Data Infrastructure Insightsドキュメント

Data Infrastructure Insights

NetApp
September 26, 2024

目次

Data Infrastructure Insightsドキュメント

NetApp Data Infrastructure Insights（旧称Cloud Insights）は、インフラ全体を可視化できるクラウドインフラ監視ツールです。Data Infrastructure Insightsを使用すると、パブリッククラウドやプライベートデータセンターを含む、すべてのリソースの監視、トラブルシューティング、最適化を実行できます。

Data Infrastructure Insightsでできること

Data Infrastructure Insightsは、ハイブリッドマルチクラウドを監視し、インフラとワークロードのフルスタックのオブザーバビリティを提供します。

- Kubernetesを含む、異機種混在インフラとワークロード向けのデータコレクタ
- オープンなTelegrafコレクターとオープンAPIにより、統合が容易になります
- 包括的なアラートと通知
- インテリジェントなインサイトを得るための機械学習
- リソース利用率を最適化
- 高度なフィルタを備えた組み込みまたはカスタマイズ可能なダッシュボードにより、回答 の質問に対する表示ノイズを最小限に抑えることができます
- ONTAP ストレージの運用状態を検出できます
- 最も重要なビジネス資産であるランサムウェア攻撃やデータ破壊攻撃からデータを保護

はじめに

- "開始する"Data Infrastructure Insightsの使用方法
- サインアップしています。では、どうすればよいですか？
  "データの取得"
  "ユーザを設定する"
- 更新が次の手順
  "アセットの準備：アノテーション"
  "目的のアセットの検索：クエリ"
  "必要なデータの表示：ダッシュボード"
  "監視とアラート"
  "データを保護する"
- これはすばらしい原料である! 準備ができました "* 予約購読 *"。

Data Infrastructure Insightsの最新情報

ネットアップは、製品やサービスの改善と強化を継続的に行っています。Data Infrastructure Insights（旧称Cloud Insights）で利用できる最新の機能をいくつか紹介します。

2024年9月

Data Infrastructure Insights（旧称Cloud Insights）の概要

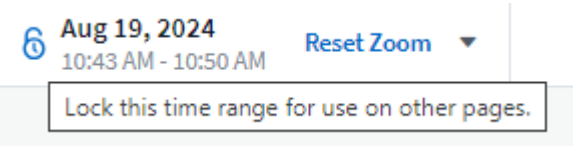
2024年9月24日（火）、NetAppは正式にCloud Insightsの名称を* Data Infrastructure Insights *（DII）に変更しました。これは、Haiyan SongがInsightユーザカンファレンスでメインステージの基調講演とInsightカンファレンスの製品プレスリリースで発表したものです。

DIIサービスは変わりません。機能の変更や変更はありません。これは、サービス名をすべてのITインフラストラクチャの機能に合わせて調整するための名称変更です。

2024年8月

時間範囲に固有のデータを表示

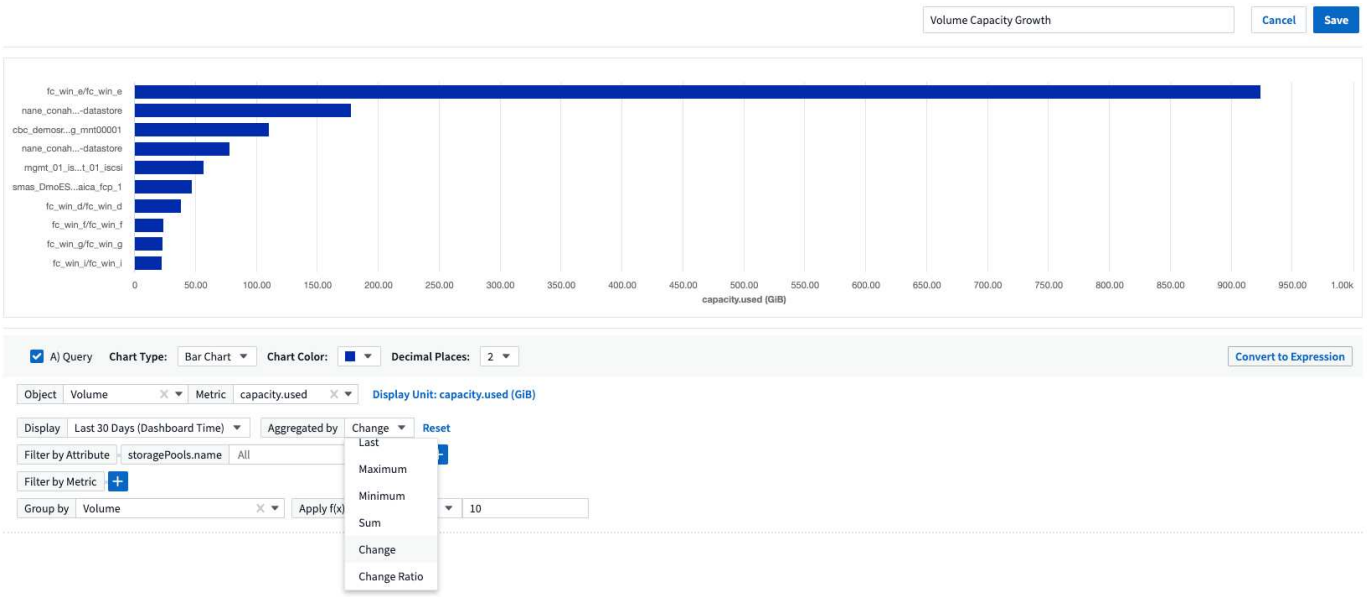
アラートを調査していますか？グラフにズームインしますか？これらの操作により、ページの時間範囲が変更されます。これで、その時間範囲をロックしたり、他のCloud Insightsページに移動したり、ロックされた時間範囲に固有のデータを確認したりできます。調査とトラブルシューティングがはるかに簡単になりました。



変更率（%）解析

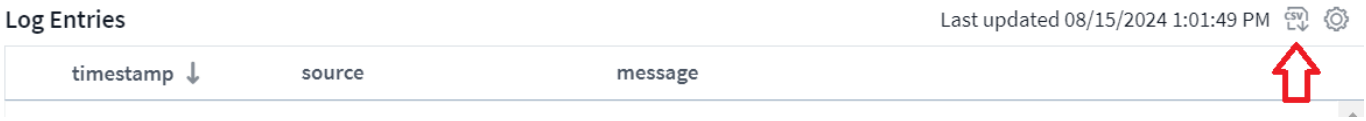
変更比率の時間集約は、時間の経過に伴うメトリック値の重要な変化と傾向を特定するのに役立ちます。これらの分析情報は、特定の時間における容量の大幅な増加や、単一ポートのパフォーマンスの変化など、何が変わったかを理解するための鍵となります。

- 変更-選択した期間内の2つのポイント間のメトリックの変化を確認します。
- 比率の変更-選択した期間内の2つのポイント間の比例的な変化を、最初のポイントを基準にして観察します。



ログクエリ結果を.csvにエクスポート

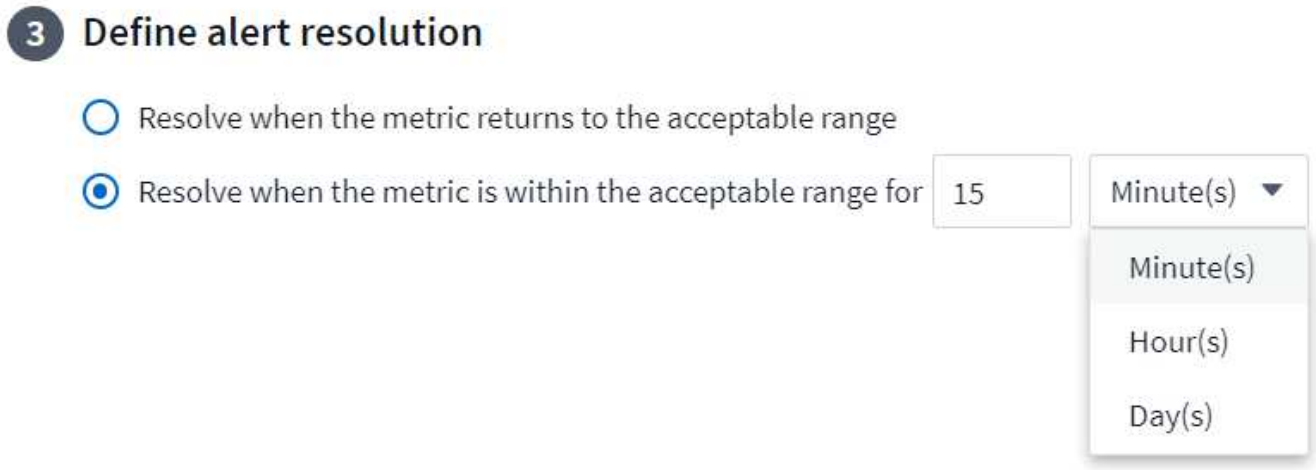
ログクエリの結果を表示する場合は、新しい[エクスポート]ボタンをクリックして、最大10,000行を.csvに簡単にエクスポートできます。これにより、データへのアクセス性が向上し、データ分析とレポート作成が容易になり、他のData Processingツールとのシームレスな統合が容易になります。



ページの[Export to CSV]ボタン"]

時間によるアラートの解決

Cloud Insightsでは、監視対象の指標が指定した期間にわたって許容範囲内に収まった場合にアラートを解決するオプションが提供されるようになりました。これにより、複数のアラートを1つに統合することで、定義されたしきい値を繰り返し超えてメトリックに関連するノイズを低減し、真の問題に集中することができます。



2024年7月

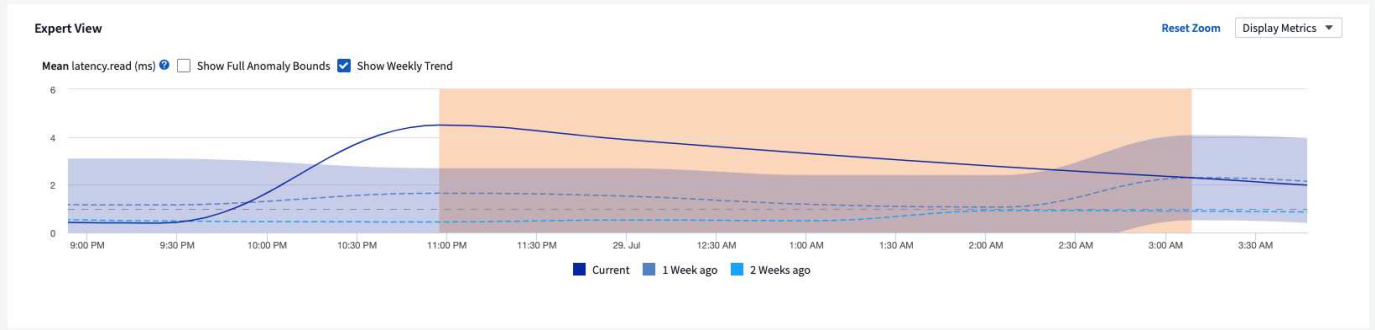
AIOps：異常検出

Cloud Insightsは、機械学習を使用して、環境内のデータパターンの予期しない変化を検出し、プロアクティブなアラートを提供して問題を早期に特定できるようにします。

データセンターの動作は、1日の時間帯や曜日によって異なります。Cloud Insightsでは、毎週の季節性を使用して、各日と時間の履歴動作を比較します。

異常検出監視では、「正常」の定義が不明な場合、時間の経過とともに動作が変化する場合、またはしきい値を手動で定義することが現実的ではない大量のデータを処理する場合などの状況に対してアラートを提供できます。

選択したオブジェクト指標でこのような異常が発生した場合に新しいアラートが生成され "異常検出モニタ" ます。



ワークロードセキュリティの強化

- NFS 4.1のサポート*

SVM Data Collectorで、ONTAP 9.151以降の* NFS 4.1 *までのNFSバージョンがサポートされるようになりました。

*新しいフォレンジックアクティビティAPI *

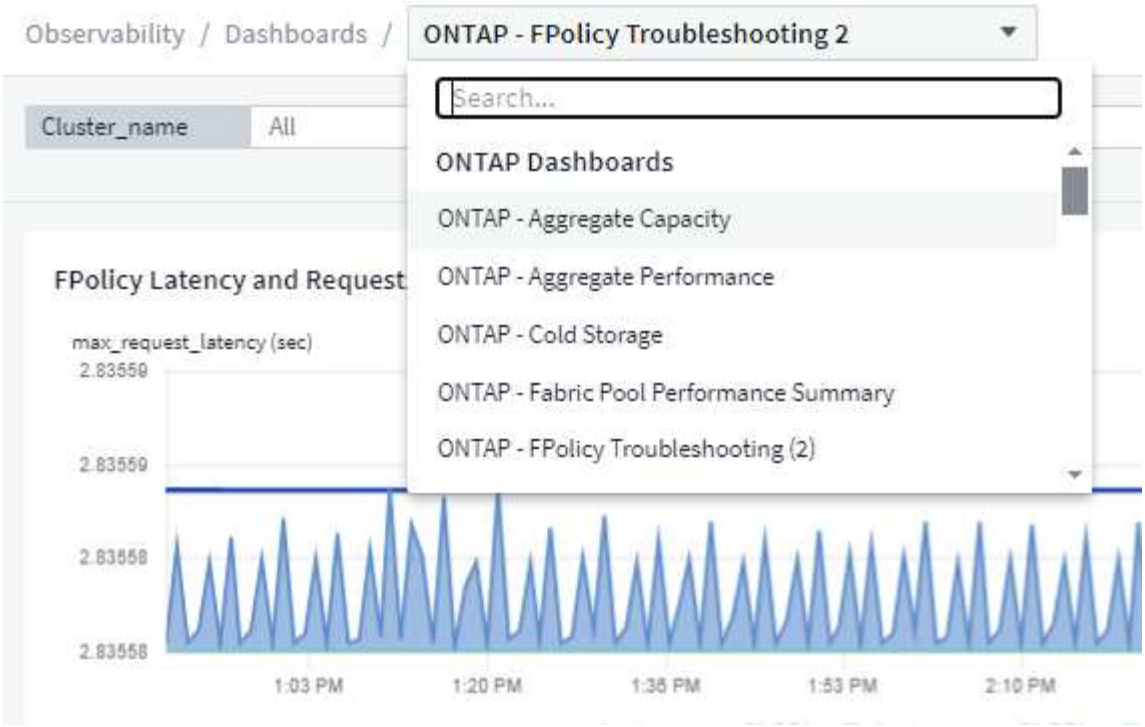
フォレンジックアクティビティ "API" に新しいバージョンが追加されました。Forensics ActivityのAPIを呼び出す場合は、* cloudsecure_forensics.activities.*v2** APIを使用します。

このAPIに複数の呼び出しを行う場合、最良の結果を得るためには、呼び出しが並列ではなく順番に実行されるようにしてください。複数の並行呼び出しが発生すると、APIがタイムアウトする可能性があります。

ダッシュボードナビゲーションの簡易化

この機能の目的は、運用ワークフローを合理化し、チーム間のコラボレーションを容易にすることです。

ダッシュボードをグループ化すると、必要な可視性をすばやく簡単に取得できます。新しいナビゲーションメニューを使用すると、場所を失うことなく異なるダッシュボード間を移動できるため、インフラの探索や管理が簡単になります。ダッシュボードグループを運用ランブックに合わせて調整し、エクスペリエンスをさらに向上させます。



2024年6月

オペレーティングシステムのサポート

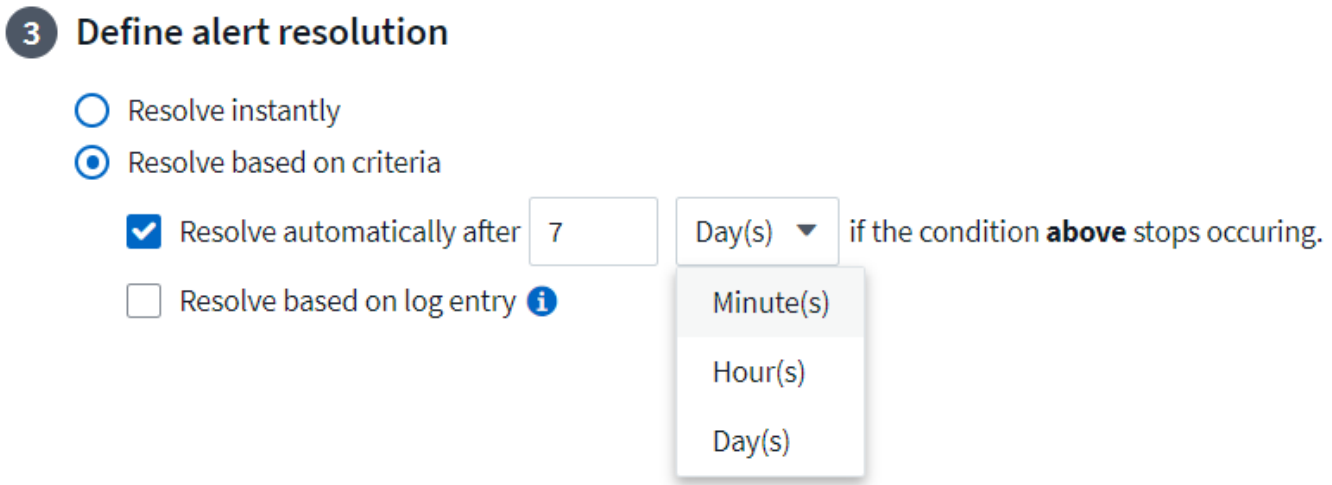
Cloud Insights Acquisition Unitでサポートされるオペレーティングシステムは次のとおりです "すでにサポートされています"：

- Red Hat Enterprise Linux 8.9、8.10、9.4
- ロッキー9.4
- AlmaLinux 9.3および9.4

2024年5月

時間に基づいてアラートを自動的に解決

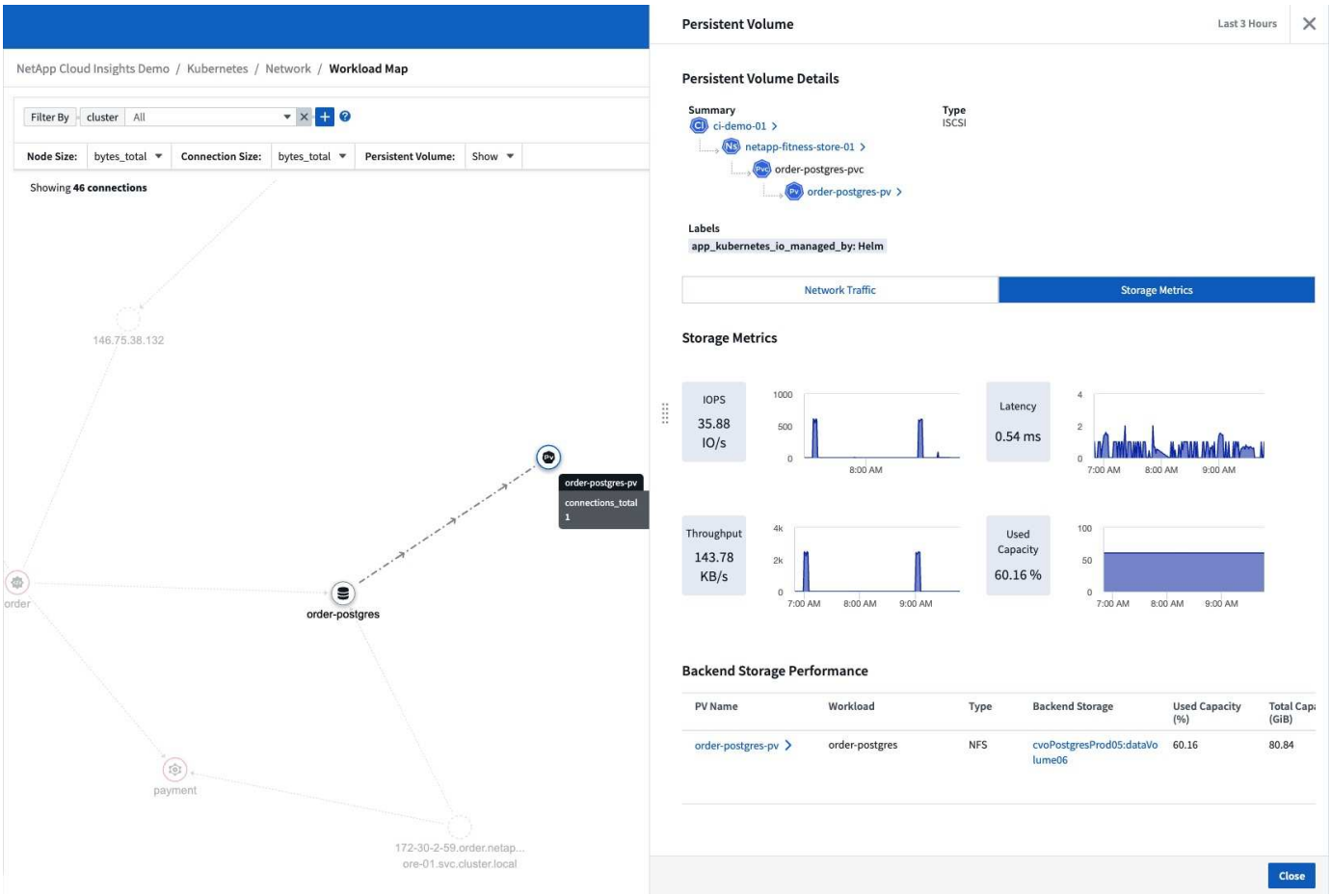
ログアラートを時間に基づいて解決できるようになりました。アラート条件の発生が停止した場合は、指定した時間が経過するとCloud Insightsで自動的にアラートを解決できます。アラートは、分、時間、日単位で解決できます。



2024年4月

Kubernetes向けのiSCSIサポート

Cloud Insightsでは、Kubernetesに関連付けられたiSCSIストレージのマッピングがサポートされるようになりました。これにより、Kubernetesのネットワークマップを使用した迅速なトラブルシューティングと、Reportingを使用したチャージバックレポートやショーバックレポートの提供が可能になりました。



オペレーティングシステムのサポート

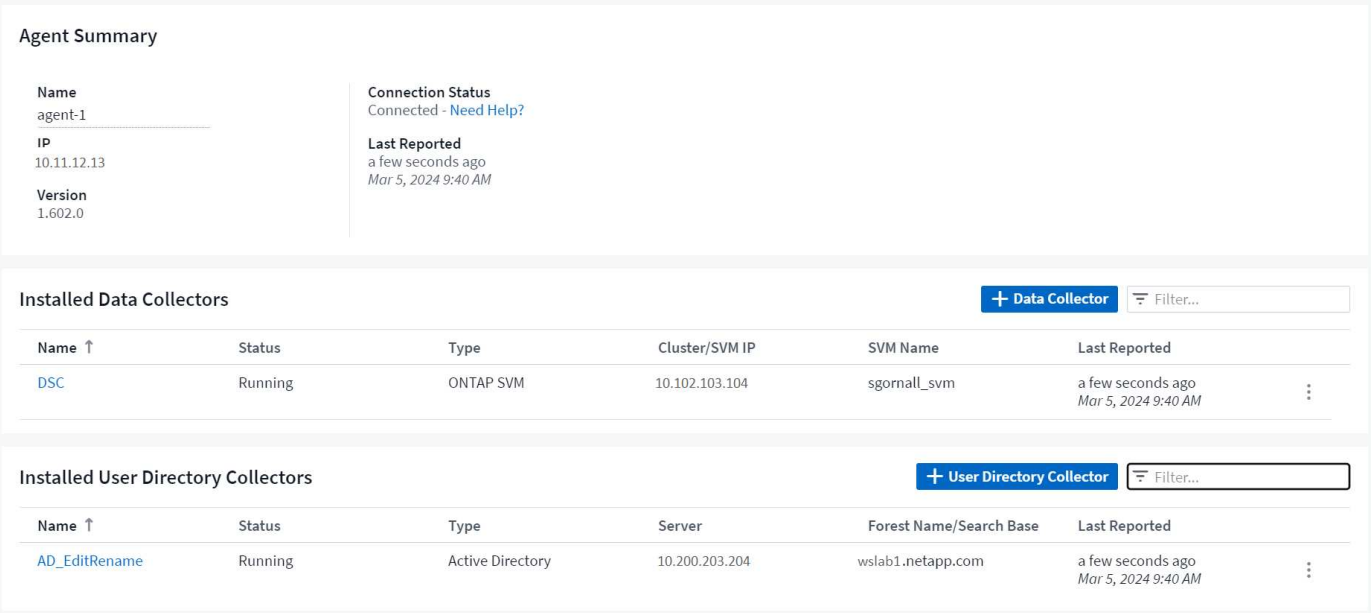
Cloud Insights Acquisition Unitでサポートされるオペレーティングシステムは次のとおりです "すでにサポートされています"：

- Oracle Enterprise Linux 8.8
- Red Hat Enterprise Linux 8.8
- ロッキー9.3
- openSUSE Leap 15.1～15.5
- SUSE Enterprise Linux Server 15、15 SP2～15 SP5

2024年3月

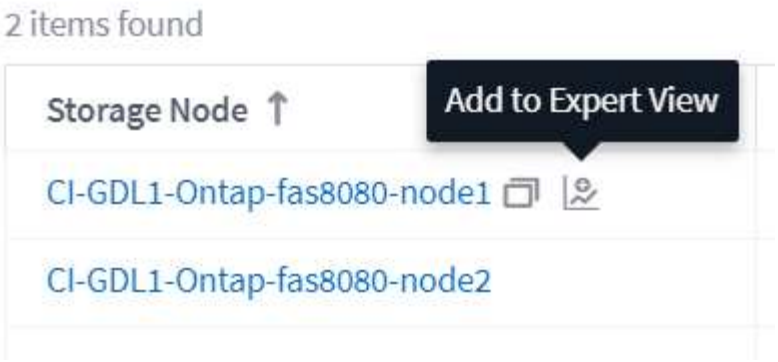
ワークロードセキュリティエージェントの詳細

各ワークロードセキュリティエージェントには独自のランディングページがあり、エージェントに関する概要情報だけでなく、そのエージェントに関連付けられているインストール済みのデータコレクタおよびユーザディレクトリコレクタも簡単に確認できます。

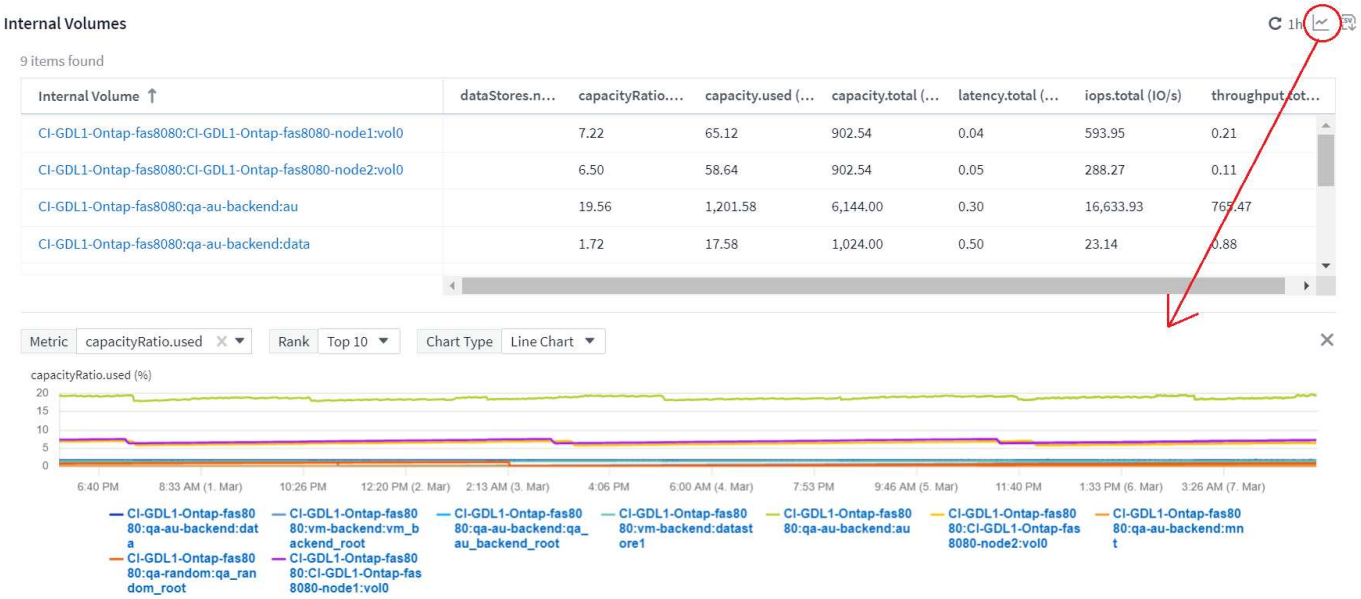


より多くのデータを迅速にグラフ化

アセットのランディングページのデータを分析する際に、エキスパートビューのグラフに簡単にデータを追加できます。ランディングページの各テーブルで、オブジェクトタイプに関連データがある場合は、そのオブジェクトにカーソルを合わせると、[エキスパートビューに追加]アイコンが表示されます。このアイコンを選択すると、そのオブジェクトが[Additional Resources]に追加され、[Expert View]チャートに表示されます。



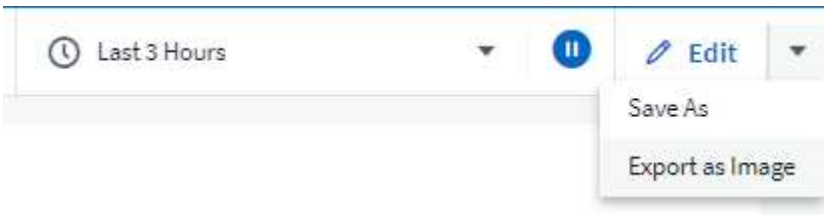
ランディングページの表のデータを独自のグラフで表示することもできます。[*Show Chart*]アイコンを選択すると、テーブルの下にグラフが表示されます。



2024年2月

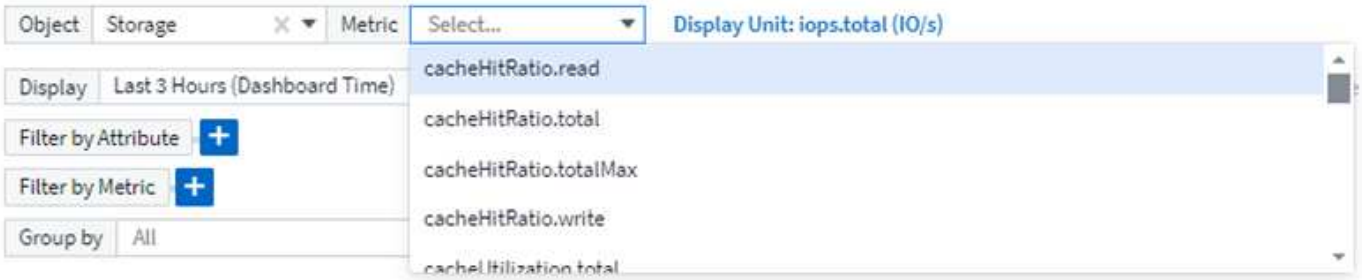
ユーザビリティの向上

右隅のドロップダウンから_Export as Image_を選択して、現在のダッシュボードの*スナップショット*を保存します。Cloud Insightsは、現在のウィジェットの状態の.pngを作成します。



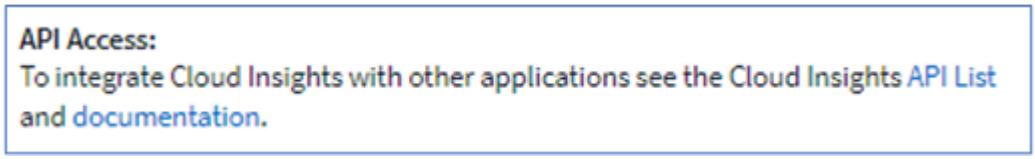
ドロップダウン"]

*ウィジェット、モニターなどのオブジェクトとメトリックの選択*がこれまで以上に簡単になりました。 目的のオブジェクトタイプを選択し、別のドロップダウンでそのオブジェクトに関連するメトリックを選択します。

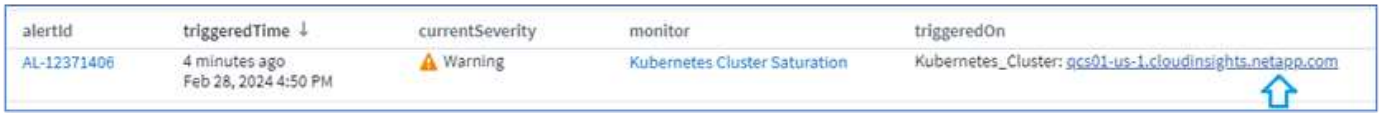


*これらのページの上部にあるアイコンを選択して、Data CollectorとAcquisition Unit *のリストを.csvにエクスポートします。

目的の情報を見つけやすくするために、[ヘルプ]>[サポート]ページが再編成されました。お客様からご要望があったため、このページに API Swagger *とユーザドキュメントへの直接リンクが追加されました。

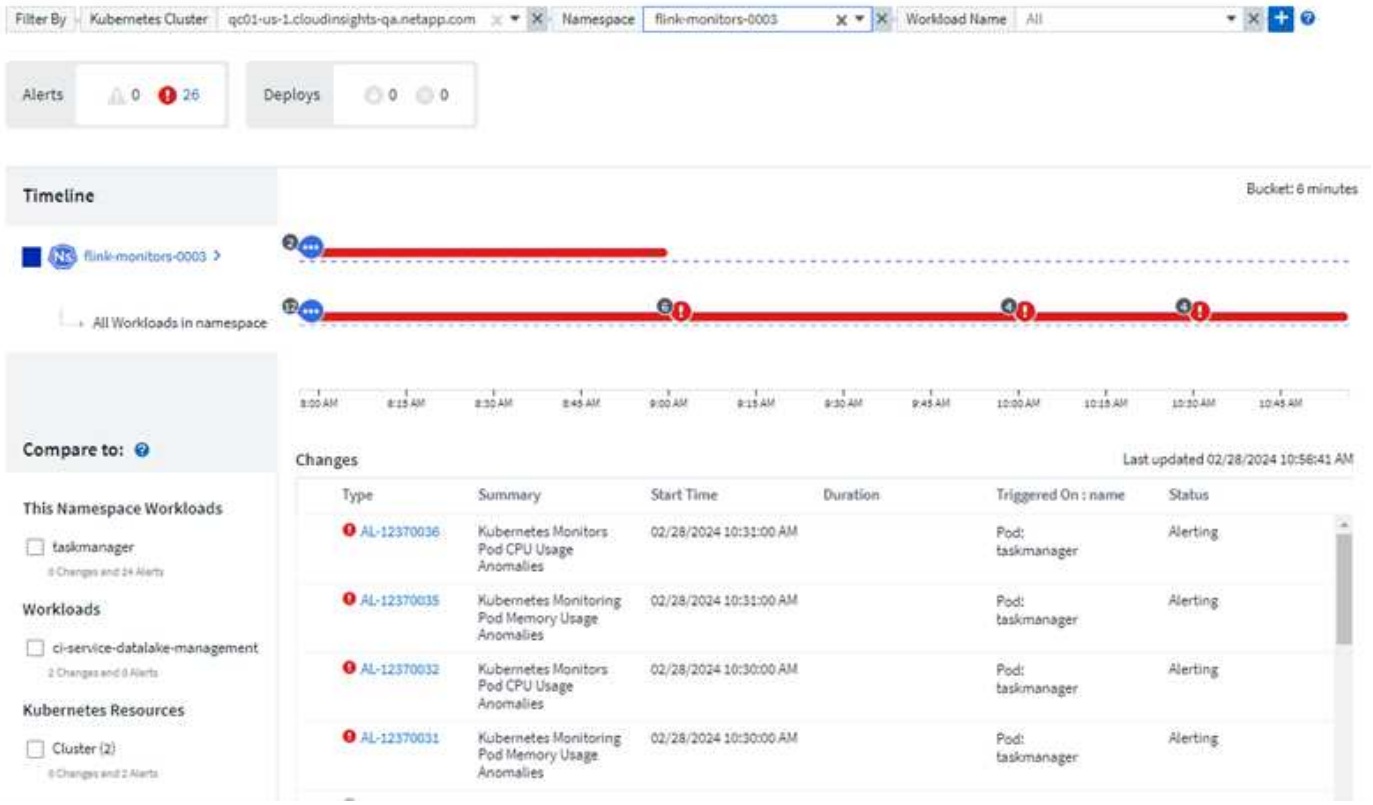


[Alerts]リストページの[triggeredOn]列にある[Links]*をクリックすると、該当するランディングページに移動します（そのオブジェクトにランディングページがある場合）。



ネームスペース内のすべての変更を表示する

Kubernetes Change Analysisで、クラスタとネームスペースを選択したときの変更のタイムラインを確認できるようになりました。以前のバージョンでは、[Workload]も選択しておく必要があります。 クラスタとネームスペースでフィルタリングすると、そのネームスペース内のすべてのワークロードの変化を示すタイムラインが1行に表示されます。



アラートの関連ログ

ログアラートを表示すると、関連するログエントリが新しいテーブルに表示されます。 ログエントリは、アラートと同じソースと期間に発生し、同じ条件の対象となる場合に関連します。[Analyze Logs]を選択して詳細を確認します。

ONTAPスイッチデータの収集

Cloud Insightsでは、ONTAPシステムのバックエンドスイッチからデータを収集できます。データコレクタの_Advanced Configuration_セクションで収集を有効にして、ONTAPシステムが次の機能を提供するように設定されていることを確認します。 "スイッチ情報" そして適切な "権限" 設定：

ワークロードセキュリティデータコレクタAPI

大規模な環境では、新しいData Collectors APIを使用してワークロードセキュリティコレクタの作成を自動化できます。詳細については、* Admin > API Access > API Documentation *に移動し、_Workload Security_APIタイプを選択します。

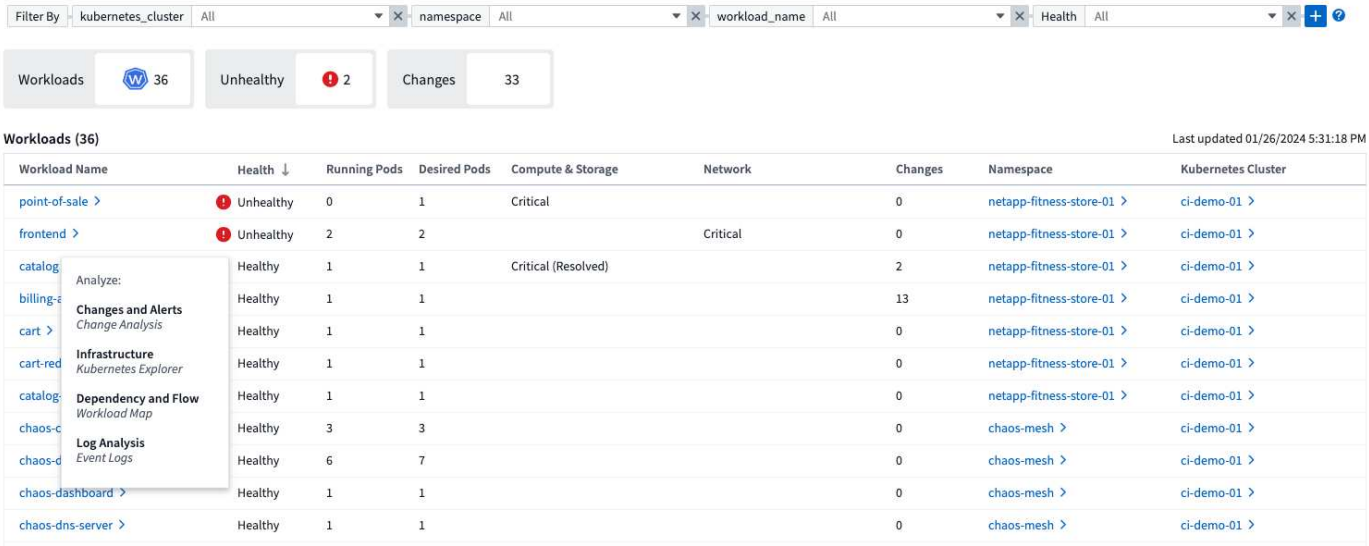
2024年1月

まだ使用していない**Cloud Insights**機能を試す

Cloud Insightsの初回トライアルに加えて、 "モジュールの評価"。たとえば、Cloud Insightsにサブスクライブしていて、ストレージと仮想マシンを監視していた場合、Kubernetesを環境に追加すると、Kubernetesオブザーバビリティの30日間トライアルに自動的に参加できます。Kubernetes Observability Managed Unitの使用状況は、試用期間が終了するまで、サブスクライブ済みのエンタイトルメントにはカウントされません。

ワークロードの健全性

ワークロードの健全性は、* Kubernetes > Explore > Workloads *ページで一目で確認できるため、どのワークロードがパフォーマンスに優れていて、どのワークロードに支援が必要かをすばやく確認できます。健全性問題がインフラ、ネットワーク、構成の変更に関連しているかどうかを簡単に特定し、ドリルダウンしてルート原因を分析します。



Data Collector のアップデート

Data Domainの識別

Data Domainコレクタが改善され、フェイルオーバー時の耐久性を確保するためにHAシステムをより適切に識別できるようになりました。この変更により、HAシステム内のData Domainアプライアンスが1回だけ原因されます。これにより、削除するアセットのアノテーションが原因されます（アレイが再識別されるため）。Data Domainオブジェクトにアノテーションを再アタッチする必要があります。

ランサムウェア検出**ML**アルゴリズムの強化

ワークロードセキュリティには、最も高度な攻撃をより迅速かつ正確に検出するための、新しい第2世代のランサムウェア検出MLアルゴリズムが含まれています。

行動の「季節性」:週末の行動は、平日と午前の行動とは異なるパターンに従う場合があります。ワークロードセキュリティアルゴリズムでは、この季節性を考慮に入れています。

廃止された機能

機能の進化に伴い、機能が廃止されることがあります。Cloud Insightsで廃止された機能の一部を次に示します。

Workload Secure REST cloudsecure_forensics.activities.v1 APIの廃止

_cloudsecure_forensics.activities.v1_APIは廃止されました。このAPIは、Storage Workload Security環境内のエンティティに関連付けられているアクティビティに関する情報を返します。このAPIはcloudsecure_forensics.activities.* v2 *_に置き換えられました。

このAPIに対してGETを実行すると、次の情報が返されました。

```
{
  "count": 24594,
  "limit": 1000,
  "offset": 0,
  "results": [
    {
      "accessLocation":
```

このAPIは次の値を返します。

```
{
  "limit": 1000,
  "meta": {
    "page": {
      "after": "lvlvk3pp.4cpzcg4kpybl",
      "before": "lvlxy3dz.4cq5ajdnl9fk",
      "size": 1000
    }
  },
  "results": [
    {
      "accessLocation": "10.249.6.220",
```

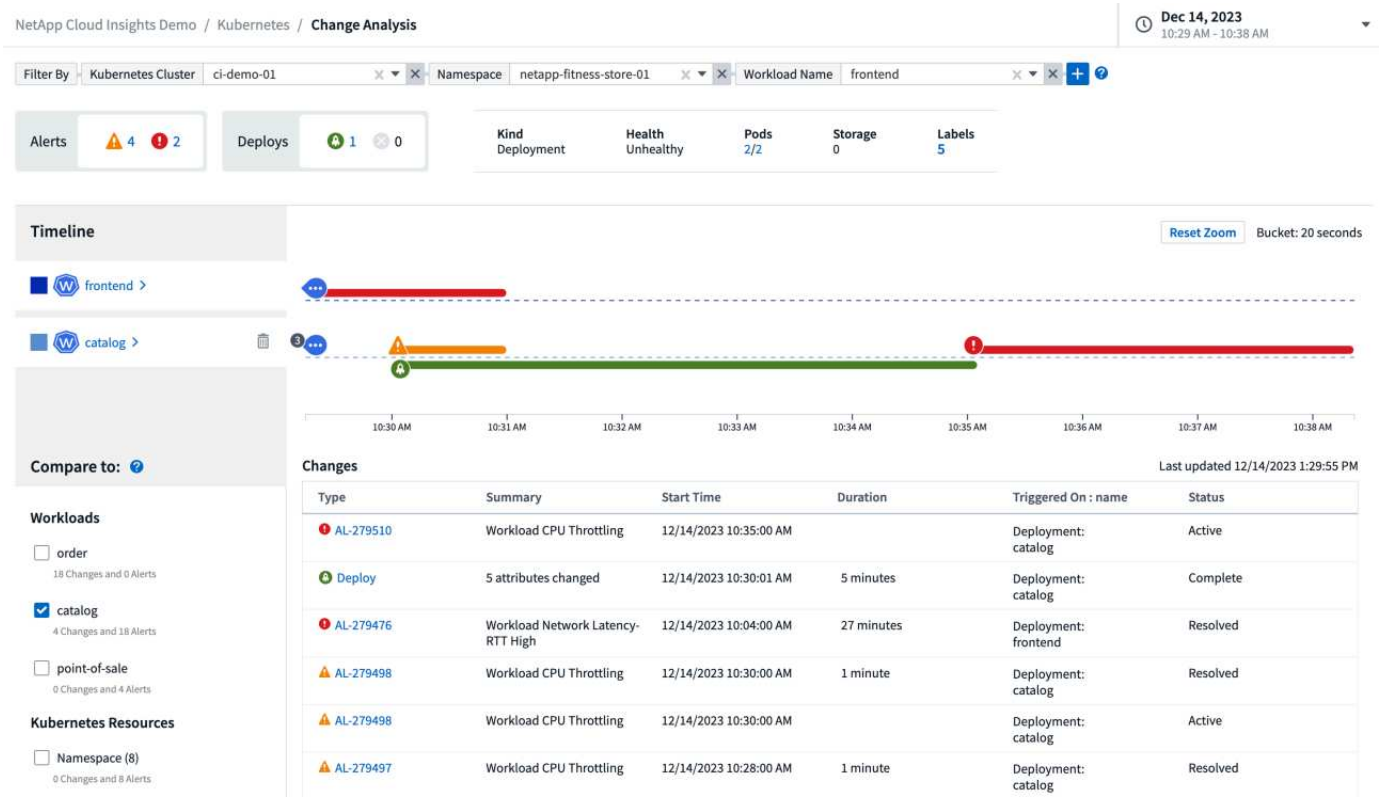
詳細については、Swaggerのドキュメント（[Admin]>[API Access]>[API Documentation]>[Workload Security]）を参照してください。

2023年12月

分析を一目で変更

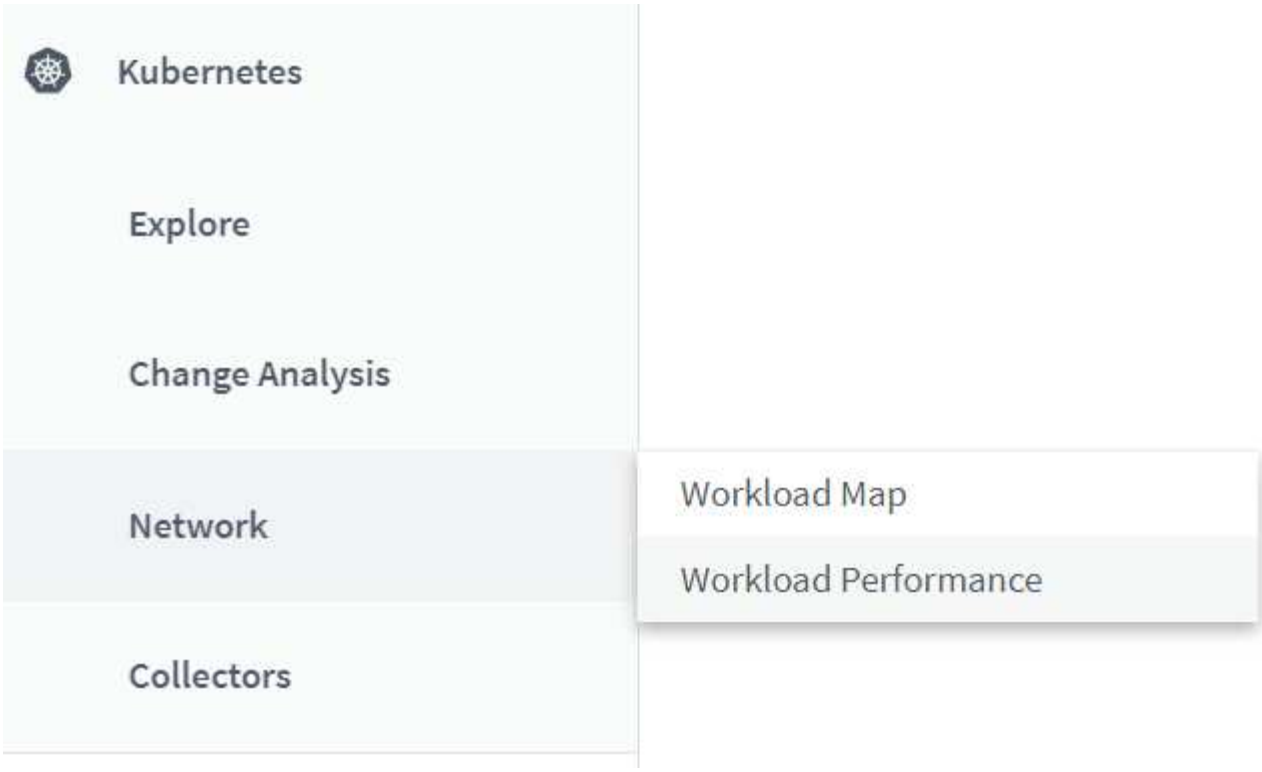
Kubernetes "変更分析" Kubernetes環境に対する最近の変更をオールインワンで確認できます。アラートと導

