OnCommand Insight のマニュアル

OnCommand Insight

NetApp
April 01, 2024

目次

OnCommand Insight のマニュアル

OnCommand Insight は単一の解決策 であり、物理環境と仮想環境のネットワーク、ストレージ、サーバにわたって、ドメイン間、マルチベンダーのリソース管理と分析を可能にします。Insightを使用すると、現在のインフラを最適化し、ビジネスニーズに合わせて運用を適切な規模に調整できます。それは何をいつ購入するかを決定するプロセスを簡素化します。また、クラウド移行の候補となるワークロードを特定することで、ハイブリッドクラウドへの移行など、複雑なテクノロジ移行の際のリスクを軽減します。Insightを使用すると、企業のITサービスデリバリチェーン全体にリソースを統合することで、ITインフラをエンドツーエンドのサービスとして管理できます。

リリースノート

リリースノート

OnCommand Insight のリリースノートはドキュメントセンターには含まれていません。NetApp Support Site のクレデンシャルでログインするように求められます。

"リリースノート.pdf" （新しいウィンドウで開きます）

OnCommand Insight とは

OnCommand Insight の概要

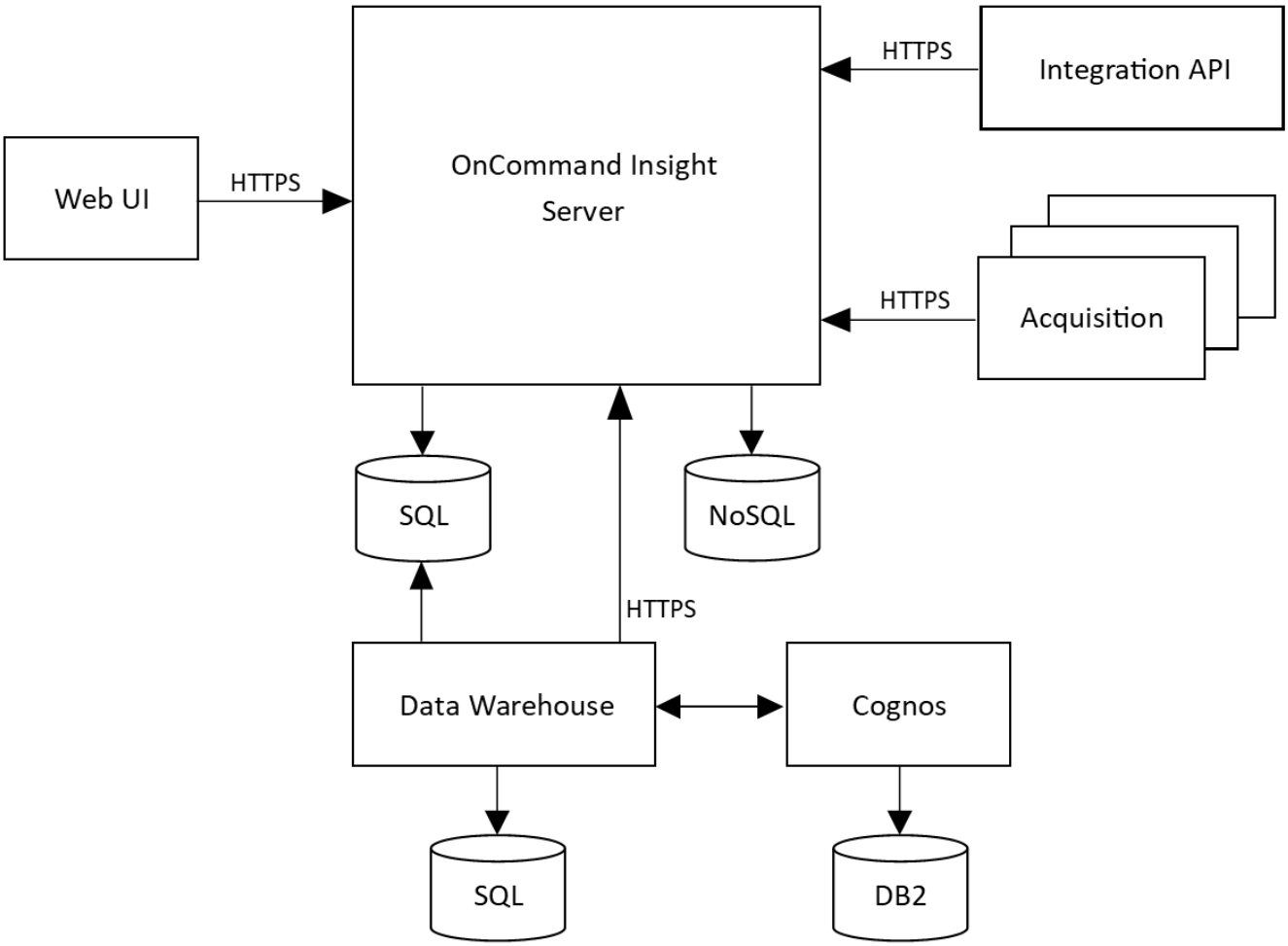
OnCommand Insight を使用すると、複雑なプライベートクラウド環境、ハイブリッドクラウド環境、仮想IT環境の運用管理を簡易化できます。Insightは単一の解決策 であり、物理環境と仮想環境のネットワーク、ストレージ、サーバにわたるドメイン間、マルチベンダーのリソース管理と分析を可能にします。

Insightを使用すると、現在のインフラを最適化し、ビジネスニーズに合わせて運用を適切な規模に調整できます。それは何をいつ購入するかを決定するプロセスを簡素化します。また、クラウド移行の候補となるワークロードを特定することで、ハイブリッドクラウドへの移行など、複雑なテクノロジ移行の際のリスクを軽減します。Insightを使用すると、企業のITサービスデリバリチェーン全体にリソースを統合することで、ITインフラをエンドツーエンドのサービスとして管理できます。

Insightアーキテクチャ

OnCommand Insight の一般的なインストールには、データ取得とレポート付きのデータウェアハウスが含まれており、すべてWebベースのUIから簡単にアクセスできます。よりセキュアな環境では、Remote Acquisition Unitを使用してデータを取得できます。

Insightアーキテクチャの主なコンポーネントを次の図に示します。



- * OnCommand Insight サーバ*

  OnCommand Insight サーバには、メインのデータリポジトリと分析コンポーネントが含まれています。環境のトポロジをエンドツーエンドで継続的に構築し、環境を分析し、インシデントや違反が検出されるとアラートを生成します。

- 取得

  Insightの収集エンジンは、1つ以上のAcquisition Unit上に構築されています。各InsightサーバにはLocal Acquisition Unitが含まれており、Remote Acquisition Unitをサポートできます。各ユニットはネットワーク上で実行されるサービスで、_data sources_というモジュールを介してデータセンター内のデバイスにアクセスし、データを収集します。Acquisition Unitで収集された情報は、分析のためにサーバに送信されます。

  収集エンジンは高度にモジュール化され、パッチを簡単に適用できるように設計されています。

- *統合API *

  APIを使用すると、外部エージェントからデータを収集できます。統合データは、クエリとウィジェットを使用してWeb UIで表示できます。ダッシュボードには、Insightの「ネイティブ」データと統合データを含めることができます。これらのダッシュボードでは、フィルタリング、ロールアップ、およびグループ化をデータに適用できます。

- * Web UI *

  InsightのHTML5 Webベースのユーザインターフェイスでは、データソースや監視環境（ポリシー、しきい値、アラートなど）を設定できます。次に、Web UIAssetダッシュボードとアセットページを使用して、潜在的な問題を特定して調査します。さまざまなウィジェットを使用してカスタムダッシュボードを作成し、それぞれのウィジェットでデータを柔軟に表示、分析、グラフ化できます。

- データウェアハウス

  OnCommand Insight データウェアハウスは、複数のInsightサーバのデータを格納し、照会や分析に使用できる共通の多次元データモデルに変換する、一元化されたリポジトリです。

  OnCommand Insight データウェアハウスでは、複数のデータマートで構成されるオープンデータベースにアクセスして、容量やパフォーマンスに関するカスタムレポート（チャージバックレポート、履歴データを使用したトレンドレポート、消費分析レポート、予測レポートなど）を生成できます。

  Data Warehouseでは、1つまたは複数のInsight環境について、レポート用にデータを統合して準備します。データには、履歴、トレンド、インベントリ、チャージバック、ショーバック、データプレゼンテーションが含まれ、データセンターのインフラストラクチャの長期的な計画をサポートします。

- * Cognos *

  CognosはInsightのレポート作成エンジンです。IBMのビジネスインテリジェンスツールで、事前定義済みのレポートを表示したり、カスタムレポートを作成したりできます。Insightのレポート機能を使用すると、Data Warehouseのデータからレポートが生成されます。

管理者、マネージャー、プランナーが**Insight**をどのように使用するか

OnCommand Insight は、ストレージ管理者、マネージャ、ストレージアーキテクトがトラブルシューティングと分析を実行するために不可欠な情報を提供します。

経験豊富なストレージ管理者は、OnCommand Insight とネットワークストレージに関する知識を活用して、次のような一般的なタスクを実行します。

- SAN環境とNAS環境を管理
- ネットワークに関する問題については、SANエンジニアと協力してください。
- 新しいストレージテクノロジを評価、テスト、環境への統合
- パフォーマンスの問題、アラート、ポリシー違反、違反、脆弱性をトラブルシューティングします。

マネージャとネットワークプランナーは、OnCommand Insight を使用して次のビジネスタスクを実行します。

- キャパシティプランニング
- プロジェクトの予算とスケジュールを策定する。
- 変化するプロジェクト需要に対応するために、プロジェクト計画を評価および修正します。
- プロジェクトの計画と経費を管理する。

- ハードウェアとソフトウェアの購入
- 容量管理、チャージバック請求、サイズ適正化、サービスレベルアグリーメントに関するビジネスレポートを提供

インストール（Linux

インストールの前提条件

OnCommand Insight をインストールする前に、現在のソフトウェアバージョンをダウンロードし、適切なライセンスを取得して、環境をセットアップする必要があります。

OnCommand Insight をインストールする前に、次のものがあることを確認してください。

- ダウンロードしたインストールパッケージに含まれている最新バージョンのOnCommand Insight ソフトウェアファイル
- ダウンロードしたOnCommand Insight バージョンを操作するためのライセンス
- 最小限のハードウェアおよびソフトウェア環境

  現在の製品では、以前のバージョンのOnCommand Insight 製品では使用されていなかった追加のハードウェアリソース（OnCommand Insight 製品の機能強化のため）が消費される可能性があります。

- OnCommand Insight サーバ、Data WarehouseとReporting、およびRemote Acquisition Unitのハードウェアとネットワークの構成を含む導入計画。

導入を計画します

導入を成功させるには、OnCommand Insight をインストールする前に特定のシステム要素を考慮する必要があります。

このタスクについて

Insightの導入計画では、次のシステム要素を考慮する必要があります。

- Insightアーキテクチャ
- 監視するネットワークコンポーネント
- Insightのインストールの前提条件とサーバ要件
- Insight Webブラウザの要件

データソースのサポート情報

設定計画の一環として、環境内のデバイスをInsightで監視できることを確認する必要があります。そのためには、データソースサポートマトリックスでオペレーティングシステム、特定のデバイス、プロトコルの詳細を確認できます。一部のデータソースは、オペレーティングシステムによっては使用できない場合があります。

データソースサポートマトリックスの最新バージョンの場所

OnCommand Insight データソースサポートマトリックスは、サービスパックのリリースごとに更新されます。ドキュメントの最新バージョンについては、を参照してください "NetApp Support Site"。。

デバイスの識別とデータソースの計画

導入計画の一環として、環境内のデバイスに関する情報を収集する必要があります。

環境内の各デバイスについて、次のソフトウェア、接続、および情報が必要です。

- OCIサーバが解決できるIPアドレスまたはホスト名
- ログイン名とパスワード
- デバイスへのアクセスのタイプ（コントローラや管理ステーションなど）

> ほとんどのデバイスには読み取り専用アクセスで十分ですが、管理者権限が必要なデバイスもあります。

- データソースポートの要件に応じたデバイスへのポート接続
- スイッチの場合、SNMPの読み取り専用コミュニティストリング（スイッチへのアクセスを許可するユーザIDまたはパスワード）
- デバイスに必要なサードパーティ製ソフトウェア（Solutions Enablerなど）。
- データソースの権限と要件の詳細については、Web UIヘルプまたは_ OnCommand Insight 構成および管理ガイド_で「ベンダー固有のデータソースリファレンス」を参照してください。

OnCommand Insight で生成されるネットワークトラフィック

OnCommand Insight で生成されるネットワークトラフィック、ネットワークを通過する処理データの量、およびOnCommand Insight によるデバイスへの負荷は、多くの要因によって異なります。

トラフィック、データ、および負荷は、次の要因に基づいて環境によって異なります。

- 生データ
- デバイスの構成
- OnCommand Insight の導入トポロジ
- インベントリデータやパフォーマンスデータソースのポーリング間隔が異なるため、低速なデバイスを検出したり帯域幅を節約したりするために、間隔を短くすることができます

OnCommand Insight で収集される生の構成データは大きく異なる場合があります。

次の例は、設定データがどのように変化し、多くの設定要因によってトラフィック、データ、および負荷がどのように影響するかを示しています。たとえば、2つのアレイにそれぞれ1、000本のディスクがあるとします。

- アレイ1：1、000本のSATAディスクがあり、すべて1TBです。1、000本のディスクがすべて1つのストレージプールに含まれ、ESXクラスタ内の同じ32ノードに対して1、000個のLUNが提供（マッピングおよびマスク）されます。
- アレイ2：2TBのデータディスクが400本、600GBのFCディスクが560本、SSDが40本あります。ストレージプールは3つありますが、FCディスクのうち320本が従来のRAIDグループで使用されています。RAIDグループに分割されたLUNは従来のマスキングタイプ（symmaskdb）を使用し、シンプロビジョニングされたプールベースのLUNは新しいマスキングタイプ（symaccess）を使用します。150の異なるホストに対

して600個のLUNが提供されました。200個のBCV（600個のLUNのうち200個のフルブロックレプリカボリューム）があります。また、別のサイトのアレイ上に存在するボリュームのリモートレプリカボリュームである200個のR2ボリュームもあります。

それぞれ1、000本のディスクと1、000個の論理ボリュームで構成されています。データセンターで消費するラックスペースが物理的に同じである場合もあれば、同じファームウェアを実行している場合もありますが、2つ目のアレイの構成は1つ目のアレイよりもはるかに複雑です。

MariaDBをアンインストールしています

OnCommand Insight またはData Warehouseをインストールする前に、InsightサーバまたはData WarehouseサーバでMariaDBをアンインストールする必要があります。アンインストールしないと、インストールを続行できません。MySQLはMariaDBと互換性がありません。MariaDBを削除せずにどちらかのサーバにインストールしようとすると、MariaDBをアンインストールするように指示するエラーメッセージが表示されてインストールが終了します。

作業を開始する前に

sudo権限が必要です。

手順

1. Insight Serverにログインします。
2. MariaDBコンポーネントのリストを取得します。

   ```
   rpm -qa | grep mariadb
   ```

3. サーバにインストールされているMariaDBコンポーネントごとに、次のコマンドを入力します。

   ```
   yum remove component_name
   ```

Insight Serverの要件

専用のサーバを使用することを推奨します。他のアプリケーションがインストールされているサーバにはInsightをインストールしないでください。製品の要件が満たされていれば、物理サーバと仮想サーバの両方がサポートされます。

OnCommand Insight サーバソフトウェアをインストールするには、sudo権限が必要です。

Insightのコンポーネントの中には、インストール時に依存パッケージが必要なものがあります。Insightをインストールする前に、YUMリポジトリにアクセスできることを確認してください。

OnCommand Insight のサイジングには、データソースのタイプとサイズ、環境内のアセットの数、ポーリング間隔など、さまざまな要素を考慮する必要があります。次のサイジング例はあくまでもガイドラインであり、Insightでテストされた一部の環境を示したものです。環境内でこれらの要素やその他の要素を変更すると、Insightのサイジング要件が変更される可能性があります。これらのガイドラインには、最大90日間のパフォーマンスアーカイブデータ用のディスクスペースが含まれます。

詳細なサイジングガイダンスについては、Insightをインストールまたはアップグレードする前に、担当のセールスエンジニアに問い合わせることを推奨します。

例：

環境要因：	テストしたディスク容量、CPU、メモリ：
80ストレージアレイ4、000ボリューム 4、000台のVM 4、000個のスイッチポート	250GBディスクスペース8コア 32GBのRAM
160個のストレージアレイ40、000個のボリューム 8、000台のVM 8、000個のスイッチポート	1TBのディスクスペース12コア 48GBのRAM

要件：

コンポーネント	必須

オペレーティングシステム	次のいずれかのライセンスバージョンを実行しているコンピュータ。他のアプリケーションレベルのソフトウェアを実行していないコンピュータ。 • Red Hat Enterprise Linux 7.3、7.4、7.5、7.6、7.7、 7.8、7.9、8.1、8.2、8.3、 8.4、8.5、8.8、9.2 • CentOS 7.2、7.5、7.6、7.7、7.8、 7.9、CentOS 8 Stream、CentOS 9 Stream • Oracle Enterprise Linux 7.5、7.6、7.7、7.8、7.9、 8.1、8.2、8.3、8.4、8.5、 8.8 ライセンスバージョンを使用すると、インストールに必要な依存関係がオペレーティングシステムによって自動的に解決されます。 Insightをインストールする前に、MariaDBをアンインストールする必要があります。 MariaDBをアンインストールすると、Postfix Mail Transport Agentも削除されます。 専用のサーバを使用することを推奨します。
仮想マシン（VM）	このコンポーネントは、インスタンスのCPUリソースとメモリリソースが予約されていれば、仮想環境で実行できます。
メモリとCPU	24~256GBのRAM 8~32コア

使用可能なディスクスペース	100GB~3TBのインストールディスクスペース 50 GB~1 TBのパフォーマンスアーカイブディスクスペース 500GB環境の例では、次のパーティション分割を推奨します。 • /optディレクトリ-- 50GB • /var/logディレクトリ-- 100GB • /var/libディレクトリ-- 350 GB マウントすることを推奨します `/opt` および `/var` ルートファイルシステムとは別のディスクに配置します (/）。 InsightのインストールスペースにはSSDディスクを使用することを推奨します。
ネットワーク	イーサネット接続とポート： • 専用の（静的な）IPアドレスを使用した100Mbpsまたは1Gbpsのイーサネット接続、およびSANのすべてのコンポーネント（FCデバイスやRemote Acquisition Unitなど）へのIP接続。 • OnCommand Insight サーバプロセスのポート要件は、80、443、1090~1100、3873、8083、4444$_{4446、5445、5455、4712}$4714、5500、 そして5501 • 取得プロセスには、ポート12123と5679が必要です。 • MySQLにはポート3306が必要です。 • Elasticsearchには、ポート9200と9310が必要です ポート443および3306は、存在するファイアウォールを介した外部アクセスを必要とします。
権限	OnCommand Insight サーバに対するsudo権限が必要です。 次のフォルダのいずれかがシンボリックリンクである場合は、リンク先ディレクトリに「755」権限があることを確認してください。 • /opt/netapp • /var/lib/netapp • /var/log/netapp

リモート接続	インストールおよびインストール後のサポートを容易にするために、WebExアクセスまたはリモートデスクトップ接続を可能にするインターネット接続。
アクセス性	HTTPSアクセスが必要です。
HTTPサーバまたはHTTPSサーバ	Apache HTTPサーバやその他のHTTPSサーバは、OnCommand Insight サーバと同じポート（443）で競合しないようにし、自動的に起動しないようにしてください。ポート443をリスンする必要がある場合は、他のポートを使用するようにOnCommand Insight サーバを設定する必要があります。

Data Warehouseサーバの要件

Data Warehouseサーバは、確立されているハードウェアおよびソフトウェアの要件に対応したコンピュータで実行する必要があります。Apache Webサーバまたはレポート作成ソフトウェアがこのマシンにインストールされていないことを確認する必要があります。

> OnCommand Insight のサイジングには、環境内のアセットの数、保持する履歴データの量など、さまざまな要素が関係します。次のData Warehouseのサイジング例はあくまでもガイドラインであり、Insightでテストされた一部の環境を示したものです。環境内でこれらの要素やその他の要素を変更すると、Insightのサイジング要件が変更される可能性があります。

詳細なサイジングガイダンスについては、Insightをインストールまたはアップグレードする前に、担当のセールスエンジニアに問い合わせることを推奨します。

例：

環境要因：	テストしたディスク容量、CPU、メモリ：
ストレージアレイ18台、VM 3、400台 4、500個のスイッチポート	200 GBのハードディスク8コア 32GBのRAM
110台のストレージアレイ11、500台のVM 14、500個のスイッチポート	300 GBハードディスク8コア 48GBのRAM

要件：

コンポーネント	必須

オペレーティングシステム	次のいずれかのライセンスバージョンを実行しているコンピュータ。他のアプリケーションレベルのソフトウェアを実行していないコンピュータ。 • Red Hat Enterprise Linux 7.3、7.4、7.5、7.6、7.7、 7.8、7.9、8.1、8.2、8.3、 8.4、8.5、8.8、9.2 • CentOS 7.2、7.5、7.6、7.7、7.8、 7.9、CentOS 8 Stream、CentOS 9 Stream • Oracle Enterprise Linux 7.5、7.6、7.7、7.8、7.9、 8.1、8.2、8.3、8.4、8.5、 8.8
仮想マシン（VM）	このコンポーネントは、インスタンスのCPUリソースとメモリリソースが予約されていれば、仮想環境で実行できます。
CPU	8~40個のCPUコア
メモリ	32GB~2TBのRAM
利用可能なディスク容量	200GB~512GBのディスクスペースには、少なくとも50GBの空きディスクスペースが必要です `/var/lib` にパーティションと25GBの空きディスクスペースがあります `/opt` および `/var/log` パーティション：
ネットワーク	• 100 Mbpsまたは1 Gbpsのイーサネット接続 • 静的IPアドレス • OnCommand Insight DWHサーバプロセスの場合は、ポート80、443、1098、1099、 3873、8083、4444～4446 • MySQLの場合は、ポート3306

Remote Acquisition Unitサーバの要件

ファイアウォールの背後、リモートサイト、プライベートネットワーク、または異なるネットワークセグメントにあるSANデバイスから情報を取得するには、Remote Acquisition Unit（RAU）をインストールする必要があります。RAUをインストールする前に、オペレーティングシステム、CPU、メモリ、およびディスクスペースの要件を満たしていることを確認する必要があります。

コンポーネント	要件

オペレーティングシステム	次のいずれかのライセンスバージョンを実行しているコンピュータ。他のアプリケーションレベルのソフトウェアを実行していないコンピュータ。 • Red Hat Enterprise Linux 7.3、7.4、7.5、7.6、7.7、 7.8、7.9、8.1、8.2、8.3、 8.4、8.5、8.8、9.2 • CentOS 7.2、7.5、7.6、7.7、7.8、 7.9、CentOS 8 Stream、CentOS 9 Stream • Oracle Enterprise Linux 7.5、7.6、7.7、7.8、7.9、 8.1、8.2、8.3、8.4、8.5、 8.8 専用のサーバを使用することを推奨します。
CPU	4 個の CPU コア
メモリ	16GB の RAM
使用可能なディスクスペース	40 GB
ネットワーク	100Mbps/1Gbpsイーサネット接続、静的IPアドレス、すべてのFCデバイスへのIP接続、OnCommand Insight サーバへの必要なポート（80または443）。
権限	RAUサーバに対するsudo権限

OnCommand Insight でサポートされているブラウザ

ブラウザベースのOnCommand InsightWeb UIは、いくつかの異なるブラウザで動作できます。

Insightでは、次のブラウザのベータ版以外の新しいリリースがサポートされます。

- Mozilla Firefox
- Google Chrome
- Microsoft Edge の場合

OnCommand Insight に対応したブラウザバージョンの完全なリストについては、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

Insightのインストール手順

インストールでは、複数のOnCommand Insightコンポーネント、Insight Server、およびData Warehouseをインストールする必要があります。

インストールには、次の主な作業が含まれます。

- OnCommand Insight インストーラをダウンロードしています
- OnCommand Insight サーバをインストールしています
- ライセンスのインストール
- DWHとReportingのインストール（オプション）。別のマシンまたは仮想マシンにインストールする必要があります。ReportingにはMicrosoft Windowsが必要です）。
- Remote Acquisition Unit（RAU）のインストール（オプション）。RAUは、ファイアウォールの内側、リモートサイト、またはプライベートネットワークに配置されたデバイスリソースから情報を取得します

インストールが完了したら、環境に関する情報を取得するようにInsightを設定する必要があります。必要な作業については、_ OnCommand Insight 構成および管理ガイド_を参照してください。

OnCommand Insight インストーラをダウンロードしています

OnCommand Insight インストーラはNetApp Support Site からダウンロードできます。

作業を開始する前に

NetApp Support Site へのログインが必要です "mysupport.netapp.com"。

また、インストールを開くための解凍ユーティリティが必要です `.ZIP` ファイル。

手順

1. OnCommand Insight をインストールするサーバにログインします。
2. NetApp Support Site からインストールファイルをダウンロードします。

OnCommand Insight サーバをインストールしています

OnCommand Insight サーバは、コマンドラインを使用してインストールします。

作業を開始する前に

インストールの前提条件をすべて満たしておく必要があります。

手順

1. sudo権限があるアカウントでInsight Serverにログインします。
2. インストールファイルが保存されているサーバー上のディレクトリに移動し、次のコマンドを入力します。

   ```
   unzip oci-<version>-linux-x86_64.zip
   ```

   インストールファイルのバージョン番号を確認してください。バージョン番号は、コマンドに表示されているものとは異なる場合があります。

3. の構文、コマンド引数、およびパラメータの使用方法を確認できます `oci-install.sh` ：

```
sudo ./oci-<version>-linux-x86_64/oci-install.sh --help
```

4. インストールスクリプトを実行します。

```
sudo ./oci-<version>-linux-x86_64/oci-install.sh
```

5. ライセンス契約を読み、同意して、画面の指示に従います。
6. Insightの消費ライセンスモデルを使用している場合は、使用状況の情報をネットアップに送信することを有効にする必要があります。入力するコマンド `Y` をクリックします。

結果

すべてのプロンプトを回答 にすると、インストールが開始されます。所要時間は約10分です（インストールされているアプリケーションによって異なります）。

OnCommand Insight Data Warehouseをインストールしています

インストールは自己完結型で、OnCommand Insight Data Warehouse（DWH）の実行と運用に必要な要素が含まれています。

作業を開始する前に

インストールの前提条件をすべて満たしておく必要があります。

このタスクについて

Data WarehouseにはCognosのレポート機能があります。InsightをLinuxサーバにインストールする場合は、Data WarehouseをWindowsサーバにインストールする場合にのみ、これらの機能を使用できます。WindowsへのData WarehouseのインストールおよびCognosのレポート機能については、_ OnCommand Insight インストールガイド（Microsoft Windows_）を参照してください。

手順

1. sudo権限があるアカウントでData Warehouseサーバにログインします。
2. インストールファイルが保存されているサーバー上のディレクトリに移動し、次のコマンドを入力します。

```
unzip oci-dwh-<version>-linux-x86_64.zip
```

インストールファイルのバージョン番号を確認してください。バージョン番号は、コマンドに表示されているものとは異なる場合があります。

3. の構文、コマンド引数、およびパラメータの使用方法を確認できます `oci-install.sh` インストールを開始する前に：

```
sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh --help
```

4. インストールスクリプトを実行します。

```
sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh
```

5. ライセンス契約を読み、同意して、画面の指示に従います。

結果

すべてのプロンプトを回答 にすると、インストールが開始されます。所要時間は約10分です（インストールされているアプリケーションによって異なります）。

Remote Acquisition Unitのインストール

OnCommand Insight 環境には1つ以上のRemote Acquisition Unit（RAU）をインストールできます。Acquisition Unitは、（data_sources_というモジュールを介して）にアクセスし、データセンター内のさまざまなデバイスからデータを収集するネットワークで実行されます。

作業を開始する前に

インストールの前提条件をすべて満たしておく必要があります。

OnCommand Insight サーバに変更情報を転送するには、少なくとも1つのポートが開いていて、RAUサーバとサーバの間で使用可能である必要があります。不明な場合は、RAUコンピュータでWebブラウザを開き、OnCommand Insight サーバに移動して検証します。

```
https://< OnCommand Insight Server hostname >:< acquisition_port >
```

Acquisitionのデフォルトポートは443ですが、サーバのインストール時に変更されている可能性があります。接続に成功すると、OnCommand Insight 応答ページが表示され、RAUとOnCommand Insight サーバの間でポートが開いて使用可能であることが示されます。

ネットワークアドレス変換またはポートアドレス変換（NAT/PAT:つまり、IPアドレスの変換）を使用する環境では、InsightではNATとデバイス間のRAUの挿入のみがサポートされます。

- サポート対象：OnCommand Insight -> NAT-> RAU ->デバイス
- サポート対象外：OnCommand Insight -> RAU -> NAT->デバイス

手順

1. sudo権限があるアカウントでRAUサーバにログインします。
2. インストールファイルが保存されているサーバー上のディレクトリに移動し、次のコマンドを入力します。

   ```
   unzip oci-rau-<version>-linux-x86_64.zip
   ```

3. の構文、コマンド引数、およびパラメータの使用方法を確認できます `oci-install.sh`：

   ```
   sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh --help
   ```

4. インストールスクリプトを実行します。

```
sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh
```

5. ライセンス契約を読んで同意し、画面の指示に従います。

   すべてのプロンプトを回答 にすると、インストールが開始されます。所要時間は約10分です（インストールされているアプリケーションによって異なります）。

Remote Acquisition Unitのインストールを検証しています

Remote Acquisition Unitが適切にインストールされていることを確認するために、サーバに接続されているRemote Acquisition Unitのステータスを表示できます。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. Acquisition Units *をクリックします。
3. 新しいRemote Acquisition Unitが正しく登録され、ステータスが「Connected」になっていることを確認します。

   ステータスが「Connected」になっていない場合は、サービスを再起動してください。Remote Acquisition Unitシステムにログインし、次のコマンドを実行します。

   ```
   oci-service.sh restart acquisition
   ```

   それでも接続されない場合は、テクニカルサポートにお問い合わせください。

インストールを確認しています

インストールが完了すると、インストールディレクトリはにあります `/opt/netapp/oci`。サポートされているブラウザでInsightを開くと、インストールされているかどうかを確認できます。Insightのログファイルを確認することもできます。

Insightを初めて開いたときに、ライセンスのセットアップページが開きます。ライセンス情報を入力したら、データソースを設定する必要があります。データソース定義の入力、およびOnCommand Insight のユーザと通知の設定については、_ Configuration and Administration Guide _を参照してください。

インストール時に問題が発生した場合は、テクニカルサポートに連絡して、必要な情報を提供してください。

新しい**Insight**コンポーネントがインストールされていることを確認します

インストールが完了したら、サーバに新しいコンポーネントが存在することを確認する必要があります。

手順

1. ログインしているサーバで現在動作しているサービスのリストを表示するには、次のように入力します。

```
sudo oci-service.sh status all
```

2. ログインしているサーバに応じて、リストに次のInsightサービスが表示されているかどうかを確認し、ステータスが「Running」であることを確認します。
   - Insightサーバ：wildfly、acquisition、mysql、elasticsearch
   - Data Warehouseサーバ：wildfly、mysql
   - Remote Acquisitionサーバ：acquisition

結果

これらのコンポーネントが表示されない場合は、テクニカルサポートにお問い合わせください。

Insightのログ

Insightには、調査やトラブルシューティングに役立つ多数のログファイルが用意されています。使用可能なログは、logディレクトリに一覧表示されます。BareTailなどのログ監視ツールを使用すると、すべてのログを一度に表示できます。

ログファイルはにあります `/var/log/netapp/oci/wildfly/` ディレクトリ。収集ログはにあります `/var/log/netapp/oci/acq` ディレクトリ。データファイルはにあります `/var/lib/netapp/oci`。

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
     ```

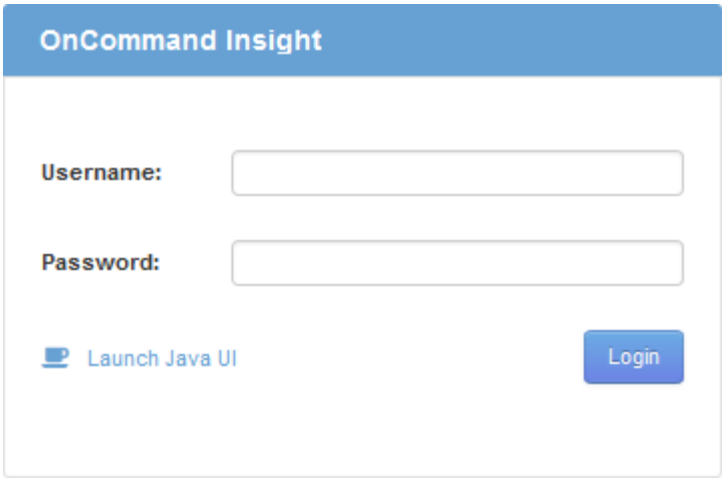
   - その他の場所からInsightを開きます。

     ```
     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）

インストールのトラブルシューティング

OnCommand Insight のインストールは、通常、インストールウィザードを使用して管理します。ただし、コンピュータ環境によっては、アップグレード中に問題が発生したり、競合が発生したりする可能性があります。

また、ソフトウェアのインストールに必要なOnCommand Insight ライセンスがすべてインストールされていることを確認する必要があります。

ライセンスがありません

OnCommand Insight 機能ごとに異なるライセンスが必要です。OnCommand Insight に表示される内容は、インストールされているライセンスによって制御されます。各ライセンスで制御される機能については、「OnCommand Insight ライセンス」セクションを参照してください。

各ライセンスで制御される機能については、「OnCommand Insight ライセンス」セクションを参照してください。

オンラインテクニカルサポートリクエストの送信

Insightのインストールで問題が発生した場合は、サポートに登録しておくとオンラインのテクニカルサポートリクエストを送信できます。

作業を開始する前に

オンラインサポートサービスを利用するには、会社のEメールアドレスを使用してサポートカスタマーとして登録する必要があります。登録はサポートサイトで行います 。

このタスクについて

カスタマーサポートがインストールの問題を解決できるようにするには、次の項目を含め、できるだけ多くの情報を収集する必要があります。

- Insightのシリアル番号
- 問題の概要
- Insightのすべてのログファイル
- エラーメッセージのスクリーンキャプチャ

手順

1. を作成します `.zip` トラブルシューティングパッケージを作成するために収集した情報のファイル。
2. サポートサイトにログインします "mysupport.netapp.com" をクリックし、* Technical Assistance *を選択します。
3. [ケースを開く]*をクリックします。
4. データのパッケージの指示に従ってください。

完了後

[Technical Assistance]ページの[Check Case Status]*を使用して、リクエストに従うことができます。

Insightのアップグレード

新しいバージョンのOnCommand Insight が利用可能になった場合は、新しい機能や問題の修正を利用するためにアップグレードが必要になることがあります。Insight ServerとData Warehouse（DWH）は別 々 にアップグレードする必要があります。

アップグレードプロセスではインストールフォルダ全体が上書きされるため、Insightのインストールディレクトリには自動または手動のバックアップを保存しないでください。これらのディレクトリのいずれかにバックアップファイルを保存している場合は、アップグレードまたはアンインストールのプロセスを実行する前に、バックアップを別の場所に移動する必要があります。

新しいバージョンのInsightでは、より多くのディスクスペース、メモリ、CPUが必要になります。Insightの最新バージョンにアップグレードする前に、インストール要件を確認してください。詳細なサイジングガイダンスについては、Insightをインストールまたはアップグレードする前に、担当のセールスエンジニアに問い合わせることを強く推奨します。

Insightソフトウェアをアップグレードする前に、セキュリティバックアップとデータベースバックアップを実行することを推奨します。

Insightをバージョン**7.3.12**以降にアップグレードしています（**Linux**）

OnCommand Insight 7.3.10-7.3.11から7.3.12以降にアップグレードする前に、OCIデータ移行ツールを実行する必要があります。

背景（ **Background** ）

OnCommand Insight バージョン7.3.12以降では、以前のバージョンと互換性のないソフトウェアが使用されます。Insightバージョン7.3.12以降には、アップグレードに役立つ*データ移行ツール*が含まれています。

OnCommand Insight バージョン7.3.9以前はサポートされなくなりました。これらのいずれかのバージョンを実行している場合は、7.3.12以降にアップグレードする前に、Insightバージョン7.3.10以降（7.3.11を推奨）にアップグレードする必要があります。

データ移行ツールの機能

移行ツールは、最初の互換性チェックを実行し、3つの異なるアップグレードパスのいずれかに従います。選択したパスは、現在のバージョンのデータ互換性に基づいています。

アップグレードの前に、Data Migration Toolを実行し、推奨される手順に従う必要があります。

始める前に

- データ移行ツールを実行する前に、OnCommand Insight システムをバックアップすることを強く推奨します。
- サーバ上のElasticsearchサービスが稼働している必要があります。
- Insightをアップグレードする前に、データベースとパフォーマンスアーカイブに対してData Migration Tool_must_beを実行してください。

データ移行ツールの実行

1. 最新バージョンのData Migration Tool（_SANScreenDataMigrationTool-x86-7.3.12-97.zip_など）と適切なInsightインストーラファイルをInsight Serverにダウンロードします。作業フォルダに解凍します。ダウンロードはにあります "NetApp Support Site"。

2. コマンドウィンドウを開き、作業フォルダに移動します。
    - Bashシェルをお勧めします。
3. 次のコマンドを使用してデータ移行ツールを実行します。
    - `*sudo./SANScreenDataMigrationTool.sh*`
4. 必要に応じて指示に従います。次に例を示します。

```
sudo ./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-132

OCI 7.3.10.8.139 is installed
Elasticsearch REST port = 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 54 obsolete indexes. Of these,
    54 indexes may be migrated with OCI server running,
       the most recent of which is for 2021-05-13

Verifying migration component is present...
SANscreen Server service is Running

Proceed with online migration of 54 indexes (y or [n])?:
```

Data Migration Toolは、システムに古いインデックスが存在するかどうかをチェックし、検出されたインデックスがあるかどうかをレポートします。存在しない場合、ツールは終了します。

SANscreen サーバサービスの実行中に、一部のインデックスが移行される場合があります。その他のものは、サーバーが停止しているときにのみ移行できます。移行できるインデックスがない場合、ツールは終了します。それ以外の場合は、指示に従ってください。

Data Migration Toolが完了すると、古いインデックスがないか再確認されます。すべてのインデックスが移行されている場合は、OnCommand Insight 7.3.12へのアップグレードがサポートされていることが通知されます。これで、Insightのアップグレードを続行できます。

```
sudo ./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-132

OCI 7.3.10.8.139 is installed
Elasticsearch REST port = 9200

Checking for obsolete (version 5) indexes...
Found 76 obsolete OCI indexes. Of these,
76 indexes may be migrated with OCI server running

SANscreen Server service is running

Proceed with online migration of 76 indexes (y or [n])? y
If you supply performance archive location, entries for any dates with
migrated
indexes will be replaced. Each orginal entry will be renamed and you may
delete
it after migration is completed.
When prompted enter the archive location including the site-name
directory.

Enter the location of the performance archive or blank if none:
Performance archive entries will not be updated

Running the migration application with options -u http://localhost:9200
--online -sa -

Preparing to migrate oci-timeseries-disk-2021-03-22: copied; backup;
delete old; restore new; cleanup; done.
Preparing to migrate oci-timeseries-internalvolume-2021-03-22: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate oci-timeseries-port-2021-03-22: copied; backup;
delete old; restore new; cleanup; done.
...
Preparing to migrate oci-timeseries-disk-2021-03-27: copied; backup;
delete old; restore new; cleanup; done.
Execution time 0:08:17
Checking for obsolete (version 5) indexes...

No obsolete indexes found. Upgrade and Inline Upgrade to 7.3.12+ are
supported
```

SANscreen サービスの停止を求めるメッセージが表示された場合は、Insightをアップグレードする前にサービスを再起動します。

検証に失敗しました

インデックスの検証が失敗した場合、移行ツールは終了前に問題を通知します。

- OnCommand Insight が存在しません：*

```
./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool V1.0

Checking OnCommand Insight Installation...
ERROR: OnCommand Insight is not installed
```

- Insightバージョンが無効です：*

```
./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.4 (126) is installed
ERROR: The OCI Data Migration Tool is intended to be run against OCI 7.3.5
- 7.3.11
```

- Elasticsearchサービスが実行されていません：*

```
./SanscreenDataMigrationTool.sh
NetApp SANScreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.11 (126) is installed

Getting installation parameters...
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
ERROR: The Elasticsearch service is not running

Please start the service and wait for initialization to complete
Then rerun OCI Data Migration Tool
```

コマンドラインオプション

Data Migration Toolには、その動作に影響するいくつかのオプションパラメータが含まれています。

オプション（Linux）	機能
-s	--silent
すべてのプロンプトを非表示にします	-a
-アーカイブ	指定すると、インデックスが移行された日付の既存のアーカイブエントリが置き換えられます。パスは、アーカイブエントリzipファイルが格納されているディレクトリを指す必要があります。 引数に「-」を指定すると、更新するパフォーマンスアーカイブがないことを示します。 この引数が指定されている場合、アーカイブ場所のプロンプトは表示されません。
-c	--check
存在する場合、スクリプトはインデックスカウントを報告した直後に終了します。	-d
--dryrun	存在する場合、移行実行可能ファイルは実行されるアクション（データの移行とアーカイブエントリの更新）を報告しますが、操作は実行しません。
-p	— port
指定した値がある場合は、ElasticsearchのRESTポートとして使用します。存在しない場合は、可能であればインストールから値を取得します。存在しない場合は、デフォルト値の9200を使用します。 一部のLinux OnCommand Insight 環境では、Elasticsearch RESTポートがデフォルトの9200ポートで実行されていない場合があります。この場合は、--portオプションを使用して値を指定します	-h
--help	使用状況の情報を表示します

トラブルシューティング

アーカイブエントリが更新された場合は、更新されたアーカイブの所有権と権限が正しいことを確認する必要があります。これらは* ocisys ocisys 644 *である必要があります。サポートされていない場合は、パフォーマンスアーカイブフォルダに移動して次のコマンドを実行します。

```
chown ocisys *
chgrp ocisys *
chmod 644 *
```

Insight Serverソフトウェアをアップグレードしています

OnCommand Insight サーバの更新は、サーバにログインしたあとに確認できます。

手順

1. Insightのツールバーで、*[Help]*アイコンをクリックします。
2. [Check for updates]*を選択します。
3. が表示されたら、* OK *をクリックします `Version is up to date` メッセージが表示されます。
4. 新しいバージョンが検出された場合は、メッセージボックスの*ここにダウンロード*リンクをクリックします。
5. [ダウンロード]ページで、[ダウンロード]*をクリックします。ダウンロードディレクトリの場所をメモします。

   NetApp Support Site から新しいバージョンをダウンロードすることもできます。
6. sudo権限があるアカウントでInsight Serverにログインします。
7. ダウンロードディレクトリに移動し、次のコマンドを入力します。

   ```
   unzip oci-<version>-linux-x86_64.zip
   ```

   インストールファイルのバージョン番号が正しいことを確認します。
8. の構文、コマンド引数、およびパラメータの使用方法を確認できます `oci-install.sh` ：

   ```
   sudo ./oci-<version>-linux-x86_64/oci-install.sh --help
   ```
9. インストールスクリプトを実行します。

   ```
   sudo ./oci-<version>-linux-x86_64/oci-install.sh
   ```
10. ライセンス契約に同意し、画面の指示に従います。

Data Warehouseソフトウェアをアップグレードしています

Insight Serverソフトウェアをアップグレードしたら、Data Warehouseソフトウェアをアップグレードする必要があります。

手順

1. sudo権限があるアカウントでData Warehouse（DWH）サーバにログインします。

2. NetApp Support Site からInsight DWHソフトウェアをダウンロードします。
3. ダウンロードディレクトリに移動し、次のコマンドを入力します。

   ```
   unzip oci-dwh-<version>-linux-x86_64.zip
   ```

   インストールファイルのバージョン番号が正しいことを確認します。

4. の構文、コマンド引数、およびパラメータの使用方法を確認できます `oci-install.sh` ：

   ```
   sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh --help
   ```

5. インストールスクリプトを実行します。

   ```
   sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh
   ```

6. ライセンス契約に同意し、画面の指示に従います。

Remote Acquisition Unitソフトウェアをアップグレード中です

Insight Serverソフトウェアをアップグレードしたあとに、Remote Acquisitionソフトウェアをアップグレードする必要があります。

手順

1. sudo権限があるアカウントでRemote Acquisition Unit（RAU）サーバにログインします。
2. NetApp Support Site からInsight RAUソフトウェアをダウンロードします。
3. ダウンロードディレクトリに移動し、次のコマンドを入力します。

   ```
   unzip oci-rau-<version>-linux-x86_64.zip
   ```

   インストールファイルのバージョン番号が正しいことを確認します。

4. の構文、コマンド引数、およびパラメータの使用方法を確認できます `oci-install.sh` ：

   ```
   sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh --help
   ```

5. インストールスクリプトを実行します。

   ```
   sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh
   ```

6. ライセンス契約に同意し、画面の指示に従います。

Windowsから**Linux**への移行

既存のWindowsがインストールされている環境でInsightをLinuxで使用するには、移行を実行する必要があります。この手順 は、Insight ServerコンポーネントとData Warehouseコンポーネントの両方で実行する必要があります。

手順

1. 現在インストールされているInsightをサーバにバックアップします。

   OnCommand Insight データベースのバックアップ方法については、OCI構成および管理ガイド_を参照してください。

2. Insight for Linuxをインストールします。
3. 以前のバージョンのデータベースをリストアします。

   OnCommand Insight データベースのリストア方法については、OCI構成および管理ガイド_を参照してください。

4. 以前のバージョンのInsight for Windowsをアンインストールします。

OnCommand Insight をアンインストールしています

必要に応じて、OnCommand Insight コンポーネントをアンインストールできます。OnCommand Insight コンポーネントは個別にアンインストールする必要があります。

各コンポーネントは個別にアンインストールされます。

OnCommand Insight サーバをアンインストールしています

必要に応じて、OnCommand Insight サーバをアンインストールできます。

作業を開始する前に

ベストプラクティス：Insightをアンインストールする前に、OnCommand Insight データベースをバックアップしてください。

手順

1. sudo権限があるアカウントでOnCommand Insight サーバにログインします。
2. OnCommand Insight ウィンドウがすべて閉じていることを確認します。
3. の構文、コマンド引数、およびパラメータの使用方法を確認できます `oci-uninstall.sh` 次のコマンドを入力します。

   ```
   sudo /usr/bin/oci-uninstall.sh --help
   ```

   通常のアンインストールでは、Insightのライセンスや日次バックアップは削除されません。インストール全体を削除するには、を使用します `--purge` とOPTIOON`oci-install.sh` コマンドを実行します

4. 次のコマンドを入力します。

   ```
   sudo /usr/bin/oci-uninstall.sh
   ```

Data Warehouseをアンインストールしています

Data Warehouseは必要に応じてアンインストールできます。

作業を開始する前に

OnCommand Insight Data Warehouse（DWH）データベースの現在のバージョンをバックアップします。

このタスクについて

OnCommand Insight Data Warehouseをアンインストールすると、以前に収集したすべてのデータが完全に削除されます。

手順

1. sudo権限があるアカウントでData Warehouseサーバにログインします。
2. OnCommand Insight ウィンドウがすべて閉じていることを確認します。
3. の構文、コマンド引数、およびパラメータの使用方法を確認できます `uninstall.sh` 次のコマンドを入力します。 `sudo /usr/bin/oci-uninstall.sh --help`
4. 次のコマンドを入力します。 `sudo /usr/bin/oci-uninstall.sh`

Remote Acquisition Unitのアンインストール

Remote Acquisition Unitが不要になった場合はアンインストールできます。

手順

1. sudo権限があるアカウントでRemote Acquisition Unitサーバにログインします。
2. OnCommand Insight ウィンドウがすべて閉じていることを確認します。
3. の構文、コマンド引数、およびパラメータの使用方法を確認できます `uninstall.sh` 次のコマンドを入力します。 `sudo /usr/bin/oci-uninstall.sh --help`
4. 次のコマンドを入力します。 `sudo /usr/bin/oci-uninstall.sh`

   アンインストールスクリプトが実行されます。プロンプトの指示に従います。

Microsoft Windows用のインストール

インストールの前提条件

OnCommand Insight をインストールする前に、現在のソフトウェアバージョンをダウンロードし、適切なライセンスを取得して、環境をセットアップする必要があります。

OnCommand Insight をインストールする前に、次のものがあることを確認してください。

- ダウンロードしたインストールパッケージに含まれている最新バージョンのOnCommand Insight ソフトウェアファイル
- ダウンロードしたOnCommand Insight バージョンを操作するためのライセンス
- 最小限のハードウェアおよびソフトウェア環境

  現在の製品では、以前のバージョンのOnCommand Insight 製品では使用されていなかった追加のハードウェアリソース（OnCommand Insight 製品の機能強化のため）が消費される可能性があります。

- OnCommand Insight サーバ、Data WarehouseとReporting、およびRemote Acquisition Unitのハードウェアとネットワークの構成を含む導入計画。
- ウィルススキャンソフトウェアを無効にしました

  OnCommand Insight のインストール中に、すべてのウイルススキャナを完全に無効にする必要があります。インストール後、Insightコンポーネントで使用されるパス（インストール、バックアップ、およびアーカイブの各パス）をウィルススキャンから除外し、全体を除外する必要があります `sanscreen` スキャンからのディレクトリ。

  また、インストール後に、IBM/DB2フォルダ（例：*C：\Program Files\IBM\DB2*）をアンチウィルススキャンから除外する必要があります。

> アップグレードまたは新しいハードウェアへの移行としてフルインストールを実行し、既存の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は、インストールを実行する前にセキュリティ設定をバックアップする必要があります。インストールの完了後、Server（Local Acquisition Unitを含む）またはData Warehouseデータベースをリストアする前に、セキュリティ設定をリストアする必要があります。DWHデータベースをリストアする前に、セキュリティ設定をすべてのInsight Serverにリストアする必要があります。
>
> インプレースアップグレード（Insight Serverでのみ使用可能）では、セキュリティ設定が適切に処理されるため、リストアする必要はありません。
>
> を使用します `securityadmin` 構成のバックアップを作成し、保存されている構成を復元するツール。詳細については、を検索してください `securityadmin` OnCommand Insight ドキュメントセンター： http://docs.netapp.com/oci-73/index.jsp

導入を計画します

導入を成功させるには、OnCommand Insight をインストールする前に特定のシステム要素を考慮する必要があります。

このタスクについて

Insightの導入計画では、次のシステム要素を考慮する必要があります。

- Insightアーキテクチャ
- 監視するネットワークコンポーネント
- Insightのインストールの前提条件とサーバ要件
- Insight Webブラウザの要件

データソースのサポート情報

設定計画の一環として、環境内のデバイスをInsightで監視できることを確認する必要があります。そのためには、データソースサポートマトリックスでオペレーティングシステム、特定のデバイス、プロトコルの詳細を確認できます。一部のデータソースは、オペレーティングシステムによっては使用できない場合があります。

データソースサポートマトリックスの最新バージョンの場所

OnCommand Insight データソースサポートマトリックスは、サービスパックのリリースごとに更新されます。ドキュメントの最新バージョンについては、を参照してください "NetApp Support Site"。。

デバイスの識別とデータソースの計画

導入計画の一環として、環境内のデバイスに関する情報を収集する必要があります。

環境内の各デバイスについて、次のソフトウェア、接続、および情報が必要です。

- OCIサーバが解決できるIPアドレスまたはホスト名
- ログイン名とパスワード
- デバイスへのアクセスのタイプ（コントローラや管理ステーションなど）

> ほとんどのデバイスには読み取り専用アクセスで十分ですが、管理者権限が必要なデバイスもあります。

- データソースポートの要件に応じたデバイスへのポート接続
- スイッチの場合、SNMPの読み取り専用コミュニティストリング（スイッチへのアクセスを許可するユーザIDまたはパスワード）
- デバイスに必要なサードパーティ製ソフトウェア（Solutions Enablerなど）。
- データソースの権限と要件の詳細については、Web UIヘルプまたは_ OnCommand Insight 構成および管理ガイド_で「ベンダー固有のデータソースリファレンス」を参照してください。

OnCommand Insight で生成されるネットワークトラフィック

OnCommand Insight で生成されるネットワークトラフィック、ネットワークを通過する処理データの量、およびOnCommand Insight によるデバイスへの負荷は、多くの要因によって異なります。

トラフィック、データ、および負荷は、次の要因に基づいて環境によって異なります。

- 生データ
- デバイスの構成
- OnCommand Insight の導入トポロジ
- インベントリデータやパフォーマンスデータソースのポーリング間隔が異なるため、低速なデバイスを検出したり帯域幅を節約したりするために、間隔を短くすることができます

OnCommand Insight で収集される生の構成データは大きく異なる場合があります。

次の例は、設定データがどのように変化し、多くの設定要因によってトラフィック、データ、および負荷がどのように影響するかを示しています。たとえば、2つのアレイにそれぞれ1、000本のディスクがあるとします。

- アレイ1：1、000本のSATAディスクがあり、すべて1TBです。1、000本のディスクがすべて1つのストレージプールに含まれ、ESXクラスタ内の同じ32ノードに対して1、000個のLUNが提供（マッピングおよびマスク）されます。
- アレイ2：2TBのデータディスクが400本、600GBのFCディスクが560本、SSDが40本あります。ストレージプールは3つありますが、FCディスクのうち320本が従来のRAIDグループで使用されています。RAIDグループに分割されたLUNは従来のマスキングタイプ（symmaskdb）を使用し、シンプロビジョニングされたプールベースのLUNは新しいマスキングタイプ（symaccess）を使用します。150の異なるホストに対して600個のLUNが提供されました。200個のBCV（600個のLUNのうち200個のフルブロックレプリカボリューム）があります。また、別のサイトのアレイ上に存在するボリュームのリモートレプリカボリュームである200個のR2ボリュームもあります。

それぞれ1、000本のディスクと1、000個の論理ボリュームで構成されています。データセンターで消費するラックスペースが物理的に同じである場合もあれば、同じファームウェアを実行している場合もありますが、2つ目のアレイの構成は1つ目のアレイよりもはるかに複雑です。

ウィルススキャンソフトウェアの無効化

システムでウイルス対策ソフトウェアがアクティブになっている場合、OnCommand Insight のインストールは失敗します。この問題を回避するには、インストール前にウィルススキャンソフトウェアを無効にします。

アクティブなウィルススキャンソフトウェアによるインストールの失敗を回避するには、各OnCommand Insight コンポーネントのインストール中に、すべてのウィルススキャンを完全に無効にする必要があります。インストール後、Insightコンポーネントで使用されるパス（インストール、バックアップ、およびアーカイブのパス）をウィルススキャンから除外する必要があります。

また、インストール後に、IBM/DB2フォルダ（例：*C：\Program Files\IBM\DB2*）をアンチウィルススキャンから除外する必要があります。

Insight Serverの要件

専用のサーバを使用することを推奨します。他のアプリケーションがインストールされているサーバにはInsightをインストールしないでください。製品の要件が満たされていれば、物理サーバと仮想サーバの両方がサポートされます。

OnCommand Insight サーバソフトウェアをインストールするには、ローカル管理者の権限が必要です。

> OnCommand Insight のサイジングには、データソースのタイプとサイズ、環境内のアセットの数、ポーリング間隔など、さまざまな要素を考慮する必要があります。次のサイジング例はあくまでもガイドラインであり、Insightでテストされた一部の環境を示したものです。環境内でこれらの要素やその他の要素を変更すると、Insightのサイジング要件が変更される可能性があります。これらのガイドラインには、最大90日間のパフォーマンスアーカイブデータ用のディスクスペースが含まれます。

詳細なサイジングガイダンスについては、Insightをインストールまたはアップグレードする前に、担当のセールスエンジニアに問い合わせることを推奨します。

例：

環境要因：	テストしたディスク容量、CPU、メモリ：
80ストレージアレイ4、000ボリューム 4、000台のVM 4、000個のスイッチポート	250GBディスクスペース8コア 32GBのRAM
160個のストレージアレイ40、000個のボリューム 8、000台のVM 8、000個のスイッチポート	1TBのディスクスペース12コア 48GBのRAM

要件：

コンポーネント	必須
オペレーティングシステム	64ビットのMicrosoft Windows Server 2016、2019、または2022（最新のサービスパックを適用）を実行しているコンピュータ。 Windows Server 2012で導入されたResilient File System（ReFS）は、OnCommand Insight と互換性がありません。OnCommand Insight のWindowsインストールは、NTFSファイルシステムでのみサポートされます。 専用のサーバを使用することを推奨します。
仮想マシン（VM）	このコンポーネントは、インスタンスのCPUリソースとメモリリソースが予約されていれば、仮想環境で実行できます。

メモリとCPU	24~256GBのRAM 8~32コア ページングファイルサイズを"`Windows managed`"に設定することを強くお勧めします。サイズが固定された小さなページングファイルは、Insightのパフォーマンスデータの正常な格納に支障をきたす可能性があります。
使用可能なディスクスペース	100GB~3TBのインストールディスクスペース 50 GB~1 TBのパフォーマンスアーカイブディスクスペース InsightのインストールスペースにはSSDディスクを使用することを推奨します。
ネットワーク	イーサネット接続とポート： • 専用の（静的な）IPアドレスを使用した100Mbpsまたは1Gbpsのイーサネット接続、およびSANのすべてのコンポーネント（FCデバイスやRemote Acquisition Unitなど）へのIP接続。 • OnCommand Insight サーバプロセスのポート要件は、80、443、1090~1100、3873、8083、4444$_{4446、5445、5455、4712}$4714、5500、 そして5501 • 取得プロセスには、ポート12123と5679が必要です。 • MySQLにはポート3306が必要です。 • Elasticsearchには、ポート9200と9310が必要です • Win2008/2012の動的ポート要件は、49152~65535です ポート443および3306は、存在するファイアウォールを介した外部アクセスを必要とします。

権限	OnCommand Insight サーバに対するローカル管理者権限が必要です。 次のフォルダのいずれかがシンボリックリンクである場合は、リンク先ディレクトリに「755」権限があることを確認してください。 • /opt/netapp • /var/lib/netapp • /var/log/netapp
リモート接続	インストールおよびインストール後のサポートを容易にするために、WebExアクセスまたはリモートデスクトップ接続を可能にするインターネット接続。
アクセス性	HTTPSアクセスが必要です。
ウィルススキャン	このOnCommand Insight コンポーネントのインストール中に、すべてのウイルススキャナを完全に無効にする必要があります。インストール後、Insightコンポーネントで使用されるパス（インストール、バックアップ、およびアーカイブのパス）をウィルススキャンから除外する必要があります。 また、インストール後に、IBM/DB2フォルダ（例：*C：\Program Files\IBM\DB2*）をアンチウィルススキャンから除外する必要があります。
HTTPサーバまたはHTTPSサーバ	Microsoftインターネットインフォメーションサービス（IIS）またはその他のHTTPSサーバは、OnCommand Insight サーバと同じポート（443）で競合しないようにし、自動的に起動しないようにします。ポート443をリスンする必要がある場合は、他のポートを使用するようにOnCommand Insight サーバを設定する必要があります。

Data Warehouseおよび**Reporting**サーバの要件

Data WarehouseとReportingサーバは、ハードウェアとソフトウェアの所定の要件に準拠したコンピュータで実行する必要があります。このコンピュータにApache Webサーバまたは Reportingソフトウェアがインストールされていないことを確認してください。

> OnCommand Insight のサイジングには、環境内のアセットの数、保持する履歴データの量など、さまざまな要素が関係します。次のData Warehouseのサイジング例はあくまでもガイドラインであり、Insightでテストされた一部の環境を示したものです。環境内でこれらの要素やその他の要素を変更すると、Insightのサイジング要件が変更される可能性があります。

詳細なサイジングガイダンスについては、Insightをインストールまたはアップグレードする前に、担当のセー

ルスエンジニアに問い合わせることを推奨します。

例：

環境要因：	テストしたディスク容量、CPU、メモリ：
ストレージアレイ18台、VM 3、400台 4、500個のスイッチポート	200 GBのハードディスク8コア 32GBのRAM
110台のストレージアレイ11、500台のVM 14、500個のスイッチポート	300 GBハードディスク8コア 48GBのRAM

要件：

コンポーネント	必須
オペレーティングシステム	64ビットのMicrosoft Windows Server 2016、2019、または2022（最新のサービスパックを適用）を実行しているコンピュータ。
仮想マシン（VM）	このコンポーネントは、インスタンスのCPUリソースとメモリリソースが予約されていれば、仮想環境で実行できます。
CPU	8~40個のCPUコア
メモリ	32 GB~2 TB RAMのベストプラクティス：ページングファイルのサイズを「Windows managed」に設定することを強く推奨します。サイズが固定された小さなページングファイルは、Insightのパフォーマンスデータの正常な格納に支障をきたす可能性があります。

使用可能なディスクスペース	200GB-2TBディスクスペースインストールには'C:ドライブに最低20GBの空き容量が必要です Windowsでは、Insight Data Warehouse with Reportingをインストールする前に、インストールドライブで8dot3の名前作成サポートを有効にする必要があります。通常、C:ドライブではデフォルトで有効になっています。ターゲットインストールドライブで8dot3名の作成が有効になっているかどうかを検証するには、次のコマンドを実行します（D:をターゲットインストールドライブに置き換えます）。 fsutil 8dot3nameクエリD： 8dot3名の作成を有効にするには、次のコマンドを実行します（D:をインストール先ドライブに置き換えます）。 fsutil 8dot3nameセットD:0
ネットワーク	• 100 Mbpsまたは1 Gbpsのイーサネット接続 • 静的IPアドレス • Data WarehouseとReportingをWindowsにインストールする前に、ポート50000が使用可能である必要があります • OnCommand Insight DWHサーバプロセスの場合は、ポート80、443、1098、1099、 3873、8083、4444〜4446 • レポートエンジンの場合は、ポート1527、9362、9300、および9399 • MySQLの場合は、ポート3306 • を実行して、DNSが正しく機能していることを確認します `nslookup` ホストに対して
ウィルススキャン	このOnCommand Insight コンポーネントのインストール中に、すべてのウイルススキャナを完全に無効にする必要があります。インストール後、Insightコンポーネントで使用されるパス（インストール、バックアップ、およびアーカイブのパス）とDWHコンポーネントのすべてのインストールパス（SANscreen、DB2、およびバックアップのパス）をウィルススキャンから除外する必要があります。

Visual Studio	Visual Studio 2019 "再配布可能" Data WarehouseとReportingをWindowsにインストールする前にインストールする必要があります。

Remote Acquisition Unitサーバの要件

ファイアウォールの背後、リモートサイト、プライベートネットワーク、または異なるネットワークセグメントにあるSANデバイスから情報を取得するには、Remote Acquisition Unit（RAU）をインストールする必要があります。RAUをインストールする前に、オペレーティングシステム、CPU、メモリ、およびディスクスペースの要件を満たしていることを確認する必要があります。

コンポーネント	要件
オペレーティングシステム	64ビットのMicrosoft Windows Server 2016、2019、または2022（最新のサービスパックを適用）を実行しているコンピュータ。
CPU	4 個の CPU コア
メモリ	16GB の RAM
使用可能なディスクスペース	40 GB
ネットワーク	100Mbps/1Gbpsイーサネット接続、静的IPアドレス、すべてのFCデバイスへのIP接続、OnCommand Insight サーバへの必要なポート（80または443）。
権限	RAUサーバに対するローカル管理者権限
ウィルススキャン	このOnCommand Insight コンポーネントのインストール中に、すべてのウイルススキャナを完全に無効にする必要があります。インストール後、Insightコンポーネントで使用されるパスをウィルススキャンから除外する必要があります。また、インストール後に、IBM/DB2フォルダ（例：*C：\Program Files\IBM\DB2*）をアンチウィルススキャンから除外する必要があります。

OnCommand Insight でサポートされているブラウザ

ブラウザベースのOnCommand InsightWeb UIは、いくつかの異なるブラウザで動作できます。

Insightでは、次のブラウザのベータ版以外の新しいリリースがサポートされます。

- Mozilla Firefox
- Google Chrome
- Microsoft Edge の場合

OnCommand Insight に対応したブラウザバージョンの完全なリストについては、を参照してください "NetApp Interoperability Matrix Tool で確認できます"。

Insightのインストール手順

のインストールでは、Insight Server、Data WarehouseおよびReportingなど、複数のOnCommand Insightコンポーネントをインストールする必要があります。インストールには、次の主な作業が含まれます。

- OnCommand Insight インストーラをダウンロードしています
- OnCommand Insight サーバをインストールしています
- ライセンスのインストール
- DWHとReportingのインストール（オプション）（別のマシンまたは仮想マシンにインストールする必要があります）
- Remote Acquisition Unit（RAU）のインストール（オプション）。RAUは、ファイアウォールの内側、リモートサイト、またはプライベートネットワークに配置されたデバイスリソースから情報を取得します
- アップグレードの場合は、OnCommand Insight レポートをアップグレードします。

インストールが完了したら、環境に関する情報を取得するようにInsightを設定する必要があります。必要な作業については、_ OnCommand Insight 構成および管理ガイド_を参照してください。

OnCommand Insight インストーラをダウンロードしています

OnCommand Insight インストーラはNetApp Support Site からダウンロードできます。

作業を開始する前に

NetApp Support Site へのログインが必要です "mysupport.netapp.com"。

手順

1. OnCommand Insight をインストールするサーバにログインします。
2. NetApp Support Site からインストールファイルをダウンロードします。

OnCommand Insight サーバをインストールしています

OnCommand Insight サーバは、OnCommand Insight セットアップウィザードを使用して簡単にインストールできます。

作業を開始する前に

インストールの前提条件をすべて満たしておく必要があります。

手順

1. 管理者権限があるアカウントでInsight Serverにログインします。
2. Windowsエクスプローラを開き、インストールファイルが保存されているディレクトリに移動します。
3. をダブルクリックします `.MSI` ダウンロードしたファイル。
4. 「 * 次へ * 」をクリックして続行します。
5. ライセンス契約を読み、**[I accept the terms in the License Agreement]***チェックボックスをオンにして、[Next]*をクリックします。
6. [Customer Information]ウィンドウに顧客名とサイト名を入力し、*[Next]*をクリックします。

   *ベストプラクティス：*サイトのプレフィックスとしてお客様名を使用します（例：NetApp）。

7. [お客様情報：NetApp ASUPの設定]*ウィンドウで、次の手順を実行します。

   a. 次のいずれかのオプションを選択して、ASUPにアップロードするデータが格納されているデータベースを選択します。

      - データベースバックアップなし：バックアップはASUPに送信されません。
      - パフォーマンスデータなしのバックアップ：バックアップを作成してASUPに送信しますが、パフォーマンスデータは含まれません。
      - パフォーマンスデータを使用したバックアップ：パフォーマンスデータを含むバックアップが作成されますが、大量のデータが生成される可能性があります `*.gz` ファイル。

      ASUPはHTTPSプロトコルを使用して配信されます。

   +

   a. [ログ]*で、データソースを記録するログなし、ベースログ、拡張ログのいずれかを選択します。
   b. 「 * 次へ * 」をクリックします。

8. 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。
9. 「 * 次へ * 」をクリックします
10. [サーバの設定]ウィンドウで、OnCommand Insight サーバを設定するための適切な設定パラメータを選択または設定します。

オプション	説明

ポータルポート（HTTP）	ユーザのWebサービス（管理タスクを実行するためのポータルなど）をサポートするためにOnCommand Insight サーバで使用されるポート。デフォルト（80）を使用します。ただし、デフォルトポートが使用中の場合は、別のポートに変更します。
ポータルポート（HTTPS）	Remote Acquisition Unitで、セキュアなチャネル経由でOnCommand Insight サーバにSAN変更情報を送信するために使用するポート。デフォルト（443）を使用します。ただし、デフォルトポートが使用中の場合は、別のポートに変更します。RAUの設定時に同じポート番号を指定します。
内部データベースポート（SQL）	OnCommand Insight サーバが実行されているPCによって内部的に使用されるポート。データベースへのアクセスポイントとして機能します。デフォルト（3306）を使用します。ただし、デフォルトポートが使用中の場合は、別のポートに変更します。

11. 「 * 次へ * 」をクリックします。
12. 続行するには*[インストール]*をクリックしてください。

    インストールには約20分かかります（インストールされているアプリケーションによって異なります）。

13. [完了] をクリックします。

OnCommand Insight Data WarehouseおよびReportingをインストールしています

インストールは自己完結型で、OnCommand Insight Data Warehouse（DWH）およびReportingユーティリティの実行と運用に必要な要素が含まれています。

作業を開始する前に

インストールまたはアップグレードを行う前に、以下の点に注意してください。

- アップグレードする場合は、DWHをバックアップします。
- ReportingをOnCommand Insight Data Warehouseをインストールするには、local*administrator*権限が必要です。
- Windows Modules Installerサービスが有効になっていることを確認します(自動または手動)。
- C:ドライブ以外にインストールする場合は、短いファイル名を有効にする必要があります。有効になっていない場合は、インストーラによって有効になります。
- DB2コンポーネントの場合、DB2 Userには_DOMAIN_USERまたは_LOCAL_USERを指定できます。
  - DB2ユーザがA_DOMAIN_USERの場合は、次の情報が必要です。
    - DB2ユーザを作成しておく必要があります。また、ユーザ名とパスワードを確認しておく必要があります

- DWHとReportingをインストールするユーザは、DB2ユーザを照会できる必要があります。これを検証するには、次のコマンドを使用します。
  - `net user <db2 user name> /domain`
- DB2ユーザがA_LOCAL_USERの場合は、次の情報が必要です。
  - DB2 Userとして実行するユーザのユーザ名とパスワード。このユーザが存在しない場合は、インストールによって作成されます。
- 注

DB2ユーザ名およびWindowsログイン名には次の制限があります。*有効な文字は次のとおりです。'A'～'Z'；'A'～'z'；'0'～'9'；'_'；'@'；'$'；'#'；'!'；'(';')';'{';'}'、'-'、および'。*特殊文字'!';'(';';'}';「-」、および「。」ユーザ名にはすべて大文字を使用する必要があります。*文字は、アルファベット、@、、または$である必要があります。数字または文字列_SYS、DBは_IBM_を使用することはできません。128バイトを超えることはできません。*ユーザー、管理者、ゲスト、パブリック、ローカル、またはSQL予約語は使用できません。

- DB2ユーザを、インストールを実行するユーザと同じにすることはできません。

手順

1. 管理者権限があるアカウントでData Warehouseサーバにログインします。
2. Data WarehouseとReporting.zipファイルをダウンロードし、インストールフォルダにファイルを展開します。
3. <download location> \OCI_DWH_installer_フォルダに移動し、_install_oci_dwh.bat_scriptを実行します。

   OnCommand Insight 7.3.10以降では、DWH / Reportingを適切にインストールするためのスクリプトを実行する必要があります。.msiインストール実行ファイルを実行しないでください。

4. DB2ドメインを入力するか、Enterキーを押してローカル・ドメインを入力します。
5. DB2ユーザー名を入力します。ユーザー名の制限については、上記を参照してください。
6. DB2ユーザのパスワードを入力します。プロンプトが表示されたら、パスワードを再入力します。
7. DB2コンポーネントのインストールパスを入力するか、デフォルトの場合はEnterキーを押します。
8. 入力した情報が表示されます。すべての設定を慎重に確認してください。Enterキーを押してインストールを開始します。
9. プロンプトが表示されたら、WindowsがDB2のインストールを続行できるようにします。
10. DB2のインストールに続いて、DWHのインストールウィザードが実行されます。指示に従って、DWHとReportingをインストールします。

    Data WarehouseとReportingのインストールが完了するまでに最大1時間かかることがあります。

IBM Cognosのドキュメントを参照してください

Reporting Portalソフトウェアを開始および停止する方法など、基本的な情報について

は、製品とともにインストールされるIBM Cognosのドキュメントを参照してください。Query Studio、Report Studio、Business Insight、Business Insight Advancedなど、IBM Cognosのレポート製品に関する情報は、WebブラウザでIBMのWebサイトのInformation Centerで検索できます。

手順

1. OnCommand Insight とともにインストールされるIBM Cognosのドキュメントを参照するには、このディレクトリに移動します。

   ```
   <install_dir\>\cognos\c10_64\webcontent\documentation\help_docs.html
   ```

2. また、OnCommand Insight Reportingポータルで使用されるIBM Cognosの個 々 のウィンドウについて説明したトピックも表示できます。ウィンドウツールバーの*？*アイコンをクリックします。

Data Warehouseと**Reporting**のインストールを確認しています

OnCommand Insight Data Warehouseのインストールが完了したら、DWHサービスとReportingサービスをすべてMicrosoft Windowsサービスで使用できることを確認する必要があります。

手順

1. Windowsの[スタート]メニューから、[コントロールパネル][システムとセキュリティ]>[管理ツール]>[サービス]の順に選択します。
2. サービスのリストに次のエントリが表示されていることを確認します。

名前/都道府県	説明
• SANscreen サーバ/実行中*	OnCommand Insight DWHサーバ
• MySQL /実行中*	OnCommand Insight SQLデータベース
• IBM Cognos / Running *	IBM Cognos Content Databaseの略
• DB2-DB2COPY1-DB2-0/Running *	DB2データベースを管理します
• DB2 Governor（DB2COPY1）/実行されていません*	DB2データベースに接続されているアプリケーションの統計情報を収集します。
• DB2 License Server（DB2COPY1）/実行されていません*	DB2ライセンスコンプライアンスを監視します。
• DB2 Management Service（DB2COPY1）/実行中*	以前のバージョンのDB2コピーとの互換性のために、DB2レジストリエントリを管理します。

DB2リモートコマンドサーバ（**DB2COPY1**）/実行中	リモートDB2コマンドの実行をサポートします。
• IBM Secure Shell Server for Windows / Not Running*	IBM Secure Shell Server for Windowsの略

Remote Acquisition Unit（RAU）のインストール

OnCommand Insight 環境に1つ以上のRAUをインストールします。

作業を開始する前に

インストールの前提条件をすべて満たしておく必要があります。

変更情報をサーバに転送するには、少なくとも1つのポートが開いていて、RAUサーバとOnCommand Insight サーバの間で使用可能である必要があります。不明な場合は、RAUコンピュータでWebブラウザを開き、OnCommand Insight サーバに移動して検証します。

```
https://< OnCommand Insight Server hostname >:< acquisition_port >
```

Acquisitionのデフォルトポートは443ですが、サーバのインストール時に変更されている可能性があります。接続に成功すると、OnCommand Insight 応答ページが表示され、RAUとOnCommand Insight サーバの間でポートが開いて使用可能になったことが示されます。

手順

1. 管理者権限があるアカウントでRAUサーバにログインします。
2. エクスプローラを開き、RAUインストールファイルが格納されているディレクトリに移動します。
3. をダブルクリックします `.MSI` ファイルをクリックしてインストールを開始します。
4. をクリックして、ライセンス契約のウィンドウに進みます。これを読んでライセンス契約の条項に同意し、[次へ]*をクリックします。
5. RAUをローカルハードドライブにインストールするか、機能全体をローカルハードドライブにインストールするかを選択します。（[Disk Usage]リンクをチェックして、十分なスペースがあることを確認できます。116MBが必要です）。 [次へ]*をクリックします。
6. [構成]ウィンドウで、サイトに固有の次のパラメータを設定します。
   - * OnCommand Insight *サーバー名またはアドレス- OnCommand Insight サーバーを識別するホスト名またはIPアドレス。RAUはこの名前/ IPを使用してサーバとの通信リンクを開きます。ホスト名を指定する場合は、DNSで解決できることを確認してください。
   - * Acquisition Unit Name *- RAUを識別する一意の名前。
   - * OnCommand Insight Secured Remote Acquisition Port（HTTPS）*- Remote Acquisition Unitが環境の変更情報をOnCommand Insight サーバに送信するために使用するポート。この設定は、OnCommand Insight サーバのインストール時に入力した値と一致し、すべてのRAUで同じである必要があります。

7. 選択内容を確認します。前に戻って変更を行うには、*[戻る]*をクリックします。「 * 次へ * 」をクリックします。
8. [インストール]*をクリックしてインストールを開始します。

   インストールが完了するまで待ちます。この処理には約5〜10分かかります。

完了後

インストールが完了すると、最後のウィンドウが表示されます。[Start Remote Acquisition Service]*ボックスをクリックしてRAUを開始し、[Finish]*をクリックしてこの処理を終了します。

Remote Acquisition Unitサービスを確認しています

Remote Acquisition Unit（RAU）のインストールが完了すると、OnCommand Insight RAUサービスをMicrosoft Windowsサービス環境で使用できるようになります。

手順

1. RAUがWindowsサービスに追加されたことを確認するには、Windowsの[スタート]メニューを開き、**[**コントロールパネル**]>*>**[サービス]*を選択します。
2. リストから*「OnCommand Insight Acq - OnCommand Insight’s Remote Acquisition Unit（RAU）」*を探します。

Remote Acquisition Unitのインストールを検証しています

Remote Acquisition Unitが適切にインストールされていることを確認するために、サーバに接続されているRemote Acquisition Unitのステータスを表示できます。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. Acquisition Units *をクリックします。
3. 新しいRemote Acquisition Unitが正しく登録され、ステータスが「Connected」になっていることを確認します。

   表示されない場合は、テクニカルサポートにお問い合わせください。

インストールを確認しています

サポートされているブラウザでInsightを開くと、インストールされているかどうかを確認できます。Insightのログファイルを確認することもできます。

Insightを初めて開いたときに、ライセンスのセットアップページが開きます。ライセンス情報を入力したら、データソースを設定する必要があります。データソース定義の入力、およびOnCommand Insight のユーザと通知の設定については、_ Configuration and Administration Guide _を参照してください。

インストール時に問題が発生した場合は、テクニカルサポートに連絡して、必要な情報を提供してください。

新しい**Insight**サービスを確認しています

インストールが完了したら、サーバでInsightコンポーネントのサービスが動作していることを確認する必要があります。

手順

1. 現在動作しているサービスのリストを表示するには、次の手順を実行します。
   a. [スタート]ボタンをクリックします。
   b. [ファイル名を指定して実行] をクリック
   c. 次のように入力します。

      ```
      cmd
      ```

   d. Enter キーを押します。
   e. [コマンドプロンプト]ウィンドウで次のように入力します。

      ```
      net start
      ```

2. 次のInsightサービスがリストに表示されているかどうかを確認します。
   - * SANscreen サーバ*
   - * SANscreen Acq*（取得プロセス）
   - * MySQL *（Insight SQLデータベース）
   - * Elasticsearch *（Insightデータ用のデータストア）これらのサービスがリストに表示されない場合は、テクニカルサポートにお問い合わせください。

Insightのログ

Insightには、調査やトラブルシューティングに役立つ多数のログファイルが用意されています。使用可能なログは、logディレクトリに一覧表示されます。BareTailなどのログ監視ツールを使用すると、すべてのログを一度に表示できます。

ログファイルはにあります `<install directory>\SANscreen\wildfly\standalone\log` ディレクトリ。収集ログはにあります `<install directory>\SANscreen\Acq\Log` ディレクトリ。

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。

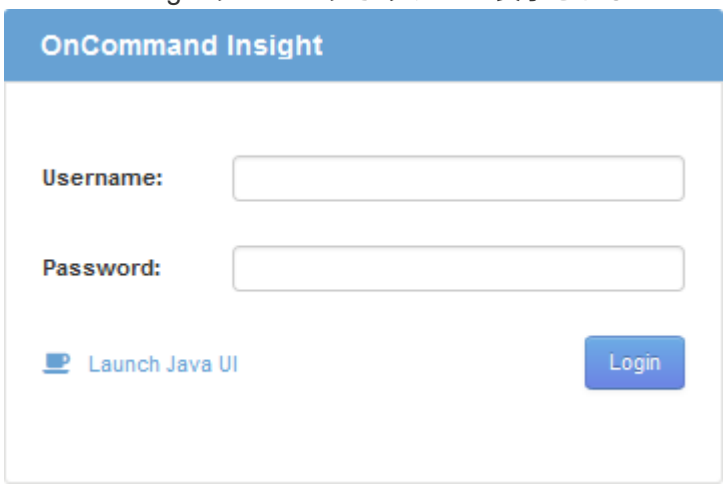
```
https://fqdn
```

- 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）

インストールのトラブルシューティング

OnCommand Insight のインストールは、通常、インストールウィザードを使用して管理します。ただし、コンピュータ環境によっては、アップグレード中に問題が発生したり、競合が発生したりする可能性があります。

また、ソフトウェアのインストールに必要なOnCommand Insight ライセンスがすべてインストールされていることを確認する必要があります。

ライセンスがありません

OnCommand Insight 機能ごとに異なるライセンスが必要です。OnCommand Insight に表示される内容は、インストールされているライセンスによって制御されます。各ライセンスで制御される機能については、「OnCommand Insight ライセンス」セクションを参照してください。

各ライセンスで制御される機能については、「OnCommand Insight ライセンス」セクションを参照してください。

オンラインテクニカルサポートリクエストの送信

Insightのインストールで問題が発生した場合は、サポートに登録しておくとオンラインのテクニカルサポートリクエストを送信できます。

作業を開始する前に

オンラインサポートサービスを利用するには、会社のEメールアドレスを使用してサポートカスタマーとして登録する必要があります。登録はサポートサイトで行います 。

このタスクについて

カスタマーサポートがインストールの問題を解決できるようにするには、次の項目を含め、できるだけ多くの情報を収集する必要があります。

- Insightのシリアル番号
- 問題の概要
- Insightのすべてのログファイル
- エラーメッセージのスクリーンキャプチャ

手順

1. を作成します `.zip` トラブルシューティングパッケージを作成するために収集した情報のファイル。
2. サポートサイトにログインします "mysupport.netapp.com" をクリックし、* Technical Assistance *を選択します。
3. [ケースを開く]*をクリックします。
4. データのパッケージの指示に従ってください。

完了後

[Technical Assistance]ページの[Check Case Status]*を使用して、リクエストに従うことができます。

OnCommand Insight のアップグレード

通常、アップグレードはすべてのInsight Server（Insight Server、Data Warehouseサーバ、Remote Acquisition Unit）で実行する必要があります。OnCommand Insight の新しいリリースのアップグレード要件については、必ずリリースノートを参照してください。

ここに記載されている要件と手順は、特に断りのないかぎり、Insight 7.xから最新バージョンにアップグレードする場合に適用されます。7.0より前のバージョンからアップグレードする場合は、アカウント担当者にお問い合わせください。

Insightをバージョン**7.3.12**以降にアップグレードしています（**Windows**）

OnCommand Insight 7.3.10-7.3.11から7.3.12以降にアップグレードする前に、OCIデータ移行ツールを実行する必要があります。

背景（ **Background** ）

OnCommand Insight バージョン7.3.12以降では、以前のバージョンと互換性のないソフトウェアが使用されます。Insightバージョン7.3.12以降には、アップグレードに役立つ*データ移行ツール*が含まれています。

> OnCommand Insight バージョン7.3.9以前はサポートされなくなりました。これらのいずれかのバージョンを実行している場合は、7.3.12以降にアップグレードする前に、Insightバージョン7.3.10以降（7.3.11を推奨）にアップグレードする必要があります。

データ移行ツールの機能

移行ツールは、最初の互換性チェックを実行し、3つの異なるアップグレードパスのいずれかに従います。選択したパスは、現在のバージョンのデータ互換性に基づいています。

> アップグレードの前に、Data Migration Toolを実行し、推奨される手順に従う必要があります。

始める前に

- データ移行ツールを実行する前に、OnCommand Insight システムをバックアップすることを強く推奨します。
- サーバ上のElasticsearchサービスが稼働している必要があります。
- Insightをアップグレードする前に、データベースとパフォーマンスアーカイブに対してData Migration Tool_must_beを実行してください。

データ移行ツールの実行

1. 最新バージョンのData Migration Tool（_SANScreenDataMigrationTool-x86-7.3.12-97.zip_など）と適切なInsightインストーラファイルをInsight Serverにダウンロードします。作業フォルダに解凍します。ダウ

ンロードはにあります "NetApp Support Site"。

2. コマンドウィンドウを開き、作業フォルダに移動します。
   - 管理者としてPowerShellを開きます。
3. 次のコマンドを使用してデータ移行ツールを実行します。
   - `.\*SANScreenDataMigrationTool.ps1*`
4. 必要に応じて指示に従います。次に例を示します。

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-121

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.10 (139) is installed

Getting installation parameters...
Installation Directory:  C:\Program Files\SANscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 54 obsolete indexes. Of these,
    54 indexes may be migrated with OCI server running,
       the most recent of which is for 2021-05-13

Verifying migration component is present...
SANscreen Server service is Running

Proceed with online migration of 54 indexes (y or [n])?:
```

Data Migration Toolは、システムに古いインデックスが存在するかどうかをチェックし、検出されたインデックスがあるかどうかをレポートします。存在しない場合、ツールは終了します。

SANscreen サーバサービスの実行中に、一部のインデックスが移行される場合があります。その他のものは、サーバーが停止しているときにのみ移行できます。移行できるインデックスがない場合、ツールは終了します。それ以外の場合は、指示に従ってください。

Data Migration Toolが完了すると、古いインデックスがないか再確認されます。すべてのインデックスが移行されている場合は、OnCommand Insight 7.3.12へのアップグレードがサポートされていることが通知されます。これで、Insightのアップグレードを続行できます。

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-127

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.10 (139) is installed

Getting installation parameters...
Installation Directory:  D:\SANscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 5 obsolete indexes. Of these,
     5 indexes need to be migrated with OCI server stopped

Verifying migration component is present...
SANscreen Server service is Stopped

Proceed with offline migration of 5 indexes (y or [n])?: y
Preparing to perform migration...
Preparing to migrate ociint-inventory-snmp_win2012_host: copied; backup;
delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_interface: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_load_average: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_storage: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_tcp_connection: copied;
backup; delete old; restore new; cleanup; done.
Execution time 0:00:15

Checking for obsolete (version 5) indexes...
No obsolete indexes found.  Upgrade to 7.3.12+ is supported.

C:\Users\root\Desktop\SANScreenDataMigrationTool-x64-7.3.12-127>
```

SANscreen サービスの停止を求めるメッセージが表示された場合は、Insightをアップグレードする前にサービスを再起動します。

検証に失敗しました

インデックスの検証が失敗した場合、移行ツールは終了前に問題を通知します。

- OnCommand Insight が存在しません：*

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool V1.0

Checking OnCommand Insight Installation...
ERROR: OnCommand Insight is not installed
```

- Insightバージョンが無効です：*

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.4 (126) is installed
ERROR: The OCI Data Migration Tool is intended to be run against OCI 7.3.5
- 7.3.11
```

- Elasticsearchサービスが実行されていません：*

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.11 (126) is installed

Getting installation parameters...
Installation Directory:  C:\Program Files\SANscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
ERROR: The Elasticsearch service is not running

