アノテーションタイプがテキストの場合は、値を入力します。

6. [保存（ Save ）] をクリックします。
7. アノテーションの割り当て後に値を変更する場合は、をクリックします 別の値を選択します。

   アノテーションのリストタイプで*[アノテーションの割り当て時に動的に値を追加する]*オプションが選択されている場合は、既存の値を選択するだけでなく、新しい値を入力して追加することもできます。

アノテーションの変更

アノテーションの名前、概要 、値を変更したり、不要になったアノテーションを削除したりできます。

手順

1. OnCommand InsightWeb UIにログインします。
2. をクリックし、[アノテーション]*を選択します。

   [アノテーション]ページが表示されます。

3. 編集するアノテーションにカーソルを合わせ、をクリックします 。

   [注釈の編集]*ダイアログボックスが表示されます。

4. アノテーションには次の変更を加えることができます。

   a. 名前、概要 、またはその両方を変更します。

      ただし、名前と概要 の最大文字数は255文字で、アノテーションのタイプを変更することはできません。また、システムレベルのアノテーションの場合、名前や概要 を変更することはできません。ただし、リストタイプのアノテーションの場合は値を追加または削除できます。

      Data Warehouseに公開されているカスタムアノテーションの名前を変更すると、履歴データが失われます。

   a. リストタイプのアノテーションに別の値を追加するには、をクリックします Add 。
   b. リストタイプのアノテーションから値を削除するには、をクリックします 。

      アノテーションルール、クエリ、またはパフォーマンスポリシーに含まれるアノテーションに関連付けられているアノテーション値は削除できません。

5. 完了したら、*[保存]*をクリックします。

完了後

Data Warehouseでアノテーションを使用する場合は、Data Warehouseでアノテーションを強制的に更新する必要があります。OnCommand Insight Data Warehouseアドミニストレーションガイド_を参照してください。

アノテーションを削除する

必要に応じて、不要になったアノテーションを削除できます。システムレベルのアノテーションや、アノテーションルール、クエリ、パフォーマンスポリシーで使用されているアノテーションは削除できません。

手順

1. OnCommand Insight Web UIにログインします。
2. をクリックし、[アノテーション]*を選択します。

   [アノテーション]ページが表示されます。

3. 削除するアノテーションにカーソルを合わせ、をクリックします 。

   確認の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。

アノテーションルールを使用してアセットにアノテーションを割り当てる

定義した条件に基づいてアセットにアノテーションを自動的に割り当てるには、アノテーションルールを設定します。OnCommand Insight は、これらのルールに基づいてアセットにアノテーションを割り当てます。Insightには、デフォルトのアノテーションルールも2つ用意されています。必要に応じて変更したり、不要な場合は削除したりできます。

デフォルトのストレージアノテーションルール

リソースにストレージのアノテーションを迅速に割り当てるために、OnCommand Insight には、ストレージ階層モデルに階層レベルを関連付ける21のデフォルトのアノテーションルールが用意されています。環境内の資産を取得すると、すべてのストレージリソースが自動的に階層に関連付けられます。

デフォルトのアノテーションルールでは、階層のアノテーションが次のように適用されます。

- 階層1のストレージ品質

  階層1のアノテーションが適用されるベンダーと指定ファミリーは次のとおりです。EMC（Symmetrix）、HDS（HDS9500V、HDS9900、HDS9900V、R600、 R700、USP r、USP V）、IBM（DS8000）、NetApp（FAS6000またはFAS6200）、およびViolin（メモリ）。

- 階層2、ストレージ品質の階層

  階層2のアノテーションが適用されるベンダーと指定ファミリーは、HP（3PAR StoreServまたはEVA）、EMC（CLARiX）、HDS（AMSまたはD800）、IBM（XIV）、NetApp（FAS3000、FAS3100、FAS3200）です。

これらのルールのデフォルト設定は階層の要件に合わせて編集することも、不要な場合は削除することもでき

ます。

アノテーションルールの作成

アノテーションを個々のアセットに手動で適用する代わりに、アノテーションルールを使用して複数のアセットに自動的にアノテーションを適用することができます。個々のアセットページで手動で設定したアノテーションは、 Insight でアノテーションルールが評価されるときにルールベースのアノテーションよりも優先されます。

作業を開始する前に

アノテーションルールのクエリを作成しておく必要があります。

このタスクについて

アノテーションタイプはルールの作成中に編集することもできますが、事前に定義しておくことを推奨します。

手順

1. OnCommand Insight Web UIにログインします。
2. をクリックし、[アノテーションルール]*を選択します。

   アノテーションルールページに、既存のアノテーションルールのリストが表示されます。
3. をクリックします

。

   [Add Rule]ダイアログボックスが表示されます。
4. 次の手順を実行します。
   a. [* 名前 *] ボックスに、ルールを説明する一意の名前を入力します。

      この名前はアノテーションルールページに表示されます。
   b. [クエリ]*をクリックし、アセットにアノテーションを適用する際にOnCommand Insight で使用するクエリを選択します。
   c. [* Annotation*] をクリックし、適用する注釈を選択します。
   d. * 値 * をクリックし、アノテーションの値を選択します。

      たとえば、 Birthday のアノテーションを選択した場合は、日付の値を指定します。
5. [保存（ Save ）] をクリックします。
6. すべてのルールをすぐに実行する場合は、 * すべてのルールを実行 * をクリックします。それ以外の場合、ルールは定期的に実行されます。

アノテーションルールの優先順位を設定します

アノテーションルールはデフォルトでOnCommand Insight は順番に評価されますが、ア

ノテーションルールが特定の順序で評価されるようにOnCommand Insight での評価順序を設定することができます。

手順

1. InsightWeb UIにログインします。
2. をクリックし、[アノテーションルール]*を選択します。

   アノテーションルールページに、既存のアノテーションルールのリストが表示されます。

3. アノテーションルールにカーソルを合わせます。

   優先順位の矢印がルールの右側に表示されます。

4. リスト内でルールを上下に移動するには、上矢印または下矢印をクリックします。

   デフォルトでは、新しいルールはルールのリストに順番に追加されます。個々のアセットページで手動で設定したアノテーションは、 Insight でアノテーションルールが評価されるときにルールベースのアノテーションよりも優先されます。

アノテーションルールの変更

アノテーションルールについて、ルールの名前、そのアノテーション、アノテーションの値、ルールに関連付けられているクエリを変更することができます。

手順

1. OnCommand InsightWeb UIにログインします。
2. をクリックし、[アノテーションルール]*を選択します。

   アノテーションルールページに、既存のアノテーションルールのリストが表示されます。

3. 変更するルールを選択します。
   - [Annotation Rules]ページでは、フィルタボックスに値を入力してアノテーションルールをフィルタできます。
   - アノテーションルールがページに収まらない場合は、ページ番号をクリックしてページごとに参照できます。
4. 次のいずれかを実行して、*[ルールの編集]*ダイアログボックスを表示します。
   - [Annotation Rules]ページが表示された場合は、アノテーションルールにカーソルを合わせ、をクリックします 。
   - アセットページで、ルールに関連付けられているアノテーションにカーソルを合わせ、ルール名が表示されたらその名前にカーソルを合わせて、ルール名をクリックします。
5. 必要な変更を行い、*[保存]*をクリックします。

アノテーションルールを削除する

ネットワーク内のオブジェクトの監視に使用していたアノテーションルールが不要にな

った場合は、削除できます。

手順

1. OnCommand InsightWeb UIにログインします。
2. をクリックし、[アノテーションルール]*を選択します。

   アノテーションルールページに、既存のアノテーションルールのリストが表示されます。

3. 削除するルールを選択します。
   - [Annotation Rules]ページでは、フィルタボックスに値を入力してアノテーションルールをフィルタできます。
   - アノテーションルールが1ページに収まらない場合は、ページ番号をクリックしてページごとに参照できます。
4. 削除するルールにカーソルを合わせ、をクリックします 。

   ルールを削除するかどうかを確認するメッセージが表示されます。

5. [OK] をクリックします。

アノテーション値のインポート

SANオブジェクト（ストレージ、ホスト、仮想マシンなど）のアノテーションをCSVファイルで管理している場合は、その情報をOnCommand Insight にインポートできます。アプリケーション、ビジネスエンティティ、アノテーション（階層や建物など）をインポートできます。

このタスクについて

次のルールが適用されます。

- アノテーション値が空の場合、そのアノテーションはオブジェクトから削除されます。
- ボリュームまたは内部ボリュームをアノテートする場合、オブジェクト名はストレージ名とボリューム名をダッシュと矢印（->）で区切った形式になります。

  ```
  <storage_name>-><volume_name>
  ```

- ストレージ、スイッチ、またはポートがアノテートされている場合、[Application]列は無視されます。
- ビジネスエンティティは、[Tenant]、[Line_of_Business]、[Business_Unit]、および[Project]の列で構成されます。

  いずれの値も空のままにすることができます。アプリケーションがすでに入力値とは異なるビジネスエンティティに関連付けられている場合は、新しいビジネスエンティティに割り当てられます。

インポートユーティリティでは、次のオブジェクトタイプとキーがサポートされます。

を入力します	キーを押します
ホスト	id-><id> または <Name> または <IP>
VM	id-><id> または <Name>
ストレージプール	id-><id> または <Storage_name>-><Storage_Pool_name>
内部ボリューム	id-><id> または <Storage_name>-><Internal_volume_name>
ボリューム	id-><id> または <Storage_name>-><Volume_name>
ストレージ	id-><id> または <Name> または <IP>
スイッチ	id-><id> または <Name> または <IP>
ポート	id-><id> または <WWN>
共有	id-><id> または <Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol> <Qtree> は、デフォルトのqtreeがある場合は省略可能です。
qtree	id-><id> または <Storage Name>-><Internal Volume Name>-><Qtree Name>

CSVファイルの形式は次のとおりです。

```
, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]
```

手順

1. Insight Web UIにログインします。
2. をクリックし、[トラブルシューティング]*を選択します。

   [トラブルシューティング]ページが表示されます。

3. ページの*[その他のタスク]セクション*で、* OnCommand Insight Portal*リンクをクリックします。
4. [Insight Connect API]*をクリックします。
5. ポータルにログインします。
6. [Annotation Import Utility]*をクリックします。
7. を保存します `.zip` ファイルを解凍し、を読んでください `readme.txt` 追加情報 およびサンプル用のファイル。
8. CSVファイルをと同じフォルダに配置します `.zip` ファイル。
9. コマンドラインウィンドウで、次のように入力します。

```
java -jar rest-import-utility.jar [-uusername] [-ppassword]
[-aserver name or IP address] [-bbatch size] [-ccase
sensitive:true/false]
[-lextra logging:true/false] csv filename
```

追加のロギングを有効にする-lオプションと、大文字と小文字を区別する-cオプションは、デフォルトでfalseに設定されます。したがって、これらの機能を使用する場合にのみ指定する必要があります。

オプションとその値の間にスペースはありません。

次のキーワードは予約されており、ユーザはこれらのキーワードをアノテーション名として指定できません。-Application-Application_Priority -Tenant-Line_of_Business -Business_Unit -Projectいずれかの予約済みキーワードを使用してアノテーションタイプをインポートしようとすると、エラーが生成されます。アノテーションの名前にこれらのキーワードを使用している場合は、インポートユーティリティツールが正常に動作するように変更する必要があります。

Annotation ImportユーティリティにはJava 8またはJava 11が必要です。インポートユーティリティを実行する前に、これらのいずれかがインストールされていることを確認してください。最新のOpenJDK 11を使用することを推奨します。

クエリを使用して複数のアセットにアノテーションを割り当てる

アセットのグループにアノテーションを割り当てると、それらのアセットを識別しやすくなり、クエリやダッシュボードでそれらの関連するアセットを使用しやすくなります。

作業を開始する前に

アセットに割り当てるアノテーションは、事前に作成しておく必要があります。

このタスクについて

クエリを使用すると、アノテーションを複数のアセットに簡単に割り当てることができます。たとえば、カスタムのアドレスアノテーションをデータセンターの特定の場所にあるすべてのアレイに割り当てる場合などです。

手順

1. アノテーションを割り当てるアセットを特定するための新しいクエリを作成します。**>+**[新しいクエリ]*をクリックします。
2. ドロップダウンで[ストレージ]*を選択します。フィルタを設定して、表示されるストレージのリストをさらに絞り込むことができます。
3. 表示されたストレージのリストで、ストレージ名の横にあるチェックボックスをクリックして1つ以上を選択します。リストの上部にあるメインのチェックボックスをクリックして、表示されているすべてのストレージを選択することもできます。
4. 必要なストレージをすべて選択したら、**[**操作**]**>*[アノテーションの編集]*をクリックします。

   [Add Annotation]ダイアログボックスが表示されます。

5. ストレージに割り当てる*と[値]を選択し、[保存]*をクリックします。

   そのアノテーションの列が表示されている場合は、選択したすべてのストレージで列が表示されます。

6. アノテーションを使用して、ウィジェットやクエリでストレージをフィルタリングできるようになりました。ウィジェットでは、次の操作を実行できます。

   a. ダッシュボードを作成するか、既存のダッシュボードを開きます。[Variable]*を追加し、上記のストレージで設定したアノテーションを選択します。変数がダッシュボードに追加されます。

   b. 追加した変数フィールドで、* any *をクリックして、フィルタするための適切な値を入力します。チェックマークをクリックして変数値を保存します。

   c. ウィジェットを追加します。ウィジェットの[Query]で、[**Filter by][+**]ボタンをクリックし、リストから適切な注釈を選択します。

   d. [Any]*をクリックし、上記で追加したアノテーション変数を選択します。作成した変数は"$`"で始まり、ドロップダウンに表示されます。

   e. 必要に応じて他のフィルタやフィールドを設定し、ウィジェットがカスタマイズされたら*[保存]*をクリックします。

   ダッシュボードのウィジェットには、アノテーションを割り当てたストレージのデータのみが表示されます。

アセットを照会しています

クエリを使用すると、環境内のアセットをユーザが選択した条件（アノテーションとパフォーマンス指標）に基づいてきめ細かく検索することで、ネットワークの監視とトラ

ブルシューティングを行うことができます。また、アセットにアノテーションを自動的に割り当てるアノテーションルールにはクエリが必要です。

クエリやダッシュボードで使用されるアセット

Insightのクエリとダッシュボードウィジェットは、さまざまなアセットタイプで使用できます

クエリ、ダッシュボードウィジェット、およびカスタムアセットページで使用できるアセットタイプは次のとおりです。フィルタ、式、表示に使用できるフィールドとカウンタは、アセットのタイプによって異なります。すべてのアセットをすべてのウィジェットタイプで使用できるわけではありません。

- アプリケーション
- データストア
- ディスク
- ファブリック
- 汎用デバイス
- ホスト
- 内部ボリューム
- iSCSI セッション
- iSCSI ネットワークポータル
- パス
- ポート
- qtree
- クォータ
- 共有
- ストレージ
- ストレージノード
- ストレージプール
- スイッチ
- テープ
- VMDK です
- 仮想マシン
- ボリューム
- ゾーン
- ゾーンメンバー

クエリを作成しています

クエリを作成して、環境内のアセットをきめ細かく検索することができます。クエリを使用すると、フィルタを追加して結果をソートし、インベントリデータとパフォーマンスデータを1つのビューに表示することで、データをスライスできます。

このタスクについて

たとえば、ボリュームのクエリを作成したり、選択したボリュームに関連付けられているストレージを検索するフィルタを追加したり、階層1などの特定のアノテーションを検索するフィルタを追加したりできます。 最後に、IOPS - Read（IO/秒）が25を超えるストレージをすべて検出するフィルタをもう1つ追加します。結果が表示されたら、クエリに関連付けられている各列で情報を昇順または降順にソートすることができます。

アセットを取得する新しいデータソースを追加したときや、アノテーションやアプリケーションの割り当てを行ったときに、クエリのインデックスが作成されたあとに、それらのアセット、アノテーション、またはアプリケーションを照会することができます。インデックスは定期的な間隔で作成されます。

手順

1. OnCommand Insight Web UIにログインします。
2. をクリックし、[+ New Query]*を選択します。
3. [リソースタイプの選択]*をクリックし、アセットのタイプを選択します。

   クエリでリソースを選択すると、いくつかのデフォルト列が自動的に表示されます。これらの列はいつでも削除したり、新しい列を追加したりできます。

4. [名前*]テキストボックスにアセットの名前を入力するか、テキストの一部を入力してアセット名を絞り込みます。

   [New Query]ページのテキストボックスでは、次のいずれかを単独で使用することも、組み合わせて使用することもできます。

   - アスタリスクを使用すると、すべての項目を検索できます。例： `vol*rhel` 「vol」で始まり「rhel」で終わるすべてのリソースを表示します。
   - 疑問符を使用すると、特定の数の文字を検索できます。例： `BOS-PRD??-S12` BOS-PRD12-S12 、BOS-PRD13-S12などを表示します。
   - OR 演算子を使用すると、複数のエンティティを指定できます。例： `FAS2240 OR CX600 OR FAS3270` 複数のストレージモデルを検出します。
   - NOT 演算子を使用すると、検索結果からテキストを除外できます。例： `NOT EMC*` 「EMC」で始まらないものをすべて検索します。を使用できます `NOT *` 値のないフィールドを表示します。
5. をクリックします をクリックしてアセットを表示します。
6. 条件を追加するには、をクリックします

をクリックし、次のいずれかを実行します。

   - と入力して特定の条件を検索し、選択します。
   - リストを下にスクロールし、条件を選択します。
   - IOPS -読み取り（IO/秒）などのパフォーマンス指標を選択した場合は、値の範囲を入力しま

す。Insightのデフォルトのアノテーションはで示されます ;重複する名前を持つ注釈を持つことができます。

条件の列が[クエリ結果]リストに追加され、リスト内のクエリの結果が更新されます。

7. 必要に応じて、をクリックします をクリックして、クエリ結果からアノテーションまたはパフォーマンス指標を削除します。

   たとえば、データストアの最大レイテンシと最大スループットを表示するクエリで結果のリストに最大レイテンシのみを表示する場合は、このボタンをクリックし、* Throughput - Max *チェックボックスをオフにします。[Query results]のリストから[Throughput - Max（MB/s）]列が削除されます。

   クエリ結果テーブルに表示される列の数によっては、追加された列を表示できない場合があります。目的の列が表示されるまで、1つまたは複数の列を削除できます。

8. をクリックし、クエリの名前を入力して[保存]*をもう一度クリックします。

   管理者ロールを持つアカウントがある場合は、カスタムダッシュボードを作成できます。カスタムダッシュボードはウィジェットライブラリの任意のウィジェットで構成でき、そのいくつかを使用してクエリ結果をカスタムダッシュボードに表示できます。カスタムダッシュボードの詳細については、_ OnCommand Insight スタートガイド_を参照してください。

   ◦ 関連情報 *

"ユーザーデータのインポートとエクスポート"

クエリを表示する

アセットの監視に使用するクエリを表示して、アセットに関するデータの表示方法を変更できます。

手順

1. OnCommand Insight Web UIにログインします。
2. [* クエリ *] をクリックし、 [* すべてのクエリを表示 *] を選択します。
3. クエリの表示方法は次のいずれかの方法で変更できます。
   ◦ [**filter**]ボックスにテキストを入力して、特定のクエリを表示できます。
   ◦ 列見出しで矢印をクリックすると、クエリの表内の列のソート順序を昇順（上矢印）または降順（下矢印）に変更できます。
   ◦ 列のサイズを変更するには、列見出しの上にカーソルを合わせ、青いバーが表示されるまで動かします。バーの上にマウスを置き、左右にドラッグします。
   ◦ 列を移動するには、列ヘッダーをクリックし、左右にドラッグします。
   ◦ クエリ結果をスクロールすると、Insightでデータソースが自動的にポーリングされるため、結果が変わる場合があります。これにより、一部の項目が表示されなくなったり、ソート方法によっては一部の項目が順序どおりに表示されない場合があります。

クエリの結果を.csvファイルにエクスポートして、データを別のアプリケーションにインポートできます。

手順

1. OnCommand Insight Web UIにログインします。
2. [* クエリ *] をクリックし、 [* すべてのクエリを表示 *] を選択します。

   [クエリ] ページが表示されます。

3. クエリをクリックします。
4. をクリックします クエリ結果をにエクスポートします `.csv` ファイル。
5. 次のいずれかを実行します。

   - [名前を付けて開く] をクリックし、次に **OK** をクリックして Microsoft Excel でファイルを開き、特定の場所にファイルを保存します。
   - [ファイルの保存] をクリックし、 [OK] をクリックして、 [ダウンロード] フォルダにファイルを保存します。表示されている列の属性のみがエクスポートされます。表示されている一部の列、特に複雑なネストされたリレーションシップの一部である列はエクスポートされません。

     アセット名にカンマが含まれている場合は、アセット名と適切な.csv形式は維持され、エクスポート時に名前が引用符で囲まれます。

     +クエリ結果をエクスポートする場合、選択または画面に表示されている行だけでなく、結果テーブルのすべての*行がエクスポートされることに注意してください。最大10,000行までエクスポートされます。

     [+]

エクスポートした .csv ファイルを Excel で開くときに、オブジェクト名またはその他のフィールドが NN:NN の形式である場合 (2 桁の数字の後にコロン、 2 桁の数字が続く) 、 Excel ではその名前がテキスト形式ではなく Time 形式であると解釈されることがあります。その結果、 Excel の列に誤った値が表示されることがあります。たとえば、「 81 ： 45 」という名前のオブジェクトは、 Excel では「 81 ： 45 ： 00 」と表示されます。これを回避するには、次の手順に従って .csv を Excel にインポートします。

[+]

```
-   Open a new sheet in Excel.
-   On the "Data" tab, choose "From Text".
-   Locate the desired .CSV file and click "Import".
-   In the Import wizard, choose "Delimited" and click Next.
-   Choose "Comma" for the delimiter and click Next.
-   Select the desired columns and choose "Text" for the
column data format.
-   Click Finish.
Your objects should show in Excel in the proper format.
```

[+]

クエリの変更

クエリに関連付けられている条件を変更して、アセットの検索条件を変更することができます。

手順

1. InsightWeb UIにログインします。
2. [* クエリ *] をクリックし、 [* すべてのクエリを表示 *] を選択します。

   [クエリ] ページが表示されます。
3. クエリ名をクリックします。
4. クエリから条件を削除するには、をクリックします 。
5. クエリに条件を追加するには、をクリックします More をクリックし、リストから条件を選択します。
6. 次のいずれかを実行します。
   - [保存]*をクリックして、最初に使用した名前でクエリを保存します。
   - [名前を付けて保存]*をクリックして、クエリを別の名前で保存します。
   - 最初に使用したクエリ名を変更するには、*[名前の変更]*をクリックします。
   - クエリ名を最初に使用した名前に戻すには、*[元に戻す]*をクリックします。

クエリの削除

アセットに関する有用な情報が収集されなくなったクエリを削除できます。アノテーションルールで使用されているクエリは削除できません。

手順

1. InsightWeb UIにログインします。
2. [* クエリ *] をクリックし、 [* すべてのクエリを表示 *] を選択します。

   [クエリ] ページが表示されます。

3. 削除するクエリにカーソルを合わせ、をクリックします 。

   クエリを削除するかどうかを確認する確認メッセージが表示されます。

4. [OK] をクリックします。

アセットに対する複数のアプリケーションの割り当てと削除

アセットに対して複数のアプリケーションを割り当てたりアセットから削除したりするには、クエリを使用します。手動でアプリケーションを割り当てたり削除したりする必要はありません。

作業を開始する前に

編集するすべてのアセットを検索するクエリを作成しておく必要があります。

手順

1. [* クエリ *] をクリックし、 [* すべてのクエリを表示 *] を選択します。

   [クエリ] ページが表示されます。

2. アセットを検索するクエリの名前をクリックします。

   クエリに関連付けられているアセットのリストが表示されます。

3. リストから目的のアセットを選択するか、をクリックします をクリックして*すべて*を選択します。

   [アクション]*ボタンが表示されます。

4. 選択したアセットにアプリケーションを追加するには、をクリックします Actions をクリックし、*[アプリケーションの編集]*を選択します。
   a. [アプリケーション]*をクリックし、1つ以上のアプリケーションを選択します。

      ホスト、内部ボリューム、および仮想マシンに対しては複数のアプリケーションを選択できますが、ボリュームに対して選択できるアプリケーションは1つだけです。

b. [保存（ Save ）] をクリックします。

5. アセットに割り当てられているアプリケーションを削除するには、をクリックします Actions をクリックし、 [アプリケーションの削除] を選択します。

   a. 削除する 1 つ以上のアプリケーションを選択します。

   b. [削除（ Delete ）] をクリックします。

   新しく割り当てたアプリケーションは、別のアセットから派生したアプリケーションよりも優先されます。たとえば、ホストから継承したアプリケーションがあるボリュームに新しいアプリケーションを割り当てた場合、派生したアプリケーションよりも新しいアプリケーションが優先されます。

アセットの複数のアノテーションの編集または削除

アセットの複数のアノテーションを編集したりアセットから削除したりするには、手動で編集または削除しなくても、クエリを使用します。

作業を開始する前に

編集するすべてのアセットを検索するクエリを作成しておく必要があります。

手順

1. [* クエリ *] をクリックし、 [* すべてのクエリを表示 *] を選択します。

   [クエリ] ページが表示されます。

2. アセットを検索するクエリの名前をクリックします。

   クエリに関連付けられているアセットのリストが表示されます。

3. リストから目的のアセットを選択するか、をクリックします ☐ をクリックして*すべて*を選択します。

   [アクション]*ボタンが表示されます。

4. アセットにアノテーションを追加したり、アセットに割り当てられているアノテーションの値を編集したりするには、をクリックします Actions をクリックし、*[アノテーションの編集]*を選択します。

   a. [アノテーション]*をクリックし、値を変更するアノテーションを選択するか、すべてのアセットに割り当てる新しいアノテーションを選択します。

   b. * 値 * をクリックし、アノテーションの値を選択します。

   c. [保存（ Save ）] をクリックします。

5. アセットに割り当てられているアノテーションを削除するには、をクリックします Actions をクリックし、*[Remove Annotation]*を選択します。

   a. [アノテーション]*をクリックし、アセットから削除するアノテーションを選択します。

   b. [削除（ Delete ）] をクリックします。

テーブル値をコピーしています

テーブル内の値をコピーして、検索ボックスやその他のアプリケーションで使用できます。

このタスクについて

テーブルまたはクエリ結果から値をコピーするには、2つの方法があります。

手順

1. 方法 1: マウスで目的のテキストを強調表示し、コピーして、検索フィールドやその他のアプリケーションに貼り付けます。
2. 方法2:長さが省略記号(…)で示されるテーブル列の幅を超える単一値フィールドの場合は、フィールドの上にカーソルを置き、クリップボードアイコンをクリックします。値は、検索フィールドやその他のアプリケーションで使用するためにクリップボードにコピーされます。

   コピーできるのは、アセットへのリンクである値のみです。また、単一の値（リスト以外）を含むフィールドのみにコピーアイコンが表示されます。

パフォーマンスポリシーの管理

OnCommand Insight では、パフォーマンスポリシーを作成して、さまざまなしきい値に基づいてネットワークを監視し、それらのしきい値を超えたときにアラートを生成することができます。パフォーマンスポリシーを使用すると、しきい値の違反を即座に検出してその影響を特定し、問題の影響と根本原因 を分析して迅速かつ効果的に対処できます。

パフォーマンスポリシーを使用すると、任意のオブジェクト（データストア、ディスク、ハイパーバイザー、内部ボリューム、ポート、 ストレージ、ストレージノード、ストレージプール、VMDK、仮想マシン、とvolume）を使用し、パフォーマンスカウンタ（合計IOPSなど）が報告されていることを確認します。しきい値の違反が発生すると、Insightによって検出され、関連するアセットページに赤い丸で表示されます。設定されている場合はEメールで通知されるほか、[Violations Dashboard]や違反を報告するカスタムダッシュボードにも表示されます。

Insightには、次のオブジェクトに対するデフォルトのパフォーマンスポリシーがいくつか用意されています。これらのポリシーは、環境に応じて変更または削除できます。

- ハイパーバイザー

  ESXスワッピングとESX利用に関するポリシーが用意されています。

- 内部ボリュームとボリューム

  リソースごとに2つのレイテンシポリシーがあり、1つはティア1用にアノテートされ、もう1つはティア2用にアノテートされます。

- ポート

  BBクレジットゼロのポリシーがあります。

- ストレージノード

  ノード利用率に関するポリシーが用意されています。

- 仮想マシン

  VMスワッピングとESXのCPUおよびメモリに関するポリシーが用意されています。

- ボリューム

  階層別およびミスアライメントされたボリュームポリシー別のレイテンシがあります。

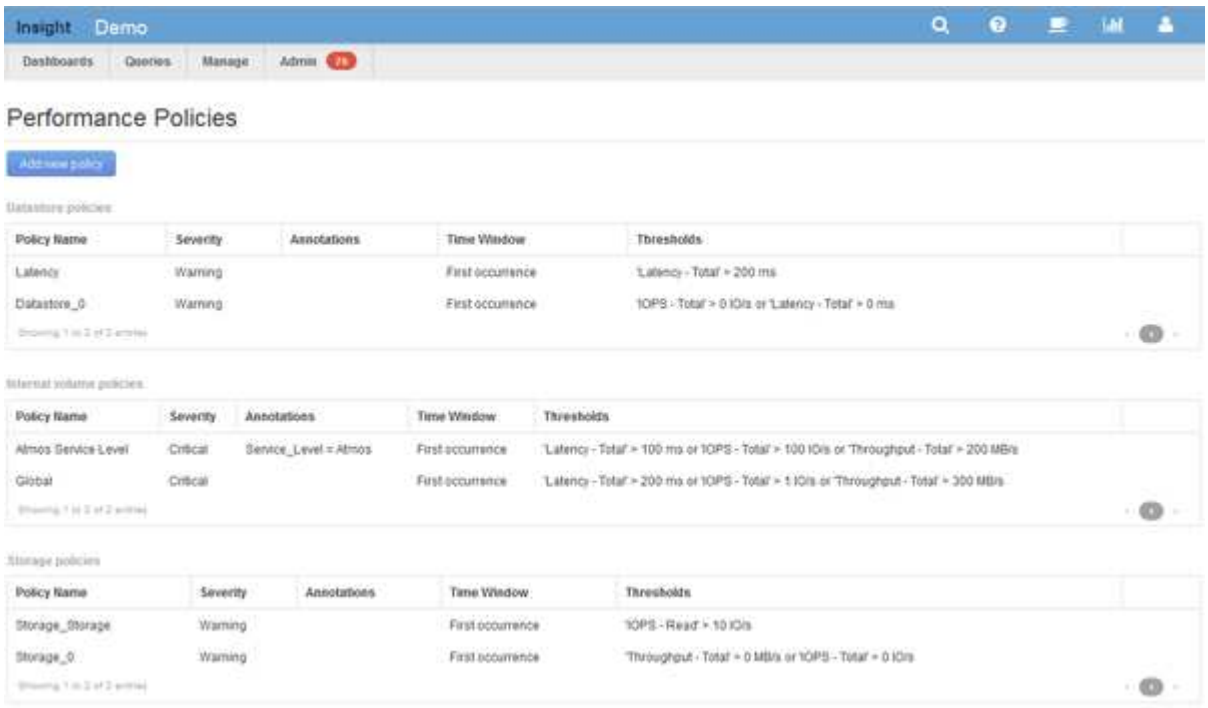
パフォーマンスポリシーの作成

パフォーマンスポリシーを作成して、ネットワーク内のリソースに関連する問題についてユーザに通知するアラートをトリガーするしきい値を設定します。たとえば、ストレージプールの合計使用率が 60% を超えたときにアラートをトリガーするパフォーマンスポリシーを作成できます。

手順

1. ブラウザでOnCommand Insight を開きます。
2. >[パフォーマンスポリシー]*を選択します。

   パフォーマンスポリシーページが表示されま



す。

   ポリシーはオブジェクト別に編成され、そのオブジェクトのリストに表示される順序で評価されます。

3. [新しいポリシーの追加]*をクリックします。

   [Add Policy]ダイアログボックスが表示されます。

4. [ポリシー名]*フィールドに、ポリシーの名前を入力します。

   オブジェクトの他のすべてのポリシーとは異なる名前を使用する必要があります。たとえば、「Latency」という名前の2つのポリシーを内部ボリュームに使用することはできませんが、内部ボリュームには「Latency」ポリシーを使用し、別のボリュームには「Latency」ポリシーを使用できます。ベストプラクティスとしては、オブジェクトタイプに関係なく、すべてのポリシーに一意の名前を常に使用することを推奨します。

5. [タイプのオブジェクトに適用]*リストから、ポリシーを適用するオブジェクトのタイプを選択します。
6. [アノテーションあり]*リストで、必要に応じてアノテーションタイプを選択し、[値]*ボックスにアノテーションの値を入力して、この特定のアノテーションが設定されたオブジェクトにのみポリシーを適用します。
7. オブジェクトタイプとして* Port を選択した場合は、 Connected to *リストからポートの接続先を選択します。
8. [Apply after a window of *]リストで、しきい値違反を示すアラートが生成されるタイミングを選択します。

   [First occurrence]オプションを指定すると、最初のデータサンプルでしきい値を超えたときにアラートがトリガーされます。それ以外のオプションでは、しきい値を超えたあと、その状態のまま一定の時間を経過した時点でアラートがトリガーされます。

9. [* with severity*] リストから、違反の重大度を選択します。
10. デフォルトでは、ポリシー違反に関するEメールアラートはグローバルEメールリストの受信者に送信されます。この設定を上書きして、特定のポリシーのアラートを特定の受信者に送信するように設定することができます。
    - リンクをクリックして受信者リストを開き、*+*ボタンをクリックして受信者を追加します。このポリシーの違反アラートは、リスト内のすべての受信者に送信されます。
11. アラートのトリガー方法を制御するには、* Create alert if any of the following are true セクションの any * リンクをクリックします。
    - 任意

      デフォルトの設定です。ポリシーに関連するいずれかのしきい値を超えたときにアラートが作成されます。

    - すべて

      ポリシーのすべてのしきい値を超えたときにアラートが作成されます。[すべて]*を選択すると、パフォーマンスポリシーに対して最初に作成するしきい値がプライマリルールと呼ばれます。プライマリルールのしきい値は、そのパフォーマンスポリシーで最も考慮する違反にする必要があります。

12. Create alert if * セクションで、パフォーマンスカウンタとオペレータを選択し、値を入力してしきい値を作成します。
13. しきい値を追加するには、*[Add threshold]*をクリックします。
14. しきい値を削除するには、ごみ箱アイコンをクリックします。
15. アラートが発生したときにポリシーの処理を停止するには、*[アラートが生成された場合に追加のポリシーを停止する]*チェックボックスをオンにします。

    たとえば、データストアのポリシーが4つあり、アラートが発生したときに処理を停止するように2つ目の

ポリシーが設定されている場合、2つ目のポリシーの違反がアクティブな間は3つ目と4つ目のポリシーは処理されません。

16. [保存（ Save ）] をクリックします。

    [パフォーマンスポリシー]ページが表示され、オブジェクトタイプのポリシーのリストにパフォーマンスポリシーが表示されます。

パフォーマンスポリシーの評価順序

[パフォーマンスポリシー]ページでは、オブジェクトタイプ別にポリシーがグループ化され、オブジェクトのパフォーマンスポリシーのリストに表示される順序でポリシーが評価されます。ネットワークで最も重要な情報を表示するために、Insightでポリシーが評価される順序を変更することができます。

Insightでは、オブジェクトのパフォーマンスデータのサンプルがシステムに取り込まれると、そのオブジェクトに該当するすべてのポリシーが順番に評価されます。ただし、アノテーションによっては、すべてのポリシーが1つのオブジェクトグループに適用されるわけではありません。たとえば、内部ボリュームに次のポリシーが設定されているとします。

- ポリシー1（Insightが提供するデフォルトポリシー）
- ポリシー2（アノテーション「`Service Level=Silver`」、*[Stop processing further policies if alert is generated]*オプションが指定
- ポリシー3（アノテーション「`Service Level=Gold」）
- ポリシー4.

アノテーションがGoldの内部ボリューム階層の場合、Insightではポリシー1が評価され、ポリシー2は無視されてからポリシー3とポリシー4が評価されます。階層にアノテーションが設定されていない場合は、ポリシーの順序に従って評価されます。そのため、ポリシー1とポリシー4のみが評価されます。Silverのアノテーションが設定された内部ボリューム階層については、ポリシー1とポリシー2が評価されます。 ただし、ポリシーのしきい値を1回超えたときにアラートがトリガーされ、ポリシーで指定された時間内にそのポリシーを超えると、リスト内の他のポリシーは評価されず、オブジェクトの現在のカウンタが評価されます。Insightでオブジェクトの次のパフォーマンスサンプルのセットがキャプチャされると、フィルタと順序に基づいてオブジェクトのパフォーマンスポリシーの評価が再開されます。

パフォーマンスポリシーの優先順位の変更

デフォルトでは、オブジェクトのポリシーは順番に評価されます。Insightでのパフォーマンスポリシーの評価順序を設定できます。たとえば、Gold Tierのストレージで違反が発生したときに処理を停止するように設定されたポリシーがある場合は、そのポリシーをリストの先頭に配置して、同じストレージアセットに対する一般的な違反が表示されないようにすることができます。

手順

1. ブラウザでInsightを開きます。
2. メニューから[パフォーマンスポリシー]*を選択します。

[パフォーマンスポリシー]ページが表示されます。

3. オブジェクトタイプのパフォーマンスポリシーのリストでポリシー名にカーソルを合わせます。

   優先順位の矢印がポリシーの右側に表示されます。

4. リスト内でポリシーを上に移動するには、上矢印をクリックします。リスト内でポリシーを下に移動するには、下矢印をクリックします。

   デフォルトでは、新しいポリシーはオブジェクトのポリシーリストに順番に追加されます。

パフォーマンスポリシーの編集

既存のパフォーマンスポリシーとデフォルトのパフォーマンスポリシーを編集して、ネットワーク内の関心のある状況をInsightで監視する方法を変更することができます。たとえば、ポリシーのしきい値を変更できます。

手順

1. ブラウザでInsightを開きます。
2. メニューから[パフォーマンスポリシー]*を選択します。

   [パフォーマンスポリシー]ページが表示されます。

3. オブジェクトのパフォーマンスポリシーのリストでポリシー名にカーソルを合わせます。
4. をクリックします 。

   [Edit Policy]ダイアログボックスが表示されます。

5. 必要な変更を行います。

   ポリシー名以外のオプションを変更すると、そのポリシーに対する既存の違反がすべて削除されます。

6. [保存]*をクリックします

パフォーマンスポリシーを削除しています

ネットワーク内のオブジェクトの監視にパフォーマンスポリシーが適用されなくなった場合は、そのポリシーを削除することができます。

手順

1. ブラウザでInsightを開きます。
2. メニューから[パフォーマンスポリシー]*を選択します。

   [パフォーマンスポリシー]ページが表示されます。

3. オブジェクトのパフォーマンスポリシーのリストでポリシーの名前にカーソルを合わせます。
4. をクリックします 。

ポリシーを削除するかどうかを確認するメッセージが表示されます。

5. [OK] をクリックします。

ユーザーデータのインポートとエクスポート

インポートとエクスポートの機能では、アノテーション、アノテーションルール、クエリ、パフォーマンスポリシー、カスタムダッシュボードを1つのファイルにエクスポートできます。このファイルは、別のOnCommand Insight サーバにインポートできます。

エクスポートおよびインポート機能は、同じバージョンのOnCommand Insight を実行しているサーバ間でのみサポートされます。

ユーザーデータをエクスポートまたはインポートするには、* Admin をクリックして Setup を選択し、Import/Export user data *タブを選択します。

インポート処理では、インポートするオブジェクトとオブジェクトタイプに応じて、データの追加、マージ、または置換が行われます。

- アノテーションタイプ
  - 同じ名前のアノテーションがターゲットシステムにない場合、アノテーションが追加されます。
  - 同じ名前のアノテーションがターゲットシステムにある場合、アノテーションタイプがリストであれば、アノテーションがマージされます。
  - 同じ名前のアノテーションがターゲットシステムにある場合、アノテーションタイプがリスト以外であれば、アノテーションが置き換えられます。

  名前が同じでタイプが異なるアノテーションがターゲットシステムにあると、インポートは失敗します。失敗したアノテーションにオブジェクトが依存している場合、誤った情報や不要な情報が表示されることがあります。インポート処理の完了後、すべてのアノテーションの依存関係を確認してください。

- アノテーションルール
  - 同じ名前のアノテーションルールがターゲットシステムにない場合は、アノテーションルールが追加されます。
  - 同じ名前のアノテーションルールがターゲットシステムにある場合、アノテーションルールが置き換えられます。

  アノテーションルールは、クエリとアノテーションの両方に依存します。インポート処理の完了後に、すべてのアノテーションルールに間違いがないかどうかを確認する必要があります。

- ポリシー
  - 同じ名前のポリシーがターゲットシステムに存在しない場合は、ポリシーが追加されます。
  - 同じ名前のポリシーがターゲットシステムに存在する場合は、ポリシーが置き換えられます。

インポート処理の完了後にポリシーの順序が乱れている可能性があります。インポート後にポリシーの順序を確認する必要があります。アノテーションが正しくないと、アノテーションに依存するポリシーが失敗することがあります。インポート後に、すべてのアノテーションの依存関係を確認する必要があります。

[+]

- クエリ
  - 同じ名前のクエリがターゲットシステムに存在しない場合は、クエリを追加します。
  - 同じ名前のクエリがターゲットシステムに存在する場合、クエリのリソースタイプが異なる場合でもクエリが置き換えられます。

クエリのリソースタイプが異なる場合、インポート後にそのクエリを使用するダッシュボードウィジェットに不要な結果や誤った結果が表示されることがあります。インポートの完了後、クエリベースのすべてのウィジェットが正しく機能しているかどうかを確認する必要があります。アノテーションが正しくないと、アノテーションに依存するクエリが失敗することがあります。インポート後に、すべてのアノテーションの依存関係を確認する必要があります。

[+]

- ダッシュボード
  - 同じ名前のダッシュボードがターゲットシステムに存在しない場合は、ダッシュボードが追加されます。
  - 同じ名前のダッシュボードがターゲットシステムにある場合、クエリのリソースタイプが異なっていても、ダッシュボードが置き換えられます。

インポートの完了後、ダッシュボードでクエリベースのすべてのウィジェットが正しく機能しているかどうかを確認する必要があります。ソースサーバーに同じ名前のダッシュボードが複数ある場合は、すべてエクスポートされます。ただし、ターゲットサーバにインポートされるのは最初のサーバだけです。インポート時のエラーを回避するには、エクスポートする前にダッシュボードの名前が一意であることを確認する必要があります。

[+]

Insightセキュリティ

OnCommand Insightには、Insight環境を高度なセキュリティで運用できる機能が用意されています。これらの機能には、暗号化、パスワードハッシュ、およびパスワードを暗号化および復号化する内部ユーザパスワードとキーペアを変更する機能が含まれます。これらの機能は、SecurityAdmin Toolを使用して、Insight環境内のすべてのサーバで管理できます。

SecurityAdminツールとは

セキュリティ管理ツールでは、ボルトの内容を変更したり、OnCommand Insightのインストール環境を調整したりすることができます。

SecurityAdminツールの主な用途は、セキュリティ設定（ボルトなど）およびパスワードの*バックアップ*および*リストア*です。たとえば、Local Acquisition Unitにバックアップを作成してRemote Acquisition Unitにリストアすることで、環境全体でパスワードの調整が可能になります。また、環境内に複数のOnCommand Insight Serverがある場合は、サーバーボルトのバックアップを作成し、パスワードを同じにするために他のサーバーに復元することもできます。これらは、SecurityAdminを使用して環境内で一貫性を確保する方法のほんの2つの例です。

OnCommand Insightデータベースをバックアップする場合は、必ず*ボルト*をバックアップすることを強くお勧めします。これを行わないと、アクセスが失われる可能性があります。

このツールには、*インタラクティブ*モードと*コマンドライン*モードの両方が用意されています。

SecurityAdmin Toolの多くの操作では、ボルトの内容が変更され、インストールも変更されます。これにより、ボルトとインストールの同期が維持されます。

例えば、

- ユーザのパスワードを変更すると、SANscreen .Usersテーブル内のユーザのエントリが新しいハッシュで更新されます。
- MySQLユーザーのパスワードを変更すると、適切なSQLステートメントが実行され、MySQLインスタンスのユーザーのパスワードが更新されます。

状況によっては、インストールに複数の変更が加えられることがあります。

- DWH MySQLユーザを変更すると、MySQLデータベースのパスワードが更新されるだけでなく、ODBCの複数のレジストリエントリも更新されます。

以降のセクションでは、これらの変更を「調整された変更」という用語で説明します。

実行モード

- 通常/デフォルト動作- SANscreenサーバサービスが実行されている必要があります

  デフォルトの実行モードでは、SecurityAdminツールは* SANscreenサーバーサービス*を実行している必要があります。サーバは認証に使用され、サーバを呼び出すことで、インストールに対する多くの調整された変更が行われます。

- 直接操作- SANscreenサーバサービスが実行中または停止している可能性があります。

  OCIサーバまたはDWHのインストール環境でツールを実行する場合は、「直接」モードでも実行できます。このモードでは、データベースを使用して認証と調整された変更が実行されます。Serverサービスは使用されません。

  動作は通常モードと同じですが、次の例外があります。

- ドメイン管理者以外のユーザに対してのみ認証がサポートされます。（パスワードとロールがLDAPではなくデータベースに存在するユーザ）。
- 「キーの置換」操作はサポートされていません。
- バックアップリストアの再暗号化手順はスキップされます。
- リカバリモードこのツールは、サーバーとデータベースの両方にアクセスできない場合でも実行できます

（例えば、ボルト内のルートパスワードが正しくないため）。

このモードで実行すると、認証ができないため、インストールに対して調整された変更を伴う操作は実行できません。

リカバリモードは、次の目的で使用できます。

- どのボールトエントリが間違っているかを判断する（検証操作を使用）
- 間違ったrootパスワードを正しい値に置き換えます。（パスワードは変更されません。ユーザは現在のパスワードを入力する必要があります）。

> ボルト内のルートパスワードが正しくなく、パスワードが不明で、正しいルートパスワードを持つボルトのバックアップが存在しない場合、SecurityAdmin Toolを使用してインストールを復元することはできません。インストールを回復する唯一の方法は、に記載されている手順に従ってMySQLインスタンスのパスワードをリセットすることです https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html。リセット手順を実行した後、correct-stored-password操作を使用して新しいパスワードをボルトに入力します。

コマンド

制限されていないコマンド

無制限のコマンドは、インストールに対して調整された変更を行います（信頼ストアを除く）。制限のないコマンドは、ユーザ認証なしで実行できます。

コマンド	説明
バックアップ-ヴォールト	ボルトを含むzipファイルを作成します。ボールトファイルへの相対パスは、インストールルートを基準としたボールトパスと一致します。 • wildfly/standalone/configuration/vault/* • acq/conf/vault/*
check-for-default-keys	ボルトのキーが7.3.16より前のインスタンスで使用されていたデフォルトボルトのキーと一致するかどうかを確認します。
correct-stored-password	ボルトに保存されている（正しくない）パスワードを、ユーザーが知っている正しいパスワードに置き換えます。 これは、ボルトとインストールが一貫していない場合に使用できます。インストール時に実際のパスワードが変更されることはありません。
change-trust-store-password	信頼ストアに使用するパスワードを変更し、新しいパスワードをボルトに保存します。信頼ストアの現在のパスワードは「既知」である必要があります。

verify-keystore	ボルトの値が正しいかどうかを確認します。 • OCIユーザの場合、パスワードのハッシュがデータベース内の値と一致しているか • MySQLユーザの場合、データベースに接続できますか • キーストアの場合、キーストアをロードし、キー（存在する場合）を読み取ることができますか？
リストキー	ボルト内のエントリを一覧表示します（保存されている値は表示されません）。

制限されたコマンド

インストールに対して調整された変更を行う非表示のコマンドでは、認証が必要です。

コマンド	説明
restore-vault-backup	現在のボルトを、指定したボルトバックアップファイルに含まれているボルトで置き換えます。 すべての連携アクションを実行して、リストアされたボルトのパスワードと一致するようにインストールを更新します。 • OCI通信ユーザのパスワードを更新する • MySQLユーザのパスワード（rootを含む）を更新する • キーストアごとに、キーストアのパスワードが「既知」の場合は、復元されたボルトのパスワードを使用してキーストアを更新します。 通常モードで実行すると、はインスタンスから各暗号化された値を読み取り、現在のボールトの暗号化サービスを使用して復号化し、復元されたボールトの暗号化サービスを使用して再暗号化し、再暗号化された値を保存します。
synchronize-with-vault	すべての連携アクションを実行して、リストアされたボルトのユーザーパスワードと一致するようにインストールを更新します。 • OCI通信ユーザのパスワードを更新します。 • MySQLユーザのパスワード（rootを含む）を更新します。
パスワードの変更	ボルトのパスワードを変更し、調整された操作を実行します。
キーの置換	新しい空のボールト（既存のボールトとは異なるキーを持つ）を作成します。次に、現在のボルトから新しいボルトにエントリをコピーします。次に、インスタンスから各暗号化された値を読み取り、現在のボールトの暗号化サービスを使用して復号化し、復元されたボールトの暗号化サービスを使用して再暗号化し、再暗号化された値を保存します。

非表示コマンド

SAツールには次のコマンドが用意されています。これらのコマンドは認証を必要としませんが、インストールに対して調整された変更を行います。

リスト・キーのアップグレード（サーバ）	ユーザーが認証されていない場合は、現在のボルトで_internalアカウントとパスワードを使用して認証します。次に、現在のヴォールトをバックアップファイル内のヴォールトに置き換え、連携したアクションを実行します。
アップグレード（取得）	現在のボールトをバックアップファイル内のボールトに置き換え、調整されたアクションを実行します。

連携されたアクション

サーバーボールト

_internal	データベースのユーザのパスワードハッシュの更新
取得	データベースのユーザのパスワードハッシュの更新 取得ボールトが存在する場合は、取得ボールトのエントリも更新します。
dwh_internalの略	データベースのユーザのパスワードハッシュの更新
cognos_adminをクリックします	データベースのユーザのパスワードハッシュの更新 DWHおよびWindowsの場合は、SANscreen /cognos/analytics/configuration/SANscreenAP.propertiesを更新して、cognos.adminプロパティをパスワードに設定します。
ルート	SQLを実行してMySQLインスタンスのユーザパスワードを更新
在庫	SQLを実行してMySQLインスタンスのユーザパスワードを更新

DWH	SQLを実行してMySQLインスタンスのユーザパスワードを更新 DWHおよびWindowsの場合は、Windowsレジストリを更新して、次のODBC関連エントリを新しいパスワードに設定します。 • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\DWH_CAPACITY\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\DWH_CAPACITY_Efficiency\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\odbc\odbc.ini\dwh_fs_util\pwd • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\odbc\odbc.ini\dwh_inventory\pwd • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\DWH_PERFORMANCE\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\DWH_PORTS\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\odbc\odbc.ini\dwh_sa\pwd • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\odbc\odbc.ini\dwh_cloud_cost\pwd
誰だ	SQLを実行してMySQLインスタンスのユーザパスワードを更新
ホスト	SQLを実行してMySQLインスタンスのユーザパスワードを更新
キーストアパスワード	キーストアを新しいパスワード-wildfly/standalone/configuration/server.keystoreで書き換えます。
信頼ストアのパスワード	キーストアを新しいパスワード-wildfly/standalone/configuration/server.trustoreで書き換えます。
キーパスワード	キーストアを新しいパスワード-wildfly/standalone/configuration/sso.jksで書き換えます。
cognos_archive	なし

Acquisition Vault

取得	なし
信頼ストアのパスワード	キーストアを新しいパスワード（存在する場合）で書き換えます。 -acq/conf/cert/client.keystore

Security Adminツールの実行-コマンドライン

コマンドラインモードでSAツールを実行する構文は次のとおりです。

```
securityadmin [-s | -au] [-db] [-lu <user> [-lp <password>]] <additional-
options>

where

-s                      selects server vault
-au                     selects acquisition vault

-db                     selects direct operation mode

-lu <user>              user for authentication
-lp <password>          password for authentication
<addition-options>      specifies command and command arguments as
described below
```

注：

- コマンドラインに「-i」オプションがない場合があります（対話モードが選択されるため）。
- 「-s」および「-au」オプションの場合：
  - 「-s」はRAUでは使用できません
  - DWHでは「-au」は使用できません
  - どちらも存在しない場合は、
    - サーバーボルトは、サーバー（Server）、DWH、およびデュアル（Dual）で選択されています。
    - RAUで収集ボールトが選択されている
- ユーザ認証には-luオプションと-lpオプションを使用します。
  - <user>が指定され、<password>が指定されていない場合は、ユーザにパスワードの入力を求められます。
  - <user>を指定せず、認証が必要な場合は、<user>と<password>の両方の入力を求められます。

『コマンド・

コマンド	使用法
correct-stored-password	`securityadmin [-s`

-au] [-db] -pt <key> [<value>]
 	
`where`
 	
-pt specifies the command ("put") <key> is the key <value> is the value. If not present, user will be prompted for value
 	
` `
	バックアップ-ヴォールト

`securityadmin [-s`	-au] [-db] -b [<backup-dir>] where -b specified command <backup-dir> is the output directory. If not present, default location of SANscreen/backup/vault is used The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip ` `
バックアップ-ヴォールト	`securityadmin [-s`
-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file ` `	リストキー

`securityadmin [-s`	-au] [-db] -l where -l specified command ```
チェックキー	`securityadmin [-s`
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys ```	verify-keystore（サーバ）

`securityadmin [-s] [-db] -v`
 	
`where`
 	
`-v specified command`
	アップグレード

`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -u where -u specified command For server vault, if -lu is not present, then authentication will be performed for <user> =_internal and <password> = _internal's password from vault. For acquisition vault, if -lu is not present, then no authentication will be attempted ```

キーの置換	`securityadmin [-s`
-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command ``	restore-vault-backup
`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file> where -r specified command <backup-file> the backup file location ``

change-password（サーバ）	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-un <user> entry ("user") name to update`
	`-p <password> new password. If <password not supplied, user will be prompted.`
	`-sh for mySQL user, use strong hash`

change - acquisitionユーザ（acquisition）のパスワード	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-p <password> new password. If <password not supplied, user will be prompted.`

change-password for truststore -_password （acquisition）	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -utp -p [<password>]`
	
	`where`
	
	`-utp specified command ("update-truststore-password")`
	`-p <password> new password. If <password not supplied, user will be prompted.`

synchronize-with-vault（サーバー）	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>`
	
	`where`
	
	`-sv specified command`

Security Admin Toolの実行-インタラクティブモード

インタラクティブ-メインメニュー

SAツールを対話型モードで実行するには、次のコマンドを入力します。

```
 securityadmin -i
```

サーバまたはデュアルインストールの場合は、SecurityAdminによってサーバまたはLocal Acquisition Unitのどちらかを選択するように求められます。

ServerおよびAcquisition Unitノードが検出されました。セキュリティを再設定する必要があるノードを選択します。

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

DWHでは、[Server]が自動的に選択されます。リモートAUでは、「Acquisition Unit」が自動的に選択されます。

Interactive Server：rootパスワードのリカバリ

サーバーモードでは、SecurityAdminツールは最初に保存されているルートパスワードが正しいことを確認します。そうでない場合、ツールはrootパスワードの回復画面を表示します。

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

オプション1を選択すると、正しいパスワードの入力を求められます。

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
```

正しいパスワードを入力すると、次のように表示されます。

```
 Password verified.  Vault updated
```

ENTERキーを押すと、サーバーの無制限メニューが表示されます。

間違ったパスワードを入力すると、次のメッセージが表示されます。

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
```

ENTERキーを押すと、リカバリメニューに戻ります。

オプション2を選択すると、正しいパスワードを読み取るバックアップファイルの名前の入力を求めるプロンプトが表示されます。

```
 Enter Backup File Location:
```

バックアップのパスワードが正しい場合は、次のように表示されます。

```
 Password verified.  Vault updated
```

ENTERキーを押すと、サーバーの無制限メニューが表示されます。

バックアップのパスワードが正しくない場合、次のメッセージが表示されます。

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
```
ENTERキーを押すと、リカバリメニューに戻ります。

Interactive-Server:正しいパスワード

「正しいパスワード」アクションは、ボルトに保存されているパスワードを変更し、インストールで必要とされる実際のパスワードと一致させるために使用されます。このコマンドは、securityadminツール以外によってインストールに変更が加えられた場合に便利です。たとえば、次のようなもの

- SQLユーザのパスワードがMySQLに直接アクセスして変更されました。
- キーストアが置き換えられたか、キーストアのパスワードがkeytoolを使用して変更されました。
- OCIデータベースがリストアされ、そのデータベースの内部ユーザ用に異なるパスワードが設定されている

「Correct Password」では、最初に正しい値を保存するパスワードを選択するように求められます。

```
Replace incorrect stored password with correct password.  (Does not change
the required password)
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

修正するエントリを選択すると、値の指定方法を求めるプロンプトが表示されます。

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

オプション1を選択すると、正しいパスワードの入力を求められます。

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
```
正しいパスワードを入力すると、次のように表示されます。

```
 Password verified.  Vault updated
```
ENTERキーを押すと、サーバーの無制限メニューに戻ります。

間違ったパスワードを入力すると、次のメッセージが表示されます。

```
Password verification failed - {additional information}
Vault entry not updated.
```

ENTERキーを押すと、サーバーの無制限メニューに戻ります。

オプション2を選択すると、正しいパスワードを読み取るバックアップファイルの名前の入力を求めるプロンプトが表示されます。

```
 Enter Backup File Location:
```
バックアップのパスワードが正しい場合は、次のように表示されます。

```
 Password verified.  Vault updated
```
ENTERキーを押すと、サーバーの無制限メニューが表示されます。

バックアップのパスワードが正しくない場合、次のメッセージが表示されます。

```
Password verification failed - {additional information}
Vault entry not updated.
```

ENTERキーを押すと、サーバーの無制限メニューが表示されます。

対話型サーバ：ボールトの内容の確認

ボルトの内容を確認（Verify Vault Contents）では、以前のバージョンのOCIで配布されたデフォルトのボルトと一致するキーがボルトにあるかどうかがチェックされ、ボルト内の各値がインストール環境と一致するかどうかがチェックされます。

各キーの結果は次のとおりです。

OK	ボルトの値が正しい

未チェック	この値はインストールに対してチェックできません
不良	値がインストール環境と一致しません
不明	想定されるエントリがありません。

```
Encryption keys secure: unique, non-default encryption keys detected

             cognos_admin: OK
                    hosts: OK
             dwh_internal: OK
                inventory: OK
                  dwhuser: OK
        keystore_password: OK
                      dwh: OK
      truststore_password: OK
                     root: OK
                _internal: OK
          cognos_internal: Not Checked
             key_password: OK
              acquisition: OK
           cognos_archive: Not Checked
 cognos_keystore_password: Missing


Press enter to continue
```

対話型サーバ：バックアップ

Backupは、バックアップzipファイルを保存するディレクトリの入力を求めます。ディレクトリがすでに存在している必要があり、ファイル名はServerSecurityBackup-yyyy-mm-dd-hh-mm.zipになります。

```
Enter backup directory location [C:\Program Files\SANscreen\backup\vault]
:

Backup Succeeded!   Backup File: C:\Program
Files\SANscreen\backup\vault\ServerSecurityBackup-2024-08-09-12-02.zip
```

対話型サーバ：ログイン

ログインアクションは、ユーザを認証し、インストールを変更する操作にアクセスするために使用されます。ユーザには管理Privilegesが必要です。サーバで実行する場合は、任意の管理者ユーザを使用できます。直接モードで実行する場合は、LDAPユーザではなくローカルユーザである必要があります。

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

または

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:
```

パスワードが正しく、ユーザが管理者ユーザである場合は、制限されたメニューが表示されます。

パスワードが正しくない場合は、次のメッセージが表示されます。

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:

Login Failed!
```

ユーザが管理者でない場合は、次のメッセージが表示されます。

```
Authenticating via server. Enter user and password

UserName: user

Password:

User 'user' does not have 'admin' role!
```

Interactive-Server:制限付きメニュー

ユーザーがログインすると、ツールに制限付きメニューが表示されます。

```
Logged in as: admin
Select Action:

2 - Change Password

3 - Verify Vault Contents

4 - Backup

5 - Restore

6 - Change Encryption Keys

7 - Fix installation to match vault

9 - Exit

Enter your choice:
```

Interactive-Server:パスワードの変更

「パスワードの変更」アクションは、インストールパスワードを新しい値に変更するために使用します。

[パスワードの変更]をクリックすると、最初に変更するパスワードを選択するように求められます。

```
Change Password
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

ユーザがMySQLユーザの場合、修正するエントリを選択すると、パスワードを強力にハッシュするかどうかを確認するメッセージが表示されます。

```
MySQL supports SHA-1 and SHA-256 password hashes. SHA-256 is stronger but
requires all clients use SSL connections

Use strong password hash? (Y/n): y
```

次に、新しいパスワードの入力を求められます。

```
New Password for '{user}':
If the password is empty, the operation is cancelled.

Password is empty - cancelling operation
```

空でないパスワードを入力すると、パスワードの確認を求めるプロンプトが表示されます。

```
New Password for '{user}':

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

変更に失敗すると、エラーまたは例外が表示されます。

対話型サーバ：リストア

Interactive Server：暗号化キーの変更

暗号化キーの変更アクションは、ボールトエントリの暗号化に使用される暗号化キーを置き換え、ボールトの暗号化サービスに使用される暗号化キーを置き換えます。暗号化サービスのキーが変更されるため、データベース内の暗号化された値は再暗号化されます。これらの値は、現在のキーで読み取られ、復号化され、新しいキーで暗号化され、データベースに保存されます。

サーバは一部のデータベースコンテンツに対して再暗号化処理を提供するため、ダイレクトモードではこのアクションはサポートされていません。

```
Replace encryption key with new key and update encrypted database values

Confirm (y/N): y

Change Encryption Keys succeeded! Restart 'Server' Service!
```

インタラクティブサーバー:インストールの修正

[インストールの修正]アクションを実行すると、インストールが更新されます。securityadminツールを使用して変更可能なすべてのインストールパスワード（rootを除く）は、ボルト内のパスワードに設定されます。

- OCIの内部ユーザのパスワードが更新されます。
- root以外のMySQLユーザのパスワードが更新されます。
- キーストアのパスワードが更新されます。