入ステータスをすぐに確認できます。変更分析を使用すると、導入と設定の変更をすべて追跡し、Kubernetesのサービス、インフラ、クラスタの健全性とパフォーマンスに関連付けることができます。

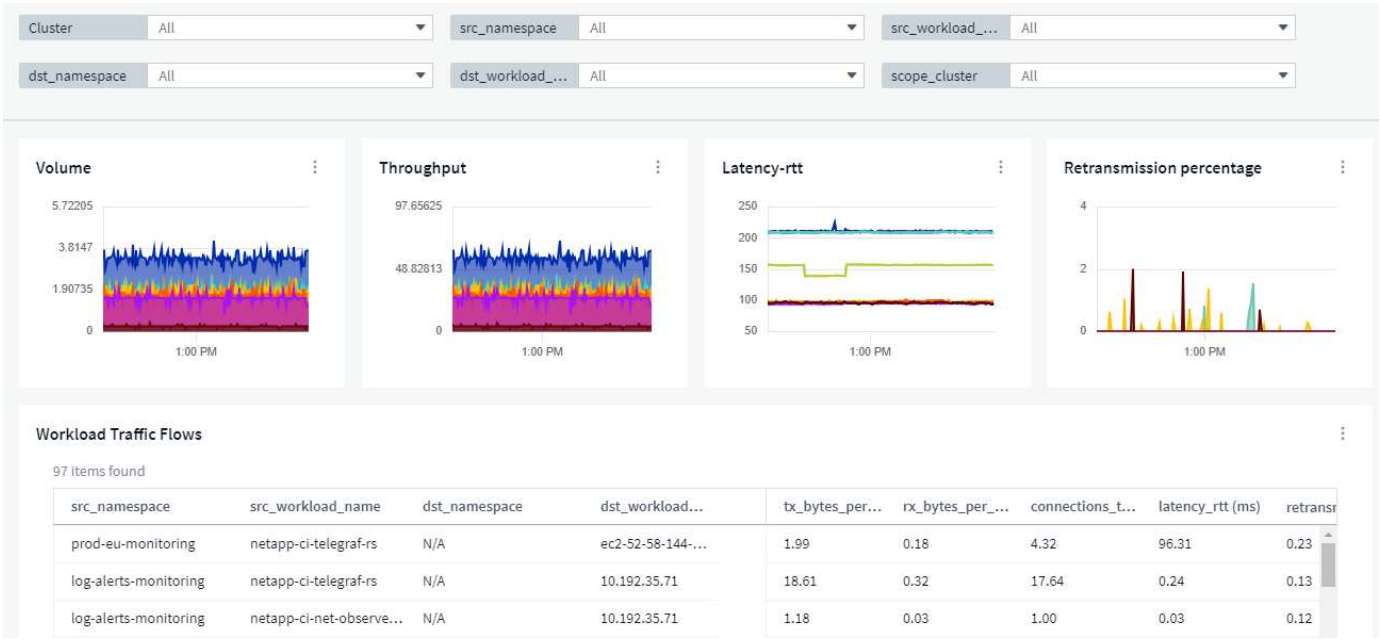


Kubernetesワークロードパフォーマンスダッシュボード

ワークロードのパフォーマンスは、Kubernetesワークロードのパフォーマンスを包括的なダッシュボードで一目で確認できます。ボリューム、スループット、レイテンシ、再送信の傾向のグラフや、環境内の各ネームスペースのワークロードトラフィックの表をすばやく確認できます。フィルタを使用すると、関心のある分野に簡単にフォーカスできます。

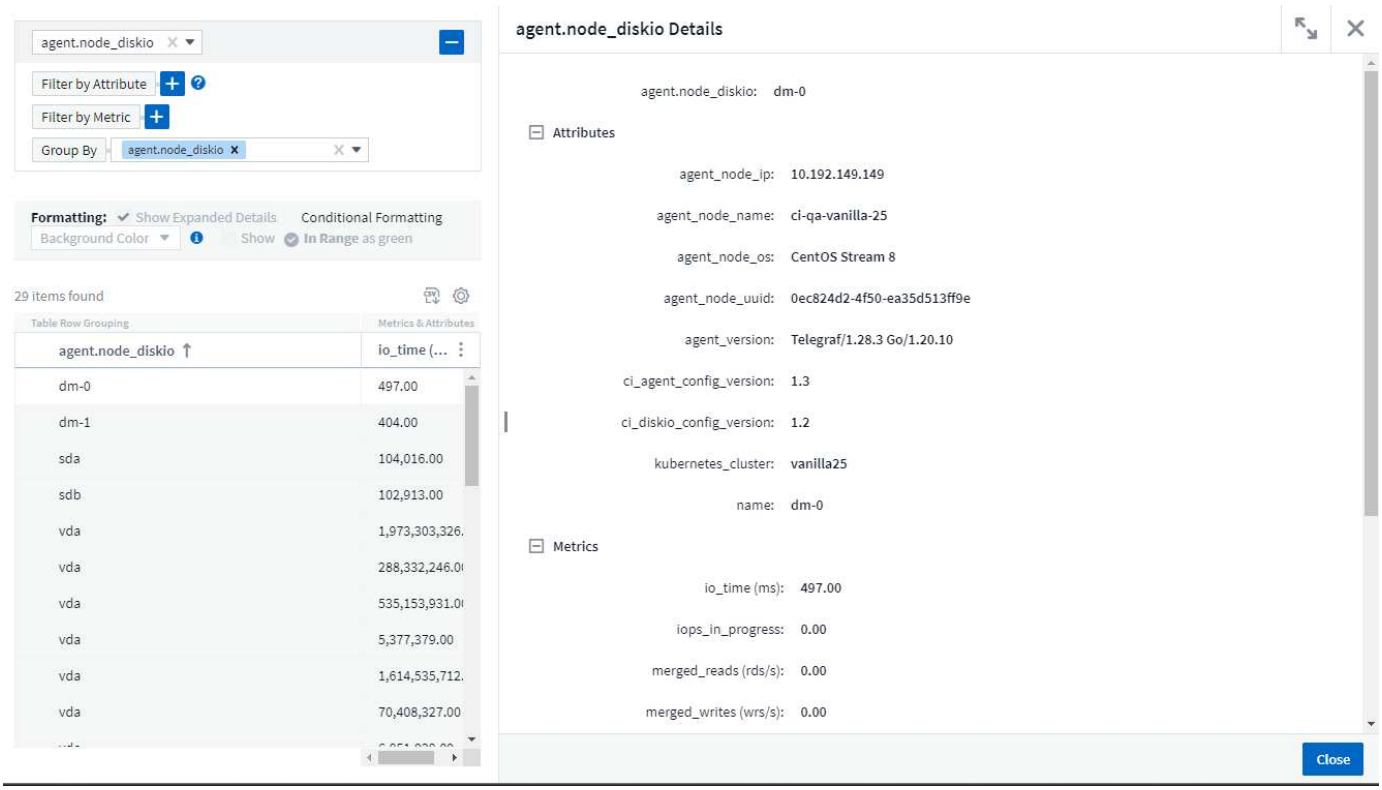


メニュー（幅= 400）"]



クエリの詳細を1つの画面に表示

クエリで行を選択すると、選択した行の属性、アノテーション、および指標の詳細がサイドパネルに表示され、オブジェクトのランディングページにドリルダウンしなくても役立つ情報が表示されます。行またはサイドパネルのリンクにより、ナビゲーションが容易になります。



Data Collectorのアップデート：

- * Brocade FOS REST *：このコレクタは「プレビュー」から移動され、一般提供されるようになりました。注意すべき点：
  - FOSでは、REST APIがFOS 8.2で導入されました。ただし、ルーティングなどの一部の機能では、9.0のREST API機能しか使用できません。
  - 8.2以降のFOSアセットが混在したファブリックと8.2より前のアセットで構成されているファブリックでは、Cloud Insights FOS RESTコレクタで古いアセットを検出できません。FOS RESTコレクタを編集して、デバイスのIPv4アドレスをカンマで区切って作成し、そのコレクタから除外することができます。
- **SELinux**: Cloud Insightsには、Linux Acquisition Unitの初期インストールが強化されており、SELinuxの強制が有効になっているLinux環境での動作の堅牢性を確保します。これらの機能拡張は_new_au環境にのみ影響します。AUのアップグレードに関連するSELinuxの問題がある場合は、NetAppサポートに連絡してSELinux構成の修正を依頼してください。

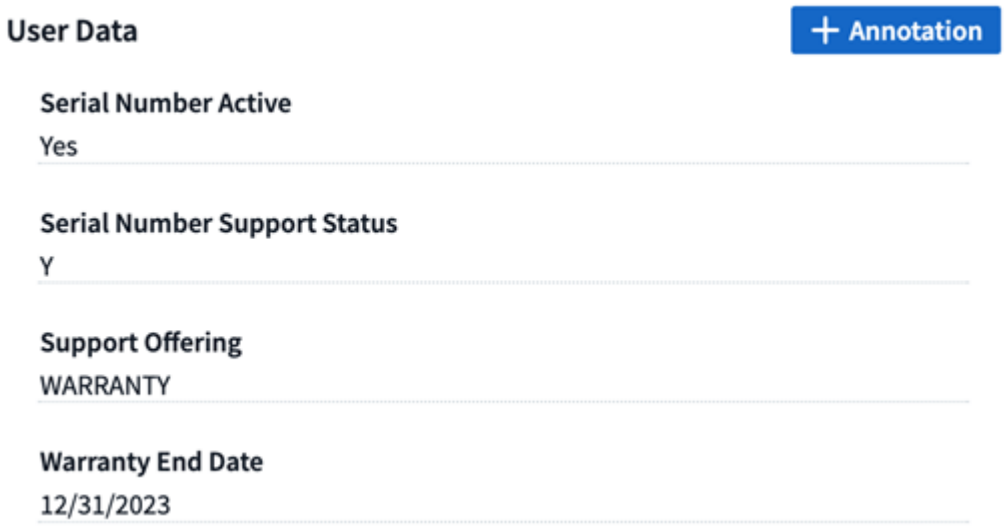
2023年11月

ワークロードのセキュリティ：コレクタの一時停止/再開

Workload Securityでは、コレクタがin_running_stateの場合、Data Collectorを一時停止できます。コレクターの「3つのドット」メニューを開き、一時停止を選択します。コレクタが一時停止している間は、ONTAPからデータが収集されず、コレクタからONTAPにデータが送信されません。収集を再開するには、[Resume]を選択します。

ストレージノードのサポート情報

ストレージノードのランディングページの_User Data_セクションには、ご利用のサポートサービス、現在のステータス、サポートステータス、保証終了日に関する情報が一目でわかるように表示されます。Cloud Insightsは現在、この情報をNetAppデバイスに対してのみ自動公開していることに注意してください。これらのサポートフィールドはアノテーションであるため、クエリやダッシュボードで使用できます。



VMwareタグをCloud Insightsアノテーションにマッピング

。 "VMware" データコレクタを使用すると、VMwareで設定されている同名タグを使用してCloud Insightsのテキスト注釈を入力できます。

FOS 9.1.1c以降のファームウェアに対するBrocade CLIコレクタの信頼性の向上

9.1.1cファームウェアを実行している一部のBrocadeファイバチャネルスイッチでは、特定のCLIコマンドの出力の先頭に「motd」ログインバナーテキストが付加されたり、ユーザがデフォルトのパスワードを変更するように警告が表示されたりすることがあります。Brocade CLIコレクタが拡張され、これら2種類の無関係なテキストが無視されるようになりました。

この機能拡張以前は、仮想ファブリックが存在しないFOS 9.1.1cスイッチだけがこのコレクタタイプで検出されていました。

2023年10月

ワークロードセキュリティの強化

ワークロードのセキュリティが改善され、次の機能が追加されました。

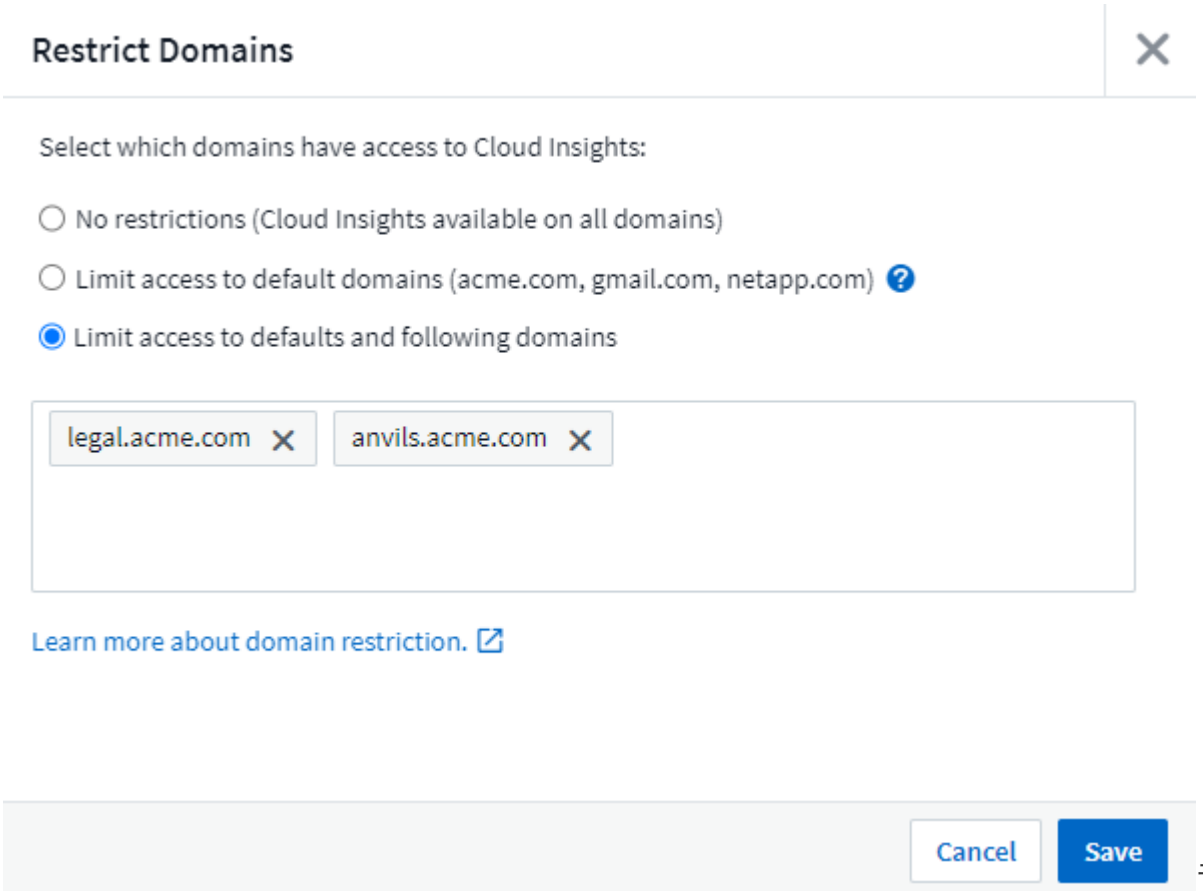
- アクセス拒否：ワークロードセキュリティをONTAPと統合して "「アクセス拒否」イベント" また、追加の分析と自動応答レイヤーを提供します。
- 許可されるファイルの種類：既知のファイル拡張子に対してランサムウェア攻撃が検出された場合、そのファイル拡張子を "許可されているファイルタイプ" 不要なアラートを回避するためのリスト。

モジュールのトライアル

Cloud Insightsの初回トライアルに加えて、 "モジュールの評価"。たとえば、インフラオブザーバビリティにすでにサブスクライブしているものの、Kubernetesを環境に追加する場合は、自動的にKubernetesオブザーバビリティの30日間トライアルに参加します。評価期間の終了時に、Kubernetes Observability Managed Unitの使用料金のみが請求されます。

指定したドメインへのアクセスを制限する

管理者とアカウント所有者は、次のことができるようになりました。 "Cloud Insightsアクセスの制限" 指定した電子メールドメインに送信します。[Admin]>[User Management]*に移動し、[_Restrict Domains]ボタンを選択します。



モーダル"]

Data Collector のアップデート

Data Collector/Acquisition Unitに次の変更が加えられています。

- * Isilon/PowerScale REST*：Cloud Insightsの強化された分析機能に、さまざまな新しい属性とメトリックが_emc_isilon.node_pool.*_という名前で追加されました。これらのカウンタと属性により、ユーザーはダッシュボードを構築して_node_pool_capacity消費量を監視することができます。異なるハードウェアノードモデルから構築されたIsilonクラスターのユーザーは複数のノードプールを持ち、ノードプールレベルでのHDD/SSD/総容量消費量を把握することは、監視と計画の両方に役立ちます。
- * Rubrik *「サービスアカウント」認証のサポート: Cloud InsightsのRubrikコレクタは、従来のHTTP基本認証(ユーザー名とパスワード)と、ユーザー名+シークレット+組織IDを必要とするRubrikのサービスアカウントアプローチの両方をサポートするようになりました。

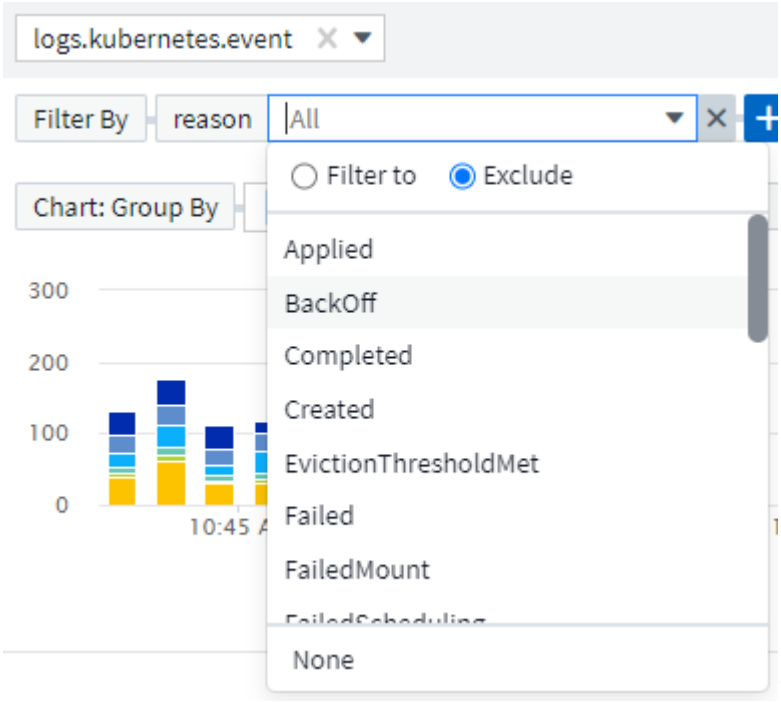
2023年9月

ログで必要なものを簡単に検索

ログクエリ（オブザーバビリティ>ログクエリ>+新規ログクエリ）には、次のものが含まれます。 "キノウカクチョウ" ログの検索を容易にし、より有益な情報を提供します。

含める/除外する

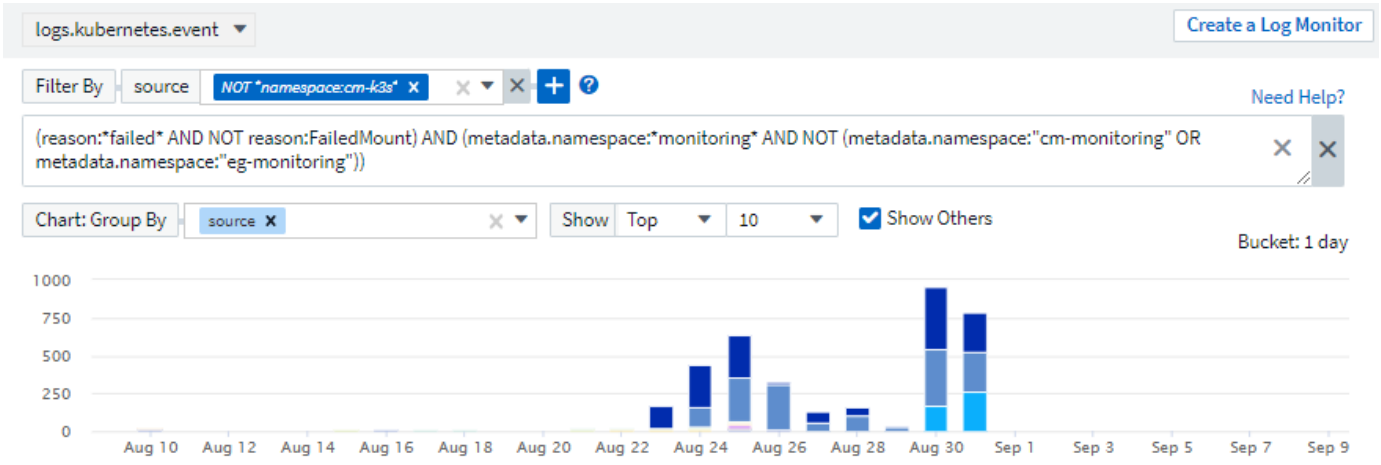
値をフィルタリングするときに、フィルタに一致する結果を*含める*か*除外*かを簡単に選択できます。「除外」を選択すると、「非<value>」フィルタが作成されます。INCLUDE値とEXCLUDE値を1つのフィルタで組み合わせることができます。



ラジオボタンを表示するフィルタ"]

高度なクエリ

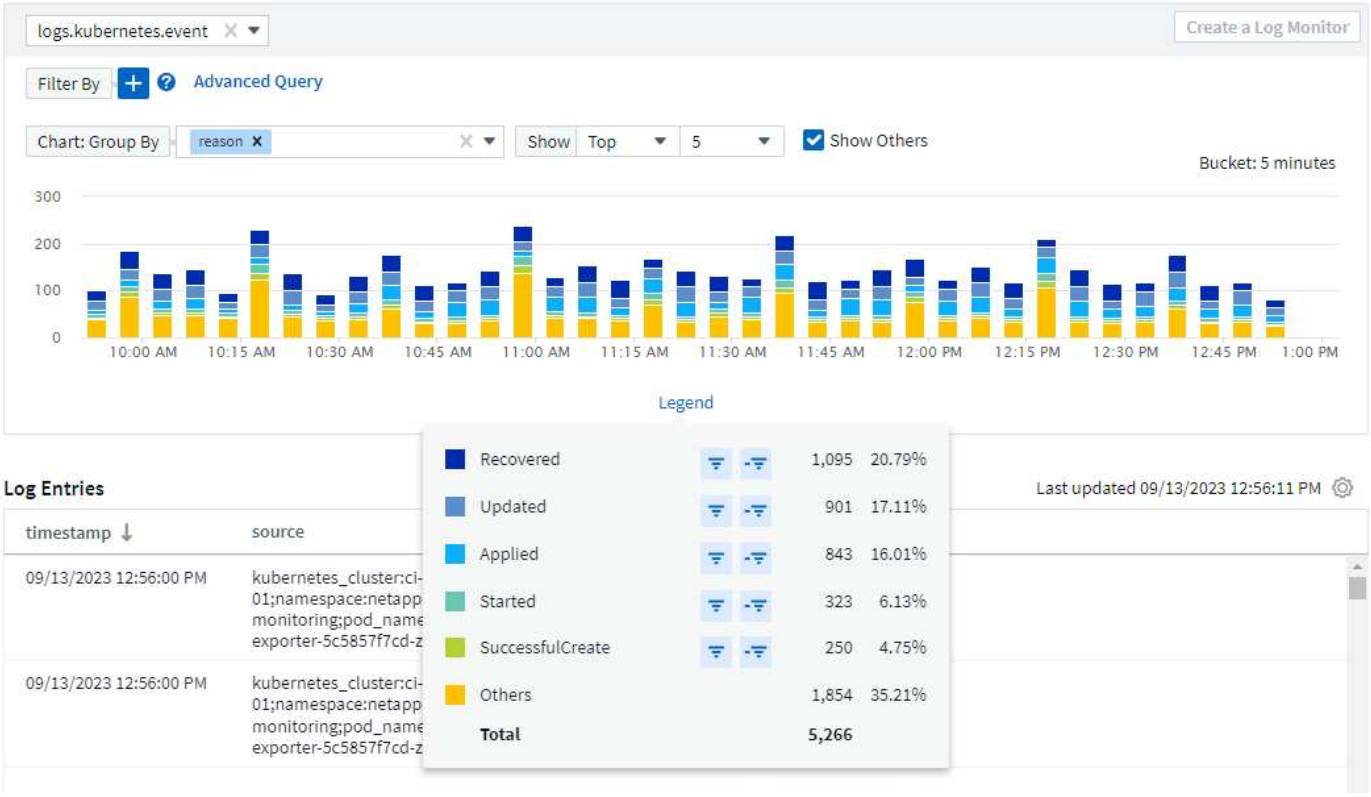
*高度なクエリ*では、AND、NOT、OR、ワイルドカードなどを使用して値を結合または除外する「自由形式」フィルタを作成できます。



[Filter By]と[Advanced Query]は、「AND」でまとめて1つのクエリを形成します。結果が結果リストとグラフに表示されます。

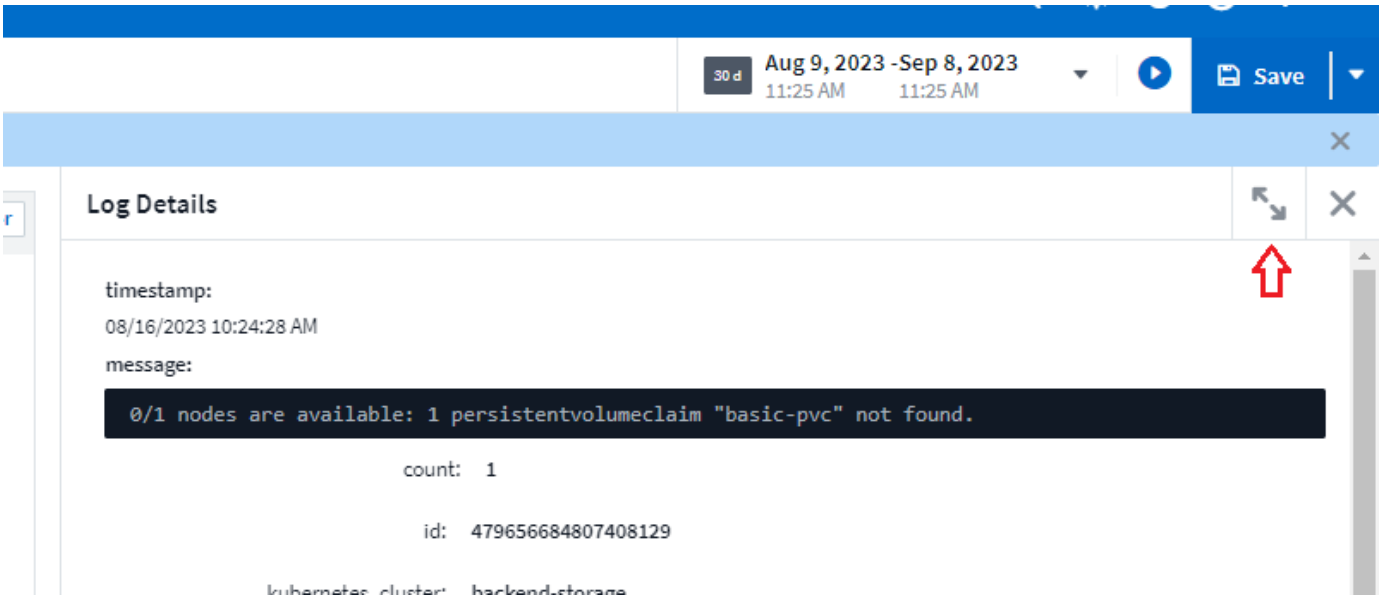
グラフでのグループ化

[*グループ化]*にログ属性を選択すると、リストとグラフに現在のフィルタの結果が表示されます。グラフでは、列が色別にグループ化されています。グラフの列にカーソルを合わせると、グラフの凡例を展開したときに表示される全体的な情報と同様に、特定のエントリに関する詳細が表示されます。 凡例では、特定のグループに含めるフィルタまたは除外フィルタを設定することもできます。



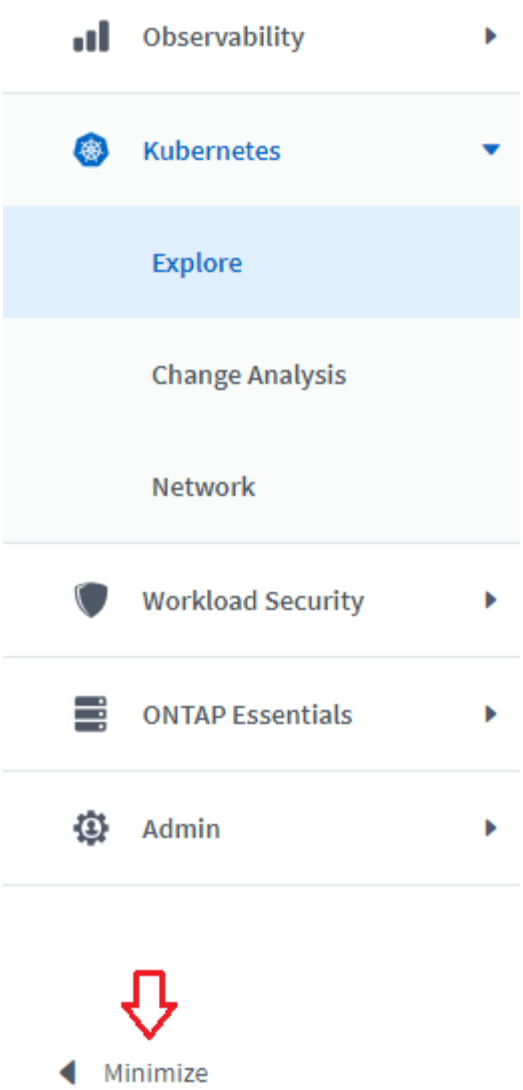
「フローティング」ログ詳細パネル

[Log Query]を使用してログを検索するときに、リスト内のエントリを選択すると、そのエントリの詳細パネルが開きます。スライドアウトパネルを「フローティング」（画面の残りの部分に表示）または「ページ内」（ページ内の独自のフレームとして表示）を選択できるようになりました。これらのビューを切り替えるには、パネルの右上隅にある[ページ内/フローティング]ボタンを選択します。



メニューを折りたたむ

左側のCloud Insightsナビゲーションメニューを折りたたむには、メニューの下にある[最小化]ボタンを選択します。メニューが最小化されている間に、アイコンにカーソルを合わせると、どのセクションが開いているかが表示されます。アイコンを選択するとメニューが開き、そのセクションに直接移動します。



Data Collectorの改善点

Cloud Insightsでは、データコレクタ情報の表示と検索が容易になりました。

- *データコレクタリストの処理がより効率的になるため、これらのリストの表示とナビゲートにかかる時間が大幅に短縮されます。多数のデータコレクタが存在する大規模な環境では、データコレクタの一覧表示が大幅に改善されます。
- Data Collector Support Matrix *は、.pdfファイルから.htmlベースのページに移行しました。これにより、ナビゲートが迅速になり、メンテナンスが容易になりました。新しいマトリックスはこちら：https://docs.netapp.com/us-en/cloudinsights/reference_data_collector_support_matrix.html

2023年8月

Isilon/PowerScaleログと高度な分析データの収集

Isilon RESTコレクタとPowerScale RESTコレクタの改善点は次のとおりです。

- Isilonログイベントはクエリやアラートで使用できます。
- Isilon高度な分析属性は、クエリ、ダッシュボード、アラートで使用できます。
  - EMC_Isilon.cluster
  - emc_isilon.node
  - emc_isilon.node_disk
  - emc_isilon.net_iface

これらは、Isilon RESTコレクタやPowerScale RESTコレクタのユーザーに対してデフォルトで有効になっています。NetAppでは、Isilon CLIベースのコレクタのユーザーは、上記のような拡張機能を利用するために、新しいREST APIベースのコレクタに移行することを強く推奨しています。

ワークロードマップの改善

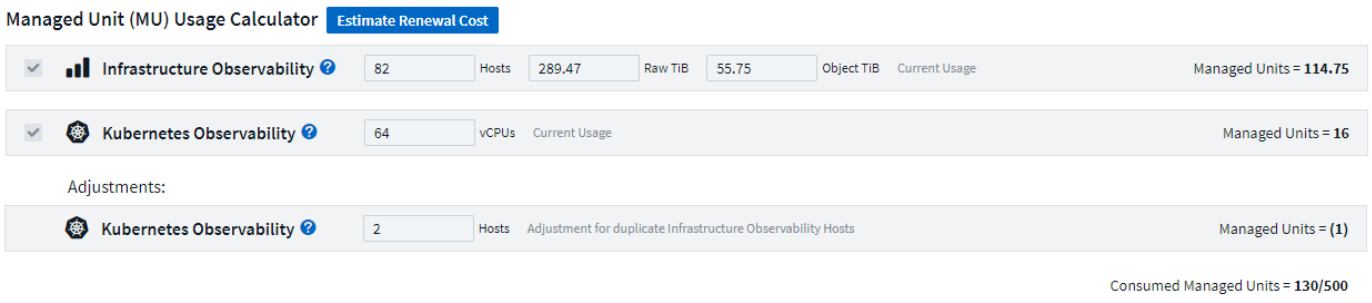
ワークロードマップは、同じワークロードと通信する場合は、類似するすべての外部サービスを1つのノードにグループ化するため、グラフの複雑さが軽減され、サービスの相互接続方法がわかりやすくなります。

グループ化されたノードを選択すると、そのノードに関連する各外部サービスのネットワークトラフィックメトリックを含む詳細な表が表示されます。

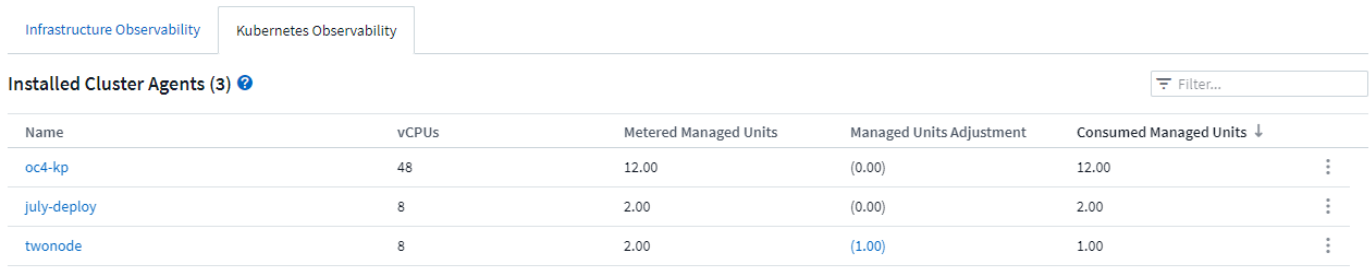
Kubernetes Managed Unitの使用状況の調整

Kubernetesクラスタ環境のコンピューティングリソースがNetApp Kubernetes Monitoring Operatorと基盤となるインフラデータコレクタ（VMwareなど）の両方によってカウントされた場合、これらのリソースの使用量が調整されて、Managed Unitのカウントが最も効率的に行われるようになります。Kubernetes MUの調整は、Admin > SubscriptionページのSummaryタブとUsageタブの両方で確認できます。

[Summary]タブ：



[Usage]タブ：



タブに表示されるK8s MU調整"]

コレクタ/取得の変更点：

Data Collector/Acquisition Unitに次の変更が加えられています。

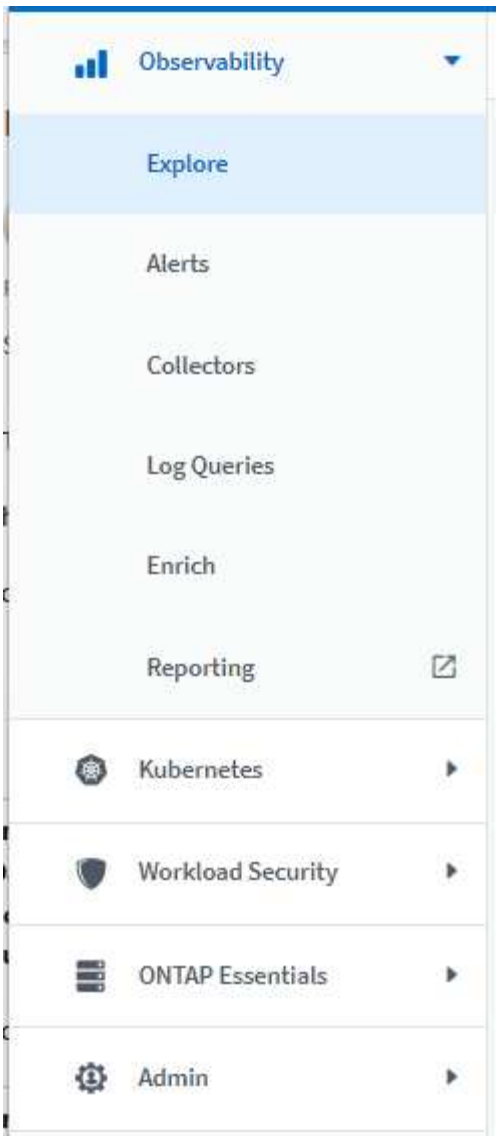
- Acquisition UnitがRHEL 8.7をサポートするようになりました。

メニューの改善

左側のナビゲーションメニューが更新され、お客様のワークフローをより適切にサポートできるようになりました。_kubernetes_などの新しいトップレベル項目は、顧客のニーズに迅速にアクセスできるようにし、統合管理者コンソールがテナント所有者の役割をサポートします。

変更のその他の例を次に示します。

- 最上位の_Observability_menuには、データ検出、アラート、ログクエリが表示されます。
- オブザーバビリティとワークロードセキュリティの[API Access]機能は1つのメニューにまとめられています。
- オブザーバビリティとワークロードセキュリティの[Notifications]機能も同様に、1つのメニューに追加されました。



各メニューに表示される機能の簡単なリストを次に示します。

オブザーバビリティ：

- 製品概要（ダッシュボード、指標クエリ、インフラに関する分析情報）
- アラート（監視とアラート）
- コレクタ（データコレクタとAcquisition Unit）
- ログクエリ
- Enrich（アノテーションとアノテーションルール、アプリケーション、デバイス解決）
- レポート作成

Kubernetes：

- クラスタの詳細とネットワークマップ

ワークロードのセキュリティ：

- アラート
- フォレンジック
- コレクタ
- ポリシー

ONTAPの基礎：

- データ保護
- セキュリティ
- アラート
- インフラ
- ネットワーキング
- ワークロード
- VMware

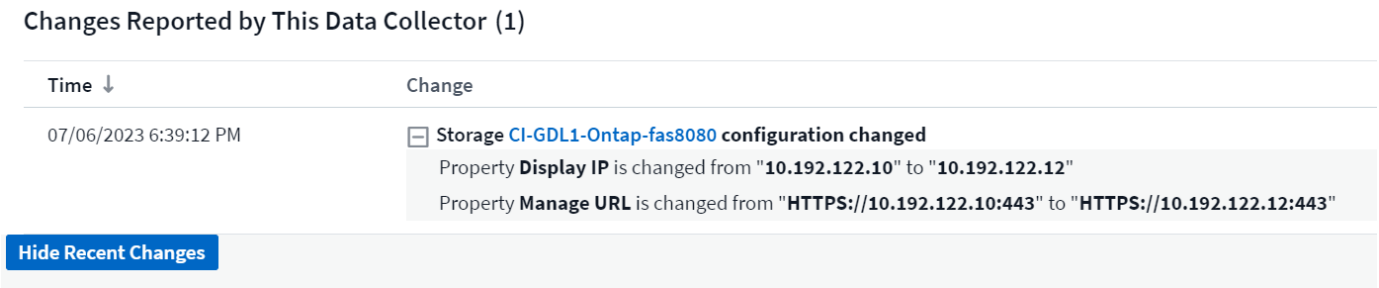
管理：

- API アクセス
- 監査
- 通知
- サブスクリプション情報
- ユーザ管理

2023年7月

最近の変更を表示します

Data Collectorのランディングページに、最近の変更のリストが表示されるようになりました。データコレクタのランディングページの下部にある[Recent Changes]ボタンをクリックするだけで、最近のデータコレクタの変更が表示されます。



オペレータの改善

に次の改善が加えられました "Kubernetesオペレータ" 導入：

- Dockerのメトリック収集をバイパスするオプション
- Telegrafデーモンセットおよびレプリカセットに許容範囲を追加およびカスタマイズする機能

Insight：コールドストレージの再利用

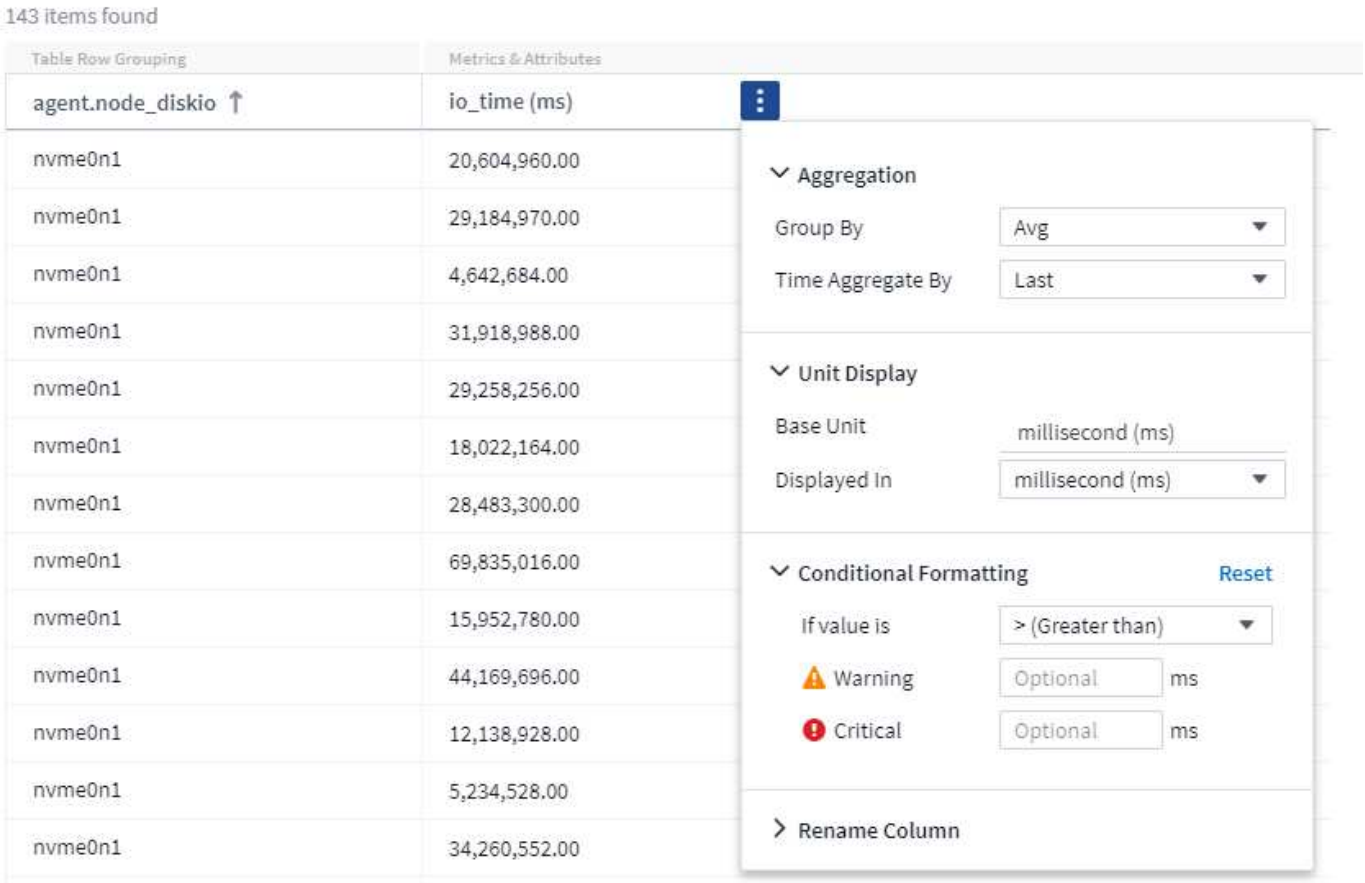
。 "ONTAPコールドストレージInsightを再利用します" FlexGroupがサポートされるようになりました。すべてのお客様がこのサービスを利用できるようになりました。

Operator Image Signatureの略

NetApp Kubernetes Monitoring Operatorのプライベートリポジトリを使用するお客様向けに、Operatorのインストール時にイメージ署名公開キーをコピーできるようになり、ダウンロードしたソフトウェアの信頼性を確認できるようになりました。オプションの手順で[_Copy Image Signature Public Key]ボタンを選択して、オペレータイメージをプライベートリポジトリにアップロードします。

クエリの集計、条件付き書式など

集計、単位の選択、条件付き書式、列の名前変更は、ダッシュボード表ウィジェットの最も便利な機能の1つであり、で同じ機能を使用できるようになりました "クエリ"。

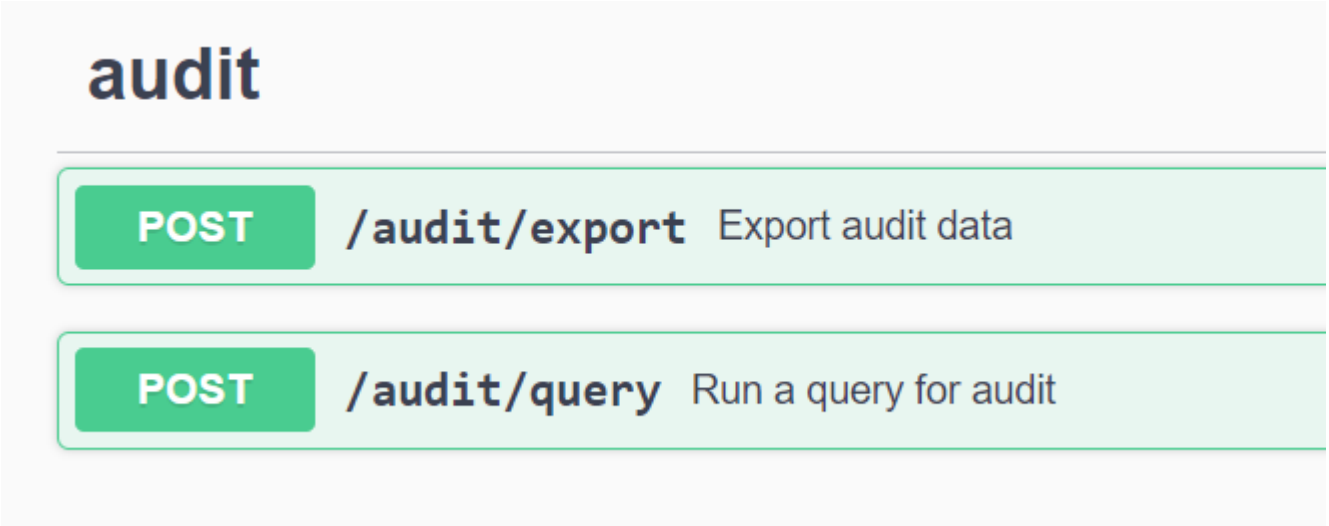


ページの結果には、集計、条件付き書式、単位表示、列名の変更が表示されます"]

これらの機能は、統合タイプのデータ（Kubernetes、ONTAP Advanced Metricsなど）で使用できるようになりました。インフラオブジェクト（ストレージ、ボリューム、スイッチなど）についても近日提供予定です。

監査用API

APIを使用して、監査対象イベントを照会またはエクスポートできるようになりました。[Admin]>[API Access]に移動し、詳細については[_API Documentation_link]を選択してください。



Data Collector：Trident Economyの略

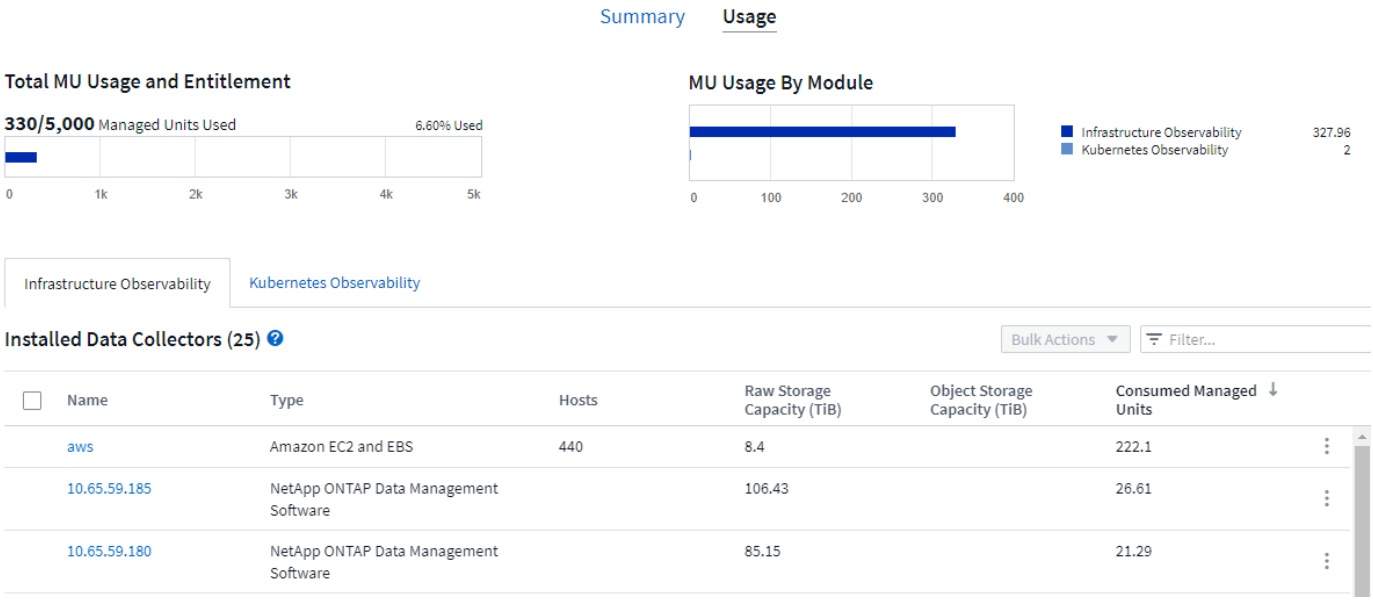
Cloud InsightsがTridentエコノミードライバをサポートするようになり、次のようなメリットが実現しました。