Please start the service and wait for initialization to complete
Then rerun OCI Data Migration Tool
```

コマンドラインオプション

Data Migration Toolには、その動作に影響するいくつかのオプションパラメータが含まれています。

オプション（Windows）	機能
-s	すべてのプロンプトを非表示にします
-perf_archive	指定すると、インデックスが移行された日付の既存のアーカイブエントリが置き換えられます。パスは、アーカイブエントリzipファイルが格納されているディレクトリを指す必要があります。 引数に「-」を指定すると、更新するパフォーマンスアーカイブがないことを示します。 この引数が指定されている場合、アーカイブ場所のプロンプトは表示されません。
-チェック	存在する場合、スクリプトはインデックスカウントを報告した直後に終了します。
-ドライラン	存在する場合、移行実行可能ファイルは実行されるアクション（データの移行とアーカイブエントリの更新）を報告しますが、操作は実行しません。

OnCommand Insight のアップグレードプロセスの概要

Insightのアップグレードを開始する前に、アップグレードプロセスについて理解しておくことが重要です。アップグレードプロセスは、Insightのほとんどのバージョンで同じです。

Insightのアップグレードプロセスで実行する作業の概要は次のとおりです。

- インストールパッケージをダウンロードしています
- Data Warehouseデータベースをバックアップしています

  データが誤ってレポートされないようにするには、Data WarehouseデータベースをInsightデータベースよりも先にバックアップしておく必要があります。

- Insightデータベースをバックアップしています

  Insightデータベースは、インプレースアップグレードを実行すると自動的にバックアップされます。アップグレード前にデータベースをバックアップし、Insight Serverとは別の場所に保存することを推奨します。アップグレードプロセスでは、Insightは新しいデータを収集しません。収集されないデータの量を最小限に抑えるには、アップグレード予定時刻の1~2時間以内にデータベースバックアップを開始する必要があります。

- Data WarehouseおよびRemote Acquisition Unitのセキュリティ設定をデフォルトの設定から変更した場合はバックアップします。

デフォルト以外のセキュリティ設定は、アップグレードの完了後、Data Warehouseデータベースをシステムにリストアする前に、Data WarehouseおよびRAUサーバにリストアする必要があります。

- Data Warehouseのカスタムレポートをバックアップしています

  Data Warehouseデータベースをバックアップすると、カスタムレポートも含まれます。Data Warehouseサーバにバックアップファイルが作成されます。Data Warehouseサーバとは別の場所にカスタムレポートをバックアップすることを推奨します。

- Data WarehouseとRemote Acquisition Unitソフトウェアのアンインストール（該当する場合

  Insight Serverはインプレースアップグレードが可能なため、ソフトウェアをアンインストールする必要はありません。インプレースアップグレードでは、データベースがバックアップされ、ソフトウェアがアンインストールされ、新しいバージョンがインストールされてから、データベースがリストアされます。

- Insight Server、Data Warehouse、およびRemote Acquisition Unitでのソフトウェアのアップグレード

  以前に適用されたライセンスはすべてレジストリに残ります。これらのライセンスを再適用する必要はありません。

- アップグレード後の手順の実行

OnCommand Insight のアップグレードチェックリスト

提供されるチェックリストを使用して、アップグレードの準備中に進捗を記録できます。これらのタスクは、アップグレードが失敗するリスクを軽減し、リカバリとリストアの作業を迅速に行うことを目的としています。

アップグレード準備のチェックリスト（必須）

条件	完了?
すべてのInsight Serverに対して、アップグレードプロセスを実行するために必要なWindowsのローカル管理者権限があることを確認します。	
Insight、Data Warehouse、またはRemote Acquisition Unitのサーバを32ビットプラットフォームにアップグレードする場合は、64ビットプラットフォームにアップグレードする必要があります。Insight 7.x以降では、64ビットプラットフォームでのみアップグレードできます。	

環境内のすべてのサーバでウィルス対策ソフトウェアを変更または無効にするために必要な権限があることを確認します。ウィルススキャンソフトウェアがアクティブな場合に発生するアップグレードの失敗を回避するには、Insightのインストールディレクトリを除外する必要があります (`disk drive:\install directory\sanscreen` アップグレード中のウィルススキャンへのアクセスを許可します。すべてのコンポーネントをアップグレードしたら、ウィルス対策ソフトウェアを再アクティブ化してかまいません。ただし、Insightのインストールディレクトリについては、スキャンからすべて除外するように設定してください。 また、インストール後に、IBM/DB2フォルダ（例：*C：\Program Files\IBM\DB2*）をアンチウィルススキャンから除外する必要があります。	

アップグレード準備のチェックリスト（ベストプラクティス）

条件	完了?
ほとんどのアップグレードには4〜8時間以上かかり、大企業では時間がかかることを考慮して、いつアップグレードするかを計画します。アップグレードにかかる時間は、使用可能なリソース（アーキテクチャ、CPU、およびメモリ）、データベースのサイズ、環境内の監視対象オブジェクトの数によって異なります。	
アップグレードプランについてアカウント担当者に問い合わせ、インストールされているInsightのバージョンとアップグレードするバージョンを伝えます。	
Insight、Data Warehouse、およびRemote Acquisition Unitに現在割り当てられているリソースが、引き続き推奨される仕様を満たしていることを確認します。すべてのサーバーの推奨サイジングガイドラインを参照してください。または、アカウント担当者に連絡してサイジングガイドラインについて相談することもできます。	
データベースのバックアップとリストアのプロセスに十分なディスクスペースがあることを確認してください。バックアッププロセスとリストアプロセスには、InsightサーバとData Warehouseサーバでバックアップファイルに使用されているディスクスペースの約5倍が必要です。たとえば、50GBのバックアップには、250~300GBの空きディスクスペースが必要です。	

InsightおよびData Warehouseのデータベースをバックアップするときは、Firefox®またはChrome™ブラウザにアクセスできることを確認してください。4GBを超えるファイルをアップロードおよびダウンロードするときに問題が発生するため、Internet Explorerは推奨されません。	
を削除します `.tmp` Insight Serverのファイル。次の場所にあります。 `<install directory>\SANscreen\wildfly\standalone\tmp`。	
重複するデータソースと運用停止されたデータソースをInsight Clientから削除します。運用が停止されたデータソースや重複したデータソースを削除すると、アップグレードの実行に必要な時間が短縮され、データ破損の可能性が軽減されます。	
Insightに付属のデフォルトのレポートに変更を加えた場合は、変更したレポートがシステムのアップグレードまたはリストア時に失われないように、別の名前で[Customer Reports]フォルダに保存してください。	
自分でまたはプロフェッショナルサービスで作成したカスタムのData Warehouseレポートがある場合は、XML形式でエクスポートして[Customer Reports]フォルダに移動し、バックアップを作成します。バックアップがData Warehouseサーバに配置されていないことを確認します。レポートを推奨フォルダに移動しないと、アップグレードプロセスでバックアップされない可能性があります。以前のバージョンのInsightでは、レポートを適切なフォルダに配置しないと、カスタムレポートや変更したレポートが失われる可能性があります。	
IBM Cognos Configurationユーティリティの設定はData Warehouseのバックアップには含まれないため、すべての設定を記録しておきます。これらの設定はアップグレード後に再設定する必要があります。ユーティリティはにあります `disk drive:\install directory\SANscreen\cognos\c10_64\bin64` Data Warehouseサーバ上のディレクトリ（を使用して実行） `cogconfigw` コマンド。または、Cognosの完全なバックアップを実行し、すべての設定をインポートすることもできます。詳細については、IBM Cognosのドキュメントを参照してください。	

アップグレード準備のチェックリスト（該当する場合）

条件	完了?
ブラウザに表示されるセキュリティ警告を原因として、Insightのインストール時に作成された自己署名証明書を内部の認証局によって署名された証明書に置き換えた場合は、にあるキーストアファイルをバックアップします。 `disk drive:\install directory\SANscreen\wildfly\standalone\configuration` アップグレード後にリストアします。これにより、Insightで作成された自己署名証明書が自己署名証明書で置き換えられます。	
環境に合わせて変更したデータソースがあり、変更内容がアップグレード後のInsightバージョンで有効かどうか不明な場合は、リカバリで問題が発生した場合にトラブルシューティングできるように、次のディレクトリのコピーを作成しておきます。 `disk drive:\install directory\SANscreen\wildfly\standalone\deployments\datasources.war`。	
を使用して、すべてのカスタムデータベーステーブルおよびビューをバックアップします `mysqldump` コマンドラインツールカスタムデータベーステーブルを復元するには、特権データベースアクセスが必要です。これらのテーブルのリストアについては、テクニカルサポートにお問い合わせください。	
カスタムの統合スクリプト、Insightデータソースに必要なサードパーティコンポーネント、バックアップなど、必要なデータがに保存されていないことを確認します `disk drive:\install directory\sanscreen` ディレクトリ。このディレクトリの内容はアップグレードプロセスによって削除されるためです。これらをから移動したことを確認してください `\sanscreen` ディレクトリを別の場所に移動します。たとえば、カスタムの統合スクリプトが環境に含まれている場合は、次のファイルを以外のディレクトリにコピーしてください `\sanscreen` ディレクトリ： `\install_dir\SANscreen\wildfly\standalone\deployments\datasources.war\new_disk_models.txt`。	

OnCommand Insight インストールパッケージのダウンロード

アップグレードを選択する前に、Insight、Data Warehouse、およびRemote Acquisition

Unit（該当する場合）のインストールパッケージをダウンロードしておく必要があります。パッケージのダウンロード時間 (`.msi` ファイル）は、使用可能な帯域幅によって異なります。

このタスクについて

インストールパッケージは、Insight Web UIを使用するか、から該当するOnCommand Insight のリンクに移動してダウンロードできます http://support.netapp.com/NOW/cgi-bin/software。

Insight Serverからインストールパッケージをダウンロードするには、次の手順を実行します。

手順

1. Webブラウザを開き、次のいずれかを入力してInsight Web UIを開きます。
   - Insight Serverで、次の作業を行います。 `https://localhost`
   - 任意の場所から： `https://IP Address:port or fqdn:port`

     ポート番号は443か、Insight Serverのインストール時に設定したポートです。URLでポート番号を指定しない場合、ポート番号はデフォルトで443になります。
2. Insightにログインします。
3. [ヘルプ]アイコンをクリックし、*[アップデートの確認]*を選択します。
4. 新しいバージョンが検出された場合は、メッセージボックスの指示に従います。

   新しいバージョンのInsightDescriptionページに移動します。
5. 概要 ページで Continue *をクリックします。
6. エンドユーザライセンス契約（EULA）が表示されたら、*[同意する]*をクリックします。
7. 各コンポーネント（Insight Server、Data Warehouse、Remote Acquisition Unitなど）のインストールパッケージのリンクをクリックし、*[名前を付けて保存]*をクリックしてインストールパッケージを保存します。

   アップグレードの前に、Data WarehouseとRemote Acquisition Unitのインストールパッケージを、それぞれのサーバのローカルディスクにコピーしておく必要があります。
8. [チェックサム]*をクリックし、各インストールパッケージに関連付けられている数値を書き留めます。
9. ダウンロードしたインストールパッケージが完了し、エラーが発生していないことを確認します。

   ファイル転送が不完全な場合、アップグレードプロセスで原因 の問題が発生する可能性があります。

   インストールパッケージのMD5ハッシュ値を生成するには、Microsoftのようなサードパーティのユーティリティを使用します"File ChecksumIntegrity Verifierの略" ユーティリティ。

データベースをバックアップしています

アップグレードの前に、Data WarehouseデータベースとOnCommand Insight データベースの両方をバックアップしておく必要があります。Data Warehouseデータベースのバ

ックアップが必要になるのは、アップグレードプロセスの後半でデータベースをリストアできるようにするためです。Insightのインプレースアップグレードではデータベースがバックアップされますが、ベストプラクティスとして、アップグレード前にデータベースをバックアップしておくことを推奨します。

データが誤ってレポートされないように、Data WarehouseデータベースをInsightデータベースよりも先にバックアップしておく必要があります。また、テスト環境がある場合は、アップグレードを続行する前にバックアップをリストアできることを確認することを推奨します。

Data Warehouseデータベースをバックアップしています

CognosのバックアップもData Warehouseデータベースをファイルにバックアップし、あとでData Warehouseポータルを使用してリストアできます。バックアップを作成すると、別のData Warehouseサーバに移行したり、新しいバージョンのData Warehouseにアップグレードしたりできます。

手順

1. Data Warehouseポータルにログインします `https://fqdn/dwh`。
2. 左側のナビゲーションペインで、*[バックアップ/リストア]*を選択します。
3. [バックアップ]*をクリックし、バックアップ構成を選択します。

   a. Performance Datamartを除くすべてのDatamarts
   b. すべてのデータマート

      この処理には30分以上かかることがあります。

   + Data Warehouseでバックアップファイルが作成され、その名前が表示されます。

4. バックアップファイルを右クリックし、目的の場所に保存します。

   ファイル名は変更しなくてもかまいませんが、Data Warehouseのインストールパス以外の場所に保存してください。

   Data Warehouseのバックアップファイルには、DWHインスタンスのMySQL、カスタムスキーマ（MySQL DB）とテーブル、LDAP設定、CognosをMySQLデータベースに接続するデータソース（Insight Serverをデータを取得するデバイスに接続するデータソースではない）が含まれています。 レポートをインポートまたはエクスポートしたタスクのインポートとエクスポート、セキュリティロール、グループ、名前空間のレポート、ユーザーアカウント Reporting Portalの変更後のレポートとカスタムレポート（保存場所に関係なく、[My Folders]ディレクトリにも保存されます）。Cognosのシステム設定パラメータ（SMTPサーバ設定など）、およびCognosのカスタムメモリ設定はバックアップされません。

   カスタムテーブルがバックアップされるデフォルトのスキーマには、次のものがあります。

dwh_capacityの略
dwh_capacity_stagingの略

dwh_dimensionsの略
dwh_fs_utilを参照してください
dwh_inventoryの略
dwh_inventory_stagingの略
dwh_inventory_transient
dwh_managementの略
dwh_performanceの略
dwh_performance_stagingの略
DWH_ポート
dwh_reportsの略
dwh_sa_stagingの略

カスタムテーブルをバックアップから除外するスキーマには、次のものがあります。

information_schema
取得
cloud_model
host_data
InnoDB
在庫
inventory_private
inventory_time
ログ

管理
MySQL
NAS
パフォーマンス
performance_schema
performance_viewsの略
SANscreen
スクラブ
サービス保証
テスト
tmp
ワークベンチ

手動で開始したバックアップでは、が使用されます `.zip` 次のファイルを含むファイルが作成されます。

- 日次バックアップ `.zip` ファイル（Cognosのレポート定義を含む）
- Aはバックアップを報告します `.zip` ファイル。[My Folders]ディレクトリにあるレポートも含め、Cognosのすべてのレポートが含まれます
- Data Warehouseデータベースのバックアップファイル Cognosでは、手動バックアップ（いつでも実行可能）に加えて、日次バックアップ（毎日という名前のファイルに自動的に生成されます `DailyBackup.zip`）をクリックします。日次バックアップには、製品に同梱されている上位フォルダとパッケージが含まれます。[My Folders]ディレクトリおよび製品の上位フォルダ以外に作成したディレクトリは、Cognosのバックアップには含まれません。

> Insightでのファイルの命名方法が原因です `.zip` ファイル。一部の解凍プログラムでは、ファイルを開くと空であることが表示されます。限り `.zip` ファイルのサイズが0より大きく、末尾がではありません `.bad` 拡張子、 `.zip` ファイルは有効です。7-ZipやWinZip®などの別の解凍プログラムでファイルを開くことができます。

OnCommand Insight データベースをバックアップしています

アップグレード後に問題 が実行された場合に最新のバックアップを保持するため

に、Insightデータベースをバックアップします。バックアップとリストアのフェーズではパフォーマンスデータは収集されないため、バックアップはできるだけアップグレードに近いタイミングで実行する必要があります。

手順

1. ブラウザでInsightを開きます。
2. **>**[トラブルシューティング]*をクリックします。
3. [トラブルシューティング]ページで、*[バックアップ]*をクリックします。

   データベースのバックアップにかかる時間は、使用可能なリソース（アーキテクチャ、CPU、およびメモリ）、データベースのサイズ、環境内の監視対象オブジェクトの数によって異なります。

   バックアップが完了すると、ファイルをダウンロードするかどうかを確認するメッセージが表示されます。

4. バックアップファイルをダウンロードします。

セキュリティ設定をバックアップしています

Insightのコンポーネントでデフォルト以外のセキュリティ設定を使用している場合は、セキュリティ設定をバックアップし、新しいソフトウェアのインストール後にすべてのコンポーネントで設定をリストアする必要があります。セキュリティ設定は、Data Warehouseデータベースのバックアップをリストアする前にリストアする必要があります。

このタスクについて

を使用します `securityadmin` 構成のバックアップを作成し、保存されている構成を復元するツール。詳細については、を検索してください `securityadmin` OnCommand Insight ドキュメントセンター：http://docs.netapp.com/oci-73/index.jsp

Data Warehouseカスタムレポートをバックアップしています

カスタムレポートを作成し、がない場合 `.xml` ソースファイルの場合は、アップグレード前にこれらのレポートをバックアップする必要があります。その後、Data Warehouseサーバ以外のサーバにコピーします。

手順

1. Data Warehouseポータルにログインします `https://fqdn/dwh`。
2. Data Warehouseツールバーで、をクリックします をクリックしてReporting Portalを開き、ログインします。
3. [ファイル]*>[開く]*を選択します。
4. レポートが格納されているフォルダを選択し、レポートを選択して*[開く]*をクリックします。
5. **>**[レポートをクリップボードにコピー]*を選択します。

6. テキストエディタを開き、レポートの内容を貼り付けて、という名前でファイルを保存します `report_name.txt`、ここで `report _name` は、レポートの名前です。
7. Data Warehouseサーバとは別のサーバにレポートを保存します。

ソフトウェアのアップグレードを実行します

必要な準備作業がすべて完了したら、該当するインストールパッケージをダウンロードして各サーバで実行することで、Insightのすべてのコンポーネントを新しいリリースにアップグレードできます。

Insightのアップグレード

必要な準備作業をすべて完了したら、Insight Serverにログインし、インストールパッケージを実行してアップグレードを完了します。アップグレードプロセスでは、既存のソフトウェアがアンインストールされ、新しいソフトウェアがインストールされてから、サーバがリブートされます。

作業を開始する前に

Insightのインストールパッケージは、サーバに配置する必要があります。

手順

1. Windowsのローカル管理者権限を持つアカウントでInsight Serverにログインします。
2. Insightのインストールパッケージを探します (`SANscreenServer-x64-version_number-build_number.msi`）Windowsエクスプローラを使用してダブルクリックします。

   OnCommand InsightSetupウィザードが表示されます。

3. 生成されたエラーが表示されないように、進行状況ウィンドウを画面の中央から離れ、*セットアップ*ウィザードウィンドウから離します。
4. セットアップウィザードの指示に従います。

   デフォルトはすべて選択したままにすることを推奨します。

完了後

アップグレードが成功したか、エラーが発生したかを確認するには、次の場所にあるアップグレードログを確認します。 `<install directory>\SANscreen\wildfly\standalone\log`。

Data Warehouseをアップグレードしています

必要な準備作業がすべて完了したら、Data Warehouseサーバにログインし、インストールパッケージを実行してアップグレードを完了できます。

このタスクについて

Data Warehouse（DWH）ではインラインアップグレードはサポートされません。DWHソフトウェアを新しいバージョンにアップグレードするには、次の手順を実行します。

> DWHをアップグレードすると、_securityadmin_toolバックアップを含むフォルダが削除されます。DWHをアップグレードする前にバックアップをバックアップすることを強く推奨します。参考までに、デフォルトのボルトフォルダは次のとおりです。
>
> - ボルトフォルダ（使用中のボルト）：`%SANSCREEN_HOME%\wildfly\standalone\configuration\vault`
> - バックアップ： `%SANSCREEN_HOME%\backup\vault`
>
> を参照してください "Data Warehouseでセキュリティを管理する" を参照してください。

手順

1. Windowsのローカル管理者権限を持つアカウントでDWHサーバにログインします。
2. DWHポータルインターフェイスを使用して、DWH DBとレポートのバックアップを作成します。
3. サーバがデフォルト以外のセキュリティ設定を使用している場合は、セキュリティ設定をバックアップします。
4. サーバからDWHソフトウェアをアンインストールします。
5. サーバをリブートして、メモリからコンポーネントを削除します。
6. DWHの新しいバージョンをサーバにインストールします。

   インストールには約2時間かかります。デフォルトはすべて選択したままにすることを推奨します。

7. デフォルト以外のセキュリティ設定をDWHサーバにリストアします。
8. DWHデータベースをサーバにリストアします。

完了後

アップグレード後にData Warehouseデータベースをリストアする必要があります。この処理には、アップグレードと同じかそれ以上の時間がかかることがあります。

> OnCommand Insight のアップグレード時に、お客様が別のInsightサーバに切り替えることがよくあります。Insightサーバを変更した場合は、Data Warehouseデータベースをリストアすると、既存のコネクタがサーバの以前のIPアドレスまたはホスト名を参照するようになります。エラーを回避するために、コネクタを削除して新しいコネクタを作成することを推奨します。

Data Warehouseのアップグレード時にカスタムの**Cognos**設定を保持

カスタムのCognos設定（デフォルト以外のSMTP Eメール設定など）は、Data Warehouseのアップグレード時に自動的にバックアップされません。カスタム設定を手動で記録し、アップグレード後にリストアする必要があります。

Data Warehouseをアップグレードする前に、保持するカスタムのCognos設定を含むチェックリストを準備し、システムをアップグレードする前にそのリストを確認します。アップグレードの完了後、値を手動でリス

トアして元の構成の設定に戻すことができます。

セキュリティ設定をバックアップしています

Insight環境でデフォルト以外のセキュリティ設定を使用している場合は、セキュリティ設定をバックアップし、新しいソフトウェアのインストール後にセキュリティ設定をリストアする必要があります。セキュリティ設定は、Data Warehouseデータベースのバックアップをリストアする前にリストアする必要があります。

このタスクについて

を使用します `securityadmin` 構成のバックアップを作成し、保存されている構成を復元するツール。詳細については、を検索してください `securityadmin` OnCommand Insight ドキュメントセンター：http://docs.netapp.com/oci-73/index.jsp

Remote Acquisition Unitサーバをアップグレードします

必要な準備作業がすべて完了したら、Remote Acquisition Unitサーバにログインし、インストールパッケージを実行してアップグレードを完了できます。このタスクは、環境内のすべてのRemote Acquisition Unitサーバで実行する必要があります。

作業を開始する前に

- OnCommand Insight をアップグレードしておく必要があります。
- OnCommand Insight インストールパッケージは、サーバ上に配置する必要があります。

手順

1. Windowsのローカル管理者権限を持つアカウントでRemote Acquisition Unitサーバにログインします。
2. Insightのインストールパッケージを探します (`RAU-x64-version_number-build_number.msi`）Windowsエクスプローラを使用してダブルクリックします。

   OnCommand Insight セットアップウィザードが表示されます。

3. 生成されたエラーが表示されないように、インストールウィザードの進行状況ウィンドウを画面の中央から離れた場所に移動します。
4. セットアップウィザードの指示に従います。

   デフォルトはすべて選択したままにすることを推奨します。

完了後

- アップグレードが成功したか、エラーが発生したかを確認するには、次の場所にあるアップグレードログを確認します。 `<install directory>\SANscreen\bin\log`。
- を使用します `securityadmin` 保存されたセキュリティを復元するためのツール

  設定詳細については、OnCommand Insight でsecurityadminを検索してください

ドキュメントセンター： http://docs.netapp.com/oci-73/index.jsp

- ブラウザのキャッシュと履歴をクリアして、サーバーから最新のデータを受信していることを確認します。

アップグレード後の手順の実行

Insightを最新バージョンにアップグレードしたら、追加の手順を実行する必要があります。

データソースパッチをインストールしています

該当する場合は、最新の機能と拡張機能を活用するために、データソース用の最新のパッチをインストールする必要があります。データソースパッチをアップロードしたら、同じタイプのすべてのデータソースにインストールできます。

作業を開始する前に

テクニカルサポートに連絡してを入手しておく必要があります `.zip` 最新のデータソースパッチを含むファイル。アップグレード前のバージョンとアップグレード後のバージョンを提供します。

手順

1. パッチファイルをInsight Serverに配置します。
2. Insightのツールバーで、*[Admin]*をクリックします。
3. [パッチ]*をクリックします。
4. [Actions]ボタンから、*[Apply patch]*を選択します。
5. ダイアログボックスで、[Browse]*をクリックして、アップロードしたパッチファイルを指定します。
6. 、[概要]、[影響を受けるデータソースタイプ]*を確認します。
7. 選択したパッチが正しい場合は、*パッチの適用*をクリックします。

   同じタイプのすべてのデータソースがこのパッチで更新されます。データソースを追加すると、データ収集が自動的に再開されます。ノードやインターフェイスの追加や削除など、ネットワークトポロジの変更も検出されます。

8. 検出プロセスを手動で強制的に実行するには、**[Data Sources]***をクリックし、データソースの横にある[Poll Again]*をクリックして、データの収集をただちに強制します。

   データソースがすでに取得プロセス中の場合、再ポーリング要求は無視されます。

OnCommand Insight のアップグレード後の証明書の置き換え

アップグレード後にOnCommand Insight Web UIを開くと、証明書に関する警告が表示されます。この警告メッセージは、アップグレード後に有効な自己署名証明書を使用できない場合に表示されます。警告メッセージが表示されないようにするには、有効な自己署名証明書をインストールして元の証明書を置き換えます。

作業を開始する前に

システムが暗号化の最小ビットレベル（1024ビット）を満たしている必要があります。

このタスクについて

証明書の警告は、システムのユーザビリティには影響しません。メッセージプロンプトでリスクを把握したことを示すと、Insightの使用に進みます。

手順

1. 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"`

   パスワードの入力を求められたら、と入力します `changeit`。

   キーストアには少なくとも1つの証明書が必要です。 `ssl certificate`。

2. を削除します `ssl certificate`： `keytool -delete -alias ssl certificate -keystore c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore`
3. 新しいキーを生成します。 `keytool -genkey -alias OCI.hostname.com -keyalg RSA -keysize 2048 -keystore "c:\ProgramFiles\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。
4. 証明書要求ファイルを生成します。 `keytool -certreq -alias localhost -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。

5. を送信します `c:\localhost.csr` 承認のためにCertification Authority（CA；認証局）にファイルを送信します。

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。

6. 承認済み証明書をインポートします。 `keytool -importcert -alias localhost -file c:\localhost2.DER -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、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`

7. SANscreen サーバサービスを再起動します。

結果

Webブラウザで証明書の警告が報告されなくなりました。

Cognosメモリを拡張しています

Data Warehouseデータベースをリストアする前に、レポート生成時間を短縮するために、CognosのJava割り当てを768MBから2、048MBに増やす必要があります。

手順

1. Data Warehouseサーバで、管理者としてコマンドプロンプトウィンドウを開きます。
2. に移動します `disk drive:\install directory\SANscreen\cognos\c10_64\bin64` ディレクトリ。
3. 次のコマンドを入力します。 `cogconfigw`

   [IBM Cognos Configuration]ウィンドウが表示されます。

   > IBM Cognos Configurationショートカットアプリケーションはを指しています `disk drive:\Program Files\SANscreen\cognos\c10_64\bin64\cognosconfigw.bat`。Insightがプログラムファイル（スペースなし）ではなくProgram Files（スペースなし）ディレクトリ（デフォルト）にインストールされている場合は、を実行します `.bat` ファイルが機能しません。この場合は、アプリケーションのショートカットを右クリックして変更します `cognosconfigw.bat` 終了： `cognosconfig.exe` ショートカットを修正します。

4. 左側のナビゲーションペインで、**[環境]**、**[IBM Cognos services]***の順に展開し、[IBM Cognos]*をクリックします。
5. [Maximum memory for Tomcat in MB]*を選択し、768 MBを2048 MBに変更します。
6. IBM Cognos Configurationツールバーで、をクリックします （保存）。

   Cognosが実行しているタスクを通知する情報メッセージが表示されます。

7. [* 閉じる *] をクリックします。
8. IBM Cognos Configurationツールバーで、をクリックします （停止）。

9. IBM Cognos Configurationツールバーで、をクリックします ▶（開始）。

Data Warehouseデータベースをリストアしています

Data Warehouseデータベースをバックアップすると、Data Warehouseでが作成されます `.zip` 同じデータベースをあとでリストアするために使用できるファイル。

このタスクについて

Data Warehouseデータベースをリストアするときに、ユーザアカウント情報もバックアップからリストアできます。ユーザ管理テーブルは、Data WarehouseのみのインストールでData Warehouseレポートエンジンで使用されます。

手順

1. Data Warehouseポータルにログインします `https://fqdn/dwh`。
2. 左側のナビゲーションペインで、*[バックアップ/リストア]*をクリックします。
3. セクションで、[参照]*をクリックし、を探します `.zip` Data Warehouseのバックアップを保持するファイル。
4. 次のオプションは両方とも選択したままにすることを推奨します。
   - データベースのリストア

     Data Warehouseの設定、データマート、接続、およびユーザアカウント情報が含まれます。

   - リストア・レポート

     カスタムレポート、事前定義済みレポート、事前定義済みレポートへの変更、およびReporting Connectionで行ったレポート設定が含まれます。

5. [* リストア] をクリックします。

   リストアステータスから移動しないでください。このコマンドを実行すると、リストアステータスは表示されなくなり、リストア処理の完了を通知するメッセージは表示されません。

6. アップグレードプロセスを確認するには、を表示します `dwh_upgrade.log` ファイル。次の場所にあります。 `<install directory>\SANscreen\wildfly\standalone\log`。

   リストアプロセスが完了すると、*[リストア]*ボタンのすぐ下にメッセージが表示されます。リストアプロセスが正常に完了すると、成功したことを示すメッセージが表示されます。リストアプロセスが失敗した場合は、原因 に発生した特定の例外を示すメッセージが表示されます。この場合は、テクニカルサポートに連絡してを提供してください `dwh_upgrade.log` ファイル。例外が発生してリストア処理が失敗すると、元のデータベースは自動的にリセットされます。

   > 「Failed upgrading Cognos content store」というメッセージが表示されてリストア処理が失敗した場合は、レポートを含めずにData Warehouseデータベースをリストアし（データベースのみ）、XMLレポートのバックアップを使用してレポートをインポートします。

Data Warehouseカスタムレポートをリストアしています

必要に応じて、アップグレード前にバックアップしたカスタムレポートを手動でリストアできます。ただし、この処理が必要になるのは、のレポートが失われて破損した場合のみです。

手順

1. テキストエディタでレポートを開き、内容を選択してコピーします。
2. Reportingポータルにログインします `https://fqdn/reporting`。
3. Data Warehouseツールバーで、をクリックします をクリックしてInsight Reportingポータルを開きます。
4. [起動]メニューから、*[Report Studio]*を選択します。
5. 任意のパッケージを選択します。

   Report Studioが表示されます。

6. [新規作成]*をクリックします。
7. [リスト]*を選択します。
8. [ツール]メニューから*[クリップボードからレポートを開く]*を選択します。

   [クリップボードからレポートを開く]*ダイアログボックスが表示されます。

9. [ファイル]メニューから*[名前を付けて保存]*を選択し、レポートを[カスタムレポート]フォルダに保存します。
10. レポートを開き、インポートされたことを確認します。

    レポートごとにこのタスクを繰り返します。

> レポートをロードすると、"`Expression parsing error`"が表示されることがあります。これは、クエリーに存在しない少なくとも1つのオブジェクトへの参照が含まれていることを意味します。つまり、[ソース]ウィンドウでレポートを検証するパッケージが選択されていないことを意味します。この場合は、[Source]ウィンドウでデータマートディメンションを右クリックし、[Report Package]を選択します。 次に、レポートに関連付けられているパッケージ（インベントリレポートの場合はインベントリパッケージ、パフォーマンスレポートの場合はいずれかのパフォーマンスパッケージ）を選択して、Report Studioで検証して保存できるようにします。

Data Warehouseに履歴データがあることを確認する

カスタムレポートをリストアしたら、カスタムレポートを表示して、Data Warehouseが履歴データを収集していることを確認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://fqdn/dwh`。

2. Data Warehouseツールバーで、をクリックします をクリックしてInsight Reportingポータルを開き、ログインします。
3. カスタムレポートが格納されているフォルダ（[Custom Reports]など）を開きます。
4. をクリックします ▶ をクリックして、このレポートの出力形式オプションを開きます。
5. 必要なオプションを選択し、*[実行]*をクリックしてストレージ、コンピューティング、スイッチの履歴データが入力されていることを確認します。

パフォーマンスアーカイブをリストアしています

パフォーマンスアーカイブを実行するシステムの場合、アップグレードプロセスでリストアされるのは7日分のアーカイブデータのみです。アップグレードの完了後に、残りのアーカイブデータをリストアできます。

このタスクについて

パフォーマンスアーカイブをリストアするには、次の手順を実行します。

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。

コネクタをテストします

アップグレードの完了後、コネクタをテストして、OnCommand Insight データウェアハウスからOnCommand Insight サーバへの接続が確立されていることを確認します。

手順

1. Data Warehouseポータルにログインします `https://fqdn/dwh`。
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。
3. 最初のコネクタを選択します。

   [Edit Connector]ページが表示されます。

4. [* テスト *] をクリックします。
5. テストに成功した場合は、**[**閉じる**]***をクリックします。失敗した場合は、**Insight Server**の名前を[名前]フィールドに、**IP**アドレスを[ホスト]フィールドに入力し、[テスト]*をクリックします。
6. Data WarehouseとInsight Serverの接続が確立されたら、*[保存]*をクリックします。

   接続に失敗した場合は、接続設定をチェックし、Insight Serverに問題がないことを確認してください。

7. [* テスト *] をクリックします。

   Data Warehouseで接続がテストされます。

抽出、変換、読み込みのスケジュールを確認します

アップグレードが完了したら、ETL（抽出、変換、読み込み）プロセスがOnCommand Insight データベースからデータを取得して変換し、データマートに保存していることを確認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://fqdn/dwh`。
2. 左側のナビゲーションペインで、*[スケジュール]*をクリックします。
3. [スケジュールの編集]*をクリックします。
4. [タイプ]リストから*または[毎週]*を選択します。

   ETLを1日1回実行するようにスケジュールを設定することを推奨します。

5. 選択した時刻がジョブを実行する時刻であることを確認します。

   これにより、ビルドジョブが自動的に実行されます。

6. [保存（ Save ）] をクリックします。

ディスクモデルを更新しています

アップグレード後はディスクモデルを更新する必要がありますが、何らかの理由でInsightで新しいディスクモデルが検出されなかった場合は、ディスクモデルを手動で更新できます。

作業を開始する前に

テクニカルサポートからを入手しておく必要があります `.zip` 最新のデータソースパッチを含むファイル。

手順

1. SANscreen Acqサービスを停止します。
2. 次のディレクトリに移動します。 `<install directory>\SANscreen\wildfly\standalone\deployments\datasources.war`。
3. 現在のを移動します `diskmodels.jar` ファイルを別の場所に保存します。
4. 新しいをコピーします `diskmodels.jar` ファイルをに挿入します `datasources.war` ディレクトリ。
5. SANscreen Acqサービスを開始します。

ビジネスインテリジェンスツールが実行されていることを確認する

必要に応じて、アップグレード後にビジネスインテリジェンスツールが実行され、データを取得していることを確認する必要があります。

BMC AtriumやServiceNowなどのビジネスインテリジェンスツールが動作しており、データを取得できることを確認します。これには、BMC ConnectorやRESTを利用したソリューションが含まれます。

アップグレードのトラブルシューティング

OnCommand Insight のアップグレード後に問題が発生した場合は、いくつかの考えられる問題に関連するトラブルシューティング情報を確認すると役立つことがあります。

Windowsの**[**スタート**]**メニューから**Cognos**を起動できない

以前の空間の存在 `\SANscreen\cognos` パス名には問題 が含まれています。詳細については、ネットアップのCustomer Success Communityで次の情報を参照してください。 https://forums.netapp.com/thread/62721。

「有効な**win32**アプリケーションではありません」というエラーメッセージが表示されます

これはMicrosoft Windowsを搭載した問題 です。この問題 を解決するには、レジストリ内のイメージパスを引用符で囲む必要があります。詳細については、次のドキュメントを参照してください。 https://support.microsoft.com/en-us/kb/812486/en-us。

注釈は表示されません

Data WarehouseのETLジョブでInsightインスタンスのアノテーションを照会するときに、エラーとして空の応答（0の結果）が返されることがあります。このエラーにより、Data Warehouseで特定のオブジェクトのアノテーションが「present」と「not present」の間で前後に移動します。詳細については、次を参照してください。 https://forums.netapp.com/docs/DOC-44167

レポートに表示される値の違い

7.0より前のバージョンでは、レポートは整数ベースでした。これらは10進数ベースになっているため、アップグレード後に値の表示方法が増減することがあります。

レポートにデータが表示されない

7.0.1では、いくつかのモデル名が変更されました（たとえば、SymmetrixがSymmetrix VMAXに変更されました）。そのため、レポートに"`symmetrix`"のフィルタが含まれている場合、レポートを実行してもデータは表示されません。レポートを変更するには、Report StudioのQuery Explorerでレポートを開き、モデル名を検索して新しいモデル名に置き換え、レポートを保存する必要があります。

ソフトウェアをアンインストールしています

Data WarehouseおよびRemote Acquisitionソフトウェアの新しいバージョンをインストールするには、古いバージョンをアンインストールする必要があります。この処理は、これらのコンポーネントをアップグレードする前に実行する必要があります。Insight Serverのソフトウェアは、インプレースアップグレード時にアンインストールされま

す。

OnCommand Insight サーバをアンインストールしています

必要に応じて、OnCommand Insight サーバをアンインストールできます。

作業を開始する前に

ベストプラクティス：Insightをアンインストールする前に、OnCommand Insight データベースをバックアップしてください。

手順

1. 管理者権限があるアカウントでOnCommand Insight サーバにログインします。
2. サーバ上のInsightウィンドウがすべて閉じていることを確認します。
3. コントロールパネルから*プログラムのアンインストール*機能を開き、削除するOnCommand Insight アプリケーションを選択します。
4. [アンインストール]*をクリックし、画面の指示に従います。

Data Warehouseソフトウェアをアンインストールしています

アップグレードする前に、Data Warehouseソフトウェアをアンインストールする必要があります。

作業を開始する前に

保持するレポートに変更を加えた場合は、Data Warehouseをアンインストールする前にバックアップを作成しておくことが重要です。Data Warehouseを完全にアンインストールすると、以前に収集したデータがすべて削除され、新しく作成または編集したレポートも含めてすべてのレポートが削除されます。

手順

1. Data Warehouseサーバにログインします。
2. サーバ上のInsightウィンドウがすべて閉じていることを確認します。
3. コントロールパネルを使用してアンインストールするには：
   a. コントロールパネルから*プログラムのアンインストール*を開き、削除するOnCommand Insight アプリケーションを選択します。[アンインストール]*をクリックし、画面の指示に従います。
   b. 削除するIBM DB2アプリケーションを選択します。[アンインストール]*をクリックし、画面の指示に従います。
   c. DB2インストールフォルダ（例：*C:\Program Files\IBM\DB2*）を削除して、DB2データベースを完全に削除します。
4. 提供されているスクリプトを使用してをアンインストールするには
   a. _uninstall_oci_dwh_uninstall_フォルダに移動<download location> し、_uninstall_oci_dwh.bat_script を実行します。
5. サーバをリブートします。

Remote Acquisition Unitソフトウェアをアンインストールしています

Remote Acquisition Unitソフトウェアを新しいバージョンにアップグレードする前に、既存のバージョンをアンインストールする必要があります。このタスクは、環境内のすべてのRemote Acquisition Unitサーバで実行する必要があります。

手順

1. Remote Acquisition Unitサーバにログインします。
2. サーバ上のすべてのOnCommand Insight ウィンドウが閉じていることを確認します。
3. コントロールパネルから*プログラムのアンインストール*機能を開き、削除するOnCommand Insight Remote Acquisition Unitプログラムを選択します。
4. [アンインストール]*をクリックし、画面の指示に従います。

構成と管理

Insightをセットアップしています

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

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

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

Web UIへのアクセス

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

手順

1. 次のいずれかを実行します。

    - InsightサーバでInsightを開きます。

      ```
      https://fqdn
      ```

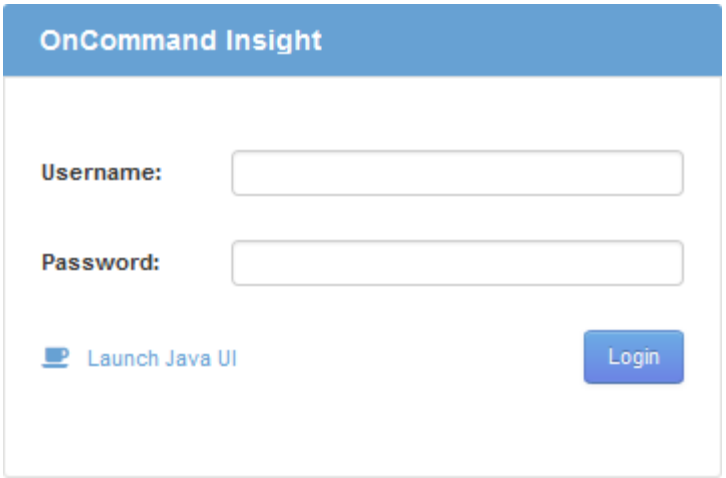
    - その他の場所からInsightを開きます。

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

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

    OnCommand Insight ダイアログボックスが表示されま

す。



2. ユーザー名とパスワードを入力し、* Login *をクリックします。

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

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

Insightのライセンスをインストールします

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

このタスクについて

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

手順

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

なっている必要があります。

完了後

ライセンスをインストールしたら、次の設定作業を実行できます。

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

OnCommand Insight ライセンス

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

- * 発見 *

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

- 保証

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

- 実行

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

- 計画

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

- * Host Utilization Pack *

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

- レポートオーサリング

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

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

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

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

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

- * 発見 *

  インベントリの取得と管理（基盤）

  変更を監視し、インベントリポリシーを管理します

- 保証

  SANパスのポリシーや違反を表示および管理します

  脆弱性を確認および管理します

  タスクと移行を表示および管理します

- 計画

  リクエストを表示および管理します

  保留中のタスクを表示および管理します

  リザベーション違反を表示および管理します

  ポートバランス違反を表示および管理します

- 実行

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

  パフォーマンスポリシーや違反を表示および管理します

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

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

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

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

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

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

ユーザアカウントの設定と管理

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

ウントを使用してください。

作業を開始する前に

次の作業を完了しておきます。

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

> 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。

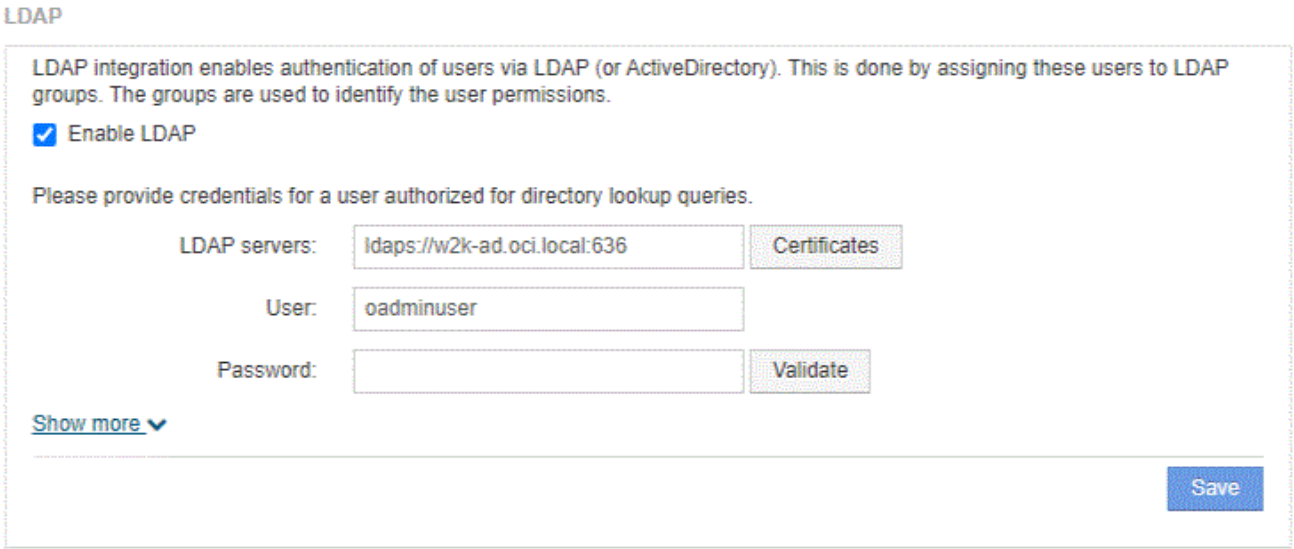
このタスクについて

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

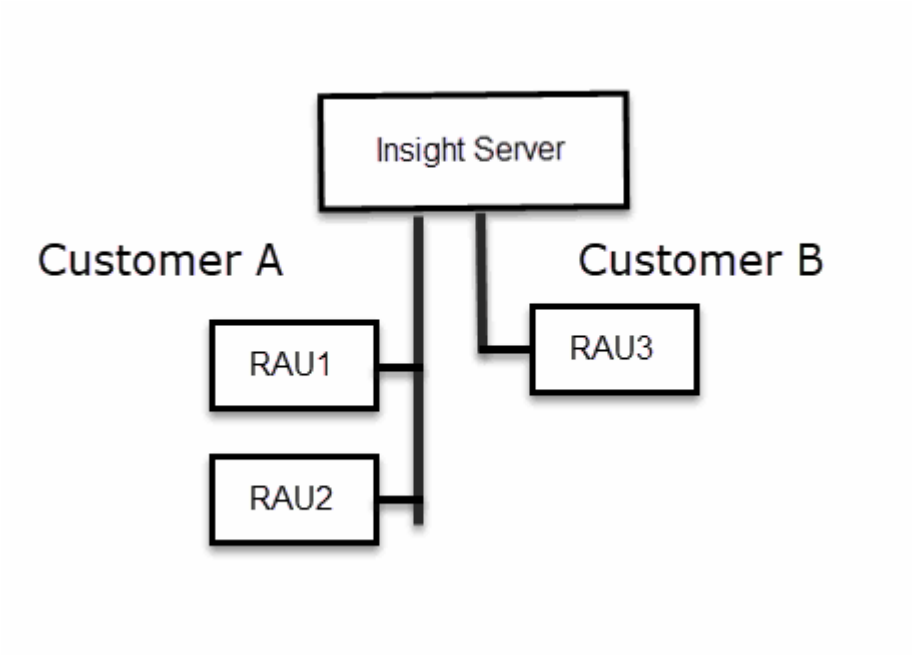
Insightシステムにデフォルト以外のセキュリティ設定が含まれている場合（パスワードのキーを変更または変更した場合）は、セキュリティ設定をバックアップする必要があります。新しいソフトウェアをインストールするか、ソフトウェアをアップグレードする場合によっては、システムをデフォルトのセキュリティ設定に戻します。システムがデフォルトの設定に戻ったら、システムを正常に動作させるために、デフォルト以外の設

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。

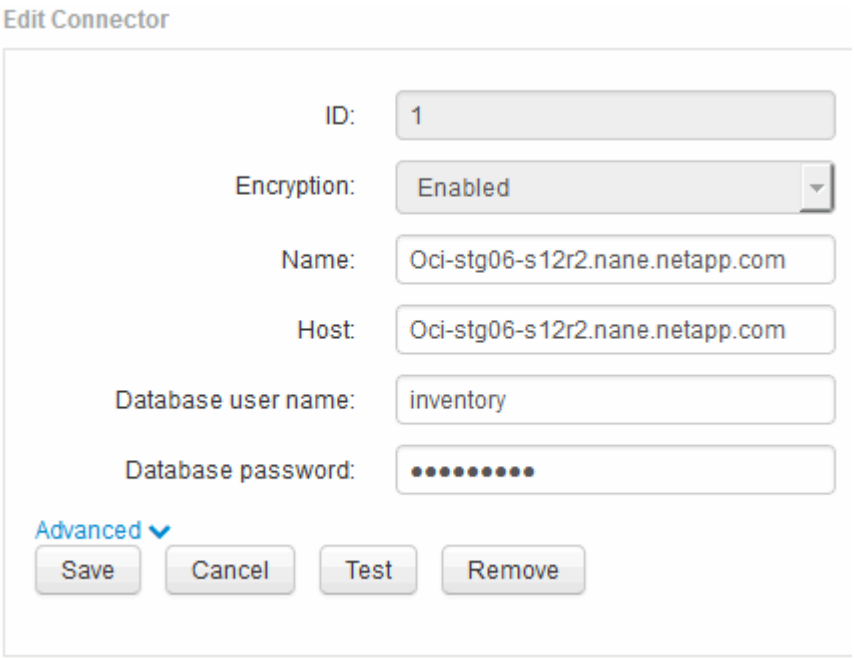
作業を開始する前に

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

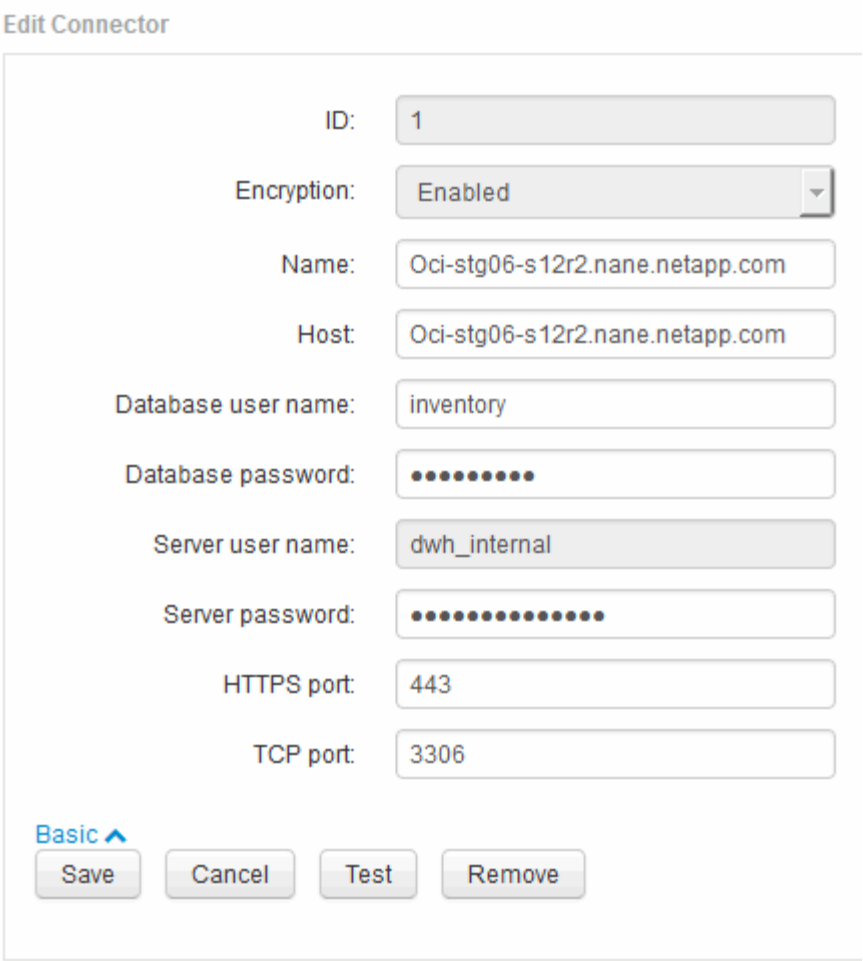
1. Data Warehouseポータルにログインします https://hostname/dwhhostnameは、OnCommand Insight Data Warehouseがインストールされているシステムの名前です。
2. 左側のナビゲーションペインで、*[コネクタ]*をクリックします。

   [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。

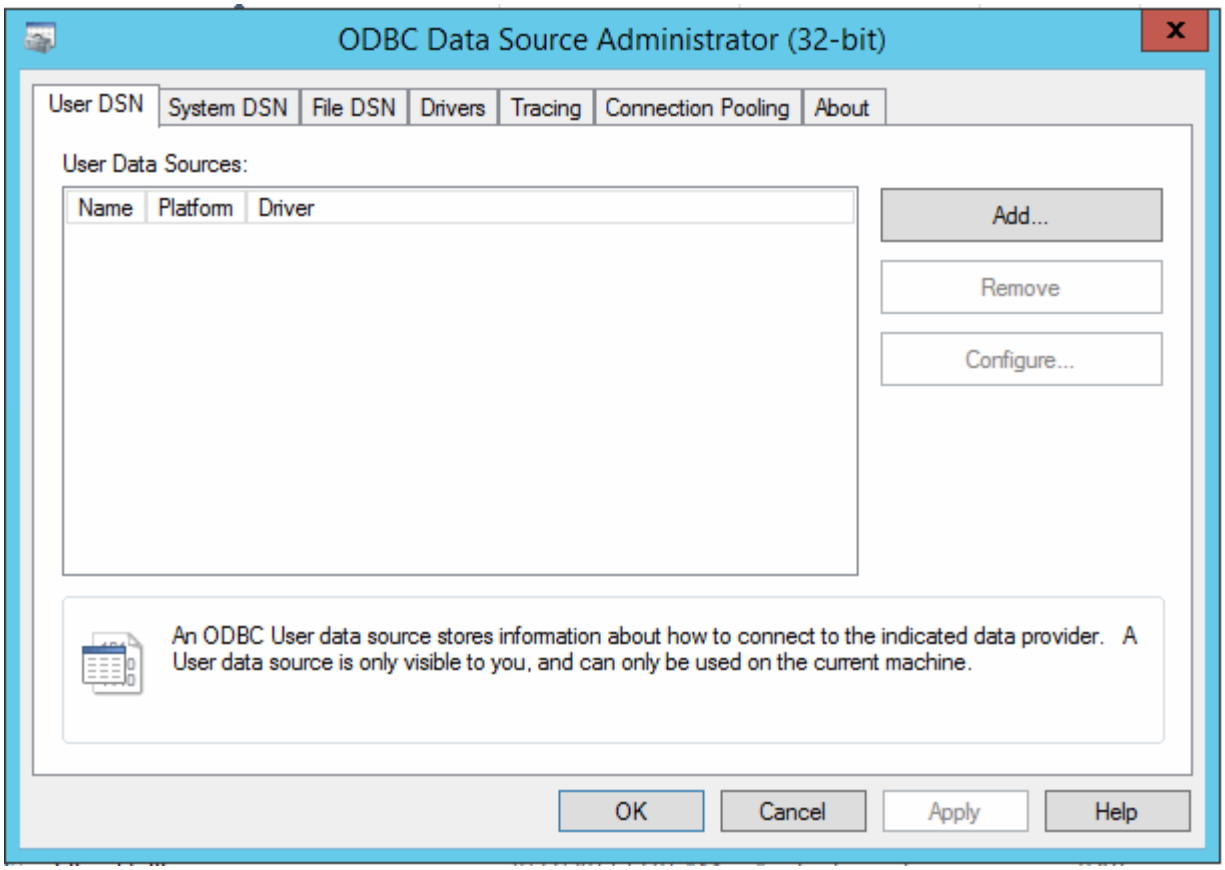
作業を開始する前に

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

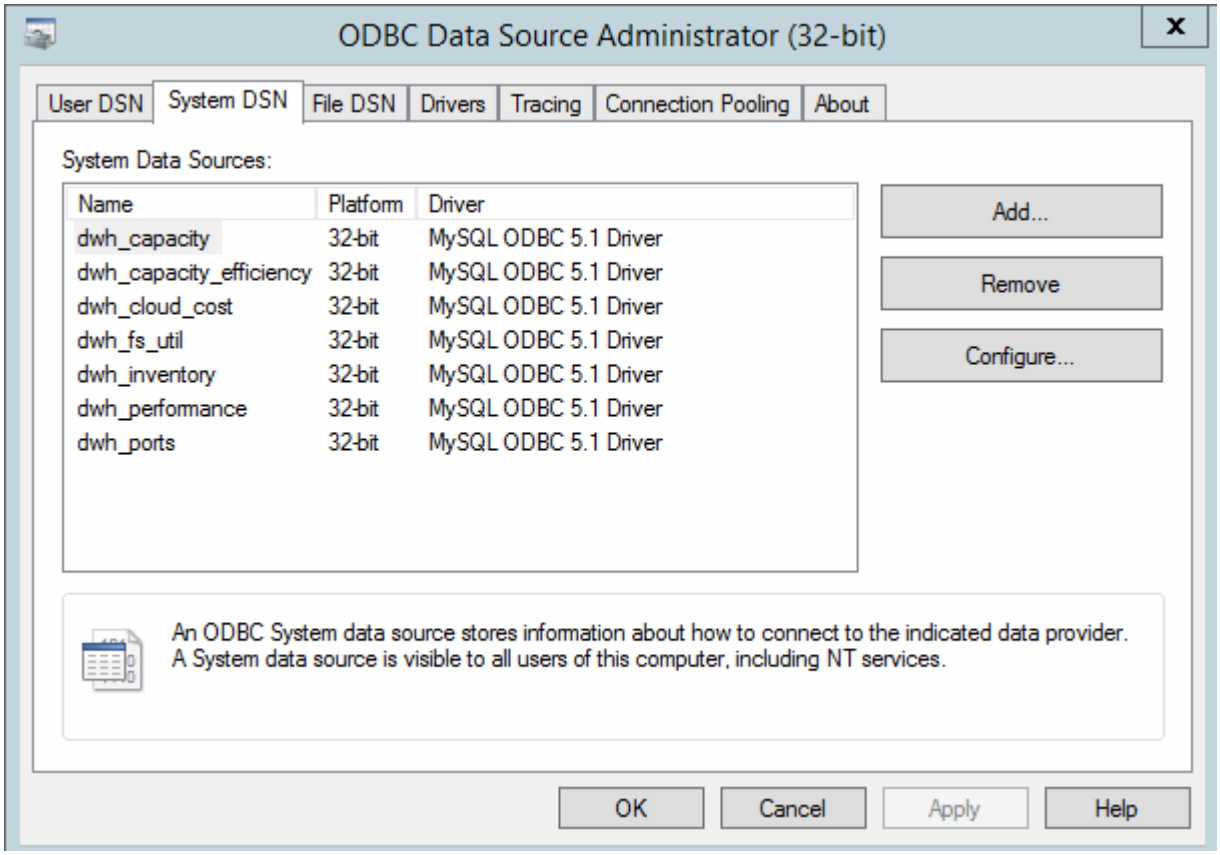
1. Data Warehouseをホストしているサーバへのリモートログインを実行します。
2. ODBC Administrationツールにアクセスします `C:\Windows\SysWOW64\odbcad32.exe`

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



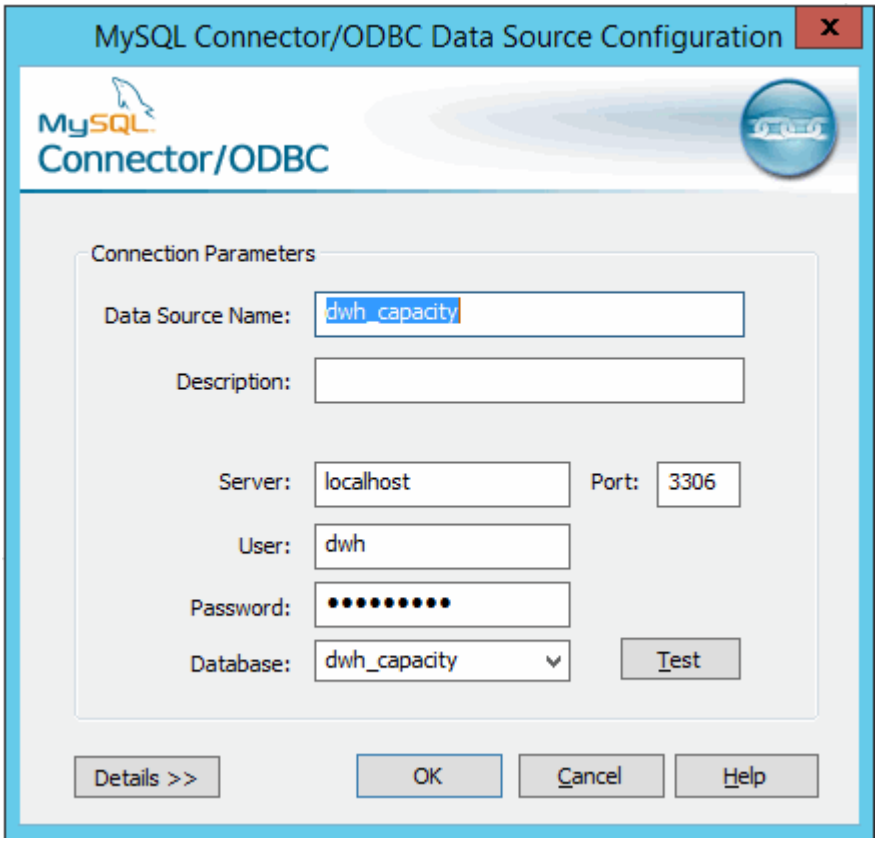
3. [システムDSN]*をクリックします

   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. 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エ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 More 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。

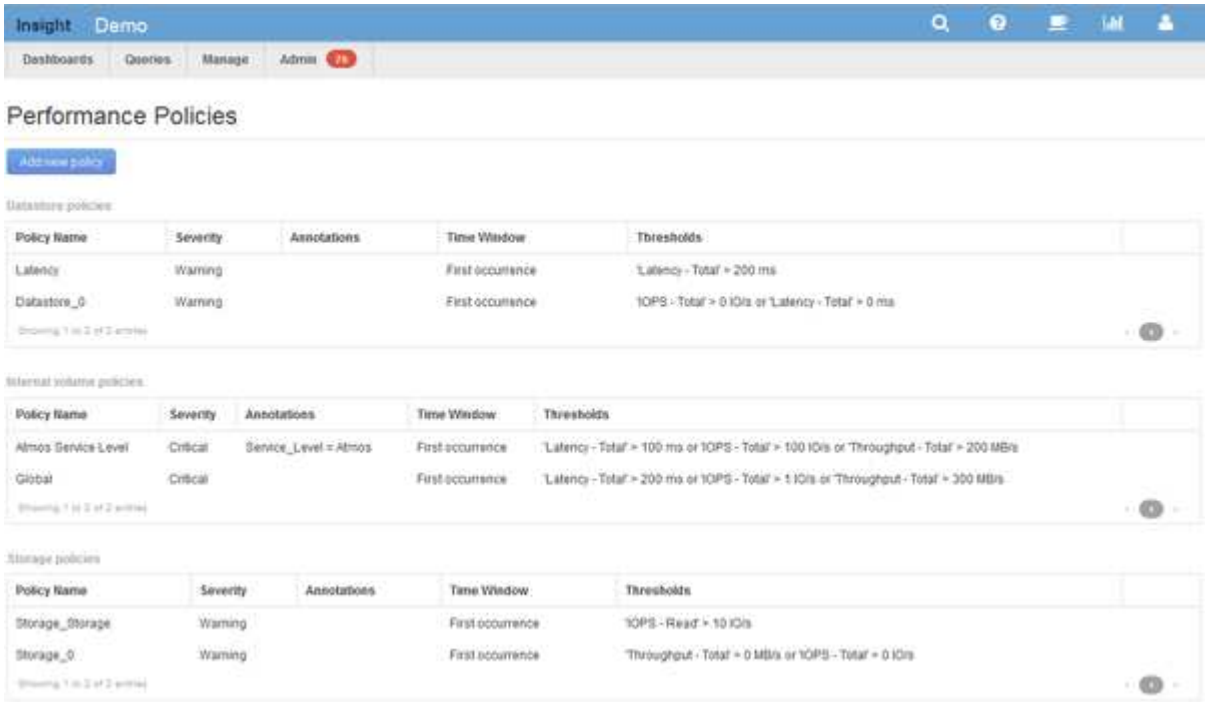
パフォーマンスポリシーの作成

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。
>
> [+]

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。

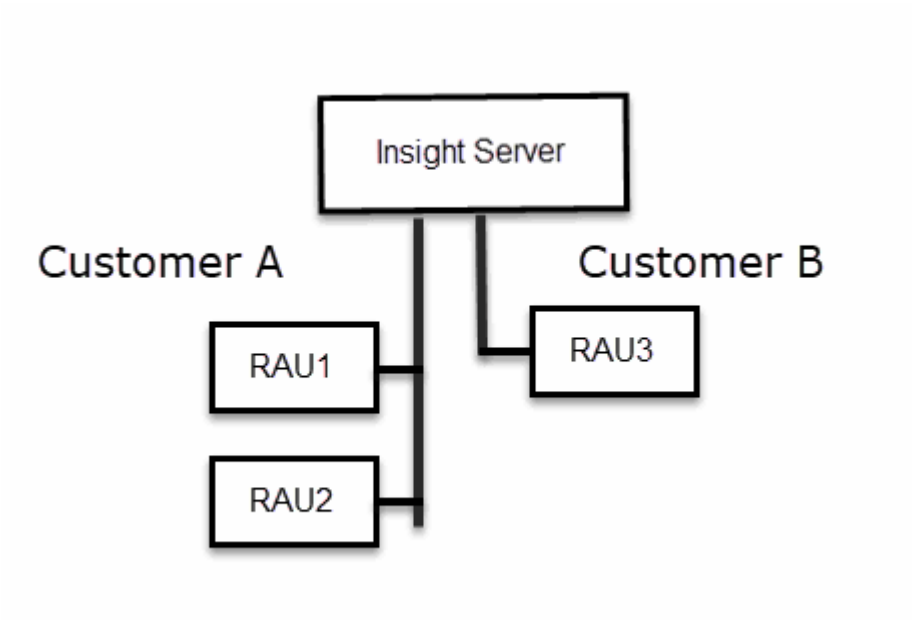
アップグレードとインストールに関する考慮事項

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。

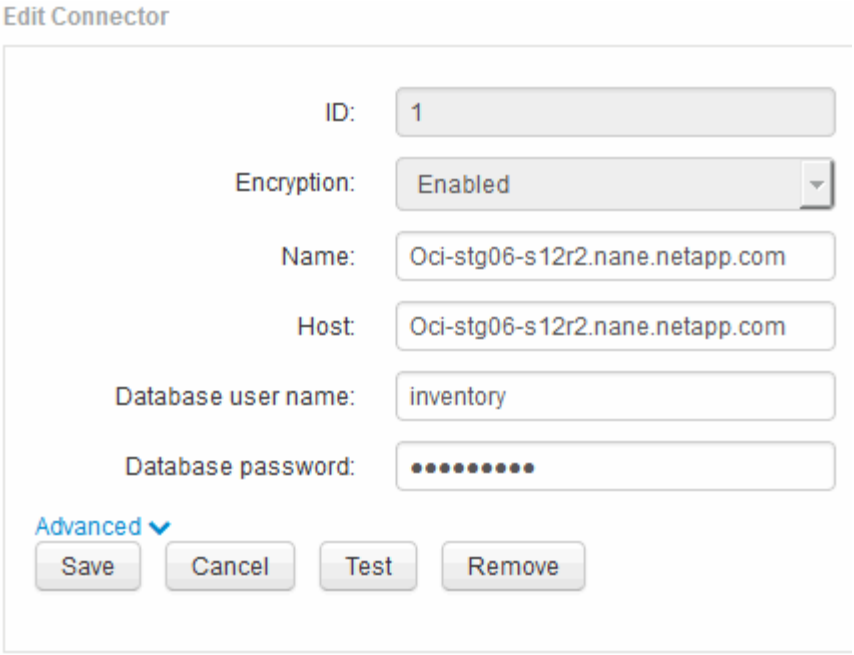
作業を開始する前に

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

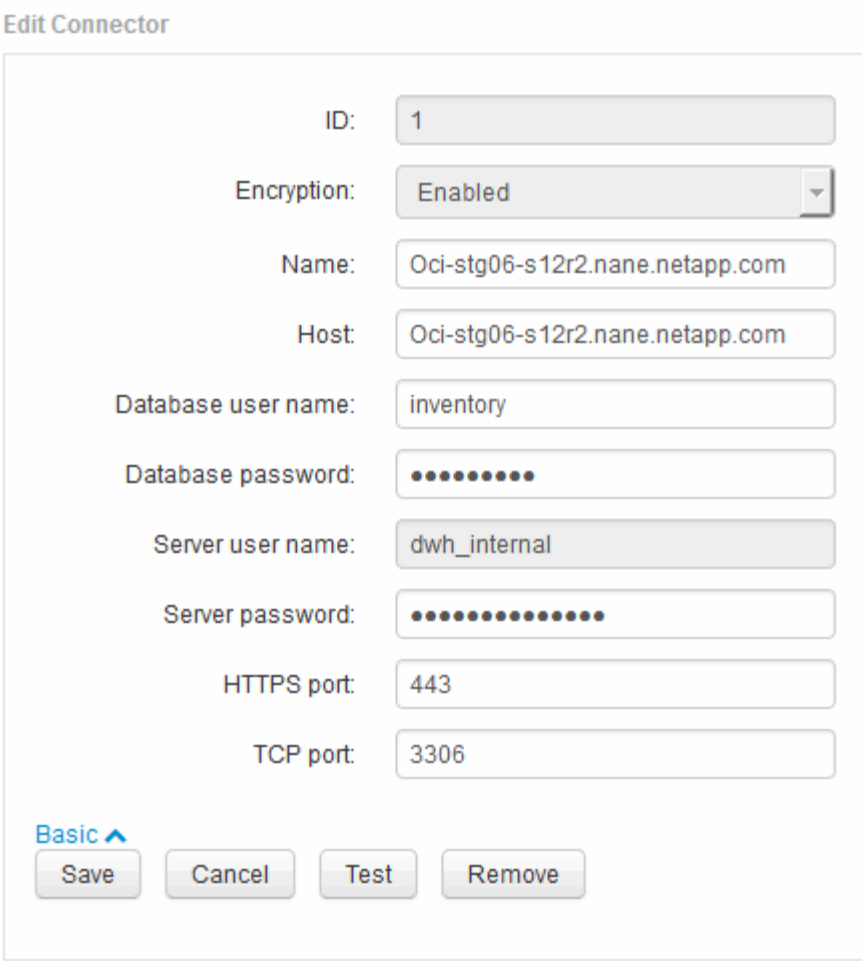
1. Data Warehouseポータルにログインします https://hostname/dwhhostnameは、OnCommand Insight Data Warehouseがインストールされているシステムの名前です。
2. 左側のナビゲーションペインで、*[コネクタ]*をクリックします。

   [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。

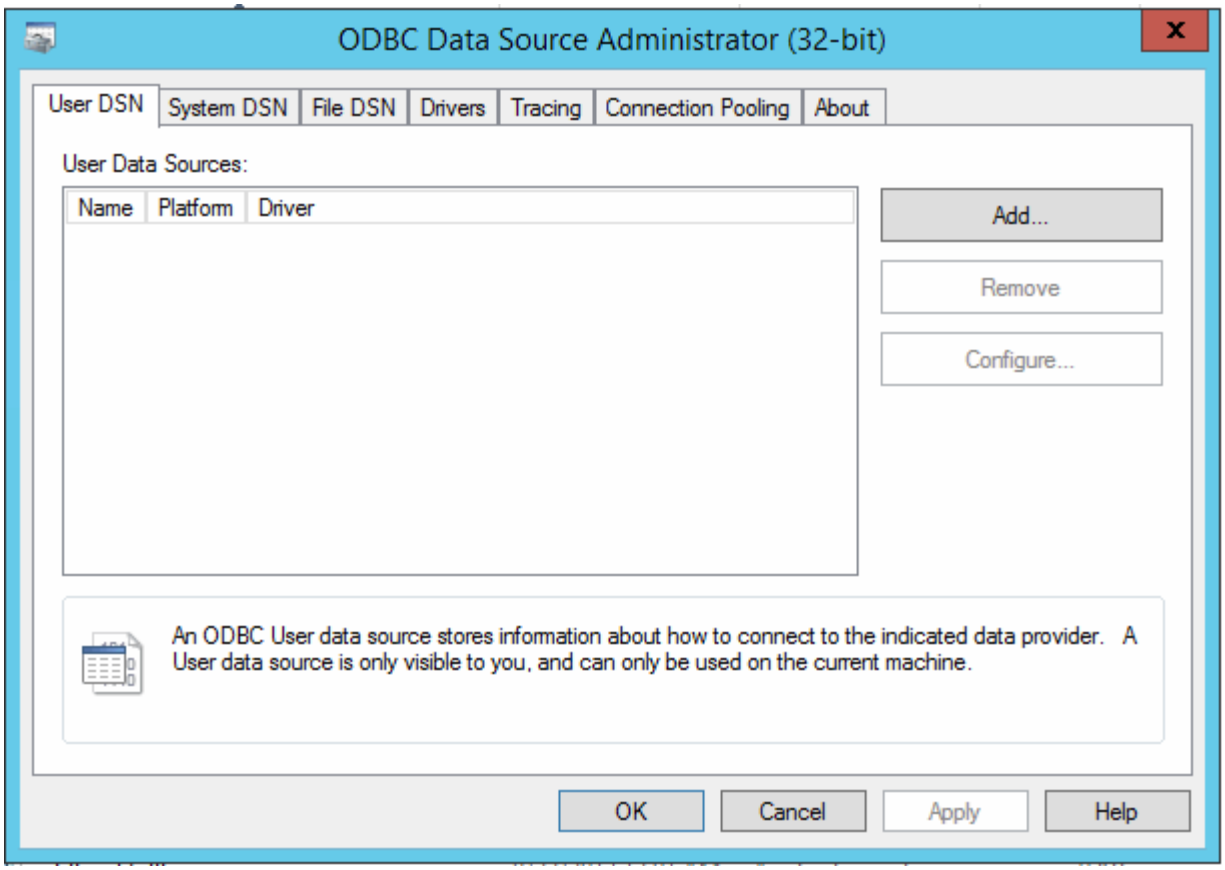
作業を開始する前に

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

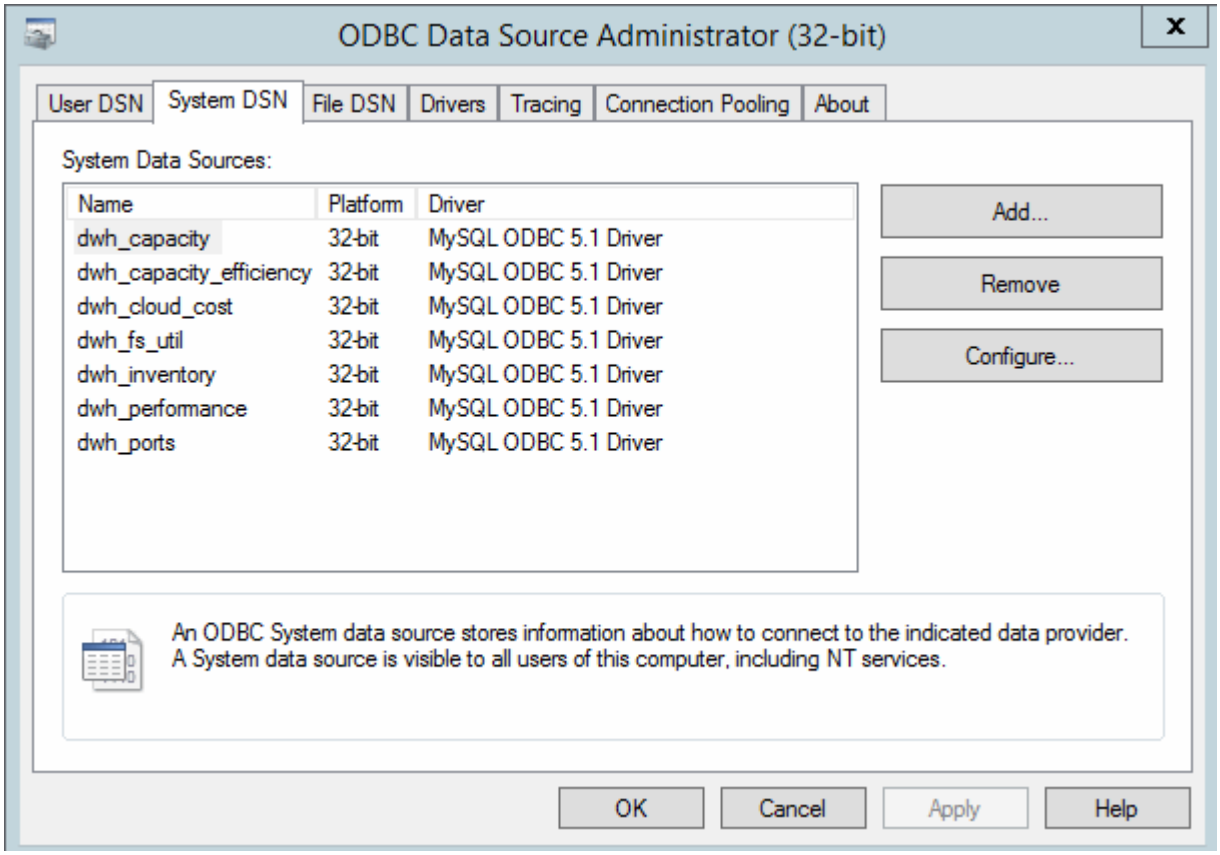
1. Data Warehouseをホストしているサーバへのリモートログインを実行します。
2. ODBC Administrationツールにアクセスします `C:\Windows\SysWOW64\odbcad32.exe`

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



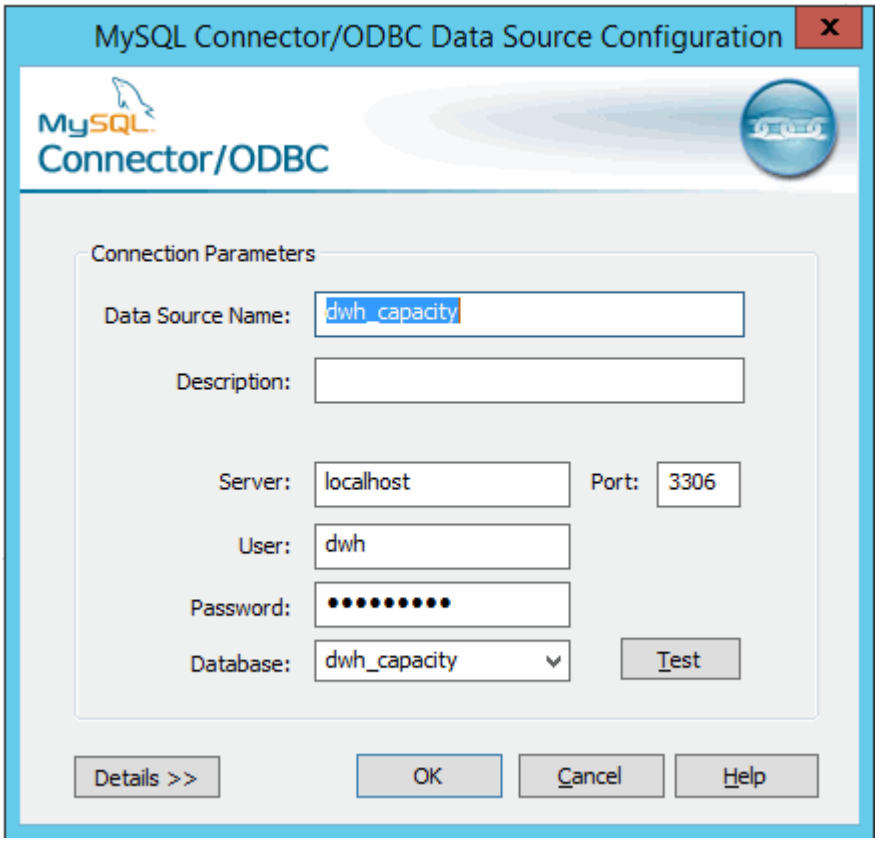
3. [システムDSN]*をクリックします

   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OnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
- "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

スマートカードおよび証明書によるログイン用にホストを設定しています

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

作業を開始する前に

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

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

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

手順

1. を使用します `regedit` でレジストリ値を変更するユーティリティ `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`：
   a. jvm_optionを変更します `DclientAuth=false` 終了： `DclientAuth=true`.

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

    すべての中間証明書について、この手順を繰り返します。

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

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

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

作業を開始する前に

> CACおよび証明書に関する最新の手順については、次の技術情報アーティクル（サポートへのログインが必要）を参照してください。
>
> - "OnCommand Insight のCommon Access Card（CAC;共通アクセスカード）認証を設定する方法"
> - "OnCommand Insight Data WarehouseのCommon Access Card（CAC；共通アクセスカード）認証の設定方法"
> - "認証局（CA）の署名付き証明書を作成し、OnComand InsightおよびOnCommand Insight Data Warehouse 7.3.xにインポートする方法"
> - "Windowsホストにインストールされている OnCommand Insight 7.3.X内で自己署名証明書を作成する方法"
> - "Cognos認証局（CA）署名証明書をOnCommand DataWarehouse 7.3.3以降にインポートする方法"

このタスクについて

一般的なクライアント設定要件は次のとおりです。

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

Linuxサーバでの**CAC**の有効化

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

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。

ビジネスエンティティ階層

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

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

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

企業階層の設計では、すべてのレベルを使用する必要はありません。

ビジネスエンティティ階層の設計

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

手順

1. ビジネスエンティティ階層の各レベルを調べて、そのレベルを会社のビジネスエンティティ階層に含める必要があるかどうかを判断します。
   - *テナント*レベルは、会社がISPで、顧客のリソース使用状況を追跡する場合に必要です。
   - *さまざまな製品ラインのデータを追跡する必要がある場合は、基幹業務（LOB）*が階層に必要です。
   - *部門ごとにデータを追跡する必要がある場合は、ビジネスユニット*が必要です。この階層レベルは、1つの部門が使用するリソースと、他の部門が使用しないリソースを分離するのに役立ちます。
   - *プロジェクト*レベルは、部門内の特殊な作業に使用できます。このデータは、企業や部門内の他のプロジェクトと比較して、個別のプロジェクトのテクノロジニーズを特定、定義、および監視するのに役立ちます。

2. 各ビジネスエンティティとそのエンティティ内のすべてのレベルの名前を示すグラフを作成します。
3. 階層内の名前をチェックして、OnCommand Insight のビューやレポートでわかりやすい名前になっていることを確認します。
4. 各ビジネスエンティティに関連付けられているアプリケーションをすべて特定します。

ビジネスエンティティを作成しています

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

このタスクについて

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

手順

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

   [Business Entities]ページが表示されます。

3. をクリックします 

新しいエンティティの構築を開始します。

   [ビジネスエンティティの追加]*ダイアログボックスが表示されます。

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

アセットへのビジネスエンティティの割り当て

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

作業を開始する前に

ビジネスエンティティを作成しておく必要があります。

このタスクについて

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

手順

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

   使用可能なビジネスエンティティのリストが表示されます。

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

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

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

複数のアセットに対するビジネスエンティティの割り当てまたは削除

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

作業を開始する前に

目的のアセットに追加するビジネスエンティティを作成しておく必要があります。

手順

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

   [アクション]*ボタンが表示されます。

4. 選択したアセットにビジネスエンティティを追加するには、をクリックします 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 More をクリックし、次のいずれかを実行します。

   - と入力して特定の条件を検索し、選択します。
   - リストを下にスクロールし、条件を選択します。
   - IOPS -読み取り（IO/秒）などのパフォーマンス指標を選択した場合は、値の範囲を入力します。Insightのデフォルトのアノテーションはで示されます ;重複する名前を持つ注釈を持つことができます。

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

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

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

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

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

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

   - 関連情報 *

"ユーザーデータのインポートとエクスポート"

クエリを表示する

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

手順

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

クエリ結果を **.csv** ファイルにエクスポートしています

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

手順

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

   [クエリ] ページが表示されます。

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

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

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

     [+]

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

     [+]

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

     [+]

クエリの変更

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

手順

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

   [クエリ] ページが表示されます。

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

クエリの削除

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

手順

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

   [クエリ] ページが表示されます。

3. 削除するクエリにカーソルを合わせ、をクリックします 🗑 。

   クエリを削除するかどうかを確認する確認メッセージが表示されます。

4. [OK] をクリックします。

アセットに対する複数のアプリケーションの割り当てと削除

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

作業を開始する前に

編集するすべてのアセットを検索するクエリを作成しておく必要があります。

手順

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

   [クエリ] ページが表示されます。

2. アセットを検索するクエリの名前をクリックします。

   クエリに関連付けられているアセットのリストが表示されます。

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

   [アクション]*ボタンが表示されます。

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

   a. [アプリケーション]*をクリックし、1つ以上のアプリケーションを選択します。

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

   b. [保存（ Save ）] をクリックします。

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

   a. 削除する 1 つ以上のアプリケーションを選択します。

   b. [削除（ Delete ）] をクリックします。

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

アセットの複数のアノテーションの編集または削除

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

作業を開始する前に

編集するすべてのアセットを検索するクエリを作成しておく必要があります。

手順

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

   [クエリ] ページが表示されます。

2. アセットを検索するクエリの名前をクリックします。

クエリに関連付けられているアセットのリストが表示されます。

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

   [アクション]*ボタンが表示されます。

4. アセットにアノテーションを追加したり、アセットに割り当てられているアノテーションの値を編集したりするには、をクリックします Actions ▾ をクリックし、*[アノテーションの編集]*を選択します。
   a. [アノテーション]*をクリックし、値を変更するアノテーションを選択するか、すべてのアセットに割り当てる新しいアノテーションを選択します。
   b. * 値 * をクリックし、アノテーションの値を選択します。
   c. [保存（ Save ）] をクリックします。
5. アセットに割り当てられているアノテーションを削除するには、をクリックします Actions ▾ をクリックし、*[Remove Annotation]*を選択します。
   a. [アノテーション]*をクリックし、アセットから削除するアノテーションを選択します。
   b. [削除（ Delete ）] をクリックします。

テーブル値をコピーしています

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

このタスクについて

テーブルまたはクエリ結果から値をコピーするには、2つの方法があります。

手順

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

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

Insightデータソース管理

データソースは、OnCommand Insight 環境の維持に使用される最も重要なコンポーネントです。Insightの主要な情報源であるため、データソースを実行状態に維持することが不可欠です。

ネットワーク内のデータソースを監視するには、データソースを選択してそのステータスに関連するイベントを確認し、問題の原因となった可能性がある変更を特定します。

個 々 のデータソースを確認するだけでなく、次の処理も実行できます。

- Insightで同様のデータソースを多数作成するには、データソースのクローンを作成します
- データソース情報を編集します
- クレデンシャルを変更
- ポーリングの制御
- データソースを削除します
- データソースパッチをインストールする
- パッチから新しいデータソースをインストールします
- ネットアップカスタマーサポート用のエラーレポートを準備

Insightでデータソースを設定します

データソースは、Insight環境を維持するうえで最も重要な要素です。データソースは、分析と検証に使用するネットワーク情報を検出します。ネットワーク内で監視できるように、Insightでデータソースを設定する必要があります。

各データソースについて、そのデータソースを定義するための固有の要件は、対応するデバイスのベンダーとモデルによって異なります。データソースを追加する前に、すべてのデバイスのネットワークアドレス、アカウント情報、パスワード、および必要に応じて次の詳細情報が必要です。

- スイッチ
- デバイス管理ステーション
- IP接続が確立されたストレージシステム
- ストレージ管理ステーション
- IP接続されていないストレージ・デバイス用の管理ソフトウェアを実行しているホスト・サーバ

データソースの定義の詳細については、このセクションの「ベンダー固有のデータソースリファレンス」を参照してください。

データソースのサポート情報

設定計画の一環として、環境内のデバイスをInsightで監視できることを確認する必要があります。そのためには、データソースサポートマトリックスでオペレーティングシステム、特定のデバイス、プロトコルの詳細を確認できます。一部のデータソースは、オペレーティングシステムによっては使用できない場合があります。

データソースサポートマトリックスの最新バージョンの場所

OnCommand Insight データソースサポートマトリックスは、サービスパックのリリースごとに更新されます。ドキュメントの最新バージョンについては、を参照してください "NetApp Support Site"。。

[データソースの追加]ダイアログボックスを使用して、データソースをすばやく追加できます。

手順

1. ブラウザでOnCommand Insight を開き、管理者権限を持つユーザとしてログインします。
2. を選択し、[Data sources]*を選択します。
3. [+追加]*ボタンをクリックします。

   データソースの追加ウィザードが開きます。

4. [設定]セクションで、次の情報を入力します。

フィールド	説明
名前	このデータソースの一意のネットワーク名を入力します。注：データソース名に使用できる文字は、アルファベット、数字、アンダースコア（_）のみです。
ベンダー	ドロップダウンからデータソースのベンダーを選択します。
モデル	ドロップダウンからデータソースのモデルを選択します。
どこで実行するか	[Local]を選択します。環境でRAUが設定されている場合はRemote Acquisition Unitを選択できます。
収集するもの	ほとんどのデータソースでは、これらのオプションは[Inventory]と[Performance]です。インベントリはデフォルトで常に選択されており、選択を解除することはできません。一部のデータソースには異なるオプションがある場合があります。選択した収集オプションによって、[Configuration]セクションと[Advanced configuration]セクションの使用可能なフィールドが変更されます。

5. [Configuration]*リンクをクリックし、選択したデータ収集タイプでデータソースに必要な基本的な設定情報を入力します。
6. 通常、このタイプのデータソースをネットワークで設定するために詳細な情報が必要な場合は、*[Advanced configuration]*リンクをクリックして追加情報 に入ります。
7. 特定のデータソースに必要な設定情報や高度な設定情報、または使用可能な設定情報の詳細については、を参照してください "ベンダー別のデータソースリファレンス"。
8. [Test]*リンクをクリックして、データソースが正しく設定されていることを確認します。

9. [保存（ Save ）] をクリックします。

スプレッドシートからデータソースをインポートする

スプレッドシートからOnCommand Insight に複数のデータソースをインポートできます。これは、検出デバイスをスプレッドシートですでに管理している場合に役立ちます。このプロセスでは新しいデータソースが追加されますが、既存のデータソースの更新には使用できません。

このタスクについて

OnCommand Insight には、データソースの作成に役立つスプレッドシートが用意されています。このスプレッドシートには次の属性があります。

- このスプレッドシートは、Microsoft Excel 2003以降で使用できます。
- 各タブには、Brocade SSH/CLIなど、1つのデータソースタイプが表示されます。
- 各行は、作成される新しいデータソースのインスタンスを表します。

スプレッドシートには、OnCommand Insight で新しいデータソースを作成するマクロが含まれています。

手順

1. でスプレッドシートを探します `<install_directory>/SANscreen/acq/bin/acqcli/SiteSurvey_DataSourceImporter_w_Macro.zip`。
2. スプレッドシートで、色の付いたセルにデータソース情報を入力します。
3. 空の行を削除します。
4. スプレッドシートからを実行します `CreateDataSources` マクロを使用してデータソースを作成します。
5. クレデンシャルの入力を求められたら、OnCommand Insight サーバの管理ユーザ名とパスワードを入力します。

   収集結果が収集ログに記録されます。

6. マクロを実行しているマシンにOnCommand Insight がインストールされているかどうかを確認するプロンプトが表示されます。

   次のいずれかを選択します。

   - いいえ：OnCommand Insight マシンで実行する必要があるバッチファイルを作成する場合は、[いいえ]を選択します。インストールディレクトリからこのバッチファイルを実行します。
   - Yes：OnCommand Insight がすでにインストールされていて、データソース情報を生成するための追加の手順が不要な場合は、[Yes]を選択します。
7. データソースが追加されたかどうかを確認するには、ブラウザでInsightを開きます。
8. Insightのツールバーで、*[Admin]*をクリックします。
9. [Data sources]リストで、インポートしたデータソースを確認します。

パッチによる新しいデータソースの追加

新しいデータソースはパッチファイルとしてリリースされ、パッチプロセスを使用してシステムにロードできます。このプロセスにより、OnCommand Insight の次のリリースまで新しいデータソースを使用できるようになります。

作業を開始する前に

インストールするパッチファイルをアップロードしておく必要があります。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [パッチ]*を選択します。
3. **>**[サービスパックまたはパッチのインストール]*を選択します。
4. [* Install Service Pack or Patch*（サービスパックまたはパッチのインストール）]ダイアログボックスで、*[Browse（参照）]*をクリックして、アップロードしたパッチファイルを探して選択します。
5. [パッチの概要]ダイアログボックスで*[次へ]*をクリックします。
6. 情報を確認し、[次へ]*をクリックして続行します。
7. [インストール]ダイアログボックスで、*[完了]*をクリックします。

データソースのクローニング

クローニング機能を使用すると、別のデータソースと同じクレデンシャルと属性を持つデータソースをすばやく追加することができます。クローンを作成すると、同じデバイスタイプの複数のインスタンスを簡単に構成できます。

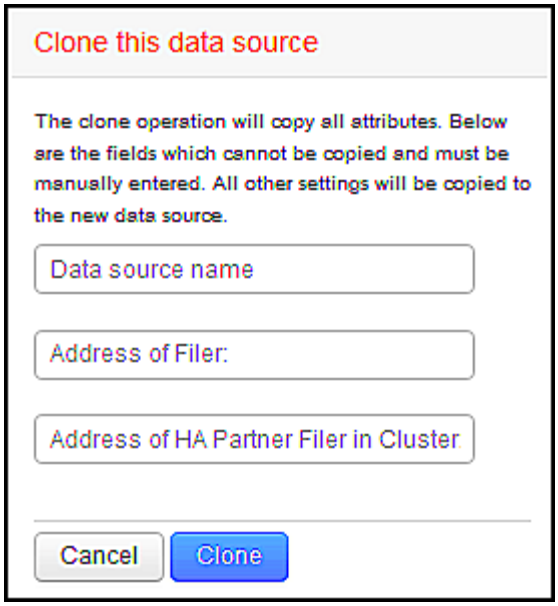
手順

1. Insightのツールバーで、*[Admin]*をクリックします。

   [Data sources]リストが開きます。

2. 新しいデータソースで使用するセットアップ情報が表示されているデータソースを強調表示します。
3. 強調表示されたデータソースの右側にある*[クローン]*アイコンをクリックします。

   [Clone this data source]ダイアログボックスには、選択したデータソースに指定する必要がある情報が表示されます。次の例は、ネットアップデータソースを示しています。



4. フィールドに必要な情報を入力します。これらの詳細を既存のデータソースからコピーすることはできません。
5. [* Clone*] をクリックします。

結果

他のすべての属性と設定がコピーされ、新しいデータソースが作成されます。

データソースの設定をテストします

データソースを追加するときは、そのデータソースを保存または更新する前に、デバイスと通信するための設定が正しいかどうかを確認できます。

データソースウィザードの*テスト*ボタンをクリックすると、指定したデバイスとの通信がチェックされます。このテストでは、次のいずれかの結果が生成されます。

- PASSED：データソースが正しく設定されています。
- 警告：テストが完了していません。処理中にタイムアウトしたか、データ収集が実行されていない可能性があります。
- Failed：設定されているデータソースが、指定されたデバイスと通信できません。設定を確認して再テストしてください。

ベンダー別のデータソースリファレンス

構成の詳細は、追加するデータソースのベンダーとモデルによって異なります。

このセクションには、ベンダーのデータソースでInsightの高度な設定手順（特別な要件や固有のコマンドなど）が必要な場合の情報が記載されています。

3PAR InServデータソース

OnCommand Insight は、3PAR InServ（Firmware 2.2.2+、SSH）データソースを使用し

て、HP 3PAR StoreServストレージアレイのインベントリを検出します。

用語集

OnCommand Insight では、3PAR InServデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
物理ディスク	ディスク
ストレージシステム	ストレージ
コントローラノード	ストレージノード
Common Provisioning Group の 1 つ	ストレージプール
仮想ボリューム	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- InServ クラスタの IP アドレスまたは FQDN
- インベントリの場合、InServサーバに対する読み取り専用のユーザ名とパスワード。
- パフォーマンスを高めるために、InServサーバに対する読み取り/書き込みのユーザ名とパスワード。
- ポート要件：22（インベントリ収集）、5988、または5989（パフォーマンス収集）[注：3PARパフォーマンスはInServ OS 3.x以降でサポートされます]
- パフォーマンス収集については、 SSH を使用して 3PAR アレイにログインし、 SMI-S が有効になっていることを確認してください。

設定

フィールド	説明
クラスタ IP	InServクラスタのIPアドレスまたは完全修飾ドメイン名
ユーザ名	InServサーバのユーザ名
パスワード	InServサーバのパスワード
SMI-SホストIP	SMI-SプロバイダホストのIPアドレス

SMI-S ユーザー名	SMI-S プロバイダホストのユーザ名
SMI-S のパスワード	SMI-S プロバイダホストのパスワード

詳細設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
デバイスを除外します	対象から除外するデバイスのIPをカンマで区切ったリスト
SSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは60秒）
SSHの再試行回数	SSHの再試行回数
SSHバナー待機タイムアウト（秒）	SSHバナーのタイムアウト（デフォルトは20秒）
SMI-Sポート	SMI-Sプロバイダホストが使用するポート
プロトコル	SMI-S プロバイダへの接続に使用するプロトコル
SMI-Sネームスペース	SMI-Sネームスペース
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
SMI-S接続の再試行回数	SMI-S接続の再試行回数

Amazon AWS EC2データソース

OnCommand Insight は、このデータソースを使用して、Amazon AWS EC2のインベントリとパフォーマンスを検出します。

前提条件

Amazon EC2 デバイスからデータを収集するには、次の情報が必要です。

- IAMアクセスキーIDが必要です
- Amazon EC2クラウドアカウントのシークレットアクセスキーが必要です
- 「組織のリスト」権限が必要です
- ポート433 HTTPS

- EC2 インスタンスは、仮想マシンまたは（自然に）ホストとしてレポートできます。EBS ボリュームは、 VM で使用されている仮想ディスクと、仮想ディスクの容量を提供するデータストアの両方として報告できます。

アクセスキーは、アクセスキー ID （ AKIAIOSFODNN7EXAMPLE など）とシークレットアクセスキー（ wJalrXUtil/K7MDENG/bPxRfiCYEXAMPLEKEY など）で構成されます。Amanzon EC2 SDK、REST、またはQuery API操作を使用する場合は、アクセスキーを使用して、EC@に行うプログラム要求に署名します。これらのキーは、 Amazon の契約に付属しています。

このデータソースの設定方法

Amazon AWS EC2データソースを設定するには、AWSアカウントのAWS IAM Access Key IDとSecret Access Keyが必要です。

次の表に従って、データソースのフィールドに入力します。

構成：

フィールド	説明
AWS リージョン	AWS リージョンを選択します
IAM ロール	AWS の AU で取得した場合にのみ使用します。IAM ロールの詳細については、以下を参照してください。
AWS IAM Access Key ID	AWS IAM Access Key ID を入力します。IAM ロールを使用しない場合は必須です。
AWS IAM Secret Access Key の略	AWS IAM Secret Access Key を入力します。IAM ロールを使用しない場合は必須です。
AWSからAPI要求の料金が請求されることは理解しています	Insightのポーリングによって作成されたAPI要求に対してAWSから課金されることを理解しているかどうかを確認するには、このチェックボックスをオンにします

高度な設定：

フィールド	説明
追加リージョンを含める	ポーリングに含める追加領域を指定します。
クロスアカウントロール	異なる AWS アカウントのリソースにアクセスするためのロール。
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）

HTTP接続およびソケットタイムアウト（秒）	HTTP接続タイムアウト（デフォルトは300秒）
AWSタグを含める	InsightのアノテーションでAWSタグがサポートされるようにするには、このオプションをオンにします
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは1、800秒）

AWSタグを**Insight**のアノテーションにマッピングする

AWS EC2データソースには、AWSで設定されているタグを使用してInsightのアノテーションを入力するオプションがあります。アノテーションにはAWSのタグとまったく同じ名前を付ける必要があります。Insightでは、常に同じ名前のテキストタイプのアノテーションが入力され、他のタイプ（数値、ブール値など）のアノテーションが入力されるように「最善の試み」が行われます。アノテーションのタイプが異なるためにデータソースにデータを入力できない場合は、アノテーションを削除してテキストタイプとして再作成する必要があります。

AWSでは大文字と小文字が区別され、Insightでは大文字と小文字が区別されないことに注意してください。そのため、Insightで「OWNER」という名前のアノテーションを作成し、AWSで「OWNER」、「OWNER」、「OWNER」という名前のタグを作成すると、AWSで使用されている「OWNER」のすべてのバリエーションがInsightの「OWNER」アノテーションにマッピングされます。

関連情報：

"IAMユーザのアクセスキーの管理"

追加リージョンを含める

AWS Data Collector * Advanced Configuration * セクションでは、 * Include extra regions * フィールドを設定して、カンマまたはセミコロンで区切って追加のリージョンを含めることができます。デフォルトでは、このフィールドは * *us-.* に設定されており、これによってすべての US AWS リージョンで収集されます。on_all_regions を収集するには、このフィールドを ***.*** に設定します。

「 * include extra regions * 」フィールドが空の場合、「 * Configuration * 」セクションの指定に従って、「 * AWS Region * 」フィールドに指定されたアセットについてデータコレクタが収集されます。

*** AWS Child Accounts**から収集*****

Insightでは、1つのAWSデータコレクタ内でのAWSの子アカウントの収集がサポートされます。この収集の設定は、 AWS 環境で実行されます。

- プライマリアカウントIDが子アカウントからEC2の詳細にアクセスできるように、各子アカウントにAWSロールを設定する必要があります。
- 各子アカウントには、ロール名が同じ文字列として設定されている必要があります
- このロール名の文字列をInsight AWS Data Collector * Advanced Configuration セクションの Cross Account Role *フィールドに入力します。

ベストプラクティス：AWSの事前定義されたAmazonEC2ReadOnlyAccessポリシーをECSプライマリアカウントに割り当てることを強く推奨します。また、AWSを照会するには、データソースで構成されているユーザに少なくとも事前定義された*AWSOrganizationsReadOnlyAccess*policyが割り当てられている必要がありま

す。

InsightがAWSの子アカウントから収集できるように環境を設定する方法については、次の資料を参照してください。

"チュートリアル： IAM ロールを使用した AWS アカウント間でのアクセスの委譲"

"AWS のセットアップ：自分が所有している別の AWS アカウントで IAM ユーザにアクセスを付与する"

"IAM ユーザに権限を委任するためのロールを作成する"

IAM ロール

_IAM Role_securityを使用する場合は、作成または指定するロールに、リソースへのアクセスに必要な適切な権限があることを確認する必要があります。

たとえば、 *InstanceEc2ReadOnly* という名前の IAM ロールを作成した場合は、この IAM ロールのすべての EC2 リソースに読み取り専用リストアクセス権限を付与するようにポリシーを設定する必要があります。また、このロールがアカウント間でロールを引き受けることができるように、 STS （セキュリティトークンサービス）アクセスを許可する必要があります。

IAM ロールを作成したら、新しい EC2 インスタンスまたは既存の EC2 インスタンスを作成するときに IAM ロールを接続できます。

IAM ロール *InstanceEc2ReadOnly* を EC2 インスタンスに接続すると、インスタンスメタデータから IAM ロール名で一時的なクレデンシャルを取得し、この EC2 インスタンスで実行されているすべてのアプリケーションから AWS リソースにアクセスできるようになります。

> IAMロールは、Acquisition UnitがAWSインスタンスで実行されている場合にのみ使用できます。

Brocade Enterprise Fabric Connectivity Managerデータソース

OnCommand Insight は、Brocade Enterprise Fabric Connectivity Manager（EFCM）データソースを使用して、Brocade EFCMスイッチのインベントリを検出します。Insightでは、EFCMバージョン9.5、9.6、9.7がサポートされます。

要件

> このデータコレクタは、OnCommand Insight 7.3.11以降では使用できません。

- EFCM サーバのネットワークアドレスまたは完全修飾ドメイン名
- EFCM のバージョンは 9.5 、 9.6 、または 9.7 である必要があります
- EFCM サーバの IP アドレス
- EFCM サーバに対する読み取り専用のユーザ名とパスワード
- 読み取り専用のユーザ名とパスワードを使用して、InsightサーバからConnectrixスイッチにポート51512経由でTelnetでアクセスできることを確認しました

設定

* フィールド *	* 概要 *
EFC サーバ	EFC サーバの IP アドレスまたは完全修飾ドメイン名
ユーザ名	スイッチのユーザ名
パスワード	スイッチのパスワード

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは15分）
ファブリック名	EFCMデータソースによってレポートされるファブリック名。ファブリック名を WWN としてレポートする場合は、空白のままにします。
通信ポート	スイッチとの通信に使用するポート
トラッピングを有効にします	デバイスからの SNMP トラップの受信時にデータ収集を有効にする場合に選択します。トラップを有効にするを選択した場合は、 SNMP も有効にする必要があります。
トラップ間の最小時間（秒）	トラップによって収集を試行する最小間隔（デフォルトは15秒）
非アクティブなゾーンセット	アクティブなゾーンセットに加えてデータ収集の対象に含める非アクティブなゾーンセットをカンマで区切ったリスト
使用する NIC	SAN デバイスをレポートする際に RAU で使用するネットワークインターフェイスを指定します
デバイスを除外します	ポーリングの対象に含めるか除外するユニットの名前をカンマで区切ったリスト
EFCMスイッチのニックネームをInsightスイッチ名として使用します	EFCMスイッチのニックネームをInsightスイッチ名として使用する場合に選択します
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

Brocade FC Switchデータソース

OnCommand Insight では、Brocade FC Switch（SSH）データソースを使用して、Factored Operating System（FOS）ファームウェア4.2以降を実行しているBrocadeスイッチデバイス（ブランド名が変更されたスイッチデバイス）のインベントリを検出します。FC スイッチとアクセスゲートウェイの両方のモードのデバイスがサポートされます。

用語集

OnCommand Insight では、Brocade FC Switchデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
スイッチ	スイッチ
ポート	ポート
仮想ファブリック、物理ファブリック	ファブリック
ゾーン	ゾーン
Logical Switch の略	Logical Switch の略
LSAN ゾーン	IVR ゾーン

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- Acquisition Unit（ローカルまたはリモート）は、BrocadeスイッチのTCPポート22への接続を開始してインベントリデータを収集します。AU は、パフォーマンスデータの収集用に UDP ポート 161 への接続も開始します。
- ファブリック内のすべてのスイッチへの IP 接続が必要です。[Discover all switches in the fabric]チェックボックスを選択すると、ファブリック内のすべてのスイッチが識別されますが、検出するにはこれらの追加スイッチへのIP接続が必要です。
- ファブリック内のすべてのスイッチで、同じアカウントがグローバルに必要です。アクセスの確認には、PuTTY （オープンソースの端末エミュレータ）を使用できます。
- Performライセンスがインストールされている場合は、SNMPパフォーマンスポーリング用に、ポート161および162をファブリック内のすべてのスイッチに対して開いておく必要があります。
- SNMP 読み取り専用コミュニティストリング

設定

フィールド	説明
スイッチ IP	スイッチの IP アドレスまたは完全修飾ドメイン名
ユーザ名	スイッチのユーザ名
パスワード	スイッチのパスワード
SNMP バージョン	SNMP バージョン
SNMP コミュニティストリング	スイッチへのアクセスに使用する SNMP の読み取り専用コミュニティストリング
SNMP ユーザ名	SNMPバージョンプロトコルのユーザ名（SNMP v3のみ）
SNMP パスワード	SNMPバージョンプロトコルのパスワード（SNMP v3のみ）

高度な設定

フィールド	説明
ファブリック名	データソースでレポートするファブリック名。ファブリック名を WWN としてレポートする場合は、空白のままにします。
デバイスを除外します	ポーリングの対象から除外するデバイスの ID をカンマで区切ったリスト
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは15分）
タイムアウト（秒）	接続タイムアウト（デフォルトは30秒）
バナー待機タイムアウト（秒）	SSHバナーのタイムアウト（デフォルトは5秒）
管理ドメインはアクティブです	管理ドメインを使用する場合に選択します
MPR データを取得する	マルチプロトコルルータ（MPR）からルーティングデータを取得する場合に選択します。

トラッピングを有効にします	デバイスからの SNMP トラップの受信時にデータ収集を有効にする場合に選択します。トラップを有効にするを選択した場合は、 SNMP も有効にする必要があります。
トラップ間の最小時間（秒）	トラップでデータ収集を試行する最小間隔（デフォルトは 10 秒）
ファブリック内のすべてのスイッチを検出します	ファブリック内のすべてのスイッチを検出する場合に選択します
HBA との優先を選択しますゾーンのエイリアス	HBA とゾーンエイリアスのどちらを優先するかを選択します
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
SNMP 認証プロトコル	SNMP 認証プロトコル（ SNMP v3 のみ）
SNMP プライバシープロトコル	SNMPプライバシープロトコル（SNMP v3のみ）
SNMP プライバシーパスワード	SNMP プライバシーパスワード（ SNMP v3 のみ）
SNMP 再試行回数	SNMP の再試行回数
SNMP タイムアウト（ミリ秒）	SNMP タイムアウト（デフォルトは 5 、 000 ミリ秒）

Brocade Sphereon/Intrepid Switchデータソース

OnCommand Insight では、Brocade Sphereon/Intrepid Switch（SNMP）データソースを使用して、Brocade Sphereon/Intrepidスイッチのインベントリを検出します。

要件

このデータコレクタは、OnCommand Insight 7.3.11以降では使用できません。

- ファブリック内のすべてのスイッチへの IP 接続が必要です。[Discover all switches in the fabric]チェックボックスを選択すると、ファブリック内のすべてのスイッチが識別されますが、検出するにはこれらの追加スイッチへのIP接続が必要です。
- SNMP V1 または SNMP V2 を使用している場合は、読み取り専用コミュニティストリングが必要です。
- ゾーニング情報を取得するには、スイッチへの HTTP アクセスが必要です。
- を実行してアクセスを検証します `snmpwalk` スイッチへのユーティリティ（を参照）`<install_path\>\bin\)`。

設定

* フィールド *	* 概要 *
球スイッチ	スイッチの IP アドレスまたは完全修飾ドメイン名
SNMP バージョン	SNMP バージョン
SNMPコミュニティ	スイッチへのアクセスに使用する SNMP の読み取り専用コミュニティストリング
ユーザ名	スイッチの SMI-S のユーザ名（ SNMP v3 のみ）
パスワード	スイッチの SMI-S のパスワード（ SNMP v3 のみ）

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは15分）
SNMP 認証プロトコル	SNMP 認証プロトコル（ SNMPv3 のみ）
SNMP プライバシープロトコル	SNMP プライバシープロトコル（ SNMPv3 のみ）
SNMP プライバシーパスワード	SNMPプライバシーパスワード
SNMP 再試行回数	SNMP の再試行回数
SNMP タイムアウト（ミリ秒）	SNMP タイムアウト（デフォルトは 5 、 000 ミリ秒）
ファブリック名	データソースでレポートするファブリック名。ファブリック名を WWN としてレポートする場合は、空白のままにします。
トラッピングを有効にします	デバイスからの SNMP トラップの受信時にデータ収集を有効にする場合に選択します。トラップを有効にするを選択した場合は、 SNMP も有効にする必要があります。
Ttrapsの最小間隔（秒）	トラップでデータ収集を試行する最小間隔（デフォルトは 10 秒）

パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

Cisco FC Switch Firmware（SNMP）データソース

OnCommand Insight では、Cisco FC Switch Firmware 2.0+（SNMP）データソースを使用して、Cisco MDSファイバチャネルスイッチおよびFCサービスが有効になっているさまざまなCisco Nexus FCoEスイッチのインベントリを検出します。さらに、このデータソースを使用して、NPVモードで実行されているシスコデバイスの多くのモデルを検出できます。

用語集

OnCommand Insight では、Cisco FC Switchデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
スイッチ	スイッチ
ポート	ポート
VSAN （仮想 SAN	ファブリック
ゾーン	ゾーン
Logical Switch の略	Logical Switch の略
ネームサーバエントリ	ネームサーバエントリ
Inter-VSAN Routing （ IVR ）ゾーン	IVR ゾーン

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ファブリック内の 1 つのスイッチまたは個々のスイッチの IP アドレス
- シャーシ検出。ファブリック検出をイネーブルにします
- SNMP V2 を使用している場合は、読み取り専用コミュニティストリングが必要です
- ポート 161 はデバイスへのアクセスに使用されます
- を使用したアクセスの検証 `snmpwalk` スイッチへのユーティリティ（を参照）`<install_path\>\bin\`)

設定

フィールド	説明
Cisco スイッチ IP	スイッチの IP アドレスまたは完全修飾ドメイン名
SNMP バージョン	パフォーマンスの取得にはSNMPバージョンv2以降が必要です
SNMP コミュニティストリング	スイッチへのアクセスに使用する SNMP の読み取り専用コミュニティストリング（ SNMP v3 は対象外）
ユーザ名	スイッチのユーザ名（ SNMP v3 のみ）
パスワード	スイッチのパスワード（ SNMPv3 のみ）

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
SNMP 認証プロトコル	SNMP 認証プロトコル（ SNMPv3 のみ）
SNMP プライバシープロトコル	SNMP プライバシープロトコル（ SNMPv3 のみ）
SNMP プライバシーパスワード	SNMPプライバシーパスワード
SNMP 再試行回数	SNMP の再試行回数
SNMP タイムアウト（ミリ秒）	SNMP タイムアウト（デフォルトは 5 、 000 ミリ秒）
トラッピングを有効にします	トラップを有効にする場合に選択します。トラッピングを有効にする場合は、 SNMP 通知も有効にする必要があります。
トラップ間の最小時間（秒）	トラップでデータ収集を試行する最小間隔（デフォルトは 10 秒）
すべてのファブリックスイッチを検出します	ファブリック内のすべてのスイッチを検出する場合に選択します
デバイスを除外します	ポーリングの対象から除外するデバイスの IP をカンマで区切ったリスト

デバイスを含める	ポーリングの対象に含めるデバイスの IP をカンマで区切ったリスト
デバイスタイプを確認します	Cisco デバイスとして明示的にアドバタイズされたデバイスのみを受け入れる場合に選択します
プライマリエイリアスタイプ	エイリアスの解決で最初に優先する情報を指定します。次のいずれかを選択します。 • デバイスエイリアス これは、ポートWWN（pWWN）のフレンドリ名であり、必要に応じてすべてのコンフィギュレーションコマンドで使用できます。Cisco MDS 9000 ファミリのすべてのスイッチは、Distributed Device Alias Services （デバイスエイリアス）をサポートしています。 • * なし * エイリアスは報告しないでください • *ポート概要 * ポートのリストでポートを識別するための概要 • ゾーンエイリアス（すべて） ゾーニング設定でのみ使用できるポートのフレンドリ名 • ゾーンエイリアス（アクティブのみ） アクティブな構成でのみ使用できるポートのフレンドリ名。これがデフォルトです。
セカンダリエイリアスタイプ	エイリアスの解決で 2 番目に優先する情報を指定します
ターシャリエイリアスタイプ	エイリアスの解決で 3 番目に優先する情報を指定します
SANTap プロキシモードサポートをイネーブルにします	Cisco スイッチで SANTap のプロキシモードを使用している場合に選択。EMC RecoverPoint を使用している場合は、 SANTap を使用していると考えられます。
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

EMC Celerraデータソース

Celerra（SSH）データソースは、Celerraストレージからインベントリ情報を収集します。このデータソースを設定するには、ストレージプロセッサのIPアドレス、および_read-only_userの名前とパスワードが必要です。

用語集

OnCommand Insight では、EMC Celerraデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
Celerra Network Serverの略	ストレージ
Celerraメタ・ボリューム/Celerraストレージ・プール	ストレージプール
File System の略	内部ボリューム
データムーバー	コントローラ
Data Moverにマウントされたファイルシステム	ファイル共有
CIFS および NFS エクスポート	共有
ディスクボリューム	バックエンド LUN

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ストレージプロセッサの IP アドレス
- 読み取り専用のユーザ名とパスワード
- SSH ポート 22

設定

フィールド	説明
Celerraのアドレス	CelerraデバイスのIPアドレスまたは完全修飾ドメイン名
ユーザ名	Celerraデバイスへのログインに使用する名前

パスワード	Celerraデバイスへのログインに使用するパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
SSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは600秒）
再試行回数	インベントリの再試行回数
SSHバナー待機タイムアウト（秒）	SSHバナーのタイムアウト（デフォルトは20秒）

EMC CLARiX（NaviCLI）データソース

このデータソースを設定する前に、ターゲットデバイスとInsight ServerにEMC Navisphere CLIがインストールされていることを確認してください。Navisphere CLIのバージョンは、コントローラのファームウェアのバージョンと一致している必要があります。パフォーマンスデータを収集するには、統計ログをオンにする必要があります。

Navisphereコマンド・ライン・インタフェースの構文