```
Fix installation - update installation passwords to match values in vault

Confirm:  (y/N): y

Installation update succeeded! Restart 'Server' Service.
```

最初の更新に失敗した時点でアクションが停止し、エラーまたは例外が表示されます。

Insight Serverでセキュリティを管理する

。 `securityadmin` ツールを使用すると、Insight Serverでセキュリティオプションを管理できます。セキュリティの管理には、パスワードの変更、新しいキーの生成、作成したセキュリティ設定の保存とリストア、デフォルト設定への設定のリストアが含まれます。

このタスクについて

を使用します `securityadmin` セキュリティ管理ツール：

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

詳細については、のドキュメントを参照してください"securityadmin"。

Local Acquisition Unit上のセキュリティの管理

。 `securityadmin` ツールを使用すると、Local Acquisition User（LAU；ローカル収集ユーザ）のセキュリティオプションを管理できます。セキュリティの管理には、キーとパスワードの管理、作成したセキュリティ設定の保存とリストア、またはデフォルト設定への設定のリストアが含まれます。

作業を開始する前に

が必要です `admin` セキュリティ設定タスクを実行するための権限。

このタスクについて

を使用します `securityadmin` セキュリティ管理ツール：

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

詳細については、手順を参照して"securityadminツール"ください。

RAUでのセキュリティの管理

。 `securityadmin` ツールを使用すると、RAUのセキュリティオプションを管理できます。場合によっては、ヴォールト設定のバックアップやリストア、暗号化キーの変更、Acquisition Unitのパスワードの更新が必要になることがあります。

このタスクについて

を使用します `securityadmin` セキュリティ管理ツール：

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

LAU / RAUのセキュリティ設定を更新する1つのシナリオは、サーバでそのユーザのパスワードが変更されたときに「acquisition」ユーザのパスワードを更新することです。LAUおよびすべてのRAUは、サーバとの通信にサーバ「acquisition」ユーザのパスワードと同じパスワードを使用します。

「acquisition」ユーザが存在するのはInsight Serverだけです。RAUまたはLAUは、サーバに接続するときにそのユーザとしてログインします。

詳細については、手順を参照して"securityadminツール"ください。

Data Warehouseでセキュリティを管理する

。 `securityadmin` ツールを使用すると、Data Warehouseサーバのセキュリティオプションを管理できます。セキュリティの管理には、DWHサーバで内部ユーザの内部パスワードを更新したり、セキュリティ設定のバックアップを作成したり、設定をデフォルトの設定にリストアしたりする作業があります。

このタスクについて

を使用します `securityadmin` セキュリティ管理ツール：

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

詳細については、のドキュメントを参照してください"securityadmin"。

OnCommand Insight の内部ユーザのパスワードを変更しています

セキュリティポリシーによっては、OnCommand Insight 環境でパスワードの変更が必要になる場合があります。1台のサーバのパスワードの一部は、環境内の別のサーバに存在するため、両方のサーバでパスワードを変更する必要があります。たとえば、Insight Serverでユーザのパスワード「inventory」を変更する場合は、そのInsight Server用に設定されたData Warehouse Server Connectorでユーザのパスワード「inventory」と一致している必要があります。

作業を開始する前に

パスワードを変更する前に、ユーザアカウントの依存関係を理解しておく必要があります。必要なすべてのサーバでパスワードを更新しないと、Insightコンポーネント間の通信に失敗します。

このタスクについて

次の表に、Insight Serverの内部ユーザパスワードと、依存するパスワードが新しいパスワードと一致する必要があるInsightコンポーネントを示します。

Insight Serverのパスワード	必要な変更
_internal	
取得	愛称はラオ
dwh_internalの略	Data Warehouse
ホスト	
在庫	Data Warehouse
ルート	

次の表に、Data Warehouseの内部ユーザパスワードと、依存するパスワードが新しいパスワードと一致する必要があるInsightコンポーネントを示します。

Data Warehouseのパスワード	必要な変更
cognos_adminをクリックします	
DWH	
dwh_internal（Server Connectorの設定UIを使用して変更）	Insightサーバ
誰だ	
ホスト	
インベントリ（Server Connector設定UIを使用して変更）	Insightサーバ
ルート	

- DWHサーバ接続設定UIでのパスワードの変更*

次の表に、LAUのユーザパスワードと、依存するパスワードが新しいパスワードと一致する必要があるInsightコンポーネントを示します。

LAUパスワード	必要な変更
取得	Insight Server、RAU

Server Connection Configuration UIを使用して「**inventory**」パスワードと「**dwh_internal**」パスワードを変更します

「inventory」または「dwh_internal」のパスワードをInsight Serverと同じパスワードに変更する必要がある場合は、Data Warehouse UIを使用します。

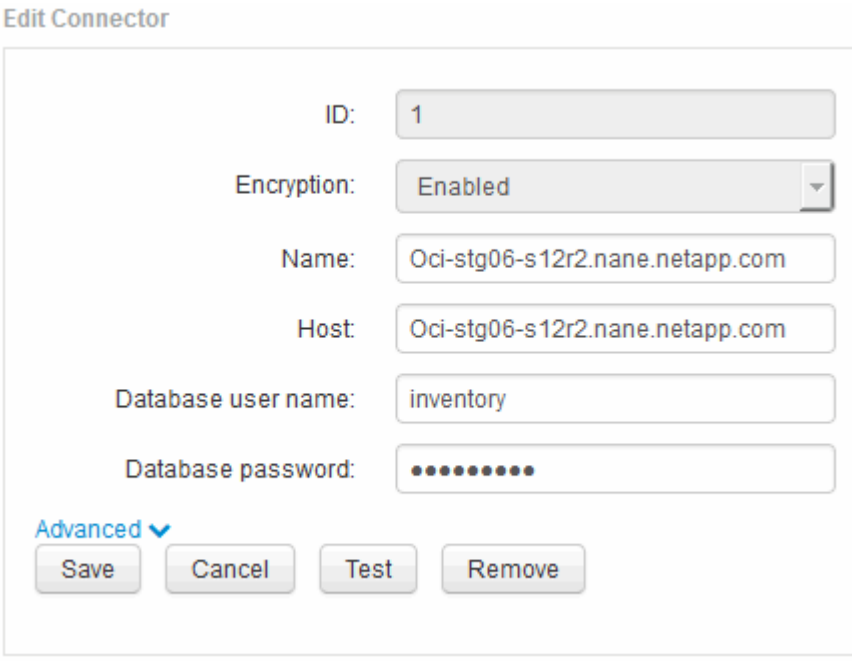
作業を開始する前に

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。

手順

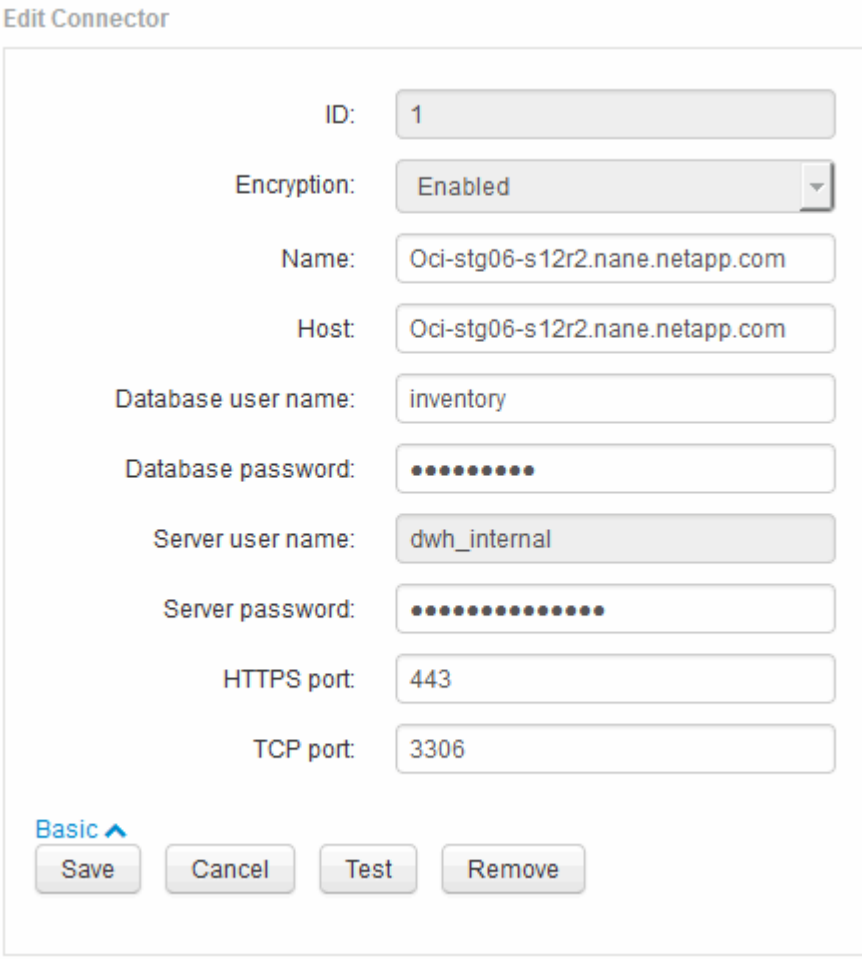
1. Data Warehouseポータルにログインします https://hostname/dwhhostnameは、OnCommand Insight Data Warehouseがインストールされているシステムの名前です。
2. 左側のナビゲーションペインで、*[コネクタ]*をクリックします。

   [Edit Connector]（コネクタの編集）*画面が表示されます。



3. 「* Database password *」フィールドに新しい「`inventory`」パスワードを入力します。
4. [保存（ Save ）] をクリックします。
5. 「`dwh_internal`」パスワードを変更するには、*[詳細設定]*をクリックします

[Edit Connector Advanced]画面が表示されます。



6. 新しいパスワードを* Server password *フィールドに入力します。
7. [保存] をクリックします .

ODBC Administrationツールを使用した**DWH**パスワードの変更

Insight ServerでDWHユーザのパスワードをで変更した場合は、Data Warehouseサーバでもパスワードを変更する必要があります。ODBC Data Source Administratorツールを使用して、Data Warehouseのパスワードを変更します。

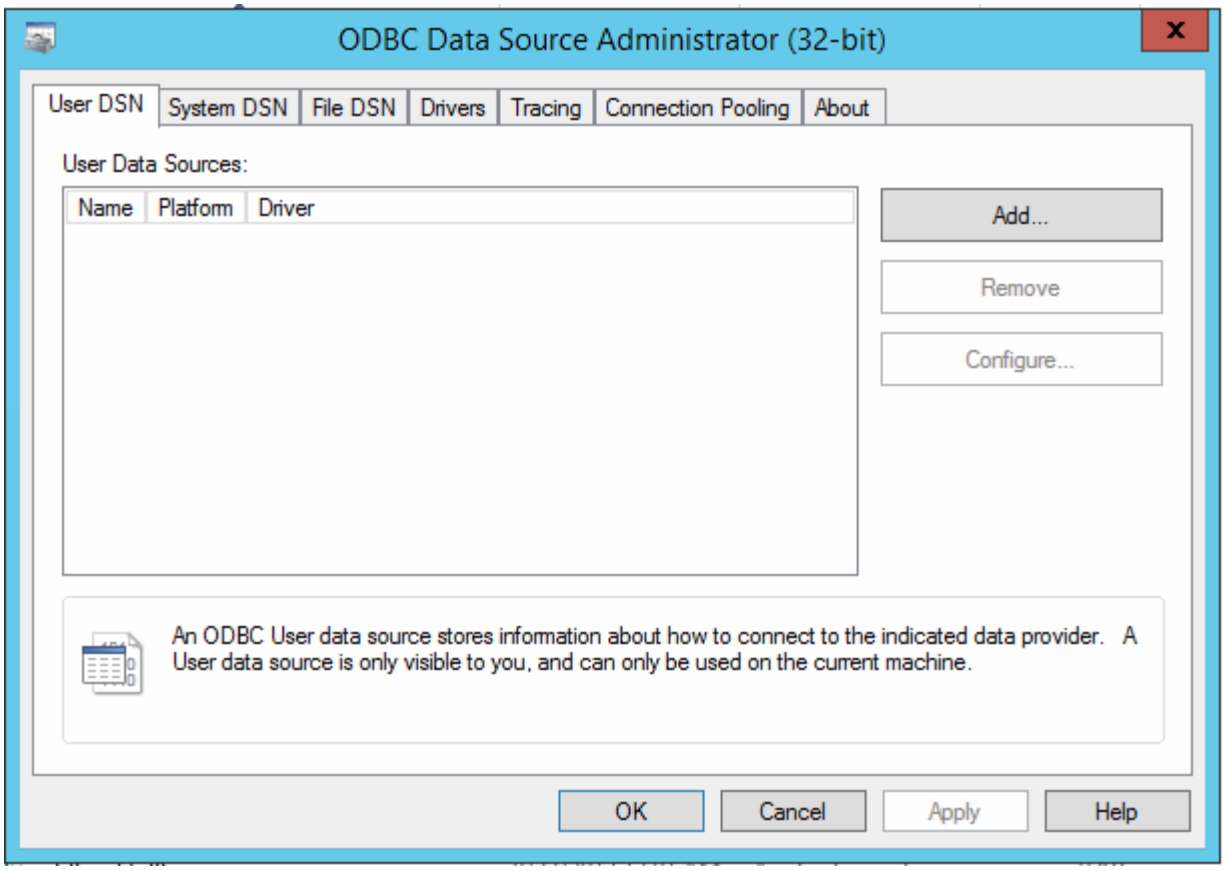
作業を開始する前に

管理者権限があるアカウントを使用してData Warehouseサーバへのリモートログインを実行する必要があります。

手順

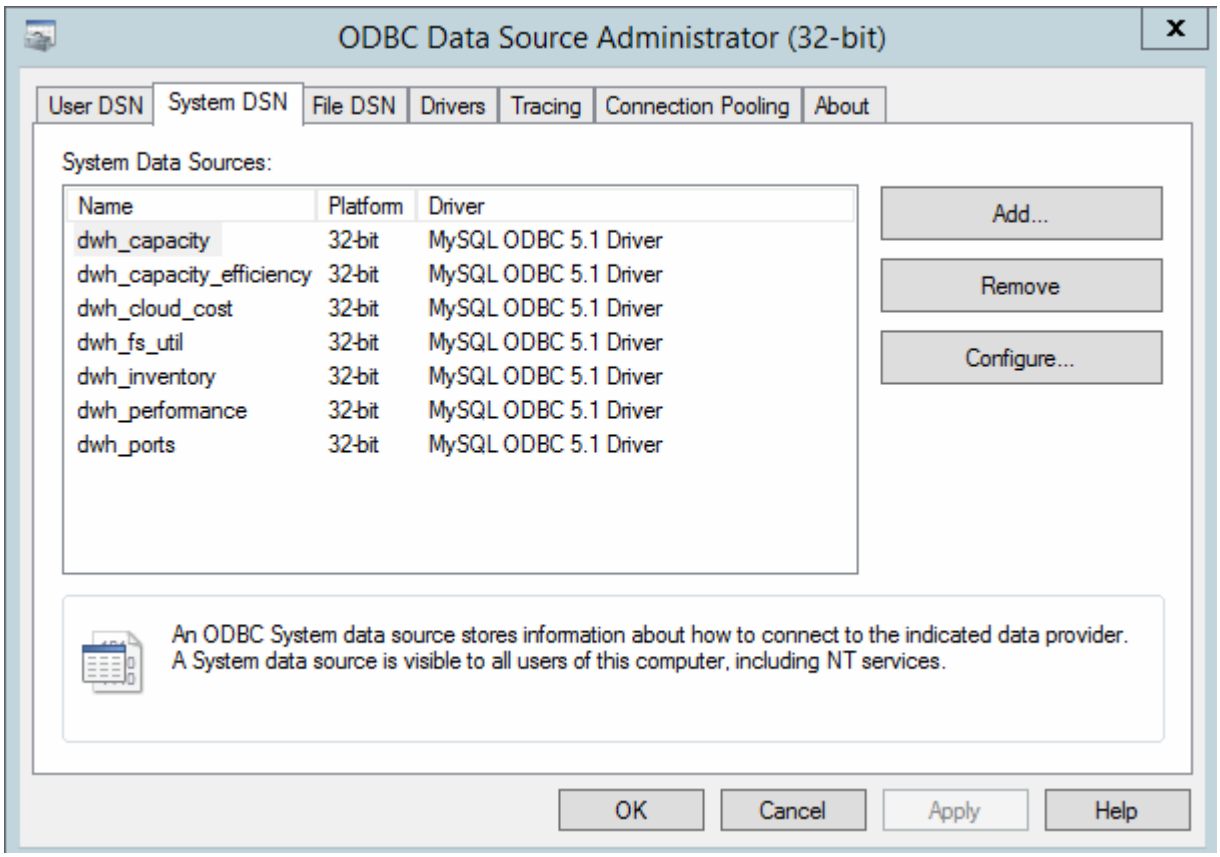
1. Data Warehouseをホストしているサーバへのリモートログインを実行します。
2. ODBC Administrationツールにアクセスします `C:\Windows\SysWOW64\odbcad32.exe`

   [ODBC Data Source Administrator]画面が表示されます。



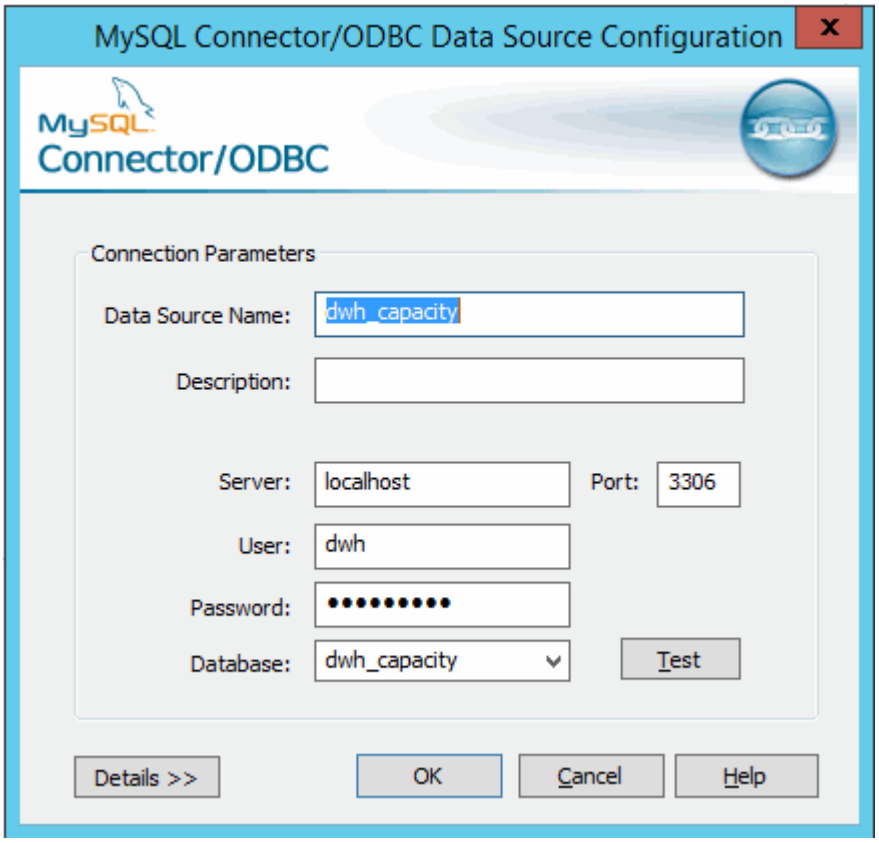
3. [システムDSN]*をクリックします

   システムデータソースが表示されます。



4. リストからOnCommand Insight データソースを選択します。
5. [設定]*をクリックします

   [Data Source Configuration]画面が表示されます。



6. [パスワード]*フィールドに新しいパスワードを入力します。

スマートカードおよび証明書によるログインのサポート

OnCommand Insight では、Insightサーバにログインするユーザの認証にスマートカード（CAC）と証明書を使用できます。これらの機能を有効にするには、システムを設定する必要があります。

CACと証明書をサポートするようにシステムを設定した後、OnCommand Insight の新しいセッションに移動すると、ブラウザにネイティブダイアログが表示され、選択する個人証明書のリストが表示されます。これらの証明書は、OnCommand Insight サーバによって信頼されたCAによって発行された個人証明書のセットに基づいてフィルタリングされます。ほとんどの場合、単一の選択があります。既定では、選択肢が1つしかない場合、Internet Explorerはこのダイアログをスキップします。

CACユーザの場合、スマートカードには複数の証明書が含まれており、信頼されたCAに一致できる証明書は1つだけです。のCAC証明書 `identification` を使用する必要があります。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "WindowsホストにインストールされているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

スマートカードおよび証明書によるログイン用にホストを設定しています

スマートカード（CAC）および証明書によるログインをサポートするには、OnCommand Insight ホストの設定を変更する必要があります。

作業を開始する前に

- システムでLDAPが有効になっている必要があります。
- LDAP `User principal account name` 属性は、ユーザのIDを含むLDAPフィールドと一致する必要があります。

を使用して_server.keystore_and/or_server.trustore_passwordsを変更した場合は"securityadmin"、SANscreen証明書をインポートする前に_ldap_serviceを再起動してください。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "WindowsホストにインストールされているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

手順

1. を使用します `regedit` でレジストリ値を変更するユーティリティ `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`：
   a. jvm_optionを変更します `DclientAuth=false` 終了： `DclientAuth=true.`
2. キーストアファイルをバックアップします。 `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. コマンドプロンプトを開き、を指定します `Run as administrator`
4. 自己生成証明書を削除します。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. 新しい証明書を生成します。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"`
6. 証明書署名要求（CSR）を生成します。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"`
7. 手順6でCSRが返されたら、証明書をインポートし、Base-64形式でエクスポートしてに保存します `"C:\temp" named servername.cer`。
8. キーストアから証明書を抽出します。`C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12`
9. p12ファイルから秘密鍵を抽出します。 `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. 手順7でエクスポートしたBase-64証明書を秘密鍵とマージします。 `openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"`
11. マージした証明書をキーストアにインポートします。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`
12. ルート証明書をインポートします。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"`
13. ルート証明書をserver.trustoreにインポートします。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"`

14. 中間証明書をインポートします。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"`

    すべての中間証明書について、この手順を繰り返します。

15. この例と一致するようにLDAPでドメインを指定します。
16. サーバを再起動します。

スマートカードおよび証明書によるログインをサポートするようにクライアントを設定しています

クライアントマシンでスマートカードを使用し、証明書によるログインを有効にするには、ミドルウェアを使用し、ブラウザを変更する必要があります。スマート・カードをすでに使用しているお客様は、クライアント・マシンに追加の変更を加える必要はありません。

作業を開始する前に

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "Windowsホストにインストールされ ているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

このタスクについて

一般的なクライアント設定要件は次のとおりです。

- ActivClientなどのスマートカードミドルウェアのインストール（を参照）
- IEブラウザの変更（を参照
- Firefoxブラウザの変更（を参照

Linuxサーバでの**CAC**の有効化

Linux OnCommand Insight サーバでCACを有効にするには、いくつかの変更が必要です。

ルートCAを信頼ストアにインポートする必要があります。

手順

1. に移動します `/opt/netapp/oci/conf/`
2. 編集 `wildfly.properties` をクリックし、の値を変更します `CLIENT_AUTH_ENABLED` 「True」へ
3. 以下にある「ルート証明書」をインポートします。
   `/opt/netapp/oci/wildfly/standalone/configuration/server.truststore`
4. サーバを再起動します

Data Warehouseでスマートカードおよび証明書によるログインを設定しています

スマートカード（CAC）および証明書によるログインをサポートするには、OnCommand Insight データウェアハウスの設定を変更する必要があります。

作業を開始する前に

- システムでLDAPが有効になっている必要があります。
- LDAP `User principal account name` 属性は、ユーザの政府機関ID番号を含むLDAPフィールドと一致する必要があります。

  政府発行のCACに保存される共通名（CN）は、通常次の形式になります。 `first.last.ID`。一部のLDAPフィールド（など）`sAMAccountName`この形式は長すぎます。これらのフィールドの場合、OnCommand Insight はCNからID番号だけを抽出します。

を使用して_server.keystore_and/or_server.trustore_passwordsを変更した場合は"securityadmin"、SANscreen証明書をインポートする前に_ldap_serviceを再起動してください。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "WindowsホストにインストールされているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

手順

1. regeditを使用して、のレジストリ値を変更します `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. jvm_optionを変更します `-DclientAuth=false` 終了： `-DclientAuth=true`。

   Linuxの場合は、を変更します `clientAuth` のパラメータ `/opt/netapp/oci/scripts/wildfly.server`

2. Data Warehouse TrustoreにCertificate Authority（CA；認証局）を追加します。

   a. コマンドウィンドウで、に進みます `..\SANscreen\wildfly\standalone\configuration`。

   b. ユーティリティを使用し `keytool`て、信頼できるCAのリストを表示します `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>`。+ server_trustoreのパスワードの設定または変更の詳細については、ドキュメントを参照してください"securityadmin"。

   各行の最初の単語はCAエイリアスを示します。

   c. 必要に応じて、CA証明書ファイル（通常は）を指定します `.pem` ファイル。Data Warehouseの信頼済みCAにお客様のCAを含めるには、に進みます `..\SANscreen\wildfly\standalone\configuration` およびを使用します `keytool` インポートコマンド： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   my_aliasは通常、でCAを簡単に識別できるエイリアスです`keytool -list` 操作。

3. OnCommand Insight サーバで、を実行します `wildfly/standalone/configuration/standalone-full.xml` でverify-clientを「requested」に更新して、ファイルを変更する必要があります `/subsystem=undertow/server=default-server/https-listener=default-https`CACを有効にします。Insight Serverにログインし、該当するコマンドを実行します。

OS	スクリプト
Windows の場合	<install dir> を参照してくださ い\enableCACforRemoteEJB.bat
Linux の場合	/opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB .sh

   スクリプトの実行後、wildflyサーバのリロードが完了するまで待ってから、次の手順に進みます。

4. OnCommand Insight サーバを再起動します。

スマートカードおよび証明書によるログインのための**Cognos**の設定（**OnCommand Insight 7.3.10**以降）

Cognosサーバでスマートカード（CAC）および証明書によるログインをサポートするに

は、OnCommand Insight Data Warehouseの設定を変更する必要があります。

作業を開始する前に

この手順 は、OnCommand Insight 7.3.10以降を実行しているシステム用です。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "Windowsホストにインストールされているインストール内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

手順

1. Cognos TrustoreにCertificate Authority（CA；認証局）を追加します。
   a. コマンドウィンドウで、に進みます `..\SANscreen\cognos\analytics\configuration\certs\`
   b. ユーティリティを使用し `keytool`て、信頼できるCAのリストを表示します。'..\..\IBM-JRE\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>

      各行の最初の単語はCAエイリアスを示します。

   c. 適切なファイルが存在しない場合は、CA証明書ファイル（通常は）を指定します `.pem` ファイル。
   d. OnCommand Insight の信頼済みCAに顧客のCAを含めるには、に進みます `..\SANscreen\cognos\analytics\configuration\certs\`。
   e. を使用します `keytool` をインポートするユーティリティ `.pem` ファイル： `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias`は通常、操作でCAを簡単に識別できるエイリアスです`keytool -list`。

   f. パスワードの入力を求められたら、_/ SANscreen /bin/cognos_info.dat_ファイルからパスワードを入力します。
   g. 回答 `yes` 証明書を信頼するように求められたら、
2. CACモードをイネーブルにするには、次の手順を実行します。
   a. 次の手順に従って、CACログアウトページを設定します。
      - Cognosポータルにログオンします（ユーザはシステム管理者グループ（cognos_admin）に属して

いる必要があります）。

- （7.3.10および7.3.11の場合のみ）[管理]→[構成]→[システム]→[セキュリティ]をクリックします
- （7.3.10および7.3.11の場合のみ）Logout Redirect URL-> Applyに対してcacLogout.htmlと入力します
- ブラウザを閉じます。

b. 実行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. IBM Cognosサービスを開始します。Cognosサービスが開始されるまで待ちます。

3. CACモードを無効にするには、次の手順を実行します。

a. 実行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. IBM Cognosサービスを開始します。Cognosサービスが開始されるまで待ちます。

c. （7.3.10および7.3.11の場合のみ）次の手順に従って、CACログアウトページの設定を解除します。

- Cognosポータルにログオンします（ユーザはシステム管理者グループ（cognos_admin）に属している必要があります）。
- [管理]→[設定]→[システム]→[セキュリティ]をクリックします
- Logout Redirect URL-> Applyに対してcacLogout.htmlと入力します
- ブラウザを閉じます。

CognosおよびDWHのCA署名SSL証明書のインポート（Insight 7.3.10以降）

SSL証明書を追加して、Data WarehouseおよびCognos環境の認証と暗号化を強化することができます。

作業を開始する前に

この手順 は、OnCommand Insight 7.3.10以降を実行しているシステム用です。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "WindowsホストにインストールされているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

このタスクについて

この手順 を実行するには、admin権限が必要です。

手順

1. IBM Cognos Configurationツールを使用してCognosを停止します。Cognosを閉じます。
2. のバックアップを作成します `..\SANScreen\cognos\analytics\configuration` および `..\SANScreen\cognos\analytics\temp\cam\freshness` フォルダ。
3. Cognosから証明書暗号化要求を生成します。Admin CMDウィンドウで、次のコマンドを実行します。
   a. CD "`\Program Files\sanscreen\cognos\analytics\bin`"
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`です。注意:ここで-Hと-Iはdnsやipaddressのようなサブジェクトの代替名を追加します。
   c. <password>の場合は、_/ SANscreen /bin/cognos_info.dat_ファイルのパスワードを使用します。
4. を開きます `c:\temp\encryptRequest.csr` ファイルを作成し、生成されたコンテンツをコピーします。
5. encryptRequest.csrコンテンツを入力し、CA署名ポータルを使用して証明書を生成します。
6. PKCS7形式を使用してルート証明書を含め、チェーン証明書をダウンロードします

   FQDNの.p7bファイルがダウンロードされます
7. CAから.p7b形式の証明書を取得します。Cognos Webサーバの証明書としてマークする名前を使用します。
8. ThirdPartyCertificateTool.batはチェーン全体をインポートできないため、すべての証明書をエクスポートするには複数の手順が必要です。チェーンを次のように個別にエクスポートして分割します。
   a. "`Crypto Shell Extensions`"の.p7b証明書を開きます。
   b. 左側のペインで「証明書」を参照します。
   c. ルートCA > All Tasks > Exportを右クリックします。
   d. Base64出力を選択します。
   e. ルート証明書として識別するファイル名を入力します。
   f. 手順8aから8eを繰り返して、すべての証明書を.cerファイルに個別にエクスポートします。
   g. ファイルにmediateX.cerとcognos.cerという名前を付けます。
9. CA証明書が1つしかない場合は、この手順を無視します。それ以外の場合は、root.cerとintermediateX.cerの両方を1つのファイルにマージします。
   a. メモ帳でroot.cerを開き、内容をコピーします。
   b. メモ帳を使用してintermediate.cerを開き、9aのコンテンツを追加します（最初に中間、次にルート）。
   c. ファイルをchain.cerとして保存します。
10. Admin CMDプロンプトを使用して、Cognosキーストアに証明書をインポートします。
    a. cd「Program Files\SANscreen\cognos\analytics\bin`」

b. ThirdPartyCertificateTool.bat - java：local -i -T -r c：\temp\root.cer

c. ThirdPartyCertificateTool.bat - java：local -i -T -r c：\temp\intermediate.cer

d. ThirdPartyCertificateTool.bat - java：local -i -e -r c：\temp\cognos.cer -t c：\temp\chain.cer

11. [IBM Cognos Configuration]を開きます。

    a. [Local Configuration]→[Security]→[Cryptography]→[Cognos]を選択します

    b. 「サードパーティCAを使用しますか？」を変更します。 Trueに設定します。

    c. 設定を保存します。

    d. Cognosを再起動します

12. Admin CMDプロンプトを使用して、最新のCognos証明書をcognos.crtにエクスポートします。

    a. CD "`C：\Program Files\SANscreen"

    b. java\bin\keytool.exe -exportcert -file c：\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password>-alias encryption

    c. <password>の場合は、_/ SANscreen /bin/cognos_info.dat_ファイルのパスワードを使用します。

13. DWHサーバのtrustoreをにバックアップします`..\SANscreen\wildfly\standalone\configuration\server.trustore`

14. Admin CMDプロンプトウィンドウを使用して、「c：\temp\cognos.crt」をDWH trustoreにインポートし、CognosとDWHの間のSSL通信を確立します。

    a. CD "`C：\Program Files\SANscreen"

    b. java\bin\keytool.exe -importcert -file c：\temp\cognos.crt -keystore wildfly\standalone\configuration\server.trustore -storepass <password>-alias cognos3rdca

    c. <password>の場合は、_/ SANscreen /bin/cognos_info.dat_ファイルのパスワードを使用します。

15. SANscreen サービスを再起動します。

16. DWHのバックアップを実行して、DWHがCognosと通信していることを確認します。

17. 次の手順は、「sl certificate」のみを変更し、デフォルトのCognos証明書を変更しない場合でも実行する必要があります。そうしないと、新しいSANscreen 証明書についてCognosから苦情が表示されたり、DWHバックアップを作成できない可能性があります。

    a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`

    b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass <password> -alias "ssl certificate"`

    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

    通常、これらの手順はCognos証明書のインポートプロセスの一環として実行します（を参照） "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

Data Warehouseでスマートカードおよび証明書によるログインを設定しています

スマートカード（CAC）および証明書によるログインをサポートするには、OnCommand Insight データウェアハウスの設定を変更する必要があります。

作業を開始する前に

- システムでLDAPが有効になっている必要があります。
- LDAP `User principal account name` 属性は、ユーザの政府機関ID番号を含むLDAPフィールドと一致する必要があります。

  政府発行のCACに保存される共通名（CN）は、通常次の形式になります。 `first.last.ID`。一部のLDAPフィールド（など）`sAMAccountName`この形式は長すぎます。これらのフィールドの場合、OnCommand Insight はCNからID番号だけを抽出します。

を使用して_server.keystore_and/or_server.trustore_passwordsを変更した場合は"securityadmin"、SANscreen証明書をインポートする前に_ldap_serviceを再起動してください。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "WindowsホストにインストールされているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

手順

1. regeditを使用して、のレジストリ値を変更します `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. jvm_optionを変更します `-DclientAuth=false` 終了： `-DclientAuth=true`。

   Linuxの場合は、を変更します `clientAuth` のパラメータ `/opt/netapp/oci/scripts/wildfly.server`

2. Data Warehouse TrustoreにCertificate Authority（CA；認証局）を追加します。

a. コマンドウィンドウで、に進みます `..\SANscreen\wildfly\standalone\configuration`。

b. ユーティリティを使用し `keytool`て、信頼できるCAのリストを表示します `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>`。+ server_trustoreのパスワードの設定または変更の詳細については、ドキュメントを参照してください"securityadmin"。

各行の最初の単語はCAエイリアスを示します。

c. 必要に応じて、CA証明書ファイル（通常は）を指定します `.pem` ファイル。Data Warehouseの信頼済みCAにお客様のCAを含めるには、に進みます `..\SANscreen\wildfly\standalone\configuration` およびを使用します `keytool` インポートコマンド： `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

my_aliasは通常、でCAを簡単に識別できるエイリアスです`keytool -list` 操作。

3. OnCommand Insight サーバで、を実行します `wildfly/standalone/configuration/standalone-full.xml` でverify-clientを「requested」に更新して、ファイルを変更する必要があります `/subsystem=undertow/server=default-server/https-listener=default-https`CACを有効にします。Insight Serverにログインし、該当するコマンドを実行します。

OS	スクリプト
Windows の場合	<install dir> を参照してください\enableCACforRemoteEJB.bat
Linux の場合	/opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB.sh

スクリプトの実行後、wildflyサーバのリロードが完了するまで待ってから、次の手順に進みます。

4. OnCommand Insight サーバを再起動します。

スマートカードおよび証明書によるログインのためのCognosの設定（OnCommand Insight 7.3.10以降）

Cognosサーバでスマートカード（CAC）および証明書によるログインをサポートするには、OnCommand Insight Data Warehouseの設定を変更する必要があります。

作業を開始する前に

この手順 は、OnCommand Insight 7.3.10以降を実行しているシステム用です。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "Windowsホストにインストールされ ているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

手順

1. Cognos TrustoreにCertificate Authority（CA；認証局）を追加します。
   a. コマンドウィンドウで、に進みます `..\SANscreen\cognos\analytics\configuration\certs\`
   b. ユーティリティを使用し `keytool`て、信頼できるCAのリストを表示します。'..\..\IBM-JRE\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>

      各行の最初の単語はCAエイリアスを示します。
   c. 適切なファイルが存在しない場合は、CA証明書ファイル（通常は）を指定します `.pem` ファイル。
   d. OnCommand Insight の信頼済みCAに顧客のCAを含めるには、に進みます `..\SANscreen\cognos\analytics\configuration\certs\`。
   e. を使用します `keytool` をインポートするユーティリティ `.pem` ファイル： `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias`は通常、操作でCAを簡単に識別できるエイリアスです`keytool -list`。
   f. パスワードの入力を求められたら、_/ SANscreen /bin/cognos_info.dat_ファイルからパスワードを入力します。
   g. 回答 `yes` 証明書を信頼するように求められたら、
2. CACモードをイネーブルにするには、次の手順を実行します。
   a. 次の手順に従って、CACログアウトページを設定します。
      - Cognosポータルにログオンします（ユーザはシステム管理者グループ（cognos_admin）に属している必要があります）。
      - （7.3.10および7.3.11の場合のみ）[管理]→[構成]→[システム]→[セキュリティ]をクリックします
      - （7.3.10および7.3.11の場合のみ）Logout Redirect URL-> Applyに対してcacLogout.htmlと入力します

- ブラウザを閉じます。

b. 実行 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. IBM Cognosサービスを開始します。Cognosサービスが開始されるまで待ちます。

3. CACモードを無効にするには、次の手順を実行します。

a. 実行 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. IBM Cognosサービスを開始します。Cognosサービスが開始されるまで待ちます。

c. （7.3.10および7.3.11の場合のみ）次の手順に従って、CACログアウトページの設定を解除します。

- Cognosポータルにログオンします（ユーザはシステム管理者グループ（cognos_admin）に属している必要があります）。
- [管理]→[設定]→[システム]→[セキュリティ]をクリックします
- Logout Redirect URL-> Applyに対してcacLogout.htmlと入力します
- ブラウザを閉じます。

CognosおよびDWHのCA署名SSL証明書のインポート（Insight 7.3.10以降）

SSL証明書を追加して、Data WarehouseおよびCognos環境の認証と暗号化を強化することができます。

作業を開始する前に

この手順 は、OnCommand Insight 7.3.10以降を実行しているシステム用です。

CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。

- "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
- "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
- "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
- "Windowsホストにインストールされ ているOnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

このタスクについて

この手順 を実行するには、admin権限が必要です。

手順

1. IBM Cognos Configurationツールを使用してCognosを停止します。Cognosを閉じます。
2. のバックアップを作成します `..\SANScreen\cognos\analytics\configuration` および `..\SANScreen\cognos\analytics\temp\cam\freshness` フォルダ。
3. Cognosから証明書暗号化要求を生成します。Admin CMDウィンドウで、次のコマンドを実行します。
   a. CD "`\Program Files\sanscreen\cognos\analytics\bin`"
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`です。注意:ここで-Hと-IはdnsやipaddressのようなsubjectAltNamesを追加します。
   c. <password>の場合は、_/ SANscreen /bin/cognos_info.dat_ファイルのパスワードを使用します。
4. を開きます `c:\temp\encryptRequest.csr` ファイルを作成し、生成されたコンテンツをコピーします。
5. encryptRequest.csrコンテンツを入力し、CA署名ポータルを使用して証明書を生成します。
6. PKCS7形式を使用してルート証明書を含め、チェーン証明書をダウンロードします

   FQDNの.p7bファイルがダウンロードされます
7. CAから.p7b形式の証明書を取得します。Cognos Webサーバの証明書としてマークする名前を使用します。
8. ThirdPartyCertificateTool.batはチェーン全体をインポートできないため、すべての証明書をエクスポートするには複数の手順が必要です。チェーンを次のように個別にエクスポートして分割します。
   a. "`Crypto Shell Extensions`"の.p7b証明書を開きます。
   b. 左側のペインで「証明書」を参照します。
   c. ルートCA > All Tasks > Exportを右クリックします。
   d. Base64出力を選択します。
   e. ルート証明書として識別するファイル名を入力します。
   f. 手順8aから8eを繰り返して、すべての証明書を.cerファイルに個別にエクスポートします。
   g. ファイルにmediateX.cerとcognos.cerという名前を付けます。
9. CA証明書が1つしかない場合は、この手順を無視します。それ以外の場合は、root.cerとintermediateX.cerの両方を1つのファイルにマージします。
   a. メモ帳でroot.cerを開き、内容をコピーします。
   b. メモ帳を使用してintermediate.cerを開き、9aのコンテンツを追加します（最初に中間、次にルート）。
   c. ファイルをchain.cerとして保存します。
10. Admin CMDプロンプトを使用して、Cognosキーストアに証明書をインポートします。
    a. cd「Program Files\SANscreen\cognos\analytics\bin`」
    b. ThirdPartyCertificateTool.bat - java：local -i -T -r c：\temp\root.cer
    c. ThirdPartyCertificateTool.bat - java：local -i -T -r c：\temp\intermediate.cer
    d. ThirdPartyCertificateTool.bat - java：local -i -e -r c：\temp\cognos.cer -t c：\temp\chain.cer

11. [IBM Cognos Configuration]を開きます。
    a. [Local Configuration]→[Security]→[Cryptography]→[Cognos]を選択します
    b. 「サードパーティCAを使用しますか？」を変更します。 Trueに設定します。
    c. 設定を保存します。
    d. Cognosを再起動します
12. Admin CMDプロンプトを使用して、最新のCognos証明書をcognos.crtにエクスポートします。
    a. CD "`C：\Program Files\SANscreen"
    b. java\bin\keytool.exe -exportcert -file c：\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password>-alias encryption
    c. <password>の場合は、_/ SANscreen /bin/cognos_info.dat_ファイルのパスワードを使用します。
13. DWHサーバのtrustoreをにバックアップしま す`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. Admin CMDプロンプトウィンドウを使用して、「c：\temp\cognos.crt」をDWH trustoreにインポートし、CognosとDWHの間のSSL通信を確立します。
    a. CD "`C：\Program Files\SANscreen"
    b. java\bin\keytool.exe -importcert -file c：\temp\cognos.crt -keystore wildfly\standalone\configuration\server.trustore -storepass <password>-alias cognos3rdca
    c. <password>の場合は、_/ SANscreen /bin/cognos_info.dat_ファイルのパスワードを使用します。
15. SANscreen サービスを再起動します。
16. DWHのバックアップを実行して、DWHがCognosと通信していることを確認します。
17. 次の手順は、「sl certificate」のみを変更し、デフォルトのCognos証明書を変更しない場合でも実行する必要があります。そうしないと、新しいSANscreen 証明書についてCognosから苦情が表示されたり、DWHバックアップを作成できない可能性があります。
    a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`
    b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass <password> -alias "ssl certificate"`
    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

    通常、これらの手順はCognos証明書のインポートプロセスの一環として実行します（を参照） "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

SSL証明書のインポート

SSL証明書を追加して強化された認証と暗号化を有効にすると、OnCommand Insight 環境のセキュリティを強化できます。

作業を開始する前に

システムが最小必要ビットレベル（1024ビット）を満たしていることを確認する必要があります。

このタスクについて

アップグレードの前にボルトをバックアップすることを強くお勧めします。

ボルトとパスワードの管理の詳細については、手順を参照してください"securityadminツール"。

手順

1. 元のキーストアファイルのコピーを作成します。 `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old`
2. キーストアの内容を表示します。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   キーストアの内容が表示されます。キーストアには少なくとも1つの証明書が必要です。 `"ssl certificate"`。
3. を削除します `"ssl certificate"`： `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. 新しいキーを生成します。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. 名と姓の入力を求められたら、使用するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を入力します。
   b. 組織および組織構造に関する次の情報を入力します。
      - Country：ISOの2文字の国の略語（USなど）
      - State or Province：組織の本社がある都道府県の名前（例：Massachusetts）
      - Locality：組織の本社がある市区町村の名前（例：Waltham）
      - Organizational name：ドメイン名を所有する組織の名前（例：NetApp）
      - Organizational unit name：証明書を使用する部門またはグループの名前（Supportなど）
      - Domain Name/Common Name：サーバのDNSルックアップに使用されるFQDN（例：www.example.com）。システムから次のような情報が返されます。 `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
   c. 入力するコマンド `Yes` Common Name（CN；共通名）がFQDNになっている場合。
   d. キーのパスワードの入力を求められたら、パスワードを入力するか、Enterキーを押して既存のキーストアパスワードを使用します。
5. 証明書要求ファイルを生成します。 `C:\Program Files\SANscreen\java64\bin\keytool.exe`

```
-certreq -alias "ssl certificate" -keystore "c:\Program
Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file
c:\localhost.csr
```

。 `c:\localhost.csr` fileは、新しく生成される証明書要求ファイルです。

6. を送信します `c:\localhost.csr` を承認のためにCertificate Authority（CA；認証局）に送信します。

   証明書要求ファイルが承認されたら、で証明書を返す必要があります `.der` の形式で入力しファイルがとして返される場合と返されない場合があります `.der` ファイル。デフォルトのファイル形式はです `.cer` Microsoft CAサービスの場合。

   ほとんどの組織のCAは、ルートCAを含む信頼チェーンモデルを使用しています。ルートCAは、多くの場合オフラインです。中間CAと呼ばれる少数の子CAの証明書にのみ署名しています。

   公開鍵（証明書）は、信頼チェーン全体（OnCommand Insight サーバの証明書に署名したCAの証明書、およびその署名CAから組織のルートCAまでのすべての証明書）を取得する必要があります。

   組織によっては、署名要求を送信すると、次のいずれかが送信される場合があります。

   - 署名済み証明書と信頼チェーン内のすべてのパブリック証明書を含むPKCS12ファイル
   - A `.zip` 個 々 のファイル（署名済み証明書を含む）および信頼チェーン内のすべてのパブリック証明書を含むファイル
   - 署名済み証明書のみ

     パブリック証明書を入手する必要があります。

7. server.keystoreの承認済み証明書をインポートします。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   a. プロンプトが表示されたら、キーストアのパスワードを入力します。

      次のメッセージが表示されます。 `Certificate reply was installed in keystore`

8. server.trustoreの承認済み証明書をインポートします。 `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"`

   a. プロンプトが表示されたら、trustoreパスワードを入力します。

      次のメッセージが表示されます。 `Certificate reply was installed in trustore`

9. を編集します `SANscreen\wildfly\standalone\configuration\standalone-full.xml` ファイル：

   次のエイリアス文字列を置き換えます。 `alias="cbc-oci-02.muccbc.hq.netapp.com"`。例：

```
<keystore path="server.keystore" relative-to="jboss.server.config.dir"
keystore-password="${VAULT::HttpsRealm::keystore_password::1}" alias="cbc-oci-
```

```
02.muccbc.hq.netapp.com" key-
password="${VAULT::HttpsRealm::key_password::1}"/>
```

10. SANscreen サーバサービスを再起動します。

    Insightが起動したら、鍵のアイコンをクリックして、システムにインストールされている証明書を表示できます。

    「Issued To」の情報が「Issued By」の情報と一致する証明書が表示された場合、まだ自己署名証明書がインストールされています。Insightのインストーラで生成される自己署名証明書の有効期限は100年です。

    この手順 でデジタル証明書に関する警告が削除されることを保証することはできません。ネットアップでは、エンドユーザのワークステーションの設定方法を制御できません。次のシナリオを検討してください。

    - Microsoft Internet ExplorerとGoogle Chromeは、どちらもWindowsでMicrosoftのネイティブ証明書機能を使用します。

      つまり、Active Directory管理者が組織のCA証明書をエンドユーザーの証明書トラスストアにプッシュすると、OnCommand Insight の自己署名証明書が内部CAインフラストラクチャによって署名された証明書に置き換えられたときに、これらのブラウザのユーザーに証明書の警告が表示されなくなります。

    - JavaおよびMozilla Firefoxには独自の証明書ストアがあります。

      システム管理者がこれらのアプリケーションの信頼された証明書ストアにCA証明書を自動で取り込んでいない場合、自己署名証明書が置き換えられても、信頼されていない証明書が原因で、Firefoxブラウザで証明書に関する警告が引き続き生成されることがあります。組織の証明書チェーンをtrustoreにインストールすることは、追加の要件です。

ビジネスエンティティ階層

ビジネスエンティティを定義して、環境のデータをより細かく追跡し、レポートすることができます。

OnCommand Insight では、ビジネスエンティティ階層に次のレベルが含まれます。

- *テナント*は、主にサービスプロバイダがリソースをお客様（ネットアップなど）に関連付けるために使用します。
- *基幹業務（LOB）*は、データストレージなど、社内の基幹業務または製品ラインです。
- *ビジネスユニット*は、法務部門やマーケティング部門などの従来のビジネスユニットを表します。
- *プロジェクト*は、多くの場合、容量チャージバックが必要なビジネスユニット内の特定のプロジェクトを識別するために使用されます。たとえば、法務部門の場合は「Patents」、マーケティング部門の場合は「Sales Events」のようになります。レベル名にはスペースを含めることができます。

企業階層の設計では、すべてのレベルを使用する必要はありません。

ビジネスエンティティ階層の設計

企業構造の要素と、ビジネスエンティティで何を表す必要があるかを理解する必要があります。これは、それらがOnCommand Insight データベースで固定構造になるためです。次の情報を使用してビジネスエンティティをセットアップできます。これらのカテゴリのデータを収集するために、すべての階層レベルを使用する必要はないことに注意してください。

手順

1. ビジネスエンティティ階層の各レベルを調べて、そのレベルを会社のビジネスエンティティ階層に含める必要があるかどうかを判断します。
   - *テナント*レベルは、会社がISPで、顧客のリソース使用状況を追跡する場合に必要です。
   - *さまざまな製品ラインのデータを追跡する必要がある場合は、基幹業務（LOB）*が階層に必要です。
   - *部門ごとにデータを追跡する必要がある場合は、ビジネスユニット*が必要です。この階層レベルは、1つの部門が使用するリソースと、他の部門が使用しないリソースを分離するのに役立ちます。
   - *プロジェクト*レベルは、部門内の特殊な作業に使用できます。このデータは、企業や部門内の他のプロジェクトと比較して、個別のプロジェクトのテクノロジニーズを特定、定義、および監視するのに役立ちます。
2. 各ビジネスエンティティとそのエンティティ内のすべてのレベルの名前を示すグラフを作成します。
3. 階層内の名前をチェックして、OnCommand Insight のビューやレポートでわかりやすい名前になっていることを確認します。
4. 各ビジネスエンティティに関連付けられているアプリケーションをすべて特定します。

ビジネスエンティティを作成しています

会社のビジネスエンティティ階層を設計したら、アプリケーションをセットアップし、ビジネスエンティティをアプリケーションに関連付けることができます。このプロセスにより、OnCommand Insight データベースにビジネスエンティティ構造が作成されます。

このタスクについて

アプリケーションとビジネスエンティティの関連付けはオプションですが、これを推奨します。

手順

1. Insight Web UIにログインします。
2. をクリックし、[ビジネスエンティティ]*を選択します。

   [Business Entities]ページが表示されます。
3. をクリックします

新しいエンティティの構築を開始します。

   [ビジネスエンティティの追加]*ダイアログボックスが表示されます。

4. 各エンティティレベル（テナント、基幹業務、ビジネスユニット、プロジェクト）について、次のいずれかを実行できます。
   - エンティティレベルリストをクリックし、値を選択します。
   - 新しい値を入力し、Enterキーを押します。
   - ビジネスエンティティにエンティティレベルを使用しない場合は、エンティティレベルの値をN/Aのままにします。
5. [保存（ Save ）] をクリックします。

アセットへのビジネスエンティティの割り当て

ビジネスエンティティをアセット（ホスト、ポート、ストレージ、スイッチ、仮想マシン、 ビジネスエンティティをアプリケーションに関連付けずにqtree、共有、ボリューム、または内部ボリューム）を割り当てることができます。ただし、ビジネスエンティティに関連するアプリケーションにアセットが関連付けられている場合は、アセットにビジネスエンティティが自動的に割り当てられます。

作業を開始する前に

ビジネスエンティティを作成しておく必要があります。

このタスクについて

ビジネスエンティティはアセットに直接割り当てることができますが、アセットにアプリケーションを割り当ててから、ビジネスエンティティをアセットに割り当てることを推奨します。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法で、ビジネスエンティティを適用するアセットを選択します。
   - [Assets Dashboard]でアセットをクリックします。
   - をクリックします ツールバーの*[アセットの検索]*ボックスを表示するには、アセットの名前を入力し、リストからアセットを選択します。
3. アセットページの*セクションで、[Business Entities]の横にある[None]*にカーソルを合わせ、をクリックします 。

   使用可能なビジネスエンティティのリストが表示されます。
4. [検索]*ボックスに入力してリストをフィルタするか、リストを下にスクロールしてリストからビジネスエンティティを選択します。

   選択したビジネスエンティティがアプリケーションに関連付けられている場合は、アプリケーション名が表示されます。この場合、ビジネスエンティティ名の横に「データベース」という単語が表示されます。エンティティをアセットに対してのみ保持し、関連付けられているアプリケーションを保持しない場合は、アプリケーションの割り当てを手動で上書きできます。
5. ビジネスエンティティから派生したアプリケーションを上書きするには、アプリケーション名にカーソルを合わせ、をクリックします をクリックし、別のビジネスエンティティを選択し、リストから別のア

プリケーションを選択します。

複数のアセットに対するビジネスエンティティの割り当てまたは削除

ビジネスエンティティを手動で割り当てたり削除したりする代わりに、クエリを使用して複数のアセットに対して割り当てたり削除したりすることができます。

作業を開始する前に

目的のアセットに追加するビジネスエンティティを作成しておく必要があります。

手順

1. 新しいクエリを作成するか、既存のクエリを開きます。
2. 必要に応じて、ビジネスエンティティを追加するアセットでフィルタを適用します。
3. リストから目的のアセットを選択するか、をクリックします をクリックして*すべて*を選択します。

   [アクション]*ボタンが表示されます。

4. 選択したアセットにビジネスエンティティを追加するには、をクリックします

。選択したアセットタイプにビジネスエンティティを割り当てることができる場合は、*[ビジネスエンティティの追加]*を選択するメニューが表示されます。これを選択します。
5. リストから目的のビジネスエンティティを選択し、*[保存]*をクリックします。

   新しいビジネスエンティティを割り当てると、アセットにすでに割り当てられているビジネスエンティティよりも優先されます。アプリケーションをアセットに割り当てると、割り当てられているビジネスエンティティも同じ方法で上書きされます。ビジネスエンティティをアセットとして割り当てると、そのアセットに割り当てられているアプリケーションよりも優先される可能性があります。

6. アセットに割り当てられているビジネスエンティティを削除するには、をクリックします

をクリックし、*[Remove Business Entity]*を選択します。
7. リストから目的のビジネスエンティティを選択し、*[削除]*をクリックします。

アノテーションの定義

OnCommand Insight でのデータの追跡方法を企業の要件に合わせてカスタマイズする場合は、アノテーションによってデータの全体像を定義できます。たとえば、アセットの耐用年数、データセンター、建物の場所、ストレージ階層、ボリューム、 および内部ボリュームのサービスレベル。

手順

1. 環境のデータを関連付ける必要がある業界固有の用語をリストします。
2. 環境データを関連付ける必要がある企業用語（ビジネスエンティティを使用してまだ追跡されていない用語）をリストします。

3. 使用できるデフォルトのアノテーションタイプがないかどうかを特定します。
4. 作成する必要があるカスタムアノテーションを特定します。

アノテーションを使用した環境の監視

企業の要件に合わせてデータを追跡するようにOnCommand Insight をカスタマイズする場合は、_annotations_という特殊なメモを定義してアセットに割り当てることができます。たとえば、アセットの終了日、データセンター、建物の場所、ストレージ階層、ボリュームのサービスレベルなどの情報をアノテートできます。

環境の監視にアノテーションを使用すると、次の作業に役立ちます。

- すべてのアノテーションタイプの定義を作成または編集します。
- アセットページを表示し、各アセットを 1 つ以上のアノテーションに関連付ける。

  たとえば、リースしているアセットのリース期限が 2 カ月以内の場合、終了日のアノテーションを適用すると、これにより、他のユーザがそのアセットを長期間使用できないようにすることができます。

- ルールを作成して、同じタイプの複数のアセットにアノテーションを自動的に適用する。
- アノテーションインポートユーティリティを使用してアノテーションをインポートする。
- アノテーションに基づいてアセットをフィルタする。
- アノテーションに基づいてレポートにデータをグループ化し、レポートを生成する。

  レポートの詳細については、OnCommand Insight レポートガイド_を参照してください。

アノテーションタイプの管理

OnCommand Insight には、アセットのライフサイクル（開始日や終了日）、建物やデータセンターの場所、階層など、カスタマイズしてレポートに表示できるデフォルトのアノテーションタイプがいくつか用意されています。デフォルトのアノテーションタイプの値を定義することも、独自のカスタムアノテーションタイプを作成することもできます。これらの値は後で編集できます。

デフォルトのアノテーションタイプ

OnCommandInsightには、デフォルトのアノテーションタイプがいくつか用意されています。これらのアノテーションを使用して、データをフィルタまたはグループ化したり、データレポートをフィルタリングしたりできます。

次のようなデフォルトのアノテーションタイプをアセットに関連付けることができます。

- アセットのライフサイクル：開始日、停止日、終了日など
- デバイスの場所の情報。データセンター、建物、フロアなど
- 品質（階層）、接続デバイス（スイッチレベル）、サービスレベルなどのアセットの分類
- ステータス（ホット（高利用率）など）

次の表に、デフォルトのアノテーションタイプを示します。これらのアノテーションの名前は必要に応じて編集できます。

アノテーションタイプ	説明	を入力します
エイリアス	リソースのフレンドリ名。	テキスト（ Text ）
誕生日	デバイスがオンラインになった日付、またはオンラインになる予定の日付。	日付
建物	ホスト、ストレージ、スイッチ、およびテープリソースの物理的な場所。	リスト
市区町村	ホスト、ストレージ、スイッチ、およびテープリソースが配置されている自治体。	リスト
コンピュートリソースグループ	Host and VM File Systemsデータソースで使用されるグループ割り当て。	リスト
大陸	ホスト、ストレージ、スイッチ、およびテープリソースの地理的な場所。	リスト
国名	ホスト、ストレージ、スイッチ、およびテープリソースが配置されている国。	リスト
データセンター	リソースの物理的な場所。ホスト、ストレージアレイ、スイッチ、およびテープで使用できます。	リスト
直接接続	ストレージリソースがホストに直接接続されているかどうか（[Yes]または[No]）を示します。	ブール値
サポート終了	リースの期限が切れた場合やハードウェアが撤去される場合など、デバイスがオフラインになる日付。	日付
ファブリックエイリアス	ファブリックのフレンドリ名。	テキスト（ Text ）

床	建物のフロア上のデバイスの場所。ホスト、ストレージアレイ、スイッチ、およびテープに対して設定できます。	リスト
ホット	定期的に頻繁に使用されている、または容量のしきい値に達しているデバイス。	ブール値
注	リソースに関連付けるコメント。	テキスト（ Text ）
ラック	リソースが配置されているラック。	テキスト（ Text ）
部屋	ホスト、ストレージ、スイッチ、およびテープリソースが配置されている建物内の部屋。	リスト
SAN	ネットワークの論理パーティション。ホスト、ストレージアレイ、テープ、スイッチ、アプリケーションで使用できます。	リスト
サービスレベル	リソースに割り当てることができる一連のサポート対象サービスレベル。内部ボリューム、 qtree 、およびボリュームの番号付きのオプションのリストが用意されています。サービスレベルを編集して、各レベルのパフォーマンスポリシーを設定できます。	リスト
都道府県	リソースが配置されている都道府県。	リスト
日没	そのデバイスに新しい割り当てを実行できないしきい値。計画的な移行や保留中のネットワークの変更に役立ちます。	日付
スイッチレベル	スイッチのカテゴリを設定するための事前定義されたオプションが含まれています。通常、これらの指定はデバイスの寿命の間維持されますが、必要に応じて編集できます。スイッチに対してのみ設定できます。	リスト

階層	を使用すると、環境内のさまざまなサービスレベルを定義できます。階層では、必要な速度などのレベルを定義できます（例： Gold や Silver ）。この機能は、内部ボリューム、 qtree 、ストレージアレイ、ストレージプール、およびボリュームに対してのみ使用できます。	リスト
違反の重大度	違反（ホストポートの欠落や冗長性の欠如など）のランク（例： Major ）。重要度の高い順に階層化されています。	リスト

エイリアス、データセンター、ホット、サービスレベル、サンセット、 スイッチレベル、サービスレベル、階層、および違反の重大度はシステムレベルのアノテーションであり、削除や名前変更はできません。変更できるのは割り当てられている値のみです。

アノテーションの割り当て方法

アノテーションは、手動またはアノテーションルールを使用して自動で割り当てることができます。また、OnCommand Insight では、アセットの取得時と継承時に一部のアノテーションが自動的に割り当てられます。アセットに割り当てたアノテーションは、アセットページの[User Data]セクションに表示されます。

アノテーションは次の方法で割り当てられます。

- アセットにアノテーションを手動で割り当てることができます。

  アノテーションがアセットに直接割り当てられている場合、そのアノテーションはアセットページに通常のテキストとして表示されます。手動で割り当てたアノテーションは、継承またはアノテーションルールで割り当てられたアノテーションよりも常に優先されます。

- アノテーションルールを作成して、同じタイプのアセットにアノテーションを自動的に割り当てることができます。

  ルールに基づいてアノテーションが割り当てられている場合、Insightのアセットページのアノテーション名の横にルール名が表示されます。

- Insightでは、階層レベルがストレージ階層モデルに自動的に関連付けられるため、アセットを取得したときにリソースにストレージのアノテーションをすばやく割り当てることができます。

  特定のストレージリソースは、事前定義された階層（階層1と階層2）に自動的に関連付けられます。たとえば、Symmetrixストレージ階層はSymmetrixおよびVMAXファミリーに基づいており、階層1に関連付けられています。デフォルト値は、階層の要件に合わせて変更できます。Insightによって割り当てられたアノテーション（階層など）については、アセットページでアノテーションの名前にカーソルを合わせると「システム定義」と表示されます。

- 一部のリソース（アセットの子）では、事前定義された階層のアノテーションをアセット（親）から取得

できます。

たとえば、ストレージにアノテーションを割り当てた場合、そのストレージに属するすべてのストレージプール、内部ボリューム、ボリューム、qtree、および共有に階層のアノテーションが適用されます。ストレージの内部ボリュームに別のアノテーションを適用すると、それ以降はすべてのボリューム、qtree、および共有にアノテーションが適用されます。アセットページのアノテーション名の横に「データベース」と表示されます。

アノテーションにコストを関連付ける

コスト関連のレポートを実行する前に、システムレベルのService Level、Switch Level、およびTierのアノテーションにコストを関連付ける必要があります。これにより、本番環境での実際の使用状況やレプリケートされた容量に基づいて、ストレージユーザへのチャージバックが可能になります。たとえば、階層レベルとしてGoldとSilverを設定し、Gold階層にSilver階層よりも高いコストを割り当てることができます。

手順

1. InsightWeb UIにログインします。
2. [管理]をクリックし、*[アノテーション]*を選択します。

   [Annotation]ページが表示されます。

3. Service Level、Switch Level、またはTierのアノテーションにカーソルを合わせ、をクリックします 。

   [Edit Annotation]ダイアログボックスが表示されます。

4. [コスト]フィールドに既存のレベルの値を入力します。

   TierアノテーションにはAuto TierとService Levelアノテーションの値が設定されており、Object Storageの値は削除できません。

5. をクリックします

をクリックしてレベルを追加します。
6. 完了したら、*[保存]*をクリックします。

カスタムアノテーションの作成

アノテーションを使用すると、ビジネスニーズに合わせて、ビジネス固有のカスタムデータをアセットに追加できます。OnCommand Insight には一連のデフォルトアノテーションが用意されていますが、別の方法でデータを表示することもできます。カスタムアノテーションのデータは、スイッチのメーカー、ポートの数、パフォーマンス統計など、すでに収集されたデバイスの補足データになります。アノテーションを使用して追加したデータはInsightで検出されません。

手順

1. Insight Web UIにログインします。

2. をクリックし、[アノテーション]*を選択します。

   アノテーションページにアノテーションのリストが表示されます。

3. をクリックします

。

   [注釈の追加]*ダイアログボックスが表示されます。

4. * Name *および*概要 *フィールドに名前と概要 を入力します。

   これらのフィールドには、 255 文字まで入力できます。

   アノテーション名の先頭または末尾にドットが付いています。 はサポートされていません。

5. * タイプ * をクリックし、このアノテーションで使用できるデータのタイプを表す次のオプションのいずれかを選択します。

   - ブール値

     これにより、yesとnoの選択肢を含むドロップダウンリストが作成されますたとえば、"`DirectAttached""アノテーションはブール型です。

   - 日付

     これにより、日付を保持するフィールドが作成されます。たとえば、アノテーションで日付を指定する場合は、このオプションを選択します。

   - リスト

     これにより、次のいずれかが作成されます。

     - 固定のドロップダウンリスト

       このアノテーションタイプをデバイスに割り当てるときにユーザがリストに値を追加することはできません。

     - 可変のドロップダウンリスト

       このリストの作成時に*[Add new values on the fly]*オプションを選択した場合、他のユーザがこのアノテーションタイプをデバイスに割り当てているときに、リストに値を追加できます。

   - 番号

     これにより、アノテーションを割り当てるユーザが数値を入力できるフィールドが作成されます。たとえば、アノテーションタイプが「floor」の場合は、「Value Type」として「number」を選択してフロア番号を入力できます。

   - テキスト（ Text ）

     これにより、自由形式のテキストを使用できるフィールドが作成されます。たとえば、アノテーションタイプとして「Language」と入力し、値タイプとして「Text」を選択し、言語を値として入力します。

タイプを設定して変更を保存したあとで、アノテーションのタイプを変更することはできません。タイプを変更する必要がある場合は、アノテーションを削除して新規に作成する必要があります。

6. 注釈タイプとして[**List**]を選択した場合は、次の手順を実行します。
   a. アセットページでアノテーションの値を追加して柔軟なリストを作成できるようにするには、「 * オンザフライで新しい値を追加」を選択します。

      たとえば、アセットページで、 Detroit 、 Tampa 、および Boston の値が設定された City アノテーションをアセットに割り当てているとします。「 * オンザフライで新しい値を追加」オプションを選択した場合は、「アノテーション」ページに移動して値を追加する代わりに、アセットページでサンフランシスコやシカゴなどの都市に直接値を追加できます。このオプションを選択しないと、アノテーションの適用時に新しいアノテーション値を追加できません。これにより固定リストが作成されます。

   b. 値と名前を*値*および*概要 *フィールドに入力します。
   c. をクリックします

 をクリックして値を追加します。
   d. をクリックします 値を削除します。
7. [保存（ Save ）] をクリックします。

   アノテーションがアノテーションページのリストに表示されます。

   ◦ 関連情報 *

"ユーザーデータのインポートとエクスポート"

アセットへのアノテーションの手動割り当て

アセットにアノテーションを割り当てると、アセットをビジネスに関連付けてソート、グループ化、レポートするのに役立ちます。アノテーションルールを使用して特定のタイプのアセットにアノテーションを自動的に割り当てることができますが、アセットページで個 々 のアセットにアノテーションを割り当てることができます。

作業を開始する前に

割り当てるアノテーションを作成しておく必要があります。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法で、アノテーションを適用するアセットを選択します。
   ◦ [Assets Dashboard]でアセットをクリックします。
   ◦ をクリックします ツールバーの*[アセットの検索]*ボックスを表示するには、アセットのタイプまたは名前を入力し、表示されるリストからアセットを選択します。

     アセットページが表示されます。

3. アセットページの*[User Data]*セクションで、をクリックします

。

   [注釈の追加] ダイアログボックスが表示されます。

4. [注釈（Annotation）]*をクリックし、リストから注釈を選択します。
5. [値]*をクリックし、選択したアノテーションのタイプに応じて次のいずれかを実行します。
   - アノテーションタイプがリスト、日付、またはブーリアンの場合は、値をリストから選択します。
   - アノテーションタイプがテキストの場合は、値を入力します。
6. [保存（ Save ）] をクリックします。
7. アノテーションの割り当て後に値を変更する場合は、をクリックします 別の値を選択します。

   アノテーションのリストタイプで*[アノテーションの割り当て時に動的に値を追加する]*オプションが選択されている場合は、既存の値を選択するだけでなく、新しい値を入力して追加することもできます。

アノテーションの変更

アノテーションの名前、概要 、値を変更したり、不要になったアノテーションを削除したりできます。

手順

1. OnCommand InsightWeb UIにログインします。
2. をクリックし、[アノテーション]*を選択します。

   [アノテーション]ページが表示されます。

3. 編集するアノテーションにカーソルを合わせ、をクリックします 。

   [注釈の編集]*ダイアログボックスが表示されます。

4. アノテーションには次の変更を加えることができます。

   a. 名前、概要 、またはその両方を変更します。

      ただし、名前と概要 の最大文字数は255文字で、アノテーションのタイプを変更することはできません。また、システムレベルのアノテーションの場合、名前や概要 を変更することはできません。ただし、リストタイプのアノテーションの場合は値を追加または削除できます。

      Data Warehouseに公開されているカスタムアノテーションの名前を変更すると、履歴データが失われます。

   a. リストタイプのアノテーションに別の値を追加するには、をクリックします

。
   b. リストタイプのアノテーションから値を削除するには、をクリックします 。

      アノテーションルール、クエリ、またはパフォーマンスポリシーに含まれるアノテーションに関連付けられているアノテーション値は削除できません。

5. 完了したら、*[保存]*をクリックします。

完了後

Data Warehouseでアノテーションを使用する場合は、Data Warehouseでアノテーションを強制的に更新する必要があります。OnCommand Insight Data Warehouseアドミニストレーションガイド_を参照してください。

アノテーションを削除する

必要に応じて、不要になったアノテーションを削除できます。システムレベルのアノテーションや、アノテーションルール、クエリ、パフォーマンスポリシーで使用されているアノテーションは削除できません。

手順

1. OnCommand Insight Web UIにログインします。
2. をクリックし、[アノテーション]*を選択します。

   [アノテーション]ページが表示されます。

3. 削除するアノテーションにカーソルを合わせ、をクリックします 。

   確認の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。

アノテーションルールを使用してアセットにアノテーションを割り当てる

定義した条件に基づいてアセットにアノテーションを自動的に割り当てるには、アノテーションルールを設定します。OnCommand Insight は、これらのルールに基づいてアセットにアノテーションを割り当てます。Insightには、デフォルトのアノテーションルールも2つ用意されています。必要に応じて変更したり、不要な場合は削除したりできます。

デフォルトのストレージアノテーションルール

リソースにストレージのアノテーションを迅速に割り当てるために、OnCommand Insight には、ストレージ階層モデルに階層レベルを関連付ける21のデフォルトのアノテーションルールが用意されています。環境内の資産を取得すると、すべてのストレージリソースが自動的に階層に関連付けられます。

デフォルトのアノテーションルールでは、階層のアノテーションが次のように適用されます。

- 階層1のストレージ品質

  階層1のアノテーションが適用されるベンダーと指定ファミリーは次のとおりです。EMC（Symmetrix）、HDS（HDS9500V、HDS9900、HDS9900V、R600、 R700、USP r、USP V）、IBM（DS8000）、NetApp（FAS6000またはFAS6200）、およびViolin（メモリ）。

- 階層2、ストレージ品質の階層

  階層2のアノテーションが適用されるベンダーと指定ファミリーは、HP（3PAR StoreServまたはEVA）、EMC（CLARiX）、HDS（AMSまたはD800）、IBM（XIV）、NetApp（FAS3000、FAS3100、FAS3200）です。

これらのルールのデフォルト設定は階層の要件に合わせて編集することも、不要な場合は削除することもできます。

アノテーションルールの作成

アノテーションを個々のアセットに手動で適用する代わりに、アノテーションルールを使用して複数のアセットに自動的にアノテーションを適用することができます。個々のアセットページで手動で設定したアノテーションは、 Insight でアノテーションルールが評価されるときにルールベースのアノテーションよりも優先されます。

作業を開始する前に

アノテーションルールのクエリを作成しておく必要があります。

このタスクについて

アノテーションタイプはルールの作成中に編集することもできますが、事前に定義しておくことを推奨します。

手順

1. OnCommand Insight Web UIにログインします。
2. をクリックし、[アノテーションルール]*を選択します。

   アノテーションルールページに、既存のアノテーションルールのリストが表示されます。

3. をクリックします

。

   [Add Rule]ダイアログボックスが表示されます。

4. 次の手順を実行します。
   a. [* 名前 *] ボックスに、ルールを説明する一意の名前を入力します。

      この名前はアノテーションルールページに表示されます。

   b. [クエリ]*をクリックし、アセットにアノテーションを適用する際にOnCommand Insight で使用するクエリを選択します。
   c. [* Annotation*] をクリックし、適用する注釈を選択します。
   d. * 値 * をクリックし、アノテーションの値を選択します。

      たとえば、 Birthday のアノテーションを選択した場合は、日付の値を指定します。

5. [保存（ Save ）] をクリックします。

6. すべてのルールをすぐに実行する場合は、 * すべてのルールを実行 * をクリックします。それ以外の場合、ルールは定期的に実行されます。

アノテーションルールの優先順位を設定します

アノテーションルールはデフォルトでOnCommand Insight は順番に評価されますが、アノテーションルールが特定の順序で評価されるようにOnCommand Insight での評価順序を設定することができます。

手順

1. InsightWeb UIにログインします。
2. をクリックし、[アノテーションルール]*を選択します。

   アノテーションルールページに、既存のアノテーションルールのリストが表示されます。

3. アノテーションルールにカーソルを合わせます。

   優先順位の矢印がルールの右側に表示されます。

4. リスト内でルールを上下に移動するには、上矢印または下矢印をクリックします。

   デフォルトでは、新しいルールはルールのリストに順番に追加されます。個々のアセットページで手動で設定したアノテーションは、 Insight でアノテーションルールが評価されるときにルールベースのアノテーションよりも優先されます。

アノテーションルールの変更

アノテーションルールについて、ルールの名前、そのアノテーション、アノテーションの値、ルールに関連付けられているクエリを変更することができます。

手順

1. OnCommand InsightWeb UIにログインします。
2. をクリックし、[アノテーションルール]*を選択します。

   アノテーションルールページに、既存のアノテーションルールのリストが表示されます。

3. 変更するルールを選択します。
   - [Annotation Rules]ページでは、フィルタボックスに値を入力してアノテーションルールをフィルタできます。
   - アノテーションルールがページに収まらない場合は、ページ番号をクリックしてページごとに参照できます。
4. 次のいずれかを実行して、*[ルールの編集]*ダイアログボックスを表示します。
   - [Annotation Rules]ページが表示された場合は、アノテーションルールにカーソルを合わせ、をクリックします 。
   - アセットページで、ルールに関連付けられているアノテーションにカーソルを合わせ、ルール名が表

示されたらその名前にカーソルを合わせて、ルール名をクリックします。

5. 必要な変更を行い、*[保存]*をクリックします。

アノテーションルールを削除する

ネットワーク内のオブジェクトの監視に使用していたアノテーションルールが不要になった場合は、削除できます。

手順

1. OnCommand InsightWeb UIにログインします。
2. をクリックし、[アノテーションルール]*を選択します。

   アノテーションルールページに、既存のアノテーションルールのリストが表示されます。

3. 削除するルールを選択します。
   - [Annotation Rules]ページでは、フィルタボックスに値を入力してアノテーションルールをフィルタできます。
   - アノテーションルールが1ページに収まらない場合は、ページ番号をクリックしてページごとに参照できます。
4. 削除するルールにカーソルを合わせ、をクリックします 。

   ルールを削除するかどうかを確認するメッセージが表示されます。

5. [OK] をクリックします。

アノテーション値のインポート

SANオブジェクト（ストレージ、ホスト、仮想マシンなど）のアノテーションをCSVファイルで管理している場合は、その情報をOnCommand Insight にインポートできます。アプリケーション、ビジネスエンティティ、アノテーション（階層や建物など）をインポートできます。

このタスクについて

次のルールが適用されます。

- アノテーション値が空の場合、そのアノテーションはオブジェクトから削除されます。
- ボリュームまたは内部ボリュームをアノテートする場合、オブジェクト名はストレージ名とボリューム名をダッシュと矢印（->）で区切った形式になります。

