



# Insightデータソース管理

## OnCommand Insight

NetApp  
October 24, 2024

# 目次

Insightデータソース管理 .....	1
Insightでデータソースを設定します .....	1
ベンダー別のデータソースリファレンス .....	5
データソースのクレデンシャルの変更 .....	100
データ収集の問題を引き起こす変更 .....	101
1つのデータソースの詳細を確認します .....	102
データソースの問題を調査しています .....	103
データソースのポーリングの制御 .....	103
データソース情報の編集 .....	104
複数のデータソースの情報を編集する .....	104
データソースタグをアノテーションにマッピングする .....	105
データソースの削除 .....	105
データソースパッチとは .....	106

# Insightデータソース管理

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

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

個々のデータソースを確認するだけでなく、次の処理も実行できます。

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

## Insightでデータソースを設定します

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

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

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

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

### データソースのサポート情報

設定計画の一環として、環境内のデバイスをInsightで監視できることを確認する必要があります。そのためには、データソースサポートマトリックスでオペレーティングシス

テム、特定のデバイス、プロトコルの詳細を確認できます。一部のデータソースは、オペレーティングシステムによっては使用できない場合があります。

データソースサポートマトリックスの最新バージョンの場所

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

データソースを追加しています

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

手順

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

データソースの追加ウィザードが開きます。

4. [設定]セクションで、次の情報を入力します。

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

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

## スプレッドシートからデータソースをインポートする

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

### このタスクについて

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

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

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

### 手順

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

収集結果が収集ログに記録されます。

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

次のいずれかを選択します。

- いいえ：OnCommand Insight マシンで実行する必要があるパ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パ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

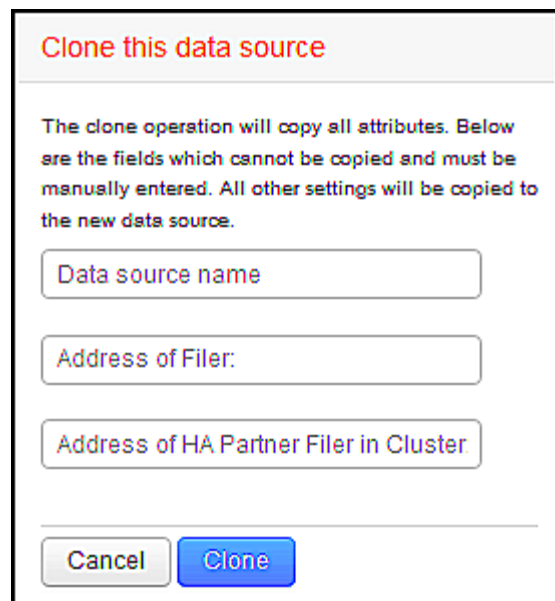
1. Insightのツールバーで、\*[Admin]\*をクリックします。

[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（wJalrXUtl/K7MDENG/bPxrFiCYEXAMPLEKEY など）で構成されます。Amazon 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AWSOrganizationsReadOnlyAccesspolicy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せん。

## 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witch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witch 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	<p>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。</p> <ul style="list-style-type: none"> <li>• デバイスエイリアス</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>• * なし *</li> </ul> <p>エイリアスは報告しないでください</p> <ul style="list-style-type: none"> <li>• *ポート概要*</li> </ul> <p>ポートのリストでポートを識別するための概要</p> <ul style="list-style-type: none"> <li>• ゾーンエイリアス（すべて）</li> </ul> <p>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</p> <ul style="list-style-type: none"> <li>• ゾーンエイリアス（アクティブのみ）</li> </ul> <p>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。</p>

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（naviseccli）
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 storsrzd
- 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	<p>接続のキャッシュ方法を選択：</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul> <div>  <p>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。</p> </div>
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ー名

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接続を開始する必要があります。データソースで使用する読み取り専用ユーザが少なくとも1人必要です。

### 用語集

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

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
ストレージアレイ	ストレージ
プロセッサ	ストレージノード
ストレージプール	ストレージプール
一般的な iSCSI ブロック情報、VMware VMFS	ボリューム
共有フォルダ	内部ボリューム

VMware NFSデータストアからのCIFS共有、NFS共有、共有	共有
Replication Remote System の略	同期
iSCSI ノード	iSCSI ターゲットノード
iSCSI イニシエータ	iSCSI ターゲットイニシエータ



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

## 要件

このデータソースを設定して使用するための要件は次のとおりです。

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

## 設定

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

## 高度な設定

フィールド	説明
-------	----

インベントリポーリング間隔（分）	インベントリのポーリング間隔（デフォルトは 40 分）
VNXe CLIポート	VNXe CLI に使用するポート
インベントリ外部プロセスタイムアウト（秒）	外部プロセスのタイムアウト（デフォルトは1、800 秒）