```
naviseccli.exe -h <IP address> -user <user> -password <password> -scope
<scope,use 0 for global scope> -port <use 443 by default> command
```

用語集

OnCommand Insight では、EMC CLARiXデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
ストレージ	ストレージ
ストレージプロセッサ	ストレージノード
シンプール、RAIDグループ	ストレージプール
LUN	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- 各CLARiXストレージ・プロセッサのIPアドレス
- CLARiXアレイに対する読み取り専用のNavisphereユーザー名とパスワード
- NavicliがInsight Server / RAUにインストールされている必要があります
- アクセスの検証：上記のユーザ名とパスワードを使用して、Insight Serverから各アレイに対してNaviCLIを実行します。
- Navicliのバージョンは'アレイ上の最新のFLAREコードに対応している必要があります
- パフォーマンスのためには、統計ログをオンにする必要があります。
- ポート要件： 80 、 443

設定

フィールド	説明
CLARiXストレージ	CLARiXストレージのIPアドレスまたは完全修飾ドメイン名
ユーザ名	CLARiXストレージ・デバイスへのログインに使用する名前
パスワード	CLARiXストレージ・デバイスへのログインに使用するパスワード
CLIのnavicli.exeパスまたはnaviseccli.exeパスへのパス	への完全パス `navicli.exe` または `naviseccli.exe` 実行ファイル

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
Secure Clientの使用（naviseccli）	セキュア・クライアントを使用する場合に選択（navseccli）
適用範囲	セキュアなクライアントの範囲デフォルトは Global です。
CLARiX CLIポート	CLARiX CLIに使用するポート

インベントリ外部プロセスタイムアウト（秒）	外部プロセスのタイムアウト（デフォルトは1、800秒）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
パフォーマンス外部プロセスのタイムアウト（秒）	外部プロセスのタイムアウト（デフォルトは1、800秒）

EMC Data Domainデータソース

このデータソースは、EMC Data Domain重複排除ストレージシステムからストレージと構成の情報を収集します。データソースを追加するには、特定の設定手順とコマンドを使用し、データソースの要件と使用に関する推奨事項を確認しておく必要があります。

用語集

OnCommand Insight では、EMC Data Domainデータソースから次のインベントリ情報を取得します。Insight で取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
配列	ストレージ
ポート	ポート
ファイルシステム	内部ボリューム
ミトリー	qtree
クォータ	クォータ
NFS 共有および CIFS 共有	ファイル共有

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- Data Domain デバイスの IP アドレス
- Data Domain ストレージに対する読み取り専用のユーザ名とパスワード

- SSH ポート 22

設定

フィールド	説明
IP アドレス	Data Domain ストレージアレイの IP アドレスまたは完全修飾ドメイン名
ユーザ名	Data Domain ストレージアレイのユーザ名
パスワード	Data Domain ストレージアレイのパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
SSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは180秒）
SSH ポート	SSH サービスポート

EMC ECC StorageScopeデータソース

EMC ECC StorageScopeデバイスには'5.x'6.0'6.1の3種類のデータ・ソースがあります

設定

このデータコレクタは、OnCommand Insight 7.3.11以降では使用できなくなりました。

* フィールド *	* 概要 *
ECCサーバ	ECCサーバのIPアドレスまたは完全修飾ドメイン名
ユーザ名	ECCサーバのユーザ名
パスワード	ECCサーバのパスワード

高度な設定

* フィールド *	* 概要 *
ECCポート	ECCサーバに使用するポート

インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは30分）
データベースに接続するプロトコル	データベースへの接続に使用されるプロトコル
ファイルシステム情報を照会します	WWNエイリアスとファイルシステムの詳細を取得する場合に選択します。

Dell EMC ECSデータソース

このデータコレクタは、 EMC ECS ストレージシステムからインベントリデータとパフォーマンスデータを取得します。データコレクタを設定するには、ECSサーバのIPアドレスと管理者レベルのドメインアカウントが必要です。

用語集

OnCommand Insight では、EMC ECSデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
クルーザー	ストレージ
テナント	ストレージプール
バケット	内部ボリューム
ディスク	ディスク

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ECS 管理コンソールの IP アドレス
- ECS システムの管理者レベルドメインアカウント
- ポート 443 （ HTTPS ）：ECS システムで TCP ポート 443 へのアウトバウンド接続が必要です。
- パフォーマンスを確保するには、 ssh/scp アクセス用の読み取り専用のユーザ名とパスワードを使用します。
- パフォーマンスを確保するには、ポート 22 が必要です。

設定

フィールド	説明

ECS ホスト	ECSシステムのIPアドレスまたは完全修飾ドメイン名
ECS ホストポート	ECS ホストとの通信に使用されるポート
ECS ベンダー ID	ECS のベンダー ID
パスワード	ECS のパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔。デフォルトは 360 分です。

EMC Isilonデータソース

Isilon SSHデータソースは、EMC IsilonスケールアウトNASストレージからインベントリとパフォーマンスを収集します。

用語集

OnCommand Insight では、EMC Isilonデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ドライブ	ディスク
クラスタ	ストレージ
ノード	ストレージノード
File System の略	内部ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- Isilon ストレージに対する管理者権限
- を使用してアクセスを検証 `telnet` ポート22に接続します

設定

フィールド	説明
IP アドレス	Isilon クラスタの IP アドレスまたは完全修飾ドメイン名
ユーザ名	Isilonクラスタのユーザ名
パスワード	Isilonクラスタのパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
SSHプロセス待機タイムアウト	SSHプロセスのタイムアウト（デフォルトは60秒）
SSH ポート	SSH サービスポート

CLIコマンドの実行

OnCommand Insight バージョン7.3.11およびサービスパック9以降、EMC Isilonデータソースには、より多くのCLIコマンドが実行されるようになる拡張機能が含まれています。データソース内でroot以外のユーザを使用している場合は、「sudoers」ファイルを設定して、そのユーザアカウントにSSH経由で特定のCLIコマンドを実行する権限を付与している可能性があります。

InsightでEMCのアクセスゾーン機能を理解するために’次の新しいCLIコマンドが追加で実行されるようになりました

- `sudo isi zone zones list --format json –verbose`
- `sudo isi zone zones list`

Insightでは、これらのコマンドの出力を解析し、既存のコマンドのインスタンスを追加で実行して、デフォルト以外のアクセスゾーンに存在するqtree、クォータ、NAS共有/エクスポートなどのオブジェクトの論理構成を取得します。この機能拡張の結果、デフォルト以外のアクセスゾーンについてこれらのオブジェクトが報告されるようになりました。Insightでは、既存のコマンド（オプションが異なる）を実行してデータを取得するため、sudoersファイルを変更する必要はありません。変更が必要になるのは、上記の新しいコマンドを導入したときだけです。

このInsightリリースにアップグレードする前に、sudoersファイルを更新してInsightサービスアカウントでこれらのコマンドが実行されるようにしてください。これを行わないと、Isilonデータソースに障害が発生します。

「ファイルシステム」統計

OnCommand Insight 7.3.12以降では、EMC Isilonデータコレクタによって、EMC Isilonのノードオブジェクトに関する「ファイルシステム」統計が導入されています。OnCommand Insight によって報告される既存のノードの統計は「ディスク」ベースです。ストレージノードのIOPSとスループットの場合、このノードのディスクはアグリゲートで何をしていますか？ただし、読み取りがメモリにキャッシュされたり、圧縮が使用されたりするワークロードの場合、ファイルシステムのワークロードは実際にディスクにヒットするワークロードよりも大幅に高くなる可能性があります。つまり、5：1で圧縮されるデータセットの場合は、「ファイルシステムの読み取りスループット」の値がストレージノードの5倍になる可能性があります。読み取りスループット、 後者はディスクからの読み取りを測定します。これは、ノードがデータを解凍してクライアントの読み取り要求を処理すると5倍に拡張されます。

Dell EMC PowerStoreデータソース

Dell EMC PowerStoreデータコレクタは、Dell EMC PowerStoreストレージからインベントリ情報を収集します。データコレクタを設定するには、ストレージプロセッサの IP アドレス、および読み取り専用のユーザ名とパスワードが必要です。

用語集

OnCommand Insight では、EMC Data Domainデータソースから次のインベントリ情報を取得します。Insight で取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ホスト	ホスト
host_volume_mapping	host_volume_mapping
ハードウェア（「 extra_details 」オブジェクトにドライブが含まれています）：ドライブ	ディスク
アプライアンス	ストレージプール
クラスタ	ストレージアレイ
ノード	ストレージノード
FC ポート	ポート
ボリューム	ボリューム
内部ボリューム	ファイルシステム
ファイルシステム	内部ボリューム

ミトリー	qtree
クォータ	クォータ
NFS 共有および CIFS 共有	ファイル共有

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ストレージプロセッサの IP アドレスまたは完全修飾ドメイン名
- 読み取り専用のユーザ名とパスワード

親シリアル番号の説明

従来、Insightでは、ストレージアレイのシリアル番号や個 々 のストレージノードのシリアル番号をレポートすることができました。ただし、一部のストレージアレイアーキテクチャはこれに適切に対応していません。PowerStoreクラスタは1~4台のアプライアンスで構成でき、各アプライアンスには2つのノードがあります。アプライアンス自体のシリアル番号がある場合、そのシリアル番号はクラスタのシリアル番号でもノードのシリアル番号でもありません。

大規模なクラスタの一部にすぎない中間アプライアンス/エンクロージャに個 々 のノードが配置されている場合、ストレージノードオブジェクトの「Parent Serial Number」属性がDell/EMC PowerStoreアレイ用に適切に設定されます。

設定

フィールド	説明
PowerStore ゲートウェイ	PowerStore ストレージの IP アドレスまたは完全修飾ドメイン名
ユーザ名	PowerStore のユーザー名
パスワード	PowerStore のパスワード

高度な設定

フィールド	説明
HTTPS ポート	デフォルトは 443 です
インベントリポーリング間隔（分）	インベントリのポーリング間隔。デフォルトは 60 分です。

OnCommand InsightのPowerStoreパフォーマンスコレクションでは、PowerStoreの5分単位のソースデータを使用します。そのため、Insightは5分ごとにそのデータをポーリングします。このポーリングは設定できません。

EMC RecoverPointデータソース

EMC RecoverPointデータソースは、EMC RecoverPointストレージからインベントリ情報を収集します。データソースを設定するには、ストレージプロセッサのIPアドレス、および_read-only_userの名前とパスワードが必要です。

EMC RecoverPointデータソースは、RecoverPointが他のストレージアレイ間で調整するボリューム間レプリケーション関係を収集します。OnCommand Insight は各RecoverPointクラスタのストレージアレイを表示し、そのクラスタ上のノードとストレージポートのインベントリデータを収集します。ストレージプールまたはボリュームのデータは収集されません。

要件

- ストレージプロセッサの IP アドレスまたは完全修飾ドメイン名
- 読み取り専用のユーザ名とパスワード
- ポート 443 経由での REST API へのアクセス
- PuTTYを使用したSSHアクセス

設定

フィールド	説明
RecoverPoint のアドレス	RecoverPoint クラスタの IP アドレスまたは完全修飾ドメイン名
ユーザ名	RecoverPoint クラスタのユーザ名
パスワード	RecoverPointクラスタのパスワード

高度な設定

フィールド	説明
TCP ポート	RecoverPoint クラスタへの接続に使用する TCP ポート
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
除外クラスタ	ポーリング時に除外するクラスタのIDまたは名前をカンマで区切ったリスト

EMC Solutions EnablerとSMI-S Performanceデータソース

OnCommand Insight は'Solutions Enablerを使用してSymmetrixストレージ・アレイを検出します `symcli` コマンドを環境内の既存のSolutions Enablerサーバと組み合わせて使用既存のSolutions Enablerサーバは、ゲートキーパーボリュームへのアクセスを通じてSymmetrixストレージアレイに接続されています。このデバイスにアクセスするには、管理者権限が必要です。

用語集

OnCommand Insight では、EMC Solutions Enablerデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
ディスクグループ	ディスクグループ
ストレージアレイ	ストレージ
ディレクター	ストレージノード
デバイスプール、 Storage Resource Pool （ SRP ；ストレージリソースプール）	ストレージプール
デバイス、TDEV	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

このデータソースを設定する前に、OnCommand Insight サーバから既存のSolutions Enablerサーバのポート2707へのTCP接続が確立されていることを確認する必要があります。OnCommand Insight は'サーバからの'symcfg list"の出力に示されているように'このサーバに対してローカルであるすべてのSymmetrixアレイを検出します

- EMC Solutions Enabler（CLI）とSMI-Sプロバイダアプリケーションがインストールされていて、Solutions Enablerサーバで実行されているバージョンと同じかそれよりも前のバージョンである必要があります。
- 適切に設定されている `{installdir}\EMC\SYMAPI\config\netcnfg` ファイルは必須です。このファイルでは、 Solutions Enabler サーバのサービス名とアクセス方法（ SECURE / NOSECURE / ANY ）を定義します。
- ストレージノードレベルで読み取り / 書き込みレイテンシが必要な場合、 SMI-S プロバイダは Unisphere for VMAX アプリケーションの実行中のインスタンスと通信する必要があります。

- Solutions Enabler （ SE ）サーバに対する管理者権限が必要です
- SE ソフトウェアに対する読み取り専用のユーザ名とパスワード
- Solutions Enabler サーバ 6.5X の要件：
  - SMIS-S V1.2用のSMI-Sプロバイダ3.3.1がインストールされています
  - インストール後、を実行します `\Program Files\EMC\SYMCLI\bin>stordaemon start storsrvd`
- Unisphere for VMAXアプリケーションが実行され、SMI-S Providerインストールによって管理されるSymmetrix VMAXストレージアレイの統計情報を収集している必要があります
- アクセスの検証：SMI-Sプロバイダが実行されていることを確認します。 `telnet <se_server\> 5988`

設定

> SMI-Sユーザ認証が有効になっていない場合、OnCommand Insight データソースのデフォルト値は無視されます。

Symmetrixアレイでsymauthが有効になっていると、OnCommand Insight がそれらのアレイを検出できなくなる可能性があります。OnCommand Insight による取得は、Solutions Enablerサーバと通信するOnCommand Insight / Remote Acquisition Unitサーバ上で、システムユーザとして実行されます。hostname\system にsymauth権限がない場合、OnCommand Insight はアレイを検出できません。

EMC Solutions Enabler Symmetrix CLIデータソースには、シンプロビジョニングおよびSymmetrix Remote Data Facility（SRDF）のデバイス構成のサポートが含まれています。

ファイバチャネルおよびスイッチのパフォーマンスパッケージの定義が提供されます。

フィールド	説明
サービス名	netcnfgファイルで指定されたサービス名
CLI の完全パス	Symmetrix CLIの完全パス

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
「除外」または「含める」を選択してリストを指定します	以下のリストにあるアレイをデータの収集時に対象に含めるか除外するかを指定します
インベントリ除外デバイス	対象に含めるか除外するデバイスの ID をカンマで区切ったリスト

接続のキャッシュ	接続のキャッシュ方法を選択： • localは、OnCommand Insight 取得サービスがSolutions Enablerサーバ上で実行されていることを意味します。サーバは検出対象のSymmetrixアレイにファイバチャネルで接続され、ゲートキーパーボリュームにアクセスできます。このオプションは、一部の Remote Acquisition Unit （RAU ）構成で使用されます。 • REMOTE_CACHEDはデフォルトであり、ほとんどの場合に使用する必要があります。このオプションでは、 NETCNFG ファイルの設定に基づいて、 IP を使用して Solutions Enabler サーバに接続します。サーバは検出対象の Symmetrix アレイにファイバチャネルで接続されていて、ゲートキーパーボリュームにアクセスできる必要があります。 • remote_cachedオプションでCLIコマンドが失敗する場合は、remoteオプションを使用します。データ収集プロセスが遅くなることに注意してください（数時間から場合によっては数日かかることがあります）。検出対象の Symmetrix アレイにファイバチャネルで接続された Solutions Enabler サーバへの IP 接続には、引き続き NETCNFG ファイルの設定が使用されます。 ⓘ この設定では、「symcfg list」の出力でremoteとしてリストされている配列に対するOnCommand Insight の動作は変更されません。OnCommand Insight は、このコマンドでローカルと表示されたデバイス上のデータのみを収集します。
CLIタイムアウト（秒）	CLIプロセスのタイムアウト（デフォルトは7200秒）
SMI-SホストIP	SMI-Sプロバイダホストの IPアドレス
SMI-Sポート	SMI-Sプロバイダホストが使用するポート
プロトコル	SMI-S プロバイダへの接続に使用するプロトコル
SMI-Sネームスペース	SMI-Sプロバイダが使用するように設定されている相互運用ネームスペース
SMI-S ユーザー名	SMI-S プロバイダホストのユーザ名

SMI-S のパスワード	SMI-S プロバイダホストのユーザ名
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 1000 秒）
パフォーマンスフィルタタイプ	下のリストに表示されたアレイをパフォーマンスデータの収集時に対象に含めるか除外するかを指定します
パフォーマンスフィルタのデバイスリスト	対象に含めるか除外するデバイスの ID をカンマで区切ったリスト
RPOポーリング間隔（秒）	RPOポーリングの間隔（デフォルトは300秒）

EMC VNXデータソース

EMC VNX（SSH）データソースを構成するには、Control StationのIPアドレス、および_read-only_usernameとパスワードが必要です。

設定

フィールド	説明
VNX IP	VNX Control Station の IP アドレスまたは完全修飾ドメイン名
VNXユーザー名	VNX Control Station のユーザー名
VNXパスワード	VNX Control Station のパスワード

要件

- Control StationのIPアドレス
- 読み取り専用のユーザ名とパスワード
- アクセスの検証：PuTTYによるSSHアクセスを確認します。

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
VNX SSHプロセス待機タイムアウト（秒）	VNX SSHプロセスのタイムアウト（デフォルトは600秒）

Celerraコマンドの再試行	Celerraコマンドの再試行回数
CLARiXインベントリの外部プロセスタイムアウト（秒）	インベントリのCLARiX外部プロセスのタイムアウト（デフォルトは1、800秒）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
CLARiX外部プロセスのパフォーマンスタイムアウト（秒）	CLARiX外部プロセスのパフォーマンスタイムアウト（デフォルトは1、800秒）

EMC VNXeデータソース

EMC VNXeデータソースは、EMC VNXeおよびUnityユニファイドストレージアレイのインベントリサポートを提供します。

このデータソースはCLIベースであり、VNXeデータソースが存在するAcquisition UnitにUnisphere for VNXe CLI（uemcli.exe）をインストールする必要があります。uemcli.exeは転送プロトコルとしてHTTPSを使用するため、Acquisition UnitからVNXe/Unityアレイへの HTTPS接続を開始できる必要があります。データソースで使用する読み取り専用ユーザが少なくとも1人必要です。

用語集

OnCommand Insight では、EMC VNXeデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
ストレージアレイ	ストレージ
プロセッサ	ストレージノード
ストレージプール	ストレージプール
一般的な iSCSI ブロック情報、 VMware VMFS	ボリューム
共有フォルダ	内部ボリューム
VMware NFSデータストアからのCIFS共有、NFS共有、共有	共有
Replication Remote System の略	同期

iSCSI ノード	iSCSI ターゲットノード
iSCSI イニシエータ	iSCSI ターゲットイニシエータ

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

このデータソースを設定して使用するための要件は次のとおりです。

- VNXe データコレクタは CLI ベースです。 VNXe データコレクタが存在する Acquisition Unit に Unisphere for VNXe CLI （ uemcli.exe ）をインストールする必要があります。
- uemcli.exe は HTTPS を転送プロトコルとして使用するため、 VNXe への HTTPS 接続を Acquisition Unit から開始できる必要があります。
- データソースで使用する読み取り専用ユーザが少なくとも1人必要です。
- 管理用 Solutions Enabler サーバの IP アドレス
- ポート 443 での HTTPS が必要です
- EMC VNXeデータコレクタは、NASおよびiSCSIによるインベントリのサポートを提供します。ファイバチャネルボリュームは検出されますが、InsightではFCマッピング、マスキング、ストレージポートについてはレポートされません。

設定

フィールド	説明
VNXe ストレージ	VNXe デバイスの IP アドレスまたは完全修飾ドメイン名
ユーザ名	VNXe デバイスのユーザ名
パスワード	VNXe デバイスのパスワード
uemcli実行可能ファイルの完全パス	への完全パス `uemcli.exe` 実行ファイル

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
VNXe CLIポート	VNXe CLI に使用するポート

インベントリ外部プロセスタイムアウト（秒）	外部プロセスのタイムアウト（デフォルトは1、800秒）

EMC VPLEXデータソース

このデータソースを設定するには、VPLEXサーバのIPアドレスと管理者レベルのドメインアカウントが必要です。

用語集

OnCommand Insight では、EMC VPLEXデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
クラスタ	ストレージ
エンジン	ストレージノード
デバイス、システム拡張	バックエンドストレージプール
仮想ボリューム	ボリューム
フロントエンドポート、バックエンドポート	ポート
分散デバイス	ストレージ同期
ストレージビュー	ボリュームマップ、ボリュームマスク
ストレージボリューム	バックエンド LUN
ITL	バックエンドパス

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- VPLEXサーバのIPアドレス
- VPLEX サーバの管理者レベルのドメインアカウント
- ポート 443 （ HTTPS ）：VPLEX 管理ステーションの TCP ポート 443 へのアウトバウンド接続が必要です。
- パフォーマンスを確保するには、 ssh/scp アクセス用の読み取り専用のユーザ名とパスワードを使用します。

- パフォーマンスを確保するには、ポート 22 が必要です。
- アクセスの検証：を使用して検証します `telnet` ポート443に接続します。デフォルトポート以外のポートの場合は、任意のブラウザでを使用します

設定

フィールド	説明
VPLEX Management Console の IP アドレス	VPLEX Management Console の IP アドレスまたは完全修飾ドメイン名
ユーザ名	VPLEX CLI のユーザ名
パスワード	VPLEX CLI のパスワード
VPLEX Management Consoleのパフォーマンスリモートの IP アドレス	VPLEX Management Console のパフォーマンスリモートの IP アドレス
パフォーマンスリモートユーザ名	VPLEX Management Console のパフォーマンスリモートのユーザ名
パフォーマンスリモートパスワード	VPLEX Management Console のパフォーマンスリモートのパスワード

高度な設定

フィールド	説明
通信ポート	VPLEX CLIに使用するポート
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）
再試行回数	インベントリの再試行回数
パフォーマンスポーリング間隔（秒）	パフォーマンスポーリング間隔（デフォルトは600秒）
パフォーマンスSSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは600秒）
SSHバナー待機タイムアウト（秒）	SSHバナーのタイムアウト（デフォルトは20秒）
再試行回数	パフォーマンスの再試行回数

EMC XtremIO（HTTP）データソースを構成するには、XtremIO Management Server（XMS）ホストアドレスと管理者権限を持つアカウントが必要です。

用語集

OnCommand Insight では、EMC XtremIOデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク（ SSD ）	ディスク
クラスタ	ストレージ
コントローラ	ストレージノード
ボリューム	ボリューム
LUN マップ	ボリュームマップ
イニシエータ、ターゲット	ボリュームマスク

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- 各XtremIO Management ServerのIPアドレス
- 管理者権限を持つアカウント
- ポート 443 へのアクセス（ HTTPS ）

設定

フィールド	説明
XMS ホスト	XtremIO Management Server の IP アドレスまたは完全修飾ドメイン名
ユーザ名	XtremIO Management Server のユーザ名
パスワード	XtremIO Management Server のパスワード

高度な設定

フィールド	説明
TCP ポート	XtremIO Management Serverへの接続に使用するTCPポート（デフォルトは443）
インベントリのポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）
パフォーマンスのポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

Fujitsu Eternusデータソース

Fujitsu Eternusデータソースには、ストレージのIPアドレスが必要です。カンマで区切ることはできません。

用語集

OnCommand Insight では、Fujitsu ETERNUSデータソースから次のインベントリ情報を取得します。Insight で取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
ストレージ	ストレージ
シンプール、フレキシブル階層プール、 RAID グループ	ストレージプール
標準ボリューム、Snap Data Volume（SDV）、 Snap Data Poolボリューム（SDPV） シンプロビジョニングボリューム（TPV）	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- Eternus ストレージの IP アドレス。カンマで区切って指定することはできません
- SSH 管理レベルのユーザ名とパスワード
- ポート 22
- ページスクロールが無効になっていることを確認します。（clientv-show-more-scroll disable）

設定

フィールド	説明
Eternus ストレージの IP アドレス	Eternus ストレージの IP アドレス
ユーザ名	Eternus ストレージのユーザ名
パスワード	胸骨に使用するパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
SSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは600秒）

Hitachi Content Platform（HCP）データソース

このデータコレクタは、 HCP 管理 API を使用して、 Hitachi Content Platform （ HCP ）をサポートします。

用語集

OnCommand Insight では、HCPデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
HCP クラスタです	ストレージ
テナント	ストレージプール
ネームスペース	内部ボリューム
ノード	ノード

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

インベントリの要件

- HCP サーバの IP アドレス
- HCP ソフトウェアおよびピア権限の読み取り専用のユーザ名およびパスワード

設定

* フィールド *	* 概要 *
HCP ホスト	HCP ホストの IP アドレスまたは完全修飾ドメイン名
HCP ポート	デフォルトは 9090 です
HCPユーザーID	HCPホストのユーザ名
HCP パスワード	HCPホストのパスワード
HCP 認証タイプ	HCP_LOCAL または active_directory を選択してください

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは900秒）

HDS HiCommand Device Managerデータソース

HDS HiCommandおよびHiCommand Liteデータソースでは、HiCommand Device Managerサーバがサポートされます。OnCommand Insight は、標準のHiCommand API を使用してHiCommandデバイスマネージャサーバと通信します。

用語集

OnCommand Insight では、HDS HiCommandおよびHiCommand Liteデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語

PDEV	ディスク
ジャーナルプール	ディスクグループ
ストレージアレイ	ストレージ
Port Controller の略	ストレージノード
アレイグループ 'DP プール	ストレージプール
論理ユニット、 LDEV	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

インベントリの要件

- HiCommand Device Manager サーバの IP アドレス
- HiCommand Device Manager ソフトウェアおよびピアの権限に対する読み取り専用のユーザ名とパスワード
- ポート要件： 2001 （ http ）または 2443 （ https ）
- アクセスの検証：
  - ピアのユーザ名とパスワードを使用してHiCommand Device Managerソフトウェアにログインします。
  - HiCommand Device Manager APIへのアクセスを確認します。 `telnet <HiCommand Device_Manager_server_ip\> 2001`

パフォーマンス要件

- HDS USP 、 USP V 、および VSP のパフォーマンス
  - Performance Monitor のライセンスが必要です。
  - 監視スイッチが有効になっている必要があります。
  - エクスポートツール (`Export.exe`）をOnCommand Insight サーバにコピーする必要があります。
  - エクスポートツールのバージョンとターゲットアレイのマイクロコードのバージョンが一致している必要があります。
- HDS AMSのパフォーマンス
  - Performance Monitorのライセンスが必要です。
  - Storage Navigator Modular 2（SNM2）CLIユーティリティがOnCommand Insight サーバにインストールされている必要があります。
  - 次のコマンドを使用して、OnCommand Insight でパフォーマンスを取得する必要があるAMS、WMS、SMSのすべてのストレージアレイを登録する必要があります。

- 登録したすべてのアレイがこのコマンドの出力に表示されていることを確認する必要があります。`auunitref.exe`。

設定

* フィールド *	* 概要 *
HiCommand サーバ	HiCommand Device Manager サーバの IP アドレスまたは完全修飾ドメイン名
ユーザ名	HiCommand Device Manager サーバのユーザ名
パスワード	HiCommand Device Manager サーバのパスワード
デバイス - VSP G1000 （ R800 ）、 VSP （ R700 ）、 HUS VM （ HM700 ）、および USP ストレージ	VSP G1000 （ R800 ）、 VSP （ R700 ）、 HUS VM （ HM700 ）、および USP ストレージのデバイスリスト。各ストレージには以下が必要です。 • Array’s IP：ストレージのIPアドレス • User Name：ストレージのユーザ名 • Password：ストレージのパスワード • Folder Containing Export Utility JAR Files（エクスポートユーティリティを含むフォルダ）：エクスポートユーティリティを含むフォルダ `.jar` ファイル
SNM2Devices - WMS/SMS/AMS ストレージ	WMS / SMS / AMS ストレージのデバイスリスト。各ストレージには以下が必要です。 • Array’s IP：ストレージのIPアドレス • Storage Navigator CLI Path：SNM2 CLIパス • Account Authentication Valid：有効なアカウント認証を選択する場合に選択します • User Name：ストレージのユーザ名 • Password：ストレージのパスワード
「 Tuning Manager 」を「 Performance 」に選択します	パフォーマンスに合わせてTuning Managerを選択し、他のパフォーマンスオプションを上書きします
Tuning Manager Host （ホストのチューニング）	Tuning Manager の IP アドレスまたは完全修飾ドメイン名
Tuning Manager ポート	Tuning Manager に使用するポート
Tuning Manager のユーザ名	Tuning Manager のユーザ名

Tuning Manager パスワード	Tuning Managerのパスワード

HDS USP、USP V、およびVSPでは、どのディスクも複数のアレイグループに属することができます。

高度な設定

フィールド	説明
HiCommand Server ポート	HiCommand Device Manager に使用するポート
HTTPs が有効です	HTTPS を有効にする場合に選択します
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
「除外」または「含める」を選択してリストを指定します	以下のリストにあるアレイをデータの収集時に対象に含めるか除外するかを指定します
デバイスを除外または含める	対象に含めるか除外するデバイスの ID またはアレイ名をカンマで区切ったリスト
ホストマネージャを照会します	ホストマネージャを照会する場合に選択します
HTTPタイムアウト（秒）	HTTP接続タイムアウト（デフォルトは60秒）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
エクスポートのタイムアウト（秒）	エクスポートユーティリティのタイムアウト（デフォルトは300秒）

Hitachi Ops Center データコレクタ

このデータコレクタは、 Hitachi Ops Center の統合されたアプリケーションスイートを使用して、複数のストレージデバイスのインベントリとパフォーマンスのデータにアクセスします。インベントリと容量を検出するには、 Operations Center のインストールに「 Common Services 」と「 Administrator 」の両方のコンポーネントを含める必要があります。パフォーマンス収集では、さらに「 Analyzer 」を導入する必要があります。

用語集

OnCommand Insightはこのデータコレクタから次のインベントリ情報を取得します。取得したアセットのタイプごとに、そのアセットに使用される最も一般的な用語が表示されます。このデータコレクタを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	**OnCommand Insight** 期間
ストレージシステム	ストレージ
ボリューム	ボリューム
パリティグループ	ストレージプール（ RAID ）、ディスクグループ
ディスク	ディスク
ストレージプール	ストレージプール（シン、スナップ）
外部パリティグループ	ストレージプール（バックエンド）、ディスクグループ
ポート	ストレージノード→コントローラノード→ポートの順にクリックします
ホストグループ	ボリュームのマッピングとマスキング
ボリュームペア	ストレージ同期

注：これらは一般的な用語の対応のみを示したものであり、このデータコレクタのすべてのケースを表しているわけではありません。

インベントリの要件

インベントリデータを収集するには、次の情報が必要です。

- 「Common Services」コンポーネントをホストするOps CenterサーバのIPアドレスまたはホスト名
- ルート/ sysadminユーザアカウントとパスワード。Ops Centerコンポーネントをホストするすべてのサーバに存在します。HDSでは、Ops Center 10.8以降まで、LDAP/SSOユーザによるREST APIサポートは実装されていませんでした

パフォーマンス要件

パフォーマンスデータを収集するには、次の要件を満たしている必要があります。

- HDS Ops Centerの「Analyzer」モジュールがインストールされている必要があります
- ストレージアレイがOps Centerの「Analyzer」モジュールにデータを供給している必要があります

設定

フィールド	説明
Hitachi Ops Center の IP アドレス	「 Common Services 」コンポーネントをホストする Ops Center サーバの IP アドレスまたは完全修飾ドメイン名
ユーザ名	Ops Center サーバのユーザ名。
パスワード	Ops Center サーバのパスワード。

高度な設定

フィールド	説明

接続タイプ	デフォルトは HTTPS （ポート 443 ）です
TCP ポートを上書きします	デフォルト以外の場合に使用するポートを指定します
インベントリポーリング間隔（分）	インベントリのポーリング間隔。デフォルトは 40. です。
「除外」または「含める」を選択してリストを指定します	下のリストに表示されたアレイをデータの収集時に対象に含めるか除外するかを指定します。
デバイスリストをフィルタリングします	対象に含めるか除外するデバイスのシリアル番号をカンマで区切ったリスト
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔デフォルトは 300. です。

HDSストレージ

HDSストレージアセットのランディングページに記載されているオブジェクトや参照に適用される用語。

HDSストレージの用語

HDS ストレージアセットランディングページにあるオブジェクトや参考資料に関連する用語を次に示します。これらの用語の多くは、他のデータコレクタにも適用されます。

- Name — GetStorageArray XML API呼び出しを介してHDS HiCommand Device Managerの「name」属性から直接取得されます
- Model - GetStorageArray XML API呼び出しを介してHDS HiCommand Device Managerの「arrayType」属性から直接取得されます
- ベンダー-- HDS
- Family - GetStorageArray XML API呼び出しを介してHDS HiCommand Device Managerの「arrayFamily」属性から直接取得されます
- IP --アレイの管理IPアドレスであり’アレイ上のすべてのIPアドレスを網羅したリストではありません
- Raw Capacity（物理容量）--ディスクロールに関係なく、このシステムのすべてのディスクの合計容量を表す2進数の値。

HITACHI Storage Poolの略

HDSストレージプールのアセットランディングページに記載されているオブジェクトや参照に適用される用語。

HDSストレージプールの用語

HDS ストレージプールのアセットランディングページにあるオブジェクトや参照に関連する用語を次に示します。これらの用語の多くは、他のデータコレクタにも適用されます。

- タイプ：値は次のいずれかになります。
  - リザーブ(Reserved)--このプールがデータボリューム以外の目的(ジャーナリング’スナップショットなど)専用の場合

- Thin Provisioning：HDPプールの場合
- RAIDグループ：いくつかの理由により’これらが表示されない可能性があります

  OCIでは、容量がどのようなコストであっても二重にカウントされることは避けたいと強く考えているHDS では、通常、ディスクから RAID グループを作成し、それらの RAID グループにプールボリュームを作成し、それらのプールボリュームからプール（多くの場合 HDP を作成しますが、特別な目的にすることもあります）を構築する必要があります。基盤となるRAIDグループとプールの両方について報告された場合、物理容量の合計がディスクの合計を大幅に超えてしまいます。

OCIのHDS HiCommandデータコレクタは、プールボリュームの容量に応じてRAIDグループのサイズを任意に縮小します。そのため、OCIでRAIDグループがまったく報告されない場合があります。また、作成されたRAIDグループにはOCI Web UIには表示されず、OCI Data Warehouse（DWH）にも表示されるようにフラグが設定されます。これらの決定の目的は、ほとんどのユーザーが気にしないことでUIが乱雑にならないようにすることです。HDSアレイに50MBの空き容量があるRAIDグループがある場合、その空き容量を有意義な結果に使用することはおそらくできません。

- HDS プールは 1 つの特定のノードに関連付けられないため、ノードなし
- Redundancy - プールの RAID レベル。複数の RAID タイプで構成される HDP プールには、複数の値が含まれる可能性があります
- Capacity % - プールでデータ使用に使用されている割合。プールの使用済み GB と合計論理 GB サイズです
- オーバーコミット容量-「このプールの論理容量は、プールの論理容量をこの割合で超過した論理ボリュームの合計により、この割合でオーバーサブスクライブされています」を示す派生値。
- snapshot - このプールでの Snapshot の使用用にリザーブされている容量が表示されます

HDSストレージノード

HDSストレージノードのアセットランディングページに記載されているオブジェクトや参照に適用される用語。

HDSストレージノードの用語

HDS ストレージノードのアセットランディングページにあるオブジェクトや参照に関連する用語を次に示します。これらの用語の多くは、他のデータコレクタにも適用されます。

- 名前—モノリシックアレイ上のフロントエンドダイレクタ(FED)またはチャネルアダプタの名前’またはモジュラーアレイ上のコントローラの名前1 つの HDS アレイに 2 つ以上のストレージノードがある
- ボリューム—ボリュームテーブルには、このストレージノードが所有するポートにマッピングされているボリュームが表示されます

Hitachi Ops Center データコレクタ

このデータコレクタは、 Hitachi Ops Center の統合されたアプリケーションスイートを使用して、複数のストレージデバイスのインベントリとパフォーマンスのデータにアクセスします。インベントリと容量を検出するには、 Operations Center のインストールに「 Common Services 」と「 Administrator 」の両方のコンポーネントを含める必要があります。パフォーマンス収集では、さらに「 Analyzer 」を導入する必要があります。

用語集

OnCommand Insightはこのデータコレクタから次のインベントリ情報を取得します。取得したアセットのタイプごとに、そのアセットに使用される最も一般的な用語が表示されます。このデータコレクタを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	**OnCommand Insight** 期間
ストレージシステム	ストレージ
ボリューム	ボリューム
パリティグループ	ストレージプール（ RAID ）、ディスクグループ
ディスク	ディスク
ストレージプール	ストレージプール（シン、スナップ）
外部パリティグループ	ストレージプール（バックエンド）、ディスクグループ
ポート	ストレージノード→コントローラノード→ポートの順にクリックします
ホストグループ	ボリュームのマッピングとマスキング
ボリュームペア	ストレージ同期

注：これらは一般的な用語の対応のみを示したものであり、このデータコレクタのすべてのケースを表しているわけではありません。

インベントリの要件

インベントリデータを収集するには、次の情報が必要です。

- 「Common Services」コンポーネントをホストするOps CenterサーバのIPアドレスまたはホスト名
- ルート/ sysadminユーザアカウントとパスワード。Ops Centerコンポーネントをホストするすべてのサーバに存在します。HDSでは、Ops Center 10.8以降まで、LDAP/SSOユーザによるREST APIサポートは実装されていませんでした

パフォーマンス要件

パフォーマンスデータを収集するには、次の要件を満たしている必要があります。

- HDS Ops Centerの「Analyzer」モジュールがインストールされている必要があります
- ストレージアレイがOps Centerの「Analyzer」モジュールにデータを供給している必要があります

設定

フィールド	説明
Hitachi Ops Center の IP アドレス	「 Common Services 」コンポーネントをホストする Ops Center サーバの IP アドレスまたは完全修飾ドメイン名
ユーザ名	Ops Center サーバのユーザ名。

フィールド	説明
パスワード	Ops Center サーバのパスワード。

高度な設定

フィールド	説明
接続タイプ	デフォルトは HTTPS （ポート 443 ）です
TCP ポートを上書きします	デフォルト以外の場合に使用するポートを指定します
インベントリポーリング間隔（分）	インベントリのポーリング間隔。デフォルトは 40. です。
「除外」または「含める」を選択してリストを指定します	下のリストに表示されたアレイをデータの収集時に対象に含めるか除外するかを指定します。
デバイスリストをフィルタリングします	対象に含めるか除外するデバイスのシリアル番号をカンマで区切ったリスト
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔デフォルトは 300. です。

HDS NAS（**HNAS**）データソース

HDS NAS（HNAS）データソースは、HDS NASクラスタの検出をサポートするためのインベントリおよび設定のデータソースです。Insightでは、NFS共有とCIFS共有、ファイルシステム（Insightの内部ボリューム）、スパン（Insightのストレージプール）の検出がサポートされています。

このデータソースはSSHベースであるため、ホストするAcquisition Unitから、HNAS自体またはクラスタが接続されているSystems Management Unit（SMU）のTCP 22へのSSHセッションを開始できる必要があります。

用語集

OnCommand Insight では、HNASデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
階層	ディスクグループ
クラスタ	ストレージ
ノード	ストレージノード
スパン（ Span ）	ストレージプール
File System の略	内部ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

このデータソースを設定して使用するための要件は次のとおりです。

- デバイスの IP アドレス
- ポート 22 、 SSH プロトコル
- ユーザ名とパスワードの権限レベル： Supervisor
- 注：このデータコレクタはSSHベースなので、ホストするAUは、HNAS自体またはクラスタが接続されているSystems Management Unit（SMU）のTCP 22へのSSHセッションを開始できる必要があります。

このデータコレクタはSSHベースなので、ホストするAUは、HNAS自体またはクラスタが接続されているSystems Management Unit（SMU）のTCP 22へのSSHセッションを開始できる必要があります。

設定

フィールド	説明
HNAS ホスト	HNAS 管理ホストの IP アドレスまたは完全修飾ドメイン名
ユーザ名	HNAS CLI のユーザ名
パスワード	HNAS CLI のパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは30分）
SSHバナー待機タイムアウト（秒）	SSHバナーのタイムアウト（デフォルトは15秒）
SSHコマンドタイムアウト（秒）	SSHコマンドのタイムアウト（デフォルトは30秒）

HP CommandView AEデータソース

HP CommandView Advanced Edition（AE）およびCommandView AE CLI/SMI（AE Lite）データソースでは、CommandView（HiCommand）Device Managerサーバからのインベントリとパフォーマンスがサポートされます。

用語集

OnCommand Insight では、HP CommandView AEおよびAE Liteデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
PDEV	ディスク
ジャーナルプール	ディスクグループ
ストレージアレイ	ストレージ
Port Controller の略	ストレージノード
アレイグループ 'DP プール	ストレージプール
論理ユニット、 LDEV	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

インベントリの要件

- HiCommand Device Manager サーバの IP アドレス
- CommandView AEソフトウェアおよびピアの権限の読み取り専用のユーザ名とパスワード
- CommandView AE Liteバージョンのデバイスマネージャには、CLIのみがライセンスされています
- ポート要件： 2001

パフォーマンス要件

- HDS USP 、 USP V 、および VSP のパフォーマンス
  - Performance Monitor のライセンスが必要です。
  - 監視スイッチが有効になっている必要があります。
  - エクスポートツール (`Export.exe`）をOnCommand Insight サーバにコピーする必要があります。
  - エクスポートツールのバージョンとターゲットアレイのマイクロコードのバージョンが一致している必要があります。
- HDS AMSのパフォーマンス
  - Performance Monitorのライセンスが必要です。
  - Storage Navigator Modular 2（SNM2）CLIユーティリティがOnCommand Insight サーバにインストールされている必要があります。
  - 次のコマンドを使用して、OnCommand Insight でパフォーマンスを取得する必要があるAMS、

WMS、SMSのすべてのストレージアレイを登録する必要があります。

- 登録したすべてのアレイがこのコマンドの出力に表示されていることを確認する必要があります。`auunitref.exe`。

設定

* フィールド *	* 概要 *
HiCommand サーバ	HiCommand Device Manager サーバの IP アドレスまたは完全修飾ドメイン名
ユーザ名	HiCommand Device Manager サーバのユーザ名
パスワード	HiCommand Device Manager サーバのパスワード
デバイス- USP、USP V、VSP/R600ストレージ	VSP G1000 （ R800 ）、 VSP （ R700 ）、 HUS VM （ HM700 ）、および USP ストレージのデバイスリスト。各ストレージには以下が必要です。 • Array’s IP：ストレージのIPアドレス • User Name：ストレージのユーザ名 • Password：ストレージのパスワード • Folder Containing Export Utility JAR Files（エクスポートユーティリティを含むフォルダ）：エクスポートユーティリティを含むフォルダ `.jar` ファイル
SNM2Devices - WMS/SMS/AMS ストレージ	WMS / SMS / AMS ストレージのデバイスリスト。各ストレージには以下が必要です。 • Array’s IP：ストレージのIPアドレス • Storage Navigator CLI Path：SNM2 CLIパス • Account Authentication Valid：有効なアカウント認証を選択する場合に選択します • User Name：ストレージのユーザ名 • Password：ストレージのパスワード
「 Tuning Manager 」を「 Performance 」に選択します	パフォーマンスに合わせてTuning Managerを選択し、他のパフォーマンスオプションを上書きします
Tuning Manager Host （ホストのチューニング）	Tuning Manager の IP アドレスまたは完全修飾ドメイン名
Tuning Manager ポート	Tuning Manager に使用するポート

Tuning Manager のユーザ名	Tuning Manager のユーザ名
Tuning Manager パスワード	Tuning Managerのパスワード

HDS USP、USP V、およびVSPでは、どのディスクも複数のアレイグループに属することができます。

高度な設定

フィールド	説明
HiCommand Server ポート	HiCommand Device Manager に使用するポート
HTTPs が有効です	HTTPS を有効にする場合に選択します
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
「除外」または「含める」を選択してリストを指定します	以下のリストにあるアレイをデータの収集時に対象に含めるか除外するかを指定します
デバイスを除外または含める	対象に含めるか除外するデバイスの ID またはアレイ名をカンマで区切ったリスト
ホストマネージャを照会します	ホストマネージャを照会する場合に選択します
HTTPタイムアウト（秒）	HTTP接続タイムアウト（デフォルトは60秒）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
エクスポートのタイムアウト（秒）	エクスポートユーティリティのタイムアウト（デフォルトは300秒）

HP EVA Storageデータソース

EVA Storage（SSSU）データソースを設定するには、Command View（CV）サーバのIPアドレス、およびCVソフトウェアに対する_read-only_usernameとパスワードが必要です。ユーザーはCVソフトウェアで定義する必要があります。

用語集

OnCommand Insight では、HP EVAデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
ディスクグループ	ディスクグループ（モデル化されていません）
ストレージセル	ストレージ
仮想ディスク	ストレージプール
仮想ディスク	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

インベントリの要件

- CVサーバのIPアドレス
- CVソフトウェアに対する読み取り専用のユーザ名とパスワード。ユーザーはCVソフトウェアで定義する必要があります。
- OnCommand Insight サーバ/ RAUにインストールされているサードパーティ製ソフトウェア：`sssu.exe`。。 `sssu.exe` バージョンはCVバージョンに対応している必要があります。
- アクセスの検証：を実行します `sssu.exe` ユーザ名とパスワードを使用したコマンド。

パフォーマンス要件

HP StorageWorks Command View EVAソフトウェアスイートがOnCommand Insight サーバーにインストールされている必要があります。または、EVAサーバにRemote Acquisition Unit（RAU）をインストールすることもできます。

1. HP StorageWorks Command View EVAソフトウェアスイートをOnCommand Insight サーバーにインストールするか、Remote Acquisition UnitをCommand View EVAサーバーにインストールします。
2. を探します `evaperf.exe` コマンドを実行します例： `c:\Program Files\Hewlett-Packard\EVA Performance Monitor\`
3. Command ViewサーバのIPを使用して、次の手順を実行します。
   a. このコマンドを実行します。860はデフォルトのポートです `Evaperf.exe server <Command View Server IP\> 860 <username\>`
   b. パスワードプロンプトでCommand Viewサーバのパスワードを入力します。

      これにより、コマンドラインプロンプトが表示され、それ以外は表示されません。
4. を実行してセットアップを確認します `evaperf.exe ls`。

   Command Viewサーバで管理されているアレイまたはコントローラのリストが表示されます。各行はEVAアレイのコントローラを示しています。

設定

* フィールド *	* 概要 *
CommandView Serverの略	EVA Storage ManagerのIPアドレスまたは完全修飾ドメイン名
ユーザ名	Command View Managerのユーザ名。名前はCommand Viewで定義する必要があります。
パスワード	Command View Managerのパスワード。
Performance User Nameの略	パフォーマンスを向上させるために、Command View Managerのユーザ名。名前はCommand Viewで定義する必要があります。
パフォーマンスパスワード	パフォーマンスを向上させるために、Command View Managerに使用するパスワード。

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
CLIホーム	CLIホームディレクトリのフルパス名 `sssu.exe` があります
インベントリ除外デバイス	対象に含めるデバイス名をカンマで区切ったリスト
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
Performance CLI Homeの略	アレイパフォーマンスの場合は、sssu.exeが格納されているCLIホームディレクトリの完全なパス名。アクセスを検証するには、を実行します `sssu.exe`
コマンドタイムアウト（秒）	`evaperf` コマンド待機タイムアウト（デフォルトは600秒）
Performance Exclude Devicesを参照してください	パフォーマンスデータの収集対象から除外するデバイスの名前をカンマで区切ったリスト

HPE Nimbleデータソース

HPE Nimble Data Collector は、 HPE Nimble ストレージアレイのインベントリとパフォ

ーマンスのデータをサポートしています。

用語集

OnCommand Insight では、HPE Nimbleデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
配列	ストレージ
ディスク	ディスク
プール	ストレージプール
ボリューム	ボリューム
イニシエータ	ストレージホストのエイリアス
コントローラ	ストレージノード
Fibre Channel インターフェイス	コントローラ

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- アレイがインストールおよび設定されていて、クライアントから完全修飾ドメイン名（ FQDN ）またはアレイ管理 IP アドレスを使用して到達できる必要があります。
- アレイで NimbleOS 2.3.x 以降が実行されている必要があります。
- アレイに対する有効なユーザ名とパスワードが必要です。
- アレイのポート 5392 が開いている必要があります。

設定

* フィールド *	* 概要 *
アレイ管理 IP アドレス	Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）またはアレイ管理 IP アドレスです。
ユーザ名	Nimble アレイのユーザ名
パスワード	Nimble アレイのパスワード

高度な設定

* フィールド *	* 概要 *
ポート	Nimble REST API が使用するポート。デフォルトは 5392. です。
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）

注：デフォルトのパフォーマンスのポーリング間隔は 300 秒で、変更することはできません。Nimble でサポートされている唯一の間隔はこれです。

Huawei OceanStorデータソース

OnCommand Insight では、Huawei OceanStor（REST / HTTPS）データソースを使用して、Huawei OceanStorストレージのインベントリを検出します。

用語集

OnCommand Insight は、Huawei OceanStorから次のインベントリおよびパフォーマンス情報を取得します。OnCommand Insight で取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータコレクタを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	OnCommand Insight 期間
ストレージプール	ストレージプール
File System の略	内部ボリューム
コントローラ	ストレージノード
FC ポート（マッピング済み）	ボリュームマップ
ホスト FC イニシエータ（マッピング済み）	ボリュームマスク
NFS / CIFS 共有	共有
共有	iSCSI ターゲットノード
iSCSI リンクイニシエータ	iSCSI イニシエータノード
ディスク	ディスク
LUN	ボリューム

要件

このデータコレクタを設定して使用するための要件は次のとおりです。

- デバイスIP
- OceanStor デバイスマネージャにアクセスするためのクレデンシャル
- ポート 8088 が使用可能であることが必要です

設定

フィールド	説明
OceanStor Host IP アドレス	OceanStor Device Manager の IP アドレスまたは完全修飾ドメイン名
ユーザ名	OceanStor Device Manager へのログインに使用するユーザ名
パスワード	OceanStor Device Manager へのログインに使用するパスワード

高度な設定

フィールド	説明
TCP ポート	OceanStor Device Managerへの接続に使用するTCPポート（デフォルトは8088）
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）

IBM Cleversafeデータソース

このデータソースは、IBM Cleversafeのインベントリとパフォーマンスのデータを収集します。

要件

このデータソースの設定に関する要件は次のとおりです。

- マネージャのIPアドレスまたはホスト名
- 同じのユーザ名とパスワード
- ポート 9440

設定

フィールド	説明
Cleversafeマネージャのホスト名またはIPアドレス	CleverSafeデバイスのホストIPアドレス
ユーザ名	Cleversafeへのログインに使用する名前
パスワード	Cleversafeへのログインに使用するパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	デフォルトは 60 分です
HTTP接続タイムアウト）	デフォルトは60秒です

IBM DSデータソース

IBM DS（CLI）データソースでサポートされるのは、DS6xxxデバイスとDS8xxxデバイスのみです。DS3xxx、DS4xxx、およびDS5xxxのデバイスは、NetApp E-Seriesデータソースでサポートされます。サポートされるモデルとファームウェアバージョンについては、Insightデータソースサポートマトリックスを参照してください。

用語集

OnCommand Insight では、IBM DSデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスクドライブモジュール	ディスク
ストレージイメージ	ストレージ
エクステントプール	ストレージプール
固定ブロックボリューム	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- 各 DS アレイの IP アドレス
- ストレージの表示名はオプションであり、外観上のみです
- 各 DS アレイの読み取り専用のユーザ名とパスワード
- サードパーティ製ソフトウェアをInsightサーバにインストール：IBM dscli
- アクセスの検証：を実行します `dscli` ユーザ名とパスワードを使用したコマンド
- ポートの要件： 80 、 443 、および 1750

設定

フィールド	説明
DSストレージ	DS Storage HostのIPアドレスまたは完全修飾ドメイン名
ユーザ名	DS CLIに使用する名前
パスワード	DS CLIのパスワード
実行可能ファイルのdscli.exeパス	への完全パス `dscli.exe`ユーティリティ。

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
ストレージ表示名	IBM DS ストレージアレイの名前
インベントリ除外デバイス	インベントリ収集の対象から除外するデバイスのシリアル番号をカンマで区切ったリスト
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
パフォーマンスフィルタタイプ	Include ：リストのデバイスからのみデータを収集します。Exclude ：リストのデバイスからデータを収集しません
パフォーマンスフィルタのデバイスリスト	パフォーマンス収集の対象に含めるか除外するデバイスの ID をカンマで区切ったリスト

IBM PowerVMデータソース

IBM PowerVM（SSH）データソースは、ハードウェア管理コンソール（HMC）で管理されるIBM POWERハードウェアインスタンスで実行されている仮想パーティションに関する情報を収集します。このデータソースを設定するには、SSHを使用してHMCにログインするためのユーザ名、およびHMCの設定に対する表示レベルの権限が必要です。

用語集

OnCommand Insight では、IBM PowerVMデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
hdisk	仮想ディスク
Managed System の略	ホスト
LPAR 、 VIO サーバ	仮想マシン
ボリュームグループ	データストア
物理ボリューム	LUN

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ハードウェア管理コンソール（ HMC ）の IP アドレス
- SSH経由でHMCにアクセスするためのユーザ名とパスワード
- ポート要件は SSH-22 です
- すべての管理システムおよび論理パーティションセキュリティドメインに対する表示権限

  ユーザには、 HMC の設定に対する表示権限も必要であり、 HMC コンソールセキュリティグループの VPD 情報を収集できる必要があります。ユーザーは、論理パーティションセキュリティグループの Virtual IO Server コマンドへのアクセスも許可されている必要があります。オペレータのロールから開始し、すべてのロールを削除することを推奨します。HMC の読み取り専用ユーザには、 AIX ホストでプロキシされたコマンドを実行する権限はありません。

- IBM のベストプラクティスは、 2 台以上の HMI でデバイスを監視することです。これにより、原因 OnCommand Insight で重複したデバイスが報告される場合があるため、このデータコレクタの詳細設定の [デバイスを除外する] リストに冗長デバイスを追加することを強くお勧めします。

設定

* フィールド *	* 概要 *
ハードウェア管理コンソール（HMC）のアドレス	PowerVM ハードウェア管理コンソールの IP アドレスまたは完全修飾ドメイン名
HMC ユーザ	ハードウェア管理コンソールのユーザ名
パスワード	ハードウェア管理コンソールのパスワード

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
SSH ポート	PowerVM への SSH に使用するポート
SSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは600秒）
再試行回数	インベントリの再試行回数
デバイスを除外します	対象から除外するデバイスの ID または表示名をカンマで区切ったリスト

IBM SVCデータソース

IBM SVCデータソースは、SSHを使用してインベントリとパフォーマンスのデータを収集し、SVCオペレーティングシステムを実行するさまざまなデバイスをサポートします。サポートされるデバイスには、 SVC 、 v7000 、 v5000 、 v3700 などのモデルが含まれます。サポートされるモデルとファームウェアバージョンについては、Insightデータソースサポートマトリックスを参照してください。

用語集

OnCommand Insight では、IBM SVCデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ドライブ	ディスク
クラスタ	ストレージ

ノード	ストレージノード
mdisk グループ	ストレージプール
仮想ディスク	ボリューム
mdisk	バックエンド LUN

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

インベントリの要件

- 各 SVC クラスタの IP アドレス
- ポート 22 を使用できます
- 公開鍵と秘密鍵のペア。Insightで生成するか、SVCですでに使用しているキーペアを再利用します

  既存のキーペアを再利用する場合は、それらのキーペアをPutty形式からOpenSSH形式に変換する必要があります。

- 公開鍵をSVCクラスタにインストールします
- 秘密鍵をデータソースで識別する必要があります
- アクセスの検証：開く `ssh` 秘密鍵を使用したSVCクラスタへのセッション

他社製ソフトウェアをインストールする必要はありません。

パフォーマンス要件

- SVC コンソールはすべての SVC クラスタに必須であり、 SVC 検出基本パッケージに必要です。
- クラスタノードから構成ノードにパフォーマンスデータファイルをコピーする場合にのみ必要な管理アクセスレベル。

  このアクセスレベルはSVC基本検出パッケージには必要ないため、SVC基本ユーザが正常に機能しない場合があります。

- ポート22が必要です
- このユーザのSSHキーと公開鍵を生成し、Acquisition Unitからアクセスできるように秘密鍵を格納する必要があります。SVC基本ユーザに適切な権限があれば、同じユーザとキーが機能します。インベントリデータとパフォーマンスデータに同じSSHキーを使用できます。
- データ収集を有効にするには、SSHを使用してSVCクラスタに接続し、次のコマンドを実行します。
  `svctask startstats -interval 1`

  または、SVC管理ユーザインターフェイスを使用してデータ収集を有効にします。

親シリアル番号の説明

従来、Insightでは、ストレージアレイのシリアル番号や個 々 のストレージノードのシリアル番号をレポートすることができました。ただし、一部のストレージアレイアーキテクチャはこれに適切に対応していません。SVCクラスタは1~4台のアプライアンスで構成でき、各アプライアンスには2つのノードがあります。アプライアンス自体のシリアル番号がある場合、そのシリアル番号はクラスタのシリアル番号でもノードのシリアル番号でもありません。

IBM SVCアレイのストレージノードオブジェクトの「Parent Serial Number」属性は、個 々 のノードが大規模なクラスタの一部にすぎない中間アプライアンス/エンクロージャ内に配置されている場合に適切に設定されます。

設定

* フィールド *	* 概要 *
クラスタ/秒IP	SVCストレージの完全修飾ドメイン名のIPアドレス
クレデンシャルタイプを指定するには、「 Password 」または「 OpenSSH Key File 」を選択してください	SSH経由でデバイスに接続するために使用するクレデンシャルタイプ
Inventory User Name の略	SVC CLI のユーザ名
Inventory Password （インベントリパスワード）	SVC CLI のパスワード
Inventory Private Key への完全パス	インベントリの秘密鍵ファイルの完全パス
Performance User Nameの略	パフォーマンス収集用のSVC CLIのユーザ名
パフォーマンスパスワード	パフォーマンス収集に使用するSVC CLIのパスワード
パフォーマンス秘密鍵への完全パス	パフォーマンスの秘密鍵ファイルの完全パス

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
デバイスを除外します	インベントリ収集の対象から除外するデバイスのIDをカンマで区切ったリスト
SSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは200秒）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

Performance Exclude Devicesを参照してください	パフォーマンス収集の対象から除外するデバイスのIDをカンマで区切ったリスト
パフォーマンスSSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは200秒）
ダンプされた統計情報ファイルをクリーンアップする場合	ダンプされた統計ファイルをクリーンアップする場合に選択します

IBM Tivoli Monitoringデータソース

このデータソースは、ファイルシステム利用率のみに使用されます。Tivoli Monitoringデータベース（Tivoli Monitoring Data Warehouseとも呼ばれます）と直接通信します。OracleデータベースとDB2データベースがサポートされています。

Oracleのエラー・メッセージ

このデータコレクタは、OnCommand Insight 7.3.11以降では使用できなくなりました。

SIDを指定して接続を試行したときに「ORA-12154」を含むエラーメッセージが表示される場合は、Oracle DBネットワークサービスの設定を再確認してください。アクセス設定で完全修飾ホスト名（「names.default_domain」など）が指定されている場合は、SIDフィールドに完全修飾サービス名を挿入してみてください。簡単な例としては、SIDへの接続があります `testdb` が失敗しており、Oracleの設定でドメインが指定されています`company.com`。ベースSIDの代わりに次の文字列を使用して接続を試行できます。`testdb.company.com`。

設定

フィールド	説明
Tivoli Monitoring Database IPの略	Tivoli MonitoringサーバのIPアドレスまたは完全修飾ドメイン名
ユーザ名	Tivoli Monitoringサーバのユーザ名
パスワード	Tivoli Monitoringサーバのパスワード

高度な設定

フィールド	説明
Tivoli Monitoringデータベースポート	Tivoliモニタリングデータベースに使用するポート
Oracle SIDまたはDB2データベース名	OracleリスナーサービスIDまたはDB2データベース名

インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
使用するデータベースドライバ	使用するデータベースドライバを選択します
データベースへの接続に使用されるプロトコル	データベースへの接続に使用されるプロトコル
データベーススキーマ	データベーススキーマを入力します

IBM TotalStorage DS4000データソース

このデータソースは、インベントリとパフォーマンスの情報を収集します。可能な構成は2つ（ファームウェア6.xと7.x以降）で、値はどちらも同じです。APIでボリュームデータの統計を収集します。

設定

* フィールド *	* 概要 *
アレイSANtricity コントローラのIPをカンマで区切ったリスト	コントローラのIPアドレスまたは完全修飾ドメイン名をカンマで区切って指定します

要件

- DS5 または FAStT の各アレイの IP アドレス
- アクセスの検証：各アレイの両方のコントローラのIPアドレスにpingを実行します。

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは30分）
パフォーマンスポーリング間隔（最大3600秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

IBM XIVデータソース

IBM XIV（CLI）データソースのインベントリの収集は、XIVコマンドラインインターフェイスを使用して実行します。XIVのパフォーマンスは、ポート5989でSMI-Sプロバイダを実行するXIVアレイにSMI-Sを呼び出して実現されます。

用語集

OnCommand Insight では、IBM XIVデータソースから次のインベントリ情報を取得します。Insightで取得した

アセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
ストレージシステム	ストレージ
ストレージプール	ストレージプール
ボリューム	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ポート要件： TCP ポート 7778
- XIV管理インターフェイスのIPアドレス
- 読み取り専用のユーザ名とパスワード
- XIV CLIがInsight ServerまたはRAUにインストールされている必要があります
- アクセスの検証：Insight Serverから、ユーザ名とパスワードを使用してXIVのユーザインターフェイスにログインします。

設定

* フィールド *	* 概要 *
IP アドレス	XIVストレージのIPアドレスまたは完全修飾ドメイン名
ユーザ名	XIV ストレージのユーザ名
パスワード	XIV ストレージのパスワード
XIV CLIディレクトリの完全パス	XIV CLIディレクトリの完全パス

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）

CLIプロセス待機タイムアウト（ミリ秒）	CLIプロセスのタイムアウト（デフォルトは7200000ミリ秒）
SMI-SホストIP	SMI-Sプロバイダホストの IPアドレス
SMI-Sポート	SMI-Sプロバイダホストが使用するポート
SMI-S プロトコル	SMI-S プロバイダへの接続に使用するプロトコル
SMI-Sネームスペース	SMI-Sネームスペース
ユーザ名	SMI-S プロバイダホストのユーザ名
パスワード	SMI-S プロバイダホストのパスワード
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）
SMI-S接続の再試行回数	SMI-S接続の再試行回数

Infinidat InfiniBoxデータソース

Infinidat InfiniBox（HTTP）データソースは、Infinidat InfiniBoxストレージから情報を収集するために使用されます。InfiniBox管理ノードにアクセスする必要があります。

用語集

OnCommand Insight では、InfiniBoxデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ドライブ	ディスク
InfiniBox	ストレージ
ノード	ストレージノード
プール	ストレージプール
ボリューム	ボリューム
FC ポート	ポート

ファイルシステム	内部ボリューム
ファイルシステム	ファイル共有
ファイルシステムエクスポート	共有

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

設定

フィールド	説明
InfiniBox ホスト	InfiniBox 管理ノードの IP アドレスまたは完全修飾ドメイン名
ユーザ名	InfiniBox 管理ノードのユーザ名
パスワード	InfiniBox 管理ノードのパスワード

高度な設定

フィールド	説明
TCP ポート	InfiniBoxサーバへの接続に使用するTCPポート（デフォルトは443）
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
接続タイムアウト	接続タイムアウト（デフォルトは60秒）

Microsoft Azure computeデータソース

OnCommand Insightsは、Azureコンピューティングデータコレクタを使用して、Azureコンピューティングインスタンスからインベントリとパフォーマンスのデータを取得します。

要件

このデータコレクタを設定するには、次の情報が必要です。

- ポート要件： 443 HTTPS
- Azure Management Rest IP （ management.azure.com ）

- Azureサービスプリンシパルアプリケーション（クライアント）ID（ユーザアカウント）
- Azureサービスプリンシパル認証キー（ユーザパスワード）

Insight Discovery用のAzureアカウントをセットアップする必要があります。アカウントを適切に設定してAzureにアプリケーションを登録すると、InsightでAzureインスタンスを検出するために必要なクレデンシャルが取得されます。検出用アカウントの設定方法については、https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portalを参照してください

設定

次の表に従って、データソースフィールドにデータを入力します。

フィールド	説明
Azure サービスプリンシパルアプリケーション（クライアント） ID （リーダーのロールが必要）	Azure へのサインイン IDリーダーの役割アクセスが必要です。
Azure テナント ID	Microsoft テナント ID
Azure サービスプリンシパルの認証キー	ログイン認証キー
Microsoft が API リクエストを請求することを理解しています	これをチェックして、 Insight のポーリングで作成された API 要求を Microsoft から課金することを理解していることを確認します。

詳細設定

次の表に従って、データソースフィールドにデータを入力します。

フィールド	説明
インベントリポーリング間隔（分）	デフォルトは 60 です。
「除外」または「含める」を選択して、タグによる VM のフィルタリングに適用します	データの収集時にタグを使用して VM を含めるか除外するかを指定します。``Include"を選択した場合、Tag Keyフィールドを空にすることはできません。
VM をフィルタするタグキーと値	+ タグのフィルタ * をクリックして、 VM のキーとタグの値に一致するキーと値をフィルタリングして、対象に含める / 除外する VM （および関連ディスク）を選択します。タグキーは必須です。タグ値はオプションです。タグ値が空の場合、タグキーと一致する限り、 VM はフィルタリングされます。
パフォーマンスポーリング間隔（秒）	

Azure NetApp Files データソース

このデータソースは、Azure NetApp Files （ANF）のインベントリとパフォーマンスのデータを取得します。

要件

このデータソースの設定に関する要件は次のとおりです。

- ポート要件： 443 HTTPS
- Azure Management Rest IP （ management.azure.com ）
- Azureサービスプリンシパルアプリケーション（クライアント）ID（ユーザアカウント）
- Azure Service Principal認証キー（ユーザパスワード）
- Cloud Insights 検出用の Azure アカウントを設定する必要があります。

  アカウントを適切に設定し、アプリケーションを Azure に登録すると、 Cloud Insights で Azure インスタンスを検出するために必要なクレデンシャルが付与されます。次のリンクでは、検出用のアカウントを設定する方法について説明します。

  https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

設定

フィールド	説明
Azureサービスプリンシパルアプリケーション（クライアント）ID	Azure へのサインイン ID
Azure テナント ID	Azure テナント ID
Azure サービスプリンシパルの認証キー	ログイン認証キー
Microsoft が API リクエストを請求することを理解しています	これをチェックして、 Insight のポーリングで作成された API 要求を Microsoft から課金することを理解していることを確認します。

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	デフォルトは 60 分です

Microsoft Hyper-Vデータソース

Microsoft Hyper-Vデータソースを設定するには、物理ホスト（ハイパーバイザー）のIPアドレスまたは解決可能なDNS名が必要です。このデータソースでは、PowerShell（以

前はWMIを使用）を使用します。

用語集

OnCommand Insight では、Hyper-Vデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
Virtual hard diskの略	仮想ディスク
ホスト	ホスト
仮想マシン	仮想マシン
Cluster Shared Volume （ CSV ；クラスタ共有ボリューム）、パーティションボリューム	データストア
Internet SCSI Device 、 Multi Path SCSI LUN の略	LUN
ファイバチャネルポート	ポート

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- Hyper-V では、データ収集とリモートアクセス / 管理用にポート 5985 が開いている必要があります。
- クラスタリンググループノードの IP アドレス
- ハイパーバイザーのローカル管理者のユーザとパスワードです
- 管理者レベルのユーザアカウント
- ポートの要件:ポート135およびダイナミックTCPポートは、Windows 2003以前の場合は1024-65535、Windows 2008の場合は49152-65535に割り当てられます。
- データコレクタがIPアドレスのみを参照している場合でも、DNS解決は成功する必要があります。
- 各Hyper-Vハイパーバイザーで、すべてのホスト上のすべてのVMに対して「リソース計測」をオンにする必要があります。これにより、各ハイパーバイザーは、各ゲストで Cloud Insights に使用できるデータを増やすことができます。この値を設定しない場合は、各ゲストのパフォーマンスメトリックが取得される回数が少なくなります。リソース計測の詳細については、 Microsoft のドキュメントを参照してください。

  "Hyper-V のリソース計測の概要"

  "Enable - VMResourceMetering"

設定

* フィールド *	* 概要 *
物理ホストの IP アドレス	物理ホスト（ハイパーバイザー）の IP アドレスまたは完全修飾ドメイン名
ユーザ名	ハイパーバイザーの管理者のユーザ名
パスワード	ハイパーバイザーのパスワードです
NT ドメイン	クラスタ内のノードで使用される DNS 名

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
接続タイムアウト（ミリ秒）	接続タイムアウト（デフォルトは60000ミリ秒）

NetApp clustered Data ONTAP データソース

このデータソースは、clustered Data ONTAP を使用するストレージシステムに使用します。読み取り専用のAPI呼び出しに使用する管理者アカウントが必要です。

用語集

OnCommand Insight では、clustered Data ONTAP データソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
RAID グループ	ディスクグループ
クラスタ	ストレージ
ノード	ストレージノード
アグリゲート	ストレージプール
LUN	ボリューム

ボリューム	内部ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- 読み取り専用のAPI呼び出しに使用する管理者アカウント
- ターゲットIPはクラスタ管理LIFです
- ネットアップクラスタにログインするためのユーザ名（デフォルトのSVMに対するONTAPIアプリケーションの読み取り専用ロール名を使用）とパスワード
- ポートの要件： 80 または 443
- ライセンス要件：FCPライセンスと、検出に必要なマッピング/マスクされたボリューム

設定

* フィールド *	* 概要 *
ネットアップ管理 IP	ネットアップクラスタの IP アドレスまたは完全修飾ドメイン名
ユーザ名	ネットアップクラスタのユーザ名
パスワード	ネットアップクラスタのパスワード

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

clustered Data ONTAP ストレージ

ネットアップのclustered Data ONTAP ストレージアセットランディングページに記載されているオブジェクトや参照に適用される用語。

clustered Data ONTAP ストレージの用語

以下の用語は、NetApp clustered Data ONTAP のストレージアセットランディングページに表示されるオブジェクトや参照先に適用されます。これらの用語の多くは、他のデータコレクタにも適用されます。

- Model --このクラスタ内で一意の個別のノードモデル名をカンマで区切ったリスト。クラスタ内のすべてのノードのモデルタイプが同じ場合、表示されるモデル名は 1 つだけです。
- vendor --新しいデータソースを設定する場合と同じベンダー名。
- シリアル番号—アレイのシリアル番号NetApp clustered Data ONTAP などのクラスタアーキテクチャストレージシステムでは、このシリアル番号が個 々 の「ストレージノード」のシリアル番号よりも有用でない場合があります。
- IP：通常は、データソースで設定されているIPまたはホスト名です。
- マイクロコードバージョン—ファームウェア。
- Raw Capacity：役割に関係なく、システム内のすべての物理ディスクの2進数の合計。
- レイテンシ：ホストに直面しているワークロードで発生している状況を読み取りと書き込みの両方で表したもの。OCIがこの価値を直接提供するのが理想的ですが、そうではないことがよくあります。OCIでは、この機能を提供するアレイの代わりに、個 々 の内部ボリュームの統計に基づいてIOPSの加重計算を実行します。
- スループット：内部ボリュームから集計された値。
- 管理—これには’デバイスの管理インタフェースのハイパーリンクが含まれている場合がありますインベントリレポートの一部としてInsightデータソースによってプログラムによって作成されます。

clustered Data ONTAP ストレージプール

NetApp clustered Data ONTAP ストレージプールのアセットランディングページに記載されているオブジェクトや参照に適用される用語。

clustered Data ONTAP ストレージプールの用語

以下に示す用語は、NetApp clustered Data ONTAPストレージプールのアセットランディングページにあるオブジェクトや参照先に適用されます。これらの用語の多くは、他のデータコレクタにも適用されます。

- ストレージ—このプールが配置されているストレージアレイ必須。
- タイプ(Type)--可能性の列挙されたリストから’説明的な値を指定します最も一般的な構成は「アグリゲート」または「RAIDグループ」です。
- ノード：このストレージアレイのアーキテクチャでプールが特定のストレージノードに属する場合は、ストレージアレイの名前が独自のランディングページへのハイパーリンクとして表示されます。
- [Uses Flash Pool]-[Yes/No Value]-このSATA / SASベースのプールには、キャッシュアクセラレーションにSSDが使用されていますか。
- redundancy — RAIDレベルまたは保護スキーム。raid_dp はデュアルパリティ、 raid_dp はトリプルパリティです。
- 容量—使用済み論理容量、使用可能容量、論理合計容量、およびこれらの使用率が表示されます。
- オーバーコミット容量：効率化テクノロジを使用して、ストレージプールの論理容量よりも大きいボリュームまたは内部ボリュームの合計容量を割り当てた場合、この割合の値は0%より大きくなります。
- スナップショット—使用中のスナップショット容量と合計容量(ストレージプールアーキテクチャがその容量の一部をスナップショット専用のセグメント領域に使用している場合)MetroCluster 構成のONTAP ではこの傾向が見られますが、他のONTAP 構成ではそうではありません。
- 利用率—このストレージプールに容量を提供しているディスクのうち、最も高いディスクビジー率を示すパーセンテージ。ディスク利用率は、必ずしもアレイのパフォーマンスと強い相関関係があるとは限りま

せん。ホスト主導のワークロードがない場合、ディスクのリビルドや重複排除処理などが原因で利用率が高くなる可能性があります。また、多くのアレイのレプリケーション実装では、内部ボリュームまたはボリュームのワークロードとして表示されずに、ディスク利用率が上昇する可能性があります。

- IOPS --このストレージプールに容量を提供しているすべてのディスクの合計IOPS。
- スループット—このストレージプールに容量を提供しているすべてのディスクの合計スループット

clustered Data ONTAP ストレージノード

NetApp clustered Data ONTAPのストレージノードのアセットランディングページに記載されている、オブジェクトや参照に適用される用語。

clustered Data ONTAP ストレージノードの用語

以下の用語は、NetApp clustered Data ONTAP ストレージプールのアセットランディングページに表示されるオブジェクトや参照先に適用されます。これらの用語の多くは、他のデータコレクタにも適用されます。

- ストレージ—このノードが属するストレージアレイ必須。
- HAパートナー-- 1つのノードが1つだけ他のノードにフェイルオーバーするプラットフォームでは、一般的にここに表示されます。
- State --ノードのヘルス。アレイが正常な状態でデータソースでインベントリを作成できる場合にのみ使用できます。
- model --ノードのモデル名。
- version --デバイスのバージョン名
- シリアル番号—ノードのシリアル番号
- memory --ベース2メモリ(使用可能な場合)。
- 利用率-- ONTAP では、これは独自のアルゴリズムによるコントローラの応力指数です。パフォーマンスポーリングが行われるたびに、 WAFL ディスクの競合率または平均 CPU 利用率の値が 0 〜 100% の範囲で報告されます。50%を超える値が続く場合は、サイズ不足を示しています。コントローラ/ノードのサイズが十分でないか、書き込みワークロードを吸収するのに十分な回転式ディスクがない可能性があります。
- IOPS：ノードオブジェクトに対するONTAP ZAPI呼び出しから直接導出されます。
- レイテンシ：ノードオブジェクトに対するONTAP ZAPI呼び出しから直接導出されます。
- スループット：ノードオブジェクトに対するONTAP ZAPI呼び出しから直接導出されます。
- processors — CPU数。

NetApp clustered Data ONTAP for Unified Managerデータソース

このデータソースは、Unified Manager（UM）6.0以降のデータベースからONTAP 8.1.xのデータを収集します。Insightは、このデータソースを使用して、UMに設定されて入力されたすべてのクラスタを検出します。効率化のため、Insightではクラスタ自体に対してZAPIは呼び出されません。このデータソースではパフォーマンスはサポートされていません。

設定

このデータコレクタは、OnCommand Insight 7.3.11以降では使用できなくなりました。

* フィールド *	* 概要 *
Unified ManagerのIP	Unified ManagerのIPアドレスまたは完全修飾ドメイン名
ユーザ名	Unified Managerのユーザ名
パスワード	Unified Managerのパスワード
ポート	Unified Managerとの通信に使用するポート（デフォルトは3306）

高度な設定

* フィールド *	* 概要 *
Inventory Poll Interval (min) Interval	インベントリポーリングの間隔（デフォルトは15分）
クラスタを除外します	対象から除外するクラスタのIPをカンマで区切ったリスト

NetApp Data ONTAP 7-Modeデータソース

Data ONTAP 7-Modeソフトウェアを使用するストレージシステムの場合は、ONTAPIデータソースを使用します。このデータソースでは、CLIを使用して容量の値を取得します。

用語集

OnCommand Insight では、NetApp Data ONTAP 7-Modeデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
RAID グループ	ディスクグループ
ストレージシステム	ストレージ

ストレージシステム	ストレージノード
アグリゲート	ストレージプール
LUN	ボリューム
ボリューム	内部ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- FAS ストレージコントローラおよびパートナーのIPアドレス
- ポート 443
- コントローラとパートナーのユーザ名とパスワード
- 7-Mode 用の次のロール権限を持つコントローラとパートナーコントローラのカスタムの管理者レベルのユーザ名とパスワードです。
  - 「 api- * 」：すべてのネットアップストレージ API コマンドの実行を OnCommand Insight に許可します。
  - 「 login-http-admin 」： HTTP 経由で OnCommand Insight がネットアップストレージに接続できるようにします。
  - 「 security-api-vfiler 」： vFiler ユニットの情報を取得する NetApp ストレージ API コマンドの実行を OnCommand Insight に許可します。
  - 「 cli-options 」：ストレージシステムオプションを読み取るために使用します。
  - 「 cli-lun 」： LUN 管理用コマンドにアクセスします。指定した LUN または LUN のクラスのステータス（ LUN のパス、サイズ、オンライン / オフライン状態、共有状態）が表示されます。
  - 「 cli-df 」：空きディスクスペースを表示する場合に使用します。
  - 「 cli-ifconfig 」：インターフェイスと IP アドレスを表示します。

設定

* フィールド *	* 概要 *
Filerのアドレス	ネットアップファイラーのIPアドレスまたは完全修飾ドメイン名
ユーザ名	NetApp Filerのユーザ名
パスワード	NetApp Filerのパスワード

クラスタ内のHAパートナーファイラーのアドレス	HAパートナーファイラーのIPアドレスまたは完全修飾ドメイン名
クラスタ内のHAパートナーファイラーのユーザ名	ネットアップHAパートナーファイラーのユーザ名
クラスタ内の HA パートナーファイラーのパスワード	ネットアップHAパートナーファイラーのパスワード

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
接続タイプ	接続タイプを選択します
接続ポート	NetApp API に使用するポート
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

ストレージシステム接続

このデータソースでデフォルトの管理ユーザを使用する代わりに、ネットアップストレージシステムに対する管理者権限を持つユーザを設定して、このデータソースがネットアップストレージシステムからデータを取得できるようにすることもできます。

ネットアップストレージシステムに接続するには、メインの pfiler （ストレージシステムが存在する pfiler ）の取得時に次の条件を満たすユーザを指定する必要があります。

- ユーザは vfiler0 （ルートファイラー / pfiler ）に属している必要があります。

  メインの pfiler を取得するときにストレージシステムが取得されます。

- 次のコマンドで、ユーザロールの機能を定義します。
  - 「 api- * 」：すべてのネットアップストレージ API コマンドの実行を OnCommand Insight に許可します。このコマンドは、 ZAPI を使用する場合は必須です。
  - 「 login-http-admin 」： HTTP 経由で OnCommand Insight がネットアップストレージに接続できるようにします。このコマンドは、 ZAPI を使用する場合は必須です。
  - 「 security-api-vfiler 」： vFiler ユニットの情報を取得する NetApp ストレージ API コマンドの実行を OnCommand Insight に許可します。
  - 「 cli-options 」：「 options 」コマンドで、パートナーの IP と有効なライセンスを取得するために使用されます。
  - 「cli-lun」：LUNを管理するためのコマンドにアクセスします。指定した LUN または LUN のクラスのステータス（ LUN のパス、サイズ、オンライン / オフライン状態、共有状態）が表示されます。

- 「 cli-df 」：「 df -s 」、「 df -r 」、「 df -A -r 」コマンドで、空きスペースを表示するために使用されます。
- 「 cli-ifconfig 」：「 ifconfig -a 」コマンドで、ファイラーの IP アドレスを取得するために使用されます。
- 「 cli-rdfile 」：「 rdfile /etc/netgroup 」コマンドで、ネットグループを取得するために使用されます。
- 「 cli-date 」：「 date 」コマンドで、 Snapshot コピーを取得する完全な日付を取得するために使用されます。
- 「 cli-snap 」：「 snap list 」コマンドで、 Snapshot コピーを取得するために使用されます。

cli-date または cli-snap の権限が付与されていない場合、データ収集は完了できますが、 Snapshot コピーは報告されません。

7-Mode データソースを正常に取得し、ストレージシステムで警告が生成されないようにするには、次のいずれかのコマンド文字列を使用してユーザロールを定義する必要があります。2 つ目の文字列は、 1 つ目の文字列を簡潔に表したものです。

```
login-http-admin,api-*,security-api-vfile,cli-rdfile,cli-options,cli-
df,cli-lun,cli-ifconfig,cli-date,cli-snap,
or
login-http-admin,api-*,security-api-vfile,cli-*
```

NetApp E-Seriesデータソース

NetApp E-Seriesデータソースは、インベントリとパフォーマンスの情報を収集します。可能な構成は 2 種類（ファームウェア 6.x とファームウェア 7.x 以降）で、値はどちらも同じです。

用語集

OnCommand Insight では、NetApp E-Seriesデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ドライブ	ディスク
ボリュームグループ	ディスクグループ
ストレージアレイ	ストレージ
コントローラ	ストレージノード
ボリュームグループ	ストレージプール

ボリューム	ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- アレイの各コントローラの IP アドレス
- ポート要件 2463

設定

* フィールド *	* 概要 *
アレイ SANtricity コントローラの IP をカンマで区切ったリスト	アレイコントローラの IP アドレスまたは完全修飾ドメイン名

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは30分）
パフォーマンスポーリング間隔（最大3600秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

Eシリーズストレージ

NetApp Eシリーズストレージのアセットランディングページに記載されているオブジェクトや参照に適用される用語。

Eシリーズストレージの用語

以下の用語は、NetApp Eシリーズストレージアセットランディングページに表示されるオブジェクトや参照先に適用されます。これらの用語の多くは、他のデータコレクタにも適用されます。

- model --デバイスのモデル名。
- vendor --新しいデータソースを設定する場合と同じベンダー名。
- シリアル番号—アレイのシリアル番号NetApp clustered Data ONTAP などのクラスタアーキテクチャストレージシステムでは、このシリアル番号が個 々 の「ストレージノード」のシリアル番号よりも有用でない場合があります。
- IP：通常は、データソースで設定されているIPまたはホスト名です。
- マイクロコードバージョン—ファームウェア。
- Raw Capacity：役割に関係なく、システム内のすべての物理ディスクの2進数の合計。

- レイテンシ：ホストに直面しているワークロードで発生している状況を読み取りと書き込みの両方で表したもの。Insightでは、ストレージ内のボリュームからIOPS加重平均を算出します。
- スループット—アレイのホスト側の合計スループットInsightでは、ボリュームのスループットを合計してこの値を算出します。
- 管理—これには’デバイスの管理インタフェースのハイパーリンクが含まれている場合がありますインベントリレポートの一部としてInsightデータソースによってプログラムによって作成されます。

Eシリーズストレージプール

NetApp Eシリーズストレージプールのアセットランディングページに記載されているオブジェクトや参照に適用される用語。

Eシリーズストレージプールの用語

以下の用語は、NetApp Eシリーズストレージプールのアセットランディングページに表示されるオブジェクトや参照先に適用されます。これらの用語の多くは、他のデータコレクタにも適用されます。

- ストレージ—このプールが配置されているストレージアレイ必須。
- タイプ(Type)--可能性の列挙されたリストから’説明的な値を指定します最も一般的な構成は「シンプロビジョニング」または「RAIDグループ」です。
- ノード：このストレージアレイのアーキテクチャでプールが特定のストレージノードに属する場合は、ストレージアレイの名前が独自のランディングページへのハイパーリンクとして表示されます。
- Flash Poolを使用（「はい」または「いいえ」）
- redundancy — RAIDレベルまたは保護スキーム。Eシリーズでは、DDPプールについて「RAID 7」が報告されます。
- 容量—使用済み論理容量、使用可能容量、論理合計容量、およびこれらの使用率が表示されます。どちらの値にもEシリーズの「予約済み」容量が含まれるため、Eシリーズのユーザインターフェイスで表示される数値と割合がどちらも大きくなります。
- オーバーコミット容量：効率化テクノロジを使用して、ストレージプールの論理容量よりも大きい合計ボリューム容量を割り当てた場合、この割合の値は0%より大きくなります。
- スナップショット—使用中のスナップショット容量と合計容量(ストレージプールアーキテクチャがその容量の一部をスナップショット専用のセグメント領域に使用している場合)
- 利用率：このストレージプールに容量を提供しているディスクのうち、ディスクビジー率が最も高い割合を示すパーセンテージ。ディスク利用率は、必ずしもアレイのパフォーマンスと強い相関関係があるとは限りません。ホスト駆動型のワークロードがない場合、ディスクのリビルドや重複排除処理などが原因で利用率が高くなる可能性があります。また、多くのアレイのレプリケーション実装では、ボリュームのワークロードとしては表示されませんが、ディスク利用率が上昇する可能性があります。
- IOPS --このストレージプールに容量を提供しているすべてのディスクの合計IOPS。
- スループット—このストレージプールに容量を提供しているすべてのディスクの合計スループット

Eシリーズストレージノード

NetApp Eシリーズストレージノードのアセットランディングページに記載されている、オブジェクトまたは参照に適用される用語。

Eシリーズストレージノードの用語

以下の用語は、NetApp Eシリーズストレージプールのアセットランディングページに表示されるオブジェクトや参照先に適用されます。これらの用語の多くは、他のデータコレクタにも適用されます。

- ストレージ—このノードが属するストレージアレイ必須。
- HAパートナー-- 1つのノードが1つだけ他のノードにフェイルオーバーするプラットフォームでは、一般的にここに表示されます。
- State --ノードのヘルス。アレイが正常な状態でデータソースでインベントリを作成できる場合にのみ使用できます。
- model --ノードのモデル名。
- version --デバイスのバージョン名
- シリアル番号—ノードのシリアル番号
- memory --ベース2メモリ(使用可能な場合)。
- 利用率：NetApp Eシリーズでは現在利用率を使用できません。
- IOPS -このノードにのみ属するボリュームのすべてのIOPSを合計して算出します。
- Latency --このコントローラでの一般的なホストのレイテンシまたは応答時間を表す数値。Insightでは、このノードにのみ属するボリュームからIOPSの加重平均を計算します。
- スループット—このコントローラ上のホストによって駆動されるスループットを表す数値。このノードにのみ属するボリュームのスループットをすべて合計して算出します。
- processors — CPU数。

NetApp Host and VM File Systemsデータソース

NetApp Host and VM File Systemsデータソースを使用して、すべてのMicrosoft WindowsホストおよびVM（仮想マシン）ファイルシステム、およびサポートされているすべてのLinux VM（仮想的にマッピングされたVMのみ）について、ファイルシステムの詳細とストレージリソースのマッピングを取得できます。 設定済みのCompute Resource Group（CRG；コンピューティングリソースグループ）でアノテートされているInsightサーバ内の既存のファイル。

一般要件

- この機能は別途購入する必要があります。

  詳細については、Insightの担当者にお問い合わせください。

- Insightのサポートマトリックスで、お使いのホストまたは仮想マシンのオペレーティングシステムがサポートされていることを確認してください。

  ファイルシステムからストレージリソースへのリンクが作成されていることを確認するには、関連するストレージベンダーまたは仮想化ベンダーのタイプとバージョンで、必要なボリュームまたは仮想ディスクの識別データが報告されていることを確認します。

Microsoft Windowsの要件

- このデータソースは、Window Management Instrumentation（WMI）データ構造を使用してデータを取得します。

  このサービスは動作しており、リモートで利用できる必要があります。特に、ポート135にアクセスできる必要があり、ファイアウォールの背後にある場合は開いておく必要があります。

- Windowsドメインユーザには、WMI構造にアクセスするための適切な権限が必要です。
- 管理者権限が必要です。
- Windows 2003以前に1024～65535が割り当てられた動的TCPポート
- ポート49152～-65535（Windows 2008の場合）

> 原則として、Insight、AU、およびこのデータソースの間にファイアウォールを使用する場合は、Microsoftチームに相談して、必要と思われるポートを特定する必要があります。

Linuxの要件

- このデータソースは、Secure Shell（SSH）接続を使用してLinux VMに対してコマンドを実行します。

  SSHサービスが動作していて、リモートで使用できる必要があります。特に、ポート22にアクセスできる必要があり、ファイアウォールの背後にある場合はポート22を開く必要があります。

- SSHユーザには、Linux VMに対して読み取り専用コマンドを実行するためのsudo権限が必要です。

  SSHへのログインとsudoパスワードチャレンジの回答 へのログインには、同じパスワードを使用する必要があります。

使用上の推奨事項

- オペレーティングシステムのクレデンシャルが同じホストおよび仮想マシンのグループには、同じ[Compute Resource Group]アノテーションをアノテートする必要があります。

  各グループにこのデータソースのインスタンスが割り当てられ、それらのホストおよび仮想マシンからファイルシステムの詳細が検出されます。

- このデータソースのインスタンスで成功率が低い場合（たとえば、グループ内の1、000台のホストおよび仮想マシンのうち、OnCommand Insight でファイルシステムの詳細が検出されるのは50台のみ）、 検出に成功したホストと仮想マシンを別のコンピューティングリソースグループに移動する必要があります。

設定

フィールド	説明
ユーザ名	適切な権限を持つオペレーティングシステムユーザーWindowsオペレーティングシステムユーザーのファイルシステムデータを取得するには、ドメインプレフィックスを含める必要があります。

パスワード	オペレーティングシステムユーザのパスワード
コンピュートリソースグループ	データソースでファイルシステムを検出するホストおよび仮想マシンのフラグとして使用されるアノテーション値。値が空の場合は、現在いずれのコンピューティングリソースグループもアノテートされていないすべてのホストおよび仮想マシンのファイルシステムがデータソースで検出されます。

高度な設定

フィールド	説明
インベントリのポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは360分）

NetApp SolidFire データソース

NetApp SolidFire データソースでは、インベントリとパフォーマンスの両方の収集について、iSCSIとFibre Channel SolidFire の両方の構成がサポートされます。

SolidFire データソースでは、SolidFire REST APIを利用します。データソースが配置されているAcquisition Unitから、SolidFire クラスタ管理IPアドレスのTCPポート443へのHTTPS接続を開始できる必要があります。データソースには、SolidFire クラスタに対してREST APIクエリを実行するためのクレデンシャルが必要です。

用語集

OnCommand Insight では、NetApp SolidFire データソースから次のインベントリ情報を取得します。Insight で取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ドライブ	ディスク
クラスタ	ストレージ
ノード	ストレージノード
ボリューム	ボリューム
Fibre Channel Port（ファイバチャネルポート）	ポート
ボリュームアクセスグループ、 LUN の割り当て	ボリュームマップ

iSCSI セッション	ボリュームマスク

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

このデータソースの設定に関する要件は次のとおりです。

- 管理仮想 IP アドレス
- ポート 443

設定

フィールド	説明
管理仮想 IP アドレス（ MVIP ）	SolidFire クラスタの管理仮想 IP アドレス
ユーザ名	SolidFire クラスタへのログインに使用するユーザ名
パスワード	SolidFire クラスタへのログインに使用するパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
TCP ポート	SolidFire サーバへの接続に使用するTCPポート（デフォルトは443）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

トラブルシューティング

SolidFire からエラーが報告されると、次のようにOnCommand Insight に表示されます。

```
An error message was received from a SolidFire device while trying to retrieve
data. The call was <method> (<parameterString> ). The error message from the
device was (check the device manual): <message>
```

ここで、

- method> は、 GET や PUT などの HTTP メソッドです。
- parameterString> は、 REST 呼び出しに含まれていたパラメータをカンマで区切ったリストです。
- <message> は、エラーメッセージとして返されたデバイスです。

NetApp StorageGRID データソース

このデータソースは、StorageGRID のインベントリとパフォーマンスのデータを収集します。

要件

このデータソースの設定に関する要件は次のとおりです。

- StorageGRID ホストの IP アドレス
- Metric Query ロールとテナントアクセスロールが割り当てられているユーザのユーザ名とパスワード
- ポート 443

設定

フィールド	説明
StorageGRID ホストIPアドレス（MVIP）	StorageGRID のホストIPアドレス
ユーザ名	StorageGRID へのログインに使用する名前
パスワード	StorageGRID へのログインに使用するパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは900秒）

OpenStackデータソース

OpenStack（REST API / KVM）データソースは、OpenStackハードウェアインスタンスに関する情報を収集します。このデータソースは、すべてのOpenStackインスタンスのインベントリデータと、オプションでVMのパフォーマンスデータを収集します。

要件

OpenStackデータソースを設定するための要件を次に示します。

- OpenStack コントローラの IP アドレス
- OpenStack管理者ロールのクレデンシャルとLinux KVMハイパーバイザーへのsudoアクセスを推奨します。

> adminアカウントまたはadminと同等の権限を使用していない場合でも、データソースからデータを取得できます。管理者以外のロールを持つユーザがAPIを呼び出すことができるように、ポリシー構成ファイル（etc/nova/policy.jsonなど）を変更する必要があります。

  - "os_compute_api：os-availability-zone：detail"："
  - "os_compute_api：os-hypervisors"："
  - os_compute_api：servers：detail：get_all_tenants "："
- パフォーマンスを収集するには、OpenStack Ceilometerモジュールをインストールして設定する必要があります。Ceilometerの設定は、を編集して行います `nova.conf` ファイルをハイパーバイザーごとに作成し、各ハイパーバイザーでNova Computeサービスを再起動します。オプション名は、 OpenStack の各リリースで変更されています。
  - Icehouse のあるホテル
  - Juno 社
  - キロ
  - リバティー
  - 三鷹
  - ニュートン
  - 八幡市
- CPU統計の場合、コンピュートノードの/etc/Nova/Nova.conf で「compute_monitors=ComputeDriverCPUMonitor」をオンにする必要があります。
- ポート要件
  - HTTP は 5000 、 Keystone サービスは 13000 、 HTTPS は 13000 です
  - KVM SSH の場合は 22
  - Nova Compute Service の場合は 8774
  - Cinder ブロックサービスの場合は 8776
  - Ceilometer パフォーマンスサービス用 8777
  - Glance Image Serviceの場合は9292

> ポートは特定のサービスにバインドされ、大規模な環境ではコントローラまたは別のホストでサービスを実行できます。

設定

* フィールド *	* 概要 *

OpenStack Controller の IP アドレス	OpenStack Controller の IP アドレスまたは完全修飾ドメイン名
OpenStack 管理者	OpenStack 管理者のユーザ名
OpenStack パスワード	OpenStack 管理に使用するパスワード
OpenStack 管理者のテナント	OpenStack 管理者のテナント
KVM sudo ユーザー	KVM Sudo ユーザー名
クレデンシャルタイプを指定するには、「 Password 」または「 OpenSSH Key File 」を選択してください	SSH経由でデバイスに接続するために使用するクレデンシャルタイプ
Inventory Private Key への完全パス	Inventory Private Key への完全パス
KVM sudo パスワード	KVM sudo パスワード

高度な設定

* フィールド *	* 概要 *
SSH を使用してハイパーバイザーのインベントリ検出を有効にし	SSH を使用してハイパーバイザーインベントリの検出を有効にする場合は、このチェックボックス
OpenStack 管理 URL のポート	OpenStack 管理 URL のポート
HTTPS を使用する	セキュア HTTP を使用する場合に選択します
HTTP 接続タイムアウト（秒）	HTTP接続のタイムアウト（デフォルトは300秒）
SSH ポート	SSH に使用するポート
SSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは30秒）
SSH プロセスの再試行回数	インベントリの再試行回数
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）

Oracle ZFSデータソース

Oracle ZFSデータソースで、インベントリとパフォーマンスの収集がサポートされるようになりました。

用語集

OnCommand Insight では、このデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ディスク（SDD）	ディスク
クラスタ	ストレージ
コントローラ	ストレージノード
LUN	ボリューム
LUN マップ	ボリュームマップ
イニシエータ、ターゲット	ボリュームマスク
共有	内部ボリューム

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

このデータソースの設定に関する要件は次のとおりです。

- ZFS Controller-1 および ZFS Controller-2 のホスト名
- 管理者のユーザ名とクレデンシャル
- ポート要件： 215 HTTP/HTTPS

設定

ZFS Controller-1 ホスト名	ストレージコントローラ 1 のホスト名
ZFS Controller-2 ホスト名	ストレージコントローラ 2 のホスト名
ユーザ名	ストレージシステム管理者ユーザアカウントのユーザ名
パスワード	管理者ユーザアカウントのパスワード

高度な設定

フィールド	説明
TCP ポート	ZFSへの接続に使用するTCPポート（デフォルトは215）
接続タイプ	HTTPまたはHTTPS
インベントリのポーリング間隔	インベントリのポーリング間隔（デフォルトは60分）
接続タイムアウト	デフォルトは60秒です
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

トラブルシューティング

このデータコレクタで問題が発生した場合の対処方法を次に示します。

問題	次の操作を実行します
" 無効なログイン資格情報 "	ZFS ユーザーアカウントとパスワードを検証します
「Configuration error」と「Rest Service is disabled」というエラーメッセージが表示されます。	このデバイスで REST サービスが有効になっていることを確認します。
「Configuration error」と表示され、「User unauthorized for command」というエラーメッセージが表示されます。	特定のロール（「advanced_analytics」など）が設定されているユーザ<userName> に含まれていない可能性があります。考えられる解決策 ： • 読み取り専用ロールを持つユーザー$｛user｝のAnalytics（統計）スコープを修正します。-[構成]→[ユーザー]画面で、ロールの上にマウスを置き、ダブルクリックして編集を許可します • [Scope]ドロップダウンメニューから[Analytics]を選択します。使用可能なプロパティのリストが表示されます。 • 一番上のチェックボックスをクリックすると、3 つのプロパティがすべて選択されます。-右側の[追加]ボタンをクリックします。 • ポップアップウィンドウの右上にある[適用]ボタンをクリックします。ポップアップウィンドウが閉じます。

Pure Storage FlashArrayデータソース

Pure Storage FlashArray（HTTP）データソースは、Pure Storage Flash Arrayから情報を収集するために使用します。Insightでは、インベントリとパフォーマンスの両方の収集がサポートされます。

用語集

OnCommand Insight では、Pure Storage FlashArrayデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
ドライブ（ SSD ）	ディスク
配列	ストレージ
コントローラ	ストレージノード
ボリューム	ボリューム
ポート	ポート
LUNマップ（ホスト、ホストグループ、ターゲットポート）	ボリュームマップ、ボリュームマスク

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ストレージシステムの IP アドレス
- Pure ストレージシステムの Administrator アカウントのユーザ名とパスワード。
- ポート要件： HTTP / HTTPS / 443

設定

* フィールド *	* 概要 *
FlashArrayホスト	FlashArray管理サーバのIIPアドレスまたは完全修飾ドメイン名
ユーザ名	FlashArray管理サーバのユーザ名
パスワード	FlashArray管理サーバのパスワード

高度な設定

* フィールド *	* 概要 *
接続タイプ	管理サーバ
TCP ポート	FlashArrayサーバへの接続に使用するTCPポート（デフォルトは443）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
パフォーマンスポーリング間隔（秒）	パフォーマンスポーリングの間隔（デフォルトは300秒）

QLogic FC Switchデータソース

QLogic FC Switch（SNMP）データソースを設定するには、FCスイッチデバイスのネットワークアドレス（IPアドレスとして指定）、およびデバイスへのアクセスに使用するsnmp_read-only_community stringが必要です。

設定

* フィールド *	* 概要 *
SANsurferスイッチ	SANSurferスイッチのIPアドレスまたは完全修飾ドメイン名
SNMP バージョン	SNMP バージョン
SNMPコミュニティ	SNMP コミュニティストリング
ユーザ名	SANSurferスイッチのユーザ名
パスワード	SANSurferスイッチのパスワード

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは15分）
SNMP 認証プロトコル	SNMP 認証プロトコル（ SNMPv3 のみ）

SNMP 再試行回数	SNMP の再試行回数
SNMP タイムアウト（ミリ秒）	SNMP タイムアウト（デフォルトは 5 、 000 ミリ秒）
トラッピングを有効にします	トラップを有効にする場合に選択します
トラップ間の最小時間（秒）	トラップでデータ収集を試行する最小間隔（デフォルトは 10 秒）
ファブリック名	データソースでレポートするファブリック名。ファブリック名を WWN としてレポートする場合は、空白のままにします。
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

Red Hat（RHEV）データソース

Red Hat Enterprise Virtualization（REST）データソースは、HTTPS経由でRHEVインスタンスに関する情報を収集します。

要件

- REST API を使用した RHEV サーバのポート 443 経由の IP アドレス
- 読み取り専用のユーザ名とパスワード
- RHEV バージョン 3.0+

設定

フィールド	説明
RHEV サーバの IP アドレス	RHEVサーバのIPアドレスまたは完全修飾ドメイン名
ユーザ名	RHEVサーバのユーザ名
パスワード	RHEVサーバのパスワード

高度な設定

フィールド	説明
HTTPS 通信ポート	RHEV への HTTPS 通信に使用するポート

インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）

Violin Flash Memory Arrayデータソース

Violin 6000-Series Flash Memory Array（HTTP）データソースは、Violin 6000シリーズフラッシュメモリアレイから分析と検証に使用するネットワーク情報を収集します。

用語集

このデータコレクタは、OnCommand Insight 7.3.11以降では使用できなくなりました。

OnCommand Insight では、Violin 6000-Series Flash Memory Arrayデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
Violin Intelligent Memory Module（VIMM）	ディスク
コンテナ	ストレージ
Memory Gatewayの略	ストレージノード
LUN	ボリューム
イニシエータ、イニシエータグループ、ターゲット	ボリュームマップ、ボリュームマスク

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- ストレージに対する読み取り専用のユーザ名とパスワードが必要です。
- ストレージIPアドレスを使用してWebブラウザでアクセスを検証します。

設定

フィールド	説明
Violin Memory Array Main GatewayのIPアドレスまたはFQDN	Violin Memory Array Main GatewayのIPアドレスまたは完全修飾ドメイン名

ユーザ名	Violin Memory Array Main Gatewayのユーザ名
パスワード	Violin Memory Array Main Gatewayのパスワード

高度な設定

フィールド	説明
通信ポート	Violinアレイとの通信に使用するポート
HTTPSが有効です	HTTPSを使用する場合に選択します
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

VMware vSphereデータソース

VMware vSphere（Web Services）データソースはESXホスト情報を収集し、Virtual Center内のすべてのオブジェクトに対して_read-only_privilegesを必要とします。

用語集

OnCommand Insight では、VMware vSphereデータソースから次のインベントリ情報を取得します。Insightで取得したアセットタイプごとに、このアセットに使用される最も一般的な用語が表示されます。このデータソースを表示またはトラブルシューティングするときは、次の用語に注意してください。

ベンダー / モデルの用語	Insightの用語
仮想ディスク	ディスク
ホスト	ホスト
仮想マシン	仮想マシン
データストア	データストア
LUN	LUN
ファイバチャネルポート	ポート

これらは一般的な用語のマッピングであり、このデータソースのすべてのケースを表しているとは限りません。

要件

- Virtual Center サーバの IP アドレス
- Virtual Center の読み取り専用のユーザ名とパスワード
- Virtual Center内のすべてのオブジェクトに対する読み取り専用権限。
- Virtual Centerサーバ上のSDKアクセス
- ポート要件： http - 80 https-443
- ユーザ名とパスワードを使用してVirtual Center Clientにログインし、と入力してSDKが有効になっていることを確認して、アクセスを検証します `telnet <vc_ip\> 443`。

設定

* フィールド *	
* 概要 *	
Virtual Center Addressの略	
Virtual CenterまたはvSphereサーバのネットワークアドレス。IP_（nnn.nnn.nnn.nnn_format）アドレス、またはDNSで解決できるホスト名で指定します。	
ユーザ名	
VMwareサーバのユーザ名。	
パスワード	
VMwareサーバのパスワード。	

高度な設定

* フィールド *	* 概要 *
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
接続タイムアウト（ミリ秒）	接続タイムアウト（デフォルトは60000ミリ秒）
で VM をフィルタリングします	VMをフィルタする方法を選択します
「除外」または「含める」を選択してリストを指定します	以下のリストにあるVMをデータの収集時に対象に含めるか除外するかを指定します

フィルタするVMのリスト（カンマ区切り、値にカンマを使用する場合はセミコロン区切り）	ポーリングの対象または対象から除外するVMをカンマまたはセミコロンで区切ったリスト
vCenterへの要求の再試行回数	vCenter要求の再試行回数
通信ポート	VMwareサーバに使用するポート
パフォーマンスポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

データソースのクレデンシャルの変更

同じタイプの複数のデータソースがユーザ名とパスワードを共有している場合は、グループ内のすべてのデバイスのパスワードを同時に変更できます。

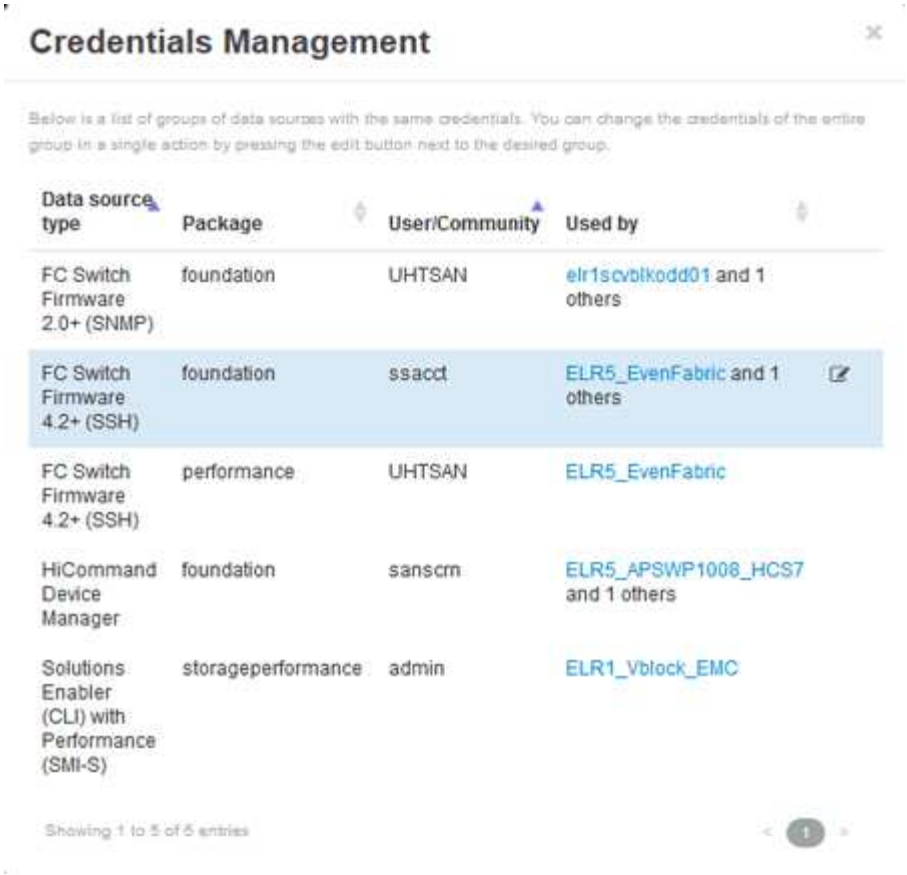
手順

1. Insightのツールバーで、*[Admin]*をクリックします。

   [データソース]*リストが開きます。

2. ボタンをクリックし、[クレデンシャルの変更]*オプションを選択します。
3. [Credentials Management]ダイアログボックスで、リストからいずれかのデータソースグループを選択します。

   右側の編集アイコン（紙の上のペン）がアクティブになります。



4. [編集（ Edit ）] をクリックします。
5. 新しいパスワードを入力し、確認のためにもう一度入力します。

データ収集の問題を引き起こす変更

OnCommand Insight でデータ収集の問題が発生している場合は、環境内での変更が原因である可能性があります。一般的なメンテナンスルールとして、Insightでの環境の変更にも対応する必要があります。

次のチェックリストを使用して、問題の原因となる可能性のあるネットワークの変更を特定できます。

- パスワードを変更しましたか？これらのパスワードはInsightで変更されましたか？
- ネットワークからデバイスを削除しましたか？また、デバイスが再検出されて再導入されないように、OnCommand Insight からデバイスを削除する必要があります。
- インフラストラクチャソフトウェア（HP CommandView EVAやEMC Solutions Enablerなど）をアップグレードしましたか。

  Acquisition Unitに適切なバージョンのクライアントツールがインストールされていることを確認します。データソースで問題が解決しない場合は、テクニカルサポートに連絡してサポートやデータソースパッチの入手を依頼する必要があります。

- すべてのOnCommand Insight Acquisition Unitで同じバージョンのOnCommand Insight が使用されていますか？Remote Acquisition UnitとLocal Acquisition Unitで異なるバージョンのOnCommand Insight が実行されている場合は、データ収集の問題を解決するために、すべてのユニットに同じバージョンをインストールしてください。

すべてのAcquisition Unitに新しいバージョンのOnCommand Insight をインストールする必要がある場合は、サポートサイトにアクセスして正しいバージョンをダウンロードしてください。

- ドメイン名を変更したか、新しいドメインを追加しましたか。デバイス解決（以前の自動解決）方法を更新する必要があります。

1つのデータソースの詳細を確認します

データソースで障害や処理速度の低下が発生した場合は、そのデータソースの詳細な情報を確認して、問題の原因 を特定できます。注意が必要な状態のデータソースは赤い丸で示されます。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。

   [データソース]*リストが開きます。問題がある可能性があるデータソースは、赤い丸で示されます。最も深刻な問題はリストの一番上にあります。

2. 問題の原因となっているデータソースを選択します。
3. データソース名のリンクをクリックします。
4. データソースの概要ページで、次のいずれかのセクションの情報を確認します。
   - イベントタイムライン

     [データソース]リストに表示されている現在のステータスに関連するイベントを一覧表示します。このサマリーのイベントは、デバイスごとに表示されます。エラーは赤で表示されます。タイムラインアイテム上にマウスポインタを置くと、追加情報 が表示されます。

   - このデータソースによって報告されたデバイス

     に、デバイスのタイプ、IPアドレス、および各デバイスの詳細情報へのリンクを示します。

   - このデータソースによって報告された変更（過去**3**週間）

     追加または削除されたデバイス、または設定に変更があったデバイスを一覧表示します。

5. データソースの情報を確認したら、ページの上部にあるボタンを使用して次のいずれかの処理を実行できます。
   - *データソースの概要 を編集して問題を修正します。
   - *再度ポーリング*は、問題が持続的であるか断続的であるかを明らかにするためにポーリングを強制します。
   - *データソースのポーリングを3、7、または30日間延期して、問題を調査して警告メッセージを停止します。
   - *データソースにパッチ*をインストールして、問題を修正します。
   - テクニカルサポート用の*エラーレポート*を準備します。
   - * Insight監視環境からデータソースを削除*します。

データソースの問題を調査しています

データソースに「* Inventory failed！」または「 Performance failed！*」というメッセージが表示され、[Impact]が[High]または[Medium]になっている場合は、データソースの概要ページにリンクされた情報を使用してこの問題を調査する必要があり

手順

1. データソースのリンクされた* Name *をクリックして、Summaryページを開きます。
2. [Summary]ページで[* Comments]領域を確認し、この問題を調査している可能性のある別のエンジニアが残したメモを確認します。
3. パフォーマンスのメッセージを確認します。
4. このデータソースに適用されているパッチがある場合は、リンクをクリックして*パッチページ*を確認し、それが問題の原因であるかどうかを確認します。
5. 追加情報 を表示するには、*イベントタイムライン*グラフのセグメントの上にマウスポインタを移動します。
6. イベントタイムラインの下に表示されるデバイスのエラーメッセージを選択し、メッセージの右側に表示される*エラーの詳細*アイコンをクリックします。

   エラーの詳細には、エラーメッセージのテキスト、考えられる原因、使用中の情報、問題を修正するために試すことができる推奨事項が含まれています。

7. [Devices reported by this data source]領域で、リストをフィルタして目的のデバイスのみを表示できます。また、デバイスのリンクされた* Name *をクリックすると、そのデバイスの_asset page_が表示されます。
8. 以前に表示したページに戻るには、次のいずれかの方法を使用します。
   - ブラウザの戻る矢印をクリックします。
   - 戻る矢印を右クリックしてページのリストを表示し、目的のページを選択します。
9. 他のリソースに関する詳細情報を表示するには、[その他のリンクされた名前]をクリックします。
10. データソースの概要ページに戻ったら、ページ下部の*変更*領域で、最近の変更が問題の原因になっていないかどうかを確認します。

データソースのポーリングの制御

データソースに変更を加えたあと、すぐにポーリングして変更を確認したり、問題の処理中にデータソースのデータ収集を1日、3日、5日間延期したりできます。

手順

1. [Admin]*をクリックし、データソースのリストビューに移動します
2. ポーリングを制御するデータソースを選択します。
3. データソース名のリンクをクリックします。
4. データソースの概要ページで、情報を確認し、次の2つのポーリングオプションのいずれかをクリックします。

- *もう一度ポーリング*を実行すると、データソースにすぐにデータが収集されます。
- *延期*し、ポーリング遅延の長さを3日、7日、または30日から選択します。

完了後

データソースでデータ収集を延期した場合に収集を再開するには、概要ページで*[再開]*をクリックします。

データソース情報の編集

データソースの設定情報は簡単に編集できます。

手順

1. [Admin]*をクリックし、データソースのリストビューに移動します
2. 編集するデータソースを探します。
3. 変更を開始するには、次のいずれかの方法を使用します。
   - 選択したデータソースの右側にある*[データソースの編集]*をクリックします。
   - 選択したデータソースのリンク名をクリックし、*[編集]*をクリックします。どちらの方法でも、[Edit data source]ダイアログボックスが開きます。
4. 必要な変更を行い、*[保存]*をクリックします。

複数のデータソースの情報を編集する

同じベンダーおよびモデルの複数のデータソースについて、ほとんどの情報を一度に編集できます。たとえば、これらのデータソースでユーザ名とパスワードが共有されている場合は、一箇所でパスワードを変更して、選択したすべてのデータソースのパスワードを更新できます。

このタスクについて

選択したデータソースについて編集できないオプションは、[データソースの編集]ダイアログボックスでグレー表示または非表示になります。また、オプションの値が「* Mixed 」と表示されている場合は、選択したデータソース間でオプションの値が異なることを示します。たとえば、選択した**2**つのデータソースの Timeout (sec)オプションが Mixed *の場合、一方のデータソースのタイムアウト値は60、もう一方のデータソースの値は90になります。 したがって、この値を120に変更してデータソースへの変更を保存すると、両方のデータソースのタイムアウト設定が120になります。

手順

1. [Admin]*をクリックし、データソースのリストビューに移動します
2. 変更するデータソースを選択します。同じベンダー、モデル、Acquisition Unitに属しているデータソースを選択する必要があります。
3. ボタンをクリックし、[編集]*オプションを選択します。
4. 編集ダイアログで、必要に応じて*設定*を変更します。
5. [Configuration]*リンクをクリックして、データソースの基本オプションを変更します。

6. [Advanced Configuration]*リンクをクリックして、データソースの詳細オプションを変更します。
7. [保存（ Save ）] をクリックします。

データソースタグをアノテーションにマッピングする

タグデータをポーリングするようにデータソースを設定すると、Insightでは、既存のInsightアノテーションのアノテーション値がタグと同じ名前で自動的に設定されます。

データソースでタグを有効にする前にInsightのアノテーションが存在していた場合は、データソースタグのデータが自動的にInsightのアノテーションに追加されます。

タグを有効にしたあとにアノテーションを作成した場合、データソースの初回のポーリングでアノテーションが自動的に更新されません。Insightのアノテーションの置き換えやデータの入力には時間がかかります。この遅延を回避するには、データソースを延期して再開することで、タグのアノテーションの更新を強制的に実行します。

データソースの削除

環境からデータソースを削除した場合は、OnCommand Insight 監視環境からも削除する必要があります。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。

   [Data sources]リストが開きます。

2. 削除するデータソースを選択します。
3. リンクされたデータソース名をクリックします。
4. 選択したデータソースの情報を概要ページで確認し、そのデータソースが削除対象であることを確認します。
5. [削除（ Delete ）] をクリックします。
6. [OK]*をクリックして操作を確定します。

データソースパッチとは

データソースパッチを適用すると、既存のパッチの問題が修正され、新しいタイプのデータソース（ベンダーやモデル）を簡単に追加できます。データソースパッチは、ネットワーク内のデータソースタイプごとにアップロードできます。パッチ適用プロセスをインストール、テスト、および管理することもできます。ただし、1つのデータソースタイプに対して一度にアクティブにできるパッチは1つだけです。

パッチごとに、次のタスクを実行できます。

- パッチを受信する各データソースの前後の比較を確認します。

- 決定を説明したり、調査を要約したりするためのコメントを書いてください。
- パッチに適切に対応していないデータソースに変更を加えます。
- Insightサーバへのパッチのコミットを承認します。
- 意図したとおりに動作しないパッチをロールバックします。
- 問題のあるパッチを別のパッチに交換します。

データソースパッチの適用

定期的に提供されるデータソースパッチを使用して、既存のデータソースの問題を修正したり、新しいベンダーのデータソースを追加したり、ベンダーの新しいモデルを追加したりできます。

作業を開始する前に

を入手しておく必要があります `.zip` 最新のデータソースを含むファイル `.patch` テクニカルサポートから入手したファイル。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [パッチ]*をクリックします。
3. [Actions]ボタンから、*[Apply patch]*を選択します。
4. ダイアログボックスで、[参照]*をクリックしてを指定します `.patch` ファイル。
5. 、**[**概要 **]**、[影響を受けるデータソースの種類]*を確認します。
6. 選択したパッチが正しい場合は、*パッチの適用*をクリックします。

   データソースの問題を修正するパッチを適用する場合は、同じタイプのすべてのデータソースがパッチで更新されるため、パッチを承認する必要があります。設定済みのデータソースに影響しないパッチは自動的に承認されます。

完了後

新しいベンダーまたは新しいモデルのデータソースを追加するパッチを適用する場合は、パッチの適用後にデータソースを追加する必要があります。

あるタイプのデータソースにパッチをインストールする

データソースパッチをアップロードしたら、同じタイプのすべてのデータソースにインストールできます。

作業を開始する前に

いずれかのタイプのデータソースにインストールするパッチファイルをアップロードしておく必要があります。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [パッチ]*をクリックします。
3. [Actions]ボタンから、*[Apply patch]*を選択します。
4. ダイアログボックスで、[Browse]*をクリックして、アップロードしたパッチファイルを指定します。
5. 、**[**概要 **]**、[影響を受けるデータソースタイプ]*を確認します。
6. 選択したパッチが正しい場合は、*パッチの適用*をクリックします。

   同じタイプのすべてのデータソースがこのパッチで更新されます。

パッチの管理

ネットワークに適用されているすべてのデータソースパッチの現在のステータスを確認できます。パッチに対してアクションを実行する場合は、現在レビュー中のパッチ（Patches Currently Under Review）テーブルでリンクされた名前をクリックします。

作業を開始する前に

少なくとも1つのパッチをアップロードしてインストールしておく必要があります。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [パッチ]*をクリックします。

   パッチがインストールされていない場合、現在レビュー中のパッチの表は空です。

3. [Patches currently under review]*で、現在適用されているデータソースパッチのステータスを確認します。
4. 特定のパッチに関連付けられている詳細を確認するには、パッチのリンク名をクリックします。
5. 選択したパッチについて、次のいずれかのオプションをクリックしてパッチに対して次の操作を実行できます。
   - *パッチを承認*パッチをデータソースにコミットします。
   - *ロールバック*パッチを削除します。
   - *パッチの置き換え*を使用すると、これらのデータソースに別のパッチを選択できます。

データソースパッチをコミットしています

Patches Summaryの情報を使用して、パッチが想定どおりに機能しているかどうかを判断し、パッチをネットワークにコミットします。

作業を開始する前に

パッチがインストールされている場合は、パッチが正常にインストールされ、承認が必要かどうかを判断する

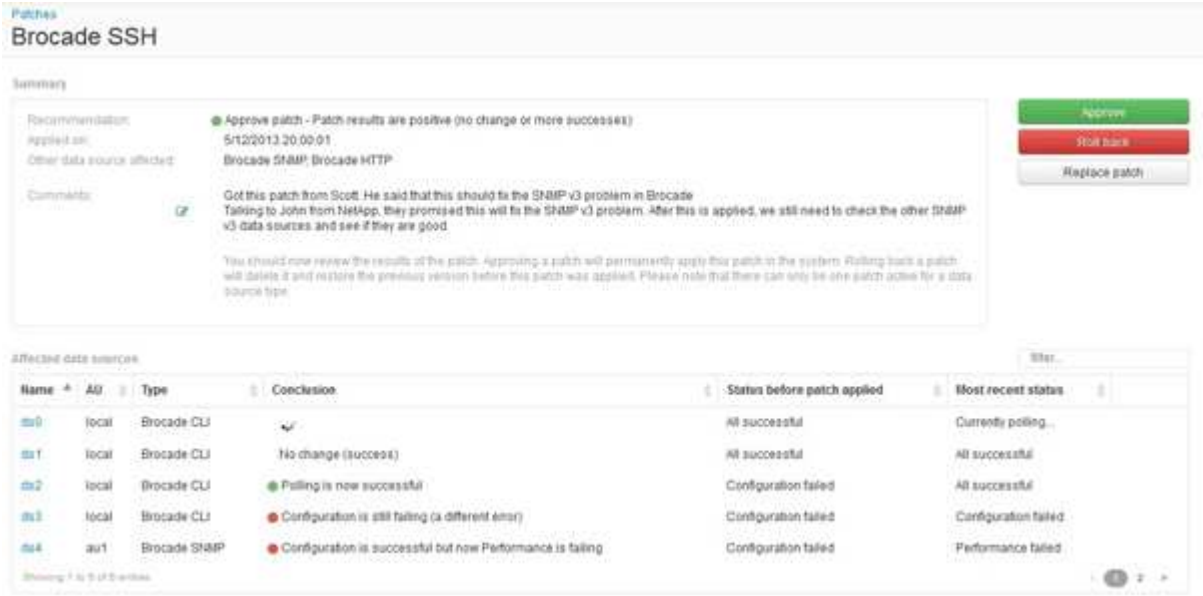
必要があります。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [パッチ]*をクリックします。

   パッチがインストールされていない場合、現在レビュー中のパッチは空です。

3. [Patches currently under review]*で、現在適用されているデータソースパッチのステータスを確認します。
4. 特定のパッチに関連付けられている詳細を確認するには、パッチのリンク名をクリックします。
5. この例に示されているパッチの概要情報で、*推奨事項*および*コメント*を確認して、パッチの進行状況を評価します。



6. 「* Data sources affected *」の表を参照して、パッチ適用前後の影響を受ける各データソースのステータスを確認します。

   パッチを適用するデータソースの1つに問題があることが懸念される場合は、[Data sources Affected]テーブルで[Linked Name]をクリックします。

7. そのタイプのデータソースにパッチを適用する必要があると判断した場合は、*[承認]*をクリックします。

   データソースが変更され、パッチが現在レビュー中のパッチから削除されます。

データソースパッチをロールバックします

データソースパッチが想定どおりに機能しない場合は、ロールバックできます。ロールバックするとパッチは削除され、パッチが適用される前のバージョンに戻ります。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。

2. [パッチ]*をクリックします。
3. [現在レビュー中のパッチ]*で、失敗したと思われるパッチのリンク名をクリックします。
4. データソースの[Patches]ページで、次の情報を確認します。
   - *概要*パッチがいつ適用されたか、影響を受けるデータソース、およびパッチに関するあなたまたはチームの他のメンバーからのコメントが記載されています。
   - *影響を受けるデータソース*には、パッチが適用されているすべてのデータソースが一覧表示され、パッチ適用前とパッチ適用後のステータスの比較が含まれます。
5. パッチの処理に失敗したデータソースの詳細を表示するには、リンクされた*[名前]*をクリックします。
   a. 概要情報を確認します。
   b. [イベントタイムライン]*で、このデータソースに影響している可能性がある設定データやパフォーマンスデータを確認します。
6. パッチが正常に終了しないと判断した場合は、ブラウザの戻る矢印をクリックしてパッチの概要ページに戻ります。
7. [ロールバック]*をクリックしてパッチを削除します。

   正常に動作する可能性が高い別のパッチがわかっている場合は、*[パッチの置き換え]*をクリックして新しいパッチをアップロードします。

デバイス解決

OnCommand Insight で監視するすべてのデバイスを検出する必要があります。環境内のパフォーマンスとインベントリを正確に追跡するには、検出が必要です。通常、環境内のほとんどのデバイスは自動デバイス解決によって検出されます。

> アップグレードを実行する際に、アップグレード元のシステムに非アクティブの自動解決ルールがあると、それらのルールはアップグレード時に削除されます。アクティブでない自動解決ルールを保持するには、アップグレードの実行前にルールをアクティブ化（チェックボックスをオンに）します。

データソースをインストールして設定すると、環境内のデバイス（スイッチ、ストレージアレイ、ハイパーバイザーとVMの仮想インフラなど）が識別されます。ただし、通常は環境内のすべてのデバイスが識別されるわけではありません。

データソースタイプのデバイスを設定したら、デバイス解決ルールを利用して環境内の残りの不明なデバイスを特定することを推奨します。デバイス解決は、次のデバイスタイプとして不明なデバイスの解決に役立ちます。

- 物理ホスト
- ストレージアレイ
- テープだ
- スイッチ

デバイス解決後に「不明」と表示されたままのデバイスは汎用デバイスとみなされ、クエリやダッシュボードにも表示できます。

似た属性の新しいデバイスが以降に環境に追加されると、作成したルールに基づいて自動的に識別されます。場合によっては、Insightで検出されないデバイスに対するデバイス解決ルールをバイパスして、手動で識別することもできます。

デバイスの識別が完了していないと、次のような問題が発生する可能性

- 不完全なパスです
- マルチパス接続が識別されない
- アプリケーションをグループ化できない
- 正確なトポロジが表示されない
- Data Warehouse や Reporting で正確なデータが表示されない

デバイス解決機能（* Manage **>** Device resolution *）には、次のタブがあります。各タブは、デバイス解決の計画と結果の表示に役割を果たします。

- 「FC Identify」には、自動デバイス解決で解決されなかったファイバチャネルデバイスのWWNとポート情報のリストが表示されます。識別されたデバイスの割合も表示されます。
- 「IP identify」には、自動デバイス解決で識別されなかったCIFS共有およびNFS共有にアクセスするデバイスのリストが含まれます。識別されたデバイスの割合も表示されます。
- 「自動解決ルール」には、ファイバチャネルデバイス解決の実行時に実行されるルールのリストが含まれます。これらのルールは、識別されないファイバチャネルデバイスを解決するために作成します。
- 「環境設定」では、環境に合わせてデバイス解決をカスタマイズするための設定オプションを提供します。

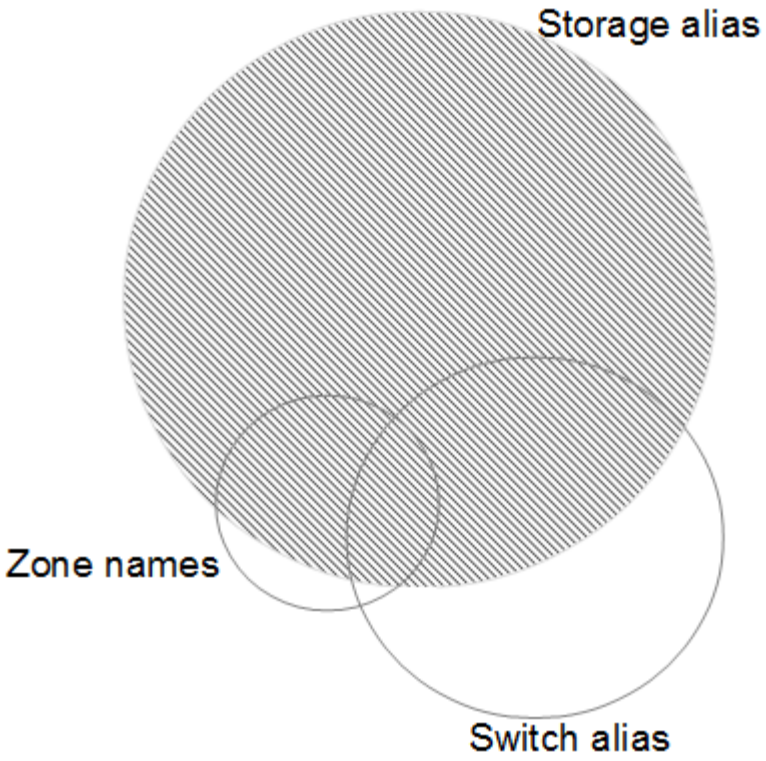
作業を開始する前に

デバイスを識別するルールを定義する前に、環境がどのように設定されているかを理解しておく必要があります。環境についての知識が多いほど、デバイスの識別が容易になります。

正確なルールを作成するには、次のような回答の質問が必要です。

- ゾーンやホストの命名基準がある場合、それらはどの程度正確であるか。
- スイッチエイリアスやストレージエイリアスを使用している場合、それらがホスト名と一致しているかどうか。
- SRMツールを使用していますか？また、SRMツールを使用してホスト名を識別できますか？SRMはどのようなカバレッジを提供しますか。
- 命名規則はどれくらいの頻度で変更されますか？
- 買収や合併によって命名規則が変わっていないかどうか。

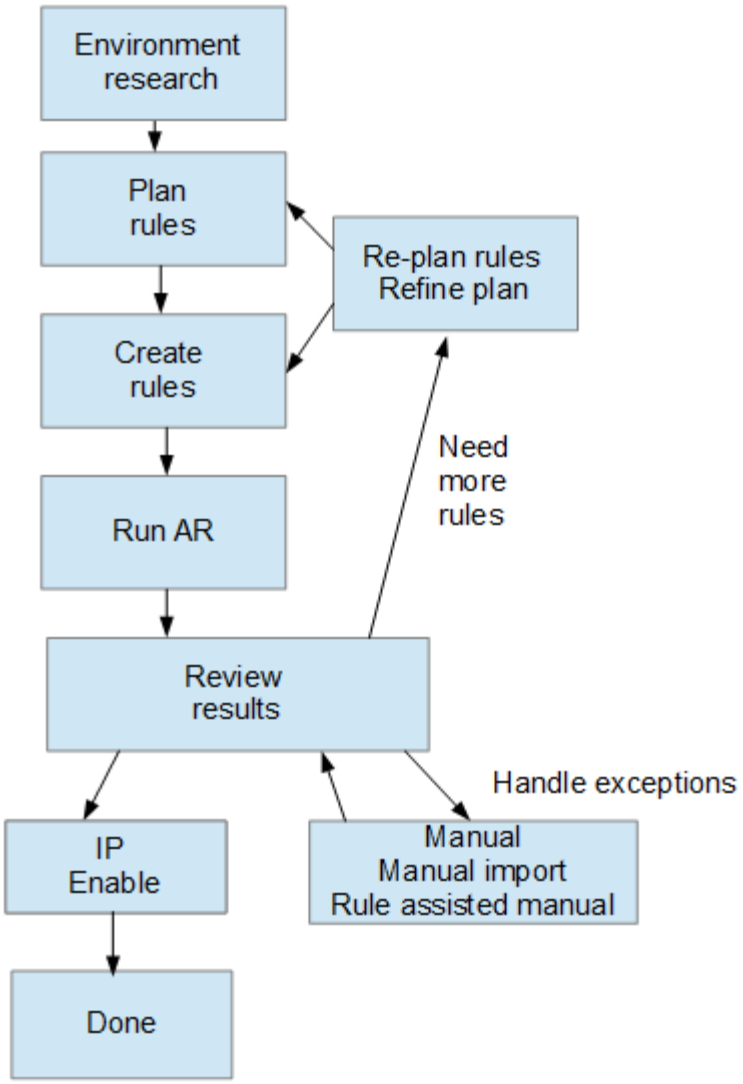
環境を分析することで、どのような命名基準があり、その信頼性がどの程度であるかを特定できるようになります。たとえば、収集した情報から、次の図のような状況であることがわかったとします。



この例では、ストレージエイリアスで最も多くのデバイスを表すことができます。ストレージエイリアスを使用してホストを識別するルールを最初に記述し、次にスイッチエイリアスを使用するルール、最後にゾーンエイリアスを使用するルールを作成します。ゾーンエイリアスやスイッチエイリアスと重なっている部分のデバイスについても、ストレージエイリアスのルールで識別できるため、ゾーンエイリアスやスイッチエイリアスに必要なルールは少なくて済みます。

環境内のデバイスを定義する手順

通常、環境内のデバイスを識別するには、次のようなワークフローを使用します。識別は反復的なプロセスであり、ルールの計画や調整が何度も必要になることがあります。



環境内に未識別のデバイス（「不明」または汎用デバイスとも呼ばれる）があり、ポーリング時にそれらのデバイスを識別するデータソースを設定すると、それらのデバイスは汎用デバイスとして表示またはカウントされなくなります。

環境に応じたデバイス解決ルールの計画

ルールを使用して環境内のデバイスを識別するプロセスは、通常は反復的なプロセスです。環境を徹底的に分析し、できるだけ多くのデバイスを識別するために複数のルールを作成する必要があります。最良のシナリオは、環境内のデバイスの100%を識別する目標を設定することです。

ルールの最も効率的な順序は、最も制限の厳しいルールを最初に配置して、ほとんどのエントリがパターンマッチングを行わないようにすることです。この場合、プロセスはより制限の厳しいルールに進みます。これにより、Insightでは各エントリにより多くのパターンを適用できるようになり、パターンマッチングやホスト識別の可能性が高まります。

ルールを作成する場合は、できるだけ多くの未識別デバイスに対応するルールを作成する必要があります。たとえば、次のようなカバレッジパターンに従うルールを作成すると、カバレッジの割合が低いルールを30個作成するよりもはるかに効率的です。

ルール	カバレッジのパーセンテージ
ルール 1	60%だ
ルール 2	25%
ルール 3	8%です
ルール4	4%です
ルール5	1%です

デバイス解決ルールを作成しています

デバイス解決ルールを作成して、OnCommand Insight で現在自動的に識別されないホスト、ストレージ、およびテープを識別します。作成したルールにより、環境内の既存のデバイスが識別されるほか、環境に追加された同様のデバイスも識別されます。

このタスクについて

ルールを作成するときは、最初に、ルールの実行対象となる情報のソース、情報の抽出に使用する方法、およびルールの結果に DNS ルックアップを適用するかどうかを特定します。

デバイスの識別に使用するソース
• ホストのSRMエイリアス • ホスト名またはテープ名が埋め込まれたストレージエイリアス • ホスト名またはテープ名が埋め込まれたスイッチエイリアス • ホスト名が埋め込まれたゾーン名
ソースからデバイス名を抽出する方法
• そのまま（SRMから名前を抽出） • 区切り文字 • 正規表現
DNS ルックアップ
DNSを使用してホスト名を確認するかどうかを指定します。

ルールは、 ［ 自動解決ルール ］ タブで作成します。以下に、ルールの作成プロセスについて説明します。

手順

1. >[デバイス解決]*をクリックします
2. タブで、+[追加]*をクリックします

   [New Rule]画面が表示されます。

   > [New Rule]画面には、正規表現を作成するためのヘルプと例を示す*？*アイコンが表示されます。

3. [* タイプ] リストで、識別するデバイスを選択します。

   [Host]または[Tape]を選択できます。

4. [* ソース *] リストで、ホストの識別に使用するソースを選択します。

   選択したソースに応じて、Insightに次の応答が表示されます。

   - [Zones]には、Insightで識別する必要があるゾーンとWWNのリストが表示されます。
   - [SRM]を選択すると、Insightで識別する必要がある未識別のエイリアスが一覧表示されます
   - [Storage alias]には、Insightで識別する必要があるストレージエイリアスとWWNのリストが表示されます
   - [Switch alias]には、Insightで識別する必要があるスイッチエイリアスのリストが表示されます

5. メソッド * リストで、ホストの識別に使用する方法を選択します。

ソース	メソッド
SRM の場合	「現状のまま」、「デリミッタ」、「正規表現」
ストレージエイリアス	"`delimiters'"、または"`regular expressions'"
スイッチエイリアス	"`delimiters'"、または"`regular expressions'"
ゾーン	"`delimiters'"、または"`regular expressions'"

   - 「デリミッタ」を使用するルールでは、デリミタとホスト名の最小長が必要です。

     ホスト名の最小文字数は、Insightでホストを識別するために使用する文字数です。Insightでは、これ以上長いホスト名に対してのみDNSルックアップが実行されます。

     delimiters を使用するルールの場合、入力文字列は区切り文字でトークン化され、ホスト名候補のリストは、隣接するトークンを複数組み合わせて作成されます。リストは、最大から最小にソートされます。たとえば、vipsnq03_hba3_emc3_12ep0の場合、リストは次のようになります。

     - vipsnq03_hba3_emc3_12ep0
     - vipsnq03_hba3_emc3
     - hba3 emc3_12ep0

        - vipsnq03_hba3.
        - emc3_12ep0
        - hba3_emc3
        - vipsnq03
        - 12ep0
        - emcs3
        - hba3.
    - 「正規表現」を使用するルールでは、正規表現、形式、および大文字と小文字の区別を選択する必要があります。
6. をクリックします ▶ Run AR すべてのルールを実行するには、ボタンの下矢印をクリックして、作成したルール（およびARの最後のフルラン以降に作成されたその他のルール）を実行します。

結果

ルールの実行結果は[FC Identify]タブに表示されます。

自動デバイス解決の更新を開始しています

デバイス解決の更新では、前回の完全な自動デバイス解決の実行後に手動で行った変更がコミットされます。更新を実行すると、デバイス解決設定に対する新しい手動のエントリのみをコミットして実行できます。完全なデバイス解決は実行されません。

手順

1. Insight Web UIにログインします。
2. >[デバイス解決]*をクリックします
3. [デバイスの解像度]画面で、[ARの実行]ボタンの下矢印をクリックします。
4. アップデートを開始するには、 * アップデート * をクリックします。

ルールに基づく手動識別

この機能は、不明なホスト、ストレージ、テープデバイス、またはそれらのグループを解決するために特定のルールまたはルールのリスト（1回限りの順序変更の有無に関係なく）を実行する特殊なケースで使用されます。

作業を開始する前に

識別されていないデバイスが多数あり、他のデバイスを正しく識別した複数のルールがある場合。

このタスクについて

> ソースにホスト名またはデバイス名の一部だけが含まれている場合は、正規表現のルールを使用して欠落しているテキストを追加するように形式を変更します。

手順

1. OnCommand Insight Web UIにログインします。
2. **>**[デバイス解決]*をクリックします
3. [FC Identify]*タブをクリックします。

   識別されたデバイスと識別されていないデバイスが表示されます。

4. 識別されていない複数のデバイスを選択
5. **>**[ホスト解決の設定]または>[テープ解決の設定]*をクリックします

   識別画面が表示され、デバイスを正しく識別したすべてのルールのリストが表示されます。

6. ルールの順序を、ニーズに合った順序に変更します。

   ルールの順序は識別画面で変更されますが、グローバルには変更されません。

7. ニーズに合った方法を選択します。

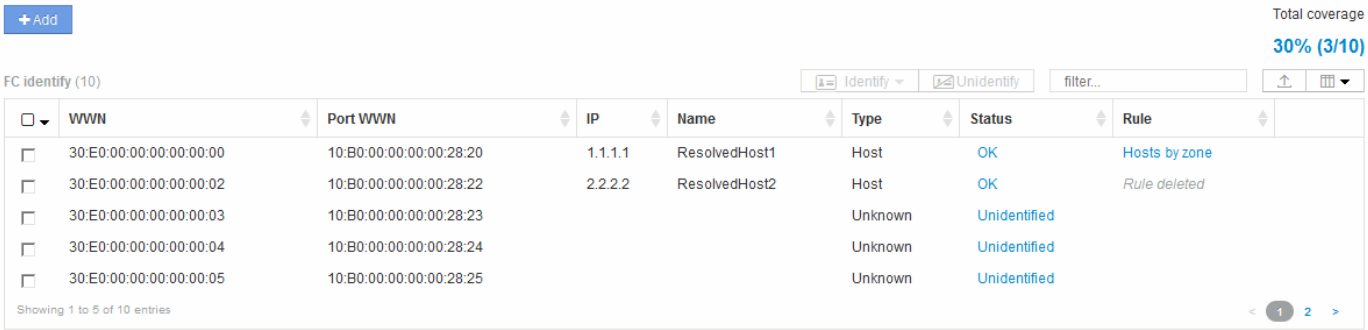
   OnCommand Insight は、一番上のメソッドから順にホスト解決プロセスを実行します。

   適用されるルールが検出されると、ルールの名前がルールの列に表示され、手動で識別されます。

ファイバチャネルデバイスの解決

[FC Identify]画面には、自動デバイス解決でホストが識別されていないFibre ChannelデバイスのWWNとWWPNが表示されます。この画面には、手動デバイス解決で解決されたデバイスも表示されます。

手動解決によって解決されたデバイスには「OK」のステータスが含まれ、デバイスの識別に使用されたルールが示されます。検出されなかったデバイスのステータスは「Unidentified」になります。このページには、デバイスの識別範囲の合計が表示されます。



一括操作を実行するには、[FC Identify]画面の左側で複数のデバイスを選択します。1つのデバイスでアクションを実行するには、デバイスにカーソルを合わせ、リストの右端にある[Identify]または[Unidentify]ボタンを選択します。

[Total coverage]リンクには、構成の「識別されたデバイス数/使用可能なデバイス数」のリストが表示されます。

- SRM エイリアス
- ストレージエイリアス
- スイッチエイリアス
- ゾーン
- ユーザ定義

ファイバチャネルデバイスを手動で追加する

ファイバチャネルデバイスは、[Device resolution FC Identify]タブの手動追加機能を使用してOnCommand Insight に手動で追加できます。このプロセスは、今後検出されることが予想されるデバイスの事前識別に使用される場合があります。

作業を開始する前に

システムにデバイス識別情報を追加するには、 WWN または IP アドレスとデバイス名を確認しておく必要があります。

このタスクについて

ホスト、ストレージ、テープ、または不明なFibre Channelデバイスは手動で追加できます。

手順

1. Insight Web UIにログインします
2. **>**[デバイス解決]*をクリックします
3. [FC Identify]*タブをクリックします。
4. 追加ボタンをクリックします。

   Add Device ダイアログが表示されます

5. WWN または IP アドレスとデバイス名を入力し、デバイスタイプを選択します。

結果

入力したデバイスが[FC Identify]タブのデバイスのリストに追加されます。"`Rule'"はManualとして識別されます。

CSVファイルからのファイバチャネルデバイス識別情報のインポート

CSVファイル内のデバイスのリストを使用して、ファイバチャネルデバイスの識別情報をOnCommand Insight デバイス解決機能に手動でインポートできます。

作業を開始する前に

デバイス識別情報をデバイス解決機能に直接インポートするには、正しくフォーマットされたCSVファイルが必要です。ファイバチャネルデバイスのCSVファイルには、次の情報が必要です。

WWN
IP
名前
を入力します

> 最初に[FC Identify]の情報をCSVファイルにエクスポートし、そのファイルに必要な変更を加えてから、そのファイルを[FC Identify]にインポートし直すことを推奨します。これにより、必要な列が適切な順序で配置されます。

[FC Identify]の情報をインポートするには

手順

1. Insight Web UIにログインします。
2. **>**[デバイス解決]*をクリックします
3. [FC Identify]*タブを選択します。
4. 識別>*ファイルから識別*をクリックします
   .
   a. インポートするCSVファイルが格納されているフォルダに移動し、目的のファイルを選択します。

   入力したデバイスが[FC Identify]タブのデバイスのリストに追加されます。「ルール」は「手動」として識別されます。

ファイバチャネルデバイスの識別情報を**CSV**ファイルにエクスポートしています

OnCommand Insight デバイス解決機能から、既存のファイバチャネルデバイスの識別情報をCSVファイルにエクスポートできます。エクスポートしたデバイス識別情報を変更してInsightに再度インポートすると、識別情報がエクスポートされたデバイスと類似したデバイスの識別に使用されます。

このタスクについて

このシナリオは、デバイスに同様の属性があり、CSVファイルで簡単に編集してからシステムにインポートできる場合に使用します。

ファイバチャネルデバイスの識別情報をCSVファイルにエクスポートすると、ファイルには次の情報が記載された順序で格納されます。

WWN
IP

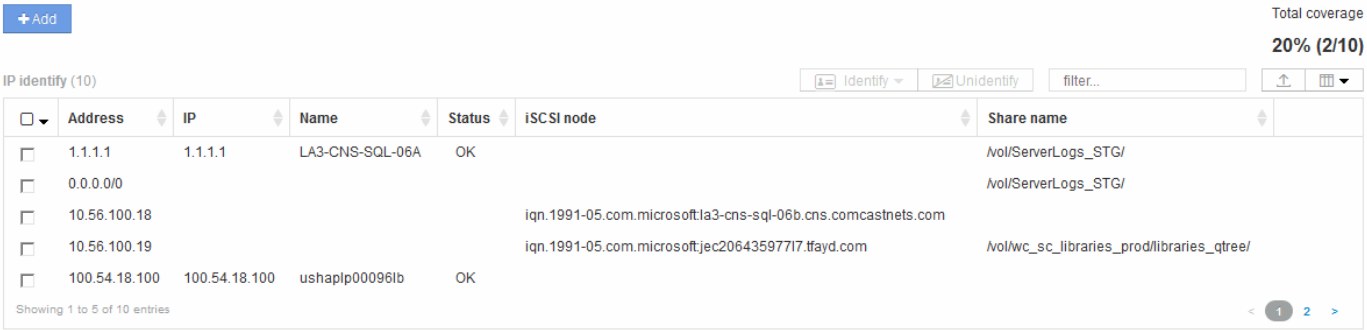
名前
を入力します

手順

1. Insight Web UIにログインします。
2. **>**[デバイス解決]*をクリックします
3. [FC Identify]*タブを選択します。
4. 識別情報をエクスポートする 1 つ以上のファイバチャネルデバイスを選択します。
5. エクスポートをクリックします をクリックします。
6. CSVファイルを開くか、ファイルを保存するかを選択します。

IP デバイスの解決

IP の識別画面には、自動デバイス解決または手動デバイス解決によって識別された iSCSI 共有と CIFS 共有または NFS 共有が表示されます。また、未識別のデバイスも表示されます。画面には、デバイスの IP アドレス、名前、ステータス、 iSCSI ノード、および共有名が表示されます。識別に成功したデバイスの割合も表示されます。



IP デバイスを手動で追加する

[IP Identify]画面の手動追加機能を使用して、IPデバイスをOnCommand Insight に手動で追加できます。

手順

1. Insight Web UIにログインします。
2. **>**[デバイス解決]*をクリックします
3. [IP Identify]*タブをクリックします。
4. 追加ボタンをクリックします。

   Add Device ダイアログが表示されます

5. アドレス、 IP アドレス、および一意のデバイス名を入力します。

結果

入力したデバイスが[IP Identify]タブのデバイスのリストに追加されます。

CSVファイルからの**IP**デバイス識別情報のインポート

CSVファイルのデバイス識別情報のリストを使用して、IPデバイス識別情報をデバイス解決機能に手動でインポートできます。

作業を開始する前に

デバイスの識別情報をインポートするには、正しい形式のCSVファイルが必要です。IPデバイスのCSVファイルには、次の情報が必要です。

住所
IP
名前

> 最初に[IP Identify]の情報をCSVファイルにエクスポートし、そのファイルに必要な変更を加えてから、[IP Identify]にファイルをインポートし直すことを推奨します。これにより、必要な列が適切な順序で配置されます。

IP識別情報をインポートするには：

手順

1. Insight Web UIにログインします。
2. **>**[デバイス解決]*をクリックします
3. [IP Identify]*タブを選択します。
4. 識別>*ファイルから識別*をクリックします
.

   a. インポートするCSVファイルが格納されているフォルダに移動し、目的のファイルを選択します。

   入力したデバイスが[IP Identify]タブのデバイスのリストに追加されます。

CSVファイルへの**IP**デバイス識別情報のエクスポート

デバイス解決機能を使用して、Insightから既存のIPデバイス識別情報をエクスポートできます。エクスポートしたデバイス識別情報を変更してInsightに再度インポートして、識別情報をエクスポートしたデバイスと類似したデバイスの識別に使用できるようにすることができます。

このタスクについて

IPデバイスの識別情報をCSVファイルにエクスポートすると、ファイルには次の情報が記載された順序で格納されます。

住所
IP
名前

手順

1. Insight Web UIにログインします。
2. **>**[デバイス解決]*をクリックします
3. [IP Identify]*タブを選択します。
4. 識別情報をエクスポートする IP デバイスを選択します。
5. エクスポートをクリックします をクリックします。
6. CSVファイルを開くか、ファイルを保存するかを選択します。

[環境設定 **]** タブでオプションを設定します

デバイス解決のプリファレンスタブでは、自動解決スケジュールの作成、識別情報を含めるストレージベンダーやテープベンダーの指定、および DNS 検索オプションの設定を行うことができます。

自動解決スケジュール

自動デバイス解決を実行するスケジュールを指定できます。

オプション	説明
間隔	曜日、時間、または分単位で自動デバイス解決を実行する場合は、このオプションを使用します。
毎日	このオプションは、自動デバイス解決を特定の時刻に毎日実行する場合に使用します。
手動で実行する	このオプションは、自動デバイス解決を手動でのみ実行する場合に使用します。
環境が変化するたびに	このオプションは、環境に変更があったときに自動デバイス解決を実行する場合に使用します。

手動でを指定すると、夜間の自動デバイス解決は無効になります。

DNS の処理オプション

DNS の処理オプションでは、次の機能を選択できます。

- DNS ルックアップの結果の処理を有効にすると、解決されたデバイスに付加する DNS 名のリストを追加できます。
- 「IPの自動解決：」を選択すると、DNSルックアップを使用して、iSCSIイニシエータおよびNFS共有にアクセスするホストに対して自動ホスト解決を有効にできます。指定しない場合は、 FC ベースの解決のみが実行されます。
- ホスト名にアンダースコアを使用できるようにすることも、標準のポートエイリアスの代わりに「接続先」のエイリアスを使用することもできます。

ストレージやテープの特定のベンダーを含めるか、除外します

ストレージやテープの特定のベンダーを自動解決の対象に含めたり除外したりできます。レガシーホストとなり、新しい環境から除外する必要があることがわかっているホストがある場合などは、特定のベンダーを除外することができます。除外したベンダーを再度追加することもできます。

> テープのデバイス解決ルールは、ベンダー環境設定でそのWWNのベンダーが*テープのみとして含まれる*に設定されているWWNに対してのみ機能します。

正規表現の例

ソースの命名方法として正規表現のアプローチを選択した場合は、OnCommand Insight の自動解決方法で使用する独自の式のガイドとして正規表現の例を使用できます。

正規表現の形式

OnCommand Insight の自動解決の正規表現を作成する場合は、というフィールドに値を入力して出力形式を設定できます `FORMAT`。

デフォルト設定はです `\1` これは、正規表現に一致するゾーン名が、正規表現で作成された最初の変数の内容で置換されることを意味します。正規表現では、かっこで囲まれた記述で変数の値が作成されます。かっこで囲まれた記述が複数ある場合、変数は左から右に数値で参照されます。変数は、任意の順序で出力形式で使用できます。定数テキストは、に追加して出力に挿入することもできます `FORMAT` フィールド。

たとえば、このゾーンの命名規則には、次のようなゾーン名があります。

```
[Zone number]_[data center]_[hostname]_[device type]_[interface number]
```

- S123_Miami_hostname1_filer_FC1 のように入力します
- S14_Tampa_hostname2_switch_fc4
- S3991_Boston_hostname3_windows2K_FC0
- S44_Raleigh_hostname4_Solaris_FC1

出力形式は次のようになります。

```
        [hostname]-[data center]-[device type]
```

そのためには、ホスト名、データセンター、およびデバイスタイプのフィールドを変数に取り込み、それらを使用して出力する必要があります。正規表現は次のようになります。

```
.*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
```

括弧が3組あるので、変数です `\1`、 `\2` および `\3` 人口が増えるでしょう

この場合、次の形式で出力を受け取ることができます。

```
\2-\1-\3
```

出力は次のようになります。

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

変数間のハイフンは、出力に一定のテキストを挿入した例を示します。

例 **1** ：ゾーン名の例

この例では、正規表現を使用してゾーン名からホスト名を抽出します。次のようなゾーン名がある場合は、正規表現を作成できます。

- S0032_myComputer1Name - HBA0
- S0434_myComputer1Name - HBA1
- S0432_myComputer1Name - HBA3

ホスト名を取り込むための正規表現は次のようになります。

```
 S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
```

これは、先頭の文字が「 S 」で、そのあとに任意の桁数の数字、アンダースコア、英数字のホスト名（ myComputer1Name ）、アンダースコアまたはハイフン、大文字の「 HBA 」、 1 桁の数字（ 0~9 ）の順に続くすべてのゾーンに一致します。ホスト名のみが変数 **\1** に格納されます。

正規表現は次のように構成要素に分割できます。

- 「 S 」はゾーン名の先頭の文字を表します。これは、ゾーン名の先頭にある「 S 」にのみ一致します。

- 角かっこで囲まれた文字 [0-9] は、「 S 」のあとの文字が 0~9 の数字でなければならないことを示します。
- + 記号は、前の角かっこ内の情報が 1 回以上存在している必要があることを示します。
- （アンダースコア）は、「 S 」のあとの数字の直後に続くゾーン名の文字がアンダースコアでなければならないことを意味します。この例のゾーンの命名規則では、ゾーン名とホスト名の区切りにアンダースコアが使用されています。
- 必須のアンダースコアのあとにあるかっこは、そのかっこで囲まれたパターンが変数 \1 に格納されることを示します。
- 角かっこで囲まれた文字 [a-zA-Z0-9] は、すべての英字（大文字と小文字の両方）と数字に一致することを示します。
- 角かっこのあとの「 * 」（アスタリスク）は、角かっこで囲まれた文字の 0 回以上の繰り返しを示します。
- 角かっこで囲まれた文字 [__] （アンダースコアとダッシュ）は、英数字のパターンのあとにアンダースコアまたはダッシュが必要であることを示します。
- 正規表現内の文字列「 HBA 」は、この文字列そのものがゾーン名に含まれている必要があることを示します。
- 最後の角かっこで囲まれた文字 [0-9] は、 0~9 の 1 桁の数字に一致します。

例 **2**

この例では、最初のアンダースコアのあとの「 E 」から 2 番目ののの前までの部分を照合し、それよりも前とあとの部分は省いています。

ゾーン： `Z_E2FHDBS01_E1NETAPP`

ホスト名： `E2FHDBS01`

- RegExp：`*.?(E.?).*?`

例 **3**

正規表現の最後のセクションの前後にあるかっこ（）は、どの部分がホスト名であるかを識別します。「 VSAN3 」の部分がホスト名である場合は、 _ （ [a-zA-Z0-9] ） .* となります

ゾーン： `A_VSAN3_SR48KENT_A_CX2578_SPA0`

ホスト名： `SR48KENT`

- RegExp：`*_[a-zA-Z0-9]+_([a-zA-Z0-9]).*`

例 **4** は、複雑な命名パターンを示しています

次のようなゾーン名がある場合は、正規表現を作成できます。

- myComputerName123 ： HBA1_Symm1_FA3
- myComputerName123 ： HBA2_Symm1_FA5
- myComputerName123 ： HBA3_Symm1_FA7

これらを取り込むために使用できる正規表現は次のとおりです。

```
([a-zA-Z0-9]*)_.*
```

。 `\1` 変数にはのみが含まれます `myComputerName123` この式で評価された後。

正規表現は次のように構成要素に分割できます。

- かっこは、そのかっこで囲まれたパターンが変数 \1 に格納されることを示します。
- 角かっこで囲まれた文字 [a-zA-Z0-9] は、任意の英字（大文字と小文字の両方）と数字に一致することを示します。
- 角かっこのあとの「 * 」（アスタリスク）は、角かっこで囲まれた文字の 0 回以上の繰り返しを示します。
- 正規表現内の文字（アンダースコア）は、その前の角かっこの部分で照合された英数字の文字列の直後に続くゾーン名の文字がアンダースコアでなければならないことを意味します。
- 。（ピリオド）は、任意の文字（ワイルドカード）に一致します。
- 「 * 」（アスタリスク）は、その前のピリオド（ワイルドカード）が 0 回以上続くことを示します。

  つまり、「 .* 」の組み合わせは任意の文字数の任意の文字を表します。

例 **5** ：パターンがないゾーン名の例

次のようなゾーン名がある場合は、正規表現を作成できます。

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

これらを取り込むために使用できる正規表現は次のとおりです。

```
(.*?)_.*
```

変数 \1 には、 *myComputerName* （ 1 つ目のゾーン名の例）または *myComputerName123* （ 2 つ目のゾーン名の例）が格納されます。したがって、この正規表現は、最初のアンダースコアの前のすべての部分に一致します。

正規表現は次のように構成要素に分割できます。

- かっこは、そのかっこで囲まれたパターンが変数 \1 に格納されることを示します。
- 「 .* 」（ピリオドとアスタリスク）は、任意の文字数の任意の文字に一致します。
- 角かっこのあとの「 * 」（アスタリスク）は、角かっこで囲まれた文字の 0 回以上の繰り返しを示します。
- 。文字は、最短一致を示します。これにより、最後のアンダースコアではなく、最初のアンダースコアでの照合が強制的に停止されます。
- 文字「 _.* 」は、最初のアンダースコア以降のすべての文字に一致します。

例 **6** ：パターンを含むコンピュータ名の例

次のようなゾーン名がある場合は、正規表現を作成できます。

- Storage1_Switch1_myComputerName123A_A1_FC1
- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

これらを取り込むために使用できる正規表現は次のとおりです。

