Insightをセットアップしています

OnCommand Insight

NetApp
April 01, 2024

目次

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
     ```

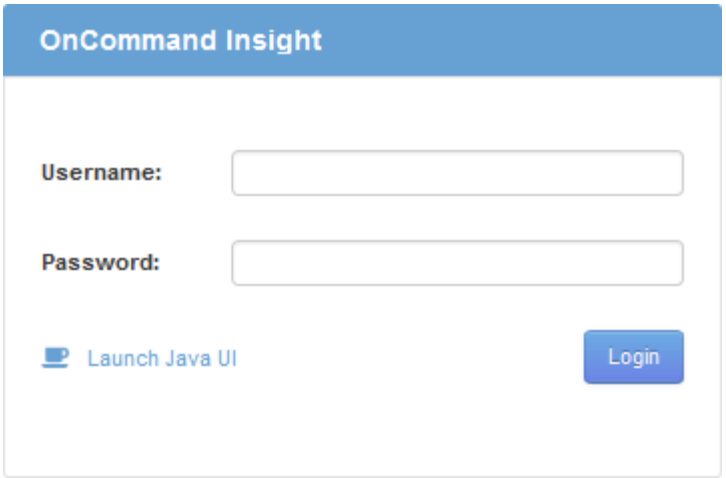
   - その他の場所からInsightを開きます。

     ```
     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。

> 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。

> 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。

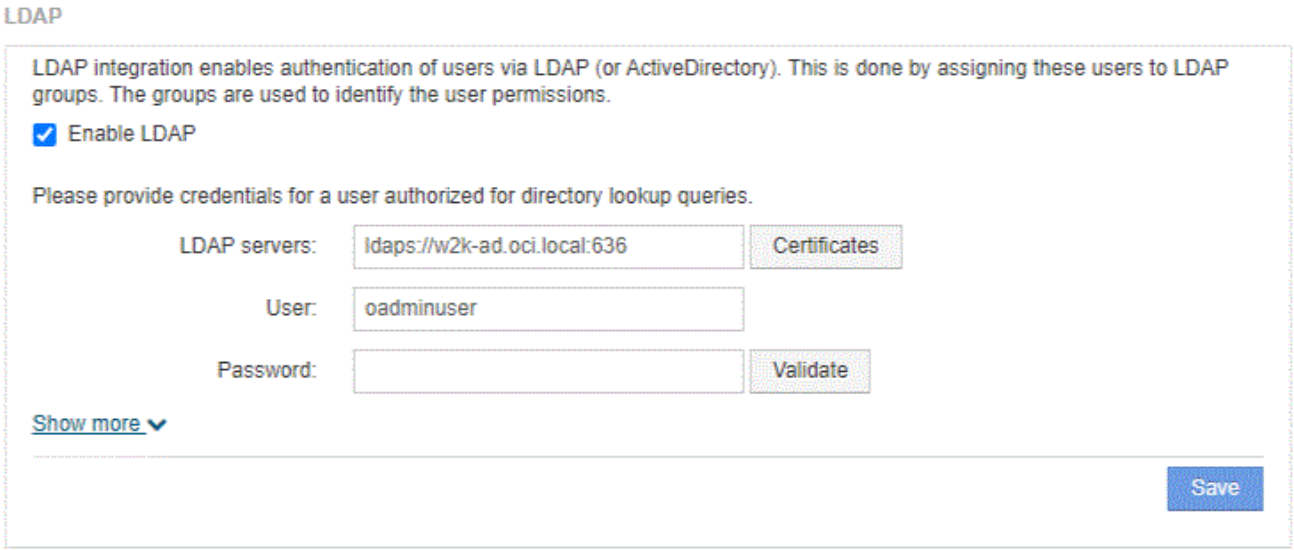
このタスクについて

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（次の図を参照）。



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。

Insightセキュリティ

OnCommand Insight の7.3.1リリースでは、強化されたセキュリティでInsight環境を運用できるようにセキュリティ機能が導入されました。暗号化、パスワードハッシュの強化、内部ユーザパスワードの変更、パスワードの暗号化と復号化を行うキーペアの変更などが含まれます。これらの機能は、Insight環境内のすべてのサーバで管理できます。

Insightのデフォルトのインストールには、環境内のすべてのサイトで同じキーと同じデフォルトパスワードを共有するセキュリティ設定が含まれています。機密データを保護するために、インストールまたはアップグレード後にデフォルトのキーとAcquisitionユーザのパスワードを変更することを推奨します。

データソースで暗号化されたパスワードは、Insight Serverデータベースに保存されます。サーバには公開鍵があり、ユーザがWebUIデータソース設定ページにパスワードを入力すると暗号化されます。サーバーには、サーバーデータベースに保存されているデータソースパスワードの復号化に必要な秘密鍵がありません。データソースのパスワードの復号化に必要なデータソースの秘密鍵があるのは、Acquisition Unit（LAU、RAU）だけです。

キーを変更しています

デフォルトキーを使用すると、環境にセキュリティの脆弱性が発生します。デフォルトでは、データソースのパスワードはInsightデータベースに暗号化されて保存されます。すべてのInsight環境に共通のキーを使用して暗号化されます。デフォルトの設定では、ネットアップに送信されるInsightデータベースには、理論的にはネットアップが復号化できるパスワードが含まれています。