```
<storage_name>-><volume_name>
```

- ストレージ、スイッチ、またはポートがアノテートされている場合、[Application]列は無視されます。
- ビジネスエンティティは、[Tenant]、[Line_of_Business]、[Business_Unit]、および[Project]の列で構成されます。

いずれの値も空のままにすることができます。アプリケーションがすでに入力値とは異なるビジネスエンティティに関連付けられている場合は、新しいビジネスエンティティに割り当てられます。

インポートユーティリティでは、次のオブジェクトタイプとキーがサポートされます。

を入力します	キーを押します
ホスト	id-><id> または <Name> または <IP>
VM	id-><id> または <Name>
ストレージプール	id-><id> または <Storage_name>-><Storage_Pool_name>
内部ボリューム	id-><id> または <Storage_name>-><Internal_volume_name>
ボリューム	id-><id> または <Storage_name>-><Volume_name>
ストレージ	id-><id> または <Name> または <IP>
スイッチ	id-><id> または <Name> または <IP>
ポート	id-><id> または <WWN>
共有	id-><id> または <Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol> <Qtree> は、デフォルトのqtreeがある場合は省略可能です。
qtree	id-><id> または <Storage Name>-><Internal Volume Name>-><Qtree Name>

CSVファイルの形式は次のとおりです。

```
, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]
```

手順

1. Insight Web UIにログインします。
2. をクリックし、[トラブルシューティング]*を選択します。

   [トラブルシューティング]ページが表示されます。

3. ページの*[その他のタスク]セクション*で、* OnCommand Insight Portal*リンクをクリックします。
4. [Insight Connect API]*をクリックします。
5. ポータルにログインします。
6. [Annotation Import Utility]*をクリックします。
7. を保存します `.zip` ファイルを解凍し、を読んでください `readme.txt` 追加情報 およびサンプル用のファイル。
8. CSVファイルをと同じフォルダに配置します `.zip` ファイル。
9. コマンドラインウィンドウで、次のように入力します。

   ```
   java -jar rest-import-utility.jar [-uusername] [-ppassword]
   [-aserver name or IP address] [-bbatch size] [-ccase
   sensitive:true/false]
   [-lextra logging:true/false] csv filename
   ```

   追加のロギングを有効にする-lオプションと、大文字と小文字を区別する-cオプションは、デフォルトでfalseに設定されます。したがって、これらの機能を使用する場合にのみ指定する必要があります。

   オプションとその値の間にスペースはありません。

次のキーワードは予約されており、ユーザはこれらのキーワードをアノテーション名として指定できません。-Application-Application_Priority -Tenant-Line_of_Business -Business_Unit -Projectいずれかの予約済みキーワードを使用してアノテーションタイプをインポートしようとすると、エラーが生成されます。アノテーションの名前にこれらのキーワードを使用している場合は、インポートユーティリティツールが正常に動作するように変更する必要があります。

Annotation ImportユーティリティにはJava 8またはJava 11が必要です。インポートユーティリティを実行する前に、これらのいずれかがインストールされていることを確認してください。最新のOpenJDK 11を使用することを推奨します。

クエリを使用して複数のアセットにアノテーションを割り当てる

アセットのグループにアノテーションを割り当てると、それらのアセットを識別しやすくなり、クエリやダッシュボードでそれらの関連するアセットを使用しやすくなります。

作業を開始する前に

アセットに割り当てるアノテーションは、事前に作成しておく必要があります。

このタスクについて

クエリを使用すると、アノテーションを複数のアセットに簡単に割り当てることができます。たとえば、カスタムのアドレスアノテーションをデータセンターの特定の場所にあるすべてのアレイに割り当てる場合などです。

手順

1. アノテーションを割り当てるアセットを特定するための新しいクエリを作成します。**>+**[新しいクエリ]*をクリックします。
2. ドロップダウンで[ストレージ]*を選択します。フィルタを設定して、表示されるストレージのリストをさらに絞り込むことができます。
3. 表示されたストレージのリストで、ストレージ名の横にあるチェックボックスをクリックして1つ以上を選択します。リストの上部にあるメインのチェックボックスをクリックして、表示されているすべてのストレージを選択することもできます。
4. 必要なストレージをすべて選択したら、**[**操作**]>***[アノテーションの編集]*をクリックします。

   [Add Annotation]ダイアログボックスが表示されます。

5. ストレージに割り当てる*と[値]を選択し、[保存]*をクリックします。

   そのアノテーションの列が表示されている場合は、選択したすべてのストレージで列が表示されます。

6. アノテーションを使用して、ウィジェットやクエリでストレージをフィルタリングできるようになりました。ウィジェットでは、次の操作を実行できます。

   a. ダッシュボードを作成するか、既存のダッシュボードを開きます。[Variable]*を追加し、上記のストレージで設定したアノテーションを選択します。変数がダッシュボードに追加されます。

b. 追加した変数フィールドで、* any *をクリックして、フィルタするための適切な値を入力します。チェックマークをクリックして変数値を保存します。

c. ウィジェットを追加します。ウィジェットの[Query]で、[**Filter by][+**]ボタンをクリックし、リストから適切な注釈を選択します。

d. [Any]*をクリックし、上記で追加したアノテーション変数を選択します。作成した変数は"$`"で始まり、ドロップダウンに表示されます。

e. 必要に応じて他のフィルタやフィールドを設定し、ウィジェットがカスタマイズされたら*[保存]*をクリックします。

ダッシュボードのウィジェットには、アノテーションを割り当てたストレージのデータのみが表示されます。

アセットを照会しています

クエリを使用すると、環境内のアセットをユーザが選択した条件（アノテーションとパフォーマンス指標）に基づいてきめ細かく検索することで、ネットワークの監視とトラブルシューティングを行うことができます。また、アセットにアノテーションを自動的に割り当てるアノテーションルールにはクエリが必要です。

クエリやダッシュボードで使用されるアセット

Insightのクエリとダッシュボードウィジェットは、さまざまなアセットタイプで使用できます

クエリ、ダッシュボードウィジェット、およびカスタムアセットページで使用できるアセットタイプは次のとおりです。フィルタ、式、表示に使用できるフィールドとカウンタは、アセットのタイプによって異なります。すべてのアセットをすべてのウィジェットタイプで使用できるわけではありません。

- アプリケーション
- データストア
- ディスク
- ファブリック
- 汎用デバイス
- ホスト
- 内部ボリューム
- iSCSI セッション
- iSCSI ネットワークポータル
- パス
- ポート
- qtree
- クォータ
- 共有

- ストレージ
- ストレージノード
- ストレージプール
- スイッチ
- テープ
- VMDK です
- 仮想マシン
- ボリューム
- ゾーン
- ゾーンメンバー

クエリを作成しています

クエリを作成して、環境内のアセットをきめ細かく検索することができます。クエリを使用すると、フィルタを追加して結果をソートし、インベントリデータとパフォーマンスデータを1つのビューに表示することで、データをスライスできます。

このタスクについて

たとえば、ボリュームのクエリを作成したり、選択したボリュームに関連付けられているストレージを検索するフィルタを追加したり、階層1などの特定のアノテーションを検索するフィルタを追加したりできます。 最後に、IOPS - Read（IO/秒）が25を超えるストレージをすべて検出するフィルタをもう1つ追加します。結果が表示されたら、クエリに関連付けられている各列で情報を昇順または降順にソートすることができます。

アセットを取得する新しいデータソースを追加したときや、アノテーションやアプリケーションの割り当てを行ったときに、クエリのインデックスが作成されたあとに、それらのアセット、アノテーション、またはアプリケーションを照会することができます。インデックスは定期的な間隔で作成されます。

手順

1. OnCommand Insight Web UIにログインします。
2. をクリックし、[+ New Query]*を選択します。
3. [リソースタイプの選択]*をクリックし、アセットのタイプを選択します。

   クエリでリソースを選択すると、いくつかのデフォルト列が自動的に表示されます。これらの列はいつでも削除したり、新しい列を追加したりできます。

4. [名前*]テキストボックスにアセットの名前を入力するか、テキストの一部を入力してアセット名を絞り込みます。

   [New Query]ページのテキストボックスでは、次のいずれかを単独で使用することも、組み合わせて使用することもできます。

   - アスタリスクを使用すると、すべての項目を検索できます。例： `vol*rhel` 「vol」で始まり「rhel」で終わるすべてのリソースを表示します。

- 疑問符を使用すると、特定の数の文字を検索できます。例： `BOS-PRD??-S12` BOS-PRD12-S12 、BOS-PRD13-S12などを表示します。
- OR 演算子を使用すると、複数のエンティティを指定できます。例： `FAS2240 OR CX600 OR FAS3270` 複数のストレージモデルを検出します。
- NOT 演算子を使用すると、検索結果からテキストを除外できます。例： `NOT EMC*` 「EMC」で始まらないものをすべて検索します。を使用できます `NOT *` 値のないフィールドを表示します。

5. をクリックします をクリックしてアセットを表示します。
6. 条件を追加するには、をクリックします

をクリックし、次のいずれかを実行します。
   - と入力して特定の条件を検索し、選択します。
   - リストを下にスクロールし、条件を選択します。
   - IOPS -読み取り（IO/秒）などのパフォーマンス指標を選択した場合は、値の範囲を入力します。Insightのデフォルトのアノテーションはで示されます ;重複する名前を持つ注釈を持つことができます。

   条件の列が[クエリ結果]リストに追加され、リスト内のクエリの結果が更新されます。
7. 必要に応じて、をクリックします をクリックして、クエリ結果からアノテーションまたはパフォーマンス指標を削除します。

   たとえば、データストアの最大レイテンシと最大スループットを表示するクエリで結果のリストに最大レイテンシのみを表示する場合は、このボタンをクリックし、* Throughput - Max *チェックボックスをオフにします。[Query results]のリストから[Throughput - Max（MB/s）]列が削除されます。

   > クエリ結果テーブルに表示される列の数によっては、追加された列を表示できない場合があります。目的の列が表示されるまで、1つまたは複数の列を削除できます。

8. をクリックし、クエリの名前を入力して[保存]*をもう一度クリックします。

   管理者ロールを持つアカウントがある場合は、カスタムダッシュボードを作成できます。カスタムダッシュボードはウィジェットライブラリの任意のウィジェットで構成でき、そのいくつかを使用してクエリ結果をカスタムダッシュボードに表示できます。カスタムダッシュボードの詳細については、_ OnCommand Insight スタートガイド_を参照してください。

   - 関連情報 *

"ユーザーデータのインポートとエクスポート"

クエリを表示する

アセットの監視に使用するクエリを表示して、アセットに関するデータの表示方法を変更できます。

手順

1. OnCommand Insight Web UIにログインします。

2. [* クエリ *] をクリックし、 [* すべてのクエリを表示 *] を選択します。
3. クエリの表示方法は次のいずれかの方法で変更できます。
   - [**filter**]ボックスにテキストを入力して、特定のクエリを表示できます。
   - 列見出しで矢印をクリックすると、クエリの表内の列のソート順序を昇順（上矢印）または降順（下矢印）に変更できます。
   - 列のサイズを変更するには、列見出しの上にカーソルを合わせ、青いバーが表示されるまで動かします。バーの上にマウスを置き、左右にドラッグします。
   - 列を移動するには、列ヘッダーをクリックし、左右にドラッグします。
   - クエリ結果をスクロールすると、Insightでデータソースが自動的にポーリングされるため、結果が変わる場合があります。これにより、一部の項目が表示されなくなったり、ソート方法によっては一部の項目が順序どおりに表示されない場合があります。

クエリ結果を **.csv** ファイルにエクスポートしています

クエリの結果を.csvファイルにエクスポートして、データを別のアプリケーションにインポートできます。

手順

1. OnCommand Insight Web UIにログインします。
2. [* クエリ *] をクリックし、 [* すべてのクエリを表示 *] を選択します。

   [クエリ] ページが表示されます。
3. クエリをクリックします。
4. をクリックします クエリ結果をにエクスポートします `.csv` ファイル。
5. 次のいずれかを実行します。
   - [名前を付けて開く] をクリックし、次に **OK** をクリックして Microsoft Excel でファイルを開き、特定の場所にファイルを保存します。
   - [ファイルの保存] をクリックし、 [OK] をクリックして、 [ダウンロード] フォルダにファイルを保存します。表示されている列の属性のみがエクスポートされます。表示されている一部の列、特に複雑なネストされたリレーションシップの一部である列はエクスポートされません。

     アセット名にカンマが含まれている場合は、アセット名と適切な.csv形式は維持され、エクスポート時に名前が引用符で囲まれます。

     +クエリ結果をエクスポートする場合、選択または画面に表示されている行だけでなく、結果テーブルのすべての*行がエクスポートされることに注意してください。最大10,000行までエクスポートされます。

     [+]

エクスポートした .csv ファイルを Excel で開くときに、オブジェクト名またはその他のフィールドが NN:NN の形式である場合 (2 桁の数字の後にコロン、 2 桁の数字が続く) 、 Excel ではその名前がテキスト形式ではなく Time 形式であると解釈されることがあります。その結果、 Excel の列に誤った値が表示されることがあります。たとえば、「 81 ： 45 」という名前のオブジェクトは、 Excel では「 81 ： 45 ： 00 」と表示されます。これを回避するには、次の手順に従って .csv を Excel にインポートします。

[+]

```
-   Open a new sheet in Excel.
-   On the "Data" tab, choose "From Text".
-   Locate the desired .CSV file and click "Import".
-   In the Import wizard, choose "Delimited" and click Next.
-   Choose "Comma" for the delimiter and click Next.
-   Select the desired columns and choose "Text" for the
column data format.
-   Click Finish.
Your objects should show in Excel in the proper format.
```

[+]

クエリの変更

クエリに関連付けられている条件を変更して、アセットの検索条件を変更することができます。

手順

1. InsightWeb UIにログインします。
2. [* クエリ *] をクリックし、 [* すべてのクエリを表示 *] を選択します。

   [クエリ] ページが表示されます。

3. クエリ名をクリックします。
4. クエリから条件を削除するには、をクリックします 。
5. クエリに条件を追加するには、をクリックします More をクリックし、リストから条件を選択します。
6. 次のいずれかを実行します。
   - [保存]*をクリックして、最初に使用した名前でクエリを保存します。
   - [名前を付けて保存]*をクリックして、クエリを別の名前で保存します。
   - 最初に使用したクエリ名を変更するには、*[名前の変更]*をクリックします。
   - クエリ名を最初に使用した名前に戻すには、*[元に戻す]*をクリックします。

クエリの削除

アセットに関する有用な情報が収集されなくなったクエリを削除できます。アノテーションルールで使用されているクエリは削除できません。

手順

1. InsightWeb UIにログインします。
2. [* クエリ *] をクリックし、 [* すべてのクエリを表示 *] を選択します。

   [クエリ] ページが表示されます。

3. 削除するクエリにカーソルを合わせ、をクリックします 。

   クエリを削除するかどうかを確認する確認メッセージが表示されます。

4. [OK] をクリックします。

アセットに対する複数のアプリケーションの割り当てと削除

アセットに対して複数のアプリケーションを割り当てたりアセットから削除したりするには、クエリを使用します。手動でアプリケーションを割り当てたり削除したりする必要はありません。

作業を開始する前に

編集するすべてのアセットを検索するクエリを作成しておく必要があります。

手順

1. [* クエリ *] をクリックし、 [* すべてのクエリを表示 *] を選択します。

   [クエリ] ページが表示されます。

2. アセットを検索するクエリの名前をクリックします。

   クエリに関連付けられているアセットのリストが表示されます。

3. リストから目的のアセットを選択するか、をクリックします をクリックして*すべて*を選択します。

   [アクション]*ボタンが表示されます。

4. 選択したアセットにアプリケーションを追加するには、をクリックします Actions をクリックし、*[アプリケーションの編集]*を選択します。

   a. [アプリケーション]*をクリックし、1つ以上のアプリケーションを選択します。

      ホスト、内部ボリューム、および仮想マシンに対しては複数のアプリケーションを選択できますが、ボリュームに対して選択できるアプリケーションは1つだけです。

b. [保存（ Save ）] をクリックします。

5. アセットに割り当てられているアプリケーションを削除するには、をクリックします Actions をクリックし、 [アプリケーションの削除] を選択します。

   a. 削除する 1 つ以上のアプリケーションを選択します。

   b. [削除（ Delete ）] をクリックします。

   新しく割り当てたアプリケーションは、別のアセットから派生したアプリケーションよりも優先されます。たとえば、ホストから継承したアプリケーションがあるボリュームに新しいアプリケーションを割り当てた場合、派生したアプリケーションよりも新しいアプリケーションが優先されます。

アセットの複数のアノテーションの編集または削除

アセットの複数のアノテーションを編集したりアセットから削除したりするには、手動で編集または削除しなくても、クエリを使用します。

作業を開始する前に

編集するすべてのアセットを検索するクエリを作成しておく必要があります。

手順

1. [* クエリ *] をクリックし、 [* すべてのクエリを表示 *] を選択します。

   [クエリ] ページが表示されます。

2. アセットを検索するクエリの名前をクリックします。

   クエリに関連付けられているアセットのリストが表示されます。

3. リストから目的のアセットを選択するか、をクリックします をクリックして*すべて*を選択します。

   [アクション]*ボタンが表示されます。

4. アセットにアノテーションを追加したり、アセットに割り当てられているアノテーションの値を編集したりするには、をクリックします Actions をクリックし、*[アノテーションの編集]*を選択します。

   a. [アノテーション]*をクリックし、値を変更するアノテーションを選択するか、すべてのアセットに割り当てる新しいアノテーションを選択します。

   b. * 値 * をクリックし、アノテーションの値を選択します。

   c. [保存（ Save ）] をクリックします。

5. アセットに割り当てられているアノテーションを削除するには、をクリックします Actions をクリックし、*[Remove Annotation]*を選択します。

   a. [アノテーション]*をクリックし、アセットから削除するアノテーションを選択します。

   b. [削除（ Delete ）] をクリックします。

テーブル値をコピーしています

テーブル内の値をコピーして、検索ボックスやその他のアプリケーションで使用できます。

このタスクについて

テーブルまたはクエリ結果から値をコピーするには、2つの方法があります。

手順

1. 方法 1: マウスで目的のテキストを強調表示し、コピーして、検索フィールドやその他のアプリケーションに貼り付けます。
2. 方法2:長さが省略記号(…)で示されるテーブル列の幅を超える単一値フィールドの場合は、フィールドの上にカーソルを置き、クリップボードアイコンをクリックします。値は、検索フィールドやその他のアプリケーションで使用するためにクリップボードにコピーされます。

   コピーできるのは、アセットへのリンクである値のみです。また、単一の値（リスト以外）を含むフィールドのみにコピーアイコンが表示されます。

Insightデータソース管理

データソースは、OnCommand Insight 環境の維持に使用される最も重要なコンポーネントです。Insightの主要な情報源であるため、データソースを実行状態に維持することが不可欠です。

ネットワーク内のデータソースを監視するには、データソースを選択してそのステータスに関連するイベントを確認し、問題の原因となった可能性がある変更を特定します。

個 々 のデータソースを確認するだけでなく、次の処理も実行できます。

- Insightで同様のデータソースを多数作成するには、データソースのクローンを作成します
- データソース情報を編集します
- クレデンシャルを変更
- ポーリングの制御
- データソースを削除します
- データソースパッチをインストールする
- パッチから新しいデータソースをインストールします
- ネットアップカスタマーサポート用のエラーレポートを準備

Insightでデータソースを設定します

データソースは、Insight環境を維持するうえで最も重要な要素です。データソースは、分析と検証に使用するネットワーク情報を検出します。ネットワーク内で監視できるように、Insightでデータソースを設定する必要があります。

各データソースについて、そのデータソースを定義するための固有の要件は、対応するデバイスのベンダーとモデルによって異なります。データソースを追加する前に、すべてのデバイスのネットワークアドレス、アカウント情報、パスワード、および必要に応じて次の詳細情報が必要です。

- スイッチ
- デバイス管理ステーション
- IP接続が確立されたストレージシステム
- ストレージ管理ステーション
- IP接続されていないストレージ・デバイス用の管理ソフトウェアを実行しているホスト・サーバ

データソースの定義の詳細については、このセクションの「ベンダー固有のデータソースリファレンス」を参照してください。

データソースのサポート情報

設定計画の一環として、環境内のデバイスをInsightで監視できることを確認する必要があります。そのためには、データソースサポートマトリックスでオペレーティングシステム、特定のデバイス、プロトコルの詳細を確認できます。一部のデータソースは、オペレーティングシステムによっては使用できない場合があります。

データソースサポートマトリックスの最新バージョンの場所

OnCommand Insight データソースサポートマトリックスは、サービスパックのリリースごとに更新されます。ドキュメントの最新バージョンについては、を参照してください "NetApp Support Site"。。

データソースを追加しています

[データソースの追加]ダイアログボックスを使用して、データソースをすばやく追加できます。

手順

1. ブラウザでOnCommand Insight を開き、管理者権限を持つユーザとしてログインします。
2. を選択し、[Data sources]*を選択します。
3. [+追加]*ボタンをクリックします。

   データソースの追加ウィザードが開きます。

4. [設定]セクションで、次の情報を入力します。

フィールド	説明
名前	このデータソースの一意のネットワーク名を入力します。注：データソース名に使用できる文字は、アルファベット、数字、アンダースコア（_）のみです。

ベンダー	ドロップダウンからデータソースのベンダーを選択します。
モデル	ドロップダウンからデータソースのモデルを選択します。
どこで実行するか	[Local]を選択します。環境でRAUが設定されている場合はRemote Acquisition Unitを選択できます。
収集するもの	ほとんどのデータソースでは、これらのオプションは[Inventory]と[Performance]です。インベントリはデフォルトで常に選択されており、選択を解除することはできません。一部のデータソースには異なるオプションがある場合があります。選択した収集オプションによって、[Configuration]セクションと[Advanced configuration]セクションの使用可能なフィールドが変更されます。

5. [Configuration]*リンクをクリックし、選択したデータ収集タイプでデータソースに必要な基本的な設定情報を入力します。
6. 通常、このタイプのデータソースをネットワークで設定するために詳細な情報が必要な場合は、*[Advanced configuration]*リンクをクリックして追加情報 に入ります。
7. 特定のデータソースに必要な設定情報や高度な設定情報、または使用可能な設定情報の詳細については、を参照して"ベンダー別のデータソースリファレンス"ください。
8. [Test]*リンクをクリックして、データソースが正しく設定されていることを確認します。
9. [保存（ Save ）] をクリックします。

スプレッドシートからデータソースをインポートする

スプレッドシートからOnCommand Insight に複数のデータソースをインポートできます。これは、検出デバイスをスプレッドシートですでに管理している場合に役立ちます。このプロセスでは新しいデータソースが追加されますが、既存のデータソースの更新には使用できません。

このタスクについて

OnCommand Insight には、データソースの作成に役立つスプレッドシートが用意されています。このスプレッドシートには次の属性があります。

- このスプレッドシートは、Microsoft Excel 2003以降で使用できます。
- 各タブには、Brocade SSH/CLIなど、1つのデータソースタイプが表示されます。
- 各行は、作成される新しいデータソースのインスタンスを表します。

スプレッドシートには、OnCommand Insight で新しいデータソースを作成するマクロが含まれています。

手順

1. でスプレッドシートを探します `<install_directory>/SANscreen/acq/bin/acqcli/SiteSurvey_DataSourceImporter_w_Macro.zip`。
2. スプレッドシートで、色の付いたセルにデータソース情報を入力します。
3. 空の行を削除します。
4. スプレッドシートからを実行します `CreateDataSources` マクロを使用してデータソースを作成します。
5. クレデンシャルの入力を求められたら、OnCommand Insight サーバの管理ユーザ名とパスワードを入力します。

   収集結果が収集ログに記録されます。

6. マクロを実行しているマシンにOnCommand Insight がインストールされているかどうかを確認するプロンプトが表示されます。

   次のいずれかを選択します。

   - いいえ：OnCommand Insight マシンで実行する必要があるバッチファイルを作成する場合は、[いいえ]を選択します。インストールディレクトリからこのバッチファイルを実行します。
   - Yes：OnCommand Insight がすでにインストールされていて、データソース情報を生成するための追加の手順が不要な場合は、[Yes]を選択します。
7. データソースが追加されたかどうかを確認するには、ブラウザでInsightを開きます。
8. Insightのツールバーで、*[Admin]*をクリックします。
9. [Data sources]リストで、インポートしたデータソースを確認します。

パッチによる新しいデータソースの追加

新しいデータソースはパッチファイルとしてリリースされ、パッチプロセスを使用してシステムにロードできます。このプロセスにより、OnCommand Insight の次のリリースまで新しいデータソースを使用できるようになります。

作業を開始する前に

インストールするパッチファイルをアップロードしておく必要があります。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [パッチ]*を選択します。
3. **>[サービスパックまたはパッチのインストール]*を選択します。
4. [* Install Service Pack or Patch*（サービスパックまたはパッチのインストール）]ダイアログボックスで、*[Browse（参照）]*をクリックして、アップロードしたパッチファイルを探して選択します。
5. [パッチの概要]ダイアログボックスで*[次へ]*をクリックします。

6. 情報を確認し、[次へ]*をクリックして続行します。
7. [インストール]ダイアログボックスで、*[完了]*をクリックします。

データソースのクローニング

クローニング機能を使用すると、別のデータソースと同じクレデンシャルと属性を持つデータソースをすばやく追加することができます。クローンを作成すると、同じデバイスタイプの複数のインスタンスを簡単に構成できます。

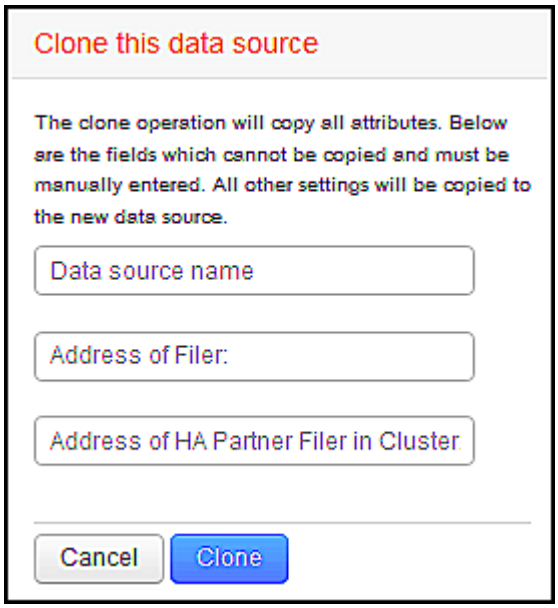
手順

1. Insightのツールバーで、*[Admin]*をクリックします。

   [Data sources]リストが開きます。

2. 新しいデータソースで使用するセットアップ情報が表示されているデータソースを強調表示します。
3. 強調表示されたデータソースの右側にある*[クローン]*アイコンをクリックします。

   [Clone this data source]ダイアログボックスには、選択したデータソースに指定する必要がある情報が表示されます。次の例は、ネットアップデータソースを示しています。



4. フィールドに必要な情報を入力します。これらの詳細を既存のデータソースからコピーすることはできません。
5. [* Clone*] をクリックします。

結果

他のすべての属性と設定がコピーされ、新しいデータソースが作成されます。

データソースの設定をテストします

データソースを追加するときは、そのデータソースを保存または更新する前に、デバイ

スと通信するための設定が正しいかどうかを確認できます。

データソースウィザードの*テスト*ボタンをクリックすると、指定したデバイスとの通信がチェックされます。このテストでは、次のいずれかの結果が生成されます。

- PASSED：データソースが正しく設定されています。
- 警告：テストが完了していません。処理中にタイムアウトしたか、データ収集が実行されていない可能性があります。
- Failed：設定されているデータソースが、指定されたデバイスと通信できません。設定を確認して再テストしてください。

ベンダー別のデータソースリファレンス

構成の詳細は、追加するデータソースのベンダーとモデルによって異なります。

このセクションには、ベンダーのデータソースでInsightの高度な設定手順（特別な要件や固有のコマンドなど）が必要な場合の情報が記載されています。

3PAR InServデータソース

OnCommand Insight は、3PAR InServ（Firmware 2.2.2+、SSH）データソースを使用して、HP 3PAR StoreServストレージアレイのインベントリを検出します。

用語集

OnCommand Insight では、3PAR InServデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
物理ディスク	ディスク
ストレージシステム	ストレージ
コントローラノード	ストレージノード
Common Provisioning Group の 1 つ	ストレージプール
仮想ボリューム	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- InServ クラスタの IP アドレスまたは FQDN

- インベントリの場合、InServサーバに対する読み取り専用のユーザ名とパスワード。
- パフォーマンスを高めるために、InServサーバに対する読み取り/書き込みのユーザ名とパスワード。
- ポート要件：22（インベントリ収集）、5988、または5989（パフォーマンス収集）[注：3PARパフォーマンスはInServ OS 3.x以降でサポートされます]
- パフォーマンス収集については、 SSH を使用して 3PAR アレイにログインし、 SMI-S が有効になっていることを確認してください。

設定

フィールド	説明
クラスタ IP	InServクラスタのIPアドレスまたは完全修飾ドメイン名
ユーザ名	InServサーバのユーザ名
パスワード	InServサーバのパスワード
SMI-SホストIP	SMI-Sプロバイダホストの IPアドレス
SMI-S ユーザー名	SMI-S プロバイダホストのユーザ名
SMI-S のパスワード	SMI-S プロバイダホストのパスワード

詳細設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
デバイスを除外します	対象から除外するデバイスのIPをカンマで区切ったリスト
SSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは60秒）
SSHの再試行回数	SSHの再試行回数
SSHバナー待機タイムアウト（秒）	SSHバナーのタイムアウト（デフォルトは20秒）
SMI-Sポート	SMI-Sプロバイダホストが使用するポート
プロトコル	SMI-S プロバイダへの接続に使用するプロトコル

SMI-Sネームスペース	SMI-Sネームスペース
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
SMI-S接続の再試行回数	SMI-S接続の再試行回数

Amazon AWS EC2データソース

OnCommand Insight は、このデータソースを使用して、Amazon AWS EC2のインベントリとパフォーマンスを検出します。

前提条件

Amazon EC2 デバイスからデータを収集するには、次の情報が必要です。

- IAMアクセスキーIDが必要です
- Amazon EC2クラウドアカウントのシークレットアクセスキーが必要です
- 「組織のリスト」権限が必要です
- ポート433 HTTPS
- EC2 インスタンスは、仮想マシンまたは（自然に）ホストとしてレポートできます。EBS ボリュームは、 VM で使用されている仮想ディスクと、仮想ディスクの容量を提供するデータストアの両方として報告できます。

アクセスキーは、アクセスキー ID （ AKIAIOSFODNN7EXAMPLE など）とシークレットアクセスキー（ wJalrXUtil/K7MDENG/bPxRfiCYEXAMPLEKEY など）で構成されます。Amanzon EC2 SDK、REST、またはQuery API操作を使用する場合は、アクセスキーを使用して、EC@に行うプログラム要求に署名します。これらのキーは、 Amazon の契約に付属しています。

このデータソースの設定方法

Amazon AWS EC2データソースを設定するには、AWSアカウントのAWS IAM Access Key IDとSecret Access Keyが必要です。

次の表に従って、データソースのフィールドに入力します。

構成：

フィールド	説明
AWS リージョン	AWS リージョンを選択します
IAM ロール	AWS の AU で取得した場合にのみ使用します。IAM ロールの詳細については、以下を参照してください。

AWS IAM Access Key ID	AWS IAM Access Key ID を入力します。IAM ロールを使用しない場合は必須です。
AWS IAM Secret Access Key の略	AWS IAM Secret Access Key を入力します。IAM ロールを使用しない場合は必須です。
AWSからAPI要求の料金が請求されることは理解しています	Insightのポーリングによって作成されたAPI要求に対してAWSから課金されることを理解しているかどうかを確認するには、このチェックボックスをオンにします

高度な設定：

フィールド	説明
追加リージョンを含める	ポーリングに含める追加領域を指定します。
クロスアカウントロール	異なる AWS アカウントのリソースにアクセスするためのロール。
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
HTTP接続およびソケットタイムアウト（秒）	HTTP接続タイムアウト（デフォルトは300秒）
AWSタグを含める	InsightのアノテーションでAWSタグがサポートされるようにするには、このオプションをオンにします
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは1、800秒）

AWSタグを**Insight**のアノテーションにマッピングする

AWS EC2データソースには、AWSで設定されているタグを使用してInsightのアノテーションを入力するオプションがあります。アノテーションにはAWSのタグとまったく同じ名前を付ける必要があります。Insightでは、常に同じ名前のテキストタイプのアノテーションが入力され、他のタイプ（数値、ブール値など）のアノテーションが入力されるように「最善の試み」が行われます。アノテーションのタイプが異なるためにデータソースにデータを入力できない場合は、アノテーションを削除してテキストタイプとして再作成する必要があります。

AWSでは大文字と小文字が区別され、Insightでは大文字と小文字が区別されないことに注意してください。そのため、Insightで「OWNER」という名前のアノテーションを作成し、AWSで「OWNER」、「OWNER」、「OWNER」という名前のタグを作成すると、AWSで使用されている「OWNER」のすべてのバリエーションがInsightの「OWNER」アノテーションにマッピングされます。

関連情報：

"IAMユーザのアクセスキーの管理"

追加リージョンを含める

AWS Data Collector * Advanced Configuration * セクションでは、 * Include extra regions * フィールドを設定して、カンマまたはセミコロンで区切って追加のリージョンを含めることができます。デフォルトでは、このフィールドは * *us-.* に設定されており、これによってすべての US AWS リージョンで収集されます。on_all_regions を収集するには、このフィールドを *.** に設定します。

「 * include extra regions * 」フィールドが空の場合、「 * Configuration * 」セクションの指定に従って、「 * AWS Region * 」フィールドに指定されたアセットについてデータコレクタが収集されます。

*** AWS Child Accounts**から収集*****

Insightでは、1つのAWSデータコレクタ内でのAWSの子アカウントの収集がサポートされます。この収集の設定は、 AWS 環境で実行されます。

- プライマリアカウントIDが子アカウントからEC2の詳細にアクセスできるように、各子アカウントにAWSロールを設定する必要があります。
- 各子アカウントには、ロール名が同じ文字列として設定されている必要があります
- このロール名の文字列をInsight AWS Data Collector * Advanced Configuration セクションの Cross Account Role *フィールドに入力します。

ベストプラクティス：AWSの事前定義されたAmazonEC2ReadOnlyAccessポリシーをECSプライマリアカウントに割り当てることを強く推奨します。また、AWSを照会するには、データソースで構成されているユーザに少なくとも事前定義された*AWSOrganizationsReadOnlyAccess*policyが割り当てられている必要があります。

InsightがAWSの子アカウントから収集できるように環境を設定する方法については、次の資料を参照してください。

"チュートリアル： IAM ロールを使用した AWS アカウント間でのアクセスの委譲"

"AWS のセットアップ：自分が所有している別の AWS アカウントで IAM ユーザにアクセスを付与する"

"IAM ユーザに権限を委任するためのロールを作成する"

IAM ロール

_IAM Role_securityを使用する場合は、作成または指定するロールに、リソースへのアクセスに必要な適切な権限があることを確認する必要があります。

たとえば、 *InstanceEc2ReadOnly* という名前の IAM ロールを作成した場合は、この IAM ロールのすべての EC2 リソースに読み取り専用リストアクセス権限を付与するようにポリシーを設定する必要があります。また、このロールがアカウント間でロールを引き受けることができるように、 STS （セキュリティトークンサービス）アクセスを許可する必要があります。

IAM ロールを作成したら、新しい EC2 インスタンスまたは既存の EC2 インスタンスを作成するときに IAM ロールを接続できます。

IAM ロール *InstanceEc2ReadOnly* を EC2 インスタンスに接続すると、インスタンスメタデータから IAM ロール名で一時的なクレデンシャルを取得し、この EC2 インスタンスで実行されているすべてのアプリケーションから AWS リソースにアクセスできるようになります。

IAMロールは、Acquisition UnitがAWSインスタンスで実行されている場合にのみ使用できます。

Brocade Enterprise Fabric Connectivity Managerデータソース

OnCommand Insight は、Brocade Enterprise Fabric Connectivity Manager（EFCM）データソースを使用して、Brocade EFCMスイッチのインベントリを検出します。Insightでは、EFCMバージョン9.5、9.6、9.7がサポートされます。

要件

このデータコレクタは、OnCommand Insight 7.3.11以降では使用できません。

- EFCM サーバのネットワークアドレスまたは完全修飾ドメイン名
- EFCM のバージョンは 9.5 、 9.6 、または 9.7 である必要があります
- EFCM サーバの IP アドレス
- EFCM サーバに対する読み取り専用のユーザ名とパスワード
- 読み取り専用のユーザ名とパスワードを使用して、InsightサーバからConnectrixスイッチにポート51512経由でTelnetでアクセスできることを確認しました

設定

* フィールド *	* 概要 *
EFC サーバ	EFC サーバの IP アドレスまたは完全修飾ドメイン名
ユーザ名	スイッチのユーザ名
パスワード	スイッチのパスワード

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは15分）
ファブリック名	EFCMデータソースによってレポートされるファブリック名。ファブリック名を WWN としてレポートする場合は、空白のままにします。
通信ポート	スイッチとの通信に使用するポート

トラッピングを有効にします	デバイスからの SNMP トラップの受信時にデータ収集を有効にする場合に選択します。トラップを有効にするを選択した場合は、 SNMP も有効にする必要があります。
トラップ間の最小時間（秒）	トラップによって収集を試行する最小間隔（デフォルトは15秒）
非アクティブなゾーンセット	アクティブなゾーンセットに加えてデータ収集の対象に含める非アクティブなゾーンセットをカンマで区切ったリスト
使用する NIC	SAN デバイスをレポートする際に RAU で使用するネットワークインターフェイスを指定します
デバイスを除外します	ポーリングの対象に含めるか除外するユニットの名前をカンマで区切ったリスト
EFCMスイッチのニックネームをInsightスイッチ名として使用します	EFCMスイッチのニックネームをInsightスイッチ名として使用する場合に選択します
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

Brocade FC Switchデータソース

OnCommand Insight では、Brocade FC Switch（SSH）データソースを使用して、Factored Operating System（FOS）ファームウェア4.2以降を実行しているBrocadeスイッチデバイス（ブランド名が変更されたスイッチデバイス）のインベントリを検出します。FC スイッチとアクセスゲートウェイの両方のモードのデバイスがサポートされます。

用語集

OnCommand Insight では、Brocade FC Switchデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
スイッチ	スイッチ
ポート	ポート
仮想ファブリック、物理ファブリック	ファブリック

ゾーン	ゾーン
Logical Switch の略	Logical Switch の略
LSAN ゾーン	IVR ゾーン

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- Acquisition Unit（ローカルまたはリモート）は、BrocadeスイッチのTCPポート22への接続を開始してインベントリデータを収集します。AU は、パフォーマンスデータの収集用に UDP ポート 161 への接続も開始します。
- ファブリック内のすべてのスイッチへの IP 接続が必要です。[Discover all switches in the fabric]チェックボックスを選択すると、ファブリック内のすべてのスイッチが識別されますが、検出するにはこれらの追加スイッチへのIP接続が必要です。
- ファブリック内のすべてのスイッチで、同じアカウントがグローバルに必要です。アクセスの確認には、PuTTY （オープンソースの端末エミュレータ）を使用できます。
- Performライセンスがインストールされている場合は、SNMPパフォーマンスポーリング用に、ポート161および162をファブリック内のすべてのスイッチに対して開いておく必要があります。
- SNMP 読み取り専用コミュニティストリング

設定

フィールド	説明
スイッチ IP	スイッチの IP アドレスまたは完全修飾ドメイン名
ユーザ名	スイッチのユーザ名
パスワード	スイッチのパスワード
SNMP バージョン	SNMP バージョン
SNMP コミュニティストリング	スイッチへのアクセスに使用する SNMP の読み取り専用コミュニティストリング
SNMP ユーザ名	SNMPバージョンプロトコルのユーザ名（SNMP v3のみ）
SNMP パスワード	SNMPバージョンプロトコルのパスワード（SNMP v3のみ）

フィールド	説明
ファブリック名	データソースでレポートするファブリック名。ファブリック名を WWN としてレポートする場合は、空白のままにします。
デバイスを除外します	ポーリングの対象から除外するデバイスの ID をカンマで区切ったリスト
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは15分）
タイムアウト（秒）	接続タイムアウト（デフォルトは30秒）
バナー待機タイムアウト（秒）	SSHバナーのタイムアウト（デフォルトは5秒）
管理ドメインはアクティブです	管理ドメインを使用する場合に選択します
MPR データを取得する	マルチプロトコルルータ（MPR）からルーティングデータを取得する場合に選択します。
トラッピングを有効にします	デバイスからの SNMP トラップの受信時にデータ収集を有効にする場合に選択します。トラップを有効にするを選択した場合は、 SNMP も有効にする必要があります。
トラップ間の最小時間（秒）	トラップでデータ収集を試行する最小間隔（デフォルトは 10 秒）
ファブリック内のすべてのスイッチを検出します	ファブリック内のすべてのスイッチを検出する場合に選択します
HBA との優先を選択しますゾーンのエイリアス	HBA とゾーンエイリアスのどちらを優先するかを選択します
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
SNMP 認証プロトコル	SNMP 認証プロトコル（ SNMP v3 のみ）
SNMP プライバシープロトコル	SNMPプライバシープロトコル（SNMP v3のみ）
SNMP プライバシーパスワード	SNMP プライバシーパスワード（ SNMP v3 のみ）

SNMP 再試行回数	SNMP の再試行回数
SNMP タイムアウト（ミリ秒）	SNMP タイムアウト（デフォルトは 5 、 000 ミリ秒 ）

Brocade Sphereon/Intrepid Switchデータソース

OnCommand Insight では、Brocade Sphereon/Intrepid Switch（SNMP）データソースを使用して、Brocade Sphereon/Intrepidスイッチのインベントリを検出します。

要件

このデータコレクタは、OnCommand Insight 7.3.11以降では使用できません。

- ファブリック内のすべてのスイッチへの IP 接続が必要です。[Discover all switches in the fabric]チェックボックスを選択すると、ファブリック内のすべてのスイッチが識別されますが、検出するにはこれらの追加スイッチへのIP接続が必要です。
- SNMP V1 または SNMP V2 を使用している場合は、読み取り専用コミュニティストリングが必要です。
- ゾーニング情報を取得するには、スイッチへの HTTP アクセスが必要です。
- を実行してアクセスを検証します `snmpwalk` スイッチへのユーティリティ（を参照） `<install_path\>\bin\)`。

設定

* フィールド *	* 概要 *
球スイッチ	スイッチの IP アドレスまたは完全修飾ドメイン名
SNMP バージョン	SNMP バージョン
SNMPコミュニティ	スイッチへのアクセスに使用する SNMP の読み取り専用コミュニティストリング
ユーザ名	スイッチの SMI-S のユーザ名（ SNMP v3 のみ）
パスワード	スイッチの SMI-S のパスワード（ SNMP v3 のみ）

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは15分 ）

SNMP 認証プロトコル	SNMP 認証プロトコル（ SNMPv3 のみ）
SNMP プライバシープロトコル	SNMP プライバシープロトコル（ SNMPv3 のみ）
SNMP プライバシーパスワード	SNMPプライバシーパスワード
SNMP 再試行回数	SNMP の再試行回数
SNMP タイムアウト（ミリ秒）	SNMP タイムアウト（デフォルトは 5 、 000 ミリ秒）
ファブリック名	データソースでレポートするファブリック名。ファブリック名を WWN としてレポートする場合は、空白のままにします。
トラッピングを有効にします	デバイスからの SNMP トラップの受信時にデータ収集を有効にする場合に選択します。トラップを有効にするを選択した場合は、 SNMP も有効にする必要があります。
Ttrapsの最小間隔（秒）	トラップでデータ収集を試行する最小間隔（デフォルトは 10 秒）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

Cisco FC Switch Firmware（SNMP）データソース

OnCommand Insight では、Cisco FC Switch Firmware 2.0+（SNMP）データソースを使用して、Cisco MDSファイバチャネルスイッチおよびFCサービスが有効になっているさまざまなCisco Nexus FCoEスイッチのインベントリを検出します。さらに、このデータソースを使用して、NPVモードで実行されているシスコデバイスの多くのモデルを検出できます。

用語集

OnCommand Insight では、Cisco FC Switchデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
スイッチ	スイッチ
ポート	ポート

VSAN （仮想 SAN	ファブリック
ゾーン	ゾーン
Logical Switch の略	Logical Switch の略
ネームサーバエントリ	ネームサーバエントリ
Inter-VSAN Routing （ IVR ）ゾーン	IVR ゾーン

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ファブリック内の 1 つのスイッチまたは個々のスイッチの IP アドレス
- シャーシ検出。ファブリック検出をイネーブルにします
- SNMP V2 を使用している場合は、読み取り専用コミュニティストリングが必要です
- ポート 161 はデバイスへのアクセスに使用されます
- を使用したアクセスの検証 `snmpwalk` スイッチへのユーティリティ（を参照） `<install_path\>\bin\`)

設定

フィールド	説明
Cisco スイッチ IP	スイッチの IP アドレスまたは完全修飾ドメイン名
SNMP バージョン	パフォーマンスの取得にはSNMPバージョンv2以降が必要です
SNMP コミュニティストリング	スイッチへのアクセスに使用する SNMP の読み取り専用コミュニティストリング（ SNMP v3 は対象外）
ユーザ名	スイッチのユーザ名（ SNMP v3 のみ）
パスワード	スイッチのパスワード（ SNMPv3 のみ）

高度な設定

フィールド	説明

インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
SNMP 認証プロトコル	SNMP 認証プロトコル（ SNMPv3 のみ）
SNMP プライバシープロトコル	SNMP プライバシープロトコル（ SNMPv3 のみ）
SNMP プライバシーパスワード	SNMPプライバシーパスワード
SNMP 再試行回数	SNMP の再試行回数
SNMP タイムアウト（ミリ秒）	SNMP タイムアウト（デフォルトは 5 、 000 ミリ秒）
トラッピングを有効にします	トラップを有効にする場合に選択します。トラッピングを有効にする場合は、 SNMP 通知も有効にする必要があります。
トラップ間の最小時間（秒）	トラップでデータ収集を試行する最小間隔（デフォルトは 10 秒）
すべてのファブリックスイッチを検出します	ファブリック内のすべてのスイッチを検出する場合に選択します
デバイスを除外します	ポーリングの対象から除外するデバイスの IP をカンマで区切ったリスト
デバイスを含める	ポーリングの対象に含めるデバイスの IP をカンマで区切ったリスト
デバイスタイプを確認します	Cisco デバイスとして明示的にアドバタイズされたデバイスのみを受け入れる場合に選択します

プライマリエイリアスタイプ	エイリアスの解決で最初に優先する情報を指定します。次のいずれかを選択します。 • デバイスエイリアス これは、ポートWWN（pWWN）のフレンドリ名であり、必要に応じてすべてのコンフィギュレーションコマンドで使用できます。Cisco MDS 9000 ファミリのすべてのスイッチは、Distributed Device Alias Services （デバイスエイリアス）をサポートしています。 • * なし * エイリアスは報告しないでください • *ポート概要 * ポートのリストでポートを識別するための概要 • ゾーンエイリアス（すべて） ゾーニング設定でのみ使用できるポートのフレンドリ名 • ゾーンエイリアス（アクティブのみ） アクティブな構成でのみ使用できるポートのフレンドリ名。これがデフォルトです。
セカンダリエイリアスタイプ	エイリアスの解決で 2 番目に優先する情報を指定します
ターシャリエイリアスタイプ	エイリアスの解決で 3 番目に優先する情報を指定します
SANTap プロキシモードサポートをイネーブルにします	Cisco スイッチで SANTap のプロキシモードを使用している場合に選択。EMC RecoverPoint を使用している場合は、 SANTap を使用していると考えられます。
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

EMC Celerraデータソース

Celerra（SSH）データソースは、Celerraストレージからインベントリ情報を収集します。このデータソースを設定するには、ストレージプロセッサのIPアドレス、および_read-only_userの名前とパスワードが必要です。

用語集

OnCommand Insight では、EMC Celerraデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
Celerra Network Serverの略	ストレージ
Celerraメタ・ボリューム/Celerraストレージ・プール	ストレージプール
File System の略	内部ボリューム
データムーバー	コントローラ
Data Moverにマウントされたファイルシステム	ファイル共有
CIFS および NFS エクスポート	共有
ディスクボリューム	バックエンド LUN

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ストレージプロセッサの IP アドレス
- 読み取り専用のユーザ名とパスワード
- SSH ポート 22

設定

フィールド	説明
Celerraのアドレス	CelerraデバイスのIPアドレスまたは完全修飾ドメイン名
ユーザ名	Celerraデバイスへのログインに使用する名前
パスワード	Celerraデバイスへのログインに使用するパスワード

高度な設定

フィールド	説明

インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
SSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは600秒）
再試行回数	インベントリの再試行回数
SSHバナー待機タイムアウト（秒）	SSHバナーのタイムアウト（デフォルトは20秒）

EMC CLARiX（NaviCLI）データソース

このデータソースを設定する前に、ターゲットデバイスとInsight ServerにEMC Navisphere CLIがインストールされていることを確認してください。Navisphere CLIのバージョンは、コントローラのファームウェアのバージョンと一致している必要があります。パフォーマンスデータを収集するには、統計ログをオンにする必要があります。

Navisphereコマンド・ライン・インタフェースの構文