```
.*?_.*?_([a-zA-Z0-9]*[ABT])_.*
```

このゾーンの命名規則には特定のパターンがあるため、上記の式を使用できます。この式は「 A 」、「 B 」、または「 T 」のいずれかで終わるすべてのホスト名（この例では「 myComputerName 」）に一致し、そのホスト名を変数 \1 に格納します。

正規表現は次のように構成要素に分割できます。

- 「 . * 」（ピリオドとアスタリスク）は、任意の文字数の任意の文字に一致します。
- 。文字は、最短一致を示します。これにより、最後のアンダースコアではなく、最初のアンダースコアでの照合が強制的に停止されます。
- アンダースコア文字は、ゾーン名の最初のアンダースコアに一致します。
- したがって、最初の.*？_の組み合わせは、最初のゾーン名の例にある_Storage1_と一致します。
- 2つ目の.*？_の組み合わせは1つ目のゾーン名と同じように動作しますが、1つ目のゾーン名の例では_Switch1_に一致します。
- かっこは、そのかっこで囲まれたパターンが変数 \1 に格納されることを示します。
- 角かっこで囲まれた文字 [a-zA-Z0-9] は、任意の英字（大文字と小文字の両方）と数字に一致することを示します。
- 角かっこのあとの「 * 」（アスタリスク）は、角かっこで囲まれた文字の 0 回以上の繰り返しを示します。
- 正規表現内の角かっこで囲まれた文字 [ABT] は、ゾーン名に含まれる「 A 」、「 B 」、または「 T 」のいずれか 1 文字に一致します
- かっこのあとの（アンダースコア）は、 [ABT] で照合された文字のあとにアンダースコアが必要であることを示します。
- 「 . * 」（ピリオドとアスタリスク）は、任意の文字数の任意の文字に一致します。

その結果、次のいずれかの英数字文字列を含む変数 \1 が原因されます。

- 前に任意の数の英数字と 2 つのアンダースコアがある
- 後ろにアンダースコア（および任意の数の英数字）がある。
- 3 番目のアンダースコアの前に、 A 、 B 、または T の最後の文字を使用した。

例 **7**

ゾーン： `myComputerName123_HBA1_Symm1_FA1`

ホスト名： `myComputerName123`

- RegExp：`*([a-zA-Z0-9]+)_.*`

例 **8**

この例では、最初ののの前のすべての部分を検出します。

ゾーン： `MyComputerName_HBA1_Symm1_FA1`

`MyComputerName123_HBA1_Symm1_FA1`

ホスト名： `MyComputerName`

- RegExp：`*(.?)_.`

例**9**

この例では、最初ののののあとから2番目ののの前までのすべての部分を検出します。

ゾーン： `Z_MyComputerName_StorageName`

ホスト名： `MyComputerName`

- RegExp：`*.?(.?).*?`

例 **10**

この例では、ゾーンの例から「 MyComputerName123 」を抽出します。

ゾーン： `Storage1_Switch1_MyComputerName123A_A1_FC1`

`Storage2_Switch2_MyComputerName123B_A2_FC2`

`Storage3_Switch3_MyComputerName123T_A3_FC3`

ホスト名： `MyComputerName123`

- RegExp：`*.?.?([a-zA-Z0-9]+)[ABT]_.`

例 **11**

ゾーン： `Storage1_Switch1_MyComputerName123A_A1_FC1`

ホスト名： `MyComputerName123A`

- RegExp：`*.?.?([a-zA-z0-9]+).*?`

例 **12**

角かっこ*の中の^（円弧またはキャレット）*は、式を否定します。たとえば、[^FF]は大文字または小文字のFを除くすべてを意味し、[^a-z]は小文字のaからzを除くすべてを意味し、上記の場合は_以外のすべてを意味します。format ステートメントは、出力ホスト名にを追加します。

ゾーン： `mhs_apps44_d_A_10a0_0429`

ホスト名： `mhs-apps44-d`

- RegExp：* `([^_])_([AB]).*`+OnCommand Insight での形式：

`([^_])_().*`OnCommand Insight での形式：

例 **13**

この例では、ストレージエイリアスの区切りにが使用されています。この場合、が文字列で実際に使用されており、式の一部ではないことを示すために、を使用する必要があります。

ストレージエイリアス： `\Hosts\E2DOC01C1\E2DOC01N1`

ホスト名： `E2DOC01N1`

- RegExp：* `\\.?\\.?\\(.*?)`

例 **14**

この例では、ゾーンの例から「 PD-RV-W-AD-2 」を抽出します。

ゾーン： `PD_D-PD-RV-W-AD-2_01`

ホスト名： `PD-RV-W-AD-2`

- RegExp：* `[^-]-(.-\d+).`+

例 **15**

この例では、形式の設定でホスト名に「 US-BV- 」を追加しています。

ゾーン： `SRV_USBVM11_F1`

ホスト名： `US-BV-M11`

- RegExp：* `SRV_USBV([A-Za-z0-9]+)_F[12]`

形式： `US-BV-\1`

Insightのメンテナンス

Insightを初めて導入し、システムを新規にセットアップする場合でも、システムを以前

から運用していた場合でも、Insightとネットワークの円滑な運用を維持するための措置を講じる必要があります。メンテナンスの重要な概念は、通常はネットワークの変更にInsightで対応する必要があるということです。

最も一般的なメンテナンスタスクは次のとおりです。

- Insightのバックアップの保持
- 期限切れのInsightライセンスを更新しています
- データソースパッチの調整
- すべてのAcquisition UnitでInsightのバージョンを更新しています
- 削除したデータソースをInsightから削除しています

Insightの管理

OnCommand Insight は環境を監視し、危機が報告される前に潜在的な問題を調査できるようにします。[Assets Dashboard]には、概要を示す円グラフ、IOPSのヒートマップ、および利用率が高い上位10個のストレージプールを示す対話型のグラフが表示されます。

手順

1. Insight **Assets Dashboard** を開き、円グラフの上にカーソルを移動して、次の3つのグラフでアセットの分布を確認します。
   - [Capacity by Vendor]には、各ベンダーのストレージの合計物理容量が表示されます。
   - [Capacity by Tier]には、各ストレージ階層の使用可能な合計容量が表示されます。
   - [Switch Ports]円グラフには、ポートのメーカーと使用済みポートの割合が表示されます。
2. [Facts About Your Environment]*を表示して、環境の使用済み容量、容量の効率、消費されているFCリソース、および仮想インフラの統計に関する情報を確認できます。
3. [Top 10 Utilized Pools]*グラフのストレージプールのバーにカーソルを合わせ、ストレージプールの使用済み容量と未使用容量を確認します。
4. [Storage IOP]*ヒートマップで大きな文字で表示されているアセット（問題のあるアセット）の名前をクリックすると、そのアセットの現在の状態をまとめたページが表示されます。
5. の右下隅にある[Virtual Machine IOPS]*ヒートマップで、大きなテキストで表示されているアセット（問題のあるアセット）の名前をクリックすると、アセットの現在の状態をまとめたページが表示されます。
6. Insightのツールバーで、*[Admin]*をクリックします。
7. 赤い丸が表示されている領域に注意してください。

   OnCommand InsightWeb UIでは、潜在的な問題が赤い丸で示されます。

8. [データソース]*をクリックして、監視しているすべてのデータソースのリストを確認します。

   [ステータス]*列に赤い丸で囲まれたメッセージが表示され、[影響]*が[高]または[中]になっているデータソースを確認します。これらはテーブルの上にあります。これらのデータソースの問題は、ネットワークの大部分に影響を及ぼします。この問題に対処する必要があります。

9. [Acquisition Units]*をクリックして、Insightを実行している各IPアドレスのステータスを確認し、必要に応じてAcquisition Unitを再起動します
10. Insightサーバのインスタンス監視の概要を表示するには、*[健全性]*をクリックします。

OnCommand Insight システムヘルスを監視しています

Insightシステムコンポーネントの現在のステータスを[Health]ページで定期的に確認する必要があります。このページには、各コンポーネントのステータスが表示され、問題 がある場合はアラートが表示されます。

手順

1. InsightWeb UIにログインします。
2. をクリックし、[ヘルス]*を選択します。

   [Health]ページが表示されます。

3. コンポーネントの現在のステータスを確認します。[* Details]*列のステータスの前に赤い丸が表示されている場合は、すぐに対処が必要な問題 を示しているため、特に注意してください。

   [Health]ページには、Insightのコンポーネントのうち、システム構成に基づいて次のいずれかまたはすべてのコンポーネントに関する情報が表示されます。

コンポーネント	テスト	詳細	表示されます
取得	インベントリデータの処理	Local Acquisition Unitのステータス	同時にポーリングするデータソースの数が実行プールの最大数の75%未満（デフォルトの最大数は30）の場合、「OK」。「Acquisition is busy」は、使用率が75%を超える場合に使用します。ポーリング間隔を長くするか、Remote Acquisition Unitを追加することを推奨します。
DWH	バックアップ	Data Warehouseのスケジュールされたバックアップのステータス	DWHのスケジュールされたバックアップが有効になっている場合は、「OK」と前回成功したDWHのバックアップ時刻が表示されます。それ以外の場合は、検出されたエラーに関する情報が表示されます。

DWH	ETL	Data WarehouseのETLのステータス	「OK」と、エラーがなければ前回成功したDWHのビルド時間が表示されます。それ以外の場合は、検出されたエラーに関する情報が表示されます。
サーバ	ASUP	ASUPのステータス	「ASUP Enabled」と前回成功したPhonehome時間（該当する場合）。「ASUP Failed」は、Phonehomeが有効になっているが問題が発生した場合に表示されます。 +バックアップディレクトリが無効な場合は、「Invalid backup location（バックアップの場所が無効です）」。 + Phonehomeが最後に成功した時刻と、最後に失敗した時刻（使用可能な場合）を表示します。 +「ASUP Disabled」（Phonehomeが無効な場合）
サーバ	自動解決	自動デバイス解決のステータス	エラーがなければ「OK」。識別エラーが解決の進行を妨げている場合は、「自動解決はブロックされています」と表示されます。 一般的なデバイスの75%未満を識別できる場合は、+"`Low success rate'"。

サーバ	Elasticsearch を指定します	Elasticsearchデータストアのステータス	エラーがなければ「OK」。Elastic Searchサービスに接続できない場合は、「Service Unavailable」と入力します。 +複数のノードが検出された場合は「Cluster mode detected」 +「High memory utilization」（ヒープ領域の使用率が85%を超えている場合） +「ステータス：赤」は、Elasticsearchでエラーが報告されたことを示します。エラーに関する情報を表示し、カスタマーサポートに問い合わせることを推奨します。
サーバ	CPU	InsightのCPU使用率	CPU負荷が65%未満の場合は「OK」。"`SシステムのCPU負荷が高くなっています。CPUの負荷を軽減します。 CPU負荷が65%を超えている場合。
サーバ	ディスクスペース	ディスクスペースのステータス	空きディスクスペース、Insightで使用されているディスクスペース、およびInsight用に予約されている推奨ディスクスペース。ディスク使用率が80%を超えている場合は「Low Disk Space（ディスクスペースが不足しています）」。
サーバ	EventBusの略	EventBusのステータス	EventBusキューが空の場合は「`EventBus is empty`」、それ以外の場合はEventBusキューのステータスが表示されます。

サーバ	インベントリデータの処理	Insight Serverのインベントリデータ処理機能のステータス	Insight Serverがビジー状態でない場合は「OK」。サーバが過去1時間の75%以上の時間でビジー状態になっている場合、「サーバはビジー状態です」と表示されます。では、データソースを追加しないようにし、環境を複数のサーバに分割することを推奨しています。
サーバ	MySQL	MySQLデータベースのステータス	問題が検出されない場合は「OK」。"'データベースにパフォーマンスの問題があります。低速クエリの数が5%を超えると、一部のクエリの実行に時間がかかりすぎます。 +"'データベース・ログ・ファイルが過去1時間に<size> を超えて増加しましたエラーログが20 KBを超える場合は、MySQLログファイルを確認してください。
サーバ	パフォーマンスアーカイブ	パフォーマンスアーカイブのステータス	「Performance archive is enabled」または「Performance archive is not enabled」というメッセージが表示されます。
サーバ	物理メモリ	物理メモリのステータス	メモリ使用率が85%未満の場合は「OK」。"`memory usage is high.メモリ使用率が85%を超える場合は、システムの安定性のために全体的なメモリフットプリントを削減します。

サーバ	サービスパック	サービスパックの有無	Insightで使用可能なサービスパックがあるかどうかが表示されます。サービスパックが使用可能な場合は、指示が表示されます。
サーバ	使用状況の情報	使用状況情報の送信ステータス	使用状況に関する情報のネットアップへの送信が有効か無効かが表示されます。無効な場合は有効にすることをお勧め最後に試行された、または最後に成功した送信時刻を表示します +発生した問題に関する情報を表示します。
サーバ	違反です	未解決の違反のステータス	未解決の違反の数が上限の75%未満の場合は「OK」。未解決の違反の数が上限の75%を超えている場合は、「Maximum number of open violations allowed is <number> 」と表示されます。パフォーマンスポリシーの設定を確認することを推奨します。 +「違反マネージャはブロックされています」は、未解決の違反の数が上限に達している場合に表示されます。 +新しい違反は作成できないので、パフォーマンスポリシーの設定を確認することを推奨します。
サーバ	週次バックアップ	週次バックアップのステータス	週次バックアップが有効になっている場合は「OK」、有効になっていない場合は「週次バックアップは有効になっていません」と表示されます。

非アクティブなデバイスの削除

使用されていないデバイスを削除すると、データをクリーンに保ち、ナビゲートしやすくなります。

このタスクについて

Insightから非アクティブなデバイスを削除するには、次の手順を実行します。

手順

1. 新しいクエリを作成するか、既存のクエリを開きます。
2. [*generic device*]、[*host*]、[*storage*]、[*switch*]、または[_tape_asset]のいずれかのタイプを選択します。
3. 「* is active 」のフィルタを追加し、フィルタを「 No *」に設定します。

   結果テーブルには、アクティブでないアセットのみが表示されます。

4. 削除するデバイスを選択します。
5. [Actions]ボタンをクリックし、[Delete Inactive Devices]を選択します。

   非アクティブなデバイスは削除され、Insightに表示されなくなります。

システムおよびユーザアクティビティの監査

予期しない変更を特定する場合は、OnCommand Insight システムとそのユーザアクティビティの監査証跡を表示できます。監査ログメッセージは、[Audit]ページに表示されるだけでなく、syslogに送信することもできます。

このタスクについて

Insightでは、ストレージネットワークやストレージネットワークの管理に影響するユーザアクティビティについて、次のような監査エントリが生成されます。

- ログインしています
- パスの許可または許可解除
- 許可されたパスの更新
- グローバルなポリシーまたはしきい値を設定します
- データソースの追加または削除
- データソースを開始または停止します
- データソースのプロパティを更新しています
- タスクの追加、編集、または削除
- アプリケーショングループを削除しています
- デバイスの ID を識別または変更する

- ユーザを作成します
- ユーザを削除します
- ユーザロールの変更
- ユーザの変更（Guest à Admin）
- ユーザからのログアウト（強制ログアウトまたは手動ログアウト）
- Acquisition Unitの削除
- ライセンスの更新
- バックアップを有効にします
- バックアップの無効化
- ASUPの有効化（同じページでプロキシの有効化が監査ログに報告される）
- ASUPの無効化（同じページでプロキシの無効化が監査ログに報告される）
- セキュリティキーの再作成、システムパスワードの変更
- アセットのアノテーションを削除/追加しています
- CACユーザーのログオン/ログオフ
- CACユーザセッションタイムアウト

手順

1. ブラウザでInsightを開きます。
2. をクリックし、[Audit]*を選択します。

   [監査]ページでは、監査エントリが表形式で表示されます。

3. テーブルでは、次の詳細を確認できます。

   - * 時間 *

     変更が行われた日時

   - * ユーザー *

     監査エントリに関連付けられているユーザの名前

   - * 役割 *

     ユーザアカウントのロール（ゲスト、ユーザ、または管理者）

   - * IP *

     監査エントリに関連付けられているIPアドレス

   - * アクション *

     監査エントリのアクティビティのタイプ

- * 詳細 *

  監査エントリの詳細

  データソースやアプリケーションなどのリソースに影響するユーザアクティビティがある場合は、そのリソースのランディングページへのリンクが詳細に表示されます。

  > データソースを削除すると、そのデータソースに関連するユーザアクティビティの詳細にデータソースのランディングページへのリンクが表示されなくなります。

4. 監査エントリを表示するには、特定の期間（1時間、3時間、24時間、3日間、7日間）を選択します。Insightでは、選択した期間について、最大1、000件の違反が表示されます。

   1ページに収まらないデータがある場合は、表の下のページ番号をクリックして、ページごとにデータを参照できます。

5. 列ヘッダーの矢印をクリックして、表内の列のソート順序を昇順（上矢印）または降順（下矢印）に変更します。デフォルトのソート順序に戻すには、他の列ヘッダーをクリックします。

   デフォルトでは、エントリは降順で表示されます。

6. [**filter**]ボックスを使用すると、必要なエントリだけを表に表示できます。

   ユーザの監査エントリのみを表示します `izzyk`を入力します `izzyk を* filter *ボックスに入力します。

ネットワーク内の違反を監視します

パフォーマンスポリシーで設定されたしきい値に基づいてInsightで違反が生成された場合は、[Violations Dashboard]で確認できます。このダッシュボードには、ネットワークで発生したすべての違反が表示され、問題を特定して対処することができます。

手順

1. ブラウザでOnCommand Insight を開きます。
2. Insightのツールバーで、**[Dashboards]***をクリックし、[Violations Dashboard]*を選択します。

   [Violations Dashboard]が表示されます。

3. [Violations by Policies]*円グラフでは、次の方法で情報を確認できます。
   - グラフの任意のスライスにカーソルを合わせると、特定のポリシーまたは指標に対する違反の総数の割合を表示できます。
   - グラフのスライスをクリックすると、そのスライスを「拡大」できます。これにより、そのスライスをグラフの残りの部分から遠ざけることで、そのスライスを強調して注意深く調べることができます。
   - をクリックできます アイコンをクリックして円グラフを全画面モードで表示し、をクリックします 円グラフを最小化するには、もう一度繰り返します。円グラフには最大5つのスライスを含めることができます。そのため、6つのポリシーで違反が発生した場合は、5つ目と6つ目のスライスが「その他」のスライスに統合されます。Insightでは、違反数が最も多いものが最初のスライスに割り当てら

れ、2番目に多いものが2番目のスライスに割り当てられます。

4. [Violations History]*チャートは次の方法で使用できます。
   - グラフにカーソルを合わせると、特定の時点で発生した違反の総数と、指定した各指標についての違反の総数のうち発生した数が表示されます。
   - 凡例ラベルをクリックすると、その凡例に関連付けられているデータをグラフから削除できます。

     凡例をクリックすると、データが再度表示されます。

   - をクリックできます アイコンをクリックしてグラフを全画面モードで表示し、をクリックします 円グラフを最小化するには、もう一度繰り返します。
5. [Violations Table]*は次の方法で使用できます。
   - をクリックできます 右上隅のアイコンをクリックしてテーブルを全画面モードで表示し、をクリックします 円グラフを最小化するには、もう一度繰り返します。

     ウィンドウサイズが小さすぎる場合、[Violations Table]には3列しか表示されませんが、をクリックすると表示されます 、追加の列（最大7列）が表示されます。

   - 特定の期間の違反を表示できます（* 1h 、 3h 、 24h 、 3d 、 7d 、 と 30d *）が表示されます。Insightでは、選択した期間について、最大1、000件の違反が表示されます。
   - [**filter**]ボックスを使用すると、必要な違反のみを表示できます。
   - 列ヘッダーの矢印をクリックすると、表内の列のソート順序を昇順（上矢印）または降順（下矢印）に変更できます。デフォルトのソート順序に戻すには、他の列ヘッダーをクリックします。

     デフォルトでは、違反は降順で表示されます。

   - [ID]列で違反をクリックすると、その違反の期間のアセットページを表示できます。
   - 概要 列でリソース（ストレージプールやストレージボリュームなど）のリンクをクリックすると、それらのリソースに関連付けられているアセットページを表示できます。
   - [ポリシー]列でパフォーマンスポリシーのリンクをクリックすると、[ポリシーの編集]ダイアログボックスが表示されます。

     生成される違反が少なすぎる場合や多すぎる場合は、ポリシーのしきい値を調整することができます。

   - 1ページに収まらないデータがある場合は、ページ番号をクリックしてページごとにデータを参照できます。
   - をクリックできます 違反を却下します。

Acquisition Unitのステータス

[Acquisition Unit]画面には、ステータスやエラーなど、すべてのAcquisition Unitが表示されます。

サーバに接続されているInsight Acquisition Unitのステータスは、* Admin **>** Acquisition Units *の表に表示されます。この表には、各Acquisition Unitについて次の情報が表示されます。

- * 名前 *

- * IP *
- * Status *はAcquisition Unitの動作ステータスです。
- **Last Reported** Acquisition Unitに接続されたデータソースが最後に報告された時刻が表示されます。
- *Note*には、AUに関連するユーザー入力のメモが表示されます。

リスト内のAcquisition Unitに問題がある場合は、[Status]フィールドに問題に関する簡単な情報を示す赤い丸が表示されます。Acquisition Unitの問題はデータ収集に影響する可能性があるため、調査する必要があります。

Acquisition Unitを再起動するには、Acquisition Unitにカーソルを合わせ、表示される[*Restart Acquisition Unit*]ボタンをクリックします。

テキストメモを追加するには、Acquisition Unitにカーソルを合わせ、表示された_Add Note_ボタン をクリックします。最後に入力したメモのみが表示されます。

Insightデータベースをリストアしています

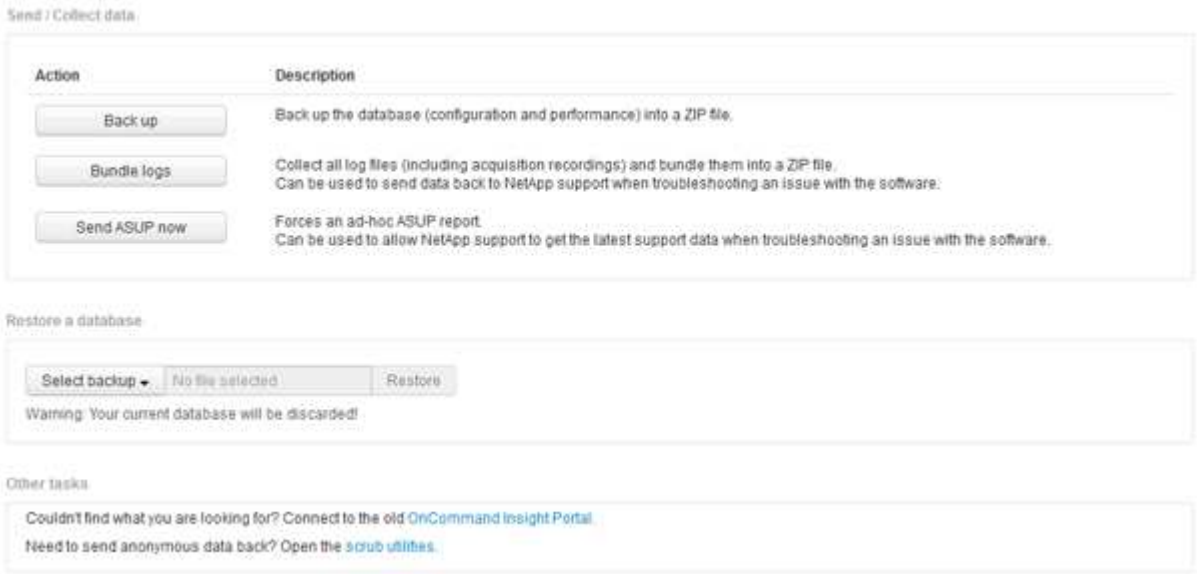
検証済みのバックアップファイルからInsightデータベースをリストアするには、[Troubleshooting]オプションを使用します。この処理を実行すると、現在のOnCommand Insight データが完全に置き換えられます。

作業を開始する前に

ベストプラクティス: OnCommand Insight データベースをリストアする前に、手動バックアッププロセスを使用して現在のデータベースのコピーを作成してください。リストアするバックアップファイルをチェックし、リストアするファイルが含まれているバックアップが正常に完了していることを確認します。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [トラブルシューティング]*をクリックします。



3. [データベースのリストア]セクションで、*[バックアップの選択]*メニューからリストアするバックアップファイルを選択します。
4. [* リストア] をクリックします。
5. すべてのデータが置き換えられるという警告が表示されたら、* OK *をクリックします

   リストア処理のステータスがリストアページに表示されます。

期限切れライセンスを更新しています

Insightのライセンスの有効期限が切れた場合は、最初にインストールしたライセンスと同じ手順 を使用して迅速にライセンスを更新できます。

手順

1. メモ帳などのテキストエディタで、ネットアップサポートから受け取った新しいライセンスファイルを開き、ライセンスキーのテキストをWindowsクリップボードにコピーします。
2. ブラウザでOnCommand Insight を開きます。
3. ツールバーの* Admin *をクリックします。
4. [設定]*をクリックします。
5. [ライセンス]タブをクリックします。
6. ［ * ライセンスの更新 * ］ をクリックします。
7. ライセンスキーのテキストを* License *テキストボックスにコピーします。
8. [更新（最も一般的な）]*操作を選択します。

   この処理を実行すると、現在アクティブなInsightライセンスに新しいライセンスが追加されます。

9. [保存（ Save ）] をクリックします。
10. Insightの消費ライセンスモデルを使用する場合は、[usage]セクションの*[Enable sending usage information to NetApp]*チェックボックスをオンにする必要があります。プロキシが適切に設定され、環境に応じて有効になっている必要があります。

ライセンスが準拠しなくなりました

Insightの[Licenses]ページに「Not Compliant」というメッセージが表示された場合、Insightで管理している容量は会社でライセンスされている容量を超えています。

「Not Compliant」メッセージは、Insightで現在管理しているテラバイト数よりも支払い済みの容量が少ないことを示します。非準拠のメッセージの横に、管理対象のテラバイト数とライセンスされたテラバイト数の差が表示されます。

Insightシステムの動作には影響しませんが、ネットアップの担当者に連絡してライセンスの適用範囲を広げ、適切なライセンスを更新する必要があります。

Insightの旧バージョンのライセンスの交換

Insightの以前のバージョンとの下位互換性がない新しいバージョンを購入した場合は、古いライセンスを新しいライセンスに置き換える必要があります。

新しいライセンスをインストールする場合は、ライセンスキーのテキストを保存する前に*置換*操作を選択する必要があります。

サービスパックの適用

サービスパックは定期的に提供されており、OnCommand Insight の修正や拡張を活用するために適用することができます。

作業を開始する前に

- サービスパックファイルをダウンロードしておく必要があります（例： `7.2service_pack_1.patch`）をNOWサイトから取得します。
- すべてのパッチを承認しておく必要があります。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [パッチ]*をクリックします。
3. [Actions]ボタンから、*[Apply patch]*を選択します。
4. ダイアログボックスで、[参照]*をクリックしてサービスパックファイルを探します。
5. 影響を受けるデータソースがあるかどうかを示す*パッチ名*、概要 *、 Impacted data source types 、および Details *（サービスパックに含まれる拡張機能）を確認します。
6. 選択したサービスパックが正しい場合は、*パッチの適用*をクリックします。

   サービスパックは自動的に承認されます。これ以上の操作は必要ありません。

特別なトラブルシューティングレポートの準備

Insightでは、ソフトウェアのインストール後にセットアップしたASUPシステムを通じて、ネットアップカスタマーサポートに情報が自動的に送信されます。ただし、トラブルシューティングレポートを作成し、特定の問題についてサポートチームとケースをオープンすることもできます。

Insightのツールを使用すると、Insightを手動でバックアップし、ログをバンドルして、その情報をネットアップのカスタマーサポートに送信できます。

OnCommand Insight データベースを手動でバックアップします

OnCommand Insight データベースの週次バックアップを有効にした場合は、必要に応じてデータベースのリストアに使用できるコピーが自動的に生成されます。リストア処理の前にバックアップを作成する必要がある場合や、ネットアップのテクニカルサポート

に送信する必要がある場合は、バックアップを作成できます `.zip` ファイルを手動で作成する。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [トラブルシューティング]*をクリックします。
3. [データの送信/収集]セクションで、*[バックアップ]*をクリックします。
4. [ファイルの保存]をクリックします。
5. [OK] をクリックします。

サポート用のログのバンドル

Insightソフトウェアの問題をトラブルシューティングする際に、ログやデータ収集の記録をまとめたzipファイル（「gz」形式）を迅速に生成して、ネットアップのカスタマーサポートに送信することができます。

手順

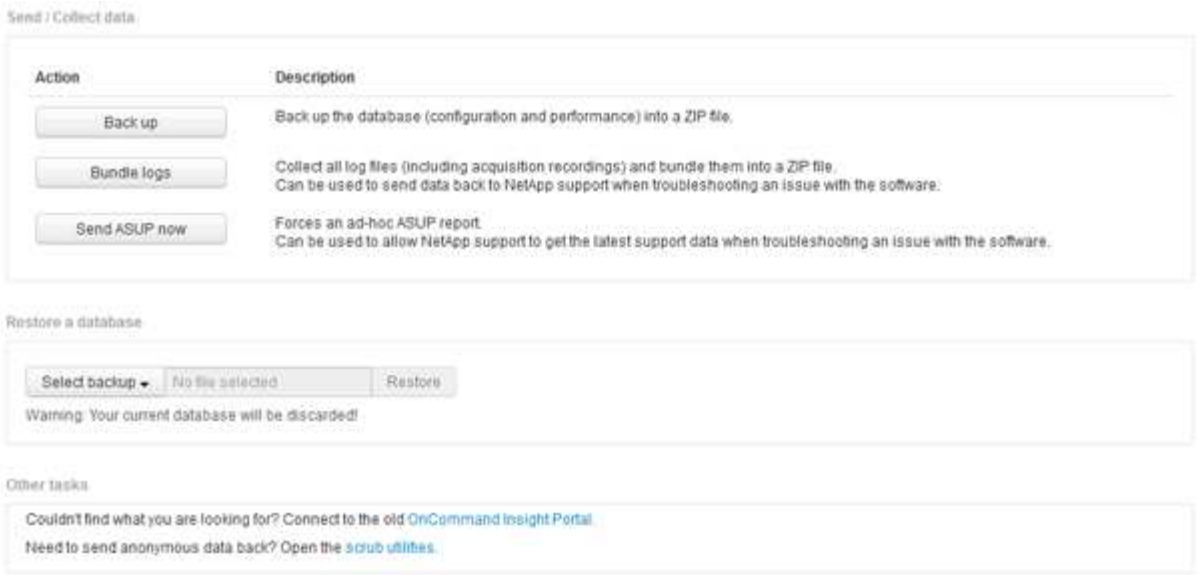
1. Insightのツールバーで、*[Admin]*をクリックします。
2. [トラブルシューティング]*をクリックします。
3. [データの送信/収集]セクションで、*[ログのバンドル]*をクリックします。
4. [ファイルの保存]をクリックします。
5. [OK] をクリックします。

ネットアップサポートに情報を送信しています

ネットアップの自動サポート（ASUP）機能は、トラブルシューティング情報をネットアップのカスタマーサポートチームに直接送信します。特別なレポートを強制的に送信できます。

手順

1. Insightのツールバーで、*[Admin]*をクリックします。
2. [設定]*をクリックします。
3. [Backup/ASUP]*タブをクリックします。
4. [データの送信/収集]領域で*[ASUPを今すぐ送信]*をクリックして、ログ、記録、バックアップをネットアップサポートに送信します。



サポートへの転送用にデータをスクラビングしています

セキュアな環境を構築しているお客様は、発生した問題をトラブルシューティングするために、ネットアップカスタマーサービスと通信し、データベース情報を犠牲にすることはありません。OnCommand Insight スクラブユーティリティを使用すると、キーワードとパターンの包括的な辞書を設定して、機密データを「クレンジング」し、スクラビングされたファイルをカスタマーサポートに送信できます。

手順

1. Web UIで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[スクラブユーティリティ]*リンクをクリックします。

   [Lookup in Dictionary]、[Scrub data]、[Build dictionary]、[Custom keywords]、および[Regular expressions]という複数のスクラビングセクションがあります。

.

+
.. [**Lookup in dictionary**]セクションで、置換する値を表示するコードを入力するか、置換するコードを表示する値を入力します。注:ルックアップを実行する前に、サポートデータからスクラブする値を識別するためのディクショナリを*ビルド*する必要があります。

1. サポートデータからスクラブする独自のキーワードを追加するには、カスタムキーワード*セクションで、メニューの**[**アクション**][**カスタムキーワードの追加**]**をクリックします。キーワードを入力し、[保存]*をクリックします。キーワードがディクショナリに追加されます。
2. [*パターン（regexp）]*を展開します。[追加（Add）]*をクリックして、新しいパターンを入力するためのダイアログボックスを表示します。
3. スクラビングする単語やフレーズを識別するために正規表現を使用するには、* regular expressions セクションにパターンを入力します。**[**メニュー**:**アクション**][**正規表現の追加**]**をクリックし、フィールドにパターンの名前と正規表現を入力して[保存]*をクリックします。情報がディクショナリに追加されました。

正規表現キャプチャグループを識別するには、パターンを丸括弧で囲む必要があります。

4. [***Build dictionary***]セクションで、[Build*]をクリックして、OnCommand Insight データベースから機密と識別されたすべての単語の辞書のコンパイルを開始します。

   完了すると、改訂されたディクショナリが使用可能であることを通知するプロンプトが表示されます。Database概要 には、ディクショナリ内のキーワードの数を示す行が含まれています。辞書でキーワードの正確さを確認してください。問題が見つかった場合に辞書を再構築するには、[データベース]ブロックの*[リセット]*をクリックして、OnCommand Insight データベースから収集されたすべてのキーワードを辞書から削除します。プロンプトが示すように、他のキーワードは削除されません。Scrubユーティリティに戻り、カスタムキーワードをもう一度入力します。

5. Scrubディクショナリを作成したら、そのディクショナリを使用してログ、XML、またはその他のテキストファイルをスクラビングし、データを匿名にすることができます。
6. ログ、XML、またはその他のテキストファイルをスクラビングするには、* Scrub data セクションで参照してファイルを探し、 Scrub file *をクリックします。

高度なトラブルシューティング

OnCommand Insight の設定を完了するには、高度なトラブルシューティングツールを使用する必要があります。これらのツールはブラウザで実行され、* Admin **>** Troubleshooting *ページから開きます。

ブラウザで高度なトラブルシューティングツールを開くには、ページ下部の*高度なトラブルシューティング*リンクをクリックします。

高度なトラブルシューティングツールを使用すると、さまざまなレポート、システム情報、インストールされているパッケージ、ログを表示したり、サーバやAcquisition Unitの再起動、DWHアノテーションの更新、アノテーションのインポートなどのさまざまな操作を実行したりできます。

使用可能なすべてのオプションについては、詳細トラブルシューティングページを参照してください。

動的なデータを無視する時間数を設定します

使用済み容量などの動的なデータの更新をOnCommand Insight が無視する時間数を設定できます。デフォルトの6時間を使用し、設定を変更しない場合、デフォルトの時間数が経過するまで、レポートは動的データで更新されません。このオプションを使用すると、動的なデータのみが変更された場合に更新が延期されるため、パフォーマンスが向上します。

このタスクについて

このオプションに値が設定されている場合、OnCommand Insight は次のルールに基づいて動的データを更新します。

- 設定は変更されず、容量データが変更された場合、データは更新されません。
- 動的なデータ（設定変更を除く）は、このオプションで指定したタイムアウト後にのみ更新されます。
- 構成が変更されると、構成データと動的データが更新されます。

このオプションの影響を受ける動的なデータには、次のものがあります。

- 容量違反のデータ
- ファイルシステムの割り当て済み容量と使用容量
- ハイパーバイザー
  - 仮想ディスクの使用容量
  - Virtual Machine Used Capacityの略
- 内部ボリューム
  - データの割り当て容量
  - データの使用容量
  - 重複排除による削減量
  - 最終アクセス時間
  - 最終Snapshot時間
  - その他の使用容量
  - Snapshot数
  - Snapshotの使用容量
  - 合計使用容量
- iSCSIセッションのイニシエータIP、ターゲットセッションID、およびイニシエータセッションID
- qtreeクォータの使用容量
- クォータで使用されているファイルと使用済み容量
- Storage Efficiencyテクノロジ、ゲイン/損失、潜在的なゲイン/損失
- ストレージプール
  - データの使用容量
  - 重複排除による削減量
  - その他の使用容量
  - Snapshotの使用容量
  - 合計使用容量
- ボリューム
  - 重複排除による削減量
  - 最終アクセス時間
  - 使用済み容量

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[高度なトラブルシューティング]*リンクをクリックします。
3. [Advanced settings]*タブをクリックし、[Acquisition Dynamic Attributes]セクションで、OnCommand

Insight がAcquisition Dynamic Attributesの動的データを無視する時間数を入力します。

4. [保存（ Save ）] をクリックします。
5. （オプション）Acquisition Unitを再起動するには、[Restart Acquisition Unit]リンクをクリックします。

   Local Acquisition Unitを再起動すると、OnCommand Insight のすべてのデータソースビューがリロードされます。この変更は次回のポーリング時に適用されるため、Acquisition Unitを再起動する必要はありません。

カスタマーサポート用のログを生成しています

カスタマーサポートから要求された場合は、トラブルシューティングのためにサーバログ、データ収集ログ、またはリモートログを生成します。

このタスクについて

ネットアップカスタマーサポートから要求があった場合は、このオプションを使用してログを生成します。

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[高度なトラブルシューティング]*をクリックします。
3. 次のページの[詳細設定]メニューで、*トラブルシューティング*リンクをクリックします。
4. [ログ]*タブをクリックし、ダウンロードするログファイルを選択します。

   ダイアログボックスが開き、ログを開くか、ログをローカルに保存できます。

システム情報の表示

OnCommand Insight サーバが導入されているシステムに関するMicrosoft WindowsのIP設定情報を表示できます。

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[高度なトラブルシューティング]*リンクをクリックします。
3. [高度なトラブルシューティング]ページで、*[レポート]*タブをクリックします。
4. [システム情報]*をクリックします。

   WindowsのIP設定には、ホスト名、DNS、IPアドレス、サブネットマスク、OS情報などの情報が含まれます。 メモリ、ブートデバイス、および接続名。

インストールされている**OnCommand Insight** コンポーネントの一覧表示

インストールされているOnCommand Insight コンポーネントのリスト（インベントリ、容量、ディメンションなど）を表示できます。 およびData Warehouseビュー。カスタ

マーサポートからこの情報の入力を求められる場合や、インストールされているソフトウェアのバージョンとインストール日時を確認する必要がある場合があります。

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[高度なトラブルシューティング]*リンクをクリックします。
3. [高度なトラブルシューティング]ページで、*[レポート]*タブをクリックします。
4. [インストールされているソフトウェアパッケージ]*をクリックします。

データベースオブジェクトの数を計算します

OnCommand Insight データベース内のオブジェクトの数を確認するには、スケールの計算機能を使用します。

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[高度なトラブルシューティング]*リンクをクリックします。
3. [高度なトラブルシューティング]ページで、*[レポート]*タブをクリックします。
4. [計算スケール]*をクリックします。

OnCommand Insight サーバを再起動しています

OnCommand Insight サーバを再起動するときは、ページを更新し、OnCommand Insight ポータルに再度ログインします。

このタスクについて

どちらのオプションも、ネットアップカスタマーサポートから要求があった場合にのみ使用してください。再起動する前に確認は行われません。

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[高度なトラブルシューティング]*リンクをクリックします。
3. 次のページの[詳細設定]メニューで、*[アクション]*タブをクリックします。
4. [サーバーの再起動]*をクリックします。

移行オプションを使用して**MySQL**データを移動しています

MySQLのデータディレクトリを別のディレクトリに移行することができます。現在のデータディレクトリは保持できます。[Troubleshooting]メニューの移行オプションを使用するか、コマンドラインを使用できます。この手順 では、トラブルシューティング>* MySQLデータの移行*オプションの使用方法について説明します。

このタスクについて

現在のデータディレクトリを保持する場合、そのディレクトリはバックアップとして保持され、名前が変更されます。

手順

1. Web UIで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. [高度なトラブルシューティング]*をクリックします。
3. [アクション]タブを選択します
4. [MySQLデータの移行]*を選択します。
5. データの移行先のパスを入力します。
6. 既存のデータディレクトリを保持するには、**[**既存のデータディレクトリを保持する**]**をオンにします。
7. [* Migrate （移行）] をクリックします

コマンドラインを使用して**MySQL**データを移動しています

MySQLのデータディレクトリを別のディレクトリに移行することができます。現在のデータディレクトリは保持できます。[Troubleshooting]メニューの移行オプションを使用することも、コマンドラインを使用することもできます。この手順 では、コマンドラインの使用方法について説明します。

このタスクについて

現在のデータディレクトリを保持する場合、そのディレクトリはバックアップとして保持され、名前が変更されます。

MySQLデータの移行ユーティリティを使用するか、を使用できます `java -jar mysqldatamigrator.jar` のOnCommand Insight パスのオプション `\bin\mysqldatamigrator` 次のパラメータを使用する必要があります。

- 必須パラメータ
  - *-path *

    データフォルダのコピー先となる新しいデータパス。
- オプションのパラメータ
  - *-myCnf <my .cnf file> *
  - *-doBackup *

    このフラグが設定されている場合、現在のデータフォルダの名前は変更されますが、削除されることはありません。

手順

1. コマンドラインツールには、次のURLからアクセスします。 `<installation path>` \bin\mysqldatamigrator\mysqldatamigrator.jar``

使用例

```
java -jar mysqldatamigrator.jar -path "C:\<new path>" -doBackup
```

アノテーションの更新を強制します

アノテーションを変更したあとすぐにレポートで使用するには、いずれかのアノテーション強制オプションを使用します。

手順

1. Web UIで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページの下部にある*[高度なトラブルシューティング]リンクをクリックします。
3. [アクション]タブをクリックします。
4. 次のいずれかのオプションを選択します。
   - * DWHアノテーションの更新*：Data Warehouseのアノテーションの更新をレポートに使用するように強制します。
   - * DWHアノテーションの更新（[Deleted]）*。Data Warehouseでアノテーションの更新（削除されたオブジェクトを含む）を強制的にレポートに使用します。

サーバリソースのステータスを確認しています

このオプションを選択すると、OnCommand Insight サーバの情報（サーバメモリ、ディスクスペース、OS、CPU、OnCommand Insight データベースの情報（InnoDBデータサイズ、データベースが存在するディスク空きスペースなど）が表示されます。

手順

1. Insightのツールバーで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、* OnCommand Insight Portal*リンクをクリックします。
3. 次のページの[詳細設定]メニューで、*トラブルシューティング*リンクをクリックします。
4. [サーバリソースステータス]*をクリックします。

   *上級OnCommand Insight ユーザーの場合:*管理者は、情報サマリーの最後にあるボタンから、データベースとサーバーの応答時間を確認するためにいくつかのSQLテストを実行できます。このオプションは、サーバリソースが少ない場合に警告を表示します。

ゴーストデータソースの検索

デバイスを削除してもデバイスデータが残っている場合は、ゴーストデータソースを見つけて削除できます。

手順

1. Web UIで、**[Admin]***をクリックし、[Troubleshooting]*を選択します。
2. ページ下部の[その他のタスク]領域で、*[高度なトラブルシューティング]*リンクをクリックします。
3. [レポート]タブで、*[ゴーストデータソース]*リンクをクリックします。

   OnCommand Insight は、発信者とそのデバイス情報のリストを生成します。

見つからないディスクモデルを追加しています

ディスクモデルが不明なために取得に失敗した場合は、そのディスクモデルをに追加できます `new_disk_models.txt` ファイルを作成し、収集を再度実行します。

このタスクについて

OnCommand Insight 取得によるストレージデバイスのポーリングの一環として、ストレージデバイス上のディスクモデルが読み取られます。Insightで認識されない新しいディスクモデルがベンダーによってアレイに追加された場合や、Insightで検索するモデル番号とストレージデバイスから返されるモデル番号が一致していない場合は、エラーが発生してそのデータソースの取得に失敗します。このエラーを回避するには、Insightで認識されるディスクモデルの情報を更新する必要があります。アップデート、パッチ、メンテナンスリリースによって新しいディスクモデルがInsightに追加されます。ただし、パッチや更新を待たずに、この情報を手動で更新することもできます。

OnCommand Insight はディスクモデルファイルを5分ごとに読み取るため、入力した新しいデータモデル情報は自動的に更新されます。変更を有効にするためにサーバを再起動する必要はありませんが、サーバとRemote Acquisition Unit（RAU）を再起動すると、次回の更新前に変更を有効にすることができます。

ディスクモデルの更新がに追加されます `new_disk_models.txt` ファイルはにあります`<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` ディレクトリ。を更新する前に、新しいディスクモデルの説明に必要な情報を確認しておきます `new_disk_models.txt` ファイル。ファイル内の情報が不正確な場合、誤ったシステムデータが生成され、取得に失敗する可能性があります。

Insightのディスクモデルを手動で更新するには、次の手順に従います。

手順

1. ディスクモデルの適切な情報を確認します。
2. テキストエディタを使用してを開きます `new_disk_models.txt` ファイル。
3. 新しいデータソースの必要な情報を追加します。
4. ファイルをに保存します `<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` サーバ上のディレクトリ。
5. をバックアップします `new_disk_models.txt` ファイルを安全な場所に保存します。以降のOnCommand Insight アップグレードでは、このファイルは上書きされます。アップグレードしたファイルにディスクモデル情報がない場合は、その情報を再入力する必要があります。

ディスクモデルの情報を確認するには、ベンダーとモデル番号を特定し、インターネットで検索します。

このタスクについて

ディスクモデルの情報は、インターネットで検索するだけで簡単に見つけることができます。検索する前に、ベンダー名とディスクモデル番号をメモしておいてください。

手順

1. インターネットでベンダー、モデル、ドキュメントタイプ「`pdf'」の高度な検索を使用して、ベンダーのデータシートやドライブのインストールガイドを検索することをお勧めします。通常、これらのデータシートは、ベンダーディスク情報の最良のソースです。
2. ベンダーの仕様では、完全なモデル番号に基づいて、必要なすべての情報が提供されるとは限りません。多くの場合、ベンダーのサイトでモデル番号の文字列のさまざまな部分を検索して、すべての情報を見つけると便利です。
3. OnCommand Insight で新しいディスクモデルを定義するには、ディスクのベンダー名、完全なモデル番号、ディスクのサイズと速度、およびインターフェイスタイプを確認します。次の表に記載されている情報を参考にしてください。

このフィールド：	これは次のとおりです。	入力内容：
モデル番号（別名キー）	必須	
ベンダー	必須	
ディスク速度（rpm）	必須	
サイズ（GB）	必須	
インターフェイスタイプ（1つ選択）	必須	ATA、SATA、SATA2、SATA3、FC、 SAS、FATA、SSD、その他
シーク時間（ミリ秒）	任意。	
最大転送速度（MB/秒）	任意。	
インターフェイスの転送速度（MB/秒）	任意。	
ベンダー/モデル情報へのリンク	オプションですが、推奨されます	

4. にその情報を入力します `new_disk_models.txt` ファイル。を参照してください "new_disk_models.txt ファイルの内容" 形式、順序、および例については、を参照してください。

new_disk_models.txtファイルの内容

。 `new_disk_models.txt` ファイルには必須フィールドとオプションフィールドがあります。フィールドはカンマで区切られているため、フィールド内にカンマを使用しないでください。

シーク時間、転送速度、および追加情報を除くすべてのフィールドが必須です。該当する場合は、ベンダー/モデルのWebサイトのリンクを[additional_info]フィールドに含めます。

テキストエディタを使用して、追加する新しいディスクモデルごとに、次の情報をこの順序でカンマで区切って入力します。

1. キー：モデル番号を使用します（必須）
2. ベンダー:名前(必須)
3. モデル番号：完全な番号（通常は「キー」と同じ値）（必須）
4. *ディスクのrpm *：例：10000または15000（必須）
5. サイズ：容量（GB）（必須）
6. インターフェイスタイプ：ATA、SATA、FC、SAS、FATA、 SSD、その他（必須）
7. シーク時間：ミリ秒（オプション）
8. 潜在的な転送速度：潜在的な転送速度（MB/秒）。ディスク自体の最大転送速度。（オプション）
9. インターフェイスの転送速度：ホストとの間の転送速度（MB/秒）（オプション）。
10. 追加情報：キャプチャする任意の追加情報 。仕様が掲載されているベンダーのページへのリンクを入力して参照することを推奨します（オプション）。

オプションのフィールドを空白のままにする場合は、必ずカンマを含めてください。

例（スペースなしで1行に1つずつ）：

```
ST373405,Seagate,ST373405,10000,73,FC,5.3,64,160,http://www.seagate.com/staticfil
es/support/disc/manuals/enterprise/cheetah/73(LP)/100109943e.pdf

SLR5B-M400SS,HITACHI,SLR5B-M400SS,1000000,400,SSD,,,,

X477_THARX04TA07,TOSHIBA,X477_THARX04TA07,7200,4000,SATA,9.5,,,https://storage.to
shiba.eu/export/sites/toshiba-sdd/media/products/datasheets/MG03ACAxxxY.pdf
```

環境の監視

Insightを使用すると、環境の問題を防止し、潜在的な問題を迅速にトラブルシューティングできます。

アセットページのデータ

アセットページには、パフォーマンスのトラブルシューティングに関するデータが表示されます。ベースアセット（仮想マシンやボリュームなど）とそのアセットに関連する

アセット（ストレージプール、ストレージノード、接続されているスイッチポートなど）の概要と、追加情報 へのリンクが表示されます。

OnCommand Insight 7.3.1以降では、すべてのアセットページに*メイン*ページと*追加データ*ページがあります。[Main]ページには、アセットの概要が表示され、グラフやトポロジなどの情報が表示されるセクションがあります。[Additional data]ページでは、現在のアセットタイプに合わせてカスタマイズ可能なダッシュボードページを設定できます。

アセットページのメインタブで、線やメッセージの横に赤い丸が表示されている場合は、監視対象の環境に問題がある可能性があります。

アセットページのタイプ

アセットページには、アセットの現在のステータスの概要と、アセットと関連するアセットに関する追加情報へのリンクが表示されます。

OnCommand Insight には、次のアセットのアセットページが用意されています。

- 仮想マシン
- ボリューム
- 内部ボリューム
- 物理ホスト
- ストレージプール
- ストレージ
- データストア
- ハイパーバイザー
- アプリケーション
- ストレージノード
- qtree
- ディスク
- VMDK です
- ポート
- スイッチ
- ファブリック
- オブジェクトストレージ（Atmos、Centera、Amazon S3など）
- ゾーン

マッピングとマスキングの情報は、[Zone]、[Volume]、[VM]、および[Host/Hypervisor]アセットページの表で確認できます。

> オブジェクトストレージアセットの概要情報は表示されますが、この情報には[データソース]詳細ページからしかアクセスできません。

環境内で特定のアセットを検索しています

検索機能を使用すると、特定のアセットに関する情報を確認できます。たとえば、システムユーザから特定のサーバに関する苦情がストレージ管理者に問い合わせられた場合、管理者はサーバ名を検索して、ステータスの概要と追加のリンク情報を示すアセットページを表示できます。

手順

1. OnCommand InsightWeb UIを開きます。
2. ツールバーのをクリックします 。

   [アセットの検索]ボックスが表示されます。

3. アセットの名前または名前の一部を入力します。
4. 検索結果から目的のリソースを選択します。

   そのリソースのアセットページが表示されます。

高度な検索技術

監視対象環境内のデータやオブジェクトを検索する場合は、複数の検索手法を使用できます。

ワイルドカード検索

文字を使用して、複数文字のワイルドカード検索を実行できます。たとえば、_applic*n_と指定すると、applicationが返されます。

検索で使用されるフレーズ

フレーズは、二重引用符で囲まれた単語のグループです（例：「Paw VNX LUN 5」）。二重引用符を使用して、名前または属性にスペースを含むドキュメントを検索できます。

ブール演算子

ブール演算子を使用すると、複数の用語を組み合わせて、より複雑なクエリを作成できます。

- または
  - OR 演算子は、デフォルトの結合演算子です。

    2 つのキーワードの間にブール演算子がない場合は、 OR 演算子が使用されます。

  - OR 演算子は、 2 つのキーワードをリンクし、どちらかの条件がドキュメントに存在する場合に一致するドキュメントを検索します。

    たとえば、「storage or netapp」と指定すると、「storage」または「netapp」のいずれかを含むドキュメントが検索されます。

    - 一致するキーワードの数が多いドキュメントほどスコアが高くなります。

- および

  AND 演算子を使用すると、両方の検索語が 1 つのドキュメント内に存在するドキュメントを検索できます。たとえば、「auroraとnetapp」と指定すると、「storage」と「netapp」の両方を含むドキュメントが検索されます。

  単語との代わりに記号&&を使用できます。

- ではありません

  NOT 演算子を使用すると、 NOT のあとのキーワードを含むすべてのドキュメントが検索結果から除外されます。たとえば、「strage not netapp」と指定すると、「strage」のみを含むドキュメントが検索され、「netapp」は検索されません。

  記号を使用できます。「NOT」という単語の代わりに。

プレフィックスとサフィックスの検索

- 検索文字列の入力を開始するとすぐに、検索エンジンによってプレフィックスとサフィックスの検索が実行され、最も一致するものが検索されます。
- 完全一致は、プレフィックスまたはサフィックスの一致よりもスコアが高くなります。スコアは、検索語と実際の検索結果との距離に基づいて計算されます。たとえば、「aurora」、「aurora1」、「aurora11」の3つのストレージがあるとします。「aur」を検索すると、3つのストレージすべてが返されます。ただし、接頭辞検索文字列との距離が最も近いため、「オーロラ」の検索結果のスコアが最も高くなります。
- また、検索エンジンは逆の順序で用語を検索します。これにより、接尾辞検索を実行できます。たとえば、検索ボックスに「345」と入力すると、検索エンジンは「345」を検索します。
- 検索では大文字と小文字は区別されません。

インデックスキーワードを使用して検索します

インデックスキーワードの数が多い検索では、スコアが高くなります。

検索文字列は、スペースで複数の検索キーワードに分けて表示されます。たとえば、「strage aurora netapp」という検索文字列は、「strage」、「aurora」、「netapp」の3つのキーワードに分割されます。3つのキーワードをすべて使用して検索が実行されます。これらのキーワードのほとんどに一致するドキュメントのスコアが最も高くなります。入力する情報が多いほど、検索結果の方が適しています。たとえば、ストレージの名前とモードでストレージを検索できます。

検索結果は、カテゴリごとに上位 3 件まで表示されます。想定していたドキュメントが見つからなかった場合は、検索文字列にキーワードを追加して検索結果を向上させることができます。

次の表に、検索文字列に追加できるインデックスキーワードのリストを示します。

カテゴリ	インデックスキーワード

ストレージ	• "ストレージ" • 名前 • ベンダー • モデル
ストレージプール	• “stragepool” • 名前 • ストレージの名前 • ストレージのIPアドレス • ストレージのシリアル番号 • ストレージベンダー • ストレージモデル • 関連付けられているすべての内部ボリュームの名前 • 関連付けられているすべてのディスクの名前
内部ボリューム	• "`internalvolume'" • 名前 • ストレージの名前 • ストレージのIPアドレス • ストレージのシリアル番号 • ストレージベンダー • ストレージモデル • ストレージプールの名前 • 関連付けられているすべての共有の名前 • 関連付けられているすべてのアプリケーションとビジネスエンティティの名前

ボリューム	• '"ボリューム'" • 名前 • ラベル • すべての内部ボリュームの名前 • ストレージプールの名前 • ストレージの名前 • ストレージのIPアドレス • ストレージのシリアル番号 • ストレージベンダー • ストレージモデル
ストレージノード	• 「Stragenode」 • 名前 • ストレージの名前 • ストレージのIPアドレス • ストレージのシリアル番号 • ストレージベンダー • ストレージモデル
ホスト	• "ホスト"" • 名前 • IP アドレス • 関連付けられているすべてのアプリケーションとビジネスエンティティの名前
データストア	• 「データストア」 • 名前 • Virtual Center IPの略 • すべてのボリュームの名前 • すべての内部ボリュームの名前

仮想マシン	• "`virtualmachine'" • 名前 • DNS名 • IP アドレス • ホストの名前 • ホストのIPアドレス • すべてのデータストアの名前 • 関連付けられているすべてのアプリケーションとビジネスエンティティの名前
スイッチ（標準と NPV ）	• "スイッチ" • IP アドレス • WWN • 名前 • シリアル番号 • モデル • ドメインID • ファブリックの名前 • ファブリックのWWN
アプリケーション	• "`application'" • 名前 • テナント • 基幹業務部門 • ビジネスユニット • プロジェクト
テープ	• "`tape'" • IP アドレス • 名前 • シリアル番号 • ベンダー
ポート	• "ポート" • WWN • 名前

ファブリック	• 「ファブリック」 • WWN • 名前

表示されるデータの時間範囲の変更

デフォルトでは、アセットページには過去24時間のデータが表示されますが、別の固定時間またはカスタムの期間を選択して表示するデータのセグメントを変更することができます。

このタスクについて

アセットの種類に関係なく、すべてのアセットページに表示されるオプションを使用して、データを表示する期間を変更することができます。

手順

1. OnCommand InsightWeb UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。
   - Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。
   - をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。
3. ページの左上隅で、次のいずれかの時間アイコンをクリックして、表示されるデータのセグメントを変更します。
   - * 3時間*

     過去3時間のデータが表示されます。

   - * 24時間*

     過去24時間のデータが表示されます。

   - * 3D *

     過去3日間のデータが表示されます。

   - * 7d *

     過去7日間のデータが表示されます。

   - * 30d *

     過去30日間のデータが表示されます。

   - カスタム

カスタムの期間を選択できるダイアログボックスが表示されます。一度に最大31日分のデータを表示できます。

4. [カスタム]*を選択した場合は、次の手順を実行します。
   a. 日付フィールドをクリックし、開始日の月、日、年を選択します。
   b. 時刻リストをクリックし、開始時刻を選択します。
   c. 終了データと終了時刻について、手順aとbの両方を繰り返します。
   d. をクリックします 。

データソースのデータ収集ステータスの確認

データソースはInsightの主要な情報源であるため、必ず実行状態を維持する必要があります。

データソースのデータ収集ステータスは、直接取得したすべてのアセットのすべてのアセットページで確認できます。次のいずれかの状況が発生する可能性があります。アセットページの右上にステータスが表示されます。

- データソースから正常に取得されました

  ステータス"`Acquired"を表示します `xxxx``", where `xxxx` アセットのデータソースの最新の取得時刻を示します。

- 取得エラーが発生しました。

  ステータス"`Acquired"を表示します `xxxx``", where `xxxx` アセットの1つ以上のデータソースの最新の取得時刻を示します 。をクリックします には、アセットの各データソース、データソースのステータス、および前回のデータ取得日時が表示されます。データソースをクリックすると、データソースの詳細ページが表示されます。

アセットが直接取得されていない場合は、ステータスは表示されません。

アセットページのセクション

アセットページには、アセットに関連する情報を含む複数のセクションが表示されます。表示されるセクションはアセットのタイプによって異なります。

まとめ

アセットページの[Summary]セクションには、特定のアセットに関する情報の概要とそのアセットに関連する問題が赤い丸で示されます。関連するアセットに関する追加情報へのハイパーリンクと、アセットに割り当てられているパフォーマンスポリシーへのハイパーリンクが表示されます。

次の例は、仮想マシンのアセットページの[Summary]セクションに表示される情報の一部を示しています。横に赤い丸が表示されている項目は、監視対象の環境に潜在的な問題があることを示しています。

Summary

Power state:	On
Guest state:	Running
Datastore:	DS_SP1_1
CPU:	41.05%
Memory:	51% (1,047 / 2,048 MB)
Capacity:	10% (19.5 / 195.3 GB)
Latency:	1.93 ms (6.00 ms max)
IOPS:	1,317.33 IO/s (4,964.00 IO/s max)
Throughput:	38.79 MB/s (142.00 MB/s max)
DNS name:	VM_Cs_travBookcomp.com
IP:	10.97.133.23
OS:	Microsoft Windows Server 2008 R2(64-bit)
Processors:	4
FC Fabrics Connected:	1
Performance Policies:	VM Latency-Critical VM Latency-Warning Comp Corp.Customer Support SLA latency Exchange SL0

[Summary]セクションを使用します

[Summary]セクションでは、アセットに関する全般的な情報を確認できます。具体的には、指標（メモリ、容量、レイテンシなど）やパフォーマンスポリシーが「原因 for Concern」であるかどうかを確認すると便利です。OnCommand Insight では、指標やパフォーマンスポリシーの横に赤い丸が表示されています。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。
   - Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。
   - をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。

     [Summary]セクションに表示される情報は、表示しているアセットページのタイプによって異なります。

3. いずれかのアセットのリンクをクリックすると、対応するアセットページを表示できます。

   たとえば、ストレージノードを表示している場合は、リンクをクリックして関連付けられているストレージのアセットページを表示したり、をクリックしてHAパートナーのアセットページを表示したりできます。

4. アセットに関連付けられている指標を表示できます。

   指標の横に赤い丸が表示されている場合、診断や解決を要する潜在的な問題があることを示しています。

   > 一部のストレージアセットについて、ボリュームの容量の表示が 100% を超えることがあります。これは、ボリュームの容量に関するメタデータが使用済み容量としてアセットから報告されるためです。

5. 該当する場合、パフォーマンスポリシーのリンクをクリックして、アセットに関連付けられているパフォーマンスポリシーを表示できます。

   パフォーマンスポリシーの横に赤い丸が表示されている場合、アセットがパフォーマンスポリシーで定義されたしきい値を超えていることを示しています。パフォーマンスポリシーを調べて、問題 を詳しく診断する必要があります。

トポロジ

[Topology]セクション（該当するアセットがある場合）では、ベースアセットとそれに関連するアセットがどのように接続されているかを確認できます。

次の例は、仮想マシンのアセットページの[Topology]セクションに表示される内容を示しています。

アセットのトポロジがセクションに収まらない場合は、代わりに*リンクをクリックしてトポロジを表示*ハイパーリンクが表示されます。

[Topology]セクションを使用します

[Topology]セクションでは、ネットワーク内のアセットの相互接続状況を確認したり、関連するアセットに関する情報を表示したりできます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。

   - Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。

- をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。[Topology]セクションはアセットページの右上にあります。

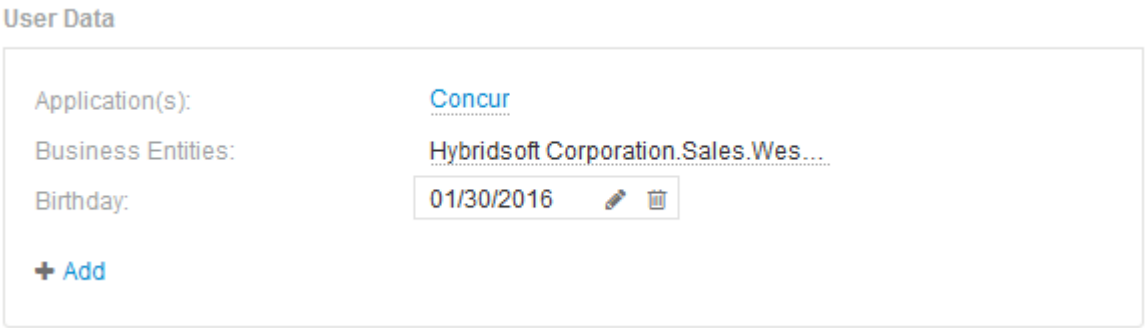
アセットのトポロジがセクションに収まらない場合は、*クリックリンクをクリックしてトポロジ*ハイパーリンクを表示します。

3. ベースアセットに関連するアセットの詳細を確認するには、トポロジで関連するアセットにカーソルを合わせ、名前をクリックします。アセットページが表示されます。

ユーザデータ

アセットページの[User Data]セクションには、ユーザが定義したアプリケーション、ビジネスエンティティ、アノテーションなどのデータが表示されます。

仮想マシンのアセットページの[User Data]セクションにアプリケーション、ビジネスエンティティ、およびアノテーションが割り当てられている場合の表示例を次に示します。



User Data セクションを使用してアプリケーションを割り当てまたは変更する

環境で実行されているアプリケーションを特定のアセット（ホスト、仮想マシン、ボリューム、内部ボリューム、ハイパーバイザー）に割り当てることができます。[User Data]セクションでは、アセットに割り当てられているアプリケーションを変更したり、アプリケーションや追加のアプリケーションをアセットに割り当てたりできます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。
   - Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。
   - をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。
3. 次の操作を実行できます。
   - アプリケーションのアセットページを表示するには、アプリケーションの名前をクリックします。
   - 割り当てられているアプリケーションを変更したり、アプリケーションや追加のアプリケーションを割り当てたりするには、アプリケーション名（アプリケーションが割り当てられている場合）にカーソルを合わせ、アプリケーションが割り当てられていない場合は*なし*にカーソルを合わせて、をクリックします を入力してアプリケーションを検索するか、リストからアプリケーションを選択し、

をクリックします 。

ビジネスエンティティに関連付けられているアプリケーションを選択した場合は、ビジネスエンティティがアセットに自動的に割り当てられます。この場合、ビジネスエンティティの名前にカーソルを合わせると、_derived_と 表示されます。エンティティをアセットに対してのみ保持し、関連付けられているアプリケーションを保持しない場合は、アプリケーションの割り当てを手動で上書きできます。

- アプリケーションを削除するには、をクリックします 。

[User Data]セクションを使用してビジネスエンティティを割り当てまたは変更する

ビジネスエンティティを定義して、環境のデータをより細かく追跡し、レポートすることができます。アセットページの[User Data]セクションで、アセットに割り当てられているビジネスエンティティを変更したり、アセットからビジネスエンティティを削除したりできます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。
   - Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。
   - をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。
3. 次の操作を実行できます。
   - 割り当てられたエンティティを変更するか、エンティティを割り当てるには、をクリックします をクリックし、リストからエンティティを選択します。
   - ビジネスエンティティを削除するには、をクリックします 。

> アセットに割り当てられているアプリケーションから派生したエンティティを削除することはできません。

User Data セクションを使用して、注釈を割り当てまたは変更する

企業の要件に合わせてデータを追跡するようにOnCommand Insight をカスタマイズする場合は、_annotations_という特殊なメモを定義してアセットに割り当てることができます。アセットページの User Data セクションには、アセットに割り当てられているアノテーションが表示されます。また、そのアセットに割り当てるアノテーションを変更することもできます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。

- Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。
- をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。

3. アセットページの*[User Data]*セクションで、をクリックします ✚Add。

   [注釈の追加] ダイアログボックスが表示されます。

4. [注釈（Annotation）]*をクリックし、リストから注釈を選択します。
5. [値]*をクリックし、選択したアノテーションのタイプに応じて次のいずれかを実行します。
   - アノテーションタイプがリスト、日付、またはブーリアンの場合は、値をリストから選択します。
   - アノテーションタイプがテキストの場合は、値を入力します。
6. [保存（ Save ）] をクリックします。

   アセットにアノテーションが割り当てられ、クエリでアノテーションに基づいてアセットをフィルタできるようになります。

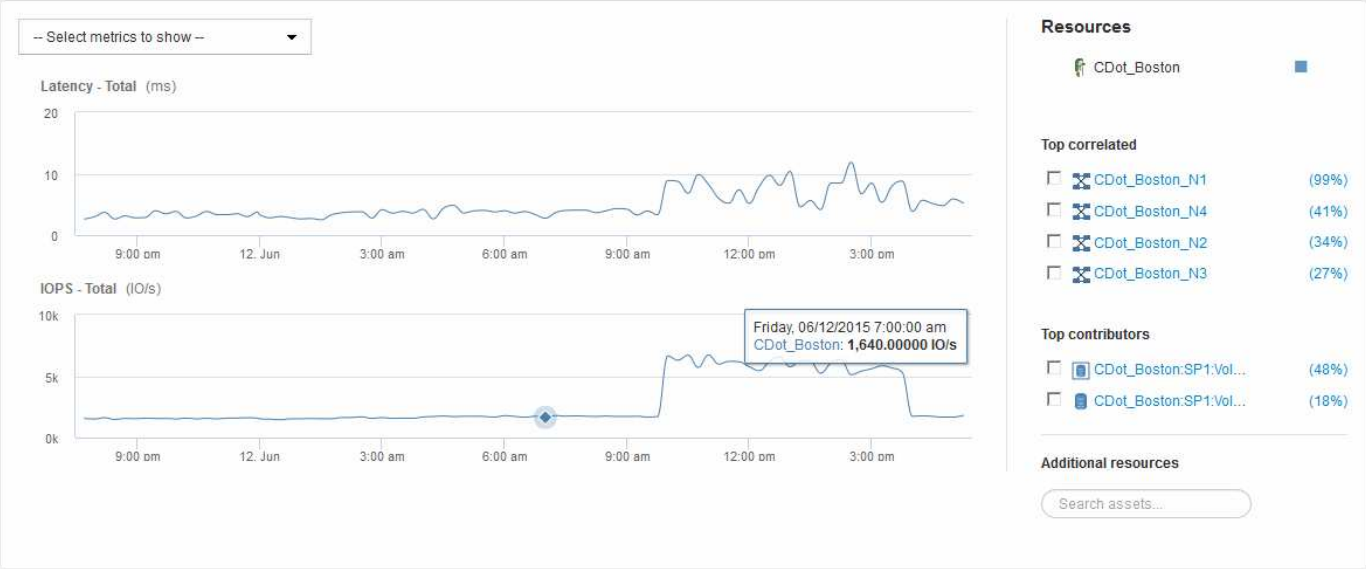
7. アノテーションの割り当て後に値を変更する場合は、をクリックします 別の値を選択します。

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

エキスパートビュー

アセットページの[Expert View]セクションでは、選択した期間（3時間、24時間、3日間、7日間、 またはカスタム期間）を使用してパフォーマンスチャートとそれに関連するアセットを表示します。

次の例は、ボリュームのアセットページの[Expert View]セクションを示しています。



選択した期間について、パフォーマンスチャートで表示する指標を選択することができます。

[Resources]セクションに、ベースアセットの名前とパフォーマンスチャートでの色が表示されます。[Top Correlated]セクションに表示するアセットが表示されない場合は、[Additional resources]セクションの*[Search assets]*ボックスを使用してアセットを検索し、パフォーマンスチャートに追加できます。リソースを追加すると、 [追加リソース] セクションにリソースが表示されます。

ベースアセットに関連するアセットがある場合、それらのアセットもリソースセクションに次のカテゴリ別に表示されます。

- 関連性が高い

  1 つ以上のパフォーマンス指標との関連性が高いアセット（割合）がベースアセットに表示されます。

- 上位貢献者

  ベースアセットへの影響が大きいアセットが表示されます。

- Greedy

  に、ホスト、ネットワーク、ストレージなど、同じリソースの共有を通じてアセットからシステムリソースを引き継ぐアセットを示します。

- デグレード

  このアセットにシステムリソースを奪われているアセットが表示されます。

エキスパートビューの指標の定義

アセットページのエキスパートビューセクションには、アセットに対して選択した期間に関する複数の指標が表示されます。各指標は独自のパフォーマンスチャートに表示されます。確認が必要なデータに応じて、チャートに表示する指標や関連するアセットを追加したり削除したりできます。

メートル法	説明
BB クレジットのゼロ受信、転送	サンプリング期間中に受信 / 送信のバッファ間クレジット数がゼロになった回数。この指標は、接続されたポートで提供できるクレジットを使い果たしたために転送が中止された回数を表します。
BB クレジットのゼロ期間の転送	サンプリング期間中に送信 BB クレジットがゼロになっていた時間（ミリ秒）。
キャッシュヒット率（合計、読み取り、書き込み）	キャッシュにヒットする要求の割合。ボリュームへのアクセス数に対するヒット数の割合が高いほど、パフォーマンスが高くなります。この列は、キャッシュヒット情報を収集しないストレージアレイについては空になります。
キャッシュ使用率（合計）	キャッシュにヒットするキャッシュ要求の合計割合

クラス 3 は破棄されます	ファイバチャネルのクラス 3 データ転送が破棄された回数。
CPU 利用率（合計）	使用可能な合計（すべての仮想 CPU ）に対する使用中のアクティブな CPU リソースの割合。
CRC エラーです	サンプリング期間中にポートで無効な Cyclic Redundancy Check （ CRC ；巡回冗長検査）が検出されたフレーム数
フレームレート	転送フレームレート（ 1 秒あたりのフレーム数）。
フレームサイズ平均（ Rx 、 Tx ）	フレームサイズに対するトラフィックの比率。この指標から、ファブリック内にフレームのオーバーヘッドがないかどうかを特定できます。
フレームサイズが長すぎます	ファイバチャネルの長すぎるデータ転送フレームの数。
フレームサイズが短すぎます	ファイバチャネルの短すぎるデータ転送フレームの数。
I/O 密度（合計、読み取り、書き込み）	ボリューム、内部ボリューム、またはストレージ要素の使用済み容量（データソースの最新のインベントリポーリングから取得）で IOPS を割った値。1 秒間の TB あたりの I/O 処理数で測定されます。
IOPS （合計、読み取り、書き込み）	I/O チャネルまたはそのチャネルの一部を通過する読み取り / 書き込み I/O サービス要求の単位時間あたりの数（ 1 秒あたりの I/O 数で測定）
IP スループット（合計、読み取り、書き込み）	合計： IP データの転送および受信速度の合計。 1 秒あたりのメガバイト数で示されます。Read：IP Throughput（Receive）：IPデータの平均受信速度（1秒あたりのメガバイト数）。 Write：IP Throughput（Transmit）：IPデータの平均転送速度（1秒あたりのメガバイト数）。
レイテンシ（合計、読み取り、書き込み）	Latency （ R&W ）：一定の時間内にデータが仮想マシンに対して読み取りまたは書き込みされるレート。1 秒あたりのメガバイト数で測定されます。 Latency：データストア内の仮想マシンからの平均応答時間。 Top Latency：データストア内の仮想マシンからの最大応答時間。

リンク障害です	サンプリング期間中にポートで検出されたリンク障害の数。
リンクリセット Rx 、 Tx	サンプリング期間中に受信または送信されたリセットリンクの数。この指標は、このポートに対して接続されたポートから発行されたリンクリセットの数を表します。
メモリ使用率（合計）	ホストで使用されるメモリのしきい値。
部分的 R/W （合計） %	RAID 5 、 RAID 1/0 、または RAID 0 の LUN において、読み取り / 書き込み処理がディスクモジュールのストライプ境界を越えた合計回数。通常、ストライプを越えると、各 LUN で追加の I/O が必要になるため、ストライプを越えることは効果がありませんこの割合が低いほど、ストライプ要素のサイズは効率的であり、ボリューム（ネットアップの LUN ）のアライメントは不適切であることを示します。 CLARiX については、ストライプを越えた回数を IOPS の合計で割った値が示されます。
ポートエラーです	サンプリング期間中または一定の期間に検出されたポートエラーのレポート。
信号損失回数	信号損失エラーの数。信号損失エラーが発生した場合は、電気的接続がなく、物理的な問題があります。
スワップレート（合計レート、インレート、アウトレート）	サンプリング期間中にディスクとアクティブメモリの間にスワップイン速度、スワップアウト速度、またはその両方が発生した速度。これは環境仮想マシンのカウンタです。
同期損失の数	同期損失エラーの数同期損失エラーが発生した場合、ハードウェアはトラフィックを認識できないか、ロックオンされません。すべての機器のデータ速度が同じでないか、光接続または物理接続の品質が低下している可能性があります。このエラーが発生するたびにポートの再同期が必要になるため、システムのパフォーマンスに影響します。単位は KB/秒です
スループット（合計、読み取り、書き込み）	I/O サービス要求への応答として一定の時間内に送受信されたデータのレート（ 1 秒あたりの MB で測定）。
タイムアウト廃棄フレーム数 - Tx	送信フレームがタイムアウトで破棄された回数。

トラフィック速度（合計、読み取り、書き込み）	サンプリング期間中に送受信されたトラフィックの量（ 1 秒あたりのメビバイト数）。
トラフィック利用率（合計、読み取り、書き込み）	サンプリング期間中の送受信トラフィックの比率、受信 / 送信 / 合計容量に対するトラフィックの比率。
利用率（合計、読み取り、書き込み）	送信（ Tx ）と受信（ Rx ）に使用できる帯域幅の割合。
書き込み保留（合計）	保留中の書き込み I/O サービス要求の数。

[エキスパートビュー（ **Expert View** ） **]** セクションの使用

エキスパートビューのセクションでは、選択した期間中に適用可能な任意の数の指標に基づいてアセットのパフォーマンスチャートを表示し、関連するアセットを追加してアセットと関連するアセットのパフォーマンスをさまざまな期間で比較および比較できます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。
   - Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。
   - をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。デフォルトでは、パフォーマンスチャートには、アセットページで選択した期間についての 2 つの指標のデータが表示されます。たとえば、ストレージの場合は、レイテンシと合計 IOPS がデフォルトで表示されます。リソースセクションには、リソースの名前とその他のリソースセクションが表示されます。ここでは、アセットを検索できます。アセットによっては、関連性の高いアセット、影響のあるリソース、 Greedy リソース、 Dedgraded セクションにアセットが表示されることもあります。
3. [Select metrics to show]*をクリックし、指標を選択してその指標のパフォーマンスチャートを追加できます。

   選択した指標のパフォーマンスチャートが追加されます。グラフには、選択した期間のデータが表示されます。期間を変更するには、アセットページの左上にある別の期間をクリックします。

   この手順をもう一度実行し、をクリックして指標をクリアできます。その指標のパフォーマンスチャートが削除されます。
4. グラフにカーソルを合わせ、アセットに応じて次のいずれかをクリックすると、表示される指標データを変更できます。
   - 読み取り*または*書き込み
   - **Tx**または*Rx** Total*がデフォルトです。
5. グラフ上でカーソルをドラッグしてデータポイントを選択すると、選択した期間における指標の値の変化を確認できます。

6. [リソース]セクションでは、次のいずれかの方法で関連するアセットをパフォーマンスチャートに追加できます（該当する場合）。
   - [Top correlated]、[Top contributors]、[Greedy]、または[Degraded]の各セクションで関連するアセットを選択すると、選択した各指標のパフォーマンスチャートにそのアセットのデータを追加できます。資産が表示されるには、最低15%の相関関係または貢献度が必要です。

     アセットを選択すると、そのアセットのグラフ上のデータポイントと同じ色のブロックがアセットの横に表示されます。

   - 表示されているアセットの名前をクリックすると、そのアセットページが表示されます。また、ベースアセットに対するアセットの関連性や影響度の割合をクリックすると、ベースアセットとアセットの関連性に関する詳細を確認できます。

     たとえば、関連性が高いアセットの横にある関連性の数値をクリックすると、ベースアセットとの関連性についてタイプ別に比較した情報メッセージが表示されます。

   - 比較のためにパフォーマンスチャートに表示したいアセットが[Top correlated]セクションに表示されない場合は、[Additional resources]セクションの*[Search assets]*ボックスを使用して他のアセットを検索できます。アセットを選択すると、[Additional resources]セクションにそのアセットが表示されます。アセットの情報の表示を中止する場合は、をクリックします 🗑 。

関連資産

該当する場合、アセットページに[Related Assets]セクションが表示されます。たとえば、ボリュームのアセットページには、ストレージプール、接続されているスイッチポート、コンピューティングリソースなどのアセットに関する情報が表示される場合があります。各セクションには、そのカテゴリに関連するアセットの表と対応するアセットページへのリンクが表示され、アセットに関連する複数のパフォーマンス統計が表示されます。

[Related Assets]セクションを使用します

[Related Assets]セクションでは、ベースアセットに関連するアセットを確認できます。関連する各アセットが、アセットの関連統計とともに表に表示されます。アセットの情報をエクスポートしたり、アセットの統計をエキスパートビューのパフォーマンスチャートで表示したり、関連するアセットの統計のみを表示するグラフを表示したりできます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。
   - Insightのツールバーで、をクリックします 🔍 をクリックし、アセットの名前を入力して、リストからアセットを選択します。
   - をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。
3. 表でのアセットの表示方法を制御するには、次の手順に従います。

- 任意のアセットの名前をクリックして、そのアセットページを表示します。
- 特定のアセットのみを表示するには、* filter *ボックスを使用します。
- 表に5個を超えるアセットがある場合は、ページ番号をクリックしてページごとにアセットを参照できます。
- 列見出しで矢印をクリックすると、表内の列のソート順序を昇順（上矢印）または降順（下矢印）に変更できます。
- 関連するアセットを[Expert View]セクションのパフォーマンスチャートに追加するには、関連するアセットにカーソルを合わせてをクリックします 。

4. テーブルに表示されている情報をにエクスポートします `.csv` ファイル：
   a. をクリックします 。
   b. Microsoft Excelでファイルを開いて特定の場所に保存するには、**[ファイルを保存]***をクリックし、[OK]*をクリックしてファイルをダウンロードフォルダに保存します。

      表示用に現在選択されている列のすべてのオブジェクト属性がファイルにエクスポートされます。表示されている列の属性のみがエクスポートされます。テーブルの最初の10,000行だけがエクスポートされることに注意してください。

5. 関連するアセットの情報を表の下のグラフに表示するには、をクリックします 次のいずれかを実行します。
   - 表示される指標データを変更するには、**[読み取り]**、**[書き込み]**、または*をクリックします。 Total * がデフォルトです。
   - をクリックします 別の指標を選択します。
   - をクリックします グラフの種類を変更します。*折れ線グラフ*がデフォルトです。
   - グラフのデータポイントにカーソルを合わせると、関連する各アセットについて選択した期間における指標の値の変化を確認できます。
   - グラフの凡例で関連するアセットをクリックして、グラフに追加または削除します。
   - 関連する他のアセットをグラフに表示するには、関連するアセットの表でページ番号をクリックします。
   - をクリックします をクリックしてグラフを閉じます。

違反

アセットに割り当てたパフォーマンスポリシーに対する違反が環境で見つかった場合、アセットページの Violations セクションを使用して違反を確認できます。パフォーマンスポリシーではネットワークのしきい値を監視し、しきい値の違反を即座に検出してその影響を特定し、問題の影響と根本原因 を分析して迅速かつ効果的に修正できます。

次の例は、ハイパーバイザーのアセットページに表示される[Violations]セクションを示しています。

Violations

filter...

Time	Description
06/05/2015 5:00:00 pm	Port balance index of 74 on esx1 exceeds the threshold of 50
06/12/2015 8:59:54 am	2 violations for esx2 with 'Swap out rate' > 3
06/12/2015 12:04:54 pm	esx1 violation with 'Swap out rate' > 3.00 KB/s (value of 86.85 KB/s)
06/12/2015 12:29:54 pm	esx1 violation with 'Swap in rate' > 3.00 KB/s (value of 59.90 KB/s)
06/12/2015 1:04:54 pm	7 violations for ds-30 with 'Latency - Total' > 50

Showing 1 to 5 of 32 entries

< 1 2 3 4 5 >

[Violations]セクションの使用

Violations セクションでは、アセットに割り当てたパフォーマンスポリシーの結果としてネットワークで発生したすべての違反を表示し、管理することができます。

手順

1. OnCommand Insight Web UIにログインします。
2. 次のいずれかの方法でアセットページを検索します。
   - Insightのツールバーで、をクリックします をクリックし、アセットの名前を入力して、リストからアセットを選択します。
   - をクリックし、[Assets Dashboard]*を選択してアセット名をクリックします。アセットページが表示されます。[Violations]セクションには、違反が発生した時刻、しきい値を超えた概要 、および違反が発生したアセットへのハイパーリンクが表示されます（例：「2 violations fir DS-30 with Latency-Total >50」）。
3. 次のオプションのタスクを実行できます。
   - 特定の違反のみを表示するには、* filter *ボックスを使用します。
   - 表内の違反数が5個を超える場合は、ページ番号をクリックして各ページを参照できます。
   - 列見出しで矢印をクリックすると、表内の列のソート順序を昇順（上矢印）または降順（下矢印）に変更できます。
   - 概要でアセット名をクリックすると、そのアセットページが表示されます。赤い丸は詳しい調査が必要な問題を示しています。

     パフォーマンスポリシーをクリックすると、ポリシーの編集ダイアログボックスが表示されます。このダイアログボックスで、パフォーマンスポリシーを確認し、必要に応じて変更を加えることができます。

   - をクリックします 問題 が原因 for Concernではなくなったと判断した場合に、リストから違反を削除します。

カスタマイズ可能なアセットページ

各アセットページのカスタマイズ可能なウィジェットに追加のデータを表示できます。アセットのページをカスタマイズすると、そのタイプのすべてのアセットのページにカスタマイズが適用されます。

アセットページウィジェットをカスタマイズするには、次の操作を実行します。

1. ページにウィジェットを追加します
2. ウィジェットのクエリまたは式を作成して、目的のデータを表示します
3. 必要に応じてフィルタを選択します
4. ロールアップまたはグループ化の方法を選択します
5. ウィジェットを保存します
6. 必要なすべてのウィジェットについて、この手順を繰り返します
7. アセットページを保存します

カスタムのアセットページに変数を追加して、ウィジェットに表示するデータをさらに絞り込むこともできます。通常の変数に加えて、各アセットタイプでは一連の「$this」変数を使用して、現在のアセットに直接関連するリソースをすばやく特定できます。たとえば、現在の仮想マシンをホストしているのと同じハイパーバイザーでホストされているすべての仮想マシンなどです。

このカスタムアセットページは、ユーザごと、およびアセットタイプごとに一意です。たとえば、ユーザAが仮想マシンのカスタムアセットページを作成すると、そのユーザの仮想マシンのアセットページにそのカスタムページが表示されます。

ユーザが表示、編集、削除できるのは、自分で作成したカスタムアセットページのみです。

カスタムアセットページは、Insightのエクスポート/インポート機能には含まれません。

「**$this**」変数について説明します

カスタマイズ可能なアセットの[Additional data]ページでは、特殊な変数を使用して、現在のアセットに直接関連する追加情報 を簡単に表示できます。

このタスクについて

アセットのカスタマイズ可能なランディングページのウィジェットで「$this」変数を使用するには、次の手順を実行します。この例では、表ウィジェットを追加します。

> 「$this」変数は、アセットのカスタマイズ可能なランディングページでのみ有効です。Insightの他のダッシュボードでは使用できません。使用可能な「$this'」変数は、アセットタイプによって異なります。

手順

1. 目的のアセットのアセットページに移動します。この例では、仮想マシン（ VM ）のアセットページを選択します。クエリまたは検索を使用して VM を選択し、リンクをクリックしてその VM のアセットページに移動します。

   VM のアセットページが開きます。

2. **>**[Additional Virtual Machine data]*ドロップダウンをクリックして、そのアセットのカスタマイズ可能なランディングページに移動します。
3. [Widget]ボタンをクリックし、[Table Widget]*を選択します。

   編集用の表ウィジェットが開きます。デフォルトでは、すべてのストレージが表に表示されます。

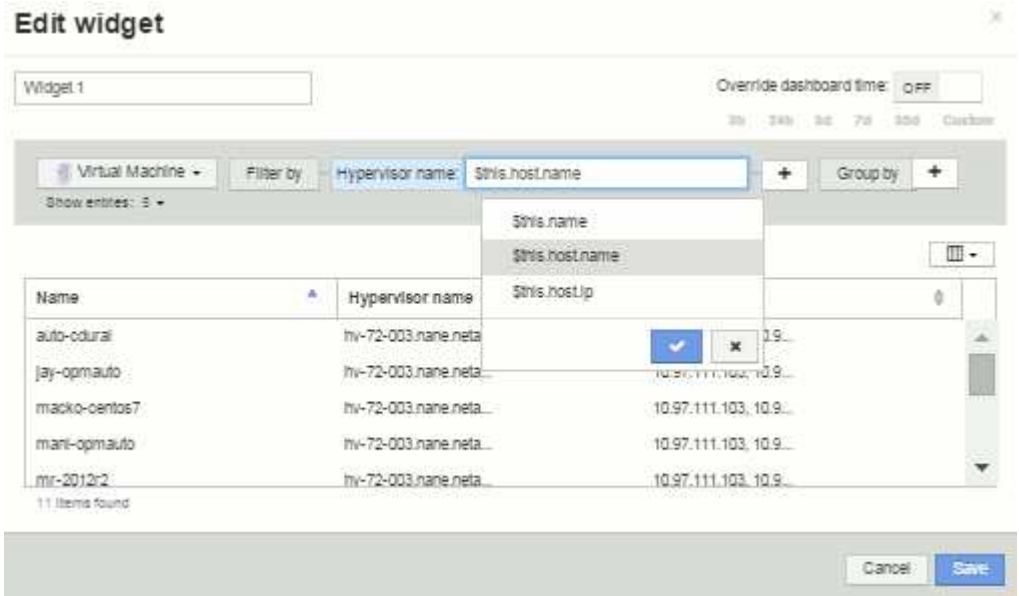
4. すべての仮想マシンを表示します。アセットセレクタをクリックし、**[ストレージ]***を[仮想マシン]*に変更します。

   これで、すべての仮想マシンが表に表示されます。

5. ボタンをクリックします そして、 hypervisor name *フィールドをテーブルに追加します。

   表内の VM ごとにハイパーバイザー名が表示されます。

6. 現在の VM をホストしているハイパーバイザーだけを表示します。フィールドの**[*+*]**ボタンをクリックし、[hypervisor name]*を選択します。
7. をクリックし、$ this.host.name *変数を選択します。チェックボタンをクリックしてフィルタを保存します。



8. 表に、現在の VM のハイパーバイザーがホストしているすべての VM が表示されます。[保存（ Save ）] をクリックします。

結果

表示するすべてのVMのアセットページに対して、この仮想マシンのアセットページ用に作成した表が表示されます。ウィジェットで*$ this.host.name *変数を使用すると、現在のアセットのハイパーバイザーが所有するVMのみが表に表示されます。

ネットワークリソースの分散

負荷分散の問題を解決するには、アセットページで問題を特定し、使用率が低い大容量ボリュームを特定します。

手順

1. ブラウザでAssets Dashboardを開きます。
2. [Virtual Machines IOPS]ヒートマップで、非常に多くの箇所で問題が報告されているVMの名前を確認します。

3. VM名をクリックしてアセットページを表示します。
4. 概要でエラーメッセージを確認します。
5. パフォーマンスグラフ、特に関連性の高いリソースを確認して、競合状態の可能性があるボリュームを特定します。
6. パフォーマンスチャートにボリュームを追加してアクティビティのパターンを比較し、問題に関連した他のリソースのアセットページを表示します。
7. アセットページの一番下までスクロールして、VMに関連付けられているすべてのリソースのリストを確認します。大容量で実行されているVMDKをメモします。これが競合の原因となっている可能性があります。
8. 負荷分散の問題を解決するには、利用率の低いリソースを特定して利用率の高いリソースから負荷を受け取るか、負荷の高いリソースから負荷の低いアプリケーションを削除します。

ネットワークパフォーマンスの確認

ストレージ環境のパフォーマンスを調べて、利用率の低いリソースや利用率の高いリソースを特定し、リスクを未然に特定して問題に発展させることができます。

Insightを使用すると、収集したストレージのデータから明らかになったパフォーマンスや可用性の問題を解決または防止できます。

Insightを使用して、次のパフォーマンス管理タスクを実行できます。

- 環境全体のパフォーマンスを監視
- 他のデバイスのパフォーマンスに影響を与えるリソースを特定する

ポートの重要性

Insight ServerとData Warehouse（DWH）サーバを確実に動作させるには、いくつかのTCPポートを空けておく必要があります。これらのポートの一部は、localhostアダプタ（127.0.0.1）にバインドされたプロセスにのみ使用されますが、コアサービスが確実に動作するためには引き続き必要です。必要なポート数は、ネットワーク全体で使用されるポートのスーパーセットです。

Insight Serverのポート

Insight Serverには、ソフトウェアファイアウォールをインストールできます。開く必要がある「穴」は、以下のようになります。

*インバウンドHTTPS 443 *- Insight WebUIをTCP 443で実行している場合は、次のいずれかのユーザを許可するために、その情報を公開する必要があります。

- Web UIのInsightユーザ
- Remote Acquisition UnitがInsight Serverへの接続を要求しています
- このInsightサーバへのコネクタを備えたOCI DWHサーバ。
- Insight REST APIとのプログラムによるやり取り

Insight Serverのホストレベルのファイアウォール機能の実装を検討している方には、企業ネットワークのすべてのIPブロックへのHTTPSアクセスを許可することをお勧めします。

インバウンド**MySQL**（**TCP 3306**）。このポートは、コネクタを備えたInsight DWHサーバにのみ公開する必要があります

Insightには多数のデータコレクタがありますが、これらはすべてポーリングベースです。Insight Will原因 its Acquisition Unit（AUS）によって、さまざまなデバイスへのアウトバウンド通信が開始されます。ホストベースのファイアウォールが「ステートフル」で、リターントラフィックがファイアウォールを通過できるようになっている限り、Insight Serverのホストベースのファイアウォールはデータ取得に影響しません。

Data Warehouseのポート

Insight DWHサーバの場合：

*インバウンドHTTPS 443 *- Insight WebUIをTCP 443で実行している場合は、次のコンシューマを許可するためにこの情報を公開する必要があります。

- DWH管理ポータルのInsight管理ユーザ

インバウンド**HTTPS**（**TCP 9300**）- Cognosのレポートインターフェイスです。ユーザがCognosのレポートインターフェイスを操作する場合は、このインターフェイスをリモートで公開する必要があります。

DWHを公開する必要がない環境を想像できます。たとえば、レポートの作成者がDWHサーバにRDP接続し、DWHサーバでレポートを作成してスケジュールを設定し、すべてのレポートをSMTP経由で配信するか、リモートファイルシステムに書き込むようにスケジュール設定します。

インバウンド**MySQL**（**TCP 3306**）。このポートを公開する必要があるのは、DWHデータとMySQLベースの統合がある場合だけです。さまざまなDWHデータマートからデータを抽出して、CMDB、チャージバックシステムなどの他のアプリケーションに取り込みますか

PCパフォーマンスの低下を分析しています

ネットワークユーザからコンピュータの動作が遅いという苦情を受けた場合は、ホストのパフォーマンスを分析し、影響を受けるリソースを特定する必要があります。

作業を開始する前に

この例では、呼び出し元がホスト名を指定しています。

手順

1. ブラウザでInsightを開きます。
2. [Search assets]*ボックスにホスト名を入力し、検索結果でホスト名をクリックします。

   リソースの_assetページ_が開きます。

3. ホストのアセットページで、ページ中央のパフォーマンスチャートを確認します。通常は事前に選択されているレイテンシとIOPSに加えて、必要に応じてさまざまなタイプのデータを表示できます。デバイスタイプに応じて、スループット、メモリ、CPU、IPスループットなど、他のタイプのデータのチェックボックスをオンにします。
4. グラフ上のポイントの概要 を表示するには、そのポイントの上にマウスポインタを置きます。
5. また、ページ上部で期間を3時間から7日まで、または使用可能なすべてのデータを選択して変更することもできます。

6. [Top correlated resources]*のリストで、アクティビティパターンがベースリソースと同じリソースがほかにないかどうかを確認します。

   リストの最初のリソースは常にベースリソースです。

   a. 関連するリソースの横にあるリンクをクリックすると、IOPSとCPUのどちらのアクティビティパターンがベースリソースと別のリソースのどちらであるかを確認できます。
   b. 関連するリソースのチェックボックスをクリックして、そのデータをパフォーマンスチャートに追加します。
   c. 関連するリソースの名前をクリックすると、そのリソースのアセットページが表示されます。

7. VMの場合も同様に、*[Top correlated resources]*でストレージプールを探し、ストレージプール名をクリックします。

関連するリソースを分析しています

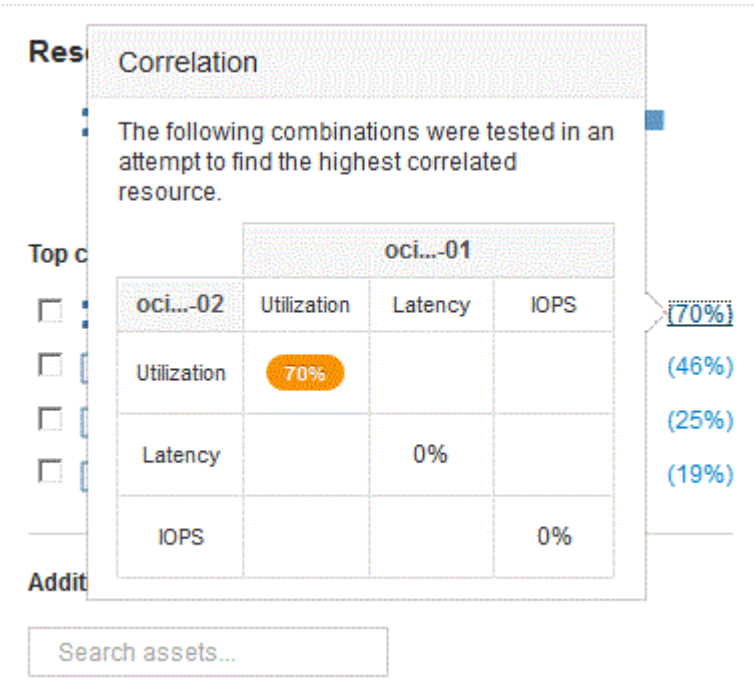
パフォーマンスの問題を調査するときにデバイスの_assetページ_を開くには、[Top correlated resources]リストを使用して、パフォーマンスチャートに表示されるデータを絞り込む必要があります。リソースの割合が高い場合は、リソースのアクティビティがベースリソースと同様であることを示します。

このタスクについて

パフォーマンスの問題を調査していて、デバイスのアセットページを開いたとします。

手順

1. [Top correlated resources]リストでは、最初のリソースがベースリソースです。リスト内の関連リソースは、アクティビティのうち最初のデバイスに対する割合でランク付けされます。関連性のリンクされたパーセンテージをクリックすると、詳細が表示されます。この例では、[Utilization]の関連性が70%になっているため、ベースリソースと関連するリソースの利用率はどちらも等しく高くなっています。



2. 関連するリソースをパフォーマンスチャートに追加するには、追加するリソースの*[Top correlated resources]*リストでチェックボックスを選択します。デフォルトでは、各リソースに使用可能な合計データが表示されますが、チェックボックスのメニューから[読み取りデータのみ]または[書き込みデータのみ]を選択できます。

   グラフでは、各リソースのパフォーマンス測定値を比較できるように、リソースごとに色が異なります。選択した測定メトリックについては、適切なタイプのデータのみがプロットされます。たとえば、CPUデータには読み取りや書き込みの指標は含まれないため、合計データのみが表示されます。

3. 関連するリソースの名前をクリックすると、そのリソースのアセットページが表示されます。
4. 分析で考慮すべきリソースが[Top correlated resources]に表示されない場合は、*[Search assets]*ボックスを使用してそのリソースを検索できます。

ファイバチャネル環境の監視

OnCommand Insightのファイバチャネルアセットページを使用して、環境内のファブリックのパフォーマンスとインベントリを監視し、原因 の問題の可能性がある変更を把握することができます。

Fibre Channelアセットページ

Insightのアセットページには、リソースに関する概要情報、トポロジ（デバイスとその接続）、パフォーマンスチャート、関連するリソースの表が表示されます。ファブリック、スイッチ、およびポートアセットのページを使用して、Fibre Channel環境を監視できます。ファイバチャネル問題 のトラブルシューティングを行う場合は、各ポートアセットのパフォーマンスチャートが特に役立ちます。このチャートには、最も影響が大きいポートのトラフィックが表示されます。また、バッファ間クレジットの指標やポートエラーも表示できます。Insightでは指標ごとに個別のパフォーマンスチャートが表示されます。

ポート指標のパフォーマンスポリシー

Insightでは、パフォーマンスポリシーを作成して、さまざまなしきい値に基づいてネットワークを監視し、それらのしきい値を超えたときにアラートを生成することができます。使用可能なポート指標に基づいて、ポートのパフォーマンスポリシーを作成できます。しきい値の違反が発生すると、Insightによって検出され、関連するアセットページに赤い丸で表示されます。設定されている場合はEメールで通知されるほか、[Violations Dashboard]や違反を報告するカスタムダッシュボードにも表示されます。

Time-To-Live （ TTL ）とデータのダウンサンプリング

OnCommand Insight 7.3以降では、データの保持期間（Time-To-Live）が7日から90日に延長されました。そのため、チャートや表用に処理されるデータがはるかに多く、データポイントが数万に及ぶ可能性があるため、データは表示前にダウンサンプリングされます。

ダウンサンプリングされると、グラフにデータの統計的な概算値が表示されるため、すべてのデータポイントを表示することなく、データの概要を効率的に把握できます。また、収集したデータは常に正確に把握できます。

ダウンサンプリングが必要な理由

Insight 7.3では、データのTime-To-Live（TTL）が90日に延長されています。これは、グラフやグラフに表示

するデータを準備するために必要な処理量が増加することを意味します。グラフをすばやく効率的に表示できるように、データはダウンサンプリングされ、グラフの全体的な形状が維持されます。そのため、そのグラフのすべてのデータポイントを処理する必要はありません。

> ダウンサンプリング中に実際のデータが失われることはありません。このあとに示す手順に従って、ダウンサンプリングされたデータではなく、実際のデータでグラフを表示することもできます。

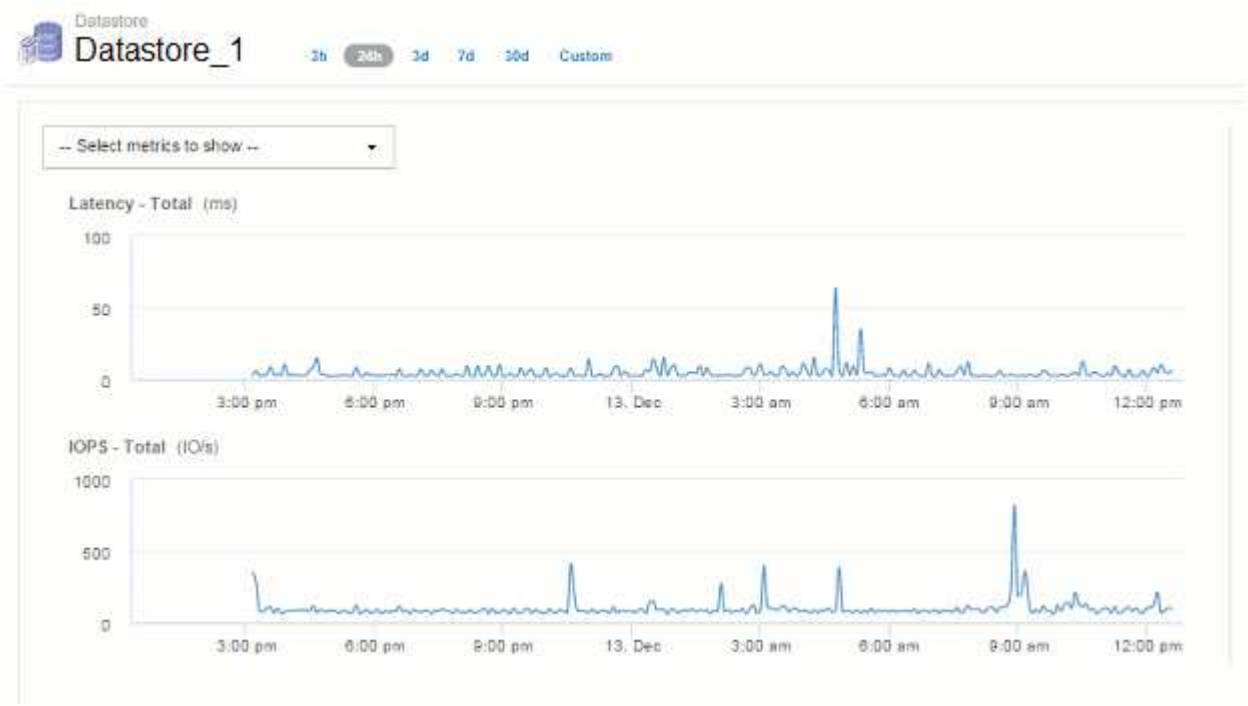
ダウンサンプリングの仕組み

データがダウンサンプリングされる条件は次のとおりです。

- 選択した時間範囲で収集されるデータが 7 日分以下の場合、ダウンサンプリングは行われません。グラフには実際のデータが表示されます
- 選択した時間範囲で収集されるデータが 7 日分を超えていても、データポイントの数が 1 、 000 個未満の場合、ダウンサンプリングは行われません。グラフには実際のデータが表示されます
- 選択した時間範囲で収集されるデータが 7 日分を超え、かつデータポイントの数が 1 、 000 を超える場合は、データがダウンサンプリングされます。グラフには概算データが表示されます。

次に、ダウンサンプリングの実際の例を示します。最初の図は、データストアのアセットページの時間セレクタで* 24h を選択して、**24**時間のレイテンシと**IOPS**のグラフを表示したものです。また、 Custom *を選択し、時間範囲を同じ24時間に設定すると、同じデータが表示されます。

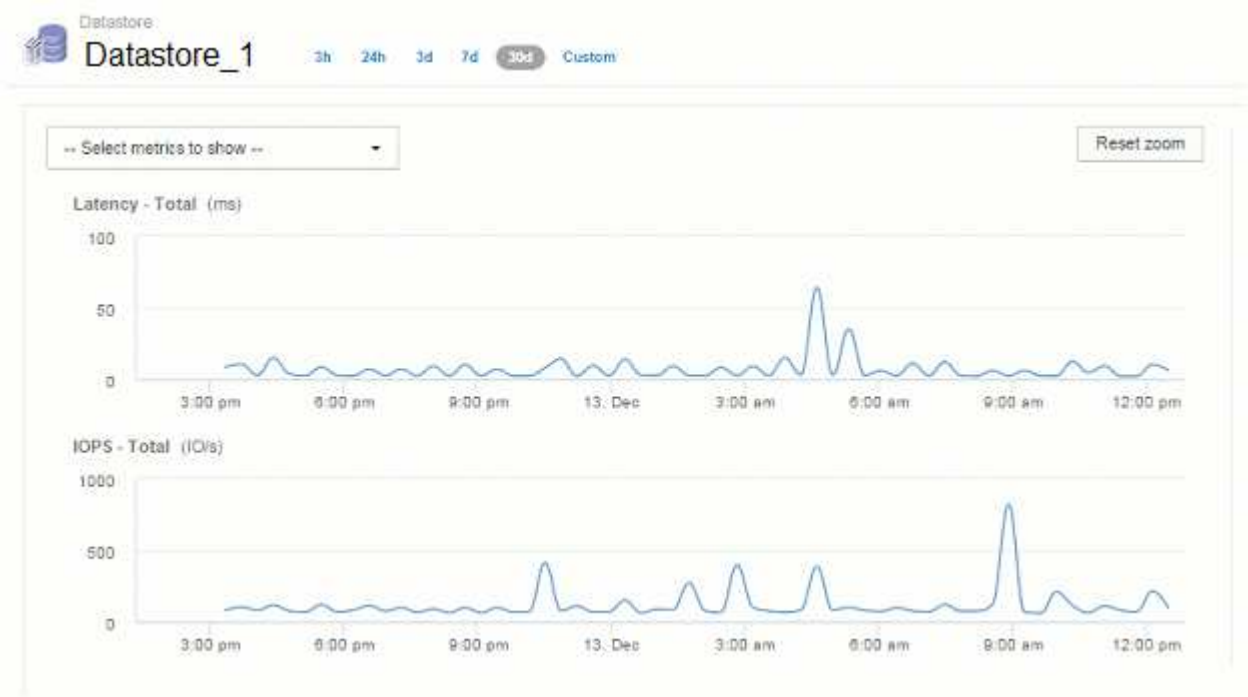
7 日未満の時間範囲を選択しており、グラフのデータポイントも 1 、 000 未満であるため、実際のデータが表示されます。ダウンサンプリングは行われません。



ただし、アセットページの時間セレクタで* 30d *を選択してデータを表示している場合は、 または、7日を超えるカスタムの期間を設定すると（または、選択した期間についてInsightで収集されたデータサンプルが1、000件を超える場合）、データがダウンサンプリングされてから表示されます。ダウンサンプリングされたグラフを拡大表示しても、表示されるのは概算データのままです。

ダウンサンプリングされたグラフを拡大表示すると、表示倍率はデジタルズームになります。表示されるのは概算データのままです。

この例を次の図に示します。時間範囲を 30 日に設定してグラフを表示してから、上記と同じ 24 時間のデータを表示するように拡大表示しています。



このダウンサンプリングされたグラフは、上記の「実際のデータ」のグラフと同じ 24 時間のデータを表示したものであるため、グラフの線の大まかな形状は同じであり、パフォーマンスデータのピークやボトムをすばやく特定することができます。

ダウンサンプリングの概算データの処理方法によっては、ダウンサンプリングされたデータとの比較でグラフの線が多少異なる場合があります実際のデータを比較したときに、グラフの線に多少の違いが見られることがあります。ただし、違いは最小限であり、表示されるデータの全体的な精度には影響しません。

ダウンサンプリングされたグラフでの違反の確認

ダウンサンプリングされたグラフを表示するときは、違反が表示されないことに注意してください。違反を確認するには、次のいずれかを実行します。

- アセットページの期間セレクタで Custom を選択し、 7 日未満の期間を入力して、その期間の実際のデータを表示します。赤の各点にカーソルを合わせます。ツールチップに発生した違反が表示されます。
- 違反ダッシュボードで期間と違反を確認します。

インベントリ履歴の削除

バージョン7.3.2以降では、インベントリ（基盤）の変更履歴が90日間保持されます。以前のバージョンのInsightでは、インストール時からインベントリの変更履歴がすべて保持されていました。古いバージョンのInsightからアップグレードすると、古いインベン

トリ履歴は削除されてから90日後に保持されます。

OnCommand Insight を現在のバージョンにアップグレードすると、履歴は最新の90日間に削除されます。Insightでは、90日分の履歴が残るまで、1日に1回発生する30日間のチャンクで履歴が削除されます。その後、履歴は毎日削除され、わずか90日分のインベントリ変更履歴が保持されます。

VMのNASパス

OnCommand Insight 7.3では、ストレージ共有への仮想マシンのNASパスがサポートされます。これらのパスは、ストレージ共有へのホストのNASパスに似ています。VMのIPアドレスが共有へのアクセスを許可されると、NASパスが作成されます。

仮想マシンのNASパスは、[Internal Volumes]ランディングページに表示されます。このページには、VMがアクセスできる内部ボリュームを特定する[Guest Mounted Storage Resources]ウィジェットが含まれています。

- NASパスは、仮想マシンがバックエンド共有にアクセスできる場合に作成されます。仮想マシンが共有にアクセスするかどうかの確認応答はありません。
- 相関関係はレイテンシとIOPSに基づいて計算されます。VMにバックエンドストレージへのNASパスがある場合は関係ありません。
- ユーザはイニシエータのIPアドレスで共有を照会できますが、パスによる照会はサポートされていません。

内部ボリュームの[Compute Resources]テーブルに、VMとNASパスが表示されるようになりました。VMごとに、CPUとメモリ、利用率とパフォーマンスのデータが表示されます。

Data Warehouseへの影響

OnCommand Insight 7.3へのアップグレード後に行われるData Warehouseに対する変更点は次のとおりです。

- dwh_inventory.nas_logicalテーブルがInventoryデータマートから削除され、ビューに置き換えられました。

  NFSパステーブルを含むInsight 7.2.xのレポートはすべて維持されます。

- Inventoryデータマートにdwh_inventory.nas_cr_logicalテーブルが追加されました。次のテーブルが含まれています。
  - コンピューティングリソース
  - 内部ボリューム
  - ストレージ
  - NAS共有

時系列としての容量

OnCommand Insight 7.3.1では、容量情報が時系列のデータとしてレポートおよびグラフに表示されます。

これまでは、データソースから取得した容量情報は「ポイントインタイム」（PIT）データのみであり、グラフで時系列のデータとして使用することはできませんでした。アセットの容量の値を次の方法で時系列のデータとして使用できるようになりました。

- 表、ウィジェット、エキスパートビューなど、時系列のデータが表示される場所でグラフ化されます
- 既存のセマンティクスを使用して違反が発生したパフォーマンスしきい値に適用されます
- 必要に応じて、式で他のパフォーマンスカウンタとともに使用します

以前のバージョンのInsightからアップグレードすると、カスタムダッシュボードのクエリやフィルタで使用されていたPIT容量の値が時系列の容量データに置き換えられます。そのため、レポートやフィルタリングの方法が、以前のバージョンのInsightでの同等のデータと若干異なる場合があります。

Data Warehouseの管理

OnCommand Insight データウェアハウスへようこそ

OnCommand Insight データウェアハウスは、複数のOnCommand Insight サーバのデータを格納し、照会や分析に使用する共通の多次元データモデルに変換する、一元化されたリポジトリです。

OnCommand Insight データウェアハウスでは、複数のデータマートで構成されるオープンデータベースにアクセスして、容量やパフォーマンスに関するカスタムレポート（チャージバックレポート、履歴データを使用したトレンドレポート、消費分析レポート、予測レポートなど）を生成できます。

Data Warehouseの機能

OnCommand Insight データウェアハウスは、複数のデータマートで構成される独立したデータベースです。

Data Warehouseには次の機能があります。

- 現在と過去の設定およびインベントリデータ。予測や計画に役立つトレンドレポートを作成できます
- 複数の多次元履歴データマートと、最新のみのInventoryデータマートが追加されています
- 事前定義クエリまたはユーザー定義クエリ用に最適化されたデータベース
- サードパーティのレポートエンジンやビジネスインテリジェンスエンジンと統合するためのプラットフォーム。次のようなものがあります。
  - 構成管理データベース
  - 財務会計システム
  - 資産管理システム

Data Warehouseのコンポーネント

Data Warehouseには複数のコンポーネントがあります。

- Data Warehouseポータル
- OnCommand Insight Reporting Portalの略
- レポートオーサリングツール

Data Warehouseポータルを使用して実行できる操作

Data WarehouseポータルはWebベースのユーザインターフェイスです。このインターフェイスを使用して、データを取得するためのオプションを設定したり、固定スケジュールを設定したりできます。Data Warehouseポータルから、OnCommand Insight のレポートポータルにもアクセスできます。

Data Warehouseポータルでは、次の操作を実行できます。

- OnCommand Insight のReportingポータルにアクセスして、事前定義済みのレポートを表示したり、レポートオーサリングツールを使用してカスタムレポートを作成したりできます。
- 複数のOnCommand Insight データベースを統合します。
- OnCommand Insight サーバへの接続を管理します。
- 現在のジョブまたは実行中のクエリのステータスを確認します。
- Data Warehouseのビルドのスケジュールを設定します。
- サイト名を編集します。
- Data Warehouseのバージョンとアップグレード履歴（モジュールのバージョン、サイト、ライセンスなどの特定の情報を含む）を表示します。
- アノテーションをインポートする。
- 履歴からビルドを構成します。
- Data Warehouseのドキュメントとデータベーススキーマを参照できます。
- Data Warehouseデータベースをリセットします。
- Data Warehouseデータベースをバックアップおよびリストアします。
- Data Warehouseの問題のトラブルシューティング
- ユーザアカウントを管理します。

Data Warehouseのソフトウェアコンポーネント

OnCommand Insight Data Warehouseには、複数のソフトウェアコンポーネントが含まれています。

- MySQL データベース

  データマートテーブルのバックエンドリポジトリ

- IBM Cognos

  OnCommand Insight のレポート作成エンジン

- Apache Derbyデータベース

  Cognosの設定とコンテンツの格納に使用されます

- ワイルドフライ

  OnCommand Insight コンポーネントをホストするJava Enterpriseアプリケーションサーバー

Data Warehouseのプロセス

Data Warehouseでは、さまざまな種類のプロセスが実行されます。

- * ETLプロセス*

抽出、変換、読み込み（ETL）プロセスは、複数のOnCommand Insight データベースからデータを取得して変換し、データマートに保存します。Data WarehouseのビルドプロセスはETLプロセスです。

- * ジョブ *

  Data Warehouseで、インベントリ、ディメンション、容量、ポート容量、VM容量などのジョブが実行され、レポートが作成されます。 ファイルシステムの利用率、パフォーマンス、容量効率、ライセンス、履歴ビルド、 動的なアノテーション、コネクタの削除、スキップされたビルド、ASUPオプション、およびメンテナンスジョブ。

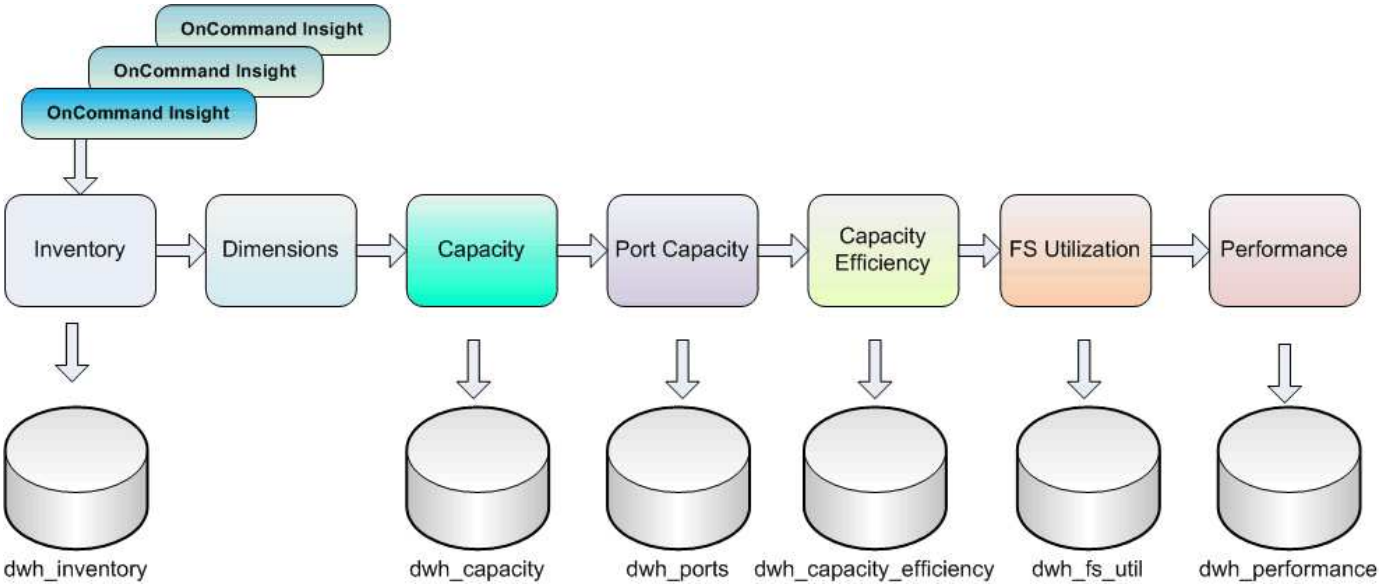
- 統合プロセス

  Data Warehouseでは、複数のOnCommand Insight サーバを同じData Warehouseデータベースに統合できます。多くの構成では、同じオブジェクトが複数のコネクタから報告される場合があります（つまり、同じスイッチが2つのOnCommand Insight インスタンスに存在する場合）。その場合、Data Warehouseは複数のオブジェクトを1つに統合します（プライマリコネクタが選択され、オブジェクトのデータはそのコネクタからのみ取得されます）。

Data Warehouseでのデータの抽出方法

抽出、変換、読み込み（ETL）プロセスは、複数のOnCommand Insight データベースからデータを取得して変換し、データマートに保存します。

OnCommand Insight コネクタは、次の図に示すように、一連のバッチジョブを起動して、複数のOnCommand Insight MySQLデータベースからデータを抽出し、さまざまなデータマートにパブリッシュします。



ETL プロセスは、次の個別プロセスで構成されます。

- 抽出

  このプロセスでは、複数のOnCommand Insight データベースからデータを取得して変換し、データマートに保存します。このプロセスは、各OnCommand Insight インスタンスに対して同時に実行されます。データクレンジングと重複排除が確実に実行されるようにするために、ETLプロセスを複数のスケジュールされたETL処理に分割することはできません。

- 変換

  このプロセスは、ビジネスロジックルールまたは関数を適用して、OnCommand Insight データベースからデータを抽出します。

- ロード

  このプロセスでは、変換されたデータがパブリックデータマートにロードされます。

ETLの頻度と日付データ

抽出、変換、読み込み（ETL）プロセスは少なくとも1日に1回は実行する必要がありますが、必要に応じて何度も実行することを選択します。

Cognosのレポート作成エンジンでは、デフォルトですべての容量とパフォーマンスのファクトが追加で処理されます。そのため、適切な時間フィルタを使用せずにETLプロセスを1日に複数回実行すると、容量データが二重にカウントされるリスクがあります。

Dateディメンションの2つの日付データ要素は、日次ETLプロセスに関連しています。複数のデータモデルで使用されるDateディメンションには、ETLの影響を受ける次のデータ要素が含まれています。

- *はデイ代表*です

  「Is Day Representative」データ要素は、1日の最初のETLプロセスの実行時に1（true）に設定されます。最初のETLプロセスが午前1時に実行される場合は、午前1時にロードされるすべてのデータについて、Is Day Representativeが1に設定されますETLプロセスそのあと（午後1時など）に2つ目のETLがスケジュールされている場合は、そのETLプロセスでロードされたデータに対して「Is Day Representative」が0（false）に設定されます。

- *が最新*です

  「Is Latest」メンバーは、各ETLプロセスが完了すると1（true）に設定されます。最初のETLプロセスが午前1時に実行される場合は、午前1時のETLプロセスで読み込まれるすべてのデータに対して「Is Latest」が1に設定されますETLプロセスそのあと（午後1時など）に別のETLプロセスがスケジュールされている場合は、午後1時にロードされるデータに対して「Is Latest」が1に設定されますETLプロセスETLプロセスでは午前1時も設定されますETLロードの「Is Latest」エントリは0（false）です。

Data Warehouseでの履歴データの保持方法

データはスケジュールに従ってData Warehouseで管理されます。データが古くなると、データレコードの保持期間が短くなります。

Data Warehouseでは、次の表に示すように、データマートおよびデータの単位に基づいて履歴データが保持されます。

データマート	測定されたオブジェクト	精度	保持期間
Performance データマート	ボリュームと内部ボリューム	毎時	14 日

Performance データマート	ボリュームと内部ボリューム	毎日	13 カ月
Performance データマート	アプリケーション	毎時	13 カ月
Performance データマート	ホスト	毎時	13 カ月
Performance データマート	ポートのスイッチパフォーマンス	毎時	5週間です
Performance データマート	ホスト、ストレージ、およびテープのスイッチパフォーマンス	毎時	13 カ月
Performance データマート	ストレージノード	毎時	14 日
Performance データマート	ストレージノード	毎日	13 カ月
Performance データマート	VM パフォーマンス	毎時	14 日
Performance データマート	VM パフォーマンス	毎日	13 カ月
Performance データマート	ハイパーバイザーのパフォーマンス	毎時	14 日
Performance データマート	ハイパーバイザーのパフォーマンス	毎日	13 カ月
Performance データマート	VMDK パフォーマンス	毎時	14 日
Performance データマート	VMDK パフォーマンス	毎日	13 カ月
Performance データマート	ディスクパフォーマンス	毎時	14 日
Performance データマート	ディスクパフォーマンス	毎日	13 カ月

Capacity データマート	すべて（個々のボリュームを除く）	毎日	13 カ月
Capacity データマート	すべて（個々のボリュームを除く）	月の代表日	14 カ月以上
Inventory データマート	個々のボリューム	現在の状態	1 日（または次の ETL まで）

13カ月（設定可能）が経過すると、Data Warehouseの次のファクトテーブルでは、容量、パフォーマンス、リソースのデータが1日に1レコードではなく1カ月に1レコードだけ保持されます。

- Chargebackファクトテーブル（dwh_capacity.chargeback_fact）
- File System Utilizationファクトテーブル（dwh_fs_util.fs_util_fact）
- Hostファクトテーブル（dwh_sa.sa_host_fact）
- Internal Volume Capacityファクトテーブル（dwh_capacity.internal_volume_capacity_fact）
- Portsファクトテーブル（dwh_ports.ports_fact）
- Qtree Capacityファクトテーブル（dwh_capacity.qtree_capacity_fact）
- Storage and Storage Pool Capacityファクトテーブル（dwh_capacity.storage_and_storage_pool_capacity_fact）
- Volume Capacityファクトテーブル（dwh_capacity.vm_capacity_fact）
- Storage Node Hourly Performanceファクトテーブル（storage_node_hourly_performance_fact）とStorage Node Daily Performanceファクトテーブル（storage_node_daily_performance_fact）

データ保持、**ETL**、および期間

OnCommand Insight Data Warehouseでは、抽出、変換、読み込み（ETL）プロセスで取得したデータが、データマートやデータの時間単位に基づいて、さまざまな期間にわたって保持されます。

Performanceデータマートおよび時間単位（ボリュームおよび内部ボリューム）

OnCommand Insight Data Warehouseでは、1時間ごとの平均値、1時間ごとの最大値、および1日の各時間（24個のデータポイント）のアクセスビットが14日間記録されます。アクセスビットはブール値で、1時間のインターバルの間にボリュームがアクセスされた場合はtrue、アクセスされなかった場合はfalseになります。前日の24個のデータポイントはすべて、その日の最初のETLプロセスで取得されます。

ETLプロセスを1時間に1回実行して1時間ごとのデータポイントを収集する必要はありません。1日のうちに追加のETLプロセスを実行しても、OnCommand Insight Serverからパフォーマンス情報が取得されません。

Performanceデータマートおよび日単位（ボリュームと内部ボリューム）

ETLが処理される毎日の平均値が計算され、Data Warehouseに入力されます。1日平均は、前日の24個のデータポイントの要約です。Performanceデータマートには、ボリュームと内部ボリュームの日単位の要約が13カ月間保持されます。

Capacityデータマートおよび日単位

Capacityデータマートは、さまざまな容量ファクトの日単位の測定値を13カ月間提供します。Data Warehouse内の容量ファクトは、ETL前のデバイスの最後のデータソース収集時点の最新情報です。

Capacityデータマートおよび月単位

Data Warehouseには、日単位の容量データが13カ月間保持されます。13カ月のしきい値に達すると、容量データが月単位で集計されます。月単位のデータは、月の代表日である日付によって反映される値に基づいています。

次の表に、月次サマリーに含まれる月次データを示します。

日付	月代表値です	割り当て容量
1月1日	1（正しい）	50TB
1月2日	0（False）	52TB
…	…	…
1月31日	0（False）	65 TB
2月1日	1（正しい）	65 TB

この表を基にした月次レポートには、1月に50TBが割り当てられ、2月に65TBが割り当てられています。1月のそれ以外の容量の値は、月単位の要約には含まれません。

Inventoryデータマート

Inventoryデータマートは履歴データではありません。ETLプロセスが実行されるたびに、Inventoryデータマートが消去されて再構築されます。そのため、Inventoryデータマートから生成されたレポートには、過去のインベントリ設定が反映されません。

Data Warehouseでの作業の開始

OnCommand Insight Data Warehouseでは、データを含むレポートを生成する前に必要なオプションを設定できます。Data Warehouseには多くの機能が含まれていますが、使用する機能はごく一部です。Data Warehouseをセットアップするには、Data Warehouseポータルのオプションを使用します。

このタスクについて

OnCommand Insight Data Warehouseをセットアップするには、ストレージ管理者が次の手順を実行する必要があります。

- Data Warehouseポータルにアクセスします
- Data WarehouseとOnCommand Insight サーバの接続

- 履歴からデータベースをビルドしています
- バックアッププロセスとリストアプロセスをセットアップします

また、ストレージ管理者が次の手順を実行することもできます。

- コマンドラインインターフェイスを使用したMySQLへのアクセス
- 日次ビルドのスケジュール設定
- レポートにマルチテナンシーを設定しています
- セットアップの問題のトラブルシューティング
  - アノテーションが表示されないのはなぜですか？
  - 失敗した履歴ビルドポイントの処理

Data Warehouseポータルを初めて使用する場合は、[Jobs]ページに情報を表示する前にData Warehouseをセットアップしておく必要があります。Data Warehouseデータベースをリセットしたあとにも、このセットアッププロセスを繰り返す必要があります。

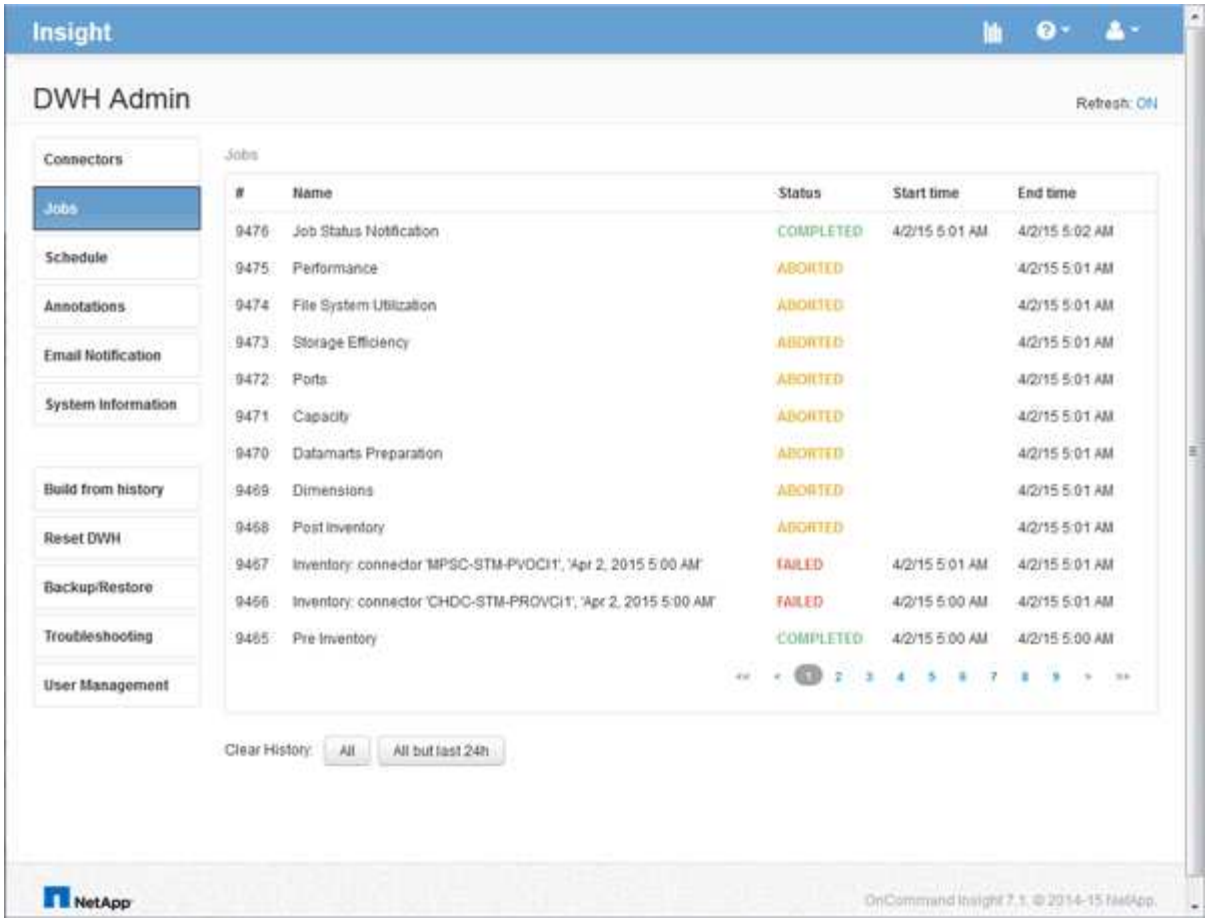
Data Warehouseポータルにアクセスします

OnCommand Insight Data WarehouseポータルはWebベースのユーザインターフェイスで、コネクタ情報の更新、ジョブキューの表示、日次ビルドのスケジュール設定、アノテーションの選択、Eメール通知の設定、システム情報の表示、データベースのビルド、Data Warehouseのリセット、データベースのバックアップとリストア、問題のトラブルシューティングを実行できます。 Data WarehouseポータルとReportingポータルのユーザアカウントを管理し、ドキュメントやスキーマ図にアクセスできます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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. ユーザ名とパスワードを入力します。
3. [* ログイン] をクリックします。

   Data Warehouseポータルが開きます。



Data Warehouseおよび**Reporting**のユーザアカウントの管理

OnCommand Insight のレポート作成ツールのユーザアカウント、ユーザ認証、およびユーザ許可は、Data Warehouse（DWH）で定義および管理されます。ユーザと管理者は、これらの設定に基づいて、使用可能なOnCommand Insight レポートの一部またはすべてにアクセスできます。

Data Warehouseのユーザ管理にアクセスするには、システム管理者の権限を持つアカウントが必要です。これには、次のもの

- Data Warehouseのすべての管理機能
- すべてのユーザアカウントの設定とメンテナンス
- データベースへの読み取りアクセス権
- ETLでのコネクタのセットアップ、Data Warehouseジョブのスケジュール設定、データベースのリセット、ロールの割り当てと変更、ユーザアカウントの追加と削除を行う機能

Data Warehouseポータルおよび**Reporting**ポータルへのアクセス

Data Warehouseポータルでは、管理オプションにアクセスできます。Data Warehouseポータルから**Reporting**ポータルにアクセスすることもできます。

手順

1. Data Warehouseポータルに管理者としてログインします `https://hostname/dwh`、ここで `hostname` 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. Data Warehouseツールバーで、をクリックします をクリックしてReportingポータルを開きます。

Reportingユーザのロール

各ユーザアカウントには、一連の権限を持つロールが割り当てられます。ユーザーの数は、各ロールに関連付けられているReportingライセンスの数によって制限されます。

各ロールで実行できる操作は次のとおりです。

- 受信者

  OnCommand Insight Reportingポータルのレポートを表示し、言語やタイムゾーンなどの個人設定を設定します。

  > 受信者は、レポートの作成、レポートの実行、レポートのスケジュール設定、レポートのエクスポート、および管理タスクの実行を行うことはできません。

- ビジネスコンシューマ

  レポートを実行し、すべての受信者オプションを実行します。

- ビジネス著者

  Business Consumerのすべてのオプションに加えて、スケジュールされたレポートの表示、対話形式でのレポートの実行、ストーリーの作成が可能です。

- * Pro Author *

  Business Authorのすべてのオプションの実行に加えて、レポートの作成、パッケージおよびデータモジュールの作成を行います。

- 管理者

  レポート定義のインポートとエクスポート、レポートの設定、データソースの設定、レポートタスクのシャットダウンと再開など、レポート管理タスクを実行します。

次の表に、各ロールの権限と許可される最大ユーザ数を示します。

フィーチャー（Feature）	受信者	ビジネスパーソン	著作家	作者プロ	管理
[チームコンテンツ] タブでレポートを表示します	はい。	はい。	はい。	はい。	はい。

レポートを実行する	いいえ	はい。	はい。	はい。	はい。
レポートのスケジュールを設定する	いいえ	はい。	はい。	はい。	はい。
外部ファイルをアップロードします	いいえ	いいえ	はい。	はい。	いいえ
ストーリーを作成します	いいえ	いいえ	はい。	はい。	いいえ
レポートを作成します	いいえ	いいえ	はい。	はい。	いいえ
パッケージとデータモジュールを作成します	いいえ	いいえ	いいえ	はい。	いいえ
管理タスクを実行	いいえ	いいえ	いいえ	いいえ	はい。
ユーザ数	OnCommand Insight ユーザの数	20	2.	1.	1.

Data WarehouseとReportingの新しいユーザを追加したときにロールの制限を超えたユーザが「非アクティブ化」として追加されます。新しいユーザにメンバーシップを付与するには、そのロールを持つ別のユーザを非アクティブ化するか削除する必要があります。

> レポートオーサリング機能を使用するにはInsight Planのライセンスが必要です。Business AuthorユーザとPro Authorユーザを追加するには、ARAP（Additional Report Authoring Package）を購入します。詳細については、OnCommand Insight の担当者にお問い合わせください。

Reportingユーザのロールは、データベースへの直接アクセスには影響しません。Reportingユーザのロールは、データマートを使用してSQLクエリを作成する機能には影響しません。

Reportingユーザを追加しています

Reportingポータルへのアクセスを必要とするユーザごとに新しいユーザアカウントを追加する必要があります。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。

作業を開始する前に

Reportingユーザを追加する前に、一意のユーザ名を割り当て、使用するパスワードを決定し、正しいユーザロールを確認しておく必要があります。これらのロールはReportingポータルに特化されています。

手順

1. Data Warehouseポータルに管理者としてログインします `https://hostname/dwh`、ここで `hostname` 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、*[ユーザ管理]*をクリックします。
3. [ユーザー管理]ウィンドウで、*[新しいユーザーの追加]*をクリックします。
4. 新しいReportingユーザについて、次の情報を入力します。
   - * ユーザー名 *

     アカウントのユーザ名（a$_{z}$、$_{A}$Z、0~9を含む英数字）
   - 電子メールアドレス

     ユーザアカウントに関連付けられたEメールアドレス。ユーザがレポートをサブスクライブする場合に必要です
   - * パスワード *

     このユーザアカウントでOnCommand Insightにログインするためのパスワード。通常はユーザが選択し、インターフェイスで確認します
   - * Insightロール*

     適切な権限を持つユーザが使用できるロール

     > OnCommand Insight ロールのオプションは、OnCommand Insight がレポーティングファシリティと同じマシンにインストールされている場合にのみ表示されます。これは一般的ではありません。
   - レポートロール

     このユーザアカウントのReportingロール（Pro Authorなど）

     > Administratorロールは一意です。このロールは任意のユーザに追加できます。
5. [追加（ Add ）] をクリックします。

ユーザアカウントの管理

Data Warehouseポータルで、ユーザアカウント、ユーザ認証、およびユーザ許可を設定できます。各ユーザアカウントには、次のいずれかの権限レベルを持つロールが割り当てられます。ユーザーの数は、各ロールに関連付けられているReportingライセンスの数によって制限されます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*[ユーザ管理]*をクリックします。

User Management

	OnCommand Insight roles			Reporting roles									
Name	Guest	User	Administrator	Recipient	Business Consumer	Business Author	Pro Author	Administrator	E-mail				
guest	X									Edit	Delete	Change password	Deactivate
user	X	X								Edit	Delete	Change password	Deactivate
admin	X	X	X				X	X		Edit		Change password	
oadmin	X	X	X							Edit		Change password	Deactivate

LDAP Configuration | Add New User | Change DWH User password

The following table shows the privileges for each reporting role:

Feature	Recipient	Business Consumer	Business Author	Pro Author	Administrator
View reports (in Public Folder tab, My Folders)	Yes	Yes	Yes	Yes	Yes
Run reports	No	Yes	Yes	Yes	Yes
Schedule Reports	No	Yes	Yes	Yes	Yes
Create reports in Query Studio	No	No	Yes	Yes	No
Create reports in Workspace (Standard)	No	Yes	Yes	Yes	No
Create reports in Workspace (Advanced)	No	No	Yes	Yes	No
Create reports in Report Studio	No	No	No	Yes	No
Perform administrative tasks	No	No	No	No	Yes

3. 次のいずれかを実行します。
   - 既存のユーザーを編集するには、そのユーザーの行を選択して*[編集]*をクリックします。
   - ユーザーのパスワードを変更するには、ユーザーの行を選択し、*パスワードの変更*をクリックします。
   - ユーザを削除するには、ユーザの行を選択し、*[削除]*をクリックします
4. ユーザーを活動化または非活動化するには、ユーザーの行を選択して*活動化*または*非活動化*をクリックします。

レポート用に**LDAP**を設定しています

Data Warehouseポータルでは、管理者がData WarehouseおよびReportingでのLDAPの使用方法を設定できます。

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Insightにログインする必要があります。

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。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*[ユーザ管理]*をクリックします。
3. [LDAP設定]*をクリックします。

4. [LDAPを有効にする]*を選択して、LDAPユーザの認証と許可のプロセスを開始します。
5. LDAPの設定に必要な変更を行います。

   ほとんどのフィールドにはデフォルト値が含まれています。デフォルト設定はActive Directoryに対して有効です。

   - 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`。

   - 紹介

     企業内に複数のドメインがある場合に、他のドメインへのパスをたどるかどうかを指定します。常にデフォルトを使用する必要があります `follow` 設定：

   - 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。

   - * LDAPサーバ*

     LDAPサーバを識別するIPアドレスまたはDNS名です。特定のポートを識別するには、を参照してください `ldap-server-address` はLDAPサーバの名前です。次の形式を使用できます。

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

     デフォルトのポートを使用するには、次の形式を使用します。