取得ユーザのパスワードを変更しています

デフォルトの「Acquisition」ユーザパスワードを使用すると、環境にセキュリティの脆弱性がもたらされます。すべてのAcquisition Unitが「Acquisition」ユーザを使用してサーバと通信します。デフォルトのパスワー

ドを使用するRAUは、理論的にはデフォルトのパスワードを使用して任意のInsightサーバに接続できます。

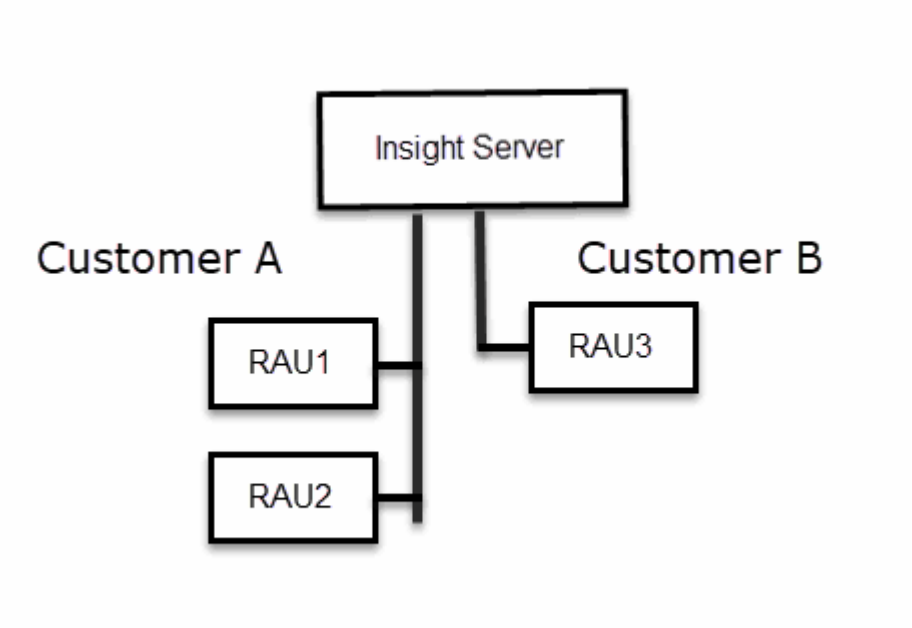
アップグレードとインストールに関する考慮事項

Insightシステムにデフォルト以外のセキュリティ設定が含まれている場合（パスワードのキーを変更または変更した場合）は、セキュリティ設定をバックアップする必要があります。新しいソフトウェアをインストールするか、ソフトウェアをアップグレードする場合によっては、システムをデフォルトのセキュリティ設定に戻します。システムがデフォルトの設定に戻ったら、システムを正常に動作させるために、デフォルト以外の設定をリストアする必要があります。

複雑なサービスプロバイダ環境でのキーの管理

サービスプロバイダは、データを収集する複数のOnCommand Insight 顧客をホストできます。これらのキーは、Insight Server上の複数のお客様による不正アクセスからお客様のデータを保護します。各お客様のデータは、それぞれのキーペアによって保護されます。

このInsightの実装は、次の図のように設定できます。



この構成では、顧客ごとに個別のキーを作成する必要があります。お客様Aでは、両方のRAUに同一のキーが必要です。顧客Bは単一のキーセットを必要とします。

顧客Aの暗号化キーを変更する手順は次のとおりです。

1. RAU1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. セキュリティ管理ツールを起動します。
3. デフォルトのキーを置き換えるには、[Change Encryption Key]を選択します。
4. [Backup]を選択して、セキュリティ設定のバックアップzipファイルを作成します。
5. RAU2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。
6. セキュリティ設定のバックアップzipファイルをRAU2にコピーします。
7. セキュリティ管理ツールを起動します。

8. RAU1から現在のサーバにセキュリティバックアップをリストアします。

顧客Bの暗号化キーを変更する手順は次のとおりです。

1. RAU3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. セキュリティ管理ツールを起動します。
3. デフォルトのキーを置き換えるには、[Change Encryption Key]を選択します。
4. [Backup]を選択して、セキュリティ設定のバックアップzipファイルを作成します。

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`

手順

1. Insight Serverへのリモートログインを実行します。
2. 対話型モードでセキュリティ管理ツールを起動します。
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     ログインクレデンシャルが要求されます。
3. 「Admin」クレデンシャルを持つアカウントのユーザ名とパスワードを入力します。
4. 「 * サーバー * 」を選択します。

   次のサーバ設定オプションを使用できます。

   - * バックアップ *

     すべてのパスワードとキーが格納されているバックアップのzipファイルを作成し、そのファイルをユーザが指定した場所、または次のデフォルトの場所に置きます。

     - Windows - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`
   - * 復元 *

作成したバックアップのzipファイルをリストアします。リストアすると、すべてのパスワードとキーがバックアップ作成時の既存の値に戻ります。

> リストアを使用すると、複数のサーバのパスワードとキーを同期できます。例：- 1台のサーバでサーバ暗号化キーを変更-ヴォールトのバックアップを作成-ヴォールトバックアップを2台目のサーバにリストアします