```
naviseccli.exe -h <IP address> -user <user> -password <password> -scope
<scope,use 0 for global scope> -port <use 443 by default> command
```

用語集

OnCommand Insight では、EMC CLARiXデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
ストレージ	ストレージ
ストレージプロセッサ	ストレージノード
シンプール、RAIDグループ	ストレージプール
LUN	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- 各CLARiXストレージ・プロセッサのIPアドレス
- CLARiXアレイに対する読み取り専用のNavisphereユーザー名とパスワード
- NavicliがInsight Server / RAUにインストールされている必要があります
- アクセスの検証：上記のユーザ名とパスワードを使用して、Insight Serverから各アレイに対してNaviCLIを実行します。
- Navicliのバージョンは'アレイ上の最新のFLAREコードに対応している必要があります
- パフォーマンスのためには、統計ログをオンにする必要があります。
- ポート要件： 80 、 443

設定

フィールド	説明
CLARiXストレージ	CLARiXストレージのIPアドレスまたは完全修飾ドメイン名
ユーザ名	CLARiXストレージ・デバイスへのログインに使用する名前
パスワード	CLARiXストレージ・デバイスへのログインに使用するパスワード
CLIのnavicli.exeパスまたはnaviseccli.exeパスへのパス	への完全パス `navicli.exe` または `naviseccli.exe` 実行ファイル

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
Secure Clientの使用（naviseccli）	セキュア・クライアントを使用する場合に選択（navseccli）
適用範囲	セキュアなクライアントの範囲デフォルトは Global です。
CLARiX CLIポート	CLARiX CLIに使用するポート
インベントリ外部プロセスタイムアウト（秒）	外部プロセスのタイムアウト（デフォルトは1、800秒）

パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
パフォーマンス外部プロセスのタイムアウト（秒）	外部プロセスのタイムアウト（デフォルトは1、800 秒）

EMC Data Domainデータソース

このデータソースは、EMC Data Domain重複排除ストレージシステムからストレージと構成の情報を収集します。データソースを追加するには、特定の設定手順とコマンドを使用し、データソースの要件と使用に関する推奨事項を確認しておく必要があります。

用語集

OnCommand Insight では、EMC Data Domainデータソースから次のインベントリ情報を取得します。Insight で取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
配列	ストレージ
ポート	ポート
ファイルシステム	内部ボリューム
ミトリー	qtree
クォータ	クォータ
NFS 共有および CIFS 共有	ファイル共有

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- Data Domain デバイスの IP アドレス
- Data Domain ストレージに対する読み取り専用のユーザ名とパスワード
- SSH ポート 22

設定

フィールド	説明
IP アドレス	Data Domain ストレージアレイの IP アドレスまたは完全修飾ドメイン名
ユーザ名	Data Domain ストレージアレイのユーザ名
パスワード	Data Domain ストレージアレイのパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
SSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは180秒）
SSH ポート	SSH サービスポート

EMC ECC StorageScopeデータソース

EMC ECC StorageScopeデバイスには'5.x'6.0'6.1の3種類のデータ・ソースがあります

設定

このデータコレクタは、OnCommand Insight 7.3.11以降では使用できなくなりました。

* フィールド *	* 概要 *
ECCサーバ	ECCサーバのIPアドレスまたは完全修飾ドメイン名
ユーザ名	ECCサーバのユーザ名
パスワード	ECCサーバのパスワード

高度な設定

* フィールド *	* 概要 *
ECCポート	ECCサーバに使用するポート
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは30分）

データベースに接続するプロトコル	データベースへの接続に使用されるプロトコル
ファイルシステム情報を照会します	WWNエイリアスとファイルシステムの詳細を取得する場合に選択します。

Dell EMC ECSデータソース

このデータコレクタは、 EMC ECS ストレージシステムからインベントリデータとパフォーマンスデータを取得します。データコレクタを設定するには、ECSサーバのIPアドレスと管理者レベルのドメインアカウントが必要です。

用語集

OnCommand Insight では、EMC ECSデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
クルーザー	ストレージ
テナント	ストレージプール
バケット	内部ボリューム
ディスク	ディスク

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ECS 管理コンソールの IP アドレス
- ECS システムの管理者レベルドメインアカウント
- ポート 443 （ HTTPS ）：ECS システムで TCP ポート 443 へのアウトバウンド接続が必要です。
- パフォーマンスを確保するには、 ssh/scp アクセス用の読み取り専用のユーザ名とパスワードを使用します。
- パフォーマンスを確保するには、ポート 22 が必要です。

設定

フィールド	説明
ECS ホスト	ECSシステムのIPアドレスまたは完全修飾ドメイン名

ECS ホストポート	ECS ホストとの通信に使用されるポート
ECS ベンダー ID	ECS のベンダー ID
パスワード	ECS のパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔。デフォルトは 360 分です。

EMC Isilonデータソース

Isilon SSHデータソースは、EMC IsilonスケールアウトNASストレージからインベントリとパフォーマンスを収集します。

用語集

OnCommand Insight では、EMC Isilonデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ドライブ	ディスク
クラスタ	ストレージ
ノード	ストレージノード
File System の略	内部ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- Isilon ストレージに対する管理者権限
- を使用してアクセスを検証 `telnet` ポート22に接続します

設定

フィールド	説明

IP アドレス	Isilon クラスタの IP アドレスまたは完全修飾ドメイン名
ユーザ名	Isilonクラスタのユーザ名
パスワード	Isilonクラスタのパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
SSHプロセス待機タイムアウト	SSHプロセスのタイムアウト（デフォルトは60秒）
SSH ポート	SSH サービスポート

CLIコマンドの実行

OnCommand Insight バージョン7.3.11およびサービスパック9以降、EMC Isilonデータソースには、より多くのCLIコマンドが実行されるようになる拡張機能が含まれています。データソース内でroot以外のユーザを使用している場合は、「sudoers」ファイルを設定して、そのユーザアカウントにSSH経由で特定のCLIコマンドを実行する権限を付与している可能性があります。

InsightでEMCのアクセスゾーン機能を理解するために'次の新しいCLIコマンドが追加で実行されるようになりました

- `sudo isi zone zones list --format json –verbose`
- `sudo isi zone zones list`

Insightでは、これらのコマンドの出力を解析し、既存のコマンドのインスタンスを追加で実行して、デフォルト以外のアクセスゾーンに存在するqtree、クォータ、NAS共有/エクスポートなどのオブジェクトの論理構成を取得します。この機能拡張の結果、デフォルト以外のアクセスゾーンについてこれらのオブジェクトが報告されるようになりました。Insightでは、既存のコマンド（オプションが異なる）を実行してデータを取得するため、sudoersファイルを変更する必要はありません。変更が必要になるのは、上記の新しいコマンドを導入したときだけです。

このInsightリリースにアップグレードする前に、sudoersファイルを更新してInsightサービスアカウントでこれらのコマンドが実行されるようにしてください。これを行わないと、Isilonデータソースに障害が発生します。

「ファイルシステム」統計

OnCommand Insight 7.3.12以降では、EMC Isilonデータコレクタによって、EMC Isilonのノードオブジェクト

に関する「ファイルシステム」統計が導入されています。OnCommand Insight によって報告される既存のノードの統計は「ディスク」ベースです。ストレージノードのIOPSとスループットの場合、このノードのディスクはアグリゲートで何をしていますか？ただし、読み取りがメモリにキャッシュされたり、圧縮が使用されたりするワークロードの場合、ファイルシステムのワークロードは実際にディスクにヒットするワークロードよりも大幅に高くなる可能性があります。つまり、5：1で圧縮されるデータセットの場合は、「ファイルシステムの読み取りスループット」の値がストレージノードの5倍になる可能性があります。読み取りスループット、 後者はディスクからの読み取りを測定します。これは、ノードがデータを解凍してクライアントの読み取り要求を処理すると5倍に拡張されます。

Dell EMC PowerStoreデータソース

Dell EMC PowerStoreデータコレクタは、Dell EMC PowerStoreストレージからインベントリ情報を収集します。データコレクタを設定するには、ストレージプロセッサの IP アドレス、および読み取り専用のユーザ名とパスワードが必要です。

用語集

OnCommand Insight では、EMC Data Domainデータソースから次のインベントリ情報を取得します。Insight で取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ホスト	ホスト
host_volume_mapping	host_volume_mapping
ハードウェア（「 extra_details 」オブジェクトにドライブが含まれています）：ドライブ	ディスク
アプライアンス	ストレージプール
クラスタ	ストレージアレイ
ノード	ストレージノード
FC ポート	ポート
ボリューム	ボリューム
内部ボリューム	ファイルシステム
ファイルシステム	内部ボリューム
ミトリー	qtree
クォータ	クォータ

NFS 共有および CIFS 共有	ファイル共有

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ストレージプロセッサの IP アドレスまたは完全修飾ドメイン名
- 読み取り専用のユーザ名とパスワード

親シリアル番号の説明

従来、Insightでは、ストレージアレイのシリアル番号や個 々 のストレージノードのシリアル番号をレポートすることができました。ただし、一部のストレージアレイアーキテクチャはこれに適切に対応していません。PowerStoreクラスタは1~4台のアプライアンスで構成でき、各アプライアンスには2つのノードがあります。アプライアンス自体のシリアル番号がある場合、そのシリアル番号はクラスタのシリアル番号でもノードのシリアル番号でもありません。

大規模なクラスタの一部にすぎない中間アプライアンス/エンクロージャに個 々 のノードが配置されている場合、ストレージノードオブジェクトの「Parent Serial Number」属性がDell/EMC PowerStoreアレイ用に適切に設定されます。

設定

フィールド	説明
PowerStore ゲートウェイ	PowerStore ストレージの IP アドレスまたは完全修飾ドメイン名
ユーザ名	PowerStore のユーザー名
パスワード	PowerStore のパスワード

高度な設定

フィールド	説明
HTTPS ポート	デフォルトは 443 です
インベントリポーリング間隔（分）	インベントリのポーリング間隔。デフォルトは 60 分です。

OnCommand InsightのPowerStoreパフォーマンスコレクションでは、PowerStoreの5分単位のソースデータを使用します。そのため、Insightは5分ごとにそのデータをポーリングします。このポーリングは設定できません。

EMC RecoverPointデータソース

EMC RecoverPointデータソースは、EMC RecoverPointストレージからインベントリ情報を収集します。データソースを設定するには、ストレージプロセッサのIPアドレス、および_read-only_userの名前とパスワードが必要です。

EMC RecoverPointデータソースは、RecoverPointが他のストレージアレイ間で調整するボリューム間レプリケーション関係を収集します。OnCommand Insight は各RecoverPointクラスタのストレージアレイを表示し、そのクラスタ上のノードとストレージポートのインベントリデータを収集します。ストレージプールまたはボリュームのデータは収集されません。

要件

- ストレージプロセッサの IP アドレスまたは完全修飾ドメイン名
- 読み取り専用のユーザ名とパスワード
- ポート 443 経由での REST API へのアクセス
- PuTTYを使用したSSHアクセス

設定

フィールド	説明
RecoverPoint のアドレス	RecoverPoint クラスタの IP アドレスまたは完全修飾ドメイン名
ユーザ名	RecoverPoint クラスタのユーザ名
パスワード	RecoverPointクラスタのパスワード

高度な設定

フィールド	説明
TCP ポート	RecoverPoint クラスタへの接続に使用する TCP ポート
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
除外クラスタ	ポーリング時に除外するクラスタのIDまたは名前をカンマで区切ったリスト

EMC Solutions Enablerと**SMI-S Performance**データソース

OnCommand Insight は'Solutions Enablerを使用してSymmetrixストレージ・アレイを検出します `symcli` コマンドを環境内の既存のSolutions Enablerサーバと組み合わせて使用既存のSolutions Enablerサーバは、ゲートキーパーボリュームへのアクセスを通じ

てSymmetrixストレージアレイに接続されています。このデバイスにアクセスするには、管理者権限が必要です。

用語集

OnCommand Insight では、EMC Solutions Enablerデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
ディスクグループ	ディスクグループ
ストレージアレイ	ストレージ
ディレクター	ストレージノード
デバイスプール、 Storage Resource Pool （ SRP ； ストレージリソースプール）	ストレージプール
デバイス、TDEV	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

このデータソースを設定する前に、OnCommand Insight サーバから既存のSolutions Enablerサーバのポート2707へのTCP接続が確立されていることを確認する必要があります。OnCommand Insight は'サーバからの'symcfg list"の出力に示されているように'このサーバに対してローカルであるすべてのSymmetrixアレイを検出します

- EMC Solutions Enabler（CLI）とSMI-Sプロバイダアプリケーションがインストールされていて、Solutions Enablerサーバで実行されているバージョンと同じかそれよりも前のバージョンである必要があります。
- 適切に設定されている `{installdir}\EMC\SYMAPI\config\netcnfg` ファイルは必須です。このファイルでは、 Solutions Enabler サーバのサービス名とアクセス方法（ SECURE / NOSECURE / ANY ）を定義します。
- ストレージノードレベルで読み取り / 書き込みレイテンシが必要な場合、 SMI-S プロバイダは Unisphere for VMAX アプリケーションの実行中のインスタンスと通信する必要があります。
- Solutions Enabler （ SE ）サーバに対する管理者権限が必要です
- SE ソフトウェアに対する読み取り専用のユーザ名とパスワード
- Solutions Enabler サーバ 6.5X の要件：
  - SMIS-S V1.2用のSMI-Sプロバイダ3.3.1がインストールされています

- インストール後、を実行します `\Program Files\EMC\SYMCLI\bin>stordaemon start storsrvd`

- Unisphere for VMAXアプリケーションが実行され、SMI-S Providerインストールによって管理されるSymmetrix VMAXストレージアレイの統計情報を収集している必要があります
- アクセスの検証：SMI-Sプロバイダが実行されていることを確認します。 `telnet <se_server\> 5988`

設定

SMI-Sユーザ認証が有効になっていない場合、OnCommand Insight データソースのデフォルト値は無視されます。

Symmetrixアレイでsymauthが有効になっていると、OnCommand Insight がそれらのアレイを検出できなくなる可能性があります。OnCommand Insight による取得は、Solutions Enablerサーバと通信するOnCommand Insight / Remote Acquisition Unitサーバ上で、システムユーザとして実行されます。hostname\system にsymauth権限がない場合、OnCommand Insight はアレイを検出できません。

EMC Solutions Enabler Symmetrix CLIデータソースには、シンプロビジョニングおよびSymmetrix Remote Data Facility（SRDF）のデバイス構成のサポートが含まれています。

ファイバチャネルおよびスイッチのパフォーマンスパッケージの定義が提供されます。

フィールド	説明
サービス名	netcnfgファイルで指定されたサービス名
CLI の完全パス	Symmetrix CLIの完全パス

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
「除外」または「含める」を選択してリストを指定します	以下のリストにあるアレイをデータの収集時に対象に含めるか除外するかを指定します
インベントリ除外デバイス	対象に含めるか除外するデバイスの ID をカンマで区切ったリスト

接続のキャッシュ	接続のキャッシュ方法を選択： • localは、OnCommand Insight 取得サービスがSolutions Enablerサーバ上で実行されていることを意味します。サーバは検出対象のSymmetrixアレイにファイバチャネルで接続され、ゲートキーパーボリュームにアクセスできます。このオプションは、一部の Remote Acquisition Unit （ RAU ）構成で使用されます。 • REMOTE_CACHEDはデフォルトであり、ほとんどの場合に使用する必要があります。このオプションでは、 NETCNFG ファイルの設定に基づいて、 IP を使用して Solutions Enabler サーバに接続します。サーバは検出対象の Symmetrix アレイにファイバチャネルで接続されていて、ゲートキーパーボリュームにアクセスできる必要があります。 • remote_cachedオプションでCLIコマンドが失敗する場合は、remoteオプションを使用します。データ収集プロセスが遅くなることに注意してください（数時間から場合によっては数日かかることがあります）。検出対象の Symmetrix アレイにファイバチャネルで接続された Solutions Enabler サーバへの IP 接続には、引き続き NETCNFG ファイルの設定が使用されます。 ⓘ この設定では、「symcfg list」の出力でremoteとしてリストされている配列に対するOnCommand Insight の動作は変更されません。OnCommand Insight は、このコマンドでローカルと表示されたデバイス上のデータのみを収集します。
CLIタイムアウト（秒）	CLIプロセスのタイムアウト（デフォルトは7200秒）
SMI-SホストIP	SMI-Sプロバイダホストの IPアドレス
SMI-Sポート	SMI-Sプロバイダホストが使用するポート
プロトコル	SMI-S プロバイダへの接続に使用するプロトコル
SMI-Sネームスペース	SMI-Sプロバイダが使用するように設定されている相互運用ネームスペース
SMI-S ユーザー名	SMI-S プロバイダホストのユーザ名

SMI-S のパスワード	SMI-S プロバイダホストのユーザ名
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 1000 秒）
パフォーマンスフィルタタイプ	下のリストに表示されたアレイをパフォーマンスデータの収集時に対象に含めるか除外するかを指定します
パフォーマンスフィルタのデバイスリスト	対象に含めるか除外するデバイスの ID をカンマで区切ったリスト
RPOポーリング間隔（秒）	RPOポーリングの間隔（デフォルトは300秒）

EMC VNXデータソース

EMC VNX（SSH）データソースを構成するには、Control StationのIPアドレス、および_read-only_usernameとパスワードが必要です。

設定

フィールド	説明
VNX IP	VNX Control Station の IP アドレスまたは完全修飾ドメイン名
VNXユーザー名	VNX Control Station のユーザー名
VNXパスワード	VNX Control Station のパスワード

要件

- Control StationのIPアドレス
- 読み取り専用のユーザ名とパスワード
- アクセスの検証：PuTTYによるSSHアクセスを確認します。

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
VNX SSHプロセス待機タイムアウト（秒）	VNX SSHプロセスのタイムアウト（デフォルトは600秒）

Celerraコマンドの再試行	Celerraコマンドの再試行回数
CLARiXインベントリの外部プロセスタイムアウト（秒）	インベントリのCLARiX外部プロセスのタイムアウト（デフォルトは1、800秒）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
CLARiX外部プロセスのパフォーマンスタイムアウト（秒）	CLARiX外部プロセスのパフォーマンスタイムアウト（デフォルトは1、800秒）

EMC VNXeデータソース

EMC VNXeデータソースは、EMC VNXeおよびUnityユニファイドストレージアレイのインベントリサポートを提供します。

このデータソースはCLIベースであり、VNXeデータソースが存在するAcquisition UnitにUnisphere for VNXe CLI（uemcli.exe）をインストールする必要があります。uemcli.exeは転送プロトコルとしてHTTPSを使用するため、Acquisition UnitからVNXe/Unityアレイへの HTTPS接続を開始できる必要があります。データソースで使用する読み取り専用ユーザが少なくとも1人必要です。

用語集

OnCommand Insight では、EMC VNXeデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
ストレージアレイ	ストレージ
プロセッサ	ストレージノード
ストレージプール	ストレージプール
一般的な iSCSI ブロック情報、 VMware VMFS	ボリューム
共有フォルダ	内部ボリューム
VMware NFSデータストアからのCIFS共有、NFS共有、共有	共有
Replication Remote System の略	同期

iSCSI ノード	iSCSI ターゲットノード
iSCSI イニシエータ	iSCSI ターゲットイニシエータ

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

このデータソースを設定して使用するための要件は次のとおりです。

- VNXe データコレクタは CLI ベースです。 VNXe データコレクタが存在する Acquisition Unit に Unisphere for VNXe CLI （ uemcli.exe ）をインストールする必要があります。
- uemcli.exe は HTTPS を転送プロトコルとして使用するため、 VNXe への HTTPS 接続を Acquisition Unit から開始できる必要があります。
- データソースで使用する読み取り専用ユーザが少なくとも1人必要です。
- 管理用 Solutions Enabler サーバの IP アドレス
- ポート 443 での HTTPS が必要です
- EMC VNXeデータコレクタは、NASおよびiSCSIによるインベントリのサポートを提供します。ファイバチャネルボリュームは検出されますが、InsightではFCマッピング、マスキング、ストレージポートについてはレポートされません。

設定

フィールド	説明
VNXe ストレージ	VNXe デバイスの IP アドレスまたは完全修飾ドメイン名
ユーザ名	VNXe デバイスのユーザ名
パスワード	VNXe デバイスのパスワード
uemcli実行可能ファイルの完全パス	への完全パス `uemcli.exe` 実行ファイル

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
VNXe CLIポート	VNXe CLI に使用するポート

インベントリ外部プロセスタイムアウト（秒）	外部プロセスのタイムアウト（デフォルトは1、800秒）

EMC VPLEXデータソース

このデータソースを設定するには、VPLEXサーバのIPアドレスと管理者レベルのドメインアカウントが必要です。

用語集

OnCommand Insight では、EMC VPLEXデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
クラスタ	ストレージ
エンジン	ストレージノード
デバイス、システム拡張	バックエンドストレージプール
仮想ボリューム	ボリューム
フロントエンドポート、バックエンドポート	ポート
分散デバイス	ストレージ同期
ストレージビュー	ボリュームマップ、ボリュームマスク
ストレージボリューム	バックエンド LUN
ITL	バックエンドパス

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- VPLEXサーバのIPアドレス
- VPLEX サーバの管理者レベルのドメインアカウント
- ポート 443 （ HTTPS ）：VPLEX 管理ステーションの TCP ポート 443 へのアウトバウンド接続が必要です。
- パフォーマンスを確保するには、 ssh/scp アクセス用の読み取り専用のユーザ名とパスワードを使用します。

- パフォーマンスを確保するには、ポート 22 が必要です。
- アクセスの検証：を使用して検証します `telnet` ポート443に接続します。デフォルトポート以外のポートの場合は、任意のブラウザでを使用します

設定

フィールド	説明
VPLEX Management Console の IP アドレス	VPLEX Management Console の IP アドレスまたは完全修飾ドメイン名
ユーザ名	VPLEX CLI のユーザ名
パスワード	VPLEX CLI のパスワード
VPLEX Management Consoleのパフォーマンスリモートipアドレス	VPLEX Management Console のパフォーマンスリモートの IP アドレス
パフォーマンスリモートユーザ名	VPLEX Management Console のパフォーマンスリモートのユーザ名
パフォーマンスリモートパスワード	VPLEX Management Console のパフォーマンスリモートのパスワード

高度な設定

フィールド	説明
通信ポート	VPLEX CLIに使用するポート
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）
再試行回数	インベントリの再試行回数
パフォーマンスポーリング間隔（秒）	パフォーマンスポーリング間隔（デフォルトは600秒）
パフォーマンスSSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは600秒）
SSHバナー待機タイムアウト（秒）	SSHバナーのタイムアウト（デフォルトは20秒）
再試行回数	パフォーマンスの再試行回数

EMC XtremIOデータソース

EMC XtremIO（HTTP）データソースを構成するには、XtremIO Management Server（XMS）ホストアドレスと管理者権限を持つアカウントが必要です。

用語集

OnCommand Insight では、EMC XtremIOデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク（ SSD ）	ディスク
クラスタ	ストレージ
コントローラ	ストレージノード
ボリューム	ボリューム
LUN マップ	ボリュームマップ
イニシエータ、ターゲット	ボリュームマスク

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- 各XtremIO Management ServerのIPアドレス
- 管理者権限を持つアカウント
- ポート 443 へのアクセス（ HTTPS ）

設定

フィールド	説明
XMS ホスト	XtremIO Management Server の IP アドレスまたは完全修飾ドメイン名
ユーザ名	XtremIO Management Server のユーザ名
パスワード	XtremIO Management Server のパスワード

高度な設定

フィールド	説明
TCP ポート	XtremIO Management Serverへの接続に使用するTCPポート（デフォルトは443）
インベントリのポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）
パフォーマンスのポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

Fujitsu Eternusデータソース

Fujitsu Eternusデータソースには、ストレージのIPアドレスが必要です。カンマで区切ることはできません。

用語集

OnCommand Insight では、Fujitsu ETERNUSデータソースから次のインベントリ情報を取得します。Insight で取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
ストレージ	ストレージ
シンプール、フレキシブル階層プール、 RAID グループ	ストレージプール
標準ボリューム、Snap Data Volume（SDV）、 Snap Data Poolボリューム（SDPV） シンプロビジョニングボリューム（TPV）	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- Eternus ストレージの IP アドレス。カンマで区切って指定することはできません
- SSH 管理レベルのユーザ名とパスワード
- ポート 22
- ページスクロールが無効になっていることを確認します。（clientv-show-more-scroll disable）

設定

フィールド	説明
Eternus ストレージの IP アドレス	Eternus ストレージの IP アドレス
ユーザ名	Eternus ストレージのユーザ名
パスワード	胸骨に使用するパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
SSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは600秒）

Hitachi Content Platform（**HCP**）データソース

このデータコレクタは、 HCP 管理 API を使用して、 Hitachi Content Platform （ HCP ）をサポートします。

用語集

OnCommand Insight では、HCPデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
HCP クラスタです	ストレージ
テナント	ストレージプール
ネームスペース	内部ボリューム
ノード	ノード

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

インベントリの要件

- HCP サーバの IP アドレス
- HCP ソフトウェアおよびピア権限の読み取り専用のユーザ名およびパスワード

設定

* フィールド *	* 概要 *
HCP ホスト	HCP ホストの IP アドレスまたは完全修飾ドメイン名
HCP ポート	デフォルトは 9090 です
HCPユーザーID	HCPホストのユーザ名
HCP パスワード	HCPホストのパスワード
HCP 認証タイプ	HCP_LOCAL または active_directory を選択してください

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは900秒）

HDS HiCommand Device Managerデータソース

HDS HiCommandおよびHiCommand Liteデータソースでは、HiCommand Device Managerサーバがサポートされます。OnCommand Insight は、標準のHiCommand APIを使用してHiCommandデバイスマネージャサーバと通信します。

用語集

OnCommand Insight では、HDS HiCommandおよびHiCommand Liteデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語

PDEV	ディスク
ジャーナルプール	ディスクグループ
ストレージアレイ	ストレージ
Port Controller の略	ストレージノード
アレイグループ 'DP プール	ストレージプール
論理ユニット、 LDEV	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

インベントリの要件

- HiCommand Device Manager サーバの IP アドレス
- HiCommand Device Manager ソフトウェアおよびピアの権限に対する読み取り専用のユーザ名とパスワード
- ポート要件： 2001 （ http ）または 2443 （ https ）
- アクセスの検証：
  - ピアのユーザ名とパスワードを使用してHiCommand Device Managerソフトウェアにログインします。
  - HiCommand Device Manager APIへのアクセスを確認します。 `telnet <HiCommand Device_Manager_server_ip\> 2001`

パフォーマンス要件

- HDS USP 、 USP V 、および VSP のパフォーマンス
  - Performance Monitor のライセンスが必要です。
  - 監視スイッチが有効になっている必要があります。
  - エクスポートツール (`Export.exe`）をOnCommand Insight サーバにコピーする必要があります。
  - エクスポートツールのバージョンとターゲットアレイのマイクロコードのバージョンが一致している必要があります。
- HDS AMSのパフォーマンス
  - Performance Monitorのライセンスが必要です。
  - Storage Navigator Modular 2（SNM2）CLIユーティリティがOnCommand Insight サーバにインストールされている必要があります。
  - 次のコマンドを使用して、OnCommand Insight でパフォーマンスを取得する必要があるAMS、WMS、SMSのすべてのストレージアレイを登録する必要があります。

◦ 登録したすべてのアレイがこのコマンドの出力に表示されていることを確認する必要があります。 `auunitref.exe`。

設定

* フィールド *	* 概要 *
HiCommand サーバ	HiCommand Device Manager サーバの IP アドレスまたは完全修飾ドメイン名
ユーザ名	HiCommand Device Manager サーバのユーザ名
パスワード	HiCommand Device Manager サーバのパスワード
デバイス - VSP G1000 （ R800 ）、 VSP （ R700 ）、 HUS VM （ HM700 ）、および USP ストレージ	VSP G1000 （ R800 ）、 VSP （ R700 ）、 HUS VM （ HM700 ）、および USP ストレージのデバイスリスト。各ストレージには以下が必要です。 • Array's IP：ストレージのIPアドレス • User Name：ストレージのユーザ名 • Password：ストレージのパスワード • Folder Containing Export Utility JAR Files（エクスポートユーティリティを含むフォルダ）：エクスポートユーティリティを含むフォルダ `.jar` ファイル
SNM2Devices - WMS/SMS/AMS ストレージ	WMS / SMS / AMS ストレージのデバイスリスト。各ストレージには以下が必要です。 • Array's IP：ストレージのIPアドレス • Storage Navigator CLI Path：SNM2 CLIパス • Account Authentication Valid：有効なアカウント認証を選択する場合に選択します • User Name：ストレージのユーザ名 • Password：ストレージのパスワード
「 Tuning Manager 」を「 Performance 」に選択します	パフォーマンスに合わせてTuning Managerを選択し、他のパフォーマンスオプションを上書きします
Tuning Manager Host （ホストのチューニング）	Tuning Manager の IP アドレスまたは完全修飾ドメイン名
Tuning Manager ポート	Tuning Manager に使用するポート
Tuning Manager のユーザ名	Tuning Manager のユーザ名

Tuning Manager パスワード	Tuning Managerのパスワード

HDS USP、USP V、およびVSPでは、どのディスクも複数のアレイグループに属することができます。

高度な設定

フィールド	説明
HiCommand Server ポート	HiCommand Device Manager に使用するポート
HTTPs が有効です	HTTPS を有効にする場合に選択します
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
「除外」または「含める」を選択してリストを指定します	以下のリストにあるアレイをデータの収集時に対象に含めるか除外するかを指定します
デバイスを除外または含める	対象に含めるか除外するデバイスの ID またはアレイ名をカンマで区切ったリスト
ホストマネージャを照会します	ホストマネージャを照会する場合に選択します
HTTPタイムアウト（秒）	HTTP接続タイムアウト（デフォルトは60秒）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
エクスポートのタイムアウト（秒）	エクスポートユーティリティのタイムアウト（デフォルトは300秒）

Hitachi Ops Center データコレクタ

このデータコレクタは、 Hitachi Ops Center の統合されたアプリケーションスイートを使用して、複数のストレージデバイスのインベントリとパフォーマンスのデータにアクセスします。インベントリと容量を検出するには、 Operations Center のインストールに「 Common Services 」と「 Administrator 」の両方のコンポーネントを含める必要があります。パフォーマンス収集では、さらに「 Analyzer 」を導入する必要があります。

用語集

OnCommand Insightはこのデータコレクタから次のインベントリ情報を取得します。取得したアセットのタイプごとに、そのアセットに使用される最も一般的な用語が表示されます。このデータコレクタを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	**OnCommand Insight** 期間
ストレージシステム	ストレージ
ボリューム	ボリューム
パリティグループ	ストレージプール（ RAID ）、ディスクグループ
ディスク	ディスク
ストレージプール	ストレージプール（シン、スナップ）
外部パリティグループ	ストレージプール（バックエンド）、ディスクグループ
ポート	ストレージノード→コントローラノード→ポートの順にクリックします
ホストグループ	ボリュームのマッピングとマスキング
ボリュームペア	ストレージ同期

注：これらは一般的な用語の対応のみを示したものであり、このデータコレクタのすべてのケースを表しているわけではありません。

インベントリの要件

インベントリデータを収集するには、次の情報が必要です。

- 「Common Services」コンポーネントをホストするOps CenterサーバのIPアドレスまたはホスト名
- ルート/ sysadminユーザアカウントとパスワード。Ops Centerコンポーネントをホストするすべてのサーバに存在します。HDSでは、Ops Center 10.8以降まで、LDAP/SSOユーザによるREST APIサポートは実装されていませんでした

パフォーマンス要件

パフォーマンスデータを収集するには、次の要件を満たしている必要があります。

- HDS Ops Centerの「Analyzer」モジュールがインストールされている必要があります
- ストレージアレイがOps Centerの「Analyzer」モジュールにデータを供給している必要があります

設定

フィールド	説明
Hitachi Ops Center の IP アドレス	「 Common Services 」コンポーネントをホストする Ops Center サーバの IP アドレスまたは完全修飾ドメイン名
ユーザ名	Ops Center サーバのユーザ名。
パスワード	Ops Center サーバのパスワード。

高度な設定

フィールド	説明

接続タイプ	デフォルトは HTTPS （ポート 443 ）です
TCP ポートを上書きします	デフォルト以外の場合に使用するポートを指定します
インベントリポーリング間隔（分）	インベントリのポーリング間隔。デフォルトは 40. です。
「除外」または「含める」を選択してリストを指定します	下のリストに表示されたアレイをデータの収集時に対象に含めるか除外するかを指定します。
デバイスリストをフィルタリングします	対象に含めるか除外するデバイスのシリアル番号をカンマで区切ったリスト
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔デフォルトは 300. です。

HDSストレージ

HDSストレージアセットのランディングページに記載されているオブジェクトや参照に適用される用語。

HDSストレージの用語

HDS ストレージアセットランディングページにあるオブジェクトや参考資料に関連する用語を次に示します。これらの用語の多くは、他のデータコレクタにも適用されます。

- Name — GetStorageArray XML API呼び出しを介してHDS HiCommand Device Managerの「name」属性から直接取得されます
- Model - GetStorageArray XML API呼び出しを介してHDS HiCommand Device Managerの「arrayType」属性から直接取得されます
- ベンダー-- HDS
- Family - GetStorageArray XML API呼び出しを介してHDS HiCommand Device Managerの「arrayFamily」属性から直接取得されます
- IP --アレイの管理IPアドレスであり'アレイ上のすべてのIPアドレスを網羅したリストではありません
- Raw Capacity（物理容量）--ディスクロールに関係なく、このシステムのすべてのディスクの合計容量を表す2進数の値。

HITACHI Storage Poolの略

HDSストレージプールのアセットランディングページに記載されているオブジェクトや参照に適用される用語。

HDSストレージプールの用語

HDS ストレージプールのアセットランディングページにあるオブジェクトや参照に関連する用語を次に示します。これらの用語の多くは、他のデータコレクタにも適用されます。

- タイプ：値は次のいずれかになります。
  - リザーブ(Reserved)--このプールがデータボリューム以外の目的(ジャーナリング'スナップショットなど)専用の場合

- Thin Provisioning：HDPプールの場合
- RAIDグループ：いくつかの理由により'これらが表示されない可能性があります

  OCIでは、容量がどのようなコストであっても二重にカウントされることは避けたいと強く考えているHDS では、通常、ディスクから RAID グループを作成し、それらの RAID グループにプールボリュームを作成し、それらのプールボリュームからプール（多くの場合 HDP を作成しますが、特別な目的にすることもあります）を構築する必要があります。基盤となるRAIDグループとプールの両方について報告された場合、物理容量の合計がディスクの合計を大幅に超えてしまいます。

OCIのHDS HiCommandデータコレクタは、プールボリュームの容量に応じてRAIDグループのサイズを任意に縮小します。そのため、OCIでRAIDグループがまったく報告されない場合があります。また、作成されたRAIDグループにはOCI Web UIには表示されず、OCI Data Warehouse（DWH）にも表示されるようにフラグが設定されます。これらの決定の目的は、ほとんどのユーザーが気にしないことでUIが乱雑にならないようにすることです。HDSアレイに50MBの空き容量があるRAIDグループがある場合、その空き容量を有意義な結果に使用することはおそらくできません。

- HDS プールは 1 つの特定のノードに関連付けられないため、ノードなし
- Redundancy - プールの RAID レベル。複数の RAID タイプで構成される HDP プールには、複数の値が含まれる可能性があります
- Capacity % - プールでデータ使用に使用されている割合。プールの使用済み GB と合計論理 GB サイズです
- オーバーコミット容量-「このプールの論理容量は、プールの論理容量をこの割合で超過した論理ボリュームの合計により、この割合でオーバーサブスクライブされています」を示す派生値。
- snapshot - このプールでの Snapshot の使用用にリザーブされている容量が表示されます

HDSストレージノード

HDSストレージノードのアセットランディングページに記載されているオブジェクトや参照に適用される用語。

HDSストレージノードの用語

HDS ストレージノードのアセットランディングページにあるオブジェクトや参照に関連する用語を次に示します。これらの用語の多くは、他のデータコレクタにも適用されます。

- 名前—モノリシックアレイ上のフロントエンドダイレクタ(FED)またはチャネルアダプタの名前'またはモジュラーアレイ上のコントローラの名前1 つの HDS アレイに 2 つ以上のストレージノードがある
- ボリューム—ボリュームテーブルには、このストレージノードが所有するポートにマッピングされているボリュームが表示されます

Hitachi Ops Center データコレクタ

このデータコレクタは、 Hitachi Ops Center の統合されたアプリケーションスイートを使用して、複数のストレージデバイスのインベントリとパフォーマンスのデータにアクセスします。インベントリと容量を検出するには、 Operations Center のインストールに「 Common Services 」と「 Administrator 」の両方のコンポーネントを含める必要があります。パフォーマンス収集では、さらに「 Analyzer 」を導入する必要があります。

用語集

OnCommand Insightはこのデータコレクタから次のインベントリ情報を取得します。取得したアセットのタイプごとに、そのアセットに使用される最も一般的な用語が表示されます。このデータコレクタを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	**OnCommand Insight** 期間
ストレージシステム	ストレージ
ボリューム	ボリューム
パリティグループ	ストレージプール（ RAID ）、ディスクグループ
ディスク	ディスク
ストレージプール	ストレージプール（シン、スナップ）
外部パリティグループ	ストレージプール（バックエンド）、ディスクグループ
ポート	ストレージノード→コントローラノード→ポートの順にクリックします
ホストグループ	ボリュームのマッピングとマスキング
ボリュームペア	ストレージ同期

注：これらは一般的な用語の対応のみを示したものであり、このデータコレクタのすべてのケースを表しているわけではありません。

インベントリの要件

インベントリデータを収集するには、次の情報が必要です。

- 「Common Services」コンポーネントをホストするOps CenterサーバのIPアドレスまたはホスト名
- ルート/ sysadminユーザアカウントとパスワード。Ops Centerコンポーネントをホストするすべてのサーバに存在します。HDSでは、Ops Center 10.8以降まで、LDAP/SSOユーザによるREST APIサポートは実装されていませんでした

パフォーマンス要件

パフォーマンスデータを収集するには、次の要件を満たしている必要があります。

- HDS Ops Centerの「Analyzer」モジュールがインストールされている必要があります
- ストレージアレイがOps Centerの「Analyzer」モジュールにデータを供給している必要があります

設定

フィールド	説明
Hitachi Ops Center の IP アドレス	「 Common Services 」コンポーネントをホストする Ops Center サーバの IP アドレスまたは完全修飾ドメイン名
ユーザ名	Ops Center サーバのユーザ名。

フィールド	説明
パスワード	Ops Center サーバのパスワード。

高度な設定

フィールド	説明
接続タイプ	デフォルトは HTTPS （ポート 443 ）です
TCP ポートを上書きします	デフォルト以外の場合に使用するポートを指定します
インベントリポーリング間隔（分）	インベントリのポーリング間隔。デフォルトは 40. です。
「除外」または「含める」を選択してリストを指定します	下のリストに表示されたアレイをデータの収集時に対象に含めるか除外するかを指定します。
デバイスリストをフィルタリングします	対象に含めるか除外するデバイスのシリアル番号をカンマで区切ったリスト
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔デフォルトは 300. です。

HDS NAS（HNAS）データソース

HDS NAS（HNAS）データソースは、HDS NASクラスタの検出をサポートするためのインベントリおよび設定のデータソースです。Insightでは、NFS共有とCIFS共有、ファイルシステム（Insightの内部ボリューム）、スパン（Insightのストレージプール）の検出がサポートされています。

このデータソースはSSHベースであるため、ホストするAcquisition Unitから、HNAS自体またはクラスタが接続されているSystems Management Unit（SMU）のTCP 22へのSSHセッションを開始できる必要があります。

用語集

OnCommand Insight では、HNASデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
階層	ディスクグループ
クラスタ	ストレージ
ノード	ストレージノード
スパン（ Span ）	ストレージプール
File System の略	内部ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

このデータソースを設定して使用するための要件は次のとおりです。

- デバイスの IP アドレス
- ポート 22 、 SSH プロトコル
- ユーザ名とパスワードの権限レベル： Supervisor
- 注：このデータコレクタはSSHベースなので、ホストするAUは、HNAS自体またはクラスタが接続されているSystems Management Unit（SMU）のTCP 22へのSSHセッションを開始できる必要があります。

このデータコレクタはSSHベースなので、ホストするAUは、HNAS自体またはクラスタが接続されているSystems Management Unit（SMU）のTCP 22へのSSHセッションを開始できる必要があります。

設定

フィールド	説明
HNAS ホスト	HNAS 管理ホストの IP アドレスまたは完全修飾ドメイン名
ユーザ名	HNAS CLI のユーザ名
パスワード	HNAS CLI のパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは30分）
SSHバナー待機タイムアウト（秒）	SSHバナーのタイムアウト（デフォルトは15秒）
SSHコマンドタイムアウト（秒）	SSHコマンドのタイムアウト（デフォルトは30秒）

HP CommandView AEデータソース

HP CommandView Advanced Edition（AE）およびCommandView AE CLI/SMI（AE Lite）データソースでは、CommandView（HiCommand）Device Managerサーバからのインベントリとパフォーマンスがサポートされます。

用語集

OnCommand Insight では、HP CommandView AEおよびAE Liteデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
PDEV	ディスク
ジャーナルプール	ディスクグループ
ストレージアレイ	ストレージ
Port Controller の略	ストレージノード
アレイグループ 'DP プール	ストレージプール
論理ユニット、 LDEV	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

インベントリの要件

- HiCommand Device Manager サーバの IP アドレス
- CommandView AEソフトウェアおよびピアの権限の読み取り専用のユーザ名とパスワード
- CommandView AE Liteバージョンのデバイスマネージャには、CLIのみがライセンスされています
- ポート要件： 2001

パフォーマンス要件

- HDS USP 、 USP V 、および VSP のパフォーマンス
  - Performance Monitor のライセンスが必要です。
  - 監視スイッチが有効になっている必要があります。
  - エクスポートツール (`Export.exe`）をOnCommand Insight サーバにコピーする必要があります。
  - エクスポートツールのバージョンとターゲットアレイのマイクロコードのバージョンが一致している必要があります。
- HDS AMSのパフォーマンス
  - Performance Monitorのライセンスが必要です。
  - Storage Navigator Modular 2（SNM2）CLIユーティリティがOnCommand Insight サーバにインストールされている必要があります。
  - 次のコマンドを使用して、OnCommand Insight でパフォーマンスを取得する必要があるAMS、

WMS、SMSのすべてのストレージアレイを登録する必要があります。

- 登録したすべてのアレイがこのコマンドの出力に表示されていることを確認する必要があります。 `auunitref.exe`。

設定

* フィールド *	* 概要 *
HiCommand サーバ	HiCommand Device Manager サーバの IP アドレスまたは完全修飾ドメイン名
ユーザ名	HiCommand Device Manager サーバのユーザ名
パスワード	HiCommand Device Manager サーバのパスワード
デバイス- USP、USP V、VSP/R600ストレージ	VSP G1000 （ R800 ）、 VSP （ R700 ）、 HUS VM （ HM700 ）、および USP ストレージのデバイスリスト。各ストレージには以下が必要です。 • Array's IP：ストレージのIPアドレス • User Name：ストレージのユーザ名 • Password：ストレージのパスワード • Folder Containing Export Utility JAR Files（エクスポートユーティリティを含むフォルダ）：エクスポートユーティリティを含むフォルダ `.jar` ファイル
SNM2Devices - WMS/SMS/AMS ストレージ	WMS / SMS / AMS ストレージのデバイスリスト。各ストレージには以下が必要です。 • Array's IP：ストレージのIPアドレス • Storage Navigator CLI Path：SNM2 CLIパス • Account Authentication Valid：有効なアカウント認証を選択する場合に選択します • User Name：ストレージのユーザ名 • Password：ストレージのパスワード
「 Tuning Manager 」を「 Performance 」に選択します	パフォーマンスに合わせてTuning Managerを選択し、他のパフォーマンスオプションを上書きします
Tuning Manager Host （ホストのチューニング）	Tuning Manager の IP アドレスまたは完全修飾ドメイン名
Tuning Manager ポート	Tuning Manager に使用するポート

Tuning Manager のユーザ名	Tuning Manager のユーザ名
Tuning Manager パスワード	Tuning Managerのパスワード

HDS USP、USP V、およびVSPでは、どのディスクも複数のアレイグループに属することができます。

高度な設定

フィールド	説明
HiCommand Server ポート	HiCommand Device Manager に使用するポート
HTTPs が有効です	HTTPS を有効にする場合に選択します
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
「除外」または「含める」を選択してリストを指定します	以下のリストにあるアレイをデータの収集時に対象に含めるか除外するかを指定します
デバイスを除外または含める	対象に含めるか除外するデバイスの ID またはアレイ名をカンマで区切ったリスト
ホストマネージャを照会します	ホストマネージャを照会する場合に選択します
HTTPタイムアウト（秒）	HTTP接続タイムアウト（デフォルトは60秒）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
エクスポートのタイムアウト（秒）	エクスポートユーティリティのタイムアウト（デフォルトは300秒）

HP EVA Storageデータソース

EVA Storage（SSSU）データソースを設定するには、Command View（CV）サーバのIPアドレス、およびCVソフトウェアに対する_read-only_usernameとパスワードが必要です。ユーザーはCVソフトウェアで定義する必要があります。

用語集

OnCommand Insight では、HP EVAデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
ディスクグループ	ディスクグループ（モデル化されていません）
ストレージセル	ストレージ
仮想ディスク	ストレージプール
仮想ディスク	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

インベントリの要件

- CVサーバのIPアドレス
- CVソフトウェアに対する読み取り専用のユーザ名とパスワード。ユーザーはCVソフトウェアで定義する必要があります。
- OnCommand Insight サーバ/ RAUにインストールされているサードパーティ製ソフトウェア： `sssu.exe`。。 `sssu.exe` バージョンはCVバージョンに対応している必要があります。
- アクセスの検証：を実行します `sssu.exe` ユーザ名とパスワードを使用したコマンド。

パフォーマンス要件

HP StorageWorks Command View EVAソフトウェアスイートがOnCommand Insight サーバーにインストールされている必要があります。または、EVAサーバにRemote Acquisition Unit（RAU）をインストールすることもできます。

1. HP StorageWorks Command View EVAソフトウェアスイートをOnCommand Insight サーバーにインストールするか、Remote Acquisition UnitをCommand View EVAサーバーにインストールします。
2. を探します `evaperf.exe` コマンドを実行します例： `c:\Program Files\Hewlett-Packard\EVA Performance Monitor\`
3. Command ViewサーバのIPを使用して、次の手順を実行します。
   a. このコマンドを実行します。860はデフォルトのポートです `Evaperf.exe server <Command View Server IP\> 860 <username\>`
   b. パスワードプロンプトでCommand Viewサーバのパスワードを入力します。

      これにより、コマンドラインプロンプトが表示され、それ以外は表示されません。
4. を実行してセットアップを確認します `evaperf.exe ls`。

   Command Viewサーバで管理されているアレイまたはコントローラのリストが表示されます。各行はEVAアレイのコントローラを示しています。

設定

* フィールド *	* 概要 *
CommandView Serverの略	EVA Storage ManagerのIPアドレスまたは完全修飾ドメイン名
ユーザ名	Command View Managerのユーザ名。名前はCommand Viewで定義する必要があります。
パスワード	Command View Managerのパスワード。
Performance User Nameの略	パフォーマンスを向上させるために、Command View Managerのユーザ名。名前はCommand Viewで定義する必要があります。
パフォーマンスパスワード	パフォーマンスを向上させるために、Command View Managerに使用するパスワード。

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
CLIホーム	CLIホームディレクトリのフルパス名 `sssu.exe` があります
インベントリ除外デバイス	対象に含めるデバイス名をカンマで区切ったリスト
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
Performance CLI Homeの略	アレイパフォーマンスの場合は、sssu.exeが格納されているCLIホームディレクトリの完全なパス名。アクセスを検証するには、を実行します `sssu.exe`
コマンドタイムアウト（秒）	`evaperf` コマンド待機タイムアウト（デフォルトは600秒）
Performance Exclude Devicesを参照してください	パフォーマンスデータの収集対象から除外するデバイスの名前をカンマで区切ったリスト

HPE Nimbleデータソース

HPE Nimble Data Collector は、 HPE Nimble ストレージアレイのインベントリとパフォ

ーマンスのデータをサポートしています。

用語集

OnCommand Insight では、HPE Nimbleデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
配列	ストレージ
ディスク	ディスク
プール	ストレージプール
ボリューム	ボリューム
イニシエータ	ストレージホストのエイリアス
コントローラ	ストレージノード
Fibre Channel インターフェイス	コントローラ

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- アレイがインストールおよび設定されていて、クライアントから完全修飾ドメイン名（ FQDN ）またはアレイ管理 IP アドレスを使用して到達できる必要があります。
- アレイで NimbleOS 2.3.x 以降が実行されている必要があります。
- アレイに対する有効なユーザ名とパスワードが必要です。
- アレイのポート 5392 が開いている必要があります。

設定

* フィールド *	* 概要 *
アレイ管理 IP アドレス	Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）またはアレイ管理 IP アドレスです。
ユーザ名	Nimble アレイのユーザ名
パスワード	Nimble アレイのパスワード

* フィールド *	* 概要 *
ポート	Nimble REST API が使用するポート。デフォルトは 5392. です。
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）

注：デフォルトのパフォーマンスのポーリング間隔は 300 秒で、変更することはできません。Nimble でサポートされている唯一の間隔はこれです。

Huawei OceanStorデータソース

OnCommand Insight では、Huawei OceanStor（REST / HTTPS）データソースを使用して、Huawei OceanStorストレージのインベントリを検出します。

用語集

OnCommand Insight は、Huawei OceanStorから次のインベントリおよびパフォーマンス情報を取得します。OnCommand Insight で取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータコレクタを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	OnCommand Insight 期間
ストレージプール	ストレージプール
File System の略	内部ボリューム
コントローラ	ストレージノード
FC ポート（マッピング済み）	ボリュームマップ
ホスト FC イニシエータ（マッピング済み）	ボリュームマスク
NFS / CIFS 共有	共有
共有	iSCSI ターゲットノード
iSCSI リンクイニシエータ	iSCSI イニシエータノード
ディスク	ディスク
LUN	ボリューム

要件

このデータコレクタを設定して使用するための要件は次のとおりです。

- デバイスIP
- OceanStor デバイスマネージャにアクセスするためのクレデンシャル
- ポート 8088 が使用可能であることが必要です

設定

フィールド	説明
OceanStor Host IP アドレス	OceanStor Device Manager の IP アドレスまたは完全修飾ドメイン名
ユーザ名	OceanStor Device Manager へのログインに使用するユーザ名
パスワード	OceanStor Device Manager へのログインに使用するパスワード

高度な設定

フィールド	説明
TCP ポート	OceanStor Device Managerへの接続に使用するTCPポート（デフォルトは8088）
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）

IBM Cleversafeデータソース

このデータソースは、IBM Cleversafeのインベントリとパフォーマンスのデータを収集します。

要件

このデータソースの設定に関する要件は次のとおりです。

- マネージャのIPアドレスまたはホスト名
- 同じのユーザ名とパスワード
- ポート 9440

設定

フィールド	説明
Cleversafeマネージャのホスト名またはIPアドレス	CleverSafeデバイスのホストIPアドレス
ユーザ名	Cleversafeへのログインに使用する名前
パスワード	Cleversafeへのログインに使用するパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	デフォルトは 60 分です
HTTP接続タイムアウト）	デフォルトは60秒です

IBM DSデータソース

IBM DS（CLI）データソースでサポートされるのは、DS6xxxデバイスとDS8xxxデバイスのみです。DS3xxx、DS4xxx、およびDS5xxxのデバイスは、NetApp E-Seriesデータソースでサポートされます。サポートされるモデルとファームウェアバージョンについては、Insightデータソースサポートマトリックスを参照してください。

用語集

OnCommand Insight では、IBM DSデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスクドライブモジュール	ディスク
ストレージイメージ	ストレージ
エクステントプール	ストレージプール
固定ブロックボリューム	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- 各 DS アレイの IP アドレス
- ストレージの表示名はオプションであり、外観上のみです
- 各 DS アレイの読み取り専用のユーザ名とパスワード
- サードパーティ製ソフトウェアをInsightサーバにインストール：IBM dscli
- アクセスの検証：を実行します `dscli` ユーザ名とパスワードを使用したコマンド
- ポートの要件： 80 、 443 、および 1750

設定

フィールド	説明
DSストレージ	DS Storage HostのIPアドレスまたは完全修飾ドメイン名
ユーザ名	DS CLIに使用する名前
パスワード	DS CLIのパスワード
実行可能ファイルのdscli.exeパス	への完全パス `dscli.exe`ユーティリティ。

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
ストレージ表示名	IBM DS ストレージアレイの名前
インベントリ除外デバイス	インベントリ収集の対象から除外するデバイスのシリアル番号をカンマで区切ったリスト
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
パフォーマンスフィルタタイプ	Include ：リストのデバイスからのみデータを収集します。Exclude ：リストのデバイスからデータを収集しません
パフォーマンスフィルタのデバイスリスト	パフォーマンス収集の対象に含めるか除外するデバイスの ID をカンマで区切ったリスト

IBM PowerVMデータソース

IBM PowerVM（SSH）データソースは、ハードウェア管理コンソール（HMC）で管理されるIBM POWERハードウェアインスタンスで実行されている仮想パーティションに関する情報を収集します。このデータソースを設定するには、SSHを使用してHMCにログインするためのユーザ名、およびHMCの設定に対する表示レベルの権限が必要です。

用語集

OnCommand Insight では、IBM PowerVMデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
hdisk	仮想ディスク
Managed System の略	ホスト
LPAR 、 VIO サーバ	仮想マシン
ボリュームグループ	データストア
物理ボリューム	LUN

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ハードウェア管理コンソール（ HMC ）の IP アドレス
- SSH経由でHMCにアクセスするためのユーザ名とパスワード
- ポート要件は SSH-22 です
- すべての管理システムおよび論理パーティションセキュリティドメインに対する表示権限

  ユーザには、 HMC の設定に対する表示権限も必要であり、 HMC コンソールセキュリティグループの VPD 情報を収集できる必要があります。ユーザーは、論理パーティションセキュリティグループの Virtual IO Server コマンドへのアクセスも許可されている必要があります。オペレータのロールから開始し、すべてのロールを削除することを推奨します。HMC の読み取り専用ユーザには、 AIX ホストでプロキシされたコマンドを実行する権限はありません。

- IBM のベストプラクティスは、 2 台以上の HMI でデバイスを監視することです。これにより、原因 OnCommand Insight で重複したデバイスが報告される場合があるため、このデータコレクタの詳細設定の [デバイスを除外する] リストに冗長デバイスを追加することを強くお勧めします。

設定

* フィールド *	* 概要 *
ハードウェア管理コンソール（HMC）のアドレス	PowerVM ハードウェア管理コンソールの IP アドレスまたは完全修飾ドメイン名
HMC ユーザ	ハードウェア管理コンソールのユーザ名
パスワード	ハードウェア管理コンソールのパスワード

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
SSH ポート	PowerVM への SSH に使用するポート
SSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは600秒）
再試行回数	インベントリの再試行回数
デバイスを除外します	対象から除外するデバイスの ID または表示名をカンマで区切ったリスト

IBM SVCデータソース

IBM SVCデータソースは、SSHを使用してインベントリとパフォーマンスのデータを収集し、SVCオペレーティングシステムを実行するさまざまなデバイスをサポートします。サポートされるデバイスには、 SVC 、 v7000 、 v5000 、 v3700 などのモデルが含まれます。サポートされるモデルとファームウェアバージョンについては、Insightデータソースサポートマトリックスを参照してください。

用語集

OnCommand Insight では、IBM SVCデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ドライブ	ディスク
クラスタ	ストレージ

ノード	ストレージノード
mdisk グループ	ストレージプール
仮想ディスク	ボリューム
mdisk	バックエンド LUN

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

インベントリの要件

- 各 SVC クラスタの IP アドレス
- ポート 22 を使用できます
- 公開鍵と秘密鍵のペア。Insightで生成するか、SVCですでに使用しているキーペアを再利用します

  既存のキーペアを再利用する場合は、それらのキーペアをPutty形式からOpenSSH形式に変換する必要があります。

- 公開鍵をSVCクラスタにインストールします
- 秘密鍵をデータソースで識別する必要があります
- アクセスの検証：開く `ssh` 秘密鍵を使用したSVCクラスタへのセッション

他社製ソフトウェアをインストールする必要はありません。

パフォーマンス要件

- SVC コンソールはすべての SVC クラスタに必須であり、 SVC 検出基本パッケージに必要です。
- クラスタノードから構成ノードにパフォーマンスデータファイルをコピーする場合にのみ必要な管理アクセスレベル。

  このアクセスレベルはSVC基本検出パッケージには必要ないため、SVC基本ユーザが正常に機能しない場合があります。

- ポート22が必要です
- このユーザのSSHキーと公開鍵を生成し、Acquisition Unitからアクセスできるように秘密鍵を格納する必要があります。SVC基本ユーザに適切な権限があれば、同じユーザとキーが機能します。インベントリデータとパフォーマンスデータに同じSSHキーを使用できます。
- データ収集を有効にするには、SSHを使用してSVCクラスタに接続し、次のコマンドを実行します。
  `svctask startstats -interval 1`

  または、SVC管理ユーザインターフェイスを使用してデータ収集を有効にします。

親シリアル番号の説明

従来、Insightでは、ストレージアレイのシリアル番号や個 々 のストレージノードのシリアル番号をレポートすることができました。ただし、一部のストレージアレイアーキテクチャはこれに適切に対応していません。SVCクラスタは1~4台のアプライアンスで構成でき、各アプライアンスには2つのノードがあります。アプライアンス自体のシリアル番号がある場合、そのシリアル番号はクラスタのシリアル番号でもノードのシリアル番号でもありません。

IBM SVCアレイのストレージノードオブジェクトの「Parent Serial Number」属性は、個 々 のノードが大規模なクラスタの一部にすぎない中間アプライアンス/エンクロージャ内に配置されている場合に適切に設定されます。

設定

* フィールド *	* 概要 *
クラスタ/秒IP	SVCストレージの完全修飾ドメイン名のIPアドレス
クレデンシャルタイプを指定するには、「 Password 」または「 OpenSSH Key File 」を選択してください	SSH経由でデバイスに接続するために使用するクレデンシャルタイプ
Inventory User Name の略	SVC CLI のユーザ名
Inventory Password （インベントリパスワード）	SVC CLI のパスワード
Inventory Private Key への完全パス	インベントリの秘密鍵ファイルの完全パス
Performance User Nameの略	パフォーマンス収集用のSVC CLIのユーザ名
パフォーマンスパスワード	パフォーマンス収集に使用するSVC CLIのパスワード
パフォーマンス秘密鍵への完全パス	パフォーマンスの秘密鍵ファイルの完全パス

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
デバイスを除外します	インベントリ収集の対象から除外するデバイスのIDをカンマで区切ったリスト
SSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは200秒）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

Performance Exclude Devicesを参照してください	パフォーマンス収集の対象から除外するデバイスのIDをカンマで区切ったリスト
パフォーマンスSSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは200秒）
ダンプされた統計情報ファイルをクリーンアップする場合	ダンプされた統計ファイルをクリーンアップする場合に選択します

IBM Tivoli Monitoringデータソース

このデータソースは、ファイルシステム利用率のみに使用されます。Tivoli Monitoringデータベース（Tivoli Monitoring Data Warehouseとも呼ばれます）と直接通信します。OracleデータベースとDB2データベースがサポートされています。

Oracleのエラー・メッセージ

このデータコレクタは、OnCommand Insight 7.3.11以降では使用できなくなりました。

SIDを指定して接続を試行したときに「ORA-12154」を含むエラーメッセージが表示される場合は、Oracle DBネットワークサービスの設定を再確認してください。アクセス設定で完全修飾ホスト名（「names.default_domain」など）が指定されている場合は、SIDフィールドに完全修飾サービス名を挿入してみてください。簡単な例としては、SIDへの接続があります `testdb` が失敗しており、Oracleの設定でドメインが指定されています`company.com`。ベースSIDの代わりに次の文字列を使用して接続を試行できます。`testdb.company.com`。

設定

フィールド	説明
Tivoli Monitoring Database IPの略	Tivoli MonitoringサーバのIPアドレスまたは完全修飾ドメイン名
ユーザ名	Tivoli Monitoringサーバのユーザ名
パスワード	Tivoli Monitoringサーバのパスワード

高度な設定

フィールド	説明
Tivoli Monitoringデータベースポート	Tivoliモニタリングデータベースに使用するポート
Oracle SIDまたはDB2データベース名	OracleリスナーサービスIDまたはDB2データベース名

インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
使用するデータベースドライバ	使用するデータベースドライバを選択します
データベースへの接続に使用されるプロトコル	データベースへの接続に使用されるプロトコル
データベーススキーマ	データベーススキーマを入力します

IBM TotalStorage DS4000データソース

このデータソースは、インベントリとパフォーマンスの情報を収集します。可能な構成は2つ（ファームウェア6.xと7.x以降）で、値はどちらも同じです。APIでボリュームデータの統計を収集します。

設定

* フィールド *	* 概要 *
アレイSANtricity コントローラのIPをカンマで区切ったリスト	コントローラのIPアドレスまたは完全修飾ドメイン名をカンマで区切って指定します

要件

- DS5 または FAStT の各アレイの IP アドレス
- アクセスの検証：各アレイの両方のコントローラのIPアドレスにpingを実行します。

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは30分）
パフォーマンスポーリング間隔（最大3600秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

IBM XIVデータソース

IBM XIV（CLI）データソースのインベントリの収集は、XIVコマンドラインインターフェイスを使用して実行します。XIVのパフォーマンスは、ポート5989でSMI-Sプロバイダを実行するXIVアレイにSMI-Sを呼び出して実現されます。

用語集

OnCommand Insight では、IBM XIVデータソースから次のインベントリ情報を取得します。Insightで取得した

アセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
ストレージシステム	ストレージ
ストレージプール	ストレージプール
ボリューム	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ポート要件： TCP ポート 7778
- XIV管理インターフェイスのIPアドレス
- 読み取り専用のユーザ名とパスワード
- XIV CLIがInsight ServerまたはRAUにインストールされている必要があります
- アクセスの検証：Insight Serverから、ユーザ名とパスワードを使用してXIVのユーザインターフェイスにログインします。

設定

* フィールド *	* 概要 *
IP アドレス	XIVストレージのIPアドレスまたは完全修飾ドメイン名
ユーザ名	XIV ストレージのユーザ名
パスワード	XIV ストレージのパスワード
XIV CLIディレクトリの完全パス	XIV CLIディレクトリの完全パス

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）

CLIプロセス待機タイムアウト（ミリ秒）	CLIプロセスのタイムアウト（デフォルトは7200000ミリ秒）
SMI-SホストIP	SMI-Sプロバイダホストの IPアドレス
SMI-Sポート	SMI-Sプロバイダホストが使用するポート
SMI-S プロトコル	SMI-S プロバイダへの接続に使用するプロトコル
SMI-Sネームスペース	SMI-Sネームスペース
ユーザ名	SMI-S プロバイダホストのユーザ名
パスワード	SMI-S プロバイダホストのパスワード
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
SMI-S接続の再試行回数	SMI-S接続の再試行回数

Infinidat InfiniBoxデータソース

Infinidat InfiniBox（HTTP）データソースは、Infinidat InfiniBoxストレージから情報を収集するために使用されます。InfiniBox管理ノードにアクセスする必要があります。

用語集

OnCommand Insight では、InfiniBoxデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ドライブ	ディスク
InfiniBox	ストレージ
ノード	ストレージノード
プール	ストレージプール
ボリューム	ボリューム
FC ポート	ポート

ファイルシステム	内部ボリューム
ファイルシステム	ファイル共有
ファイルシステムエクスポート	共有

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

設定

フィールド	説明
InfiniBox ホスト	InfiniBox 管理ノードの IP アドレスまたは完全修飾ドメイン名
ユーザ名	InfiniBox 管理ノードのユーザ名
パスワード	InfiniBox 管理ノードのパスワード

高度な設定

フィールド	説明
TCP ポート	InfiniBoxサーバへの接続に使用するTCPポート（デフォルトは443）
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
接続タイムアウト	接続タイムアウト（デフォルトは60秒）

Microsoft Azure computeデータソース

OnCommand Insightsは、Azureコンピューティングデータコレクタを使用して、Azureコンピューティングインスタンスからインベントリとパフォーマンスのデータを取得します。

要件

このデータコレクタを設定するには、次の情報が必要です。

- ポート要件： 443 HTTPS
- Azure Management Rest IP （ management.azure.com ）

- Azureサービスプリンシパルアプリケーション（クライアント）ID（ユーザアカウント）
- Azureサービスプリンシパル認証キー（ユーザパスワード）

Insight Discovery用のAzureアカウントをセットアップする必要があります。アカウントを適切に設定してAzureにアプリケーションを登録すると、InsightでAzureインスタンスを検出するために必要なクレデンシャルが取得されます。検出用アカウントの設定方法については、https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portalを参照してください

設定

次の表に従って、データソースフィールドにデータを入力します。

フィールド	説明
Azure サービスプリンシパルアプリケーション（クライアント） ID （リーダーのロールが必要）	Azure へのサインイン IDリーダーの役割アクセスが必要です。
Azure テナント ID	Microsoft テナント ID
Azure サービスプリンシパルの認証キー	ログイン認証キー
Microsoft が API リクエストを請求することを理解しています	これをチェックして、 Insight のポーリングで作成された API 要求を Microsoft から課金することを理解していることを確認します。

詳細設定

次の表に従って、データソースフィールドにデータを入力します。

フィールド	説明
インベントリポーリング間隔（分）	デフォルトは 60 です。
「除外」または「含める」を選択して、タグによる VM のフィルタリングに適用します	データの収集時にタグを使用して VM を含めるか除外するかを指定します。``Include"を選択した場合、Tag Keyフィールドを空にすることはできません。
VM をフィルタするタグキーと値	+ タグのフィルタ * をクリックして、 VM のキーとタグの値に一致するキーと値をフィルタリングして、対象に含める / 除外する VM （および関連ディスク）を選択します。タグキーは必須です。タグ値はオプションです。タグ値が空の場合、タグキーと一致する限り、 VM はフィルタリングされます。
パフォーマンスポーリング間隔（秒）	

Azure NetApp Files データソース

このデータソースは、Azure NetApp Files （ANF）のインベントリとパフォーマンスのデータを取得します。

要件

このデータソースの設定に関する要件は次のとおりです。

- ポート要件： 443 HTTPS
- Azure Management Rest IP （ management.azure.com ）
- Azureサービスプリンシパルアプリケーション（クライアント）ID（ユーザアカウント）
- Azure Service Principal認証キー（ユーザパスワード）
- Cloud Insights 検出用の Azure アカウントを設定する必要があります。

  アカウントを適切に設定し、アプリケーションを Azure に登録すると、 Cloud Insights で Azure インスタンスを検出するために必要なクレデンシャルが付与されます。次のリンクでは、検出用のアカウントを設定する方法について説明します。

  https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

設定

フィールド	説明
Azureサービスプリンシパルアプリケーション（クライアント）ID	Azure へのサインイン ID
Azure テナント ID	Azure テナント ID
Azure サービスプリンシパルの認証キー	ログイン認証キー
Microsoft が API リクエストを請求することを理解しています	これをチェックして、 Insight のポーリングで作成された API 要求を Microsoft から課金することを理解していることを確認します。

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	デフォルトは 60 分です

Microsoft Hyper-Vデータソース

Microsoft Hyper-Vデータソースを設定するには、物理ホスト（ハイパーバイザー）のIPアドレスまたは解決可能なDNS名が必要です。このデータソースでは、PowerShell（以

前はWMIを使用）を使用します。

用語集

OnCommand Insight では、Hyper-Vデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
Virtual hard diskの略	仮想ディスク
ホスト	ホスト
仮想マシン	仮想マシン
Cluster Shared Volume （ CSV ；クラスタ共有ボリューム）、パーティションボリューム	データストア
Internet SCSI Device 、 Multi Path SCSI LUN の略	LUN
ファイバチャネルポート	ポート

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- Hyper-V では、データ収集とリモートアクセス / 管理用にポート 5985 が開いている必要があります。
- クラスタリンググループノードの IP アドレス
- ハイパーバイザーのローカル管理者のユーザとパスワードです
- 管理者レベルのユーザアカウント
- ポートの要件:ポート135およびダイナミックTCPポートは、Windows 2003以前の場合は1024-65535、Windows 2008の場合は49152-65535に割り当てられます。
- データコレクタがIPアドレスのみを参照している場合でも、DNS解決は成功する必要があります。
- 各Hyper-Vハイパーバイザーで、すべてのホスト上のすべてのVMに対して「リソース計測」をオンにする必要があります。これにより、各ハイパーバイザーは、各ゲストで Cloud Insights に使用できるデータを増やすことができます。この値を設定しない場合は、各ゲストのパフォーマンスメトリックが取得される回数が少なくなります。リソース計測の詳細については、 Microsoft のドキュメントを参照してください。

  "Hyper-V のリソース計測の概要"

  "Enable - VMResourceMetering"

設定

* フィールド *	* 概要 *
物理ホストの IP アドレス	物理ホスト（ハイパーバイザー）の IP アドレスまたは完全修飾ドメイン名
ユーザ名	ハイパーバイザーの管理者のユーザ名
パスワード	ハイパーバイザーのパスワードです
NT ドメイン	クラスタ内のノードで使用される DNS 名

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
接続タイムアウト（ミリ秒）	接続タイムアウト（デフォルトは60000ミリ秒）

NetApp clustered Data ONTAP データソース

このデータソースは、clustered Data ONTAP を使用するストレージシステムに使用します。読み取り専用のAPI呼び出しに使用する管理者アカウントが必要です。

用語集

OnCommand Insight では、clustered Data ONTAP データソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
RAID グループ	ディスクグループ
クラスタ	ストレージ
ノード	ストレージノード
アグリゲート	ストレージプール
LUN	ボリューム

ボリューム	内部ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- 読み取り専用のAPI呼び出しに使用する管理者アカウント
- ターゲットIPはクラスタ管理LIFです
- ネットアップクラスタにログインするためのユーザ名（デフォルトのSVMに対するONTAPIアプリケーションの読み取り専用ロール名を使用）とパスワード
- ポートの要件： 80 または 443
- ライセンス要件：FCPライセンスと、検出に必要なマッピング/マスクされたボリューム

設定

* フィールド *	* 概要 *
ネットアップ管理 IP	ネットアップクラスタの IP アドレスまたは完全修飾ドメイン名
ユーザ名	ネットアップクラスタのユーザ名
パスワード	ネットアップクラスタのパスワード

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

clustered Data ONTAP ストレージ

ネットアップのclustered Data ONTAP ストレージアセットランディングページに記載されているオブジェクトや参照に適用される用語。

clustered Data ONTAP ストレージの用語

以下の用語は、NetApp clustered Data ONTAP のストレージアセットランディングページに表示されるオブジェクトや参照先に適用されます。これらの用語の多くは、他のデータコレクタにも適用されます。

- Model --このクラスタ内で一意の個別のノードモデル名をカンマで区切ったリスト。クラスタ内のすべてのノードのモデルタイプが同じ場合、表示されるモデル名は 1 つだけです。
- vendor --新しいデータソースを設定する場合と同じベンダー名。
- シリアル番号—アレイのシリアル番号NetApp clustered Data ONTAP などのクラスタアーキテクチャストレージシステムでは、このシリアル番号が個 々 の「ストレージノード」のシリアル番号よりも有用でない場合があります。
- IP：通常は、データソースで設定されているIPまたはホスト名です。
- マイクロコードバージョン—ファームウェア。
- Raw Capacity：役割に関係なく、システム内のすべての物理ディスクの2進数の合計。
- レイテンシ：ホストに直面しているワークロードで発生している状況を読み取りと書き込みの両方で表したもの。OCIがこの価値を直接提供するのが理想的ですが、そうではないことがよくあります。OCIでは、この機能を提供するアレイの代わりに、個 々 の内部ボリュームの統計に基づいてIOPSの加重計算を実行します。
- スループット：内部ボリュームから集計された値。
- 管理—これには'デバイスの管理インタフェースのハイパーリンクが含まれている場合がありますインベントリレポートの一部としてInsightデータソースによってプログラムによって作成されます。

clustered Data ONTAP ストレージプール

NetApp clustered Data ONTAP ストレージプールのアセットランディングページに記載されているオブジェクトや参照に適用される用語。

clustered Data ONTAP ストレージプールの用語

以下に示す用語は、NetApp clustered Data ONTAPストレージプールのアセットランディングページにあるオブジェクトや参照先に適用されます。これらの用語の多くは、他のデータコレクタにも適用されます。

- ストレージ—このプールが配置されているストレージアレイ必須。
- タイプ(Type)--可能性の列挙されたリストから'説明的な値を指定します最も一般的な構成は「アグリゲート」または「RAIDグループ」です。
- ノード：このストレージアレイのアーキテクチャでプールが特定のストレージノードに属する場合は、ストレージアレイの名前が独自のランディングページへのハイパーリンクとして表示されます。
- [Uses Flash Pool]-[Yes/No Value]-このSATA / SASベースのプールには、キャッシュアクセラレーションにSSDが使用されていますか。
- redundancy — RAIDレベルまたは保護スキーム。raid_dp はデュアルパリティ、 raid_dp はトリプルパリティです。
- 容量—使用済み論理容量、使用可能容量、論理合計容量、およびこれらの使用率が表示されます。
- オーバーコミット容量：効率化テクノロジを使用して、ストレージプールの論理容量よりも大きいボリュームまたは内部ボリュームの合計容量を割り当てた場合、この割合の値は0%より大きくなります。
- スナップショット—使用中のスナップショット容量と合計容量(ストレージプールアーキテクチャがその容量の一部をスナップショット専用のセグメント領域に使用している場合)MetroCluster 構成のONTAP ではこの傾向が見られますが、他のONTAP 構成ではそうではありません。
- 利用率—このストレージプールに容量を提供しているディスクのうち、最も高いディスクビジー率を示すパーセンテージ。ディスク利用率は、必ずしもアレイのパフォーマンスと強い相関関係があるとは限りま

せん。ホスト主導のワークロードがない場合、ディスクのリビルドや重複排除処理などが原因で利用率が高くなる可能性があります。また、多くのアレイのレプリケーション実装では、内部ボリュームまたはボリュームのワークロードとして表示されずに、ディスク利用率が上昇する可能性があります。

- IOPS --このストレージプールに容量を提供しているすべてのディスクの合計IOPS。
- スループット—このストレージプールに容量を提供しているすべてのディスクの合計スループット

clustered Data ONTAP ストレージノード

NetApp clustered Data ONTAPのストレージノードのアセットランディングページに記載されている、オブジェクトや参照に適用される用語。

clustered Data ONTAP ストレージノードの用語

以下の用語は、NetApp clustered Data ONTAP ストレージプールのアセットランディングページに表示されるオブジェクトや参照先に適用されます。これらの用語の多くは、他のデータコレクタにも適用されます。

- ストレージ—このノードが属するストレージアレイ必須。
- HAパートナー-- 1つのノードが1つだけ他のノードにフェイルオーバーするプラットフォームでは、一般的にここに表示されます。
- State --ノードのヘルス。アレイが正常な状態でデータソースでインベントリを作成できる場合にのみ使用できます。
- model --ノードのモデル名。
- version --デバイスのバージョン名
- シリアル番号—ノードのシリアル番号
- memory --ベース2メモリ(使用可能な場合)。
- 利用率-- ONTAP では、これは独自のアルゴリズムによるコントローラの応力指数です。パフォーマンスポーリングが行われるたびに、 WAFL ディスクの競合率または平均 CPU 利用率の値が 0 ～ 100% の範囲で報告されます。50%を超える値が続く場合は、サイズ不足を示しています。コントローラ/ノードのサイズが十分でないか、書き込みワークロードを吸収するのに十分な回転式ディスクがない可能性があります。
- IOPS：ノードオブジェクトに対するONTAP ZAPI呼び出しから直接導出されます。
- レイテンシ：ノードオブジェクトに対するONTAP ZAPI呼び出しから直接導出されます。
- スループット：ノードオブジェクトに対するONTAP ZAPI呼び出しから直接導出されます。
- processors — CPU数。

NetApp clustered Data ONTAP for Unified Managerデータソース

このデータソースは、Unified Manager（UM）6.0以降のデータベースからONTAP 8.1.xのデータを収集します。Insightは、このデータソースを使用して、UMに設定されて入力されたすべてのクラスタを検出します。効率化のため、Insightではクラスタ自体に対してZAPIは呼び出されません。このデータソースではパフォーマンスはサポートされていません。

設定

このデータコレクタは、OnCommand Insight 7.3.11以降では使用できなくなりました。

* フィールド *	* 概要 *
Unified ManagerのIP	Unified ManagerのIPアドレスまたは完全修飾ドメイン名
ユーザ名	Unified Managerのユーザ名
パスワード	Unified Managerのパスワード
ポート	Unified Managerとの通信に使用するポート（デフォルトは3306）

高度な設定

* フィールド *	* 概要 *
Inventory Poll Interval (min) Interval	インベントリポーリングの間隔（デフォルトは15分）
クラスタを除外します	対象から除外するクラスタのIPをカンマで区切ったリスト

NetApp Data ONTAP 7-Modeデータソース

Data ONTAP 7-Modeソフトウェアを使用するストレージシステムの場合は、ONTAPIデータソースを使用します。このデータソースでは、CLIを使用して容量の値を取得します。

用語集

OnCommand Insight では、NetApp Data ONTAP 7-Modeデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
RAID グループ	ディスクグループ
ストレージシステム	ストレージ

ストレージシステム	ストレージノード
アグリゲート	ストレージプール
LUN	ボリューム
ボリューム	内部ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- FAS ストレージコントローラおよびパートナーのIPアドレス
- ポート 443
- コントローラとパートナーのユーザ名とパスワード
- 7-Mode 用の次のロール権限を持つコントローラとパートナーコントローラのカスタムの管理者レベルのユーザ名とパスワードです。
  - 「 api- * 」：すべてのネットアップストレージ API コマンドの実行を OnCommand Insight に許可します。
  - 「 login-http-admin 」： HTTP 経由で OnCommand Insight がネットアップストレージに接続できるようにします。
  - 「 security-api-vfiler 」： vFiler ユニットの情報を取得する NetApp ストレージ API コマンドの実行を OnCommand Insight に許可します。
  - 「 cli-options 」：ストレージシステムオプションを読み取るために使用します。
  - 「 cli-lun 」： LUN 管理用コマンドにアクセスします。指定した LUN または LUN のクラスのステータス（ LUN のパス、サイズ、オンライン / オフライン状態、共有状態）が表示されます。
  - 「 cli-df 」：空きディスクスペースを表示する場合に使用します。
  - 「 cli-ifconfig 」：インターフェイスと IP アドレスを表示します。

設定

* フィールド *	* 概要 *
Filerのアドレス	ネットアップファイラーのIPアドレスまたは完全修飾ドメイン名
ユーザ名	NetApp Filerのユーザ名
パスワード	NetApp Filerのパスワード

クラスタ内のHAパートナーファイラーのアドレス	HAパートナーファイラーのIPアドレスまたは完全修飾ドメイン名
クラスタ内のHAパートナーファイラーのユーザ名	ネットアップHAパートナーファイラーのユーザ名
クラスタ内の HA パートナーファイラーのパスワード	ネットアップHAパートナーファイラーのパスワード

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
接続タイプ	接続タイプを選択します
接続ポート	NetApp API に使用するポート
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

ストレージシステム接続

このデータソースでデフォルトの管理ユーザを使用する代わりに、ネットアップストレージシステムに対する管理者権限を持つユーザを設定して、このデータソースがネットアップストレージシステムからデータを取得できるようにすることもできます。

ネットアップストレージシステムに接続するには、メインの pfiler （ストレージシステムが存在する pfiler ）の取得時に次の条件を満たすユーザを指定する必要があります。

- ユーザは vfiler0 （ルートファイラー / pfiler ）に属している必要があります。

  メインの pfiler を取得するときにストレージシステムが取得されます。

- 次のコマンドで、ユーザロールの機能を定義します。
  - 「 api- * 」：すべてのネットアップストレージ API コマンドの実行を OnCommand Insight に許可します。このコマンドは、 ZAPI を使用する場合は必須です。
  - 「 login-http-admin 」： HTTP 経由で OnCommand Insight がネットアップストレージに接続できるようにします。このコマンドは、 ZAPI を使用する場合は必須です。
  - 「 security-api-vfiler 」： vFiler ユニットの情報を取得する NetApp ストレージ API コマンドの実行を OnCommand Insight に許可します。
  - 「 cli-options 」：「 options 」コマンドで、パートナーの IP と有効なライセンスを取得するために使用されます。
  - 「cli-lun」：LUNを管理するためのコマンドにアクセスします。指定した LUN または LUN のクラスのステータス（ LUN のパス、サイズ、オンライン / オフライン状態、共有状態）が表示されます。

- 「 cli-df 」：「 df -s 」、「 df -r 」、「 df -A -r 」コマンドで、空きスペースを表示するために使用されます。
- 「 cli-ifconfig 」：「 ifconfig -a 」コマンドで、ファイラーの IP アドレスを取得するために使用されます。
- 「 cli-rdfile 」：「 rdfile /etc/netgroup 」コマンドで、ネットグループを取得するために使用されます。
- 「 cli-date 」：「 date 」コマンドで、 Snapshot コピーを取得する完全な日付を取得するために使用されます。
- 「 cli-snap 」：「 snap list 」コマンドで、 Snapshot コピーを取得するために使用されます。

cli-date または cli-snap の権限が付与されていない場合、データ収集は完了できますが、 Snapshot コピーは報告されません。

7-Mode データソースを正常に取得し、ストレージシステムで警告が生成されないようにするには、次のいずれかのコマンド文字列を使用してユーザロールを定義する必要があります。2 つ目の文字列は、 1 つ目の文字列を簡潔に表したものです。