```
ldap://ldap-server-address
```

> When entering multiple LDAP servers in this field, separate entries with a comma, and ensure that the correct port number is used in each entry.
> + LDAP証明書をインポートするには、*[証明書のインポート]*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。

- 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
```

- * Insight Server admins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`。

- * Insight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`。

- * Insight Users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`。

- * Insight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`。

- レポート管理者グループ

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

- * Reporting Pro Authorsグループ*

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

- レポートビジネス作成者グループ

  Insight ReportingのBusiness Authors権限を持つユーザのLDAPグループ。デフォルトはです

`insight.report.business.authors`。

- ビジネス消費者グループの報告

  Insight Reporting Business Consumers権限を持つユーザのLDAPグループ。デフォルトはです `insight.report.business.consumers`。

- レポート受信者グループ

  Insight Reportingの受信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.report.recipients`。

6. 変更を加えた場合は、* Directory lookup user および Directory lookup user password *フィールドに値を入力します。

   これらのフィールドに変更後の値を入力しないと、変更内容は保存されません。

7. [ディレクトリルックアップユーザパスワードの確認]フィールドにディレクトリルックアップユーザパスワードを再入力し、*[パスワードの検証]*をクリックしてサーバ上のパスワードを検証します。
8. をクリックして変更を保存します。変更を削除するには、[キャンセル]*をクリックします。

Data WarehouseとOnCommand Insight サーバの接続

コネクタは、OnCommand Insight データウェアハウスからOnCommand Insight サーバへの接続を確立します。Data Warehouseは1つ以上のOnCommand Insight サーバに接続できます。OnCommand Insight データベースへの接続またはデータベースからの接続を追加または削除できます。

このタスクについて

Data Warehouseでは、コネクタ名とともに使用されるグローバル一意IDがコネクタに割り当てられます。コネクタの追加後、Data WarehouseはOnCommand Insight データベースにOnCommand Insight のサイト名とバージョンを照会します。

データソースへの接続にSSLを使用するかどうかを選択できます。セキュアなデータソースを選択すると、OnCommand Insight リモートデータベースとの通信時に接続にSSLが使用されます。

Data Warehouseでは、複数のOnCommand Insight 環境のデータをまとめて表示できます。この統合データベースは’次の情報を提供します

- Globally Unique Identifierの略

  各オブジェクトには、IDの競合を回避し、重複検出を可能にするために、個 々 のサイトで使用されるIDとは無関係なグローバル一意のIDが割り当てられます。これらのIDはすべてのデータマートで共有されます。このIDは、InventoryデータマートテーブルのComment列にあるGlobally Unique ID（GUID）です。

- 重複はありません

  複数のOnCommand Insight データベースに存在するエンティティは’統合データベースに1回だけ登録されます

- 現在のレコード

  統合データベース（Inventoryデータマート）のデータは常に最新です。

接続を追加または編集するときに、接続をテストすることもできます。このテストでは、次のことが行われます。

- ホストのIPアドレス、ユーザ名、およびパスワードを確認し、接続を確立できることを確認します。

  無効な接続は赤で表示されます。

- OnCommand Insight のバージョンとData Warehouseのバージョンを比較します。

  バージョンに互換性がない場合は、エラーメッセージが表示されます。

- 前回のData Warehouse処理で、OnCommand Insight データベースが別のデータベースに変更またはリストアされていないことが確認されます。変更があった場合は、エラーメッセージが表示されます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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。

   コネクタ(Connectors)テーブルは最初は空白で表示され’コネクタを追加するとコネクタ情報が表示されます

3. [新規（New）]*をクリックして、新しいコネクタを追加します。
4. 次のように入力します。

   - * 暗号化 *

     SSL暗号化を使用してData Warehouse要求を実行できるようにするには、を選択します `Enabled`。

   - * 名前 *

     [コネクタ（Connectors）]ビューでコネクタを識別するコネクタ名。

   - * ホスト *

     ホストの IP アドレス

   - * ユーザー名 *

     “inventory”

     > このユーザ名とパスワードを使用して、リモートOnCommand Insight データベースにログインし、データに対してクエリを実行できます。

   - * パスワード *

" SANscreen "

5. ホストへのTCP接続に使用するポートを指定するには、*[詳細設定]*をクリックし、TCPポート番号を入力します。
6. ホストへのHTTPS接続に使用するポート（デフォルトポート以外）を指定するには、*[詳細設定]*をクリックし、ポート番号を入力します。
7. [* テスト *] をクリックします。

   Data Warehouseで接続がテストされます。

8. [保存（ Save ）] をクリックします。

   複数のインストールに対して複数の接続を入力すると、Data Warehouseは、データの抽出元となるデータベースごとに1つずつ、独立したビルドプロセスを呼び出します。このような構築プロセスでは、OnCommand Insight データベースからデータが抽出され、統合データベースにロードされます。

Data Warehouseデータベースの履歴からのビルドの概要

OnCommand Insight サーバの履歴データを使用してData Warehouseデータベースを構築できます。Data Warehouseでは、[build from history]のスケジュールに従って、OnCommand Insight サーバからデータが抽出され、Data Warehouseデータマートがビルドされます。

このオプションでは特別なライセンスは必要なく、インベントリデータがビルドに含まれます。ただし、容量情報を作成するには、OnCommand Insight PlanライセンスとOnCommand Insight Performライセンスが必要です。

履歴または現行のいずれかのビルドがすでに実行されている場合、最後のジョブより前の日付にビルドを実行することはできません。つまり、現在のビルドを実行した場合、履歴からビルドすることはできません。具体的には、2012年1月1日に終了した履歴からビルドを実行した場合、2011年にビルドを実行することはできません。

履歴ビルドに1日または2日の失敗したETLプロセスが含まれていない場合は、この数日間だけ履歴をビルドしないでください。履歴データはより長い期間のものであり、1日か2日でトレンドが大きく変わることはありません。履歴から再構築する場合は、履歴全体を再構築します。

[履歴からビルド]ビューには、すべてのコネクタからのすべてのビルドジョブが表示されます。たとえば、すべてのコネクタのインベントリジョブ、ビルド実行ごとのポート容量ジョブ、アノテーションジョブなどが表示されます。

[Build from History]を設定する前に、次の作業を実行する必要があります。

- コネクタを設定する必要があります。
- アノテーションはOnCommand Insight に入力する必要があり、古いOnCommand Insight ポータルの*[Force Update of Annotations for DWH（DWHのアノテーションの強制更新）]オプション*を使用して手動で更新できます。または、設定後15分で自動的に更新されます。

Data Warehouseデータベースを履歴からビルドするジョブを追加する

Data Warehouseデータベースは、OnCommand Insight サーバに保持されている履歴デ

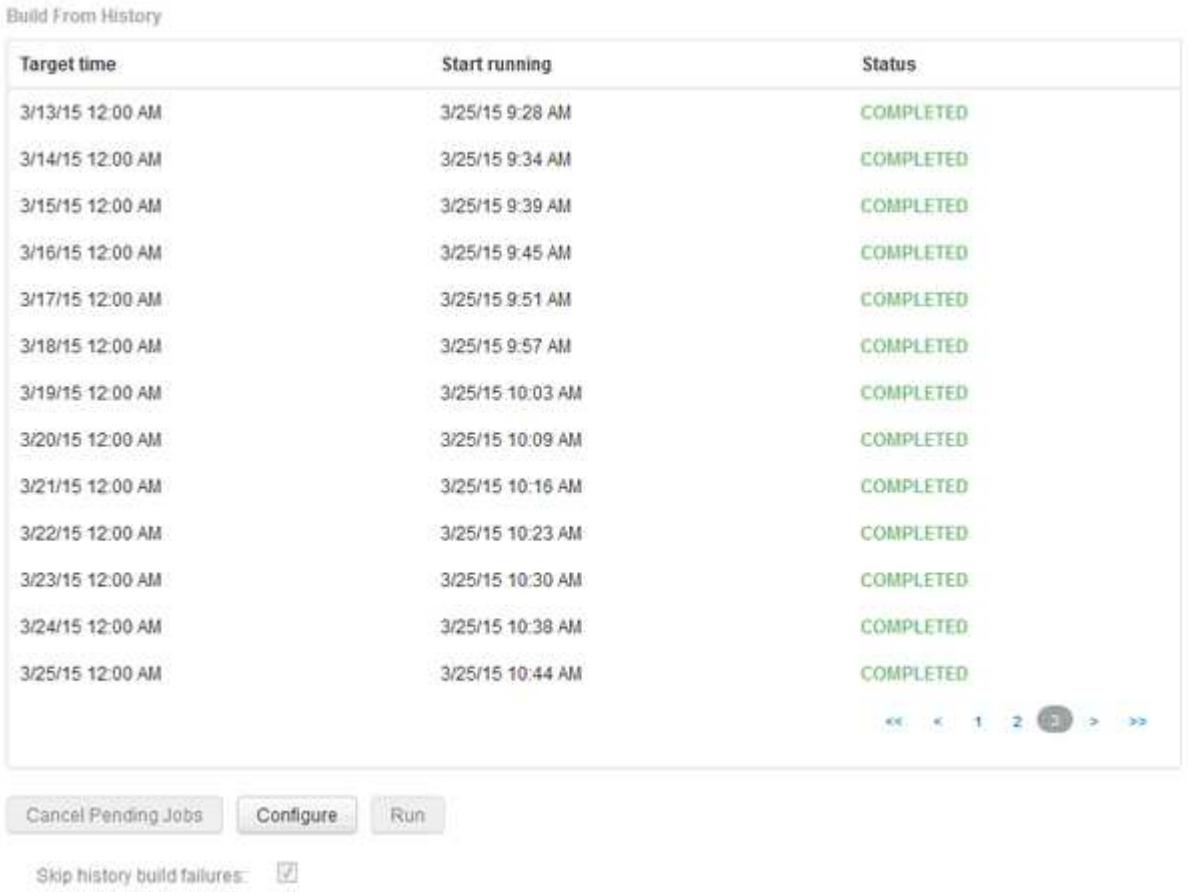
ータを使用して構築できます。これにより、予測レポートを実行できます。

作業を開始する前に

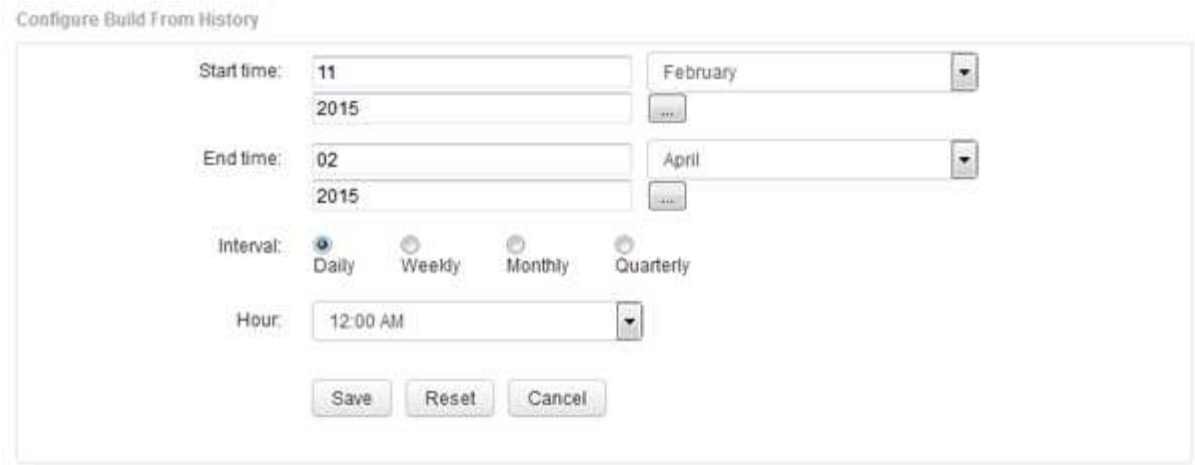
OnCommand Insight サーバでアノテーションを更新し、Data Warehouseのアノテーション情報を強制的に更新しておく必要があります。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*[履歴からビルド]*をクリックします。



3. [**Configure**] をクリックします。



4. 開始時刻と終了時刻を入力します。

   これらの日付を選択できるカレンダーを表示するには、月名の近くにある下向き矢印をクリックします。

   時刻の形式は、Data Warehouseサーバのロケールによって異なります。

   開始時刻と終了時刻は、Data Warehouseが接続されているすべてのOnCommand Insight サーバに格納されている履歴の範囲内である必要があります（Data Warehouseポータルの[Connectors]オプションで設定）。デフォルトの開始時刻と終了時刻は、最大有効期間を反映します。Data Warehouseのビルドジョブは、指定した時間に自動的に実行されます。

   > 「4年間毎日」のように非現実的なスケジュールを設定すると、ビルドサイクルは1460回になり、完了までに10日かかる場合があります。

5. 間隔を選択します。

   毎月または毎週の間隔を選択すると、[日]フィールドが表示されます。[Monthly]を選択した場合は、[Day]が日付になります。[Weekly]を選択した場合、[Day]は日曜日から土曜日になります。

6. ビルドを実行する時間を選択します。
7. オプションをデフォルト設定に戻すには、*[リセット]*をクリックします。
8. [保存（ Save ）] をクリックします。
9. ページで、スケジュールによる自動ビルド以外でビルドを実行するには、[実行]*をクリックします。

   [Target Time]列には、このエントリが作成された時刻が表示されます。[ステータス]列には、ビルドが完了したか失敗したかが表示されます。

履歴からビルドジョブをキャンセルしています

計画されたすべてのジョブをキャンセルできます。ジョブのステータスが「中止」になります。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname`

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、*[履歴からビルド]*をクリックします。
3. [キャンセル（ Cancel ）] をクリックします。

Data Warehouseデータベースをバックアップしています

Cognosのバックアップも含まれるData Warehouseデータベースをファイルにバックアップし、あとでData Warehouseポータルを使用してリストアできます。バックアップを作成すると、別のData Warehouseサーバに移行したり、新しいバージョンのData Warehouseにアップグレードしたりできます。

手順

1. Data Warehouseポータルにログインします `https://fqdn/dwh`。
2. 左側のナビゲーションペインで、*[バックアップ/リストア]*を選択します。
3. [バックアップ]*をクリックし、バックアップ構成を選択します。

   a. Performance Datamartを除くすべてのDatamarts
   b. すべてのデータマート

      この処理には30分以上かかることがあります。

   + Data Warehouseでバックアップファイルが作成され、その名前が表示されます。

4. バックアップファイルを右クリックし、目的の場所に保存します。

   ファイル名は変更しなくてもかまいませんが、Data Warehouseのインストールパス以外の場所に保存してください。

   Data Warehouseのバックアップファイルには、DWHインスタンスのMySQL、カスタムスキーマ（MySQL DB）とテーブル、LDAP設定、CognosをMySQLデータベースに接続するデータソース（Insight Serverをデータを取得するデバイスに接続するデータソースではない）が含まれています。 レポートをインポートまたはエクスポートしたタスクのインポートとエクスポート、セキュリティロール、グループ、名前空間のレポート、ユーザーアカウント Reporting Portalの変更後のレポートとカスタムレポート（保存場所に関係なく、[My Folders]ディレクトリにも保存されます）。Cognosのシステム設定パラメータ（SMTPサーバ設定など）、およびCognosのカスタムメモリ設定はバックアップされません。

   カスタムテーブルがバックアップされるデフォルトのスキーマには、次のものがあります。

dwh_capacityの略
dwh_capacity_stagingの略
dwh_dimensionsの略
dwh_fs_utilを参照してください

dwh_inventoryの略
dwh_inventory_stagingの略
dwh_inventory_transient
dwh_managementの略
dwh_performanceの略
dwh_performance_stagingの略
DWH_ポート
dwh_reportsの略
dwh_sa_stagingの略

カスタムテーブルをバックアップから除外するスキーマには、次のものがあります。

information_schema
取得
cloud_model
host_data
InnoDB
在庫
inventory_private
inventory_time
ログ
管理
MySQL

NAS
パフォーマンス
performance_schema
performance_viewsの略
SANscreen
スクラブ
サービス保証
テスト
tmp
ワークベンチ

手動で開始したバックアップでは、が使用されます `.zip` 次のファイルを含むファイルが作成されます。

- 日次バックアップ `.zip` ファイル（Cognosのレポート定義を含む）
- Aはバックアップを報告します `.zip` ファイル。[My Folders]ディレクトリにあるレポートも含め、Cognosのすべてのレポートが含まれます
- Data Warehouseデータベースのバックアップファイル Cognosでは、手動バックアップ（いつでも実行可能）に加えて、日次バックアップ（毎日という名前のファイルに自動的に生成されます `DailyBackup.zip`）をクリックします。日次バックアップには、製品に同梱されている上位フォルダとパッケージが含まれます。[My Folders]ディレクトリおよび製品の上位フォルダ以外に作成したディレクトリは、Cognosのバックアップには含まれません。

> Insightでのファイルの命名方法が原因です `.zip` ファイル。一部の解凍プログラムでは、ファイルを開くと空であることが表示されます。限り `.zip` ファイルのサイズが0より大きく、末尾がではありません `.bad` 拡張子、 `.zip` ファイルは有効です。7-ZipやWinZip®などの別の解凍プログラムでファイルを開くことができます。

カスタムレポートおよびレポートアーティファクトのバックアップ

7.0より前のバージョンのInsightで作成したカスタムレポートを最新バージョンにアップグレードする場合は、アップグレードインストールの前にレポートとレポートアーティファクトをバックアップし、アップグレードインストール後にリストアする必要があります。また、レポートアーティファクトの保存に使用するフォルダにも注意する必要があります。

このタスクについて

事前定義済みのレポートに変更を加えた場合は、それらのレポートのコピーを別のフォルダに作成します。これにより、事前設計されたアーティファクトを更新しても、変更内容が上書きされることはありません。

[My Folders]領域にレポートがある場合は、レポートが失われないように[Custom Reports]フォルダにコピーする必要があります。

Data Warehouseデータベースをリストアしています

Data Warehouseデータベースはを使用してリストアできます `.zip` Data Warehouseデータベースのバックアップ時に作成されたファイル。

このタスクについて

Data Warehouseデータベースをリストアする場合は、ユーザアカウント情報もバックアップからリストアできます。ユーザ管理テーブルは、Data Warehouseのみのインストールでの Data Warehouseレポートエンジンで使用されます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*[バックアップ/リストア]*をクリックします。
3. セクションで、[参照]*をクリックし、を探します `.zip` Data Warehouseのバックアップを含むファイル。
4. レポートまたはユーザアカウントデータをリストアする場合は、次のチェックボックスのいずれかまたは両方を選択します。
   - データベースのリストア

     Data Warehouseの設定、データマート、接続、およびユーザアカウント情報が含まれます。
   - リストア・レポート

     カスタムレポート、事前設計済みレポート、事前設計済みレポートに対する変更、Reporting Portalで作成したレポート設定が含まれます。

     > 名前にスラッシュ（/）または開いたブラケット（[）を含むカスタムレポートがデータベースバックアップに含まれている場合（たとえば、US IT Center Switch Port Boston/July）、リストア処理によってレポートの名前が変更され、スラッシュまたは開いたブラケットがアンダースコアに置き換えられます（例： US IT Center Switch Port Boston_July）。
5. [* リストア] をクリックします。

   リストアプロセスが完了すると、[Restore]ボタンの下にメッセージが表示されます。リストアプロセスが正常に完了すると、成功したことを示すメッセージが表示されます。リストアプロセスが失敗した場合は、エラーの原因となった特定の例外がメッセージに表示されます。例外が発生してリストアプロセスが失敗すると、元のデータベースは自動的にリセットされます。

レポートにマルチテナンシーを設定しています

OnCommand Insight Data Warehouseでは、ユーザを1つ以上のビジネスエンティティに関連付けることで、Reportingでマルチテナンシー（「マルチテナンシー」または「マルチテナンシー」と略されることがあります）に対応します。この機能を使用すると、管理者は、ユーザー属性またはユーザーの所属に応じてデータまたはレポートを分離できます。

ビジネスエンティティでは、容量チャージバックの目的で次の値を使用して階層を使用します。

- テナント：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）：企業内の基幹業務（「ハードウェア」や「ソフトウェア」など）。
- Business Unit：「Sales」や「Marketing」などの従来のビジネスユニット。
- Project：容量チャージバックを割り当てるプロジェクト。

マルチテナンシーを設定するプロセスの主な手順は次のとおりです。

- Data Warehouseユーザアカウントを設定
- Reporting Portalでグループを作成します。
- ユーザを1つ以上のグループ（ビジネスエンティティ）に割り当てます。
- ユーザを1つ以上のビジネスエンティティに割り当てます。たとえば、「NetApp」に関連付けられているユーザは、テナントとして「NetApp」を持つすべてのビジネスエンティティにアクセスできます。
- ユーザが表示する必要のあるレポートのみを表示できることをテストします。

次の点は、ユーザがレポートデータにアクセスする方法をまとめたものです。

- どのグループにも割り当てられていないユーザは、すべてのデータにアクセスできます。
- どのグループにも割り当てられているユーザは、ビジネスエンティティがないとレコードにアクセスできません。

たとえば、次の部門があり、これらの部門内のユーザに対してレポートを分離する必要があるとします。

ユーザ	エンジニアリング	サポート	財務	法律
ユーザ 1	X	X		
ユーザ 2			X	X
ユーザー3		X		

ユーザアカウントの設定

ユーザアカウントを設定するには、いくつかの手順を実行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/dwh`、ここで `hostname` 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、*[ユーザ管理]*をクリックします。
3. 各ユーザアカウントを設定します。

ビジネスエンティティへのユーザの割り当て

ビジネスエンティティにユーザを割り当てるには、一連の手順を実行する必要があります。Data Warehouseでは、ユーザを1つ以上のビジネスエンティティに関連付けることで、Reportingでマルチテナンシー（「マルチテナンシー」または「マルチテナンシー」）に対応できます。これにより、管理者は、ユーザの属性または所属に応じてデータまたはレポートを分離できます。

手順

1. Data Warehouseポータルに管理者としてログインします `https://hostname/dwh`、ここで `hostname` 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. Data Warehouseツールバーで、をクリックします をクリックしてReporting Portalを開きます。
3. ユーザー名とパスワードを入力し、* Login *をクリックします。
4. [Launch]メニューから、*[IBM Cognos Administration]*を選択します。
5. [セキュリティ]タブをクリックします。
6. ディレクトリで、* cognos *を選択します。
7. Cognosフォルダに、ビジネスエンティティ用の新しいサブフォルダ「BEs」を作成します。
8. BEsフォルダを開きます。
9. [新しいグループ]*アイコンをクリックして、さまざまな権限レベルに対応するグループを追加します。

   権限レベルには、ビジネスエンティティのフルネーム（netapp.N/Aなど）またはプレフィックス（netapp.N/A.Financeなど）を指定できます。どちらの形式でも、ビジネスエンティティ（NetApp.N/A.Finance）内のすべてのプロジェクトにアクセスできます。

   [New Group]ウィザードが表示されます。
10. ウィザードの各ページに情報を入力します。
11. ビジネスエンティティを選択し、*[詳細]*をクリックします。
12. [メンバーの設定]*をクリックします。
13. [追加（ Add ）] をクリックします。
14. SANscreen ディレクトリを選択します。
15. ユーザのリストから、ビジネスエンティティに含める各ユーザを選択し、[Selected Entries]ボックスに追加します。
16. [OK] をクリックします。
17. 同じ手順を繰り返して、各ビジネスエンティティグループにメンバーを追加します。

セットアップの問題のトラブルシューティング

アノテーション、ビルド、レポートには、セットアップ時に発生する可能性のある一般的な問題がいくつかあります。これらの問題をトラブルシューティングするには、概説されている手順に従います。

アノテーションが表示されない理由

Data Warehouseでアノテーションが表示されない場合は、アノテーションを強制的に更新してからData Warehouseのビルドを開始する必要があります。

アノテーションが欠落していると、Data Warehouseへのデータのインポート方法とレポートへのデータの表示方法に影響します。たとえば、アノテーション「階層」を使用できない場合、Data Warehouseのレポートでストレージシステムを階層別にグループ化することはできません。

Data Warehouseのアノテーションを強制的に更新します

OnCommand Insight からData Warehouseへのアノテーションの更新を開始できます。

このタスクについて

アノテーションは、次の2つのオプションのいずれかを使用して更新できます。

- 削除されたオブジェクトを含める：削除されたホスト、ストレージアレイ、スイッチなど、すでに存在しなくなったデバイスに関するデータが含まれます。これは、履歴データポイントを使用してData Warehouseデータをビルドする場合に必要です。
- 削除されたオブジェクトを含めない：削除されたオブジェクトを除外する場合は、このオプションを選択します。

手順

1. OnCommand Insight ポータルに管理者としてログインします `https://hostname`、ここで `hostname` は、OnCommand Insight がインストールされているシステムの名前です。
2. **>**[トラブルシューティング]をクリックします。ページの下部にある[高度なトラブルシューティング]*をクリックします。
3. タブで、[DWHアノテーションの更新（削除を含む）]*をクリックします。

Data Warehouseの手動ビルドを生成します

OnCommand Insight でアノテーションを強制的に更新（一時データを実行）したら、Data Warehouseのビルドを開始する必要があります。スケジュールされた次回のビルドまで待つか、今すぐビルドを開始できます。

手順

1. Data Warehouseポータルに管理者としてログインします `https://hostname/dwh`、ここで `hostname` 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、*[スケジュール]*をクリックします。

3. [今すぐビルド]*をクリックします。

Data Warehouseへのユーザ定義アノテーションのインポート

OnCommand Insight で強制的にアノテーションを更新したら、Data Warehouseで必要なアノテーションを選択し、Data Warehouseのビルドを開始する必要があります。スケジュールされた次回のビルドまで待つか、今すぐビルドを開始できます。

手順

1. Data Warehouseポータルに管理者としてログインします `https://hostname/dwh`、ここで `hostname` 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、*注釈*をクリックします。

Annotations

Annotation	Column Name	Target Object	Published
Compute_Resource_Group	Compute_Resource_Group	Virtual Machine	
Data_Center	dataCenter	Host	✔
Data_Center	dataCenter	Storage	✔
Data_Center	dataCenter	Switch	✔
Note	Note	Switch	
Switch_Level	switchLevel	Switch	✔
Tier	Tier	Internal Volume	
Tier	Tier	Qtree	
Tier	Tier	Storage	
Tier	Tier	Storage Pool	
Tier	Tier	Volume	

Edit

リストには、アノテーションタイプごとに行が表示され、アノテーションを割り当てることができるターゲットオブジェクトが1つずつ表示されます。[Published]列のチェックマークは、アノテーションが特定のターゲットオブジェクトに対してすでに選択されており、Data Warehouseデータマートですでに使用できることを示しています。

3. OnCommand Insight からアノテーションをインポートする方法を編集するには、*編集*をクリックします。

Edit Annotations

Annotation	Column Name	Target Object	Published All / None	Init With Current All / None
Compute_Resource_Group	Compute_Resource_Group	Virtual Machine	☐	☐
Data_Center	dataCenter	Host	☑	☐
Data_Center	dataCenter	Storage	☑	☐
Data_Center	dataCenter	Switch	☑	☐
Note	Note	Switch	☐	☐
Switch_Level	switchLevel	Switch	☑	☐
Tier	Tier	Internal Volume	☐	☐
Tier	Tier	Qtree	☐	☐
Tier	Tier	Storage	☐	☐
Tier	Tier	Storage Pool	☐	☐
Tier	Tier	Volume	☐	☐

Save Cancel

4. アノテーションプロセスを編集するには、次の手順を実行します。
   - OnCommand Insight から取得したアノテーションをData Warehouseデータベースに追加するには、* Published *を選択します。すべてのオブジェクトのすべての注釈を選択するには、*すべて*をクリックします。[なし]*をクリックして、すべてのオプションが選択されていないことを確認します。

     特定のオブジェクトのインベントリテーブルおよび関連するデータマートからアノテーション列を削除する場合は、このオプションをオフにします。カスタム設計のレポートでアノテーションデータが使用されている場合、そのレポートは正常に実行されません。

   - Data Warehouseディメンションテーブルの履歴データを現在のアノテーション値で初期化する場合は、* Init with Current をオンにします。すべてのオブジェクトのすべての注釈を選択するには、*すべて*をクリックします。**[**なし**]***をクリックして、すべてのオプションが選択されていないことを確認します。このチェックボックスは、注釈がパブリッシュされると無効になります。このチェックボックスは、パブリッシュされていない注釈に対して有効になります。たとえば、アノテーションタイプ「`floor`」でアノテートされ、値「`1`」を取得したホストが**host_dimension**テーブルに**3**行ある場合、 Init with current を選択すると、**host_dimension**テーブルの**3**行すべてに対して「`floor`」列の値「`1`」が関連付けられます。「*現在の値で初期化」が選択されていない場合、そのホストの最新の行だけが「floor」列に「1」と表示されます。

5. [保存（ Save ）] をクリックします。

   アノテーションを削除すると、原因 によってデータ構造が変更されたりデータが失われたりすることを示す警告メッセージが表示されます。

6. 続行するには、*[はい]*をクリックします。

   Data Warehouseで非同期アノテーションジョブが開始され、要求された変更が適用されます。ジョブは[Jobs]ページで確認できます。Data Warehouseデータベーススキーマの変更内容を確認することもできます。

失敗した履歴ビルドポイントの処理

[Skip history build failures]オプションを有効にすると、失敗したビルドをすべて省略して履歴からビルドできます。

これを行うと、履歴からのビルドが続行されます。このオプションを有効にすると、ビルドが失敗した場合、Data Warehouseではビルドが続行され、失敗したビルドは無視されます。この場合、スキップされたビルドのデータポイントは履歴データにありません。このオプションを有効にしない場合にビルドが失敗すると、以降のジョブはすべて中止されます。

Data Warehouseを使用して実行できる管理タスク

OnCommand Insight Data WarehouseはWebベースのユーザインターフェイスです。OnCommand Insight Data Warehouseでデータを設定およびトラブルシューティングしたり、OnCommand Insight からデータを取得するスケジュールを設定したりできます。

Data Warehouseポータルでは、次の管理タスクを実行できます。

- 現在のジョブまたは実行中のクエリのステータスを確認します
- アノテーションを管理します
- E メール通知を設定
- カスタムレポートにアクセスして作成します
- Data Warehouseのドキュメントとデータベーススキーマを確認します
- サイト名を編集します
- Data Warehouseのバージョンとアップグレード履歴を確認します
- Data Warehouseデータを履歴からビルドします
- Data Warehouseデータベースをリセットします
- Data Warehouseデータベースをバックアップおよびリストアします
- Data Warehouseの問題のトラブルシューティングとOnCommand Insight のログの確認
- ユーザアカウントを管理する

ジョブの管理

現在のジョブとそのステータスのリストを表示できます。ビルドサイクルの最初のジョブは太字で表示されます。Data Warehouseがコネクタごと、およびデータマートごとに実行するビルドは、ジョブとみなされます。

このタスクについて

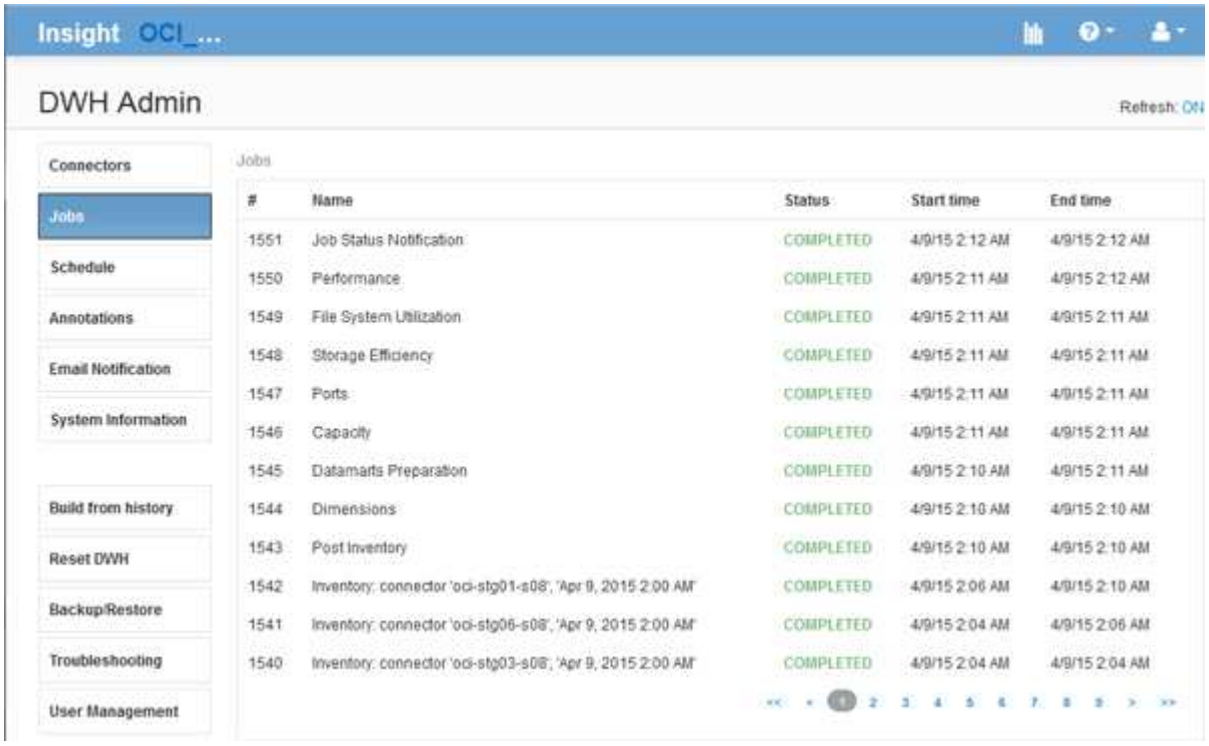
スケジュールまたは開始した保留中のジョブはキャンセルできます。以前に実行したジョブの履歴をクリアすることもできます。保留中、実行中、または中止処理中でないジョブの履歴をクリアできます。過去24時間を除くすべての履歴またはすべての履歴をクリアして、最終日のエントリを除くすべてのエントリを削除できます。

次のタイプのジョブに関する情報を表示できます。ライセンス、事前在庫品、在庫品、在庫品後、ディメンション、 データマートの準備、容量、ポート、Storage Efficiency、ファイルシステムの利用率、 パフォーマンス、ジョブステータス通知、履歴ビルド、動的アノテーション、コネクタの削除、 ビルド、Phone Home、およびメンテナンスがスキップされました。

メンテナンスジョブは毎週実行され、MySQLツールを使用してデータベースを最適化します。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*[ジョブ]*をクリックします。



[保留中]ステータスが表示された場合は、[キャンセル]リンクが表示されます。

3. 保留中のジョブをキャンセルするには、*キャンセル*をクリックします。
4. ジョブ履歴を削除するには、**[**すべて**]***または[過去24時間以外のすべて]*をクリックします。

Data Warehouseの健常性を監視しています

Data Warehouse（DWH）には、DWHの状態に関する情報を表示するヘルスモニタが含まれています。DWHの*ページと[ジョブ]ページにアラームメッセージが表示されるほか、接続されている**Insight**サーバに送信され、[管理]**>**[ヘルス]*ページに表示されます。

DWHでは10分ごとに指標が収集され、次の状況でアラームが表示されます。

- Insightサーバへの接続が停止しています
- ディスク利用率が90%を超えています

- レポート（Cognos）サービスが停止しています
- クエリは、いずれかのテーブルに対して長時間ロックを保持しています
- メンテナンスジョブが無効になっている
- 自動バックアップは無効になっています
- セキュリティリスク：デフォルトの暗号化キーが検出されました

Data Warehouseでのヘルスモニタの警告は、最大30日間停止できます。

Eメール通知を有効にすると、これらのイベントもEメールで報告されます。電子メールには添付ファイルが含まれていないことに注意してください。

これらのイベントはに記録されます `dwh_troubleshoot.log` 次の場所にあるファイル：

- Windows の場合 `<install dir>\SANscreen\Wildfly\Standalone\Logs`
- Linux ： `/var/log/netapp/oci/wildfly/`

日次ビルドのスケジュール設定

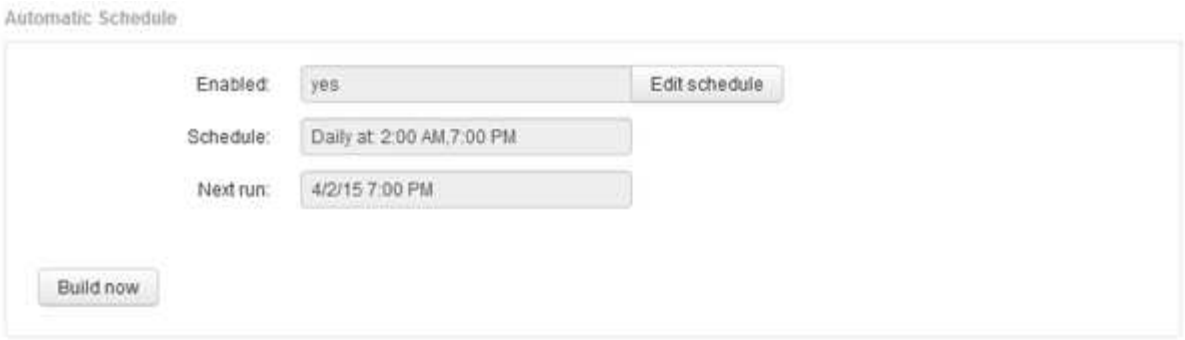
Data Warehouseは、[Build now]コントロールを使用していつでも手動でビルドできますが、ベストプラクティスとして、自動ビルドをスケジュールして、Data Warehouseデータベースをビルドするタイミングと頻度を定義することを推奨します。Data Warehouseでは、コネクタごとおよびデータマートごとにビルドジョブが実行されます。Data Warehouseでは、ライセンスとインベントリ用にコネクタごとにビルドジョブが実行され、それ以外のすべてのビルドジョブ（容量など）が統合データベースで実行されます。

このタスクについて

Data Warehouseは、ビルドされるたびに、すべてのコネクタに対してインベントリジョブを実行します。インベントリジョブが完了すると、Data Warehouseでディメンション、容量、および残りのデータマートのジョブが実行されます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*[スケジュールの編集]*をクリックします。



3. ダイアログボックスで、[編集]*をクリックして新しいスケジュールを追加します。

4. 頻度-毎週を選択してください。
5. ジョブを実行する各曜日の時刻を選択します。
6. ビルドを実行しない日数には「N/A」を選択します。
7. スケジュールを有効にするには、*[有効]*を選択します。

> このチェックボックスをオンにしないと、スケジュールによるビルドは実行されません。

8. [保存（ Save ）] をクリックします。
9. スケジュールされた自動ビルド以外でData Warehouseをビルドするには、*[今すぐビルド]*をクリックします。

週次スケジュールの設定

Data Warehouseは、[Build now]コントロールを使用していつでも手動でビルドできますが、ベストプラクティスとして、自動ビルドをスケジュールして、Data Warehouseデータベースをビルドするタイミングと頻度を定義することを推奨します。Data Warehouseでは、コネクタごとおよびデータマートごとにビルドジョブが実行されます。Data Warehouseでは、ライセンスとインベントリ用にコネクタごとにビルドジョブが実行され、それ以外のすべてのビルドジョブ（容量など）が統合データベースで実行されます。週次スケジュールでは、曜日ごとにビルドを実行する時刻を指定できます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*[スケジュールの編集]*をクリックします。
3. 頻度-毎週を選択してください。
4. ジョブを実行する各曜日の時刻を選択します。
5. ビルドを実行しない日数には「N/A」を選択します。
6. スケジュールを有効にするには、*[有効]*を選択します。

   このチェックボックスをオンにしないと、スケジュールによるビルドは実行されません。

7. [保存（ Save ）] をクリックします。
8. スケジュールされた自動ビルド以外でData Warehouseをビルドするには、*[今すぐビルド]*をクリックします。

日次バックアップのスケジュール設定

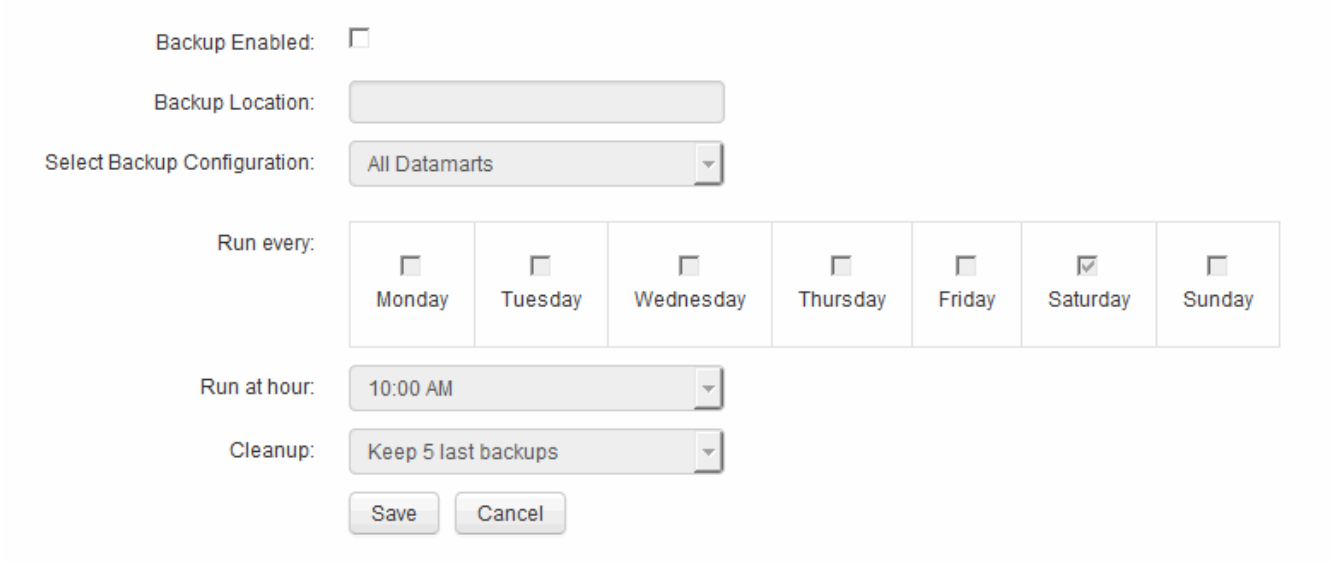
Data Warehouseは[Backup/Restore]制御を使用していつでも手動でバックアップできますが、ベストプラクティスとして、自動バックアップをスケジュールして、Data Warehouseデータベースおよび Cognosコンテンツストアをバックアップするタイミングと頻度を定義することを推奨します。バックアップを使用すると、データ損失から保護され、必要に応じてData Warehouseデータベースをリストアできます。また、新しいData Warehouseサーバに移行する場合や、新しいバージョンのData Warehouseにアップグレードする場合にも、バックアップを使用します。

このタスクについて

Data Warehouseサーバがビジー状態でない時間帯にバックアップをスケジュールすると、バックアップのパフォーマンスが向上し、ユーザへの影響が軽減されます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*[スケジュール]*をクリックします。
3. ダイアログボックスで、[編集]*をクリックして新しいスケジュールを追加します。



4. スケジュールされたバックアップを有効にするには、*[バックアップ有効]*を選択します。
5. バックアップファイルを保存する場所を指定します。
6. バックアップするデータを指定します。
7. バックアップを実行する曜日（複数可）を指定します。
8. バックアップを開始する時刻を指定します。
9. 保持する過去のバックアップコピーの数を指定します。
10. [保存（ Save ）] をクリックします。

Data Warehouseでのカスタムスクリプトの実行

Data Warehouseでは、カスタマイズしたデータをData Warehouseで準備するカスタムスクリプトを実行するジョブを作成できます。

作業を開始する前に

カスタムスクリプトがData Warehouseのアップグレード時に削除されないようにするには、カスタムスクリプトをSANscreen ディレクトリに保存しないでください。

このタスクについて

ジョブで指定できるスクリプトは1つだけです。1つのスクリプトから複数のスクリプトとコマンドを実行できます。

手順

1. Data Warehouseで、**[DWH Admin]**>*[Schedule]*を選択します。
2. [Script enabled]*チェックボックスを選択します。
3. [* Script Location*（スクリプトの場所）]テキストボックスにスクリプト名の絶対パスを入力します。
4. [保存（ Save ）] をクリックします。

結果

Data Warehouseジョブエンジンは、「カスタムスクリプト」ジョブを実行するタスクをスケジュールします。このジョブは、他のバックグラウンドプロセスとの競合を避けるために、ETLのあとに実行されるようにスケジュールされます。ジョブは「履歴からビルド」操作では実行されません。

アノテーションを使用して実行できる操作

アノテーションを使用すると、環境内のオブジェクトに関連する情報を定義し、そのアノテーションに基づいてオブジェクトを追跡できます。たとえば、環境内のデバイスに建物番号やフロア番号のアノテーションを追加し、データセンターの1階にあるすべてのデバイスを返すクエリを作成できます。

また、特定のデータセンターまたはビジネスエンティティ内のすべてのデバイスを確認し、ティア1ストレージを最も多く使用しているビジネスエンティティを特定することもできます。そのためには、OnCommand Insight Web UIを使用して、データセンター、ビジネスエンティティ、または階層のアノテーションをデバイスに割り当てます。その後、選択したユーザ定義のアノテーションをOnCommand Insight からData Warehouseに取り込むことができます。これは、オブジェクトに割り当てられているアノテーション値をカスタムレポートに表示する場合に使用します。

Data Warehouseに伝播するユーザ定義のアノテーションを指定できます。アノテーションは、インベントリのオブジェクトテーブルおよびデータマートの関連するディメンションテーブルに列として追加されます。OnCommand Insight ユーザインターフェイスを使用してリソースのアノテーションを更新し、Data Warehouseのビルドを開始するか次回のビルドまで待機すると、次の表に結果が表示されます。

- dwh_inventory.annotation_value
- dwh_inventory.object_to_annotation

OnCommand Insight で入力したアノテーションがData Warehouseに含まれていることを確認するには、次の主要なプロセスを実行する必要があります。

- Data Warehouseにアノテーションをインポートする前に、アノテーションがOnCommand Insight で準備されていることを確認する必要があります。

  そのためには、トラブルシューティング>* Data Warehouseのアノテーションの強制更新*オプションを手動で実行するか、スケジュールされた次の一時データ実行プロセスが実行されるまで待つことができます。アノテーションを強制的に更新する場合は、OnCommand Insight サーバで一時データ（アノテーション値など）が計算されてデータベーステーブルに格納され、Data WarehouseのETLプロセスがデータを読み取れるようになります。アノテーションデータは15分ごとに自動的に更新されますが、強制的に更新する頻度を増やすこともできます。

- 次に、Data Warehouse **Annotations**オプションを使用してData Warehouseにアノテーションをインポートします。
- OnCommand Insight Reportingポータルのレポートオーサリングツールを使用して作成するレポートにアノテーションを含める場合は、OnCommand Insight Reportingのメタデータモデルを更新する必要があります。

Data Warehouseをアップグレードすると、データベースのリストアプロセス中にアノテーションジョブが自動的に実行されます。アノテーションジョブは、WildFlyの起動時にも自動的に実行されます。

WildFlyは、OnCommand Insight Javaコードを実行するアプリケーションサーバであり、OnCommand Insight サーバとデータウェアハウスの両方に必要です。

OnCommand Insight でアノテーションを準備しています

アノテーションをData Warehouseにインポートする前に、OnCommand Insight でアノテーションを準備しておく必要があります。

手順

1. OnCommand Insight ポータルに管理者としてログインします `https://hostname`、ここで `hostname` は、OnCommand Insight がインストールされているシステムの名前です。
2. **>**[トラブルシューティング]をクリックします。ページの下部にある[高度なトラブルシューティング]*をクリックします。
3. タブで、[DWHアノテーションの更新（削除を含む）]*をクリックします。

Data Warehouseへのユーザ定義アノテーションのインポート

OnCommand Insight で強制的にアノテーションを更新したら、Data Warehouseで必要なアノテーションを選択し、Data Warehouseのビルドを開始する必要があります。スケジュールされた次回のビルドまで待つか、今すぐビルドを開始できます。

手順

1. Data Warehouseポータルに管理者としてログインします `https://hostname/dwh`、ここで `hostname` 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、*注釈*をクリックします。

Annotations

Annotation	Column Name	Target Object	Published
Compute_Resource_Group	Compute_Resource_Group	Virtual Machine	
Data_Center	dataCenter	Host	✔
Data_Center	dataCenter	Storage	✔
Data_Center	dataCenter	Switch	✔
Note	Note	Switch	
Switch_Level	switchLevel	Switch	✔
Tier	Tier	Internal Volume	
Tier	Tier	Qtree	
Tier	Tier	Storage	
Tier	Tier	Storage Pool	
Tier	Tier	Volume	

Edit

リストには、アノテーションタイプごとに行が表示され、アノテーションを割り当てることができるターゲットオブジェクトが1つずつ表示されます。[Published]列のチェックマークは、アノテーションが特定のターゲットオブジェクトに対してすでに選択されており、Data Warehouseデータマートですでに使用できることを示しています。

3. OnCommand Insight からアノテーションをインポートする方法を編集するには、*編集*をクリックします。

Edit Annotations

Annotation	Column Name	Target Object	Published All / None	Init With Current All / None
Compute_Resource_Group	Compute_Resource_Group	Virtual Machine	☐	☐
Data_Center	dataCenter	Host	☑	☐
Data_Center	dataCenter	Storage	☑	☐
Data_Center	dataCenter	Switch	☑	☐
Note	Note	Switch	☐	☐
Switch_Level	switchLevel	Switch	☑	☐
Tier	Tier	Internal Volume	☐	☐
Tier	Tier	Qtree	☐	☐
Tier	Tier	Storage	☐	☐
Tier	Tier	Storage Pool	☐	☐
Tier	Tier	Volume	☐	☐

Save Cancel

4. アノテーションプロセスを編集するには、次の手順を実行します。
   - OnCommand Insight から取得したアノテーションをData Warehouseデータベースに追加するには、* Published *を選択します。すべてのオブジェクトのすべての注釈を選択するには、*すべて*をクリックします。[なし]*をクリックして、すべてのオプションが選択されていないことを確認します。

     特定のオブジェクトのインベントリテーブルおよび関連するデータマートからアノテーション列を削除する場合は、このオプションをオフにします。カスタム設計のレポートでアノテーションデータが使用されている場合、そのレポートは正常に実行されません。

   - Data Warehouseディメンションテーブルの履歴データを現在のアノテーション値で初期化する場合は、* Init with Current をオンにします。すべてのオブジェクトのすべての注釈を選択するには、*すべて*をクリックします。**[なし]***をクリックして、すべてのオプションが選択されていないことを確認します。このチェックボックスは、注釈がパブリッシュされると無効になります。このチェックボックスは、パブリッシュされていない注釈に対して有効になります。たとえば、アノテーションタイプ「`floor`」でアノテートされ、値「`1`」を取得したホストが**host_dimension**テーブルに**3**行ある場合、 Init with current を選択すると、**host_dimension**テーブルの**3**行すべてに対して「`floor`」列の値「`1`」が関連付けられます。「*現在の値で初期化」が選択されていない場合、そのホストの最新の行だけが「floor」列に「1」と表示されます。

5. [保存（ Save ）] をクリックします。

   アノテーションを削除すると、原因 によってデータ構造が変更されたりデータが失われたりすることを示す警告メッセージが表示されます。

6. 続行するには、*[はい]*をクリックします。

   Data Warehouseで非同期アノテーションジョブが開始され、要求された変更が適用されます。ジョブは[Jobs]ページで確認できます。Data Warehouseデータベーススキーマの変更内容を確認することもできます。

[Jobs]リストでのアノテーションジョブの表示

[Jobs]リストにアノテーションジョブを表示し、アノテーションの変更をData Warehouseデータマートに適用できます。

手順

1. Data Warehouseポータルに管理者としてログインします `https://hostname/dwh`、ここで `hostname` 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、*[ジョブ]*をクリックします。

データベーススキーマでのアノテーションの変更の表示

データベーススキーマには、特定のテーブルの変更が反映されます。

このタスクについて

たとえば、ストレージアレイにアノテーションを追加すると、Inventoryデータマートなどのデータマートのstorageテーブルまたはswitchテーブルにアノテーションが表示されます。

OnCommand Insight のユーザインターフェイスを使用してリソースのアノテーションを更新し、Data Warehouseのビルドを開始（または次回のビルドまで待機）すると、インベントリ内の対応するオブジェクト（dwh_inventory）および対応するディメンションテーブルでも新しい列が追加または削除されます （該当するデータマート内）。結果は次の表に表示されます。

- dwh_inventory.annotation_value
- dwh_inventory.object_to_annotation

手順

1. をクリックします Data Warehouseツールバーで* Documentation *を選択します。
2. [データベーススキーマ]*を選択します。
3. 左側の*ペインで、 dwh_inventory セクションまでスクロールし、 switch *をクリックします。

Database Schema

Databases

storage_port
storage_to_applica
switch
switch_port
switch_port_to_app
switch_to_applicati
tape
tape_controller
tape_port
tier
violation
virtual_switch
virtual_to_backend
vm_to_application
volume
volume_in_storage

dwh_inventory.switch

Column	Type	Nullable	Description
id	int(11)	false	GUID of the switch.
fabricId	int(11)	true	GUID of the fabric on which this switch is configured to operate. References: • **id** in dwh_inventory.fabric
identifier	varchar (255)	false	Identifier of the device.
wwn	varchar (255)	false	WWN of the switch.
ip	varchar (255)	false	IP address of the switch.
Name	varchar (255)	false	Name of the switch.
Manufacturer	varchar (255)	true	Manufacturer of the switch
Model	varchar (255)	true	Manufacturer's model of the switch.
Firmware	varchar (255)	true	Firmware version running on the switch.

4. dwh_inventory.switch *テーブルに変更が反映されます。

Database Schema

Databases

host_group_dimen
internal_volume_c
internal_volume_di
qtree_capacity_fac
qtree_dimension
service_level_dim
storage_dimension
storage_pool_dime
tier_dimension
vm_capacity_fact
vm_dimension
volume_fact_curre

dwh_capacity.storage_dimension

Column	Type	Nullable	Description
tk	int(11)	false	TK of this storage array row.
name	varchar (255)	false	Name of the storage array.
identifier	varchar (255)	false	Identifier of the device.
ip	varchar (255)	false	IP address of the storage array.
model	varchar (255)	true	Manufacturer's model of the storage array.
manufacturer	varchar (255)	true	Manufacturer of the storage array.
serialNumber	varchar (255)	true	Serial number for the storage array.
microcodeVersion	varchar (255)	true	Version of the firmware running on the storage array.
family	varchar (255)	true	Family name of the storage array (e.g. Clariion, Symmetrix etc).
id	int(11)	true	GUID of the storage array in **dwh_inventory.storage**.

storage_dimensionsテーブルにdatacenterアノテーション列が表示されます。

Eメール通知の設定

Data Warehouseのジョブが正常に完了しなかった場合に、Data Warehouseから特定のEメールアドレスにEメールを送信するように設定できます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*[Email Notification]*をクリックします。
3. 次のように入力します。
   - SMTPサーバアドレス

     組織内でSMTPサーバとして機能しているサーバを指定します。ホスト名またはIPアドレスをnn.nnn.nnn.nnn形式で指定します。ホスト名を指定する場合は、そのホスト名をDNSで解決できることを確認してください。

   - SMTPサーバのユーザ名とパスワード

     Eメールサーバにアクセスするためのユーザ名を指定します。SMTPサーバでユーザがサーバにログインする必要がある場合にのみ必要です。これは、アプリケーションへのログインとEメールへのアクセスに使用するユーザ名と同じです。

   - 通知が有効です

     *はい*通知を有効にします。*いいえ*通知を無効にします。

   - 送信者のEメール

     通知の送信に使用するEメールアドレスを指定します。組織内の有効なEメールアドレスを指定する必要があります。

   - 受信者のEメール

     常にEメールを受信するユーザー（複数可）のEメールアドレスを指定します。複数のアドレスを指定する場合はカンマで区切ります。

   - E メールの件名

     通知の件名を指定します。

   - Eメールの署名

     Eメールの一番下に表示される情報（部署名など）を指定します。

Reportingポータルへのアクセス

Data WarehouseポータルからReportingポータルにアクセスし、Workspace AdvancedやReport Studioなどのレポートオーサリングツールを使用してカスタムレポートを作成できます。

手順

1. Data Warehouseツールバーで、をクリックします をクリックしてInsight Reportingポータルを開きます。
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。

Data Warehouseデータベーススキーマのドキュメントの表示

Data Warehouseデータベーススキーマの情報を確認できます。

手順

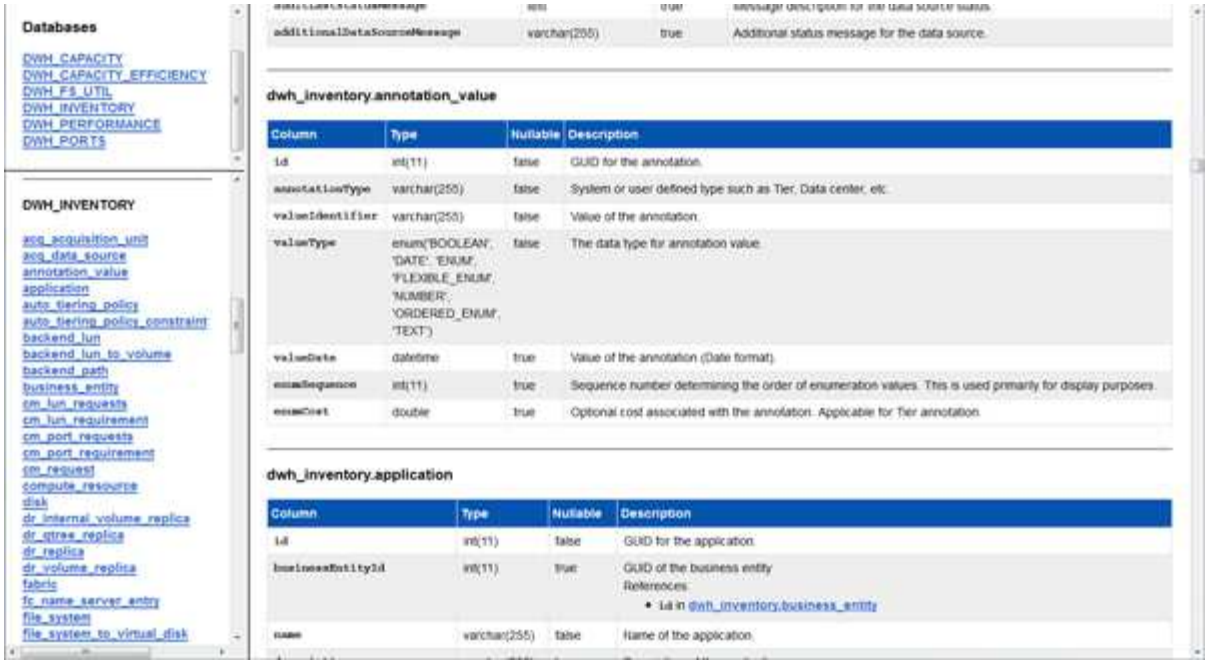
1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` は、OnCommand Insight Data Warehouseがインストールされているシステムの名前です。
2. Data Warehouseツールバーで、をクリックします をクリックし、*[スキーマ]*を選択します。

Data Warehouseデータベーススキーマの表示

データベーススキーマを表示して、別のAPIでデータを使用する方法を理解したり、SQLクエリを開発したりすることができます。schemaオプションを使用すると、スキーマ内のすべてのデータベース、テーブル、および列が一覧表示されます。テーブルの関係を示すデータベーススキーマ図を確認することもできます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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. をクリックします をクリックし、* Documentation *を選択します。
3. [データベーススキーマ]*を選択します。
4. たとえば、**[データベース]***ペインで dwh_inventory *をクリックします。
5. ペインで、 dwh_inventory セクションまで下にスクロールし、 annotation_value *テーブルをクリックします。



dwh_inventory.annotationテーブルが表示されます。

システム情報の表示

システム、モジュール、ライセンス、およびData Warehouseのアップグレード情報を表示できます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*[システム情報]*をクリックします。
3. [システム]タブで、システム情報を確認し、必要に応じて次の手順を実行してサイト名を編集します。
   a. [サイト名の編集]*をクリックします
   b. 新しいサイト名を入力し、*[保存]*をクリックします。
4. アプリケーション情報（アプリケーション名、モジュール、バージョン、およびインストール日）を表示するには、*[アプリケーション情報]*タブをクリックします。
5. ライセンス情報（プロトコル、コード、有効期限、数量）を表示するには、*[ライセンス]*タブをクリックします。
6. アプリケーションのアップグレード情報（アプリケーション名、開始日、終了日、時刻、ユーザー、 をクリックしてください）、*アップグレード履歴*をクリックします。

詳細オプション

Data Warehouseには、さまざまな高度なオプションがあります。

失敗したビルドをスキップします

最初のビルドの後、ビルドが失敗することがあります。失敗したビルドのあとにすべてのジョブが正常に完了するようにするには、*[Skip history build failures]*オプションを有効にします。

このタスクについて

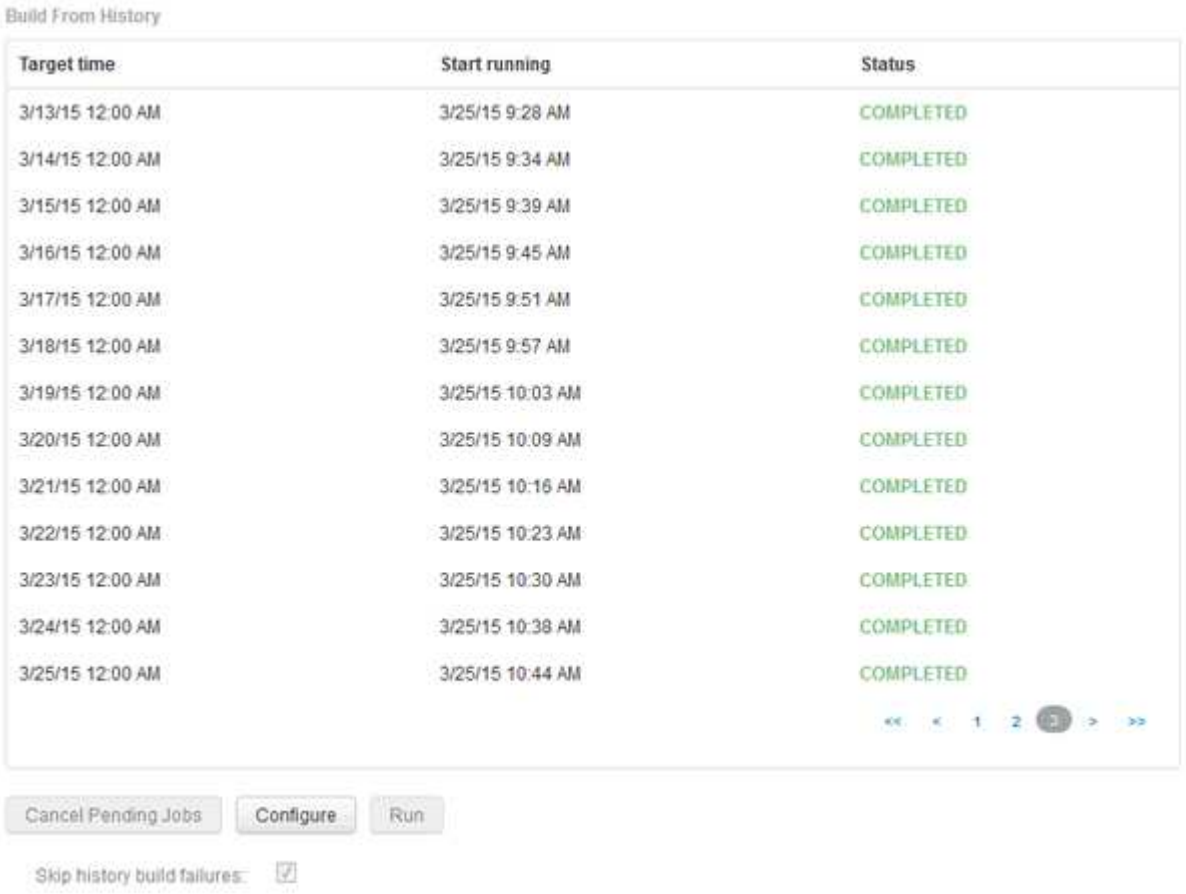
ビルドが失敗し、*[Skip history build failures]*オプションが有効になっている場合、Data Warehouseはビルドを続行し、失敗したビルドは無視します。この場合、スキップされたビルドのデータポイントは履歴データにありません。

このオプションは、ビルドが失敗した場合にのみ使用してください。

[Build from History]でビルドが失敗し、*[Skip history build failures]*チェックボックスが選択されていない場合、以降のジョブはすべて中止されます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*[履歴からビルド]*をクリックします。



3. [**Configure**] をクリックします。
4. ビルドを設定します。

5. [保存（ Save ）] をクリックします。
6. 失敗したビルドをスキップするには、*[ビルドの失敗の履歴をスキップする]*をオンにします。

   このチェックボックスは、* Run *ボタンが有効になっている場合にのみ表示されます。

7. スケジュールされた自動ビルド以外でビルドを実行するには、*[実行]*をクリックします。

Data Warehouseデータベースまたは**Reporting**サーバをリセットしています

Data Warehouseデータマートの内容を削除し、設定されているすべてのコネクタを削除できます。この処理は、インストールまたはアップグレードが正常に完了せず、Data Warehouseデータベースが中間の状態になった場合に実行します。Inventoryデータモデルまたは Cognos Reportingデータモデルのみを削除することもできます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*[DWHデータベースのリセット]*をクリックします。
3. 次のいずれかのオプションをクリックします。

   - * DWHデータベースのリセット*

     これにより、すべてのData Warehouseデータマートの内容と設定済みのコネクタがすべて削除され、カスタム設定を行わずにData Warehouseがインストールされたデフォルトの状態になります。このオプションは、接続しているサーバを変更したあとにサーバで別のData Warehouseデータベースを誤ってリストアし、インストール済みのデフォルトの状態に戻す必要がある場合などに選択します。レポートは削除されません。（レポートはCognos Content Storeに保存されます）。

   - 在庫のみリセット

     これにより、Inventoryデータモデルの内容のみが削除されます。履歴データは削除されません。

   - レポートコンテンツのリセット

     これにより、レポーティングサーバのコンテンツがリセットされます。これにより、既存のカスタムレポートがすべて削除されます。このオプションを選択する前に、レポートをバックアップしてください。

   警告メッセージが表示されます。

4. 続行するには、*[はい]*をクリックします。

6.3より前のバージョンのレポートのリストアとアップグレード

6.3より前のバージョンのInsightをアップグレードする場合は、レポートアーティファクトを手動でリストアする必要があります。

作業を開始する前に

トピック「Data Warehouse（DWH）のアップグレード」および「カスタムレポートおよびレポートアーティファクトのバックアップ」の手順に従います。

手順

1. バージョン6.3より前のリリースからレポートアーティファクトをリストアするには、に作成して保存したExport Backup.zipファイルをコピーします `<install>\cognos\c10_64\deployment` ディレクトリ。
2. ブラウザを開き、に移動します `http://<server>:<port>/reporting` インストール中に使用したサーバおよびポート用。
3. ユーザー名とパスワードを入力し、* Login *をクリックします。
4. メニューから[Insight Reporting Administration]*を選択します。
5. [* 構成 *] タブをクリックします。

   データモデルの変更により、古いパッケージのレポートは実行されず、アップグレードが必要になる場合があります。

6. [コンテンツ管理]*をクリックします。
7. [新規インポート]*ボタンをクリックします。
8. アーカイブが配置ディレクトリにコピーされていることを確認します（例： `backup6.0.zip`）を選択し、*[Next]*をクリックします。
9. アーカイブを保護するためのパスワードを入力した場合は、パスワードを入力して* OK *をクリックします。
10. 名前を変更します `Export...` 終了： `Import Backup` [次へ]*をクリックします。
11. 各パッケージ名の横にある鉛筆のアイコンをクリックし、必要に応じて新しいターゲット名を入力します。たとえば、を追加します `_original` 既存の名前のサフィックス。次に、 [OK] をクリックします。
12. すべてのパッケージのターゲットパッケージ名を変更したら、すべての青いフォルダを選択し、*次へ*をクリックして続行します。
13. デフォルト値をすべて受け入れます。
14. をクリックし、[実行]*を選択します。
15. このインポートの詳細を確認し、* OK *をクリックします。
16. [更新]*をクリックすると、インポートのステータスが表示されます。
17. インポートが完了したら、*[閉じる]*をクリックします。

結果

[Public Folders]タブに2セットのパッケージが表示されます。たとえば、があるとします `7.0` サフィックス（新しいバージョンの場合）とが付いたサフィックス `_original` （またはbackup/restore手順 で入力したもの）サフィックス。これには、古いレポートが含まれます。データモデルの変更により、古いパッケージのレポートは実行されず、アップグレードが必要になる場合があります。ポータルタブが現在のバージョンのポータルページを指すようになりました。

コマンドラインインターフェイスを使用した**MySQL**へのアクセス

Data Warehouseのデータ要素には、レポートオーサリングツールを使用してアクセスできるだけでなく、MySQLユーザとして接続することで直接アクセスすることもできます。MySQLユーザとして接続して、独自のアプリケーションでデータ要素を使用することもできます。

このタスクについて

接続方法はたくさんあります。次の手順は、1つの方法を示しています。

MySQLにアクセスする場合は、Data Warehouseがインストールされているマシンの MySQLデータベースに接続します。MySQLのデフォルトのポートは3306ですが、インストール時に変更できます。ユーザ名とパスワードは、dwhuser / netapp123です。

手順

1. Data Warehouseがインストールされているマシンで、コマンドラインウィンドウを開きます。
2. OnCommand Insight ディレクトリ内のmysqlディレクトリにアクセスします。
3. 次のユーザー名とパスワードを入力します。 `mysql -udwhuser -pnetapp123`

   Data Warehouseがインストールされている場所に応じて、次の情報が表示されます。

   ```
   c:\Program Files\SANscreen\mysql\bin> mysql -udwhuser -pnetapp123
   ```

   ```
   Welcome to the MySQL monitor. Commands end with ; or \g.
   Your MySQL connection id is 882
   Server version: 5.1.28-rc-community MySQL Community Server (GPL)
   ```

   ```
   Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
   ```

4. Data Warehouseデータベースを表示します。 `show databases;`

   次のメッセージが表示されます。

```
mysql> show databases;
+-------------------------+
| Database                |
+-------------------------+
| information_schema      |
| dwh_capacity            |
| dwh_capacity_efficiency |
| dwh_fs_util             |
| dwh_inventory           |
| dwh_performance         |
| dwh_ports               |
+-------------------------+
```

Data Warehouseのトラブルシューティング

Data Warehouseのトラブルシューティングに関連するさまざまなタスクを実行できます。

- OnCommand Insight ASUPを使用する。
- OnCommand Insight ログを表示します。
- アップグレードとビジネスエンティティに関連する問題を解決する。
- 複数のOnCommand Insight サーバの統合に関連する問題を解決します。

複数のOnCommand Insight サーバを同じData Warehouseデータベースに統合できます。多くの設定では、複数のコネクタから同じオブジェクトが報告される場合があります（つまり、同じスイッチが2つのOnCommand Insight インスタンスに存在する場合）。このような場合、Data Warehouseは複数のオブジェクトを1つに統合します（プライマリコネクタが選択され、オブジェクトのデータはそのコネクタからのみ取得されます）。

ストレージ管理者は、[Troubleshooting]ページを使用して、統合の問題に関連する問題を解決できます。

ASUPを使用した問題 の解決

ASUPのログをテクニカルサポートに送信して、トラブルシューティングの支援を受けることができます。Data WarehouseのASUPは自動的に実行されるように設定されます。Data Warehouseポータルでは、自動送信プロセスを無効にしたり、Data Warehouseデータベースのバックアップを含めるように指定したり、ASUPへの転送を開始したりできます。

ログの情報は、HTTPSプロトコルを使用してテクニカルサポートに転送されます。ASUPを使用してデータを転送するには、Insight ServerでASUPを最初に設定する必要があります。

Data WarehouseからOnCommand Insight サーバにログが送信されます。このサーバは、Data Warehouseポータルの[Connectors]ページにリストされている最初のコネクタです。自動プロセスでは、次のファイルが送信されます。

- Data Warehouseのログ。次のログが記録されます。
  - boot.log（バックアップを含む）
  - dwh.log（dwh.log.1などのバックアップを含む）
  - dhw_troubleshoot.log
  - dwh_upgrade.log（バックアップを含む）
  - WildFly.log（バックアップを含む）
  - ldap.log（バックアップを含む）
  - Data Warehouse管理データベースのSQLダンプ
  - mysql：my.cnf、.err、およびスロークエリのログ
  - 完全なInnoDBステータス
- Cognosのログ。次のログが記録されます。
  - cognos-logs.zip

    にあるCognosログファイルが含まれています `<install>\cognos\c10_64\logs` ディレクトリ。また、Cognosで生成されるログ、およびOnCommand Insight Reportingに対するユーザのログインとログアウトがすべて記録されたOnCommand のInsightAP.logファイルも含まれます。

  - DailyBackup.zip

    [Public Folders]にあるレポートアーティファクトのバックアップが含まれています。[マイフォルダ]の内容はこれには含まれません。

  - Cognos *`version`*`site name`_content_store.zip

    Cognos Content Storeのフルバックアップが格納されています。

トラブルシューティングレポートは手動で生成できます。トラブルシューティングレポートの.zipファイルには、Data Warehouseに関する次の情報が含まれています。

- boot.log（バックアップを含む）
- dwh.log（dwh.log.1などのバックアップを含む）
- dwh_upgrade.log（バックアップを含む）
- wildfly.log（バックアップを含む）
- ldap.log（バックアップを含む）
- c：\Program Files\SANscreen\wildfly\standalone\log\dwh\内のダンプファイル
- Data Warehouse管理データベースのSQLダンプ
- mysql：my.cnf、.err、およびスロークエリのログ
- 完全なInnoDBステータス

> OnCommand Insight データベースのバックアップは、ASUPからテクニカルサポートに自動的に送信されません。

ASUPの自動送信を無効にしています

すべてのネットアップ製品には、環境で発生した問題のトラブルシューティングに最大限のサポートを提供する自動化された機能が搭載されています。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。Data Warehouseではデフォルトで ASUPが有効になっていますが、情報の送信が不要になった場合は無効にすることができます。

手順

1. 左側のナビゲーションペインで、*トラブルシューティング*をクリックします。
2. ASUPから日次レポートが送信されないようにするには、[無効化]*をクリックします。

   ASUPが無効になったことを示すメッセージが表示されます。

Data Warehouseデータベースのバックアップを含む

デフォルトでは、トラブルシューティングのサポートを受けるためにASUPからテクニカルサポートに送信されるのはData Warehouseのログファイルだけですが、Data Warehouseデータベースのバックアップを含めるように指定して、送信するデータのタイプを選択することもできます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*トラブルシューティング*をクリックします。
3. ASUPにData Warehouseデータベースのバックアップを含めるように指定するには、*[Include DWH Database Backup]*リストをクリックし、バックアップに含めるデータのタイプとして次のいずれかのオプションを選択します。
   - すべて（パフォーマンスを含む）
   - パフォーマンスを除くすべて
   - 在庫のみ
4. [更新（ Update ）] をクリックします。

Insightのログを ASUPに送信しています

ASUPのログをテクニカルサポートに送信して、トラブルシューティングの支援を受けることができます。Data WarehouseのASUPは自動的に実行されるように設定されます。Data Warehouseポータルでは、自動送信プロセスを無効にしたり、Data Warehouseデータベースのバックアップを含めるように指定したり、ASUPへの転送を開始したりできます。ASUPレポートを要求すると、Data Warehouseポータルの[Jobs]ページにレポート要求がジョブとして表示されます。

このタスクについて

ジョブは、他のジョブの処理と同様に、ジョブキューによって管理されます。保留状態または実行中のASUPジョブがすでにある場合は、ジョブキューに保留中の要求または実行中の要求が含まれているためにASUPレポート要求をジョブ要求に追加できないことを示すエラーメッセージが表示されます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*トラブルシューティング*をクリックします。
3. トラブルシューティング*ページの* OnCommand Insight ASUP セクションで、[DWHトラブルシューティングレポートのダウンロード]*をクリックしてトラブルシューティングレポートを取得します。
4. Data Warehouseポータル*の[Connectors]ページで最初のコネクタとしてリストされているOnCommand Insight サーバにレポートを送信するには、*[Send Now]*をクリックします。

OnCommand Insight ログの表示

Data WarehouseとCognosのさまざまなログをOnCommand Insight で表示できます。

このタスクについて

トラブルシューティングとステータスの情報は、CognosとData Warehouseのログファイルで確認できます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*トラブルシューティング*をクリックします。
3. セクションで、[ログファイル]*をクリックします。

   次のログファイルが表示されます。

dwh.log
Data Warehouseのジョブのステータスが表示されます
wildfly.log
WildFlyアプリケーションサーバーに関する情報を提供します
dwh_upgradeログ
Data Warehouseでのアップグレードに関する情報を提供します
ldap.log

	LDAP認証に関連するメッセージを記録します
dwh_troubleshoot.log	
	DWHの問題のトラブルシューティングに役立つメッセージが記録されます
sanscreenap.log	
	サーバへの接続、Cognosリポジトリへの認証とアクセス、およびその他のプロセスに関する情報が表示されます
cognosserver.log	
	Cognosのログ

4. 表示するログファイルの名前をクリックします。

複数サーバシャーシの統合に関する問題

ホスト、アダプタ、SANスイッチ、およびストレージアレイについて報告するコネクタを表示できます。また、オブジェクトについてレポートするさまざまなコネクタを表示し、プライマリコネクタ（オブジェクトに対して選択されたコネクタ）を識別することもできます。

ホストとアダプタの統合に関する問題の表示

ホストとその関連アダプタについて報告されるデータは、Inventoryデータマートから取得されます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*トラブルシューティング*をクリックします。
3. セクションで、[Hosts and Adapters]*をクリックします。

> この例の構成は有効な構成ではありません。プリンシパルコネクタと使用可能なコネクタがlocalhostにあることから、Insight ServerとDWHが同じサーバにインストールされていることがわかります。この例の目的は、統合テーブルを理解することです。

Hosts and Adapters Consolidation

Filter

Host GUID	Host Name	Host IP	Adapter GUID	Adapter WWN	Principal Connector	Available Connectors	Insight ID	Insight Change Time
288	Agassi	192.1.168.71			localhost (1)	localhost (1)	9927	11/18/10 1:36 PM
			576	40:A0:00:00:00:00:00:84	localhost (1)	localhost (1)	9928	11/18/10 1:36 PM
			577	40:A0:00:00:00:00:00:85	localhost (1)	localhost (1)	9930	11/18/10 1:36 PM
305	AI_Host1	192.1.168.88			localhost (1)	localhost (1)	12254	11/18/10 1:38 PM
			597	40:A0:00:00:00:00:01:05	localhost (1)	localhost (1)	12255	11/18/10 1:38 PM
306	AI_Host2	192.1.168.89			localhost (1)	localhost (1)	12257	11/18/10 1:38 PM
			598	40:A0:00:00:00:00:01:06	localhost (1)	localhost (1)	12258	11/18/10 1:38 PM
307	AI_Host3	192.1.168.90			localhost (1)	localhost (1)	12260	11/18/10 1:38 PM

すべてのホストとアダプタについて、ホストとアダプタについて報告するコネクタごとに行が作成され、ホストとアダプタの取得元であるプライマリコネクタも表示されます。ホストとアダプタの場合のみ、あるコネクタから報告されるホストのアダプタが別のコネクタから報告されることがあります。

各コネクタのホスト/アダプタのOnCommand Insight 変更時刻を確認することもできます。このパラメータを使用すると、ホスト/アダプタがOnCommand Insight で更新された日時と、同じホスト/アダプタが他のOnCommand Insight サーバで更新された日時を検出できます。

4. 必要に応じて、テキストの一部を入力して* Filter をクリックし、このビューでデータをフィルタリングします。フィルタをクリアするには、 Filter ボックスのテキストを削除し、 Filter *をクリックします。ホスト名、ホストIP、アダプタWWN、またはOnCommand Insight オブジェクトIDでフィルタリングできます。

   フィルタでは大文字と小文字が区別されます。

5. 次のデータを確認します。
   - *ホストGUID *

     このタイプの統合デバイス（ホスト）のグローバル一意識別子

   - * ホスト名 *

Data Warehouseに表示される統合ホストの名前

- *ホストIP *

  統合ホストのIPアドレス

- *アダプタGUID *

  ホストアダプタのグローバル一意識別子

- *アダプタWWN *

  ホストアダプタのWWN

- プリンシパルコネクタ

  データの実際のソースであったOnCommand Insight コネクタの名前

- 使用可能なコネクタ

  統合ホスト/アダプタが存在するすべてのOnCommand Insight コネクタ

- * Insight ID *

  関連するレポートコネクタの統合ホスト/アダプタのOnCommand Insight ID

- * Insight Change Time *

  ホスト/アダプタのOnCommand Insight で更新が行われたとき、および同じホスト/アダプタが他のOnCommand Insight サーバで更新されたとき

6. コネクタの詳細を取得するには、コネクタをクリックします。

   コネクタに関する次の情報が表示されます。

   - ホスト名
   - そのコネクタに対して最後にData Warehouseジョブが実行された日時
   - そのコネクタから最後に変更を受信した日時
   - そのコネクタが参照しているOnCommand Insight サーバーのバージョン

ストレージアレイの統合に関する問題の表示

ストレージアレイについて報告されるデータは、Inventoryデータマートから取得されます。すべてのストレージアレイについて、ストレージアレイについて報告するコネクタごとに行が表示され、各アレイの作成元であるプライマリコネクタも表示されます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*トラブルシューティング*をクリックします。
3. シャーシ統合*セクションで、* SANストレージアレイ*をクリックします。
4. 必要に応じて、このビューでデータをフィルタリングするには、[フィルタ]ボックスにテキストの一部を入力し、**[フィルタ]***をクリックします。フィルタをクリアするには、**[フィルタ]**ボックスのテキストを削除し、[フィルタ]*をクリックします。フィルタには、ストレージ名、ストレージIP、ベンダーモデル、OnCommand Insight オブジェクトIDを使用できます。

   フィルタでは大文字と小文字が区別されます。

5. 次のデータを確認します。
   - * GUID *

     このタイプの統合デバイス（ストレージアレイ）のグローバル一意識別子

   - * 名前 *

     Data Warehouseに表示される統合ストレージアレイの名前

   - * IP *

     統合ストレージアレイのIPアドレス

   - ベンダーおよびモデル

     統合ストレージアレイを販売するベンダーの名前とメーカーのモデル番号

   - プリンシパルコネクタ

     データの実際のソースであったOnCommand Insight コネクタの名前

   - 使用可能なコネクタ

     統合ストレージ・アレイが存在するすべてのOnCommand Insight コネクタ

   - * Insight ID *

     プリンシパルコネクタが配置されているOnCommand Insight シャーシ上の統合ストレージアレイのID

   - * Insight Change Time *

     ストレージアレイのOnCommand Insight で更新が行われた日時、および同じストレージアレイが他のOnCommand Insight サーバで更新された日時

スイッチの統合に関する問題の表示

スイッチについて報告されるデータは、Inventoryデータマートから取得されます。すべてのスイッチについて、スイッチについて報告するコネクタごとに行が表示され、各スイッチの取得元であるプライマリコネクタも表示されます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、[*トラブルシューティング]をクリックします。
3. Chassis Consolidation（シャーシ統合）セクションで、 SAN Switches（SANスイッチ）*をクリックします。
4. 必要に応じて、テキストの一部を入力して* Filter をクリックし、このビューでデータをフィルタリングします。フィルタをクリアするには、**[**フィルタ（**Filter**）**]**ボックスをクリアし、[フィルタ（Filter）]*をクリックします。フィルタには、スイッチ名、スイッチIP、ベンダーモデル、またはOnCommand Insight オブジェクトIDを使用できます。

   フィルタでは大文字と小文字が区別されます。

5. 次のデータを確認します。
   - * GUID *

     このタイプの統合デバイス（ストレージアレイ）のグローバル一意識別子

   - * 名前 *

     Data Warehouseで表示される統合ストレージアレイの名前

   - * IP *

     統合ストレージアレイのIPアドレス

   - ベンダーおよびモデル

     統合ストレージアレイを販売するベンダーの名前とメーカーのモデル番号

   - **WWN**

     統合スイッチのWWN

   - プリンシパルコネクタ

     データの実際のソースであったOnCommand Insight コネクタの名前

   - 使用可能なコネクタ

     統合ストレージ・アレイが存在するすべてのOnCommand Insight コネクタ

   - * Insight ID *

     プリンシパルコネクタが配置されているOnCommand Insight シャーシ上の統合ストレージアレイのID

   - * Insight Change Time *

     ストレージアレイのOnCommand Insight で更新が行われた日時、および同じストレージアレイが他のOnCommand Insight サーバで更新された日時

Data Warehouseの[Troubleshooting]ビューの[Annotation Consolidation]ビューには、使用可能なすべてのアノテーションタイプとそれらを適用できるオブジェクトタイプを含むテーブルが表示されます。

このタスクについて

アノテーション値の統合は、アノテーションタイプの値に基づいて行われます。ストレージアレイには、それぞれ異なるコネクタから取得される2つの階層値があります。したがって、一方のコネクタにgoldという名前でティアが定義され、もう一方のコネクタでgoldyという名前でティアが定義されている場合、この情報はData Warehouseに2つの個別のティアとして表示されます。

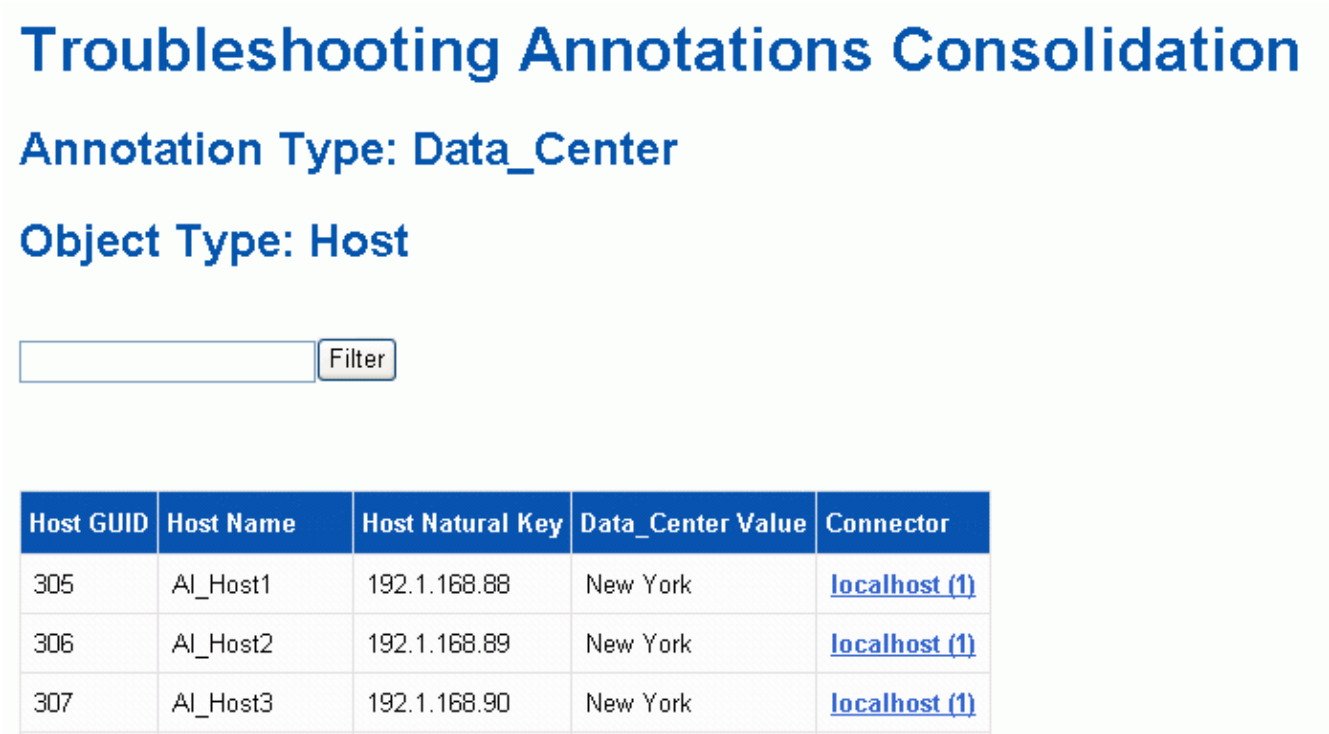
一部のアノテーションタイプでは同じオブジェクトに複数のアノテーション値を割り当てることができるため、Data Warehouseではオブジェクト（「host」など）に複数のアノテーション値を割り当てることができます（「data center 1」と「data center 2」を同じホストに割り当てることもできます）。

ボリュームのティアアノテーションは、一般的なアノテーションテーブルとは多少異なります。環境内には大量のボリュームが存在する可能性があり、それらをすべてData Warehouseに表示すると、情報のユーザビリティに影響する可能性があります。そのため、[Annotations Consolidation]ビューには、複数のティア値が割り当てられているボリュームと、そのボリュームを含むストレージのみが表示されます。

手順

1. Data Warehouseポータルにログインします `https://hostname/dwh`、ここで `hostname` 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、*トラブルシューティング*をクリックします。
3. セクションで、オブジェクトの行の[Show]*をクリックします。

   Data_Centerのアノテーションの例を次に示します。



レポート作成

OnCommand Insight Reportingへようこそ

OnCommand Insight Reportingは、事前定義済みのレポートを表示したり、カスタムレポートを作成したりできるビジネスインテリジェンスツールです。OnCommand Insightのレポート機能を使用すると、Data Warehouse（DWH）データからレポートが生成されます。

OnCommand Insight Reportingでは、次のタスクを実行できます。

- 事前定義済みのレポートを実行します
- カスタムレポートを作成する
- レポートの形式と配信方法をカスタマイズする
- レポートが自動的に実行されるようにスケジュールを設定する
- レポートを E メールで送信
- データのしきい値を色で表します

事前定義済みのレポートは、標準のOnCommand Insight レポートです。このガイドでは、すべての製品ライセンスで使用できる事前定義済みレポートについて説明します。

OnCommand Insight Reportingポータルへのアクセス

OnCommand Insight のレポートポータルには、Webブラウザ、Data Warehouse、またはInsightサーバから直接アクセスできます。Reportingポータルを使用して、事前定義済みのレポートにアクセスしたり、Data Warehouseのデータを使用して独自のレポートを作成したりできます。

Webブラウザから Reportingポータルにアクセスします

手順

1. Web ブラウザを開きます。
2. 次のURLを入力します。 `https://server-name:9300/bi`

   9300は、インストール時に指定されたデフォルトポートです。別のポートが指定されている場合は、ポートを変更する必要があります。

3. ユーザー名とパスワードを入力し、* OK *をクリックします。

Insight Serverから Reportingポータルにアクセスする

手順

1. Web ブラウザを開きます。

2. 次のURLを入力してInsight Serverにアクセスします。 `https://server-name`
3. ユーザー名とパスワードを入力し、* OK *をクリックします。
4. Insightのツールバーで、をクリックします 。
5. 表示されるログインページで、ユーザー名とパスワードを入力し、* OK *をクリックします。

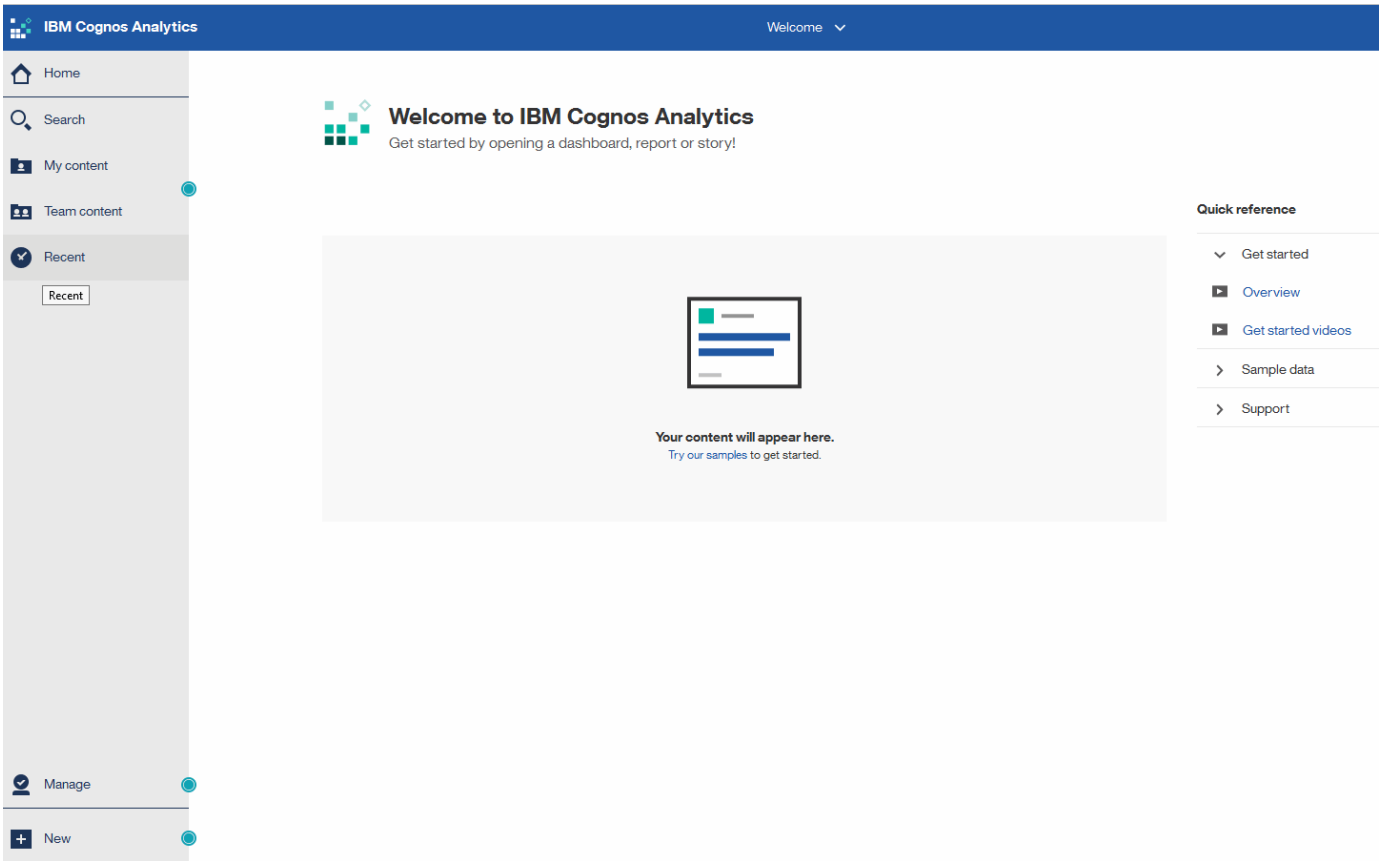
Data Warehouseから**Reporting**ポータルにアクセスする

手順

1. Web ブラウザを開きます。
2. 次のURLを入力してData Warehouseにアクセスします。 `https://server-name/dwh`
3. ユーザー名とパスワードを入力し、* OK *をクリックします。
4. Data Warehouseツールバーで、をクリックします 。
5. 表示されるログインページで、ユーザー名とパスワードを入力し、* OK *をクリックします。

結果

IBM Cognos Analyticsのようこそページが表示されます。これは、OnCommand Insight Reportingポータルのデフォルトのランディングページです。



インストールされているライセンスによる違い

OnCommand Insight レポートのデータは、購入したOnCommand Insight ライセンスに

基づいています。たとえば、Planライセンスがない場合、インベントリデータマートに容量とパフォーマンスのポイントインタイムデータ（現在）が表示されますが、デバイスの容量データやパフォーマンスデータをトレンド分析（一定期間にわたるレポート）することはできません。

プランライセンスがないと、新しいレポートを作成したり、既存のレポートを編集したりすることができなくなります。OnCommand Insight システムで使用可能なレポートが、ドキュメントの図と異なる場合があります。これらの違いは、システムにインストールされているライセンスと、図の作成に使用されたシステムのライセンスの違いによるものです。

ライセンスの詳細については、『OnCommand Insight インストールガイド』を参照してください。

Reportingユーザのロール

各ユーザアカウントには、一連の権限を持つロールが割り当てられます。ユーザーの数は、各ロールに関連付けられているReportingライセンスの数によって制限されます。

各ロールで実行できる操作は次のとおりです。

- 受信者

  OnCommand Insight Reportingポータルのレポートを表示し、言語やタイムゾーンなどの個人設定を設定します。

  > 受信者は、レポートの作成、レポートの実行、レポートのスケジュール設定、レポートのエクスポート、および管理タスクの実行を行うことはできません。

- ビジネスコンシューマ

  レポートを実行し、すべての受信者オプションを実行します。

- ビジネス著者

  Business Consumerのすべてのオプションに加えて、スケジュールされたレポートの表示、対話形式でのレポートの実行、ストーリーの作成が可能です。

- * Pro Author *

  Business Authorのすべてのオプションの実行に加えて、レポートの作成、パッケージおよびデータモジュールの作成を行います。

- 管理者

  レポート定義のインポートとエクスポート、レポートの設定、データソースの設定、レポートタスクのシャットダウンと再開など、レポート管理タスクを実行します。

次の表に、各ロールの権限と許可される最大ユーザ数を示します。

フィーチャー（Feature）	受信者	ビジネスパーソン	著作家	作者プロ	管理

[チームコンテンツ] タブでレポートを表示します	はい。	はい。	はい。	はい。	はい。
レポートを実行する	いいえ	はい。	はい。	はい。	はい。
レポートのスケジュールを設定する	いいえ	はい。	はい。	はい。	はい。
外部ファイルをアップロードします	いいえ	いいえ	はい。	はい。	いいえ
ストーリーを作成します	いいえ	いいえ	はい。	はい。	いいえ
レポートを作成します	いいえ	いいえ	いいえ	はい。	いいえ
パッケージとデータモジュールを作成します	いいえ	いいえ	いいえ	はい。	いいえ
管理タスクを実行	いいえ	いいえ	いいえ	いいえ	はい。
ユーザ数	OnCommand Insight ユーザの数	20	2.	1.	1.