- 暗号化キーの変更

  プロキシユーザパスワード、SMTPユーザパスワード、LDAPユーザパスワードなどの暗号化または復号化に使用するサーバ暗号化キーを変更します。

  > 暗号化キーを変更する場合は、アップグレードまたはインストール後にリストアできるように、新しいセキュリティ設定をバックアップする必要があります。

- パスワードの更新

  Insightで使用される内部アカウントのパスワードを変更します。次のオプションが表示されます。

  - _internal
  - 取得
  - cognos_adminをクリックします
  - dwh_internalの略
  - ホスト
  - 在庫
  - ルート

> 一部のアカウントは、パスワードを変更したときに同期する必要があります。たとえば、サーバで「acquisition」ユーザのパスワードを変更した場合は、LAU、RAU、DWHでも「acquisition」ユーザのパスワードを同じパスワードに変更する必要があります。また、パスワードを変更する場合は、アップグレードまたはインストール後に復元できるように、新しいセキュリティ設定をバックアップする必要があります。

- デフォルトにリセット

  キーとパスワードをデフォルト値にリセットします。デフォルト値はインストール時に指定された値です。

- * 終了 *

  を終了します `securityadmin` ツール。

  a. 変更するオプションを選択し、プロンプトの指示に従います。

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`

手順

1. Insight Serverへのリモートログインを実行します。
2. 対話型モードでセキュリティ管理ツールを起動します。
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     ログインクレデンシャルが要求されます。
3. 「Admin」クレデンシャルを持つアカウントのユーザ名とパスワードを入力します。
4. Local Acquisition Unit *を選択して、Local Acquisition Unitのセキュリティ設定を再設定します。

   次のオプションが表示されます。

   - * バックアップ *

     すべてのパスワードとキーが格納されているバックアップのzipファイルを作成し、そのファイルをユーザが指定した場所、または次のデフォルトの場所に置きます。

     - Windows - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`
   - * 復元 *

     作成したバックアップのzipファイルをリストアします。リストアすると、すべてのパスワードとキーがバックアップ作成時の既存の値に戻ります。

     > リストアを使用すると、複数のサーバのパスワードとキーを同期できます。例：- LAUで暗号化キーを変更-ヴォールトのバックアップを作成-各RAUにヴォールトバックアップをリストアします

   - 暗号化キーの変更

     デバイスのパスワードの暗号化または復号化に使用するAU暗号化キーを変更します。

> 暗号化キーを変更する場合は、アップグレードまたはインストール後にリストアできるように、新しいセキュリティ設定をバックアップする必要があります。

- パスワードの更新

  「acquisition」ユーザアカウントのパスワードを変更します。

> 一部のアカウントは、パスワードを変更したときに同期する必要があります。たとえば、サーバで「acquisition」ユーザのパスワードを変更した場合は、LAU、RAU、DWHでも「acquisition」ユーザのパスワードを同じパスワードに変更する必要があります。また、パスワードを変更する場合は、アップグレードまたはインストール後に復元できるように、新しいセキュリティ設定をバックアップする必要があります。

- デフォルトにリセット

  acquisitionユーザのパスワードとacquisitionユーザの暗号化キーをデフォルト値にリセットします。デフォルト値はインストール時に指定したパスワードと暗号化キーです。

- * 終了 *

  を終了します `securityadmin` ツール。

5. 設定するオプションを選択し、プロンプトの指示に従います。

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「acquisition」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。すべてのRAUおよびLAUでは、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。

RAUでセキュリティオプションを管理するには、次の手順を実行します。

手順

1. RAUを実行しているサーバへのリモートログインを実行します

2. 対話型モードでセキュリティ管理ツールを起動します。
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     ログインクレデンシャルが要求されます。

3. 「Admin」クレデンシャルを持つアカウントのユーザ名とパスワードを入力します。

RAUのメニューが表示されます。

- * バックアップ *

  すべてのパスワードとキーが格納されているバックアップのzipファイルを作成し、そのファイルをユーザが指定した場所、または次のデフォルトの場所に置きます。

  - Windows - `C:\Program Files\SANscreen\backup\vault`
  - Linux - `/var/log/netapp/oci/backup/vault`

- * 復元 *

  作成したバックアップのzipファイルをリストアします。リストアすると、すべてのパスワードとキーがバックアップ作成時の既存の値に戻ります。

  > リストアを使用すると、複数のサーバのパスワードとキーを同期できます。例：- 1つのサーバで暗号化キーを変更-ヴォールトのバックアップを作成-ヴォールトバックアップを2つ目のサーバにリストアします

- 暗号化キーの変更

  デバイスパスワードの暗号化または復号化に使用するRAU暗号化キーを変更します。

  > 暗号化キーを変更する場合は、アップグレードまたはインストール後にリストアできるように、新しいセキュリティ設定をバックアップする必要があります。

- パスワードの更新

  「acquisition」ユーザアカウントのパスワードを変更します。

  > 一部のアカウントは、パスワードを変更したときに同期する必要があります。たとえば、サーバで「acquisition」ユーザのパスワードを変更した場合は、LAU、RAU、DWHでも「acquisition」ユーザのパスワードを同じパスワードに変更する必要があります。また、パスワードを変更する場合は、アップグレードまたはインストール後に復元できるように、新しいセキュリティ設定をバックアップする必要があります。