## EMC VPLEXデータソース

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

### 用語集

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

ベンダー / モデルの用語	Insightの用語
クラスタ	ストレージ
エンジン	ストレージノード
デバイス、システム拡張	バックエンドストレージプール
仮想ボリューム	ボリューム
フロントエンドポート、バックエンドポート	ポート
分散デバイス	ストレージ同期
ストレージビュー	ボリュームマップ、ボリュームマスク
ストレージボリューム	バックエンド LUN
ITL	バックエンドパス



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

## 要件

- VPLEXサーバのIPアドレス
- VPLEX サーバの管理者レベルのドメインアカウント
- ポート 443 （HTTPS）：VPLEX 管理ステーションの TCP ポート 443 へのアウトバウンド接続が必要です。
- パフォーマンスを確保するには、ssh/scp アクセス用の読み取り専用のユーザ名とパスワードを使用します。
- パフォーマンスを確保するには、ポート 22 が必要です。
- アクセスの検証：を使用して検証します telnet ポート443に接続します。デフォルトポート以外のポートの場合は、任意のブラウザでを使用します

## 設定

フィールド	説明
VPLEX Management Console の IP アドレス	VPLEX Management Console の IP アドレスまたは完全修飾ドメイン名
ユーザ名	VPLEX CLI のユーザ名
パスワード	VPLEX CLI のパスワード
VPLEX Management ConsoleのパフォーマンスリモートIPアドレス	VPLEX Management Console のパフォーマンスリモートの IP アドレス
パフォーマンスリモートユーザ名	VPLEX Management Console のパフォーマンスリモートのユーザ名
パフォーマンスリモートパスワード	VPLEX Management Console のパフォーマンスリモートのパスワード

## 高度な設定

フィールド	説明
通信ポート	VPLEX CLIに使用するポート
インベントリポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは20分）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）
再試行回数	インベントリの再試行回数



パフォーマンスポーリング間隔（秒）	パフォーマンスポーリング間隔（デフォルトは600秒）
パフォーマンスSSHプロセス待機タイムアウト（秒）	SSHプロセスのタイムアウト（デフォルトは600秒）
SSHバナー待機タイムアウト（秒）	SSHバナーのタイムアウト（デフォルトは20秒）
再試行回数	パフォーマンスの再試行回数

## EMC XtremIOデータソース

EMC XtremIO（HTTP）データソースを構成するには、XtremIO Management Server（XMS）ホストアドレスと管理者権限を持つアカウントが必要です。

### 用語集

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

ベンダー / モデルの用語	Insightの用語
ディスク（SSD）	ディスク
クラスタ	ストレージ
コントローラ	ストレージノード
ボリューム	ボリューム
LUN マップ	ボリュームマップ
イニシエータ、ターゲット	ボリュームマスク



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

### 要件

- 各XtremIO Management ServerのIPアドレス
- 管理者権限を持つアカウント
- ポート 443 へのアクセス（HTTPS）

## 設定

フィールド	説明
XMS ホスト	XtremIO Management Server の IP アドレスまたは完全修飾ドメイン名
ユーザ名	XtremIO Management Server のユーザ名
パスワード	XtremIO Management Server のパスワード

## 高度な設定

フィールド	説明
TCP ポート	XtremIO Management Serverへの接続に使用するTCPポート（デフォルトは443）
インベントリのポーリング間隔（分）	インベントリポーリングの間隔（デフォルトは60分）
接続タイムアウト（秒）	接続タイムアウト（デフォルトは60秒）
パフォーマンスのポーリング間隔（秒）	パフォーマンスのポーリング間隔（デフォルトは 300 秒）

## Fujitsu Eternusデータソース

Fujitsu Eternusデータソースには、ストレージのIPアドレスが必要です。カンマで区切ることはできません。

## 用語集

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

ベンダー / モデルの用語	Insightの用語
ディスク	ディスク
ストレージ	ストレージ
シンプール、フレキシブル階層プール、RAID グループ	ストレージプール

標準ボリューム、Snap Data Volume (SDV) 、 Snap Data Poolボリューム (SDPV) シンプロビジョニングボリューム (TPV)	ボリューム
---	-------



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

## 要件

- Eternus ストレージの IP アドレス。カンマで区切って指定することはできません
- SSH 管理レベルのユーザ名とパスワード
- ポート 22
- ページスクロールが無効になっていることを確認します。(clientv-show-more-scroll disable)

## 設定

フィールド	説明
Eternus ストレージの IP アドレス	Eternus ストレージの IP アドレス
ユーザ名	Eternus ストレージのユーザ名
パスワード	胸骨に使用するパスワード