Data WarehouseとReportingの新しいユーザを追加したときにロールの制限を超えたユーザが「非アクティブ化」として追加されます。新しいユーザにメンバーシップを付与するには、そのロールを持つ別のユーザを非アクティブ化するか削除する必要があります。

> レポートオーサリング機能を使用するにはInsight Planのライセンスが必要です。Business AuthorユーザとPro Authorユーザを追加するには、ARAP（Additional Report Authoring Package）を購入します。詳細については、OnCommand Insight の担当者にお問い合わせください。

Reportingユーザのロールは、データベースへの直接アクセスには影響しません。Reportingユーザのロールは、データマートを使用してSQLクエリを作成する機能には影響しません。

セキュリティヘッダーの有効化

HTTPヘッダーを設定すると、Cognos Analytics Webアプリケーションの全体的なセキュ

リティを強化できます。

応答ヘッダーを追加するには：

- Cognos Analytics UIにログインし、*[Manage]>[Configuration]>[System]>[Advanced Settings]*に移動します
- 次のキー/値を追加して適用します。
  - キー： `BIHeaderFilter.responseHeaders`
  - 値： `[{"name":"X-FRAME-OPTIONS","value":"SAMEORIGIN"},{"name":"X-XSS-Protection","value":"1"},{"name":"X-Content-Type-Options","value":"nosniff"}]`
- ヘッダーを有効にするには、ブラウザをリフレッシュしてください。

レポート作成が容易に

OnCommand Insight Reportingポータルから事前定義済みのレポートを生成したり、他のユーザにEメールで送信したり、変更したりできます。複数のレポートを使用して、デバイス、ビジネスエンティティ、または階層でフィルタリングできます。このレポートツールは、 IBM Cognos をベースとしたツールで、さまざまなデータ表示オプションが用意されています。

- OnCommand Insight の事前定義済みレポートには、インベントリ、ストレージ容量、チャージバック、パフォーマンス、ストレージ効率、 クラウドのコストデータを削減できます。これらの事前定義済みレポートを変更して、変更内容を保存できます。

使用可能なレポートデータは、次のようないくつかの要素によって制御されます。

- ロールごとに定義されるOnCommand Insight Reportingポータルにログインします。
- レポートのデータを格納するOnCommand InsightData Warehouseのセットアップ。

HTML 、 PDF 、 CSV 、 XML などのさまざまな形式でレポートを生成できます。 Excel などです。

OnCommand Insight では、ユーザをビジネスユニットに関連付けることで、Reportingでマルチテナンシーを実現できます。この機能を使用すると、管理者は、ユーザーまたは所属先の属性に従ってデータまたはレポートを分離できます。

> Cognosバージョン11.1.2以降では、レポートURLは「安定している」とはみなされず、変更される場合があります。ブックマークされたレポートURLがある場合、これらのブックマークは失敗する可能性があります。詳細については、次のサイトを参照してください。
> http://queryvision.com/ibm-analytics-11-x-urls-they-are-a-changing/

> OnCommand Insight では、新しいデータモジュール機能を使用しないかぎり、IBM Cognosのパッケージを使用して作成されたダッシュボードはサポートされません。

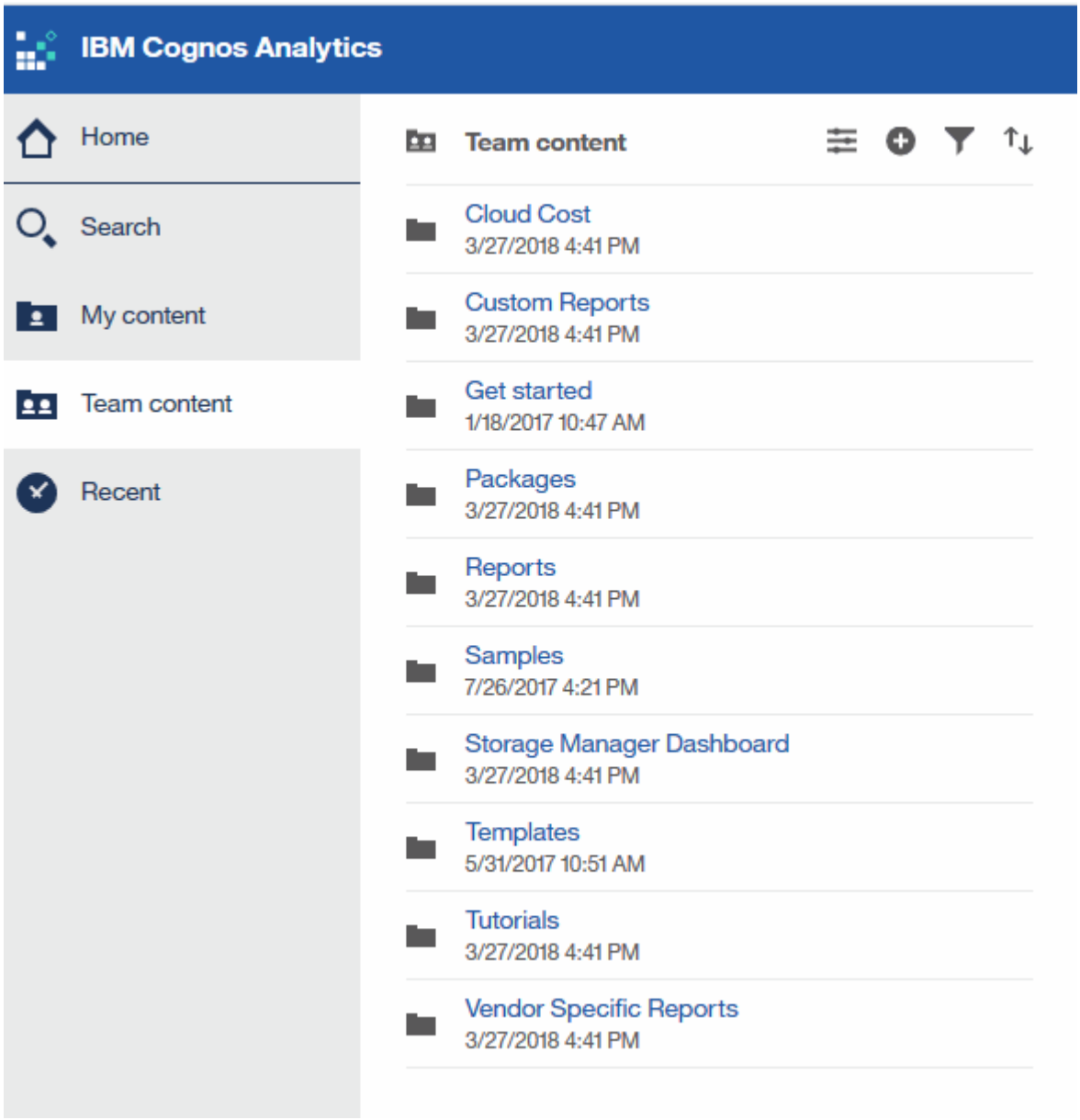
事前定義済みの**OnCommand Insight** レポートへの移動

Reportingポータルを開くと、OnCommand Insight レポートで必要な情報のタイプを選

択するには、[チーム]コンテンツフォルダが出発点になります。

手順

1. 左側のナビゲーションペインで、*[チームコンテンツ]*をクリックし、使用する情報カテゴリを選択します。



2. [*Reports] をクリックして、事前定義済みレポートにアクセスします。
3. レポートの作成方法については、**[はじめに]**、**[サンプル]**、*[チュートリアル]*をクリックしてください。

Storage Manager Dashboardで実行できる操作

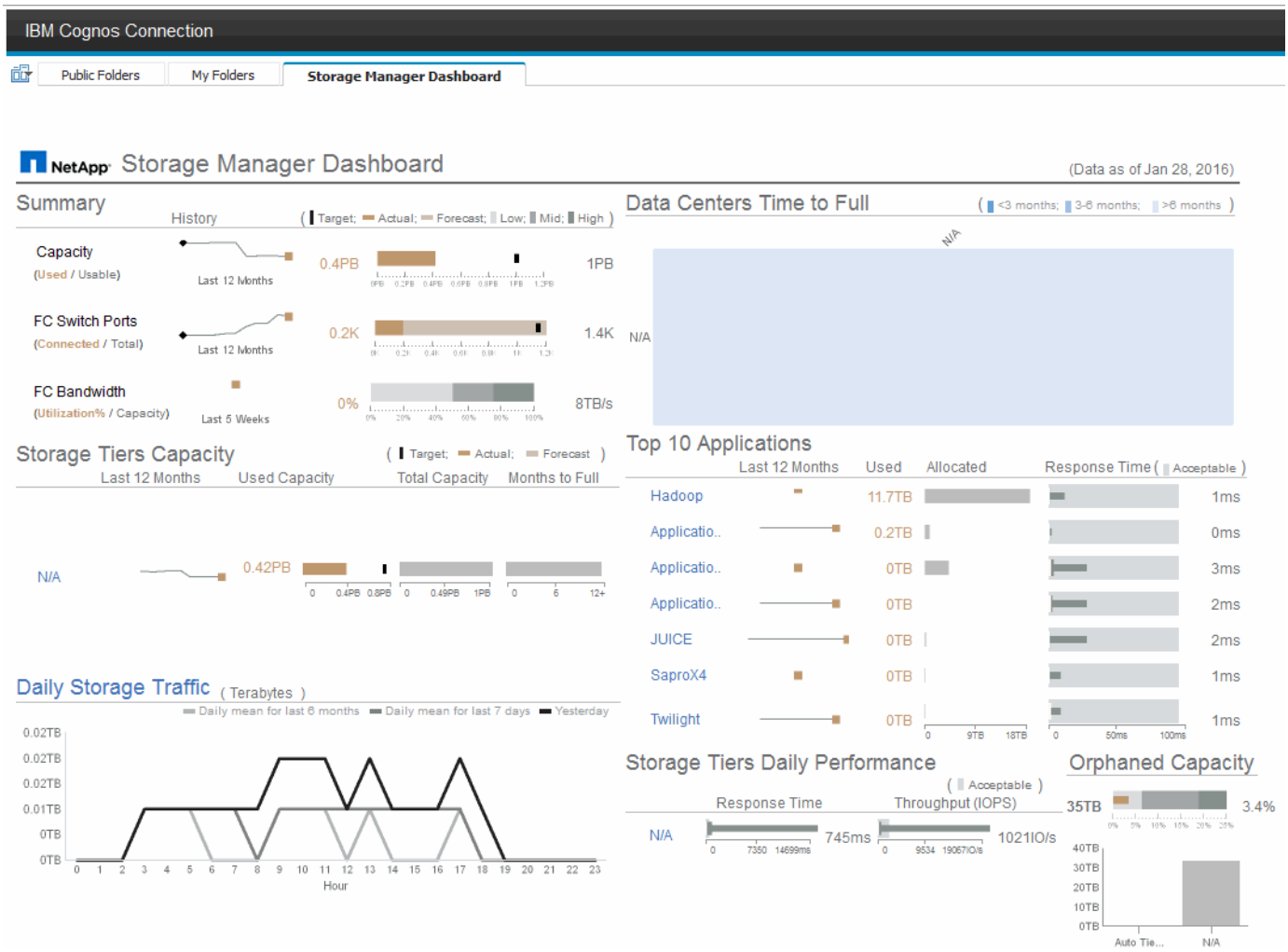
ストレージサービスの日々の管理には、 Storage Manager のダッシュボードを使用できます。

Storage Manager Dashboard では、一定期間のリソース使用量をまとめて表示し、許容範囲および過去何日

間かのアクティビティと比較することができます。ストレージサービスの主要なパフォーマンス指標だけが表示されるため、データセンターの管理方法についての決定を下すことができます。

このダッシュボードは 7 つのコンポーネントで構成され、ストレージ環境の特定の要素に関するコンテキスト情報が表示されます。ストレージサービスの要素をドリルダウンして、最も関心のあるセクションについて詳細な分析を実施できます。

まとめ



このコンポーネントには、使用済みのストレージ容量と使用可能なストレージ容量、スイッチポートの総数と接続されているスイッチポートの数、接続されているスイッチポートの合計利用率と総帯域幅、および一定期間にわたるこれらのトレンドが表示されます。実際の利用率を低、中、高の範囲と比較して表示することができます。これにより、Insightの予測と目的の実際の利用率を、ターゲットに基づいて比較し、比較することができます。容量とスイッチポートについては、このターゲットを設定できます。予測は、現在の増加率と設定した日付による外挿によって算出されます。将来使用日に基づいて予測された使用済み容量がターゲットを超えると、容量の横にアラート（赤い丸）が表示されます。

ストレージ階層容量

このコンポーネントには、使用済みの階層容量と階層に割り当てられた容量が表示され、 12 カ月間での使用済み容量の増減と容量の上限に到達するまでの月数が表示されます。実際の使用状況、Insightによる使用状況の予測、および設定可能な容量のターゲットが表示されます。将来使用日に基づいて予測された使用済み容量がターゲットを超えると、階層の横にアラート（赤い丸）が表示されます。

いずれかの階層をクリックすると、 Storage Pools Capacity and Performance Details レポートを表示できます。このレポートには、空き容量と使用済み容量、上限に到達するまでの日数、および選択した階層内のすべてのプールのパフォーマンス（ IOPS と応答時間）の詳細が表示されます。また、このレポート内のいずれかのストレージまたはストレージプール名をクリックすると、リソースの現在の状態をまとめたアセットページを表示できます。

日次ストレージトラフィック

このコンポーネントには、環境のパフォーマンス、増加率、変更率、潜在的な問題が過去 6 カ月間と比較してどのように発生しているかが表示されます。また、平均トラフィックと過去 7 日間および前日のトラフィックの比較も表示されます。周期的（過去 7 日間）な変化と季節的（過去 6 カ月間）な変化の両方を示す情報が提供されるため、インフラのパフォーマンスについての異常を可視化できます。

タイトル（**[**毎日のストレージトラフィック**]**）をクリックすると、[Storage Traffic Details]レポートが表示されます。このレポートには、各ストレージシステムについて、前日のストレージトラフィックの1時間ごとのヒートマップが表示されます。レポート内のいずれかのストレージ名をクリックすると、リソースの現在の状態をまとめたアセットページが表示されます。

データセンターがフルになるまでの時間

このコンポーネントには、Insightで予測される増加率に基づいて、すべてのデータセンターとすべての階層が表示され、ストレージの各階層について各データセンターに残っている容量が表示されます。階層の容量レベルは青で表示され、色が暗くなるほど、その場所の階層が上限に到達するまでの時間が少なくなります。

階層のセクションをクリックすると、 Storage Pools Days to Full Details レポートを表示できます。このレポートには、合計容量、空き容量、選択した階層とデータセンター内のすべてのプールが上限に到達するまでの日数が表示されます。レポート内のいずれかのストレージまたはストレージプール名をクリックすると、リソースの現在の状態をまとめたアセットページが表示されます。

上位 **10** 個のアプリケーション

このコンポーネントには、使用済み容量に基づく上位 10 個のアプリケーションが表示されます。この領域には、階層によるデータの割り当てに関係なく、インフラの現在の使用済み容量と共有状況が表示されます。過去 7 日間のユーザエクスペリエンスを可視化して、応答時間が許容可能な（または許容できない）範囲にあるかどうかを確認できます。

また、アプリケーションがパフォーマンスのサービスレベル目標（ SLO ）を満たしているかどうかを示すトレンドも表示されます。前週の最小応答時間、最初の四分位数、 3 番目の四分位数、および最大応答時間を表示できます。中央値は、許容可能な SLO に対して表示され、設定可能です。応答時間の中央値が許容可能な SLO 範囲に含まれていない場合は、アプリケーションの横にアラート（赤い丸）が表示されます。アプリケーションをクリックすると、リソースの現在の状態をまとめたアセットページを表示できます。

ストレージ階層の日次パフォーマンス

このコンポーネントには、過去 7 日間の応答時間と IOPS についての階層のパフォーマンスの概要が表示されます。このパフォーマンスは、ユーザが設定可能な SLO と比較したものです。これにより、階層の統合、階層から提供されるワークロードの再調整、または特定の階層に関する問題の特定の機会があるかどうかを確認できます。応答時間の中央値または IOPS の中央値が許容可能な SLO 範囲に含まれていない場合は、階層の横にアラート（赤い丸）が表示されます。

階層名をクリックすると、 Storage Pools Capacity and Performance Details レポートを表示できます。このレポートには、空き容量と使用済み容量、上限に到達するまでの日数、および選択した階層内のすべてのプールのパフォーマンス（ IOPS と応答時間）の詳細が表示されます。レポート内のいずれかのストレージまたは

ストレージプールをクリックすると、リソースの現在の状態をまとめたアセットページが表示されます。

孤立容量

このコンポーネントには、孤立容量の合計と階層別の孤立容量が表示されます。使用可能な総容量の許容範囲と比較され、孤立している実際の容量が表示されます。孤立容量には、設定に起因するものとパフォーマンスに起因するものがあります。_設定によって孤立したストレージ_ホストにストレージが割り当てられている状況を示します。ただし、設定が正しく実行されていないため、ホストはストレージにアクセスできません。_orphaned by performance_isは、ホストからアクセスするようにストレージが正しく設定されている場合です。ただし、ストレージトラフィックが発生していません。

水平の積み上げ棒は許容範囲を示します。グレーの色が暗くなるほど、許容できない状況になります。実際の状況は、孤立している実際の容量を示す細いブロンズバーとともに表示されます。

階層をクリックすると、 Orphaned Storage Details レポートを表示できます。このレポートには、選択した階層について、設定およびパフォーマンスが原因で孤立していると特定されたすべてのボリュームが表示されます。このレポート内のいずれかのストレージ、ストレージプール、またはボリュームをクリックすると、リソースの現在の状態をまとめたアセットページが表示されます。

事前定義済みのレポートを使用した回答に関する一般的な質問への

OnCommand Insight には、レポート作成に関する一般的な要件に対応する事前定義済みのレポートが用意されており、関係者がストレージインフラに関する十分な情報に基づいて意思決定を行うために必要な重要な分析情報を得ることができます

以下の事前定義されたレポートは、チームコンテンツ>*レポート*または*チームコンテンツ*>*ベンダー固有のレポート*で使用できます。

NetApp Storage Automation Storeでは、新しいバージョンのレポートを入手できる場合があります。Automation Storeで定期的にレポートを確認する必要があります。

- * AWSクラウドのコストデータ*

  クラウドコストレポートにはすべての資産がまとめて表示されるため、環境内で動的に拡張されるクラウドベースサービスとオンプレミスサービスの使用状況とコストを追跡、分析、最適化できます。

  このレポートでは、インフラとコストの相関関係を示し、明確で実用的なレポートを提供して、集中的なキャパシティプランニングと廃棄物の検出を通じて適切なサイジングを確実に行うことができます。

- アプリケーションサービスレベルの容量とパフォーマンス

  Application Service Level Capacity and Performance レポートには、アプリケーションの概要が表示されます。この情報は、キャパシティプランニングや移行計画に使用できます。

- チャージバック

  Chargeback レポートには、ストレージ容量のチャージバックとアカウンタビリティの情報がホスト、アプリケーション、およびビジネスエンティティ別に表示され、現在のデータと履歴データの両方が含まれます。

  データが二重に収集されないようにするために、 ESX サーバを対象から除外し、 VM のみを監視してください。

このレポートの最新版は、 NetApp Storage Automation Store から入手できます。

- データソース

  Data Sources レポートには、サイトにインストールされているすべてのデータソース、データソースのステータス（ success / failure ）、およびステータスメッセージが表示されます。このレポートには、データソースのどこで問題が発生したかに関する情報が記載されていますデータソースが正しく機能しないと、Insightでのレポートの精度と製品の一般的な操作性に影響します。

- * ESXとVMのパフォーマンス*

  ESX と VM のパフォーマンス比較レポートには、 ESX サーバと VM の平均および最大の IOPS 、スループット、レイテンシ、利用率が表示されます。データが二重に収集されないようにするために、 ESX サーバを対象から除外し、 VM のみを監視してください。

  このレポートの最新版は、 NetApp Storage Automation Store から入手できます。

- ファブリックの概要

  Fabric Summary レポートには、ポート数、ファームウェアバージョン、ライセンスステータスなど、スイッチとスイッチの情報が表示されます。このレポートには NPV スイッチポートは含まれません。

- *ホストHBA *

  Host HBAs レポートには、環境内のホストの概要と、 HBA のベンダー、モデル、ファームウェアバージョン、および HBA が接続されているスイッチのファームウェアレベルが表示されます。このレポートを使用して、スイッチまたは HBA のファームウェアのアップグレードを計画する際にファームウェアの互換性を分析できます。

- ホストのサービスレベルの容量とパフォーマンス

  Host Service Level Capacity and Performance レポートには、ブロック専用アプリケーションのホスト別のストレージ利用率の概要が表示されます。

- ホストの概要

  Host Summary レポートには、選択した各ホストのストレージ利用率の概要と、 Fibre Channel ホストおよび iSCSI ホストの情報が表示されます。このレポートを使用して、ポートとパス、 Fibre Channel と iSCSI の容量、および違反数を比較できます。

- ライセンスの詳細

  License Details レポートには、すべてのサイトで、ライセンスが付与されているリソースの数が表示されます。このレポートには、すべてのサイトでの実際のライセンス数の合計も表示されます。この合計には、複数のサーバで管理されるストレージアレイが重複してカウントされることがあります。

- マッピングされているがマスクされていないボリューム

  Mapped but not Masked Volumes レポートには、 LUN は特定のホストにマッピングされているが、そのホストに対してマスクされていないボリュームが表示されます。このようなボリュームは、マスクが解除された、運用を終了した LUN である可能性があります。マスクされていないボリュームにはどのホストからもアクセスできるため、データが破損しやすくなります。

- ネットアップの容量とパフォーマンス

  NetApp Capacity and Performance レポートには、割り当て済み容量、使用済み容量、コミット済み容量のグローバルデータ、および容量のトレンドとパフォーマンスデータが表示されます。

- * OCIスコアカード*

  OCIスコアカードレポートには、OnCommand Insight によって検出されたすべてのアセットの概要と一般的なステータスが表示されます。ステータスは、緑色、黄色、赤色のフラグで示されます。

  - 緑は正常な状態を示します
  - 黄色は、環境内に潜在的な問題があることを示します
  - 赤は、注意が必要な問題 を示します。レポートのすべてのフィールドは、レポートに付属のデータディクショナリに記載されています。

- ストレージの概要

  Storage Summary レポートには、 raw 、割り当て済み、ストレージプール、およびボリュームについて、使用済み容量と未使用の容量のデータの概要が表示されます。このレポートは、検出されたすべてのストレージの概要を示します。

  このレポートの新しいバージョンは、NetApp Storage Automation Storeで入手できます。

- * VMの容量とパフォーマンス*

  仮想マシン（ VM ）環境とその使用容量が表示されます。VM の電源がオフになっている場合など、一部のデータを表示するには、 VM ツールを有効にする必要があります。

- * VMパス*

  VM Paths レポートは、仮想マシンが実行されているホスト、どのホストがどの共有ボリュームにアクセスしているか、アクティブなアクセスパスが何であるか、および容量の割り当てと使用量がどのようなものであるかについて、データストアの容量データとパフォーマンスの指標を提供します。

- シンプール別の**HDS**容量

  HDS Capacity by Thin Pool レポートには、シンプロビジョニングされたストレージプールで使用可能な容量が表示されます。

- アグリゲート別のネットアップ容量

  NetApp Capacity by Aggregate レポートには、アグリゲートの合計 raw スペース、合計スペース、使用済みスペース、使用可能なスペース、およびコミット済みスペースが表示されます。

- シック・アレイ別の**Symmetrix**容量

  Symmetrix Capacity by Thick Array レポートには、 raw 容量、使用可能な容量、空き容量、マッピングされた容量、マスクされた容量が表示されます。 合計空き容量を確認します。

- シン・プール別の**Symmetrix**容量

  Symmetrix Capacity by Thin Pool レポートには、 raw 容量、使用可能な容量、使用済み容量、空き容量、使用済みの割合が表示されます。 サブスクライブ済み容量およびサブスクリプション率：

- アレイ別の**XIV**容量

  XIV Capacity by Array レポートには、アレイの使用済み容量と未使用の容量が表示されます。

- プール別の**XIV**容量

  XIV Capacity by Pool レポートには、ストレージプールの使用済み容量と未使用の容量が表示されます。

Cognosを使用したレポートの作成**11**

Cognos 11を使用したレポートの作成は、以前のバージョンのCognosとは異なります。この手順 を使用して、事前定義されたOnCommand Insight レポートを使用してレポートを作成します。

このタスクについて

次の手順に従って、複数のデータセンター内のストレージおよびストレージプールの物理容量に関する簡単なレポートを生成します。

手順

1. ツールバーで、をクリックします
2. [レポート（ Report ）] をクリックします
3. **>**[空白]*をクリックします
4. **>***クールブルー>*[OK]*をクリックします

   [ソース] タブと [データ] タブが表示されます

5. **>***をクリックします
6. ファイルを開くダイアログで、チームコンテンツ>*パッケージ*をクリックします

   利用可能なパッケージのリストが表示されます。

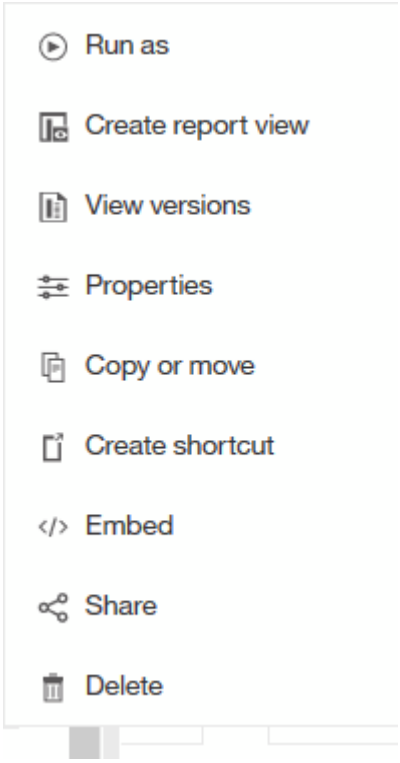
7. **>**[開く]*をクリックします
8. をクリックします

   レポートで使用できるスタイルが表示されます。

9. [**List**] をクリックします

   リストとクエリに適切な名前を追加します

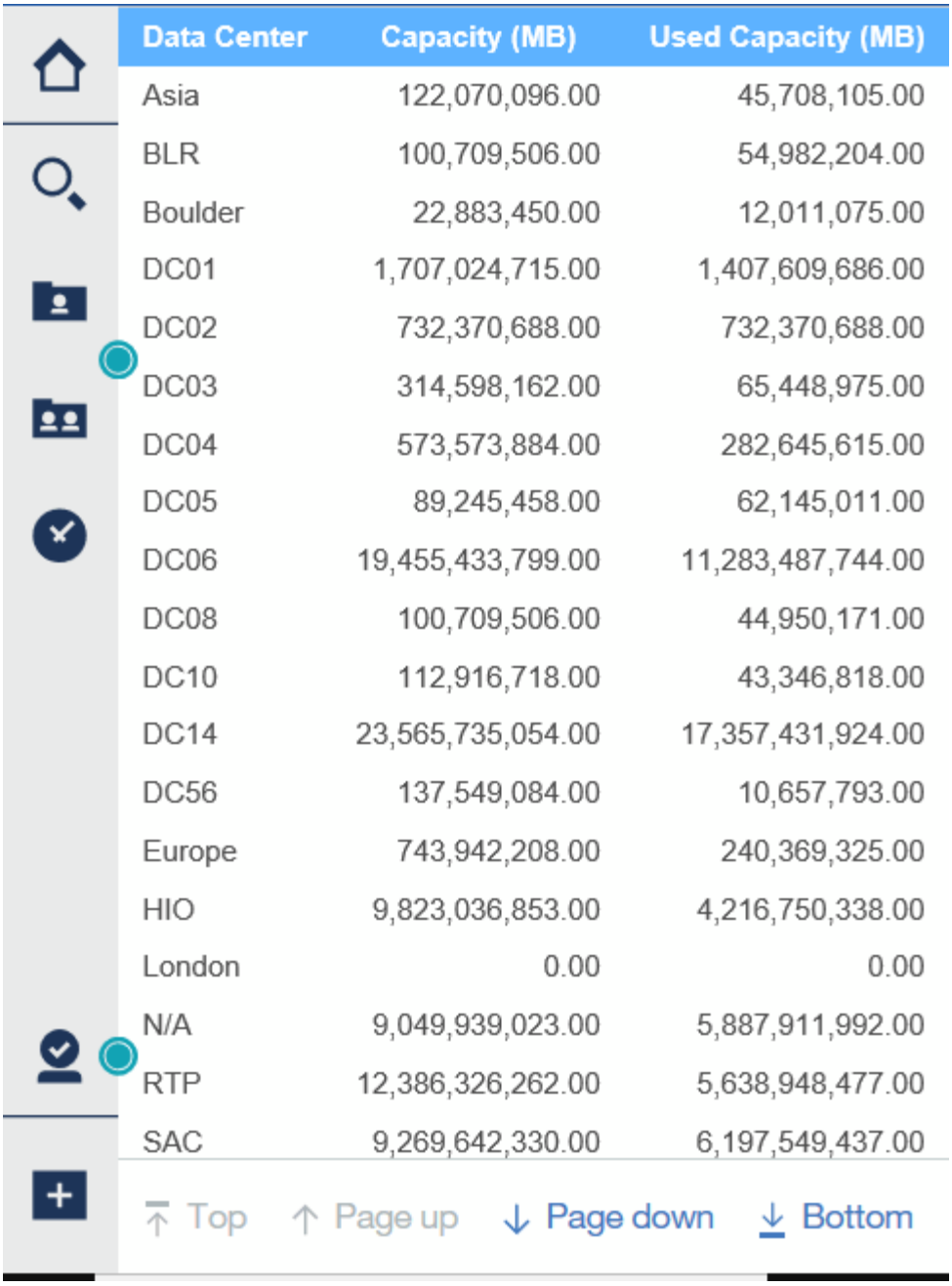
10. [OK] をクリックします。
11. [物理容量]*を展開します
12. 最下位レベルの* Data Center *に展開します

13. ドラッグします Data Center をクリックします。
14. [容量（MB）]*を展開します
15. [Capacity（MB）]*を[Reporting]パレットにドラッグします。
16. [Used Capacity（MB）]*をレポートパレットにドラッグします。
17. をクリックして、レポートを実行します 

をクリックし、出力タイプを選択します。

結果

次のようなレポートが作成されます。



Data Center	Capacity (MB)	Used Capacity (MB)
Asia	122,070,096.00	45,708,105.00
BLR	100,709,506.00	54,982,204.00
Boulder	22,883,450.00	12,011,075.00
DC01	1,707,024,715.00	1,407,609,686.00
DC02	732,370,688.00	732,370,688.00
DC03	314,598,162.00	65,448,975.00
DC04	573,573,884.00	282,645,615.00
DC05	89,245,458.00	62,145,011.00
DC06	19,455,433,799.00	11,283,487,744.00
DC08	100,709,506.00	44,950,171.00
DC10	112,916,718.00	43,346,818.00
DC14	23,565,735,054.00	17,357,431,924.00
DC56	137,549,084.00	10,657,793.00
Europe	743,942,208.00	240,369,325.00
HIO	9,823,036,853.00	4,216,750,338.00
London	0.00	0.00
N/A	9,049,939,023.00	5,887,911,992.00
RTP	12,386,326,262.00	5,638,948,477.00
SAC	9,269,642,330.00	6,197,549,437.00

レポートの管理

各レポートについて、[Actions]列の[* More *]リンクを選択し、レポートのプロパティの設定、レポートのスケジュール設定、レポートのEメール送信など、すべてのレポート処理にアクセスできます。管理者は、他のユーザよりも多くの管理オプションを使用できます。

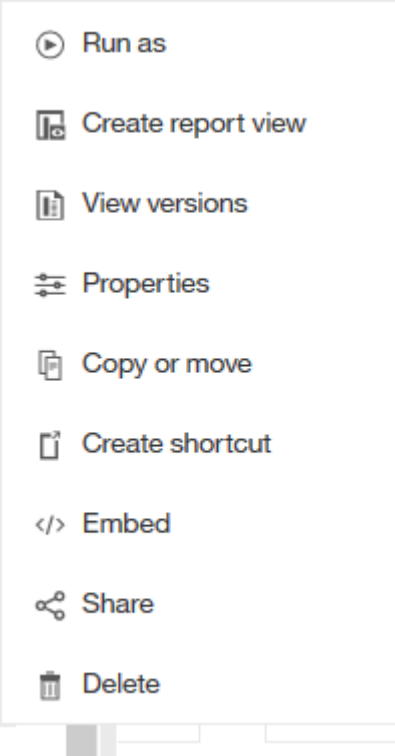
管理者は、OnCommand Insight ロールに応じて他のレポートユーザの権限を設定できます。

レポートの出力形式と配信方法をカスタマイズする

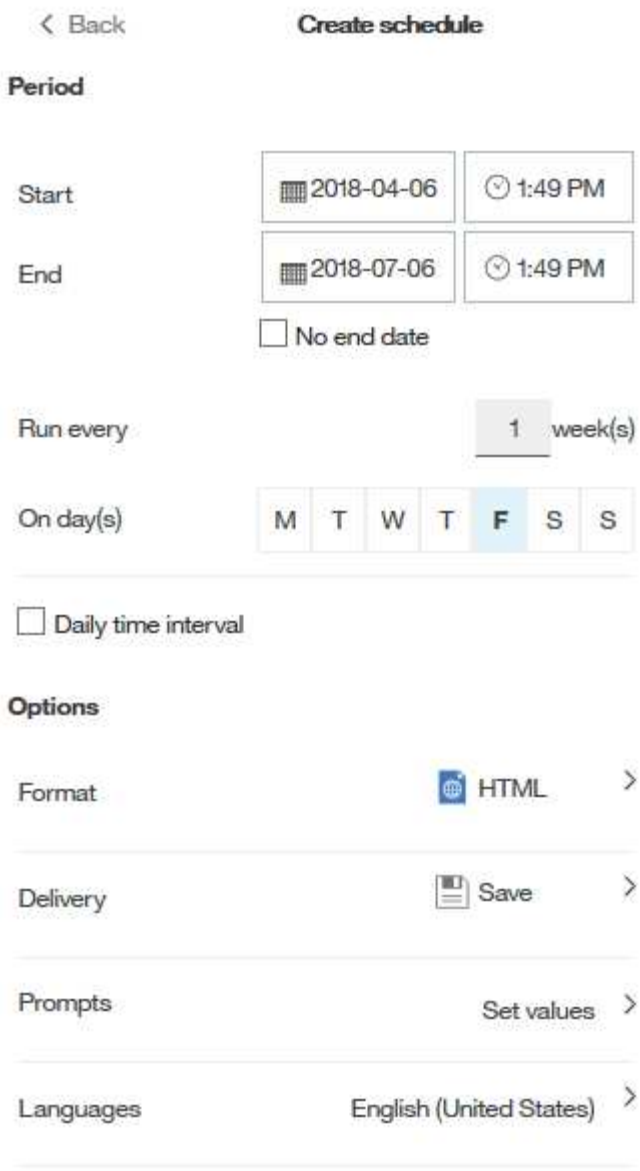
レポートの形式と配信方法をカスタマイズできます。

手順

1. OnCommand Insight レポートポータルを開き、カスタマイズするレポートを選択して*[…]*をクリックします。



2. **>**[スケジュール]*をクリックします



3. 次のオプションを設定できます。
   - レポートを実行するスケジュール。
   - *形式*レポート出力。
   - *配信*レポートを印刷、保存、または電子メールで送信します。
   - *言語*レポートが配信される言語を定義します。
4. [* 作成 *] をクリックして、選択した内容を使用してレポートを作成します。

レポートをクリップボードにコピーしています

レポートをクリップボードにコピーするには、次の手順を実行します。

手順

1. Cognos 11 Reportingポータルを開きます。 https://server-name:9300/bi/

2. ツールバーで、をクリックします
3. [レポート（ Report ）] をクリックします
4. [* ページ *] アイコンをクリックします

   [レポート（Report）]アイコン Report が表示されます

5. [レポート（Report）]*アイコンを左クリックします

   レポートオプションが表示されます。

6. [レポートをクリップボードにコピーする *] をクリックします。

クリップボードからレポート（ XML ）を開く

以前クリップボードにコピーされたレポート仕様を開くことができます。

このタスクについて

Reportingユーザインターフェイスに入るには、新しいレポートを作成するか、既存のレポートを開きます

手順

1. Cognos 11 Reportingポータルを開きます。 https://server-name:9300/bi/
2. ツールバーで、をクリックします
3. [レポート（ Report ）] をクリックします
4. [* ページ *] アイコンをクリックします

   [レポート（Report）]アイコン Report が表示されます

5. [レポート（Report）]*アイコンを左クリックします

   レポートオプションが表示されます。

6. [クリップボードからレポートを開く *] をクリックします。

カスタムアドホックレポートの作成

レポートオーサリングツールを使用してカスタムレポートを作成できます。作成したレポートは、保存して定期的に実行できます。レポートの結果は、自分や他のユーザに E メールで自動送信できます。

このセクションの例では、任意のOnCommand Insight データモデルで使用できる次のプロセスを示します。

- レポートで回答する質問を特定しています

- 結果をサポートするために必要なデータを決定する
- レポートのデータ要素を選択しています

レポートを設計する前に行う必要がある作業

カスタムレポートを設計する前に、いくつかの前提条件となるタスクを完了する必要があります。これらの作業を完了しないと、不正確または不完全なレポートが生成される可能性があります。

たとえば、デバイスの識別プロセスを完了していないと、正確な容量レポートが生成されません。また、アノテーション（階層、ビジネスユニット、データセンターなど）の設定が完了していないと、ドメイン全体でデータが正確にレポートされず、一部のデータポイントで「N/A」と表示されることがあります。

レポートを設計する前に、次の作業を完了してください。

- すべてのデータソースを設定します。詳細については、OnCommand Insight 構成および管理ガイド_を参照してください。
- 環境内のデバイスとリソースにアノテーション（階層、データセンター、ビジネスユニットなど）を入力します。OnCommand Insight Data Warehouseでは履歴情報が収集されるため、レポートを生成する前にアノテーションを安定させておくと便利です。
- 抽出、変換、読み込み（ETL）プロセスでOnCommand Insight サーバからのデータを受け入れるようにOnCommand Insight データウェアハウスを設定します。

レポートの作成プロセス

アドホックレポートを作成するプロセスには、いくつかのタスクが含まれます。

- レポートの結果を計画します。
- 結果をサポートするデータを特定します。
- データが格納されているデータモデル（ Chargeback データモデル、 Inventory データモデルなど）を選択します。
- レポートのデータ要素を選択します。
- 必要に応じて、レポート結果の書式設定、並べ替え、フィルタリングを行います。

カスタムレポートの結果を計画する方法

レポートデザインツールを開く前に、レポートから必要な結果を計画することができます。レポートオーサリングツールでは、レポートを簡単に作成でき、詳細な計画は必要ないかもしれませんが、レポートを必用としている担当者にレポートの要件について確認しておくことを推奨します。

- 回答の正確な質問を特定します。例：
  - 残りの容量
  - ビジネスユニットあたりのチャージバックコスト
  - 階層別の容量 - 各ビジネスユニットが適切なストレージ階層に配置されているか

- 必要な電力と冷却コストを予測するにはどうすればよいですか。（リソースにアノテーションを追加することで、カスタマイズしたメタデータを追加）

- 回答をサポートするために必要なデータ要素を特定します。
- 回答に表示するデータ間の関係を特定します。「容量に関連するポートを確認したい」など、非論理的な関係を質問に含めないでください。
- データに必要な計算があれば特定します。
- 結果を制限するために必要なフィルタリングのタイプを決定します。
- 現在のデータまたは履歴データのどちらを使用する必要があるかを判断します。
- レポートにアクセス権を設定してデータの閲覧を特定のユーザに制限する必要があるかどうかを判断します。
- レポートの配布方法を特定します。たとえば、設定されたスケジュールで電子メールで送信するか、チームコンテンツフォルダ領域に含める必要がありますか？
- レポートの管理者を決定します。これは、設計の複雑さに影響する可能性があります。
- レポートのモックアップを作成します。

レポートの設計に関するヒント

レポートを設計するときは、いくつかのヒントが役立つことがあります。

- 現在のデータと履歴データのどちらを使用する必要があるかを判断します。

  ほとんどのレポートでは、Data Warehouse内の最新のデータについてのみレポートする必要があります。

- Data Warehouseでは、容量とパフォーマンスに関する履歴情報は提供されますが、インベントリに関する情報は提供されません。
- すべてのユーザにすべてのデータが表示されますが、データを特定のユーザに制限しなければならない場合もあります。

  ユーザごとに情報を分割するには、レポートを作成し、レポートにアクセス権限を設定します。

Reportingデータモデル

企業は、検出されてOnCommand Insight データウェアハウスに格納されるデータを活用できます。OnCommand Insight データウェアハウスは、複数の情報ソースのデータを格納して共通の多次元データモデルに変換する一元化されたリポジトリで、クエリと分析を効率的に実行できます。

このリポジトリから、チャージバック、消費分析、予測などのカスタムレポートを生成できます。これらのレポートには、回答 で次のような情報が含まれます。

- 所有しているインベントリ
- インベントリの場所
- アセットの使用者

- ビジネスユニットに割り当てられているストレージのチャージバック
- スイッチポートにはどの程度のヘッドルームがありますか。
- ストレージ容量の追加購入が必要になるまでの期間
- ビジネスユニットが適切なストレージ階層に配置されているか。
- 1 カ月、 1 四半期、 1 年のストレージ割り当ての変化

OnCommand Insight Reportingに付属のデータモデルを使用して、レポートオーサリングツールを使用してレポートを設計およびスケジュールできます。

データモデルの概要

OnCommand Insight には、レポート開発で使用する複数のデータモデルが用意されています。各データモデルは、クエリや検索ができるようにデータを集約したものです。たとえば、キャパシティプランニングに関するレポートでは、Capacityデータモデルを使用します。

OnCommand Insight エンタープライズレポートデータモデルは、データ要素とデータ要素間のインタラクティブな関係を提供し、データのビジネスビューを提供します。これらのデータ要素と関係を使用して、ネットアップが推奨するIBM Cognos Analyticsレポート生成ツールを使用してレポートを作成できます。

OnCommand Insight には、独自のSQLクエリの開発に使用できるデータマートも用意されています。これらのSQLクエリデータマートとレポートに使用されるデータモデルには違いがあります。個 々 のOnCommand Insight Reportingデータモデルは、データマートで提供される基盤となるOnCommand Insight データベーススキーマを使用します。ただし、データモデルは追加のテーブルを使用し、場合によってはテーブル内の新しい要素を使用します。たとえば、このデータモデルには、データベーススキーマおよびデータマートのCapacityファクトテーブルに基づいて、Storage CapacityデータモデルにMonthly Capacityファクトテーブルが含まれています。データモデルは、データベーススキーマテーブルの値をフィルタリングして、月の情報のみを表示します。

データマートで使用されるデータベーススキーマとデータモデルの違いを示すもう1つの例として、[Violation]テーブルと[Violation Type]列があります。データモデルは、データベース内のプログラムによって指定された値を、OnCommand Insight Web UIに表示されるテキストと一致するように変換します。

OnCommand Insight データモデル

OnCommand Insight には複数のデータモデルが用意されており、事前定義されたレポートを選択することも、独自のカスタムレポートを作成することもできます。

各データモデルにはシンプルなデータマートと高度なデータマートが含まれています。

- シンプルなデータマートを使用すると、よく使用されるデータ要素にすばやくアクセスできます。Data Warehouseデータの最新のSnapshotのみが含まれ、履歴データは含まれません。
- 高度なデータマートは、シンプルなデータマートから利用可能なすべての値と詳細を提供し、履歴データ値へのアクセスを含みます。
- 容量データモデル

  ストレージ容量、ファイルシステム利用率、内部ボリュームの容量、ポート容量、 qtree 容量に関する回答の情報を表示します。 仮想マシン（ VM ）の容量が必要です。Capacity データモデルは、複数の容量

データモデルをまとめたコンテナです。このデータモデルを使用して、さまざまなタイプの情報を収集したレポートを作成できます。

- ストレージおよびストレージプール容量データモデル

  ストレージとストレージプール、および物理ストレージプールと仮想ストレージプールの両方のデータについて、ストレージ容量のリソース計画に関する回答の情報を確認できます。このシンプルなデータモデルを使用すると、フロアの容量に関連する回答の質問や、一定期間にわたる階層別およびデータセンター別のストレージプールの使用容量に関する情報を確認できます。

  容量に関するレポートを初めて作成する場合は、シンプルでターゲットが限定されたこのデータモデルを使用してください。このデータモデルを使用すると、次のような回答の情報を確認できます。

  - 物理ストレージの容量しきい値の 80% に達するまでの予測日
  - 特定の階層のアレイ上の物理ストレージ容量
  - メーカー、ファミリー、およびデータセンター別のストレージ容量
  - すべての階層のアレイにおけるストレージ利用率のトレンド
  - 利用率が最も高い上位 10 個のストレージシステム
  - ストレージプールのストレージ利用率のトレンド
  - 割り当て済みの容量
  - 割り当て可能な容量

- * File System Utilizationデータモデル*

  ファイルシステム利用率に関する情報を回答 で確認できます。このデータモデルを使用すると、ファイルシステムレベルでホスト別の容量利用率を確認できます。管理者は、ファイルシステムごとの割り当て済み容量と使用済み容量、およびファイルシステムタイプを確認したり、ファイルシステムタイプ別のトレンドを特定したりできます。このデータモデルを使用すると、次の情報を回答で確認できます。

  - ファイルシステムのサイズ
  - データはどこに保管され、どのようにアクセスされるか（ローカル、 SAN など）。
  - ファイルシステム容量の過去の傾向は何ですか。そして、これに基づいて、将来のニーズにどのような対応を期待できますか？

- 内部ボリューム容量データモデル

  一定期間にわたる内部ボリュームの使用済み容量、割り当て済みの容量、および使用容量に関する回答の情報を確認できます。

  - 利用率が事前に定義されたしきい値を上回っている内部ボリューム
  - トレンドに基づいて容量が不足する危険がある内部ボリュームはどれですか？
  - 内部ボリュームの使用済み容量と割り当て済み容量の割合

- * Port Capacityデータモデル*

  一定期間にわたるスイッチポートの接続、ポートのステータス、およびポートの速度に関する回答の情報を確認できます。次のような回答 の質問は、新しいスイッチの購入を計画するのに役立ちます。

- （データセンター、スイッチベンダー、ポート速度に応じて）リソース（ポート）の可用性を予測するポート消費予測を作成するには、どうすればよいですか。
- 容量不足になり、データ速度、データセンター、ベンダー、ホストポートとストレージポートの数が提供される可能性があるポートはどれですか？
- 一定期間にわたるスイッチポートの容量のトレンド
- ポートの速度
- 必要なポート容量のタイプ、および特定のポートタイプまたはベンダーで容量が不足しそうな組織
- いつまでに容量を購入して利用可能にするべきか

◦ * Qtree Capacityデータモデル*

一定期間にわたる qtree 利用率のトレンドを（使用済み容量と割り当て済み容量の比較などのデータを使用して）確認できます。さまざまなディメンション（ビジネスエンティティ、アプリケーション、階層、サービスレベルなど）別に情報を表示できます。このデータモデルを使用すると、次の情報を回答で確認できます。

- アプリケーションまたはビジネスエンティティごとに設定されている制限値に対する qtree の使用済み容量
- キャパシティプランニングを実施するための使用済み容量と空き容量のトレンド
- 使用容量が最も多いビジネスエンティティ
- 使用容量が最も多いアプリケーション

◦ * VM Capacityデータモデル*

仮想環境とその使用容量を報告できます。このデータモデルを使用すると、 VM とデータストアの一定期間にわたる使用容量の変化を報告できます。このデータモデルは、シンプロビジョニングと仮想マシンのチャージバックデータも提供します。

- VM とデータストアにプロビジョニングされた容量に基づいて容量のチャージバックを決定する方法
- VM で使用されていない容量、およびそのうちの空き容量、孤立している容量、その他の状態の容量
- 消費傾向に基づいて何を購入する必要がありますか？
- ストレージのシンプロビジョニングと重複排除のテクノロジを使用することで達成される Storage Efficiency による削減効果VM Capacity データモデルの容量は、仮想ディスク（ VMDK ）から取得されます。つまり、 VM Capacity データモデルを使用した場合の VM のプロビジョニング済みサイズは、その VM の仮想ディスクのサイズです。これは、OnCommand Insight の[Virtual Machines]ビューに表示されるプロビジョニング済み容量とは異なります。この容量には、VM自体のプロビジョニング済みサイズが表示されます。

◦ ボリューム容量データモデル

環境内のボリュームのすべての要素を分析し、ベンダー、モデル、階層、サービスレベル、およびデータセンター別にデータを整理できます。孤立ボリューム、未使用ボリューム、および保護ボリューム（レプリケーションに使用）に関連する容量を表示できます。また、さまざまなボリュームテクノロジ（ iSCSI または FC ）を表示したり、アレイの仮想化の問題について仮想ボリュームと非仮想ボリュームを比較したりすることもできます。このデータモデルを使用すると、次のような回答の情報を確認できます。

        - 利用率が事前に定義されたしきい値を上回っているボリューム
        - 孤立ボリューム容量のデータセンターにおけるトレンド
        - 仮想化またはシンプロビジョニングされているデータセンター容量
        - レプリケーション用に予約する必要があるデータセンター容量
- チャージバックデータモデル

  ストレージリソース（ボリューム、内部ボリューム、 qtree ）の使用済み容量と割り当て済み容量に関する回答の情報を確認できます。このデータモデルは、ストレージ容量のチャージバックとアカウンタビリティの情報をホスト、アプリケーション、およびビジネスエンティティ別に提供します。現在のデータと履歴データの両方が含まれます。レポートデータは、サービスレベルとストレージ階層で分類できます。

  このデータモデルを使用すると、ビジネスエンティティで使用されている容量を検出することでチャージバックレポートを生成できます。このデータモデルでは、複数のプロトコル（ NAS 、 SAN 、 FC 、 iSCSI など）についてのレポートをまとめて作成できます。

  - 内部ボリュームがないストレージの場合、チャージバックレポートにはボリューム別のチャージバックが表示されます。
  - 内部ボリュームがあるストレージの場合：
    - ビジネスエンティティがボリュームに割り当てられている場合、チャージバックレポートにはボリューム別のチャージバックが表示されます。
    - ビジネスエンティティがボリュームではなく qtree に割り当てられている場合、チャージバックレポートには qtree 別のチャージバックが表示されます。
    - ビジネスエンティティがボリュームにも qtree にも割り当てられていない場合、チャージバックレポートには内部ボリュームが表示されます。
    - ボリューム別、 qtree 別、または内部ボリューム別のチャージバックを表示するかどうかは内部ボリュームごとに決定されるため、同じストレージプール内の別々の内部ボリュームで異なるレベルのチャージバックが表示される可能性があります。容量ファクトはデフォルトの期間後にパージされます。詳細については、 Data Warehouse のプロセスを参照してください。

    Chargebackデータモデルを使用するレポートには、Storage Capacityデータモデルを使用するレポートと異なる値が表示されることがあります。

  - ネットアップストレージシステムでないストレージアレイの場合、両方のデータモデルのデータは同じです。
  - NetApp および Celerra のストレージシステムの場合、 Chargeback データモデルは（ボリューム、内部ボリューム、または qtree の） 1 つのレイヤを使用して料金を請求し、 Storage Capacity データモデルは（ボリュームと内部ボリュームの）複数のレイヤを使用して料金を加算します。
- 在庫データモデル

  ホスト、ストレージシステム、スイッチ、ディスク、テープなどのインベントリリソースに関する回答の質問にお答えします。 qtree 、クォータ、仮想マシンとサーバ、および汎用デバイスです。Inventory データモデルには、レプリケーション、 FC パス、 iSCSI パス、 NFS パス、および違反に関する情報を表示するサブマートが複数含まれています。Inventory データモデルには履歴データは含まれません。このデータマートを使用して回答 を実行できる質問には、次のようなものがあります。

  - 所有しているアセットとその場所
  - アセットの使用者

- 所有しているデバイスの種類と、デバイスのコンポーネントを教えてください。
- OS あたりのホスト数とホスト上のポート数
- 各データセンターには、ベンダーごとにどのようなストレージアレイがありますか。
- 各データセンターには、ベンダーあたりいくつのスイッチがありますか。
- ライセンスが設定されていないポートの数
- どのベンダーのテープを使用していますか。また、各テープにはポートがいくつありますか。
- レポートの作成を開始する前に、すべての汎用デバイスが識別されていますか。
- ホストとストレージボリュームまたはテープ間のパス
- 汎用デバイスとストレージボリュームまたはテープ間のパス
- データセンターごとの各タイプの違反数
- レプリケートされた各ボリュームの、ソースボリュームとターゲットボリューム
- Fibre Channel ホストの HBA とスイッチとの間にファームウェアの互換性の問題またはポート速度の不一致があるか

- パフォーマンスデータモデル

  ボリューム、アプリケーションボリューム、内部ボリューム、スイッチ、アプリケーションのパフォーマンスに関する回答の質問に回答できます。 VM 、 VMDK 、 ESX と VM 、ホスト、およびアプリケーションノードです。このデータモデルを使用すると、回答に複数のタイプのパフォーマンス管理に関する情報を記載したレポートを作成できます。

  - 特定の期間に使用またはアクセスされていないボリュームまたは内部ボリューム
  - アプリケーション用のストレージ（未使用）に関する潜在的な構成ミスを特定できるか？
  - アプリケーションの全体的なアクセス動作パターン
  - 特定のアプリケーションに階層型ボリュームが適切に割り当てられているか
  - アプリケーションのパフォーマンスに影響を与えずに、実行中のアプリケーションに安価なストレージを使用できますか？
  - 現在設定されているストレージへのアクセスが多いアプリケーションスイッチパフォーマンスのテーブルを使用すると、次の情報を取得できます。
  - 接続されたポート経由でホストトラフィックが分散されているか。
  - 多数のエラーが発生しているスイッチまたはポート
  - ポートパフォーマンスに基づいて最も使用されているスイッチはどれですか？
  - 使用率の低いスイッチのうち、ポートのパフォーマンスに基づくものは何ですか。
  - ポートのパフォーマンスに基づくホストのトレンド分析スループット
  - 特定の 1 つのホスト、ストレージシステム、テープ、またはスイッチの過去 X 日間のパフォーマンス利用率
  - 特定のスイッチでトラフィックを生成しているデバイス（たとえば、利用率の高いスイッチを使用しているデバイス）
  - 環境内の特定のビジネスユニットのスループットディスクパフォーマンスのテーブルを使用すると、次の情報を取得できます。

- ディスクのパフォーマンスデータに基づく、指定されたストレージプールのスループット
- 最も使用されているストレージプール
- 特定のストレージのディスク利用率の平均
- ディスクパフォーマンスデータに基づくストレージシステムまたはストレージプールの使用状況のトレンド
- 特定のストレージプールのディスク使用率のトレンドVM と VMDK のパフォーマンスのテーブルを使用すると、次の情報を取得できます。
- 仮想環境のパフォーマンスが最適化されているか
- 最も高いワークロードを報告している VMDK
- 異なるデータストアにマッピングされた VM から報告されたパフォーマンスを使用して、階層化の再決定を行うにはどうすればよいですか。パフォーマンスデータモデルには、階層の妥当性、アプリケーション用のストレージの構成ミス、およびボリュームと内部ボリュームの最終アクセス時刻を特定するための情報が含まれています。このデータモデルは、応答時間、 IOPS 、スループット、保留中の書き込み数、アクセスステータスなどのデータを提供します。

- * Storage Efficiencyデータモデル*

  一定期間にわたるストレージの削減率と可能性を追跡できます。このデータモデルには、プロビジョニング済み容量のデータだけでなく、使用済みまたは消費済みの容量（物理的な測定値）も格納されます。たとえば、シンプロビジョニングが有効な場合、OnCommand Insight はデバイスから取得された容量を示します。また、このモデルを使用して、重複排除が有効な場合の効率を判断することもできます。Storage Efficiency データマートを使用すると、回答に関するさまざまな情報を確認できます。

  - シンプロビジョニングと重複排除を実装した場合の Storage Efficiency による削減効果
  - データセンター全体でのストレージ削減量
  - 過去の容量のトレンドに基づいて、ストレージを追加購入する必要があるのはいつですか？
  - シンプロビジョニングや重複排除などのテクノロジを有効にした場合の容量の増加
  - ストレージ容量にリスクがありますか？

データモデルのファクトテーブルとディメンションテーブル

各データモデルには、ファクトテーブルとディメンションテーブルの両方が含まれています。

- ファクトテーブル：量、物理容量、使用可能な容量など、測定されたデータが含まれます。ディメンションテーブルへの外部キーが含まれます。
- ディメンションテーブル：データセンターやビジネスユニットなど、ファクトに関する説明が含まれます。ディメンションはデータを分類する構造であり、多くの場合、複数の階層で構成されます。ディメンション属性は、ディメンション値の説明に役立ちます。

（レポート内の列に表示される）複数のディメンション属性を使用して、データモデルに含まれる各ディメンションのデータをアクセスするレポートを作成します。

レポートの作成に使用されるすべてのデータ要素の説明については、「データ用語集」を参照してください。

データモデル要素で使用される色

データモデル要素の色には意味があります。

- 黄色のアセット：測定値を表します。
- 黄色以外のアセット：属性を表します。これらの値は集計されません。

1 つのレポートで複数のデータモデルを使用する

通常は、レポートごとに 1 つのデータモデルを使用します。ただし、複数のデータモデルのデータを結合したレポートを作成することができます。

複数のデータモデルのデータを結合したレポートを作成するには、ベースとして使用するデータモデルを 1 つ選択し、追加のデータマートからデータを収集する SQL クエリを作成します。SQL の Join 機能を使用して、複数のクエリのデータを 1 つのクエリに結合し、レポートの作成に使用できます。

たとえば、各ストレージアレイの現在の容量を確認し、アレイのカスタムアノテーションを取得するとします。このレポートは、 Storage Capacity データモデルを使用して作成できます。Current Capacity テーブルとディメンションテーブルの要素を使用し、別途 SQL クエリを追加して Inventory データモデルのアノテーション情報にアクセスします。最後に、ストレージ名と結合条件を使用して Inventory のストレージデータを Storage Dimension テーブルにリンクして、データを結合します。

よく寄せられる質問

一般的な質問

このFAQでは、OnCommand Insight に関する一般的な質問に回答します。

OnCommand Insight （OCI）が導入されたのはいつですか。

OCIは、業界で最も成熟したインフラ監視製品の1つであり、10年以上にわたって活発な開発が行われている。以前はOnaroまたはSANscreen と呼ばれていたSANscreen の名称は、OnCommand 製品スイートに参加したときに変更され、現在はOnCommand Insight 、より一般的にはInsightまたはOCIと呼ばれています。

OCIの環境への導入にはどれくらいの時間がかかりますか。

OCIは単にソフトウェアをダウンロードするだけです。ソフトウェアは、 2 台の専用の仮想サーバまたは物理サーバにインストールされます。一般的なインストールはわずか 2 時間で完了し、インベントリ、容量、パフォーマンスのデータの提供はほぼ即座に開始されます。パフォーマンスとベストプラクティスのポリシー、ユーザアノテーション、およびコスト情報の設定を追加する場合は、計画についてさらに検討する必要があります。

OCIにはエージェント、コレクタ、プローブが必要ですか。

OCIは100%エージェントレスで、エージェント、タップ、プローブを使用する必要はありません。すべてのデバイス検出は読み取り専用で、アウトオブバンドおよび IP 経由で実行されます。

OCIはどのようにしてデバイスを検出し、接続しますか？

OCIのセットアップでは、データセンター環境にすでに存在していることが多いネイティブのAPIとプロトコルを利用するため、エージェントやプローブは必要ありません。SSH 、 HTTP 、 SMIS 、および CLI は、ほんの一例です。デバイスエレメントマネージャ（EMCのUnisphereなど）がすでに存在する場合、OCIはエレメントマネージャと通信して既存の環境データを取得します。ほとんどのデバイス検出では、 IP アドレスと読み取り専用のユーザ名とパスワードのみが必要です。これらのデバイス検出は、OCIのVMwareデータソースのように「1対多」にすることができます。VMware vCenterを検出することで、OCIはそのすべてのESXiホストと関連するVMを1つのIPアドレスとクレデンシャルで検出します。

OCIにはプロフェッショナルサービスが必要ですか。それは利用でき、それらは何を提供するか。

中規模の環境の場合は、導入、設定、統合のほか、さまざまなカスタムレポートやデータ検証の機能を提供するプロフェッショナルサービスを推奨します。OCIチームとアカウントエンゲージメントマネージャーと簡単に話し合うことで、パートナー様に最もメリットがあるサービスを見極めることができます。

OCIは、どのくらいの頻度で新機能や改善点の更新をリリースしますか？

製品の更新とサービスパックは、OCIの複数のバージョンで利用できます。メジャーリリースまたはマイナーリリースは、通常、数か月ごとに提供され、新しいデバイスサポートやファームウェアのリリース頻度が高くなっています。どちらも support.netapp.com のダウンロードサイトから入手できます。新しいディスクモデルなど、メーカーから頻繁にリリースされる一部の更新は、OCIソフトウェアに自動的にプッシュされます。また、OCIデータソースデバイス収集は、開発の修正や更新の直後にオンサイトでパッチを適用できます。

OCIの管理チームは、新しいデータソースの要求にどのように優先順位を付けますか。

OCIの製品管理チームは、すべてのお客様の機能強化と相互運用性機能に関する要望（IFR）を積極的に追跡している。各リクエストの詳細は、実現可能性について評価され、お客様のニーズと戦略的なビジネスへの全体的な影響に基づいて優先順位が付けられます。リクエストはいったん承認されると、対応レベルに基づいてサイズが決定され、将来の開発に向けてスケジュールされます。OCIの開発プロセスは即応性に優れているため、定期的にスケジュールされたリリースサイクルの外で新しいデータソースを利用できるようになります。ネットアップのアカウント担当者は、お客様からのお問い合わせや、新しいリクエストの送信にご協力いただけます。データソースにオンサイトでパッチを適用できるため、OCIをアップグレードする必要はありません。

私の会社は Linux で完全に動いています。OCIはLinuxでも動作しますか。

はい。OCIでは、複数のLinuxとWindowsをサポートしています。Cognos（OCIとData Warehouseで使用されるIBMのレポート作成ツール）はWindowsでのみサポートされるため、レポート作成にOCIを使用する場合はWindowsサーバでレポート作成ツールを実行する必要があります。『OCIインストールガイド』には、各OCIコンポーネントのサーバ要件とサポートされるオペレーティングシステムが記載されています。

OCIは、インターネットアクセスのないセキュアな環境に適していますか。

はい。OCIは、Fortune 500企業上位10社に加え、世界中の大手銀行、医療機関、研究機関、政府機関で使用されています。OCIは、米軍共通アクセスカード（CAC）をサポートし、地理的に分散した環境やファイアウォールが厳しい環境向けのソリューションを提供している。

OnCommand Unified Manager （ OCUM ）が clustered 解決策の管理 であることを私は聞き続けています。OCIを使用する理由を教えてください。

OnCommand Unified Managerはストレージアレイの「デバイス管理」レイヤで機能し、clustered Data ONTAP （cDOT）アレイとそのクラスタインターコネクトについて、インシデントベースやイベントベースで詳細に分析します。OCIでは、7-Mode、clustered Data ONTAP 、その他の他社製アレイで構成されるオンプレミス環境とグローバルに分散した環境を包括的に把握できます。仮想マシンからスピンドルに至るまでエンドツーエンドの可視性を提供することで、容量、パフォーマンス、コストモデリングのトレンドと予測の履歴を把握し、データセンター管理に対するプロアクティブなサービス品質アプローチを促進できます。

Automation Storefrontに記載されているOnCommand Insight セカンダリETLとは何ですか。

一部のOnCommand Insight オートメーションStorefrontレポートのダウンロードで参照されている「セカンダリETL」要件は、OnCommand Insight データウェアハウスにデータを取り込むために、キャプチャされたデータの追加抽出、変換、読み込み(ETL)を呼び出すために使用される、開発されたプロフェッショナルサービスの実装を指します。

セカンダリ ETL プロセスの主な目的は、より複雑なレポートの生成を高速化したり、毎日実行するようにスケジュールしたりできるように、「バッチ」データをプリフェッチすることです。

このセカンダリETLは、OnCommand Insight データウェアハウス管理ガイドで詳しく説明されている推奨される「1日に1回」ETLに追加されています。

ネットアッププロフェッショナルサービスは、既存のOnCommand Insight レポートスケジュール、自動バックアップ、拡張性、その他のシステムパフォーマンスアクティビティへの影響を回避するために、セカンダリETLスクリプトを設定することを認定されています。ETL スクリプトの作成やデータ検証のニーズについては、ネットアップの営業担当者にお問い合わせのうえ、ネットアップのプロフェッショナルサービスがどのよ

うにサポートされるかをご相談ください。追加情報

OnCommand Insight ライセンス

OnCommand Insight のライセンスに関する一般的な質問と回答が表示されます。

OCIライセンスの概要

OCIのライセンスは容量単位で提供される。お客様は、有効にするモジュールごとにライセンスを購入する必要があります。

- Discover *はAssure、Perform、Planの前提条件であり、単独では提供されません。Discoverのライセンスは、管理対象容量（TB）単位で付与されます。

*Assure *は、管理容量（FC、NAS、iSCSI、FCoEのすべてのストレージインフラストラクチャに対する単一の料金単位）でライセンスされます。

- Perform *には、管理対象容量（TB）単位でライセンスが付与されます。

*プラン*には、管理対象容量（TB）単位でライセンスが付与されます。

「管理容量」は、フォーマット前の物理ディスク、仮想ディスク、およびテープのraw容量として定義されます。これは、オンプレミスとクラウドの両方でInsightによって検出されたすべてのストレージに当てはまります。

ほとんどのデータソースでは、ディスクの物理容量（2進法）が使用されます。スペアディスク、未割り当てディスク、RAIDディスクなど、ディスクロールは考慮されません。

Insightのライセンスには、*恒久ライセンス*と*サブスクリプション*の2種類があります。

*恒久ライセンス*適用されるライセンス条件に従って取得したソフトウェアの特定のバージョン/リリースを無期限に使用することができます。ソフトウェアサポートプラン（SSP）を購入されたお客様の場合、ネットアップは、サポートサービス条件に従って更新が利用可能になった時点で、NetApp Support Site を通じて一般提供されているソフトウェアアップデートへのアクセスを提供します。ネットアップでは、ネットアップテクニカルサポートセンターで決定された特別なパッチも提供しています。

*サブスクリプション*は、以下の権利を付与するソフトウェアの固定ライセンスです。

- オンプレミスのソフトウェアは、適用されるライセンス条件に従い、限られた期間（通常は12カ月）のみ使用してください
- 期間中、ソフトウェアサポート（旧称SSP）を受ける
- ライセンス契約者は、事実上、市販されている最新のバージョン、リリース、またはアップデートを使用することができます。ただし、ソフトウェアのサポートを受けることはできません

各固定期間（通常は12カ月）の終了時に、追加の固定期間（通常は12カ月）にライセンスを更新できます。ライセンスが更新されない場合、ライセンシーはソフトウェアを使用する権利を失い、SSPの特典を受ける権利を失い、ライセンシーはソフトウェアのすべてのコピーを破棄する必要があります。

OCIライセンスモジュールの詳細については、こちらをご覧ください

OCIには、今日のデータセンター環境のニーズを満たすために4つのコアライセンスモジュールが用意されている。これらのモジュールは、* Discover、Perform、Assure、Plan *です。Discoverは基本モジュールであり、その他のすべてのモジュール購入に必要です。

[Discover]*モジュールを使用すると、OCIでデータセンター内のアセットを特定し、デバイスサービスパスを動的にマッピングできます。容量、ベンダー情報、モデル、ファームウェア、シリアル番号などの情報が提供されます。

- perform *は、OCIのパフォーマンス収集モジュールです。Performは、IOPS、スループット、レイテンシ、CPUとメモリの情報のほか、その他の分析情報を収集します。

*Assure *は'ファイバ・チャネル環境と効率化テクノロジーに重点を置いていますファイバチャネルおよびiSCSI環境におけるリスクの特定と管理に役立ちます。Assureは、マスキング、マッピング、およびアラートに関する情報や、ファブリックの冗長性、スイッチホップ、ファンアウト比率、シンプロビジョニングなどの効率化に関するベストプラクティスポリシーも提供します。

*プラン*では、オンプレミスのハイブリッド環境と世界中に分散したデータセンター環境において、コンピューティング、ファブリック、各種ストレージ（clustered Data ONTAP、7-Mode、サードパーティ）のトレンドを特定して予測することができます。保持期間が長くなります。Data Warehouseは、レポートオーサリングを可能にする組み込みのインテリジェンスで構成されており、エンタープライズ共有ストレージ環境で指標が二重にカウントされることを回避します。「すぐに使用できる」製品化されたレポートを生成してスケジュール設定することも、統合されたレポートオーサリングツール「ドラッグアンドドロップ」を使用して独自のレポートを作成することもできます。

構成とサポートされているデバイス

このFAQでは、OnCommand Insight 構成とサポートされているデバイスに関する一般的な質問に回答します。

OCIによって環境が変更されるか。

いいえOCIは、環境に関する情報を収集する読み取り専用のツールです。OCIでアセットや設定を変更することはありません。

OCIでデバイスに必要な権限レベルのアクセス権を教えてください。

デバイスがサポートしている場合、ほとんどの場合、読み取り専用アクセスが必要です。読み取り専用アクセスを許可しないソリューションもあるため、適切な昇格されたアクセス許可が必要になります。

OCIはどのくらいの頻度で情報を収集しますか。

OCIでは通常、5分ごとにパフォーマンスデータが収集され、論理構造と物理構造の検出は0.5時間ごとに行われますOCIでは、推奨されるベストプラクティスと拡張性に従ってデフォルトのポーリング間隔が設定されますが、それらの間隔をユーザが完全に制御することはできます。

OCIが環境に与える影響

OCIのエージェントレス、アウトオブバンド、パッシブなIP通信は、セットアップ、メンテナンス、データセ

ンターのエコシステムへの影響を最小限に抑えるのに役立つ。OCIのパフォーマンス開発チームは、パフォーマンス自体の監視アクティビティにおいて、データセンターのパフォーマンスへの影響を最小限に抑えるための優れた対策を講じている。通常の運用環境では影響はごくわずかで、利用率の高いテクノロジプラットフォームやパフォーマンスの低いテクノロジプラットフォームで、リラックスした状態や強化が可能です。詳細については、『OnCommand Insight インストールガイド』を参照してください。

OCIですべてのホスト**/ VM**を一覧表示するにはどうすればよいですか。

OCIにはウィジェットやクエリリスト機能が補完されており、データセンターアセットのインベントリ形式の一覧を表示できます。スピンドルとその間に配置されたさまざまな構成要素を仮想マシンで一覧表示することができ、クエリ、ウィジェット、ダッシュボード、データウェアハウスレポートにアクセスできます。RESTful API からアクセスできます。

OCIでは、関連する非ハイパーバイザーホスト（物理サーバ）に対して同じタイプのサポートを提供していますか。

VMwareなどのハイパーバイザーは、ESXiホストとそれに関連する仮想マシン（VM）に関する詳細情報を提供します。物理サーバについては、ホストHBAまでの指標が収集されます。OCIでは、特許申請中のテクノロジを使用して物理サーバを検出する独自の方法を採用しています。ストレージやスイッチが検出されると、物理サーバのホスト名がファブリックエイリアス情報に含まれます。OCIによってこれらのホスト名が選択され、DNSで一致すると、ホストが自動的にOCIに追加されます。この方法により、手動での入力更新やツールインベントリのメンテナンスが必要なくなります。

異機種混在環境全体で、**OCI**で提供されるデバイスのメトリック深度（パリティ）は同じですか。

サードパーティのプラットフォームとベンダーのテクノロジ全体で、標準化、共通性、および命名方法にはさまざまなレベルがあります。OCIでは、容量とパフォーマンスの情報を一貫したフレームワークに標準化しようとします。容量やパフォーマンスの一部の指標は、 IOPS 、レイテンシ、物理容量など、デバイスのカウンタからネイティブに提供されます。カウンタが指定されていない場合、OCIは値を要約しようとします（たとえば、基盤となるボリュームのIOPSや容量の合計など）。どちらも使用できない場合は、さまざまな計算アルゴリズムを使用して指標の値を取得しようとします。OCIでは、一般的なSNMP統合機能を使用して、現在OCIで収集されていない追加の指標を組み込むことができます。

OCIでは**Fibre Channel**スイッチはサポートされていますか。

はい。OCIでは、ストレージ資産からデータを収集するだけでなく、環境内のCisco、Brocade、QLogicスイッチからインベントリとパフォーマンスのデータも取得します。

インフラ全体のトポロジビューは使用できますか。**OCI**に「エンドツーエンドの可視性」が表示されるか。

はい。OCIでは、論理構造と物理構造を動的に検出してマッピングすることで、コンピューティング、ファブリック、仮想化、バックエンドストレージのトポロジビューをエンドツーエンドでインタラクティブに表示できます。トポロジアイコンを使用すると、影響を受けるリソースへのクイック起動ナビゲーションが可能になり、共有ストレージ環境でのワークロードや違反の特定に役立ちます。

拡張性と使いやすさ

このFAQでは、OnCommand Insight の拡張性と使いやすさに関する一般的な質問に回答

します。

OCIの拡張性

OCIは、相互運用性と最小限の設置面積で取得できる資産の数の点で業界をリードしています。OCIの中核には、仮想サーバまたは物理サーバが2台必要です。1台はデータセンターのすべての資産を検出する運用サーバ用、もう1台は長期的な履歴レポートを作成するための統合データウェアハウス用です。OCIのエンタープライズ環境では、数百のアレイ、数万の仮想マシン、10万のファイバチャネルパス、10万以上のファイバチャネルポートがすべて単一のサーバインスタンスでサポートされています。

OCIアプリケーションの管理には何人の担当者が必要ですか。

OCIでは、1人のユーザが管理できます。一方、OCIには、ビジネス環境内の複数の担当者が使用できる機能があり、それぞれに役割が異なり、レポート、トラブルシューティング、分析のニーズも異なります。設定の問題を表示するヘルスメニューや通知メニューから、ファブリックに接続されている物理ホストの自動検出まで、ツールのメンテナンスを最小限に抑えるためにあらゆる努力が払われています。柔軟なアノテーションにより、あらゆるタイプのユーザのエコシステムデータにビジネスコンテキストが反映されます。OCIでは、ストレージ管理者、ファブリック管理者、仮想化管理者からキャパシティプランニング担当者、ビジネスアナリスト、エグゼクティブまで、ビジネスサイロやテクノロジ全体で情報を共有できます。

OCIはカスタムレポートをサポートしていますか。

はい。OCIでは、IBM Cognosビジネスインテリジェンスツールを使用してレポートを作成できます。このツールを使用すると、OCIのデータウェアハウスで収集されたデータを基に、完全にカスタマイズされた独自のレポートを作成できます。

カスタムレポートは簡単に作成できますか？

OCIのレポート機能は、初心者と上級者の両方に対応しています。OCIには、「ドラッグアンドドロップ」のレポートオーサリング機能や、より高度なユーザサービスやプロフェッショナルサービス契約向けのSQLクエリベースのレポート作成機能など、さまざまなレポートオーサリング機能が用意されています。OCIに組み込まれたビジネスインテリジェンス解決策 （IBM Cognos）は、容量の二重カウントなどのよくある間違いを回避する。すぐに使えるレポート、ウィジェット、クエリ、ダッシュボードを追加することで、誰もが必要とするレポートを作成できます。

レポートテンプレートはOCIコミュニティストアからダウンロードすることもできます。

OCIでは、シンプルな「信号機」でパフォーマンスと可用性を表示できますか。

はい。OCI Data WarehouseおよびReportingでは、値が赤/黄/緑の「条件付きスタイル」など、色が強化されたレポートを作成できます。レポートに色付きのフォントや背景を生成することは、エンドユーザとプロフェッショナルサービスの両方で実装できます。OCIウィジェットライブラリを使用すると、ビジネス固有のパフォーマンス指標をダッシュボードに表示できます。

パフォーマンスのトラブルシューティング

このFAQでは、OnCommand Insight のパフォーマンスのトラブルシューティングに関する一般的な質問に回答します。

環境内のすべての **Greedy** リソースのリストを作成するにはどうすればよいですか。

OCIの相関分析は、指定されたサービスパスについて、システムリソースを大量に消費しているリソースやパフォーマンスが低下しているリソースを特定するのに役立つ。相関フィーチャーの生成された解析は ' 各オブジェクトを表示しながらリアルタイムで実行されます提供される分析によって、パフォーマンスの問題のトラブルシューティングやルート原因の特定に必要な時間が大幅に短縮されます。定義されたパフォーマンスポリシーで発生した違反の調査は、 Greedy リソースやパフォーマンスが低下したリソースを検出するためのエントリポイントの 1 つです。最新のクエリ機能を使用しているウィジェットとダッシュボードのどちらも、想定 IOPS （ Greedy ）、利用率、レイテンシを超えるリソースのフィルタリング、ソート、可視化に役立ちます。

OCIでは、パフォーマンスの問題を**1**箇所で診断できますか。

はい。OCIでのパフォーマンストラブルシューティングには、さまざまな方法があります。OCIには、さまざまなアラート方法があります。SNMP 、 syslog 、 E メールで送信されるアラートがよく使用されます。Eメールで送信されたアラートを使用すると、影響を受けるリソースをすばやくクリックしてOCI内で起動できます。グローバル検索ウィンドウでは、リソース名を入力するだけで状況の分析を開始できます。

OCIのViolation Dashboardでは、イベント数、期間、時刻に基づいて作業の優先順位を設定できます。アラートの種類には、レイテンシ、IOPS、利用率、重大度、ビジネスユニット、関連するアプリケーションなどがあります。

OCIの相関分析は、影響を受けるリソースに関連付けられているオブジェクトを比較し、IOPS、レイテンシ、利用率、CPU、BBクレジットへの影響を判定するのに役立つ。

OCIのクエリテクノロジとウィジェットダッシュボードを使用すると、データセンター内の問題領域を対象に、詳細な情報を体系的に表示できます。

OCIは**7-Mode**から**clustered Data ONTAP**への移行に役立ちますか。

はい。OCIは、既存のワークロードのニーズや移行後の検証に非常に役立つ情報を提供します。今日のデータセンターの最新化におけるOCIの役割は、変更管理シミュレーション、移行前の最適化計画、適切なサービス階層の定義を可能にする。OCIでは、数回クリックするだけで、数千ものNFS共有やファイバチャネルパス全体のビジネスへの影響を簡単に収集し、関連付けることができます。OCIは、移行から機器更改まで、信頼性の高い適切なサイズの移行を実現し、計画外のサービス停止を軽減するための手段を提供します。

OCIのパフォーマンス監視の「実際の時間」はどのようなものですか。

OCIは、オンプレミスとハイブリッドクラウドの両方のデータセンター管理で*ほぼリアルタイム*とみなされます。データソースのポーリングをより頻繁に実行するように設定できますが、ほとんどのユーザは、ほとんどのデバイスでパフォーマンス収集間隔を5分未満に設定しても、分析上の大きなメリットは得られません。収集頻度を増やすと、管理対象のオブジェクトや実行される分析に不要な負荷がかかる可能性があります。もちろん、より詳細な収集が必要になる場合もあります。OCIでは、お客様のデータセンター環境のニーズに合わせて、デバイスインベントリやパフォーマンスのポーリング間隔を設定できるなど、柔軟性に優れています。

「合計」が「読み取り」と「書き込み」で異なるのはなぜですか？

場合によっては、カウンタの_Total_がそのカウンタの_reads_plus_writes_の合計と等しくないことがあります。この問題が発生する可能性があるのは、いくつかの場合です。

- IOPS *：読み取りと書き込みに加えて、ストレージアレイやその他のアセットで、ワークロードのデータ

フローに関係のない内部処理が処理されます。これらの処理は、「システム」、「メタデータ」、または単に「その他」の処理と呼ばれることもあり、Snapshot、重複排除、スペース再割り当てなどの内部プロセスに起因する可能性があります。このような場合、特定のアセットに対するシステム処理の量を調べるには、_Total_IOPSから_Read_and_Write_IOPSの合計を差し引きます。読み取り IOPS と書き込み IOPS の合計は、データフローに直接関連する合計 IOPS です。

レイテンシ：合計応答時間は時間で加重された平均であるため、処理の合計応答時間（レイテンシ）が書き込み応答時間より_less than _と報告されることがあります。I/O ワークロードは多くの場合書き込み処理よりも多くの読み取り処理で構成され、書き込みでは一般にレイテンシが大きくなります。たとえば、平均レイテンシが 5 ミリ秒で 10 個の読み取り処理を実行したワークロードの場合、平均レイテンシが 10 ミリ秒の 5 つの書き込み処理を実行した場合、合計加重平均レイテンシは、読み取り回数と平均読み取りレイテンシの合計で計算されます。 書き込み数に平均書き込みレイテンシを掛けた値を、 I/O 処理の合計数で割った値。たとえば、（ 10 × 5 + 5 × 10 ） / （ 10 + 5 ） = 6.33 ミリ秒のようになります。

オーバーコミットされたスペースで**OCI**と**OCUM**の値が異なるのはなぜですか？

OnCommand Unified Manager（OCUM）の「プロビジョニング」スペースの概念には、FlexVol（OnCommand Insight 内部ボリューム）が拡張される可能性がある自動拡張の制限が含まれている場合があります。OCIの「容量」には自動拡張時の制限は反映されません。そのため、自動拡張FlexVolがある環境では、OCUMでプロビジョニングされる合計容量がOCIストレージレベルの「オーバーコミット容量」の合計容量を超えます。FlexVolの容量と自動拡張時の容量の差がデルタになります。

環境の管理

このFAQでは、OnCommand Insight 環境の管理に関する一般的な質問に回答します。

OCIへのアクセスを特定のユーザに許可し、表示対象を特定のリソース（**SVM** と関連するボリューム、 **VM** 、サーバ）

OCIでは、ロールベースアクセスが可能です。たとえば、ReportingへのアクセスはOCIのData Warehouseレポートで制御されます。レポートは、スケジュール設定したり、 PDF 、 HTML 、 CSV 形式で電子メールで送信したり、ファイル共有や、表示する前にユーザーに認証を要求する URL に送信したりできます。ユーザベースのアクセス権は、 Admins 、 users 、および guests の形式で付与されます。Active Directory / LDAP のサポートも利用できます。

Insightを他のツールと統合する

このFAQでは、OnCommand Insight と他のツールの統合に関する一般的な質問に回答します。

OCIは他のツールと統合できますか。また、どのような統合ポイントを利用できますか。

はい。OCIは拡張可能な（オープンな）解決策 で、サードパーティのオーケストレーションシステム、ビジネス管理システム、変更管理システム、チケット発行システムとの統合や、カスタムのCMDB統合が可能です。OCIでは、完全に公開されたRESTful APIとオープンなMySQLデータベースのプライマリ統合ポイントにより、データを簡単かつ効果的に移動し、ユーザはデータにシームレスにアクセスできる。

InsightのSwaggerベースのAPIドキュメントは、製品の*（？）で確認できます。 [Help]>[REST API Documentation]*。

Insight BMC Connectorとは何ですか。

OnCommand Insight Connector for BMCは、OnCommand Insight Data Warehouse（DWH）とBMC Atrium Configuration Management Database（CMDB）を統合します。Insight Connector for BMCは、ネットワークストレージシステム（ストレージユニット、ホストストレージサービス、VSストレージサービス、VMストレージサービスなど）、およびそれらのデバイス（ホスト、ストレージスイッチ、VMストレージサービスなど）との関係について、保存されている物理データと論理データをマッピングします。 およびテープ）を使用し、それらを構成アイテムおよび関係としてBMC CMDBにインポートします。OnCommand Insight Connector for BMCの詳細については、NetApp Support Site を参照してください。

OCIはSCOMまたはVROPに対応していますか。

はい。OCIは多くのビジネス管理ソリューションを補完するものであり、データセンターのストレージ、コンピューティング、ハイパーバイザー、ファブリックに関する情報の信頼できるソースと考えられています。OCIをご利用のお客様は、OCIのRESTful APIと拡張可能なMySQLデータベースを活用して、BMC Remedy、ServiceNow、SCOM、Vrops、Splunkなどのさまざまなアプリケーションを いくつか例を挙げましょう。OCIでは、ほぼすべての記録ソースから情報をインポートしたり、収集した環境指標をサードパーティの一般的な監視、チケット処理、CMDB請求、オーケストレーションシステムに送信したりすることで、統合を拡張している。

OCIでは、すでに使用しているクラウドサービスや使用を検討しているクラウドサービスを使用できますか。

はい。OCIでは、従来のオンプレミス環境と即応性に優れたハイブリッドクラウド環境の両方を管理することで、ビジネスサービスのニーズに最も適した対費用効果の高いプラットフォームを見極めることができます。OCIは移行前と移行後の分析に活用できるため、クラウドに適したワークロードを特定するのに役立つ。適切なクラウドサービスを選択するには、過去の容量のトレンド分析、パフォーマンス、コストのすべてが必要です。OCIのI/O密度などの指標を活用したサービス設計ワークショップは、環境を最適化しているかどうか、クラウドが有効かどうかなど、回答 に関する質問にも役立ちます。OCIの対象範囲は、NetApp Private Storage、Cloud ONTAP 、Amazon S3、OpenStack KVMをサポートすることで拡大を続けている。OCIは、特に容量計画、パフォーマンス、サービス品質、チャージバックの可視化が重要な領域で、ネットアップのクラウド管理キャンペーンで引き続き重要な役割を果たしている。

OCIでインシデントをインシデント管理解決策 で開くことはできますか。

はい。OCIの違反イベントは、トラップまたはsyslogとしてSNMPでトリガーおよび送信できます。一部のイベントはRESTful APIでトリガーおよび送信できます。提供されたイベントに含まれる詳細は、多くのサードパーティのインシデント管理およびチケットソリューションで解釈できます。

ビジネスユニットや部門にリソースを割り当てることはできますか？

はい。OCIにはアノテーションと呼ばれるメタデータのタグ付け方法が組み込まれています。ビジネスユニット、基幹業務、テナント、プロジェクトをデータセンターリソースに割り当てることで、資産、キャパシティプランニング、トラブルシューティング、レポート作成に関するビジネスコンテキストをより充実させることができます。

OCIはWork Flow Automator（WFA）と連携できますか。

OCIの成功には、サードパーティのCMDB、課金、オーケストレーションテクノロジとの統合機能が重要な価値であり、WFAも例外ではありません。ネットアップのプロフェッショナルサービスは、現在WFAワークフローとOCIを使用して成功を収めている数多くの統合を実施してきました。OCI用のWFAコネクタはNetApp Automation Storefrontからダウンロードできます。

OCIでパフォーマンスデータを保持する期間

OCIサーバには、90日間のほぼリアルタイムのパフォーマンスと、現在の（ポイントインタイムの）インベントリ（論理構成要素と物理構成要素）が格納されます。

OCIのパフォーマンスポーリング間隔はユーザが設定できます。ほとんどのベンダーでは、ストレージパフォーマンスは通常5分ごとに設定されています。パフォーマンス/インベントリデータは、長期的な履歴レポートと予測レポートを作成するために、毎日OCI Data Warehouse（DWH）に送信されます。DWHでは、このデータが集計データ（毎時、日次、月次ロールアップデータ）に変換されます。ストレージ/コンピューティング/ファブリックの構成/マッピングに関する環境履歴の監視など、「変化」を追跡する機能には、現時点では制限は定義されていません。

Data Warehouseでは、データマートおよびデータの単位に基づいて履歴データが保持されます。

パフォーマンス計画レポートはありますか？

はい。OCIには複数のレポートが用意されています。また、ユースケースに基づいて、ネットアップのプロフェッショナルサービスカタログで提供されているレポートも多数用意されています。Data Warehouseモジュールには、ユーザが独自のレポートを作成できるCognosのレポートオーサリングツールも付属しています。また、コミュニティで生成されるレポートテンプレートや、NetApp Automation Storefrontからダウンロードすることもできます。

Data ONTAP ストレージのIOPS

このFAQでは、Data ONTAP ストレージシステムのIOPS値をどのように算出するかについて、よくある質問に回答します。

Data ONTAP ストレージシステムからストレージIOPSを取得する方法

- ストレージアレイレベルのIOPSは、内部ボリュームのIOPSから集計されます
- ストレージノードレベルのIOPSにはメタデータOPSが含まれます
- ストレージプールレベルのIOPSにメタデータOPSは含まれません。測定されるのはディスクのみです
- 内部ボリュームレベルのIOPSには、読み取り+書き込みOPS（処理）+その他のOPSが含まれます

質問-アグリゲートIOPSがノードIOPSよりも高くなることがあるのはどのような場合ですか。

clustered Data ONTAP 8.3.1より前のバージョンでは、ノードのIOPSはプロトコルのIOPSで構成されています。clustered Data ONTAP 8.3.1では、以降は、システム構成要素の指標で構成されます。これには、データ要求やフロントドアからの要求が含まれますが、SnapMirrorや重複排除などのバックエンドタスクは含まれません。一方、これらのタスクではディスクIOPSが生成されるため、アグリゲートIOPSが生成されます。そのため、アグリゲートIOPSがノードIOPSよりも高くなる可能性があります。

質問-メタデータまたはその他のOPSはどのように計算されますか

その他のOPS =合計-（読み取り+書き込み）

ハウツーガイド

『Getting Started with Insight』

OnCommand Insight をインストールし、適切なライセンスを取得したら、重要なデータを表示するための環境の準備を開始するためには、いくつかのタスクを実行する必要があります。

一般的な環境で実行されるタスクには、次のものがあります。

1. *アセットに注釈を付けて、クエリやレポート作成の準備をします。最初に使用するアノテーションには、データセンター、階層、サービスレベルなどがあります。
2. 重要なデータを表示し、トラブルシューティングに役立つクエリの作成
3. *アプリケーション*および*ビジネスエンティティ*をアセットに割り当てる
4. *パフォーマンスポリシー*および*アラート*を作成して、それらのポリシーに対する違反を検出します
5. ニーズやユーザーの役割に応じてデータを強調表示するカスタムダッシュボードの作成

通知を設定する

パフォーマンスポリシー、グローバルパス、容量違反などのイベントがトリガーされたときに、Eメール、SNMP、syslogを使用して通知を送信するようにInsightを設定できます。また、データソースエラーやAcquisition Unitの障害など、システムレベルのイベントに関するEメール通知を送信するようにInsightを設定することもできます。

これらは基本的な手順です。通知の詳細については、「Configuration and administration」>「Insight configuration and administration」>「Setting up Insight」を参照してください。

通知用の**E**メールを設定します

Insightでは、パフォーマンスポリシー違反などのイベントがトリガーされたときにEメール通知を送信できます。

このタスクについて

電子メール通知を設定するには、次の基本的な手順に従います。

手順

1. **>**[通知]をクリックし、[電子メール]*セクションに移動します。
2. [サーバ]ボックスにSMTPサーバの名前を入力します。完全修飾ドメイン名またはIPアドレスのいずれかを入力できます。
3. SMTPユーザ名と（SMTPサーバで必要な場合）パスワードを入力します。
4. [送信者のEメール]ボックスに、通知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。

5. [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。
6. [受信者]ボックスで、をクリックします ＋Eメールアドレスを入力し、* OK *をクリックします。
7. [保存（ Save ）] をクリックします。

   Eメールアドレスを編集または削除したり、テストEメールを送信したりするには、アドレスを選択して、表示される適切なボタンをクリックします。

   特定のパフォーマンスポリシー違反が発生した場合に特定の個人またはグループにEメール通知を送信するようにInsightを設定できます。たとえば、クラウドアセットの違反をあるグループに送信し、物理ホストのイベントを別のグループに送信することができます。個 々 のポリシー通知を設定するには、**[**管理**]>***[パフォーマンスポリシー]*に移動してください。

ロギング用の**syslog**を設定しています

Insightでは、容量やパスの違反、およびパフォーマンスのアラートについてsyslogイベントを送信できます。

このタスクについて

Insightでsyslog通知を設定するには、次の基本的な手順を実行します。

手順

1. **>**[通知]をクリックし、 syslog *セクションに移動します。
2. [* Syslog enabled]*チェックボックスをオンにします。
3. [**Server**]フィールドに、ログサーバのIPアドレスを入力します。
4. [**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。
5. [保存（ Save ）] をクリックします。

通知用の**SNMP**の設定

Insightでは、違反やデータソースのしきい値を超えたときなど、イベントがトリガーされたときにSNMP通知を送信できます。

このタスクについて

InsightでSNMPを設定するには、次の基本的な手順を実行します。

手順

1. **>**[通知]をクリックし、[SNMP]*セクションに移動します。
2. をクリックし、[Add trap source]*を選択します。
3. [SNMPトラップ受信者の追加]ダイアログボックスで、SNMPトラップメッセージの送信先の* IP *アドレスと*ポート*を入力します。コミュニティストリング*には、SNMPトラップメッセージに「public」を使

用します。

4. [保存（ Save ）] をクリックします。

アセットの準備：アノテーション

アノテーションを使用すると、選択したアセットに特定のタグやラベルを関連付けることができ、アセットの管理やレポート作成に役立ちます。

会社のアノテーションを作成します

このガイドでは、照会、フィルタリング、アラート通知、およびレポートに使用できる環境のアノテーションを作成、カスタマイズする方法について説明します。

アノテーションは、環境内の特定のアセットに関連付けるメモまたはタグです。OnCommand Insight には、アセットに対して必要に応じて設定できるアノテーションがいくつか用意されています。また、ビジネスニーズに基づいて独自のカスタムアノテーションを作成することもできます。

ここで紹介する例は、新しいお客様の環境で最初に構成され、追加のアクションのベースラインとして使用されるものです。アノテーションのニーズは環境によって異なる場合がありますが、ここで説明する手順を参考にして、必要なアセットに必要なアノテーションを設定できます。

このガイドの説明は、次の前提に基づいています。

- OnCommand Insight サーバをインストールし、適切なライセンスを取得しておきます。
- すべての選択肢ではなく、ベストプラクティスを検討したいと考えています。
- これらは単なる例であり、特定のニーズが異なる可能性があることを理解している。

このガイドでは、既存のアノテーションの変更とカスタムアノテーションの作成について説明します

この例の環境では、データセンター、ティア、サービスレベル、環境に応じてアセットを一覧表示できるようにしたいと考えています。

データセンターのアノテーションの設定

データセンターのアノテーションは、通常、ストレージアレイ、スイッチ、または物理ホストのアセットをデータセンターの場所に関連付けるときに使用します。データセンターのアノテーションを環境内の他のアセットに関連付けることもできます。

手順

- 管理者権限を持つユーザとして Insight にログインします。
- **>**[アノテーション]*を選択します。
- アノテーションを選択し、[Edit]*アイコンをクリックします。
- [+Add]*をクリックし、最初のデータセンターの名前と概要 をアノテーションリストに追加します。
- 他のデータセンターについても同じ手順を実行します。
- 完了したら、*[保存]*をクリックします。

データセンターのアノテーションの例：

名前	説明
DC1_SVL	サニーベールビル1
DC2_SVLb3	SVL Bldg3エンジン
DC3_NY	ニューヨーク
DC4_ロンドン	ロンドン
…	

Insightには、ニーズに合わせて値を定義または変更できるアノテーションタイプがいくつか用意されています。これらのデフォルトのアノテーションタイプは、Insight Web UIとレポートで常に使用できます。新しく作成したカスタムアノテーションはInsight Web UIに表示されますが、レポートで使用できるようにするには追加の手順が必要です。レポートにカスタムアノテーションを含める方法については、を参照してください。ネットアップのカスタマーサポート担当者にお問い合わせください。

> ユーザによっては、アセットの場所をデータセンターのアノテーションではなく国のアノテーションで設定したり、データセンターのアノテーションと組み合わせて設定したりする傾向があります。ただし、国のアノテーションはInsight Data Warehouseではカスタムのアノテーションタイプとして扱われるため、データセンターと同じようにレポートに表示されない場合があります。

階層のアノテーションを設定します

階層のアノテーションは、コスト計算などの目的でアセットを対応する階層に関連付けるために使用します。Insightには、階層のデフォルトのアノテーションが多数用意されています。階層の命名規則に応じて変更したり、必要に応じて独自の階層を作成したりできます。

階層のアノテーションを設定する際は、次の点に注意してください。

- コストはギガバイトあたりのコストです。
- 階層1、2、3は、ディスクタイプ別にストレージアレイレベルで構成されるデフォルトの階層です。ただし、多くのお客様は、1つのアレイ内で複数のディスクタイプを使用したり、同じタイプのアレイ間でディスクタイプを使用したりすることになります。
- ディスクタイプやディスク速度に基づいて階層のアノテーションを作成することを推奨します。これは一般的な階層化の手法であり、お客様独自のニーズが異なる場合があります。

手順

- アノテーションを選択し、[Edit]*アイコンをクリックします。
- 必要に応じて、*+追加*をクリックし、最初の階層の名前と概要 をアノテーションリストに追加します。
- 他の階層についても同じ手順を実行します。

- 完了したら、*[保存]*をクリックします。

階層のアノテーションの例：

名前	説明	GBあたりのコスト
Auto Tier（自動階層）	自動ストレージ階層化	0.5
ティア1 SSD	オールフラッシュアレイ	0.5
ティア2 SAS	（ SAS ）。	0.25
ティア3 SATA	SATA	0.1
…		

サービスレベルのアノテーションを設定します

サービスレベルのアノテーションは、アセットをそれぞれのサービスレベルに関連付けるために使用します。

サービスレベルのアノテーションは、通常、自動階層化を使用するお客様の環境でのみ設定されます。Insight Data Warehouseでは階層が推奨されます。プロビジョニングコストとプロビジョニングコストを比較する場合は、サービスレベルを使用することを推奨します顧客コスト。両方がData Warehouseに存在する場合は、サービスレベルが階層より優先されます。

手順

- アノテーションを選択し、[Edit]*アイコンをクリックします。
- [+Add]*をクリックし、最初のサービスレベルの名前と概要 をアノテーションリストに追加します。
- 他のサービスレベルについても同じ手順を実行します。
- 完了したら、*[保存]*をクリックします。

サービスレベルのアノテーションの例：

名前	説明	GBあたりのコスト
サービスレベル1	FCまたはSAS、ローカルとリモートのミラー、テープを搭載したFAS コントローラ	0.93
サービスレベル2	FCまたはSAS、ローカルおよびリモートミラーを搭載したFAS コントローラ	0.85

サービスレベル3	SATAおよびローカルミラーを備えたFAS コントローラ	0.48です
…		

カスタムの環境アノテーションを設定します

環境のアノテーションは、ラボ、研究開発、本番環境など、アセットを環境の場所や用途に関連付けるためのカスタムアノテーションです。 など Environmentアノテーションを作成してこれらのアセットに設定すると、たとえば、本番環境のアセットとは別にラボのアセットを簡単に検索、フィルタ、レポートできます。

手順

- **>**[アノテーション]*を選択します。
- ページの上部にある*+追加*ボタンをクリックします。
- 「* Name 」に「 Environment *」と入力します。
- 概要 *には、'*アセット環境タイプ'"と入力します。
- *タイプ*で、*リスト*を選択します。リストを作成するための新しいフィールドが表示されます。
- ここでは、*[Add new assets on the fly]*チェックボックスをオフのままにします。選択項目のリストに新しい環境を追加し、アセットに関連付ける場合は、このチェックボックスをオンにします。
- 最初の環境の名前と概要 を入力します。
- [+追加]*をクリックし、他の環境でも同じ手順を実行します。
- 完了したら、*[保存]*をクリックします。

環境のアノテーションの例：

名前	説明
研究室だ	研究室だ
開発	開発
PRD	本番環境
…	

アセットの検索：クエリ

強力なクエリを使用して、環境内のアセットを簡単に検索して表示できます。

これで最初のアノテーションが作成されました。次に、それらのアノテーションを特定のアセットに関連付ける方法を見てみましょう。

以降の例では、これらのアノテーションを特定のアセットに適用します。たとえば、特定のデータセンターにあるすべてのストレージアレイを一覧表示するクエリを作成し、それらのストレージアレイに適切なアノテーションを付けます。次に、特定の階層とサービスレベルに属するアセットについても同じ手順を実行します。

クエリを実行してデータセンターにアノテーションを適用します

クエリを使用して、環境内の適切なアセットにアノテーションを関連付けます。この例では、選択したアセットにデータセンターのアノテーションを関連付けます。

Insightでは、データソースの取得時に、検出した各アセットの名前（その他の情報を含む）が収集されます。この例では、すべてのストレージアレイに、格納されているデータセンターに基づいて名前が付けられていることを前提としています（サニーベールにあるアレイの場合は「<label> 」など）。Insightのクエリを使用すると、アセットへのアノテーションを簡単に設定できます。

- 管理者権限を持つユーザとしてInsightにログインします
- [Queries]>[*+New Query]*を選択します
- フィールドのドロップダウンリストで、[ストレージ]*を選択します。すべてのストレージアレイのリストが表示されます。
- 「* Name * filter」フィールドに「`SVL'」と入力し、をクリックします ボタンを押します（またはEnterキーを押します）。クエリ結果リストが更新され、文字列"`SVL`"を含む配列のみが表示されるようになりました。
- フィルタする場合は、[Query]ページのテキストボックスで次の文字を単独で使用するか、組み合わせて使用して検索を絞り込むことができます。
  - 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。たとえば、「vol * rhel」と指定すると、先頭が「vol」で末尾が「rhel」のアセットが表示されます。
  - 疑問符を使用すると、特定の数の文字を検索できます。たとえば、「`SVL-PRD??-S12`」をフィルタリングすると、SVL-PRD12-S12、SVL-PRD13-S12などが表示されます。
  - 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。たとえば、「'FAS2240 or CX600 or FAS3270'」と指定すると、複数のストレージモデルが検出されます。
- このデータセンターに関連付けるストレージアレイを選択します。目的のアレイをすべて選択したら、**[Actions]***ボタンをクリックし、[Edit annotation]*を選択します。
- ダイアログで、[データセンター]*アノテーションを選択します。
- 目的の*値*を選択します（例：“DC1_SVL”）。
- [保存（ Save ）] をクリックします。
- [Query results]ページに[Data Center]列が表示されない場合は、**[Columns]***ボタンをドロップダウンして[Data Center]*を選択します。
- 必要に応じて、[Query]ページの右上にある*[Save]*ボタンをクリックし、一意で明示的な名前を指定することで、あとで使用できるようにクエリを保存できます。たとえば、「ストレージアレイ- SVLデータセンター」と入力します。

「SVL」アノテーションを他のアセットに関連付ける場合は、新しいクエリを作成し、アセットタイプごとに次の手順を実行します。

それぞれのデータセンターのアセットについて、上記の手順を繰り返します。

階層を照会してアノテーションを適用しています

クエリを使用して、環境内の適切なアセットにアノテーションを関連付けます。ここでは、これらの階層を適切なアセットに関連付けます。

前の手順で、階層のアノテーションを設定しました。この例では、階層をストレージプールに関連付けます。階層のアノテーションは次のように設定されていると想定します。

価値	説明	GBあたりのコスト
ティア1 SSD	オールフラッシュアレイ	0.5
ティア2 SAS	（ SAS ）。	0.25
ティア3 SATA	SATA	0.1

環境内のすべてのSSDディスクを検索し、「階層1 SSD」アノテーションを関連付けます。

- 管理者権限を持つユーザとしてInsightにログインします
- [Queries]>[*+New Query]*を選択します
- フィールドのドロップダウンリストで、[ストレージプール]*を選択します。すべてのストレージプールのリストが表示されます。
- [名前]フィールドは今回は役に立たない可能性があるため、別のフィールドを使用してみましょう。[More]*ドロップダウンをクリックし、[Least performing disk type]を選択します。このフィールドには、該当するディスクタイプが表示されます。フィールドに「`SSD'」と入力し、をクリックします ボタンを押します。クエリ結果のリストには、SSDストレージプールのみが表示されます。
- さらに絞り込むには、* More *ドロップダウンをクリックして追加フィールドを選択します。
- この階層に関連付けるストレージプールを選択します。必要なストレージプールをすべて選択したら、**[操作]***ボタンをクリックし、[アノテーションの編集]*を選択します。
- ダイアログで、[階層]*アノテーションを選択します。
- リストから目的の*値*を選択します。この例では、「階層1 SSD」を選択します。
- [保存（ Save ）] をクリックします。
- [Query]の結果ページに[Tier]列が表示されない場合は、**[Columns]***ボタンをドロップダウンして[Tier]*を選択します。アセットに適切なアノテーションが関連付けられていることを確認します。
- [Query]ページの右上にある*[Save]*ボタンをクリックし、一意で明示的な名前を付けてクエリを保存します。たとえば、「ストレージプール-階層1 SSD」と入力します。

「階層1のSSD」というアノテーションを他のアセットに関連付ける場合は、新しいクエリを作成し、アセットタイプごとに次の手順を実行します。

残りの階層のアセットについても、同じ手順を繰り返します。

サービスレベルと環境のアノテーション

学習した手順と概念を使用して、サービスレベルと環境のアノテーションを適切なアセットに追加します。

サービスレベルと環境のアノテーションを環境内の適切なアセットに追加するには、前述の手順に従って、必要なアセットと適切なサービスレベルまたは環境のアノテーションを選択します。同じアセットに複数のアノテーションを関連付けることができます。そのため、Insightで環境をより柔軟に管理できるようになります。

これで、クエリを作成してアセットにアノテーションを付けることができました。次のようなさまざまな方法でアノテーションを使用できます。

- 必要なアセットでイベントが発生したときにアラートを生成するパフォーマンスポリシー
- アクティビティを監視するカスタムダッシュボードとウィジェット
- レポート作成

企業構造：ビジネスエンティティとアプリケーションの設定

企業構造の要素を理解することで、資産の使用状況を追跡し、コストを報告することができます。

会社のビジネスエンティティの設定

企業構造のビジネス要素を理解することで、資産の使用状況を追跡し、コストを報告することができます。ここでは、会社のビジネスエンティティを設定します。

このタスクについて

OnCommand Insight では、ビジネスエンティティを最大4つのレベルの階層で定義できます。

- テナント

  主にサービスプロバイダがリソースを顧客に関連付けるために使用します。テナントレベルは、ISPが顧客のリソース使用状況を追跡する場合に必要です。

- 基幹業務（**LOB**）

  企業内の基幹業務や製品ライン（データストレージなど）。異なる製品ラインのデータを追跡する必要がある場合は、基幹業務部門が階層に必要です。

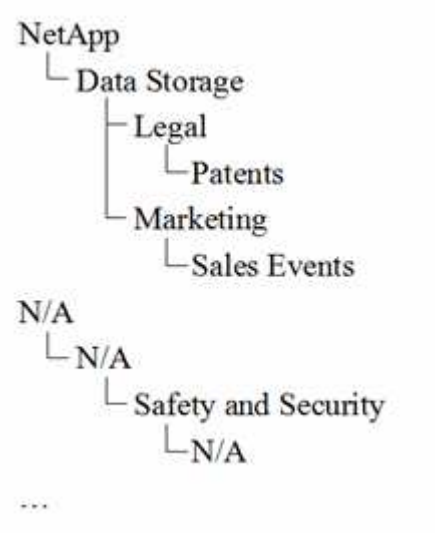
- ビジネスユニット

  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。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 *

多くの場合、容量の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、法務部門のプロジェクト名は「特許」、マーケティング部門のプロジェクト名は「販売イベント」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。

ビジネスエンティティ階層の例を次に示します。



ベストプラクティス：各行にビジネスエンティティが1つだけ表示される表を作成します。

テナント	基幹業務部門	ビジネスユニット	プロジェクト
NetApp Inc.	データストレージ	法律	特許
NetApp Inc.	データストレージ	マーケティング	セールスイベント
該当なし	該当なし	安全とセキュリティ	該当なし
…			

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。使用しないレベルには「N/A」を選択できます。

Insightでビジネスエンティティ階層を作成するには、次の手順を実行します。

手順

1. 管理者権限を持つユーザとして Insight にログインします。
2. **>**[ビジネスエンティティ]*を選択します。
3. [+追加]*ボタンをクリックします
4. [Tenant]*ボックスをクリックし、テナント名を入力します。

   環境のテナントをすでに入力している場合は、既存のテナントのリストが表示され、そこから選択できます。テナントがこのビジネスエンティティに該当しない場合は、「N/A」を選択することもできます。

5. [Line of Business]、[Business Unit]、[Project]についても同じ手順を繰り返します。
6. [保存（ Save ）] をクリックします。

完了後

ベストプラクティス：

- ビジネス階層をテーブルにマッピングし、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。
- アプリケーションを作成する前に、Insightでビジネスエンティティを作成します。
- 各ビジネスエンティティに関連付けるすべてのアプリケーションを特定してリストします。

会社のアプリケーションを設定します

会社の環境で使用されているアプリケーションを理解すると、資産の使用状況を追跡し、コストを報告するのに役立ちます。ここでは、会社のアプリケーションを設定し、適切なアセットに関連付けます。

このタスクについて

「company_sectionのビジネスエンティティの設定」セクションでは、いくつかのビジネスエンティティを作成しました。それぞれのビジネスエンティティに関連付けるすべてのアプリケーションをリストアップすることを推奨します。OnCommand Insight を使用すると、使用状況やコストレポートなどのアプリケーションに関連するデータを追跡できます。

環境で実行されているアプリケーションに関連付けられているデータを追跡するには、まずそれらのアプリケーションを定義し、適切なアセットに関連付ける必要があります。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：

このチュートリアルでは、マーケティングチームがExchange電子メールに使用する仮想マシンの使用状況を追跡します。ビジネスエンティティを定義する際に作成した次の表を覚えておいてください。このワークシートに列を追加して、各ビジネスエンティティで使用されているアプリケーションを表示します。（この表はあくまでワークシートの例です。Insightのビジネスエンティティテーブルに[Applications]列は表示されません）。

テナント	基幹業務部門	ビジネスユニット	プロジェクト	アプリケーション
ネットアップ	データストレージ	法律	特許	Oracle Identity Manager 、 Oracle On Demand 、 PatentBuy
ネットアップ	データストレージ	マーケティング	セールスイベント	Exchange 、 Oracle 共有データベース、 BlastOff Event Planner
該当なし	該当なし	安全とセキュリティ	該当なし	該当なし

…				

- Insightでのアプリケーションの作成：*

手順

1. 管理者権限を持つユーザとして Insight にログインします。
2. **>**[アプリケーション]*を選択します
3. [+追加]*ボタンをクリックします
4. アプリケーションの名前を入力します（この例では、「Exchange」と入力します）。
5. アプリケーションの優先度を選択します
6. 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、*[Business Entity]*ドロップダウンから1つ選択します。それ以外の場合は、「なし」のままにしておくことができます。
7. 各ホストがクラスタ内の同じボリュームにアクセスできるようにする場合は、**[**ボリューム共有の検証**]***ボックスがオンになっていることを確認します。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。ボリューム共有を使用しない場合は、[ボリューム共有の検証]*ボックスの選択を解除します。これにはAssureライセンスが必要です。
8. [保存] をクリックします .
9. 環境内の他のすべてのアプリケーションについて、この手順を繰り返します。

完了後

マーケティングチームがExchangeアプリケーションを使用していることがわかります。ストレージの追加がいつ必要になるかを予測するために、Exchangeでの仮想マシンの使用率を確認したいと考えています。次に、Exchangeアプリケーションをマーケティングのすべての VMに関連付けます。これを実現する最も簡単な方法は、クエリを使用することです。

次の手順に従って、各アプリケーションを適切なアセットに関連付けることができます。

アセットへのアプリケーションの関連付け：

これでアプリケーションが作成され（必要に応じてビジネスエンティティに関連付けられました）、これらのアプリケーションを環境内のアセットに関連付けることができます。この例では、Exchangeアプリケーションを社内の複数の仮想マシンに関連付けます。これを行う最も簡単な方法は、クエリです。

1. [Queries]>[*+New query]*を選択します。
2. [Select Resource Type]*ドロップダウンで、[*Virtual Machine*]を選択します
3. ここでは、マーケティングチームがアセットの名前に文字列「`mktg`」を付けると仮定します。[Name]フィルタボックスに「`mktg`」（引用符なし）と入力し、[apply]（チェックマーク）ボタンをクリックします。
4. 「*mktg*」という文字列を含むすべてのVMのリストが表示されます。
5. 必要に応じて、* More *ドロップダウンをクリックし、フィルタを追加します。

6. Exchangeに使用するVMをVM名の横にあるチェックボックスをクリックして選択するか、列の上部にあるチェックボックスをクリックしてすべてのVMを選択します。
7. 目的のVMを選択したら、**[Actions]***ボタンをクリックし、[Add Application]*を選択します。
8. [Assign Application]ダイアログで、*[Application]*ドロップダウンをクリックし、「Exchange」を選択します。
9. [保存（ Save ）] をクリックします。
10. 必要に応じてこの手順を繰り返して、Exchangeアプリケーションを他のアセット（ホスト、ボリュームなど）に関連付けます。

アラート用のパフォーマンスポリシーを作成しています

パフォーマンスポリシーを使用すると、監視し、特定の条件が満たされたときにアラートを送信できます。

このタスクについて

これでアセットのアノテートが完了しました。次に、Sunnyvale（DC1_SVL）データセンターのいずれかのストレージアレイでレイテンシが2ミリ秒を超えたときにアラートを表示するためのパフォーマンスポリシーを作成します。このような状況が発生した場合は、選択した受信者にEメールを送信します。

手順

1. **>**[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]ページが開きます。いくつかのデフォルトポリシーがすでに設定されており、必要に応じて変更できます。ただし、新しいポリシーを作成します。

2. [+追加]*ボタンをクリックします。

   [ポリシーの追加]*ダイアログが開きます。

3. [ポリシー名]フィールドに「SVL Data Center Latency policy」と入力します。

   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、内部ボリュームの「 Latency 」という名前の 2 つのポリシーを使用することはできませんが、内部ボリュームの「 Latency 」ポリシーと別のボリュームの「 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。

4. で、[ストレージ]*を選択します。
5. フィールドで、[Data Center]*は「DC1_SVL」を選択します（または、ここで目的のデータセンターの名前を選択します）。
6. *最初の発生*のウィンドウの後に適用します。

   [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。

7. [重大度*あり]リストから*[警告]*を選択します。

8. [Eメール受信者]*で、をクリックしてグローバル受信者リストを上書きします。**+**をクリックして最初に希望するアラート受信者のメールアドレスを追加し、*OK*をクリックします。他のEメール受信者についても、同じ手順を繰り返します。
9. [Create alert if * any* of the following are true]はデフォルトの選択のままにします。これにより、設定されたいずれかのしきい値に達した場合にアラートが送信されます。設定されたしきい値の*すべて*を満たした場合にのみアラートを送信するように選択することもできます。
10. 最初のしきい値を設定するには、ドロップダウンで* Latency - Total *を選択し、2ミリ秒を超える値に設定します。
11. 必要に応じて、**[Add threshold]***ボタンをクリックして、アラートの対象となるしきい値を追加します。ポリシーを希望どおりにカスタマイズしたら、[保存]*をクリックします。
12. [Stop processing further policies if alert is generated]を選択することもできます。これにより、このポリシーの条件が満たされると、追加のポリシーアラートが停止します。
13. 新しいポリシーを必要な数だけ追加して、ビジネスニーズに応じてさまざまな条件に基づいて他の受信者にアラートを設定できます。特定の受信者を指定せずに設定されたポリシーは、* Admin **>** Notifications * ページで設定されたグローバル受信者リストにアラートを送信します

完了後

新しいポリシーはそれぞれ保存時に自動的にアクティブ化され、ポリシーの条件（*violation*）が満たされると受信者にアラートが送信されます。これらの違反は、**[Dashboards]**>*[Violations Dashboard]*で監視することもできます。

ダッシュボードを使用してデータを強調表示する

これでアセットにアノテートを付け、違反のアラートを通知するパフォーマンスポリシーを設定できました。次に、対象となる特定のデータを強調表示するダッシュボードを作成します。

このタスクについて

この例では、VMのパフォーマンスデータを表示する単一のウィジェットを使用してダッシュボードを作成することで、ダッシュボードの作成の概要を示します。ウィジェットは1つのダッシュボードに必要な数だけ追加でき、ダッシュボードは必要な数だけ作成できます。ウィジェットは、必要に応じてサイズを変更したり移動したりできます。

ダッシュボードとウィジェットの詳細については、OnCommand Insight のドキュメントを参照してください。

手順

1. 管理者権限を持つユーザとして Insight にログインします。
2. メニューから、**[**+New dashboard]*を選択します。

   [New dashboard]ページが開きます。

3. ベストプラクティス：ダッシュボードを作成したらすぐに名前を付けて保存してください。ボタンをクリックし、[名前]*フィールドにダッシュボードの一意の名前を入力します。たとえば、「VM Performance Dashboard」と入力します。[保存（ Save ）] をクリックします。

4. 必要に応じて、「編集」スイッチを「オン」にスライドして編集モードを有効にします。これにより、ダッシュボードにウィジェットを追加できるようになります。
5. ボタンをクリックし、[Table]*を選択して新しい表ウィジェットをダッシュボードに追加します。

   ウィジェットを編集（ Edit Widget ）ダイアログが開きます。

6. [Name]フィールドで「Widget 1」を削除し、「Virtual Machine Performance table」と入力します。
7. アセットタイプのドロップダウンをクリックし、**[**ストレージ**]***を[仮想マシン]*に変更します。

   表のデータが更新され、環境内のすべての仮想マシンが表示されます。

8. テーブルに列を追加するには、*列*をクリックします ボタンをクリックし、*Data Center*、_ Storage name_、_Tier_などの目的の列を選択します。これらの列を基準にテーブルをソートできます。
9. このダッシュボードで重要なデータを表示するためのフィルタを必要に応じて設定できます。たとえば、アノテーションが「階層1 - SSD」の仮想マシンのみを表示するように選択できます。[Filter by]*の横にある[+]ボタンをクリックし、*Tier*を選択します。[Any]*をクリックし、「Tier 1 - SSD」と入力します。をクリックします ボタンをクリックしてフィルタを保存します。

   これで、「SD」階層の仮想マシンのみが表に表示されます。

10. 結果をグループ化するには、*[Group by]*の横にある[+]ボタンをクリックし、グループ化の基準とするフィールド（[Data Center]など）を選択します。グループ化はテーブルに自動的に適用されます。
11. ウィジェットをカスタマイズしたら、*[保存]*ボタンをクリックします。

    表ウィジェットがダッシュボードに保存されます。

12. ダッシュボード上のウィジェットの右下をドラッグすると、ウィジェットのサイズを変更できます。
13. ウィジェットを追加するには、[**+Widget**]ボタンをクリックします。各ウィジェットは、保存時にダッシュボードに追加されます。
14. 必要な変更をすべて行ったら、*[保存]*をクリックしてダッシュボードを保存します。
15. 別のデータを強調表示するダッシュボードを追加で作成することもできます。

カスタムダッシュボードの作成

OnCommand Insight 7.3には、ユーザにとって重要なデータの運用ビューと、そのデータのワンストップビューを提供する、強化されたカスタムダッシュボード機能が含まれています。

OnCommand Insight では、さまざまなウィジェットを使用してカスタムダッシュボードを作成できるため、ITプラットフォーム全体でインフラデータの運用ビューを柔軟に作成でき、それぞれのダッシュボードでデータの表示とグラフ化を柔軟に行うことができます。このハウツーでは、VMのパフォーマンスを強調するダッシュボードの例を作成します。

このハウツーはあくまでも例であり、すべてのシナリオを網羅しているわけではありません。ここで説明する概念と手順を使用して、特定のニーズに固有のデータを強調する独自のカスタムダッシュボードを作成できます。

- 概要 *

カスタムダッシュボードは、次のいずれかの方法で作成します。

- ダッシュボード>*+新しいダッシュボード*
- **[Dashboards]**>*をクリックし、[+Add]*をクリックします

[New Dashboard]画面にはいくつかのコントロールがあります。

- 時間セレクタ：カスタムの日付範囲セレクタを使用して、3時間から90日間の範囲のダッシュボードデータを表示できます。ウィジェットごとにこのグローバルな期間を無効にすることができます。
- *編集*ボタン:「オン」を選択すると編集モードが有効になり、ダッシュボードに変更を加えることができます。新しいダッシュボードは、デフォルトで編集モードで開きます。
- *保存*ボタン：ダッシュボードを保存、名前変更、または削除できます。
- *変数*ボタン：変数をダッシュボードに追加できます。変数を変更すると、すべてのウィジェットが一度に更新されます。変数の詳細については、を参照してください "カスタムダッシュボードの概念"
- *ウィジェット*ボタン。任意の数の表、グラフ、またはその他のウィジェットをダッシュボードに追加できます。

ウィジェットは、サイズを変更したり、ダッシュボード内で別の位置に移動したりすることで、現在のニーズに合わせてデータを見やすくすることができます。

ウィジェットタイプ

次のタイプのウィジェットから選択できます。

*表*ウィジェット：選択したフィルタおよび列に従ってデータを表示する表。テーブルデータは、グループにまとめて、折りたたんだり展開したりすることができます。

折れ線グラフ、スプライングラフ、面積グラフ、積み上げ面グラフ：時系列グラフウィジェットで、パフォーマンスやその他のデータを経時的に表示できます。

*単一値*ウィジェット：カウンタから直接取得することも、クエリや式を使用して計算することもできる単一の値を表示するウィジェットです。たとえば、環境内のすべてのストレージの合計IOPSをダッシュボードの上部に1つの値として表示できます。

*棒グラフ：上位または下位の5、10、20、または50の値を表示するグラフ。

- Box Plot * chart：1つのチャートのデータの最小、最大、中央値、および下位4分の1と上位4分の1の範囲のプロット。

*散布図*グラフ：IOPSやレイテンシなど、関連するデータをポイントとしてプロットします。この例では、レイテンシが高くIOPSが低いアセットを簡単に確認できます。

また、選択できるレガシーウィジェットも多数あります。[**Widgets**]ドロップダウンで[* **Show More…**]を選択すると、これらのウィジェットが表示されます。

カスタムダッシュボードの概念

カスタムダッシュボードとウィジェットを使用すると、データの表示方法を柔軟に変更

できます。ここでは、カスタムダッシュボードを最大限に活用するのに役立つ概念をいくつか紹介します。各概念については、以降のセクションで詳しく説明します。

- 変数 *

変数を使用すると、ダッシュボードの一部またはすべてのウィジェットに表示するデータを一度に変更できます。各ウィジェットで共通の変数を使用するように設定することで、1か所で行われた変更は、各ウィジェットに表示されているデータを原因 して自動的に更新します。

複数のクエリおよび/または式

各時系列ウィジェット（折れ線グラフ、スプライングラフ、面グラフ、積み上げ面グラフ）には、表示するデータを決定するクエリや式を最大5つ設定でき、1つのグラフで異なるデータセットを比較できます。たとえば、折れ線グラフにストレージとVMの両方のIOPSを表示したり、すべてのストレージプールのスループットとレイテンシを1つのグラフで比較したりできます。

ロールアップとグループ化

各ウィジェットに表示されるデータは、収集されたデータポイントを集計したものです。このデータは、次のいずれかの方法で集計できます。

- Avg：収集されたデータの平均値を集計します
- Max：収集されたデータの最大値を集計します
- Min：収集されたデータの最小値を集計します
- Sum：収集されたデータの合計を集計します

デフォルトでは、収集されたすべてのデータが集計されて1つのエントリ（すべて）としてグラフまたは表に表示されます。データセンターや階層などの特定の属性のデータを集計して、必要なグループにデータを分散することもできます。ウィジェットには、選択した属性のデータのみが表示されます。

表ウィジェットでは、選択した属性に応じてデータをグループ化できます。たとえば、テーブルをデータセンター別にグループ化できます。グループは自由に展開または折りたたむことができます。表内のパフォーマンスデータは、ウィジェットで設定した集計方法（平均、最大、最小、または合計）に従ってグループヘッダーに集計されます。

表ウィジェットは任意の列でソートでき、列は必要に応じて移動またはサイズ変更できます。

上/下

グラフウィジェットの結果セットを制限したり、ウィジェットに上位N件の結果を表示するか、下位N件の結果を表示するかを選択したりする場合に使用します。このオプションは、データがロールアップされていない場合、または特定の属性別にロールアップされている場合に選択できます。

ダッシュボード時間を上書き

デフォルトでは、ダッシュボードに追加するほとんどのウィジェットには、ダッシュボードの時間範囲設定（3h、24h、3d、7d、30d、またはカスタムの範囲）に従ってデータが表示されます。ただし、この時間設定を個 々 のウィジェットで無効にして、ダッシュボードの時間設定に関係なく、特定の期間のデータを強制的に表示することができます。

これらの概念については、次のセクションで詳しく説明します。

ダッシュボードの変数を使用すると、ダッシュボード上の複数のウィジェットでデータをすばやく簡単にフィルタリングできます。

作業を開始する前に

この例では、* City *アノテーション（City属性とも呼ばれます）を複数のストレージアセットに設定する必要があります。

結果がはっきりわかるように、ストレージごとに異なる都市を設定します。

このタスクについて

変数を使用すると、カスタムダッシュボードの一部またはすべてのウィジェットでデータをすばやく簡単にフィルタできます。次の手順では、変数を使用するウィジェットを作成し、それらの変数をダッシュボードで使用する方法を示します。

手順

1. 管理者権限を持つユーザとしてInsightにログインします
2. **>**+[新しいダッシュボード]*をクリックします。
3. ウィジェットを追加する前に、ダッシュボードデータのフィルタリングに使用する変数を定義します。[Variable]*ボタンをクリックします。

   属性のリストが表示されます。

4. ここでは、「 City 」に基づいてフィルタするようにダッシュボードを設定します。リストから* City *属性を選択します。

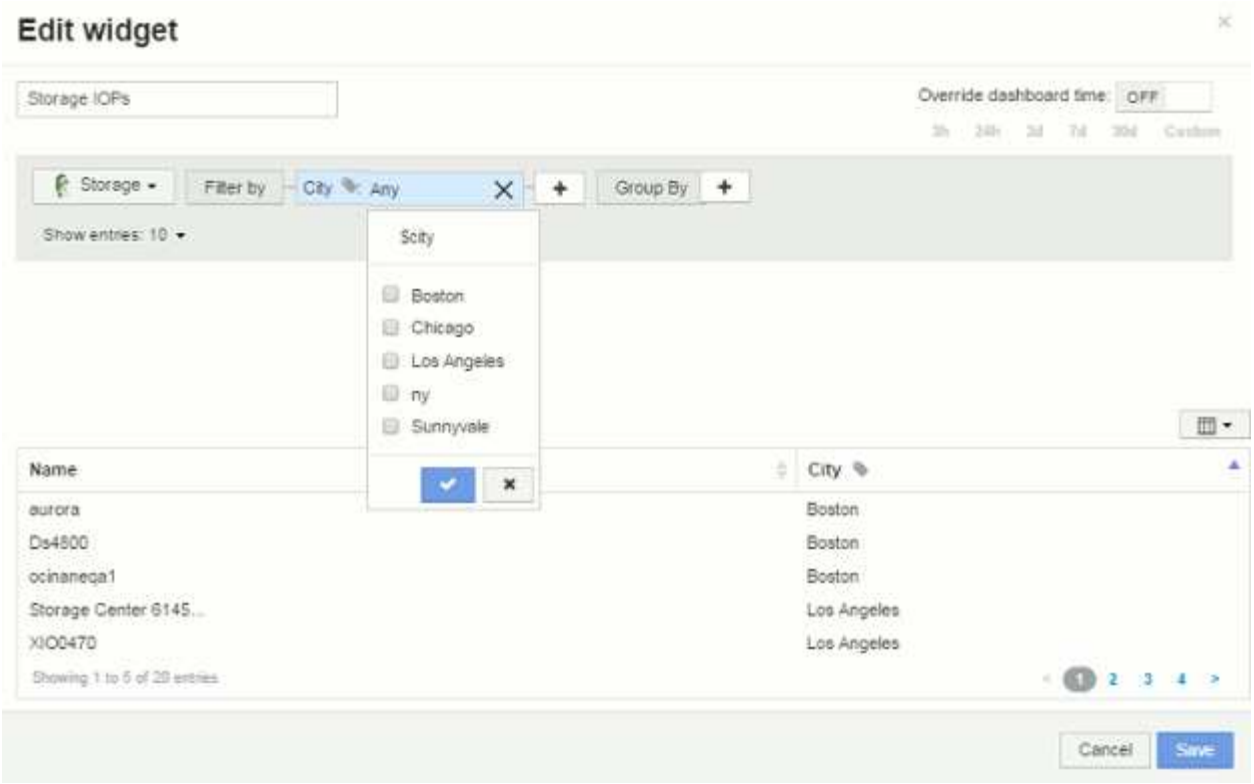
   $city 変数フィールドが作成され、ダッシュボードに追加されます。

5. 次に、この変数を使用するようにウィジェットに指示します。これを説明する最も簡単な方法は、[City]列を表示する表ウィジェットを追加することです。[Widget]ボタンをクリックし、[*Table]ウィジェットを選択します。
6. まず、列ピッカーから[City]フィールドを選択して、テーブルに追加します ボタンを押します。

   City はリストタイプの属性であるため、以前に定義された選択肢のリストが含まれています。テキスト、ブーリアン、日付タイプの属性を選択することもできます。

7. 次に、**[+**でフィルタ**]***ボタンをクリックし、[City]*を選択します。
8. [City]で選択可能なフィルタを表示するには、*[Any]*をクリックします。リストの一番上に「$city」が表示されるようになりました。これまで利用可能だった選択肢に加えて、リストの一番上に「$city」が表示されます。このダッシュボード変数を使用するには、「$city」を選択します。

   「$city」オプションは、メインダッシュボードページで以前に定義した場合にのみここに表示されます。変数が以前に定義されていない場合は、フィルタの既存の選択肢のみが表示されます。選択した属性タイプに該当する変数のみが、そのフィルタのドロップダウンに表示されます。