- デフォルトにリセット

  暗号化キーとパスワードをデフォルト値にリセットします。デフォルト値はインストール時に指定された値です。

- * 終了 *

を終了します `securityadmin` ツール。

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`

手順

1. Data Warehouseサーバへのリモートログインを実行します。
2. 対話型モードでセキュリティ管理ツールを起動します。
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     ログインクレデンシャルが要求されます。
3. 「Admin」クレデンシャルを持つアカウントのユーザ名とパスワードを入力します。

   Data Warehouseのセキュリティ管理メニューが表示されます。

   - * バックアップ *

     すべてのパスワードとキーが格納されたバックアップのzipファイルを作成し、ユーザが指定した場所、またはデフォルトの場所にファイルを配置します。

     - Windows - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`
   - * 復元 *

     作成したバックアップのzipファイルをリストアします。リストアすると、すべてのパスワードとキーがバックアップ作成時の既存の値に戻ります。

     リストアを使用すると、複数のサーバのパスワードとキーを同期できます。例：- 1つのサーバで暗号化キーを変更-ヴォールトのバックアップを作成-ヴォールトバックアップを2つ目のサーバにリストアします

     [+]

- 暗号化キーの変更

  コネクタのパスワードやSMPTのパスワードなど、パスワードの暗号化や復号化に使用するDWH暗号化キーを変更します。

- パスワードの更新

  特定のユーザアカウントのパスワードを変更します。

  - _internal
  - 取得
  - cognos_adminをクリックします
  - DWH
  - dwh_internalの略
  - 誰だ
  - ホスト
  - 在庫
  - ルート

> dwhuser、hosts、inventory、またはrootのパスワードを変更する場合は、SHA-256パスワードハッシュを使用できます。このオプションでは、アカウントにアクセスするすべてのクライアントがSSL接続を使用する必要があります。