```
login-http-admin,api-*,security-api-vfile,cli-rdfile,cli-options,cli-
df,cli-lun,cli-ifconfig,cli-date,cli-snap,
or
login-http-admin,api-*,security-api-vfile,cli-*
```

NetApp E-Seriesデータソース

NetApp E-Seriesデータソースは、インベントリとパフォーマンスの情報を収集します。可能な構成は 2 種類（ファームウェア 6.x とファームウェア 7.x 以降）で、値はどちらも同じです。

用語集

OnCommand Insight では、NetApp E-Seriesデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ドライブ	ディスク
ボリュームグループ	ディスクグループ
ストレージアレイ	ストレージ
コントローラ	ストレージノード
ボリュームグループ	ストレージプール

ボリューム	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- アレイの各コントローラの IP アドレス
- ポート要件 2463

設定

* フィールド *	* 概要 *
アレイ SANtricity コントローラの IP をカンマで区切ったリスト	アレイコントローラの IP アドレスまたは完全修飾ドメイン名

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは30分）
パフォーマンスポーリング間隔（最大3600秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

Eシリーズストレージ

NetApp Eシリーズストレージのアセットランディングページに記載されているオブジェクトや参照に適用される用語。

Eシリーズストレージの用語

以下の用語は、NetApp Eシリーズストレージアセットランディングページに表示されるオブジェクトや参照先に適用されます。これらの用語の多くは、他のデータコレクタにも適用されます。

- model --デバイスのモデル名。
- vendor --新しいデータソースを設定する場合と同じベンダー名。
- シリアル番号—アレイのシリアル番号NetApp clustered Data ONTAP などのクラスタアーキテクチャストレージシステムでは、このシリアル番号が個 々 の「ストレージノード」のシリアル番号よりも有用でない場合があります。
- IP：通常は、データソースで設定されているIPまたはホスト名です。
- マイクロコードバージョン—ファームウェア。
- Raw Capacity：役割に関係なく、システム内のすべての物理ディスクの2進数の合計。

- レイテンシ：ホストに直面しているワークロードで発生している状況を読み取りと書き込みの両方で表したもの。Insightでは、ストレージ内のボリュームからIOPS加重平均を算出します。
- スループット—アレイのホスト側の合計スループットInsightでは、ボリュームのスループットを合計してこの値を算出します。
- 管理—これには'デバイスの管理インタフェースのハイパーリンクが含まれている場合がありますインベントリレポートの一部としてInsightデータソースによってプログラムによって作成されます。

Eシリーズストレージプール

NetApp Eシリーズストレージプールのアセットランディングページに記載されているオブジェクトや参照に適用される用語。

Eシリーズストレージプールの用語

以下の用語は、NetApp Eシリーズストレージプールのアセットランディングページに表示されるオブジェクトや参照先に適用されます。これらの用語の多くは、他のデータコレクタにも適用されます。

- ストレージ—このプールが配置されているストレージアレイ必須。
- タイプ(Type)--可能性の列挙されたリストから'説明的な値を指定します最も一般的な構成は「シンプロビジョニング」または「RAIDグループ」です。
- ノード：このストレージアレイのアーキテクチャでプールが特定のストレージノードに属する場合は、ストレージアレイの名前が独自のランディングページへのハイパーリンクとして表示されます。
- Flash Poolを使用（「はい」または「いいえ」）
- redundancy — RAIDレベルまたは保護スキーム。Eシリーズでは、DDPプールについて「RAID 7」が報告されます。
- 容量—使用済み論理容量、使用可能容量、論理合計容量、およびこれらの使用率が表示されます。どちらの値にもEシリーズの「予約済み」容量が含まれるため、Eシリーズのユーザインターフェイスで表示される数値と割合がどちらも大きくなります。
- オーバーコミット容量：効率化テクノロジを使用して、ストレージプールの論理容量よりも大きい合計ボリューム容量を割り当てた場合、この割合の値は0%より大きくなります。
- スナップショット—使用中のスナップショット容量と合計容量(ストレージプールアーキテクチャがその容量の一部をスナップショット専用のセグメント領域に使用している場合)
- 利用率：このストレージプールに容量を提供しているディスクのうち、ディスクビジー率が最も高い割合を示すパーセンテージ。ディスク利用率は、必ずしもアレイのパフォーマンスと強い相関関係があるとは限りません。ホスト駆動型のワークロードがない場合、ディスクのリビルドや重複排除処理などが原因で利用率が高くなる可能性があります。また、多くのアレイのレプリケーション実装では、ボリュームのワークロードとしては表示されませんが、ディスク利用率が上昇する可能性があります。
- IOPS --このストレージプールに容量を提供しているすべてのディスクの合計IOPS。
- スループット—このストレージプールに容量を提供しているすべてのディスクの合計スループット

Eシリーズストレージノード

NetApp Eシリーズストレージノードのアセットランディングページに記載されている、オブジェクトまたは参照に適用される用語。

Eシリーズストレージノードの用語

以下の用語は、NetApp Eシリーズストレージプールのアセットランディングページに表示されるオブジェクトや参照先に適用されます。これらの用語の多くは、他のデータコレクタにも適用されます。

- ストレージ—このノードが属するストレージアレイ必須。
- HAパートナー-- 1つのノードが1つだけ他のノードにフェイルオーバーするプラットフォームでは、一般的にここに表示されます。
- State --ノードのヘルス。アレイが正常な状態でデータソースでインベントリを作成できる場合にのみ使用できます。
- model --ノードのモデル名。
- version --デバイスのバージョン名
- シリアル番号—ノードのシリアル番号
- memory --ベース2メモリ(使用可能な場合)。
- 利用率：NetApp Eシリーズでは現在利用率を使用できません。
- IOPS -このノードにのみ属するボリュームのすべてのIOPSを合計して算出します。
- Latency --このコントローラでの一般的なホストのレイテンシまたは応答時間を表す数値。Insightでは、このノードにのみ属するボリュームからIOPSの加重平均を計算します。
- スループット—このコントローラ上のホストによって駆動されるスループットを表す数値。このノードにのみ属するボリュームのスループットをすべて合計して算出します。
- processors — CPU数。

NetApp Host and VM File Systemsデータソース

NetApp Host and VM File Systemsデータソースを使用して、すべてのMicrosoft WindowsホストおよびVM（仮想マシン）ファイルシステム、およびサポートされているすべてのLinux VM（仮想的にマッピングされたVMのみ）について、ファイルシステムの詳細とストレージリソースのマッピングを取得できます。 設定済みのCompute Resource Group（CRG；コンピューティングリソースグループ）でアノテートされているInsightサーバ内の既存のファイル。

一般要件

- この機能は別途購入する必要があります。

  詳細については、Insightの担当者にお問い合わせください。

- Insightのサポートマトリックスで、お使いのホストまたは仮想マシンのオペレーティングシステムがサポートされていることを確認してください。

  ファイルシステムからストレージリソースへのリンクが作成されていることを確認するには、関連するストレージベンダーまたは仮想化ベンダーのタイプとバージョンで、必要なボリュームまたは仮想ディスクの識別データが報告されていることを確認します。

Microsoft Windowsの要件

- このデータソースは、Window Management Instrumentation（WMI）データ構造を使用してデータを取得します。

  このサービスは動作しており、リモートで利用できる必要があります。特に、ポート135にアクセスできる必要があり、ファイアウォールの背後にある場合は開いておく必要があります。

- Windowsドメインユーザには、WMI構造にアクセスするための適切な権限が必要です。
- 管理者権限が必要です。
- Windows 2003以前に1024～65535が割り当てられた動的TCPポート
- ポート49152～-65535（Windows 2008の場合）

原則として、Insight、AU、およびこのデータソースの間にファイアウォールを使用する場合は、Microsoftチームに相談して、必要と思われるポートを特定する必要があります。

Linuxの要件

- このデータソースは、Secure Shell（SSH）接続を使用してLinux VMに対してコマンドを実行します。

  SSHサービスが動作していて、リモートで使用できる必要があります。特に、ポート22にアクセスできる必要があり、ファイアウォールの背後にある場合はポート22を開く必要があります。

- SSHユーザには、Linux VMに対して読み取り専用コマンドを実行するためのsudo権限が必要です。

  SSHへのログインとsudoパスワードチャレンジの回答 へのログインには、同じパスワードを使用する必要があります。

使用上の推奨事項

- オペレーティングシステムのクレデンシャルが同じホストおよび仮想マシンのグループには、同じ[Compute Resource Group]アノテーションをアノテートする必要があります。

  各グループにこのデータソースのインスタンスが割り当てられ、それらのホストおよび仮想マシンからファイルシステムの詳細が検出されます。

- このデータソースのインスタンスで成功率が低い場合（たとえば、グループ内の1、000台のホストおよび仮想マシンのうち、OnCommand Insight でファイルシステムの詳細が検出されるのは50台のみ）、 検出に成功したホストと仮想マシンを別のコンピューティングリソースグループに移動する必要があります。

設定

フィールド	説明
ユーザ名	適切な権限を持つオペレーティングシステムユーザーWindowsオペレーティングシステムユーザーのファイルシステムデータを取得するには、ドメインプレフィックスを含める必要があります。

パスワード	オペレーティングシステムユーザのパスワード
コンピュートリソースグループ	データソースでファイルシステムを検出するホストおよび仮想マシンのフラグとして使用されるアノテーション値。値が空の場合は、現在いずれのコンピューティングリソースグループもアノテートされていないすべてのホストおよび仮想マシンのファイルシステムがデータソースで検出されます。

高度な設定

フィールド	説明
インベントリのポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは360分）

NetApp SolidFire データソース

NetApp SolidFire データソースでは、インベントリとパフォーマンスの両方の収集について、iSCSIとFibre Channel SolidFire の両方の構成がサポートされます。

SolidFire データソースでは、SolidFire REST APIを利用します。データソースが配置されているAcquisition Unitから、SolidFire クラスタ管理IPアドレスのTCPポート443へのHTTPS接続を開始できる必要があります。データソースには、SolidFire クラスタに対してREST APIクエリを実行するためのクレデンシャルが必要です。

用語集

OnCommand Insight では、NetApp SolidFire データソースから次のインベントリ情報を取得します。Insight で取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ドライブ	ディスク
クラスタ	ストレージ
ノード	ストレージノード
ボリューム	ボリューム
Fibre Channel Port（ファイバチャネルポート）	ポート
ボリュームアクセスグループ、 LUN の割り当て	ボリュームマップ

iSCSI セッション	ボリュームマスク

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

このデータソースの設定に関する要件は次のとおりです。

- 管理仮想 IP アドレス
- ポート 443

設定

フィールド	説明
管理仮想 IP アドレス（ MVIP ）	SolidFire クラスタの管理仮想 IP アドレス
ユーザ名	SolidFire クラスタへのログインに使用するユーザ名
パスワード	SolidFire クラスタへのログインに使用するパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
TCP ポート	SolidFire サーバへの接続に使用するTCPポート（デフォルトは443）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

トラブルシューティング

SolidFire からエラーが報告されると、次のようにOnCommand Insight に表示されます。

```
An error message was received from a SolidFire device while trying to retrieve
data. The call was <method> (<parameterString> ). The error message from the
device was (check the device manual): <message>
```

ここで、

- method> は、 GET や PUT などの HTTP メソッドです。
- parameterString> は、 REST 呼び出しに含まれていたパラメータをカンマで区切ったリストです。
- <message> は、エラーメッセージとして返されたデバイスです。

NetApp StorageGRID データソース

このデータソースは、StorageGRID のインベントリとパフォーマンスのデータを収集します。

要件

このデータソースの設定に関する要件は次のとおりです。

- StorageGRID ホストの IP アドレス
- Metric Query ロールとテナントアクセスロールが割り当てられているユーザのユーザ名とパスワード
- ポート 443

設定

フィールド	説明
StorageGRID ホストIPアドレス（MVIP）	StorageGRID のホストIPアドレス
ユーザ名	StorageGRID へのログインに使用する名前
パスワード	StorageGRID へのログインに使用するパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは900秒）

OpenStackデータソース

OpenStack（REST API / KVM）データソースは、OpenStackハードウェアインスタンスに関する情報を収集します。このデータソースは、すべてのOpenStackインスタンスのインベントリデータと、オプションでVMのパフォーマンスデータを収集します。

要件

OpenStackデータソースを設定するための要件を次に示します。

- OpenStack コントローラの IP アドレス
- OpenStack管理者ロールのクレデンシャルとLinux KVMハイパーバイザーへのsudoアクセスを推奨します。

> adminアカウントまたはadminと同等の権限を使用していない場合でも、データソースからデータを取得できます。管理者以外のロールを持つユーザがAPIを呼び出すことができるように、ポリシー構成ファイル（etc/nova/policy.jsonなど）を変更する必要があります。

  - "os_compute_api：os-availability-zone：detail"："""
  - "os_compute_api：os-hypervisors"："""
  - os_compute_api：servers：detail：get_all_tenants "："""
- パフォーマンスを収集するには、OpenStack Ceilometerモジュールをインストールして設定する必要があります。Ceilometerの設定は、を編集して行います `nova.conf` ファイルをハイパーバイザーごとに作成し、各ハイパーバイザーでNova Computeサービスを再起動します。オプション名は、 OpenStack の各リリースで変更されています。
  - Icehouse のあるホテル
  - Juno 社
  - キロ
  - リバティー
  - 三鷹
  - ニュートン
  - 八幡市
- CPU統計の場合、コンピュートノードの/etc/Nova/Nova.conf で「compute_monitors=ComputeDriverCPUMonitor」をオンにする必要があります。
- ポート要件
  - HTTP は 5000 、 Keystone サービスは 13000 、 HTTPS は 13000 です
  - KVM SSH の場合は 22
  - Nova Compute Service の場合は 8774
  - Cinder ブロックサービスの場合は 8776
  - Ceilometer パフォーマンスサービス用 8777
  - Glance Image Serviceの場合は9292

> ポートは特定のサービスにバインドされ、大規模な環境ではコントローラまたは別のホストでサービスを実行できます。

設定

* フィールド *	* 概要 *

OpenStack Controller の IP アドレス	OpenStack Controller の IP アドレスまたは完全修飾ドメイン名
OpenStack 管理者	OpenStack 管理者のユーザ名
OpenStack パスワード	OpenStack 管理に使用するパスワード
OpenStack 管理者のテナント	OpenStack 管理者のテナント
KVM sudo ユーザー	KVM Sudo ユーザー名
クレデンシャルタイプを指定するには、「 Password 」または「 OpenSSH Key File 」を選択してください	SSH経由でデバイスに接続するために使用するクレデンシャルタイプ
Inventory Private Key への完全パス	Inventory Private Key への完全パス
KVM sudo パスワード	KVM sudo パスワード

高度な設定

* フィールド *	* 概要 *
SSH を使用してハイパーバイザーのインベントリ検出を有効にし	SSH を使用してハイパーバイザーインベントリの検出を有効にする場合は、このチェックボックス
OpenStack 管理 URL のポート	OpenStack 管理 URL のポート
HTTPS を使用する	セキュア HTTP を使用する場合に選択します
HTTP 接続タイムアウト（秒）	HTTP接続のタイムアウト（デフォルトは300秒）
SSH ポート	SSH に使用するポート
SSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは30秒）
SSH プロセスの再試行回数	インベントリの再試行回数
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）

Oracle ZFSデータソース

Oracle ZFSデータソースで、インベントリとパフォーマンスの収集がサポートされるようになりました。

用語集

OnCommand Insight では、このデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク（SDD）	ディスク
クラスタ	ストレージ
コントローラ	ストレージノード
LUN	ボリューム
LUN マップ	ボリュームマップ
イニシエータ、ターゲット	ボリュームマスク
共有	内部ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

このデータソースの設定に関する要件は次のとおりです。

- ZFS Controller-1 および ZFS Controller-2 のホスト名
- 管理者のユーザ名とクレデンシャル
- ポート要件： 215 HTTP/HTTPS

設定

ZFS Controller-1 ホスト名	ストレージコントローラ 1 のホスト名
ZFS Controller-2 ホスト名	ストレージコントローラ 2 のホスト名
ユーザ名	ストレージシステム管理者ユーザアカウントのユーザ名
パスワード	管理者ユーザアカウントのパスワード

高度な設定

フィールド	説明
TCP ポート	ZFSへの接続に使用するTCPポート（デフォルトは215）
接続タイプ	HTTPまたはHTTPS
インベントリのポーリング間隔	インベントリのポーリング間隔（デフォルトは60分）
接続タイムアウト	デフォルトは60秒です
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

トラブルシューティング

このデータコレクタで問題が発生した場合の対処方法を次に示します。

問題	次の操作を実行します
" 無効なログイン資格情報 "	ZFS ユーザーアカウントとパスワードを検証します
「Configuration error」と「Rest Service is disabled」というエラーメッセージが表示されます。	このデバイスで REST サービスが有効になっていることを確認します。
「Configuration error」と表示され、「User unauthorized for command」というエラーメッセージが表示されます。	特定のロール（「advanced_analytics」など）が設定されているユーザ<userName> に含まれていない可能性があります。考えられる解決策 ： • 読み取り専用ロールを持つユーザー${user} のAnalytics（統計）スコープを修正します。-[構成]→[ユーザー]画面で、ロールの上にマウスを置き、ダブルクリックして編集を許可します • [Scope]ドロップダウンメニューから[Analytics]を選択します。使用可能なプロパティのリストが表示されます。 • 一番上のチェックボックスをクリックすると、3つのプロパティがすべて選択されます。-右側の[追加]ボタンをクリックします。 • ポップアップウィンドウの右上にある[適用]ボタンをクリックします。ポップアップウィンドウが閉じます。

Pure Storage FlashArrayデータソース

Pure Storage FlashArray（HTTP）データソースは、Pure Storage Flash Arrayから情報を収集するために使用します。Insightでは、インベントリとパフォーマンスの両方の収集がサポートされます。

用語集

OnCommand Insight では、Pure Storage FlashArrayデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ドライブ（ SSD ）	ディスク
配列	ストレージ
コントローラ	ストレージノード
ボリューム	ボリューム
ポート	ポート
LUNマップ（ホスト、ホストグループ、ターゲットポート）	ボリュームマップ、ボリュームマスク

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ストレージシステムの IP アドレス
- Pure ストレージシステムの Administrator アカウントのユーザ名とパスワード。
- ポート要件： HTTP / HTTPS / 443

設定

* フィールド *	* 概要 *
FlashArrayホスト	FlashArray管理サーバのIIPアドレスまたは完全修飾ドメイン名
ユーザ名	FlashArray管理サーバのユーザ名
パスワード	FlashArray管理サーバのパスワード

高度な設定

* フィールド *	* 概要 *
接続タイプ	管理サーバ
TCP ポート	FlashArrayサーバへの接続に使用するTCPポート（デフォルトは443）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
パフォーマンスポーリング間隔（秒）	パフォーマンスポーリングの間隔（デフォルトは300秒）

QLogic FC Switchデータソース

QLogic FC Switch（SNMP）データソースを設定するには、FCスイッチデバイスのネットワークアドレス（IPアドレスとして指定）、およびデバイスへのアクセスに使用するsnmp_read-only_community stringが必要です。

設定

* フィールド *	* 概要 *
SANsurferスイッチ	SANSurferスイッチのIPアドレスまたは完全修飾ドメイン名
SNMP バージョン	SNMP バージョン
SNMPコミュニティ	SNMP コミュニティストリング
ユーザ名	SANSurferスイッチのユーザ名
パスワード	SANSurferスイッチのパスワード

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは15分）
SNMP 認証プロトコル	SNMP 認証プロトコル（ SNMPv3 のみ）

SNMP 再試行回数	SNMP の再試行回数
SNMP タイムアウト（ミリ秒）	SNMP タイムアウト（デフォルトは 5 、 000 ミリ秒 ）
トラッピングを有効にします	トラップを有効にする場合に選択します
トラップ間の最小時間（秒）	トラップでデータ収集を試行する最小間隔（デフォルトは 10 秒）
ファブリック名	データソースでレポートするファブリック名。ファブリック名を WWN としてレポートする場合は、空白のままにします。
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

Red Hat（RHEV）データソース

Red Hat Enterprise Virtualization（REST）データソースは、HTTPS経由でRHEVインスタンスに関する情報を収集します。

要件

- REST API を使用した RHEV サーバのポート 443 経由の IP アドレス
- 読み取り専用のユーザ名とパスワード
- RHEV バージョン 3.0+

設定

フィールド	説明
RHEV サーバの IP アドレス	RHEVサーバのIPアドレスまたは完全修飾ドメイン名
ユーザ名	RHEVサーバのユーザ名
パスワード	RHEVサーバのパスワード

高度な設定

フィールド	説明
HTTPS 通信ポート	RHEV への HTTPS 通信に使用するポート

インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）

Violin Flash Memory Arrayデータソース

Violin 6000-Series Flash Memory Array（HTTP）データソースは、Violin 6000シリーズフラッシュメモリアレイから分析と検証に使用するネットワーク情報を収集します。

用語集

このデータコレクタは、OnCommand Insight 7.3.11以降では使用できなくなりました。

OnCommand Insight では、Violin 6000-Series Flash Memory Arrayデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
Violin Intelligent Memory Module（VIMM）	ディスク
コンテナ	ストレージ
Memory Gatewayの略	ストレージノード
LUN	ボリューム
イニシエータ、イニシエータグループ、ターゲット	ボリュームマップ、ボリュームマスク

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ストレージに対する読み取り専用のユーザ名とパスワードが必要です。
- ストレージIPアドレスを使用してWebブラウザでアクセスを検証します。

設定

フィールド	説明
Violin Memory Array Main GatewayのIPアドレスまたはFQDN	Violin Memory Array Main GatewayのIPアドレスまたは完全修飾ドメイン名

ユーザ名	Violin Memory Array Main Gatewayのユーザ名
パスワード	Violin Memory Array Main Gatewayのパスワード

高度な設定

フィールド	説明
通信ポート	Violinアレイとの通信に使用するポート
HTTPSが有効です	HTTPSを使用する場合に選択します
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

VMware vSphereデータソース

VMware vSphere（Web Services）データソースはESXホスト情報を収集し、Virtual Center内のすべてのオブジェクトに対して_read-only_privilegesを必要とします。

用語集

OnCommand Insight では、VMware vSphereデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
仮想ディスク	ディスク
ホスト	ホスト
仮想マシン	仮想マシン
データストア	データストア
LUN	LUN
ファイバチャネルポート	ポート

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- Virtual Center サーバの IP アドレス
- Virtual Center の読み取り専用のユーザ名とパスワード
- Virtual Center内のすべてのオブジェクトに対する読み取り専用権限。
- Virtual Centerサーバ上のSDKアクセス
- ポート要件： http - 80 https-443
- ユーザ名とパスワードを使用してVirtual Center Clientにログインし、と入力してSDKが有効になっていることを確認して、アクセスを検証します `telnet <vc_ip\> 443`。

設定

* フィールド *	
* 概要 *	
Virtual Center Addressの略	
Virtual CenterまたはvSphereサーバのネットワークアドレス。IP_（nnn.nnn.nnn.nnn_format）アドレス、またはDNSで解決できるホスト名で指定します。	
ユーザ名	
VMwareサーバのユーザ名。	
パスワード	
VMwareサーバのパスワード。	

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
接続タイムアウト（ミリ秒）	接続タイムアウト（デフォルトは60000ミリ秒）
で VM をフィルタリングします	VMをフィルタする方法を選択します
「除外」または「含める」を選択してリストを指定します	以下のリストにあるVMをデータの収集時に対象に含めるか除外するかを指定します

フィルタするVMのリスト（カンマ区切り、値にカンマを使用する場合はセミコロン区切り）	ポーリングの対象または対象から除外するVMをカンマまたはセミコロンで区切ったリスト
vCenterへの要求の再試行回数	vCenter要求の再試行回数
通信ポート	VMwareサーバに使用するポート
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

データソースのクレデンシャルの変更

同じタイプの複数のデータソースがユーザ名とパスワードを共有している場合は、グループ内のすべてのデバイスのパスワードを同時に変更できます。

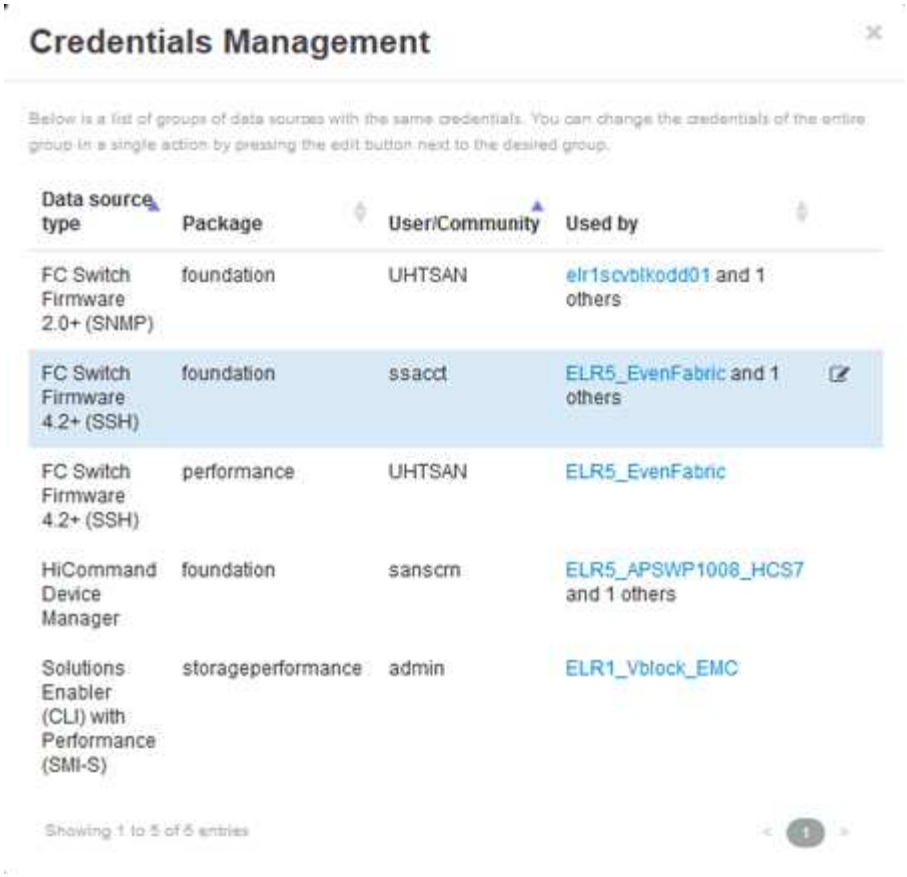
手順

1. Insightのツールバーで、*[Admin]*をクリックします。

   [データソース]*リストが開きます。

2. ボタンをクリックし、[クレデンシャルの変更]*オプションを選択します。
3. [Credentials Management]ダイアログボックスで、リストからいずれかのデータソースグループを選択します。

   右側の編集アイコン（紙の上のペン）がアクティブになります。



4. [編集（ Edit ）] をクリックします。
5. 新しいパスワードを入力し、確認のためにもう一度入力します。

データ収集の問題を引き起こす変更

OnCommand Insight でデータ収集の問題が発生している場合は、環境内での変更が原因である可能性があります。一般的なメンテナンスルールとして、Insightでの環境の変更にも対応する必要があります。

次のチェックリストを使用して、問題の原因となる可能性のあるネットワークの変更を特定できます。

- パスワードを変更しましたか？これらのパスワードはInsightで変更されましたか？
- ネットワークからデバイスを削除しましたか？また、デバイスが再検出されて再導入されないように、OnCommand Insight からデバイスを削除する必要があります。
- インフラストラクチャソフトウェア（HP CommandView EVAやEMC Solutions Enablerなど）をアップグレードしましたか。

  Acquisition Unitに適切なバージョンのクライアントツールがインストールされていることを確認します。データソースで問題が解決しない場合は、テクニカルサポートに連絡してサポートやデータソースパッチの入手を依頼する必要があります。

- すべてのOnCommand Insight Acquisition Unitで同じバージョンのOnCommand Insight が使用されていますか？Remote Acquisition UnitとLocal Acquisition Unitで異なるバージョンのOnCommand Insight が実行されている場合は、データ収集の問題を解決するために、すべてのユニットに同じバージョンをインストールしてください。

すべてのAcquisition Unitに新しいバージョンのOnCommand Insight をインストールする必要がある場合は、サポートサイトにアクセスして正しいバージョンをダウンロードしてください。

- ドメイン名を変更したか、新しいドメインを追加しましたか。デバイス解決（以前の自動解決）方法を更新する必要があります。

1つのデータソースの詳細を確認します

データソースで障害や処理速度の低下が発生した場合は、そのデータソースの詳細な情報を確認して、問題の原因 を特定できます。注意が必要な状態のデータソースは赤い丸で示されます。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。

   [データソース]*リストが開きます。問題がある可能性があるデータソースは、赤い丸で示されます。最も深刻な問題はリストの一番上にあります。

2. 問題の原因となっているデータソースを選択します。
3. データソース名のリンクをクリックします。
4. データソースの概要ページで、次のいずれかのセクションの情報を確認します。
   - イベントタイムライン

     [データソース]リストに表示されている現在のステータスに関連するイベントを一覧表示します。このサマリーのイベントは、デバイスごとに表示されます。エラーは赤で表示されます。タイムラインアイテム上にマウスポインタを置くと、追加情報 が表示されます。

   - このデータソースによって報告されたデバイス

     に、デバイスのタイプ、IPアドレス、および各デバイスの詳細情報へのリンクを示します。

   - このデータソースによって報告された変更（過去3週間）

     追加または削除されたデバイス、または設定に変更があったデバイスを一覧表示します。

5. データソースの情報を確認したら、ページの上部にあるボタンを使用して次のいずれかの処理を実行できます。
   - *データソースの概要 を編集して問題を修正します。
   - *再度ポーリング*は、問題が持続的であるか断続的であるかを明らかにするためにポーリングを強制します。
   - *データソースのポーリングを3、7、または30日間延期して、問題を調査して警告メッセージを停止します。
   - *データソースにパッチ*をインストールして、問題を修正します。
   - テクニカルサポート用の*エラーレポート*を準備します。
   - * Insight監視環境からデータソースを削除*します。

データソースの問題を調査しています

データソースに「* Inventory failed！」または「 Performance failed！*」というメッセージが表示され、[Impact]が[High]または[Medium]になっている場合は、データソースの概要ページにリンクされた情報を使用してこの問題を調査する必要があり

手順

1. データソースのリンクされた* Name *をクリックして、Summaryページを開きます。
2. [Summary]ページで[* Comments]領域を確認し、この問題を調査している可能性のある別のエンジニアが残したメモを確認します。
3. パフォーマンスのメッセージを確認します。
4. このデータソースに適用されているパッチがある場合は、リンクをクリックして*パッチページ*を確認し、それが問題の原因であるかどうかを確認します。
5. 追加情報 を表示するには、*イベントタイムライン*グラフのセグメントの上にマウスポインタを移動します。
6. イベントタイムラインの下に表示されるデバイスのエラーメッセージを選択し、メッセージの右側に表示される*エラーの詳細*アイコンをクリックします。

   エラーの詳細には、エラーメッセージのテキスト、考えられる原因、使用中の情報、問題を修正するために試すことができる推奨事項が含まれています。

7. [Devices reported by this data source]領域で、リストをフィルタして目的のデバイスのみを表示できます。また、デバイスのリンクされた* Name *をクリックすると、そのデバイスの_asset page_が表示されます。
8. 以前に表示したページに戻るには、次のいずれかの方法を使用します。
   - ブラウザの戻る矢印をクリックします。
   - 戻る矢印を右クリックしてページのリストを表示し、目的のページを選択します。
9. 他のリソースに関する詳細情報を表示するには、[その他のリンクされた名前]をクリックします。
10. データソースの概要ページに戻ったら、ページ下部の*変更*領域で、最近の変更が問題の原因になっていないかどうかを確認します。

データソースのポーリングの制御

データソースに変更を加えたあと、すぐにポーリングして変更を確認したり、問題の処理中にデータソースのデータ収集を1日、3日、5日間延期したりできます。

手順

1. [Admin]*をクリックし、データソースのリストビューに移動します
2. ポーリングを制御するデータソースを選択します。
3. データソース名のリンクをクリックします。
4. データソースの概要ページで、情報を確認し、次の2つのポーリングオプションのいずれかをクリックします。

- *もう一度ポーリング*を実行すると、データソースにすぐにデータが収集されます。
- *延期*し、ポーリング遅延の長さを3日、7日、または30日から選択します。

完了後

データソースでデータ収集を延期した場合に収集を再開するには、概要ページで*[再開]*をクリックします。

データソース情報の編集

データソースの設定情報は簡単に編集できます。

手順

1. [Admin]*をクリックし、データソースのリストビューに移動します
2. 編集するデータソースを探します。
3. 変更を開始するには、次のいずれかの方法を使用します。
   - 選択したデータソースの右側にある*[データソースの編集]*をクリックします。
   - 選択したデータソースのリンク名をクリックし、*[編集]*をクリックします。どちらの方法でも、[Edit data source]ダイアログボックスが開きます。
4. 必要な変更を行い、*[保存]*をクリックします。

複数のデータソースの情報を編集する

同じベンダーおよびモデルの複数のデータソースについて、ほとんどの情報を一度に編集できます。たとえば、これらのデータソースでユーザ名とパスワードが共有されている場合は、一箇所でパスワードを変更して、選択したすべてのデータソースのパスワードを更新できます。

このタスクについて

選択したデータソースについて編集できないオプションは、[データソースの編集]ダイアログボックスでグレー表示または非表示になります。また、オプションの値が「* Mixed 」と表示されている場合は、選択したデータソース間でオプションの値が異なることを示します。たとえば、選択した**2**つのデータソースの Timeout (sec)オプションが Mixed *の場合、一方のデータソースのタイムアウト値は60、もう一方のデータソースの値は90になります。 したがって、この値を120に変更してデータソースへの変更を保存すると、両方のデータソースのタイムアウト設定が120になります。

手順

1. [Admin]*をクリックし、データソースのリストビューに移動します
2. 変更するデータソースを選択します。同じベンダー、モデル、Acquisition Unitに属しているデータソースを選択する必要があります。
3. ボタンをクリックし、[編集]*オプションを選択します。
4. 編集ダイアログで、必要に応じて*設定*を変更します。
5. [Configuration]*リンクをクリックして、データソースの基本オプションを変更します。

6. [Advanced Configuration]*リンクをクリックして、データソースの詳細オプションを変更します。
7. [保存（ Save ）] をクリックします。

データソースタグをアノテーションにマッピングする

タグデータをポーリングするようにデータソースを設定すると、Insightでは、既存のInsightアノテーションのアノテーション値がタグと同じ名前で自動的に設定されます。

データソースでタグを有効にする前にInsightのアノテーションが存在していた場合は、データソースタグのデータが自動的にInsightのアノテーションに追加されます。

タグを有効にしたあとにアノテーションを作成した場合、データソースの初回のポーリングでアノテーションが自動的に更新されません。Insightのアノテーションの置き換えやデータの入力には時間がかかります。この遅延を回避するには、データソースを延期して再開することで、タグのアノテーションの更新を強制的に実行します。

データソースの削除

環境からデータソースを削除した場合は、OnCommand Insight 監視環境からも削除する必要があります。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。

   [Data sources]リストが開きます。

2. 削除するデータソースを選択します。
3. リンクされたデータソース名をクリックします。
4. 選択したデータソースの情報を概要ページで確認し、そのデータソースが削除対象であることを確認します。
5. [削除（ Delete ）] をクリックします。
6. [OK]*をクリックして操作を確定します。

データソースパッチとは

データソースパッチを適用すると、既存のパッチの問題が修正され、新しいタイプのデータソース（ベンダーやモデル）を簡単に追加できます。データソースパッチは、ネットワーク内のデータソースタイプごとにアップロードできます。パッチ適用プロセスをインストール、テスト、および管理することもできます。ただし、1つのデータソースタイプに対して一度にアクティブにできるパッチは1つだけです。

パッチごとに、次のタスクを実行できます。

- パッチを受信する各データソースの前後の比較を確認します。

- 決定を説明したり、調査を要約したりするためのコメントを書いてください。
- パッチに適切に対応していないデータソースに変更を加えます。
- Insightサーバへのパッチのコミットを承認します。
- 意図したとおりに動作しないパッチをロールバックします。
- 問題のあるパッチを別のパッチに交換します。

データソースパッチの適用

定期的に提供されるデータソースパッチを使用して、既存のデータソースの問題を修正したり、新しいベンダーのデータソースを追加したり、ベンダーの新しいモデルを追加したりできます。

作業を開始する前に

を入手しておく必要があります `.zip` 最新のデータソースを含むファイル `.patch` テクニカルサポートから入手したファイル。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [パッチ]*をクリックします。
3. [Actions]ボタンから、*[Apply patch]*を選択します。
4. ダイアログボックスで、[参照]*をクリックしてを指定します `.patch` ファイル。
5. 、**[概要]**、[影響を受けるデータソースの種類]*を確認します。
6. 選択したパッチが正しい場合は、*パッチの適用*をクリックします。

   データソースの問題を修正するパッチを適用する場合は、同じタイプのすべてのデータソースがパッチで更新されるため、パッチを承認する必要があります。設定済みのデータソースに影響しないパッチは自動的に承認されます。

完了後

新しいベンダーまたは新しいモデルのデータソースを追加するパッチを適用する場合は、パッチの適用後にデータソースを追加する必要があります。

あるタイプのデータソースにパッチをインストールする

データソースパッチをアップロードしたら、同じタイプのすべてのデータソースにインストールできます。

作業を開始する前に

いずれかのタイプのデータソースにインストールするパッチファイルをアップロードしておく必要があります。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [パッチ]*をクリックします。
3. [Actions]ボタンから、*[Apply patch]*を選択します。
4. ダイアログボックスで、[Browse]*をクリックして、アップロードしたパッチファイルを指定します。
5. 、**[概要]**、[影響を受けるデータソースタイプ]*を確認します。
6. 選択したパッチが正しい場合は、*パッチの適用*をクリックします。

   同じタイプのすべてのデータソースがこのパッチで更新されます。

パッチの管理

ネットワークに適用されているすべてのデータソースパッチの現在のステータスを確認できます。パッチに対してアクションを実行する場合は、現在レビュー中のパッチ（Patches Currently Under Review）テーブルでリンクされた名前をクリックします。

作業を開始する前に

少なくとも1つのパッチをアップロードしてインストールしておく必要があります。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [パッチ]*をクリックします。

   パッチがインストールされていない場合、現在レビュー中のパッチの表は空です。

3. [Patches currently under review]*で、現在適用されているデータソースパッチのステータスを確認します。
4. 特定のパッチに関連付けられている詳細を確認するには、パッチのリンク名をクリックします。
5. 選択したパッチについて、次のいずれかのオプションをクリックしてパッチに対して次の操作を実行できます。
   - *パッチを承認*パッチをデータソースにコミットします。
   - *ロールバック*パッチを削除します。
   - *パッチの置き換え*を使用すると、これらのデータソースに別のパッチを選択できます。

データソースパッチをコミットしています

Patches Summaryの情報を使用して、パッチが想定どおりに機能しているかどうかを判断し、パッチをネットワークにコミットします。

作業を開始する前に

パッチがインストールされている場合は、パッチが正常にインストールされ、承認が必要かどうかを判断する

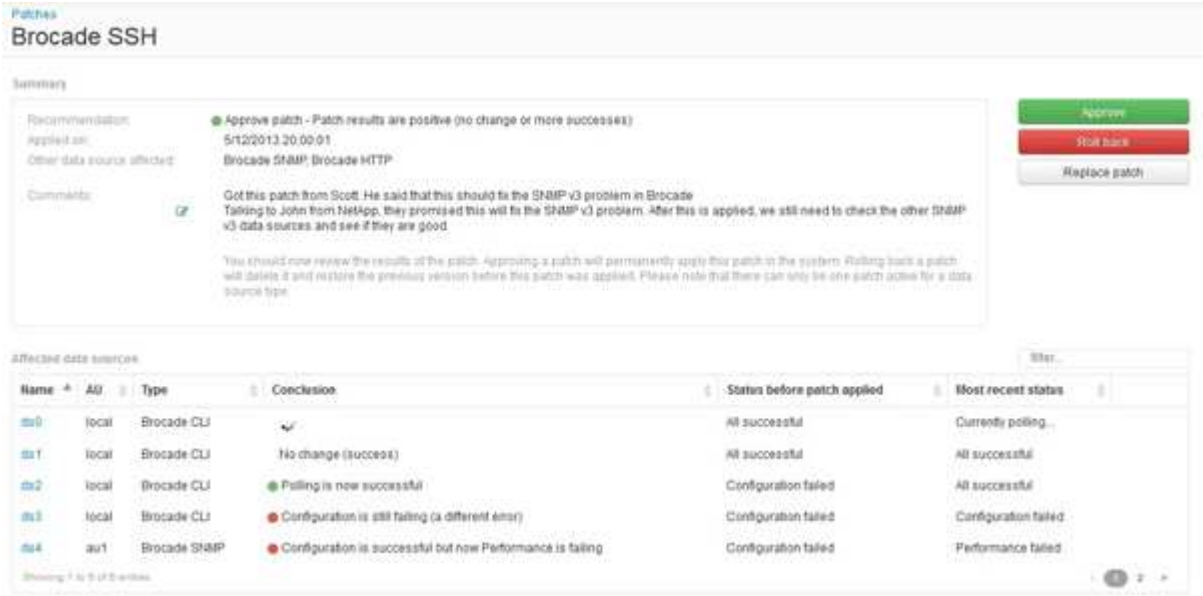
必要があります。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [パッチ]*をクリックします。

   パッチがインストールされていない場合、現在レビュー中のパッチは空です。

3. [Patches currently under review]*で、現在適用されているデータソースパッチのステータスを確認します。
4. 特定のパッチに関連付けられている詳細を確認するには、パッチのリンク名をクリックします。
5. この例に示されているパッチの概要情報で、*推奨事項*および*コメント*を確認して、パッチの進行状況を評価します。



6. 「* Data sources affected *」の表を参照して、パッチ適用前後の影響を受ける各データソースのステータスを確認します。

   パッチを適用するデータソースの1つに問題があることが懸念される場合は、[Data sources Affected]テーブルで[Linked Name]をクリックします。

7. そのタイプのデータソースにパッチを適用する必要があると判断した場合は、*[承認]*をクリックします。

   データソースが変更され、パッチが現在レビュー中のパッチから削除されます。

データソースパッチをロールバックします

データソースパッチが想定どおりに機能しない場合は、ロールバックできます。ロールバックするとパッチは削除され、パッチが適用される前のバージョンに戻ります。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。

2. [パッチ]*をクリックします。
3. [現在レビュー中のパッチ]*で、失敗したと思われるパッチのリンク名をクリックします。
4. データソースの[Patches]ページで、次の情報を確認します。
   - *概要*パッチがいつ適用されたか、影響を受けるデータソース、およびパッチに関するあなたまたはチームの他のメンバーからのコメントが記載されています。
   - *影響を受けるデータソース*には、パッチが適用されているすべてのデータソースが一覧表示され、パッチ適用前とパッチ適用後のステータスの比較が含まれます。
5. パッチの処理に失敗したデータソースの詳細を表示するには、リンクされた*[名前]*をクリックします。
   a. 概要情報を確認します。
   b. [イベントタイムライン]*で、このデータソースに影響している可能性がある設定データやパフォーマンスデータを確認します。
6. パッチが正常に終了しないと判断した場合は、ブラウザの戻る矢印をクリックしてパッチの概要ページに戻ります。
7. [ロールバック]*をクリックしてパッチを削除します。

   正常に動作する可能性が高い別のパッチがわかっている場合は、*[パッチの置き換え]*をクリックして新しいパッチをアップロードします。

デバイス解決

OnCommand Insight で監視するすべてのデバイスを検出する必要があります。環境内のパフォーマンスとインベントリを正確に追跡するには、検出が必要です。通常、環境内のほとんどのデバイスは自動デバイス解決によって検出されます。

> アップグレードを実行する際に、アップグレード元のシステムに非アクティブの自動解決ルールがあると、それらのルールはアップグレード時に削除されます。アクティブでない自動解決ルールを保持するには、アップグレードの実行前にルールをアクティブ化（チェックボックスをオンに）します。

データソースをインストールして設定すると、環境内のデバイス（スイッチ、ストレージアレイ、ハイパーバイザーとVMの仮想インフラなど）が識別されます。ただし、通常は環境内のすべてのデバイスが識別されるわけではありません。

データソースタイプのデバイスを設定したら、デバイス解決ルールを利用して環境内の残りの不明なデバイスを特定することを推奨します。デバイス解決は、次のデバイスタイプとして不明なデバイスの解決に役立ちます。

- 物理ホスト
- ストレージアレイ
- テープだ
- スイッチ

デバイス解決後に「不明」と表示されたままのデバイスは汎用デバイスとみなされ、クエリやダッシュボードにも表示できます。

似た属性の新しいデバイスが以降に環境に追加されると、作成したルールに基づいて自動的に識別されます。場合によっては、Insightで検出されないデバイスに対するデバイス解決ルールをバイパスして、手動で識別することもできます。

デバイスの識別が完了していないと、次のような問題が発生する可能性

- 不完全なパスです
- マルチパス接続が識別されない
- アプリケーションをグループ化できない
- 正確なトポロジが表示されない
- Data Warehouse や Reporting で正確なデータが表示されない

デバイス解決機能（* Manage > Device resolution *）には、次のタブがあります。各タブは、デバイス解決の計画と結果の表示に役割を果たします。

- 「FC Identify」には、自動デバイス解決で解決されなかったファイバチャネルデバイスのWWNとポート情報のリストが表示されます。識別されたデバイスの割合も表示されます。
- 「IP identify」には、自動デバイス解決で識別されなかったCIFS共有およびNFS共有にアクセスするデバイスのリストが含まれます。識別されたデバイスの割合も表示されます。
- 「自動解決ルール」には、ファイバチャネルデバイス解決の実行時に実行されるルールのリストが含まれます。これらのルールは、識別されないファイバチャネルデバイスを解決するために作成します。
- 「環境設定」では、環境に合わせてデバイス解決をカスタマイズするための設定オプションを提供します。

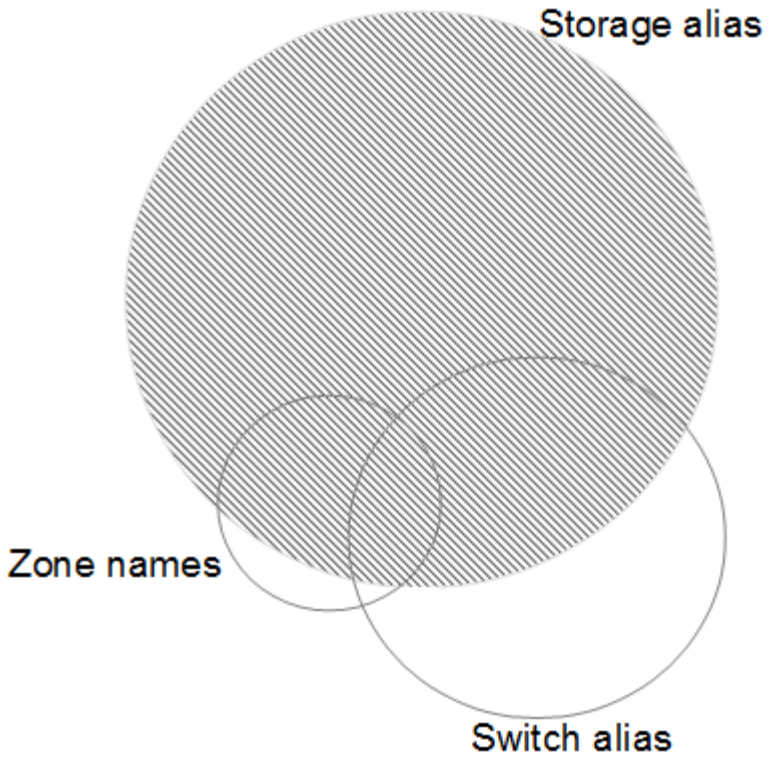
作業を開始する前に

デバイスを識別するルールを定義する前に、環境がどのように設定されているかを理解しておく必要があります。環境についての知識が多いほど、デバイスの識別が容易になります。

正確なルールを作成するには、次のような回答の質問が必要です。

- ゾーンやホストの命名基準がある場合、それらはどの程度正確であるか。
- スイッチエイリアスやストレージエイリアスを使用している場合、それらがホスト名と一致しているかどうか。
- SRMツールを使用していますか？また、SRMツールを使用してホスト名を識別できますか？SRMはどのようなカバレッジを提供しますか。
- 命名規則はどれくらいの頻度で変更されますか？
- 買収や合併によって命名規則が変わっていないかどうか。

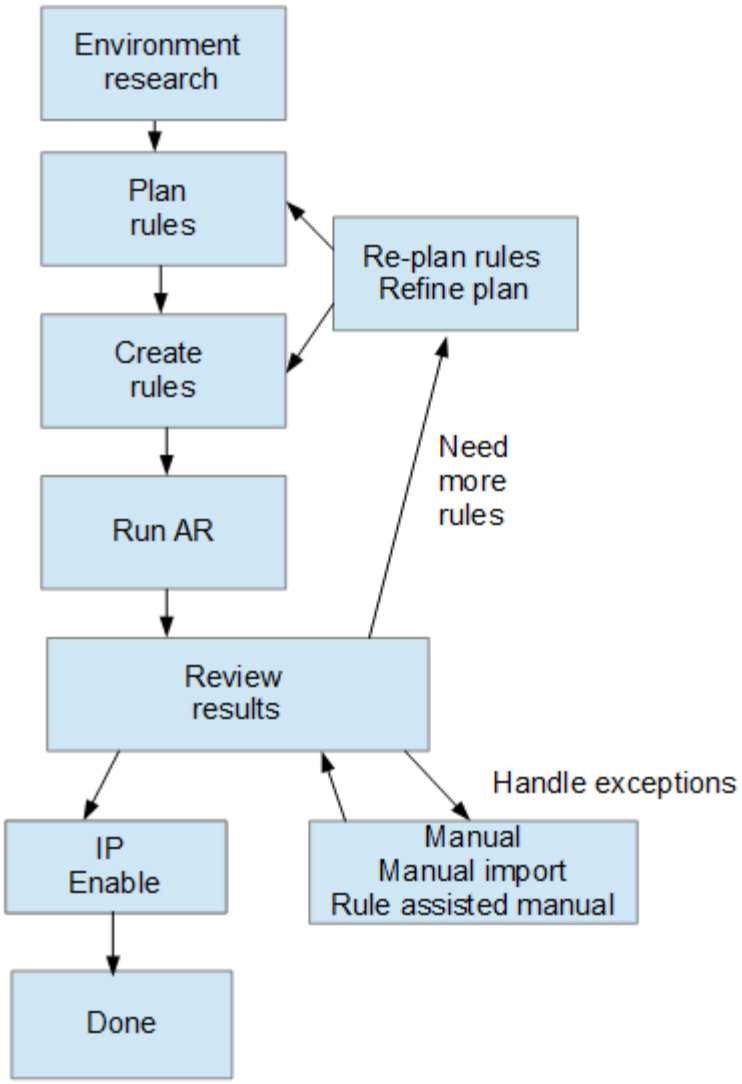
環境を分析することで、どのような命名基準があり、その信頼性がどの程度であるかを特定できるようになります。たとえば、収集した情報から、次の図のような状況であることがわかったとします。



この例では、ストレージエイリアスで最も多くのデバイスを表すことができます。ストレージエイリアスを使用してホストを識別するルールを最初に記述し、次にスイッチエイリアスを使用するルール、最後にゾーンエイリアスを使用するルールを作成します。ゾーンエイリアスやスイッチエイリアスと重なっている部分のデバイスについても、ストレージエイリアスのルールで識別できるため、ゾーンエイリアスやスイッチエイリアスに必要なルールは少なくて済みます。

環境内のデバイスを定義する手順

通常、環境内のデバイスを識別するには、次のようなワークフローを使用します。識別は反復的なプロセスであり、ルールの計画や調整が何度も必要になることがあります。



環境内に未識別のデバイス（「不明」または汎用デバイスとも呼ばれる）があり、ポーリング時にそれらのデバイスを識別するデータソースを設定すると、それらのデバイスは汎用デバイスとして表示またはカウントされなくなります。

環境に応じたデバイス解決ルールの計画

ルールを使用して環境内のデバイスを識別するプロセスは、通常は反復的なプロセスです。環境を徹底的に分析し、できるだけ多くのデバイスを識別するために複数のルールを作成する必要があります。最良のシナリオは、環境内のデバイスの100%を識別する目標を設定することです。

ルールの最も効率的な順序は、最も制限の厳しいルールを最初に配置して、ほとんどのエントリがパターンマッチングを行わないようにすることです。この場合、プロセスはより制限の厳しいルールに進みます。これにより、Insightでは各エントリにより多くのパターンを適用できるようになり、パターンマッチングやホスト識別の可能性が高まります。

ルールを作成する場合は、できるだけ多くの未識別デバイスに対応するルールを作成する必要があります。たとえば、次のようなカバレッジパターンに従うルールを作成すると、カバレッジの割合が低いルールを30個作成するよりもはるかに効率的です。

ルール	カバレッジのパーセンテージ
ルール 1	60%だ
ルール 2	25%
ルール 3	8%です
ルール4	4%です
ルール5	1%です

デバイス解決ルールを作成しています

デバイス解決ルールを作成して、OnCommand Insight で現在自動的に識別されないホスト、ストレージ、およびテープを識別します。作成したルールにより、環境内の既存のデバイスが識別されるほか、環境に追加された同様のデバイスも識別されます。

このタスクについて

ルールを作成するときは、最初に、ルールの実行対象となる情報のソース、情報の抽出に使用する方法、およびルールの結果に DNS ルックアップを適用するかどうかを特定します。

デバイスの識別に使用するソース
• ホストのSRMエイリアス • ホスト名またはテープ名が埋め込まれたストレージエイリアス • ホスト名またはテープ名が埋め込まれたスイッチエイリアス • ホスト名が埋め込まれたゾーン名
ソースからデバイス名を抽出する方法
• そのまま（SRMから名前を抽出） • 区切り文字 • 正規表現
DNS ルックアップ
DNSを使用してホスト名を確認するかどうかを指定します。

ルールは、 ［ 自動解決ルール ］ タブで作成します。以下に、ルールの作成プロセスについて説明します。

手順

1. >[デバイス解決]*をクリックします
2. タブで、+[追加]*をクリックします

   [New Rule]画面が表示されます。

   [New Rule]画面には、正規表現を作成するためのヘルプと例を示す*？*アイコンが表示されます。

3. [* タイプ] リストで、識別するデバイスを選択します。

   [Host]または[Tape]を選択できます。

4. [* ソース *] リストで、ホストの識別に使用するソースを選択します。

   選択したソースに応じて、Insightに次の応答が表示されます。

   - [Zones]には、Insightで識別する必要があるゾーンとWWNのリストが表示されます。
   - [SRM]を選択すると、Insightで識別する必要がある未識別のエイリアスが一覧表示されます
   - [Storage alias]には、Insightで識別する必要があるストレージエイリアスとWWNのリストが表示されます
   - [Switch alias]には、Insightで識別する必要があるスイッチエイリアスのリストが表示されます

5. メソッド * リストで、ホストの識別に使用する方法を選択します。

ソース	メソッド
SRM の場合	「現状のまま」、「デリミッタ」、「正規表現」
ストレージエイリアス	"`delimiters'"、または"`regular expressions'"
スイッチエイリアス	"`delimiters'"、または"`regular expressions'"
ゾーン	"`delimiters'"、または"`regular expressions'"

   - 「デリミッタ」を使用するルールでは、デリミタとホスト名の最小長が必要です。

     ホスト名の最小文字数は、Insightでホストを識別するために使用する文字数です。Insightでは、これ以上長いホスト名に対してのみDNSルックアップが実行されます。

     delimiters を使用するルールの場合、入力文字列は区切り文字でトークン化され、ホスト名候補のリストは、隣接するトークンを複数組み合わせて作成されます。リストは、最大から最小にソートされます。たとえば、vipsnq03_hba3_emc3_12ep0の場合、リストは次のようになります。

     - vipsnq03_hba3_emc3_12ep0
     - vipsnq03_hba3_emc3
     - hba3 emc3_12ep0

- vipsnq03_hba3.
- emc3_12ep0
- hba3_emc3
- vipsnq03
- 12ep0
- emcs3
- hba3.

◦ 「正規表現」を使用するルールでは、正規表現、形式、および大文字と小文字の区別を選択する必要があります。

6. をクリックします

すべてのルールを実行するには、ボタンの下矢印をクリックして、作成したルール（およびARの最後のフルラン以降に作成されたその他のルール）を実行します。

結果

ルールの実行結果は[FC Identify]タブに表示されます。

自動デバイス解決の更新を開始しています

デバイス解決の更新では、前回の完全な自動デバイス解決の実行後に手動で行った変更がコミットされます。更新を実行すると、デバイス解決設定に対する新しい手動のエントリのみをコミットして実行できます。完全なデバイス解決は実行されません。

手順

1. Insight Web UIにログインします。
2. >[デバイス解決]*をクリックします
3. [デバイスの解像度]画面で、[ARの実行]ボタンの下矢印をクリックします。
4. アップデートを開始するには、 * アップデート * をクリックします。

ルールに基づく手動識別

この機能は、不明なホスト、ストレージ、テープデバイス、またはそれらのグループを解決するために特定のルールまたはルールのリスト（1回限りの順序変更の有無に関係なく）を実行する特殊なケースで使用されます。

作業を開始する前に

識別されていないデバイスが多数あり、他のデバイスを正しく識別した複数のルールがある場合。

このタスクについて

ソースにホスト名またはデバイス名の一部だけが含まれている場合は、正規表現のルールを使用して欠落しているテキストを追加するように形式を変更します。

手順

1. OnCommand Insight Web UIにログインします。
2. >[デバイス解決]*をクリックします
3. [FC Identify]*タブをクリックします。

   識別されたデバイスと識別されていないデバイスが表示されます。

4. 識別されていない複数のデバイスを選択
5. >[ホスト解決の設定]または>[テープ解決の設定]*をクリックします

   識別画面が表示され、デバイスを正しく識別したすべてのルールのリストが表示されます。

6. ルールの順序を、ニーズに合った順序に変更します。

   ルールの順序は識別画面で変更されますが、グローバルには変更されません。

7. ニーズに合った方法を選択します。

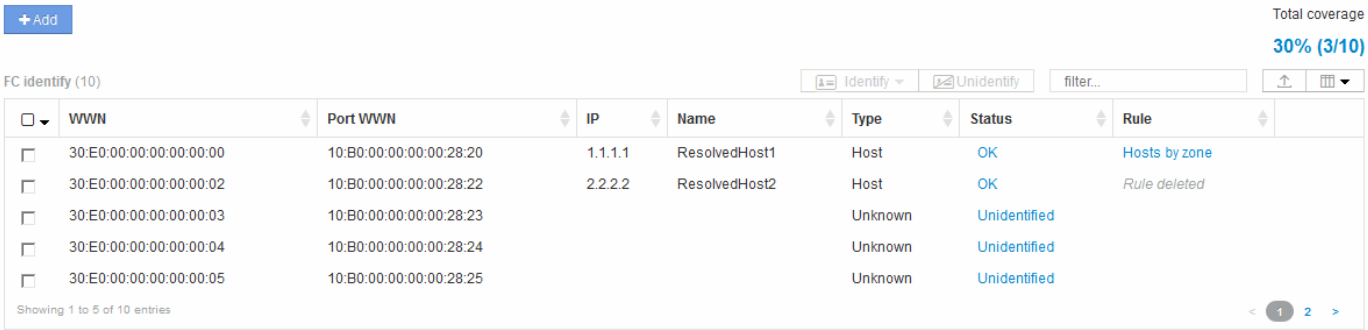
   OnCommand Insight は、一番上のメソッドから順にホスト解決プロセスを実行します。

   適用されるルールが検出されると、ルールの名前がルールの列に表示され、手動で識別されます。

ファイバチャネルデバイスの解決

[FC Identify]画面には、自動デバイス解決でホストが識別されていないFibre ChannelデバイスのWWNとWWPNが表示されます。この画面には、手動デバイス解決で解決されたデバイスも表示されます。

手動解決によって解決されたデバイスには「OK」のステータスが含まれ、デバイスの識別に使用されたルールが示されます。検出されなかったデバイスのステータスは「Unidentified」になります。このページには、デバイスの識別範囲の合計が表示されます。



一括操作を実行するには、[FC Identify]画面の左側で複数のデバイスを選択します。1つのデバイスでアクションを実行するには、デバイスにカーソルを合わせ、リストの右端にある[Identify]または[Unidentify]ボタンを選択します。

[Total coverage]リンクには、構成の「識別されたデバイス数/使用可能なデバイス数」のリストが表示されます。

- SRM エイリアス
- ストレージエイリアス
- スイッチエイリアス
- ゾーン
- ユーザ定義

ファイバチャネルデバイスを手動で追加する

ファイバチャネルデバイスは、[Device resolution FC Identify]タブの手動追加機能を使用してOnCommand Insight に手動で追加できます。このプロセスは、今後検出されることが予想されるデバイスの事前識別に使用される場合があります。

作業を開始する前に

システムにデバイス識別情報を追加するには、 WWN または IP アドレスとデバイス名を確認しておく必要があります。

このタスクについて

ホスト、ストレージ、テープ、または不明なFibre Channelデバイスは手動で追加できます。

手順

1. Insight Web UIにログインします
2. **>**[デバイス解決]*をクリックします
3. [FC Identify]*タブをクリックします。
4. 追加ボタンをクリックします。

   Add Device ダイアログが表示されます

5. WWN または IP アドレスとデバイス名を入力し、デバイスタイプを選択します。

結果

入力したデバイスが[FC Identify]タブのデバイスのリストに追加されます。"`Rule'"はManualとして識別されます。

CSVファイルからのファイバチャネルデバイス識別情報のインポート

CSVファイル内のデバイスのリストを使用して、ファイバチャネルデバイスの識別情報をOnCommand Insight デバイス解決機能に手動でインポートできます。

作業を開始する前に

デバイス識別情報をデバイス解決機能に直接インポートするには、正しくフォーマットされたCSVファイルが必要です。ファイバチャネルデバイスのCSVファイルには、次の情報が必要です。

WWN
IP
名前
を入力します

最初に[FC Identify]の情報をCSVファイルにエクスポートし、そのファイルに必要な変更を加えてから、そのファイルを[FC Identify]にインポートし直すことを推奨します。これにより、必要な列が適切な順序で配置されます。

[FC Identify]の情報をインポートするには

手順

1. Insight Web UIにログインします。
2. **>**[デバイス解決]*をクリックします
3. [FC Identify]*タブを選択します。
4. 識別>*ファイルから識別*をクリックします .
   a. インポートするCSVファイルが格納されているフォルダに移動し、目的のファイルを選択します。

   入力したデバイスが[FC Identify]タブのデバイスのリストに追加されます。「ルール」は「手動」として識別されます。

ファイバチャネルデバイスの識別情報を**CSV**ファイルにエクスポートしています

OnCommand Insight デバイス解決機能から、既存のファイバチャネルデバイスの識別情報をCSVファイルにエクスポートできます。エクスポートしたデバイス識別情報を変更してInsightに再度インポートすると、識別情報がエクスポートされたデバイスと類似したデバイスの識別に使用されます。

このタスクについて

このシナリオは、デバイスに同様の属性があり、CSVファイルで簡単に編集してからシステムにインポートできる場合に使用します。

ファイバチャネルデバイスの識別情報をCSVファイルにエクスポートすると、ファイルには次の情報が記載された順序で格納されます。

WWN
IP

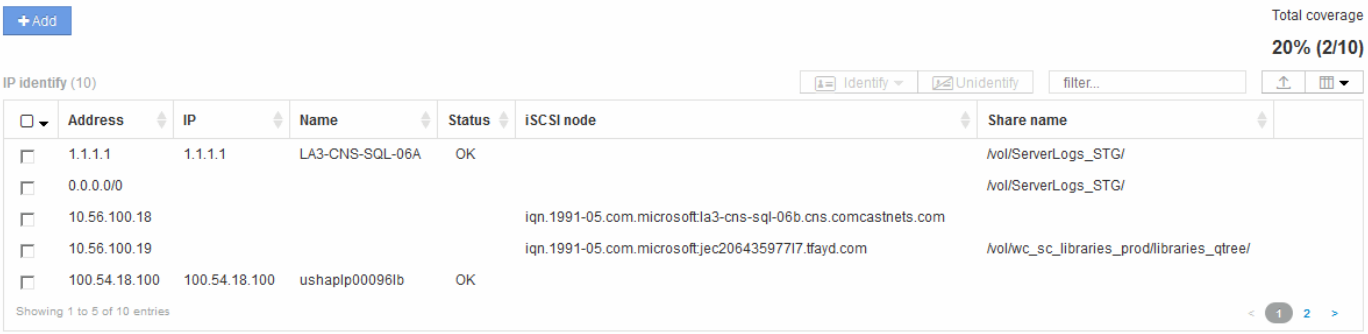
名前
を入力します

手順

1. Insight Web UIにログインします。
2. >[デバイス解決]*をクリックします
3. [FC Identify]*タブを選択します。
4. 識別情報をエクスポートする 1 つ以上のファイバチャネルデバイスを選択します。
5. エクスポートをクリックします をクリックします。
6. CSVファイルを開くか、ファイルを保存するかを選択します。

IP デバイスの解決

IP の識別画面には、自動デバイス解決または手動デバイス解決によって識別された iSCSI 共有と CIFS 共有または NFS 共有が表示されます。また、未識別のデバイスも表示されます。画面には、デバイスの IP アドレス、名前、ステータス、 iSCSI ノード、および共有名が表示されます。識別に成功したデバイスの割合も表示されます。



IP デバイスを手動で追加する

[IP Identify]画面の手動追加機能を使用して、IPデバイスをOnCommand Insight に手動で追加できます。

手順

1. Insight Web UIにログインします。
2. >[デバイス解決]*をクリックします
3. [IP Identify]*タブをクリックします。
4. 追加ボタンをクリックします。

   Add Device ダイアログが表示されます

5. アドレス、 IP アドレス、および一意のデバイス名を入力します。

結果

入力したデバイスが[IP Identify]タブのデバイスのリストに追加されます。

CSVファイルからの**IP**デバイス識別情報のインポート

CSVファイルのデバイス識別情報のリストを使用して、IPデバイス識別情報をデバイス解決機能に手動でインポートできます。

作業を開始する前に

デバイスの識別情報をインポートするには、正しい形式のCSVファイルが必要です。IPデバイスのCSVファイルには、次の情報が必要です。

住所
IP
名前

最初に[IP Identify]の情報をCSVファイルにエクスポートし、そのファイルに必要な変更を加えてから、[IP Identify]にファイルをインポートし直すことを推奨します。これにより、必要な列が適切な順序で配置されます。

IP識別情報をインポートするには：

手順

1. Insight Web UIにログインします。
2. **>**[デバイス解決]*をクリックします
3. [IP Identify]*タブを選択します。
4. 識別>*ファイルから識別*をクリックします .
   a. インポートするCSVファイルが格納されているフォルダに移動し、目的のファイルを選択します。

   入力したデバイスが[IP Identify]タブのデバイスのリストに追加されます。

CSVファイルへの**IP**デバイス識別情報のエクスポート

デバイス解決機能を使用して、Insightから既存のIPデバイス識別情報をエクスポートできます。エクスポートしたデバイス識別情報を変更してInsightに再度インポートして、識別情報をエクスポートしたデバイスと類似したデバイスの識別に使用できるようにすることができます。

このタスクについて

IPデバイスの識別情報をCSVファイルにエクスポートすると、ファイルには次の情報が記載された順序で格納されます。

住所
IP
名前

手順

1. Insight Web UIにログインします。
2. >[デバイス解決]*をクリックします
3. [IP Identify]*タブを選択します。
4. 識別情報をエクスポートする IP デバイスを選択します。
5. エクスポートをクリックします をクリックします。
6. CSVファイルを開くか、ファイルを保存するかを選択します。

[環境設定] タブでオプションを設定します

デバイス解決のプリファレンスタブでは、自動解決スケジュールの作成、識別情報を含めるストレージベンダーやテープベンダーの指定、および DNS 検索オプションの設定を行うことができます。

自動解決スケジュール

自動デバイス解決を実行するスケジュールを指定できます。

オプション	説明
間隔	曜日、時間、または分単位で自動デバイス解決を実行する場合は、このオプションを使用します。
毎日	このオプションは、自動デバイス解決を特定の時刻に毎日実行する場合に使用します。
手動で実行する	このオプションは、自動デバイス解決を手動でのみ実行する場合に使用します。
環境が変化するたびに	このオプションは、環境に変更があったときに自動デバイス解決を実行する場合に使用します。

手動でを指定すると、夜間の自動デバイス解決は無効になります。

DNS の処理オプション

DNS の処理オプションでは、次の機能を選択できます。

- DNS ルックアップの結果の処理を有効にすると、解決されたデバイスに付加する DNS 名のリストを追加できます。
- 「IPの自動解決：」を選択すると、DNSルックアップを使用して、iSCSIイニシエータおよびNFS共有にアクセスするホストに対して自動ホスト解決を有効にできます。指定しない場合は、 FC ベースの解決のみが実行されます。
- ホスト名にアンダースコアを使用できるようにすることも、標準のポートエイリアスの代わりに「接続先」のエイリアスを使用することもできます。

ストレージやテープの特定のベンダーを含めるか、除外します

ストレージやテープの特定のベンダーを自動解決の対象に含めたり除外したりできます。レガシーホストとなり、新しい環境から除外する必要があることがわかっているホストがある場合などは、特定のベンダーを除外することができます。除外したベンダーを再度追加することもできます。

テープのデバイス解決ルールは、ベンダー環境設定でそのWWNのベンダーが*テープのみとして含まれる*に設定されているWWNに対してのみ機能します。

正規表現の例

ソースの命名方法として正規表現のアプローチを選択した場合は、OnCommand Insight の自動解決方法で使用する独自の式のガイドとして正規表現の例を使用できます。

正規表現の形式

OnCommand Insight の自動解決の正規表現を作成する場合は、というフィールドに値を入力して出力形式を設定できます `FORMAT`。

デフォルト設定はです `\1`これは、正規表現に一致するゾーン名が、正規表現で作成された最初の変数の内容で置換されることを意味します。正規表現では、かっこで囲まれた記述で変数の値が作成されます。かっこで囲まれた記述が複数ある場合、変数は左から右に数値で参照されます。変数は、任意の順序で出力形式で使用できます。定数テキストは、に追加して出力に挿入することもできます `FORMAT` フィールド。

たとえば、このゾーンの命名規則には、次のようなゾーン名があります。