- ポッドとONTAPのqtreeのマッピングとパフォーマンス指標を可視化
- Kubernetesポッドからバックエンドストレージへのシームレスなトラブルシューティングと簡単なナビゲーションを提供します
- 監視機能でバックエンドのパフォーマンスの問題をプロアクティブに検出します

2023年6月

使用状況を確認してください

2023年6月より、Cloud Insightsでは、機能セットに基づくManaged Unitの使用量の内訳を提供しています。インフラのManaged Unit（MU）の使用状況やKubernetesに関連付けられたMUの使用状況をすばやく表示、監視できるようになりました。



Kubernetes Network Monitoring and Mapは、すべてのユーザに使用できます

。 *"Kubernetesのネットワークパフォーマンスとマップ"* Kubernetesワークロード間の依存関係をマッピングすることでトラブルシューティングを簡易化し、Kubernetesのネットワークパフォーマンスのレイテンシや異常をリアルタイムで可視化して、ユーザに影響が及ぶ前にパフォーマンスの問題を特定します。多くのお客様がプレビュー中に役立つと感じており、今では誰もが楽しめるようになっています。

コレクタ/取得の変更点：

Data Collector/Acquisition Unitに次の変更が加えられています。

- Data DomainおよびCohesity MUは、40 TiB：1 MUで計測されます。

- Acquisition UnitでRHELとRocky 9.0および9.1がサポートされるようになりました。

新しいONTAP Essentialsダッシュボード

次のONTAP Essentialsダッシュボードがプレビュー環境で使用可能になり、すべてのユーザーが使用できるようになりました。

- セキュリティダッシュボード
- データ保護ダッシュボード（ローカルとリモートの保護の概要を含む）

追加のシステムモニタ

Cloud Insightsには、次のシステムモニタが付属しています。

- Storage VM FCPサービスを使用できません
- Storage VM iSCSIサービスを使用できません

2023年5月

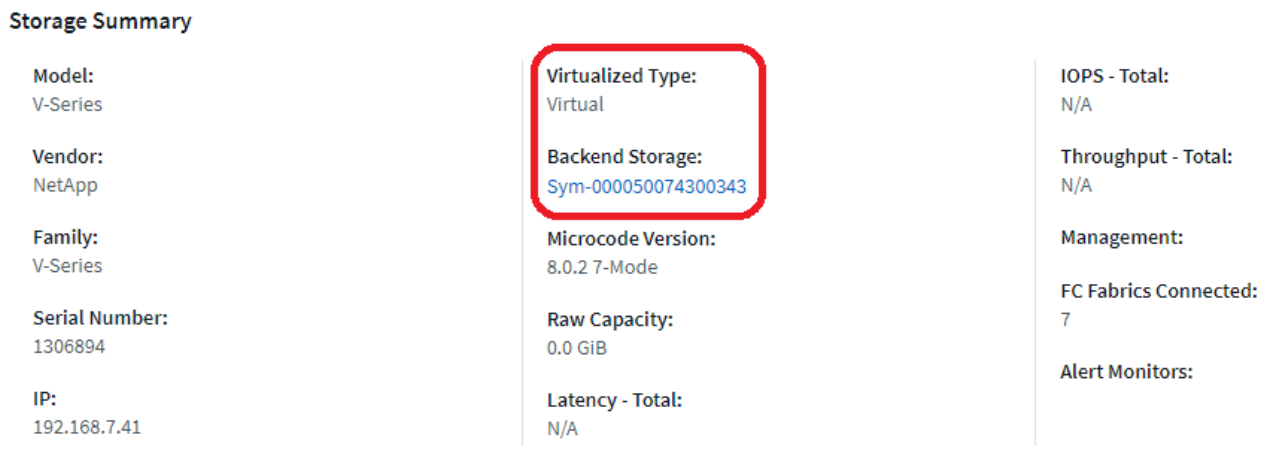
Kubernetes Monitoring Operatorのインストールが改善されました

のインストールと設定 "NetApp Kubernetes Monitoring Operator" 以下の改善により、これまで以上に簡単になりました。

- 環境 "構成設定" は、自己文書化された単一の構成ファイルに保持されます。
- Kubernetes Monitoring Operatorイメージをプライベートリポジトリにアップロードするためのステップバイステップの手順。
- 単一のコマンドで簡単にアップグレードでき、カスタム構成を維持しながらKubernetes Monitoringをアップグレードできます。
- セキュリティの強化：APIキーがシークレットを安全に管理します。
- CI / CD自動化ツールとの統合と導入が容易

ストレージ仮想化

Cloud Insights では、ローカルストレージがあるストレージアレイと他のストレージアレイが仮想化されているストレージアレイを区別できます。これにより、コストを関連付け、フロントエンドからインフラのバックエンドまで、パフォーマンスを区別することができます。



新しいWebhookパラメータ

を作成する場合 "ウェブフック" 通知。Webhook定義に次のパラメータを含めることができます。

- %%TriggeredOnKeys%%
- %%TriggeredOnValues%%

Kubernetesのデータをレポートします

Cloud Insightsで収集されたKubernetesデータ（Persistent Volumes（PV）、PVC、ワークロード、クラスタ、ネームスペースなど）をレポートに使用できるようになり、チャージバック、トレンド分析、予測、TTF計算、 また、Kubernetesの指標に関するその他のビジネスレポートも提供しています。

新規のお客様にはデフォルトのONTAP システムモニタが有効になっています

新しいCloud Insights 環境では、多くのONTAP システムモニタがデフォルトで有効になっています（*resumed*）。以前は、ほとんどのモニタはデフォルトで_Paused_stateに設定されていました。ビジネスニーズは会社によって異なるため、を参照することを常にお勧めします "システムモニタ" アラートの必要性に応じて、それぞれを一時停止または再開します。

2023年4月

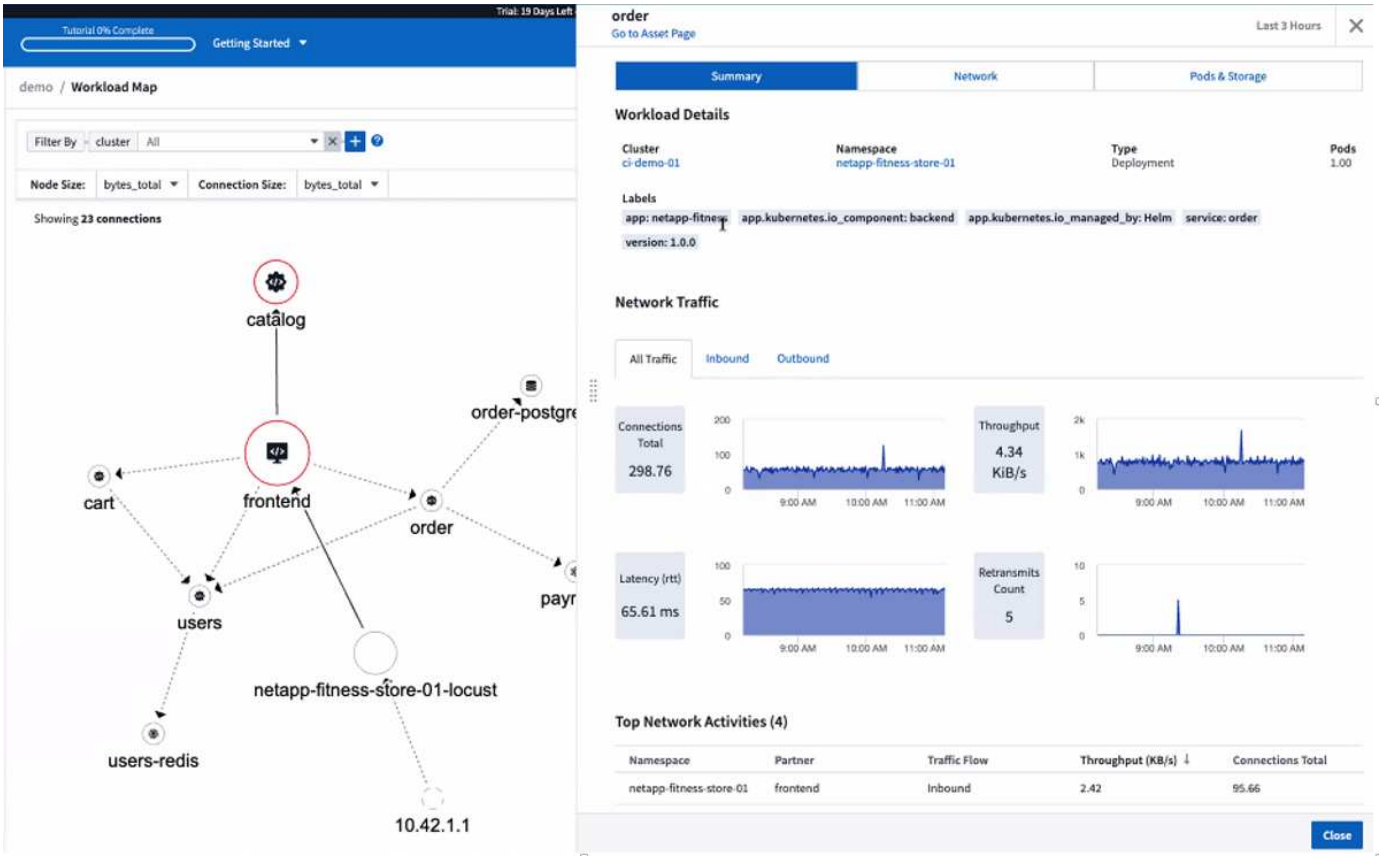
Kubernetesのパフォーマンス監視とマッピング

。 *"Kubernetesのネットワークパフォーマンスとマップ"* Kubernetesワークロード間の依存関係をマッピングすることで、トラブルシューティングを簡易化します。Kubernetesのネットワークパフォーマンスのレイテンシや異常をリアルタイムで可視化し、ユーザに影響が及ぶ前にパフォーマンスの問題を特定します。
この機能は、Kubernetesのトラフィックフローを分析、監査することで全体的なコストを削減するのに役立ちます。

主な特長：
•ワークロードマップは、Kubernetesワークロードの依存関係とフローを示し、ネットワークとパフォーマンスの問題を明らかにします。
•Kubernetesポッド、ワークロード、ノード間のネットワークトラフィックを監視し、トラフィックとレイテ

ンシの問題の原因を特定します。
•入力、出力、リージョン間、ゾーン間のネットワークトラフィックを分析することで、全体的なコストを削減します。

「スライドアウト」の詳細を示すワークロードマップ：

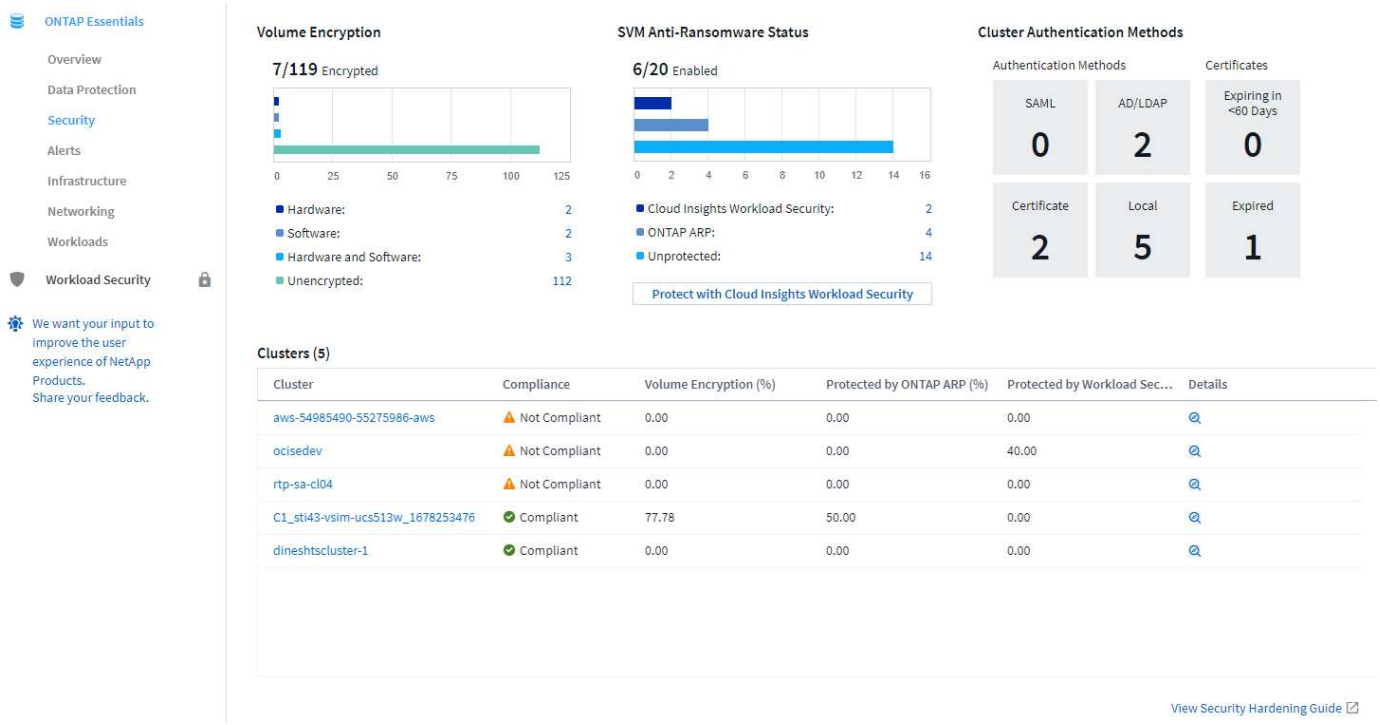


パネルと詳細を示すワークロードマップの例"]

Kubernetesのパフォーマンスの監視とマップは、として使用できます "プレビュー（ Preview ）" フィーチャー（ Feature ）：

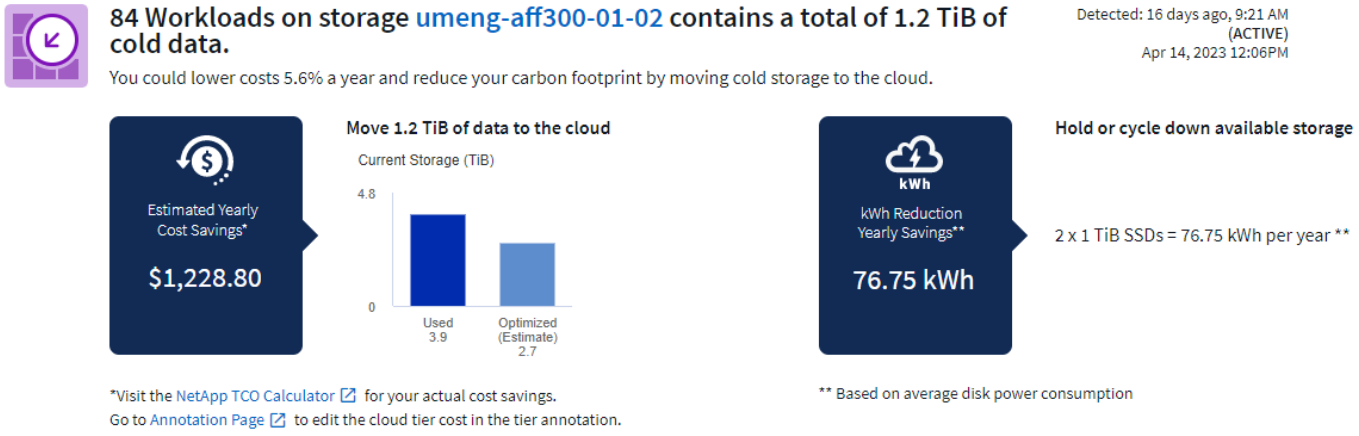
ONTAP Essentialsセキュリティダッシュボード

。 "セキュリティダッシュボード" では、現在のセキュリティ状況を瞬時に把握でき、ハードウェアとソフトウェアのボリューム暗号化、ランサムウェア対策のステータス、クラスタの認証方法をグラフで確認できます。セキュリティダッシュボードは、として使用できます "プレビュー（ Preview ）" フィーチャー（ Feature ）：



ONTAP コールドストレージを再利用します

ONTAP コールドストレージの再利用_Insightは、ONTAP システム上のボリュームについて、コールド容量、潜在的なコスト/電力削減、推奨される対処方法に関するデータを提供します。



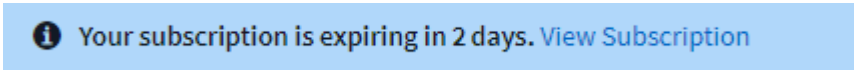
このインサイトでは、次のような質問を回答 できます。

- ストレージクラスタ上のコールドデータの量は、（a）高コストのSSDディスク、（b）HDDディスク、（c）仮想ディスクにどれくらいありますか？
- 最適化されていないストレージに関して、最も影響を与えているワークロードは何ですか？
- 特定のワークロードでデータがコールドである期間（日数）

Reclaim ONTAP コールドストレージ_はとみなされます "_プレビュー" このため、機能は変更される場合があります。

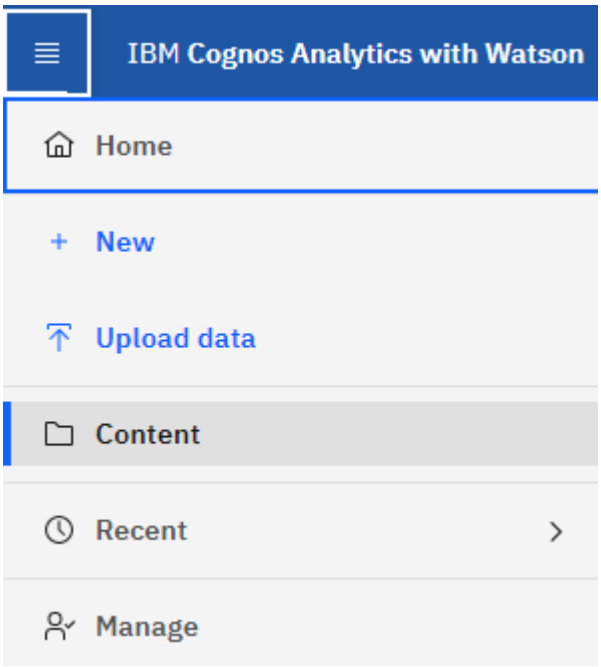
サブスクリプション通知はバナーメッセージも制御します

サブスクリプション通知の受信者を設定する（[Admin]>[Notifications]）では、サブスクリプション関連の製品内バナー通知を表示するユーザも制御できるようになりました。



レポート機能の外観が一新されました

Cloud Insights レポート画面の外観が新しくなり、メニューナビゲーションの一部が変更されていることがわかります。これらの画面とナビゲーションの変更は、現在のバージョンで更新されています "レポートドキュメント"。



モニタはデフォルトで一時停止されています

新しいCloud Insights 環境の場合は、次の点に注意してください "システム定義のモニタ" デフォルトではアラート通知は送信しません。モニタに1つ以上の配信方法を追加して、アラートを通知するモニタの通知を有効にする必要があります。
既存のCloud Insights 環境では、現在_Paused_stateにあるシステム定義モニタのdefault_global_notification受信者リストが削除されました。現在アクティブなシステム定義モニターの通知設定と同様に、ユーザー定義通知も変更されません。

[API Metering]タブをお探しですか？

APIメーターは、[サブスクリプション]ページから*[管理者]>[APIアクセス]ページに移動しました。

2023年3月

Cloud Connection for ONTAP 9.9以降は廃止されました

Cloud Connection for ONTAP 9.9以降のデータコレクタは廃止されました。 2023年4月4日以降、環境内のCloud Connectionデータコレクタでデータが収集されなくなり、ポーリング時にエラーが表示されます。Cloud Connectionデータコレクタは、次回の更新でCloud Insights から完全に削除されます。

2023年4月4日より前のリリースでは、クラウド接続で現在収集されているすべてのONTAP システムについて、新しいNetApp ONTAP データ管理ソフトウェアデータコレクタを設定する必要があります。 "詳細はこちら。"。

2023年1月

新しいログモニタ

私達は約ダースを加えた "追加のシステムモニタ" インターコネクトリンクの切断、ハートビートの問題などに関するアラートを送信します。また、SnapMirrorの自動再同期、MetroCluster ミラーリング、FabricPool ミラー再同期の変更に関するアラートを通知するために、3つの新しいデータ保護ログモニタが追加されました。

これらのモニタの一部はデフォルトで_enabled_byになっています。これらのモニタにアラートを送信しない場合は、_pause_themを実行する必要があります。また、これらのモニタは通知を配信するように設定されていないことに注意してください。電子メールまたはWebフックでアラートを送信する場合は、これらのモニタで通知の受信者を設定する必要があります。

すべてのダッシュボードテーブルウィジェットの.csvエクスポート

データへのアクセスを確保することは不可欠です。 CSVエクスポートは、クエリするデータのタイプ（アセットや統合）に関係なく、すべての指標クエリ、ダッシュボード表ウィジェット、オブジェクトランディングページで使用できます。

列の選択、列の名前変更、単位変換などのデータのカスタマイズも、新しいエクスポート機能に含まれるようになりました。

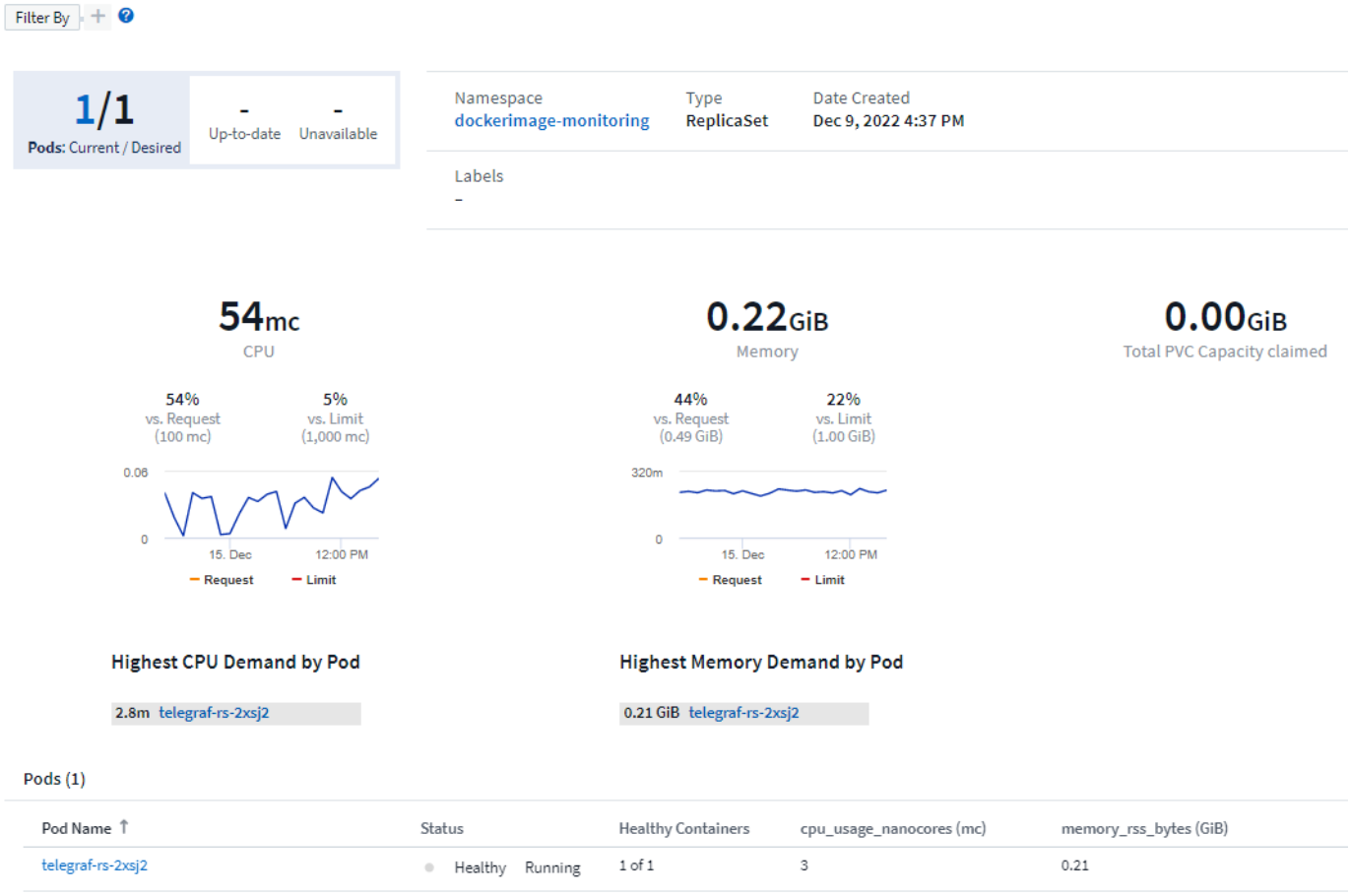
2022年12月

Cloud Insights トライアルでランサムウェア防御やその他のセキュリティ機能をご確認ください

本日より、Cloud Insights の新しいトライアル版に登録することで、ランサムウェア検出や自動化されたユーザーブロック応答ポリシーなどのセキュリティ機能を調べることができます。トライアルにサインアップしていない場合は、今すぐお試しください。

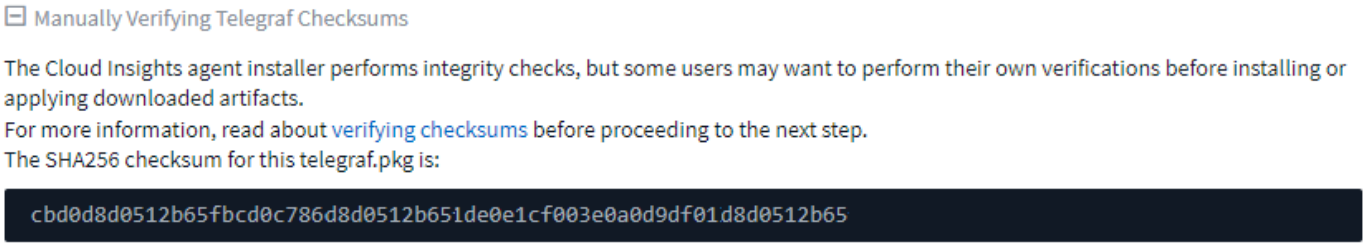
Kubernetesワークロードには独自のランディングページがあります

ワークロードはKubernetes環境の重要な要素であるため、Cloud Insights はこれらのワークロードのランディングページを提供できるようになりました。ここから、Kubernetesワークロードに影響する問題を表示、調査、トラブルシューティングできます。



チェックサムをチェックしてください

WindowsおよびLinux用のエージェントのインストール中にチェックサム値を提供するように依頼されましたが、これは素晴らしいアイデアだと思います。ここには次のようなものがあります

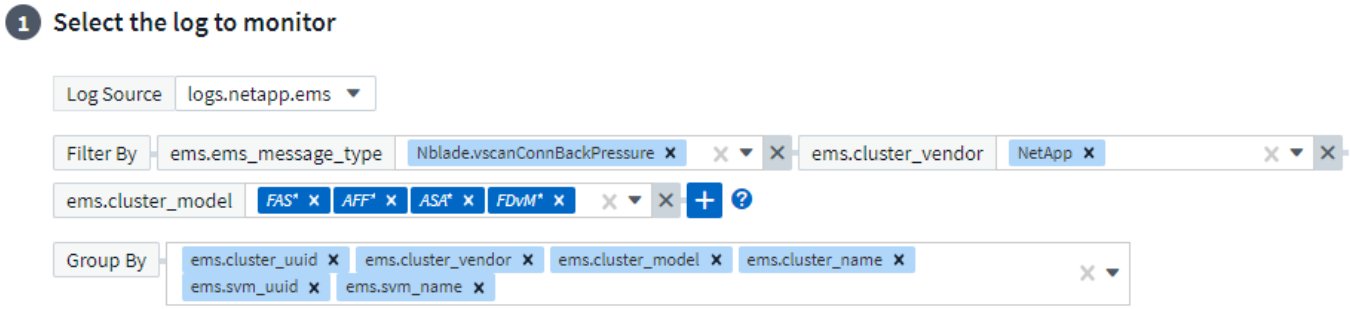


ログ・アラートの改善

グループ化

ログモニタを作成または編集するときに、「グループ化」属性を設定して、より集中的なアラートを生成でき

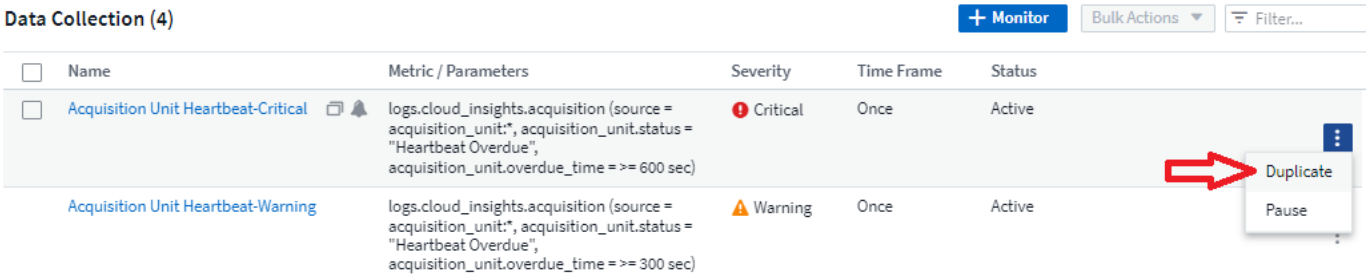
るようになりました。モニタ定義の「フィルタ」設定の下にある「グループ化」属性を探します。



この変更により、メトリックモニタとログモニタは、モニタ定義の「グループ化基準」の部分を正規化することで機能パリティになります。このパリティにより、お客様は、システム定義のすべての*システム定義デフォルトモニターのクローン/複製を作成して、さらにカスタマイズすることができます。

複製

これで、変更ログ、Kubernetesログ、およびData Collectorログモニタを複製（複製）できるようになりました。これにより、新しいカスタムログモニタが作成され、特定の定義に変更できます。



11 SnapMirrorを対象としたビジネス継続性を実現する、新しいデフォルトのONTAP モニタ

私たちは、10個近くの新しい製品を追加しました "システムモニタ" SnapMirror for Business Continuity（SMBC）については、SMBC証明書およびONTAP メディエーターの変更を通知します。

2022年11月

40以上の新しいセキュリティ、データ収集、CVOの監視が追加されました！

Cloud Volume 、セキュリティ、およびデータ保護に関する潜在的な問題を警告するために、システム定義の新しいモニターが多数追加されました。これらのモニターの詳細については、こちらをご覧ください "こちらをご覧ください"。

2022年10月

ONTAP の自律的ランサムウェア防御統合によるランサムウェア検出の精度と精度の向上

Cloud Secure は、ONTAP との統合を通じてランサムウェアの検出を改善します "自律的なランサムウェア防御" （ARP）。

Cloud Secure は、潜在的なボリュームファイル暗号化アクティビティでONTAP ARPイベントを受信します

- ボリューム暗号化イベントとユーザアクティビティを関連付けて、破損の原因となっているユーザを特定する。
- 攻撃をブロックする自動応答ポリシーを実装します。
- 影響を受けたファイルを特定し、迅速なリカバリとデータ侵害の調査に役立ちます。

2022年9月

Basic Editionで使用可能なモニタ

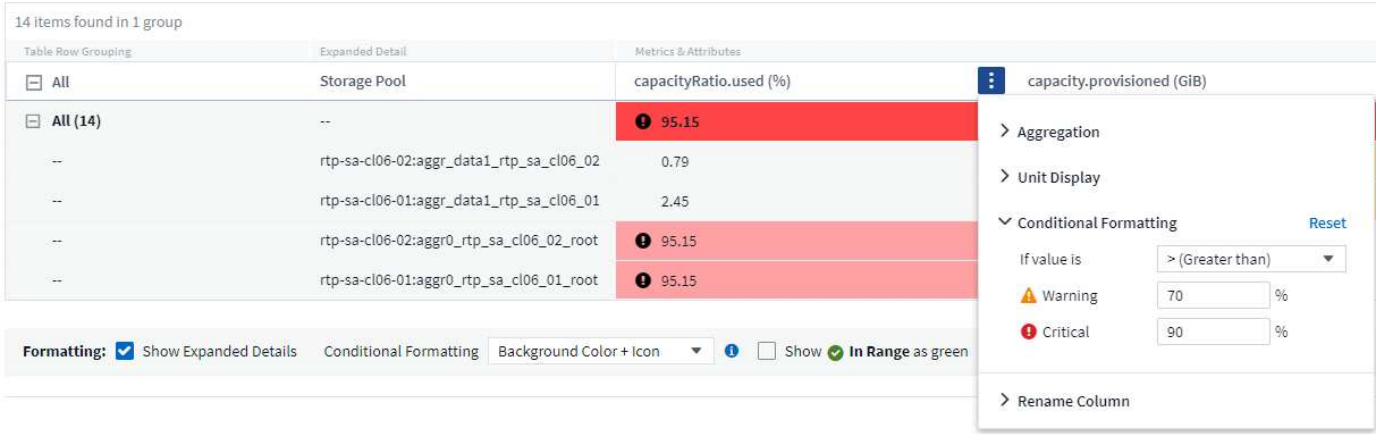
ONTAP "デフォルトのモニタ" Cloud Insights Basic Editionで使用できるようになりました。これには、70を超えるインフラ監視と30のワークロード例が含まれます。

ONTAP PowerダッシュボードとStorageGRID ダッシュボード

ダッシュボードギャラリーには、ONTAP 電源と温度の新しいダッシュボードと、StorageGRID 用の4つのダッシュボードが含まれています。ONTAP の電力測定基準やStorageGRID データを収集している環境では、[*+ from Gallery]を選択して、これらのダッシュボードをインポートします。

しきい値が表形式で一目でわかるようにします

条件付き書式を使用すると、表ウィジェットで警告レベルと重大レベルのしきい値を設定して強調表示し、異常なデータポイントを瞬時に可視化できます。

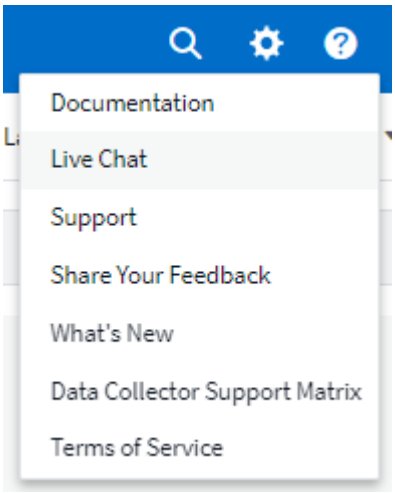


Security Monitorサービスの略

Cloud Insights では、ONTAP システムでFIPSモードが無効になっていることが検出されるとアラートが生成されます。詳細については、をご覧ください "システムモニタ"にアクセスして、この領域をご覧ください。近日公開予定のセキュリティモニターがさらに増えます。

どこからでもチャットできます

新しい* Help > Live Chat *リンクを選択すると、任意のCloud Insights 画面からネットアップサポートスペシャリストとチャットできます。ヘルプはから入手できます。 アイコンをクリックします。



より目に見える洞察

環境でが使用されている場合 "インサイト" Spress_or_Kubernetes名前空間の_共有リソースのように、影響を受けるリソースのアセットランディングページには、Insight自体へのリンクが含まれるようになり、探索とトラブルシューティングが迅速になりました。

新しいデータコレクタ

- Amazon S3（プレビュー版）
- Brocade FOS 9.0.x
- Dell/EMC PowerStore 3.0.0.0

Data Collector のその他のアップデート

これで、すべてのデータソースが最適化され、Acquisition Unitの更新やパッチの適用後にパフォーマンスのポーリングが再開されるようになりました。

オペレーティングシステムのサポート

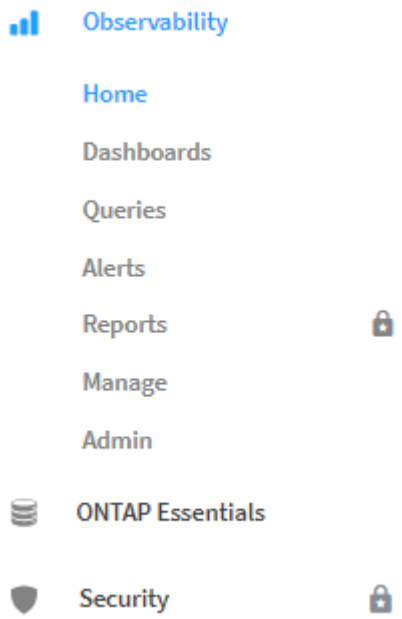
Cloud Insights Acquisition Unitでサポートされるオペレーティングシステムは次のとおりです "すでにサポートされています"：

- Red Hat Enterprise Linux 8.5、8.6

2022年8月

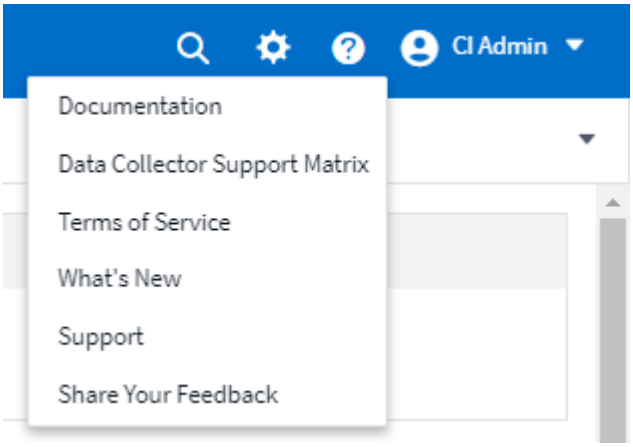
Cloud Insights の外観は新しくなっています。

今月から、「モニターと最適化」という名称が「観察性」に変更されました。ダッシュボード、クエリ、アラート、レポートなど、お気に入りの機能がすべてここに表示されます。また、新しい「セキュリティ」メニューで「Cloud Secure 」を探します。メニューのみが変更されています。機能は変更されていません。



「ヘルプ」メニューを検索していますか？

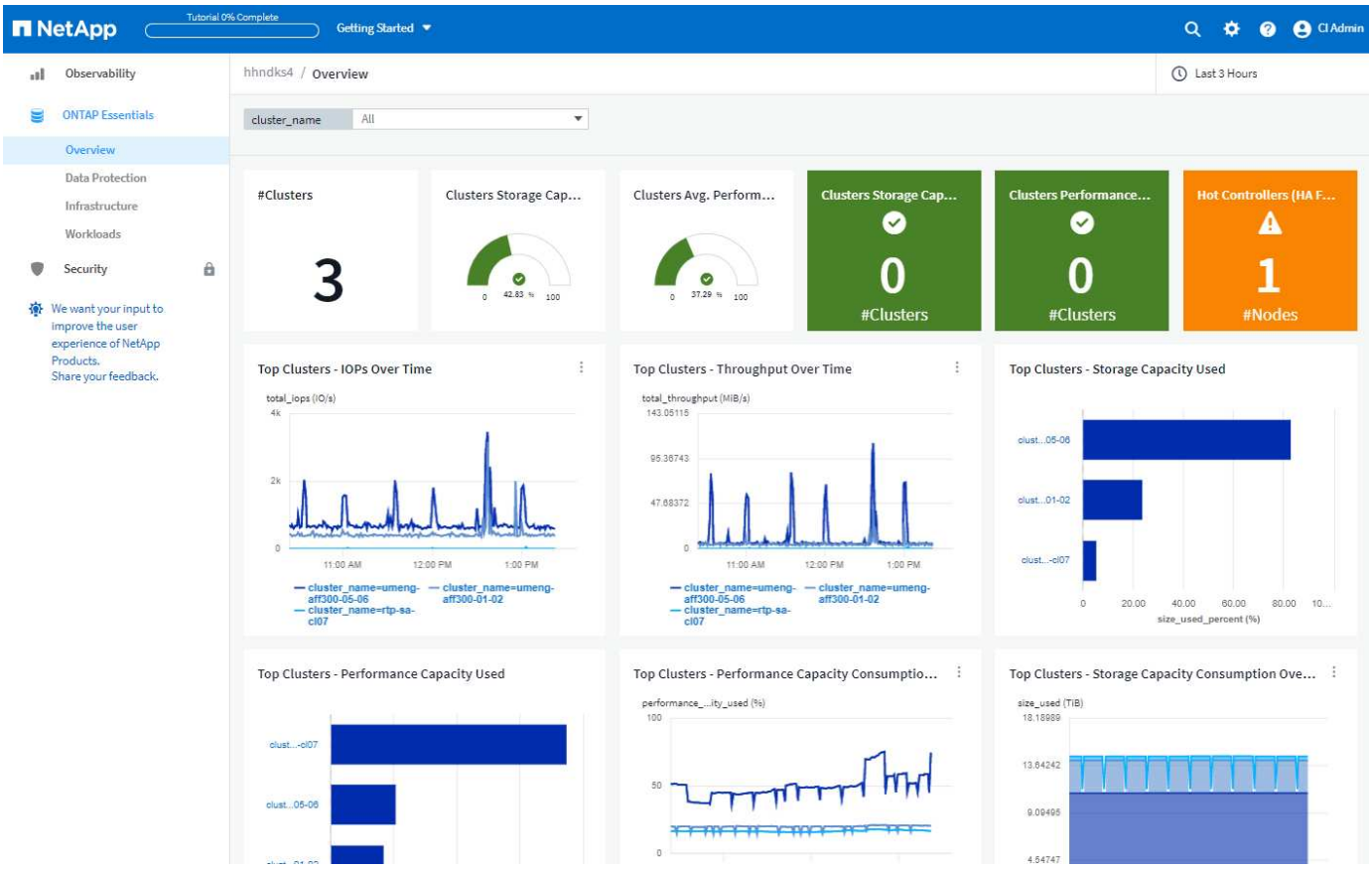
画面の右上に表示されるようになりました。



どこから始めるべきかわからない場合は、ONTAP の基礎を確認してください。

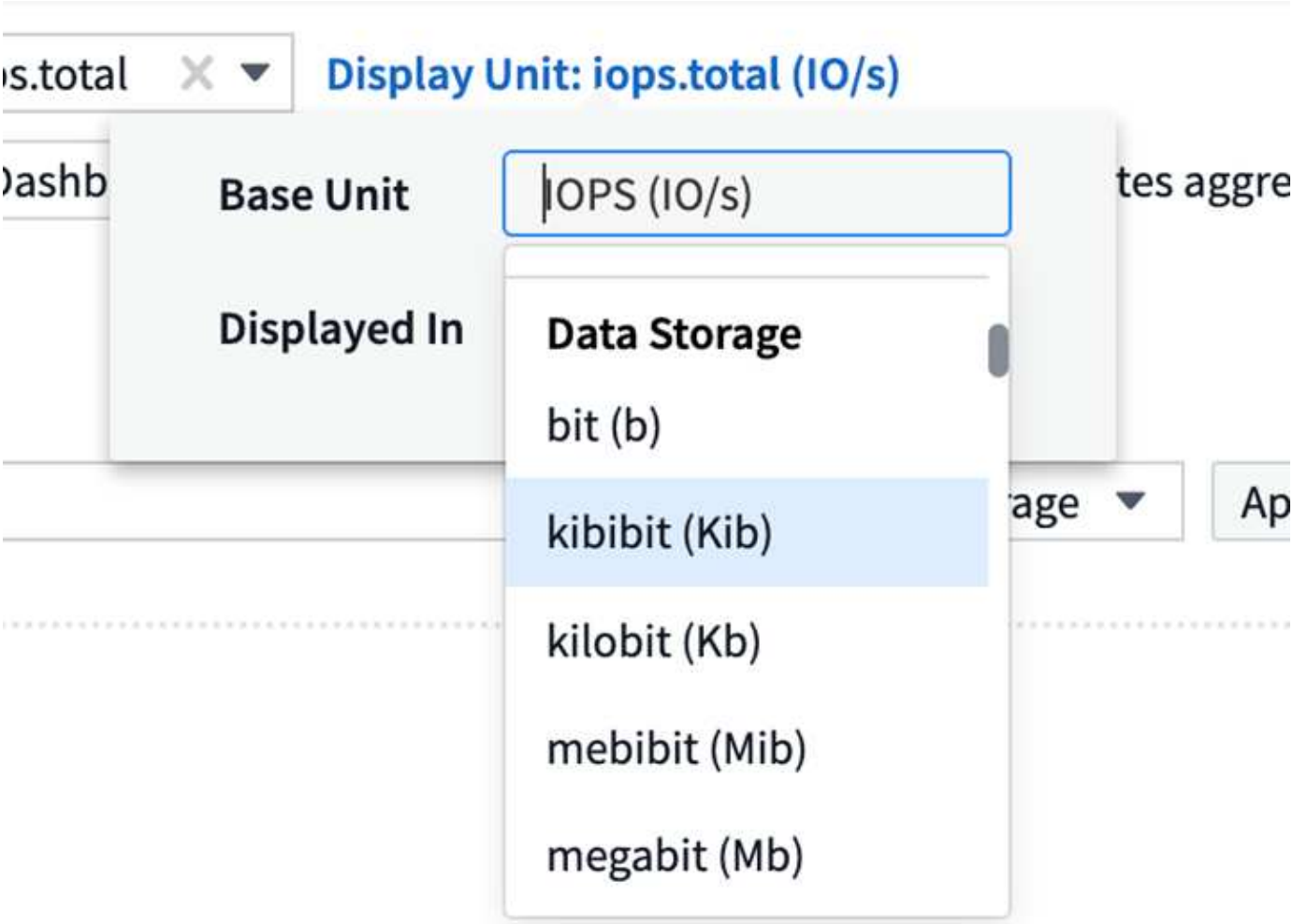
"* ONTAP Essentials *" は、NetApp ONTAP のインベントリ、ワークロード、データ保護に関する詳細なビューを提供する一連のダッシュボードとワークフローで、ストレージ容量やパフォーマンスを日々予測することもできます。利用率の高いコントローラが稼働しているかどうかを確認することもできます。ONTAP Essentialsは、ネットアップONTAP のすべての監視ニーズに最適な環境です。

ONTAP Essentialsは、すべてのエディションで利用可能です。既存のONTAP オペレータや管理者が直感的に操作できるように設計されており、ActiveIQ Unified Managerからサービスベースの管理ツールへの移行を容易にします。



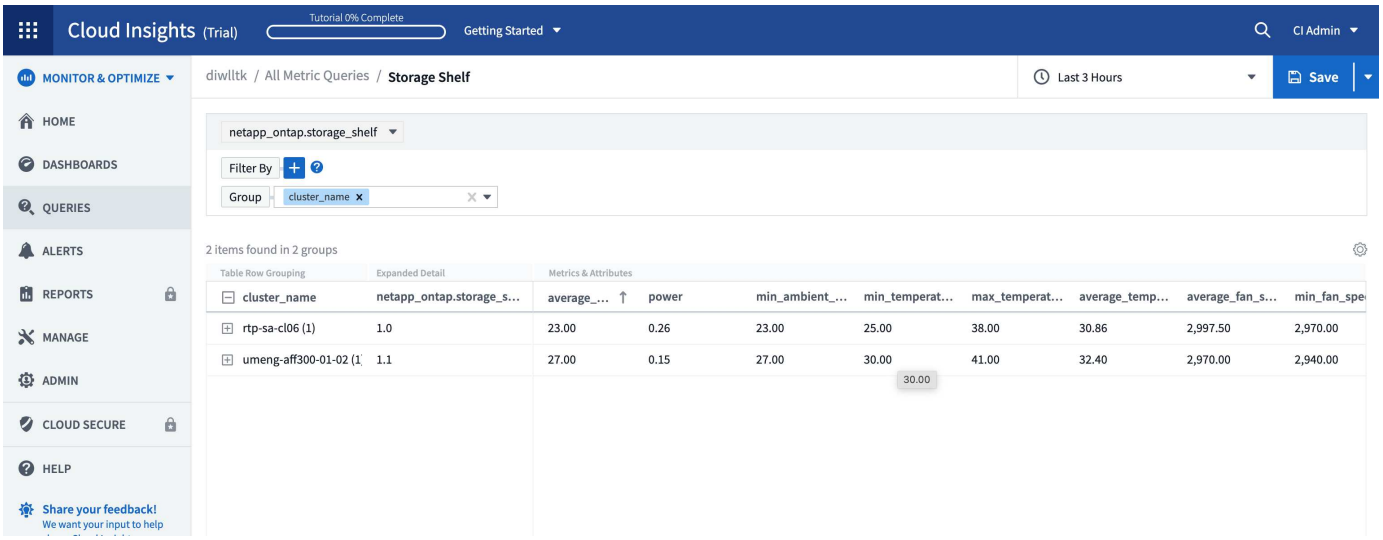
ストレージデータファミリーはマージされます

それを求められて、今それを持っている。ストレージ2および10進数のデータ単位が、ビットとバイトからテビッツやテラバイトに至る1つのファミリーに統合され、ダッシュボードにデータを簡単に表示できるようになりました。また、データレートは、現在では大きなファミリーの1つとなっています。