+

- デフォルトにリセット

  暗号化キーとパスワードをデフォルト値にリセットします。デフォルト値はインストール時に指定された値です。

- * 終了 *

  を終了します `securityadmin` ツール。

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。

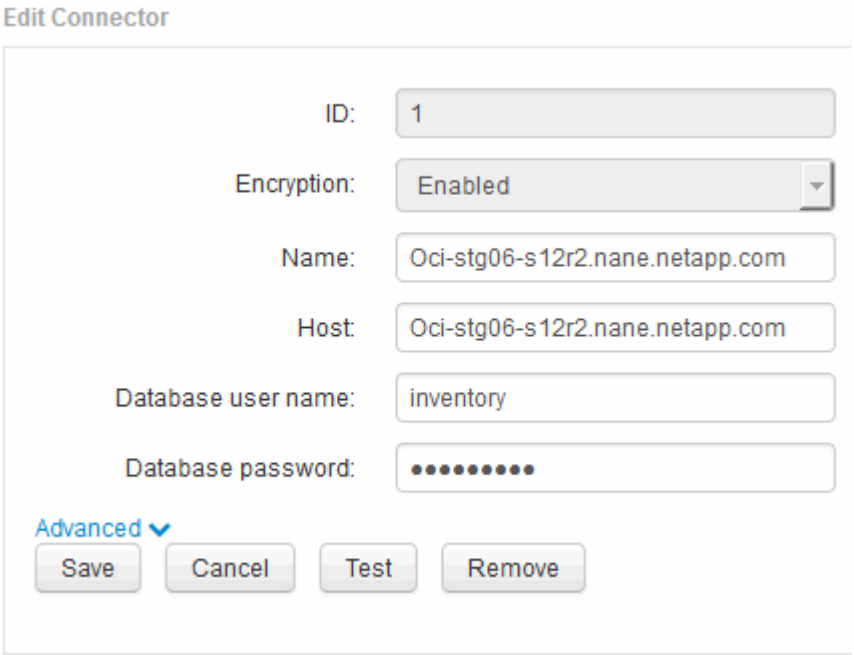
作業を開始する前に

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

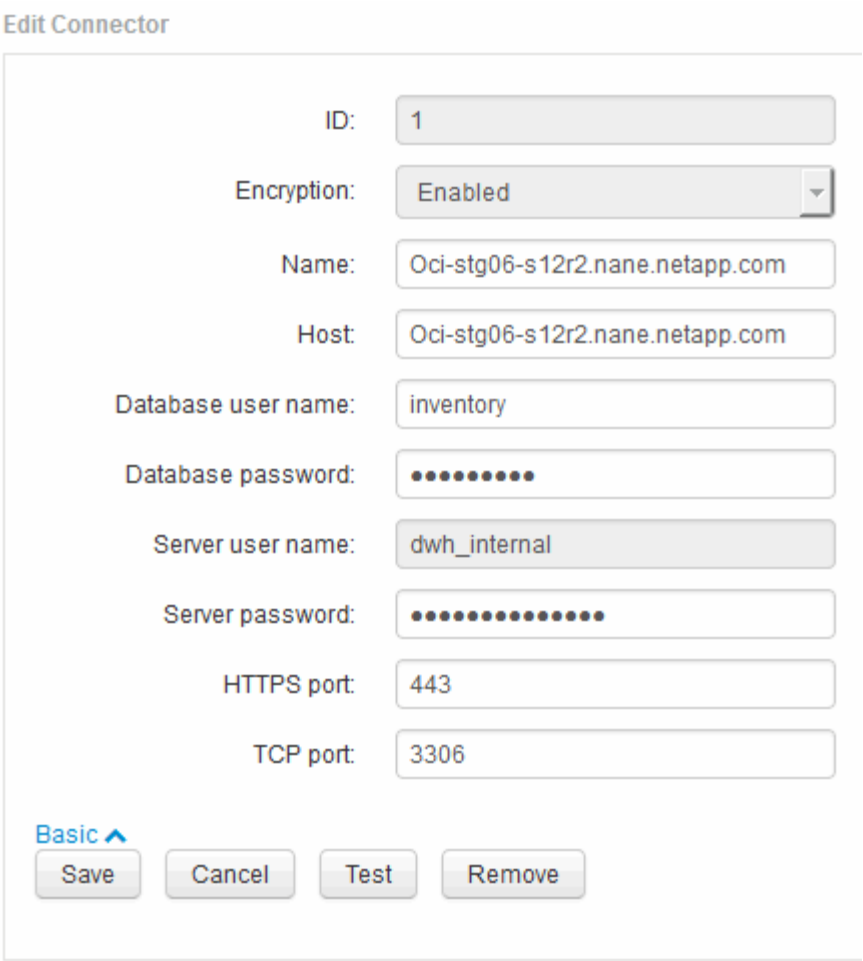
1. Data Warehouseポータルにログインします https://hostname/dwhhostnameは、OnCommand Insight Data Warehouseがインストールされているシステムの名前です。
2. 左側のナビゲーションペインで、*[コネクタ]*をクリックします。