9. * ウィジェットを保存します。
10. ダッシュボードページで、$city変数の横にある* any *をクリックし、表示する都市を選択します。

    表ウィジェットが更新され、選択した都市のみが表示されます。$city変数の値は自由に変更できます。$city変数を使用するように設定されているダッシュボードのすべてのウィジェットが自動的に更新され、選択した値のデータのみが表示されます。

11. 設定が完了したら、必ずダッシュボードを * 保存 * してください。

ダッシュボードの変数の詳細

ダッシュボードの変数にはいくつかの種類があり、さまざまなフィールドで使用できます。また、命名規則もあります。ここでは、これらの概念について説明します。

変数の型

変数には、次のタイプがあります。

- テキスト * ：英数字の文字列。これがデフォルトの変数タイプです。
- 数値 * ：数値または数値の範囲。
- Boolean *：True/False、Yes/No、0/1などの値を持つフィールドに使用します ブール変数の場合、選択肢は_Yes_、*No*、*None*、_Any_です。
- 日付 * ：日付または日付の範囲。

「汎用」変数

汎用変数または汎用変数を設定するには、*変数*ボタンをクリックし、上記のいずれかのタイプを選択しま

す。これらのタイプは常にドロップダウンリストの上部に表示されます。変数にはデフォルトの名前（例：「$var1」）が付けられ、特定のアノテーションや属性には関連付けられません。

汎用変数を設定すると、ウィジェットでその変数を使用して、そのタイプの_any_fieldをフィルタリングできます。たとえば、*Name*、*Alias*、および_Vendor_（すべてテキストタイプの属性）を表示する表ウィジェットがあり、「$var1」がテキストタイプの変数である場合、ウィジェット内のこれらのフィールドごとに$var1変数を使用するフィルタを設定できます。他のウィジェットでも、テキストフィールドに $var1 を使用するように設定できます。

ダッシュボードページで、$var1に値（「`netapp`」など）を設定すると、その変数を使用するように設定された_all_widgets内のフィールドの_all_がフィルタリングされます。これにより、ダッシュボードで選択したデータを複数のウィジェットで一度に更新できます。

汎用的な変数はその型のどのフィールドでも使用できるので、その機能を変更することなく汎用的な変数の名前を変更できます。

> すべての変数は、特定の属性に対して作成したものであっても、「汎用」変数として扱われます。これは、そのタイプの属性またはアノテーションに対してフィルタを設定すると、そのタイプの設定済み変数がすべて表示されるためです。ただし、汎用変数を使用して複数のフィールドにわたって値をフィルタリングする場合は、上記の_Name/Alias/Vendor_Exampleのように汎用変数を作成することを推奨します。

変数の命名規則

変数名：

- 常に先頭に"$`"を付ける必要があります。これは、変数を設定するときに自動的に追加されます。
- 特殊文字は使用できません。使用できるのは、 a~z のアルファベットと 0~9 の数字のみです。
- 「$」記号を含めて20文字以内にする必要があります。
- 大文字と小文字は区別されません。$CityNameと$CityNameは同じ変数です。
- 既存の変数名と同じにすることはできません。
- "$`"記号だけにすることはできません。

変数を使用するウィジェット

変数は次のウィジェットで使用できます。

- エリアチャート
- 棒グラフ
- ボックスプロットグラフ（ Box Plot Chart ）
- 折れ線グラフ
- 散布図
- 単一値ウィジェット
- スプライングラフ（ Spline Chart ）
- 積み上げ面グラフ

- 表ウィジェット

ウィジェットの凡例の表示

ダッシュボードのウィジェットは、凡例の有無に関係なく表示できます。

ウィジェットの凡例は、次のいずれかの方法でダッシュボードでオンまたはオフにできます。

1. ウィジェット自体を作成または編集するときは、[凡例]チェックボックスをオンにしてウィジェットを保存します。
2. 編集モードのダッシュボードで、ウィジェットの[Options]ボタンをクリックし、メニューの[Legends]チェックボックスをオンにします。

ウィジェットに表示されるデータを編集および変更すると、そのウィジェットの凡例が動的に更新されます。

凡例が表示されているときに、凡例が示すアセットのランディングページにアクセス可能な場合は、凡例がそのアセットページへのリンクとして表示されます。

ダッシュボードウィジェットのクエリとフィルタ

ダッシュボードウィジェットのクエリは、データ表示を管理するための強力なツールです。ここでは、ウィジェットのクエリに関する注意事項を示します。

一部のウィジェットでは、最大 5 つのクエリを設定できます。クエリごとに固有の折れ線などのグラフがウィジェットに出力されます。1 つのクエリに集計方法、グループ化、上位 / 下位などを設定しても、ウィジェットの他のクエリには影響しません。

目のアイコンをクリックすると、クエリが一時的に非表示になります。クエリの表示と非表示を切り替えると、ウィジェットに自動的に表示される情報が更新されます。これにより、ウィジェットの作成時に表示されるデータを個々のクエリで確認することができます。

次のタイプのウィジェットでは、複数のクエリを設定できます。

- 面グラフ
- 積み上げ面グラフ
- 折れ線グラフ
- スプライングラフ
- 単一値ウィジェット

残りのタイプのウィジェットでは、クエリを 1 つだけ設定できます。

- 表
- 棒グラフ
- ボックスプロット
- 散布図

ダッシュボードのクエリでのフィルタリング

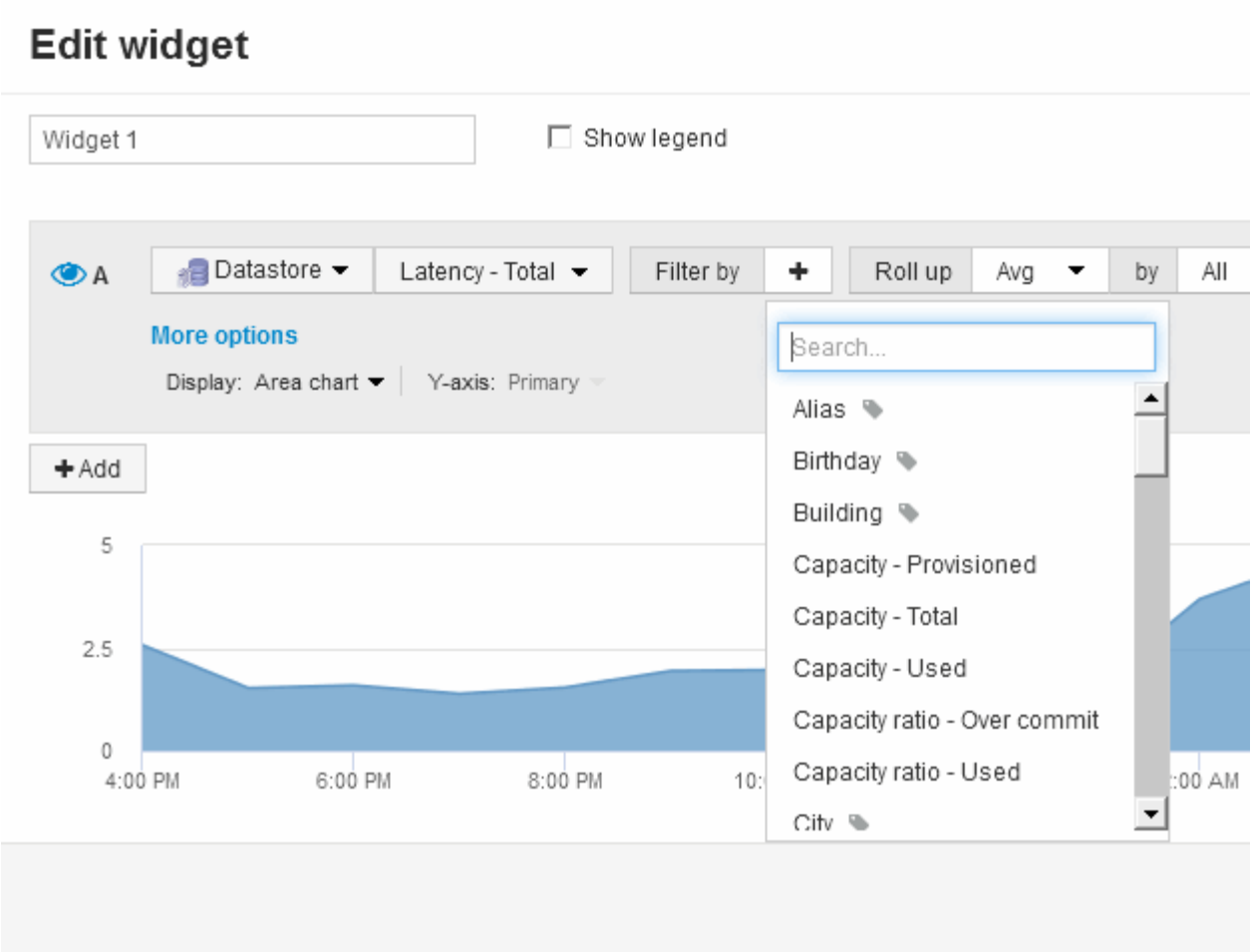
次のいずれかを使用してフィルタリングし、クエリ内の任意の*テキストフィールド*で検索を絞り込むことができます。

- 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 *` null値を含むフィールドを表示します。

フィルタ文字列を二重引用符で囲むと、 Insight では、最初と最後の引用符の間のすべての部分が完全に一致するものとして扱われます。引用符内の特殊文字または演算子は、リテラルとして扱われます。たとえば、「*」をフィルタリングすると、リテラルアスタリスクである結果が返されます。この場合、アスタリスクはワイルドカードとして扱われません。演算子 AND 、 OR 、および NOT は、二重引用符で囲まれた場合にもリテラル文字列として扱われます。

クエリとフィルタで返されるオブジェクトを特定する

クエリとフィルタで返されるオブジェクトは、次の図に示すようになります。「タグ」が割り当てられているオブジェクトはアノテーションであり、タグのないオブジェクトはパフォーマンスカウンタまたはオブジェクト属性です。



ロールアップと集約

ダッシュボードウィジェットに表示されるデータは、取得したデータポイントを集計したもので、ダッシュボードを柔軟かつ簡潔に表示できます。

各ウィジェットに表示されるデータは、収集中に収集された基盤となるデータポイントの集計です。たとえば、ストレージ IOPS の経過を示す折れ線グラフでは、データセンターごとにグラフ線を表示してデータをすばやく比較できます。このデータは、次のいずれかの方法で集計できます。

- * Avg * ：収集されたデータの平均値として各行を表示します。
- * 最大 * ：各行を基になるデータの *maximum* として表示します。
- * 最小 * ：各行を基になるデータの *minimum* として表示します。
- * 合計 * ：各行を基になるデータの *SUM*(合計) として表示します。

そのためには、ウィジェットのクエリで、最初にアセットタイプ（_Storage_など）と指標（*IOPS-Total*など）を選択します。[Roll up]*で、集計方法（_avg_など）を選択し、データの集計に使用する属性またはアノテーション（_Data Center_など）を選択します。ウィジェットが自動的に更新され、各データセンターの線が表示されます。

収集されたデータの_all_をグラフまたは表に集計することもできます。この場合、ウィジェットのクエリごとに1本の線が表示され、収集されたすべてのアセットについて、選択した指標の平均値、最小値、最大値、または合計値が表示されます。

クエリにフィルタを設定している場合は、フィルタされたデータに基づいて集計されます。

任意のフィールド（_Model_など）でウィジェットを集計する場合でも、そのフィールドのデータをグラフまたは表に正しく表示するには、そのフィールドのデータを* Filter by *で絞り込む必要があります。

*データの集計：*データポイントを分、時間、日のバケットに集計してから（選択した場合）データを属性別に集計することで、時系列グラフ（折れ線、領域など）をさらに調整できます。データポイントは、[Avg]、[Max]、[Min]、[Sum]のいずれかに基づいて集計するか、選択した間隔で収集された[Last data]ポイントで集計するかを選択できます。集計方法を選択するには、ウィジェットの「クエリ」セクションで「その他のオプション」をクリックします。

指定できる最小間隔は10分です。短い間隔と長い時間範囲を組み合わせると、「集計間隔の結果、データポイントが多すぎます」という結果になることがあります。 警告。間隔が短い場合は、ダッシュボードの期間を 7 日に延長するとこのように表示されることがあります。この場合、より短い期間を選択するまで、集約間隔は一時的に1時間に延長されます。

棒グラフウィジェットおよび単一値ウィジェットでデータを集約することもできます。

ほとんどのアセットカウンタは、デフォルトでは *Avg* に集約されます。一部のカウンタは、デフォルトで_Max_、*Min*、または_Sum_に集約されます。たとえば、デフォルトでは、ポートエラーでアグリゲートは *sum* に、ストレージ *IOPS* アグリゲートは *_Avg* になります。

ダッシュボードウィジェットに上位/下位の結果を表示します

カスタムダッシュボードのグラフウィジェットでは、集計データの上位または下位の結果を表示したり、表示する結果の数を選択したりできます。表ウィジェットでは、表示する行数を選択し、任意の列でソートできます。

グラフウィジェットの上位 / 下位表示機能

グラフウィジェットでは、特定の属性でデータを集計することを選択すると、上位または下位の結果を表示することができます。ただし、 _All_attributes で集計することを選択した場合は、上位または下位の結果を選択することはできません。

表示する結果を選択するには、クエリの * Show * フィールドで * Top * または * Bottom * を選択し、表示されるリストから値を選択します。

表ウィジェットにエントリが表示されます

表ウィジェットでは、表に表示する結果の数を選択できます。5、10、20、50のいずれかの結果を選択できます。表では、いずれかの列を基準に結果を昇順または降順でオンデマンドでソートすることができるため、上位または下位の結果を表示するオプションはありません。

クエリの * エントリの表示 * フィールドから値を選択すると、ダッシュボードのテーブルに表示する結果の数を選択できます。

表示する結果が多いほど、ダッシュボードに保存したウィジェットは長くなります。ウィジェットのサイズを表示されている行数より小さくすることはできません。

表ウィジェットでのグループ化

表ウィジェット内のデータは使用可能な属性別にグループ化できるため、データの概要

だけでなく、データの詳細も確認できます。表内の指標が集計され、各行を折りたためば全体のデータが見やすくなります。

表ウィジェットでは、設定した属性に基づいてデータをグループ化できます。たとえば、ストレージIOPSの合計を、それらのストレージが配置されているデータセンター別に表示できます。また、仮想マシンをホストするハイパーバイザーに従ってグループ化された仮想マシンの表を表示することもできます。リストで各グループを展開すると、そのグループのアセットが表示されます。

グループ化は、* Table *ウィジェットタイプでのみ使用できます。

パフォーマンスデータの集計

表ウィジェットにパフォーマンスデータの列（ *iops-Total* など）を含める場合は、データのグループ化を選択する際に、その列の集計方法を選択できます。デフォルトの集計方法では、グループ行の基になるデータの_average_が表示されます。また、データの_sum_、*minimum*、または_maximum_を表示するように選択することもできます。

グループ化の例（集計の説明を含む）

表ウィジェットでは、データをグループ化して見やすくすることができます。

このタスクについて

この例では、すべての VM をデータセンター別にグループ化して表示する表を作成します。

手順

1. ダッシュボードを作成または開き、 * 表 * ウィジェットを追加します。
2. このウィジェットのアセットタイプとして*[Virtual Machine]*を選択します。
3. 列セレクタをクリックします [*Hypervisor name_and_IOPS - Total*]を選択します。

   表にこれらの列が表示されます。

4. IOPS がない VM は無視し、合計 IOPS が 1 を超える VM だけを表示するように設定します。[Filter by]+ボタンをクリックし、[IOPS - Total]を選択します。**[*any**]をクリックし、[**from**]フィールドに「1」と入力します。[* から *] フィールドは空のままにします。チェックボタンをクリックしてフィルタを適用します。

   これで、合計 IOPS が 1 以上の VM がすべて表示されます。この表にはグループ化はありません。すべての VM が表示されている。

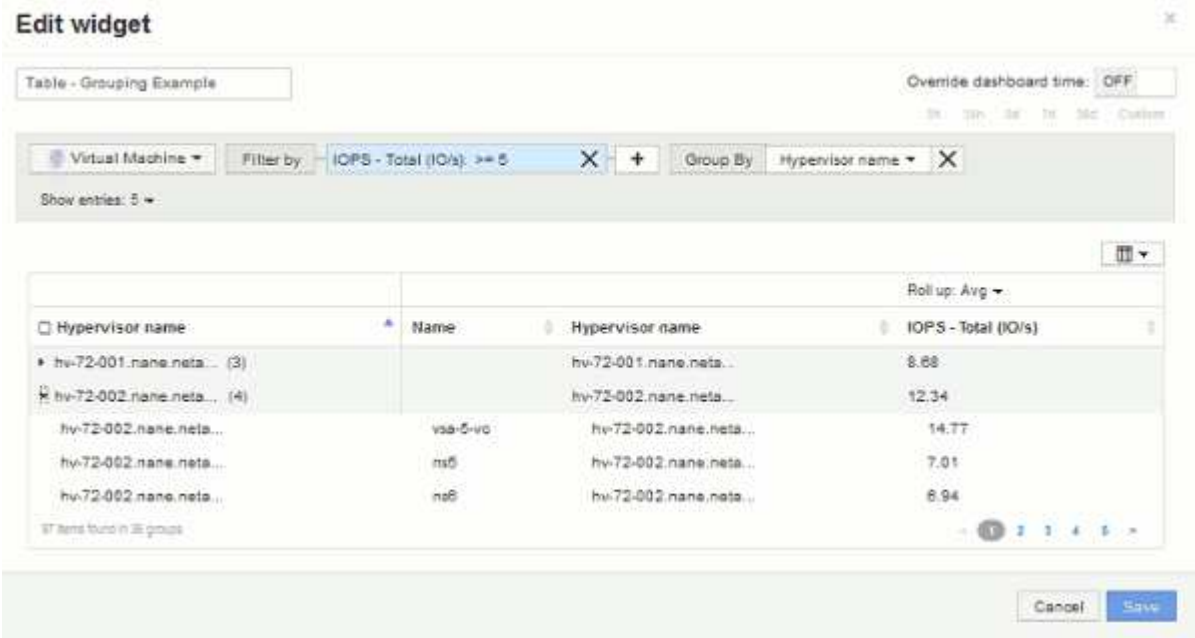
5. [+でグループ化]ボタンをクリックします。

   グループ化方法としてデフォルトで* all *が選択されているため、すべてのVMが「all」という名前の1つのグループに移動されます。

6. IOPS - Total_columnの上に* Roll up *オプションが表示されます。デフォルトの集計方法は *Avg* です。つまり、このグループに表示されている数値は、グループ内の各 VM の合計 IOPS の平均値です。この列を_Avg_、*Sum*、*Min*、_Max_でロールアップすることができます。表示された列にパフォーマンス指標が含まれている場合は、それぞれ個別に集計することができます。

7. をクリックし、[ハイパーバイザー名]*を選択します。

   VM のリストがハイパーバイザーでグループ化されます。各ハイパーバイザーを展開すると、そのハイパーバイザーがホストしている VM を表示できます。



8. [保存（ Save ）] をクリックして、テーブルをダッシュボードに保存します。ウィジェットのサイズを変更できます。
9. 保存 * をクリックしてダッシュボードを保存します。

個 々 のウィジェットでダッシュボードの時間を上書きする

メインダッシュボードの期間設定は、ウィジェットごとに無効にすることができます。これらのウィジェットでは、ダッシュボードの期間ではなく、各ウィジェットに対して設定された期間に基づいてデータが表示されます。

ダッシュボードの時間を上書きしてウィジェットで独自の期間を使用するには、ウィジェットの編集モードで*を[On]に設定し、ウィジェットの期間を選択します。 ウィジェットをダッシュボードに保存します。

ウィジェットには、ダッシュボードで選択した期間に関係なく、設定した期間に従ってデータが表示されます。

ウィジェットに対して設定した期間は、ダッシュボード上の他のウィジェットには影響しません。

1次軸と**2**次軸について説明します

2番目の軸を使用すると、異なる測定単位を使用する2つの異なる値セットのデータを簡単に表示できます。

このタスクについて

グラフに表示されるデータには、指標ごとに使用する測定単位が異なります。たとえば、 IOPS の測定単位は 1 秒あたりの I/O 処理数（ IO/s ）であるのに対し、レイテンシは単純に時間（ミリ秒、マイクロ秒、秒など

）で測定されます。これらの両方の指標を、 Y 軸で 1 つの値セットを示す 1 つの折れ線グラフに出力すると、レイテンシの数値（通常は数ミリ秒単位）が IOPS （通常は数千単位）と同じ目盛りで表示されるため、レイテンシの線が見えなくなります。

ただし、一次（左側）の Y 軸に測定単位を 1 つ設定し、二次（右側）の Y 軸にもう一方の測定単位を設定することで、両方のデータセットをわかりやすい 1 つのグラフにまとめることができます。これで、個々の指標がそれぞれの目盛りで出力されます。

手順

1. ダッシュボードを作成するか、開きます。[Line chart]、[* spline chart]、[* area chart]、または[* stacked area chart]ウィジェットをダッシュボードに追加します。
2. アセットタイプ（* Storage など）を選択し、最初の指標として IOPS - Total *を選択します。必要なフィルタを設定し、必要に応じて集計方法を選択します。

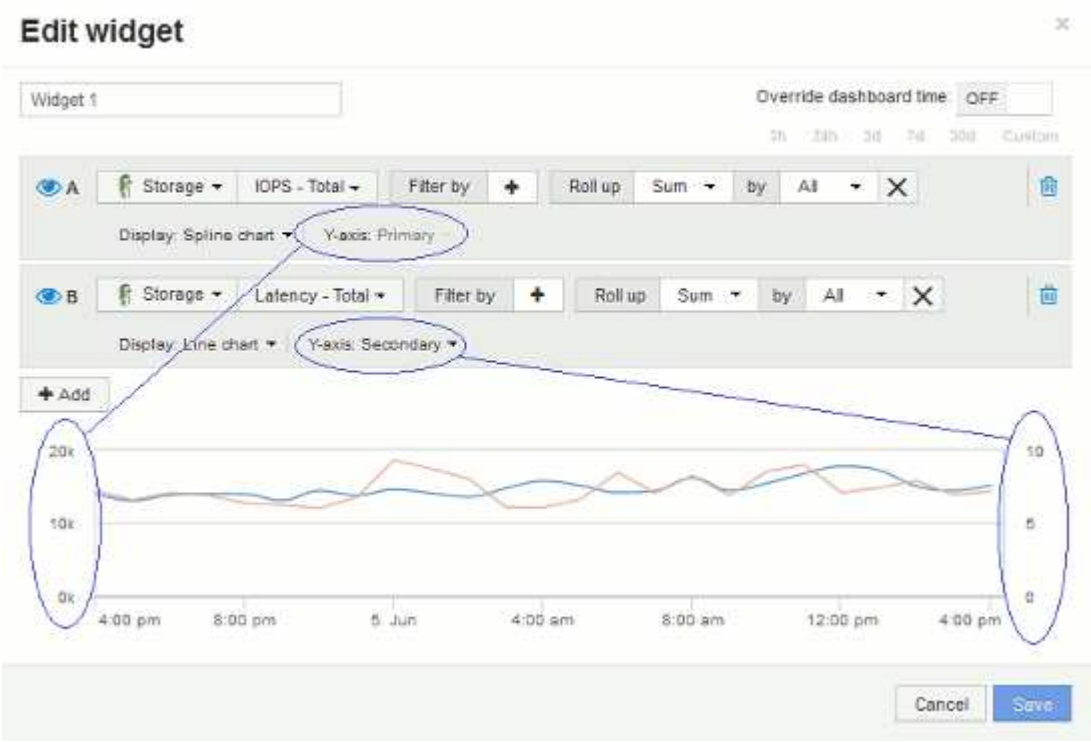
   折れ線グラフに IOPS の線が出力され、左側に目盛りが表示されます。

3. をクリックして、グラフに**2**行目を追加します。この線では、指標として[Latency - Total]*を選択します。

   グラフの下部にこの線が表示されます。これは、IOPSの線と同じ目盛りで描画されているためです。

4. レイテンシクエリで、 * Y 軸：セカンダリ * を選択します。

   これで Latency の線が Latency 用の目盛りでグラフの右側に表示されます。



ダッシュボードウィジェットの式

時系列ウィジェットの式を使用すると、選択した指標を使用して計算に基づいてデータを表示できます。

ダッシュボードでは、任意の時系列ウィジェット（折れ線、スプライン、面、積み上げ面）を使用して選択した指標で式を作成し、その計算結果を 1 つのグラフに表示できます。次の例では、式を使用して特定の問題を解決します。最初の例は、環境内のすべてのストレージアセットの合計 IOPS に占める読み取り IOPS の割合を表示するウィジェットです。2つ目の例では、環境で発生する「システム」IOPSや「オーバーヘッド」IOPS、つまりデータの読み取りや書き込み以外のIOPSを可視化しています。

式の例：読み取り**IOPS**の割合

式を使用すると、合計に対する割合など、別の方法で指標を表示できます。

このタスクについて

この例では、合計IOPSに占める読み取りIOPSの割合を表示します。これは次の式と考えることができます。

- 読み取りの割合=（読み取りIOPS /合計IOPS）x 100

このデータは、ダッシュボードに折れ線グラフで表示できます。これを行うには、次の手順を実行します。

手順

1. 新しいダッシュボードを作成するか、既存のダッシュボードを*編集モード*で開きます。
2. ダッシュボードにウィジェットを追加します。[* Area chart* （エリアグラフ * ）] を

   ウィジェットが編集モードで開きます。デフォルトでは、ストレージ*アセットの IOPS -合計*を示すクエリが表示されます。必要に応じて、別のアセットタイプを選択します。

3. [Convert to Expression]*ボタンをクリックします。

   現在のクエリが式モードに変換されます。式モードのときはアセットタイプを変更できません。式モードでは、ボタンが*[クエリに戻す]*に変わります。いつでもクエリモードに切り替えるには、このボタンをクリックします。モードを切り替えるとフィールドがデフォルトにリセットされるので注意してください。

   ここでは、* Expression *モードのままにします。

4. 指標がアルファベット変数フィールド「**`a'`**」に表示されるようになりました。**[`b]**変数フィールドで、[Select]をクリックし、[IOPS - Read]*を選択します。

   変数フィールドの後にある**+**ボタンをクリックすると、式に合計5つのアルファベット変数を追加できます。読み取りの割合の例では、合計IOPS（「a」）と読み取りIOPS（「b」）のみが必要です。

5. [**Expression**] フィールドでは、各変数に対応する文字を使用して式を作成します。読み取りIOPSの割合=（読み取りIOPS /合計IOPS）x 100_であることがわかっているため、次のように式を書きます。`(b / a) * 100`
6. **Label** フィールドは、式を識別します。ラベルを"`Read Percentage`"に変更するか、同様に意味のあるものに変更してください。
7. * Units *フィールドを"`%`"または"`percent`"に変更します。

   グラフに、選択したストレージデバイスの読み取り IOPS の割合が時系列で表示されます。必要に応じて、フィルタを設定するか、別の集計方法を選択できます。集計方法として* Sum *を選択すると、すべてのパーセント値が合計され、100%を超える可能性があることに注意してください。

8. グラフをダッシュボードに保存するには、 * 保存 * をクリックします。

   折れ線グラフ、スプライングラフ、または*積み上げ面グラフ*ウィジェットでも式を使用できます。

式の例：システム **I/O**

式を使用すると、他の指標から計算できるデータを自由にグラフ化できます。

このタスクについて

例2：OnCommand Insight はデータソースから多数の指標を取得します。その中には、読み取り、書き込み、合計IOPSがあります。ただし、収集によって報告されるIOPSの合計に「システム」IOPSが含まれることがあります。これは、データの読み取りや書き込みの直接的な一部ではないI/O処理です。このシステム I/O はオーバーヘッド I/O と考えることもできますが、適切なシステム運用には必要ですが、データの運用には直接関係しているわけではありません。

これらのシステム I/O を表示するには、収集によって報告された合計 IOPS から読み取り IOPS と書き込み IOPS を差し引きます。式は次のようになります。

- システムIOPS =合計IOPS -（読み取りIOPS +書き込みIOPS）

このデータは、ダッシュボードに折れ線グラフで表示できます。これを行うには、次の手順を実行します。

手順

1. 新しいダッシュボードを作成するか、既存のダッシュボードを*編集モード*で開きます。
2. ダッシュボードにウィジェットを追加します。「 * 線グラフ * 」を選択します。

   ウィジェットが編集モードで開きます。デフォルトでは、ストレージ*アセットの IOPS -合計*を示すクエリが表示されます。必要に応じて、別のアセットタイプを選択します。

3. ボタンをクリックして、クエリのコピーを作成します。

   重複するクエリが元のクエリの下に追加されます。

4. 2 番目のクエリで、 * 式に変換 * ボタンをクリックします。

   現在のクエリが式モードに変換されます。いつでもクエリモードに切り替えるには、 [クエリに戻る] をクリックします。モードを切り替えるとフィールドがデフォルトにリセットされるので注意してください。

   ここでは、* Expression *モードのままにします。

5. 指標がアルファベット変数フィールド「`**a'**」に表示されるようになりました。**[IOPS - Total]***をクリックし、[IOPS - Read]*に変更します。。
6. [b]変数フィールドで、**[Select]***をクリックし、[IOPS - Write]*を選択します。
7. [**Expression**] フィールドでは、各変数に対応する文字を使用して式を作成します。ここでは、単純に次のように式を記述します。 `a + b`。[**Display**]セクションで、この式に[*** Area chart**]を選択します。
8. **Label** フィールドは、式を識別します。ラベルを「システムIOPS」に変更するか、同等の意味のあるものに変更します。

合計 IOPS の折れ線グラフが表示され、その下に読み取り IOPS と書き込み IOPS を組み合わせた面グラフが表示されます。この 2 つのグラフの間が、データの読み取り処理や書き込み処理に直接関係していない IOPS を表します。

9. グラフをダッシュボードに保存するには、 * 保存 * をクリックします。

カスタムダッシュボード：仮想マシンのパフォーマンス

OnCommand Insightのカスタムダッシュボードとウィジェットを使用して、インベントリやパフォーマンスの傾向を運用ビューで確認できます。

このタスクについて

現在、 IT 運用が直面している課題は多数あります。管理者は少ないリソースでより多くの成果を達成するよう求められており、動的なデータセンターを完全に可視化することは必須条件です。この例では、環境内の仮想マシンのパフォーマンスに関する運用状況を把握できるウィジェットを使用したカスタムダッシュボードを作成する方法を説明します。この例を実行し、独自のニーズに合わせてウィジェットを作成することで、フロントエンド仮想マシン（VM）のパフォーマンスとバックエンドストレージのパフォーマンスの比較を可視化したり、VMのレイテンシとI/O要求を表示したりできます。

カスタムダッシュボードを使用すると、作業の優先順位を設定し、利用可能なリソースを特定できます。ワークロードの増減に対応し、新たな問題の検出と修正にかかる時間を最小限に抑えることができます。カスタムダッシュボードを使用すると、ビジネスクリティカルなインフラを優先度の高いビューで表示でき、マルチベンダーのテクノロジ全体でパフォーマンスの可用性を特定するのに役立ちます。

ここでは、以下を含む仮想マシンのパフォーマンス用ダッシュボードを作成します。

- VM 名とパフォーマンスデータをリストするテーブル
- VM のレイテンシをストレージのレイテンシと比較するグラフ
- VM の読み取り IOPS 、書き込み IOPS 、合計 IOPS を示すグラフ
- VM の最大スループットを示すグラフ

ここで紹介するのは基本的な例です。ダッシュボードをカスタマイズして、運用のベストプラクティスに合わせてパフォーマンスデータをハイライト表示し、比較することができます。

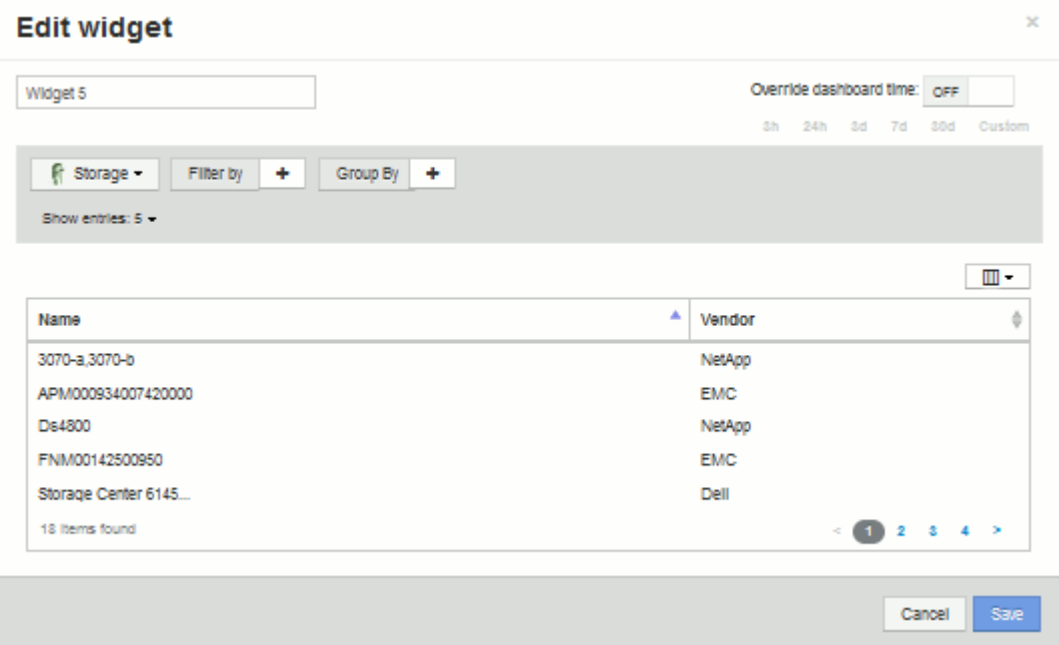
手順

1. 管理者権限を持つユーザとして Insight にログインします。
2. メニューから、**[**+New dashboard]*を選択します。

   [New dashboard]ページが開きます。

3. ダッシュボードにわかりやすい名前を付けましょう。[保存（ Save ）] をクリックします。[名前]フィールドに、ダッシュボードの一意の名前を入力します（例：「VM Performance by Application」）。
4. 「 * 保存 * 」をクリックして、ダッシュボードに新しい名前を付けて保存します。
5. 次に、ウィジェットを追加します。必要に応じて、「編集」スイッチを「オン」にスライドして編集モードを有効にします。
6. ボタンをクリックし、[Table widget]*を選択して新しい表ウィジェットをダッシュボードに追加します。

ウィジェットを編集（ Edit Widget ）ダイアログが開きます。デフォルトの名前は「Widget 1」で、環境内のすべてのストレージに関するデフォルトのデータが表示されます。



7. このウィジェットをカスタマイズできます。[Name]フィールドで「Widget 1」を削除し、「Virtual Machine Performance table」と入力します。
8. アセットタイプのドロップダウンをクリックし、**[**ストレージ**]***を[仮想マシン]*に変更します。

   表のデータが更新され、環境内のすべての仮想マシンが表示されます。現時点では、この表にはVM名のみが表示されています。表に列をいくつか追加してみましょう。

9. [列]*をクリックします ボタンをクリックして、_ Data Center_、ストレージ名、_ IOPS - Total_を選択します。検索に名前を入力して、目的のフィールドをすばやく表示することもできます。

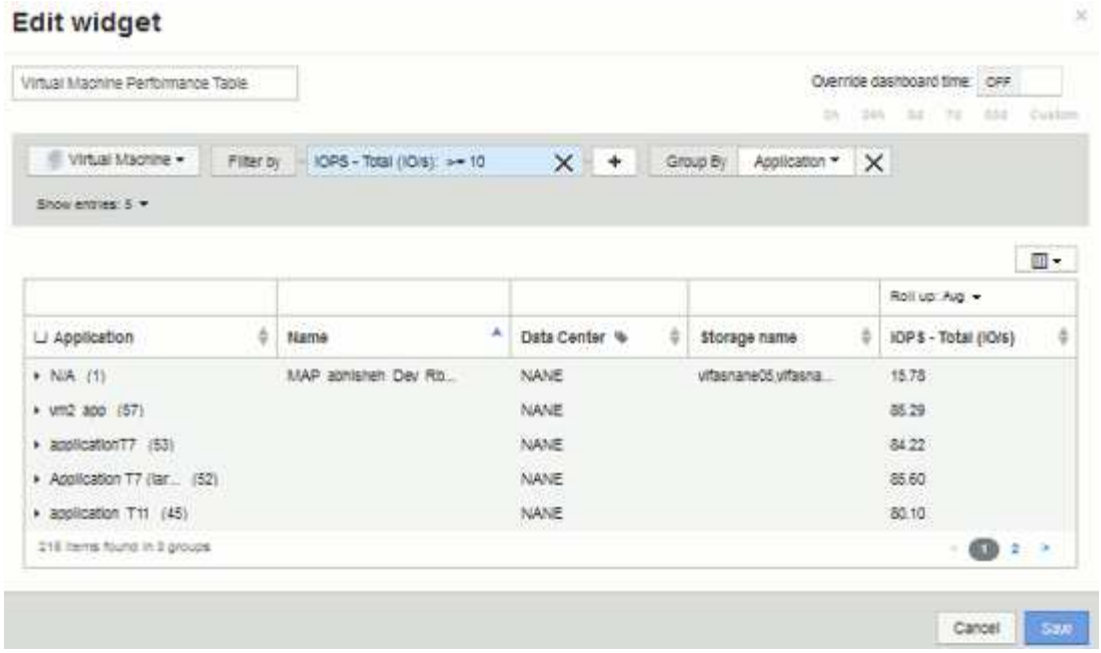
   これらの列が表に表示されます。これらの列のいずれかを使用してテーブルをソートできます。列はウィジェットに追加した順序で表示されます。

10. この演習では、あまり使用されていない VM は除外するため、合計 IOPS が 10 未満のものをフィルタで除外します。の横にある**[+]**ボタンをクリックし、***IOPS - Total***（***IO/s***）**_**を選択します。**[*any**]をクリックし、[**from**]フィールドに「10」と入力します。[* から *] フィールドは空のままにします。をクリックします ボタンをクリックしてフィルタを保存します。

    これで、合計 IOPS が 10 以上の VM のみが表に表示されます。

11. 結果をグループ化すると、表をさらに折りたたむことができます。[グループ化]*の横にある[+]ボタンをクリックし、グループ化に使用するフィールド（[アプリケーション]、[クラスタ]など）を選択します。グループ化が自動的に適用されます。

    これで、設定に従ってテーブルの行がグループ化されます。グループは必要に応じて展開または折りたたむことができます。グループ化された行には、各列の集計データが表示されます。一部の列では、その列の集計方法を選択できます。



12. 表ウィジェットをカスタマイズしたら、*[Save]*ボタンをクリックします。

    表ウィジェットがダッシュボードに保存されます。

13. ダッシュボード上のウィジェットの右下をドラッグすると、ウィジェットのサイズを変更できます。すべての列が明確に表示されるようにウィジェットの幅を広げます。保存 * をクリックして、現在のダッシュボードを保存します。

14. 次に、 VM のパフォーマンスを表示するグラフをいくつか追加します。VMのレイテンシとストレージのレイテンシを比較する折れ線グラフを作成します。

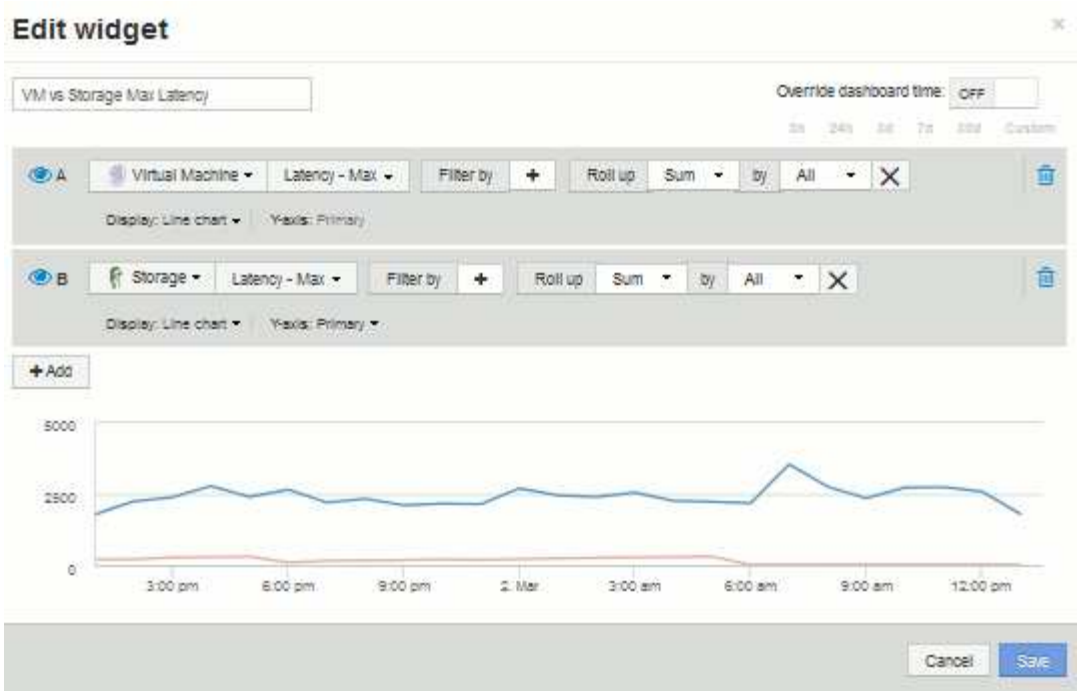
15. 必要に応じて、「編集」スイッチを「オン」にスライドして編集モードを有効にします。

16. [Widget]*ボタンをクリックし、[Line Chart]*を選択して新しい折れ線グラフウィジェットをダッシュボードに追加します。

    ウィジェットを編集（ Edit Widget ）ダイアログが開きます。[Name]*フィールドをクリックし、このウィジェットの名前を「VM vs Storage Max Latency」に変更します。

17. を選択し、[レイテンシ-最大]を選択します。任意のフィルターを設定するか、 * フィルターを * 空のままにします。「*ロールアップ」では、「すべて」で「合計」を選択します。このデータは**Line Chart**として表示し、Y-Axisは* Primary *のままにします。

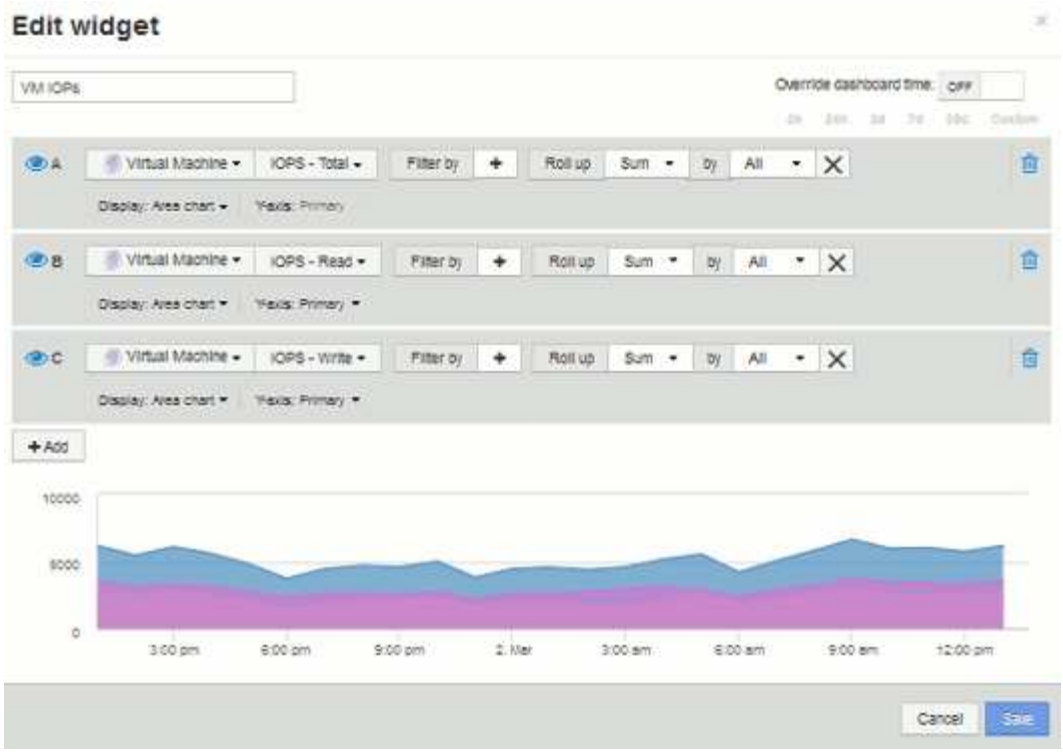
18. ボタンをクリックして、**2**行目のデータ行を追加します。この線では、[ストレージ]と[レイテンシ-最大]を選択します。任意のフィルターを設定するか、 * フィルターを * 空のままにします。「*ロールアップ」では、「すべて」で「合計」を選択します。このデータは**Line Chart**として表示し、Y-Axisは* Primary *のままにします。



19. [保存]*をクリックして、このウィジェットをダッシュボードに追加します。
20. 次に、 VM の読み取り IOPS 、書き込み IOPS 、合計 IOPS を 1 つのグラフに表示するグラフを追加します。
21. ボタンをクリックし、[Area Chart]*を選択して新しい面グラフウィジェットをダッシュボードに追加します。

    ウィジェットを編集（ Edit Widget ）ダイアログが開きます。[Name]*フィールドをクリックし、このウィジェットに「VM IOPS」という名前を付けます。

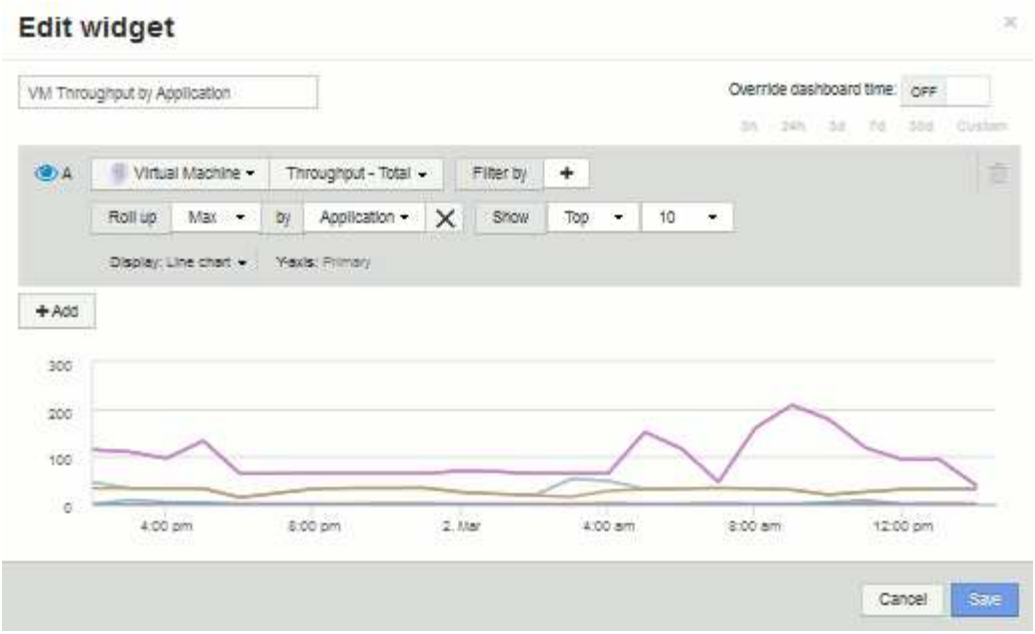
22. を選択し、[IOPS - Total]を選択します。任意のフィルターを設定するか、 * フィルターを * 空のままにします。「*ロールアップ」では、「すべて」で「合計」を選択します。このデータを**Area Chart**として表示し、Y-Axisは* Primary *のままにします。
23. [+ Add]ボタンをクリックして、2つ目のデータ行を追加します。この行では、**[Virtual Machine]***を選択し、[IOPS - Read]を選択します。**[Y-Axis]**は[Primary]*のままにします。
24. [+ Add]ボタンをクリックして、3つ目のデータ行を追加します。この行では、**[Virtual Machine]***を選択し、[IOPS - Write]を選択します。**[Y-Axis]**は[Primary]*のままにします。



25. [保存]*をクリックして、このウィジェットをダッシュボードに追加します。
26. 次に、 VM に関連付けられているアプリケーションごとに VM のスループットを表示するグラフを追加します。これにはロールアップ機能を使用します。
27. [Widget]*ボタンをクリックし、[Line Chart]*を選択して新しい折れ線グラフウィジェットをダッシュボードに追加します。

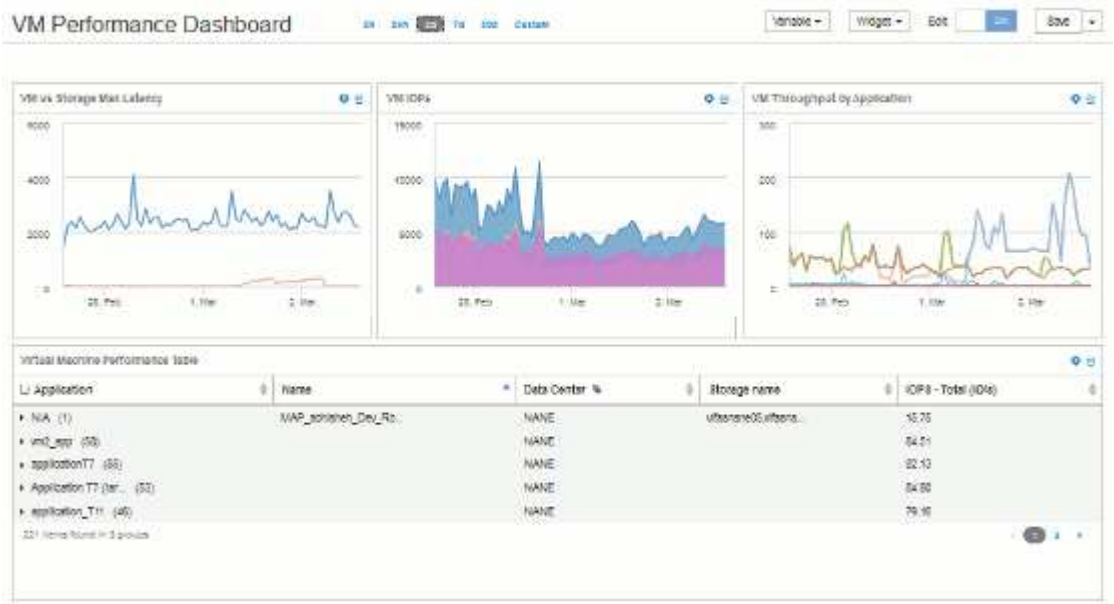
    ウィジェットを編集（ Edit Widget ）ダイアログが開きます。[Name]*フィールドをクリックし、このウィジェットに「VM Throughput by Application」という名前を付けます。

28. を選択し、[スループット-合計]を選択します。任意のフィルターを設定するか、 * フィルターを * 空のままにします。*ロールアップ*では、「最大」を選択し、「アプリケーション」または「名前」を選択します。トップ**10** *アプリケーションを表示します。このデータは**Line Chart**として表示し、**Y-Axis**はPrimary *のままにします。



29. [保存]*をクリックして、このウィジェットをダッシュボードに追加します。
30. ウィジェットを移動するには、ウィジェット上部の任意の場所でマウスボタンを押したまま新しい場所にドラッグします。ウィジェットの右下をドラッグすると、ウィジェットのサイズを変更できます。変更を行ったら、必ずダッシュボードを*保存*してください。

    最終的なVMパフォーマンスダッシュボードは次のようになります。



変数を含むストレージノードの利用率ダッシュボードの例

ストレージ、ストレージプール、ノード、階層、利用率、レイテンシに変数を使用するStorage Analysis 用のカスタムダッシュボードを作成します。

作業を開始する前に

Insightのダッシュボードについてよく理解しておくことを推奨しますが、必須ではありません。

このタスクについて

次の手順では、ストレージ、ストレージプール、ノード、階層、利用率、およびレイテンシに変数を使用する、カスタムの Storage Analysis Overview ダッシュボードを作成します。次の例の変数を使用して、ダッシュボードで使用できる 1 つ以上のウィジェットで表示するアセットや指標をフィルタリングします。これらの変数をフィルタとして使用するウィジェットは、ダッシュボードの変数フィールドに入力した値に従ってフィルタされたコンテンツをオンデマンドで表示するように更新されます。これにより、複数のグラフやグラフをすばやくフィルタして、関心のある特定の領域にドリルダウンできます。

この例の手順に従って、次のようなダッシュボードを作成します。これらのウィジェットを変更したり、任意の数のウィジェットを追加して、選択したデータを強調表示することができます。

手順

1. 新しいダッシュボードを作成し、「Analysis：Storage Overview」という名前か、わかりやすい名前を付けます。
2. ドロップダウンをクリックし、[テキスト（Text）]*変数タイプを選択します。デフォルトでは、変数の名前は_$var1_です。[*$var1*]をクリックして名前を編集し、[*$storage*]に変更してから、チェックマークをクリックして変数を保存します。を繰り返して、*$NODE*、*$POOL*、および_$VOLUME_のテキスト変数を作成します。
3. 上記のプロセスを繰り返して、*$ utilization*_および$ latency _という名前の* number *タイプの変数を作成します。
4. [Variable]*ドロップダウンをクリックし、*Tier_annotation*を検索します。これを選択して、$tier_という名前の変数を作成します。

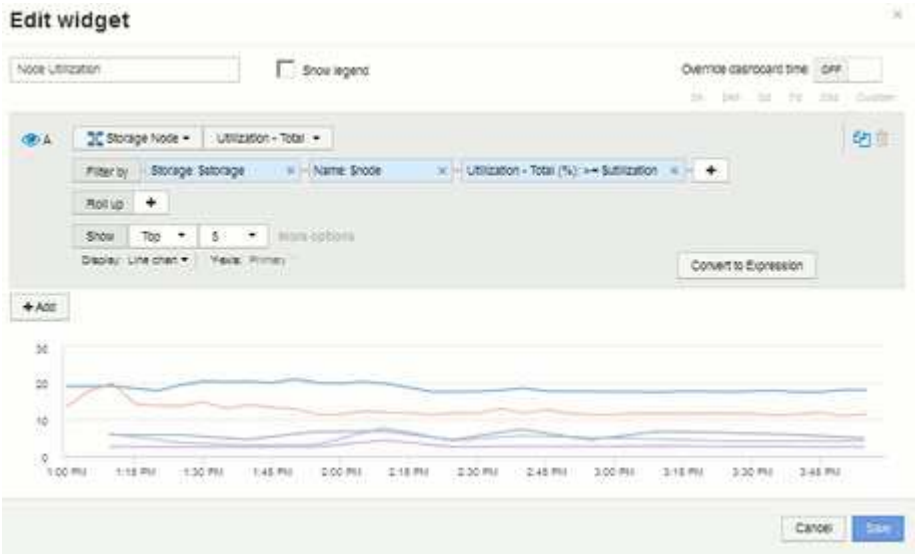
変数はいつでも追加できますが、あらかじめ作成しておくと簡単に作成できるため、作成時にすべてのウィジェットで使用できるようになります。

5. ウィジェットを追加するには、[Widget]ドロップダウンをクリックし、[***line chart**]または[**area chart**]ウィジェットを選択します。ウィジェットに「Node Utilization」という名前を付けます。アセットタイプ*をクリックし、[ストレージノード]に変更します。グラフデータとして Utilization - Total *を選択します。
6. [+でフィルタ]ボタンをクリックしてフィルタを追加します。を検索して選択し、[Any]*をクリックして_$storage_variableを選択します。
7. **+**ボタンをクリックして、*Name*に別のフィルタを追加します。変数を_$NODE_に設定します。

   アノテーション名フィルタには、さまざまな変数を割り当てることができます。ウィジェットのオブジェクトに応じて、名前と変数のペアを最下位レベルで使用します。例：

   - ノードにフォーカスしたウィジェットの* Name *フィルタに_$node_variableを割り当てることができます。
   - プールに焦点を当てたウィジェットの* Name *フィルタに_$pool_variableを割り当てることができます。
8. [**+**]ボタンをクリックして、* Utilization - Total (%)*用の別のフィルタを追加します。変数を_>=$utilization_に設定します。
9. フィールドを折りたたむには、[*ロールアップ]フィールドの後にある[*X]をクリックします。
10. を選択し、[Save]*をクリックしてウィジェットを保存し、ダッシュボードに戻ります。

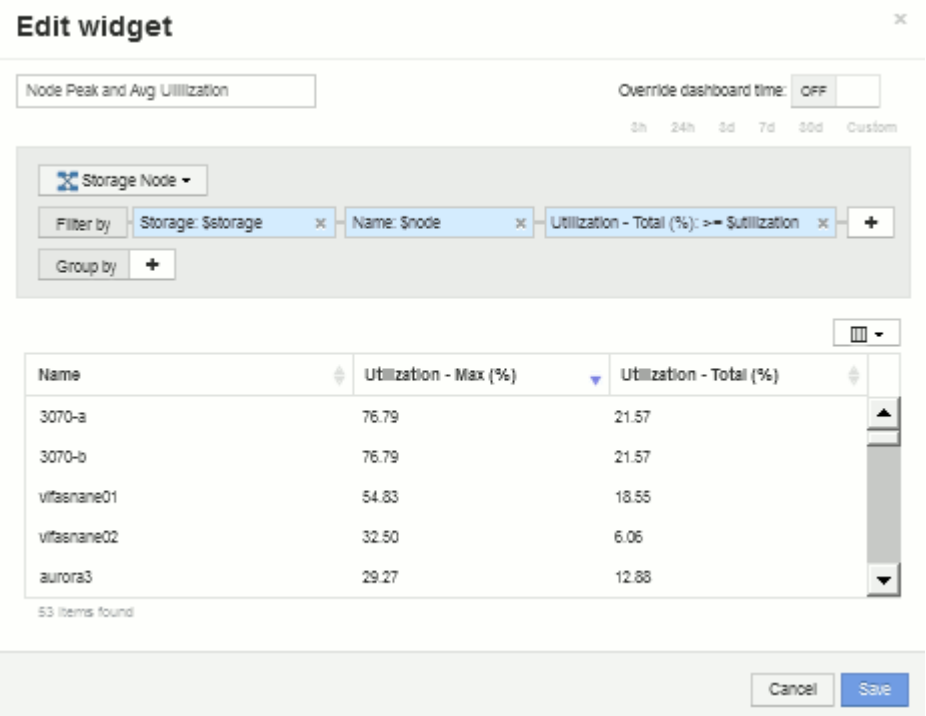
    ウィジェットは次のようになります。



11. 別の折れ線グラフウィジェットまたは面グラフウィジェットをダッシュボードに追加します。アセットタイプとして*を選択し、グラフの指標として[レイテンシ-合計]*を選択します。
12. [+でフィルタ]ボタンをクリックして、**[**ストレージ：**$STORAGE]***および[名前：$NODE]*のフィルタを追加します。
13. のフィルタを追加し、$latency *変数を選択します。
14. ウィジェットに「Node Latency」という名前を付けて保存します。
15. サポートテーブルを追加すると、作成したグラフの詳細（最大ノード利用率や平均ノード利用率など）を

表示できます。ダッシュボードに* Tableウィジェット*を追加し、アセットタイプとして* Storage Node を選択して、 Storage：$storage 、 Name：$node 、 Utilization - Total：$utilization *のフィルタを作成します。

16. 表に、* Utilization - Max 、 Utilization - Total *、またはその他の必要な列を追加します。
17. ウィジェットに「Node Peak and Avg Utilization」という名前を付けて保存します。



18. 同じ手順を繰り返して、[ノードレイテンシ]の表を作成します。必要に応じて*、[レイテンシ-合計]*、またはその他の列が表示されます。
19. ダッシュボードを全体的に表示するには、次の一部またはすべてのグラフウィジェットと表ウィジェットを追加します。

チャート	表
ストレージプール利用率	ストレージプールの最大利用率と平均利用率
ストレージプールのスループット	ストレージプールの最大スループットと平均スループット
ボリュームレイテンシ	ボリュームの最大レイテンシと平均レイテンシ
Volume IOPS の略	ボリュームの最大IOPSと平均IOPS

1. ウィジェットは、ダッシュボードのどの位置にでも移動したり、サイズを変更したりできます。完了したら、必ず*[保存]*ダッシュボードを保存します。

   最後のダッシュボードは次のようになります。

2. 変数を使用して、ダッシュボード内の特定のアセットに絞り込むことができます。変数フィールドに値を入力すると、ウィジェットが自動的に更新されて変数が反映されます。たとえば、$utilization変数フィールドに「15」と入力すると、その変数を使用するウィジェットには、合計利用率が15%以上のアセットのみが表示されます。

   ノード利用率ウィジェットに表示されたすべてのノードのうち上位 5 つを表示：

ノード利用率ウィジェットに使用率が 15% 以上のノードが表示されている場合：

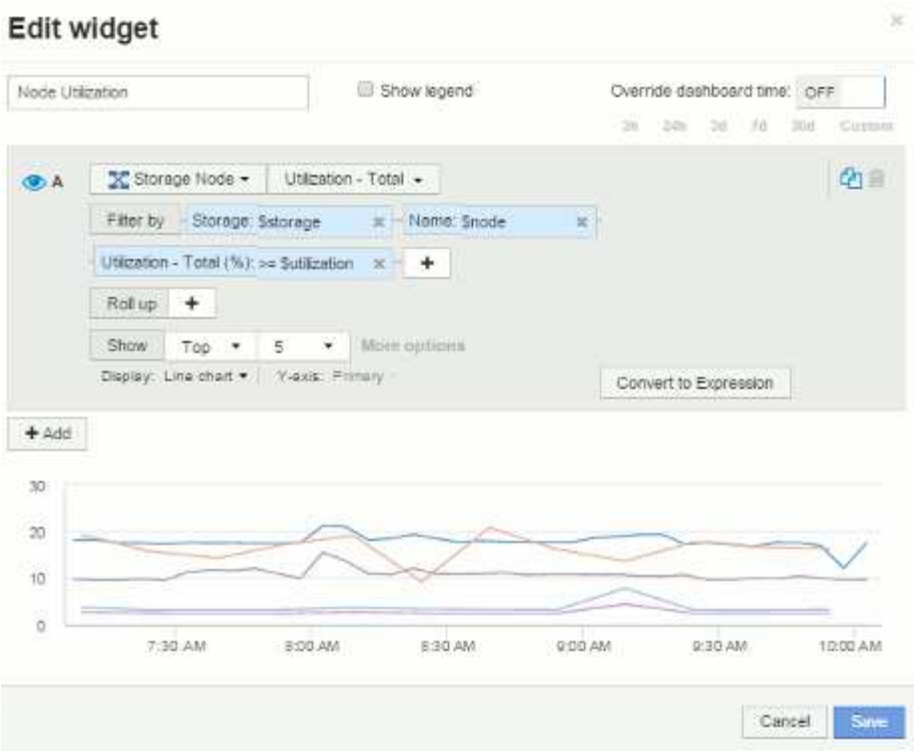
3. ウィジェットを作成する際は、次の点に注意してください。
   - $tier変数は、* Tier *アノテーションでアノテートされているリソースにのみ影響します。
   - ウィジェットが指定した変数を受け入れるように設計されているかどうかによっては、すべてのフィルタがすべてのウィジェットに影響するわけではありません。
   - 数値変数は、指定された値の"`greater than or equal"として適用されます。ストレージ階層のどのレベルのウィジェットでも、ウィジェットの実行元のアセットに対して変数が有効であれば、任意の変数をフィルタとして使用できます。ノードレベルからストレージプールからボリュームウィジェットに移動すると、フィルタとして割り当てる変数が増えます。たとえば、Storage Nodeレベルのウィジェットでは、*Storage_and_Name_*変数をフィルタとして割り当てることができます。ストレージプールレベルでは、_ストレージ、ノード、ストレージプール、_名前_がすべて使用可能です。必要に応じて変数を割り当て、スタック内の最下位レベルで $name 変数を使用します。これにより、ウィジェットを実行している実際のアセット名で $ name 変数をフィルタできます。

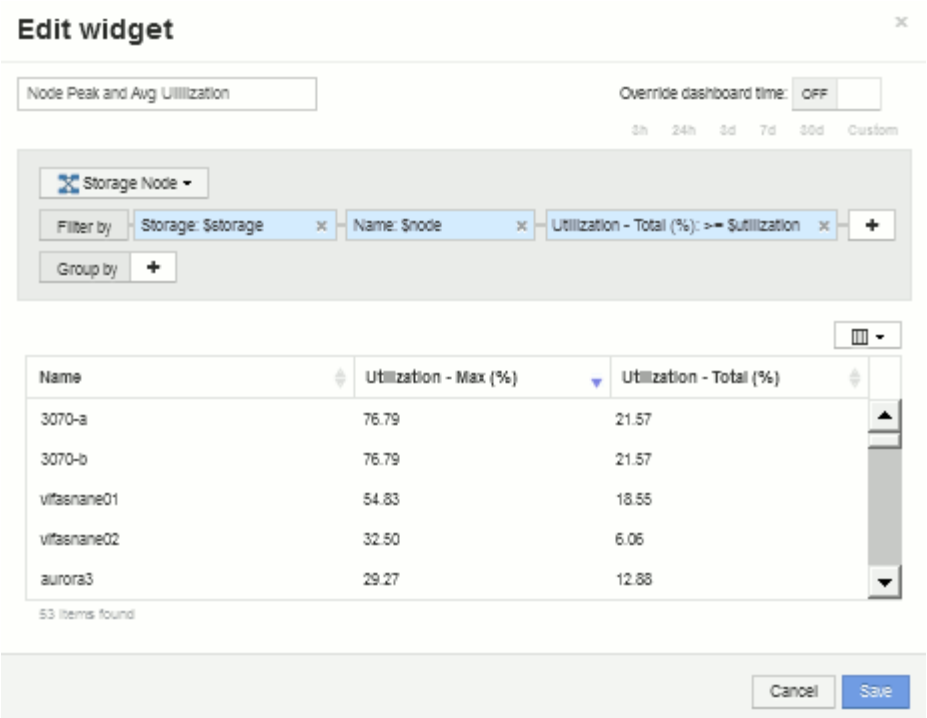
ノードダッシュボードウィジェットの設定例

ノードダッシュボードのウィジェット設定と変数の例。

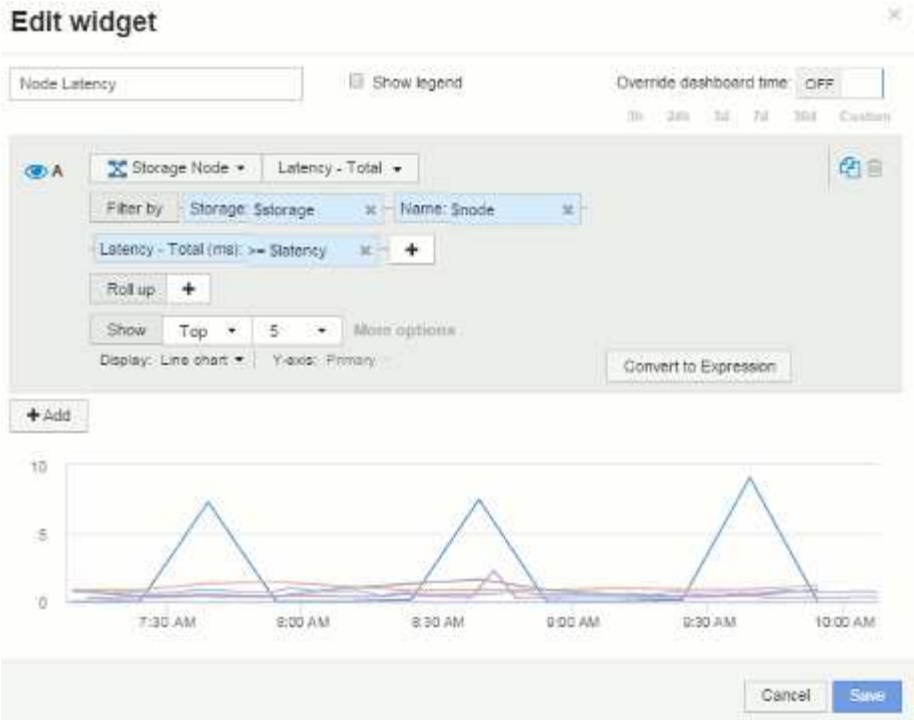
以下は、ストレージノードダッシュボードの各ウィジェットの設定例です。

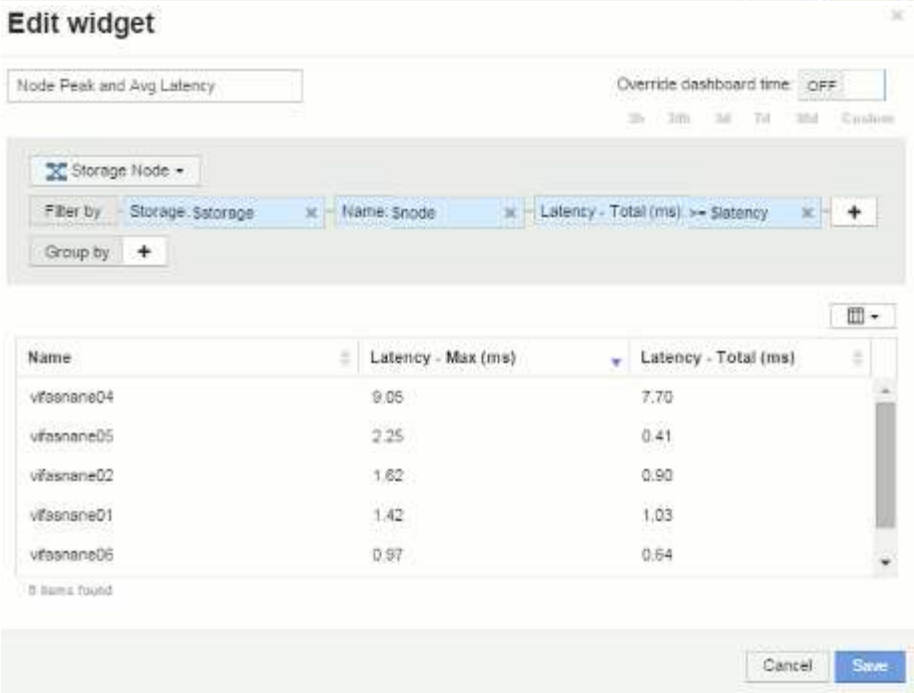
ノード利用率：


Edit widget
Node Utilization
Show legend
Override dashboard time:
OFF
A
Storage Node
Utilization - Total
Filter by
Storage: $storage
Name: $node
Utilization - Total (%): >= $utilization
Roll up
Show
Top
5
More options
Display: Line chart
Y-axis: Primary
Convert to Expression
Add
30
20
10
0
7:30 AM
8:00 AM
8:30 AM
9:00 AM
9:30 AM
10:00 AM
Cancel
Save

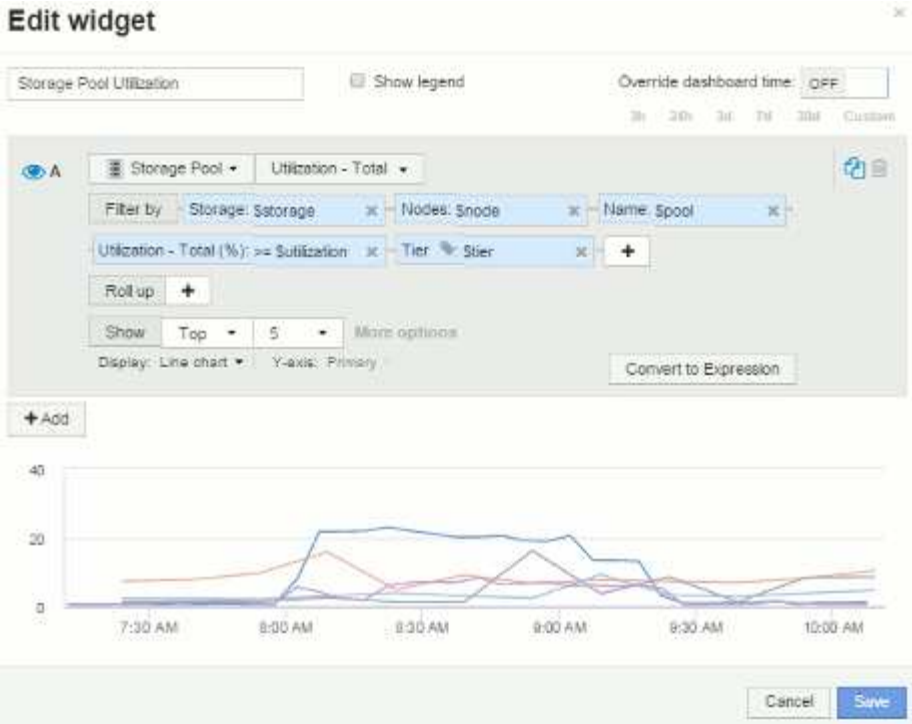

Edit widget
Node Peak and Avg Utilization
Override dashboard time:
OFF
Storage Node
Filter by
Storage: $storage
Name: $node
Utilization - Total (%): >= $utilization
Group by
Name
Utilization - Max (%)
Utilization - Total (%)
3070-a
76.79
21.57
3070-b
76.79
21.57
vifasnane01
54.83
18.55
vifasnane02
32.50
6.06
aurora3
29.27
12.88
53 items found
Cancel
Save

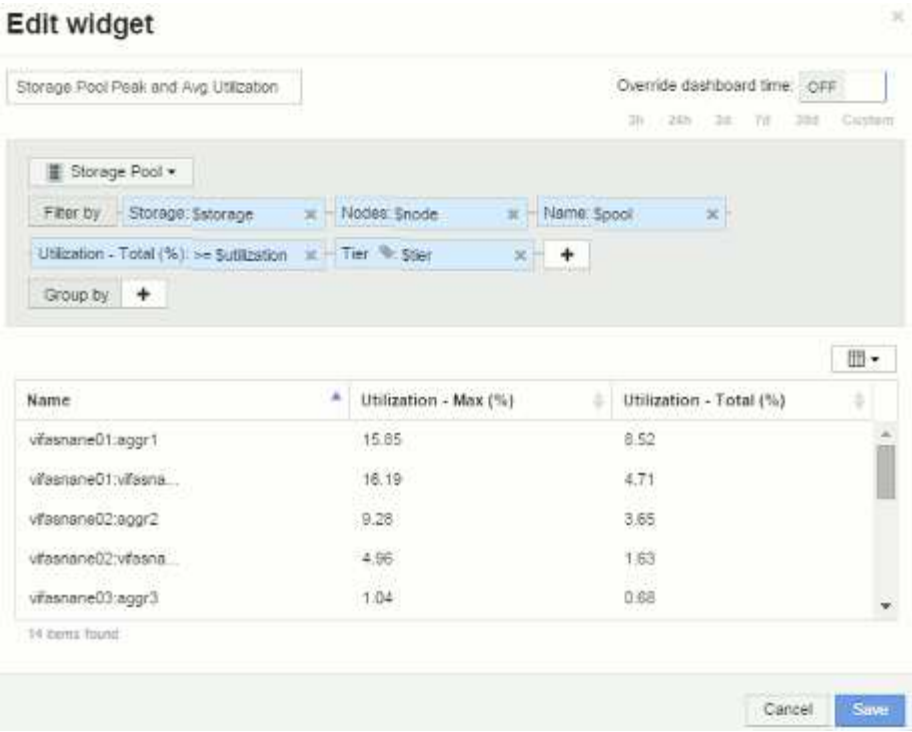
ノードのレイテンシ：



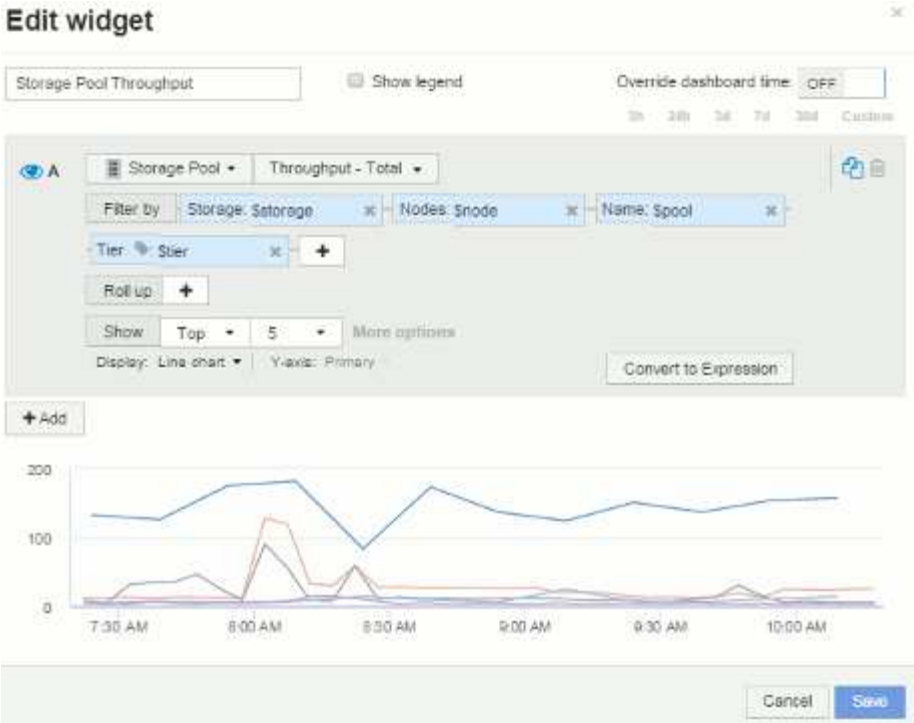


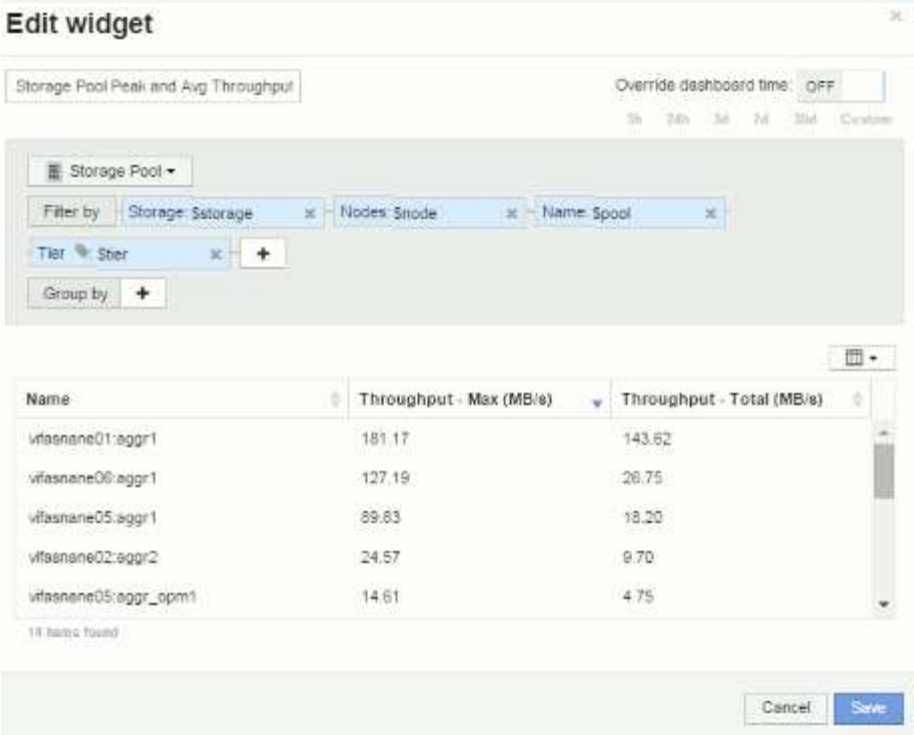
ストレージプールの利用率：



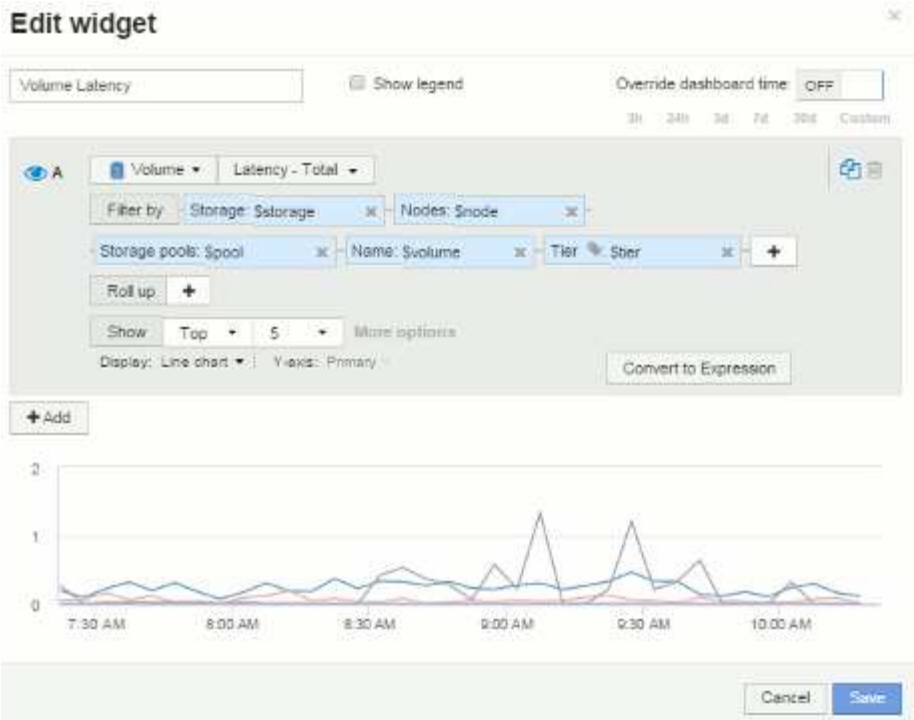


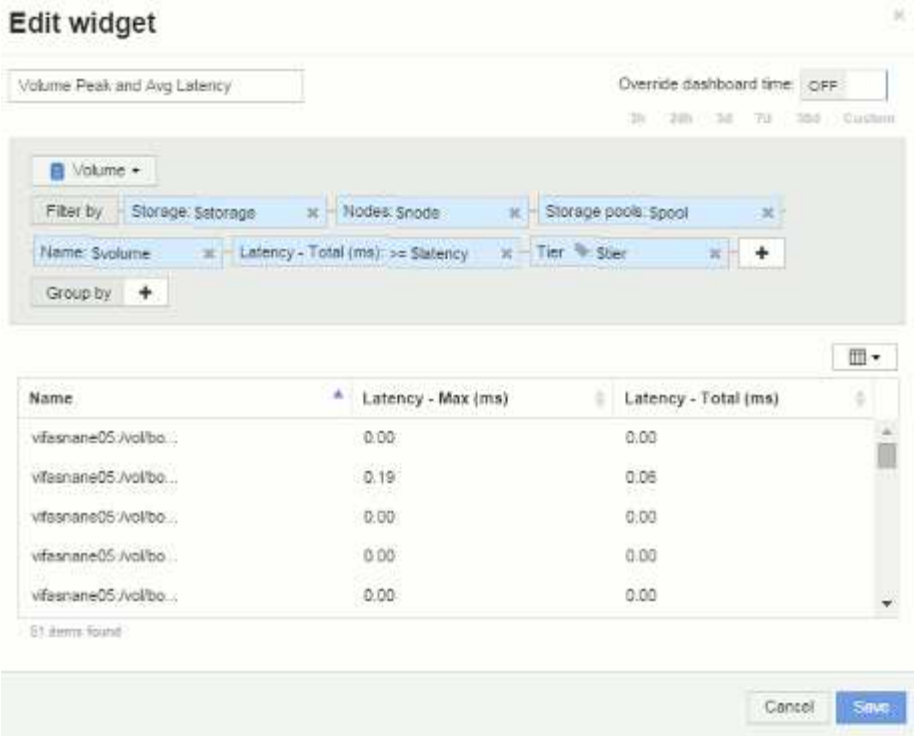
ストレージプールのスループット：


Edit widget
Storage Pool Throughput
Show legend
Override dashboard time
OFF
A
Storage Pool
Throughput - Total
Filter by
Storage: $storage
Nodes: $node
Name: $pool
Tier
$tier
Roll up
Show
Top
5
More options
Display: Line chart
Y-axis: Primary
Convert to Expression
Add
200
100
0
7:30 AM
8:00 AM
8:30 AM
9:00 AM
9:30 AM
10:00 AM
Cancel
Save

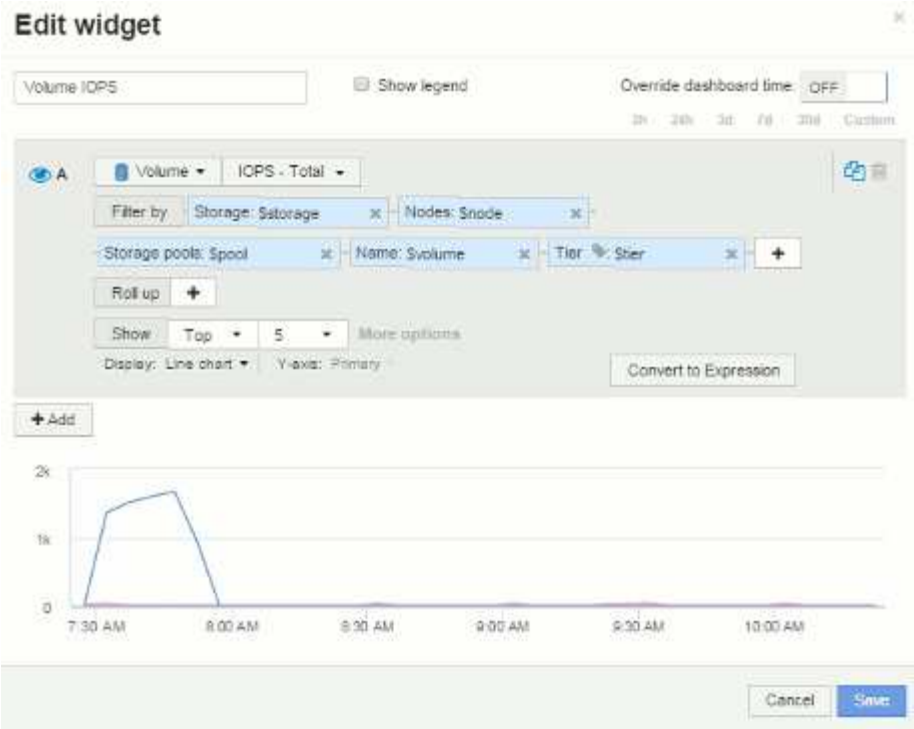

Edit widget
Storage Pool Peak and Avg Throughput
Override dashboard time
OFF
Storage Pool
Filter by
Storage: $storage
Nodes: $node
Name: $pool
Tier
$tier
Group by
Name
Throughput - Max (MB/s)
Throughput - Total (MB/s)
vifasnane01:aggr1
181.17
143.62
vifasnane06:aggr1
127.19
28.75
vifasnane05:aggr1
89.83
18.20
vifasnane02:aggr2
24.57
9.70
vifasnane05:aggr_opm1
14.61
4.75
Cancel
Save

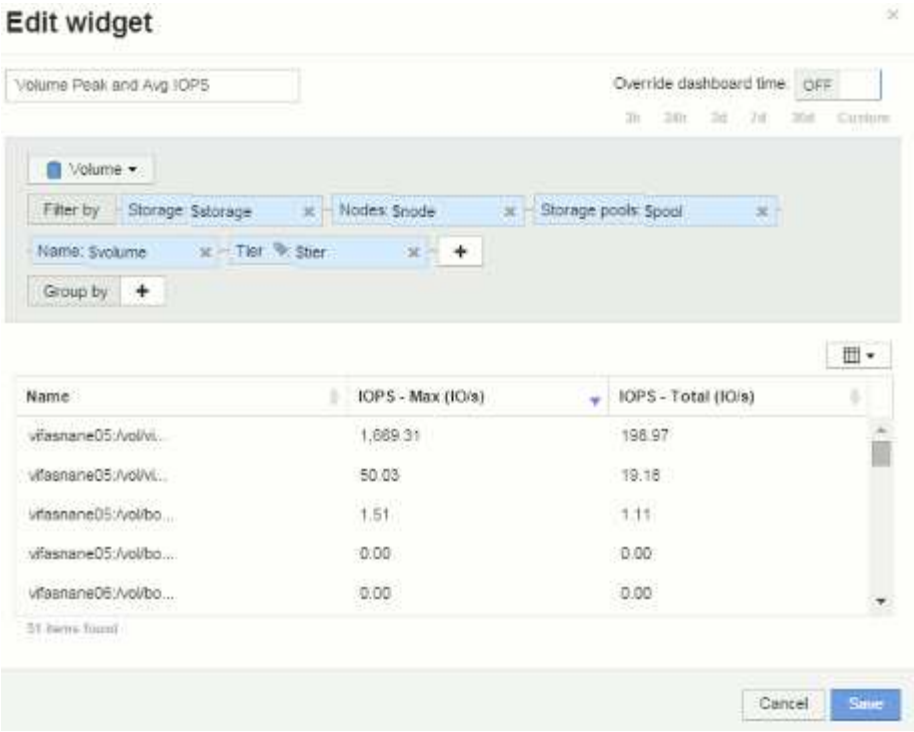
ボリュームレイテンシ：


Edit widget
Volume Latency
Show legend
Override dashboard time
OFF
A
Volume
Latency - Total
Filter by
Storage: $storage
Nodes: $node
Storage pools: $pool
Name: $volume
Tier
$tier
Roll up
Show
Top
5
More options
Display: Line chart
Y-axis: Primary
Convert to Expression
Add
2
1
0
7:30 AM
8:00 AM
8:30 AM
9:00 AM
9:30 AM
10:00 AM
Cancel
Save


Edit widget
Volume Peak and Avg Latency
Override dashboard time
OFF
Volume
Filter by
Storage: $storage
Nodes: $node
Storage pools: $pool
Name: $volume
Latency - Total (ms): >= $latency
Tier
$tier
Group by
Name
Latency - Max (ms)
Latency - Total (ms)
vifasnane05:/vol/bo...
0.00
0.00
vifasnane05:/vol/bo...
0.19
0.06
vifasnane05:/vol/bo...
0.00
0.00
vifasnane05:/vol/bo...
0.00
0.00
vifasnane05:/vol/bo...
0.00
0.00
61 items found
Cancel
Save

ボリュームIOPS：





ダッシュボードとウィジェットのベストプラクティス

ここでは、ダッシュボードとウィジェットを最大限に活用するためのヒントやコツを紹介します。

ベストプラクティス：適切な指標を見つける

OnCommand Insight では、カウンタと指標の名前がデータソースごとに異なる場合があります。

ダッシュボードウィジェットの指標やカウンタを検索するときは、予期しない名前で指標が分類されることがあります。OnCommand Insight のドロップダウンリストは通常アルファベット順ですが、用語がリストに表示されない場合があります。たとえば、ほとんどのリストで「 raw capacity 」は「 used capacity 」から離れた位置に表示されます。

ベストプラクティス：* Filter by *などのフィールドや列セレクタなどの場所で検索機能を使用します あなたが探しているものを見つけるために。たとえば、「cap」と検索すると、名前に「capacity」が含まれているすべての指標がどこで発生しているかに関係なく表示されます。その後、その短いリストから必要な指標を簡単に選択できます。

以下は、指標を検索する際に有効なキーワードの例です。

検索する項目	次の検索も試してください。
CPU	プロセッサ
容量	使用済み容量物理容量 プロビジョニングされた容量 ストレージプールの容量 <other asset type> の容量 書き込み済み容量
ディスク速度	ディスク速度が最も低いディスクタイプ
ホスト	HypervisorHostsの略
ハイパーバイザー	HostIハイパーバイザー
マイクロコード	ファームウェア
名前	AliasHypervisorの名前 ストレージ名 <other asset type> 名 単純な名前 リソース名 ファブリックエイリアス

読み取り / 書き込み	部分的なR/WPending書き込み IOPS -書き込み 書き込み済み容量 レイテンシ-読み取り キャッシュ使用率-読み取り
仮想マシン	仮想VMI

これは包括的なリストではありません。これらは検索キーワードの一例です。

ベストプラクティス：適切なアセットの検索

ウィジェットのフィルタや検索で参照できるInsightのアセットは、アセットタイプによって異なります。

ダッシュボードでは、ウィジェットの作成時に使用するアセットタイプによって、フィルタリングや列の追加が可能な他のアセットタイプカウンタが決まります。ウィジェットを作成する際は、次の点に注意してください。

アセットタイプ / カウンタ	フィルタ可能なアセット
仮想マシン	VMDK です
データストア	内部ボリュームVMDK 仮想マシン ボリューム
ハイパーバイザー	仮想マシン
ハイパーバイザーです	ホスト
ホスト	内部ボリューム
クラスタ	HostVirtual Machineの略
ファブリック	ポート

これは包括的なリストではありません。

ベストプラクティス：リストに表示されない特定のアセットタイプをフィルタリングする場合は、別のアセットタイプを使用してクエリを作成してみてください。

散布図の例:軸を知る

散布図ウィジェットでカウンタの順序を変更すると、データを表示する軸が変更されます。

このタスクについて

この例では、 IOPS が低いにも関わらずレイテンシが高い低パフォーマンスの VM を示す散布図を作成します。

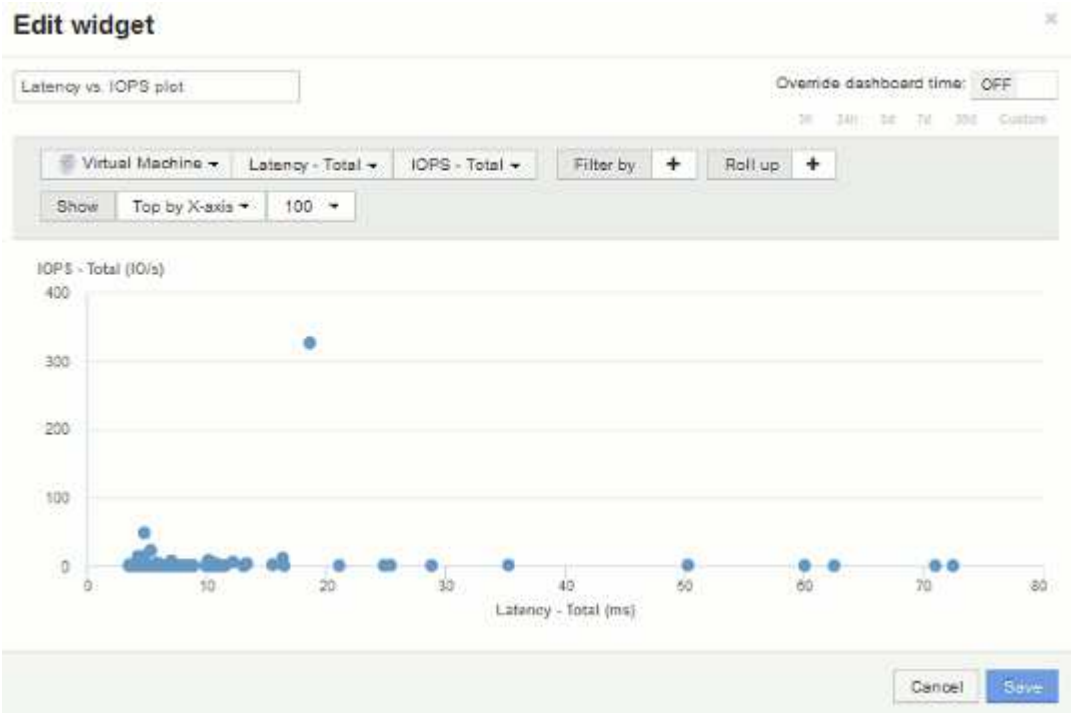
手順

1. ダッシュボードを編集モードで作成または開き、 * 散布図 * ウィジェットを追加します。
2. アセットタイプを選択します（例：* Virtual Machine *）。
3. 出力する最初のカウンタを選択します。この例では、*[レイテンシ-合計]*を選択します。

   _Latency - Total _ がグラフの X 軸に沿って表示されます。

4. プロットする 2 番目のカウンタを選択します。この例では、* IOPS - Total *を選択します。

   _IOPS - Total _ がグラフの Y 軸に沿って表示されます。VM のレイテンシが高いほど、グラフの右側に表示されます。上位 X 軸 * の設定が最新であるため、レイテンシが高い上位 100 個の VM のみが表示されます。

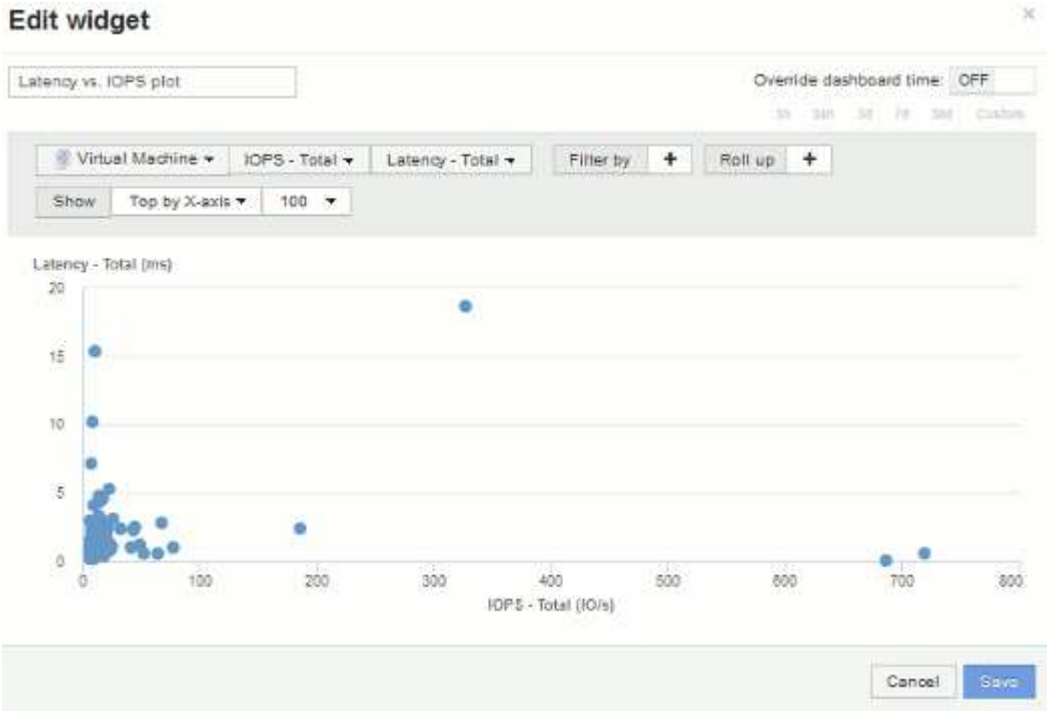


5. 最初のカウンタを* IOPS - Total に、**2**番目のカウンタを Latency - Total *に設定して、カウンタの順序を逆にします。

   _latency-Total_がグラフのY軸に、*IOPS-Total*がX軸に表示されるようになりました。今度は VM の IOPS が高いほど、グラフの右側に表示されます。

   「 X 軸上」の設定は変更されていないため、ウィジェットには、現在 X 軸に沿ってプロットされている

上位 100 個の IOPS の高い VM が表示されます。



6. X 軸上の N 、 Y 軸上の N 、 X 軸下の N 、 Y 軸下の N 、または Y 軸下の N をグラフに表示するように選択できます。この最後の例では、IOPS_の合計IOPS _が最も高い上位100台のVMがグラフに表示されています。[Top by Y-axis]に変更すると、合計レイテンシが最も高いVMが100台表示されます。

   散布図では、ポイントをクリックするとそのリソースのアセットページが開きます。

パフォーマンスポリシーの作成

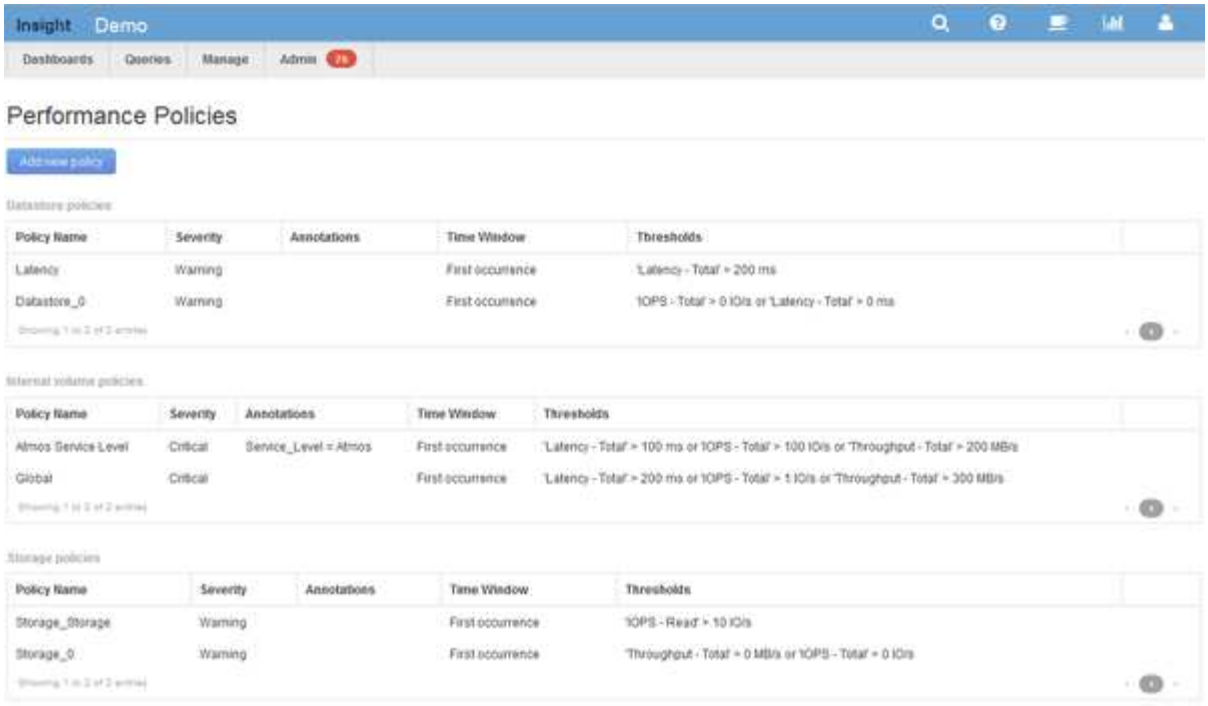
パフォーマンスポリシーを作成して、ネットワーク内のリソースに関連する問題についてユーザに通知するアラートをトリガーするしきい値を設定します。たとえば、ストレージプールの合計使用率が 60% を超えたときにアラートをトリガーするパフォーマンスポリシーを作成できます。

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。

ネットワーク内の違反を監視します

パフォーマンスポリシーで設定されたしきい値に基づいてInsightで違反が生成された場合は、[Violations Dashboard]で確認できます。このダッシュボードには、ネットワークで発生したすべての違反が表示され、問題を特定して対処することができます。

手順

1. ブラウザでOnCommand Insight を開きます。
2. Insightのツールバーで、**[Dashboards]***をクリックし、[Violations Dashboard]*を選択します。

   [Violations Dashboard]が表示されます。

3. [Violations by Policies]*円グラフでは、次の方法で情報を確認できます。
   - グラフの任意のスライスにカーソルを合わせると、特定のポリシーまたは指標に対する違反の総数の割合を表示できます。
   - グラフのスライスをクリックすると、そのスライスを「拡大」できます。これにより、そのスライスをグラフの残りの部分から遠ざけることで、そのスライスを強調して注意深く調べることができます。
   - をクリックできます アイコンをクリックして円グラフを全画面モードで表示し、をクリックします 円グラフを最小化するには、もう一度繰り返します。円グラフには最大5つのスライスを含めることができます。そのため、6つのポリシーで違反が発生した場合は、5つ目と6つ目のスライスが「その他」のスライスに統合されます。Insightでは、違反数が最も多いものが最初のスライスに割り当てられ、2番目に多いものが2番目のスライスに割り当てられます。
4. [Violations History]*チャートは次の方法で使用できます。
   - グラフにカーソルを合わせると、特定の時点で発生した違反の総数と、指定した各指標についての違反の総数のうち発生した数が表示されます。
   - 凡例ラベルをクリックすると、その凡例に関連付けられているデータをグラフから削除できます。

     凡例をクリックすると、データが再度表示されます。

   - をクリックできます アイコンをクリックしてグラフを全画面モードで表示し、をクリックします 円グラフを最小化するには、もう一度繰り返します。
5. [Violations Table]*は次の方法で使用できます。
   - をクリックできます 右上隅のアイコンをクリックしてテーブルを全画面モードで表示し、をクリックします 円グラフを最小化するには、もう一度繰り返します。

     ウィンドウサイズが小さすぎる場合、[Violations Table]には3列しか表示されませんが、をクリックすると表示されます 、追加の列（最大7列）が表示されます。

   - 特定の期間の違反を表示できます（* 1h 、 3h 、 24h 、 3d 、 7d 、 と 30d *）が表示されます。Insightでは、選択した期間について、最大1、000件の違反が表示されます。

- [**filter**]ボックスを使用すると、必要な違反のみを表示できます。
- 列ヘッダーの矢印をクリックすると、表内の列のソート順序を昇順（上矢印）または降順（下矢印）に変更できます。デフォルトのソート順序に戻すには、他の列ヘッダーをクリックします。

  デフォルトでは、違反は降順で表示されます。

- [ID]列で違反をクリックすると、その違反の期間のアセットページを表示できます。
- 概要 列でリソース（ストレージプールやストレージボリュームなど）のリンクをクリックすると、それらのリソースに関連付けられているアセットページを表示できます。
- [ポリシー]列でパフォーマンスポリシーのリンクをクリックすると、[ポリシーの編集]ダイアログボックスが表示されます。

  生成される違反が少なすぎる場合や多すぎる場合は、ポリシーのしきい値を調整することができます。

- 1ページに収まらないデータがある場合は、ページ番号をクリックしてページごとにデータを参照できます。
- をクリックできます ✖ 違反を却下します。

ファイバチャネルのBBクレジット0エラーのトラブルシューティング

ファイバチャネルでは、バッファ間クレジット（BBクレジット）を使用して転送フローが制御されます。クレジット値はポートからフレームが送信されると減少し、ポートが応答を受信すると補充されます。ポートのBBクレジットが補充されないと、伝送フローが影響を受ける可能性があります。ポートには、フレームが順番に組み立てられて配信されるまで、一時的にフレームを保存するためのメモリ（バッファ）が必要です。バッファの数はポートが格納できるフレームの数であり、バッファクレジットと呼ばれます。

特定のポートで使用可能なクレジットが0に近づくと、0に達するとポートが送信を停止し、BBクレジットが補充されるまで再開しないという警告が表示されます。

Insightのパフォーマンスポリシーでは、次のポート指標にしきい値を設定できます。

BBクレジットゼロ-受信
サンプリング期間中に受信バッファ間クレジット数がゼロになった回数
BBクレジットゼロ-転送
サンプリング期間中に送信のバッファ間クレジット数がゼロになった回数
BBクレジットゼロ-合計

接続されているポートで提供できるクレジットを使い果たしたために、このポートが送信を停止した回数	
BBクレジットゼロ期間-治療	
サンプリング期間中にTx BBクレジットがゼロだった時間（ミリ秒）	

BBクレジットエラーは、次のような状況が原因で発生する可能性があります。

- 比率の高いFCフレームのサイズが最大サイズよりも大幅に小さい場合は、BBクレジットの追加が必要になる可能性があります。
- 環境におけるワークロードの変化により、ワークロードに接続されているポートやデバイス（ストレージノードなど）に影響が及ぶ可能性があります。

ファブリック、スイッチ、およびポートアセットのページを使用して、Fibre Channel環境を監視できます。ポートアセットページには、リソースに関する概要情報、トポロジ（デバイスとその接続）、パフォーマンスチャート、および関連するリソースの表が表示されます。ファイバチャネルの問題のトラブルシューティングでは、各ポートアセットのパフォーマンスグラフに影響が大きいポートのトラフィックが表示されるため、このグラフが役立ちます。ポートアセットのページには、バッファ間クレジットの指標とポートエラーも表示されます。Insightでは、指標ごとに個別のパフォーマンスチャートが表示されます。

ポートのパフォーマンスポリシーとしきい値を作成する

ポートに関連付けられている指標のしきい値を設定したパフォーマンスポリシーを作成できます。デフォルトでは、パフォーマンスポリシーは作成時に指定したタイプのすべてのデバイスに適用されます。特定のデバイスまたはデバイスセットのみをパフォーマンスポリシーに含める場合は、アノテーションを作成します。わかりやすいように、この手順 ではアノテーションは使用しません。

作業を開始する前に

このパフォーマンスポリシーでアノテーションを使用する場合は、パフォーマンスポリシーを作成する前にアノテーションを作成する必要があります。

手順

1. Insightのツールバーで、**[管理]**>*[パフォーマンスポリシー]*をクリックします

   既存のポリシーが表示されます。スイッチポート用のポリシーが存在する場合は、既存のポリシーを編集して新しいポリシーとしきい値を追加できます。

2. 既存のポートポリシーを編集するか、新しいポートポリシーを作成します

   - 既存のポリシーの右端にある鉛筆のアイコンをクリックします。手順「d」および「e」で説明されているしきい値を追加します。
   - [+追加]*をクリックして新しいポリシーを追加します

     i. 「ポリシー名」に「スロードレインデバイス」を追加します

     ii. オブジェクトタイプとしてポートを選択します

iii. の"`Apply after window`"に最初に出現したものを入力します

iv. [BB credit zero - Rx]に「1,000,000」と入力します

v. [BB credit zero - Tx]のしきい値として「1、000、000」を入力します

vi. [STOP processing further policies if alert is generated]をクリックします。

vii. 「保存」をクリックします。

作成したポリシーは、設定したしきい値を24時間監視します。しきい値を超えると、違反が報告されます。

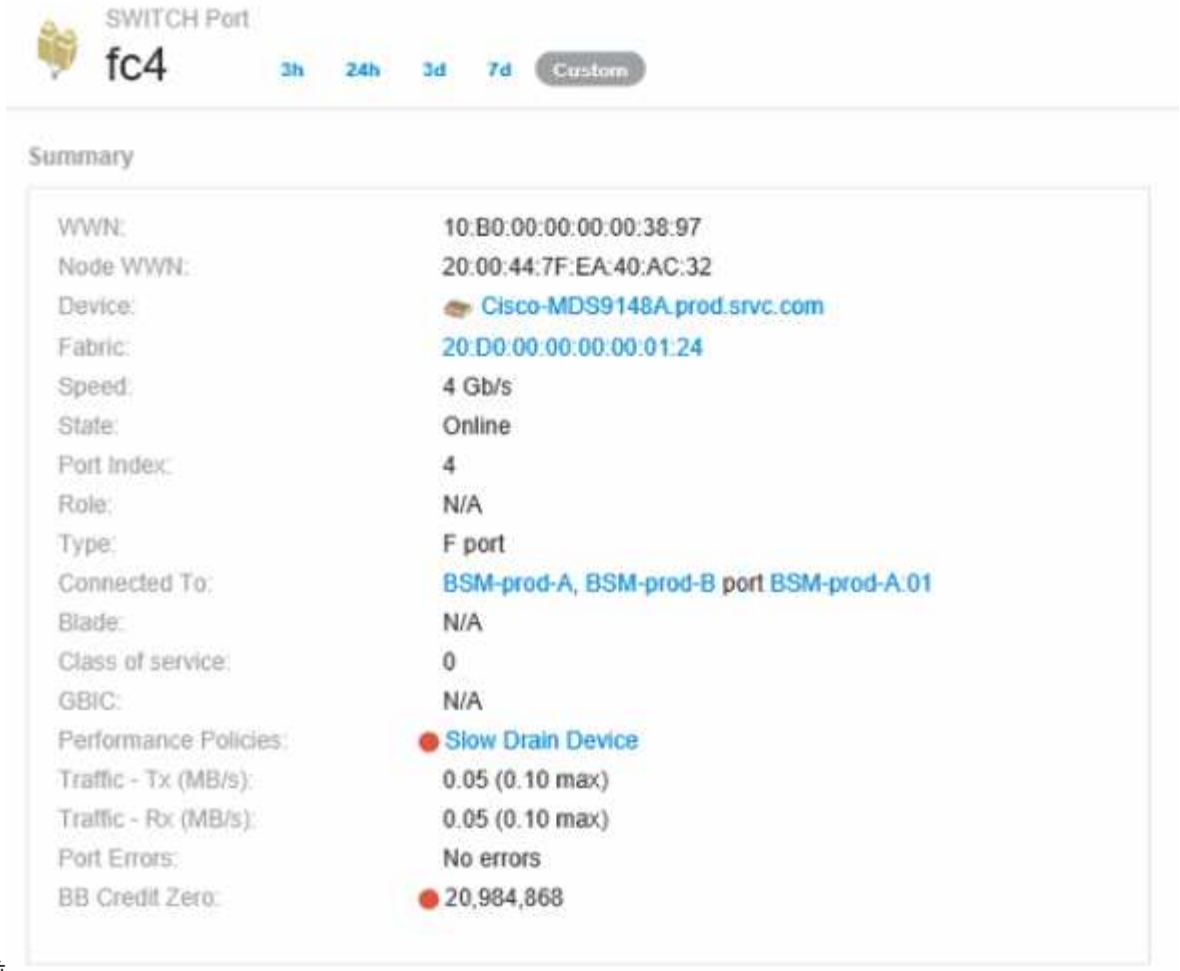
3. **>**[違反ダッシュボード]*をクリックします

   システムで発生したすべての違反が表示されます。違反を検索またはソートして、「低ドレインデバイス」違反を表示します。[Violations Dashboard]には、パフォーマンスポリシーに設定されたしきい値を超える「BB Credit 0」エラーが発生したすべてのポートが表示されます。[Violations Dashboard]で強調表示されている各スイッチポートからポートのランディングページへのリンクが表示されます。

4. 強調表示されているポートのリンクをクリックすると、ポートのランディングページが表示されます。

   ポートのランディングページが表示され、BBクレジット0のトラブルシューティングに役立つ次の情報が含まれます。

   - ポートが接続されているデバイス
   - 違反を報告しているポート（ファイバチャネルスイッチポート）のID。
   - ポートの速度
   - 関連付けられているノードとポートの名



前

5. 下にスクロールしてポートの指標を確認します。Select metrics to show **>** BB credit zero *をクリックして、BBクレジットのグラフを表示します。

6. [Top correlated]*をクリックします

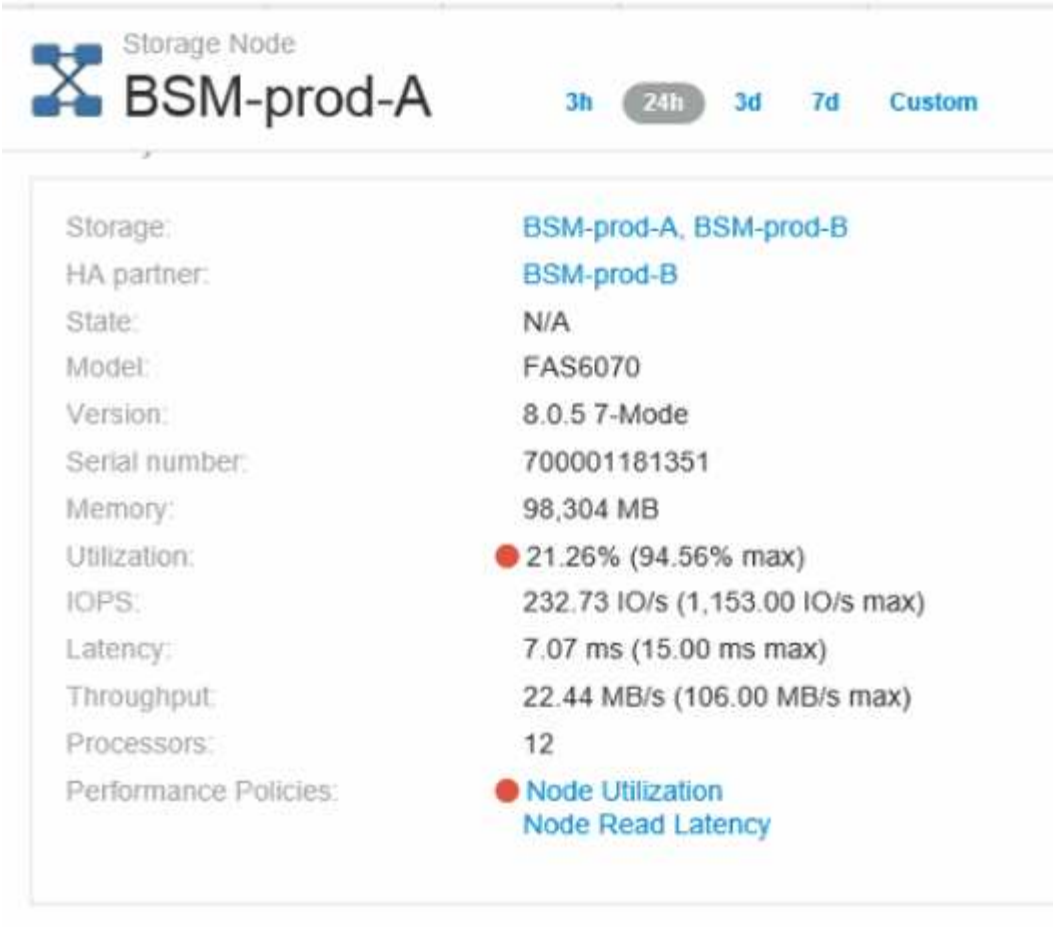
   関連する上位のリソース分析には、パフォーマンスと最も関連性の高いリソースとして、ポートに接続されているコントローラノードが表示されます。この手順では、ポートのアクティビティのIOPS指標をノードのアクティビティ全体と比較します。ディスプレイには、TxおよびRx BB Credit Zero指標とコントローラノードのIOPSが表示されます。ディスプレイには次の情報が表示されます。

   - コントローラのIOは、ポートトラフィックと密接に関連しています

- ポートがサーバにIOを送信しているときにパフォーマンスポリシー違反が発生しました。
- ポートパフォーマンス違反がストレージコントローラの高いIOPS負荷に関連して発生していることから、ストレージノードのワークロードが違反の原因である可能性があります。

7. ポートのランディングページに戻り、ストレージコントローラノードのランディングページにアクセスしてワークロードの指標を分析します。

   ノードは利用率違反を示し、指標はバッファ間クレジットのゼロ状態に関連する高い「キャッシュ読み取り回数」を示しています。



8. ノードのランディングページで、関連するリソースリストからポートを選択し、指標メニューからノードの使用率データ（キャッシュ使用率データなど）を選択することで、BBクレジットのゼロ点を比較できます。

このデータから、キャッシュヒット率が他の指標と反比例していることがわかります。ストレージノードでは、キャッシュからのサーバの負荷に応答する代わりに、大量のキャッシュ読み取りが置き換えられています。ほとんどのデータをキャッシュではなくディスクから取得する必要があるため、ポートからサーバへのデータ送信に遅延が生じている可能性があります。パフォーマンス問題の原因 は、I/O動作の変化を引き起こしたワークロードであり、ノードキャッシュとその構成が原因 である可能性があります。この問題は、ノードのキャッシュサイズを増やすか、キャッシュアルゴリズムの動作を変更することで解決できる場合があります。

インフラの分析

このトピックでは、環境内のインフラの一部を分析する際に使用する手順を記載します。この演習で収集する手順、ビュー、およびデータは、例として仮想コンピューティングオブジェクトを使用しています。環境内の他のアセットについても、それぞれのアセットに関連するカウンタを使用して同様の手順で分析します。この演習の目的は、データセンター内の資産の特性を監視および把握するためにInsightで提供されるさまざまなオプションを理解することです。

このタスクについて

インフラの状態を分析するために実行できるアクションには、次のようなものがあります。

- オブジェクトの動作を時間の経過とともに観察します
- あるオブジェクトの指標を、類似する上位10個のオブジェクトの指標と比較します
- オブジェクトの数を比較します
- 上位10個のオブジェクトを平均値と比較します
- 指標Aとを比較しますBをクリックしてカテゴリと異常を表示します
- オブジェクトの範囲を他のオブジェクトと比較します
- 式を使用して、Web UIに表示されない指標を表示します

実行する分析ごとにウィジェットを使用して、インフラ内のオブジェクトのこれらすべてのビューをダッシュボードで作成できます。ダッシュボードを保存して、インフラ上の最新データにすばやくアクセスできるようにすることができます。

オブジェクトの動作を時間の経過とともに観察します

単一のオブジェクトの動作を観察して、そのオブジェクトが想定される運用レベル内で動作しているかどうかを判断できます。

手順

1. クエリを使用して、分析対象となるVMを特定します。* Query **>**+ New query **>** Virtual machine **>**"name"*

   名前フィールドを空白のままにすると、すべてのVMが返されます。この演習で使用するVMを選択します。VMのリストをスクロールして選択できます。

2. 収集する情報の新しいダッシュボードを作成します。ツールバーで、**[**ダッシュボード**]**>*+[新しいダッシ

ュボード]*をクリックします。

3. 新しいダッシュボードで、変数>*テキスト*を選択します。

   a. クエリでVM名をとして追加します`$var1` 価値。

   b. チェックボックスをクリックします。

   この変数を使用すると、分析するオブジェクトの異なるセットを簡単に切り替えることができます。分析の他のステップでは、最初に選択した単一のVMに対する追加の分析にこの変数を再利用できます。変数は、複数のオブジェクトを識別するときに便利になります。