ストレージで使用されている電力量

netapp_ontap.storage_shelf、netapp_ontap.system_node、netapp_ontap.clusterの各指標を使用して、ONTAPストレージシェルフとノードの消費電力、温度、ファン速度を表示および監視します（消費電力のみ）。



プレビューからサイズ変更されたフィーチャー

次の機能がプレビューから除外され、すべてのお客様が利用できるようになりました。

* 特徴 *	* 概要 *
Kubernetesネームスペースのスペースが不足しています	Space_Insightで実行されている_Kubernetes名前空間では'容量不足のリスクがあるKubernetesネームスペース上のワークロードを確認できます各スペースがフルになるまでに推定される残り日数を確認できます "詳細はこちら"
応力の下の共有リソース	Stress_INSIGHTの_Shared Resourceは、AI/MLを使用して、リソース競合が環境におけるパフォーマンス低下の原因となっている場所を自動的に特定し、影響を受けたワークロードを強調表示し、推奨される対処方法を提供してパフォーマンスの問題をより迅速に解決します。 "詳細はこちら"
Cloud Secure –攻撃に対するユーザアクセスをブロックします	攻撃が検出されたときにユーザーアクセスをブロックする機能により、ビジネスクリティカルなデータの保護を強化できます。 アクセスは、自動応答ポリシーを使用して自動的にブロックすることも、アラートまたはユーザの詳細ページから手動でブロックすることもできます。 "詳細はこちら"

データ収集の健全性

Cloud Insights には、Acquisition Unit用に2つの新しいハートビートモニタと、データコレクタの障害を通知する2つのモニタが用意されています。これらのコマンドを使用すると、データ収集の問題を迅速に通知できます。

Data Collection_monitorグループで次のモニタを使用できるようになりました。

- Acquisition Unit Heartbeat - Criticalをクリックします

- Acquisition Unit Heartbeat -警告
- コレクタでエラーが
- コレクタ警告

デフォルトでは、これらのモニタは_Paused _状態になっています。アラートをアクティブ化すると、データ収集の問題に関するアラートが表示されます。

APIトークンの自動更新

APIアクセストークンを自動更新に設定できるようになりました。この機能を有効にすると、期限切れトークン用に新しい/更新されたAPIアクセストークンが自動的に生成されます。期限切れトークンを使用しているCloud Insights エージェントは、対応する新規または更新されたAPIアクセストークンを使用するように自動的に更新されるため、シームレスな運用を継続できます。トークンを作成するときは、［トークンを自動的に更新］チェックボックスをオンにします。この機能は、現在のところ、Kubernetesプラットフォームで実行されているCloud Insights エージェントと最新のNetApp Kubernetes Monitoring Operatorでサポートされています。

Basic Editionは、これまで以上に多くの機能を提供します

トライアルは終了していますが、サブスクリプションがお客様に適しているかどうかまだ確認されていませんか？Basic Editionでは、現在のONTAP データコレクタでCloud Insights を引き続き使用できますが、VMwareのバージョン、トポロジ、およびIOS/Throughput / Latencyのデータも引き続きキャプチャできます。ストレージシステムでプレミアムサポートを受けているネットアップのお客様も、Cloud Insights のサポートを受けることができます。

詳細を確認する準備はできましたか？

ヘルプ>サポートページの「*ラーニングセンター」セクションで、NetApp University Cloud Insights コースへのリンクを確認できます。

オペレーティングシステムのサポート

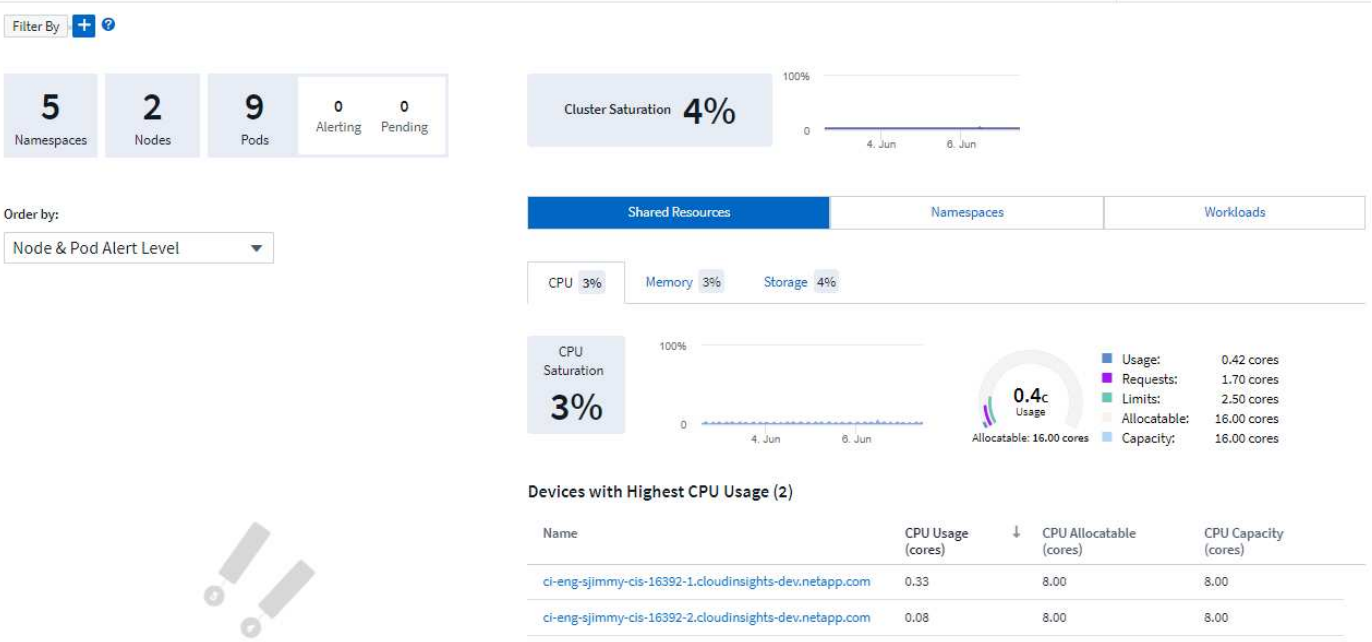
Cloud Insights Acquisition Unitでは、さらに次のオペレーティングシステムがサポートされます "すでにサポートされています"：

- Windows 11の場合

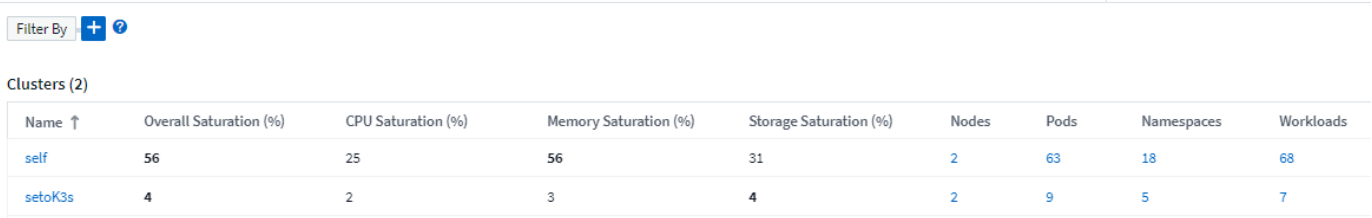
2022年6月

Kubernetesのクラスタの飽和などの詳細情報

Cloud Insights を使用すると、Kubernetes環境の調査がこれまでになく簡単になります。このページでは、彩度の詳細だけでなく、ネームスペースとワークロードをより明確に表示する、クラスタの詳細ページが改善されています。

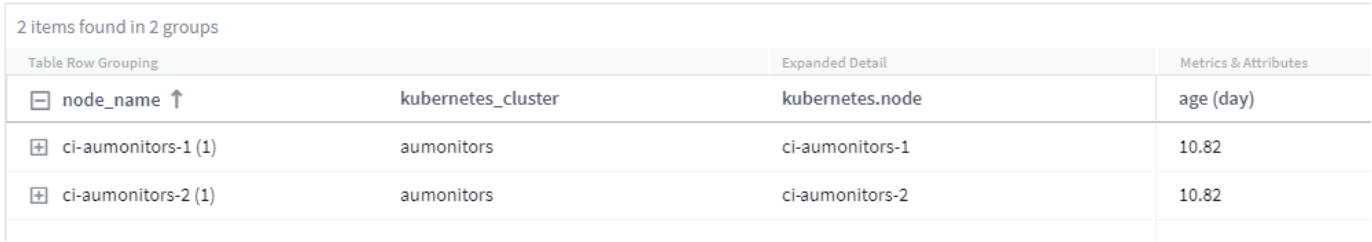


クラスタリストページでは、ノード、ポッド、ネームスペース、ワークロードの数に加えて、飽和状態の情報も簡単に確認できます。



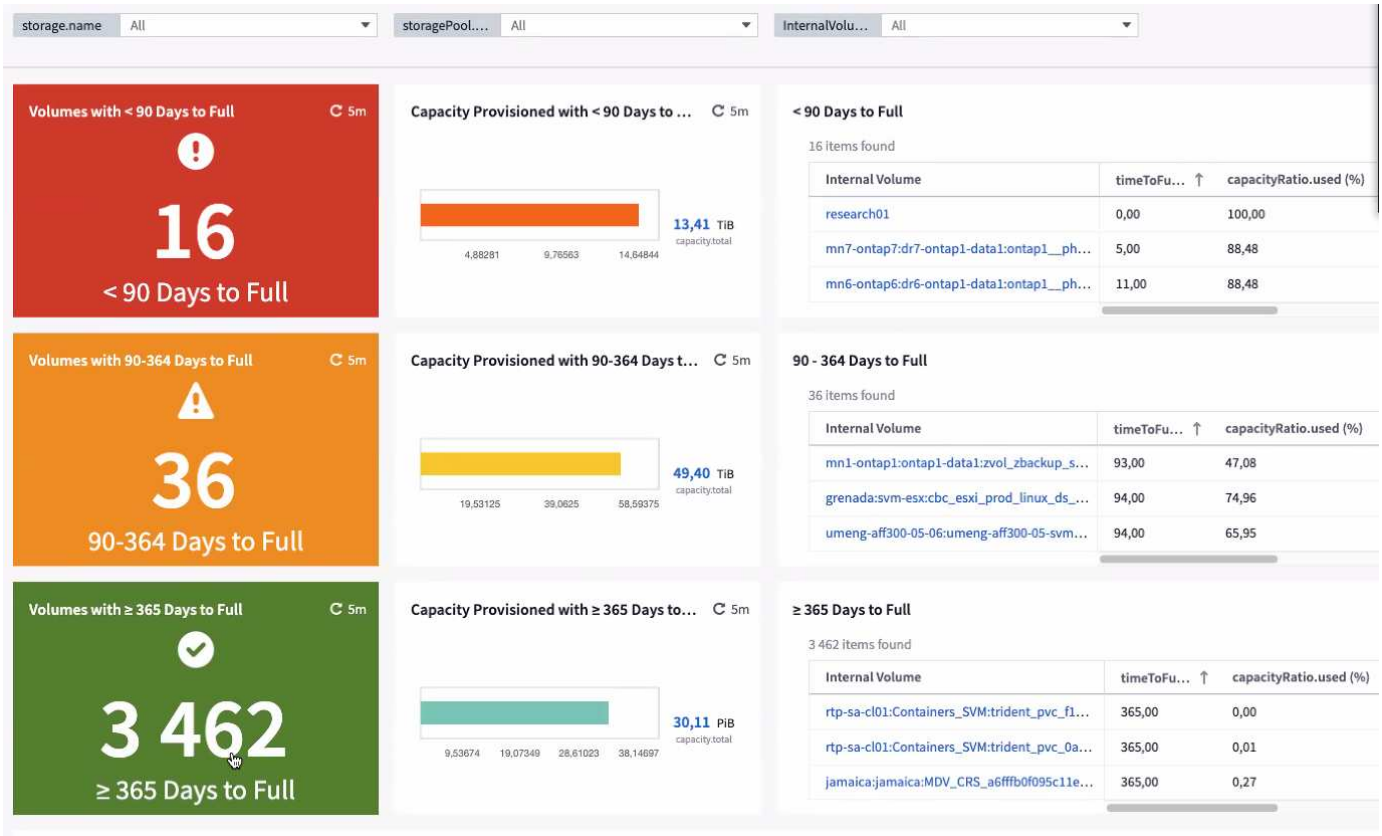
Kubernetesクラスタはどれくらい前ですか？

クラスタは世界で始まったばかりですか？それとも長いデジタルライフを体験したことがありますか？_Ageは、Kubernetesノードについて収集された時間メトリックとして追加されました。



容量のフルまでの時間予測

Cloud Insights は、監視対象の各内部ボリュームの容量がなくなるまでの日数を予測するダッシュボードを提供します。これらの値を設定することで、システム停止のリスクを大幅に軽減できます。

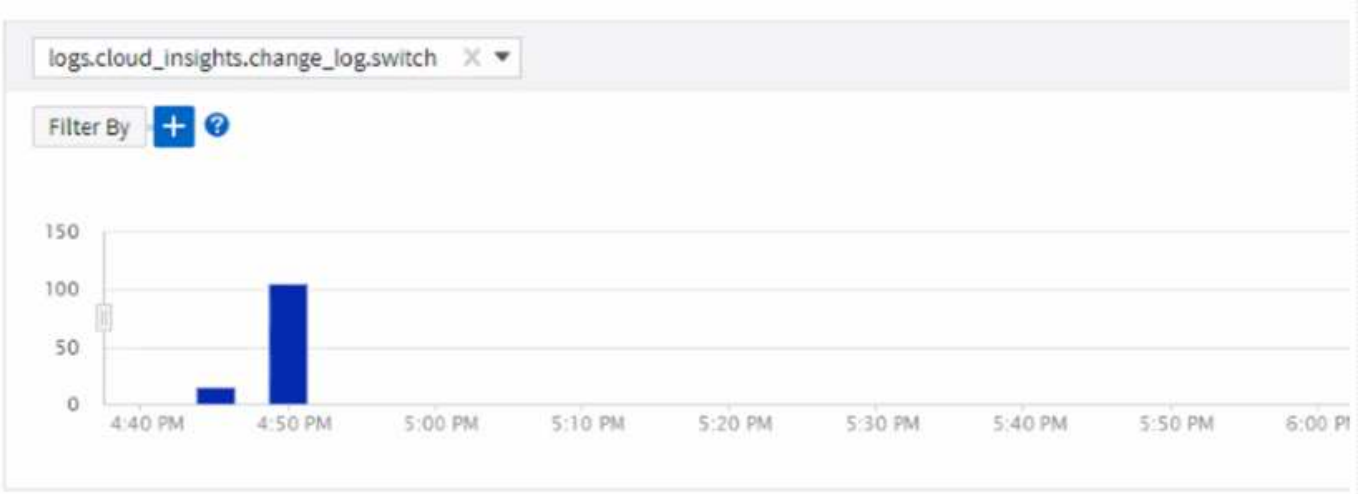


TTFカウンタは'ストレージ'ストレージ・プール'ボリュームにも使用できますこれらのオブジェクト用にダッシュボードが追加されるように、このスペースを監視してください。

Time to Fullの予測は_Preview_から移動し、すべての顧客に展開されます。

環境の変化

ONTAP 変更ログのエントリは、ログエクスプローラで確認できます。



Log Entries

timestamp	name	object_type	message
06/08/2022 4:52:51 PM	fc19	Port	Port with name:fc19 has been created
06/08/2022 4:52:51 PM	fc20	Port	Port with name:fc20 has been created
06/08/2022 4:52:51 PM	fc23	Port	Port with name:fc23 has been created
06/08/2022 4:52:51 PM	fc22	Port	Port with name:fc22 has been created

オペレーティングシステムのサポート

Cloud Insights Acquisition Unitでサポートされるオペレーティングシステムは次のとおりです "すでにサポートされています"：

- CentOSストリーム9.
- Windows 2022

Telegraf Agent を更新

テレグラム統合データの取り込みのためのエージェントがバージョン*1.22.3*に更新され、性能とセキュリティが向上しました。
更新を希望するユーザーは、の適切なアップグレードセクションを参照できます "エージェントのインストール" ドキュメント
以前のバージョンのエージェントは、ユーザの操作を必要とせずに引き続き機能します。

フィーチャーのプレビュー（ Preview Features

Cloud Insights では、多数のエキサイティングなプレビュー機能が定期的にハイライトされています。これらの機能をプレビューする場合は、にお問い合わせください "ネットアップの営業チーム" を参照してください。

* 特徴 *	* 概要 *

Kubernetesネームスペースのスペースが不足しています	Space_Insightで実行されている_Kubernetes名前空間では'容量不足のリスクがあるKubernetesネームスペース上のワークロードを確認できます各スペースがフルになるまでに推定される残り日数を確認できます "詳細はこちら"
Cloud Secure –攻撃に対するユーザアクセスをブロックします	攻撃が検出されたときにユーザーアクセスをブロックする機能により、ビジネスクリティカルなデータの保護を強化できます。 アクセスは、自動応答ポリシーを使用して自動的にブロックするか、アラートまたはユーザの詳細ページから手動でブロックできます。 "詳細はこちら"
応力の下の共有リソース	Stress_INSIGHTの_Shared Resourceは、AI/MLを使用して、リソース競合が環境におけるパフォーマンス低下の原因となっている場所を自動的に特定し、影響を受けたワークロードを強調表示し、推奨される対処方法を提供してパフォーマンスの問題をより迅速に解決します。 "詳細はこちら"

2022年5月

ネットアップサポートとチャットでライブチャットできます

ネットアップのサポート担当者とライブチャットできます。 [ヘルプ]>[サポート]ページで、[チャット]アイコンをクリックするか、[お問い合わせ]セクションの_Chat_をクリックしてチャットセッションを開始します。チャットサポートは、米国の平日にStandard EditionおよびPremium Editionユーザが利用できます。

Kubernetesオペレータ

Cloud Insights の高度なKubernetes監視機能とクラスタエクスプローラを使用すると、作業を簡単に開始できます。

。 "Kubernetes監視オペレータ" （NKMO）は、Kubernetes for Cloud Insights Insightsをインストールする際に推奨される方法です。より柔軟な構成で、より少ない手順で監視を行うことができます。また、Kubernetesクラスタ内で実行されている他のソフトウェアを監視する機会も強化されています。

詳細と前提条件については、上のリンクをクリックしてください

APIを使用してユーザと招待を管理します

Cloud Insights の強力なAPIを使用して、ユーザと招待を管理できるようになりました。詳細については、を参照してください "API Swaggerドキュメント"。

データ収集アラート

コレクタに失敗したため、重要なメトリックをお見逃しなく！

データコレクタをこれまで以上に簡単に追跡できるようになりました "アラート" データコレクタとAcquisition Unitの障害
デフォルトでは、これらのモニタは_Paused _です。有効にするには、お使いのモニタのページに移動し、「Acquisition Unit Shutdown」および「Collector Failed」を探して再開します。

ONTAP ストレージの変更に関するアラート

ストレージの予期しない変更がシステム停止につながるのを避けましょう。

ONTAP システムでFlexVol、ノード、およびSVMの変更や削除が検出されたときにアラートを受け取るようにCloud Insights を設定できるようになりました。

フィーチャーのプレビュー（ Preview Features

Cloud Insights では、多数のエキサイティングなプレビュー機能が定期的にハイライトされています。これらの機能をプレビューする場合は、にお問い合わせください "ネットアップの営業チーム" を参照してください。

* 特徴 *	* 概要 *
Kubernetesネームスペースのスペースが不足しています	Space_Insightで実行されている_Kubernetes名前空間では'容量不足のリスクがあるKubernetesネームスペース上のワークロードを確認できます各スペースがフルになるまでに推定される残り日数を確認できます "詳細はこちら"
内部ボリュームとボリューム容量のフル予測	Cloud Insights は、監視対象の各内部ボリュームおよびボリュームの容量がなくなるまでの日数を予測できます。この値を設定することで、システム停止のリスクを大幅に軽減できます。
Cloud Secure –攻撃に対するユーザアクセスをブロックします	攻撃が検出されたときにユーザーアクセスをブロックする機能により、ビジネスクリティカルなデータの保護を強化できます。 アクセスは、自動応答ポリシーを使用して自動的にブロックするか、アラートまたはユーザの詳細ページから手動でブロックできます。 "詳細はこちら"

応力の下の共有リソース	Stress_INSIGHTの_Shared Resourceは、AI/MLを使用して、リソース競合が環境におけるパフォーマンス低下の原因となっている場所を自動的に特定し、影響を受けたワークロードを強調表示し、推奨される対処方法を提供してパフォーマンスの問題をより迅速に解決します。 "詳細はこちら"

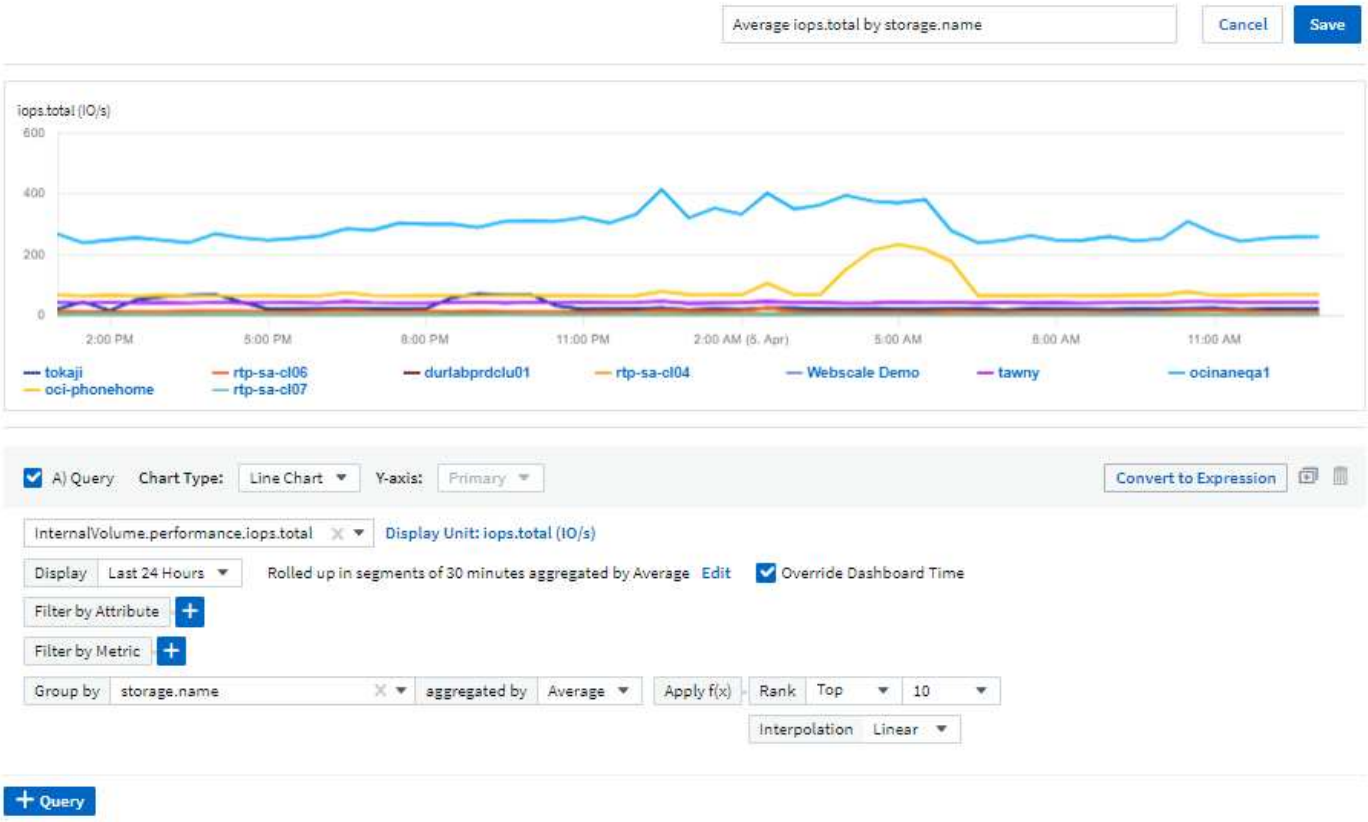
2022年4月

フィードバックを共有してください。

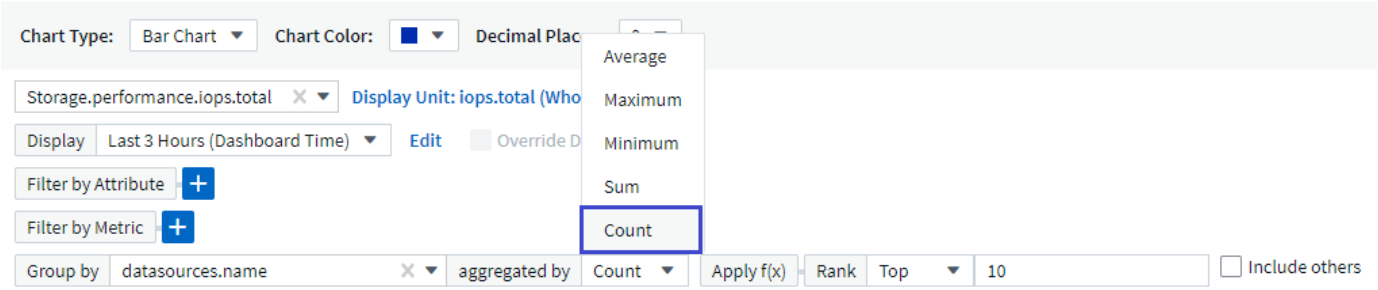
Cloud Insights の形成に役立つ情報をご用意しました。ネットアップの「 Insights to Action 」プログラムに参加すると、ポイントや賞品を獲得できます。 "* 今すぐ登録 *" ！

ダッシュボードエディタが更新されました

ダッシュボード作成ツールを徹底的に見直し、データをより迅速に視覚化できるようにしました。Cloud Insights の [ダッシュボード] ページに移動して、既存のダッシュボードを編集したり、ダッシュボードギャラリーから追加したり、独自のダッシュボードを作成してチェックアウトしたりできます。



また、新しい Count 集約方式も導入されています。 棒グラフ、棒グラフ、円グラフ、円グラフの各ウィジェットでデータをグループ化すると、選択した指標の関連オブジェクトの数をすばやく簡単に表示できます。



を示す [Aggregation] ドロップダウン"]

また、折れ線グラフで 3 つのうちの 1 つを選択できるようになりました "補間" 方法：

- なし - 補間は行われません
- 線形 - 既存の点間のデータポイントを補間します
- 階段（ Stair ） - 前のデータ点を補間されたデータ点として使用します

Kubernetes インフラの監視機能が強化されました

Cloud Insights では、ポッド、デモ onset 、 ReplicaSets が作成または削除されたとき、および新しい展開が作成されたときにアラートを生成することで、 Kubernetes 環境の変更に優先的に対応します。Kubernetes ではデフォルトのステータスが _paused_state に監視されるため、必要なものだけを有効にする必要があります。

フィーチャーのプレビュー（ Preview Features

Cloud Insights では、多数のエキサイティングなプレビュー機能が定期的にハイライトされています。これらの機能をプレビューする場合は、にお問い合わせください "ネットアップの営業チーム" を参照してください。

* 特徴 *	* 概要 *
内部ボリュームとボリューム容量のフル予測	Cloud Insights は、監視対象の各内部ボリュームおよびボリュームの容量がなくなるまでの日数を予測できます。この値を設定することで、システム停止のリスクを大幅に軽減できます。
Cloud Secure –攻撃に対するユーザアクセスをブロックします	攻撃が検出されたときにユーザーアクセスをブロックする機能により、ビジネスクリティカルなデータの保護を強化できます。 アクセスは、自動応答ポリシーを使用して自動的にブロックするか、アラートまたはユーザの詳細ページから手動でブロックできます。 "詳細はこちら"
応力の下の共有リソース	Stress Insight の共有リソースでは、 AI/ML を使用して、リソース競合が環境におけるパフォーマンス低下の原因となっている場所を自動的に特定し、影響を受けたワークロードを強調表示し、推奨される対処方法を提供して、パフォーマンスの問題をより迅速に解決します。 "詳細はこちら"

新しい **Data Collector**

- * Cohesity SmartFiles *-このREST APIベースのコヒリティ・クラスターを取得して、「ビュー」（CI内部ボリューム）、各種ノード、パフォーマンスメトリックの収集を行います。

Data Collector のその他のアップデート

次のデータコレクタでのパフォーマンスデータの収集と表示が改善されました。

- Brocade CLI
- Dell/EMC VPLEX 、 PowerStore 、 Isilon / PowerScale 、 VNX Block / Clariion CLI 、 XtremIO 、 Unity/VNXe
- Pure FlashArray

これらのパフォーマンス強化機能は、 VMware や Cisco のほか、すべてのネットアップデータコレクタですでに利用できます。今後数カ月にわたって、他のすべてのデータコレクタに展開される予定です。

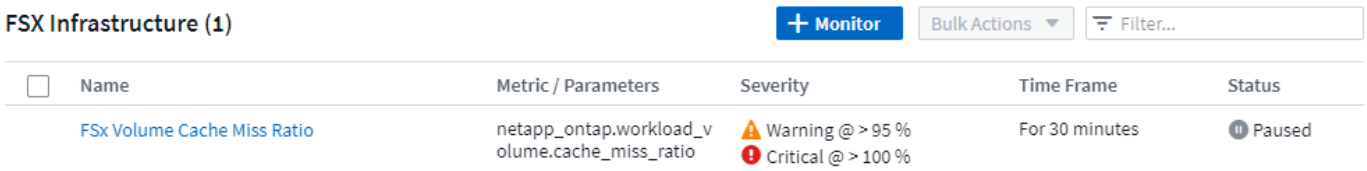
2022年3月

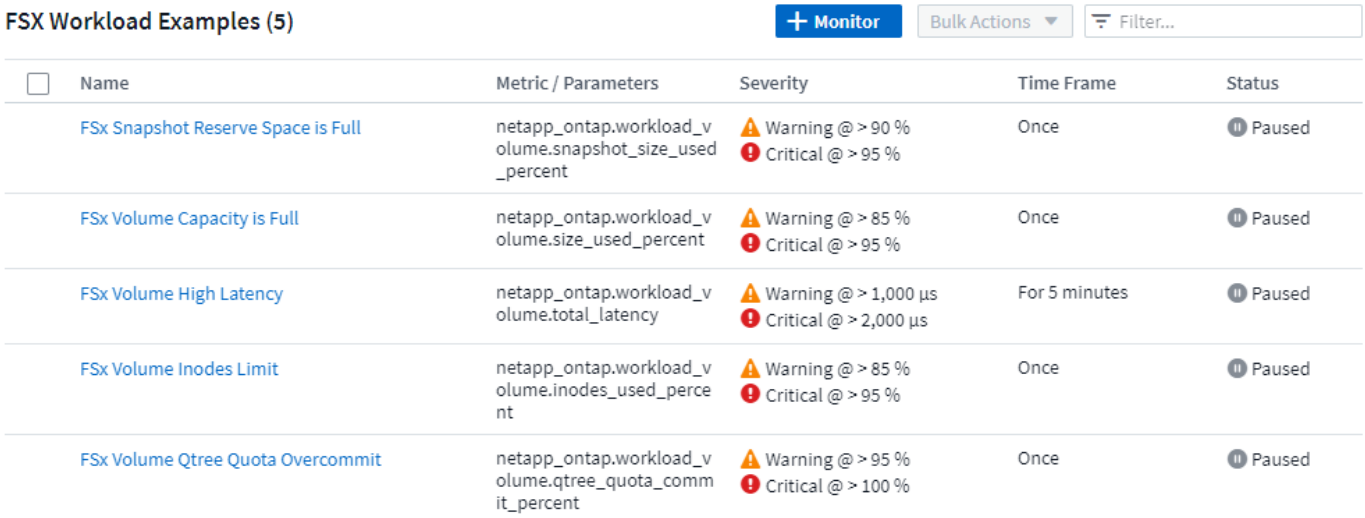
ONTAP 9.9 以降のクラウド接続

。 "ONTAP 9.9 以降でのネットアップクラウド接続" データコレクタを使用すると、外部 Acquisition Unit をインストールする必要がなくなるため、トラブルシューティング、メンテナンス、および初期導入が簡単になります。

NetApp ONTAP モニタ用の新しい **FSX**

NetApp ONTAP 環境向けの FSX の監視は、簡単に行うことができます "システム定義のモニタ" インフラ（指標）とワークロード（ログ）の両方に対応します。





すべてのユーザが利用できる新しい **Cloud Secure** 機能

環境のセキュリティがこれまで以上に強化され、次の Cloud Secure 機能が一般提供されました。

* 特徴 *	* 概要 *
データ破壊–ファイル削除攻撃の検出	異常な大規模なファイル削除アクティビティを検出し、悪意のあるユーザによる悪意のあるファイルアクセスをブロックし、自動応答ポリシーを使用してスナップショットを自動的に作成します。
警告とアラートの通知は別々に表示されます	警告とアラートの通知は別の受信者に送信できるため、適切なチームに情報を提供できます

Telegraf Agent を更新

テレグラム統合データの取り込みのためのエージェントがバージョン **1.2** に更新され、性能とセキュリティが向上しました。
更新を希望するユーザーは、の適切なアップグレードセクションを参照できます "エージェントのインストール" ドキュメント
以前のバージョンのエージェントは、ユーザの操作を必要とせずに引き続き機能します。

Data Collector のアップデート

- Broadcom Fibre Channel Switches データコレクタは、各インベントリポーリングで発行される CLI コマンドの数を減らすように最適化されています。

2022年2月

Cloud Insights は **Apache log4j** の脆弱性を解決します

お客様のセキュリティは、ネットアップの最優先事項です。Cloud Insights には、最新の Apache log4j の脆弱性に対処するためのソフトウェアライブラリの更新が含まれています。

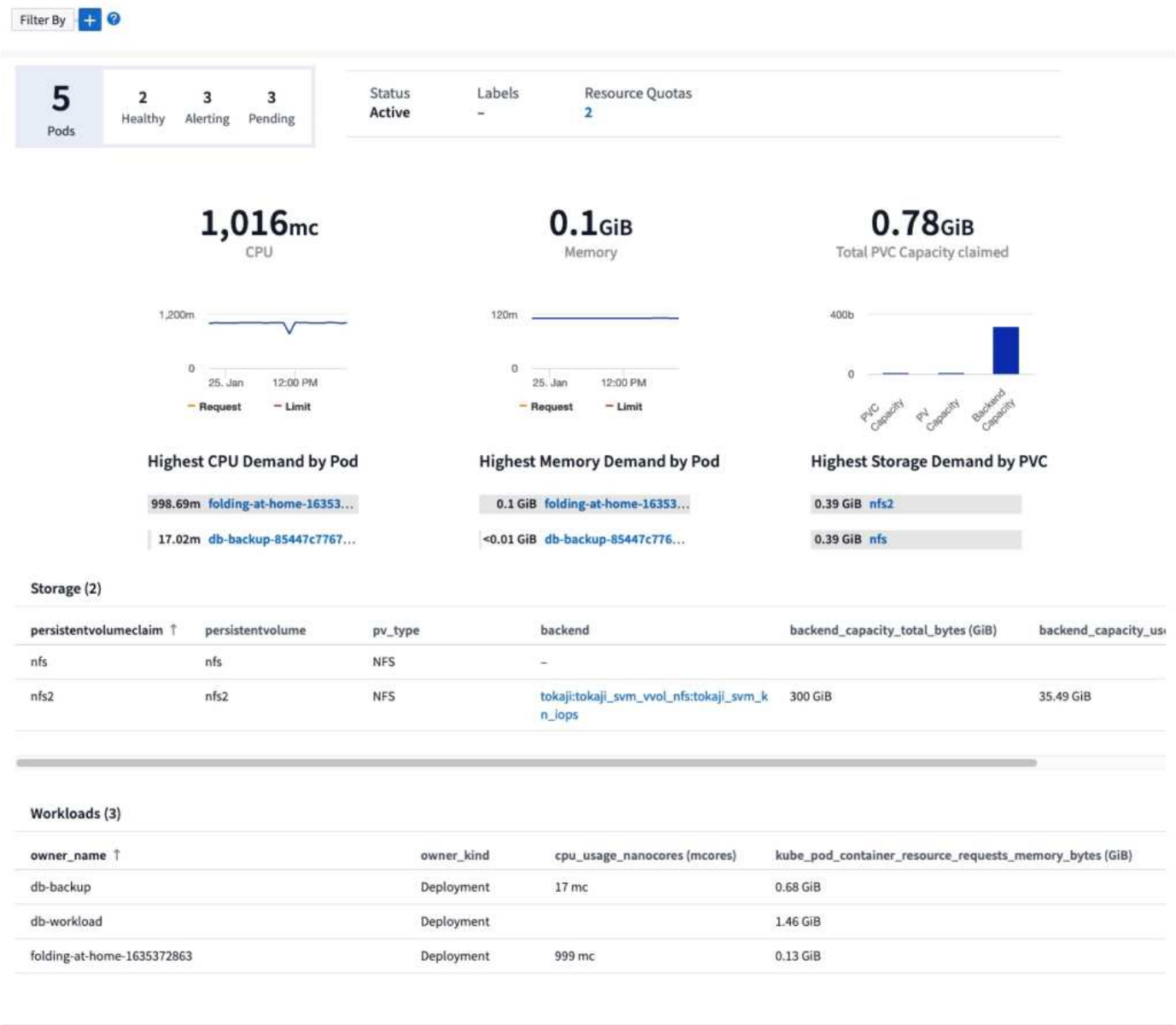
ネットアップの Product Security Advisory Web サイトに掲載されている次の資料を参照してください。

"CVE-20121-44228"
"CVE-20121-45046"
"（CVE-2021-45105"

これらの脆弱性の詳細と、ネットアップの対応については、を参照してください "ネットアップのニュースルーム"。

Kubernetes のネームスペースの詳細ページ

Kubernetes 環境の探索は、クラスタの名前空間の情報詳細ページにより、かつてないほど優れています。ネームスペースの詳細ページには、ネームスペースに使用されているすべてのアセットの概要が表示されます。これには、バックエンドのすべてのストレージリソースとその容量利用率が含まれます。



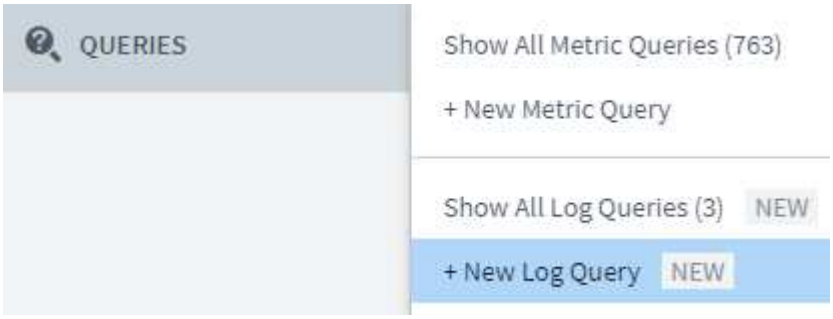
2021年12月

ONTAP システムをさらに緊密に統合

ネットアップの Event Management System （ EMS ；イベント管理システム）との新たな統合により、 ONTAP ハードウェア障害に対するアラート生成を簡易化できます。
"調査とアラート" Cloud Insights の下位レベルの ONTAP メッセージを使用して、トラブルシューティングのワークフローを通知および改善し、 ONTAP 要素管理ツールへの依存をさらに軽減します。

ログを照会しています

ONTAP システムの場合、 Cloud Insights クエリには強力な機能が搭載されています "ログエクスプローラ"を使用すると、 EMS ログエントリの調査とトラブルシューティングを簡単に行うことができます。



Data Collector レベルの通知。

システム定義のアラート用モニタとカスタム作成のモニタに加えて、 ONTAP データコレクタのアラート通知も設定できます。これにより、他のモニタアラートとは無関係に、コレクタレベルのアラートの受信者を指定できます。

Cloud Secure ロールの柔軟性が向上します

に基づいて、ユーザに Cloud Secure 機能へのアクセスを許可できます "ロール" 管理者が設定します。

ロール	Cloud Secureアクセス
管理者	アラート、フォレンジック、データコレクタ、自動応答ポリシー、 Cloud Secure 用 API など、すべての Cloud Secure 機能を実行できます。 管理者は、他のユーザを招待することもできますが、割り当てることができるのは Cloud Secure ロールのみです。
ユーザ	アラートを表示および管理し、フォレンジックを表示できます。ユーザーロールは、アラートステータスの変更、メモの追加、スナップショットの手動作成、ユーザーアクセスのブロックを行うことができます。
ゲスト	アラートおよびフォレンジックを表示できます。ゲストロールでは、アラートステータスの変更、メモの追加、スナップショットの手動作成、ユーザーアクセスのブロックはできません。

オペレーティングシステムのサポート

CentOS 8.x のサポートは、現在 * CentOS 8 Stream * のサポートに置き換えられています。CentOS 8.x は、2021 年 12 月 31 日にサポート終了となります。

Data Collector のアップデート

ベンダーの変更を反映した Cloud Insights データコレクタ名がいくつか追加されています。

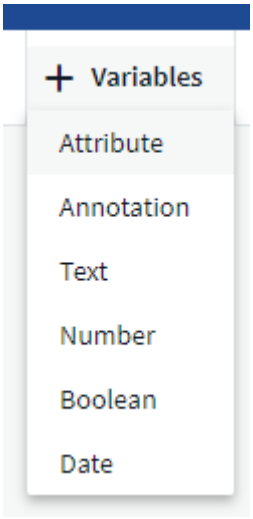
ベンダー / モデル	前の名前
Dell EMC PowerScale	Isilon
HPE Alletra 9000/Primera	3PAR
HPE Alletra 6000	Nimble

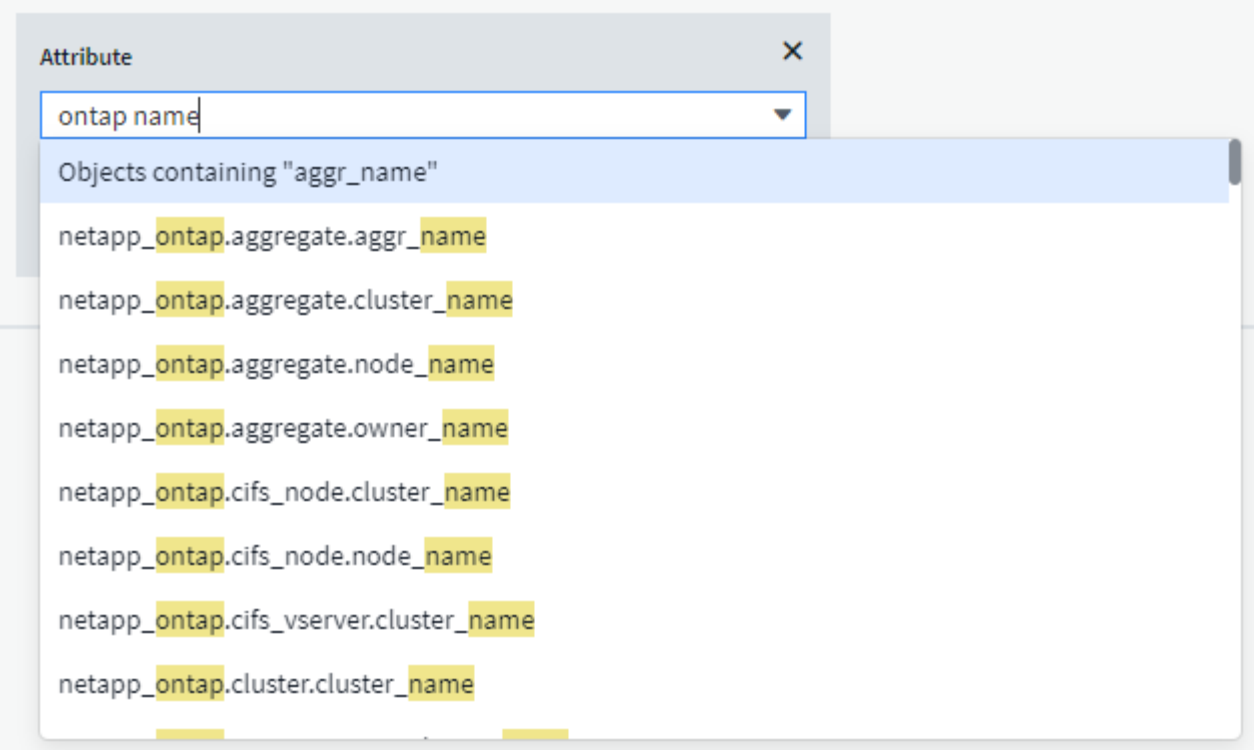
2021年11月

Adaptive Dashboards （アダプティブダッシュボード

_ 属性の新しい変数と、ウィジェットで変数を使用する機能 _ 。

ダッシュボードは、かつてないほど強力で柔軟性に優れています。属性変数を使用してアダプティブダッシュボードを構築することで、ダッシュボードを即座にフィルタリングできます。これらと既存の他のものを使用する "変数（ variables ）" 環境全体の指標を確認するためのダッシュボードを 1 つ作成し、リソース名、タイプ、場所などでシームレスにフィルタリングダウンできるようになりました。ウィジェットの数値変数を使用して、ストレージサービスの GB あたりのコストなど、物理指標をコストに関連付けます。



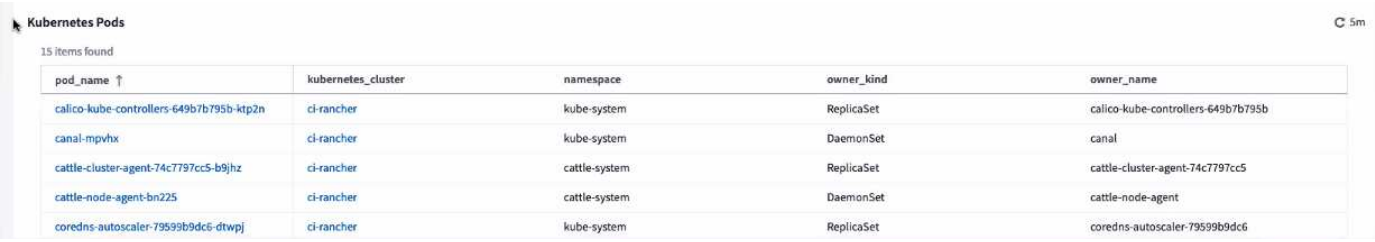


API 経由で Reporting Database にアクセスします

サードパーティのレポート作成ツール、 ITSM ツール、自動化ツールとの統合機能が強化されました。 Cloud Insights の強力な機能です "API" Cognos Reporting 環境を使用せずに、 Cloud Insights Reporting データベースを直接照会できます。

VM ランディングページのポッドテーブル

VM と Kubernetes ポッド間のシームレスなナビゲーション：トラブルシューティングとパフォーマンスヘッドルーム管理を向上させるために、関連する Kubernetes ポッドの表が VM ランディングページに表示されるようになりました。



Data Collector のアップデート

- ECS で、ストレージとノードのファームウェアが報告されるようになりました
- Isilon のプロンプト検出機能が向上しました
- Azure NetApp Files は、パフォーマンスデータをより迅速に収集します
- StorageGRID でシングルサインオン (SSO) がサポートされるようになりました。
- Brocade CLI は、 X—4 のモデルを適切に報告します

サポートされているその他のオペレーティングシステム

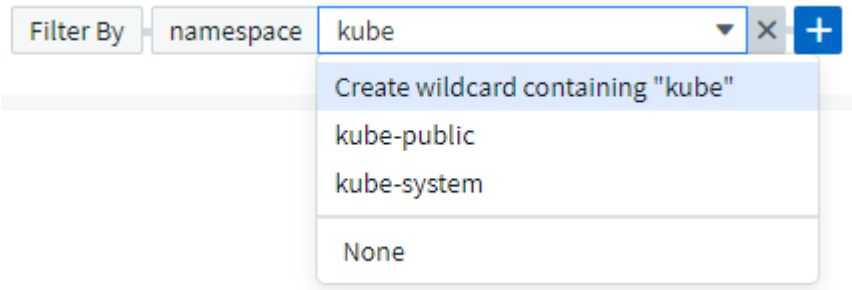
Cloud Insights Acquisition Unit では、すでにサポートされている OS に加え、次のオペレーティングシステムがサポートされます。

- CentOS （ 64 ビット） 8.4
- Oracle Enterprise Linux （ 64 ビット） 8.4
- Red Hat Enterprise Linux （ 64 ビット） 8.4