   [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。

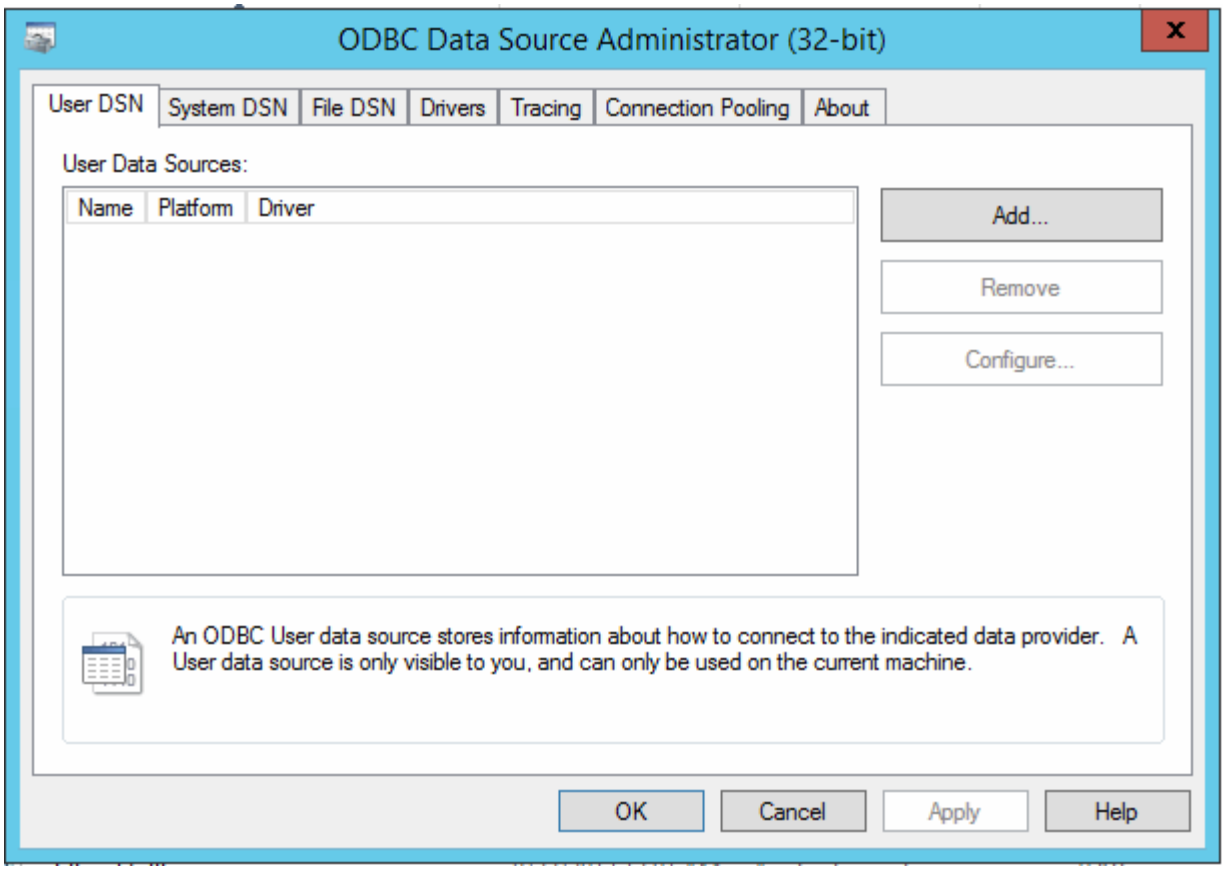
作業を開始する前に

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

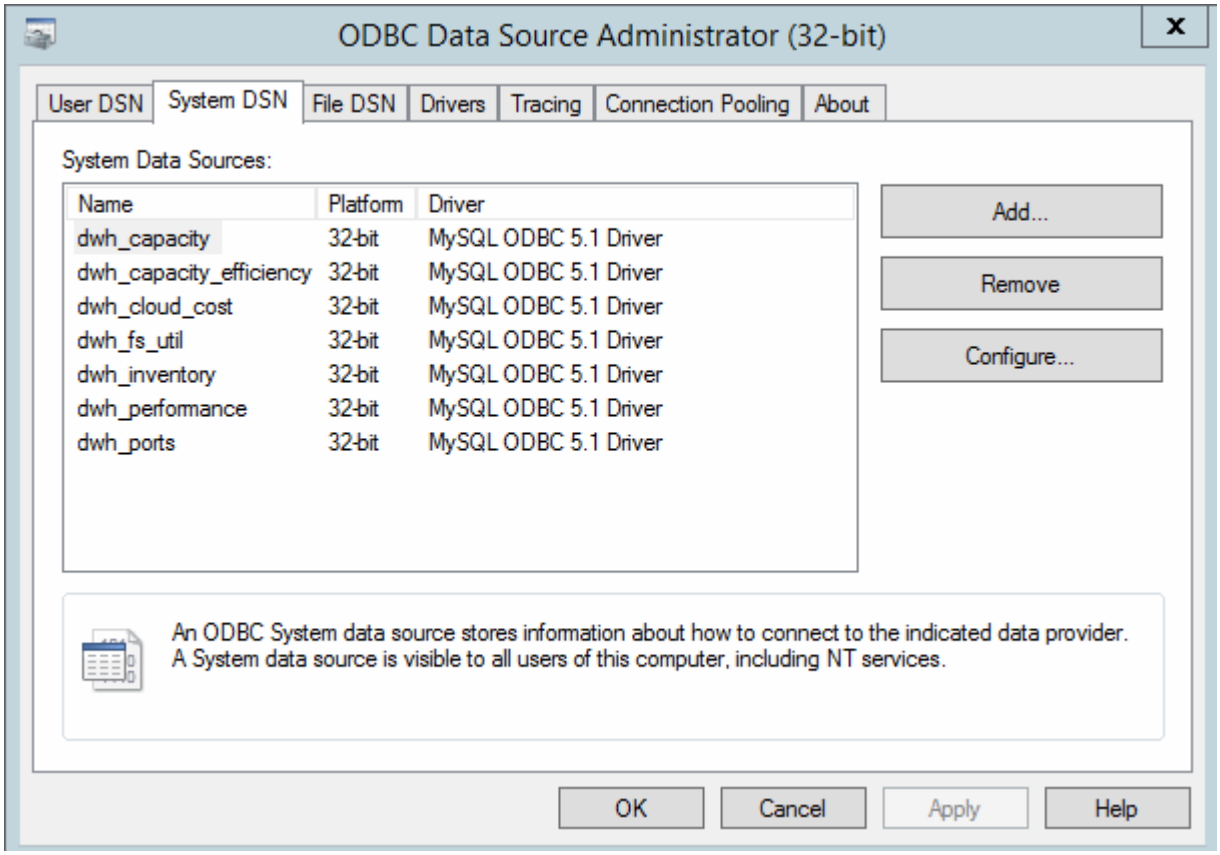
1. Data Warehouseをホストしているサーバへのリモートログインを実行します。
2. ODBC Administrationツールにアクセスします `C:\Windows\SysWOW64\odbcad32.exe`