```
[Zone number]_[data center]_[hostname]_[device type]_[interface number]
```

- S123_Miami_hostname1_filer_FC1 のように入力します
- S14_Tampa_hostname2_switch_fc4
- S3991_Boston_hostname3_windows2K_FC0
- S44_Raleigh_hostname4_Solaris_FC1

出力形式は次のようになります。

```
        [hostname]-[data center]-[device type]
```

そのためには、ホスト名、データセンター、およびデバイスタイプのフィールドを変数に取り込み、それらを使用して出力する必要があります。正規表現は次のようになります。

```
.*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
```

括弧が3組あるので、変数です `\1`、 `\2` および `\3` 人口が増えるでしょう

この場合、次の形式で出力を受け取ることができます。

```
\2-\1-\3
```

出力は次のようになります。

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

変数間のハイフンは、出力に一定のテキストを挿入した例を示します。

例 **1** ：ゾーン名の例

この例では、正規表現を使用してゾーン名からホスト名を抽出します。次のようなゾーン名がある場合は、正規表現を作成できます。

- S0032_myComputer1Name - HBA0
- S0434_myComputer1Name - HBA1
- S0432_myComputer1Name - HBA3

ホスト名を取り込むための正規表現は次のようになります。

```
 S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
```

これは、先頭の文字が「 S 」で、そのあとに任意の桁数の数字、アンダースコア、英数字のホスト名（ myComputer1Name ）、アンダースコアまたはハイフン、大文字の「 HBA 」、 1 桁の数字（ 0~9 ）の順に続くすべてのゾーンに一致します。ホスト名のみが変数 **\1** に格納されます。

正規表現は次のように構成要素に分割できます。

- 「 S 」はゾーン名の先頭の文字を表します。これは、ゾーン名の先頭にある「 S 」にのみ一致します。

- 角かっこで囲まれた文字 [0-9] は、「 S 」のあとの文字が 0~9 の数字でなければならないことを示します。
- + 記号は、前の角かっこ内の情報が 1 回以上存在している必要があることを示します。
- （アンダースコア）は、「 S 」のあとの数字の直後に続くゾーン名の文字がアンダースコアでなければならないことを意味します。この例のゾーンの命名規則では、ゾーン名とホスト名の区切りにアンダースコアが使用されています。
- 必須のアンダースコアのあとにあるかっこは、そのかっこで囲まれたパターンが変数 \1 に格納されることを示します。
- 角かっこで囲まれた文字 [a-zA-Z0-9] は、すべての英字（大文字と小文字の両方）と数字に一致することを示します。
- 角かっこのあとの「 * 」（アスタリスク）は、角かっこで囲まれた文字の 0 回以上の繰り返しを示します。
- 角かっこで囲まれた文字 [__] （アンダースコアとダッシュ）は、英数字のパターンのあとにアンダースコアまたはダッシュが必要であることを示します。
- 正規表現内の文字列「 HBA 」は、この文字列そのものがゾーン名に含まれている必要があることを示します。
- 最後の角かっこで囲まれた文字 [0-9] は、 0~9 の 1 桁の数字に一致します。

例 **2**

この例では、最初のアンダースコアのあとの「 E 」から 2 番目ののの前までの部分を照合し、それよりも前とあとの部分は省いています。

ゾーン： `Z_E2FHDBS01_E1NETAPP`

ホスト名： `E2FHDBS01`

- RegExp：* `.?(E.?).*?`

例 **3**

正規表現の最後のセクションの前後にあるかっこ（）は、どの部分がホスト名であるかを識別します。「 VSAN3 」の部分がホスト名である場合は、 _ （ [a-zA-Z0-9] ） .* となります

ゾーン： `A_VSAN3_SR48KENT_A_CX2578_SPA0`

ホスト名： `SR48KENT`

- RegExp：* `_[a-zA-Z0-9]+_([a-zA-Z0-9]).*`

例 **4** は、複雑な命名パターンを示しています

次のようなゾーン名がある場合は、正規表現を作成できます。

- myComputerName123 ： HBA1_Symm1_FA3
- myComputerName123 ： HBA2_Symm1_FA5
- myComputerName123 ： HBA3_Symm1_FA7

これらを取り込むために使用できる正規表現は次のとおりです。

```
([a-zA-Z0-9]*)_.*
```

。 `\1` 変数にはのみが含まれます `myComputerName123` この式で評価された後。

正規表現は次のように構成要素に分割できます。

- かっこは、そのかっこで囲まれたパターンが変数 \1 に格納されることを示します。
- 角かっこで囲まれた文字 [a-zA-Z0-9] は、任意の英字（大文字と小文字の両方）と数字に一致することを示します。
- 角かっこのあとの「 * 」（アスタリスク）は、角かっこで囲まれた文字の 0 回以上の繰り返しを示します。
- 正規表現内の文字（アンダースコア）は、その前の角かっこの部分で照合された英数字の文字列の直後に続くゾーン名の文字がアンダースコアでなければならないことを意味します。
- 。（ピリオド）は、任意の文字（ワイルドカード）に一致します。
- 「 * 」（アスタリスク）は、その前のピリオド（ワイルドカード）が 0 回以上続くことを示します。

  つまり、「 .* 」の組み合わせは任意の文字数の任意の文字を表します。

例 **5** ：パターンがないゾーン名の例

次のようなゾーン名がある場合は、正規表現を作成できます。

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

これらを取り込むために使用できる正規表現は次のとおりです。

```
(.*?)_.*
```

変数 \1 には、 *myComputerName* （ 1 つ目のゾーン名の例）または *myComputerName123* （ 2 つ目のゾーン名の例）が格納されます。したがって、この正規表現は、最初のアンダースコアの前のすべての部分に一致します。

正規表現は次のように構成要素に分割できます。

- かっこは、そのかっこで囲まれたパターンが変数 \1 に格納されることを示します。
- 「 .* 」（ピリオドとアスタリスク）は、任意の文字数の任意の文字に一致します。
- 角かっこのあとの「 * 」（アスタリスク）は、角かっこで囲まれた文字の 0 回以上の繰り返しを示します。
- 。文字は、最短一致を示します。これにより、最後のアンダースコアではなく、最初のアンダースコアでの照合が強制的に停止されます。
- 文字「 _.* 」は、最初のアンダースコア以降のすべての文字に一致します。

例 **6** ：パターンを含むコンピュータ名の例

次のようなゾーン名がある場合は、正規表現を作成できます。

- Storage1_Switch1_myComputerName123A_A1_FC1
- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

これらを取り込むために使用できる正規表現は次のとおりです。

```
.*?_.*?_([a-zA-Z0-9]*[ABT])_.*
```

このゾーンの命名規則には特定のパターンがあるため、上記の式を使用できます。この式は「 A 」、「 B 」、または「 T 」のいずれかで終わるすべてのホスト名（この例では「 myComputerName 」）に一致し、そのホスト名を変数 \1 に格納します。

正規表現は次のように構成要素に分割できます。

- 「 .* 」（ピリオドとアスタリスク）は、任意の文字数の任意の文字に一致します。
- 。文字は、最短一致を示します。これにより、最後のアンダースコアではなく、最初のアンダースコアでの照合が強制的に停止されます。
- アンダースコア文字は、ゾーン名の最初のアンダースコアに一致します。
- したがって、最初の.*？_の組み合わせは、最初のゾーン名の例にある_Storage1_と一致します。
- 2つ目の.*？_の組み合わせは1つ目のゾーン名と同じように動作しますが、1つ目のゾーン名の例では_Switch1_に一致します。
- かっこは、そのかっこで囲まれたパターンが変数 \1 に格納されることを示します。
- 角かっこで囲まれた文字 [a-zA-Z0-9] は、任意の英字（大文字と小文字の両方）と数字に一致することを示します。
- 角かっこのあとの「 * 」（アスタリスク）は、角かっこで囲まれた文字の 0 回以上の繰り返しを示します。
- 正規表現内の角かっこで囲まれた文字 [ABT] は、ゾーン名に含まれる「 A 」、「 B 」、または「 T 」のいずれか 1 文字に一致します
- かっこのあとの（アンダースコア）は、 [ABT] で照合された文字のあとにアンダースコアが必要であることを示します。
- 「 .* 」（ピリオドとアスタリスク）は、任意の文字数の任意の文字に一致します。

その結果、次のいずれかの英数字文字列を含む変数 \1 が原因されます。

- 前に任意の数の英数字と 2 つのアンダースコアがある
- 後ろにアンダースコア（および任意の数の英数字）がある。
- 3 番目のアンダースコアの前に、 A 、 B 、または T の最後の文字を使用した。

例 **7**

ゾーン： `myComputerName123_HBA1_Symm1_FA1`

ホスト名： `myComputerName123`

- RegExp：* `([a-zA-Z0-9]+)_.*`

例 **8**

この例では、最初ののの前のすべての部分を検出します。

ゾーン： `MyComputerName_HBA1_Symm1_FA1`

`MyComputerName123_HBA1_Symm1_FA1`

ホスト名： `MyComputerName`

- RegExp：* `(.?)_.`

例**9**

この例では、最初ののののあとから2番目ののの前までのすべての部分を検出します。

ゾーン： `Z_MyComputerName_StorageName`

ホスト名： `MyComputerName`

- RegExp：* `.?(.?).*?`

例 **10**

この例では、ゾーンの例から「 MyComputerName123 」を抽出します。

ゾーン： `Storage1_Switch1_MyComputerName123A_A1_FC1`

`Storage2_Switch2_MyComputerName123B_A2_FC2`

`Storage3_Switch3_MyComputerName123T_A3_FC3`

ホスト名： `MyComputerName123`

- RegExp：* `.?.?([a-zA-Z0-9]+)[ABT]_.`

例 **11**

ゾーン： `Storage1_Switch1_MyComputerName123A_A1_FC1`

ホスト名： `MyComputerName123A`

- RegExp：* `.?.?([a-zA-z0-9]+).*?`

例 **12**

角かっこ*の中の^（円弧またはキャレット）*は、式を否定します。たとえば、[^FF]は大文字または小文字のFを除くすべてを意味し、[^a-z]は小文字のaからzを除くすべてを意味し、上記の場合は_以外のすべてを意味します。format ステートメントは、出力ホスト名にを追加します。

ゾーン： `mhs_apps44_d_A_10a0_0429`

ホスト名： `mhs-apps44-d`

- RegExp：* `([^_])_([AB]).*`+OnCommand Insight での形式：

`([^_])_().*`OnCommand Insight での形式：

例 **13**

この例では、ストレージエイリアスの区切りにが使用されています。この場合、が文字列で実際に使用されており、式の一部ではないことを示すために、を使用する必要があります。

ストレージエイリアス： `\Hosts\E2DOC01C1\E2DOC01N1`

ホスト名： `E2DOC01N1`

- RegExp：* `\\.?\\.?\\(.*?)`

例 **14**

この例では、ゾーンの例から「 PD-RV-W-AD-2 」を抽出します。

ゾーン： `PD_D-PD-RV-W-AD-2_01`

ホスト名： `PD-RV-W-AD-2`

- RegExp：* `[^-]-(.-\d+).+`

例 **15**

この例では、形式の設定でホスト名に「 US-BV- 」を追加しています。

ゾーン： `SRV_USBVM11_F1`

ホスト名： `US-BV-M11`

- RegExp：* `SRV_USBV([A-Za-z0-9]+)_F[12]`

形式： `US-BV-\1`

Insightのメンテナンス

Insightを初めて導入し、システムを新規にセットアップする場合でも、システムを以前

から運用していた場合でも、Insightとネットワークの円滑な運用を維持するための措置を講じる必要があります。メンテナンスの重要な概念は、通常はネットワークの変更にInsightで対応する必要があるということです。

最も一般的なメンテナンスタスクは次のとおりです。

- Insightのバックアップの保持
- 期限切れのInsightライセンスを更新しています
- データソースパッチの調整
- すべてのAcquisition UnitでInsightのバージョンを更新しています
- 削除したデータソースをInsightから削除しています

Insightの管理

OnCommand Insight は環境を監視し、危機が報告される前に潜在的な問題を調査できるようにします。[Assets Dashboard]には、概要を示す円グラフ、IOPSのヒートマップ、および利用率が高い上位10個のストレージプールを示す対話型のグラフが表示されます。

手順

1. Insight **Assets Dashboard** を開き、円グラフの上にカーソルを移動して、次の3つのグラフでアセットの分布を確認します。
   - [Capacity by Vendor]には、各ベンダーのストレージの合計物理容量が表示されます。
   - [Capacity by Tier]には、各ストレージ階層の使用可能な合計容量が表示されます。
   - [Switch Ports]円グラフには、ポートのメーカーと使用済みポートの割合が表示されます。
2. [Facts About Your Environment]*を表示して、環境の使用済み容量、容量の効率、消費されているFCリソース、および仮想インフラの統計に関する情報を確認できます。
3. [Top 10 Utilized Pools]*グラフのストレージプールのバーにカーソルを合わせ、ストレージプールの使用済み容量と未使用容量を確認します。
4. [Storage IOP]*ヒートマップで大きな文字で表示されているアセット（問題のあるアセット）の名前をクリックすると、そのアセットの現在の状態をまとめたページが表示されます。
5. の右下隅にある[Virtual Machine IOPS]*ヒートマップで、大きなテキストで表示されているアセット（問題のあるアセット）の名前をクリックすると、アセットの現在の状態をまとめたページが表示されます。
6. Insightのツールバーで、*[Admin]*をクリックします。
7. 赤い丸が表示されている領域に注意してください。

   OnCommand InsightWeb UIでは、潜在的な問題が赤い丸で示されます。
8. [データソース]*をクリックして、監視しているすべてのデータソースのリストを確認します。

   [ステータス]*列に赤い丸で囲まれたメッセージが表示され、[影響]*が[高]または[中]になっているデータソースを確認します。これらはテーブルの上にあります。これらのデータソースの問題は、ネットワークの大部分に影響を及ぼします。この問題に対処する必要があります。

9. [Acquisition Units]*をクリックして、Insightを実行している各IPアドレスのステータスを確認し、必要に応じてAcquisition Unitを再起動します
10. Insightサーバのインスタンス監視の概要を表示するには、*[健全性]*をクリックします。

OnCommand Insight システムヘルスを監視しています

Insightシステムコンポーネントの現在のステータスを[Health]ページで定期的に確認する必要があります。このページには、各コンポーネントのステータスが表示され、問題 がある場合はアラートが表示されます。

手順

1. InsightWeb UIにログインします。
2. をクリックし、[ヘルス]*を選択します。

   [Health]ページが表示されます。

3. コンポーネントの現在のステータスを確認します。[* Details]*列のステータスの前に赤い丸が表示されている場合は、すぐに対処が必要な問題 を示しているため、特に注意してください。

   [Health]ページには、Insightのコンポーネントのうち、システム構成に基づいて次のいずれかまたはすべてのコンポーネントに関する情報が表示されます。

コンポーネント	テスト	詳細	表示されます
取得	インベントリデータの処理	Local Acquisition Unitのステータス	同時にポーリングするデータソースの数が実行プールの最大数の75%未満（デフォルトの最大数は30）の場合、「OK」。「Acquisition is busy」は、使用率が75%を超える場合に使用します。ポーリング間隔を長くするか、Remote Acquisition Unitを追加することを推奨します。
DWH	バックアップ	Data Warehouseのスケジュールされたバックアップのステータス	DWHのスケジュールされたバックアップが有効になっている場合は、「OK」と前回成功したDWHのバックアップ時刻が表示されます。それ以外の場合は、検出されたエラーに関する情報が表示されます。

DWH	ETL	Data WarehouseのETLのステータス	「OK」と、エラーがなければ前回成功したDWHのビルド時間が表示されます。それ以外の場合は、検出されたエラーに関する情報が表示されます。
サーバ	ASUP	ASUPのステータス	「ASUP Enabled」と前回成功したPhonehome時間（該当する場合）。「ASUP Failed」は、Phonehomeが有効になっているが問題が発生した場合に表示されます。 +バックアップディレクトリが無効な場合は、「Invalid backup location（バックアップの場所が無効です）」。 + Phonehomeが最後に成功した時刻と、最後に失敗した時刻（使用可能な場合）を表示します。 +「ASUP Disabled」（Phonehomeが無効な場合）
サーバ	自動解決	自動デバイス解決のステータス	エラーがなければ「OK」。識別エラーが解決の進行を妨げている場合は、「自動解決はブロックされています」と表示されます。 一般的なデバイスの75%未満を識別できる場合は、+"`Low success rate'"。

サーバ	Elasticsearch を指定します	Elasticsearchデータストアのステータス	エラーがなければ「OK」。Elastic Searchサービスに接続できない場合は、「Service Unavailable」と入力します。 +複数のノードが検出された場合は「Cluster mode detected」 +「High memory utilization」（ヒープ領域の使用率が85%を超えている場合） +「ステータス：赤」は、Elasticsearchでエラーが報告されたことを示します。エラーに関する情報を表示し、カスタマーサポートに問い合わせることを推奨します。
サーバ	CPU	InsightのCPU使用率	CPU負荷が65%未満の場合は「OK」。"`SシステムのCPU負荷が高くなっています。CPUの負荷を軽減します。 CPU負荷が65%を超えている場合。
サーバ	ディスクスペース	ディスクスペースのステータス	空きディスクスペース、Insightで使用されているディスクスペース、およびInsight用に予約されている推奨ディスクスペース。ディスク使用率が80%を超えている場合は「Low Disk Space（ディスクスペースが不足しています）」。
サーバ	EventBusの略	EventBusのステータス	EventBusキューが空の場合は「`EventBus is empty`」、それ以外の場合はEventBusキューのステータスが表示されます。

サーバ	インベントリデータの処理	Insight Serverのインベントリデータ処理機能のステータス	Insight Serverがビジー状態でない場合は「OK」。サーバが過去1時間の75%以上の時間でビジー状態になっている場合、「サーバはビジー状態です」と表示されます。では、データソースを追加しないようにし、環境を複数のサーバに分割することを推奨しています。
サーバ	MySQL	MySQLデータベースのステータス	問題が検出されない場合は「OK」。"'データベースにパフォーマンスの問題があります。低速クエリの数が5%を超えると、一部のクエリの実行に時間がかかりすぎます。 +"'データベース・ログ・ファイルが過去1時間に<size> を超えて増加しましたエラーログが20 KBを超える場合は、MySQLログファイルを確認してください。
サーバ	パフォーマンスアーカイブ	パフォーマンスアーカイブのステータス	「Performance archive is enabled」または「Performance archive is not enabled」というメッセージが表示されます。
サーバ	物理メモリ	物理メモリのステータス	メモリ使用率が85%未満の場合は「OK」。"`memory usage is high.メモリ使用率が85%を超える場合は、システムの安定性のために全体的なメモリフットプリントを削減します。

サーバ	サービスパック	サービスパックの有無	Insightで使用可能なサービスパックがあるかどうかが表示されます。サービスパックが使用可能な場合は、指示が表示されます。
サーバ	使用状況の情報	使用状況情報の送信ステータス	使用状況に関する情報のネットアップへの送信が有効か無効かが表示されます。無効な場合は有効にすることをお勧め最後に試行された、または最後に成功した送信時刻を表示します +発生した問題に関する情報を表示します。
サーバ	違反です	未解決の違反のステータス	未解決の違反の数が上限の75%未満の場合は「OK」。未解決の違反の数が上限の75%を超えている場合は、「Maximum number of open violations allowed is <number> 」と表示されます。パフォーマンスポリシーの設定を確認することを推奨します。 +「違反マネージャはブロックされています」は、未解決の違反の数が上限に達している場合に表示されます。 +新しい違反は作成できないので、パフォーマンスポリシーの設定を確認することを推奨します。
サーバ	週次バックアップ	週次バックアップのステータス	週次バックアップが有効になっている場合は「OK」、有効になっていない場合は「週次バックアップは有効になっていません」と表示されます。

非アクティブなデバイスの削除

使用されていないデバイスを削除すると、データをクリーンに保ち、ナビゲートしやすくなります。

このタスクについて

Insightから非アクティブなデバイスを削除するには、次の手順を実行します。

手順

1. 新しいクエリを作成するか、既存のクエリを開きます。
2. [*generic device*]、[*host*]、[*storage*]、[*switch*]、または[_tape_asset]のいずれかのタイプを選択します。
3. 「* is active 」のフィルタを追加し、フィルタを「 No *」に設定します。

   結果テーブルには、アクティブでないアセットのみが表示されます。

4. 削除するデバイスを選択します。
5. [Actions]ボタンをクリックし、[Delete Inactive Devices]を選択します。

   非アクティブなデバイスは削除され、Insightに表示されなくなります。

システムおよびユーザアクティビティの監査

予期しない変更を特定する場合は、OnCommand Insight システムとそのユーザアクティビティの監査証跡を表示できます。監査ログメッセージは、[Audit]ページに表示されるだけでなく、syslogに送信することもできます。

このタスクについて

Insightでは、ストレージネットワークやストレージネットワークの管理に影響するユーザアクティビティについて、次のような監査エントリが生成されます。

- ログインしています
- パスの許可または許可解除
- 許可されたパスの更新
- グローバルなポリシーまたはしきい値を設定します
- データソースの追加または削除
- データソースを開始または停止します
- データソースのプロパティを更新しています
- タスクの追加、編集、または削除
- アプリケーショングループを削除しています
- デバイスの ID を識別または変更する

- ユーザを作成します
- ユーザを削除します
- ユーザロールの変更
- ユーザの変更（Guest à Admin）
- ユーザからのログアウト（強制ログアウトまたは手動ログアウト）
- Acquisition Unitの削除
- ライセンスの更新
- バックアップを有効にします
- バックアップの無効化
- ASUPの有効化（同じページでプロキシの有効化が監査ログに報告される）
- ASUPの無効化（同じページでプロキシの無効化が監査ログに報告される）
- セキュリティキーの再作成、システムパスワードの変更
- アセットのアノテーションを削除/追加しています
- CACユーザーのログオン/ログオフ
- CACユーザセッションタイムアウト

手順

1. ブラウザでInsightを開きます。
2. をクリックし、[Audit]*を選択します。

   [監査]ページでは、監査エントリが表形式で表示されます。

3. テーブルでは、次の詳細を確認できます。

   - * 時間 *

     変更が行われた日時

   - * ユーザー *

     監査エントリに関連付けられているユーザの名前

   - * 役割 *

     ユーザアカウントのロール（ゲスト、ユーザ、または管理者）

   - * IP *

     監査エントリに関連付けられているIPアドレス

   - * アクション *

     監査エントリのアクティビティのタイプ

◦ * 詳細 *

監査エントリの詳細

データソースやアプリケーションなどのリソースに影響するユーザアクティビティがある場合は、そのリソースのランディングページへのリンクが詳細に表示されます。

データソースを削除すると、そのデータソースに関連するユーザアクティビティの詳細にデータソースのランディングページへのリンクが表示されなくなります。

4. 監査エントリを表示するには、特定の期間（1時間、3時間、24時間、3日間、7日間）を選択します。Insightでは、選択した期間について、最大1、000件の違反が表示されます。

   1ページに収まらないデータがある場合は、表の下のページ番号をクリックして、ページごとにデータを参照できます。

5. 列ヘッダーの矢印をクリックして、表内の列のソート順序を昇順（上矢印）または降順（下矢印）に変更します。デフォルトのソート順序に戻すには、他の列ヘッダーをクリックします。

   デフォルトでは、エントリは降順で表示されます。

6. [**filter**]ボックスを使用すると、必要なエントリだけを表に表示できます。

   ユーザの監査エントリのみを表示します `izzyk`を入力します `izzyk を* filter *ボックスに入力します。

ネットワーク内の違反を監視します

パフォーマンスポリシーで設定されたしきい値に基づいてInsightで違反が生成された場合は、[Violations Dashboard]で確認できます。このダッシュボードには、ネットワークで発生したすべての違反が表示され、問題を特定して対処することができます。

手順

1. ブラウザでOnCommand Insight を開きます。
2. Insightのツールバーで、**[Dashboards]***をクリックし、[Violations Dashboard]*を選択します。

   [Violations Dashboard]が表示されます。

3. [Violations by Policies]*円グラフでは、次の方法で情報を確認できます。
   - グラフの任意のスライスにカーソルを合わせると、特定のポリシーまたは指標に対する違反の総数の割合を表示できます。
   - グラフのスライスをクリックすると、そのスライスを「拡大」できます。これにより、そのスライスをグラフの残りの部分から遠ざけることで、そのスライスを強調して注意深く調べることができます。
   - をクリックできます アイコンをクリックして円グラフを全画面モードで表示し、をクリックします 円グラフを最小化するには、もう一度繰り返します。円グラフには最大5つのスライスを含めることができます。そのため、6つのポリシーで違反が発生した場合は、5つ目と6つ目のスライスが「その他」のスライスに統合されます。Insightでは、違反数が最も多いものが最初のスライスに割り当てら

れ、2番目に多いものが2番目のスライスに割り当てられます。

4. [Violations History]*チャートは次の方法で使用できます。
   - グラフにカーソルを合わせると、特定の時点で発生した違反の総数と、指定した各指標についての違反の総数のうち発生した数が表示されます。
   - 凡例ラベルをクリックすると、その凡例に関連付けられているデータをグラフから削除できます。

     凡例をクリックすると、データが再度表示されます。

   - をクリックできます アイコンをクリックしてグラフを全画面モードで表示し、をクリックします 円グラフを最小化するには、もう一度繰り返します。
5. [Violations Table]*は次の方法で使用できます。
   - をクリックできます 右上隅のアイコンをクリックしてテーブルを全画面モードで表示し、をクリックします 円グラフを最小化するには、もう一度繰り返します。

     ウィンドウサイズが小さすぎる場合、[Violations Table]には3列しか表示されませんが、をクリックすると表示されます 、追加の列（最大7列）が表示されます。

   - 特定の期間の違反を表示できます（* 1h 、 3h 、 24h 、 3d 、 7d 、 と 30d *）が表示されます。Insightでは、選択した期間について、最大1、000件の違反が表示されます。
   - [**filter**]ボックスを使用すると、必要な違反のみを表示できます。
   - 列ヘッダーの矢印をクリックすると、表内の列のソート順序を昇順（上矢印）または降順（下矢印）に変更できます。デフォルトのソート順序に戻すには、他の列ヘッダーをクリックします。

     デフォルトでは、違反は降順で表示されます。

   - [ID]列で違反をクリックすると、その違反の期間のアセットページを表示できます。
   - 概要 列でリソース（ストレージプールやストレージボリュームなど）のリンクをクリックすると、それらのリソースに関連付けられているアセットページを表示できます。
   - [ポリシー]列でパフォーマンスポリシーのリンクをクリックすると、[ポリシーの編集]ダイアログボックスが表示されます。

     生成される違反が少なすぎる場合や多すぎる場合は、ポリシーのしきい値を調整することができます。

   - 1ページに収まらないデータがある場合は、ページ番号をクリックしてページごとにデータを参照できます。
   - をクリックできます 違反を却下します。

Acquisition Unitのステータス

[Acquisition Unit]画面には、ステータスやエラーなど、すべてのAcquisition Unitが表示されます。

サーバに接続されているInsight Acquisition Unitのステータスは、* Admin > Acquisition Units *の表に表示されます。この表には、各Acquisition Unitについて次の情報が表示されます。

- * 名前 *

- * IP *
- * Status *はAcquisition Unitの動作ステータスです。
- **Last Reported** Acquisition Unitに接続されたデータソースが最後に報告された時刻が表示されます。
- *Note*には、AUに関連するユーザー入力のメモが表示されます。

リスト内のAcquisition Unitに問題がある場合は、[Status]フィールドに問題に関する簡単な情報を示す赤い丸が表示されます。Acquisition Unitの問題はデータ収集に影響する可能性があるため、調査する必要があります。

Acquisition Unitを再起動するには、Acquisition Unitにカーソルを合わせ、表示される[*Restart Acquisition Unit*]ボタンをクリックします。

テキストメモを追加するには、Acquisition Unitにカーソルを合わせ、表示された_Add Note_ボタン をクリックします。最後に入力したメモのみが表示されます。

Insightデータベースをリストアしています

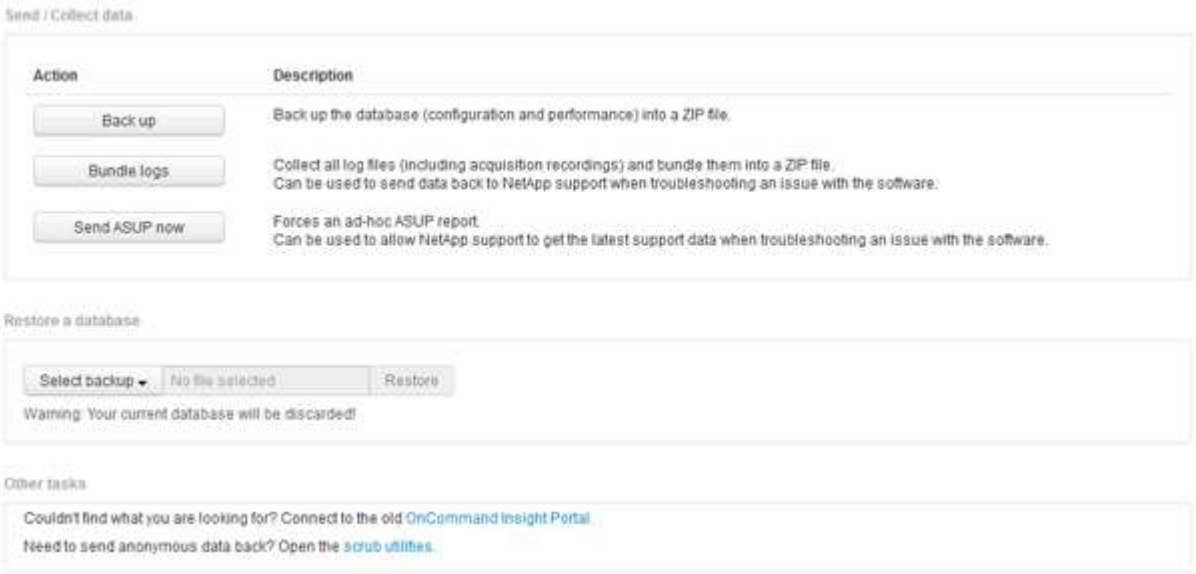
検証済みのバックアップファイルからInsightデータベースをリストアするには、[Troubleshooting]オプションを使用します。この処理を実行すると、現在のOnCommand Insight データが完全に置き換えられます。

作業を開始する前に

ベストプラクティス: OnCommand Insight データベースをリストアする前に、手動バックアッププロセスを使用して現在のデータベースのコピーを作成してください。リストアするバックアップファイルをチェックし、リストアするファイルが含まれているバックアップが正常に完了していることを確認します。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [トラブルシューティング]*をクリックします。



3. [データベースのリストア]セクションで、*[バックアップの選択]*メニューからリストアするバックアップファイルを選択します。
4. [* リストア] をクリックします。
5. すべてのデータが置き換えられるという警告が表示されたら、* OK *をクリックします

   リストア処理のステータスがリストアページに表示されます。

期限切れライセンスを更新しています

Insightのライセンスの有効期限が切れた場合は、最初にインストールしたライセンスと同じ手順 を使用して迅速にライセンスを更新できます。

手順

1. メモ帳などのテキストエディタで、ネットアップサポートから受け取った新しいライセンスファイルを開き、ライセンスキーのテキストをWindowsクリップボードにコピーします。
2. ブラウザでOnCommand Insight を開きます。
3. ツールバーの* Admin *をクリックします。
4. [設定]*をクリックします。
5. [ライセンス]タブをクリックします。
6. ［ * ライセンスの更新 * ］ をクリックします。
7. ライセンスキーのテキストを* License *テキストボックスにコピーします。
8. [更新（最も一般的な）]*操作を選択します。

   この処理を実行すると、現在アクティブなInsightライセンスに新しいライセンスが追加されます。

9. [保存（ Save ）] をクリックします。
10. Insightの消費ライセンスモデルを使用する場合は、[usage]セクションの*[Enable sending usage information to NetApp]*チェックボックスをオンにする必要があります。プロキシが適切に設定され、環境に応じて有効になっている必要があります。

ライセンスが準拠しなくなりました

Insightの[Licenses]ページに「Not Compliant」というメッセージが表示された場合、Insightで管理している容量は会社でライセンスされている容量を超えています。

「Not Compliant」メッセージは、Insightで現在管理しているテラバイト数よりも支払い済みの容量が少ないことを示します。非準拠のメッセージの横に、管理対象のテラバイト数とライセンスされたテラバイト数の差が表示されます。

Insightシステムの動作には影響しませんが、ネットアップの担当者に連絡してライセンスの適用範囲を広げ、適切なライセンスを更新する必要があります。

Insightの旧バージョンのライセンスの交換

Insightの以前のバージョンとの下位互換性がない新しいバージョンを購入した場合は、古いライセンスを新しいライセンスに置き換える必要があります。

新しいライセンスをインストールする場合は、ライセンスキーのテキストを保存する前に*置換*操作を選択する必要があります。

サービスパックの適用

サービスパックは定期的に提供されており、OnCommand Insight の修正や拡張を活用するために適用することができます。

作業を開始する前に

- サービスパックファイルをダウンロードしておく必要があります（例： `7.2service_pack_1.patch`）をNOWサイトから取得します。
- すべてのパッチを承認しておく必要があります。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [パッチ]*をクリックします。
3. [Actions]ボタンから、*[Apply patch]*を選択します。
4. ダイアログボックスで、[参照]*をクリックしてサービスパックファイルを探します。
5. 影響を受けるデータソースがあるかどうかを示す*パッチ名*、概要 *、 Impacted data source types 、および Details *（サービスパックに含まれる拡張機能）を確認します。
6. 選択したサービスパックが正しい場合は、*パッチの適用*をクリックします。

   サービスパックは自動的に承認されます。これ以上の操作は必要ありません。

特別なトラブルシューティングレポートの準備

Insightでは、ソフトウェアのインストール後にセットアップしたASUPシステムを通じて、ネットアップカスタマーサポートに情報が自動的に送信されます。ただし、トラブルシューティングレポートを作成し、特定の問題についてサポートチームとケースをオープンすることもできます。

Insightのツールを使用すると、Insightを手動でバックアップし、ログをバンドルして、その情報をネットアップのカスタマーサポートに送信できます。

OnCommand Insight データベースを手動でバックアップします

OnCommand Insight データベースの週次バックアップを有効にした場合は、必要に応じてデータベースのリストアに使用できるコピーが自動的に生成されます。リストア処理の前にバックアップを作成する必要がある場合や、ネットアップのテクニカルサポート

に送信する必要がある場合は、バックアップを作成できます `.zip` ファイルを手動で作成する。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [トラブルシューティング]*をクリックします。
3. [データの送信/収集]セクションで、*[バックアップ]*をクリックします。
4. [ファイルの保存]をクリックします。
5. [OK] をクリックします。

サポート用のログのバンドル

Insightソフトウェアの問題をトラブルシューティングする際に、ログやデータ収集の記録をまとめたzipファイル（「gz」形式）を迅速に生成して、ネットアップのカスタマーサポートに送信することができます。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [トラブルシューティング]*をクリックします。
3. [データの送信/収集]セクションで、*[ログのバンドル]*をクリックします。
4. [ファイルの保存]をクリックします。
5. [OK] をクリックします。

ネットアップサポートに情報を送信しています

ネットアップの自動サポート（ASUP）機能は、トラブルシューティング情報をネットアップのカスタマーサポートチームに直接送信します。特別なレポートを強制的に送信できます。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [設定]*をクリックします。
3. [Backup/ASUP]*タブをクリックします。
4. [データの送信/収集]領域で*[ASUPを今すぐ送信]*をクリックして、ログ、記録、バックアップをネットアップサポートに送信します。

サポートへの転送用にデータをスクラビングしています

セキュアな環境を構築しているお客様は、発生した問題をトラブルシューティングするために、ネットアップカスタマーサービスと通信し、データベース情報を犠牲にすることはありません。OnCommand Insight スクラブユーティリティを使用すると、キーワードとパターンの包括的な辞書を設定して、機密データを「クレンジング」し、スクラビングされたファイルをカスタマーサポートに送信できます。

手順

1. Web UIで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[スクラブユーティリティ]*リンクをクリックします。

   [Lookup in Dictionary]、[Scrub data]、[Build dictionary]、[Custom keywords]、および[Regular expressions]という複数のスクラビングセクションがあります。

.

+ .. [**Lookup in dictionary**]セクションで、置換する値を表示するコードを入力するか、置換するコードを表示する値を入力します。注:ルックアップを実行する前に、サポートデータからスクラブする値を識別するためのディクショナリを*ビルド*する必要があります。

1. サポートデータからスクラブする独自のキーワードを追加するには、カスタムキーワード*セクションで、メニューの**[**アクション**][**カスタムキーワードの追加**]**をクリックします。キーワードを入力し、[保存]*をクリックします。キーワードがディクショナリに追加されます。
2. [*パターン（regexp）]*を展開します。[追加（Add）]*をクリックして、新しいパターンを入力するためのダイアログボックスを表示します。
3. スクラビングする単語やフレーズを識別するために正規表現を使用するには、* regular expressions セクションにパターンを入力します。**[**メニュー**:**アクション**][**正規表現の追加**]**をクリックし、フィールドにパターンの名前と正規表現を入力して[保存]*をクリックします。情報がディクショナリに追加されました。

正規表現キャプチャグループを識別するには、パターンを丸括弧で囲む必要があります。

4. [**Build dictionary**]セクションで、[Build*]をクリックして、OnCommand Insight データベースから機密と識別されたすべての単語の辞書のコンパイルを開始します。

   完了すると、改訂されたディクショナリが使用可能であることを通知するプロンプトが表示されます。Database概要 には、ディクショナリ内のキーワードの数を示す行が含まれています。辞書でキーワードの正確さを確認してください。問題が見つかった場合に辞書を再構築するには、[データベース]ブロックの*[リセット]*をクリックして、OnCommand Insight データベースから収集されたすべてのキーワードを辞書から削除します。プロンプトが示すように、他のキーワードは削除されません。Scrubユーティリティに戻り、カスタムキーワードをもう一度入力します。

5. Scrubディクショナリを作成したら、そのディクショナリを使用してログ、XML、またはその他のテキストファイルをスクラビングし、データを匿名にすることができます。
6. ログ、XML、またはその他のテキストファイルをスクラビングするには、* Scrub data セクションで参照してファイルを探し、 Scrub file *をクリックします。

高度なトラブルシューティング

OnCommand Insight の設定を完了するには、高度なトラブルシューティングツールを使用する必要があります。これらのツールはブラウザで実行され、* Admin > Troubleshooting *ページから開きます。

ブラウザで高度なトラブルシューティングツールを開くには、ページ下部の*高度なトラブルシューティング*リンクをクリックします。

高度なトラブルシューティングツールを使用すると、さまざまなレポート、システム情報、インストールされているパッケージ、ログを表示したり、サーバやAcquisition Unitの再起動、DWHアノテーションの更新、アノテーションのインポートなどのさまざまな操作を実行したりできます。

使用可能なすべてのオプションについては、詳細トラブルシューティングページを参照してください。

動的なデータを無視する時間数を設定します

使用済み容量などの動的なデータの更新をOnCommand Insight が無視する時間数を設定できます。デフォルトの6時間を使用し、設定を変更しない場合、デフォルトの時間数が経過するまで、レポートは動的データで更新されません。このオプションを使用すると、動的なデータのみが変更された場合に更新が延期されるため、パフォーマンスが向上します。

このタスクについて

このオプションに値が設定されている場合、OnCommand Insight は次のルールに基づいて動的データを更新します。

- 設定は変更されず、容量データが変更された場合、データは更新されません。
- 動的なデータ（設定変更を除く）は、このオプションで指定したタイムアウト後にのみ更新されます。
- 構成が変更されると、構成データと動的データが更新されます。

このオプションの影響を受ける動的なデータには、次のものがあります。

- 容量違反のデータ
- ファイルシステムの割り当て済み容量と使用容量
- ハイパーバイザー
  - 仮想ディスクの使用容量
  - Virtual Machine Used Capacityの略
- 内部ボリューム
  - データの割り当て容量
  - データの使用容量
  - 重複排除による削減量
  - 最終アクセス時間
  - 最終Snapshot時間
  - その他の使用容量
  - Snapshot数
  - Snapshotの使用容量
  - 合計使用容量
- iSCSIセッションのイニシエータIP、ターゲットセッションID、およびイニシエータセッションID
- qtreeクォータの使用容量
- クォータで使用されているファイルと使用済み容量
- Storage Efficiencyテクノロジ、ゲイン/損失、潜在的なゲイン/損失
- ストレージプール
  - データの使用容量
  - 重複排除による削減量
  - その他の使用容量
  - Snapshotの使用容量
  - 合計使用容量
- ボリューム
  - 重複排除による削減量
  - 最終アクセス時間
  - 使用済み容量

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[高度なトラブルシューティング]*リンクをクリックします。
3. [Advanced settings]*タブをクリックし、[Acquisition Dynamic Attributes]セクションで、OnCommand

Insight がAcquisition Dynamic Attributesの動的データを無視する時間数を入力します。

4. [保存（ Save ）] をクリックします。
5. （オプション）Acquisition Unitを再起動するには、[Restart Acquisition Unit]リンクをクリックします。

   Local Acquisition Unitを再起動すると、OnCommand Insight のすべてのデータソースビューがリロードされます。この変更は次回のポーリング時に適用されるため、Acquisition Unitを再起動する必要はありません。

カスタマーサポート用のログを生成しています

カスタマーサポートから要求された場合は、トラブルシューティングのためにサーバログ、データ収集ログ、またはリモートログを生成します。

このタスクについて

ネットアップカスタマーサポートから要求があった場合は、このオプションを使用してログを生成します。

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[高度なトラブルシューティング]*をクリックします。
3. 次のページの[詳細設定]メニューで、*トラブルシューティング*リンクをクリックします。
4. [ログ]*タブをクリックし、ダウンロードするログファイルを選択します。

   ダイアログボックスが開き、ログを開くか、ログをローカルに保存できます。

システム情報の表示

OnCommand Insight サーバが導入されているシステムに関するMicrosoft WindowsのIP設定情報を表示できます。

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[高度なトラブルシューティング]*リンクをクリックします。
3. [高度なトラブルシューティング]ページで、*[レポート]*タブをクリックします。
4. [システム情報]*をクリックします。

   WindowsのIP設定には、ホスト名、DNS、IPアドレス、サブネットマスク、OS情報などの情報が含まれます。 メモリ、ブートデバイス、および接続名。

インストールされている**OnCommand Insight** コンポーネントの一覧表示

インストールされているOnCommand Insight コンポーネントのリスト（インベントリ、容量、ディメンションなど）を表示できます。 およびData Warehouseビュー。カスタ

マーサポートからこの情報の入力を求められる場合や、インストールされているソフトウェアのバージョンとインストール日時を確認する必要がある場合があります。

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[高度なトラブルシューティング]*リンクをクリックします。
3. [高度なトラブルシューティング]ページで、*[レポート]*タブをクリックします。
4. [インストールされているソフトウェアパッケージ]*をクリックします。

データベースオブジェクトの数を計算します

OnCommand Insight データベース内のオブジェクトの数を確認するには、スケールの計算機能を使用します。

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[高度なトラブルシューティング]*リンクをクリックします。
3. [高度なトラブルシューティング]ページで、*[レポート]*タブをクリックします。
4. [計算スケール]*をクリックします。

OnCommand Insight サーバを再起動しています

OnCommand Insight サーバを再起動するときは、ページを更新し、OnCommand Insight ポータルに再度ログインします。

このタスクについて

どちらのオプションも、ネットアップカスタマーサポートから要求があった場合にのみ使用してください。再起動する前に確認は行われません。

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[高度なトラブルシューティング]*リンクをクリックします。
3. 次のページの[詳細設定]メニューで、*[アクション]*タブをクリックします。
4. [サーバーの再起動]*をクリックします。

移行オプションを使用して**MySQL**データを移動しています

MySQLのデータディレクトリを別のディレクトリに移行することができます。現在のデータディレクトリは保持できます。[Troubleshooting]メニューの移行オプションを使用するか、コマンドラインを使用できます。この手順 では、トラブルシューティング>* MySQLデータの移行*オプションの使用方法について説明します。

このタスクについて

現在のデータディレクトリを保持する場合、そのディレクトリはバックアップとして保持され、名前が変更されます。

手順

1. Web UIで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. [高度なトラブルシューティング]*をクリックします。
3. [アクション]タブを選択します
4. [MySQLデータの移行]*を選択します。
5. データの移行先のパスを入力します。
6. 既存のデータディレクトリを保持するには、**[**既存のデータディレクトリを保持する**]**をオンにします。
7. [* Migrate （移行）] をクリックします

コマンドラインを使用して**MySQL**データを移動しています

MySQLのデータディレクトリを別のディレクトリに移行することができます。現在のデータディレクトリは保持できます。[Troubleshooting]メニューの移行オプションを使用することも、コマンドラインを使用することもできます。この手順 では、コマンドラインの使用方法について説明します。

このタスクについて

現在のデータディレクトリを保持する場合、そのディレクトリはバックアップとして保持され、名前が変更されます。

MySQLデータの移行ユーティリティを使用するか、を使用できます `java -jar mysqldatamigrator.jar` のOnCommand Insight パスのオプション `\bin\mysqldatamigrator` 次のパラメータを使用する必要があります。

- 必須パラメータ
  - *-path *

    データフォルダのコピー先となる新しいデータパス。
- オプションのパラメータ
  - *-myCnf <my .cnf file> *
  - *-doBackup *

    このフラグが設定されている場合、現在のデータフォルダの名前は変更されますが、削除されることはありません。

手順

1. コマンドラインツールには、次のURLからアクセスします。 `<installation path> \bin\mysqldatamigrator\mysqldatamigrator.jar``

使用例

```
java -jar mysqldatamigrator.jar -path "C:\<new path>" -doBackup
```

アノテーションの更新を強制します

アノテーションを変更したあとすぐにレポートで使用するには、いずれかのアノテーション強制オプションを使用します。

手順

1. Web UIで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページの下部にある*[高度なトラブルシューティング]リンクをクリックします。
3. [アクション]タブをクリックします。
4. 次のいずれかのオプションを選択します。
   - * DWHアノテーションの更新*：Data Warehouseのアノテーションの更新をレポートに使用するように強制します。
   - * DWHアノテーションの更新（[Deleted]）*。Data Warehouseでアノテーションの更新（削除されたオブジェクトを含む）を強制的にレポートに使用します。

サーバリソースのステータスを確認しています

このオプションを選択すると、OnCommand Insight サーバの情報（サーバメモリ、ディスクスペース、OS、CPU、OnCommand Insight データベースの情報（InnoDBデータサイズ、データベースが存在するディスク空きスペースなど）が表示されます。

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、* OnCommand Insight Portal*リンクをクリックします。
3. 次のページの[詳細設定]メニューで、*トラブルシューティング*リンクをクリックします。
4. [サーバリソースステータス]*をクリックします。

   *上級OnCommand Insight ユーザーの場合:*管理者は、情報サマリーの最後にあるボタンから、データベースとサーバーの応答時間を確認するためにいくつかのSQLテストを実行できます。このオプションは、サーバリソースが少ない場合に警告を表示します。

ゴーストデータソースの検索

デバイスを削除してもデバイスデータが残っている場合は、ゴーストデータソースを見つけて削除できます。

手順

1. Web UIで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[高度なトラブルシューティング]*リンクをクリックします。
3. [レポート]タブで、*[ゴーストデータソース]*リンクをクリックします。

   OnCommand Insight は、発信者とそのデバイス情報のリストを生成します。

見つからないディスクモデルを追加しています

ディスクモデルが不明なために取得に失敗した場合は、そのディスクモデルをに追加できます `new_disk_models.txt` ファイルを作成し、収集を再度実行します。

このタスクについて

OnCommand Insight 取得によるストレージデバイスのポーリングの一環として、ストレージデバイス上のディスクモデルが読み取られます。Insightで認識されない新しいディスクモデルがベンダーによってアレイに追加された場合や、Insightで検索するモデル番号とストレージデバイスから返されるモデル番号が一致していない場合は、エラーが発生してそのデータソースの取得に失敗します。このエラーを回避するには、Insightで認識されるディスクモデルの情報を更新する必要があります。アップデート、パッチ、メンテナンスリリースによって新しいディスクモデルがInsightに追加されます。ただし、パッチや更新を待たずに、この情報を手動で更新することもできます。

OnCommand Insight はディスクモデルファイルを5分ごとに読み取るため、入力した新しいデータモデル情報は自動的に更新されます。変更を有効にするためにサーバを再起動する必要はありませんが、サーバとRemote Acquisition Unit（RAU）を再起動すると、次回の更新前に変更を有効にすることができます。

ディスクモデルの更新がに追加されます `new_disk_models.txt` ファイルはにありま す`<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` ディレクトリ。を更新する前に、新しいディスクモデルの説明に必要な情報を確認しておきます `new_disk_models.txt` ファイル。ファイル内の情報が不正確な場合、誤ったシステムデータが生成され、取得に失敗する可能性があります。

Insightのディスクモデルを手動で更新するには、次の手順に従います。

手順

1. ディスクモデルの適切な情報を確認します。
2. テキストエディタを使用してを開きます `new_disk_models.txt` ファイル。
3. 新しいデータソースの必要な情報を追加します。
4. ファイルをに保存します `<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` サーバ上のディレクトリ。
5. をバックアップします `new_disk_models.txt` ファイルを安全な場所に保存します。以降のOnCommand Insight アップグレードでは、このファイルは上書きされます。アップグレードしたファイルにディスクモデル情報がない場合は、その情報を再入力する必要があります。

ディスクモデルの情報を確認するには、ベンダーとモデル番号を特定し、インターネットで検索します。

このタスクについて

ディスクモデルの情報は、インターネットで検索するだけで簡単に見つけることができます。検索する前に、ベンダー名とディスクモデル番号をメモしておいてください。

手順

1. インターネットでベンダー、モデル、ドキュメントタイプ「`pdf`」の高度な検索を使用して、ベンダーのデータシートやドライブのインストールガイドを検索することをお勧めします。通常、これらのデータシートは、ベンダーディスク情報の最良のソースです。
2. ベンダーの仕様では、完全なモデル番号に基づいて、必要なすべての情報が提供されるとは限りません。多くの場合、ベンダーのサイトでモデル番号の文字列のさまざまな部分を検索して、すべての情報を見つけると便利です。
3. OnCommand Insight で新しいディスクモデルを定義するには、ディスクのベンダー名、完全なモデル番号、ディスクのサイズと速度、およびインターフェイスタイプを確認します。次の表に記載されている情報を参考にしてください。

このフィールド：	これは次のとおりです。	入力内容：
モデル番号（別名キー）	必須	
ベンダー	必須	
ディスク速度（rpm）	必須	
サイズ（GB）	必須	
インターフェイスタイプ（1つ選択）	必須	ATA、SATA、SATA2、SATA3、FC、 SAS、FATA、SSD、その他
シーク時間（ミリ秒）	任意。	
最大転送速度（MB/秒）	任意。	
インターフェイスの転送速度（MB/秒）	任意。	
ベンダー/モデル情報へのリンク	オプションですが、推奨されます	

4. にその情報を入力します `new_disk_models.txt` ファイル。を参照してください "new_disk_models.txt ファイルの内容" 形式、順序、および例については、を参照してください。

new_disk_models.txtファイルの内容

。 `new_disk_models.txt` ファイルには必須フィールドとオプションフィールドがあります。フィールドはカンマで区切られているため、フィールド内にカンマを使用しないでください。

シーク時間、転送速度、および追加情報を除くすべてのフィールドが必須です。該当する場合は、ベンダー/モデルのWebサイトのリンクを[additional_info]フィールドに含めます。

テキストエディタを使用して、追加する新しいディスクモデルごとに、次の情報をこの順序でカンマで区切って入力します。

1. キー：モデル番号を使用します（必須）
2. ベンダー:名前(必須)
3. モデル番号：完全な番号（通常は「キー」と同じ値）（必須）
4. *ディスクのrpm *：例：10000または15000（必須）
5. サイズ：容量（GB）（必須）
6. インターフェイスタイプ：ATA、SATA、FC、SAS、FATA、 SSD、その他（必須）
7. シーク時間：ミリ秒（オプション）
8. 潜在的な転送速度：潜在的な転送速度（MB/秒）。ディスク自体の最大転送速度。（オプション）
9. インターフェイスの転送速度：ホストとの間の転送速度（MB/秒）（オプション）。
10. 追加情報：キャプチャする任意の追加情報 。仕様が掲載されているベンダーのページへのリンクを入力して参照することを推奨します（オプション）。

オプションのフィールドを空白のままにする場合は、必ずカンマを含めてください。

例（スペースなしで1行に1つずつ）：

```
ST373405,Seagate,ST373405,10000,73,FC,5.3,64,160,http://www.seagate.com/staticfiles/support/disc/manuals/enterprise/cheetah/73(LP)/100109943e.pdf