2021年10月

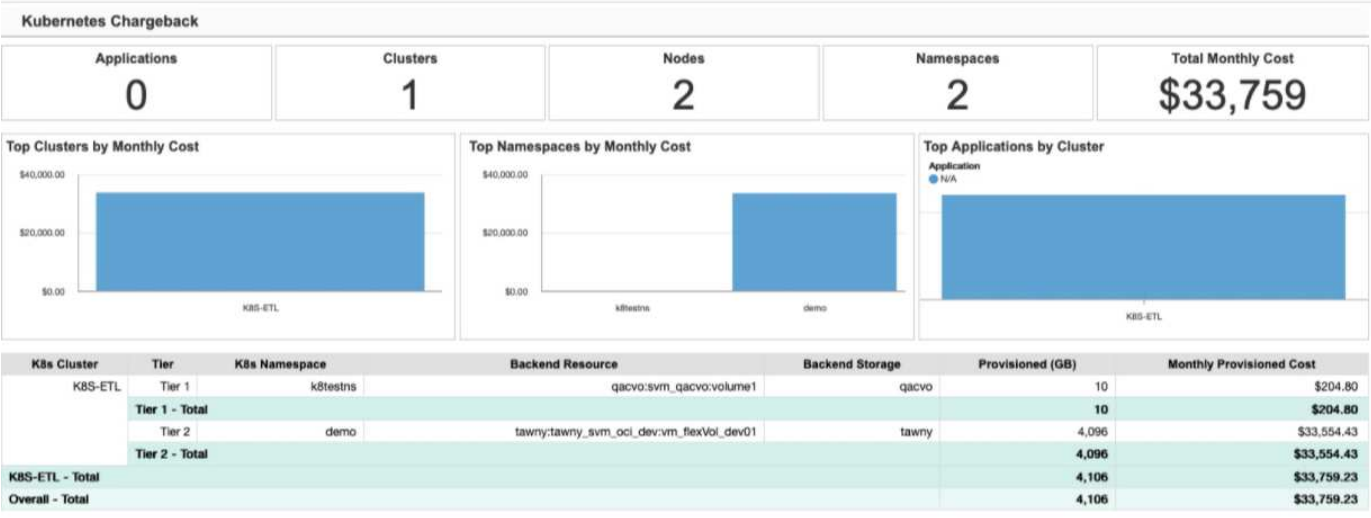
K8S Explorer ページのフィルター

"Kubernetes エクスプローラ" ページフィルタを使用すると、 Kubernetes クラスタ、ノード、およびポッドの探索に表示されるデータを集中的に制御できます。



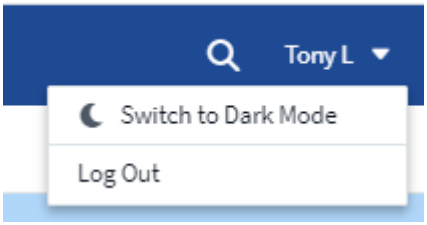
レポート用の K8s データ

Reporting で Kubernetes データを使用できるようになりました。チャージバックやその他のレポートを作成できます。Kubernetes チャージバックデータを Reporting に渡すには、 Kubernetes クラスタとそのバックエンドストレージへのアクティブな接続が必要です。また、 Cloud Insights が Kubernetes クラスタとの間でデータを受信している必要があります。バックエンドストレージからデータを受信していない場合、 Cloud Insights は Kubernetes オブジェクトデータを Reporting に送信できません。

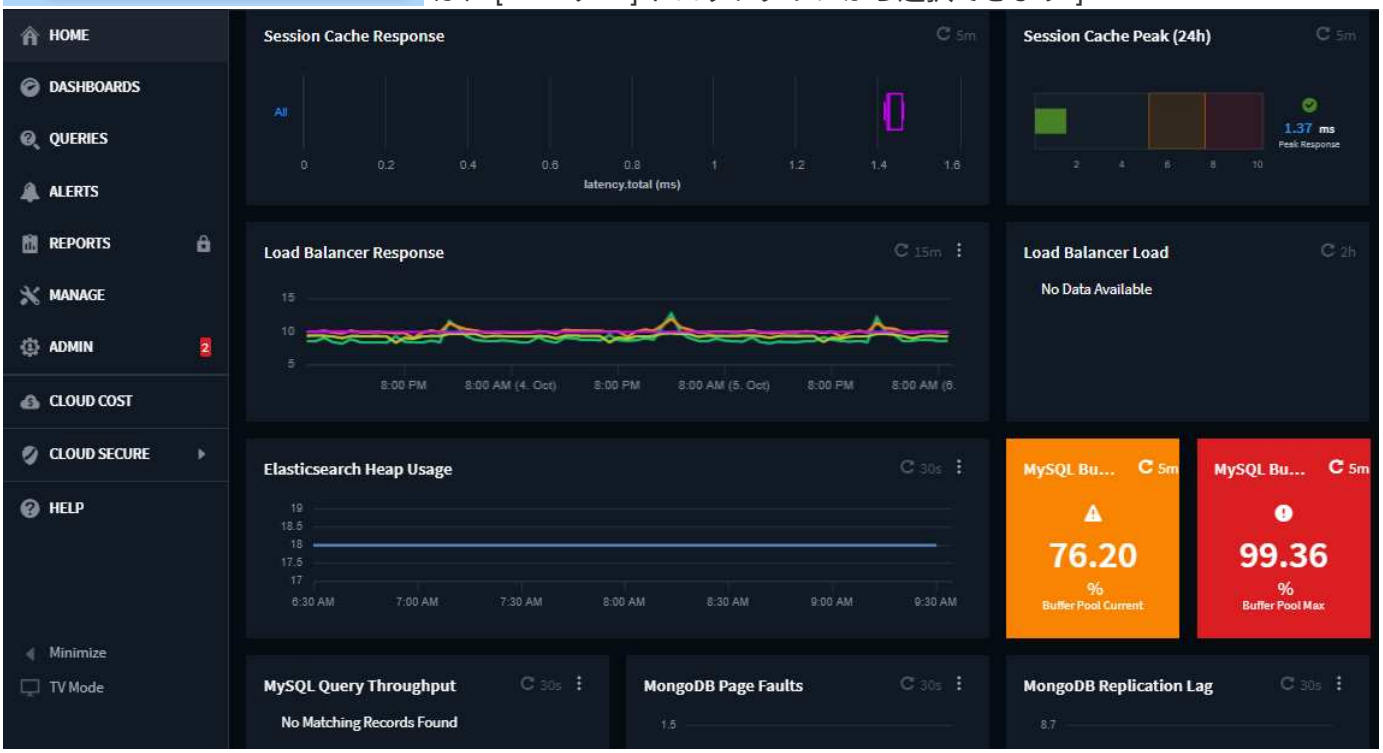


ダークテーマが到着しました

あなたの多くは暗い主題を求め、 Cloud Insights は答えた。ライトテーマとダークテーマを切り替えるには、ユーザー名の横にあるドロップダウンをクリックします。



は、 [ユーザー] ドロップダウンから選択できます"]



Data Collector のサポート

Cloud Insights データコレクタにいくつかの改善を加えました。主な特長は次のとおりです。

- Amazon FSX for ONTAP の新しいコレクタ

2021年9月

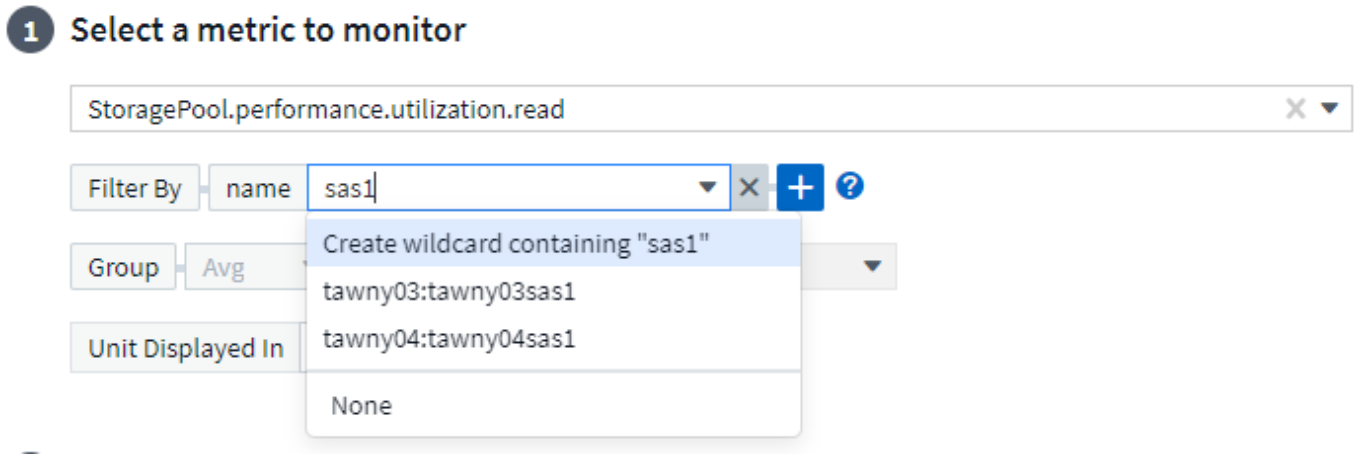
パフォーマンスポリシーが監視対象になりました

監視とアラートは、 Cloud Insights 全体でパフォーマンスポリシーと違反に取って代わるものです。 "モニタとのアラート" 環境内の潜在的な問題や傾向をより柔軟に把握できます。

モニタでのオートコンプリートの推奨事項、ワイルドカード、および式

アラートを監視するモニタを作成する際に、フィルタを入力すると予測が可能になり、モニタのメトリックや

属性を簡単に検索して見つけることができます。また、入力したテキストに基づいてワイルドカードフィルタを作成することもできます。



Telegraf Agent を更新

テレグラム統合データの取り込みのためのエージェントがバージョン * 1.19.3* に更新され、性能とセキュリティが向上しました。
更新を希望するユーザーは、の適切なアップグレードセクションを参照できます "エージェントのインストール" ドキュメント
以前のバージョンのエージェントは、ユーザの操作を必要とせずに引き続き機能します。

Data Collector のサポート

Cloud Insights データコレクタにいくつかの改善を加えました。主な特長は次のとおりです。

- Microsoft Hyper-V コレクタで、 WMI ではなく PowerShell が使用されるようになりました
- 並行呼び出しのため、 Azure VM と VHD コレクタの処理速度が最大 10 倍になりました
- HPE Nimble は、フェデレーテッド構成と iSCSI 構成をサポートしています

また、常にデータ収集を改善しているため、次のような最近の変更点があります。

- EMC Powerstore の新しいコレクタ
- Hitachi Ops Center の新しいコレクタです
- Hitachi Content Platform の新しいコレクタ
- ONTAP コレクタを拡張して、ファブリックプールをレポートします
- ストレージプールとボリュームのパフォーマンスで ANF を強化
- EMC ECS で、ストレージノードとストレージパフォーマンス、およびバケット内のオブジェクト数が強化されました
- ストレージノードと qtree の指標で EMC Isilon が強化されました
- EMC Symetrix のボリューム QoS 制限メトリックが強化されました
- ストレージノードの親シリアル番号を持つ強化された IBM SVC および EMC PowerStore

2021年8月

新しい監査ページのユーザーインターフェイス

。 "監査ページ" よりシンプルなインターフェイスを提供し、監査イベントを .csv ファイルにエクスポートできるようになりました。

ユーザロール管理の強化

Cloud Insights では、ユーザロールとアクセス制御をより自由に割り当てることができるようになりました。ユーザに、監視、レポート、および Cloud Secure に対する詳細な権限を個別に割り当てることができるようになりました。

つまり、監視、最適化、レポート機能への管理アクセスをより多くのユーザに許可しながら、機密性の高い Cloud Secure 監査およびアクティビティデータへのアクセスを必要なユーザだけに制限できます。

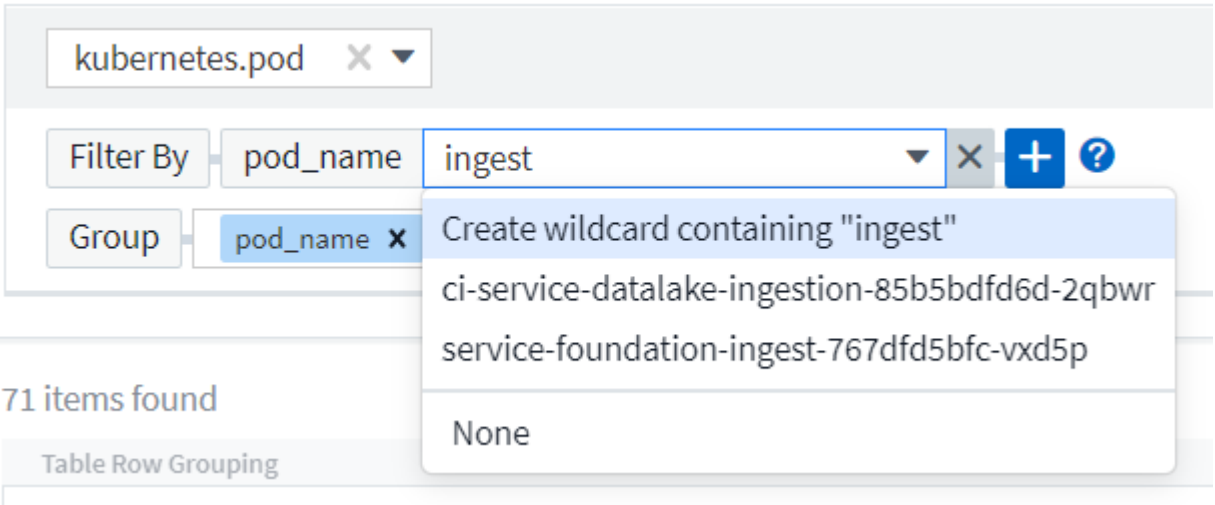
"詳細はこちら" Cloud Insights のドキュメントに記載されている各アクセスレベルについて

2021年6月

[フィルタ] での推奨事項、ワイルドカード、および式のオートコンプリート

このリリースの Cloud Insights では、クエリやウィジェットでフィルタリングする名前と値をすべて把握している必要はありません。フィルタリングを行う場合は、入力を開始 Cloud Insights するだけで、テキストに基づいて値が提示されます。ウィジェットに表示するアプリケーション名や Kubernetes 属性を検索する必要はありません。

フィルタを入力すると、選択可能な結果のスマートリストが表示されます。また、現在のテキストに基づいて * ワイルドカードフィルタ * を作成するオプションも表示されます。このオプションを選択すると、ワイルドカード式に一致するすべての結果が返されます。もちろん、フィルタに追加する値を個別に複数選択することもできます。



また、 NOT または OR を使用して、フィルタに * 式 * を作成したり、「 None 」オプションを選択してフィ

ールドで null 値をフィルタリングしたりすることもできます。

詳細については、をご覧ください "フィルタリングオプション" クエリおよびウィジェットで使用できます。

Edition で使用可能な API

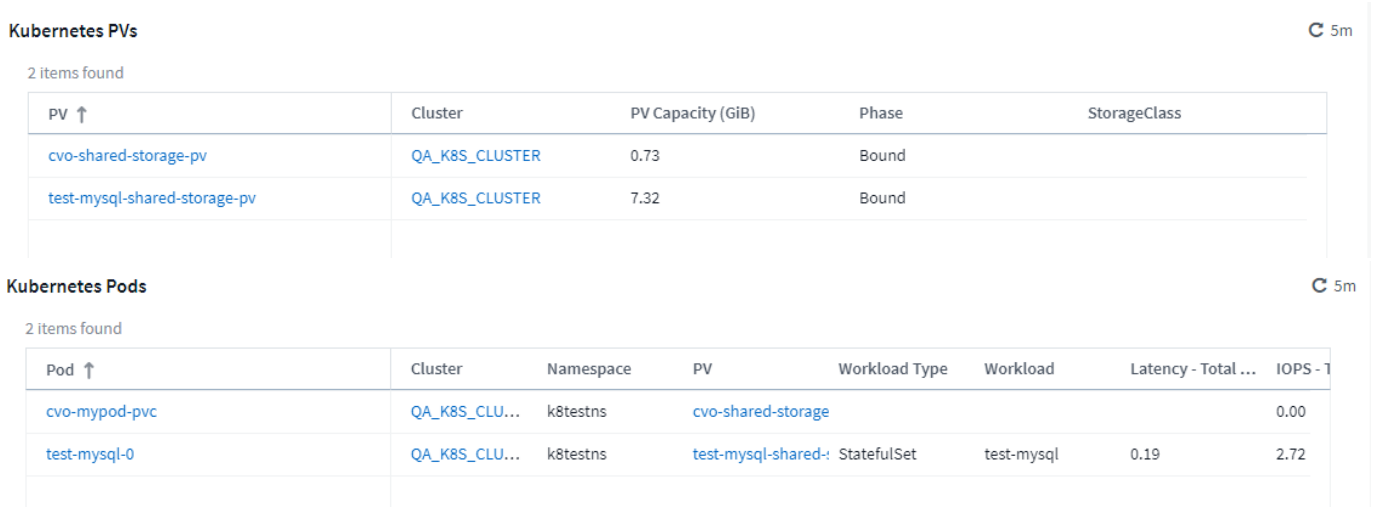
Cloud Insights の強力な API にはこれまで以上にアクセス可能であり、 Alerts API が Standard Edition および Premium Edition で利用可能になりました。
各エディションで使用できる API は次のとおりです。

API カテゴリ	基本	標準	Premium サービス
Acquisition Unit の略	✔	✔	✔
データ収集	✔	✔	✔
アラート		✔	✔
資産		✔	✔
データの取り込み		✔	✔

Kubernetes の PV とポッドの可視化

Cloud Insights を使用すると、 Kubernetes 環境のバックエンドストレージを可視化し、 Kubernetes ポッドと永続的ボリューム（ PVS ）を把握できます。IOPS 、レイテンシ、スループットなどの PV カウンタを、 1 台のポッドで使用されている PV カウンターから PV まで、そしてバックエンドのストレージデバイスまでのすべての方法で追跡できるようになりました。

ボリュームまたは内部ボリュームのランディングページに、次の 2 つの新しいテーブルが表示される。

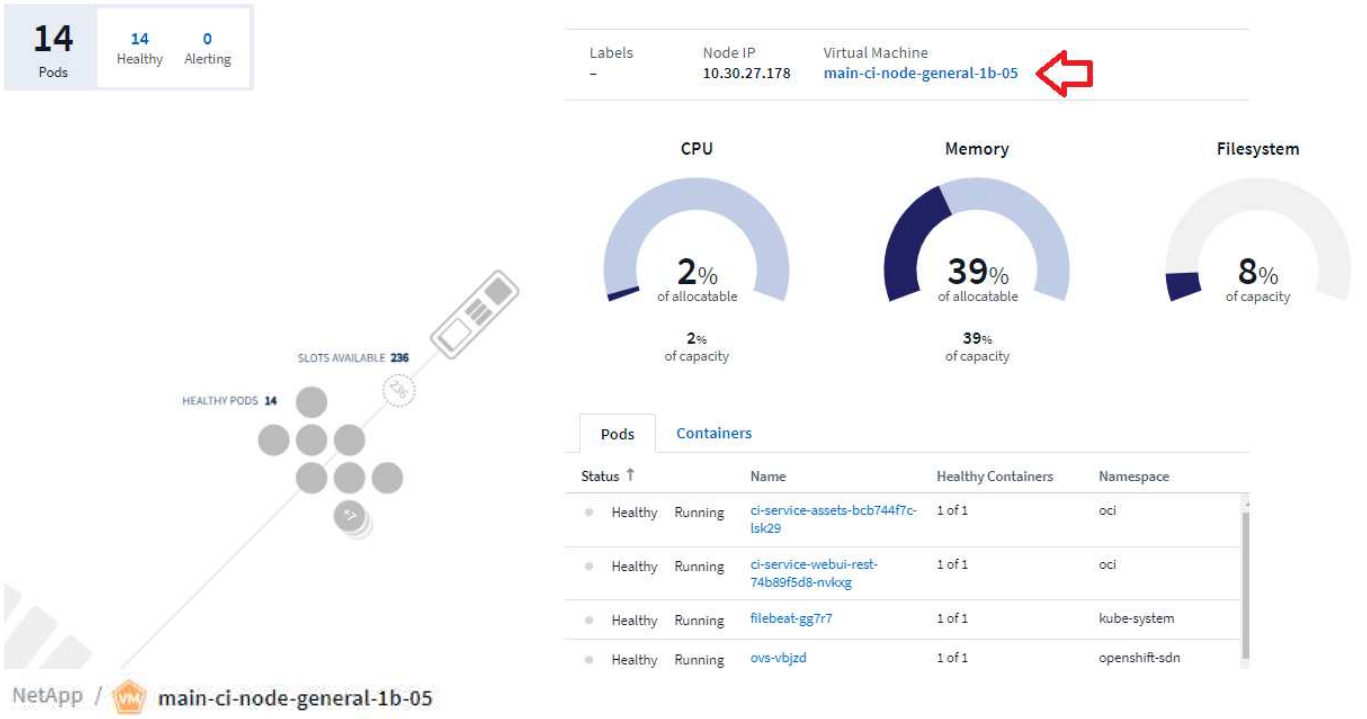


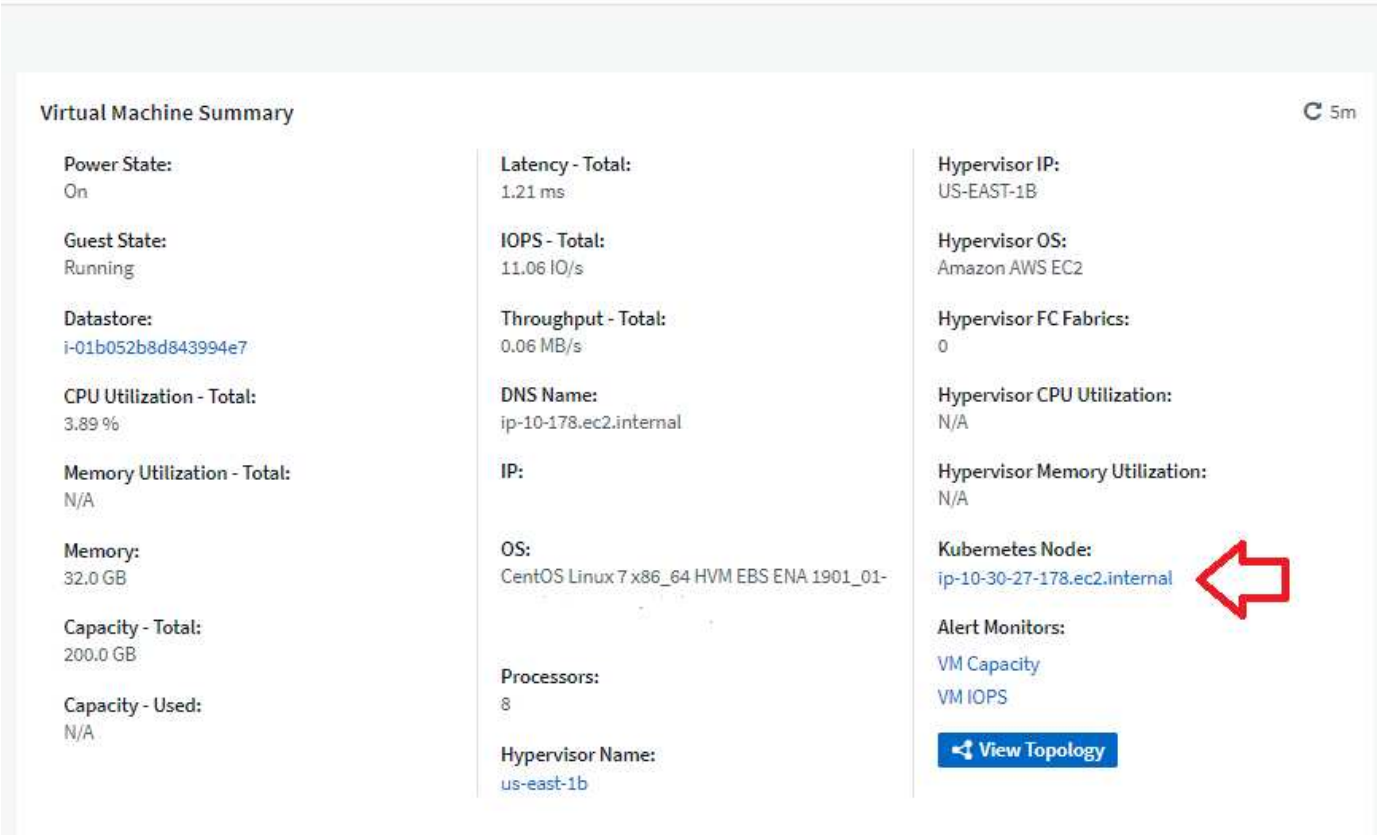
これらの新しいテーブルを利用するには、現在の Kubernetes エージェントをアンインストールして新規にインストールすることをお勧めします。Kbe State-Metrics バージョン 2.1.0 以降もインストールする必要があります。

Kubernetes ノードから VM リンク

Kubernetes Node ページで、をクリックしてノードの VM ページを開くことができます。VM ページには、ノ

ード自体へのリンクも表示されます。





パフォーマンスポリシーの置き換えをアラート監視します

Cloud Insights は、複数のしきい値、 webhook 、 E メールによるアラート送信、単一のインターフェイスを使用したすべての指標のアラート送信などの利点を追加するために、 2021 年 7 月から 8 月までの間、 Standard Edition および Premium Edition のお客様を * Performance Policies * から * Monitor * に変換しま

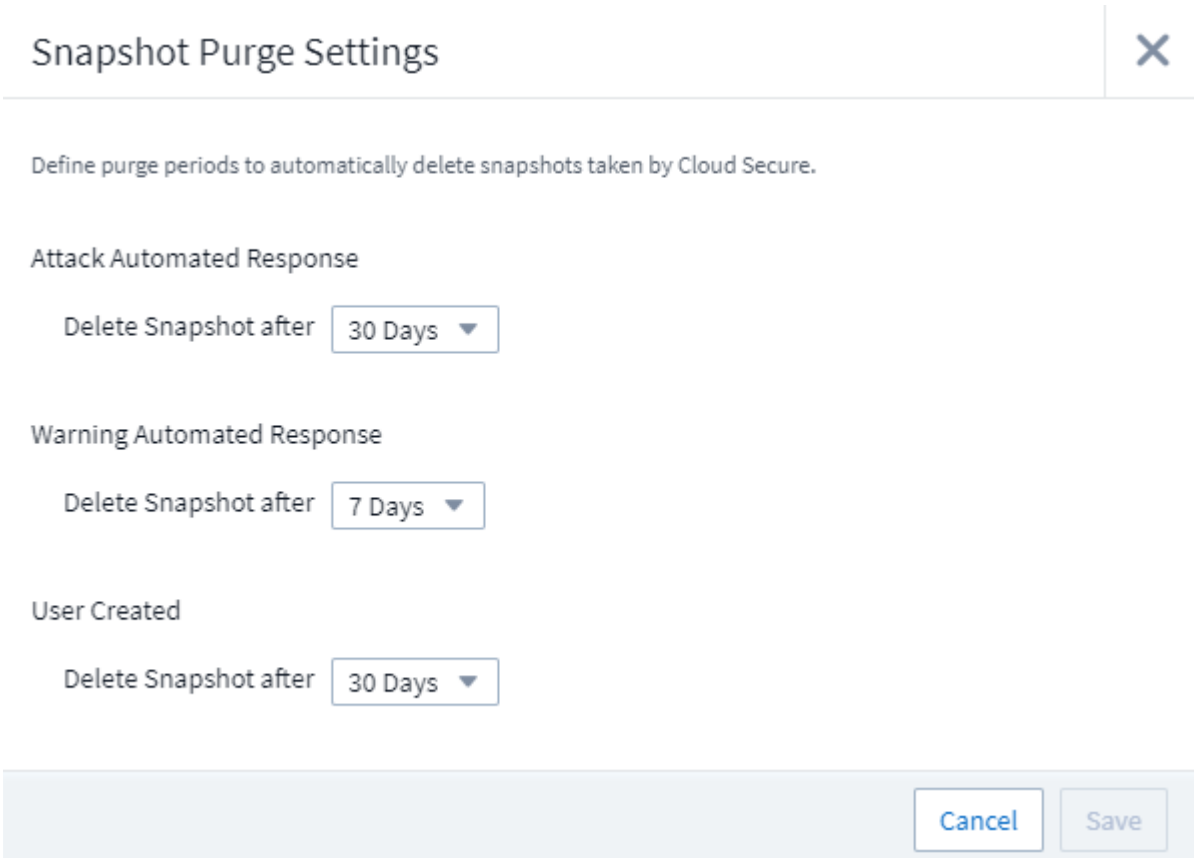
す。の詳細を確認してください "アラートと監視"では、このエキサイティングな変化に合わせて調整してください。

Cloud Secure は NFS をサポートしています

Cloud Secure で ONTAP データ収集用の NFS がサポートされるようになりました。SMB および NFS ユーザアクセスを監視し、ランサムウェア攻撃からデータを保護
また、 Cloud Secure は、 NFS ユーザ属性を収集するための Active Directory および LDAP ユーザディレクトリもサポートしています。

Cloud Secure スナップショットのパージ

Cloud Secure では、スナップショットパージ設定に基づいてスナップショットが自動的に削除されるため、ストレージスペースが節約され、手動でスナップショットを削除する必要がなくなります。



Cloud Secure のデータ収集速度

1 つのデータコレクタエージェントシステムで、 Cloud Secure に 1 秒あたり最大 20,000 のイベントをポストできるようになりました。

2021年5月

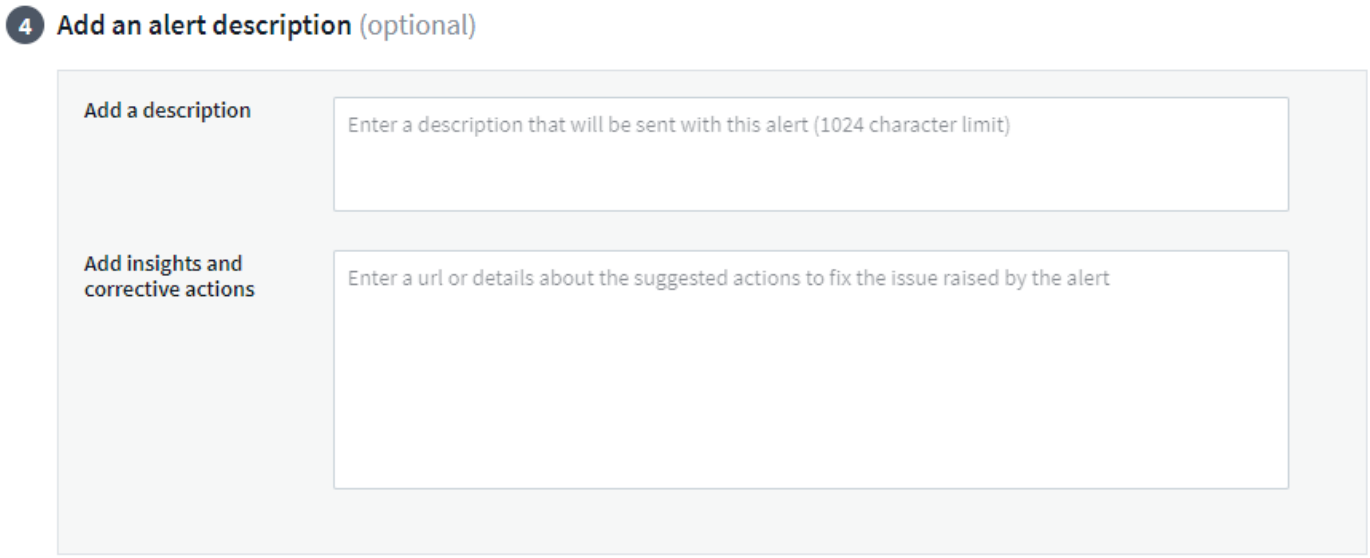
4 月に行った変更の一部を以下に示します。

Telegraf Agent を更新

テレグラム統合データの取り込み用エージェントは、パフォーマンスとセキュリティが向上し、バージョン 1.17.3 に更新されました。
更新を希望するユーザーは、の適切なアップグレードセクションを参照できます "エージェントのインストール" ドキュメント
以前のバージョンのエージェントは、ユーザの操作を必要とせずに引き続き機能します。

アラートに対処方法を追加します

オプションの概要を追加し、 [アラート概要の追加] セクションに入力して、モニタの作成または変更時に追加のインサイトや修正アクションを追加できるようになりました。概要がアラートとともに送信されます。Insights と対処方法のフィールドには、アラートに対処するための詳細な手順とガイダンスが表示され、アラートのランディングページの概要セクションに表示されます。



すべてのエディションの Cloud Insights API

API アクセスがすべてのエディションの Cloud Insights で利用できるようになりました。
Basic エディションのユーザは、 Acquisition Unit と Data Collector のアクションを自動化できるようになりました。また、 Standard Edition ユーザは、メトリックを照会してカスタムメトリックを取り込むことができます。
Premium Edition では、引き続きすべての API カテゴリをフルに使用できます。

API カテゴリ	基本	標準	Premium サービス
Acquisition Unit の略	✔	✔	✔
データ収集	✔	✔	✔
資産		✔	✔
データの取り込み		✔	✔
Data Warehouse			✔

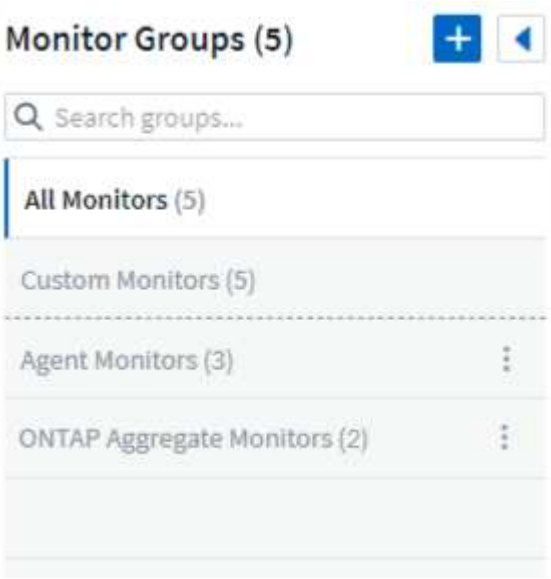
API の使用方法の詳細については、を参照してください "APIドキュメント"。

2021年4月

モニタの管理が容易になります

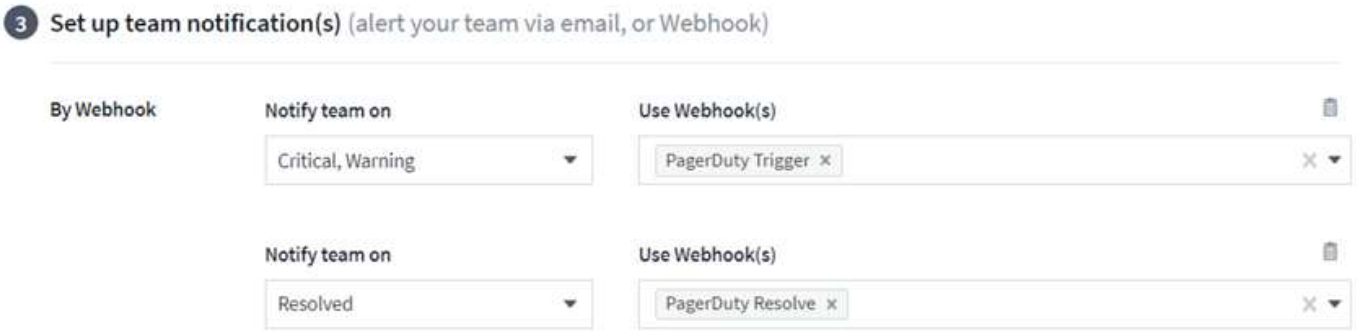
"グループ化を監視します" 環境内のモニタの管理を簡易化します。複数のモニタをグループ化して、 1 つのモニタとして一時停止できるようになりました。たとえば、インフラストラクチャのスタックで更新が発生している場合は、それらのすべてのデバイスからのアラートを 1 回のクリックで一時停止できます。

モニタグループは、 ONTAP デバイスの管理を Cloud Insights に向上させる、画期的な新機能の最初の部分です。



webhook を使用した拡張アラートオプション

多くの商用アプリケーションをサポートしています "ウェブフック" 標準入力インターフェイスとして使用します。Cloud Insights では、このような配信チャネルの多くがサポートされるようになりました。 Slack 、 PagerDuty 、 Teams 、および Discord 用のデフォルトテンプレートが用意されています。また、カスタマイズ可能な汎用 Web フックを使用して、他の多くのアプリケーションをサポート



デバイス識別機能の向上

監視とトラブルシューティングを改善し、正確なレポートを作成するためには、 IP アドレスやその他の ID ではなく、デバイス名を理解しておくと役立ちます。Cloud Insights では、というルールベースのアプローチを使用して、環境内のストレージデバイスと物理ホストデバイスの名前を自動的に識別できるようになりました

"* デバイス解決 *"（ * Manage * メニューで使用できます）。

もっと情報を求められました！

お客様からの一般的な質問では、データの範囲を視覚化するためのデフォルトオプションが用意されています。そのため、サービス全体で次の 5 つの新しい選択肢が時間範囲ピッカーで利用できるようになりました。

- 過去 30 分
- 過去2時間
- 過去6時間
- 過去12時間
- 過去2日間

1 つの Cloud Insights 環境で複数のサブスクリプションを登録できます

4 月 2 日より、 Cloud Insights は、 1 つの Cloud Insights インスタンスで 1 つの顧客に対して同じエディションタイプの複数のサブスクリプションをサポートします。これにより、お客様は、 Cloud Insights サブスクリプションの一部をインフラ購入と共存させることができます。複数のサブスクリプションについては、ネットアップの営業にお問い合わせください。

パスを選択します

Cloud Insights のセットアップ中に、監視とアラートの開始方法と、ランサムウェアと内部の脅威の検出方法を選択できるようになりました。Cloud Insights は、選択したパスに基づいて開始環境を設定します。他のパスはあとでいつでも設定できます。

簡単な Cloud Secure オンボーディング

また、 Cloud Secure の使用を今まで以上に簡単に開始でき、セットアップのための新しいチェックリストも追加されています。

いつものように、お客様のご提案をお待ちしております。ng-cloudinsights-customerfeedback@netapp.com に送信します。

2021年2月

Telegraf Agent を更新

テレグラム統合データの取り込み用エージェントは、脆弱性およびバグ修正を含むバージョン 1.17.0 に更新されました。

Cloud Cost Analyzer

Spot by NetAppとクラウドコストの効果を体験してください。過去、現在、予想される支出に関する詳細なコスト分析が可能で、環境内のクラウドの使用状況を可視化できます。クラウドコストダッシュボードでは、クラウドのコストを明確に把握し、個々のワークロード、アカウント、サービスを詳細に把握できます。

クラウドコストは、次のような大きな課題に役立ちます。

- クラウドコストの追跡と監視
- 廃棄物と潜在的な最適化領域を特定する
- 実行可能アクションアイテムを配信しています

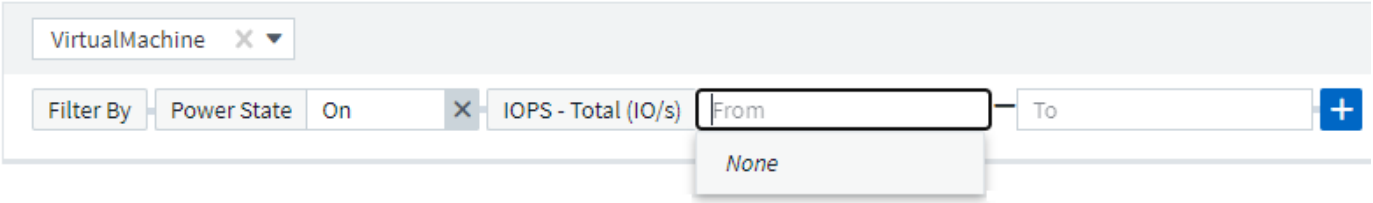
クラウドコストは監視に重点を置いています。ネットアップのアカウントで Full Spot by NetApp にアップグレードすると、コストを自動削減し、環境を最適化できます。

フィルタを使用した **null** 値を持つオブジェクトのクエリ

Cloud Insights では、フィルタを使用して、値が NULL / なしの属性とメトリックを検索できるようになりました。このフィルタリングは、次の場所で任意の属性や指標に対して実行できます。

- をクリックします
- ダッシュボードウィジェットおよびページ変数で使用できます
- をクリックします
- モニターを作成するとき

NULL / なしの値をフィルタリングするには ' 該当するフィルタのドロップダウンに *None* オプションが表示されたら ' そのオプションを選択します



複数リージョンのサポート

本日より、世界中のさまざまな地域で Cloud Insights サービスを提供します。これにより、米国外のお客様のパフォーマンスが向上し、セキュリティが強化されます。Cloud Insights / Cloud Secure は、環境を作成したリージョンに応じて情報を格納します。

をクリックします "こちらをご覧ください" を参照してください。

2021年1月

その他の **ONTAP** メトリックの名前変更

ONTAP システムからのデータ収集の効率化に向けて継続的に取り組んでいる一環として、以下の ONTAP 指標の名前が変更されました。

既存のダッシュボードウィジェットやこれらのいずれかの指標を使用するクエリがある場合は、新しい指標名を使用するようにそれらのウィジェットを編集または再作成する必要があります。

前のメトリック名	新しいメトリック名
NetApp_ONTAP.DISK_constituent.total_transfers	NetApp_ONTAP.disk_constituent.total_iops
NetApp_ONTAP.disk.total_transfers	NetApp_ONTAP.disk.total_iops
NetApp_ONTAP.FCP_LIF.READ_DATA	NetApp_ONTAP.FCP_LIF.READ_Throughput

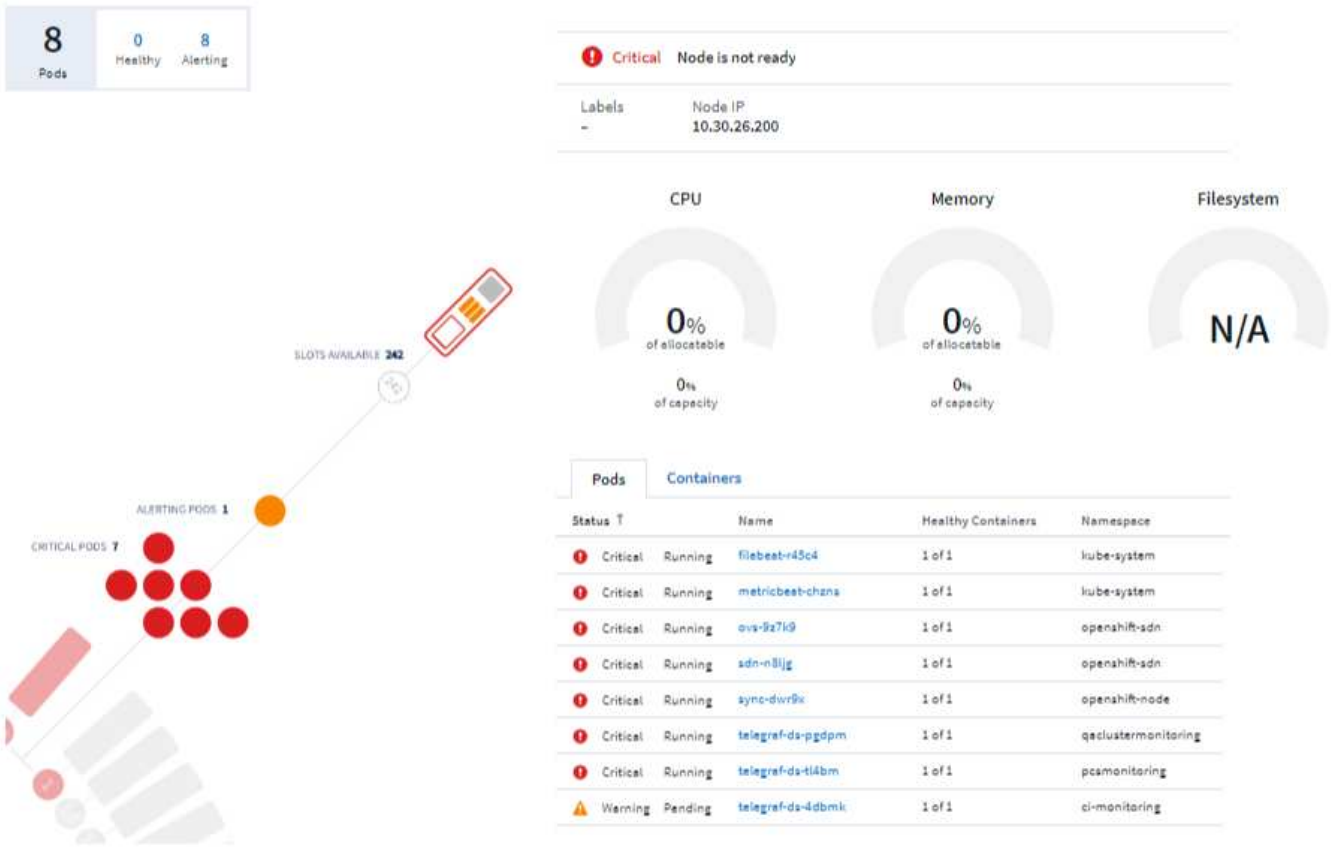
前のメトリック名	新しいメトリック名
NetApp_ONTAP.fcp_lif.write_data	NetApp_ONTAP.fcp_lif.write_throughput
NetApp_ONTAP.iscsi_lif.read_data	NetAppONTAP.iscsi_lif.read_throughput
NetApp_ONTAP.iscsi_lif.write_data	NetAppONTAP.iscsi_lif.write_throughput
NetApp_ONTAP.LIF.recv_data	NetAppONTAP.LIF.recv_throughput
netapp_ontap.lif.sent_data	netapp_ontap.lif.sent_throughput
NetApp_ONTAP.LUN.READ_DATA	NetApp_ONTAP.LUN.READ_Throughput
NetApp_ONTAP.LUN.write_data	NetApp_ONTAP.LUN.write_throughput
NetApp_ONTAP.nic_common_rx_bytes	NetApp_ONTAP.nic_common_rx_throughput
NetApp_ONTAP.nic_common.tx_bytes	NetApp_ONTAP.nic_common.tx_throughput
NetApp_ontap .path.read_data	NetApp_ontap 。 path.read_throughput
NetApp_ontap .path.write_data	NetApp_ontap 。 path.write_throughput
NetApp_ontap .path.total_data	NetApp_ontap 。 path.total_throughput
NetApp_ONTAP.policy_group.read_data	NetAppONTAP.policy_group.read_throughput
NetApp_ONTAP.policy_group.write_data	NetAppONTAP.policy_group.write_throughput
NetApp_ONTAP.policy_group.other_data	NetAppONTAP.policy_group.other_throughput
NetApp_ONTAP.policy_group.total_data	NetAppONTAP.policy_group.total_throughput
NetAppONTAP.system_node.disk_data_read	NetAppONTAP.SYSTEM_NODE.DISK_Throughput 読み取り
NetApp_ONTAP.system_node.disk_data_written に書き込まれている	NetApp_ONTAP.SYSTEM_NODE.DISK_Throughput _ Written
NetApp_ONTAP.SYSTEM_NODE.HDD_DATA 読み取り	NetAppONTAP.SYSTEM_NODE.HDD_Throughput 読み取り
NetApp_ONTAP.system_node.HDD_data_written に作成されている必要があります	NetApp_ONTAP.SYSTEM_NODE.HDD_Throughput _ Written
NetApp_ONTAP.SYSTEM_NODE.SSD_DATA 読み取り	NetAppONTAP.SYSTEM_NODE.SSD_Throughput 読み取り
NetApp_ONTAP.system_node.ssd_data_written	NetAppONTAP.SYSTEM_NODE.SSD_Throughput _ Written
netapp_ontap.system_node.net_data_recv	netapp_ontap.system_node.net_throughput_recv
netapp_ontap.system_node.net_data_sent	netapp_ontap.system_node.net_throughput_sent
NetApp_ONTAP.SYSTEM_NODE.FCP_DATA _ recv	NetApp_ONTAP.SYSTEM_NODE.FCP_Throughput _ recv
NetApp_ONTAP.SYSTEM_NODE.FCP_DATA _ 送信されました	NetApp_ONTAP.SYSTEM_NODE.FCP_Throughput 送信
NetApp_ONTAP.volume_node.cifs_read_data	NetAppONTAP.volume_node.cifs_read_throughput
NetAppONTAP.volume_node.cifs_write_data	NetAppONTAP.volume_node.cifs_write_throughput

前のメトリック名	新しいメトリック名
NetAppONTAP.volume_node.nfs_read_data	NetAppONTAP.volume_node.nfs_read_throughput
NetAppONTAP.volume_node.nfs_write_data	NetAppONTAP.volume_node.nfs_write_throughput
NetAppONTAP.volume_node.iscsi_data	NetAppONTAP.volume_node.iscsi_throughput
NetAppONTAP.volume_node.iscsi_write_data	NetAppONTAP.volume_node.iscsi_write_throughput
NetAppONTAP.volume_node.fcp_read_data	NetAppONTAP.volume_node.fcp_read_throughput
NetAppONTAP.volume_node.fcp_write_data	NetAppONTAP.volume_node.fcp_write_throughput
NetApp_ONTAP.volume_read_data を選択します	NetAppONTAP.volume_read_throughput
NetAppONTAP.volume_write_data	NetAppONTAP.volume_write_throughput
NetApp_ONTAP.workload .read_data	NetAppONTAP.workload .read_throughput
NetApp_ONTAP.workload .write_data	NetAppONTAP.workload .write_throughput
NetAppONTAP.workload _volume. read_data	NetAppONTAP.workload _volume. read_throughput
NetApp_ONTAP.workload _volume_write_data	NetAppONTAP.workload _volume. write_throughput

新しい **Kubernetes** エクスプローラ

。 "Kubernetes エクスプローラ" Kubernetes クラスタのトポロジをわかりやすく表示できるため、エキスパートでなくても、クラスタレベルからコンテナやストレージまで、問題や依存関係をすばやく特定できます。

Kubernetes 環境内のクラスタ、ノード、ポッド、コンテナ、ストレージのステータス、使用状況、健全性に関する Kubernetes Explorer のドリルダウンの詳細を使用して、さまざまな情報を調べることができます。



2020年12月

Kubernetes のインストールを簡易化

Kubernetes Agent のインストールは合理化され、ユーザの操作が少なくて済みます。 "Kubernetes Agent をインストールします" Kubernetes のデータ収集機能が追加されました。