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



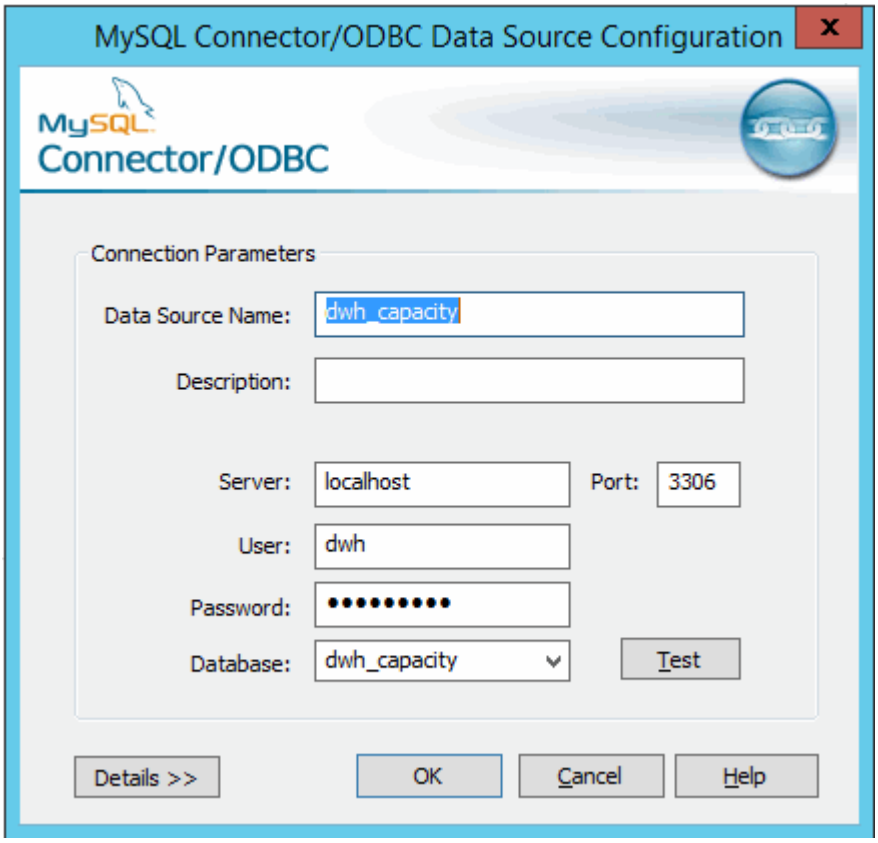
3. [システムDSN]*をクリックします

   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on Command 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。

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on Command 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。

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. 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.keystore`

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。

> 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. を使用します `keytool` 信頼されたCAをリスト表示するユーティリティ： `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore`

```
-storepass changeit
```

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 7.3.5~7.3.9**）

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 7.3.5~7.3.9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. を使用します `keytool` 信頼されたCAをリスト表示するユーティリティ：
      ```
      ..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet
      ```
      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：
      ```
      ..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -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。
   f. パスワードの入力を求められたら、と入力します `NoPassWordSet`。
   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、を実行します `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. CACモードをディセーブルにするには、を実行します `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

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. を使用します `keytool` 信頼されたCAをリスト表示するユーティリティ： `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      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、でCAを簡単に識別できるエイリアスです`keytool -list` 操作。
   f. パスワードの入力を求められたら、と入力します `NoPassWordSet`。
   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用のCA署名SSL証明書のインポート（Insight 7.3.5から7.3.9）

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、OnCommnand Insight 7.3.5~7.3.9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. のバックアップを作成します `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`。
2. の下にある「certs」フォルダと「csk」フォルダのバックアップを作成します `..\SANScreen\cognos\analytics\configuration`。
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 NoPassWordSet -a RSA -d “CN=FQDN,O=orgname,C=US” -r c:\temp\encryptRequest.csr`
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を認証局（CA）に送信してSSL証明書を取得します。

   「`S an：dns=fqdn」のような属性を追加してください(例: hostname.netapp.com)`"はSubjectAltNameを追加します)。Google Chromeバージョン58以降では、証明書にSubjectAltNameがない場合に苦情が表示されます。

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8c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intermediate.cerを開き、コンテンツをコピーします。
   b. メモ帳でroot.cerを開き、9aの内容を保存します。
   c. ファイルをCA.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\ca.cer

   これにより、CA.cerがルート認証局として設定されます。

c. ThirdPartyCertificateTool.bat - java：local -i -e -r c：\temp\cognos.cer -t c：\temp\ca.cer

   これにより、cognos.cerがca.cerによって署名された暗号化証明書として設定されます。

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. "D：\Program Files\SANscreen\Java\bin\keytool .exe"-exportcert -file “c：\temp\cognos.crt”-keystore" D：\Program Files\SANscreen\cognos\analytics\configuration\certs\CAMKeystore"-storetype PKCS12 -storepass NoPassWordSet -alias -alias

13. 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. "D：\Program Files\SANscreen\Java\bin\keytool .exe"-importcert -file “c：\temp\cognos.crt”-keystore" D：\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"-storepass changeit -alias cognoscert

14. SANscreen サービスを再起動します。

15. 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。

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 NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d “CN=server.domain.com,O=NETAPP,C=US” -H “server.domain.com” -I “ipaddress”`。注意:ここで-Hと-IはdnsやipaddressのようなsubjectAltNamesを追加します。
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 NoPassWordSet -alias encryption
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 changeit -alias cognos3rdca
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 changeit -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。

> 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. を使用します `keytool` 信頼されたCAをリスト表示するユーティリティ： `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      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 7.3.5~7.3.9）