SLR5B-M400SS,HITACHI,SLR5B-M400SS,1000000,400,SSD,,,,

X477_THARX04TA07,TOSHIBA,X477_THARX04TA07,7200,4000,SATA,9.5,,,https://storage.toshiba.eu/export/sites/toshiba-sdd/media/products/datasheets/MG03ACAxxxY.pdf
```

環境の監視

Insightを使用すると、環境の問題を防止し、潜在的な問題を迅速にトラブルシューティングできます。

アセットページのデータ

アセットページには、パフォーマンスのトラブルシューティングに関するデータが表示されます。ベースアセット（仮想マシンやボリュームなど）とそのアセットに関連する

アセット（ストレージプール、ストレージノード、接続されているスイッチポートなど）の概要と、追加情報 へのリンクが表示されます。

OnCommand Insight 7.3.1以降では、すべてのアセットページに*メイン*ページと*追加データ*ページがあります。[Main]ページには、アセットの概要が表示され、グラフやトポロジなどの情報が表示されるセクションがあります。[Additional data]ページでは、現在のアセットタイプに合わせてカスタマイズ可能なダッシュボードページを設定できます。

アセットページのメインタブで、線やメッセージの横に赤い丸が表示されている場合は、監視対象の環境に問題がある可能性があります。

アセットページのタイプ

アセットページには、アセットの現在のステータスの概要と、アセットと関連するアセットに関する追加情報へのリンクが表示されます。

OnCommand Insight には、次のアセットのアセットページが用意されています。

- 仮想マシン
- ボリューム
- 内部ボリューム
- 物理ホスト
- ストレージプール
- ストレージ
- データストア
- ハイパーバイザー
- アプリケーション
- ストレージノード
- qtree
- ディスク
- VMDK です
- ポート
- スイッチ
- ファブリック
- オブジェクトストレージ（Atmos、Centera、Amazon S3など）
- ゾーン

マッピングとマスキングの情報は、[Zone]、[Volume]、[VM]、および[Host/Hypervisor]アセットページの表で確認できます。

オブジェクトストレージアセットの概要情報は表示されますが、この情報には[データソース]詳細ページからしかアクセスできません。

環境内で特定のアセットを検索しています

検索機能を使用すると、特定のアセットに関する情報を確認できます。たとえば、システムユーザから特定のサーバに関する苦情がストレージ管理者に問い合わせられた場合、管理者はサーバ名を検索して、ステータスの概要と追加のリンク情報を示すアセットページを表示できます。

手順

1. OnCommand InsightWeb UIを開きます。
2. ツールバーのをクリックします 。

   [アセットの検索]ボックスが表示されます。
3. アセットの名前または名前の一部を入力します。
4. 検索結果から目的のリソースを選択します。

   そのリソースのアセットページが表示されます。

高度な検索技術

監視対象環境内のデータやオブジェクトを検索する場合は、複数の検索手法を使用できます。

ワイルドカード検索

文字を使用して、複数文字のワイルドカード検索を実行できます。たとえば、_applic*n_と指定すると、applicationが返されます。

検索で使用されるフレーズ

フレーズは、二重引用符で囲まれた単語のグループです（例：「Paw VNX LUN 5」）。二重引用符を使用して、名前または属性にスペースを含むドキュメントを検索できます。

ブール演算子

ブール演算子を使用すると、複数の用語を組み合わせて、より複雑なクエリを作成できます。

- または
  - OR 演算子は、デフォルトの結合演算子です。

    2 つのキーワードの間にブール演算子がない場合は、 OR 演算子が使用されます。
  - OR 演算子は、 2 つのキーワードをリンクし、どちらかの条件がドキュメントに存在する場合に一致するドキュメントを検索します。

    たとえば、「storage or netapp」と指定すると、「storage」または「netapp」のいずれかを含むドキュメントが検索されます。

◦ 一致するキーワードの数が多いドキュメントほどスコアが高くなります。

- および

  AND 演算子を使用すると、両方の検索語が 1 つのドキュメント内に存在するドキュメントを検索できます。たとえば、「auroraとnetapp」と指定すると、「storage」と「netapp」の両方を含むドキュメントが検索されます。

  単語との代わりに記号&&を使用できます。

- ではありません

  NOT 演算子を使用すると、 NOT のあとのキーワードを含むすべてのドキュメントが検索結果から除外されます。たとえば、「strage not netapp」と指定すると、「strage」のみを含むドキュメントが検索され、「netapp」は検索されません。

  記号を使用できます。「NOT」という単語の代わりに。

プレフィックスとサフィックスの検索

- 検索文字列の入力を開始するとすぐに、検索エンジンによってプレフィックスとサフィックスの検索が実行され、最も一致するものが検索されます。
- 完全一致は、プレフィックスまたはサフィックスの一致よりもスコアが高くなります。スコアは、検索語と実際の検索結果との距離に基づいて計算されます。たとえば、「aurora」、「aurora1」、「aurora11」の3つのストレージがあるとします。「aur」を検索すると、3つのストレージすべてが返されます。ただし、接頭辞検索文字列との距離が最も近いため、「オーロラ」の検索結果のスコアが最も高くなります。
- また、検索エンジンは逆の順序で用語を検索します。これにより、接尾辞検索を実行できます。たとえば、検索ボックスに「345」と入力すると、検索エンジンは「345」を検索します。
- 検索では大文字と小文字は区別されません。

インデックスキーワードを使用して検索します

インデックスキーワードの数が多い検索では、スコアが高くなります。

検索文字列は、スペースで複数の検索キーワードに分けて表示されます。たとえば、「strage aurora netapp」という検索文字列は、「strage」、「aurora」、「netapp」の3つのキーワードに分割されます。3つのキーワードをすべて使用して検索が実行されます。これらのキーワードのほとんどに一致するドキュメントのスコアが最も高くなります。入力する情報が多いほど、検索結果の方が適しています。たとえば、ストレージの名前とモードでストレージを検索できます。

検索結果は、カテゴリごとに上位 3 件まで表示されます。想定していたドキュメントが見つからなかった場合は、検索文字列にキーワードを追加して検索結果を向上させることができます。

次の表に、検索文字列に追加できるインデックスキーワードのリストを示します。

カテゴリ	インデックスキーワード

ストレージ	• "ストレージ" • 名前 • ベンダー • モデル
ストレージプール	• “stragepool” • 名前 • ストレージの名前 • ストレージのIPアドレス • ストレージのシリアル番号 • ストレージベンダー • ストレージモデル • 関連付けられているすべての内部ボリュームの名前 • 関連付けられているすべてのディスクの名前
内部ボリューム	• "`internalvolume"' • 名前 • ストレージの名前 • ストレージのIPアドレス • ストレージのシリアル番号 • ストレージベンダー • ストレージモデル • ストレージプールの名前 • 関連付けられているすべての共有の名前 • 関連付けられているすべてのアプリケーションとビジネスエンティティの名前

ボリューム	• '"ボリューム"' • 名前 • ラベル • すべての内部ボリュームの名前 • ストレージプールの名前 • ストレージの名前 • ストレージのIPアドレス • ストレージのシリアル番号 • ストレージベンダー • ストレージモデル
ストレージノード	• 「Stragenode」 • 名前 • ストレージの名前 • ストレージのIPアドレス • ストレージのシリアル番号 • ストレージベンダー • ストレージモデル
ホスト	• "ホスト"" • 名前 • IP アドレス • 関連付けられているすべてのアプリケーションとビジネスエンティティの名前
データストア	• 「データストア」 • 名前 • Virtual Center IPの略 • すべてのボリュームの名前 • すべての内部ボリュームの名前

仮想マシン	• "`virtualmachine'" • 名前 • DNS名 • IP アドレス • ホストの名前 • ホストのIPアドレス • すべてのデータストアの名前 • 関連付けられているすべてのアプリケーションとビジネスエンティティの名前
スイッチ（標準と NPV ）	• "スイッチ" • IP アドレス • WWN • 名前 • シリアル番号 • モデル • ドメインID • ファブリックの名前 • ファブリックのWWN
アプリケーション	• "`application'" • 名前 • テナント • 基幹業務部門 • ビジネスユニット • プロジェクト
テープ	• "`tape'" • IP アドレス • 名前 • シリアル番号 • ベンダー
ポート	• "ポート" • WWN • 名前

ファブリック	• 「ファブリック」 • WWN • 名前

表示されるデータの時間範囲の変更

デフォルトでは、アセットページには過去24時間のデータが表示されますが、別の固定時間またはカスタムの期間を選択して表示するデータのセグメントを変更することができます。

このタスクについて

アセットの種類に関係なく、すべてのアセットページに表示されるオプションを使用して、データを表示する期間を変更することができます。

手順

1. OnCommand InsightWeb UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。
   - Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。
   - をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。
3. ページの左上隅で、次のいずれかの時間アイコンをクリックして、表示されるデータのセグメントを変更します。
   - * 3時間*

     過去3時間のデータが表示されます。
   - * 24時間*

     過去24時間のデータが表示されます。
   - * 3D *

     過去3日間のデータが表示されます。
   - * 7d *

     過去7日間のデータが表示されます。
   - * 30d *

     過去30日間のデータが表示されます。
   - カスタム

カスタムの期間を選択できるダイアログボックスが表示されます。一度に最大31日分のデータを表示できます。

4. [カスタム]*を選択した場合は、次の手順を実行します。
   a. 日付フィールドをクリックし、開始日の月、日、年を選択します。
   b. 時刻リストをクリックし、開始時刻を選択します。
   c. 終了データと終了時刻について、手順aとbの両方を繰り返します。
   d. をクリックします 。

データソースのデータ収集ステータスの確認

データソースはInsightの主要な情報源であるため、必ず実行状態を維持する必要があります。

データソースのデータ収集ステータスは、直接取得したすべてのアセットのすべてのアセットページで確認できます。次のいずれかの状況が発生する可能性があります。アセットページの右上にステータスが表示されます。

- データソースから正常に取得されました

  ステータス"`Acquired"を表示します `xxxx``", where `xxxx` アセットのデータソースの最新の取得時刻を示します。

- 取得エラーが発生しました。

  ステータス"`Acquired"を表示します `xxxx``", where `xxxx` アセットの1つ以上のデータソースの最新の取得時刻を示します ⚠ 。をクリックします ⚠ には、アセットの各データソース、データソースのステータス、および前回のデータ取得日時が表示されます。データソースをクリックすると、データソースの詳細ページが表示されます。

アセットが直接取得されていない場合は、ステータスは表示されません。

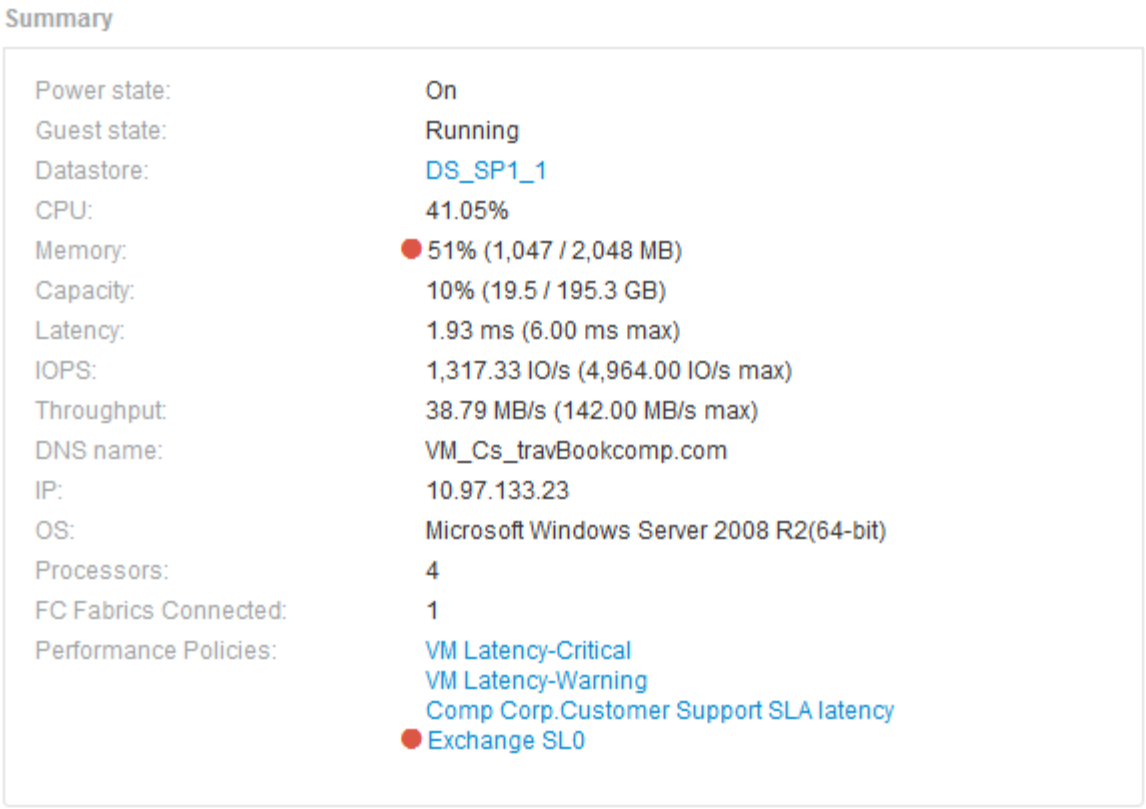
アセットページのセクション

アセットページには、アセットに関連する情報を含む複数のセクションが表示されます。表示されるセクションはアセットのタイプによって異なります。

まとめ

アセットページの[Summary]セクションには、特定のアセットに関する情報の概要とそのアセットに関連する問題が赤い丸で示されます。関連するアセットに関する追加情報へのハイパーリンクと、アセットに割り当てられているパフォーマンスポリシーへのハイパーリンクが表示されます。

次の例は、仮想マシンのアセットページの[Summary]セクションに表示される情報の一部を示しています。横に赤い丸が表示されている項目は、監視対象の環境に潜在的な問題があることを示しています。



[Summary]セクションを使用します

[Summary]セクションでは、アセットに関する全般的な情報を確認できます。具体的には、指標（メモリ、容量、レイテンシなど）やパフォーマンスポリシーが「原因 for Concern」であるかどうかを確認すると便利です。OnCommand Insight では、指標やパフォーマンスポリシーの横に赤い丸が表示されています。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。
   - Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。
   - をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。

   [Summary]セクションに表示される情報は、表示しているアセットページのタイプによって異なります。
3. いずれかのアセットのリンクをクリックすると、対応するアセットページを表示できます。

   たとえば、ストレージノードを表示している場合は、リンクをクリックして関連付けられているストレージのアセットページを表示したり、をクリックしてHAパートナーのアセットページを表示したりできます。

4. アセットに関連付けられている指標を表示できます。

   指標の横に赤い丸が表示されている場合、診断や解決を要する潜在的な問題があることを示しています。

   一部のストレージアセットについて、ボリュームの容量の表示が 100% を超えることがあります。これは、ボリュームの容量に関するメタデータが使用済み容量としてアセットから報告されるためです。

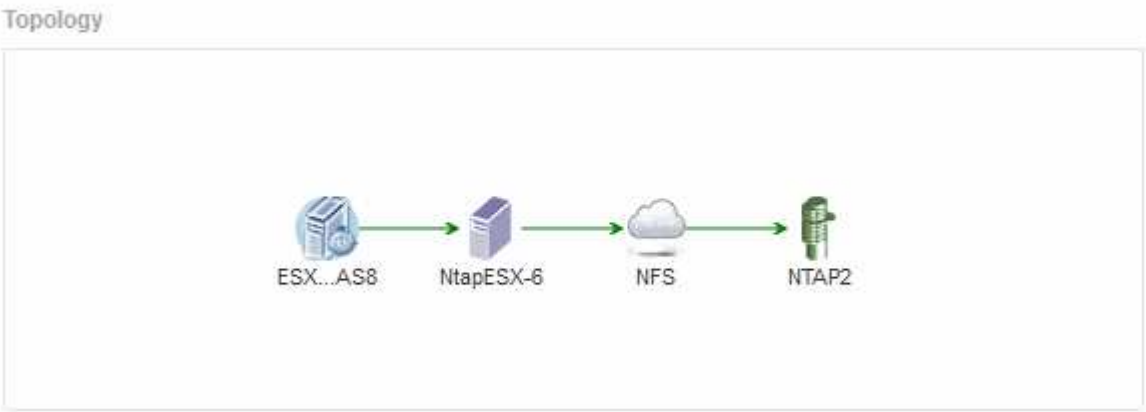
5. 該当する場合、パフォーマンスポリシーのリンクをクリックして、アセットに関連付けられているパフォーマンスポリシーを表示できます。

   パフォーマンスポリシーの横に赤い丸が表示されている場合、アセットがパフォーマンスポリシーで定義されたしきい値を超えていることを示しています。パフォーマンスポリシーを調べて、問題 を詳しく診断する必要があります。

トポロジ

[Topology]セクション（該当するアセットがある場合）では、ベースアセットとそれに関連するアセットがどのように接続されているかを確認できます。

次の例は、仮想マシンのアセットページの[Topology]セクションに表示される内容を示しています。



アセットのトポロジがセクションに収まらない場合は、代わりに*リンクをクリックしてトポロジを表示*ハイパーリンクが表示されます。

[Topology]セクションを使用します

[Topology]セクションでは、ネットワーク内のアセットの相互接続状況を確認したり、関連するアセットに関する情報を表示したりできます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。

   - Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。

◦ をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。[Topology]セクションはアセットページの右上にあります。

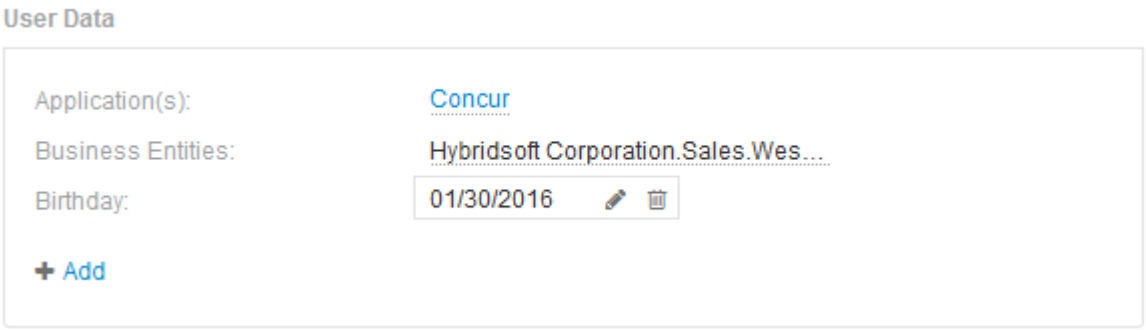
アセットのトポロジがセクションに収まらない場合は、*クリックリンクをクリックしてトポロジ*ハイパーリンクを表示します。

3. ベースアセットに関連するアセットの詳細を確認するには、トポロジで関連するアセットにカーソルを合わせ、名前をクリックします。アセットページが表示されます。

ユーザデータ

アセットページの[User Data]セクションには、ユーザが定義したアプリケーション、ビジネスエンティティ、アノテーションなどのデータが表示されます。

仮想マシンのアセットページの[User Data]セクションにアプリケーション、ビジネスエンティティ、およびアノテーションが割り当てられている場合の表示例を次に示します。



User Data セクションを使用してアプリケーションを割り当てまたは変更する

環境で実行されているアプリケーションを特定のアセット（ホスト、仮想マシン、ボリューム、内部ボリューム、ハイパーバイザー）に割り当てることができます。[User Data]セクションでは、アセットに割り当てられているアプリケーションを変更したり、アプリケーションや追加のアプリケーションをアセットに割り当てたりできます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。
   ◦ Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。
   ◦ をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。
3. 次の操作を実行できます。
   ◦ アプリケーションのアセットページを表示するには、アプリケーションの名前をクリックします。
   ◦ 割り当てられているアプリケーションを変更したり、アプリケーションや追加のアプリケーションを割り当てたりするには、アプリケーション名（アプリケーションが割り当てられている場合）にカーソルを合わせ、アプリケーションが割り当てられていない場合は*なし*にカーソルを合わせて、をクリックします を入力してアプリケーションを検索するか、リストからアプリケーションを選択し、

をクリックします 。

ビジネスエンティティに関連付けられているアプリケーションを選択した場合は、ビジネスエンティティがアセットに自動的に割り当てられます。この場合、ビジネスエンティティの名前にカーソルを合わせると、_derived_と 表示されます。エンティティをアセットに対してのみ保持し、関連付けられているアプリケーションを保持しない場合は、アプリケーションの割り当てを手動で上書きできます。

- アプリケーションを削除するには、をクリックします 。

[User Data]セクションを使用してビジネスエンティティを割り当てまたは変更する

ビジネスエンティティを定義して、環境のデータをより細かく追跡し、レポートすることができます。アセットページの[User Data]セクションで、アセットに割り当てられているビジネスエンティティを変更したり、アセットからビジネスエンティティを削除したりできます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。
   - Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。
   - をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。
3. 次の操作を実行できます。
   - 割り当てられたエンティティを変更するか、エンティティを割り当てるには、をクリックします をクリックし、リストからエンティティを選択します。
   - ビジネスエンティティを削除するには、をクリックします 。

> アセットに割り当てられているアプリケーションから派生したエンティティを削除することはできません。

User Data セクションを使用して、注釈を割り当てまたは変更する

企業の要件に合わせてデータを追跡するようにOnCommand Insight をカスタマイズする場合は、_annotations_という特殊なメモを定義してアセットに割り当てることができます。アセットページの User Data セクションには、アセットに割り当てられているアノテーションが表示されます。また、そのアセットに割り当てるアノテーションを変更することもできます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。

- Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。
- をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。

3. アセットページの*[User Data]*セクションで、をクリックします + Add 。

   [注釈の追加] ダイアログボックスが表示されます。

4. [注釈（Annotation）]*をクリックし、リストから注釈を選択します。
5. [値]*をクリックし、選択したアノテーションのタイプに応じて次のいずれかを実行します。
   - アノテーションタイプがリスト、日付、またはブーリアンの場合は、値をリストから選択します。
   - アノテーションタイプがテキストの場合は、値を入力します。
6. [保存（ Save ）] をクリックします。

   アセットにアノテーションが割り当てられ、クエリでアノテーションに基づいてアセットをフィルタできるようになります。

7. アノテーションの割り当て後に値を変更する場合は、をクリックします 別の値を選択します。

   アノテーションのリストタイプで*[アノテーションの割り当て時に動的に値を追加する]*オプションが選択されている場合は、既存の値を選択するだけでなく、新しい値を入力して追加することもできます。

エキスパートビュー

アセットページの[Expert View]セクションでは、選択した期間（3時間、24時間、3日間、7日間、 またはカスタム期間）を使用してパフォーマンスチャートとそれに関連するアセットを表示します。

次の例は、ボリュームのアセットページの[Expert View]セクションを示しています。

選択した期間について、パフォーマンスチャートで表示する指標を選択することができます。

[Resources]セクションに、ベースアセットの名前とパフォーマンスチャートでの色が表示されます。[Top Correlated]セクションに表示するアセットが表示されない場合は、[Additional resources]セクションの*[Search assets]*ボックスを使用してアセットを検索し、パフォーマンスチャートに追加できます。リソースを追加すると、 [追加リソース] セクションにリソースが表示されます。

ベースアセットに関連するアセットがある場合、それらのアセットもリソースセクションに次のカテゴリ別に表示されます。

- 関連性が高い

  1 つ以上のパフォーマンス指標との関連性が高いアセット（割合）がベースアセットに表示されます。

- 上位貢献者

  ベースアセットへの影響が大きいアセットが表示されます。

- Greedy

  に、ホスト、ネットワーク、ストレージなど、同じリソースの共有を通じてアセットからシステムリソースを引き継ぐアセットを示します。

- デグレード

  このアセットにシステムリソースを奪われているアセットが表示されます。

エキスパートビューの指標の定義

アセットページのエキスパートビューセクションには、アセットに対して選択した期間に関する複数の指標が表示されます。各指標は独自のパフォーマンスチャートに表示されます。確認が必要なデータに応じて、チャートに表示する指標や関連するアセットを追加したり削除したりできます。

メートル法	説明
BB クレジットのゼロ受信、転送	サンプリング期間中に受信 / 送信のバッファ間クレジット数がゼロになった回数。この指標は、接続されたポートで提供できるクレジットを使い果たしたために転送が中止された回数を表します。
BB クレジットのゼロ期間の転送	サンプリング期間中に送信 BB クレジットがゼロになっていた時間（ミリ秒）。
キャッシュヒット率（合計、読み取り、書き込み）	キャッシュにヒットする要求の割合。ボリュームへのアクセス数に対するヒット数の割合が高いほど、パフォーマンスが高くなります。この列は、キャッシュヒット情報を収集しないストレージアレイについては空になります。
キャッシュ使用率（合計）	キャッシュにヒットするキャッシュ要求の合計割合

クラス 3 は破棄されます	ファイバチャネルのクラス 3 データ転送が破棄された回数。
CPU 利用率（合計）	使用可能な合計（すべての仮想 CPU ）に対する使用中のアクティブな CPU リソースの割合。
CRC エラーです	サンプリング期間中にポートで無効な Cyclic Redundancy Check （ CRC ；巡回冗長検査）が検出されたフレーム数
フレームレート	転送フレームレート（ 1 秒あたりのフレーム数）。
フレームサイズ平均（ Rx 、 Tx ）	フレームサイズに対するトラフィックの比率。この指標から、ファブリック内にフレームのオーバーヘッドがないかどうかを特定できます。
フレームサイズが長すぎます	ファイバチャネルの長すぎるデータ転送フレームの数。
フレームサイズが短すぎます	ファイバチャネルの短すぎるデータ転送フレームの数。
I/O 密度（合計、読み取り、書き込み）	ボリューム、内部ボリューム、またはストレージ要素の使用済み容量（データソースの最新のインベントリポーリングから取得）で IOPS を割った値。1 秒間の TB あたりの I/O 処理数で測定されます。
IOPS （合計、読み取り、書き込み）	I/O チャネルまたはそのチャネルの一部を通過する読み取り / 書き込み I/O サービス要求の単位時間あたりの数（ 1 秒あたりの I/O 数で測定）
IP スループット（合計、読み取り、書き込み）	合計： IP データの転送および受信速度の合計。 1 秒あたりのメガバイト数で示されます。Read：IP Throughput（Receive）：IPデータの平均受信速度（1秒あたりのメガバイト数）。 Write：IP Throughput（Transmit）：IPデータの平均転送速度（1秒あたりのメガバイト数）。
レイテンシ（合計、読み取り、書き込み）	Latency （ R&W ）：一定の時間内にデータが仮想マシンに対して読み取りまたは書き込みされるレート。1 秒あたりのメガバイト数で測定されます。 Latency：データストア内の仮想マシンからの平均応答時間。 Top Latency：データストア内の仮想マシンからの最大応答時間。

リンク障害です	サンプリング期間中にポートで検出されたリンク障害の数。
リンクリセット Rx 、 Tx	サンプリング期間中に受信または送信されたリセットリンクの数。この指標は、このポートに対して接続されたポートから発行されたリンクリセットの数を表します。
メモリ使用率（合計）	ホストで使用されるメモリのしきい値。
部分的 R/W （合計） %	RAID 5 、 RAID 1/0 、または RAID 0 の LUN において、読み取り / 書き込み処理がディスクモジュールのストライプ境界を越えた合計回数。通常、ストライプを越えると、各 LUN で追加の I/O が必要になるため、ストライプを越えることは効果がありませんこの割合が低いほど、ストライプ要素のサイズは効率的であり、ボリューム（ネットアップの LUN ）のアライメントは不適切であることを示します。 CLARiX については、ストライプを越えた回数を IOPS の合計で割った値が示されます。
ポートエラーです	サンプリング期間中または一定の期間に検出されたポートエラーのレポート。
信号損失回数	信号損失エラーの数。信号損失エラーが発生した場合は、電気的接続がなく、物理的な問題があります。
スワップレート（合計レート、インレート、アウトレート）	サンプリング期間中にディスクとアクティブメモリの間にスワップイン速度、スワップアウト速度、またはその両方が発生した速度。これは環境仮想マシンのカウンタです。
同期損失の数	同期損失エラーの数同期損失エラーが発生した場合、ハードウェアはトラフィックを認識できないか、ロックオンされません。すべての機器のデータ速度が同じでないか、光接続または物理接続の品質が低下している可能性があります。このエラーが発生するたびにポートの再同期が必要になるため、システムのパフォーマンスに影響します。単位は KB/秒です
スループット（合計、読み取り、書き込み）	I/O サービス要求への応答として一定の時間内に送受信されたデータのレート（ 1 秒あたりの MB で測定）。
タイムアウト廃棄フレーム数 - Tx	送信フレームがタイムアウトで破棄された回数。

トラフィック速度（合計、読み取り、書き込み）	サンプリング期間中に送受信されたトラフィックの量（ 1 秒あたりのメビバイト数）。
トラフィック利用率（合計、読み取り、書き込み）	サンプリング期間中の送受信トラフィックの比率、受信 / 送信 / 合計容量に対するトラフィックの比率。
利用率（合計、読み取り、書き込み）	送信（ Tx ）と受信（ Rx ）に使用できる帯域幅の割合。
書き込み保留（合計）	保留中の書き込み I/O サービス要求の数。

[エキスパートビュー（ **Expert View** ） **]** セクションの使用

エキスパートビューのセクションでは、選択した期間中に適用可能な任意の数の指標に基づいてアセットのパフォーマンスチャートを表示し、関連するアセットを追加してアセットと関連するアセットのパフォーマンスをさまざまな期間で比較および比較できます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。
   - Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。
   - をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。デフォルトでは、パフォーマンスチャートには、アセットページで選択した期間についての 2 つの指標のデータが表示されます。たとえば、ストレージの場合は、レイテンシと合計 IOPS がデフォルトで表示されます。リソースセクションには、リソースの名前とその他のリソースセクションが表示されます。ここでは、アセットを検索できます。アセットによっては、関連性の高いアセット、影響のあるリソース、 Greedy リソース、 Dedgraded セクションにアセットが表示されることもあります。
3. [Select metrics to show]*をクリックし、指標を選択してその指標のパフォーマンスチャートを追加できます。

   選択した指標のパフォーマンスチャートが追加されます。グラフには、選択した期間のデータが表示されます。期間を変更するには、アセットページの左上にある別の期間をクリックします。

   この手順をもう一度実行し、をクリックして指標をクリアできます。その指標のパフォーマンスチャートが削除されます。
4. グラフにカーソルを合わせ、アセットに応じて次のいずれかをクリックすると、表示される指標データを変更できます。
   - 読み取り*または*書き込み
   - **Tx**または*Rx** Total*がデフォルトです。
5. グラフ上でカーソルをドラッグしてデータポイントを選択すると、選択した期間における指標の値の変化を確認できます。

6. [リソース]セクションでは、次のいずれかの方法で関連するアセットをパフォーマンスチャートに追加できます（該当する場合）。

   - [Top correlated]、[Top contributors]、[Greedy]、または[Degraded]の各セクションで関連するアセットを選択すると、選択した各指標のパフォーマンスチャートにそのアセットのデータを追加できます。資産が表示されるには、最低15%の相関関係または貢献度が必要です。

     アセットを選択すると、そのアセットのグラフ上のデータポイントと同じ色のブロックがアセットの横に表示されます。

   - 表示されているアセットの名前をクリックすると、そのアセットページが表示されます。また、ベースアセットに対するアセットの関連性や影響度の割合をクリックすると、ベースアセットとアセットの関連性に関する詳細を確認できます。

     たとえば、関連性が高いアセットの横にある関連性の数値をクリックすると、ベースアセットとの関連性についてタイプ別に比較した情報メッセージが表示されます。

   - 比較のためにパフォーマンスチャートに表示したいアセットが[Top correlated]セクションに表示されない場合は、[Additional resources]セクションの*[Search assets]*ボックスを使用して他のアセットを検索できます。アセットを選択すると、[Additional resources]セクションにそのアセットが表示されます。アセットの情報の表示を中止する場合は、をクリックします 。

関連資産

該当する場合、アセットページに[Related Assets]セクションが表示されます。たとえば、ボリュームのアセットページには、ストレージプール、接続されているスイッチポート、コンピューティングリソースなどのアセットに関する情報が表示される場合があります。各セクションには、そのカテゴリに関連するアセットの表と対応するアセットページへのリンクが表示され、アセットに関連する複数のパフォーマンス統計が表示されます。

[Related Assets]セクションを使用します

[Related Assets]セクションでは、ベースアセットに関連するアセットを確認できます。関連する各アセットが、アセットの関連統計とともに表に表示されます。アセットの情報をエクスポートしたり、アセットの統計をエキスパートビューのパフォーマンスチャートで表示したり、関連するアセットの統計のみを表示するグラフを表示したりできます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。

   - Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。

   - をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。

3. 表でのアセットの表示方法を制御するには、次の手順に従います。

- 任意のアセットの名前をクリックして、そのアセットページを表示します。
- 特定のアセットのみを表示するには、* filter *ボックスを使用します。
- 表に5個を超えるアセットがある場合は、ページ番号をクリックしてページごとにアセットを参照できます。
- 列見出しで矢印をクリックすると、表内の列のソート順序を昇順（上矢印）または降順（下矢印）に変更できます。
- 関連するアセットを[Expert View]セクションのパフォーマンスチャートに追加するには、関連するアセットにカーソルを合わせてをクリックします 。

4. テーブルに表示されている情報をにエクスポートします `.csv` ファイル：
   a. をクリックします 。
   b. Microsoft Excelでファイルを開いて特定の場所に保存するには、**[ファイルを保存]***をクリックし、[OK]*をクリックしてファイルをダウンロードフォルダに保存します。

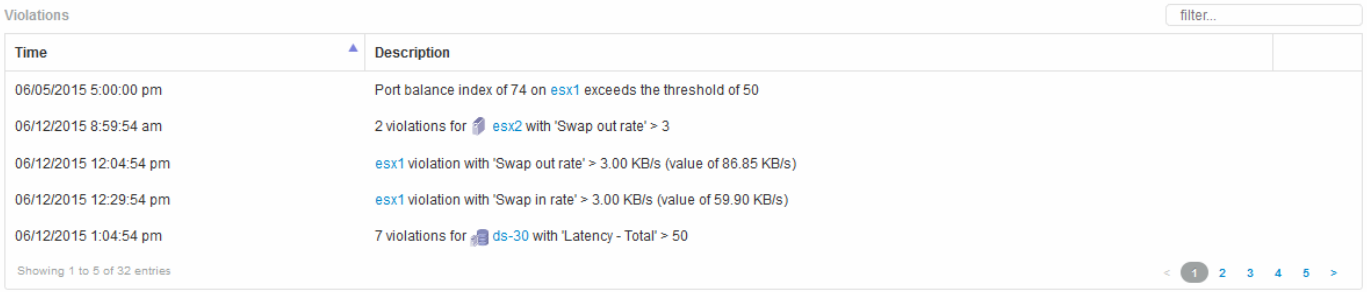
      表示用に現在選択されている列のすべてのオブジェクト属性がファイルにエクスポートされます。表示されている列の属性のみがエクスポートされます。テーブルの最初の10,000行だけがエクスポートされることに注意してください。

5. 関連するアセットの情報を表の下のグラフに表示するには、をクリックします 次のいずれかを実行します。
   - 表示される指標データを変更するには、**[読み取り]**、**[書き込み]**、または*をクリックします。 Total *がデフォルトです。
   - をクリックします 別の指標を選択します。
   - をクリックします グラフの種類を変更します。*折れ線グラフ*がデフォルトです。
   - グラフのデータポイントにカーソルを合わせると、関連する各アセットについて選択した期間における指標の値の変化を確認できます。
   - グラフの凡例で関連するアセットをクリックして、グラフに追加または削除します。
   - 関連する他のアセットをグラフに表示するには、関連するアセットの表でページ番号をクリックします。
   - をクリックします をクリックしてグラフを閉じます。

違反

アセットに割り当てたパフォーマンスポリシーに対する違反が環境で見つかった場合、アセットページの Violations セクションを使用して違反を確認できます。パフォーマンスポリシーではネットワークのしきい値を監視し、しきい値の違反を即座に検出してその影響を特定し、問題の影響と根本原因 を分析して迅速かつ効果的に修正できます。

次の例は、ハイパーバイザーのアセットページに表示される[Violations]セクションを示しています。



[Violations]セクションの使用

Violations セクションでは、アセットに割り当てたパフォーマンスポリシーの結果としてネットワークで発生したすべての違反を表示し、管理することができます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。
   - Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。
   - をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。[Violations]セクションには、違反が発生した時刻、しきい値を超えた概要 、および違反が発生したアセットへのハイパーリンクが表示されます（例：「2 violations fir DS-30 with Latency-Total >50」）。
3. 次のオプションのタスクを実行できます。
   - 特定の違反のみを表示するには、* filter *ボックスを使用します。
   - 表内の違反数が5個を超える場合は、ページ番号をクリックして各ページを参照できます。
   - 列見出しで矢印をクリックすると、表内の列のソート順序を昇順（上矢印）または降順（下矢印）に変更できます。
   - 概要でアセット名をクリックすると、そのアセットページが表示されます。赤い丸は詳しい調査が必要な問題を示しています。

     パフォーマンスポリシーをクリックすると、ポリシー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で、パフォーマンスポリシーを確認し、必要に応じて変更を加えることができます。

   - をクリックします 問題 が原因 for Concernではなくなったと判断した場合に、リストから違反を削除します。

カスタマイズ可能なアセットページ

各アセットページのカスタマイズ可能なウィジェットに追加のデータを表示できます。アセットのページをカスタマイズすると、そのタイプのすべてのアセットのページにカスタマイズが適用されます。

アセットページウィジェットをカスタマイズするには、次の操作を実行します。

1. ページにウィジェットを追加します
2. ウィジェットのクエリまたは式を作成して、目的のデータを表示します
3. 必要に応じてフィルタを選択します
4. ロールアップまたはグループ化の方法を選択します
5. ウィジェットを保存します
6. 必要なすべてのウィジェットについて、この手順を繰り返します
7. アセットページを保存します

カスタムのアセットページに変数を追加して、ウィジェットに表示するデータをさらに絞り込むこともできます。通常の変数に加えて、各アセットタイプでは一連の「$this」変数を使用して、現在のアセットに直接関連するリソースをすばやく特定できます。たとえば、現在の仮想マシンをホストしているのと同じハイパーバイザーでホストされているすべての仮想マシンなどです。

このカスタムアセットページは、ユーザごと、およびアセットタイプごとに一意です。たとえば、ユーザAが仮想マシンのカスタムアセットページを作成すると、そのユーザの仮想マシンのアセットページにそのカスタムページが表示されます。

ユーザが表示、編集、削除できるのは、自分で作成したカスタムアセットページのみです。

カスタムアセットページは、Insightのエクスポート/インポート機能には含まれません。

「**$this**」変数について説明します

カスタマイズ可能なアセットの[Additional data]ページでは、特殊な変数を使用して、現在のアセットに直接関連する追加情報 を簡単に表示できます。

このタスクについて

アセットのカスタマイズ可能なランディングページのウィジェットで「$this」変数を使用するには、次の手順を実行します。この例では、表ウィジェットを追加します。

> 「$this」変数は、アセットのカスタマイズ可能なランディングページでのみ有効です。Insightの他のダッシュボードでは使用できません。使用可能な「$this'」変数は、アセットタイプによって異なります。

手順

1. 目的のアセットのアセットページに移動します。この例では、仮想マシン（ VM ）のアセットページを選択します。クエリまたは検索を使用して VM を選択し、リンクをクリックしてその VM のアセットページに移動します。

   VM のアセットページが開きます。

2. **>**[Additional Virtual Machine data]*ドロップダウンをクリックして、そのアセットのカスタマイズ可能なランディングページに移動します。
3. [Widget]ボタンをクリックし、[Table Widget]*を選択します。

   編集用の表ウィジェットが開きます。デフォルトでは、すべてのストレージが表に表示されます。

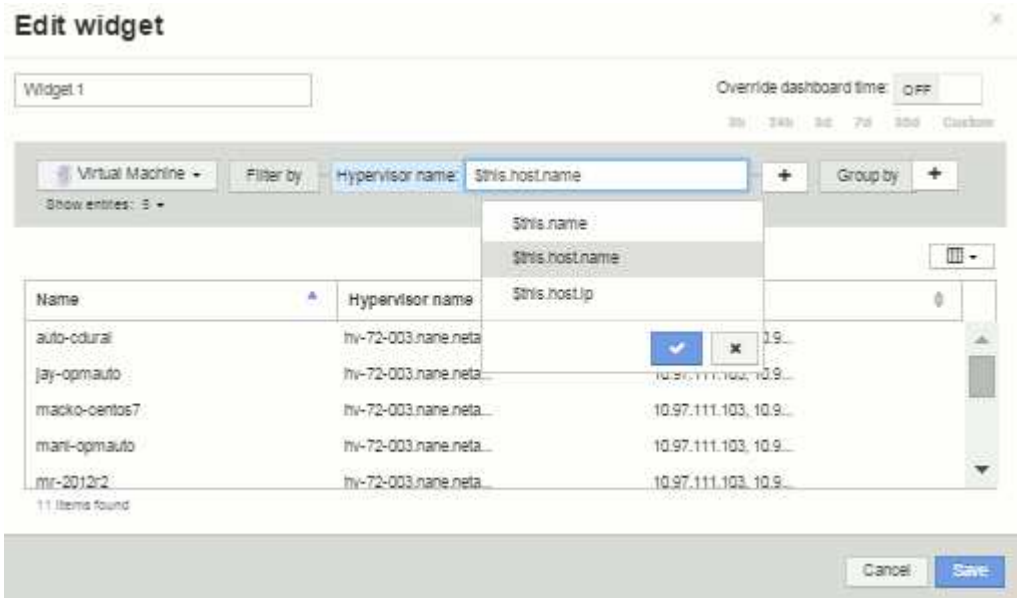
4. すべての仮想マシンを表示します。アセットセレクタをクリックし、**[**ストレージ**]***を[仮想マシン]*に変更します。

   これで、すべての仮想マシンが表に表示されます。

5. ボタンをクリックします そして、 hypervisor name *フィールドをテーブルに追加します。

   表内の VM ごとにハイパーバイザー名が表示されます。

6. 現在の VM をホストしているハイパーバイザーだけを表示します。フィールドの**[***+*]ボタンをクリックし、[hypervisor name]*を選択します。
7. をクリックし、$ this.host.name *変数を選択します。チェックボタンをクリックしてフィルタを保存します。



8. 表に、現在の VM のハイパーバイザーがホストしているすべての VM が表示されます。[保存（ Save ）]をクリックします。

結果

表示するすべてのVMのアセットページに対して、この仮想マシンのアセットページ用に作成した表が表示されます。ウィジェットで*$ this.host.name *変数を使用すると、現在のアセットのハイパーバイザーが所有するVMのみが表に表示されます。

ネットワークリソースの分散

負荷分散の問題を解決するには、アセットページで問題を特定し、使用率が低い大容量ボリュームを特定します。

手順

1. ブラウザでAssets Dashboardを開きます。
2. [Virtual Machines IOPS]ヒートマップで、非常に多くの箇所で問題が報告されているVMの名前を確認します。

3. VM名をクリックしてアセットページを表示します。
4. 概要でエラーメッセージを確認します。
5. パフォーマンスグラフ、特に関連性の高いリソースを確認して、競合状態の可能性があるボリュームを特定します。
6. パフォーマンスチャートにボリュームを追加してアクティビティのパターンを比較し、問題に関連した他のリソースのアセットページを表示します。
7. アセットページの一番下までスクロールして、VMに関連付けられているすべてのリソースのリストを確認します。大容量で実行されているVMDKをメモします。これが競合の原因となっている可能性があります。
8. 負荷分散の問題を解決するには、利用率の低いリソースを特定して利用率の高いリソースから負荷を受け取るか、負荷の高いリソースから負荷の低いアプリケーションを削除します。

ネットワークパフォーマンスの確認

ストレージ環境のパフォーマンスを調べて、利用率の低いリソースや利用率の高いリソースを特定し、リスクを未然に特定して問題に発展させることができます。

Insightを使用すると、収集したストレージのデータから明らかになったパフォーマンスや可用性の問題を解決または防止できます。

Insightを使用して、次のパフォーマンス管理タスクを実行できます。

- 環境全体のパフォーマンスを監視
- 他のデバイスのパフォーマンスに影響を与えるリソースを特定する

ポートの重要性

Insight ServerとData Warehouse（DWH）サーバを確実に動作させるには、いくつかのTCPポートを空けておく必要があります。これらのポートの一部は、localhostアダプタ（127.0.0.1）にバインドされたプロセスにのみ使用されますが、コアサービスが確実に動作するためには引き続き必要です。必要なポート数は、ネットワーク全体で使用されるポートのスーパーセットです。

Insight Serverのポート

Insight Serverには、ソフトウェアファイアウォールをインストールできます。開く必要がある「穴」は、以下のようになります。

*インバウンドHTTPS 443 *- Insight WebUIをTCP 443で実行している場合は、次のいずれかのユーザを許可するために、その情報を公開する必要があります。

- Web UIのInsightユーザ
- Remote Acquisition UnitがInsight Serverへの接続を要求しています
- このInsightサーバへのコネクタを備えたOCI DWHサーバ。
- Insight REST APIとのプログラムによるやり取り

Insight Serverのホストレベルのファイアウォール機能の実装を検討している方には、企業ネットワークのすべてのIPブロックへのHTTPSアクセスを許可することをお勧めします。

インバウンド**MySQL**（**TCP 3306**）。このポートは、コネクタを備えたInsight DWHサーバにのみ公開する必要があります

Insightには多数のデータコレクタがありますが、これらはすべてポーリングベースです。Insight Will原因 its Acquisition Unit（AUS）によって、さまざまなデバイスへのアウトバウンド通信が開始されます。ホストベースのファイアウォールが「ステートフル」で、リターントラフィックがファイアウォールを通過できるようになっている限り、Insight Serverのホストベースのファイアウォールはデータ取得に影響しません。

Data Warehouseのポート

Insight DWHサーバの場合：

*インバウンドHTTPS 443 *- Insight WebUIをTCP 443で実行している場合は、次のコンシューマを許可するためにこの情報を公開する必要があります。

- DWH管理ポータルのInsight管理ユーザ

インバウンド**HTTPS**（**TCP 9300**）- Cognosのレポートインターフェイスです。ユーザがCognosのレポートインターフェイスを操作する場合は、このインターフェイスをリモートで公開する必要があります。

DWHを公開する必要がない環境を想像できます。たとえば、レポートの作成者がDWHサーバにRDP接続し、DWHサーバでレポートを作成してスケジュールを設定し、すべてのレポートをSMTP経由で配信するか、リモートファイルシステムに書き込むようにスケジュール設定します。

インバウンド**MySQL**（**TCP 3306**）。このポートを公開する必要があるのは、DWHデータとMySQLベースの統合がある場合だけです。さまざまなDWHデータマートからデータを抽出して、CMDB、チャージバックシステムなどの他のアプリケーションに取り込みますか

PCパフォーマンスの低下を分析しています

ネットワークユーザからコンピュータの動作が遅いという苦情を受けた場合は、ホストのパフォーマンスを分析し、影響を受けるリソースを特定する必要があります。

作業を開始する前に

この例では、呼び出し元がホスト名を指定しています。

手順

1. ブラウザでInsightを開きます。
2. [Search assets]*ボックスにホスト名を入力し、検索結果でホスト名をクリックします。

   リソースの_assetページ_が開きます。

3. ホストのアセットページで、ページ中央のパフォーマンスチャートを確認します。通常は事前に選択されているレイテンシとIOPSに加えて、必要に応じてさまざまなタイプのデータを表示できます。デバイスタイプに応じて、スループット、メモリ、CPU、IPスループットなど、他のタイプのデータのチェックボックスをオンにします。
4. グラフ上のポイントの概要 を表示するには、そのポイントの上にマウスポインタを置きます。
5. また、ページ上部で期間を3時間から7日まで、または使用可能なすべてのデータを選択して変更することもできます。

6. [Top correlated resources]*のリストで、アクティビティパターンがベースリソースと同じリソースがほかにないかどうかを確認します。

   リストの最初のリソースは常にベースリソースです。

   a. 関連するリソースの横にあるリンクをクリックすると、IOPSとCPUのどちらのアクティビティパターンがベースリソースと別のリソースのどちらであるかを確認できます。

   b. 関連するリソースのチェックボックスをクリックして、そのデータをパフォーマンスチャートに追加します。

   c. 関連するリソースの名前をクリックすると、そのリソースのアセットページが表示されます。

7. VMの場合も同様に、*[Top correlated resources]*でストレージプールを探し、ストレージプール名をクリックします。

関連するリソースを分析しています

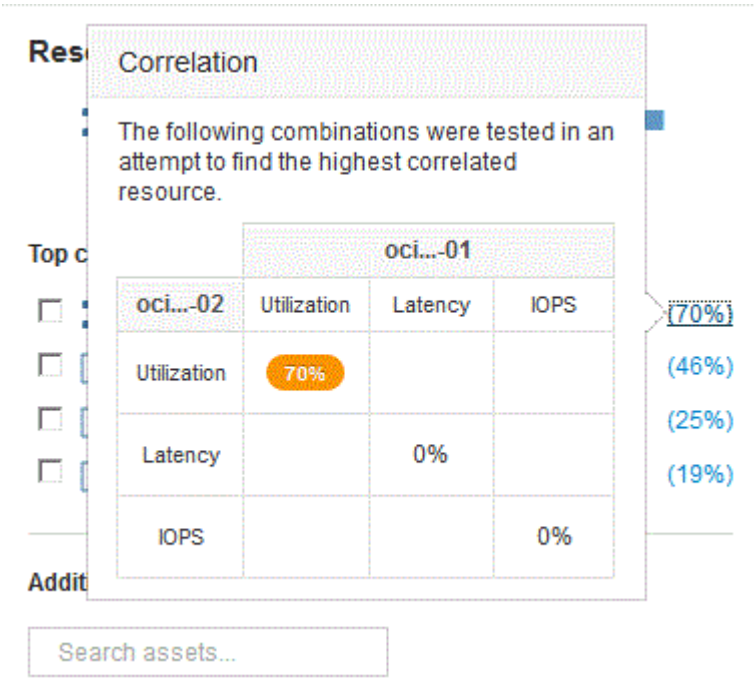
パフォーマンスの問題を調査するときにデバイスの_assetページ_を開くには、[Top correlated resources]リストを使用して、パフォーマンスチャートに表示されるデータを絞り込む必要があります。リソースの割合が高い場合は、リソースのアクティビティがベースリソースと同様であることを示します。

このタスクについて

パフォーマンスの問題を調査していて、デバイスのアセットページを開いたとします。

手順

1. [Top correlated resources]リストでは、最初のリソースがベースリソースです。リスト内の関連リソースは、アクティビティのうち最初のデバイスに対する割合でランク付けされます。関連性のリンクされたパーセンテージをクリックすると、詳細が表示されます。この例では、[Utilization]の関連性が70%になっているため、ベースリソースと関連するリソースの利用率はどちらも等しく高くなっています。



2. 関連するリソースをパフォーマンスチャートに追加するには、追加するリソースの*[Top correlated resources]*リストでチェックボックスを選択します。デフォルトでは、各リソースに使用可能な合計データが表示されますが、チェックボックスのメニューから[読み取りデータのみ]または[書き込みデータのみ]を選択できます。

   グラフでは、各リソースのパフォーマンス測定値を比較できるように、リソースごとに色が異なります。選択した測定メトリックについては、適切なタイプのデータのみがプロットされます。たとえば、CPUデータには読み取りや書き込みの指標は含まれないため、合計データのみが表示されます。

3. 関連するリソースの名前をクリックすると、そのリソースのアセットページが表示されます。
4. 分析で考慮すべきリソースが[Top correlated resources]に表示されない場合は、*[Search assets]*ボックスを使用してそのリソースを検索できます。

ファイバチャネル環境の監視

OnCommand Insightのファイバチャネルアセットページを使用して、環境内のファブリックのパフォーマンスとインベントリを監視し、原因 の問題の可能性がある変更を把握することができます。

Fibre Channelアセットページ

Insightのアセットページには、リソースに関する概要情報、トポロジ（デバイスとその接続）、パフォーマンスチャート、関連するリソースの表が表示されます。ファブリック、スイッチ、およびポートアセットのページを使用して、Fibre Channel環境を監視できます。ファイバチャネル問題 のトラブルシューティングを行う場合は、各ポートアセットのパフォーマンスチャートが特に役立ちます。このチャートには、最も影響が大きいポートのトラフィックが表示されます。また、バッファ間クレジットの指標やポートエラーも表示できます。Insightでは指標ごとに個別のパフォーマンスチャートが表示されます。

ポート指標のパフォーマンスポリシー

Insightでは、パフォーマンスポリシーを作成して、さまざまなしきい値に基づいてネットワークを監視し、それらのしきい値を超えたときにアラートを生成することができます。使用可能なポート指標に基づいて、ポートのパフォーマンスポリシーを作成できます。しきい値の違反が発生すると、Insightによって検出され、関連するアセットページに赤い丸で表示されます。設定されている場合はEメールで通知されるほか、[Violations Dashboard]や違反を報告するカスタムダッシュボードにも表示されます。

Time-To-Live （ **TTL** ）とデータのダウンサンプリング

OnCommand Insight 7.3以降では、データの保持期間（Time-To-Live）が7日から90日に延長されました。そのため、チャートや表用に処理されるデータがはるかに多く、データポイントが数万に及ぶ可能性があるため、データは表示前にダウンサンプリングされます。

ダウンサンプリングされると、グラフにデータの統計的な概算値が表示されるため、すべてのデータポイントを表示することなく、データの概要を効率的に把握できます。また、収集したデータは常に正確に把握できます。

ダウンサンプリングが必要な理由

Insight 7.3では、データのTime-To-Live（TTL）が90日に延長されています。これは、グラフやグラフに表示

するデータを準備するために必要な処理量が増加することを意味します。グラフをすばやく効率的に表示できるように、データはダウンサンプリングされ、グラフの全体的な形状が維持されます。そのため、そのグラフのすべてのデータポイントを処理する必要はありません。

ダウンサンプリング中に実際のデータが失われることはありません。このあとに示す手順に従って、ダウンサンプリングされたデータではなく、実際のデータでグラフを表示することもできます。

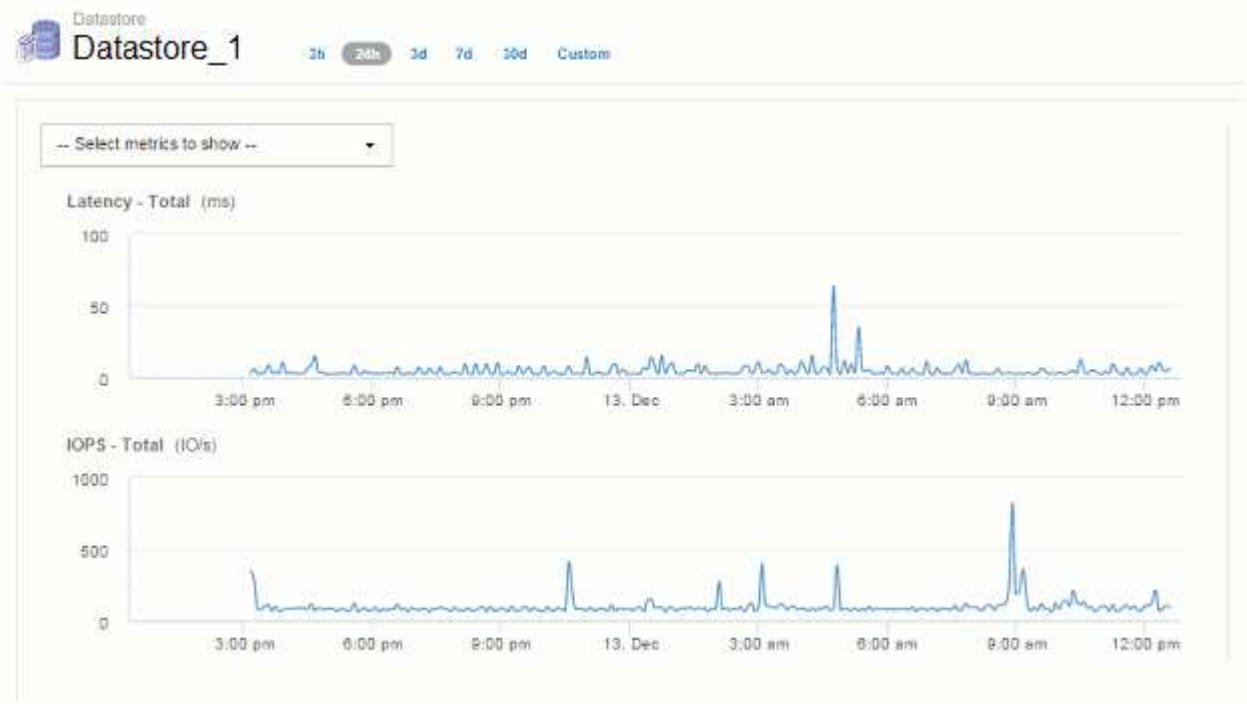
ダウンサンプリングの仕組み

データがダウンサンプリングされる条件は次のとおりです。

- 選択した時間範囲で収集されるデータが 7 日分以下の場合、ダウンサンプリングは行われません。グラフには実際のデータが表示されます
- 選択した時間範囲で収集されるデータが 7 日分を超えていても、データポイントの数が 1 、 000 個未満の場合、ダウンサンプリングは行われません。グラフには実際のデータが表示されます
- 選択した時間範囲で収集されるデータが 7 日分を超え、かつデータポイントの数が 1 、 000 を超える場合は、データがダウンサンプリングされます。グラフには概算データが表示されます。

次に、ダウンサンプリングの実際の例を示します。最初の図は、データストアのアセットページの時間セレクタで* 24h を選択して、**24**時間のレイテンシと**IOPS**のグラフを表示したものです。また、 Custom *を選択し、時間範囲を同じ24時間に設定すると、同じデータが表示されます。

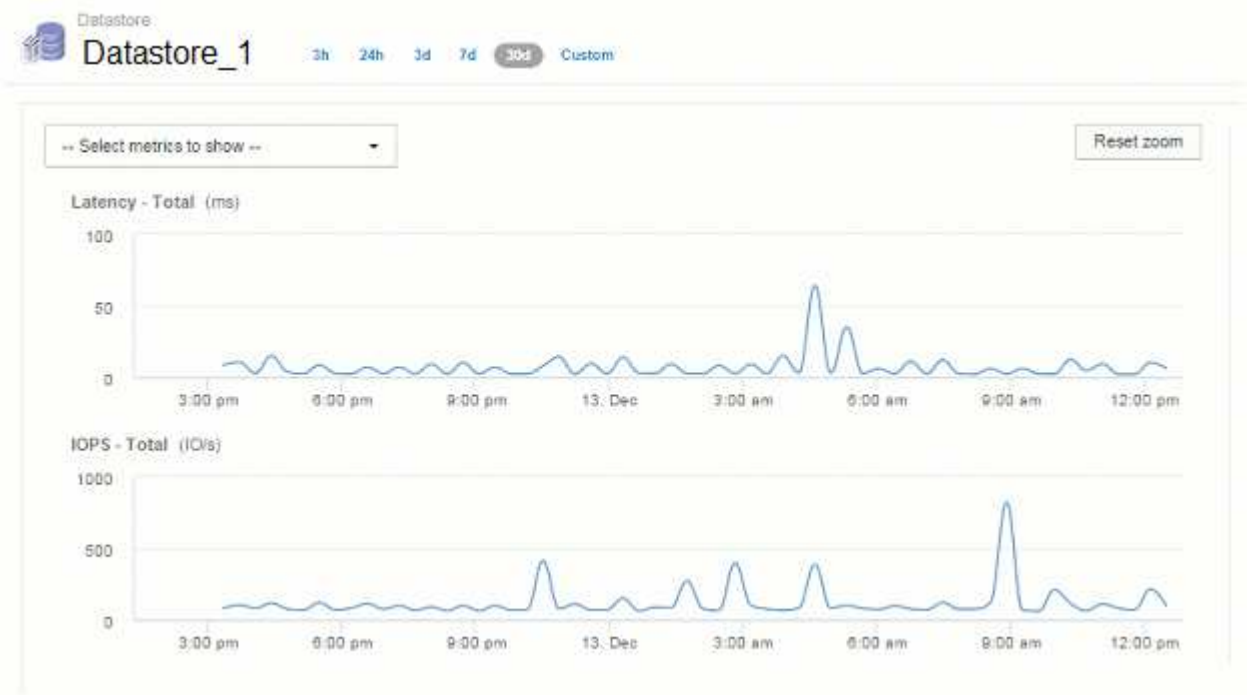
7 日未満の時間範囲を選択しており、グラフのデータポイントも 1 、 000 未満であるため、実際のデータが表示されます。ダウンサンプリングは行われません。



ただし、アセットページの時間セレクタで* 30d *を選択してデータを表示している場合は、 または、7日を超えるカスタムの期間を設定すると（または、選択した期間についてInsightで収集されたデータサンプルが1、000件を超える場合）、データがダウンサンプリングされてから表示されます。ダウンサンプリングされたグラフを拡大表示しても、表示されるのは概算データのままです。

ダウンサンプリングされたグラフを拡大表示すると、表示倍率はデジタルズームになります。表示されるのは概算データのままです。

この例を次の図に示します。時間範囲を 30 日に設定してグラフを表示してから、上記と同じ 24 時間のデータを表示するように拡大表示しています。



このダウンサンプリングされたグラフは、上記の「実際のデータ」のグラフと同じ 24 時間のデータを表示したものであるため、グラフの線の大まかな形状は同じであり、パフォーマンスデータのピークやボトムをすばやく特定することができます。

ダウンサンプリングの概算データの処理方法によっては、ダウンサンプリングされたデータとの比較でグラフの線が多少異なる場合があります実際のデータを比較したときに、グラフの線に多少の違いが見られることがあります。ただし、違いは最小限であり、表示されるデータの全体的な精度には影響しません。

ダウンサンプリングされたグラフでの違反の確認

ダウンサンプリングされたグラフを表示するときは、違反が表示されないことに注意してください。違反を確認するには、次のいずれかを実行します。

- アセットページの期間セレクタで Custom を選択し、 7 日未満の期間を入力して、その期間の実際のデータを表示します。赤の各点にカーソルを合わせます。ツールチップに発生した違反が表示されます。
- 違反ダッシュボードで期間と違反を確認します。

インベントリ履歴の削除

バージョン7.3.2以降では、インベントリ（基盤）の変更履歴が90日間保持されます。以前のバージョンのInsightでは、インストール時からインベントリの変更履歴がすべて保持されていました。古いバージョンのInsightからアップグレードすると、古いインベン

トリ履歴は削除されてから90日後に保持されます。

OnCommand Insight を現在のバージョンにアップグレードすると、履歴は最新の90日間に削除されます。Insightでは、90日分の履歴が残るまで、1日に1回発生する30日間のチャンクで履歴が削除されます。その後、履歴は毎日削除され、わずか90日分のインベントリ変更履歴が保持されます。

VMのNASパス

OnCommand Insight 7.3では、ストレージ共有への仮想マシンのNASパスがサポートされます。これらのパスは、ストレージ共有へのホストのNASパスに似ています。VMのIPアドレスが共有へのアクセスを許可されると、NASパスが作成されます。

仮想マシンのNASパスは、[Internal Volumes]ランディングページに表示されます。このページには、VMがアクセスできる内部ボリュームを特定する[Guest Mounted Storage Resources]ウィジェットが含まれています。

- NASパスは、仮想マシンがバックエンド共有にアクセスできる場合に作成されます。仮想マシンが共有にアクセスするかどうかの確認応答はありません。
- 相関関係はレイテンシとIOPSに基づいて計算されます。VMにバックエンドストレージへのNASパスがある場合は関係ありません。
- ユーザはイニシエータのIPアドレスで共有を照会できますが、パスによる照会はサポートされていません。

内部ボリュームの[Compute Resources]テーブルに、VMとNASパスが表示されるようになりました。VMごとに、CPUとメモリ、利用率とパフォーマンスのデータが表示されます。

Data Warehouseへの影響

OnCommand Insight 7.3へのアップグレード後に行われるData Warehouseに対する変更点は次のとおりです。

- dwh_inventory.nas_logicalテーブルがInventoryデータマートから削除され、ビューに置き換えられました。

  NFSパステーブルを含むInsight 7.2.xのレポートはすべて維持されます。

- Inventoryデータマートにdwh_inventory.nas_cr_logicalテーブルが追加されました。次のテーブルが含まれています。
  - コンピューティングリソース
  - 内部ボリューム
  - ストレージ
  - NAS共有

時系列としての容量

OnCommand Insight 7.3.1では、容量情報が時系列のデータとしてレポートおよびグラフに表示されます。

これまでは、データソースから取得した容量情報は「ポイントインタイム」（PIT）データのみであり、グラフで時系列のデータとして使用することはできませんでした。アセットの容量の値を次の方法で時系列のデータとして使用できるようになりました。

- 表、ウィジェット、エキスパートビューなど、時系列のデータが表示される場所でグラフ化されます
- 既存のセマンティクスを使用して違反が発生したパフォーマンスしきい値に適用されます
- 必要に応じて、式で他のパフォーマンスカウンタとともに使用します

以前のバージョンのInsightからアップグレードすると、カスタムダッシュボードのクエリやフィルタで使用されていたPIT容量の値が時系列の容量データに置き換えられます。そのため、レポートやフィルタリングの方法が、以前のバージョンのInsightでの同等のデータと若干異なる場合があります。

OCI Data Collectorのサポートマトリックス

『Data Collector Support Matrix』には、ベンダーやモデルの情報など、OCIでサポートされるデータコレクタのリファレンスが記載されています。

HP Enterprise 3PAR/Alletra 9000/Primera StoreServストレージ

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
HPE_3PAR 20450 HPE_3PAR 7200 HPE_3PAR 7400 HPE_3PAR 7440c HPE_3PAR 7450c HPE_3PAR 8200 HPE_3PAR 8400 HPE_3PAR 8440 HPE_3PAR 8450 HPE_3PAR A670 HP_3PAR 7200 HPAR 7200	3.2.2（MU2）3.2.2（MU4）3.2.2（MU6）3.3.1（MU2）3.3.1（MU5）4.4.1リリースタイプ：標準サポートリリース

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		Protocol Controller（プロトコルコントローラ）	実施しました	SSH	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		~~Protocol Controller（プロトコルコントローラ）~~	~~実施しました~~	~~SSH~~	
	ボリューム参照	名前	実施しました	SSH	
		ストレージIP	実施しました	SSH	
	WWNエイリアス	ホストのエイリアス	実施しました	SSH	
		オブジェクトタイプ	実施しました	SSH	
		ソース	実施しました	SSH	
		WWN	実施しました	SSH	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		サーバID	実施しました	SMI-Sの使用	
		Snapshotの使用容量	実施しました	SMI-Sの使用	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		Snapshotの使用容量の比率	実施しました	SMI-Sの使用	時系列で報告されます
	ボリューム	キャッシュヒット率読み取り	実施しました	SMI-Sの使用	
		キャッシュヒット率の合計	実施しました	SMI-Sの使用	
		キャッシュヒット率書き込み	実施しました	SMI-Sの使用	
		物理容量	実施しました	SMI-Sの使用	
		合計容量	実施しました	SMI-Sの使用	
		使用済み容量	実施しました	SMI-Sの使用	
		使用容量の比率	実施しました	SMI-Sの使用	
		容量比率の書き込み	実施しました	SMI-Sの使用	
		IOPS読み取り	実施しました	SMI-Sの使用	ディスクの読み取りIOPS数
		IOPSの合計	実施しました	SMI-Sの使用	
		IOPS -書き込み	実施しました	SMI-Sの使用	
		キーを押します	実施しました	SMI-Sの使用	
		レイテンシ読み取り	実施しました	SMI-Sの使用	
		レイテンシ合計	実施しました	SMI-Sの使用	
		レイテンシライト	実施しました	SMI-Sの使用	
		部分ブロック率	実施しました	SMI-Sの使用	
		サーバID	実施しました	SMI-Sの使用	
		スループット読み取り	実施しました	SMI-Sの使用	
		合計スループット	実施しました	SMI-Sの使用	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	SMI-Sの使用	
		書き込み保留中です	実施しました	SMI-Sの使用	合計書き込み保留中です

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
3PAR SMI-Sの2つのタイプがあります	SMI-Sの使用	HTTP / HTTPS	5988/5989		正しい	正しい	正しい	正しい
3Par CLI	SSH	SSH	22		正しい	正しくない	正しい	正しい

Amazon AWS EC2

このデータコレクタでサポートされるモデルとバージョン：

APIバージョン：

- 2014/10/01

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					
360					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		ションID			
	仮想マシンディスク	OID	実施しました	HTTPS	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		VirtualDisk OID	実施しました	HTTPS	
		仮想マシンOID	実施しました	HTTPS	
	ホスト	ホストOS	実施しました	HTTPS	
		IPS	実施しました	HTTPS	
		メーカー	実施しました	HTTPS	
		名前	実施しました	HTTPS	
		OID	実施しました	HTTPS	
	情報	API概要 の略	実施しました	HTTPS	
		API名	実施しました	HTTPS	
		APIのバージョン	実施しました	HTTPS	
		データソース名	実施しました	HTTPS	情報
		日付	実施しました	HTTPS	
		発信者ID	実施しました	HTTPS	
		Originatorキー	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
EC2 API	HTTPS	HTTPS	443		正しい	正しい	正しい	正しい

Brocade ファイバチャネルスイッチ

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
184.0 Brocade Brocade 200E Brocade 300E Brocade Brocade 4024 Embedded Brocade 4100 Brocade 4900 Brocade 5000 Brocade 5100 Brocade 5300 Brocade 5480 Embedded Brocade 6505 Brocade 6510 Brocade 6520 Brocade 7800 Brocade 7840 Brocade DCX8510-4 Brocade DCX8510-8 Brocade G620 Brocade G630 Brocade M5424 Embedded Brocade M6505 Brocade VA-40FC Brocade X6-4 Brocade X6-8	v8.1.0.0a v8.1.0c v6.1.0h v6.2.1b v6.2.2b v6.2.2g v6.4.2b v6.4.1b v6.4.2a v7.0.2c v7.0.2c v7.2.1d v7.4.0a v7.4.1b v7.4.0a v7.4.1b v8.4

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		データス			
		raw速度ギガビット	実施しました	SSH	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		不明な接続	実施しました	SSH	
		WWN	実施しました	SSH	
	スイッチ	ドメインID	実施しました	SSH	
		ファームウェアバージョン	実施しました	SSH	
		IP	実施しました	SSH	
		URLの管理	実施しました	SSH	
		メーカー	実施しました	SSH	
		モデル	実施しました	SSH	
		名前	実施しました	手動入力	
		シリアル番号	実施しました	SSH	
		スイッチのロール	実施しました	SSH	
		スイッチの状態	実施しました	SSH	
		スイッチのステータス	実施しました	SSH	
		を入力します	ギャップ	SSH	
		VSANがイネーブルです	実施しました	SSH	
		WWN	実施しました	SSH	
	WWNエイリアス	ホストのエイリアス	実施しました	SSH	
		オブジェクトタイプ	実施しました	SSH	
		ソース	実施しました	SSH	
		WWN	実施しました	SSH	
	ゾーン	ゾーン名	実施しました	SSH	
	ゾーンメンバー	を入力します	ギャップ	SSH	
		WWN	実施しました	SSH	
	ゾーニング機能	アクティブな構成	実施しました	SSH	
		コンフィギュレーション名（Configuration Name）	実施しました	SSH	
		WWN	実施しました	SSH	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

		ポートエラー信号損失	実施しました	SNMP	ポートエラー信号損失
製品	カテゴリ	ポートエラー同期損失（Feature/Attribute）	実施しました	使用するプロトコル	追加情報
		ポートエラー送信破棄タイムアウト	実施しました	SNMP	ポートエラータイムアウトの破棄
		合計ポートエラー数	実施しました	SNMP	合計ポートエラー数
		サーバID	実施しました	SNMP	
		トラフィックフレームレート	実施しました	SNMP	
		合計トラフィックフレームレート	実施しました	SNMP	
		トラフィックフレームレート	実施しました	SNMP	
		平均フレームサイズ	実施しました	SNMP	トラフィックの平均フレームサイズ
		Tx Frames（送信フレーム）	実施しました	SNMP	トラフィックの平均フレームサイズ
		トラフィック受信率	実施しました	SNMP	
		合計トラフィックレート	実施しました	SNMP	
		トラフィック送信レート	実施しました	SNMP	
		トラフィック受信使用率	実施しました	SNMP	
		合計トラフィック利用率	実施しました	SNMP	合計トラフィック使用率
		トラフィック送信使用率	実施しました	SNMP	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Brocade SNMP	SNMP	SNMPv1、SNMPv2、SNMPv3	161		正しい	正しい	正しい	正しい
Brocade SSH	SSH	SSH	22		正しくない	正しくない	正しい	正しい
データソースウィザードの設定	手動入力				正しい	正しい	正しい	正しい

Brocade Network Advisor HTTP

このデータコレクタでサポートされるモデルとバージョン：

APIバージョン：

- 14.4.5

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎	ファブリック	名前	実施しました	HTTP/S	
		WWN	実施しました	HTTP/S	
	情報	API概要 の略	実施しました	HTTP/S	
		API名	実施しました	HTTP/S	
		APIのバージョン	実施しました	HTTP/S	
		データソース名	実施しました	HTTP/S	情報
		日付	実施しました	HTTP/S	
		発信者ID	実施しました	HTTP/S	
		Originatorキー	実施しました	HTTP/S	
	WWNエイリアス	ホストのエイリアス	実施しました	HTTP/S	
		オブジェクトタイプ	実施しました	HTTP/S	
		ソース	実施しました	HTTP/S	
		WWN	実施しました	HTTP/S	
	ゾーン	ゾーン名	実施しました	HTTP/S	
	ゾーンメンバー	を入力します	ギャップ	HTTP/S	
		WWN	実施しました	HTTP/S	
	ゾーニング機能	アクティブな構成	実施しました	HTTP/S	
		コンフィギュレーション名（Configuration Name）	実施しました	HTTP/S	
		WWN	実施しました	HTTP/S	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス	ポート	BBクレジットゼロ合計	実施しました	HTTP/S	BBクレジットゼロ合計
		BBクレジットゼロ送信	実施しました	HTTP/S	BBクレジットゼロ送信
		BBクレジットゼロMS送信	実施しました	HTTP/S	BBクレジットゼロMS送信
		Port Errorsクラス3破棄	実施しました	HTTP/S	
		ポートエラーCRC	実施しました	HTTP/S	ポートエラーCRC
		Port Errors Enc In（ポートエラーエンクロージャ入力）	実施しました	HTTP/S	Port Errors Enc In（ポートエラーエンクロージャ入力）
		ポートエラーショートフレーム	実施しました	HTTP/S	短いフレームによるポートエラーです
		ポートエラーリンク障害	実施しました	HTTP/S	ポートエラーリンク障害
		ポートエラー信号損失	実施しました	HTTP/S	ポートエラー信号損失
		ポートエラー同期損失	実施しました	HTTP/S	ポートエラー同期が失われました
		ポートエラー送信破棄タイムアウト	実施しました	HTTP/S	ポートエラータイムアウトの破棄
		合計ポートエラー数	実施しました	HTTP/S	合計ポートエラー数

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Brocade Network Advisor REST API	HTTP / HTTPS	HTTP / HTTPS	80 / 443		正しい	正しい	正しい	正しい

Cisco MDS / Nexusファブリックスイッチ

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
8978-E16 DS-C9124-2-K9 DS-C9124-K9 DS-C9134-K9 DS-C9140-K9 DS-C9148-16P-K9 DS-C9148-48P-K9 DS-C9148-48P-K9 DS-C9148S-K9 DS-C9148S-K9 C9148S-C9148D-C9148T-K-DS C929	3.2（2c）4.1（3a）5.0（1a）5.0（3.13e）5.0（3）N2（4.04i）5.0（3）N2（4.13j）5.0（3）N2（4.21k）5.2（8c）5.2（8g）5.2（8h）5.2（8i）6.2（1）1）6.2（1）2（1（1）2（1）2（1（1（1）6.2（1）1）2（1）2（1）2（1）2（1）

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

	ゾーン	ゾーン名	実施しました	SNMP	
		ゾーンタイプ	実施しました	SNMP	
製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
	ゾーンメンバー	を入力します WWN	ギャップ	SNMP	
			実施しました	SNMP	
	ゾーニング機能	アクティブな構成	実施しました	SNMP	
		コンフィギュレーション名（Configuration Name）	実施しました	SNMP	
		デフォルトのゾーニング動作	実施しました	SNMP	
		コントロールのマージ	実施しました	SNMP	
		WWN	実施しました	SNMP	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

		信破棄タイムアウト			イムアウトの破棄
		合計ポートエラー数	実施しました	SNMP	合計ポートエラー数
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）ID	ステータス	使用するプロトコル	追加情報
			実施しました	SNMP	
		トラフィックフレームレート	実施しました	SNMP	
		合計トラフィックフレームレート	実施しました	SNMP	
		トラフィックフレームレート	実施しました	SNMP	
		平均フレームサイズ	実施しました	SNMP	トラフィックの平均フレームサイズ
		Tx Frames（送信フレーム）	実施しました	SNMP	トラフィックの平均フレームサイズ
		トラフィック受信率	実施しました	SNMP	
		合計トラフィックレート	実施しました	SNMP	
		トラフィック送信レート	実施しました	SNMP	
		トラフィック受信使用率	実施しました	SNMP	
		合計トラフィック利用率	実施しました	SNMP	合計トラフィック使用率
		トラフィック送信使用率	実施しました	SNMP	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Cisco SNMP	SNMP	SNMPv1（インベントリのみ）、SNMP v2、SNMP v3	161		正しい	正しい	正しい	正しい

EMC Celerra（SSH）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
NSX VG8 VNX5600	5.5.38-1 7.1.76-4 7.1.79-8 8.1.9-184

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					
380					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		合計割り当て済み容量	実施しました	SSH	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		合計使用容量	実施しました	SSH	合計容量（MB）
		ボリューム	ギャップ	SSH	
		仮想	実施しました	SSH	ストレージ仮想化デバイスですか？

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Celerra CLIの場合	SSH	SSH			正しい	正しくない	正しい	正しい

EMC CLARiX（NaviCLI）

このデータコレクタでサポートされるモデルとバージョン：

APIハアシヨン	モデル	ファームウェアバージョン
6.28 7.32 7.33	CX4-120 VNX5200 VNX5400 VNX5500 VNX5600 VNX5700 VNX5800 VNX7600 VNX8000	04.28.000.5.008 05.32.000.5.218 05.32.000.5.219 05.32.000.5.221 05.32.000.5.249 05.33.009.5.155 05.33.009.5.184 05.33.009.5.186 05.33.009.5.218 05.33.009.5.35.05.35.238