2020年11月

その他のダッシュボード

ONTAP に焦点を当てた次のダッシュボードがギャラリーに追加され、インポート可能になりました。

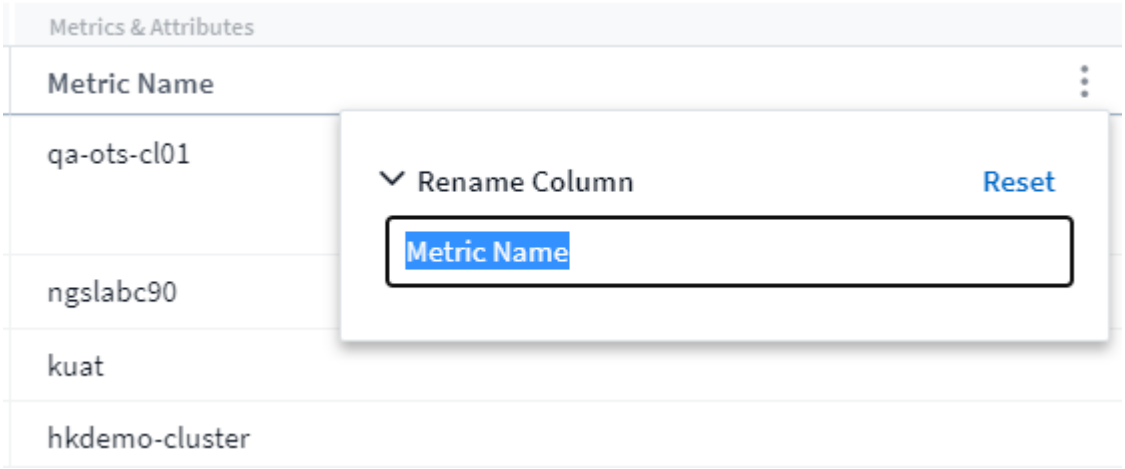
- ONTAP ：アグリゲートのパフォーマンスと容量
- ONTAP FAS / AFF - 容量利用率
- ONTAP FAS/AFF - クラスタ容量
- ONTAP FAS / AFF - 効率性
- ONTAP FAS / AFF - FlexVol のパフォーマンス

- ONTAP FAS / AFF ノードの運用 / 最適ポイント
- ONTAP FAS / AFF - ポスト前の容量削減
- ONTAP ：ネットワークポートのアクティビティ
- ONTAP ：ノードプロトコルのパフォーマンス
- ONTAP ：ノードワークロードのパフォーマンス（フロントエンド）
- ONTAP ：プロセッサ
- ONTAP ： SVM ワークロードのパフォーマンス（フロントエンド）
- ONTAP ：ボリュームワークロードのパフォーマンス（フロントエンド）

表ウィジェットの列名を変更します

表ウィジェットの *Metrics* および *Attributes* セクションで列の名前を変更するには、編集モードでウィジェットを開き、列の上部にあるメニューをクリックします。新しい名前を入力して、 *Save*(保存) をクリックするか、 *Reset* (リセット) をクリックして列を元の名前に戻します。

これは、表ウィジェットでの列の表示名にのみ影響します。指標 / 属性名は、基になるデータ自体では変更されません。



2020年10月

統合データのデフォルトの拡張

表ウィジェットのグループ化により、 Kubernetes 、 ONTAP Advanced Data 、およびエージェントノードのデフォルトの拡張が可能になりました。たとえば、 Kubernetes Nodes *by_Cluster* をグループ化すると、クラスタごとの表に行が表示されます。そのあと、各クラスタの行を展開すると、ノードオブジェクトのリストが表示されます。

Basic Edition テクニカルサポート

Standard Edition および Premium Edition に加えて、 Cloud Insights Basic Edition をご利用のお客様にもテクニカルサポートをご利用いただけるようになりました。また、 Cloud Insights を使用すると、ネットアップサ

ポートチケットを作成するためのワークフローが簡易化されています。

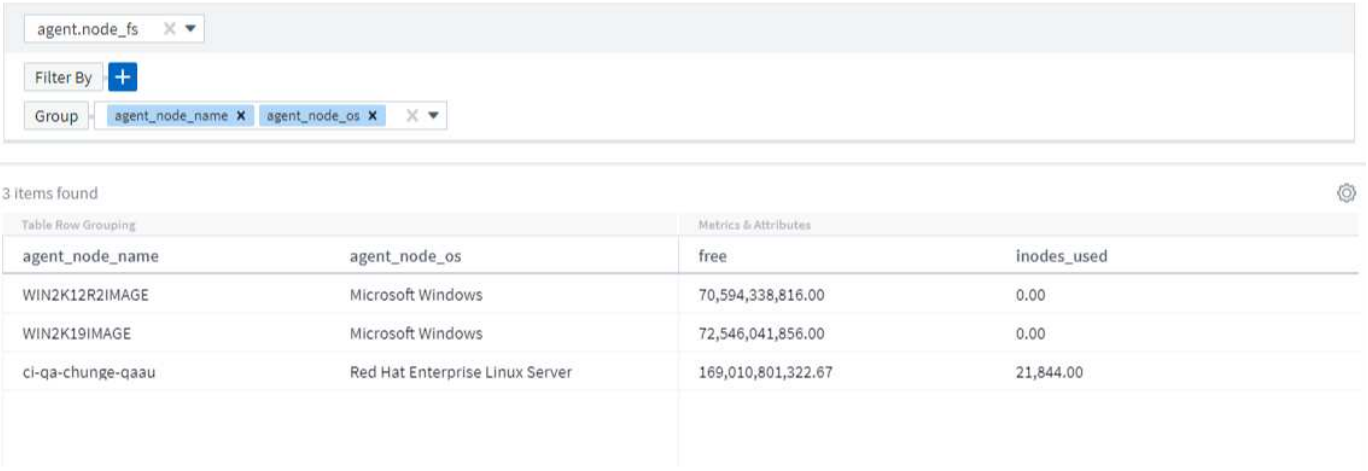
Cloud Secure 公開 API

Cloud Secure はをサポートします "REST API" アクティビティおよびアラート情報へのアクセス用。これは、 Cloud Secure 管理 UI で作成された API アクセストークンを使用して実行されます。 API アクセストークンは、 REST API にアクセスするために使用されます。Swagger の REST API のドキュメントは Cloud Secure と統合されています。

2020年9月

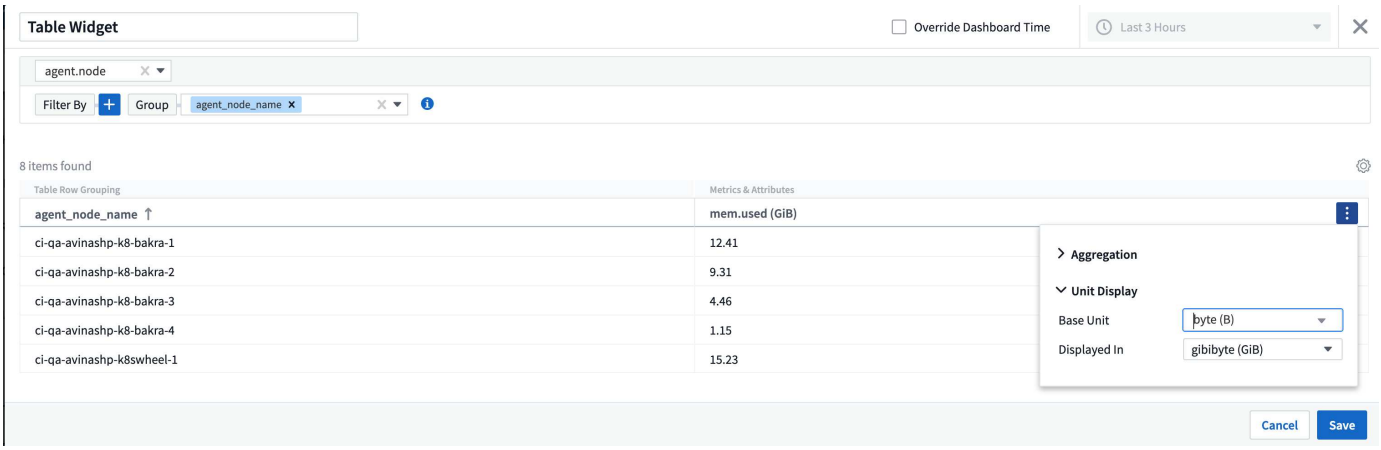
統合データを含むクエリーページ

Cloud Insights クエリページでは、統合データ（ Kubernetes 、 ONTAP Advanced Metrics など）をサポートしています。統合データを使用している場合、クエリ結果の表には「分割画面」ビューが表示され、左側にオブジェクト / グループ化が、右側にオブジェクトデータ（属性 / 指標）が表示されます。統合データをグループ化するための属性を複数選択することもできます。



表ウィジェットでの単位表示形式

表ウィジェットで、指標 / カウンタデータを表示する列（ギガバイト、 MB/ 秒など）を単位で表示できるようになりました。メトリックの表示単位を変更するには、列ヘッダーの「 3 つのドット」メニューをクリックし、「単位表示」を選択します。使用可能な任意の単位から選択できます。使用可能な単位は、表示列の指標データのタイプによって異なります。



Acquisition Unit の詳細ページ

Acquisition Unit に専用のランディングページが追加されました。このページでは、 AU ごとに役立つ詳細情報やトラブルシューティングに役立つ情報を確認できます。。 "AU 詳細ページ" AU のデータコレクタおよび有用なステータス情報へのリンクを示します。

Cloud Secure Docker 依存関係が削除されました

Cloud Secure による Docker への依存は解消されました。Cloud Secure エージェントのインストールに Docker は不要になりました。

Reporting User Roles の場合

Cloud Insights Premium Edition と Reporting を使用している場合は、環境内のすべての Cloud Insights ユーザに、 Reporting アプリケーションへのシングルサインオン（ SSO ）ログイン（など）が付与されます Cognos ）。メニューの * Reports * リンクをクリックすると、レポートに自動的にログインします。

Cloud Insights でのユーザロールによって、の割り当てが決まります "Reporting ユーザのロール"：

Cloud Insights ロール	Reporting ロール	レポート権限
ゲスト	消費者	レポートの表示、スケジュール設定、実行、および言語やタイムゾーンなどの個人設定を行うことができます。消費者は、レポートの作成や管理タスクの実行はできません。
ユーザ	作成者	すべてのコンシューマ機能を実行できるだけでなく、レポートやダッシュボードの作成と管理も可能です。
管理者	管理者	レポートの構成やレポートタスクのシャットダウンおよび再起動など、すべての管理タスクだけでなく、作成者のすべての機能も実行できます。

Cloud Insights レポートは 500 MU 以上の環境で使用できます。

現在の Premium Edition のお客様で、レポートを保持したい場合は、こちらをお読みください "既存のお客様にとって重要な注意事項です"。

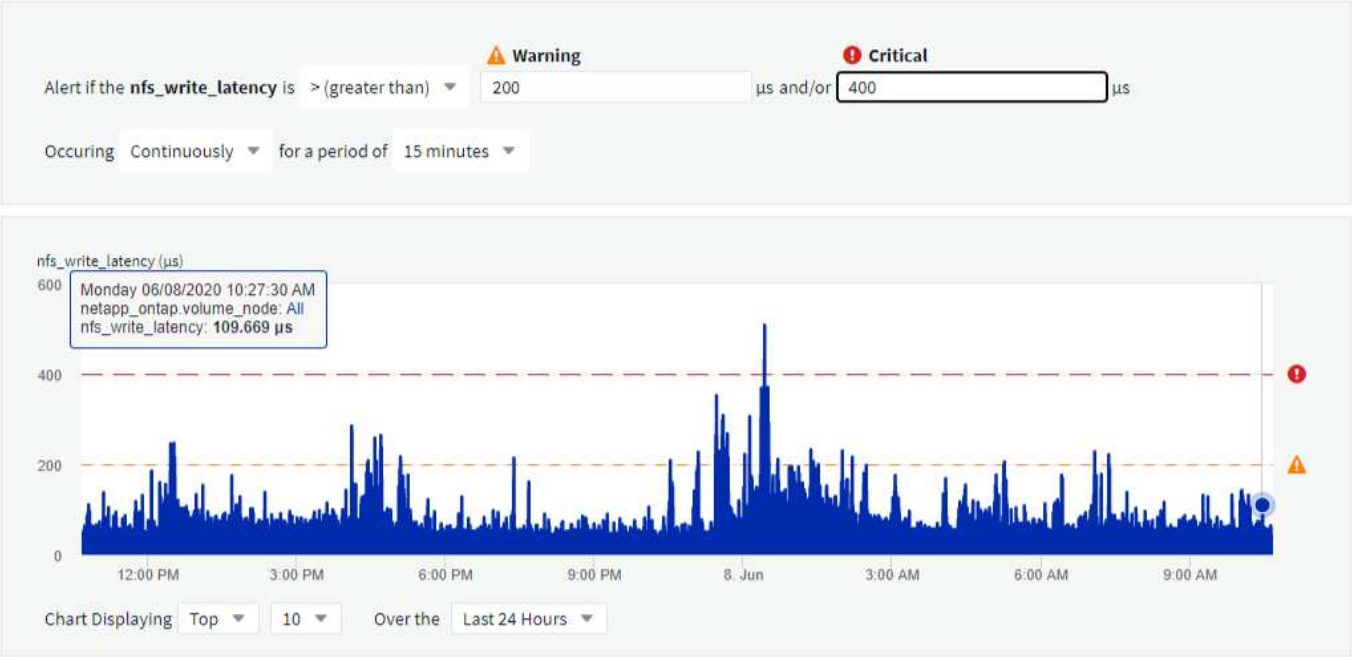
データ取り込み用の新しい **API** カテゴリ

Cloud Insights では、 * データの取り込み * API カテゴリが追加され、カスタムデータとエージェントをより詳細に制御できるようになりました。この API カテゴリおよびその他の API カテゴリの詳細なドキュメントは、 Cloud Insights で * Admin > API Access * に移動し、 _API Documentation_link をクリックすると参照できます。AUの詳細ページとAUリストページに表示される[メモ]フィールドでAUにコメントを添付することもできます。

2020年8月

監視とアラート生成

Cloud Insights Standard Edition には、ストレージオブジェクト、 VM 、 EC2 、およびポートのパフォーマンスポリシーを設定できるようになったほか、次の機能が追加されました "モニタを設定します" Kubernetes 、 ONTAP の高度な指標、 Telegraf プラグインの統合データのしきい値用。アラートをトリガーするオブジェクト指標ごとに監視を作成し、警告レベルまたは重大レベルのしきい値の条件を設定し、各レベルに必要な E メール受信者を指定するだけです。そのあとで、を実行できます "アラートを表示および管理します" 傾向を追跡したり、問題をトラブルシューティングしたりできます。



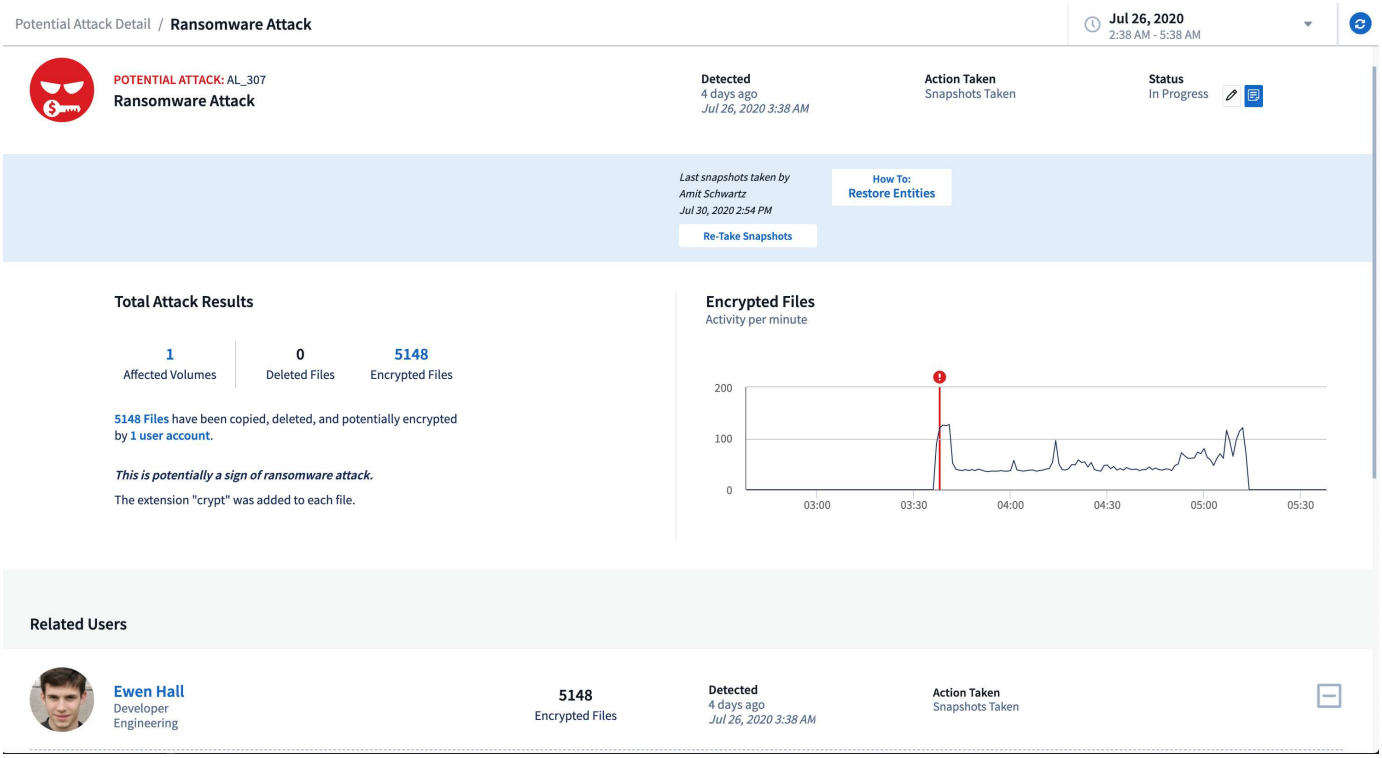
2020 年 7 月

Snapshot_Actionを実行しますCloud Secure

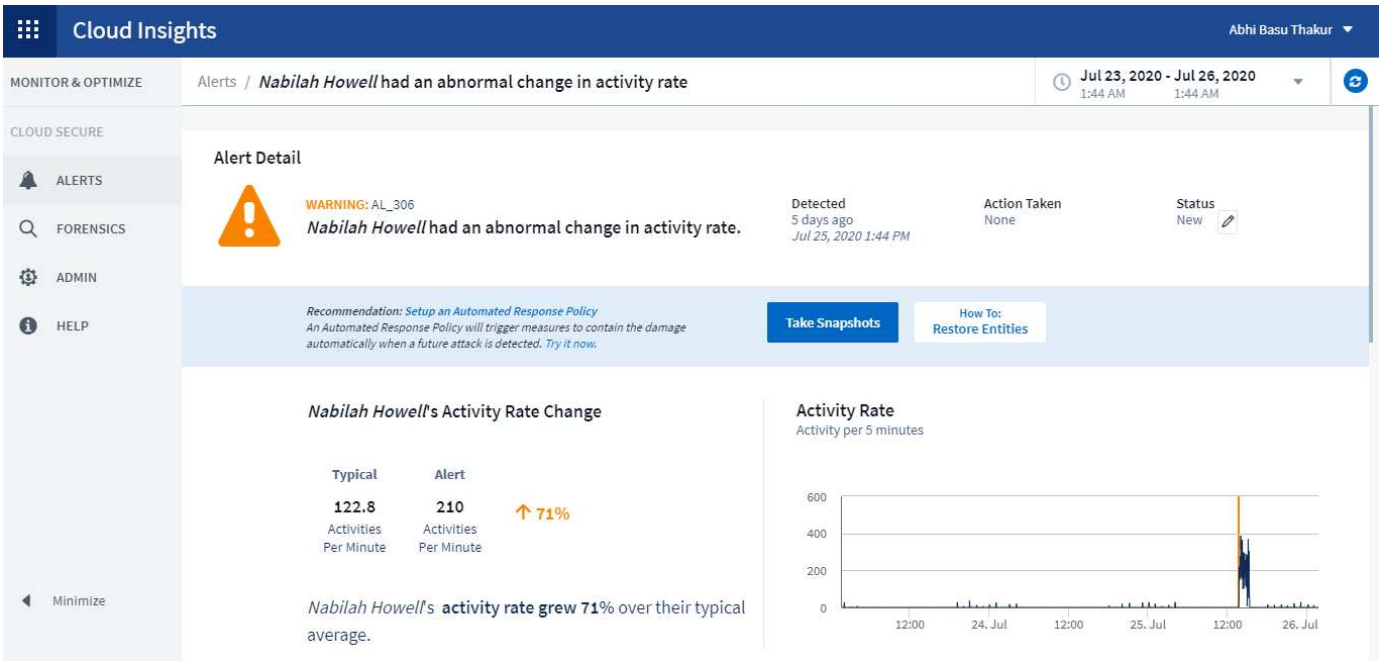
Cloud Secure は、悪意のあるアクティビティが検出されたときにスナップショットを自動的に取得することでデータを保護し、データを安全にバックアップします。

ランサムウェア攻撃やその他の異常なユーザアクティビティが検出されたときにスナップショットを取る自動応答ポリシーを定義できます。
アラートページから手動で Snapshot を作成することもできます。

自動 Snapshot の作成：



手動スナップショット：



メトリック / カウンタの更新

Cloud Insights UI および REST API で使用できる容量カウンタを次に示します。これまでは、これらのカウンタは Data Warehouse / Reporting でのみ使用できていました。

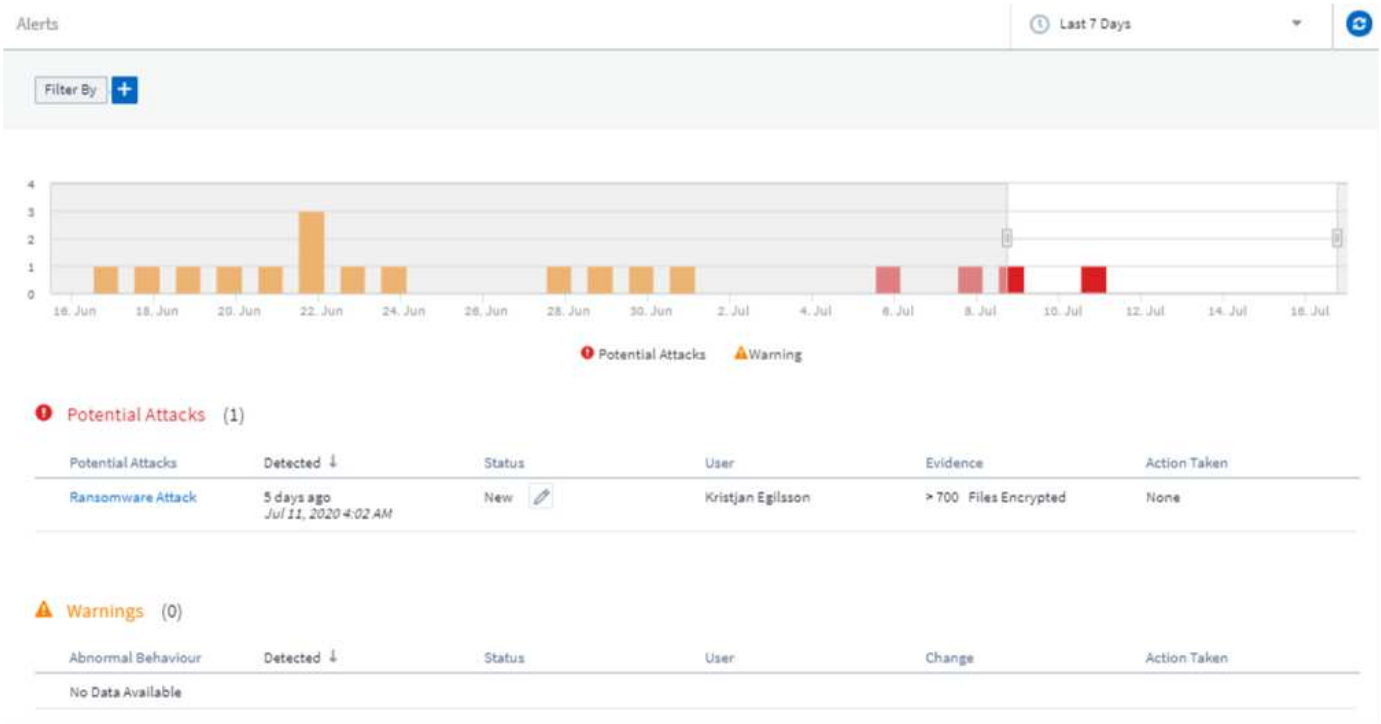
オブジェクトタイプ（ **Object Type** ）	カウンタ
ストレージ	容量-スペア物理容量 容量-物理容量で障害が発生しました
ストレージプール	Data Capacity - Usedの略 データ容量-合計 その他の容量-使用済み その他の容量-合計 容量-物理容量 容量-ソフトリミット
内部ボリューム	Data Capacity - Usedの略 データ容量-合計 その他の容量-使用済み その他の容量-合計 クローンの削減容量-合計

Cloud Secure の潜在的な攻撃検出

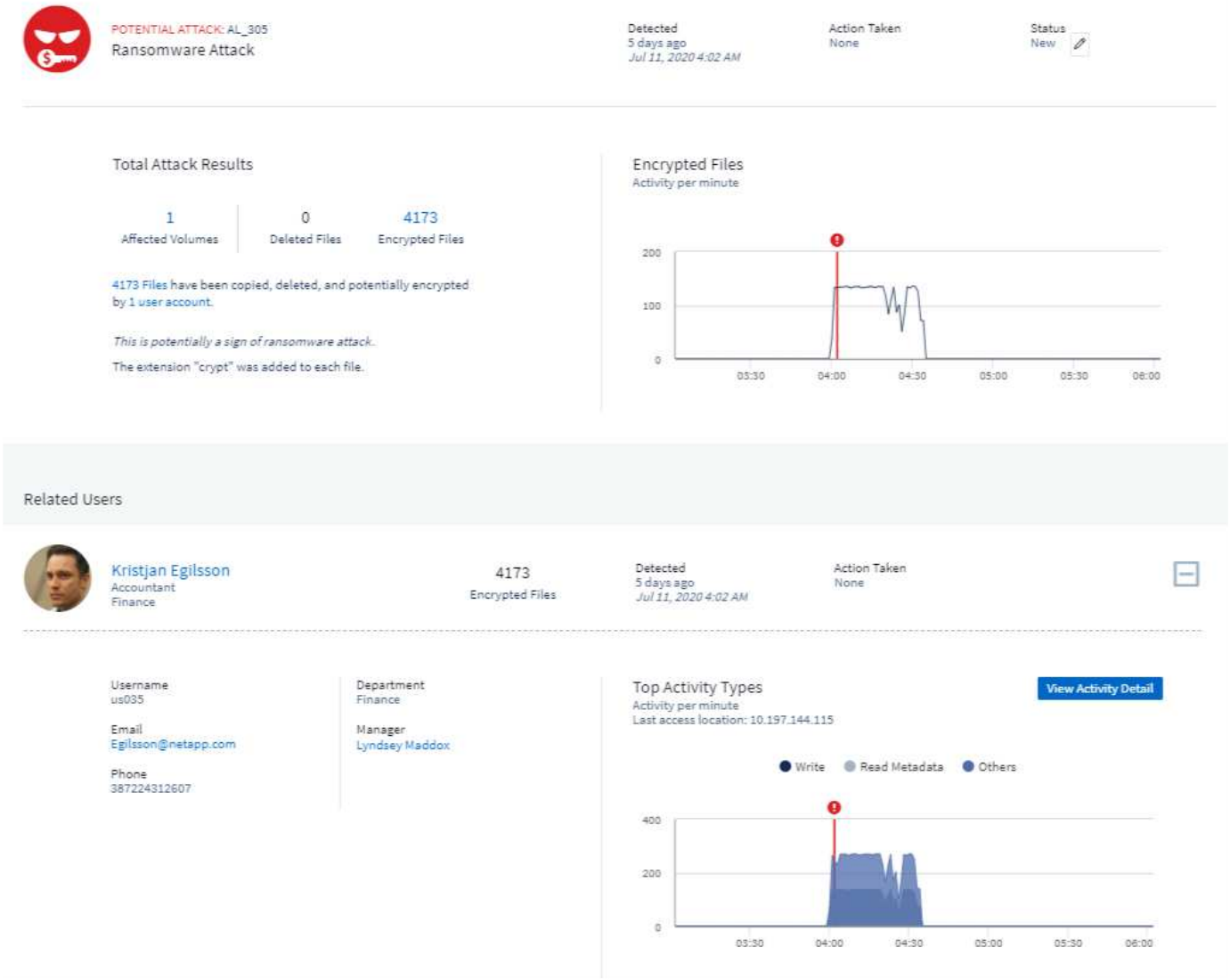
Cloud Secure はランサムウェアなどの潜在的な攻撃を検出するようになりました[Alerts] リストページでアラートをクリックすると ' 次のような詳細ページが開きます

- 攻撃の時間
- 関連付けられているユーザおよびファイルアクティビティ
- 実行されたアクション
- 追加情報は、潜在的なセキュリティ違反の追跡を支援します

ランサムウェア攻撃の可能性を示すアラートページ：



ランサムウェア攻撃の詳細ページ：



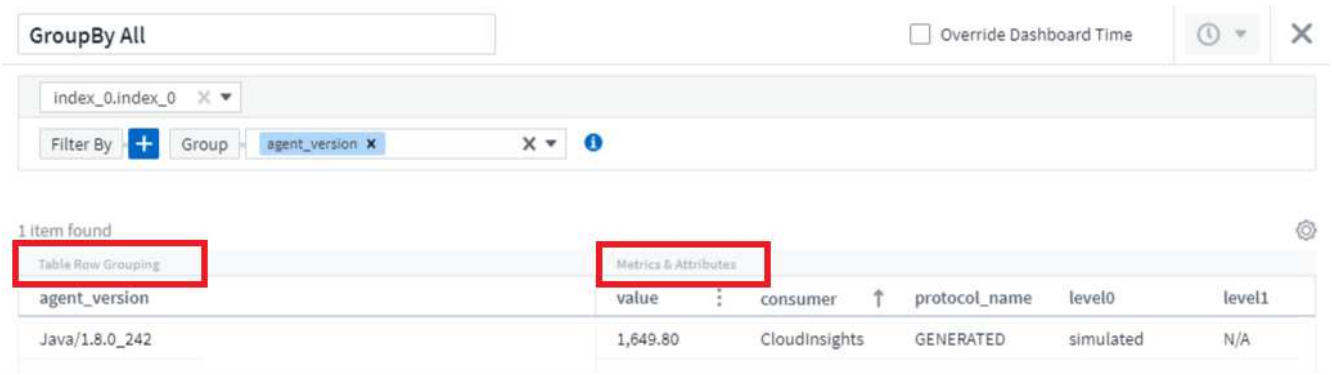
AWS で Premium Edition に登録

Cloud Insights の試用期間中は、次の操作を実行できます "セルフサブスクライブ" AWS Marketplace から Cloud Insights Standard Edition または Premium Edition に移動する。これまでは、 AWS Marketplace でのみ Standard Edition に自分で登録することができました。

拡張テーブルウィジェット

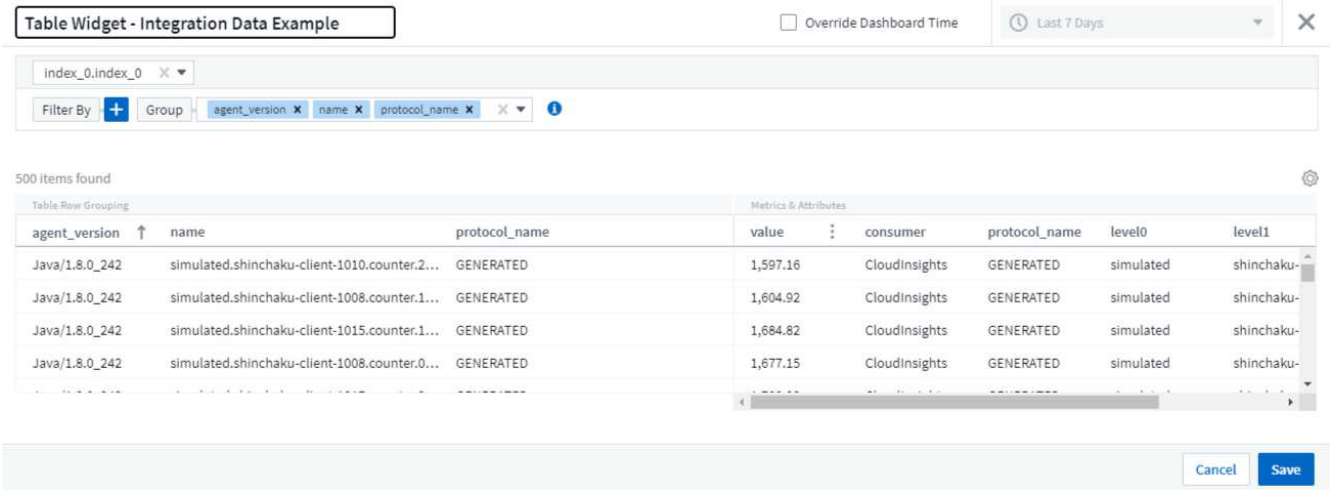
ダッシュボード / アセットページの表ウィジェットには、次の拡張機能が含まれています。

- 「分割画面」ビュー：表ウィジェットの左側にはオブジェクト / グループ化、右側にはオブジェクトデータ（属性 / 指標）が表示されます。



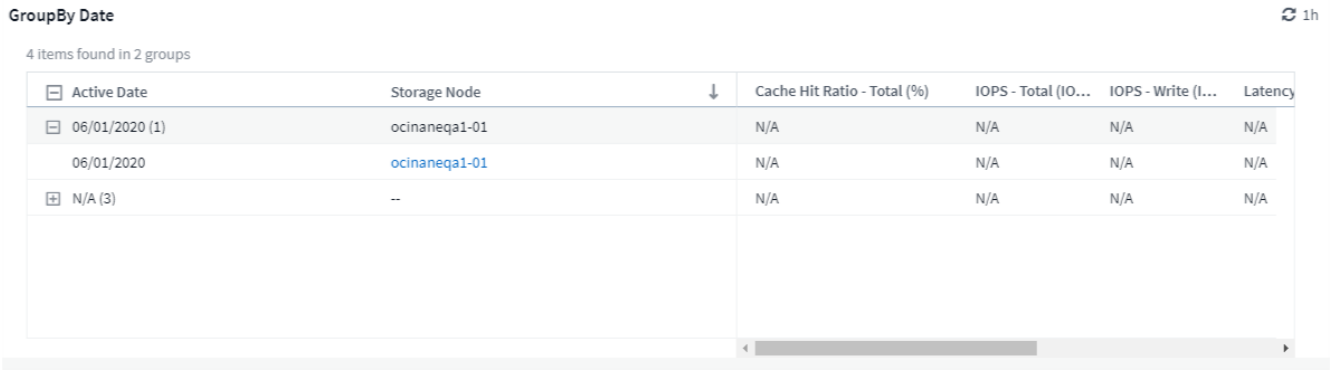
- 複数の属性のグループ化：統合データ（ Kubernetes 、 ONTAP Advanced Metrics 、 Docker など）については、グループ化の対象として複数の属性を選択できます。選択したグループ化属性に従ってデータが表示されます。

  統合データによるグループ化（編集モードで表示）：



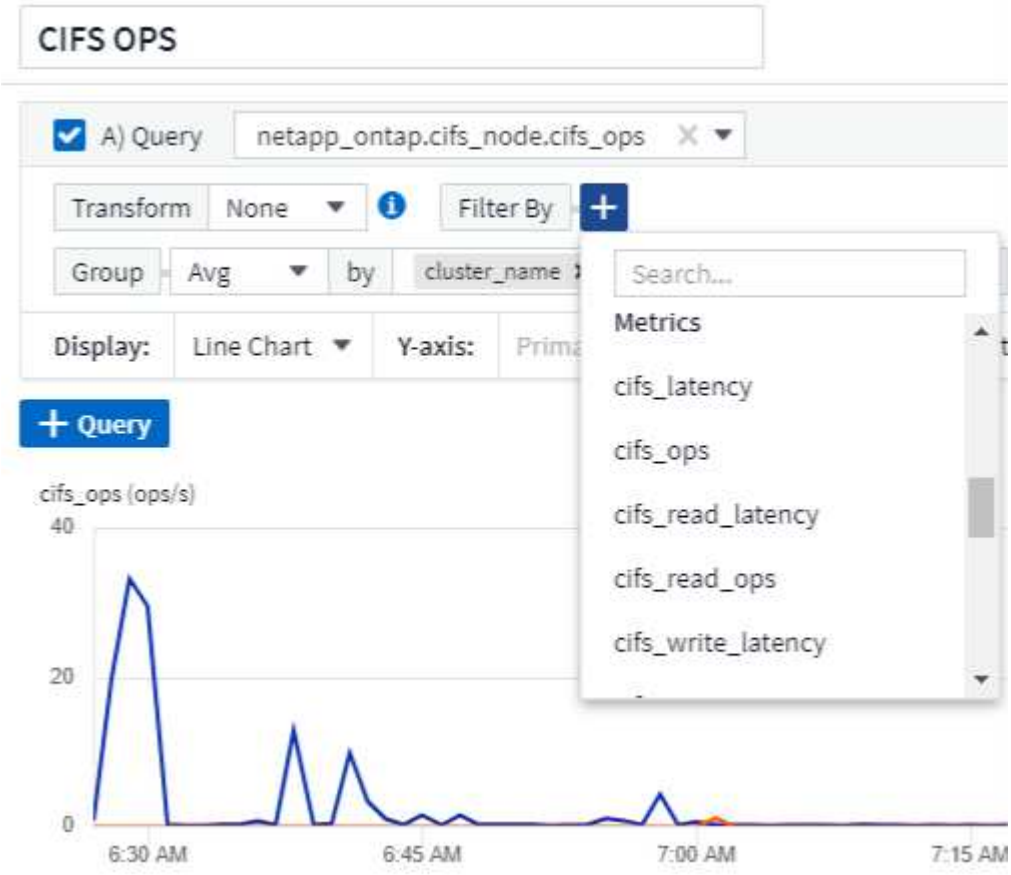
- インフラデータ（ストレージ、 EC2 、 VM 、ポートなど）をグループ化することは、従来と同様に単一の属性によって行われます。オブジェクトではない属性によってグループ化する場合、テーブルでグループ行を展開すると、グループ内のすべてのオブジェクトが表示されます。

  インフラストラクチャデータによるグループ化（表示モードで表示）：

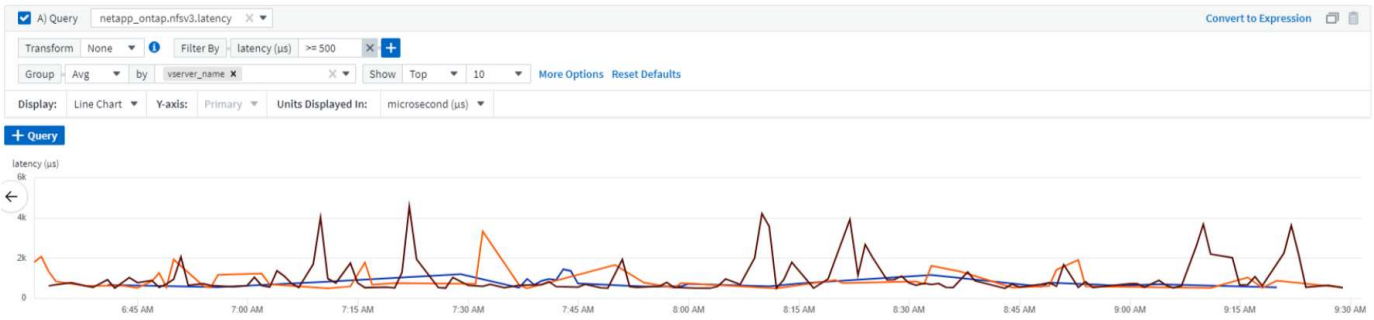


メトリックフィルタリング

ウィジェット内のオブジェクトの属性でフィルタリングできるだけでなく、指標もフィルタリングできるようになりました。



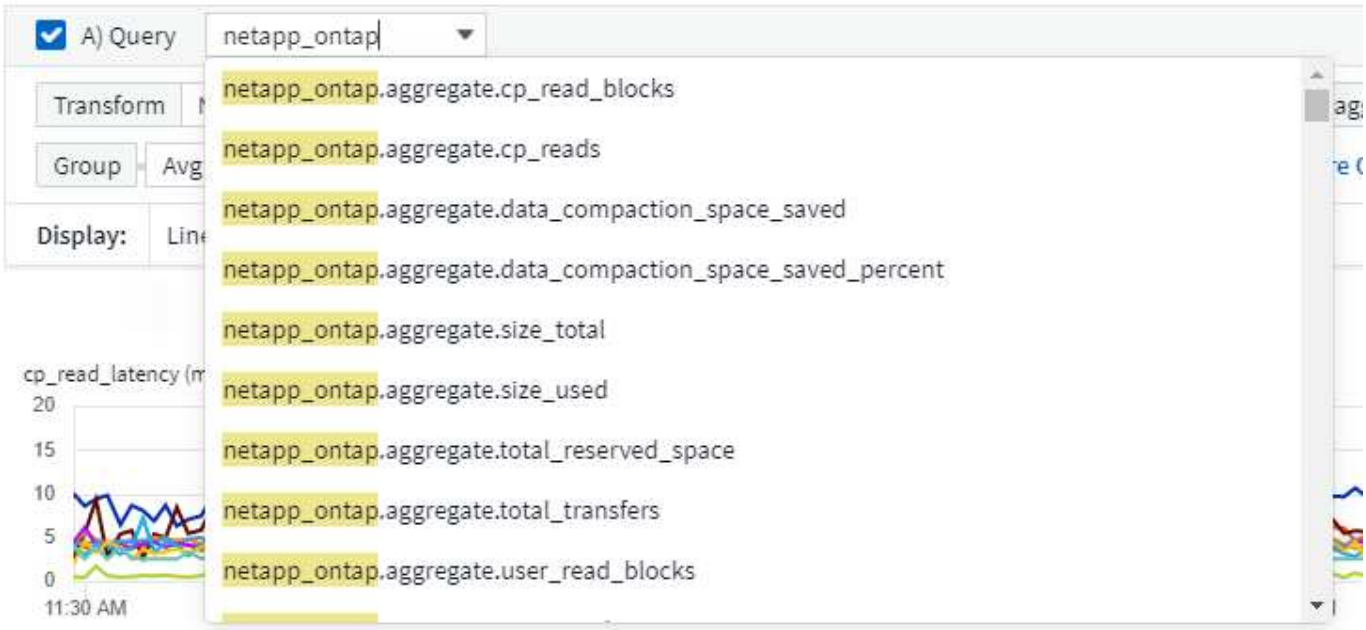
統合データ（ Kubernetes 、 ONTAP 高度なデータなど）を使用する場合、指標フィルタリングを使用すると、データ系列の集計値でフィルタが機能し、グラフからオブジェクト全体が削除されるのとは異なり、プロットされたデータ系列から個々のデータポイントや一致しないデータポイントが削除されます。



ONTAP 詳細カウンタデータ

Cloud Insights は、 ONTAP デバイスから収集された多数のカウンタと指標を提供する NetApp ONTAP 固有の * Advanced Counter Data * を利用しています。 ONTAP の Advanced Counter データは、ネットアップのすべてのお客様がご利用になれます。 ONTAPこれらの指標を使用して、 Cloud Insights のウィジェットやダッシュボードで、カスタマイズした幅広いデータを視覚化できます。

ONTAP の高度なカウンタを確認するには、ウィジェットのクエリで「 NetApp_ONTAP 」を検索し、カウンタから選択します。



カウンタ名の一部を入力することで、検索条件を絞り込むことができます。例：

- LIF _
- _ アグリゲート _
- _ 外付け _ VScan サーバ _
- その他

次の点に注意してください。

- 新しい ONTAP データコレクタでは、高度なデータ収集がデフォルトで有効になります。既存の ONTAP データコレクタに対して高度なデータ収集を有効にするには、データコレクタを編集し、 _Advanced Configuration_Section を展開します。
- 7-Mode の ONTAP では高度なデータ収集を使用できません。

Advanced Counter Dashboards のことです

Cloud Insights には、 ONTAP アドバンストカウンタの可視化を開始するのに役立つ、さまざまな設計済みダッシュボードが用意されています。これらのダッシュボードでは、 _ アグリゲートパフォーマンス _ 、 _ ボリュームワークロード _ 、 _ プロセッサアクティビティ _ などのトピックを確認できます。ONTAP データコレクタが 1 つ以上設定されている場合は、ダッシュボード一覧ページのダッシュボードギャラリーからインポートできます。

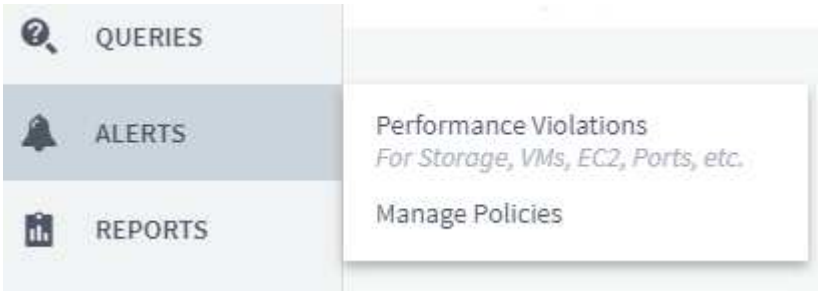
詳細はこちら。

ONTAP 詳細データの詳細については、次のリンクを参照してください。

- https://mysupport.netapp.com/site/tools/tool-eula/netapp-harvest （注：ネットアップサポートにサインインする必要があります）。
- https://nabox.org/faq/

ポリシーと違反メニュー

パフォーマンスポリシーと違反が [* アラート] メニューに表示されるようになりました。ポリシーと違反機能は変更されません。



Telegraf Agent を更新

テレグラム統合データの取り込み用エージェントがに更新されました "バージョン 1.14"には、バグ修正、セキュリティ修正、および新しいプラグインが含まれています。

注： Kubernetes プラットフォームで Kubernetes データコレクタを設定する際、「 clusterrole 」属性に必要な権限がないため、ログに「 HTTP status 403 Forbidden 」エラーが表示されることがあります。

この問題を回避するには、エンドポイントアクセスクラスタロールの _rules に以下の強調表示された行を追加し、 Tegraf ポッドを再起動します。

```
rules:
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - extensions
  - policy
  - rbac.authorization.k8s.io
  attributeRestrictions: null
  resources:
  - nodes/metrics
  - nodes/proxy     <== Add this line
  - nodes/stats
  - pods            <== Add this line
  verbs:
  - get
  - list            <== Add this line
```

2020 年 6 月

Data Collector エラーレポートの簡易化

データコレクタページの *Send Error Report* ボタンを使用すると、データコレクタエラーのレポートが簡単になります。ボタンをクリックすると、エラーに関する基本情報がネットアップに送信され、問題の調査が求められます。Cloud Insights を押すと、ネットアップに通知されたことを示すメッセージが表示され、 Error Report ボタンが無効になります。このボタンをクリックすると、データコレクタについてのエラーレポートが送信されたことを示します。このボタンは、ブラウザページが更新されるまで無効のままです。

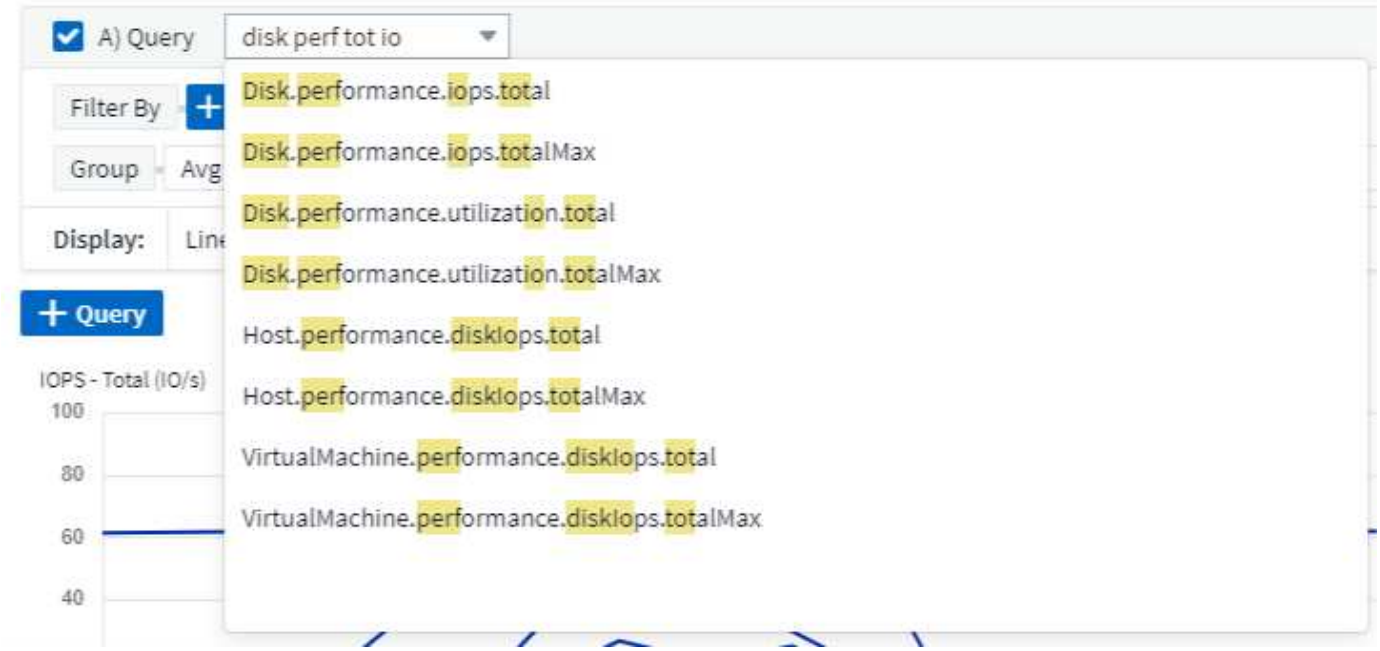
ボタン"]