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 7.3.5~7.3.9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. を使用します `keytool` 信頼されたCAをリスト表示するユーティリティ：
   ```
   ..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet
   ```
   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：
   ```
   ..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -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。
   f. パスワードの入力を求められたら、と入力します `NoPassWordSet`。
   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、を実行します `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. CACモードをディセーブルにするには、を実行します `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

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. を使用します `keytool` 信頼されたCAをリスト表示するユーティリティ： `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      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、でCAを簡単に識別できるエイリアスです`keytool -list` 操作。
   f. パスワードの入力を求められたら、と入力します `NoPassWordSet`。

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用のCA署名SSL証明書のインポート（Insight 7.3.5から7.3.9）

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、OnCommnand Insight 7.3.5~7.3.9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. のバックアップを作成します `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`。
2. の下にある「certs」フォルダと「csk」フォルダのバックアップを作成します `..\SANScreen\cognos\analytics\configuration`。
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 NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr`
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を認証局（CA）に送信してSSL証明書を取得します。

   「`S an：dns=fqdn」のような属性を追加してください(例: hostname.netapp.com)`"はSubjectAltNameを追加します)。Google Chromeバージョン58以降では、証明書にSubjectAltNameがない場合に苦情が表示されます。

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8c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intermediate.cerを開き、コンテンツをコピーします。

   b. メモ帳でroot.cerを開き、9aの内容を保存します。

   c. ファイルをCA.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\ca.cer

       これにより、CA.cerがルート認証局として設定されます。

    c. ThirdPartyCertificateTool.bat - java：local -i -e -r c：\temp\cognos.cer -t c：\temp\ca.cer

       これにより、cognos.cerがca.cerによって署名された暗号化証明書として設定されます。

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. "D：\Program Files\SANscreen\Java\bin\keytool .exe"-exportcert -file “c：\temp\cognos.crt”-keystore" D：\Program Files\SANscreen\cognos\analytics\configuration\certs\CAMKeystore"-storetype PKCS12 -storepass NoPassWordSet -alias -alias

13. 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. "D：\Program Files\SANscreen\Java\bin\keytool .exe"-importcert -file “c：\temp\cognos.crt”-keystore" D：\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"-storepass changeit -alias cognoscert

14. SANscreen サービスを再起動します。

15. 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。

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 NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d “CN=server.domain.com,O=NETAPP,C=US” -H “server.domain.com” -I “ipaddress”`。注意:ここで-Hと-IはdnsやipaddressのようなsubjectAltNamesを追加します。
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 NoPassWordSet -alias encryption
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 changeit -alias cognos3rdca

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 changeit -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

> この手順 を実行する前に、既存のをバックアップしておく必要があります `server.keystore` をクリックし、バックアップに名前を付けます `server.keystore.old`。の破損または損傷 `server.keystore` ファイルを使用すると、Insight Serverの再起動後にInsight Serverが動作しなくなることがあります。バックアップを作成した場合、問題が発生したときに古いファイルに戻すことができます。

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"`

    a. パスワードの入力を求められたら、と入力します `changeit`。

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 ✚Add 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 Actions ▾ 。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 Actions ▾ 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 ✚Add 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 ✚Add 。

   [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 ✚Add 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 ✚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。
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 。

   [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。

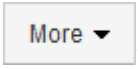
手順

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。

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。

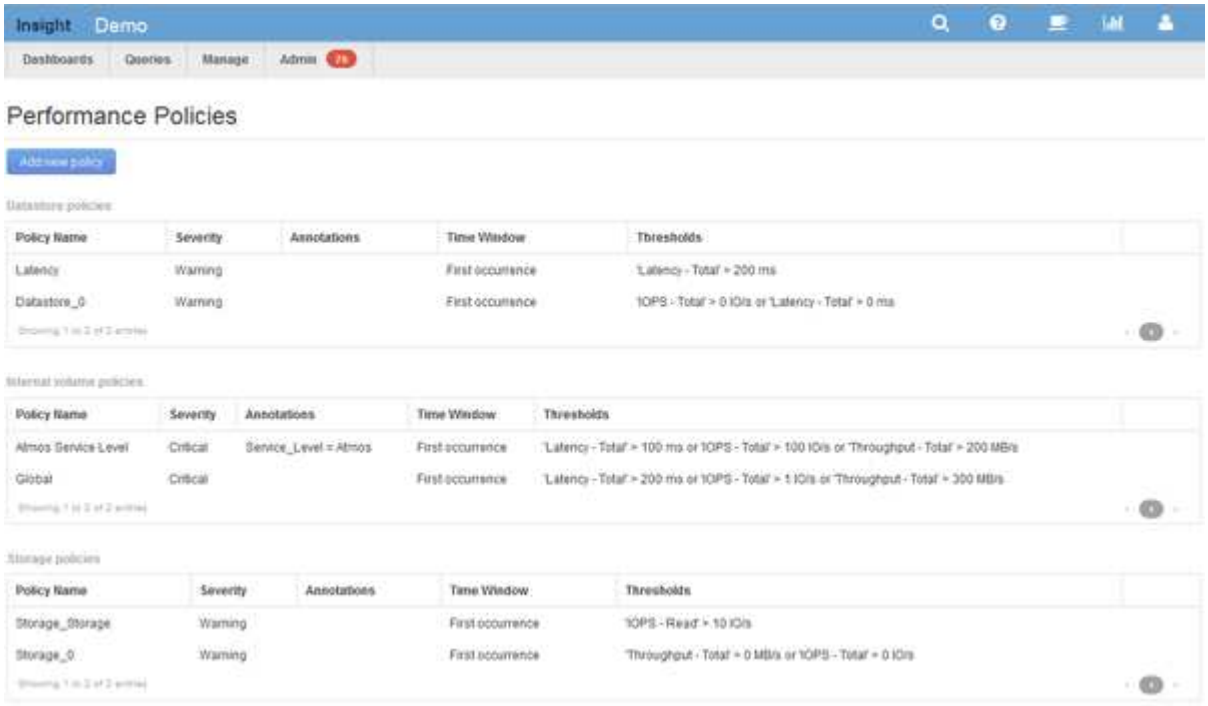
パフォーマンスポリシーの作成

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。
>
> [+]