## 高度な設定

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

## Hitachi Content Platform (HCP) データソース

このデータコレクタは、HCP 管理 API を使用して、Hitachi Content Platform (HCP) をサポートします。

## 用語集

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

ベンダー / モデルの用語	Insightの用語
HCP クラスタです	ストレージ
テナント	ストレージプール
ネームスペース	内部ボリューム
ノード	ノード



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

## インベントリの要件

- HCP サーバの IP アドレス
- HCP ソフトウェアおよびピア権限の読み取り専用のユーザ名およびパスワード

## 設定

* フィールド *	* 概要 *
HCP ホスト	HCP ホストの IP アドレスまたは完全修飾ドメイン名
HCP ポート	デフォルトは 9090 です
HCP ユーザー ID	HCP ホストのユーザ名
HCP パスワード	HCP ホストのパスワード
HCP 認証タイプ	HCP_LOCAL または active_directory を選択してください

## 高度な設定

フィールド	説明
インベントリポーリング間隔 (分)	インベントリポーリングの間隔 (デフォルトは60分)
パフォーマンスポーリング間隔 (秒)	パフォーマンスのポーリング間隔 (デフォルトは900秒)

## HDS HiCommand Device Managerデータソース

HDS HiCommandおよびHiCommand Liteデータソースでは、HiCommand Device Managerサーバがサポートされます。OnCommand Insight は、標準のHiCommand APIを使用してHiCommandデバイスマネージャサーバと通信します。

### 用語集

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

ベンダー / モデルの用語	Insightの用語
PDEV	ディスク
ジャーナルプール	ディスクグループ
ストレージアレイ	ストレージ
Port Controller の略	ストレージノード
アレイグループ 'DP プール	ストレージプール
論理ユニット、 LDEV	ボリューム



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

### インベントリの要件

- HiCommand Device Manager サーバの IP アドレス
- HiCommand Device Manager ソフトウェアおよびピアの権限に対する読み取り専用のユーザ名とパスワード
- ポート要件： 2001 （ http ） または 2443 （ https ）
- アクセスの検証：
  - ピアのユーザ名とパスワードを使用してHiCommand Device Managerソフトウェアにログインします。
  - HiCommand Device Manager APIへのアクセスを確認します。 telnet <HiCommand Device\_Manager\_server\_ip> 2001

### パフォーマンス要件

- HDS USP 、 USP V 、 および VSP のパフォーマンス

- Performance Monitor のライセンスが必要です。
- 監視スイッチが有効になっている必要があります。
- エクスポートツール (Export.exe) を OnCommand Insight サーバにコピーする必要があります。
- エクスポートツールのバージョンとターゲットアレイのマイクロコードのバージョンが一致している必要があります。

• HDS AMSのパフォーマンス

- Performance Monitorのライセンスが必要です。
- Storage Navigator Modular 2 (SNM2) CLIユーティリティがOnCommand Insight サーバにインストールされている必要があります。
- 次のコマンドを使用して、OnCommand Insight でパフォーマンスを取得する必要があるAMS、WMS、SMSのすべてのストレージアレイを登録する必要があります。
- 登録したすべてのアレイがこのコマンドの出力に表示されていることを確認する必要があります。  
auunitref.exe。

## 設定

* フィールド *	* 概要 *
HiCommand サーバ	HiCommand Device Manager サーバの IP アドレスまたは完全修飾ドメイン名
ユーザ名	HiCommand Device Manager サーバのユーザ名
パスワード	HiCommand Device Manager サーバのパスワード
デバイス - VSP G1000 (R800)、VSP (R700)、HUS VM (HM700)、および USP ストレージ	<p>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。</p> <ul style="list-style-type: none"> <li>• Array's IP：ストレージのIPアドレス</li> <li>• User Name：ストレージのユーザ名</li> <li>• Password：ストレージのパスワード</li> <li>• 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</li> </ul>

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。 <ul style="list-style-type: none"> <li>• Array's IP：ストレージのIPアドレス</li> <li>• Storage Navigator CLI Path：SNM2 CLIパス</li> <li>• 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</li> <li>• User Name：ストレージのユーザ名</li> <li>• Password：ストレージのパスワード</li> </ul>
「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 を有効にする場合を選択します
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を選択します

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。
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	<p>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。</p> <ul style="list-style-type: none"> <li>• Array's IP：ストレージのIPアドレス</li> <li>• User Name：ストレージのユーザ名</li> <li>• Password：ストレージのパスワード</li> <li>• 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</li> </ul>
SNM2Devices - WMS/SMS/AMS ストレージ	<p>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。</p> <ul style="list-style-type: none"> <li>• Array's IP：ストレージのIPアドレス</li> <li>• Storage Navigator CLI Path：SNM2 CLIパス</li> <li>• 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</li> <li>• User Name：ストレージのユーザ名</li> <li>• Password：ストレージのパスワード</li> </ul>
「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 サーバにインストールするか、Remote Acquisition UnitをCommand View EVAサーバ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 <code>sssu.exe</code> 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、 <code>sssu.exe</code> 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 <code>sssu.exe</code>
コマンドタイムアウト（秒）	<code>evaperf</code> 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
エクステンションプール	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 情報を収集する必要があります。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 FASiT 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する 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 などのクラスター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：効率化テクノロジーを使用して、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 のバス、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ー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：効率化テクノロジーを使用して、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