4. 新しいダッシュボードに折れ線グラフウィジェットを追加します。* Widget **>** Line chart *。

   a. デフォルトのアセットタイプを仮想マシンに変更します。**[**仮想マシン**]**>*[レイテンシ-合計]*をクリックします。

   b. **>**[名前]**>**$var1 *をクリックします。

   c. ダッシュボードの期間を変更します。* Override dashboard time **>** on **>** 7 days *。

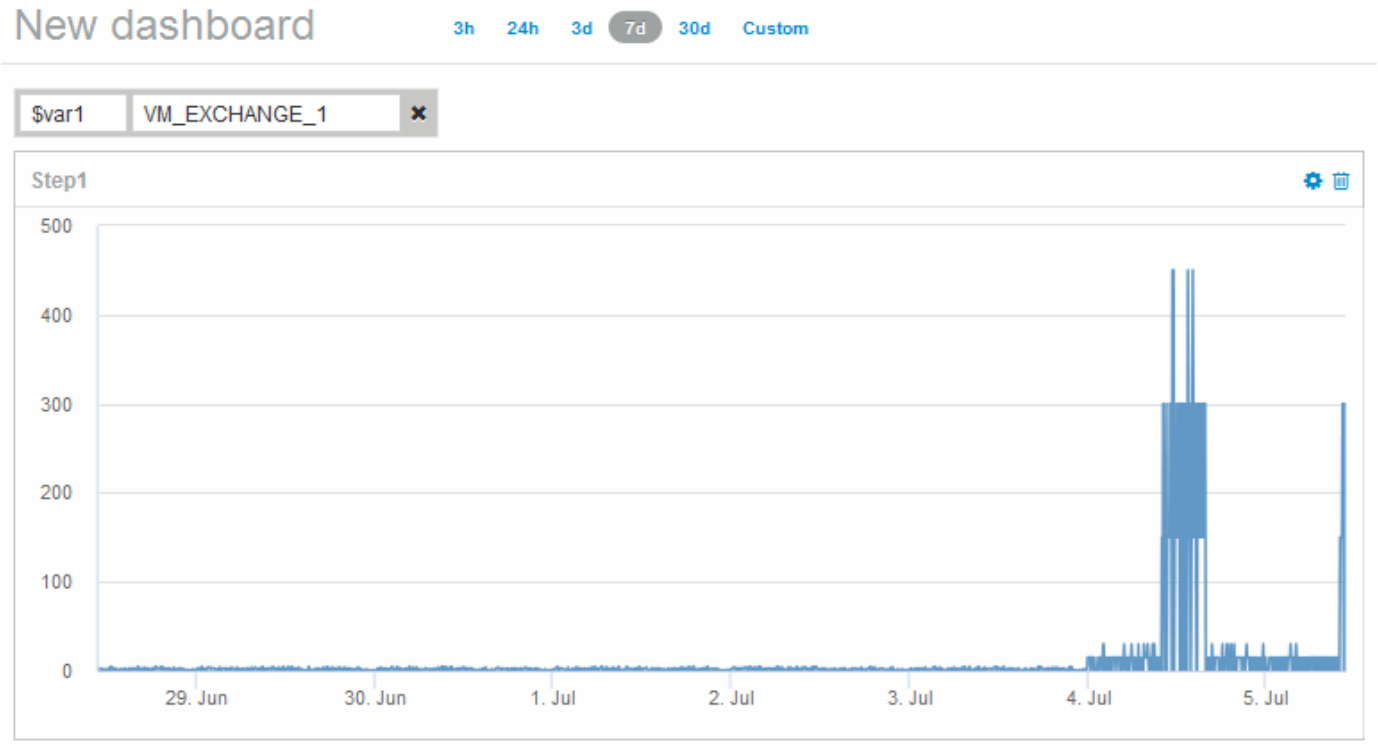
      表示期間は、プリセットのいずれかを使用するか、カスタムの期間を指定して変更できます。

   +ダッシュボードに、指定した期間におけるVMのIOPS - Total *が表示されます。

5. ウィジェットに名前を割り当て、ウィジェットを保存します。

結果

ウィジェットには次のようなデータが表示されます。



表示された7日間のうち、短期間にVMのレイテンシが異常に高くなっていることが示されています。

合計レイテンシが上位10個のオブジェクトを、類似するすべてのオブジェクトの平均レイテンシと比較します

上位10個の合計レイテンシがあるVMを平均合計レイテンシと比較して、平均範囲から極端に外れているVMを特定できます。この情報は、VM上でワークロードを分散するための決定に役立ちます。

手順

1. 積み上げ面グラフを含むウィジェットを新しいダッシュボードに追加します。* Widget > Stacked Area Chart *

   a. デフォルトのデバイスを仮想マシンに変更します。[ストレージ]>*>[合計レイテンシ]*をクリックします

      ウィジェットに、すべてのVMの24時間の合計レイテンシを示す積み上げ面グラフが表示されます。

   b. このウィジェットで、すべてのVMの合計レイテンシの平均値を表示する2つ目の表示を作成します。* Widget > Line chart *

   c. デフォルトのデバイスを仮想マシンに変更します。[仮想マシン]>*[レイテンシ-合計]*をクリックします

      ウィジェットに、デフォルトの24時間の合計レイテンシを示す折れ線グラフが表示されます。

   d. ロールアップ*バーの X をクリックし、*表示>*トップ*>* 10 *を選択します

   合計レイテンシに基づく上位10個のVMが表示されます。

2. すべてのVMの平均合計レイテンシを上位10個の合計IOPSと比較するには、次の手順を実行します。

   a. 「* + 追加」をクリックします。

   b. デフォルトのデバイスを仮想マシンに変更します。[ストレージ]>*>[IOPS total]*をクリックします

   c. ロールアップ*バーの X をクリックし、*表示>*トップ*>* 10 *を選択します

      レイテンシが高いオブジェクトが10個表示され、平均レイテンシが折れ線グラフに表示されます。

      + image::../media/analytics-Top10-avg.gif[]

   +平均レイテンシは1.6ミリ秒ですが、上位10個のVMではレイテンシが200ミリ秒を超えています。

1つのオブジェクトの合計レイテンシを、上位10個のオブジェクトの合計レイテンシと比較します

次の手順では、1つのVMの合計レイテンシを、仮想インフラ全体で合計レイテンシが上位10個になっているVMと比較します。

手順

1. 折れ線グラフ付きのウィジェットを新しいダッシュボードに追加します。* Widget > Line Chart *

a. デフォルトのデバイスを仮想マシンに変更します。**[**ストレージ**]>*>**[レイテンシ-合計]*をクリックします

   ウィジェットに、すべてのVMの24時間の合計レイテンシが面グラフに表示されます。

b. このウィジェットで、すべてのVMの合計レイテンシの平均値を表示する2つ目の表示を作成します。* Widget **>** Line chart *

c. デフォルトのデバイスを仮想マシンに変更します。**[**ストレージ**]>*>**[レイテンシ-合計]*をクリックします

   ウィジェットに、デフォルトの24時間の合計レイテンシを示す折れ線グラフが表示されます。

d. ロールアップ*バーの X をクリックし、*表示>*トップ*>* 10 *を選択します

2. 上位10位と比較するVMを追加します。

   a. 「 * + 追加」をクリックします。

   b. デフォルトのデバイスを仮想マシンに変更します。**[**ストレージ**]>*>**[合計レイテンシ]*をクリックします

   c. **>**[名前]**>**$var1 *をクリックします

3. [凡例を表示]*をクリックします

結果

凡例には、分析対象の各VMが表示されます。VM_Exchange_1を簡単に特定して、環境内の上位10個のVMと同様のレイテンシが発生しているかどうかを確認できます。

指標**A**と指標**B**を比較してカテゴリと異常を表示します

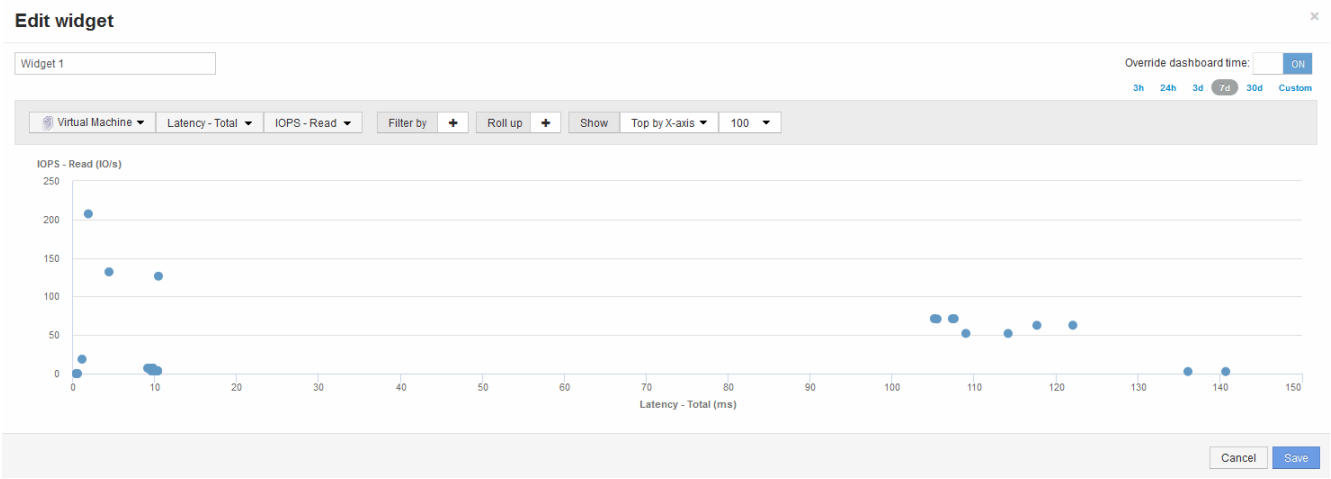
散布図を使用して、オブジェクトごとに2セットのデータを表示できます。たとえば、各オブジェクトのIOPS読み取りと合計レイテンシを表示するように指定できます。このグラフを使用すると、IOPSと合計レイテンシの両方に基づいて、問題があると思われるオブジェクトを特定できます。

手順

1. 散布図を含むウィジェットを新しいダッシュボードに追加します。* Widget **>** Scatter Plot Chart *

2. デフォルトのデバイスを仮想マシンに変更します。**[**ストレージ**]>*>**[合計レイテンシ]**>**[IOPS読み取り]*をクリックします

   次のような散布図が表示されます。



式を使用して別の指標を識別します

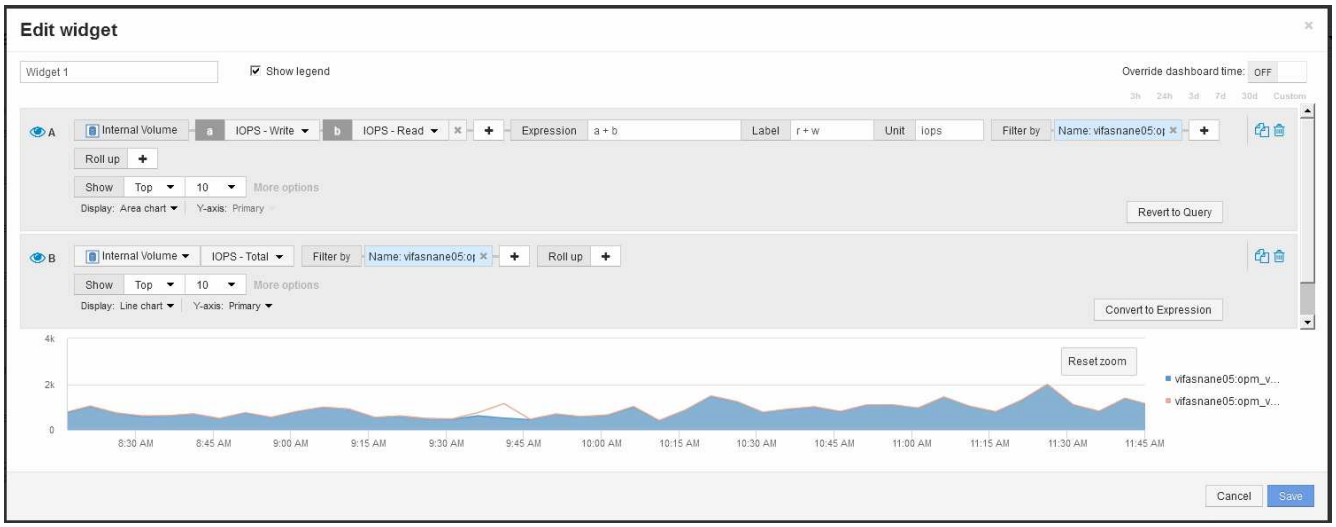
式を使用すると、システムオーバーヘッドによって発生するIOPSなど、Web UIで提供されない指標を表示できます。

このタスクについて

内部ボリュームのオーバーヘッド処理など、読み取りまたは書き込み以外の処理で生成される合計IOPSを式で表示できます。

手順

1. ダッシュボードにウィジェットを追加します。[* Area chart* （エリアグラフ * ）] を
2. デフォルトのデバイスを内部ボリュームに変更します。**[**ストレージ**]>*>**[IOPS書き込み]*をクリックします
3. [Convert to Expression]*ボタンをクリックします。
4. IOPS - Write 指標がアルファベット変数フィールド「 A *」に表示されるようになりました。
5. 「* b 」変数フィールドで、 Select をクリックし、 IOPS - Read *を選択します。
6. [式]フィールドに「* a + b 」と入力します。**[*Display**]セクションで、式として[* **Area chart**]を選択します。
7. [Filter by]*フィールドに、分析する内部ボリュームの名前を入力します。
8. **Label** フィールドは、式を識別します。ラベルを「R+W IOPS'」などのわかりやすい名前に変更します。
9. [***+Add**]をクリックして、ウィジェットに合計IOPSの線を追加します。
10. デフォルトのデバイスを内部ボリュームに変更します。**[**ストレージ**]>*>**[IOPS合計]*をクリックします
11. [Filter by]*フィールドに、分析する内部ボリュームの名前を入力します。



読み取りIOPSと書き込みIOPSを組み合わせた青の折れ線グラフに、合計IOPSが折れ線で表示されます。9：30と9：45の間のギャップは、非読み取りと非書き込みのIO（オーバーヘッド）処理を示しています。

シンプロビジョニングのリスクの最小化の概要

今日のハイブリッド IT データセンターでは、管理者は、シンプロビジョニングなどの容量効率化テクノロジを使用して割り当てを制御し、かつて使用できなかった容量を活用することで、物理的な範囲を超えたリソース利用率を拡大する必要があります。

OnCommand Insight は、ITサービススタック内のシンプロビジョニングされた複数のレイヤにわたって、ほぼリアルタイムで容量の使用状況と使用状況の詳細を表示します。オーバーサブスクリプションリスクを適切に管理できないと、ビジネスに不必要なダウンタイムが発生する可能性があります。

ストレージプールを監視しています

ストレージプールの各ランディングページには、オーバーサブスクリプション率、関連するリソース、 LUN とディスクの利用率、ストレージプールで発生したポリシー違反や違反が表示されます。

ストレージプールのランディングページを使用して、仮想インフラをサポートしている物理資産に潜在的な問題がないか確認します。容量と容量の比率のトレンドを 30 日間にわたって追跡したり、カスタムの期間を使用したりできます。ストレージプールのステータスを監視するには、以降のセクションのデータに注意してください。

- * 概要 *

  このセクションでは、次の内容について説明します。

  - ストレージプールの容量情報には、物理容量とオーバーコミット容量が含まれます。
  - アグリゲートがオーバーサブスクライブされているかどうかとその量。
  - 発生したポリシー違反。
- ストレージリソースとディスクセクション

ストレージリソースセクションには、LUN利用率が表示されます。

[Disks]セクションには、ストレージプールを構成する個 々 のディスクが表示されます。

- * リソース *

  このセクションでは、VMDKとLUNの関連付けについて理解し、ストレージとVMのアプリケーションパスを理解します。

- 違反セクション

  [Violations]セクションには、ストレージプールに対して設定されているパフォーマンスポリシーへの違反が表示されます。

データストアの監視

データストアランディングページでは、オーバーサブスクリプション率、 LUN とディスクの利用率、関連するリソース、データストアで発生したポリシーの違反を確認できます。

このランディングページでは、仮想インフラの問題を特定できます。容量と容量の比率のトレンドを追跡することで、容量の変化を予測できます。

- * 概要 *

  このセクションでは、次の内容について説明します。

  - データストアの容量情報には、物理容量とオーバーコミット容量が含まれます。
  - オーバーコミット容量の割合。
  - レイテンシ、 IOPS 、およびスループットの指標。

- * VMDK *

  [VMDKs]セクションには、仮想ディスクの容量とパフォーマンスが表示されます。

- ストレージリソース

  このセクションには、データストアに関連する内部ボリュームの使用済み容量とパフォーマンス指標が表示されます。

- * リソース *

  このセクションでは、VMDKとLUNの相関関係、およびストレージとVMのアプリケーションパスについて説明します。

- 違反セクション

  [Violations]セクションには、データストアに設定されているパフォーマンスポリシーへの違反が表示されます。

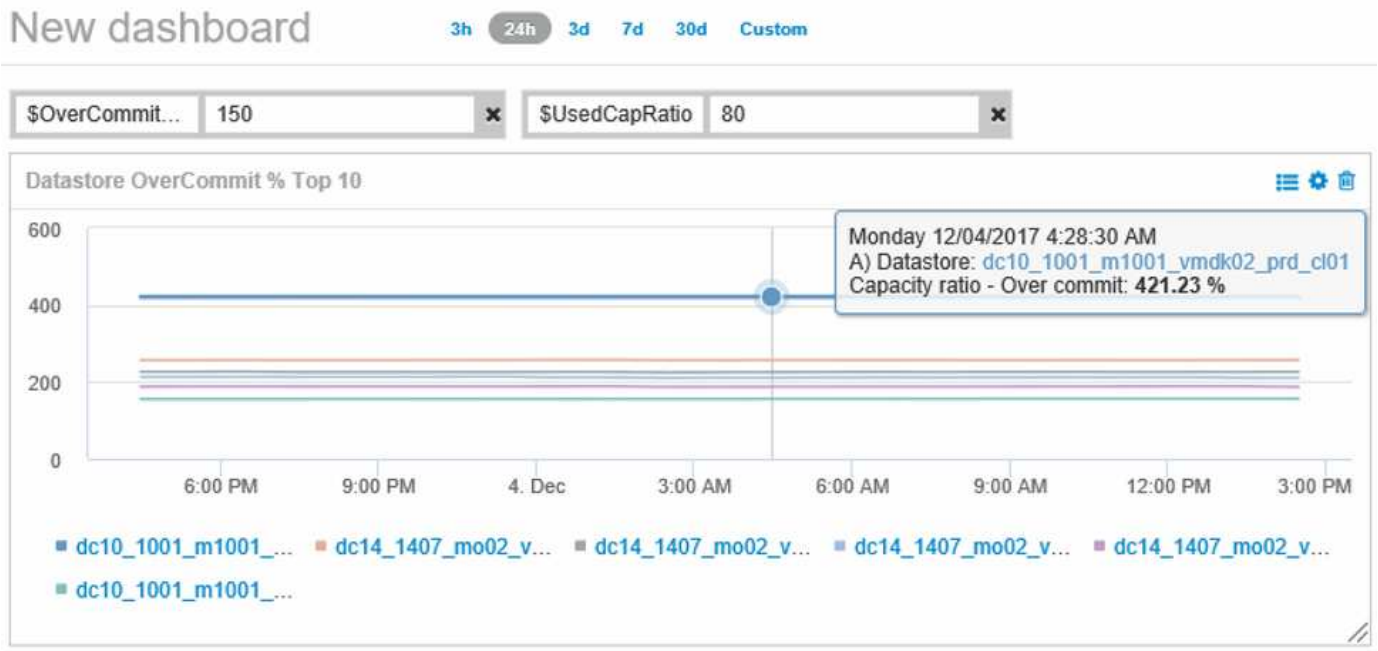
シンプロビジョニング環境を監視するダッシュボードを作成する

OnCommand Insightの柔軟性に優れたダッシュボードウィジェットの設計と表示チャートオプションにより、容量の使用状況や使用状況、シンプロビジョニングされたデータセンターインフラにおけるリスクを最小限に抑えるための戦略的情報を詳細に分析できます。

監視するデータストアとストレージプールの情報へのアクセスを提供するダッシュボードを作成できます。

ダッシュボードを使用したデータストア情報へのアクセス

仮想インフラ内で監視するデータにすばやくアクセスできるダッシュボードの作成が必要になることがあります。ダッシュボードには、次のようなウィジェットを含めることができます。データストアのオーバーコミット率に基づく上位 10 個のデータストアを特定するウィジェットや、データストアの容量データを表示するウィジェットを指定することができます。ダッシュボードでは、変数を使用して、使用済み容量が 80% を超えているデータストアとオーバーコミットされたデータストアを表示します。



Overcommit Subscription %

Name	Capacity - Total (GB)	Capacity - Used (GB)	Capacity - Provisioned (GB)	Capacity ratio - Over commit (%)	Capacity ratio - Used (%)
dc14_1407_...1_prd_cl03	5,008.00	4,091.04	12,876.38	257.12	81.69
dc14_1407_...2_prd_cl03	6,936.69	5,872.31	14,633.80	210.96	84.66
dc14_1407_...3_prd_cl03	9,437.03	7,951.36	17,639.86	186.92	84.26
dc14_1407_...4_prd_cl03	7,911.09	6,627.00	17,891.24	226.15	83.77

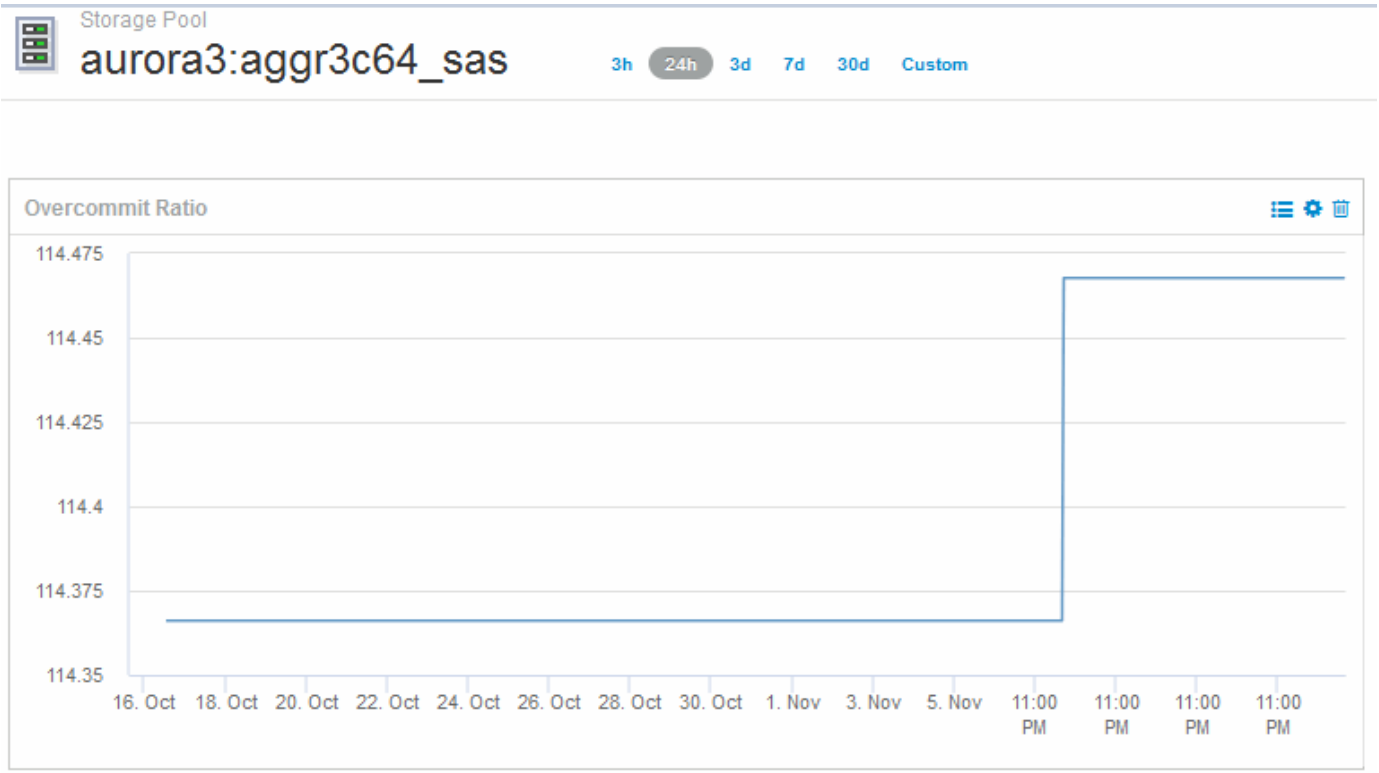
4 items found

シンプロビジョニング環境の監視に使用できるその他のウィジェットには、次のような情報が含まれます。

- データストアに関連付けられたVMDKの容量
- VMの容量
- データストアの使用容量のトレンド分析

ダッシュボードを使用したストレージプール情報へのアクセス

ダッシュボードには、次のようなウィジェット、使用済み物理ストレージ容量、ストレージプールのオーバーコミット容量などを表示できます。



パフォーマンスポリシーを使用してシンプロビジョニングのリスクを軽減する

仮想インフラのしきい値を超えたときにアラートを生成するには、パフォーマンスポリシーを作成する必要があります。アラートを使用すると、原因が処理を中断または停止する前に、環境内の変更に対応できます。

仮想インフラの監視に役立つポリシーは次のとおりです。

- データストア

  データストアでは次のポリシーを使用できます。

  - 容量比率 - オーバーコミット
  - 容量比率 - 使用済み
  - Capacity - 使用済みです

    - 容量 - 合計
- ストレージプール

  シンプロビジョニング環境では、次のポリシーを使用してストレージに関連する容量の停止を防ぐことができます。

    - プロビジョニング済み容量
    - 使用済みパフォーマンス容量
    - 容量比率 - オーバーコミット
    - 容量比率 - 使用済み

これらのポリシーから拡張して、次のような仮想インフラストラクチャの容量を監視できます。

- 内部ボリューム
- LUN
- ディスク
- VMDK
- 仮想マシン

ポリシーはアノテーションを使用して設定できます。アプリケーションをサポートする特定のアセットに同じアノテーションを割り当てる。たとえば、データストアにアノテーションを割り当てたり、シンプロビジョニングアプリケーションのストレージプールにアノテーションを割り当てたりできます。本番環境用の Production というアノテーション、開発環境用の Development などのアノテーションを設定することができます。アセットがサポートしているアプリケーションのタイプに応じて、しきい値や警告の重要度を変更することができます。たとえば、本番アプリケーションのデータストアのしきい値に違反すると_critical warning_が発生し、開発環境でも同じ違反で_warning_のみが発生する可能性があります。定義済みのポリシーにアノテーションを組み込むと、重要度の低いアセットに関する不要なアラート通知をさらに削減できます。

ストレージプールの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、ストレージプールのアセットのしきい値を超えたときに通知するアラートをトリガーすることができます。

作業を開始する前に

この手順は、ストレージプールがシンプロビジョニングされていることを前提としています。

このタスクについて

停止につながる可能性のあるストレージプールの変更を監視してレポートするポリシーを作成する。シンプロビジョニングされた物理ストレージプールでは、物理容量を監視し、オーバーコミット率を監視します。

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表示され、リストに表示されている順序で評価されます。通知が有効になっている場合（* Admin > Notifications *）、パフォーマンスポリシーに違反したときにEメールを送信するようにInsightを設定できます。

3. [*+追加]をクリックして、新しいポリシーを作成します。
4. [ポリシー名]*に、ストレージプールのポリシー名を入力します。
5. [タイプのオブジェクトに適用]*で[ストレージプール]を選択します。
6. [* Apply after window of *] に、最初のオカレンスを入力する。
7. [* （ * ）] に重大度 * を入力します
8. しきい値を超えたときに通知を受け取る E メール受信者を設定します。

   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。このポリシーに関する違反のアラートがリスト内のすべての受信者に送信されます。

9. * 次のいずれかに該当する場合はアラートを作成します。 * 容量比率を入力してください - 使用済み >85%

結果

この構成では、ストレージプールの物理容量の 85% を超える容量が使用されている場合に、重大な警告メッセージが送信されます。物理メモリの 100% を使用すると、アプリケーションに障害が発生します。

追加のストレージプールポリシーを作成します

このタスクについて

追加の「容量比率-使用済み」ポリシーを作成します。このポリシーを使用すると、ストレージプールの使用済み容量が75%を超えたときに警告メッセージが表示されます。通知が有効になっている場合（* Admin > Notifications *）、パフォーマンスポリシーに違反したときにEメールを送信するようにInsightを設定できます。

データストアのパフォーマンスポリシーの作成

監視対象のストレージプールに関連するデータストアに関連付けられた指標のしきい値を設定したパフォーマンスポリシーを作成できます。デフォルトでは、パフォーマンスポリシーは作成時に指定したタイプのすべてのデバイスに適用されます。特定のデバイスまたはデバイスセットのみをパフォーマンスポリシーに含める場合は、アノテーションを作成します。

作業を開始する前に

パフォーマンスポリシーでアノテーションを使用する場合、ポリシーを作成する前にアノテーションが存在している必要があります。

このタスクについて

監視しているデータストアが設定したしきい値を超えたときに通知するパフォーマンスポリシーを作成します。必要に応じてグローバルポリシーがすでにシステムに含まれている場合や、データストアにアノテーションをアノテートする場合はアノテーションを使用するポリシーも機能する場合があります。

手順

1. Insightのツールバーで、**[管理]**>*[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。既存のパフォーマンスポリシーを確認し、監視するしきい値の指標に対応する既存のポリシーを特定します。

2. [+追加]*をクリックして新しいポリシーを追加します
3. 「ポリシー名」を追加します。

   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、データストアには「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。

4. オブジェクトタイプとして「 Datastore 」を選択します
5. "`First occurrence`"をクリックします。

   [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。

6. 「警告」をクリックします。
7. 「アラートの作成」では、* Capacity ratio-over commit を選択し、> 150 *に設定します

   容量に関連するアラート（**Capacity total**やCapacity Used*など）を追加で作成することもできます。

ホストおよび**VM**のファイルシステム使用率データを収集しています

Host and VM File SystemsデータソースとHost Utilizationライセンスを組み合わせることで、既知のホストおよびVMについて、ファイルシステムレベルでのレポートとチャージバックを作成できます。

OnCommand Insight はストレージデバイスからデータを収集します。ストレージデバイスのほとんどは、ボリュームをブロックデバイスとして報告します。これにより、Insightではストレージレベルで利用率をレポートできますが、ファイルシステムレベルではレポートできません。ストレージアレイは通常、書き込まれたブロックを認識しますが、解放されたブロックは認識しません。

クライアントホストとVMがファイルシステムを実装（NTFS、ext *…） これらのブロックデバイスの上にあります。ほとんどのファイルシステムは、ディレクトリとファイルのメタデータを含む目次を保持しています。ファイルが削除されると、そのエントリは目次から単純に削除されます。これらのファイルによって使用

されたブロックはファイルシステムによる再利用の対象になりますが、ストレージアレイは再利用を認識しません。Insightでファイルシステムの使用状況をレポートするには、正確なチャージバックを実現するために、ファイルシステムをクライアントホストまたはVMの観点から収集する必要があります。

Insightでは、* NetApp Host and VM File System データソースと Host Utilization ライセンスを組み合わせて、このレベルのファイルシステム利用率データを収集できます。コストが正確にレポートされるように、**VM**には適切な Compute Resource Group *という名前を付け、関連するストレージアレイには適切な*階層*のアノテーションを適切なコストでアノテートする必要があります。

> Host Utilizationライセンスは、Insightの他のライセンスとは異なり、容量ベースのライセンスではなく、リソースベースのライセンスです。

ファイルシステム収集用に**Insight**を設定します

ファイルシステム利用率データを収集するようにInsightを設定するには、Host Utilization Packライセンスをインストールし、NetApp Host and VM File Systemsデータソースを設定する必要があります。

作業を開始する前に

Host Utilization Packライセンスをインストールしていない場合は、インストールします。ライセンスは、* Admin **>** Setup ページの Licenses *タブで確認できます。

Host and VM File Systemsデータソースでは、Insightで現在収集または検出されている既知の*コンピューティングリソース*（ホストおよびVM）について、ファイルシステムの利用率とファイルシステムのメタデータのみが報告されます。

- 仮想マシンは、Hyper-VやVMwareなどのハイパーバイザーデータソースによって収集されます。
- ホストはデバイス解決によって検出されます。

適切な階層のアノテーションが適切なストレージリソースに表示されている必要があります。

接続された次のブロックストレージデバイスがサポートされます。

- NetApp clustered Data ONTAP （clustered Data ONTAP）
- NetApp 7-Mode
- クラリオン
- Windows：FC、iSCSI用のVMware仮想ディスク（VMDK）
- Linux：VMware VMDK（iSCSIおよびFCはサポートされません）

コンピューティングリソースグループ*は、共通の管理クレデンシャルを共有するホストや仮想マシンをグループ化できるアノテーションです。

手順

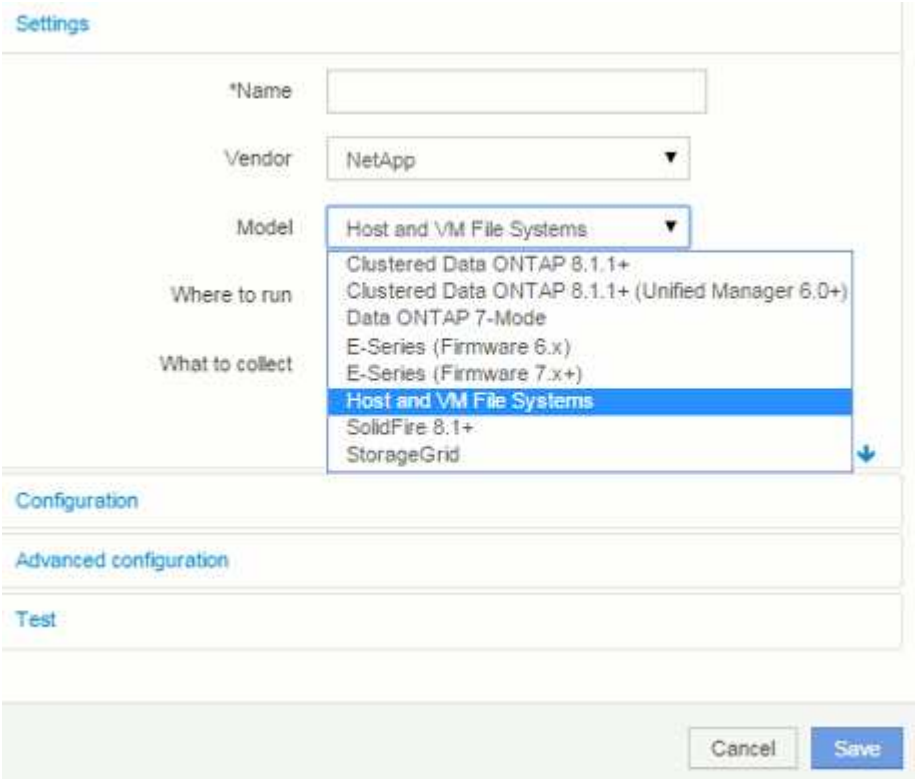
1. 最初に、コンピューティングリソースグループ*に含めるホストや仮想マシンをアノテートします。**[**クエリ**]>***+[新しいクエリ]*に移動し、_Virtual Machine_assetsを検索します。

   この手順は、_Host_assetsについても繰り返す必要があります。

2. テーブルの右側にある列セレクタをクリックし、*[Compute Resource Group]*列を選択してクエリ結果テーブルに表示します。
3. 目的のコンピューティングリソースグループに追加する仮想マシンを選択します。フィルタを使用して特定のアセットを検索できます。
4. ボタンをクリックし、[Edit annotation]*を選択します。
5. [*Compute Resource Group*]アノテーションを選択し、[*value*]フィールドで目的のリソースグループ名を選択します。

   選択したVMにリソースグループのアノテーションが追加されます。リソースグループ名は、あとでHost and VM File Systemsデータソースで設定する名前と一致している必要があります。

6. コンピューティングリソースグループのHost and VM File Systemsデータソースを設定するには、* Admin **>** Data sources および Add * The_NetApp Host and VM File Systems_data sourceをクリックします。



7. [設定]セクションで、ファイルシステムデータを取得するための適切な権限を持つオペレーティングシステムユーザーの*[ユーザー名]および*[パスワード]を入力します。Windowsオペレーティングシステムユーザの場合、Windows環境でドメインプレフィックスが使用されている場合は、ドメインプレフィックスを含める必要があります。

   LinuxにインストールされているInsight Acquisition Unit（AU）はLinuxのコンピューティングリソースについてレポートできますが、WindowsにインストールされているAUはLinuxまたはWindowsのいずれかのコンピューティングリソースと通信できます。

8. ファイルシステムの利用率データの収集元となるアセットの*[コンピューティングリソースグループ]*の名前を入力します。この名前は、上記のアセットへのアノテートに使用したリソースグループの名前と一致している必要があります。

   [Compute Resource Group]フィールドを空のままにした場合は、[Compute Resource Group]アノテーションのないホストまたはVMのデータがデータソースで収集されます。

9. [**Advanced Configuration**]セクションで、このデータソースのポーリング間隔を入力します。通常、デフォルトの6時間で十分です。
10. 保存する前に、データソース接続を*テスト*することをお勧めします。接続が成功すると、グループに含まれているコンピューティングリソースターゲットの数も表示されます。
11. [保存（ Save ）] をクリックします。Host and VM File Systemsデータソースの次回のポーリング時にデータの収集が開始されます。
12. 収集されたファイルシステムデータは、ホストまたはVMのアセットページの[File System]ウィジェットで確認できます。

File Systems

Name	Capacity (Used / Total GB)	Type	Storage Resource
/	9.15% (11.0 / 120.0)	xfs	vifasnane:...:vm_oci_
/boot	23.79% (0.1 / 0.5)	xfs	vifasnane:...:vm_oci_
/dev/dm-1	7.8	swap	vifasnane:...:vm_oci_

Showing 1 to 3 of 3 entries

13. 作成するコンピューティングリソースグループごとに、上記の手順を繰り返します。各コンピューティングリソースグループに専用のHost and VM File Systemsデータソースを関連付ける必要があります。

    ファイルシステム情報は、環境内の従来のVMwareまたはHyper-Vデータソースですでに取得されているホストおよびVMについて収集されます。

ファイルシステムのチャージバックとレポート

ファイルシステムのチャージバックは、常にストレージの観点から実行されます。特定のコンピューティングリソースグループに対してアノテートされた仮想マシンに関連付けられているストレージアレイは、そのリソースグループのチャージバックレポートに含まれます。

作業を開始する前に

ファイルシステム利用率のチャージバックに含める仮想マシンには、適切なコンピューティングリソースグループ名をアノテートする必要があります。これらの仮想マシンに関連付けられているストレージアレイには、適切な階層のアノテーションがアノテートされている必要があります。これらのアノテーションを設定したあとにData WarehouseへのETLが実行されている必要があります。

手順

1. 通常は、レポートサーバーでブラウザを開きます `https://<host or IP>:9300/p2pd``http://<host or IP\>:9300/bi (7.3.3 or later)` ログインします。
2. [File System Utilization]*パッケージを選択し、新しいレポートを作成します。

3. データマートから項目をドラッグアンドドロップしてレポートを作成します。

   以下の例は非常に単純なレポートです。特定のビジネスニーズに基づいて作成された複雑なレポートを作成できます。

Name	Type	Allocated Capacity GB	Used Capacity GB	Tier Name	Cost	Storage Name
/	xfs	119.96	9.96	N/A		vifasnane05,vifasnane06
/	xfs	5,492.53	799.63	Tier 1	100	vifasnane
/boot	xfs	0.48	0.17	N/A		vifasnane05,vifasnane06
/boot	xfs	8.72	2.41	Tier 1	100	vifasnane
/dev/dm-1	swap	7.81	0.00	N/A		vifasnane05,vifasnane06
/dev/dm-1	swap	140.61	0.78	Tier 1	100	vifasnane
C:\	NTFS	948.27	331.98	Tier 1	100	vifasnane
PHYSICALDRIVE0: System Reserved	NTFS	1.70	1.41	Tier 1	100	vifasnane

チャージバックデータをレポートするようにシステムを設定しています

チャージバックレポートには、ストレージ容量のチャージバックとアカウンタビリティの情報がホスト、アプリケーション、およびビジネスエンティティ別に表示され、現在のデータと履歴データの両方が含まれます。

このガイドでは、サービスレベルのコストとストレージ使用コストに関するアカウンタビリティを示すチャージバックレポートを生成するようにInsightを設定する方法について説明します。このガイドの目的は、シンプルなチャージバックレポートを作成するために必要な手順を説明し、Insightユーザ固有の環境でチャージバックを設定する際に使用できるオプションを理解することです。

このレポート例では、アプリケーションごとにプロビジョニングされたリソースとリソースのコストを特定します。レポートの出力は、Insightで次のデータを定義して作成します

- ストレージ階層
- 各ストレージ階層に関連付けられたコスト
- プロビジョニングされたストレージ容量
- サービスレベル

- サービスレベルあたりのコスト

以降のセクションでは、このデータにInsight Reportingからアクセスできるように設定する手順について説明します。

チャージバックで使用するアノテーションの定義

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、データの全体像を把握するために必要な特殊なアノテーションを定義できます。 たとえば、アセットの寿命、アセットが配置されているデータセンター、ストレージのGBあたりのコストを定義するストレージ階層などをアノテーションで定義できます。

このタスクについて

このガイドのチャージバックレポートの例では、サービスレベルと階層レベルのデータを提供しています。サービスレベルと階層レベルごとにアノテーションを作成し、サービスレベルと階層レベルのコストを定義する必要があります。

手順

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

   アノテーションページが表示されます。

3. [Service Level]または[Tier]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. 新しい階層とコストを追加するには、*[追加]*をクリックします。

   レポートの例では、階層とサービスレベルの名前に「Gold」、「Sliver」、「Bronze」という貴金属の例えが使用されています。Tier 1、Level 2、Supremeなど、組織によって選択された命名規則を使用できます。

5. 「Gold-Fast」、「Gold」、「Silver」、「Bronze」の各階層の値と、それぞれに関連するコストを入力します。

   入力する値によって、アプリケーションで使用されるストレージのGBあたりのコストが定義されます。サービスレベルのコストは、サービスを提供するコスト、または消費者にサービスを提供するための実際の価格にすることができます。これらのコストはチャージバックレポートで報告されます。

6. 完了したら、*[保存]*をクリックします。

チャージバックで使用するアプリケーションを定義します

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コストデータを追跡するには、まず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。

> この例では、アプリケーションをビジネスエンティティに関連付けていません。

手順

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

   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. [Name]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。レポートで特定されたアプリケーション（African Tours、APAC Commercial Salesなど）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、*[ビジネスエンティティ]*をクリックし、リストからエンティティを選択します。
7. ボリューム共有は使用しません。**[**検証**]**[ボリューム共有]ボックスをクリックしてオフにします。
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。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

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特定のアセットに関連付ける必要があります。簡単なアドホック方式を使用して、アプリケーションをアセットに適用できます。アプリケーションを一括で適用する場合は、クエリメソッドを使用して、アプリケーションに割り当てるアセットを特定する必要があります。

一時的な方法を使用してアプリケーションをアセットに割り当てます

アプリケーションをアセットに割り当てて、アプリケーションが使用するアセットのリソースを識別できるようにします。アセットにコストが割り当てられている場合は、アプリケーションによって発生するコストを特定でき、リソースがサイズで測定される場合は、リソースを補充する必要があるかどうかを判断できます。

このタスクについて

アセットにアプリケーションを割り当てるには、次のメソッドを使用します。

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、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。

オプション	説明
アセットのリストに移動します	>[アセットダッシュボード]*をクリックし、アセットを選択します。
アセットを検索します	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]*と表示されています）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。

クエリを使用してアセットにアプリケーションを割り当てます

アプリケーションをアセットに割り当てて、アプリケーションが使用するアセットのリソースを識別できるようにします。アセットにコストが割り当てられている場合は、アプリケーションによって発生するコストを特定でき、リソースがサイズで測定される場合は、リソースを補充する必要があるかどうかを判断できます。

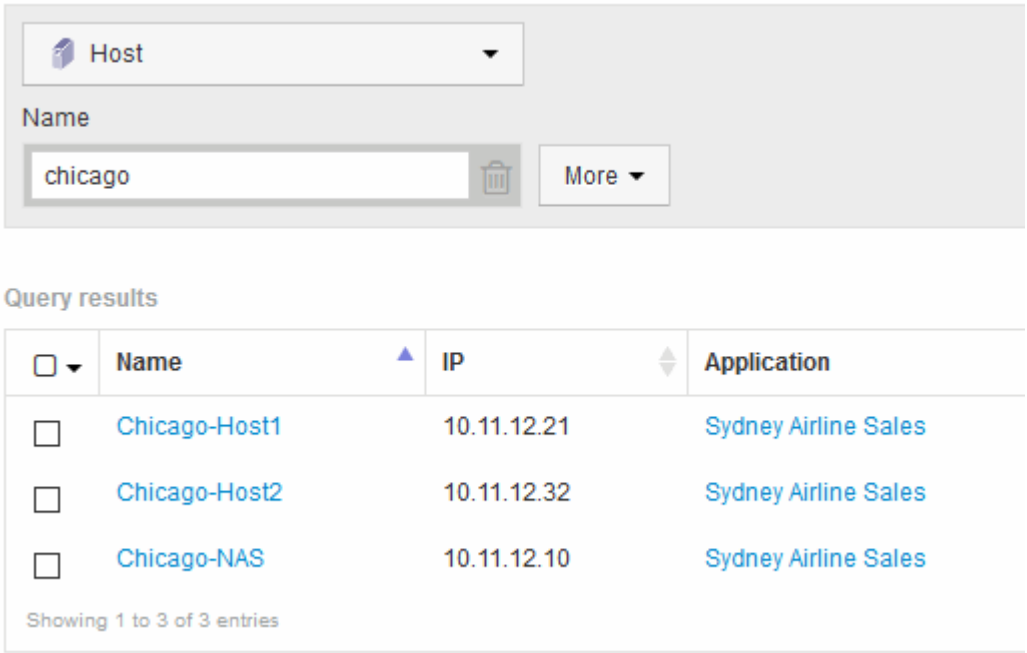
このタスクについて

クエリを使用すると、1つのアプリケーションに複数のアセットを割り当てるタスクを簡易化できます。

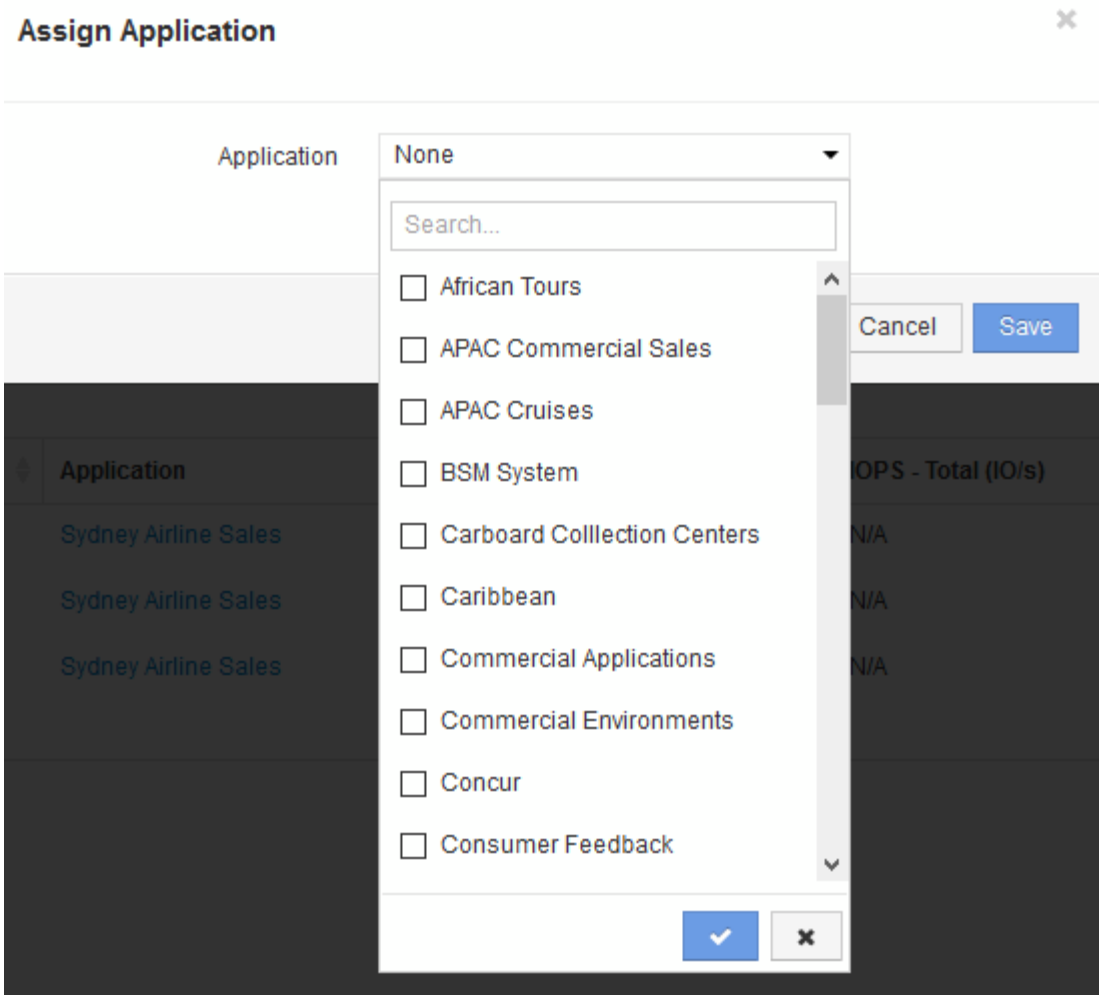
手順

1. アプリケ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。たとえば、地理的な場所に関連する特定の名前を持つホストに割り当てる場合は、**[Queries]>**[+ New Query]*をクリックします
2. [ホスト]*をクリックします
3. [名前]フィールドにと入力します `Chicago`

   のすべてのホストが表示されます `Chicago` 名前の一部として。



4. クエリで特定されたホストを1つ以上選択します。
5. **>**[アプリケーションの追加]*をクリックします



[アプリケーションの割り当て]ダイアログが表示されます。

6. ホストに割り当てるアプリケーションを選択し、をクリックします
7. [保存（ Save ）] をクリックします。

   [User Data]セクションにアプリケーション名が表示されます。

単純なチャージバックレポートの作成

チャージバックレポートを使用すると、管理者やマネージャーは、アプリケーション、ビジネスエンティティ、サービスレベル、階層別に使用容量を評価できます。チャージバックレポートには、容量のアカウンタビリティ、過去の容量のアカウンタビリティ、トレンド分析データが含まれます。これらのレポートのデータは、OnCommand Insight データウェアハウスから構築およびスケジュール設定されます。

作業を開始する前に

サンプルレポートを作成するには、ストレージ階層のコストをレポートするようにシステムを設定する必要があります。次の作業を完了する必要があります。

- 階層のアノテーションを定義します。
- アノテーションにコストを割り当てます。
- データを追跡するアプリケーションを定義します。
- アプリケーションをアセットに割り当てます。

このタスクについて

この例では、Cognos Workspace Advancedレポートツールを使用してチャージバックレポートを作成します。Workspace Advancedでは、データ要素をレポートパレットにドラッグアンドドロップしてレポートを作成できます。

手順

1. OnCommand Insight Web UIで、レポートアイコンをクリックします。
2. Reporting Portalにログインします。
3. IBM Cognos Connectionツールバーで、* Launch **>** Cognos Worksapce Advanced *をクリックします

   Workspace Advancedパッケージ画面が開きます。

4. **>**[チャージバック]*をクリックします

   [IBM Workspace Advanace]画面が表示されます。

5. [新規作成]*をクリックします
6. [新しい*レポート]ダイアログで、*[リスト]*をクリックしてリストレポートを指定します。

   レポートパレットが表示され、ソース見出しの下にチャージバックの「サンプルデータマート」と「高度なデータマート」が表示されます。

7. 各データマートの横にある矢印をクリックして展開します。

   データマートのすべての内容が表示されます。

8. 「サンプルデータマート」からレポートパレットの左端の列に「アプリケーション」をドラッグします。

   パレットに項目をドラッグすると、列が縮小されて強調表示されます。アプリケーションデータを強調表示された列にドロップすると、すべてのアプリケーションが列に正しく表示されます。

9. 「単純なデータマート」からレポートパレットの次の列に「階層」をドラッグします。

   各アプリケーションに関連付けられたストレージ階層がパレットに追加されます。

10. 「Simple Data Mart」の「Tier Cost」をレポートパレットの次の列にドラッグします。
11. [Simple Data Mart]から[Provisioned capacity]をレポートパレットの次の列にドラッグします。
12. Ctrlキーを押しながら、パレットの「Tier cost」列と「Provisioned capacity」列を選択します。
13. 選択した列のいずれかでマウスを右クリックします。
14. **>**[ティアコスト]*[プロビジョニング済み容量DB]*をクリックします

「Tier Cost * Provision Capacity GB」というタイトルの新しい列がパレットに追加されます。

15. [Tier Cost]*[Provision Capacity GB]*列を右クリックします。
16. **>**[データ型]*をクリックします
17. **>**[通貨]*をクリックします
18. [OK] をクリックします。

    これで、列データがUS通貨としてフォーマットされました。

19. [Tier Cost * Provision Capacity GB]を右クリックし、*[Edit Data Item Label]*を選択します
20. [Name]フィールドを「Provisioned Capacity Cost」に置き換えます。
21. レポートを実行するには、* Run **>** Run report -html *をクリックします

    次のようなレポートが表示されます。

Application	Service Level	Service Level Cost	Tier	Tier Cost	Provisioned Capacity GB	Provisioned Capacity Cost
APAC Commercial Sales	Gold-Fast	12	Gold-Fast	12	674.04	$8,088.42
APAC Commercial Sales	Silver	10	Silver	7	1,903.83	$13,326.82
APAC Cruises	Gold-Fast	12	Gold-Fast	12	730.20	$8,762.44
African Tours	Gold	12	Gold	10	4,856.12	$48,561.16
African Tours	Silver	10	Silver	7	1,480.85	$10,365.93
CRM	Bronze	3	Bronze	3	5,689.08	$17,067.23
Caribbean	Gold	12	Gold	10	4,590.41	$45,904.08
Commercial Applications	Bronze	3	Bronze	3	14,312.88	$42,938.64
Commercial Applications	Gold-Fast	12	Gold-Fast	12	40,308.42	$483,701.05
Commercial Environments	Bronze	3	Bronze	3	16,812.27	$50,436.81
Commercial Environments	Gold	12	Gold	10	9,313.51	$93,135.13
Commercial Environments	Silver	10	Silver	7	1,480.79	$10,365.54
Concur	Gold	12	Gold	10	247.39	$2,473.91
Concur	Gold-Fast	12	Gold-Fast	12	575.17	$6,902.09
Consumer Feedback	Gold	12	Gold	10	1,335.89	$13,358.94

I/O 密度レポートに内部データボリュームのみが記載されていることを確認する

ネットアップストレージシステムでは、ルートアグリゲートにルートボリュームが含まれています。ルートボリュームには、ストレージシステムを管理および制御するための特別なディレクトリと構成ファイルが格納されています。管理処理と制御処理によって、ルートアグリゲートで大量のアクティビティが発生する可能性があります。Insightシステムで IO密度が高い上位10個の内部ボリュームを照会すると、結果にはネットアップのルートアグリゲートが上位10個のメンバーとして含まれることがあります。

環境を監視する際には、どの内部データボリュームが高い I/O 密度を生成しているかを特定することが重要です。データボリュームだけを正確に特定するには、ネットアップの内部ボリュームを、 I/O 密度の監視に使用するクエリから分離する必要があります。

このガイドでは、ネットアップのルートアグリゲートを簡単に特定し、それらを内部ボリュームのクエリの結果から分離する方法と、システムにネットアップの新しいルートアグリゲートが追加されるたびにそれらを除外するルールを作成する方法について説明します。I/O密度レポートを内部データボリュームから取得するには、Insightの次の機能を使用します。

- Insight で監視しているネットアップのルートアグリゲートを特定するクエリを作成する。
- ネットアップのルートアグリゲートのそれぞれにアノテーションを割り当てる。
- ネットアップのアグリゲートを除外するアノテーションルールを作成します

環境内でネットアップのルートアグリゲートを特定するクエリの作成

クエリは、ユーザが選択した条件に基づいて、細かいレベルまで検索する機能です。クエリを使用すると、ネットアップのルートアグリゲートが含まれている環境内の内部ボリュームを検索できます。

手順

1. OnCommand Insight Web UIで、環境内のネットアップのルートアグリゲートを特定するクエリを作成します。**[Queries]**>*>[Select Resource Type]*
2. [ストレージプール]*をクリックします
3. ルートアグリゲートの名前を入力します

   この例では、名前に「aggr0」を使用しています。アグリゲートの作成時には、次の要件に従って名前を指定する必要があります。

   - 先頭の文字にはアルファベットまたはアンダースコア（ _ ）を使用する必要があります。
   - アルファベット、数字、アンダースコアのみを使用できます。
   - 250 文字以内で指定します。アグリゲートの名前は通常、 aggr0 、 aggr_0 などの形式にします。環境内のネットアップのルートアグリゲートをすべて特定するには、反復的なプロセスが必要となる場合があります。
4. [保存（ Save ）] をクリックし、新しい照会の名前を入力する。

   前述のとおり、この作業は反復的なプロセスになる場合があり、ネットアップのすべてのルートアグリゲートを特定するために複数のクエリが必要になることがあります。

クエリで返されるルートボリューム用のアノテーションを作成します

アノテーションはアセットに割り当てる特殊なメモで、アノテーションによってアセットをフィルタすることができます。作成したアノテーションは、環境内のネットアップのルートアグリゲートを特定し、それらのアグリゲートを特定のレポートに含めないようにするために使用します。

作業を開始する前に

「High I/O Density」レポートから除外するルートアグリゲートをすべて特定しておく必要があります。

手順

1. クエリを使用して特定したすべてのネットアップルートアグリゲートに関連付けるアノテーションを作成します。* Manage **>** Annotations *
2. [追加（ Add ）] をクリックします。
   a. アノテーションの名前として「 * RootAggr 」と入力します
   b. アノテーションの概要として「 * Remove root aggregate from "High I/O Density" report * 」と入力します
   c. アノテーションのタイプとして「 * Boolean * 」と入力します
3. [保存（ Save ）] をクリックします。

I/O 密度に関するレポートから特定のアグリゲートを自動的に除外するための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。アノテーションルールは、ユーザが作成するクエリに基づいてシステム上で実行されるもので、新しいアセットを既存のアセットセットに追加します。これらのアセットセットをレポートから除外すると、新しいアセットも自動的に除外されます。

作業を開始する前に

環境内で特定したネットアップのルートアグリゲートを識別するクエリを作成し、保存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. **>**[アノテーションルール]*をクリックします
3. [追加（ Add ）] をクリックします。

   [Add Rule]ダイアログボックスが表示されます。

4. 次の手順を実行します。
   a. [Name]ボックスに、ルールを説明する一意の名前「'RootAggrExclude'」を入力します。
   b. [Query]をクリックし、アノテーションルールを適用するためにInsightで使用するクエリ「Aggregate0」を選択します。
   c. [Annotation]をクリックし、「'Root agg exclude'」を選択します。
   d. [値（Value）]をクリックし、「True

統合データを収集しています

統合データをOnCommand Insight システムにインポートできます。データは、パフォーマンスデータを収集するデーモンとして実行されるオープンソースソフトウェアcollectd

を使用してインポートすることも、一般的なSNMPデータを収集できる統合SNMPデータソースを使用してインポートすることもできます。

統合データのデータフロー

次の環境 OnCommand Insight サーバに提供できる統合データの総量。

- 100コールのキューが維持されます。

  クライアントがキュー内で1分以上待機すると、タイムアウトエラーが発生します。

- 統合データの推奨取り込み速度は、クライアントごとに1分あたり1回です。
- 使用できる統合オブジェクトタイプは300に制限されています。

collectdソフトウェアおよびドキュメントへのアクセス

出力ライタープラグインソフトウェアおよびcollectdのドキュメントは、ネットアップのGitHubサイトから入手できます。 https://github.com/NetApp/OCI_collectd

統合データのバックアップとリストア

統合データのバックアップとリストアは、OnCommand Insight パフォーマンスデータのバックアップとリストアのポリシーに従ってモデル化されます。パフォーマンスデータのバックアップが設定されている場合は、統合データもバックアップに含まれます。パフォーマンスバックアップと同様に、最新7日間の統合データがバックアップに含まれます。バックアップに含まれている統合データは、リストア処理でリストアされます。

ライセンス

統合データをレポートするには、Performライセンスが必要です。Performライセンスが存在しない場合、エラーが発生し、「Perform license required to report integration data」というメッセージが表示されます。

SNMP統合データを収集しています

SNMP統合データソースを使用すると、OnCommand Insight で一般的なSNMPデータを収集できます。

統合パック

SNMP統合データソースでは、「統合パック」を使用して、収集される統合値、およびそれらの値を提供するSNMPオブジェクトを定義します。

統合パックは次のもので構成されます。

- 特定のデバイスタイプ（スイッチ、ルータなど）のSNMPオブジェクトに関する統合ペイロードの内容を定義するJSON構成ファイル（integration.json）。
- 統合パックが依存するMIBファイルのリスト。

統合パックでは、複数のデータタイプを定義できます。たとえば、RHELホストを統合する場合は、アップタイム、ユーザ数、実行中のプロセス数などの一般的なシステム情報に対してデータタイプを定義し、メモリや

ファイルシステムの使用状況に関するデータに対しては2つ目のデータタイプを定義できます。一般的に、各データ型は"`flat`でなければならず、ネストされたデータを含むことはできません。

1つの統合パックで定義できるデータ型は最大24個です。Insightでは、収集される統合データの量が制限されます。1分間に24個を超えるレポートを取り込みようとすると、速度エラーが発生します。

統合タイプの名前は、次のルールに従う必要があります。

- 名前の1文字目を_、-、+にすることはできません
- 名前に次の文字を使用することはできません：#、\、/、*、？、 "、<、>、|、'、 '、
- UTF-8でエンコードされた100バイトを超えることはできません
- を指定できません。または

統合ファイル形式

統合パックは、SNMPオブジェクトに関する統合ペイロードの内容を定義するJSON構成ファイル（integration.json）が含まれたZIPファイルです。また、すべてのMIBファイルとその依存関係が格納されたMIBsフォルダも含まれています。

。 `integration.json` ファイルはZIPファイルの最上位レベルに存在し、MIBファイルはZIP内の「resources/mibs」サブディレクトリに存在する必要があります。ZIPファイルには、必要に応じて「readme.txt」などのファイルを含めることもできます。統合ZIP構造の例は次のとおりです。

```
.
├── integration.json
└── resources
    └── mibs
        ├── IANAifType-MIB.txt
        ├── IF-MIB.txt
        ├── INET-ADDRESS-MIB.txt
        ├── IP-MIB.txt
        ├── RFC1155-SMI.txt
        ├── RFC-1212.txt
        ├── RFC1213-MIB.txt
        ├── SNMPv2-CONF.txt
        ├── SNMPv2-MIB.txt
        ├── SNMPv2-SMI.txt
        ├── SNMPv2-TC.txt
        └── TCP-MIB.txt
```

SNMP統合パックのインポート

SNMP統合パックをOnCommand Insight にインポートするには、Web UIを使用します。統合パックは、で定義されている「integrationPackName」の値で識別されます `integration.json` ZIPファイルに含まれている構成ファイル。

作業を開始する前に

OnCommand Insight サーバにインポートする統合パックを含む適切な形式のZIPファイルを作成しておく必要があります。

このタスクについて

SNMP統合パックをInsight Serverにインポートするには、次の手順を実行します。

手順

1. * Admin **>** Setup **>** SNMP Integration *をクリックします
2. [ファイルの選択]*をクリックして、SNMPパッケージを含むローカルファイルを選択します。

   選択したファイルが[ファイル]ボックスに表示されます。

   > 同じ名前の既存の統合パックは上書きされます。

3. [インポート]*をクリックします

   ファイルがInsight Serverにインポートされます。

SNMP統合データソースを作成しています

統合SNMPデータソースは、BrocadeおよびCiscoのOnCommand Insight データソースに含まれている他のSNMPベースのデータソースと同様に、共通のSNMP設定プロパティを提供します。

作業を開始する前に

SNMP統合データソースを使用してデータを収集するには、次の条件を満たしている必要があります。

- このSNMPデータソースに使用する統合パックをインポートしておく必要があります。
- すべてのターゲットデバイスで同じ資格情報が共有されます。
- すべてのターゲットデバイスは、設定された統合パックによって参照されるSNMPオブジェクトを実装します。

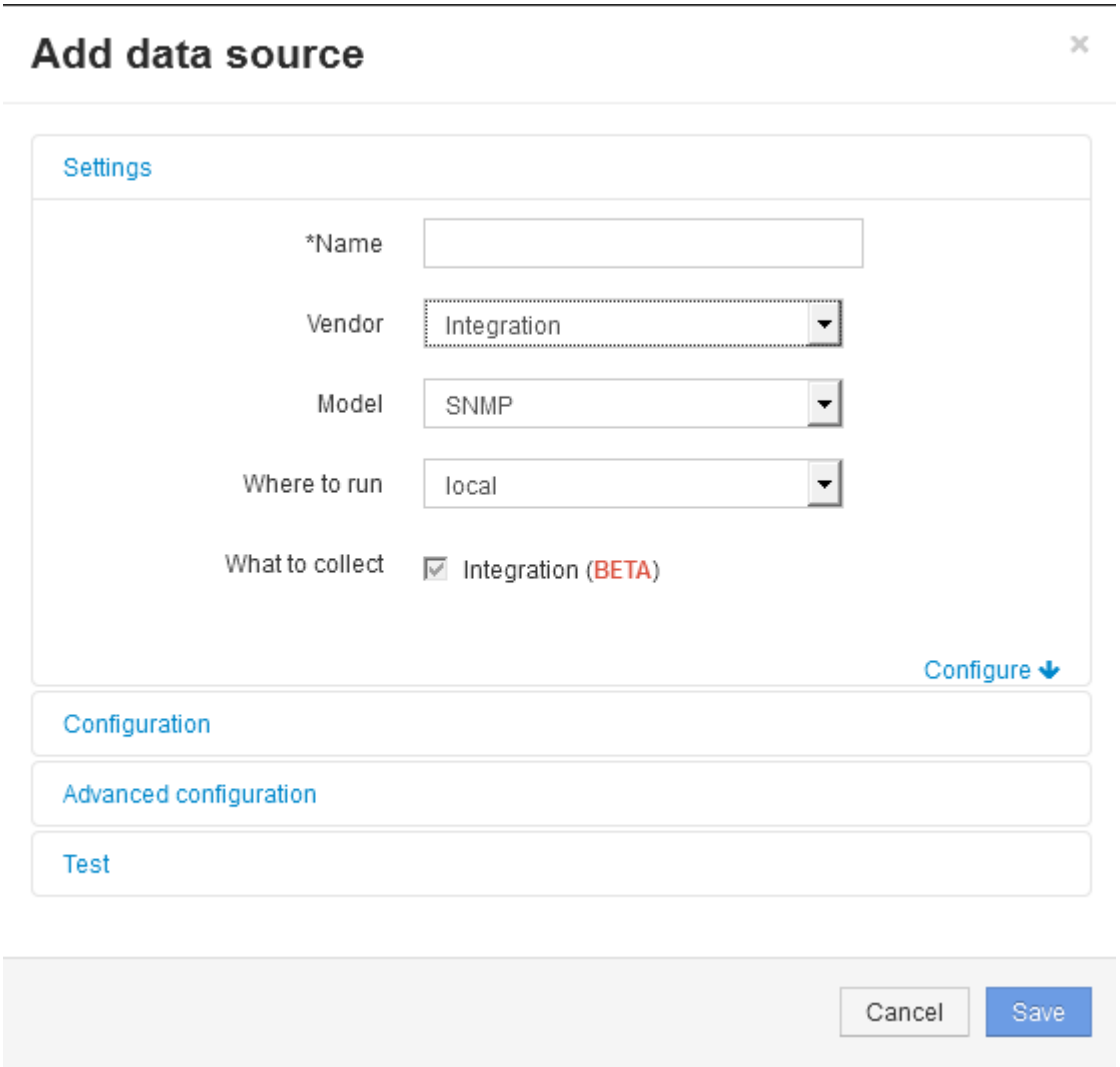
このタスクについて

SNMP統合データソースを作成するには、データソース作成ウィザードでベンダー「Integration」およびモデル「SNMP」を選択します。

手順

1. OnCommand Insight Web UIで、**[**管理**]>***[データソース]*をクリックします
2. 「 * + 追加」をクリックします。
3. データソースの名前を入力します
4. Vendor（ベンダー）で* Integration（統合）*を選択します

5. [Model]で、*[SNMP]*を選択します



6. [What to collect]で*[Integration]*をオンにします

   このデータソース上の唯一のパッケージであり、デフォルトでオンになっています。

7. [設定]*をクリックします
8. SNMPデータの収集元となるシステムのIPアドレスを入力します
9. インポートしたSNMP統合パックを選択します
10. 統合ポーリング間隔を設定します
11. SNMPのバージョンを選択します
12. SNMPコミュニティストリングを入力します

    SNMP V1およびV2の場合。

13. データの収集元となるシステムのユーザ名とパスワードを追加します。

    SNMP V3の場合。

14. [詳細設定]*をクリックします

    [Advanced Configuration]のデフォルト設定が表示されます。必要に応じてこれらの設定を変更します。

integration.jsonファイルの情報

integration.jsonファイルは、ペイロードを識別します。

次の図は、シンプルなintegration.jsonファイルを色分けしたものです。添付の表は、ファイル内のオブジェクトの機能を示しています。

```
{
 "integrationPackName": "WindowsSnmp",
 "description": "Generic integration for mibs supported by the default
SNMP  Agent for Windows 2012, including HOST-RESOURCES",
 "acquisitionType": "SNMP",
 "integrationTypes": [
   {
    "integrationType":      "snmp_win2012_host",
    "name": {
     "mibModuleName":     "RFC1213-MIB",
     "objectName":        "sysName"
    },
    "identifiers": {
     "hostname": {
      "mibModuleName":     "RFC1213-MIB",
     }
    },
    "attributes": {
     "description": {
      "mibModuleName":     "RFC1213-MIB",
      "objectName":        "sysDescr"
     },
     "snmp_sys_obj_id": {
      "mibModuleName":     "RFC1213-MIB",
      "objectName":        "sysObjectID"
     }
    },
    "dataPoints": {
     "uptime": {
      "num": {
       "mibModuleName":   "RFC1213-MIB",
       "objectName":      "sysUpTime"
      }
     }
    }
   }]}
```

Blue	Reserved
Red	User customizable strings and IDs
Green	MIB names
Purple	MIB object
Black	JSON structure

integration.jsonファイルについて

各フィールドには次の特徴があります。

- 「identifiers」セクションは、Insightで新しい「オブジェクト」を作成するための一意の複合キーです
- 「attributes」は、オブジェクトに関するサポートメタデータを提供します。

  どちらの場合も、そのオブジェクトの最新のレポートの値（識別子で識別）のみが保持されます。

- 「dataPoints」は時系列データであり、数値である必要があります。Insightでは、レポートされるすべての値を90日間（デフォルト）保持し、特定されたオブジェクトに時系列でリンクします。

数値式

デフォルトでは、すべての値式は統合ペイロードで文字列として報告されます。「identifiers」と「attributes」は文字列値のみを定義できます。「dataPoints」は文字列または数値を定義できます。数値は、次のいずれかの修飾キーを使用して定義されます。

- Num -カウンタが最後に初期化されてから受信した合計バイト数
- Delta -ポーリング間隔中に受信したバイト数
- rate -ポーリング間隔中の平均受信レート（1秒あたりのバイト数）

  ポーリング間隔中の平均受信速度（1秒あたりのメガバイト数）は、rate処理とmath処理を組み合わせて実行できます

算術演算

。 `integration.json` ファイルは、加算、減算、乗算、除算の算術演算をサポートしています。次の例は、JSONファイルの乗算、除算、および合計の処理を示しています。

```
"network_utilization":
{
  "mult": [
    {
      "div": [
        {
          "sum": [
            "rate": {
              "mibModuleName":  "IF-MIB",
              "objectName":     "ifHCOutOctets",
              "comment":        "bytes per second out"
            },
            "rate": {
              "mibModuleName":  "IF-MIB",
              "objectName":     "ifHCInOctets",
              "comment":        "bytes per second in"
            }
          ]
        },
        {
          "num": {
            "mibModuleName":  "IF-MIB",
            "objectName":     "ifSpeed",
            "comment":        "1,000,000 bits per second"
          }
        }
      ]
    },
    {
      "const":                0.0008,
      "comment":        "normalize to ratio of bits and convert to percent:
                        8 * 100 / 1,000,000 = 0.0008"
    }
  ]
}
```

キーワード

統合パックキーワードstringは、通常は16進数形式でレンダリングされ、代わりにASCII文字としてレンダリングされるオクテット文字列またはオクテット文字列から派生した独自の型を強制するために実装されています。

多くの場合、オクテット文字列には、MACアドレスやWWNなどのバイナリデータが含まれています。

```
"interface_mac": {
          "mibModuleName":      "IF-MIB",
          "objectName":         "ifPhysAddress"
         }
```

ifPhysAddressはタイプPhysAddressです。これはオクテット文字列です。

```
  PhysAddress ::= TEXTUAL-CONVENTION
                DISPLAY-HINT "1x:"
                STATUS       current
                DESCRIPTION
                               "Represents media- or physical-level
addresses."
                SYNTAX       OCTET STRING
```

ifPhysAddressがデフォルトで16進数でレンダリングされると、結果は次のようになります。

```
"interface_mac": "00:50:56:A2:07:E7"
```

ただし、ASCIIとして解釈するオクテット文字列またはオクテット文字列から派生した独自の型がある場合は、「string」キーワードを使用できます。

```
        "string_test_1": {
          "string": {
            "mibModuleName":      "IF-MIB",
            "objectName":         "ifPhysAddress"
          }
        },

        "string_test_2": {
          "string": [
            {
              "mibModuleName":      "IF-MIB",
              "objectName":         "ifPhysAddress"
            },
            {
              "const": "JSD"
            },
            {
              "mibModuleName":      "IF-MIB",
              "objectName":         "ifPhysAddress"
            }
          ]
        }
```

次の例では、キーワードは既存の文字列連結規則に従い、用語の間に1つのスペースを挿入します。

```
      "string_test_1": "PV¢ç",
              "string_test_2": "PV¢ç JSD PV¢ç"
```

「string」キーワードは、1つの用語または用語のリストに作用しますが、ネストされた式には作用しません。ネストされた式は、dataPoint式でのみサポートされます。datapoint式で"string"式を使用しようとすると、次のようなエラーが発生します。

*java.lang.IllegalArgumentException:*インテグレーションパック*'GenericSwitch32'*インデックス*'snmp_generic_interface_32'*セクション*'dataPoints'*キー*'String_test_3'*サポートされていない*JSON*数値式*'{"string":{"mibModuleName":"if-mib",":":"ifPhysAddress"}}}'*

DisplayString、SnmpAdminStringなどの一部の派生オクテット文字列タイプは、「string」キーワードよりもハードコードされています。これは、SnmpAdminStringがUTF-8で特別にエンコードされており、正しく処理したいためです。一方、「string」キーワードは、1文字あたりのシングルバイトASCIIコードを想定したsnmp_frameworkから返されるデフォルトの文字列表現を強制的に使用します。

アプリケーションのパフォーマンス問題の分析

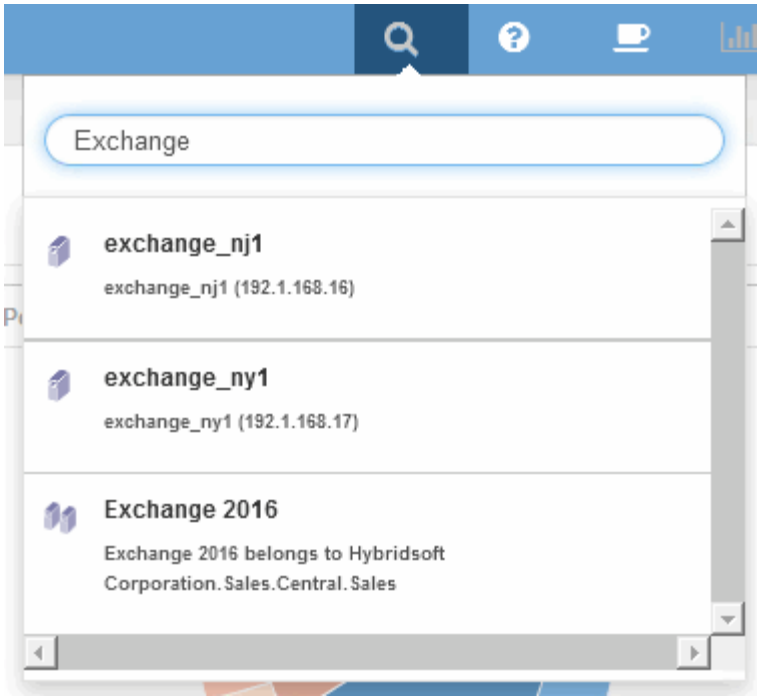
このドキュメントでは、ユーザや管理者に影響を与えているアプリケーションのパフォーマンスの問題に関するレポートに対処するための手順について説明します。たとえば、Exchangeアプリケーションの処理速度が1日中遅くなっているとユーザから苦情が寄せられています。

このタスクについて

OnCommand Insight では、アプリケーションは設定されたエンティティです。アプリケーションに名前とビジネスエンティティを割り当て、そのアプリケーションにコンピューティングリソースとストレージリソースを割り当てます。これにより、インフラストラクチャの健全性をエンドツーエンドでより適切に把握し、インフラストラクチャ資産管理をより積極的に管理できるようになります。

手順

1. 問題 の調査を開始するには、Insightツールバーを使用してExchangeアプリケーションのグローバル検索を実行します。



検索を実行するときに、オブジェクト名の前にオブジェクト記述子を追加して検索結果を絞り込むことができます。

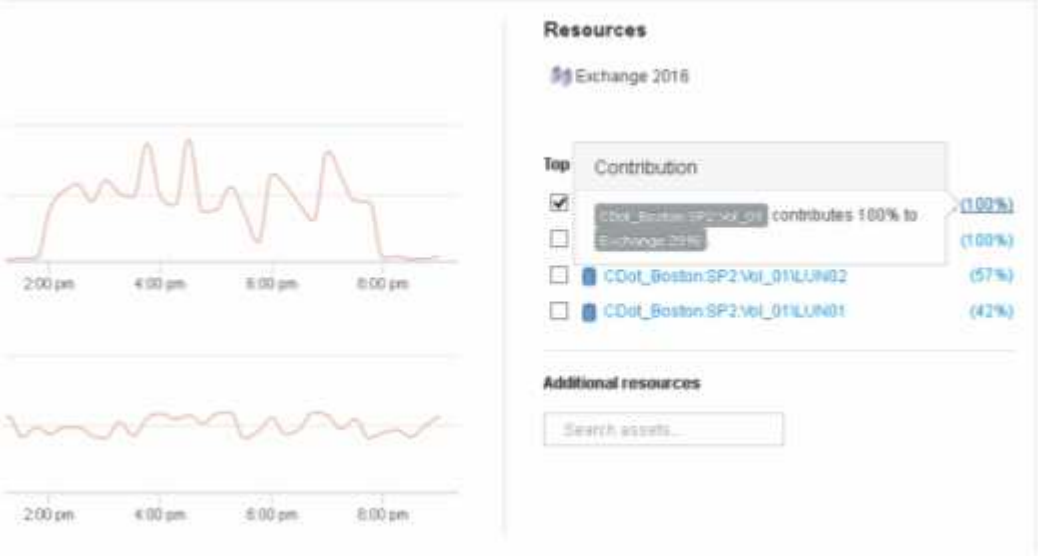
2. 検索結果から「Exchange 2016」を選択すると、アプリケーションのランディングページが表示されます。

アプリケーションランディングページには、次の情報が記載されています。

- 選択した24時間のレイテンシグラフの右側にレイテンシの増加が表示されます。
- レイテンシが増加しても、IOPSレベルに大きな変化はありません。レイテンシの増加は、アプリケー

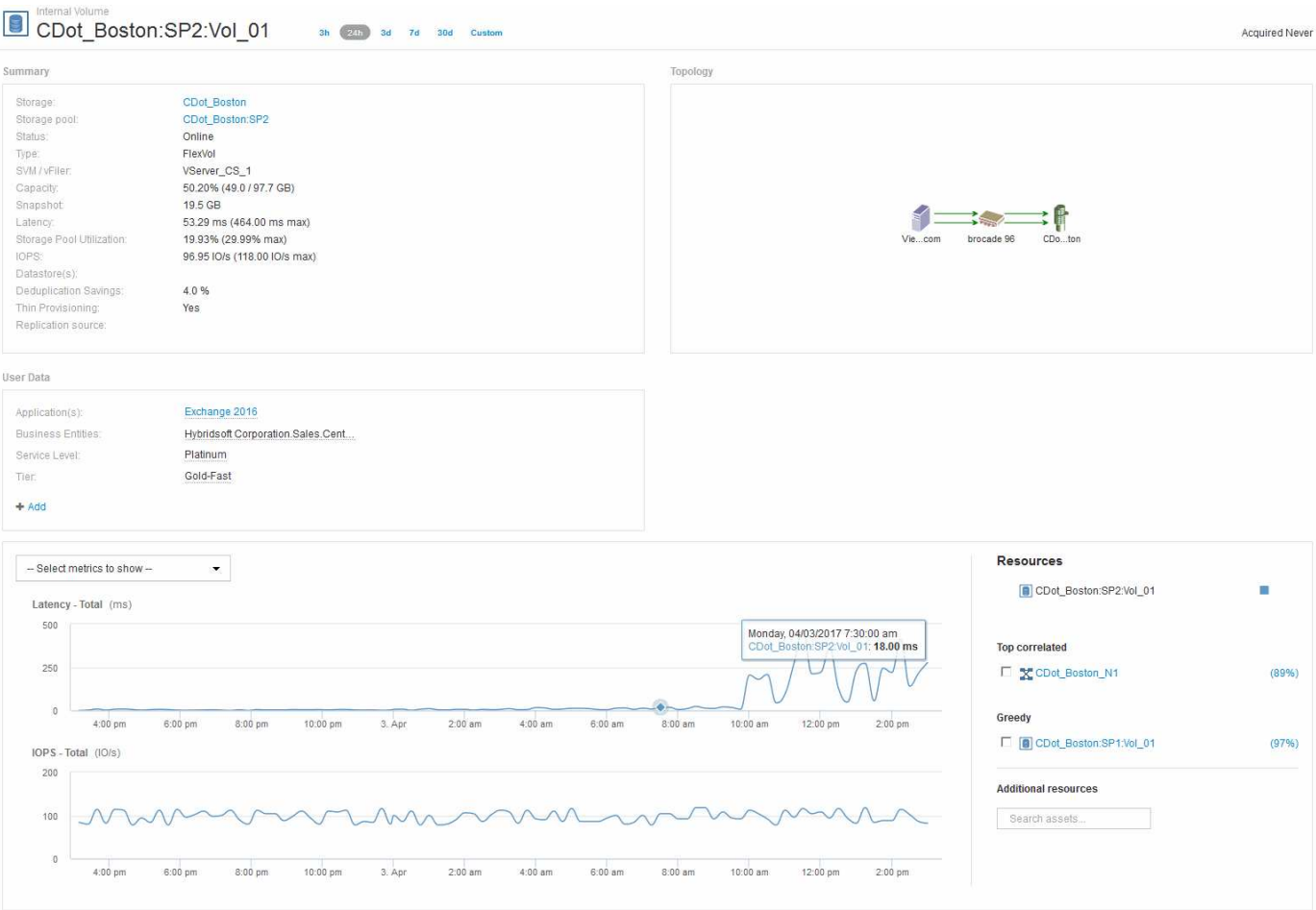
ションの使用率が高いことによるものではないようです。レイテンシの急上昇の原因となる可能性があるストレージのIOPS要求は実際には高くありません。レイテンシの増加は、外部要因が原因である可能性があります。

- [Top contributors]セクションのグラフの右側で、選択した内部ボリュームCDot_Boston：SP2：Vol_01の100%をクリックします。このリソースがExchange 2016アプリケーションに100%貢献していることが表示されます。



- この内部ボリュームCDot_Boston：SP2：Vol_01のナビゲーションリンクをクリックして、内部ボリュームのランディングページにアクセスします。内部ボリュームを分析すると、レイテンシの急増に関連する情報が得られる場合があります。

内部ボリュームを確認しています



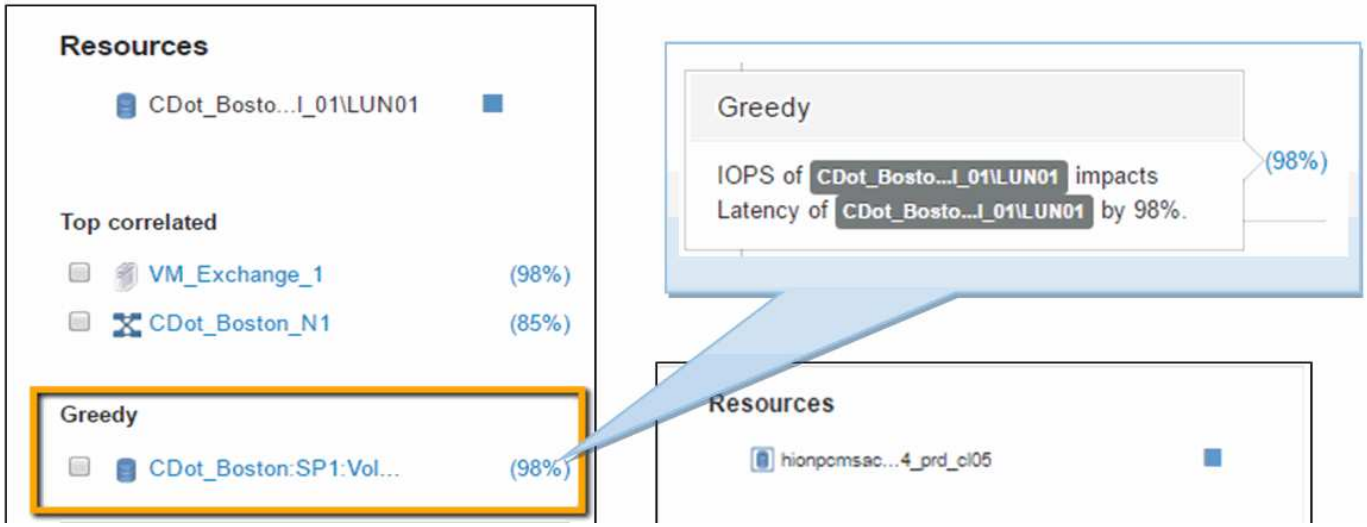
内部ボリュームのランディングページには、次の情報が表示されます。

- 内部ボリュームのパフォーマンスグラフは、レイテンシとIOPSの両方について、アプリケーションのパフォーマンスに表示されていたグラフと一致します。
- 関連するアセットが表示される[Resources]セクションで、「Greedy」リソース（CDot_Boston：SP1：Vol_01）が特定されます。

Greedyリソースは、Insightの相関分析で特定されます。システムを大量に消費しているリソースやパフォーマンスが低下しているリソースは、同じ共有リソースを使用する「ピア」です。GreedyリソースのIOPSまたは利用率は、デグレード状態のリソースのIOPSまたはレイテンシに悪影響を及ぼします。

GreedyリソースとDegradedリソースは、仮想マシン、ボリューム、内部ボリュームのランディングページで特定できます。各ランディングページには、最大2つのGreedyリソースが表示されます。

関連性のランキング（%）を選択すると、Greedyリソース分析の結果が表示されます。たとえば、Greedy Percentageの値をクリックすると、デグレード状態のアセットに対する処理に影響する処理がアセットに対して表示されます。次の例を参照してください。

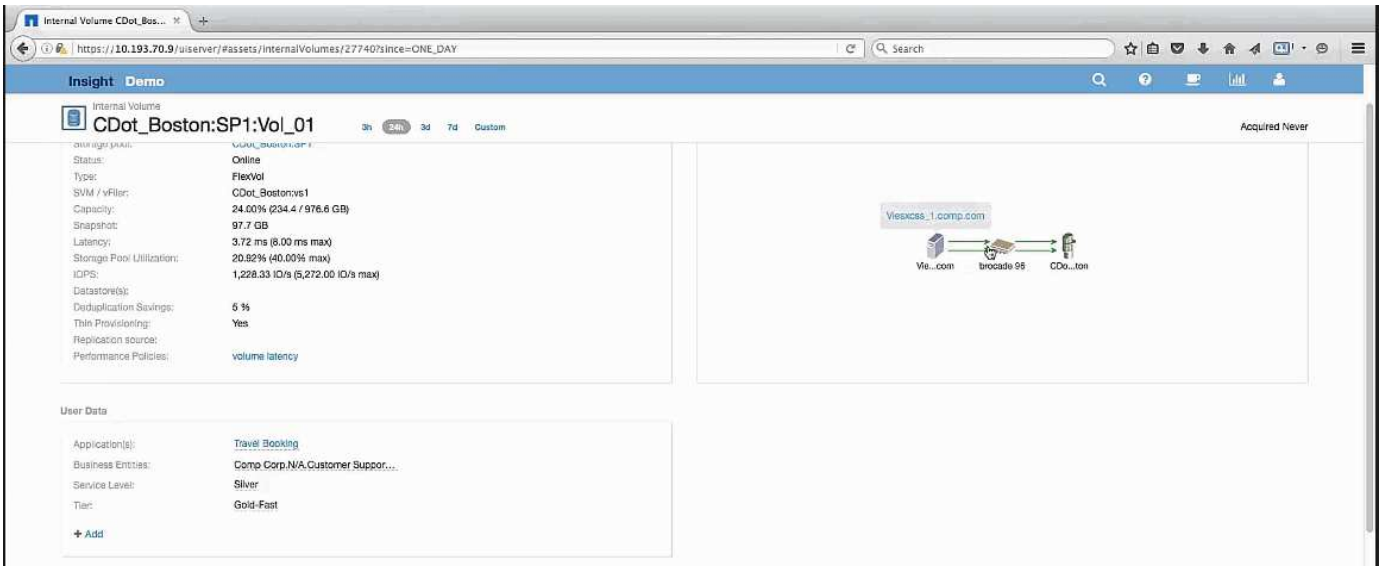


デグレード状態のリソースを特定したら、デグレード（%）のスコアを選択して、デグレード状態のリソースに影響している処理とリソースを特定できます。

貪欲なリソースを調べています

Greedyリソースと特定された内部ボリュームをクリックすると、ボリュームCDot_Boston：SP1：Vol_01のランディングページが開きます。

この内部ボリュームは、概要の詳細では別のアプリケーション（Travel Booking）のリソースであり、別のストレージプールに含まれていますが、Exchange 2016の内部ボリューム（CDot_Boston_N1）と同じノードにあります。



ランディングページには以下が表示されます。

- Travel Bookingアプリケーションに関連付けられている内部ボリューム。
- 新しいストレージプールが関連するリソースで識別されます。
- 調査していた元の内部ボリューム（CDot_Boston：SP2：Vol_01）は「Degraded」と表示されます。
- パフォーマンスグラフでは、アプリケーションのレイテンシは安定しており、IOPSの急増もExchangeアプリケーションのレイテンシとほぼ同じです。

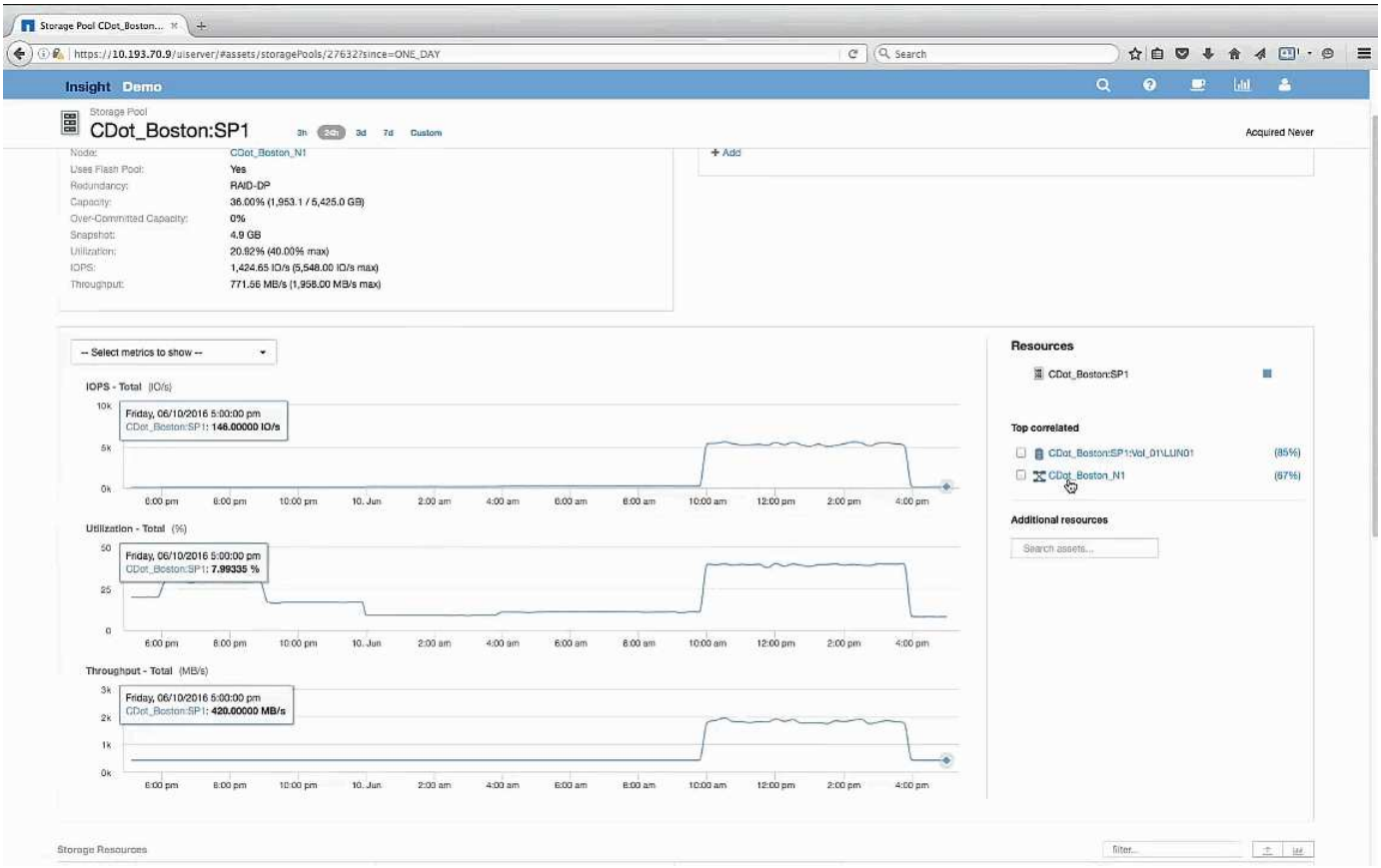
  これは、Exchangeアプリケーションでのレイテンシの急増が、このボリュームでのIOPSの急増が原因である可能性があることを示している可能性があります。

[Resource]セクションのグラフの右側に、関連付けられているDegradedリソース（Exchange 2016内部ボリュームCDot_Boston：SP2：Vol_01）が表示されます。チェックボックスをクリックして、パフォーマンスグラフにデグレード状態の内部ボリュームを含めます。2つのパフォーマンスグラフを合わせると、レイテンシとIOPSの急増がほぼ同じタイミングで発生していることがわかります。これは、Travel Bookingアプリケーションをよりよく理解したいことを示しています。アプリケーションでIOPSの急増がなぜ長引いているのかを理解する必要があります。

Travel Bookingアプリケーションに関連付けられているストレージプールを調べると、アプリケーションでIOPSの急増が発生している理由がわかる場合があります。[CDot_Boston：SP1]をクリックして、ストレージプールのランディングページを表示します。

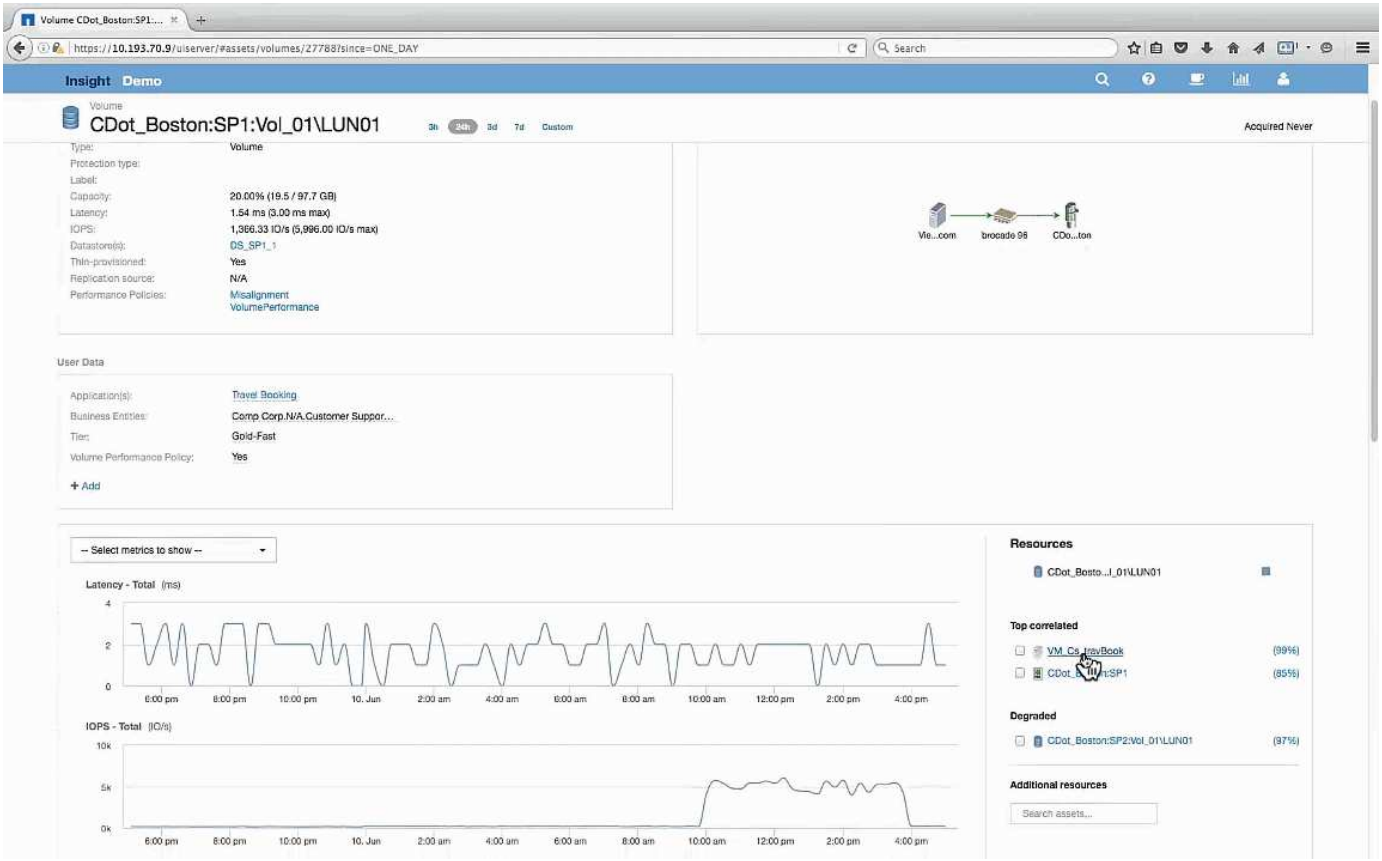
ストレージプールを確認します

ストレージプールのランディングページを確認すると、関連するアセットと同じIOPSスパイクが表示されます。[Resources]セクションでは、このストレージプールのランディングページが旅行アプリケーションのボリュームにリンクしていることを確認できます。ボリュームをクリックすると、ボリュームのランディングページが開きます。



ボリュームを確認しています

ボリュームのランディングページには、関連するアセットと同じIOPSの急上昇が表示されます。



[Resources]セクションに、Travel BookingアプリケーションのVMが表示されます。VMのリンクをクリックすると、VMのランディングページが表示されます。

VMを確認しています

VMのランディングページで、CPU利用率とメモリ利用率を表示する追加の指標を選択します。CPUとメモリの利用率のグラフは、どちらも容量のほぼ100%で動作していることを示しています。これは、Exchangeサーバの問題はストレージの問題ではなく、VMのCPUとメモリの使用率が高く、結果としてディスクへのI/Oのメモリスワップが原因であることを示しています。

この問題を解決するには、追加の同様のリソースを探すことができます。[Additional resources]入力ダイアログに「Node」と入力し、Exchange VMに似たアセットの指標を表示します。この比較は、変更が必要な場合にワークロードをホストするのに適したノードを特定するのに役立ちます。

AWS課金データを収集してレポートする

Amazon AWS Cloud Costデータソースは、Amazonによって生成された課金データを統合データとしてInsightにインポートし、データウェアハウスでレポートを作成できるよ

うにします。

クラウドの課金データをInsightで利用できるようにするには、次の3つの要素があります。

AWSアカウント情報を確認しています。

データを収集するために、InsightでAWS Cloud Costデータソースを設定します。

ETLを使用してData Warehouseにデータを送信し、レポートで使用できるようにします。

AWSでInsightのデータ収集を準備しています

Insightでクラウドのコストデータを収集できるように、AWSアカウントが適切に設定されている必要があります。

このタスクについて

次の手順は、AWSアカウントを介して実行されます。詳細については、Amazonのドキュメントを参照してください。 "http://docs.aws.amazon.com"。AWSクラウドアカウントのセットアップに詳しくない場合は、クラウドプロバイダにお問い合わせください。

> これらの手順は便宜的に提供されており、発行時点で正しいと考えられています。ネットアップは、これらの手順が正確であることを保証するものではありません。AWSアカウントの設定に関する情報やサポートについては、クラウドプロバイダまたはAWSアカウントの所有者にお問い合わせください。

ベストプラクティス：課金レポートをアップロードするS3バケットを所有するアカウントと同じアカウントにプライマリIAMユーザを作成し、このユーザを使用してAWS課金データを設定および収集することを推奨します。

Insightによるデータ収集を許可するようにAWSアカウントを設定するには、次の手順を実行します。

手順

1. Identity Access Management（IAM）ユーザとしてAWSアカウントにログインします。適切に収集するには、グループIAMアカウントではなく、プライマリIAMアカウントにログインします。
2. Amazon S3 *に移動してバケットを作成します。一意のバケット名を入力し、リージョンが正しいことを確認します。
3. Amazon Cost and Usage Reportを有効にします。を参照してください https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports-gettingstarted-turnonreports.html を参照してください。
   a. AWS **Billing and Cost Management Dashboard** に移動し、* Reports *を選択します。
   b. をクリックし、**[**レポート名**]**にと入力します。**[**時間単位**]***で**[**毎日**]**を選択します。**[**リソース**ID]***を含めるチェックボックスをオンにし、[次へ]*をクリックします。
   c. [Select delivery options]ページの[Sample Policy]リンクをクリックします。ボックス内のサンプルポリシーテキストをクリップボードにコピーします。[* 閉じる *] をクリックします。
   d. 作成したS3バケットに戻り、**[Permissions]***タブをクリックして[Bucket Policy]*ボタンを選択します。
   e. サンプルポリシーのテキストを貼り付けて、を置き換えます `<bucketname>` 実際のバケット名を次

の行に入力します。 `"Resource": "arn:aws:s3:: <bucketname>"`。*ポリシーを保存*します。

f. [Create Report]画面に戻り、S3バケットにと入力して*[Verify]*ボタンをクリックします。「 * 次へ * 」をクリックします。

g. 情報を確認し、*[確認して完了]*をクリックします。

4. InsightでAWSからデータを収集するには、権限を付与する必要があります。次のリンクでは、「* List All Buckets *」（手順4.1）に権限を付与し、フォルダ内のオブジェクトに権限を設定する方法（手順5.2）について詳しく説明します。 https://docs.aws.amazon.com/AmazonS3/latest/dev/walkthrough1.html。
5. IAMコンソールで、**[Policies]***に移動し、[Create policy]*をクリックします。
6. フィールドに名前を入力し、下部にある[ポリシーの作成]*をクリックします。
7. IAMコンソールでユーザを選択し、画面下部の*[インラインポリシーの追加]*を選択します。
8. [Choose a service]*をクリックし、[S3]を選択します。
9. * JSON *タブに移動します。AWSウォークスルーの手順5.1.2.gのJSONサンプルテキストをJSONボックスにコピーします。
10. JSONの_companybucket_and_Development_fieldsをS3情報に置き換えます。
11. [ポリシーの確認]*をクリックして、ポリシー設定を確認します。

AWS Cloud Costデータソースを設定しています

AWS Cloud Costデータソースは、Insightのデータソースと同様に設定します。

作業を開始する前に

Amazon AWSアカウントのセットアップとInsightのデータ収集の準備が完了している必要があります。また、次の情報を入手しておく必要があります。

- レポート名（ Report Name ）
- S3バケット名
- S3バケットが配置されているAWSリージョン。
- レポートパスプレフィックス

このタスクについて

AWSアカウントの準備が整い、適切な権限が設定されたら、課金レポートデータを収集するようにOnCommand Insight を設定できます。

> 課金データの取得元となる課金対象のユーザ/アカウントごとに、個別のAWS Cloud Costデータソースを追加する必要があります。

手順

1. OnCommand Insight に管理者としてログインします。
2. **>**[Data sources]*をクリックして、[Insight Data Source]ページを開きます。
3. 新しいデータソースを追加するには、**+**追加*をクリックします。**Amazon** *を選択し、 AWS Cloud Cost *

を選択します。

4. [Configuration]*セクションで、*Report name*、*S3 Bucket_name*、*_S3 Region*（S3バケットが存在するリージョンを指定する必要があります）、*Report path prefix*、*AWS IAM Access Key ID*、および_AWS IAM Secret Access Key _を入力します。不明な点がある場合は、クラウドプロバイダまたはAWSアカウントの所有者に問い合わせてください。
5. このチェックボックスをオンにすると、InsightデータソースでAPI要求とデータ転送がAWSから課金されることを確認できます。
6. [Advanced Configuration]*で、HTTP接続とソケットタイムアウトを入力します。デフォルトは 300 秒です。
7. [保存（ Save ）] をクリックします。

AWSクラウドコストのデータを**Insight**で処理しています

Insightは、前月のAWS請求レポートから月に1回データを収集し、その月の最終的なクラウドコストを反映します。

AWS Cloud Costデータソースをセットアップしたあと、S3に対して請求レポートを生成済みの場合は、最初のデータソースポーリングの直後から最大3カ月分のデータが取得されます。

Insightでは、AWSの「最後の」データを月に1回収集します。この収集は前月の終わりから数日後に行われるため、AWSは実際のデータを最終的に処理することができます。

AWSの課金データはInsightのData Warehouseに送信され、レポート作成に使用されます。

各データソースは、1つの課金対象アカウント/ユーザに対して設定する必要があることに注意してください。

クラウドコストのデータを**Insight**でレポート

Insightで収集された月単位のクラウドコストデータはデータウェアハウスに送信され、Cloud Costデータマートでレポートに使用できます。

作業を開始する前に

AWSからクラウドコストデータを収集するようにデータソースを設定しておく必要があります。課金対象の各ユーザ/アカウントには、個別のデータソースが必要です。

Insightでデータの収集を開始するまでに少なくとも36時間かかります。

そのあとに少なくとも1回はETLを実行して、データをデータウェアハウスに送信します。

このタスクについて

データが収集されてData Warehouseに送信されたら、事前設定された任意のレポートでデータを表示したり、カスタムレポートを作成したりできます。Insightのクラウドコストデータマートにデータが保存されます。

事前設定されたレポートのいずれかでクラウドコストデータを表示するには、次の手順を実行します。

手順

1. 次のいずれかの方法でInsight Reportingを開きます。
   - [Reporting Portal]アイコンをクリックします InsightサーバのWeb UIまたはData Warehouse UIで使用します。
   - 次のURLを入力して、Reportingを直接起動します。 `https://<dwh_server_name\>:9300/p2pd/servlet/dispatch` または `https://<dwh_server_name\>:9300/bi` (7.3.3 and later)
2. Reportingにログインしたら、**[Public Folders]***をクリックし、[Cloud Cost]*を選択します。
3. AWS請求データは、* Cloud Cost フォルダにある利用可能なレポートで表示できます。また、 Packages フォルダにある Cloud Cost Datamart *を使用して独自のカスタムレポートを作成することもできます。

ServiceNowとの統合

OnCommand Insight はServiceNow管理ソフトウェアと統合されており、製品が個別に提供するよりも大きな価値を提供します。

Insightでは、Pythonスクリプトを使用してデータをServiceNowと統合し、次の情報を同期できます。

- ServiceNowサーバのストレージ資産データ
- ServiceNowサーバのホストおよびVMのURL
- ホスト/ VMとストレージの関係

Service Now統合の準備と前提条件

ServiceNow、Insight、およびPythonミドルウェアコネクタを統合する前に、必要な準備と前提条件を満たしている必要があります。

推奨されるワークフロー

ServiceNowとInsightを統合する際に強く推奨されるワークフローは次のとおりです。

1. 最初にPythonミドルウェアコネクタを開発インスタンスにデプロイします。
2. 開発インスタンスですべての障害が特定されて修正されたことを確認したら、テスト/ステージインスタンスにコネクタをデプロイします。
3. ステージングインスタンスで正しい動作を確認したら、本番インスタンスにコネクタをデプロイします。

これらのいずれかの段階で問題が見つかった場合は、ロールバック手順に従ってコネクタを無効にしてから、問題をトラブルシューティングして再導入してください。

一般的な前提条件：

- Pythonミドルウェアコネクタは、スタンドアロンホストまたはVM（推奨）、またはInsight Serverのホスト/ VMを使用してホストできます。
- 本番用Insight Serverをバックアップし、開発用インスタンスに導入することを強く推奨します。

- ServiceNowがCMDB内のサーバを正確に検出している必要があります。
- Insightでストレージ環境とコンピューティング環境を正確に検出する必要があります。
- ポート443および80をInsight ServerおよびServiceNowインスタンスに接続します。

ServiceNowの前提条件：

- 開発/テスト用のインスタンスを使用することを強く推奨します。
- ServiceNowアップデートセットをロードする権限。
- ユーザを作成する権限。
- ServiceNowバージョンジャカルタ以降

Insightの前提条件：

- 開発/テスト用のインスタンスを使用することを強く推奨します。
- ユーザを作成する権限（Admin権限）。
- Insightバージョン7.3.1以降がサポートされていますが、Insightを最大限に活用するために最新バージョンを使用してください。

Pythonミドルウェアコネクタの前提条件：

- Pythonバージョン3.6以降がインストールされています。
- Pythonをインストールするときは、チェックボックスをオンにしてすべてのユーザーを有効にします。これにより、標準的なアプリケーションのインストール場所にPythonが設定されます。
- Pythonをインストールするときは、このチェックボックスをオンにして、インストーラがパスを更新できるようにします。それ以外の場合は、パスを手動で更新する必要があります。
- Python * pysnow および requests *ライブラリをダウンロードします。

ServiceNow Pythonコネクタをダウンロードしています

ServiceNow統合用のPythonコネクタをダウンロードし、任意の場所に展開する必要があります。

手順

1. から* ServiceNow Integration Connector *をダウンロードします "NetApp Storefront"。
2. などのフォルダに.zipファイルを展開します `c:\OCI2SNOW`。

   統合コネクタスクリプトの名前はです `oci_snow_sync.pyz`。

統合のために**ServiceNow**を設定しています

ServiceNowとInsightを統合するには、いくつかのセットアップタスクが必要です。

このタスクについて

ServiceNowとInsightを統合する場合は、次のタスクを実行する必要があります。

ServiceNow側：

- ロールの昇格
- アップデートセットをインストールします
- ユーザを設定します

Insight側：

- ServiceNowユーザを追加します

Pythonコネクタ側：

- Pythonをインストールします
- 追加のライブラリをインストールします
- コネクタを初期化します
- config.iniファイルを編集します
- コネクタをテストします
- コネクタを同期化します
- 毎日のタスク実行のスケジュールを設定します

各項目については、以降のセクションで詳しく説明します。

ロールを昇格します

Insightと統合するには、ServiceNowのロールをsecurity_adminに昇格する必要があります。

手順

1. 管理者権限でServiceNowインスタンスにログインします。
2. ドロップダウンで[ロールの昇格]*を選択し、自分のロールをsecurity_adminに昇格します。[OK] をクリックします。

アップデートセットをインストールします

ServiceNowとOnCommand Insight の統合の一環として、データを抽出およびロードするための特定のフィールドとテーブルをコネクタに提供するために、事前設定されたデータをServiceNowにロードするアップデートセットをインストールする必要があります。

手順

1. 「取得したアップデートセット」を検索して、ServiceNowのリモートアップデートセットテーブルに移動

します。

2. [Import Update Set from XML]をクリックします。
3. アップデートセットは、以前にローカルドライブにダウンロードしたPythonコネクタ.zipファイル（この例では、）にあります `C:\OCI2SNOW` フォルダ）をクリックします `\update_sets` サブフォルダ。[Choose File]*をクリックし、このフォルダの.xmlファイルを選択します。[アップロード] をクリックします。
4. 更新セットがロードされたら、それを開き、*[更新セットのプレビュー]*をクリックします。

   エラーが検出された場合は、更新セットをコミットする前に修正する必要があります。

5. エラーがない場合は、*[Commit Update Set]*をクリックします。

   アップデート・セットがコミットされると、* System Update Sets **>** Update Sources *ページに表示されます。

ServiceNow統合**-**ユーザを設定します

Insightに接続してデータを同期するには、ServiceNowユーザを設定する必要があります。

このタスクについて

手順

1. ServiceNowでサービスアカウントを作成します。ServiceNowにログインし、* system security **>** users and groups **>** users *に移動します。[New]*をクリックします。
2. ユーザ名を入力します。この例では、統合ユーザとして「OCI2SNOW」を使用します。このユーザのパスワードを入力します。

   > この方法では、ドキュメント全体で「OCI2SNOW」という名前のサービスアカウントユーザを使用します。別のサービスアカウントを使用することもできますが、環境全体で一貫したアカウントであることを確認してください。

3. メニューバーを右クリックし、*[保存]*をクリックします。これにより、ロールを追加するためにこのユーザにとどまることができます。
4. [編集]*をクリックし、このユーザに次のロールを追加します。
   - 資産
   - import_transformer
   - REST_SERVICE
5. [保存（ Save ）] をクリックします。
6. 同じユーザをOnCommand Insight に追加する必要があります。Administrator権限を持つユーザとしてInsightにログインします。
7. * Admin **>** Setup に移動し、 Users *タブをクリックします。
8. ボタンをクリックし、[ユーザーの追加]*を選択します。
9. nameに「OCI2SNOW」と入力します。上記で別のユーザ名を使用した場合は、その名前をここに入力し

ます。上記のServiceNowユーザと同じパスワードを入力します。Eメールフィールドは空白のままにしてもかまいません。

10. このユーザに* User *ロールを割り当てます。[保存（ Save ）] をクリックします。

Pythonとライブラリをインストールします

Pythonは、Insight Serverにインストールすることも、スタンドアロンのホストやVMにインストールすることもできます。

手順

1. VMまたはホストに、Python 3.6以降をダウンロードします。
2. カスタムインストールを選択し、次のオプションを選択します。これらは、コネクタスクリプトを適切に操作するために必要なものであるか、または強くお勧めします。
   - すべてのユーザーのランチャーをインストールします
   - パスにPythonを追加します
   - install pip (Pythonが他のパッケージをインストールできるようにする)
   - TK/Tclとアイドルを取り付けます
   - Pythonテストスイートをインストールします
   - すべてのユーザーにPYランチャーをインストールします
   - ファイルをPythonに関連付けます
   - インストールされているアプリケーションのショートカットを作成します
   - 環境変数にPythonを追加します
   - 標準ライブラリを事前コンパイルします
3. Pythonがインストールされたら、Pythonライブラリ「`re quests`」と「`psnow`」をインストールします。次のコマンドを実行します。 `python -m pip install requests pysnow`

   *注：*このコマンドは、プロキシ環境で動作している場合に失敗することがあります。この問題 を回避するには、各Pythonライブラリを手動でダウンロードし、インストール要求を1つずつ正しい順序で実行する必要があります。

   コマンドはいくつかのファイルをインストールします。

4. Pythonライブラリが正しくインストールされていることを確認します。次のいずれかの方法でPythonを起動します。
   - cmdプロンプトを開き、と入力します `python`
   - Windowsの場合は、**[**スタート**]***を開き、[Python]**>**[Python-python.exe]<version> *を選択します
5. Pythonプロンプトで、と入力します `modules`

   Pythonは、モジュールのリストを収集している間、しばらく待つように要求し、それが表示されます。

Pythonミドルウェアをセットアップします

Pythonと必要なライブラリがインストールされたので、OnCommand InsightとServiceNowと通信するようにミドルウェアコネクタを設定できます。

手順

1. コネクタソフトウェアをダウンロードしたホストまたはVMで、管理者としてcmdウィンドウを開き、に変更します `\OCI2SNOW\` フォルダ。
2. 空の* config.ini*ファイルを生成するには、スクリプトを初期化する必要があります。次のコマンドを実行します。 `oci_snow_sync.pyz init`
3. テキストエディタで**config.ini**fileを開き、[OCI]セクションで次の変更を行います。
   - 「* url *」をに設定します <code><a href="https://<name.domain>" class="bare">https://<name.domain>;</code> または <code><a href="https://<ip" class="bare">https://<ip address></code> （Insightインスタンス）。
   - 作成したInsightユーザ（OCI2SNOWなど）に、* user と password *を設定します。
   - include_off_vms を false *に設定します
4. [SNOW]セクションで、次の変更を行います。
   - Instance *をServiceNowインスタンスのFQDNまたはIPアドレスに設定します
   - *User*および*Password*をServiceNowサービスアカウントユーザ（OCI2SNOWなど）に設定します。
   - OCI URL の*フィールドで、 URL *フィールドを「`u_oci_url`」に設定します。このフィールドは、コネクタOCIの更新セットの一部として作成されます。これはお客様の環境で変更できますが、変更する場合は、こことServiceNowで変更する必要があります。このフィールドはそのままにしておくことを推奨します。
   - *filter_status*フィールドを"`installed, in Stock`に設定します。ステータスが異なる場合は、新しいレコードをアップロードする前に、すべてのレコードをInsightレコードと一致させるために、ここでステータスを設定する必要があります。ほとんどの場合、このフィールドは変更されません。
   - **stale_status**を"`Retired"に設定します。
5. [プロキシ]セクションは、プロキシサーバーを使用する場合にのみ必要です。このセクションを使用する必要がある場合は、次の設定を確認してください。
   - ；https = http://<host>:<port>
   - ；http= http://<host>:<port>
   - ；include_oci = True
   - ；INCLUDE_SNOW = True
6. [Log]セクションは、より詳細なデバッグ情報が必要な場合にのみ編集してください。
7. コネクタをテストするには、管理者としてcmdプロンプトを開き、\OCI2SNOWフォルダに移動します。次のコマンドを実行します。 `oci_snow_sync.pyz test`

   詳細については、を参照してください `logs\` フォルダ。

コネクタを同期しています

ServiceNow、Insight、およびコネクタを適切に設定したら、コネクタを同期できます。

手順

1. cmdプロンプトを開き、\OCI2SNOWフォルダに移動します。
2. 次のコマンドを2回実行します。1回目の同期で項目が更新され、2回目の同期で関係が更新されます。
   `oci_snow_sync.pyz sync`
3. ServiceNowインスタンスのStorage Serverテーブルに値が入力されていることを確認します。ストレージサーバを開き、そのストレージに関連するリソースが表示されていることを確認します。

同期を毎日実行するようスケジュール設定しています

Windowsタスクスケジューラを使用して、ServiceNowコネクタを自動的に同期できます。

このタスクについて

自動同期により、Insightのデータが定期的にServiceNowに移動されます。スケジューリングには任意の方法を使用できます。次の手順では、Windowsタスクスケジューラを使用して自動同期を実行します。

手順

1. Windowsの画面で、**[**スタート**]***をクリックし、[実行]**>**[タスクスケジューラ]*と入力します。
2. [基本タスクの作成…]*をクリックします
3. 「OCI2SNOW Connector Sync」のようなわかりやすい名前を入力します。タスクの概要 を入力します。「 * 次へ * 」をクリックします。
4. タスク*毎日*を実行する場合に選択します。「 * 次へ * 」をクリックします。
5. タスクを実行する時刻を選択します。「 * 次へ * 」をクリックします。
6. アクションで、*プログラムの開始*を選択します。「 * 次へ * 」をクリックします。
7. [プログラム/スクリプト*]フィールドにと入力します `C:\OCI2SNOW\oci_snow_sync_pyz`。[*Arguments*]フィールドにと入力します `sync`。[開始場所（Start in *）]フィールドにと入力します `C:\OCI2SNOW`。[次へ]*をクリックします。
8. 概要の詳細を確認し、*[完了]*をクリックします。

   これで、同期が毎日実行されるようにスケジュールされました。

法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

http://www.netapp.com/us/legal/copyright.aspx

商標

NetApp 、 NetApp のロゴ、および NetApp の商標ページに記載されているマークは、 NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

http://www.netapp.com/us/legal/netapptmlist.aspx

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

https://www.netapp.com/us/media/patents-page.pdf

プライバシーポリシー

https://www.netapp.com/us/legal/privacypolicy/index.aspx

注意

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

"OnCommand Insight 7.3.15に関する注意事項"

"OnCommand Insight 7.3.14に関する注意事項"

"OnCommand Insight 7.3.13に関する注意事項"