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		ニング			
		を入力します	ギャップ	CLI	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		UUID	実施しました	CLI	
		使用済み容量	実施しました	CLI	
	ボリュームマップ	LUN	実施しました	CLI	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	CLI	
		ストレージポート	実施しました	CLI	
		を入力します	ギャップ	CLI	
	ボリュームマスク	イニシエータ	実施しました	CLI	
		Protocol Controller（プロトコルコントローラ）	実施しました	CLI	
		ストレージポート	実施しました	CLI	
		を入力します	ギャップ	CLI	
	ボリュームメンバー	容量	実施しました	CLI	Snapshotの使用容量（MB単位）
		名前	実施しました	CLI	
		ランク	実施しました	CLI	
		合計物理容量	実施しました	CLI	合計物理容量（アレイ上のすべてのディスクの合計）
		冗長性	実施しました	CLI	冗長性レベル
		ストレージプールID	実施しました	CLI	
		使用済み容量	実施しました	CLI	
	WWNエイリアス	ホストのエイリアス	実施しました	CLI	
		IP	実施しました	CLI	
		オブジェクトタイプ	実施しました	CLI	
		ソース	実施しました	CLI	
		WWN	実施しました	CLI	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

		ストレージプールの容量	実施しました	CLI	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		キーを押します	実施しました	CLI	
		サーバID	実施しました	CLI	
	ストレージプール	プロビジョニング済み容量	実施しました	CLI	
		物理容量	実施しました	CLI	
		合計容量	実施しました	CLI	
		使用済み容量	実施しました	CLI	
		オーバーコミット容量率です	実施しました	CLI	時系列で報告されます
		使用容量の比率	実施しました	CLI	
		キーを押します	実施しました	CLI	
		その他の合計容量	実施しました	CLI	
		その他の使用容量	実施しました	CLI	
		サーバID	実施しました	CLI	
		Snapshotのリザーブ容量	実施しました	CLI	
		Snapshotの使用容量	実施しました	CLI	
		Snapshotの使用容量の比率	実施しました	CLI	時系列で報告されます
	ボリューム	物理容量	実施しました	CLI	
		合計容量	実施しました	CLI	
		使用済み容量	実施しました	CLI	
		使用容量の比率	実施しました	CLI	
		キーを押します	実施しました	CLI	
		サーバID	実施しました	CLI	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Navi CLIの場合	CLI		6389、2162、2163、443（HTTPS）/ 80（HTTP）		正しい	正しい	正しい	正しくない

EMC Data Domain（SSH）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
DD2500 DD4200 DD4500 DD6300 DD670 DD6800 DD6900 DD9300 DD9400 DD990	5.4.6.0-503967 5.5.0.9-471508 5.5.2.1-486308 6.1.0.5-567091 6.2.1.30-663869 6.2.1.50-680189 7.10.1.15-1078832 7.10.1.20-1090468 7.2.0.70-686759 7.6.0.40-691389 7.7.7.7.7.7.7.7.7.7.0-105.1076.76.1076.76.76.1076.1.1076.1.1076.1.1076.1.1076.1.10187

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		使用可能な物理比率	実施しました	SSH	使用可能容量から物理容量への変換率
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			実施しました	SSH	
		シンプロビジョニングがサポートされます	実施しました	SSH	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		合計割り当て済み容量	実施しました	SSH	
		合計使用容量	実施しました	SSH	合計容量（MB）
		を入力します	ギャップ	SSH	
		仮想	実施しました	SSH	ストレージ仮想化デバイスですか？

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Data Domain CLIの略	SSH	SSH	22		正しい	正しい	正しい	正しい

EMC ECS

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
ECS の場合	3.6.1.3 3.7.0.6 3.8.0.6 3.8.1.1

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
	ストレージノード	名前	実施しました	HTTPS	
		UUID	実施しました	HTTPS	
		ステータス	実施しました	HTTPS	
		ソフトウェアバージョン	実施しました	HTTPS	
	ストレージプール	DWH容量に含める	実施しました	HTTPS	ACQからDWHのCapacityで対象となるストレージプールを制御する方法
		名前	実施しました	HTTPS	
		物理ディスク容量（MB）	実施しました	HTTPS	ストレージプールの物理容量として使用されます
		RAID グループ	実施しました	HTTPS	このストレージプールがRAIDグループかどうかを示します
		使用可能な物理比率	実施しました	HTTPS	使用可能容量から物理容量への変換率
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニングがサポートされます	実施しました	HTTPS	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		合計割り当て済み容量	実施しました	HTTPS	
		合計使用容量	実施しました	HTTPS	合計容量（MB）
		を入力します	ギャップ	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
EMC ECS REST API	HTTPS	HTTPS	443		正しい	正しい	正しい	正しい

Dell EMC Isilon / PowerScale（CLI）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
A200 A2000 A300 A3000 F800 H400 H500 H500-4U - シングル-128GB-1GE-2x10GE SFP+-30TB-1638GB SSD H700 NL400 NL410トレースバック（最新のコールは最後）：X210 X400 sudo Python	9.2.1.12 9.4.0.14 9.4.0.17 9.5.0.7 v8.0.0.6 v8.0.0.7

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		合計割り当て済み容量	実施しました	SSH	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		合計使用容量	実施しました	SSH	合計容量（MB）
		ボリューム	ギャップ	SSH	
		仮想	実施しました	SSH	ストレージ仮想化デバイスですか？

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

					クの合計）
		失敗した物理容量	実施しました	SSH	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		失敗した物理容量	実施しました	SSH	
	ストレージノードデータ	IOPS読み取り	実施しました	SSH	ファイルシステム上の読み取りIOPSの数
		IOPS -書き込み	実施しました	SSH	ファイルシステムのIOPS書き込み
		ファイルスループット読み込み	実施しました	SSH	
		ファイルシステムスループット	実施しました	SSH	ファイルシステムスループット書き込み
		IOPS読み取り	実施しました	SSH	ディスクの読み取りIOPS数
		IOPSの合計	実施しました	SSH	
		IOPS -書き込み	実施しました	SSH	
		キーを押します	実施しました	SSH	
		レイテンシ合計	実施しました	SSH	
		サーバID	実施しました	SSH	
		スループット読み取り	実施しました	SSH	
		合計スループット	実施しました	SSH	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	SSH	
		利用率の合計	実施しました	SSH	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Isilon SSH	SSH	SSH	22		正しい	正しくない	正しい	正しい

EMC PowerStore REST

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
PowerStore 1000T PowerStore 5000T PowerStore 5200T	2.1.1.1 3.2.1.0 3.5.0.2

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

	ク					
		Protocol Controller（プロトコルコントローラ）	実施しました			
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報	
		追加します	ギャップ			
	WWNエイリアス	ホストのエイリアス	実施しました			
		オブジェクトタイプ	実施しました			
		ソース	実施しました			
		WWN	実施しました			
パフォーマンス	ストレージ	失敗した物理容量	実施しました			
		物理容量	実施しました			
		スペアの物理容量	実施しました		スペアディスクの物理容量（スペアの全ディスクの合計）	
		ストレージプールの容量	実施しました			
		IOPS：その他	実施しました			
		IOPS読み取り	実施しました		ディスクの読み取りIOPS数	
		IOPSの合計	実施しました			
		IOPS -書き込み	実施しました			
		キーを押します	実施しました			
		レイテンシ読み取り	実施しました			
		レイテンシ合計	実施しました			
		レイテンシライト	実施しました			
		サーバID	実施しました			

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
EMC PowerStore REST API	HTTPS	HTTPS	443		正しい	正しい	正しい	正しい

EMC RecoverPoint（HTTP）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
RecoverPoint	5.1.SP3.P1（G.69）5.1.SP4.HF1（H.86）5.1.SP4.P1（H.89）

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

		量			の物理容量（スペアの全ディスクの合計）
製品	カテゴリ	仮想ーチャー/属性（**Feature/Attribute**）	実施しました	使用するプロトコル	追加情報ジ仮想化デバイスですか？
	ストレージノード	メモリサイズ	ギャップ	HTTPS	デバイスメモリ（MB単位）
		モデル	実施しました	HTTPS	
		名前	実施しました	HTTPS	
		プロセッサ数	実施しました	HTTPS	デバイスCPU
		シリアル番号	実施しました	HTTPS	
		都道府県	実施しました	HTTPS	デバイスの状態を説明するフリーテキスト
		UUID	実施しました	HTTPS	
		バージョン	実施しました	HTTPS	ソフトウェアバージョン
	ストレージ同期	モード	実施しました	HTTPS	
		モード列挙	実施しました	HTTPS	
		ソースストレージ	実施しました	HTTPS	
		ソースボリューム	実施しました	HTTPS	
		都道府県	実施しました	HTTPS	デバイスの状態を説明するフリーテキスト
		状態の列挙	実施しました	HTTPS	
		ターゲットストレージ	実施しました	HTTPS	
		ターゲットボリューム	実施しました	HTTPS	
		テクノロジ	実施しました	HTTPS	ストレージ効率化の原因となるテクノロジが変化しています

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
RecoverPoint REST API	HTTPS	HTTPS	443		正しい	正しい	正しい	正しい

EMC Symmetrix CLI

このデータコレクタでサポートされるモデルとバージョン：

APIハアシヨン	モデル	ファームウェアバージョン
V10.0.0.0 V10.0.0.3 V10.0.1.0 V10.0.1.3 V10.1.0.0 V10.1.0.0 V8.3.0.3 V8.3.0.6 V9.2.0.0 V9.2.3.0 V9.2.3.4 V9.2.3.6 V9.2.4.1 V9.2.4.2 V9.2.4.6	PMax8000 PowerMax_2000 PowerMax_8000 VMAX-1 VMAX250F VMAX40K VMAX450F VMAX950F	A076.286.194（16F40000）ビルド115 5978.479.479（175A0000）ビルド372 5978.711.711（175A0000）ビルド179 5978.711.711（175A0000）ビルド205 5978.711.711（175A0000）ビルド239 5978.78.78.711.711.711（174）ビルド1797000）ビルド1797000）ビルド

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		トコルコントローラ）			
製品	カテゴリ	ストレージポート/フィーチャー/属性（Feature/Attribute）	実施しましたステータス	使用するプロトコル	追加情報
		出力します	ギャップ		
	ボリュームメンバー	自動階層化	実施しました		このストレージプールが他のプールとの自動階層化に参加しているかどうかを示します
		容量	実施しました		Snapshotの使用容量（MB単位）
		シリンダ	実施しました		
		名前	実施しました		
		ランク	実施しました		
		合計物理容量	実施しました		合計物理容量（アレイ上のすべてのディスクの合計）
		冗長性	実施しました		冗長性レベル
		ストレージプールID	実施しました		
		UUID	実施しました		
	WWNエイリアス	ホストのエイリアス	実施しました		
		オブジェクトタイプ	実施しました		
		ソース	実施しました		
		WWN	実施しました		

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス	ボリューム	キャッシュヒット率読み取り	実施しました		
		キャッシュヒット率の合計	実施しました		
		キャッシュヒット率書き込み	実施しました		
		物理容量	実施しました		
		合計容量	実施しました		
		使用済み容量	実施しました		
		使用容量の比率	実施しました		
		IOPS読み取り	実施しました		ディスクの読み取りIOPS数
		IOPSの合計	実施しました		
		IOPS -書き込み	実施しました		
		キーを押します	実施しました		
		レイテンシ読み取り	実施しました		
		レイテンシ合計	実施しました		
		レイテンシライト	実施しました		
		サーバID	実施しました		
		スループット読み取り	実施しました		
		合計スループット	実施しました		ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました		
		書き込み保留中です	実施しました		合計書き込み保留中です

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
SYMCLI	CLI		2707		正しい	正しい	正しい	正しい
Symmetrix SMI-S	SMI-Sの使用	HTTP / HTTPS	5988/5989		正しい	正しくない	正しくない	正しい

Dell Unisphere REST

このデータコレクタでサポートされるモデルとバージョン：

APIハアシヨン	モデル	ファームウェアバージョン
v10.0.1.3 v10.1.0.1 v10.1.0.5 v10.1.0.6 V9.2.4.7 V9.2.4.9	PowerMax_2000 PowerMax_2500 PowerMax_8000 PowerMax_8500 VMAX250F VMAX950F	5978.714.714 5978.714.714ビルド6 5978.714.714ビルド61 5978.714.714ビルド85 6079.225.0ビルド127 6079.225.0ビルド216

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		トコルコントローラ）			
製品	カテゴリ	ストレージポート	実施しました	HTTPS	
		フィーチャー/属性（Feature/Attribute）	スステータス	使用するプロトコル	追加情報
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	WWNエイリアス	ホストのエイリアス	実施しました	HTTPS	
		オブジェクトタイプ	実施しました	HTTPS	
		ソース	実施しました	HTTPS	
		WWN	実施しました	HTTPS	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

					込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		利用率の合計	実施しました	HTTPS	
	ストレージ	キャッシュヒット率読み取り	実施しました	HTTPS	
		キャッシュヒット率の合計	実施しました	HTTPS	
		キャッシュヒット率書き込み	実施しました	HTTPS	
		失敗した物理容量	実施しました	HTTPS	
		物理容量	実施しました	HTTPS	
		スペアの物理容量	実施しました	HTTPS	スペアディスクの物理容量（スペアの全ディスクの合計）
		ストレージプールの容量	実施しました	HTTPS	
		IOPS：その他	実施しました	HTTPS	
		IOPS読み取り	実施しました	HTTPS	ディスクの読み取りIOPS数
		IOPSの合計	実施しました	HTTPS	
		IOPS -書き込み	実施しました	HTTPS	
		キーを押します	実施しました	HTTPS	
		レイテンシ読み取り	実施しました	HTTPS	
		レイテンシ合計	実施しました	HTTPS	
		レイテンシライト	実施しました	HTTPS	
		サーバID	実施しました	HTTPS	
		スループット読み取り	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	
		書き込み保留中です	実施しました	HTTPS	合計書き込み保留中です

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Dell Unisphere API	HTTPS	HTTPS	443		正しい	正しい	正しい	正しい

EMC VNX（SSH）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
VNX5300 VNX5400 VNX5800 VNX7500	05.32.000.5.219 05.32.000.5.221 05.32.000.5.225 05.33.009.5.186

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		トコルコントローラ）			
製品	カテゴリ	ストレージポート	実施しました	SSH	追加情報
		フィーチャー/属性（Feature/Attribute）を入力します	ステータス	使用するプロトコル	
			ギャップ	SSH	
	ボリュームマスク	イニシエータ	実施しました	SSH	
		Protocol Controller（プロトコルコントローラ）	実施しました	SSH	
		ストレージポート	実施しました	SSH	
		を入力します	ギャップ	SSH	
	WWNエイリアス	ホストのエイリアス	実施しました	SSH	
		IP	実施しました	SSH	
		オブジェクトタイプ	実施しました	SSH	
		ソース	実施しました	SSH	
		WWN	実施しました	SSH	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

		ストレージプールの容量	実施しました	SSH		
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）を押します	ステータス	使用するプロトコル	追加情報	
		キーを押します	実施しました	SSH		
		サーバID	実施しました	SSH		
	ストレージプール	プロビジョニング済み容量	実施しました	SSH		
		物理容量	実施しました	SSH		
		合計容量	実施しました	SSH		
		使用済み容量	実施しました	SSH		
		オーバーコミット容量率です	実施しました	SSH	時系列で報告されます	
		使用容量の比率	実施しました	SSH		
		キーを押します	実施しました	SSH		
		その他の合計容量	実施しました	SSH		
		その他の使用容量	実施しました	SSH		
		サーバID	実施しました	SSH		
	ボリューム	物理容量	実施しました	SSH		
		合計容量	実施しました	SSH		
		使用済み容量	実施しました	SSH		
		使用容量の比率	実施しました	SSH		
		キーを押します	実施しました	SSH		
		サーバID	実施しました	SSH		

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
VNX SSH およびCLI	SSH	SSH	22		正しい	正しくない	正しい	正しい

EMC VNXeおよびUnity Unisphere（CLI）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
Unity 300 Unity 300F Unity 350F Unity 450F Unity 480F Unity 550F Unity 600 Unity 600F Unity 650F Unity 680F Unity 880 Unity 880F VNXe3200	3.1.17.10223906 4.2.3.9670635 4.5.1.0.5.001 5.0.2.0.5.009 5.0.6.0.5.008 5.0.7.0.5.008 5.1.0.0.5.394 5.1.2.0.5.007 5.1.3.0.5.003 5.2.1.0.5.013 5.2.2.0.5.004 5.3.0.5.008 5.3.0.5.008 5.4.0.0.5.094

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		シンプロビジョニング	実施しました	HTTPS	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		UUID	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
	ボリュームマップ	LUN	実施しました	HTTPS	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
パフォーマンス	ディスク	IOPS読み取り	実施しました	HTTPS	ディスクの読み取りIOPS数
		IOPSの合計	実施しました	HTTPS	
		IOPS -書き込み	実施しました	HTTPS	
		キーを押します	実施しました	HTTPS	
		サーバID	実施しました	HTTPS	
		スループット読み取り	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
VNXeとUnisphere CLI	HTTPS	HTTPS	443		正しい	正しい	正しい	正しい

EMC VPLEX

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
VPLEX	6.1.0.00.00.23 6.1.0.01.00.13 6.1.0.02.00.04

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		合計使用容量	実施しました	HTTP/S	合計容量（MB）
		を入力します	ギャップ	HTTP/S	
製品	カテゴリ	仮想ーチャー/属性（**Feature/Attribute**）	実施しました	使用するプロトコル	追加情報ジ仮想化デバイスですか？
	ボリューム	容量	実施しました	HTTP/S	Snapshotの使用容量（MB単位）
		名前	実施しました	HTTP/S	
		合計物理容量	実施しました	HTTP/S	合計物理容量（アレイ上のすべてのディスクの合計）
		冗長性	実施しました	HTTP/S	冗長性レベル
		ストレージプールID	実施しました	HTTP/S	
		シンプロビジョニング	実施しました	HTTP/S	
		UUID	実施しました	HTTP/S	
		仮想	実施しました	HTTP/S	ストレージ仮想化デバイスですか？
	ボリュームマップ	LUN	実施しました	HTTP/S	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTP/S	
		ストレージポート	実施しました	HTTP/S	
		を入力します	ギャップ	HTTP/S	
	ボリュームマスク	イニシエータ	実施しました	HTTP/S	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTP/S	
		ストレージポート	実施しました	HTTP/S	
		を入力します	ギャップ	HTTP/S	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

					込み）（MB/秒）
		スループット書き込み	実施しました	SSH	
製品	カテゴリ	スイッチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		物理容量の合計	実施しました	SSH	
	ボリューム	物理容量	実施しました	SSH	
		合計容量	実施しました	SSH	
		IOPSの合計	実施しました	SSH	
		キーを押します	実施しました	SSH	
		レイテンシ読み取り	実施しました	SSH	
		レイテンシ合計	実施しました	SSH	
		レイテンシライト	実施しました	SSH	
		サーバID	実施しました	SSH	
		スループット読み取り	実施しました	SSH	
		合計スループット	実施しました	SSH	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	SSH	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
EMC VPLEX CLI	SSH	SSH	22		正しい	正しい	正しい	正しい
EMC VPLEX API	HTTP / HTTPS	HTTP / HTTPS	80 / 443		正しい	正しい	正しい	正しい

EMC XtremIO（HTTP）

このデータコレクタでサポートされるモデルとバージョン：

APIハアシヨン	モデル	ファームウェアバージョン
4.2.2 6.2.1 6.3.1 6.3.2 6.3.3 6.4.0	1ブリック、48TB 1X20TB 2ブリック、251TB 2X20TB 3ブリック、283TB 4ブリック、503TB 4X10TB 6X20TB 8X20TB	4.0.25-27 4.0.31-11 6.1.0-99_X2 6.2.1-36_X2 6.3.3-8_X2 6.4.0-36_hotfix_2_X2

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		ターゲットボリューム	実施しました	HTTPS	
		テクノロジフィーチャー/属性（**Feature/Attribute**）	実施しましたステータス	HTTPS使用するプロトコル	ストレージ効率化の情報追加情報となるテクノロジが変化しています
製品	カテゴリ				
	ボリューム	容量	実施しました	HTTPS	Snapshotの使用容量（MB単位）
		ディスクサイズ	実施しました	HTTPS	ディスクサイズのカンマ区切りリスト（GB）
		ディスク速度	実施しました	HTTPS	ディスク速度のカンマ区切りリスト（rpm）
		ディスクタイプ	使用できません	HTTPS	
		名前	実施しました	HTTPS	
		合計物理容量	実施しました	HTTPS	合計物理容量（アレイ上のすべてのディスクの合計）
		冗長性	実施しました	HTTPS	冗長性レベル
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニング	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
		UUID	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？
	ボリュームマップ	LUN	実施しました	HTTPS	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

		キーを押します	実施しました	HTTPS		
		サーバID	実施しました	HTTPS		
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報	
	ストレージノードデータ	キーを押します	実施しました	HTTPS		
		サーバID	実施しました	HTTPS		
	ボリューム	物理容量	実施しました	HTTPS		
		合計容量	実施しました	HTTPS		
		使用済み容量	実施しました	HTTPS		
		使用容量の比率	実施しました	HTTPS		
		IOPS読み取り	実施しました	HTTPS	ディスクの読み取りIOPS数	
		IOPSの合計	実施しました	HTTPS		
		IOPS -書き込み	実施しました	HTTPS		
		キーを押します	実施しました	HTTPS		
		レイテンシ読み取り	実施しました	HTTPS		
		レイテンシ合計	実施しました	HTTPS		
		レイテンシライト	実施しました	HTTPS		
		部分ブロック率	実施しました	HTTPS		
		サーバID	実施しました	HTTPS		
		スループット読み取り	実施しました	HTTPS		
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）	
		スループット書き込み	実施しました	HTTPS		

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
EMC XtremIO REST API	HTTPS	HTTPS	443		正しい	正しい	正しい	正しい

NetApp Eシリーズ

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
2650 2660 2704 2806 5600 5700	8.10.15.0 8.20.11.60 8.20.16.0 8.20.5.60 8.40.0.3 8.40.60.2 8.63.0.2 8.72.0.0 8.72.1.0 8.72.2.0 8.73.0.0 8.74.2.0

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		書き込み済み容量	実施しました	RMI	このボリュームに書き込まれた合計容量（MB）
製品	カテゴリ ボリュームマップ	フィーチャー/属性（**Feature/Attribute**）	ステータス 実施しました	使用するプロトコル RMI	追加情報 バックエンドLUNの名前
	ボリュームマスク	イニシエータ	実施しました	RMI	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		その他の合計容量	実施しました	RMI	
		その他の使用容量	実施しました	RMI	
製品	カテゴリ	ライセンス属性（Feature/Attribute）ID	ステータス	使用するプロトコル	追加情報
			実施しました	RMI	
	ボリューム	キャッシュヒット率読み取り	実施しました	RMI	
		キャッシュヒット率の合計	実施しました	RMI	
		キャッシュヒット率書き込み	実施しました	RMI	
		物理容量	実施しました	RMI	
		合計容量	実施しました	RMI	
		使用済み容量	実施しました	RMI	
		使用容量の比率	実施しました	RMI	
		IOPS読み取り	実施しました	RMI	ディスクの読み取りIOPS数
		IOPSの合計	実施しました	RMI	
		IOPS -書き込み	実施しました	RMI	
		キーを押します	実施しました	RMI	
		レイテンシ読み取り	実施しました	RMI	
		レイテンシ合計	実施しました	RMI	
		レイテンシライト	実施しました	RMI	
		サーバID	実施しました	RMI	
		スループット読み取り	実施しました	RMI	
		合計スループット	実施しました	RMI	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	RMI	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
SANtricity APIの略	RMI	TCP			正しい	正しい	正しくない	正しくない

HDS HCP（HTTPS）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
Hitachi Content Platform の略	9.6.2.37 9.6.3.33

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
	ストレージノード	名前	実施しました	HTTPS	
		UUID	実施しました	HTTPS	
	ストレージプール	DWH容量に含める	実施しました	HTTPS	ACQからDWHのCapacityで対象となるストレージプールを制御する方法
		名前	実施しました	HTTPS	
		物理ディスク容量（MB）	実施しました	HTTPS	ストレージプールの物理容量として使用されます
		RAID グループ	実施しました	HTTPS	このストレージプールがRAIDグループかどうかを示します
		使用可能な物理比率	実施しました	HTTPS	使用可能容量から物理容量への変換率
		ソフトリミット（MB）	実施しました	HTTPS	ボリュームの作成またはサイズ変更処理で定義される論理ボリュームサイズ
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニングがサポートされます	実施しました	HTTPS	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		合計割り当て済み容量	実施しました	HTTPS	
		合計使用容量	実施しました	HTTPS	合計容量（MB）
		を入力します	ギャップ	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス	ストレージ	失敗した物理容量	実施しました		
		物理容量	実施しました		
		スペアの物理容量	実施しました		スペアディスクの物理容量（スペアの全ディスクの合計）
		ストレージプールの容量	実施しました		
		キーを押します	実施しました		
		サーバID	実施しました		
	ストレージノードデータ	キーを押します	実施しました		
		サーバID	実施しました		
		スループット読み取り	実施しました		
		合計スループット	実施しました		ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました		
		利用率の合計	実施しました		

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
HDS HCP REST API	HTTPS	HTTPS	9090		正しい	正しい	正しい	正しい

HiCommand Device Managerの略

このデータコレクタでサポートされるモデルとバージョン：

APIハアシヨン	モデル	ファームウェアバージョン
8.6.4 8.7.7 8.8.1 8.8.3 8.8.5	D850XS HM700 HM800M R800	0988/J-W DKC：73-03-69-00/00 DKC：80-06-92-00/00 DKC：83-05-48-40/00 DKC：83-05-50-40/00 SVP：73-03-68/00 SVP：80-06-87/00 SVP：83-05-52-40/00 SVP：83-05-54

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		シンプロビジョニング	実施しました	HDS XML API	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）を入力します	ステータス	使用するプロトコル	追加情報
		仮想	ギャップ	HDS XML API	
		使用済み容量	実施しました	HDS XML API	
	ボリュームマップ	LUN	実施しました	HDS XML API	バックエンドLUNの名前
		マスキングが必要です	実施しました	HDS XML API	
		Protocol Controller（プロトコルコントローラ）	実施しました	HDS XML API	
		ストレージポート	実施しました	HDS XML API	
	ボリュームマスク	イニシエータ	実施しました	HDS XML API	
		Protocol Controller（プロトコルコントローラ）	実施しました	HDS XML API	
		ストレージポート	実施しました	HDS XML API	
	ボリュームメンバー	名前	実施しました	HDS XML API	
		ストレージプールID	実施しました	HDS XML API	
		ランク	実施しました	HDS XML API	
		シリンダ	実施しました	HDS XML API	
		容量	実施しました	HDS XML API	Snapshotの使用容量（MB単位）
		合計物理容量	実施しました	HDS XML API	合計物理容量（アレイ上のすべてのディスクの合計）
		使用済み容量	実施しました	HDS XML API	
	WWNエイリアス	ホストのエイリアス	実施しました	HDS XML API	
		オブジェクトタイプ	実施しました	HDS XML API	
		ソース	実施しました	HDS XML API	
		WWN	実施しました	HDS XML API	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス	ディスク	IOPS読み取り	実施しました	エクスポート/CLI	ディスクの読み取りIOPS数
		IOPSの合計	実施しました	エクスポート/CLI	
		IOPS -書き込み	実施しました	エクスポート/CLI	
		キーを押します	実施しました	エクスポート/CLI	
		サーバID	実施しました	エクスポート/CLI	
		スループット読み取り	実施しました	エクスポート/CLI	
		合計スループット	実施しました	エクスポート/CLI	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	エクスポート/CLI	
		利用率の合計	実施しました	エクスポート/CLI	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
エクスポートユーティリティ（USPV）/SNM CLI（AMS）	エクスポート/CLI				正しくない	正しくない	正しくない	正しくない
HiCommand Device Manager XML API	HDS XML API	HTTP / HTTPS	2001		正しい	正しい	正しい	正しい

HDS HNAS（CLI）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
G600 HNAS 4100	14.6.7520.04

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					を説明するフリーテキスト
		UUID	実施しました	SSH	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			実施しました	SSH	ソフトウェアバージョン
	ストレージプール	データの使用容量	実施しました	SSH	
		重複排除が有効です	実施しました	SSH	ストレージプールで重複排除が有効になっている
		DWH容量に含める	実施しました	SSH	ACQからDWHのCapacityで対象となるストレージプールを制御する方法
		名前	実施しました	SSH	
		RAID グループ	実施しました	SSH	このストレージプールがRAIDグループかどうかを示します
		使用可能な物理比率	実施しました	SSH	使用可能容量から物理容量への変換率
		Snapshotの使用容量	実施しました	SSH	
		ストレージプールID	実施しました	SSH	
		シンプロビジョニングがサポートされます	実施しました	SSH	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		合計割り当て済み容量	実施しました	SSH	
		合計使用容量	実施しました	SSH	合計容量（MB）
		を入力します	ギャップ	SSH	
		仮想	実施しました	SSH	ストレージ仮想化デバイスですか？

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
HDS HNAS CLI	SSH	SSH	22		正しい	正しい	正しい	正しい

HPE Nimble / Alletra 6000ストレージ

このデータコレクタでサポートされるモデルとバージョン：

APIハアシヨン	モデル	ファームウェアバージョン
V1	AF40 AF80 HF60	5.0.3.100-575430 -オプト5.2.1.600-841103 -オプト

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	WWNエイリアス	ホストのエイリアス	実施しました	HTTPS	
		オブジェクトタイプ	実施しました	HTTPS	
		ソース	実施しました	HTTPS	
		WWN	実施しました	HTTPS	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス	ストレージ	失敗した物理容量	実施しました	HTTPS	
		物理容量	実施しました	HTTPS	
		スペアの物理容量	実施しました	HTTPS	スペアディスクの物理容量（スペアの全ディスクの合計）
		ストレージプールの容量	実施しました	HTTPS	
		IOPS：その他	実施しました	HTTPS	
		IOPS読み取り	実施しました	HTTPS	ディスクの読み取りIOPS数
		IOPSの合計	実施しました	HTTPS	
		IOPS -書き込み	実施しました	HTTPS	
		キーを押します	実施しました	HTTPS	
		レイテンシ読み取り	実施しました	HTTPS	
		レイテンシ合計	実施しました	HTTPS	
		レイテンシライト	実施しました	HTTPS	
		サーバID	実施しました	HTTPS	
		スループット読み取り	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
HP Nimble REST API	HTTPS	HTTPS	5392		正しい	正しくない	正しい	正しい

HUAWEI OceanStor（REST / HTTPS）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
5500 V3 6800 V3	V300R006C50

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		合計使用容量	実施しました	HTTPS	合計容量（MB）
		を入力します	ギャップ	HTTPS	
製品	カテゴリ	仮想ーチャー/属性（**Feature/Attribute**）	実施しました	使用するプロトコル	追加情報
	ボリューム	容量	実施しました	HTTPS	Snapshotの使用容量（MB単位）
		ジャンクションパス	実施しました	HTTPS	
		名前	実施しました	HTTPS	
		合計物理容量	実施しました	HTTPS	合計物理容量（アレイ上のすべてのディスクの合計）
		冗長性	実施しました	HTTPS	冗長性レベル
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニング	実施しました	HTTPS	
		UUID	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？
	ボリュームマップ	LUN	実施しました	HTTPS	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Huawei OceanStor REST API	HTTPS	HTTPS	8088		正しい	正しい	正しい	正しい
Huawei OceanStor パフォーマンスREST API	HTTPS	HTTPS	8088		正しい	正しくない	正しい	正しい

IBM SVC（CLI）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
2076-112 2076-124 2076-12F 2076-212 2076-224 2076-24G 2076-524 2076-624 2076-724 2076-824 2077-24F 2077-324 4657-924 4662-6H2 9840-AE1 9843-AE3 S3	1.5.2.5 1.6.1.0 1.6.1.5 7.8.1.11 7.8.1.13 7.8.1.5 7.8.1.7 7.8.1.8 8.1.3.5 8.1.3.6 8.2.1.11 8.2.1.8 8.3.1.2 8.3.1.5 8.4.0.10 8.5.0.11 8.5.0.11 8.5.0.11 8.5.0.9 8.5.3.1 8.6.0.4

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		書き込み済み容量	実施しました	SSH	ホストによってこのボリュームに書き込まれた合計容量（MB）
製品	カテゴリ	フィーチャー/属性縮が有効になりました **Feature Attribute**	ステータス	使用するプロトコル	追加情報
		暗号化	実施しました	SSH	
	ボリュームマップ	LUN	実施しました	SSH	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	SSH	
		ストレージポート	実施しました	SSH	
	ボリュームマスク	イニシエータ	実施しました	SSH	
		Protocol Controller（プロトコルコントローラ）	実施しました	SSH	
		ストレージポート	実施しました	SSH	
		を入力します	ギャップ	SSH	
	WWNエイリアス	ホストのエイリアス	実施しました	SSH	
		オブジェクトタイプ	実施しました	SSH	
		ソース	実施しました	SSH	
		WWN	実施しました	SSH	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		ト容量率です			れます
		使用容量の比率	実施しました	SSH	
製品	カテゴリ	フィールド/属性（Feature/Attribute）を押します	ステータス	使用するプロトコル	追加情報
		キーを押します	実施しました	SSH	
		サーバID	実施しました	SSH	
	ボリューム	物理容量	実施しました	SSH	
		合計容量	実施しました	SSH	
		使用済み容量	実施しました	SSH	
		書き込み済み容量	実施しました	SSH	
		使用容量の比率	実施しました	SSH	
		容量比率の書き込み	実施しました	SSH	
		キーを押します	実施しました	SSH	
		サーバID	実施しました	SSH	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
IBM SVC CLI	SSH	SSH	22		正しい	正しくない	正しい	正しい

Infinidat Infinibox（HTTP）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
F4304 F4304T F6260 F6306	7.1.14.0

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		トコルコントローラ）			
製品	カテゴリ	ストレージポート	実施しました	HTTPS	追加情報
		フィーチャー/属性（Feature/Attribute）を入力します	ステータス ギャップ	使用するプロトコル HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	WWNエイリアス	ホストのエイリアス	実施しました	HTTPS	
		オブジェクトタイプ	実施しました	HTTPS	
		ソース	実施しました	HTTPS	
		WWN	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Infinidat REST API	HTTPS	HTTPS	443		正しい	正しい	正しい	正しい

Microsoft Hyper-V

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		使用済み容量	実施しました	WMI		
	仮想マシンディスク	OID	実施しました	WMI		
製品	カテゴリ	フィーチャー属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報	
		VirtualDisk OID	実施しました	WMI		
		仮想マシンOID	実施しました	WMI		
	ホスト	ホストのCPU数	実施しました	WMI		
		ホストのCPU速度	実施しました	WMI		
		ホストドメイン	実施しました	WMI		
		ホストインストールメモリ	実施しました	WMI		
		ホストモデル	実施しました	WMI		
		NIC数	実施しました	WMI		
		NIC速度	実施しました	WMI		
		IPS	実施しました	WMI		
		メーカー	実施しました	WMI		
		名前	実施しました	WMI		
		OID	実施しました	WMI		
		プラットフォームタイプ	実施しました	WMI		
	情報	データソース名	実施しました	WMI	情報	
		日付	実施しました	WMI		
		発信者ID	実施しました	WMI		

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
PowerShell	WS-Management	HTTP	5985		正しい	正しくない	正しくない	正しい
WMI	WMI	WMI	135		正しい	正しくない	正しい	正しい

NetApp 7-Mode

このデータコレクタでサポートされるモデルとバージョン：

APIハアシヨン	モデル	ファームウェアバージョン
1.12 1.17 1.19 1.20 1.21	FAS2220 FAS2240-2 FAS2240-4 FAS2554 FAS3210 FAS3250 FAS3270 FAS6240 FAS8040 FAS8060 N6070	8.1.1 7-Mode 8.1.4P6 7-Mode 8.2.3P2 7-Mode 8.2.3P3 7-Mode 8.2.3P6 7-Mode 8.2.4P4 7-Mode 8.2.4P5 7-Mode 8.2.5P3 7-Mode 8.2.5P4 7-Mode Data ONTAPリリース7.3.3 Data ONTAPリリース7.3.4

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		ルID			
		シンプロビジョニング	実施しました		
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		を入力します	ギャップ		
		仮想容量	実施しました		
	ボリュームマップ	LUN	実施しました		バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました		
		を入力します	ギャップ		
	ボリュームマスク	イニシエータ	実施しました		
		Protocol Controller（プロトコルコントローラ）	実施しました		
		ストレージポート	実施しました		
		を入力します	ギャップ		

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

						込み）（MB/秒）
製品	カテゴリ	スループット書き込み	実施しました	使用するプロトコル	追加情報	
		イニチャー/属性（Feature/Attribute）	ステータス			
		利用率の合計	実施しました			
	ストレージプール	プロビジョニング済み容量	実施しました			
		物理容量	実施しました			
		合計容量	実施しました			
		使用済み容量	実施しました			
		オーバーコミット容量率です	実施しました		時系列で報告されます	
		使用容量の比率	実施しました			
		合計データ容量	実施しました			
		データの使用容量	実施しました			
		キーを押します	実施しました			
		サーバID	実施しました			
		Snapshotのリザーブ容量	実施しました			
		Snapshotの使用容量	実施しました			
		Snapshotの使用容量の比率	実施しました		時系列で報告されます	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
NetApp 7-Mode ZAPI	ZAPI	ZAPI			正しい	正しい	正しい	正しい

NetApp clustered Data ONTAP 8.1.1+

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
AFF-A150 AFF FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 - A200 FAS2240-A220 - A250 AFF - A300 FAS-A400 - A700 AFF - A700s AFF AFF FAS2620 FAS2650 FAS2720 FAS2750 - A800 - A900 AFF - C190 AFF - C250 - C400 AFF - C800 AFF8040 AFF8080 CDvM200 DM5100F FAS2240-2 FAS2520 FAS2552 FAS2554 AFF FAS3220 FAS8060 FAS8050 FAS8060 FAS8060 FAS8060 FAS500f FAS8080 AFF FAS8060 AFF FAS8080 AFF FAS8080 AFF FAS8080 AFF	12.1P114.11 P12.1P5 8.2.4P3 8.3.1P2 8.3.2 8.3.2P5 8.3.2P8 9.1.0 9.1.0P19 9.1.0P20 9.10.1P11 9.10.1P12 9.10.1P13 9.10.1P14 9.10.1P15 9.10.1P14 9.10.1P18 9.10.1P9.11 9.11.5 P9.11 P9.11 P9.11

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		QoS制限IOPS	実施しました	HTTPS	
		QoS制限MBps	実施しました	HTTPS	
		QoS制限（物理ポリシー	実施しました	HTTPS	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		Qos	実施しました	HTTPS	
	ボリュームマップ	LUN	実施しました	HTTPS	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		書き込み	実施しました			
		読み取り利用率	実施しました	HTTPS		
製品	カテゴリ	利用率の合計	実施しました	HTTPS	追加情報	
		利用率ライト	実施しました	HTTPS		
	ボリューム	キーを押します	実施しました	HTTPS		
		サーバID	実施しました	HTTPS		
		スループット読み取り	実施しました	HTTPS		
		スループット書き込み	実施しました	HTTPS		
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）	
		レイテンシ読み取り	実施しました	HTTPS		
		レイテンシライト	実施しました	HTTPS		
		レイテンシ合計	実施しました	HTTPS		
		IOPS読み取り	実施しました	HTTPS	ディスクの読み取りIOPS数	
		IOPS -書き込み	実施しました	HTTPS		
		IOPSの合計	実施しました	HTTPS		
		部分ブロック率	実施しました	HTTPS		

フィーチャー/属性（Feature/Attribute）
ステータス
使用するプロトコル

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
NetApp ONTAP API	HTTP / HTTPS	HTTP / HTTPS	80 / 443		正しい	正しい	正しい	正しい

NetApp SolidFire 8.1+

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
H410S-1 SF19210 SF2405 SF38410 SF4805 FC0025 FCN001 H410S-0 H610S-1 SF19210 SF2405 SF38410 SF4805	11.1.0.72 11.3.1.5 12.3.0.958 12.3.1.103 12.3.2.3 12.5.0.897 12.7.0.380 9.3.0.40

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		トIOPS			
		QoS制限IOPS	実施しました	HTTPS	
製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
		QoS最小IOPS	実施しました	HTTPS	
		QoSポリシー	実施しました	HTTPS	
	ボリュームマップ	LUN	実施しました	HTTPS	バックエンドLUNの名前
		マスキングが必要です	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

		その他の合計容量	実施しました	HTTPS	
		その他の使用容量	実施しました	HTTPS	
製品	カテゴリ	フィーチャー属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
		サーバID	実施しました	HTTPS	
	ボリューム	物理容量	実施しました	HTTPS	
		合計容量	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		使用容量の比率	実施しました	HTTPS	
		圧縮による総削減量	実施しました	HTTPS	
		IOPS読み取り	実施しました	HTTPS	ディスクの読み取りIOPS数
		IOPSの合計	実施しました	HTTPS	
		IOPS -書き込み	実施しました	HTTPS	
		キーを押します	実施しました	HTTPS	
		レイテンシ読み取り	実施しました	HTTPS	
		レイテンシ合計	実施しました	HTTPS	
		レイテンシライト	実施しました	HTTPS	
		部分ブロック率	実施しました	HTTPS	
		サーバID	実施しました	HTTPS	
		スループット読み取り	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	
		利用率の合計	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
SolidFire REST API	HTTPS	HTTPS	443		正しい	正しい	正しい	正しい

NetApp StorageGRID（HTTPS）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
Webスケール	11.6.0.11 11.6.0.7 11.7.0.4 11.7.0.8 11.8.0.5 3.1 3.4 3.5 4.0

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		量利用率（MB）			
		ノード-使用済み容量-使用済みメタデータ（MB）	実施しました	HTTPS	
製品	カテゴリ	ユーザー属性（Feature/Attribute）名	ステータス	使用するプロトコル	追加情報
		ノード	実施しました	HTTPS	
	ストレージプール	DWH容量に含める	実施しました	HTTPS	ACQからDWHのCapacityで対象となるストレージプールを制御する方法
		名前	実施しました	HTTPS	
		物理ディスク容量（MB）	実施しました	HTTPS	ストレージプールの物理容量として使用されます
		RAID グループ	実施しました	HTTPS	このストレージプールがRAIDグループかどうかを示します
		使用可能な物理比率	実施しました	HTTPS	使用可能容量から物理容量への変換率
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニングがサポートされます	実施しました	HTTPS	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		合計割り当て済み容量	実施しました	HTTPS	
		合計使用容量	実施しました	HTTPS	合計容量（MB）
		を入力します	ギャップ	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

		ストレージプールの容量	実施しました		
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）ID	ステータス	使用するプロトコル	追加情報
		キーを押します	実施しました		
		サーバID	実施しました		
	ストレージノードデータ	キーを押します	実施しました		
		ノード容量利用率-許容されるメタデータ	実施しました		
		ノードの容量利用率-合計	実施しました		
		ノード-使用可能容量利用率	実施しました		
		ノード使用容量利用率	実施しました		
		ノード-容量使用状況-使用済みメタデータ	実施しました		
		サーバID	実施しました		
		スループット読み取り	実施しました		
		合計スループット	実施しました		ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました		
	ストレージプール	プロビジョニング済み容量	実施しました		
		物理容量	実施しました		
		合計容量	実施しました		
		使用済み容量	実施しました		
		オーバーコミット容量率です	実施しました		時系列で報告されます
		使用容量の比率	実施しました		
		キーを押します	実施しました		
		サーバID	実施しました		

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
StorageGRID REST API	HTTPS	HTTPS	443		正しい	正しくない	正しい	正しい

Nutanixストレージ（REST）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
HX3310 NX-8150-G5 HX3310 HX3321 HX5510 NX-8155-G6 NX-8155-G7 XC640-10コアXC740xd-12 XC740xd-12コア	5.20.2.1 5.20.4.6 6.5.4 6.5.5 6.5.5.6 6.5.7 6.5.6.5 6.7.1.7 6.8 6.8.1

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		合計割り当て済み容量	実施しました	HTTPS	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		合計使用容量	実施しました	HTTPS	合計容量（MB）
		を入力します	ギャップ	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？
	ボリューム	容量	実施しました	HTTPS	Snapshotの使用容量（MB単位）
		ジャンクションパス	実施しました	HTTPS	
		名前	実施しました	HTTPS	
		qtree ID	実施しました	HTTPS	qtreeの一意のID
		合計物理容量	実施しました	HTTPS	合計物理容量（アレイ上のすべてのディスクの合計）
		冗長性	実施しました	HTTPS	冗長性レベル
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニング	実施しました	HTTPS	
		UUID	実施しました	HTTPS	
	ボリュームマップ	LUN	実施しました	HTTPS	バックエンドLUNの名前
		ストレージポート	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	ストレージポート	実施しました	HTTPS	
		イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス	ストレージ	失敗した物理容量	実施しました	HTTPS	
		物理容量	実施しました	HTTPS	
		スペアの物理容量	実施しました	HTTPS	スペアディスクの物理容量（スペアの全ディスクの合計）
		ストレージプールの容量	実施しました	HTTPS	
		IOPS：その他	実施しました	HTTPS	
		IOPS読み取り	実施しました	HTTPS	ディスクの読み取りIOPS数
		IOPSの合計	実施しました	HTTPS	
		IOPS -書き込み	実施しました	HTTPS	
		キーを押します	実施しました	HTTPS	
		レイテンシ読み取り	実施しました	HTTPS	
		レイテンシ合計	実施しました	HTTPS	
		レイテンシライト	実施しました	HTTPS	
		サーバID	実施しました	HTTPS	
		スループット読み取り	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Nutanix REST API	HTTPS	HTTPS	443		正しい	正しい	正しい	正しい

Oracle ZFS（HTTPS）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
Sun ZFS Storage 7330 Sun ZFS Storage 7420 Sun ZFS Storage 7430	1-1.1 2013.06.05.7.28

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		UUID	実施しました	HTTP/S	
		使用済み容量	実施しました	HTTP/S	
製品	カテゴリ	仮想ーチャー/属性（**Feature/Attribute**）	実施しました	使用するプロトコル	追加情報ジ仮想化デバイスですか？
	ボリュームマップ	LUN	実施しました	HTTP/S	バックエンドLUNの名前
		マスキングが必要です	実施しました	HTTP/S	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTP/S	
		ストレージポート	実施しました	HTTP/S	
		を入力します	ギャップ	HTTP/S	
	ボリュームマスク	イニシエータ	実施しました	HTTP/S	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTP/S	
		ストレージポート	実施しました	HTTP/S	
		を入力します	ギャップ	HTTP/S	
パフォーマンス	ストレージノードデータ	キャッシュヒット率の合計	実施しました		
		IOPSの合計	実施しました		
		キーを押します	実施しました		
		サーバID	実施しました		
		利用率の合計	実施しました		

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Oracle ZFS REST API	HTTP / HTTPS	HTTP / HTTPS	215		正しい	正しい	正しい	正しい

Pure Storage FlashArray（HTTP）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
DFSC1 FA - X20R3 FA - X50R2 FA - X70R3 FA - X70R4 FA - X90R2 FA - X90R3 FA - X90R4	6.1.21 6.3.1 6.3.10 6.3.9 6.5.1 6.5.2 6.5.4

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		を入力します	ギャップ	HTTP/S	
		使用済み容量	実施しました	HTTP/S	
製品	カテゴリ	仮想ーチャー/属性（**Feature/Attribute**）	実施しました	使用するプロトコル	追加情報ジ仮想化デバイスですか？
	ボリュームマップ	LUN	実施しました	HTTP/S	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTP/S	
		ストレージポート	実施しました	HTTP/S	
		を入力します	ギャップ	HTTP/S	
	ボリュームマスク	イニシエータ	実施しました	HTTP/S	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTP/S	
		ストレージポート	実施しました	HTTP/S	
		を入力します	ギャップ	HTTP/S	
	WWNエイリアス	ホストのエイリアス	実施しました	HTTP/S	
		オブジェクトタイプ	実施しました	HTTP/S	
		ソース	実施しました	HTTP/S	
		WWN	実施しました	HTTP/S	

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス	ストレージ	失敗した物理容量	実施しました		
		物理容量	実施しました		
		スペアの物理容量	実施しました		スペアディスクの物理容量（スペアの全ディスクの合計）
		ストレージプールの容量	実施しました		
		IOPS：その他	実施しました		
		IOPS読み取り	実施しました		ディスクの読み取りIOPS数
		IOPSの合計	実施しました		
		IOPS -書き込み	実施しました		
		キーを押します	実施しました		
		レイテンシ読み取り	実施しました		
		レイテンシ合計	実施しました		
		レイテンシライト	実施しました		
		サーバID	実施しました		
		スループット読み取り	実施しました		
		合計スループット	実施しました		ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました		

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Pure Storage REST API	HTTP / HTTPS	HTTP / HTTPS	80 / 443		正しい	正しい	正しい	正しい

VMware vSphere（Webサービス）

このデータコレクタでサポートされるモデルとバージョン：

APIバージョン：

- VMware vCenter Server 5.5.0ビルド1750787
- VMware vCenter Server 5.5.0ビルド3252642
- VMware vCenter Server 5.5.0ビルド4180647
- VMware vCenter Server 5.5.0ビルド-9911218
- VMware vCenter Server 6.0.0ビルド13638472
- VMware vCenter Server 6.0.0ビルド14510545
- VMware vCenter Server 6.0.0ビルド-4541947
- VMware vCenter Server 6.0.0ビルド-5318200
- VMware vCenter Server 6.0.0ビルド9313458
- VMware vCenter Server 6.5.0ビルド10964411
- VMware vCenter Server 6.5.0ビルド17994927
- VMware vCenter Server 6.5.0ビルド18499837
- VMware vCenter Server 6.5.0ビルド-18711281
- VMware vCenter Server 6.5.0ビルド-19757181
- VMware vCenter Server 6.5.0ビルド-22499743
- VMware vCenter Server 6.5.0ビルド-7515524
- VMware vCenter Server 6.5.0ビルド-9451637
- VMware vCenter Server 6.7.0ビルド-16046713
- VMware vCenter Server 6.7.0ビルド18485185
- VMware vCenter Server 6.7.0ビルド19299595
- VMware vCenter Server 6.7.0ビルド-19832280
- VMware vCenter Server 6.7.0ビルド20504362
- VMware vCenter Server 6.7.0ビルド-22509732

- VMware vCenter Server 6.7.0ビルド-22509751
- VMware vCenter Server 7.0.1ビルド17491160
- VMware vCenter Server 7.0.3ビルド19234570
- VMware vCenter Server 7.0.3ビルド-19717403
- VMware vCenter Server 7.0.3ビルド- 20051473
- VMware vCenter Server 7.0.3ビルド- 20150588
- VMware vCenter Server 7.0.3ビルド-20395099
- VMware vCenter Server 7.0.3ビルド20845200
- VMware vCenter Server 7.0.3ビルド-20990077
- VMware vCenter Server 7.0.3ビルド-21290409
- VMware vCenter Server 7.0.3ビルド-21477706
- VMware vCenter Server 7.0.3ビルド-21784236
- VMware vCenter Server 7.0.3ビルド-22357613
- VMware vCenter Server 7.0.3ビルド-22837322
- VMware vCenter Server 7.0.3ビルド-23788036
- VMware vCenter Server 7.0.3ビルド-24026615
- VMware vCenter Server 8.0.1ビルド-22368047
- VMware vCenter Server 8.0.1ビルド-22742005
- VMware vCenter Server 8.0.1ビルド-23525738
- VMware vCenter Server 8.0.1ビルド-24005165
- VMware vCenter Server 8.0.2ビルド-22385739
- VMware vCenter Server 8.0.2ビルド-22617221
- VMware vCenter Server 8.0.2ビルド-23319993
- VMware vCenter Server 8.0.2ビルド-23504390
- VMware vCenter Server 8.0.2ビルド-23929136
- VMware vCenter Server 8.0.3ビルド-24022515
- VMware vCenter Server 8.0.3ビルド-24091160

このデータコレクタでサポートされる製品：

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

製品	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		使用済み容量	実施しました	Webサービス	
	仮想マシンディスク	OID	実施しました	Webサービス	
製品	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		VirtualDisk OID	実施しました	Webサービス	
		仮想マシンOID	実施しました	Webサービス	
	ホスト	ホストのCPU数	実施しました	Webサービス	
		ホストのCPU速度	実施しました	Webサービス	
		ホストドメイン	実施しました	Webサービス	
		ホストインストールメモリ	実施しました	Webサービス	
		ホストモデル	実施しました	Webサービス	
		NIC数	実施しました	Webサービス	
		NIC速度	実施しました	Webサービス	
		IPS	実施しました	Webサービス	
		メーカー	実施しました	Webサービス	
		名前	実施しました	Webサービス	
		OID	実施しました	Webサービス	
		プラットフォームタイプ	実施しました	Webサービス	
	iSCSIノード	ホストのエイリアス	実施しました	Webサービス	
		ノード名	実施しました	Webサービス	
		OID	実施しました	Webサービス	
		を入力します	ギャップ	Webサービス	
	情報	API概要 の略	実施しました	Webサービス	
		API名	実施しました	Webサービス	
		APIのバージョン	実施しました	Webサービス	
		クライアントAPI名	実施しました	Webサービス	
		クライアントAPIバージョン	実施しました	Webサービス	
		データソース名	実施しました	Webサービス	情報
		日付	実施しました	Webサービス	
		発信者ID	実施しました	Webサービス	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
VMware REST API	Webサービス	HTTP / HTTPS	80 / 443		正しい	正しい	正しい	正しい

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。