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ます、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おり、リモートで利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ます、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接続を開始する必要があります。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。	<p>特定のロール（「advanced_analytics」など）が設定されているユーザ&lt;userName&gt; に含まれていない可能性があります。考えられる解決策：</p> <ul style="list-style-type: none"> <li>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</li> <li>[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。</li> <li>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。</li> <li>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。</li> </ul>
---	---

## 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IP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。

* フィールド *
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。

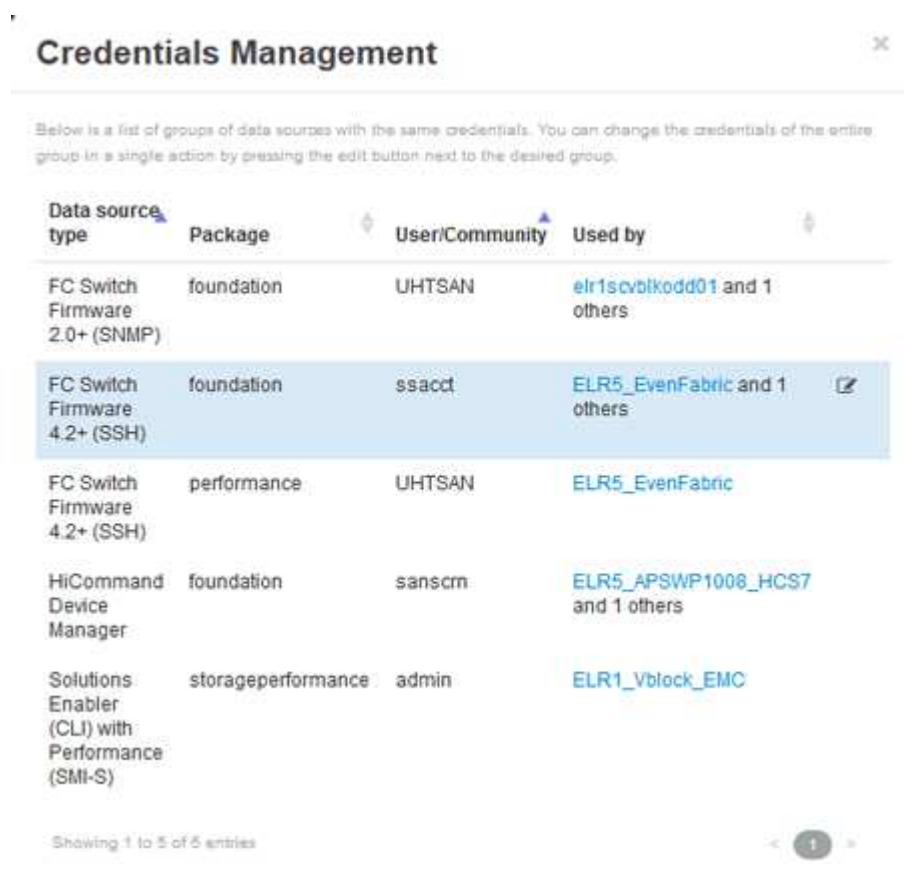
### 手順

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ます

### 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。

**Patches**  
**Brocade SSH**

**Summary**

Recommendation: ✔ Approve patch - Patch results are positive (no change or more successes)

Applied on: 5/12/2013 20:00:01

Other data source affected: Brocade SNMP, Brocade HTTP

Comments: ✔ Got this patch from Scott. He said that this should fix the SNMP v3 problem in Brocade. Talking to John from NetApp, they promised this will fix the SNMP v3 problem. After this is applied, we still need to check the other SNMP v3 data sources and see if they are good.

You should now review the results of the patch. Approving a patch will permanently apply this patch to the system. Rolling back a patch will delete it and restore the previous version before this patch was applied. Please note that there can only be one patch active for a data source type.

Buttons: Approve, Roll back, Replace patch

**Affected data sources**

Name	Alt	Type	Conclusion	Status before patch applied	Most recent status
ds0		local	Brocade CLI	All successful	Currently polling...
ds1		local	Brocade CLI	No change (success)	All successful
ds2		local	Brocade CLI	Rolling back now successful	All successful
ds3		local	Brocade CLI	Configuration is still failing (a different error)	Configuration failed
ds4		au1	Brocade SNMP	Configuration is successful but now Performance is failing	Configuration failed

Showing 1 to 5 of 5 entries

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。

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。