ウィジェットの改良

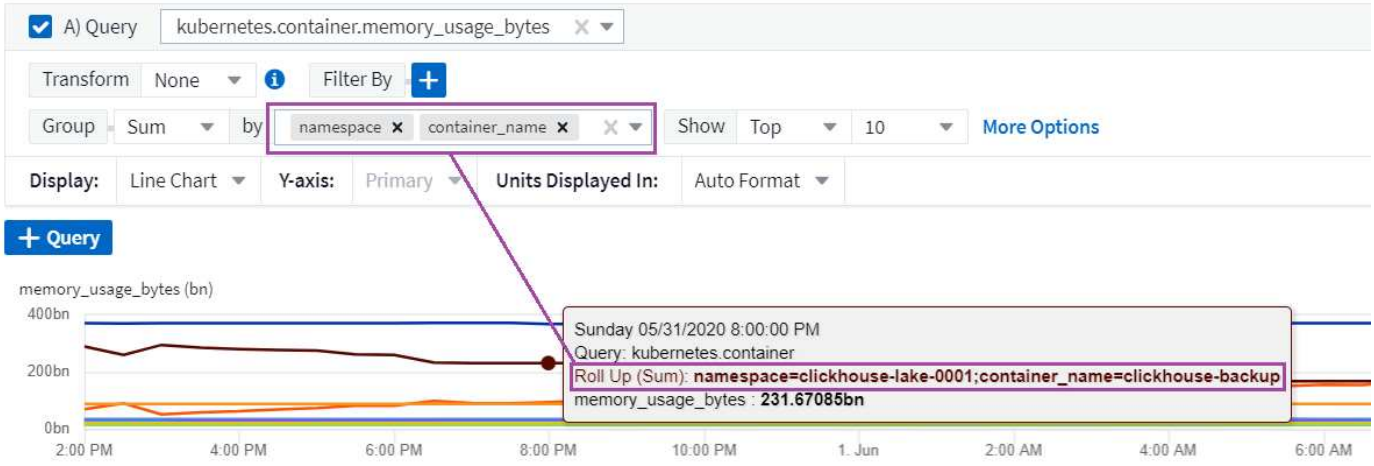
ダッシュボードウィジェットでは、次の点が強化されています。これらの機能強化はプレビュー機能とみなされ、すべての Cloud Insights 環境で利用できるわけではありません。

- 新しいオブジェクト / 指標選択機能：オブジェクト（ストレージ、ディスク、ポート、ノードなど）と関連する指標（ IOPS 、レイテンシ、 CPU 数など）を、強力な検索機能を備えた 1 つの包括的なドロップダウンウィジェットで使用できるようになりました。ドロップダウンに複数の条件を部分的に入力する

と、それらの条件を満たすすべてのオブジェクト指標が Cloud Insights に表示されます。



- 複数のタグのグループ化：統合データ（ Kubernetes など）を操作する場合、複数のタグ / 属性でデータをグループ化できます。たとえば、 Kubernetes のネームスペースとコンテナ名別のメモリ使用量の合計です。



2020年5月

Reporting User Roles の場合

Reporting に追加されたロールは次のとおりです。

- Cloud Insights コンシューマ：レポートの実行と表示が可能です
- Cloud Insights Author ： Consumer 機能を実行できるほか、レポートやダッシュボードを作成、管理することもできます

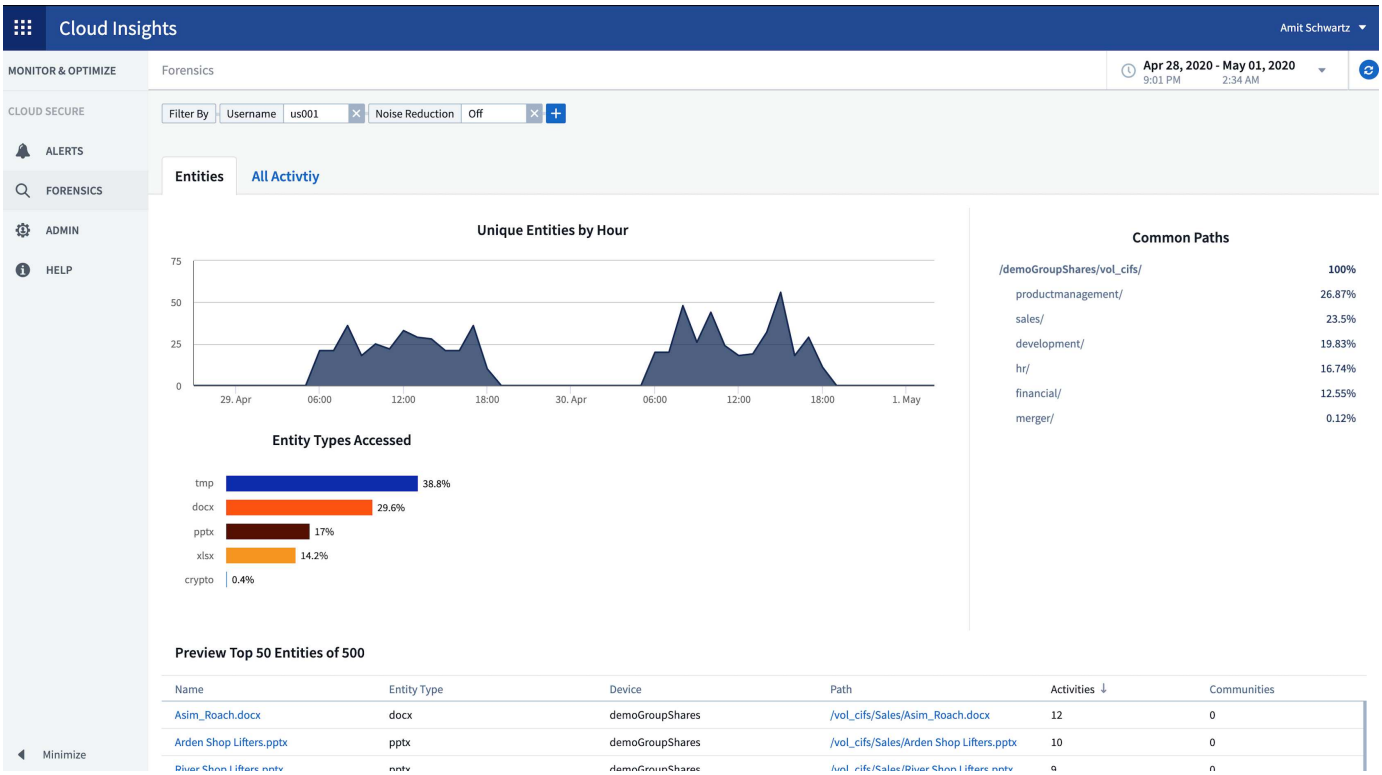
- Cloud Insights 管理者：作成者機能およびすべての管理タスクを実行できます

Cloud Secure アップデート

Cloud Insights では、 Cloud Secure に関する次の最近の変更が行われています

Forensics > Activity Forensics ページでは、ユーザーアクティビティを分析および調査するための 2 つのビューを提供しています。

- ユーザアクティビティに重点を置いたアクティビティビュー（操作は何か？どこで実施したか？）
- ユーザーがアクセスしたファイルに焦点を合わせたエンティティビュー。

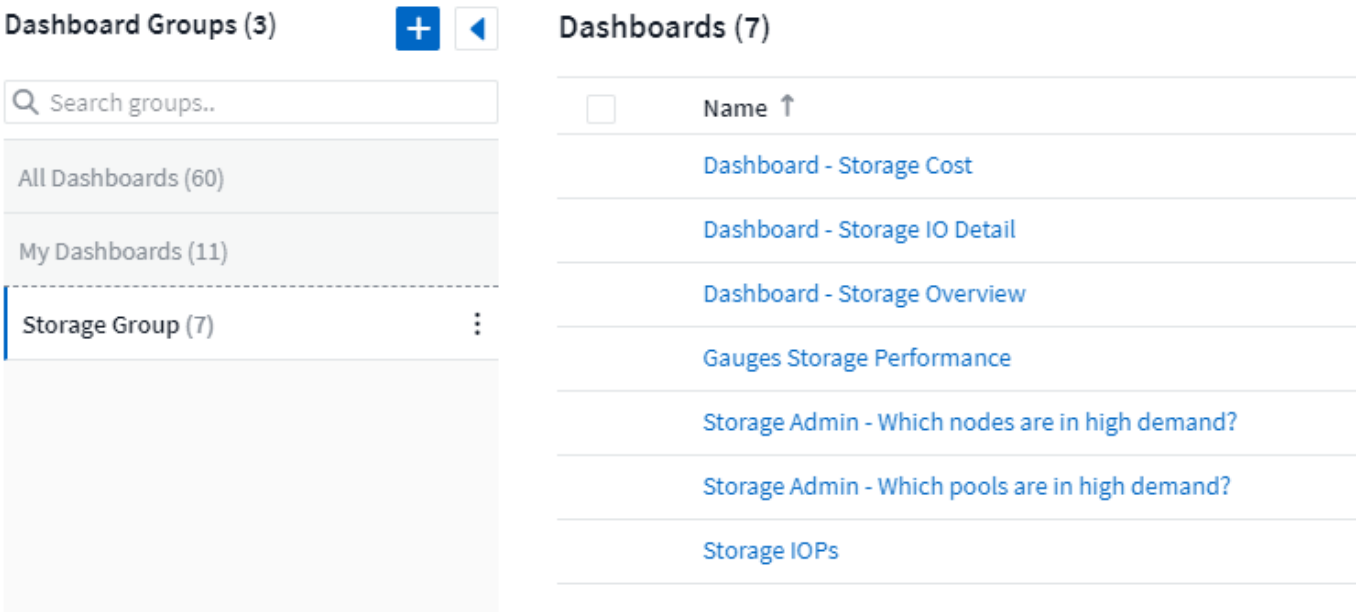


また、アラート E メール通知にアラートページへの直接リンクが追加されました。

ダッシュボードのグループ化

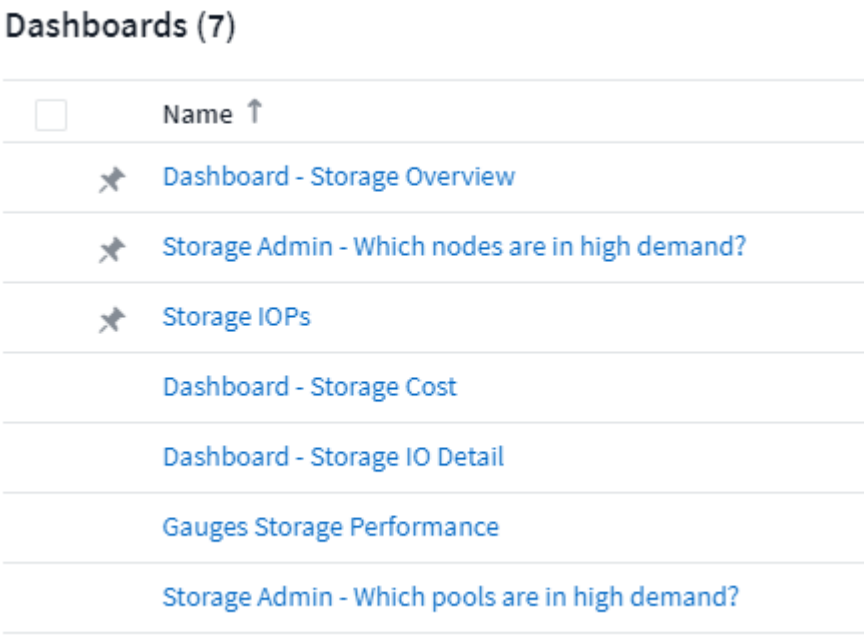
ダッシュボードのグループ化により、パフォーマンスが向上します " ダッシュボードの管理" あなたに関係があります。関連するダッシュボードをグループに追加して、ストレージや仮想マシンなどを「ワンストップ」で管理できます。

グループはユーザごとにカスタマイズされるため、 1 人のグループが他のユーザと異なる場合があります。グループは必要な数だけ作成でき、各グループにダッシュボードをいくつでも配置できます。



ダッシュボードのピン留め

お気に入りが常にリストの先頭に表示されるように、ダッシュボードを固定することができます。



TV モードと自動更新

"TV モードと自動更新" ダッシュボードやアセットページにほぼリアルタイムでデータを表示できます。

- *TV モード * は、すっきりとしたディスプレイを提供します。ナビゲーションメニューは非表示になっており、データ表示用の画面のスペースが増えます。
- ダッシュボードとアセットランディングページのウィジェットのデータ * 自動更新 * 選択したダッシュボードの期間（ダッシュボードの時間を上書きするように設定されている場合は、ウィジェットの時間範囲

）で設定された更新間隔（ 10 秒ごと）に基づいてデータが表示されます。

TV モードと自動更新機能を組み合わせることで、 Cloud Insights データのライブビューが提供され、シームレスなデモンストレーションや社内モニタリングに最適です。

（2020年4月

ダッシュボードの新しい時間範囲の選択肢

ダッシュボードおよびその他の Cloud Insights ページの時間範囲の選択に *Last 1 Hour_Last 15 Minutes* が含まれるようになりました。

Cloud Secure アップデート

Cloud Insights では、 Cloud Secure に関する次の最近の変更が行われています

- ファイルおよびフォルダのメタデータの変更が認識され、ユーザが権限、所有者、またはグループ所有権を変更したかどうかを確認できるようになりました。
- ユーザアクティビティレポートを CSV にエクスポートします。

Cloud Secure は、ファイルおよびフォルダに対するすべてのユーザアクセス操作を監視して監査します。アクティビティ監査では、内部セキュリティポリシーへの準拠、 PCI 、 GDPR 、 HIPAA などの外部コンプライアンス要件への準拠、データ侵害やセキュリティインシデント調査を実施できます。

デフォルトのダッシュボード時間

ダッシュボードのデフォルトの期間は、 24 時間ではなく 3 時間に変更されました。

集約時間の最適化

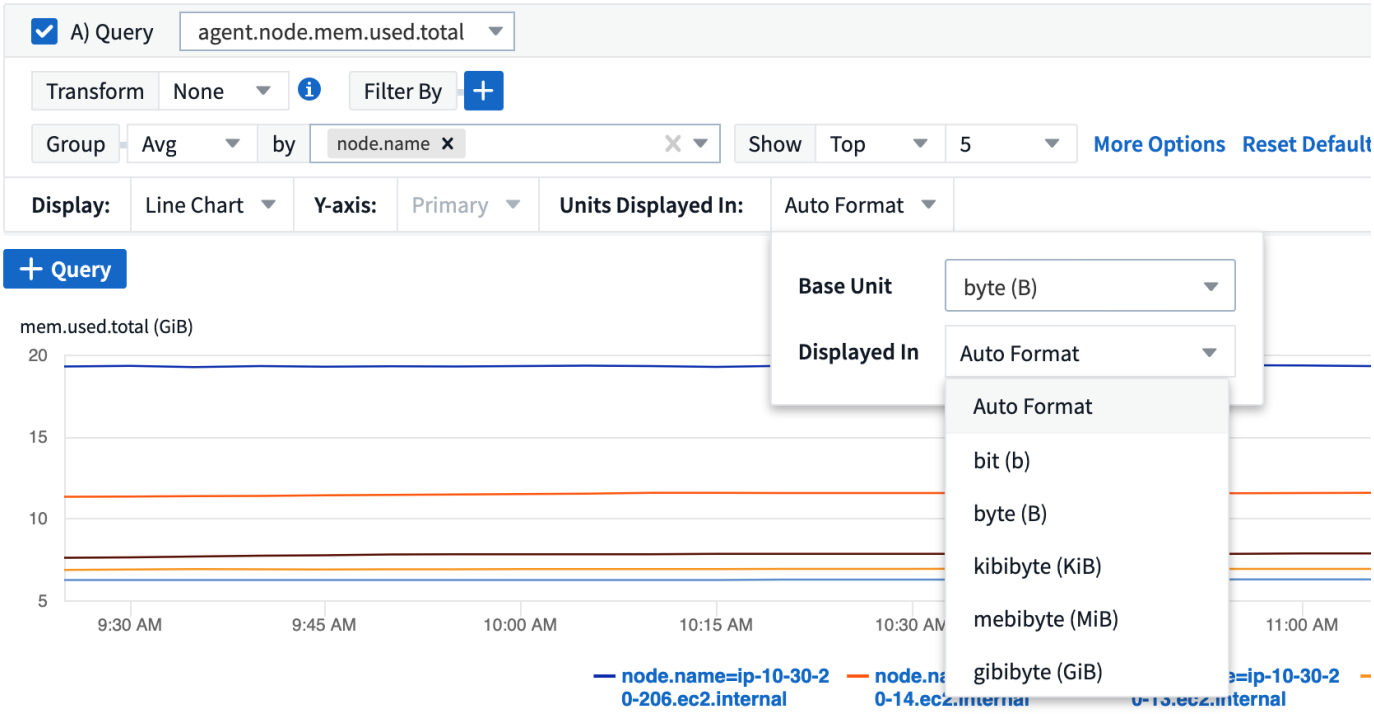
最適化 "時間の集約" タイムシリーズウィジェット（ライン、スプライン、エリア、積み上げ面グラフ）の間隔は、ダッシュボード / ウィジェットの 3 時間および 24 時間の時間範囲でより頻繁になり、データをより迅速にグラフ化できます。

- 3 時間の時間範囲は、 1 分の集約間隔に最適化されます。これまでは 5 分でした。
- 24時間の時間範囲は、30分の集約間隔に最適化されます。以前は 1 時間でしたが、

カスタムインターバルを設定して、最適化された集計を上書きすることもできます。

単位の自動フォーマットを表示します

ほとんどのウィジェットでは、 Cloud Insights は値を表示するベースユニットを認識しています。たとえば、*mabm*,*unse*,*percent*,_milliseconds(ms) _ 、 など "自動的にフォーマットします" 最も読み取り可能な単位のウィジェット。たとえば、データ値が 1 、 234 、 5678 、 890 バイトの場合、自動的に 1.23 ギビバイトにフォーマットされます。多くの場合、 Cloud Insights は取得するデータの最適な形式を認識しています。最適な形式がわからない場合や、自動書式設定を上書きするウィジェットの場合は、目的の形式を選択できます。

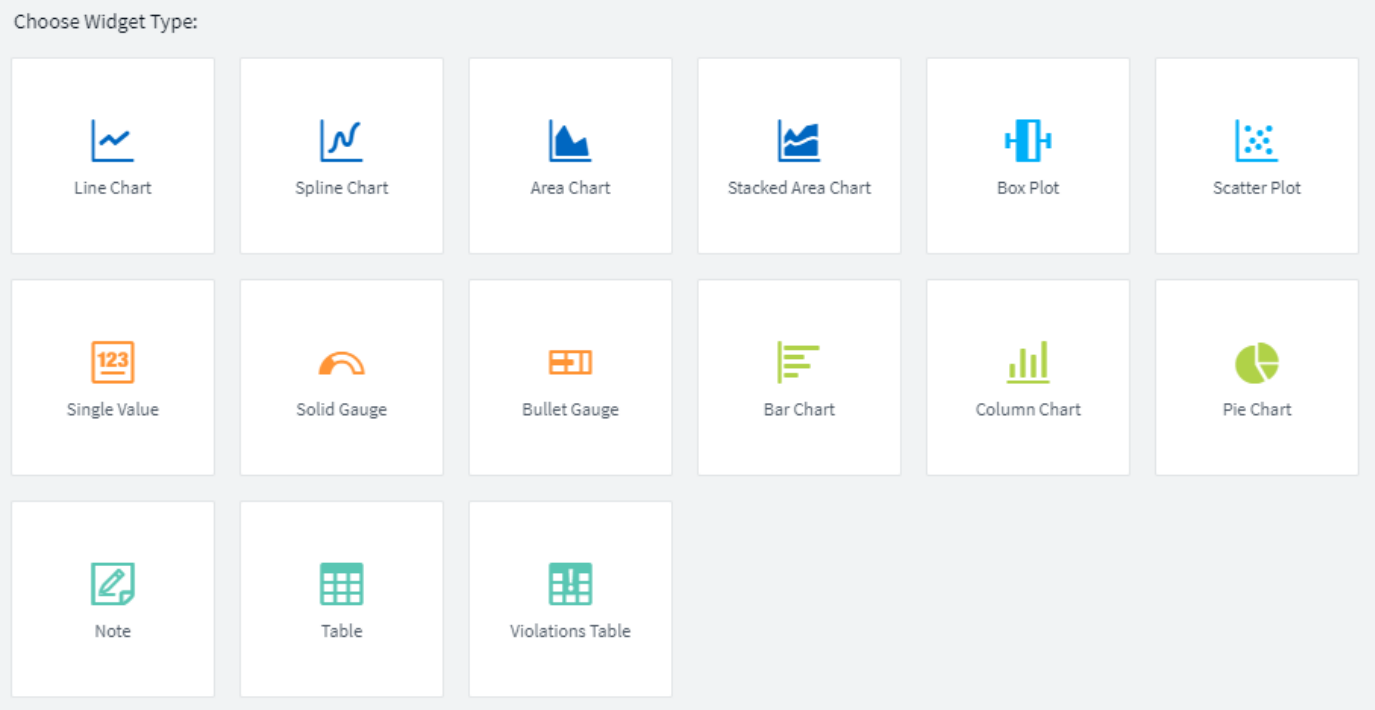


API を使用してアノテーションをインポート

Cloud Insights Premium Edition の強力な API を使用して、次のことが可能になりました "アノテーションをインポートする" をクリックし、 .csv ファイルを使用してオブジェクトに割り当てます。アプリケーションをインポートし、ビジネスエンティティを同じように割り当てることもできます。

ウィジェットセレクタの簡易化

すべてのウィジェットタイプを 1 つの一度に表示する新しいウィジェットセレクタでは、ダッシュボードやアセットランディングページにウィジェットを簡単に追加できます。追加するウィジェットタイプを特定するために、ウィジェットタイプのリストをスクロールする必要がなくなりました。関連ウィジェットは、新しいセレクタの近くで色分けされ、グループ化されます。



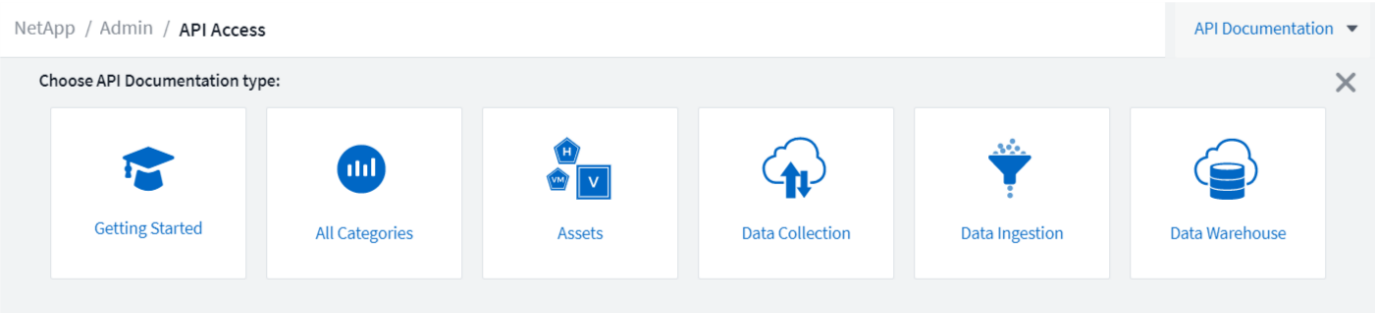
（2020年2月

Premium Edition の API

Cloud Insights Premium Edition には、が付属しています "強力な API" これを使用して、 Cloud Insights を CMDB や他のチケットシステムなどの他のアプリケーションと統合できます。

Swagger ベースの詳細情報は、 * Admin > API Acccess * の * API Documentation リンクから参照できます。Swagger では、 API の簡単な概要情報と使用状況の情報を提供しており、環境内の各 API を試すことができます。

Cloud Insights API では、アクセストークンを使用して、資産や収集などのカテゴリの API にアクセスする権限ベースのアクセスを提供します。



Data Collector を追加した後の初期ポーリング

以前は、新しいデータコレクタを設定すると、 Cloud Insights はデータコレクタをただちにポーリングして collector_inventory_data を収集しましたが、設定されたパフォーマンスポーリング間隔（通常は 15 分）まで

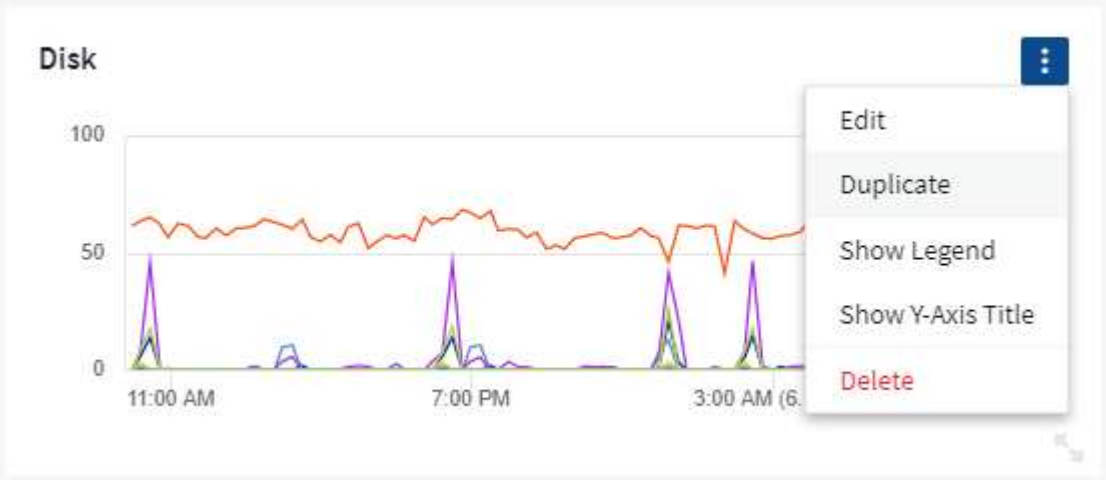
待機して initial_performion_data が収集されます。そのあと、別の間隔を待ってから 2 回目のパフォーマンスポーリングを開始します。つまり、新しいデータコレクタから有意義なデータが取得されるまでに、最大 30 分 _ かかることになります。

データコレクタ "ポーリング" は、インベントリのポーリング直後に最初のパフォーマンスポーリングが行われるように大幅に改善され、最初のパフォーマンスポーリングが完了してから数秒以内に 2 番目のパフォーマンスポーリングが実行されるようになりました。これにより、 Cloud Insights は、非常に短時間でダッシュボードやグラフに有用なデータの表示を開始できます。

このポーリング動作は、既存のデータコレクタの設定を編集したあとにも発生します。

ウィジェットの重複を容易にします

ダッシュボードやランディングページにウィジェットのコピーを簡単に作成できるようになりました。ダッシュボード編集モードで、ウィジェットのメニューをクリックし、 * 複製 * を選択します。ウィジェットエディタが起動し、元のウィジェットの設定とウィジェット名に「 copy 」というサフィックスが付きます。必要な変更を簡単に加えて、新しいウィジェットを保存することができます。ウィジェットはダッシュボードの下部に配置され、必要に応じて配置することができます。すべての変更が完了したら、必ずダッシュボードを保存してください。



シングルサインオン（ SSO ）

Cloud Insights Premium Edition では、管理者は * を有効にできます"単一 Sign-On"* （ SSO ）は、企業ドメイン内のすべてのユーザの Cloud Insights へのアクセスを個別に招待する必要がありません。SSO が有効になっている場合、同じドメインの E メールアドレスを持つすべてのユーザは、各自の企業クレデンシャルを使用して Cloud Insights にログインできます。

SSO は Cloud Insights Premium Edition でのみ使用可能で、 Cloud Insights で有効にする前に設定する必要があります。SSO 設定にはが含まれます "アイデンティティフェデレーション" NetApp Cloud Central を使用フェデレーションを使用すると、シングルサインオンユーザが、社内ディレクトリのクレデンシャルを使用して NetApp Cloud Central アカウントにアクセスできます。

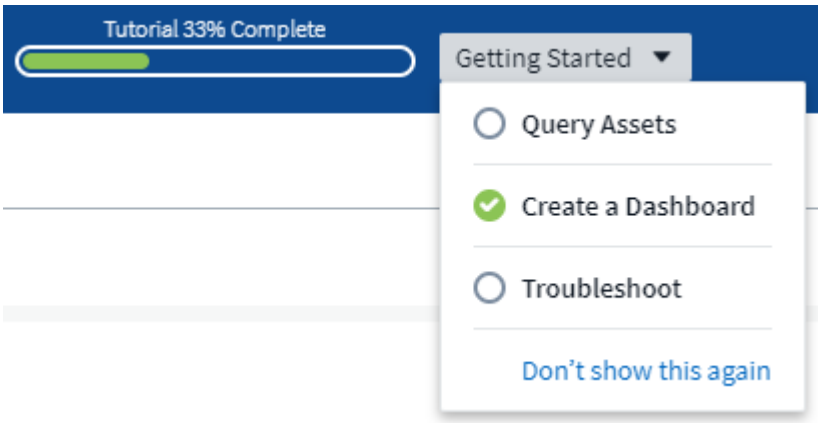
2020年1月

Swagger REST API のドキュメント

Swagger では、 Cloud Insights で使用可能な REST API のほか、その用途や構文についても説明しています。Cloud Insights API の詳細については、を参照してください "ドキュメント"。

Feature Tutorials Progress Bar (機能チュートリアルの進行状況

機能チュートリアルのチェックリストは上部のバナーに移動され、進行状況を示すインジケータが表示されます。チュートリアルは、閉じるまで各ユーザーに提供され、 Cloud Insights では常に利用できます "ドキュメント"。



Acquisition Unit の変更

Acquisition Unit （ AU ）をインストール済みの AU と同じ名前のホストまたは VM にインストールする場合、 Cloud Insights では、 AU 名に「 _1 」、「 _2 」を追加して一意の名前が保証されます。 など。これは、最初に Cloud Insights から AU を削除せずに、同じ VM から AU をアンインストールして再インストールする場合にも当てはまります。別の AU 名を使用したい場合は、問題ありません。インストール後に AU の名前を変更できます。

ウィジェットの時間集約を最適化

ウィジェットでは、設定した _Optimised _ time 集計間隔または _Custom_interval のいずれかを選択できます。最適化された集計では、ダッシュボードで選択した時間範囲（ダッシュボードの時間を上書きする場合はウィジェットの時間範囲）に基づいて、適切な時間間隔が自動的に選択されます。間隔は、ダッシュボードまたはウィジェットの時間範囲が変更されると動的に変わります。

「 Getting Started with Cloud Insights 」プロセスがシンプルになりました

Cloud Insights の使用を開始するプロセスが簡易化され、初回セットアップがスムーズになり、簡単になりました。最初のデータコレクタを選択し、指示に従います。Cloud Insights では、データコレクタと、必要なエージェントまたは Acquisition Unit の設定手順を説明します。ほとんどの場合、最初のダッシュボードも 1 つ以上インポートするため、環境に関する分析情報を短時間で取得できます（ Cloud Insights で意味のあるデータを収集するには最大 30 分かかります）。

その他の改善点：

- Acquisition Unit のインストールはシンプルで、処理も高速です。
- [アルファベット順のデータコレクタ] を選択すると、探しているデータコレクタを簡単に見つけることができます。
- Data Collector のセットアップ手順の改善がより簡単になりました。
- 経験豊富なユーザーは、ボタンをクリックするだけで、開始プロセスを省略できます。
- 新しい進行状況バーには、進行中の状態が表示されます。

（2019年12月

ビジネスエンティティはフィルタで使用できます

ビジネスエンティティのアノテーションは、クエリ、ウィジェット、パフォーマンスポリシー、およびランディングページのフィルタで使用できます。

ドリルダウンは、単一値ウィジェットとゲージウィジェット、および「すべて」でロールされたウィジェットで使用できます。

単一値ウィジェットまたはゲージウィジェットの値をクリックすると、ウィジェットで最初に使用されたクエリの結果を示すクエリページが開きます。また、データが「すべて」で集計されているウィジェットの凡例をクリックすると、ウィジェットで最初に使用したクエリの結果を示すクエリページも開きます。

試用期間が延長されました

Cloud Insights の無償トライアルに登録された新規ユーザは、製品を評価するために 30 日間の期間を用意しています。これは、過去 14 日間の試用期間からの増加です。

管理ユニットの計算

Cloud Insights の管理ユニット（ MU ）の計算が次のように変更されました。

- 1 台の管理対象ユニット = 2 台のホスト（任意の仮想マシンまたは物理マシン）
- 1 管理ユニット = 物理ディスクまたは仮想ディスクのフォーマットされていない容量の 4TB

この変更により、既存の Cloud Insights サブスクリプションを使用して監視できる環境容量が 2 倍になります。

（2019年11月

（2019年10月

レポート作成

"* Cloud Insights Reporting*" は、事前定義済みのレポートを表示したりカスタムレポートを作成したりできる、ビジネスインテリジェンスツールです。Reporting を使用すると、次のタスクを実行できます。

- 事前定義済みのレポートを実行します
- カスタムレポートを作成する
- レポートの形式と配信方法をカスタマイズする
- レポートが自動的に実行されるようにスケジュールを設定する
- レポートを E メールで送信
- データのしきい値を色で表します

Cloud Insights レポートでは、チャージバック、消費分析、予測などの領域用のカスタムレポートを生成できます。また、回答に関する次のような質問にも対応できます。

- 所有しているインベントリ
- インベントリの場所
- アセットの使用者
- ビジネスユニットに割り当てられているストレージのチャージバック
- ストレージ容量の追加購入が必要になるまでの期間
- ビジネスユニットが適切なストレージ階層に配置されているか。
- 1 カ月、 1 四半期、 1 年のストレージ割り当ての変化

Cloud Insights * Premium Edition * ではレポート作成が可能です。

Active IQ の機能拡張

"Active IQ のリスク" ダッシュボードテーブルのウィジェットで使用するだけでなく、照会できるオブジェクトとしても使用できるようになりました。次のリスクオブジェクト属性が含まれています。
*カテゴリ
*緩和カテゴリ
*潜在的影響
*リスクの詳細
*重大度
*ソース
*ストレージ
*ストレージノード
* UIカテゴリ

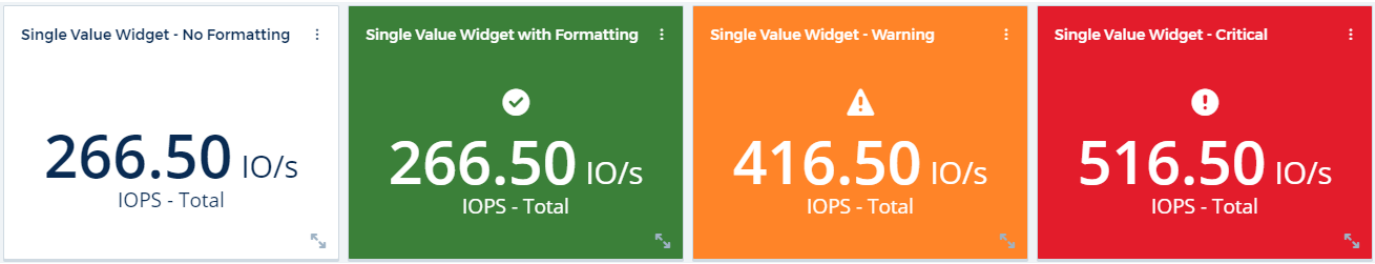
2019 年 9 月

新しいゲージウィジェット

ダッシュボードに単一値のデータを表示するウィジェットが、指定したしきい値に基づいて人目を引く色で 2 つ追加されました。値は、 * ソリッドゲージ * または * Bullet Gauge * のいずれかを使用して表示できます。警告範囲内にある値はオレンジで表示されます。Critical 範囲の値は赤で表示されます。警告しきい値を下回る値は緑で表示されます。

単一値ウィジェットの条件付きカラーフォーマット

設定したしきい値に基づいて、背景色の単一値ウィジェットを表示できるようになりました。



オンボーディング中にユーザーを招待する

オンボーディングプロセスの任意の時点で、 [管理] 、 [ユーザー管理] 、 [ユーザー] の順にクリックして、 Cloud Insights 環境に他のユーザーを招待できます。オンボーディングが完了してデータが収集されると、 _Guest_or_User_roles を持つユーザにはより大きなメリットがもたらされることに注意してください。

Data Collector 詳細ページの改善

データコレクタの詳細ページが改善され、読み取り可能な形式でエラーが表示されるようになりました。エラーがページ上の別のテーブルに表示されるようになりました。データコレクタで複数のエラーが発生した場合は、エラーがそれぞれ別の行に表示されます。

（2019年8月

すべて対使用可能なデータコレクタ

データコレクタを環境に追加するときに、サブスクリプションレベルまたはすべてのデータコレクタに基づいて使用可能なデータコレクタのみを表示するようにフィルタを設定できます。

Active IQ 統合

Cloud Insights は、ネットアップのお客様とそのハードウェア / ソフトウェアシステムに対し、可視化、分析、その他のサポート関連サービスを提供するネットアップ ActiveIQ からデータを収集します。Cloud Insights は、 ONTAP データ管理システムと統合されます。を参照してください "Active IQ" を参照してください。

（2019年7月

ダッシュボードの機能強化

ダッシュボードとウィジェットが次のように改善されました。

- 合計、最小、最大、平均に加えて、 * カウント * は単一値ウィジェットでの集計オプションになりました。「カウント」でロールアップする場合、 Cloud Insights はオブジェクトがアクティブであるかどうかをチェックし、アクティブなオブジェクトだけをカウントに追加します。結果の番号は、集約およびフィルタの対象となります。
- 単一値ウィジェットでは、 0 、 1 、 2 、 3 、または 4 桁の小数桁数を表示するように選択できるようになりました。
- 折れ線グラフには、 1 つのカウンタをプロットするときの軸ラベルと単位が表示されます。
- * Transform * オプションは、すべての指標の時系列ウィジェットでサービス統合データに使用できるようになりました。タイムシリーズウィジェット（ Line 、 Spline 、 Area 、 Stacked Area ）のサービス統合（ Telegraf ）カウンタまたはメトリックの場合、任意の方法を選択できます "値を変換します"。なし（表示値はそのまま）、合計、デルタ、累積など

Basic Edition へのダウングレード

過去 7 日間にポーリングを正常に完了した設定済みのネットアップデバイスがない場合、 Basic Edition へのダウングレードが失敗してエラーメッセージが表示されます。

収集 **Kue-State-Metrics**

。 "Kubernetes Data Collector を実行します" kube-state-metrics プラグインからオブジェクトとカウンタを収集し、 Cloud Insights で監視できる指標の数と範囲を大幅に拡大します。

（2019年6月

Cloud Insights エディション

Cloud Insights には、予算とビジネスニーズに合わせて、さまざまなエディションが用意されています。ネットアップサポートアカウントをお持ちの既存のお客様は、 7 日間のデータ保持期間をご利用いただけます。また、無料の * Basic Edition * をご利用いただくことで、ネットアップのデータ収集ツールへのアクセス、専門的なテクニカルサポートなどのデータ保持期間を延長できます。 * Standard Edition * をご利用ください。使用可能な機能の詳細については、ネットアップのを参照してください "Cloud Insights の機能です" サイト

新しいインフラストラクチャデータコレクタ： **NetApp HCI**

- "NetApp HCI 仮想センター" は、インフラストラクチャデータコレクタとして追加されました。HCI Virtual Center データコレクタは、 NetApp HCI ホスト情報を収集します。 Virtual Center 内のすべてのオブジェクトに対する読み取り専用の権限が必要です。

HCI のデータコレクタが取得するのは HCI Virtual Center のみです。ストレージシステムからデータを収集するには、ネットアップも設定する必要があります "SolidFire" データコレクタ：

2019 年 5 月

新しいサービスデータコレクター： **Kapacitor**

- "カパトール" は、サービスのデータコレクタとして追加されています。

Telegraf によるサービスとの統合

Cloud Insights では、スイッチやストレージなどのインフラデバイスからデータを取得するだけでなく、を使用してさまざまなオペレーティングシステムやサービスからデータを収集できるようになりました "Tegraf の代理店" 統合データの収集用。Telegraf はプラグインベースのエージェントで、メトリックの収集とレポートに使用できます。入力プラグインは、システム /OS に直接アクセスするか、サードパーティ API を呼び出すか、または設定されたストリームをリスニングすることによって、エージェントに必要な情報を収集するために使用されます。

現在サポートされているインテグレーションのドキュメントは、左側のメニューの「 * Reference and Support * 」の下にあります。

Storage Virtual Machine のアセット

- Storage Virtual Machine （ SVM ）は、 Cloud Insights でアセットとして使用できます。SVM には独自のアセットランディングページがあり、検索、クエリ、フィルタで表示および使用できます。SVM は、ダ

ッシュボードウィジェットやアノテーションに関連付けることもできます。

Acquisition Unit のシステム要件の削減

- Acquisition Unit （ AU ）ソフトウェアのシステム CPU およびメモリの要件が削減されました。新しい要件は次のとおりです。

* コンポーネント *	* 旧要件 *	* 新しい要件 *
CPU コア	4.	2.
メモリ	16GB	8 GB

サポートされているその他のプラットフォーム

- 現在、これらのプラットフォームには次のプラットフォームが追加されています "Cloud Insights でサポートされます" ：

Linux の場合	Windows の場合
CentOS 7.3（64ビット CentOS 7.4 64ビット CentOS 7.6 64ビット Debian 9 64ビット Red Hat Enterprise Linux 7.3（64ビット） Red Hat Enterprise Linux 7.4（64ビット） Red Hat Enterprise Linux 7.6（64ビット） Ubuntu Server 18.04 LTS	Microsoft Windows 10 64ビット Microsoft Windows Server 2008 R2 Microsoft Windows Server 2019の略

2019年4月

タグで仮想マシンをフィルタリングします

次のデータコレクタを設定するときに、タグまたはラベルに従って、データ収集に仮想マシンを含めるか除外するかをフィルタリングできます。

- "Amazon EC2"
- "Azure"
- "Google Cloud Platform の 1 つです"

2019 年 3 月

サブスクリプション関連イベントの E メール通知

- E メールの受信者を選択できます "通知" サブスクリプション関連のイベントが発生した場合（トライアルの有効期限が近づいている、またはアカウントを登録しているなど）。これらの通知の受信者は、次のい

ずれかから選択できます。

- すべてのアカウント所有者
- すべての管理者
- 指定する追加の E メールアドレス

その他のダッシュボード

- AWS を中心とした新しい機能 "ダッシュボード" ギャラリーに追加されており、インポート可能です：
  - AWS Admin - どの EC2 が需要の高いか
  - AWS EC2 Instance Performance by Region

2019年2月

AWS の子アカウントから収集しています

- Cloud Insights はをサポートします "AWS の子アカウントから収集します" 単一のデータコレクタ内。Cloud Insights が子アカウントから収集できるように AWS 環境を設定する必要があります。

Data Collector の命名

- Data Collector 名に、英字、数字、およびアンダースコアのほかに、ピリオド（ . ）、ハイフン（ - ）、およびスペース（）を含めることができるようになりました。名前の先頭と末尾にスペース、ピリオド、ハイフンを使用することはできません。

Acquisition Unit for Windows の略

- Cloud Insights Acquisition Unit は Windows サーバ / VM に設定できます。ウィンドウを確認します "前提条件" をインストールする前に "Acquisition Unit ソフトウェアの略"。

（2019年1月

「 Owner 」フィールドは読み取りやすくなっています

- ダッシュボードリストとクエリリストでは、「所有者」フィールドのデータは、以前はわかりやすい所有者名ではなく、認証 ID 文字列でした。「 Owner 」フィールドに、よりシンプルでわかりやすい所有者名が表示されるようになりました。

サブスクリプションページでの管理ユニットの内訳

- **[Admin] > [Subscription]** ページにリストされている各データコレクタについて、ホストとストレージの管理ユニット (MU) カウントの内訳と合計が表示されるようになりました。

(2018年12月).

UI ロード時間の改善

- Cloud Insights のユーザインターフェイス（ UI ）の初回ロード時間が大幅に短縮されました。また、メタデータがロードされている環境では、更新時間を短縮することもできます。

データコレクタを一括編集します

- 複数のデータコレクタの情報を同時に編集できます。[オブザーバビリティ（Observability）]>[コレクタ（Collectors）]ページで、変更するデータコレクタを選択し、[一括アクション（Bulk Actions）]*ボタンをクリックします。「 * 編集」を選択し、必要なフィールドを変更します。

  同じベンダーとモデルのデータコレクタを選択し、同じ Acquisition Unit に配置する必要があります。

サポートページとサブスクリプションページはオンボーディング中に利用できます

- オンボーディングワークフロー中に、ヘルプ > サポート * ページと * 管理者 > サブスクリプション * ページに移動できます。このページから戻るとオンボーディングワークフローに戻りますが、ブラウザのタブを閉じていないことが条件です。

（2018年11月

ネットアップの営業担当者または AWS Marketplace で登録

- Cloud Insights への登録と請求がネットアップから直接可能になりました。このサービスは、 AWS Marketplace で提供されるセルフサービスサブスクリプションに加えて提供されます。新しい * Contact Sales * リンクが、 * Admin > Subscription * ページに表示されます。環境内の管理対象ユニット（ MU ）が 1 、 000 以上であることが予想される場合は、 Contact Sales リンクからネットアップの営業担当者に問い合わせることを推奨します。

テキスト注釈ハイパーリンク

- テキスト型注釈にハイパーリンクを含めることができるようになりました。

チュートリアル

- Cloud Insights では、最初のユーザ（管理者またはアカウント所有者）が新しい環境にログインする際のオンボーディング手順が追加されました。このチュートリアルでは、 Acquisition Unit のインストール、初期データコレクタの設定、および有用なダッシュボードの選択を行います。

Gallery からダッシュボードをインポートします

- オンボーディング中にダッシュボードを選択するだけでなく、 [ダッシュボード（ * Dashboards ）] > [すべてのダッシュボードを表示（ Show All Dashboards ）] * を使用してダッシュボードをインポートし、 [ギャラリーから * + （ * + from Gallery *

ダッシュボードの複製

- ダッシュボードを複製する機能が、ダッシュボードリストページに各ダッシュボードのオプションメニューの選択肢として追加されました。また、ダッシュボードのメインページ自体については、 _Save_menu から選択できます。

Cloud Central の製品メニュー

- 他の NetApp Cloud Central 製品に切り替えるメニューは、画面の右上に移動しました。

データインフラの分析情報をオンボーディング

Data Infrastructure Insightsの使用を開始する前に、* NetApp BlueXP *ポータルにサインアップする必要があります。NetApp BlueXP へのログインをすでにお持ちの場合は、いくつかの簡単な手順でData Infrastructure Insightsの無償トライアルを開始できます。

NetApp BlueXPアカウントの作成

ネットアップのクラウドサービスの利用を開始するには、を参照してください "* NetApp BlueXP *" [Get Started]をクリックします。

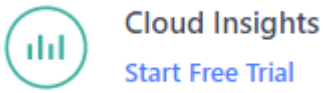
- まだサインアップしていない場合は、*サインアップ*を選択します
- 有効なビジネス用 E メールアドレスを入力し、パスワードを選択してください。
- 会社名と氏名を入力します。
- 利用条件に同意し、* Continue（続行）*を選択します。
- BlueXPのガイドに従って操作を開始します。

NetApp BlueXPへのログインをすでにお持ちの場合はどうすればよいですか？

NetApp BlueXPアカウントを取得したら、で*を選択するだけです " **NetApp BlueXP *"** ポータルページ。

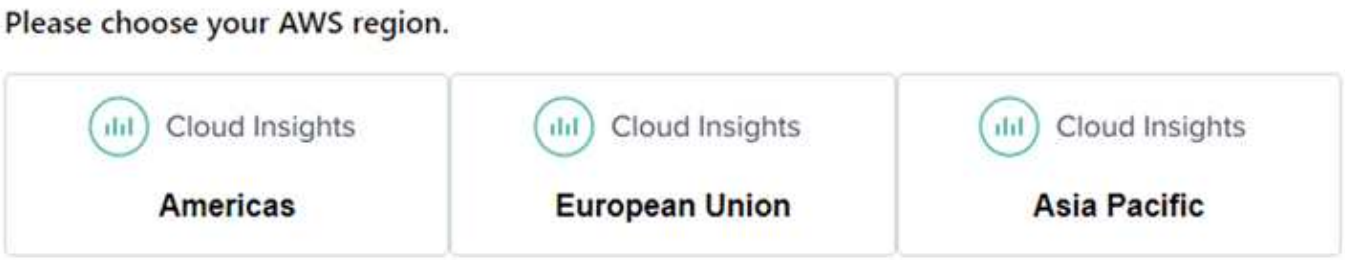
E メールアドレスとパスワードを入力します。その後、ネットアップのクラウドサービスに関するページに移動します。

[Data Infrastructure Insights]を選択します。



Data Infrastructure Insights無償トライアルを開始する

Data Infrastructure Insightsに初めてログインする場合は、[Data Infrastructure Insights Offering]で*[Start Free Trial]*をクリックします。Data Infrastructure Insightsでは、環境を配置する地域の選択など、企業の環境を作成する手順を順を追って説明します。



環境の作成が完了したら、BlueXP クレデンシャルを使用してログインし、30日間のData Infrastructure

Insights無償トライアルを開始できます。このトライアルでは、Data Infrastructure Insightsが提供する機能を確認できます。

無償トライアルでは、"サブスクリプションを開始します"Data Infrastructure Insightsをいつでも試すことができます。サブスクリプションを購入すると、現在のサブスクリプションに基づいてData Infrastructure Insightsの機能を使用できます。

サインインして実行します

環境の作成が完了したら、いつでもNetApp BlueXP ポータルにログインし、*[Go to Data Infrastructure Insights（データインフラのインサイトに移動）]*をクリックするだけです。データインフラの分析情報環境が直接表示されます。

ブラウザを開いて、Data Infrastructure Insights環境のURLに直接アクセスすることもできます。次に例を示します。

```
 \https://<environment-prefix>.c01.cloudinsights.netapp.com/
```

また、 URL
は各ユーザーの招待メールにも含まれ、簡単にアクセスしたりブックマークを付けたりできます。BlueXPにまだログインしていない場合は、ログインするように求められます。

新規ユーザが環境のURLにアクセスするには、引き続きBlueXPへのアクセスに登録する必要があります。

新しい環境に初めてログインするときは、のセットアップ手順が表示されます "* データの収集を開始 *"。

ログアウトしています

Data Infrastructure Insightsからログアウトするには、**[ユーザ名]***をクリックし、[ログアウト]*を選択します。BlueXPのサインイン画面に戻ります。

Data Infrastructure Insightsからログアウトすると、BlueXP からログアウトされます。BlueXP サインインを使用する他のNetAppクラウドサービスからもログアウトされます。

非アクティブ時のタイムアウト

操作がない状態が6時間（360分）続くと、デフォルトではBlueXPからユーザがログアウトされます。アクティビティに関係なく、ユーザは7日後にログアウトされます。

セキュリティ

データインフラ分析情報のセキュリティ

ネットアップでは、製品とお客様にデータセキュリティを最大限に活用することが何よりも重要です。Data Infrastructure Insightsは、リリースのライフサイクル全体を通じてセキュリティのベストプラクティスに従い、可能な限り最善の方法でお客様の情報とデータを確実に保護します。

セキュリティの概要

物理的セキュリティ

Data Infrastructure Insightsの本番インフラは、Amazon Web Services（AWS）でホストされています。Data Infrastructure Insights本番サーバの物理的および環境的なセキュリティ関連の制御（建物やドアで使用されるロックやキーなど）は、AWSによって管理されます。AWS によると、「ビデオ監視、侵入検知システム、その他の電子的手段を利用して、専門のセキュリティスタッフが、境界と建物の両方で物理アクセスを制御します。認定スタッフは、多要素認証メカニズムを利用してデータセンターのフロアにアクセスします。」

Data Infrastructure Insightsは、"共有責任モデル"AWSで説明されているのベストプラクティスに従っています。

製品のセキュリティ

Data Infrastructure Insightsは、アジャイルの原則に沿った開発ライフサイクルに従います。そのため、リリースサイクルの長い開発手法と比較して、セキュリティ志向のソフトウェアの不具合に迅速に対処することができます。継続的な統合手法を使用することで、機能とセキュリティの両方の変化に迅速に対応できます。変更管理手順とポリシーは、変更がいつどのように発生するかを定義し、本番環境の安定性を維持するのに役立ちます。インパクトのある変更は、正式に伝達され、調整され、適切にレビューされ、本番環境にリリースされる前に承認されます。

ネットワークセキュリティ

Data Infrastructure Insights環境内のリソースへのネットワークアクセスは、ホストベースのファイアウォールによって制御されます。各リソース（ロードバランサや仮想マシンインスタンスなど）にはホストベースのファイアウォールがあり、インバウンドトラフィックを、そのリソースが機能を実行するために必要なポートだけに制限します。

Data Infrastructure Insightsは、侵入検出サービスなどのさまざまなメカニズムを使用して、本番環境のセキュリティ異常を監視します。

リスク評価

Data Infrastructure Insightsチームは、形式化されたリスクアセスメントプロセスに従い、リスクを特定して評価する体系的で反復可能な方法を提供し、リスクをリスク治療計画を通じて適切に管理できるようにします。

データ保護

Data Infrastructure Insights本番環境は、すべてのサービスとコンポーネントに対して複数のアベイラビリティゾーンを使用して、非常に冗長なインフラ内にセットアップされます。可用性の高い冗長なコンピューティン

グインフラを利用するとともに、重要なデータを定期的にバックアップし、リストアを定期的にテストします。正式なバックアップ・ポリシーと手順により ' ビジネス・アクティビティの中断による影響を最小限に抑え ' 情報システムや災害の影響からビジネス・プロセスを保護し ' 適切なタイミングで適切な再開を実現します

認証およびアクセス管理

Data Infrastructure Insightsへのすべてのアクセスは、HTTPSを介したブラウザUIの操作を通じて行われます。認証は、サードパーティのサービスである Auth0 を介して行われます。ネットアップでは、すべてのクラウドデータサービスの認証レイヤとして、この機能を一元化しています。

Data Infrastructure Insightsは、Data Infrastructure Insights本番環境への論理アクセスに関する「最小権限」や「ロールベースアクセス制御」など、業界のベストプラクティスに従っています。アクセスは厳密な必要性に基づいて制御され、多要素認証メカニズムを使用する一部の承認された担当者にのみ許可されます。

お客様のデータの収集と保護

すべてのお客様のデータは、パブリックネットワークを経由して転送中に暗号化され、保存中に暗号化されます。Data Infrastructure Insightsは、システム内のさまざまなポイントでの暗号化を利用して、Transport Layer Security（TLS）や業界標準のAES-256アルゴリズムなどのテクノロジを使用してお客様のデータを保護します。

顧客のプロビジョニング解除

E メール通知はさまざまな間隔で送信され、お客様のサブスクリプションが期限切れになることを通知します。サブスクリプションの期限が切れると、 UI は制限され、データ収集の猶予期間が始まります。その後、お客様に E メールで通知します。トライアルサブスクリプションには 14 日間の猶予期間があり、有料サブスクリプションアカウントには 28 日間の猶予期間があります。猶予期間が終了すると、お客様にはアカウントが 2 日以内に削除されることを電子メールで通知します。有料のお客様は、サービスを利用しないよう直接リクエストすることもできます。

期限切れのテナントと関連するすべての顧客データは、猶予期間の終了時、またはお客様からアカウントの終了を要求されたことを確認した時点で、Data Infrastructure Insights Operations（SRE）チームによって削除されます。どちらの場合も、 SRE チームは API 呼び出しを実行してアカウントを削除します。API 呼び出しで、テナントインスタンスとすべての顧客データが削除されます。カスタマーの削除は、同じ API を呼び出し、カスタマーテナントのステータスが「削除済み」であることを確認することで確認できます。

セキュリティインシデント管理

Data Infrastructure Insightsは、NetAppの製品セキュリティインシデント対応チーム（PSIRT）プロセスと統合されており、既知の脆弱性を検出、評価、解決します。PSIRT は、カスタマーレポート、内部エンジニアリング、 CVE データベースなどの広く認識されているソースなど、複数のチャネルから脆弱性情報を取得します。

Data Infrastructure Insightsエンジニアリングチームが問題を検出した場合、チームはPSIRTプロセスを開始し、問題を評価し、潜在的に修正します。

また、Data Infrastructure Insightsのお客様やリサーチャーは、Data Infrastructure Insights製品のセキュリティ上の問題を特定し、テクニカルサポートまたはNetAppのインシデント対応チームに直接報告することもできます。このような場合は、Data Infrastructure InsightsチームがPSIRTプロセスを開始し、問題を評価して、潜在的に修正します。

脆弱性および侵入テスト

Data Infrastructure Insightsは、業界のベストプラクティスに従い、社内外のセキュリティ専門家や企業を使用して定期的に脆弱性と侵入テストを実施します。

セキュリティ認識トレーニング

Data Infrastructure Insightsのすべての担当者は、それぞれの役割に応じて開発されたセキュリティトレーニングを受けています。これにより、各担当者は、それぞれの役割に固有のセキュリティ関連の課題に対処できるようになります。

コンプライアンス

Data Infrastructure Insightsは、セキュリティ、プロセス、サービスについて外部の公認会計士事務所から独立した第三者監査および検証を実施しています。これには、SOC 2監査の完了も含まれます。

NetAppセキュリティアドバイザリ

ネットアップが提供しているセキュリティアドバイザリを表示できます。 "こちらをご覧ください"。

情報と地域

ネットアップでは、お客様の情報のセキュリティを非常に重視しています。Data Infrastructure Insightsで情報を保存する方法と場所をご紹介します。

Data Infrastructure Insightsにはどのような情報が保存されますか？

Data Infrastructure Insightsには次の情報が格納されます。

- パフォーマンスデータ

  パフォーマンスデータは、監視対象のデバイス / ソースのパフォーマンスに関する情報を提供する時系列のデータです。たとえば、ストレージシステムによって配信される IOS の数、ファイバチャネルポートのスループット、 Web サーバによって配信されるページ数、データベースの応答時間などです。

- インベントリデータ

  インベントリデータは、監視対象のデバイス / ソースを記述するメタデータと、その設定方法で構成されます。たとえば、インストールされているハードウェアとソフトウェアのバージョン、ストレージシステム内のディスクとLUN、CPUコア、RAMと仮想マシンのディスク、データベースの表領域、SANスイッチ上のポートの数とタイプ、ディレクトリとファイルの名前（ストレージワークロードのセキュリティが有効な場合）などです

- 設定データ

  これは、顧客のインベントリや操作を管理するために使用される、顧客から提供された構成データの要約です。たとえば、監視対象デバイスのホスト名や IP アドレス、ポーリング間隔、タイムアウト値などです

- 秘密

シークレットは、Data Infrastructure Insights Acquisition Unitがお客様のデバイスやサービスにアクセスするために使用するクレデンシャルで構成されます。これらのクレデンシャルは強力な非対称暗号化を使用して暗号化され、秘密鍵はAcquisition Unitにのみ格納され、お客様の環境から離れることはありません。Privileged Data Infrastructure InsightsのSREであっても、この設計により、プレーンテキストで顧客シークレットにアクセスできません。

- 機能データ

  このデータは、ネットアップがクラウドデータサービスを提供することで生成されます。このサービスは、クラウドデータサービスの開発、導入、運用、メンテナンス、セキュリティの各分野をネットアップに通知します。機能データには、顧客情報や個人情報は含まれません。

- ユーザーアクセスデータ

  NetApp BlueXP が各地域のData Infrastructure Insightsサイトと通信できるようにする認証およびアクセス情報（ユーザの承認に関連するデータなど）。

- ストレージワークロードのセキュリティユーザディレクトリデータ

  ワークロードセキュリティ機能が有効になっていて、ユーザーディレクトリコレクタを有効にすることを選択した場合、ユーザー表示名、企業の電子メールアドレス、およびActive Directoryから収集されたその他の情報が保存されます。

  ユーザディレクトリデータとは、ワークロードセキュリティユーザディレクトリデータコレクタによって収集されたユーザディレクトリ情報であり、データインフラインサイト/ワークロードセキュリティのユーザ自身に関するデータではありません。

- 明示的な個人データは一切ありません。 * インフラストラクチャとサービスのリソースから収集されます。収集される情報は、パフォーマンス指標、設定情報、インフラメタデータのみで構成され、ネットアップの自動サポートや ActiveIQ など、多くのベンダーの電話ホームと同様です。ただし、お客様の命名規則に応じて、共有、ボリューム、 VM 、 qtree のデータ アプリケーションなどには、個人を特定できる情報が含まれる場合があります。

ワークロードのセキュリティが有効になっている場合、システムはさらに、個人を特定可能な情報を含むSMBまたはその他の共有上のファイル名とディレクトリ名を調べます。お客様がWorkload Security User Directory Collector（Active Directoryを介してWindows SIDをユーザ名にマッピングする）を有効にした場合、表示名、企業のEメールアドレス、および選択したその他の属性がData Infrastructure Insightsによって収集され、保存されます。

さらに、Data Infrastructure Insightsへのアクセスログは維持され、サービスへのログインに使用されたユーザのIPアドレスとEメールアドレスが記録されます。

情報はどこに保存されますか？

Data Infrastructure Insightsには、環境が作成されたリージョンに基づいて情報が格納されます。

ホスト領域には、次の情報が格納されます。

- カウンタやパフォーマンス指標などの計測情報と資産 / オブジェクト情報
- Acquisition Unit の情報
- 機能データ

- Data Infrastructure Insights内のユーザアクティビティに関する情報を監査
- ワークロードセキュリティActive Directoryの情報
- ワークロードのセキュリティ監査情報

以下の情報は、Data Infrastructure Insights環境をホストしているリージョンに関係なく、米国内に存在します。

- サイト / アカウント所有者などの環境サイト（「テナント」とも呼ばれる）情報。
- NetApp BlueXP が各地域のData Infrastructure Insightsサイトと通信できるようにするための情報（ユーザの承認に関連する情報を含む）。
- Data Infrastructure Insightsのユーザとテナントの関係に関連する情報。

ホストリージョン

ホスト領域は次のとおりです。

- US ： us-east-1
- EMEA ： EU-central -1
- APAC ： AP-南東 部 -2

詳細情報

ネットアップのプライバシーとセキュリティの詳細については、次のリンクを参照してください。

- "トラストセンター"
- "クロスボーダーデータ転送"
- "企業規則の拘束"
- "サードパーティのデータ要求への対応"
- "ネットアッププライバシーの原則"

securityadminツール

Data Infrastructure Insightsには、強化されたセキュリティで環境を運用できるセキュリティ機能が含まれています。この機能には、暗号化、パスワードハッシュの改善、内部ユーザパスワードの変更、およびパスワードの暗号化と復号化を行うキーペアの変更が含まれます。

機密データを保護するために、インストールまたはアップグレードの完了後にデフォルトキーと_Acquisition_userパスワードを変更することを推奨します。

データソース暗号化されたパスワードはData Infrastructure Insightsに保存されます。Data Infrastructure Insightsでは、ユーザがデータコレクタの設定ページでパスワードを入力すると、公開鍵を使用してパスワードが暗号化されます。Data Infrastructure Insightsには、データコレクタのパスワードの復号化に必要な秘密鍵はありません。データコレクタのパスワードの復号化に必要なデータコレクタの秘密鍵があるのは、Acquisition Unit（AUS）だけです。

アップグレードとインストールに関する考慮事項

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

Acquisition Unit上でセキュリティを管理する

SecurityAdminツールを使用すると、Data Infrastructure Insightsのセキュリティオプションを管理できます。このツールはAcquisition Unitシステムで実行されます。セキュリティの管理には、キーとパスワードの管理、作成したセキュリティ設定の保存とリストア、またはデフォルト設定への設定のリストアが含まれます。

作業を開始する前に

- Acquisition Unitソフトウェア（SecurityAdminツールを含む）をインストールするには、AUシステムに対する管理者権限が必要です。
- その後SecurityAdminツールにアクセスする必要がある管理者以外のユーザがいる場合は、そのユーザを_cisys_groupに追加する必要があります。_cisys_groupは、AUのインストール中に作成されます。

AUのインストール後、SecurityAdminツールはAcquisition Unitシステムの次のいずれかの場所にあります。

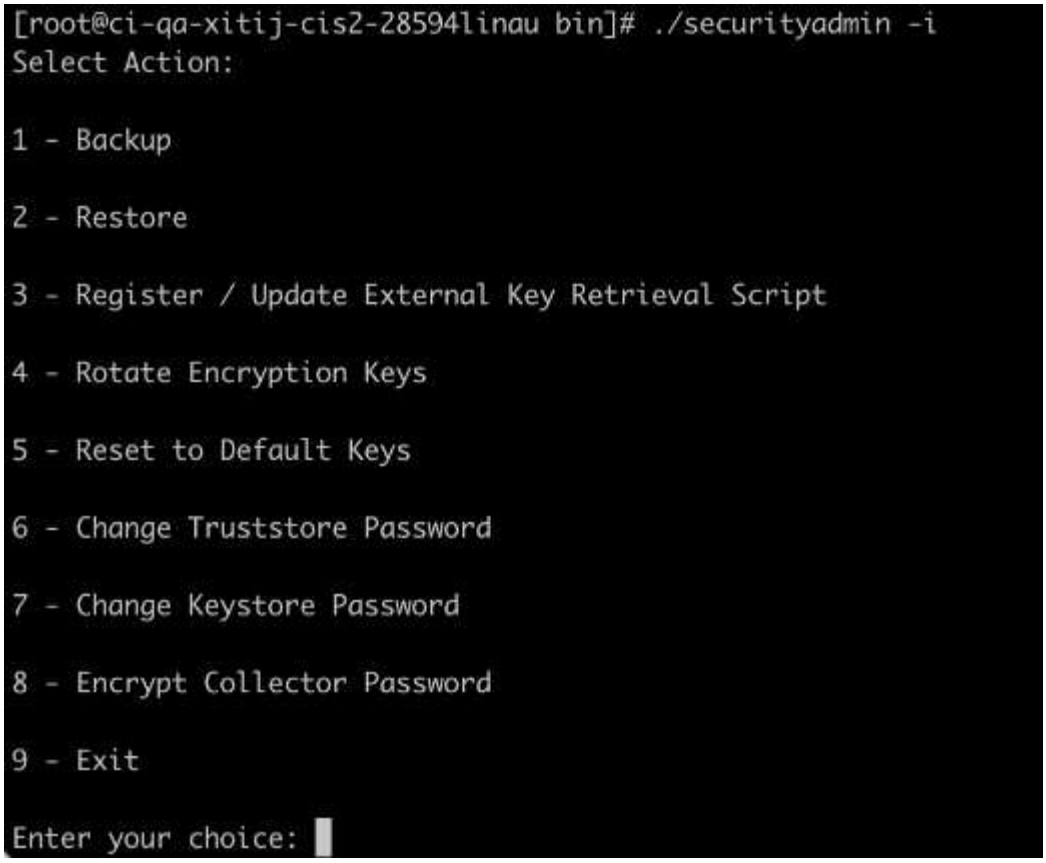
```
Windows - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

SecurityAdmin Toolを使用する

SecurityAdminツールを対話型モード（-i）で起動します。

SecurityAdminツールは対話モードで使用することをお勧めします。これは、コマンドラインでシークレットが渡されないようにするためです。シークレットはログに記録されます。

次のオプションが表示されます。



1. * バックアップ *

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

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

   ヴォールトバックアップには機密情報が含まれているため、安全に保管することを推奨します。

2. * 復元 *

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

   復元を使用すると、次の手順を使用して、複数のサーバーのパスワードとキーを同期できます。1) AUの暗号化キーを変更します。2）ヴォールトのバックアップを作成します。3）バックアップを各AUSにリストアします。

3. 外部キー取得スクリプトの登録/更新

   外部スクリプトを使用して、デバイスパスワードの暗号化または復号化に使用するAU暗号化キーを登録または変更します。

   暗号化キーを変更した場合、アップグレードまたはインストール後にリストアできるように、新しいセキュリティ設定をバックアップしておく必要があります。

注:このオプションはLinuxでのみ使用できます。

SecurityAdminツールで独自のキー取得スクリプトを使用する場合は、次の点に注意してください。

- 現在サポートされているアルゴリズムは、2048ビット以上のRSAです。
- スクリプトは、秘密鍵と公開鍵をプレーンテキストで返す必要があります。スクリプトは、暗号化された秘密鍵と公開鍵を返さないでください。
- スクリプトは、生のエンコードされた内容を返す必要があります（PEM形式のみ）。
- 外部スクリプトには_execute_permissionsが必要です。

4. 暗号化キーのローテーション

   暗号化キーをローテーションします（現在のキーの登録を解除し、新しいキーを登録します）。外部キー管理システムのキーを使用するには、公開鍵IDと秘密鍵IDを指定する必要があります。

5. デフォルトキーにリセット

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

6. 信頼ストアのパスワードの変更

   信頼ストアのパスワードを変更します。

7. キーストアパスワードの変更

   キーストアのパスワードを変更します。

8. コレクタパスワードの暗号化

   暗号化データコレクタのパスワード。

9. * 終了 *

   SecurityAdminツールを終了します。

設定するオプションを選択し、画面の指示に従います。

ツールを実行するユーザを指定します

管理されたセキュリティ意識の高い環境にいる場合は、_cisys_groupを持っていなくても、特定のユーザーにSecurityAdminツールを実行してもらいたい場合があります。

これを行うには、AUソフトウェアを手動でインストールし、アクセスするユーザ/グループを指定します。

- APIを使用して、CIインストーラをAUシステムにダウンロードして解凍します。
  - 1回限りの認証トークンが必要になります。API Swaggerのドキュメント（_Admin > API Access_および_API Documentation_linkを選択）を参照し、_get /au/oneTimeToken_APIのセクションを参照してください。
  - トークンを取得したら、_get /au/installers/｛platform｝/｛version｝_apiを使用してインストーラファ

イルをダウンロードします。プラットフォーム（LinuxまたはWindows）とインストーラのバージョンを指定する必要があります。

- ダウンロードしたインストーラファイルをAUシステムにコピーして解凍します。
- ファイルが格納されているフォルダに移動し、ユーザとグループを指定してrootとしてインストーラを実行します。

```
./cloudinsights-install.sh <User> <Group>
```

指定したユーザまたはグループが存在しない場合は、作成されます。ユーザーはSecurityAdminツールにアクセスできます。

プロキシを更新または削除しています

SecurityAdminツールでAcquisition Unitのプロキシ情報を設定または削除するには、次のように_- pr_パラメータを指定してツールを実行します。

```
[root@ci-eng-linau bin]# ./securityadmin -pr
usage: securityadmin -pr -ap <arg> | -h | -rp | -upr <arg>

The purpose of this tool is to enable reconfiguration of security aspects
of the Acquisition Unit such as encryption keys, and proxy configuration,
etc. For more information about this tool, please check the Data
Infrastructure Insights
Documentation.

-ap,--add-proxy <arg>       add a proxy server.  Arguments: ip=ip
                             port=port user=user password=password
                             domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
-h,--help
-rp,--remove-proxy          remove proxy server
-upr,--update-proxy <arg>   update a proxy.  Arguments: ip=ip port=port
                             user=user password=password domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
```

たとえば、プロキシを削除するには、次のコマンドを実行します。

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
```

コマンドの実行後にAcquisition Unitを再起動する必要があります。

プロキシを更新するには、コマンドを使用します

```
./securityadmin -pr -upr <arg>
```

外部キーの取得

UNIXシェルスクリプトを指定すると、Acquisition Unitによって実行され、キー管理システムから*秘密鍵*と*

公開鍵*を取得できます。

キーを取得するために、Data Infrastructure Insightsはスクリプトを実行し、_key id_と_key type_の2つのパラメータを渡します。キーID _は、キー管理システム内のキーを識別するために使用できます。_Key type _には、「public」または「private」を指定します。キータイプが「public」の場合、スクリプトは公開鍵を返す必要があります。キータイプが「private」の場合は、秘密鍵を返す必要があります。

Acquisition Unitにキーを戻すには、標準出力にキーを出力する必要があります。スクリプトは、標準出力にキーをprint_only_theで出力する必要があります。他のテキストは標準出力に出力しないでください。要求されたキーが標準出力に出力されると、スクリプトは終了コード0で終了する必要があります。その他の戻りコードはエラーと見なされます。

スクリプトはSecurityAdminツールを使用してAcquisition Unitに登録する必要があります。このツールでは、Acquisition Unitとともにスクリプトが実行されます。スクリプトには、rootおよび"cisys"ユーザに対する_read_and_execute_permissionが必要です。登録後にシェルスクリプトを変更した場合は、変更したシェルスクリプトをAcquisition Unitに再登録する必要があります。

入力パラメータ:キーID	顧客のキー管理システムでキーを識別するために使用するキー識別子。
入力パラメータ:キータイプ	パブリックまたはプライベート。
出力	要求されたキーを標準出力に出力する必要があります。現在、2048ビットRSAキーがサポートされています。キーは次の形式でエンコードおよび印刷する必要があります- 秘密鍵形式- PEM、DERエンコードPKCS8 PrivateKeyInfo RFC 5958 公開鍵形式- PEM、DERエンコードX.509 SubjectPublicKeyInfo RFC 5280
終了コード	成功のためのゼロの終了コード。他のすべての終了値は失敗と見なされます。
スクリプト権限	スクリプトには、rootおよび「cisys」ユーザに対する読み取りおよび実行権限が必要です。
ログ	スクリプトの実行が記録されます。ログは次の場所にあります。 /var/log/netapp/cloudinsights/securityadmin/securityadmin.log /var/log/netapp/cloudinsights/acq/acq.log

APIで使用するパスワードの暗号化

オプション8では、パスワードを暗号化し、APIを介してデータコレクタに渡すことができます。

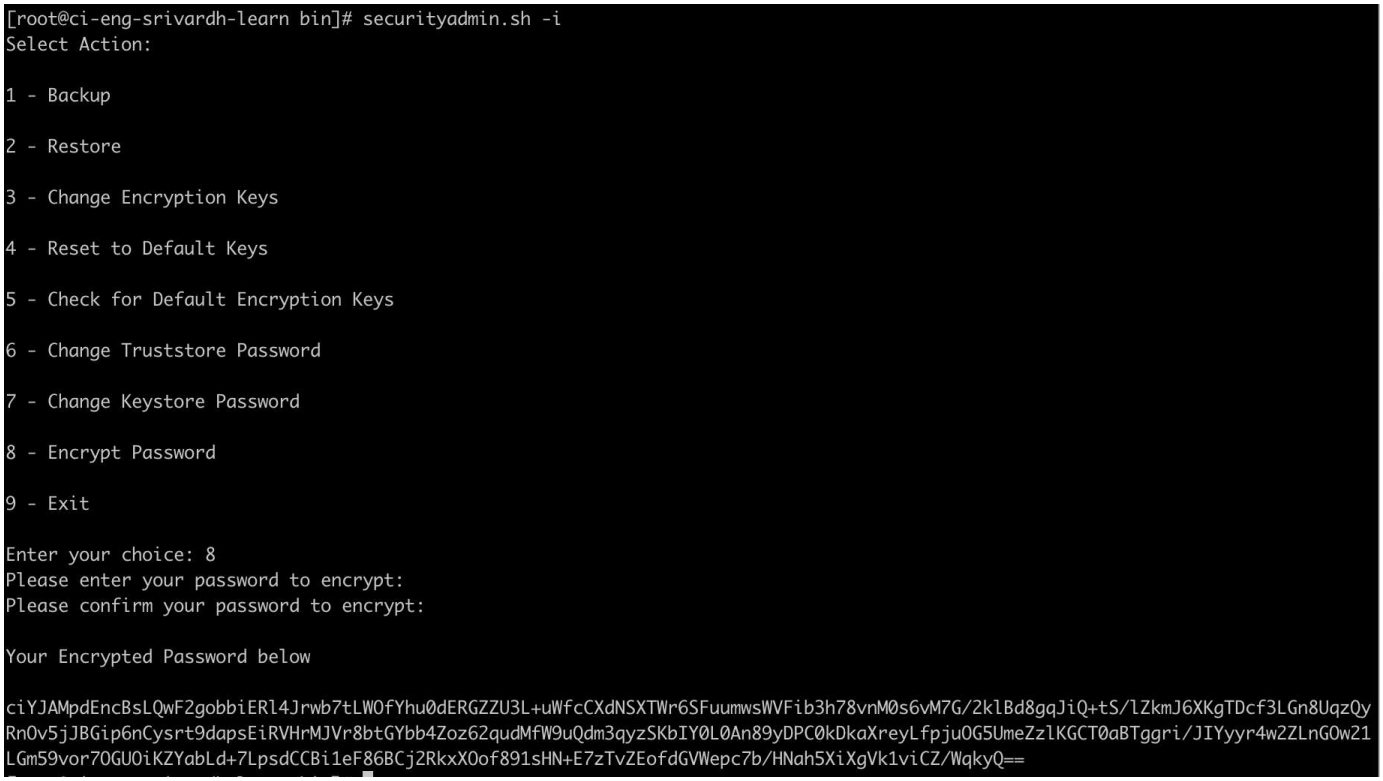
SecurityAdminツールを対話型モードで起動し、オプション8:_Encrypt Password_を選択します。

```
securityadmin.sh -i
```
暗号化するパスワードの入力を求められます。入力した文字は画面に表示されません。
プロンプトが表示されたら、パスワードを再入力します。

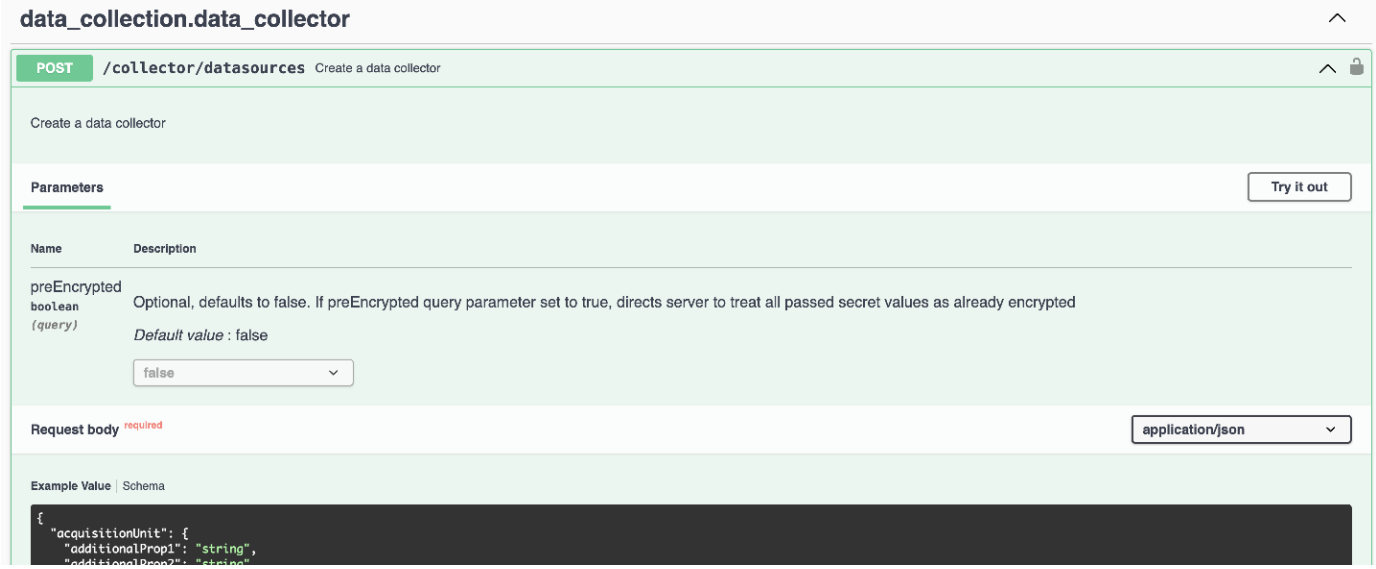
または、スクリプトでコマンドを使用する場合は、コマンドラインで「-enc」パラメータを指定して_securityadmin.sh_を使用し、暗号化されていないパスワードを渡します。

```
securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["CLIの例"]
```

暗号化されたパスワードが画面に表示されます。先頭または末尾の記号を含む文字列全体をコピーします。



暗号化されたパスワードをデータコレクタに送信するには、データ収集APIを使用します。このAPIのSwaggerは* Admin > API Access *にあり、[API Documentation]リンクをクリックします。「データ収集」APIタイプを選択します。 *data_collection.data_collector_heading*で、この例の_/collector/datasources_POST APIを選択します。



_preEncrypted_optionを_True_に設定した場合、APIコマンドを通過するパスワードは*すでに暗号化されている*として扱われます。APIはパスワードを再暗号化しません。APIを構築するときは、以前に暗号化されたパスワードを適切な場所に貼り付けるだけです。

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true

```
{
"name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
"J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnlBVsAWyLmORxFAw
vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZlY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```

APIで使用するパスワードの暗号化

オプション8では、パスワードを暗号化し、APIを介してデータコレクタに渡すことができます。

SecurityAdminツールを対話型モードで起動し、オプション8:_Encrypt Password_を選択します。

```
 securityadmin.sh -i
```
暗号化するパスワードの入力を求められます。入力した文字は画面に表示されません。
プロンプトが表示されたら、パスワードを再入力します。

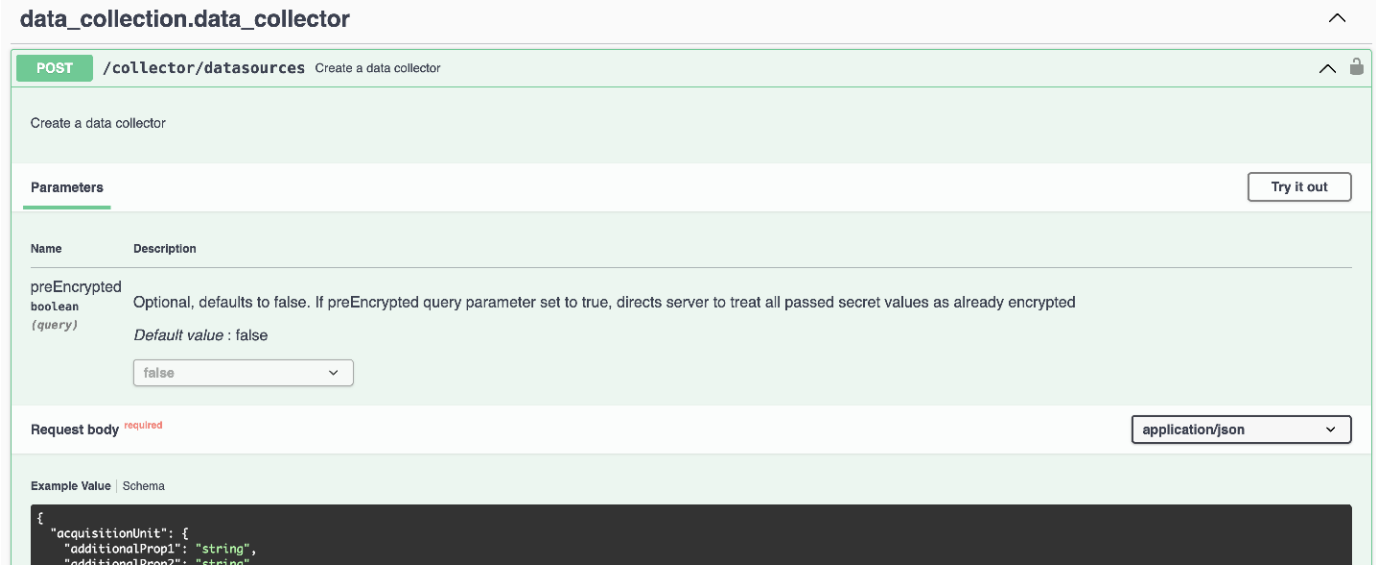
または、スクリプトでコマンドを使用する場合は、コマンドラインで「-enc」パラメータを指定して_securityadmin.sh_を使用し、暗号化されていないパスワードを渡します。

```
 securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["CLIの例"]
```

暗号化されたパスワードが画面に表示されます。先頭または末尾の記号を含む文字列全体をコピーします。

```
[root@ci-eng-srivardh-learn bin]# securityadmin.sh -i
Select Action:

1 - Backup

2 - Restore

3 - Change Encryption Keys

4 - Reset to Default Keys

5 - Check for Default Encryption Keys

6 - Change Truststore Password

7 - Change Keystore Password

8 - Encrypt Password

9 - Exit

Enter your choice: 8
Please enter your password to encrypt:
Please confirm your password to encrypt:

Your Encrypted Password below

ciYJAMpdEncBsLQwF2gobbiERl4Jrwb7tLWOfYhu0dERGZZU3L+uWfcCXdNSXTWr6SFuumwsWVFib3h78vnM0s6vM7G/2klBd8gqJiQ+tS/lZkmJ6XKgTDcf3LGn8UqzQy
RnOv5jJBGip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSKbIY0L0An89yDPC0kDkaXreyLfpjuOG5UmeZzlKGCT0aBTggri/JIYyyr4w2ZLnGOw21
LGm59vor7OGUOiKZYabLd+7LpsdCCBi1eF86BCj2RkxXOof891sHN+E7zTvZEofdGVWepc7b/HNah5XiXgVk1viCZ/WqkyQ==
```

暗号化されたパスワードをデータコレクタに送信するには、データ収集APIを使用します。このAPIのSwaggerは* Admin > API Access *にあり、[API Documentation]リンクをクリックします。「データ収集」APIタイプを選択します。 *data_collection.data_collector_heading*で、この例の_/collector/datasources_POST APIを選択します。



_preEncrypted_optionを_True_に設定した場合、APIコマンドを通過するパスワードは*すでに暗号化されている*として扱われます。APIはパスワードを再暗号化しません。APIを構築するときは、以前に暗号化されたパスワードを適切な場所に貼り付けるだけです。

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true


```
{
"name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
"J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnlBVsAWyLmORxFAw
vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZlY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```

はじめに

機能チュートリアル

Data Infrastructure Insightsには、データの迅速かつ簡単な検索、問題のトラブルシューティング、企業環境に関する分析情報の提供を可能にする便利な機能が搭載されています。強力なクエリでデータを簡単に検索し、ダッシュボードでデータを視覚化し、設定したデータしきい値の E メールアラートを送信します。

Data Infrastructure Insightsには、これらの機能を理解し、ビジネス分析戦略を効果的に実装するのに役立つビデオチュートリアルが多数用意されています。Data Infrastructure Insights環境にアクセスできるすべてのユーザが、このチュートリアルを利用できます。

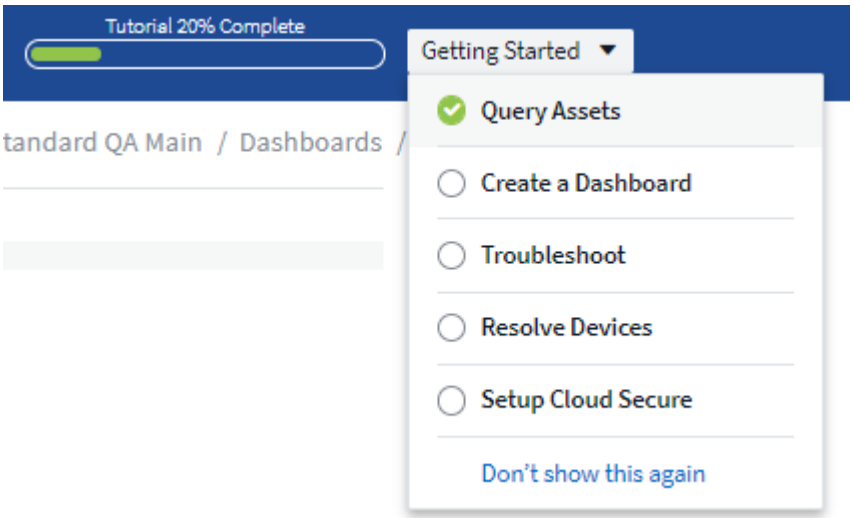
はじめに

Data Infrastructure Insightsの仕組みを説明する簡単なチュートリアルをご覧ください。

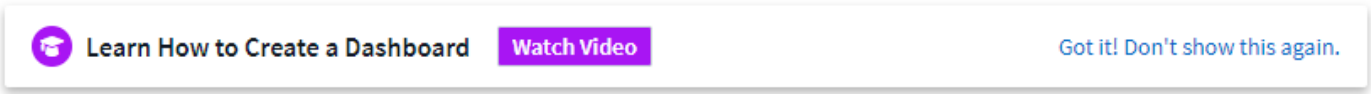
► https://docs.netapp.com/ja-jp/cloudinsights//media/howTo.mp4 *(video)*

チェックリストとビデオチュートリアル

Data Infrastructure Insightsサイトに表示される「スタートアップチェックリスト」*には、いくつかの便利なタスクと概念が記載されています。チェックリストの項目を選択すると、その概念に適した[Data Infrastructure Insights]ページが表示されます。たとえば、_Create a Dashboard_itemをクリックすると、Data Infrastructure Insights * Dashboards *ページが開きます。



ページの上部には、ダッシュボードの作成方法を示すビデオチュートリアルへのリンクがあります。ビデオは、 [got it （取得）] をクリックするまで何度でも表示できます。このビデオには、この Again_link を表示しないでください。ビデオは、 [ダッシュボード] ページを閉じるまで、 [ダッシュボード] ページに移動するたびに使用できます。



ビデオを少なくとも 1 回見た後、チェックリストの _ ダッシュボード項目の作成 _ がオフになり、チュートリアルが完了したことを示します。次のチュートリアルに進むことができます。

チュートリアルは好きな順番で表示できます。終了するまで何度でも表示できます。

チェックリストを削除します

チェックリストの下部にある [この項目を今後表示しない] リンクをクリックするまで、 [スタートアップチェックリスト] がサイトに表示されます。このチェックリストを却下しても、メッセージヘッダーバーから各チュートリアルを却下するまでは、該当するData Infrastructure Insightsの各ページでチュートリアルを使用できます。

チュートリアルを表示します

データを照会しています

► https://docs.netapp.com/ja-jp/cloudinsights//media/Queries.mp4 *(video)*

ダッシュボードの作成

► https://docs.netapp.com/ja-jp/cloudinsights//media/Dashboards.mp4 *(video)*

トラブルシューティング

► https://docs.netapp.com/ja-jp/cloudinsights//media/Troubleshooting.mp4 *(video)*

デバイスを解決します

► https://docs.netapp.com/ja-jp/cloudinsights//media/AHR_small.mp4 *(video)*

データの収集中

データの収集を開始しています

Data Infrastructure Insightsに登録して初めて環境にログインすると、次の手順に従ってデータの収集と管理を開始します。

データコレクタによって、ストレージデバイス、ネットワークスイッチ、仮想マシンなどのデータソースから情報が検出されます。収集された情報は、分析、検証、監視、およびトラブルシューティングに使用されます。

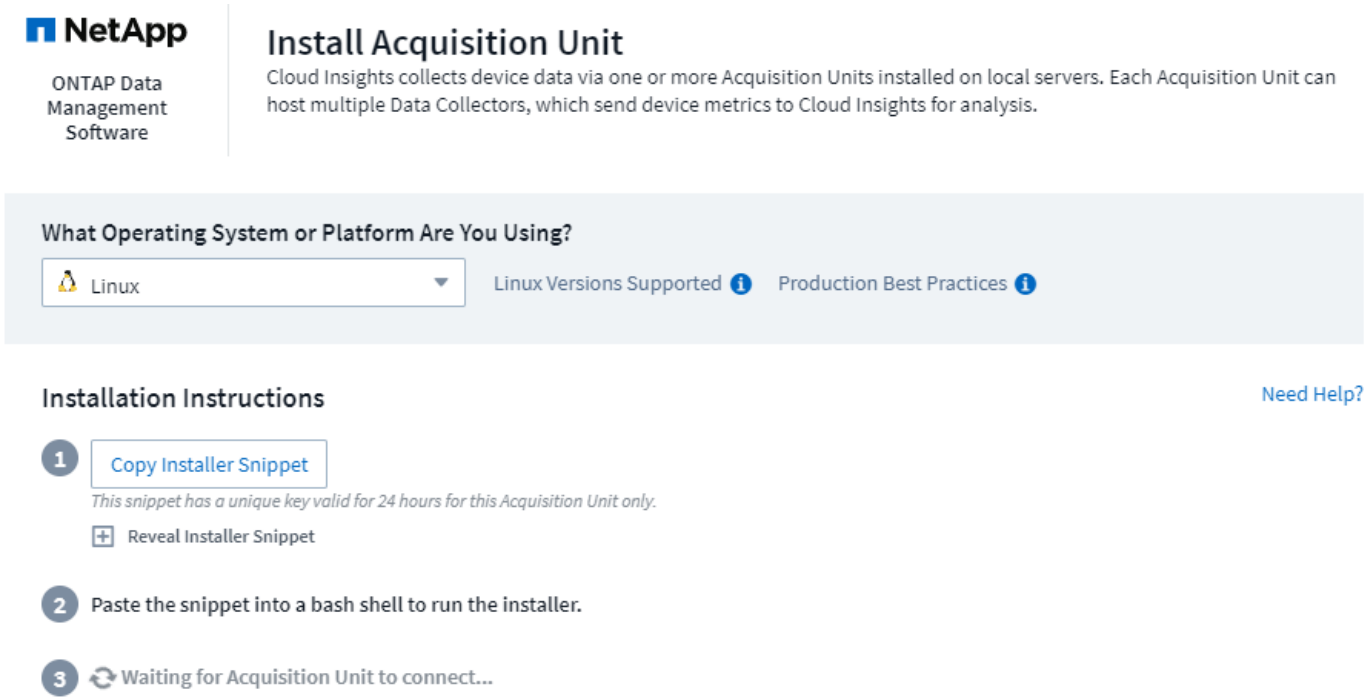
Data Infrastructure Insightsには、次の3種類のデータコレクタがあります。

- インフラ（ストレージデバイス、ネットワークスイッチ、コンピューティングインフラ）
- オペレーティングシステム（VMwareやWindowsなど）
- サービス（Kafkaなど）

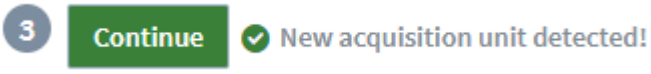
サポートされているベンダーとモデルから最初のデータコレクタを選択してください。あとでデータコレクタを簡単に追加できます。

Acquisition Unit をインストールする

_Infrastructure_dataコレクタを選択した場合は、Data Infrastructure Insightsにデータを挿入するためにAcquisition Unitが必要です。収集対象のデータセンターにあるサーバまたはVMにAcquisition Unitソフトウェアをダウンロードしてインストールする必要があります。1 つの Acquisition Unit を複数のデータコレクタに使用できます。



- に従ってください "手順" Acquisition Unit のインストール用に表示されます。Acquisition Unit ソフトウェアをインストールすると、 Continue ボタンが表示され、次の手順に進みます。



Acquisition Unit は、必要に応じてあとから追加で設定することもできます。たとえば、異なる Acquisition Unit でリージョンのデータセンターから情報を収集する場合があります。

Data Collector - インフラストラクチャを設定します

_Infrastructure_data コレクタの場合は、表示されるデータコレクタフィールドに入力するように求められます。

- データコレクタに一意でわかりやすい名前を付けます。
- 必要に応じて、クレデンシャル（ユーザ名とパスワード）を入力してデバイスに接続します。
- _Configuration_Section_and _Advanced Configuration_Sections に他の必須フィールドを入力します。
- [コレクタの追加] をクリックして、データコレクタを保存します。

あとで追加のデータコレクタを設定できます。

Data Collector の設定 - オペレーティングシステムとサービス

オペレーティングシステム

Operating System_dataコレクタの場合は、プラットフォーム（Linux、Windows）を選択してData Infrastructure Insights Agentをインストールします。サービスからデータを収集するには、少なくとも 1 人のエージェントが必要です。また、エージェントはホスト自体からデータを収集し、Data Infrastructure Insightsで使用します。このデータは、ウィジェットなどでは「ノード」データに分類されます

- エージェントホストまたは VM でターミナルまたはコマンドウィンドウを開き、表示されたコマンドを貼り付けてエージェントをインストールします。
- インストールが完了したら、 [* Complete Setup* （セットアップの完了）] をクリックします。

サービス

_Service_data コレクタの場合は、タイルをクリックして、そのサービスの指示ページを開きます。

- プラットフォームとエージェントアクセスキーを選択します。
- そのプラットフォームにエージェントがインストールされていない場合は、指示に従ってエージェントをインストールします。
- [* Continue （続行）] をクリックして、データコレクタの説明ページを開きます。
- 指示に従ってデータコレクタを設定します。
- 設定が完了したら、 [* Complete Setup* （セットアップの完了）] をクリックします。

ダッシュボードを追加します

設定対象として選択した初期データコレクタのタイプ（ストレージ、スイッチなど）に応じて、関連するダッシュボードが 1 つ以上インポートされます。たとえば、ストレージデータコレクタを設定している場合、ストレージ関連の一連のダッシュボードがインポートされ、そのダッシュボードがData Infrastructure Insightsのホームページとして設定されます。ホームページは、 [ダッシュボード（ *Dashboards ）]>[すべてのダッシュボードを表示（ Show All Dashboards ）] リストから変更できます。

追加のダッシュボードは、あとからインポートすることも、インポートすることもでき "自分で作成します"。

これで終了です

初期セットアッププロセスが完了すると、環境でデータの収集が開始されます。

初期セットアッププロセスが中断された場合（ブラウザウィンドウを閉じた場合など）は、次の手順を手動で実行する必要があります。

- Data Collector を選択します
- プロンプトが表示されたら、 Agent または Acquisition Unit をインストールします
- Data Collector を設定します

便利な定義

Data Infrastructure Insightsのデータコレクタや機能について説明する際には、次の定義が役立ちます。

- コレクタのライフサイクル:コレクタは'ライフサイクルの次のいずれかの状態に属します
  - プレビュー：限定された容量または限定された視聴者に提供されます。 "フィーチャーをプレビューします" データコレクタは、プレビュー期間後にGAになる予定です。プレビュー期間は、対象者や機能によって異なります。
  - * GA *：エディションまたは機能セットに基づいて、すべてのお客様が一般に利用できる機能またはデータコレクタ。
  - 廃止予定：機能上の持続可能性がなくなった、または今後アップする予定の環境 データコレクタ。非推奨のデータコレクタは、多くの場合、新しい機能上更新されたデータコレクタに置き換えられます。
  - *Deleted *:削除され、使用できなくなったデータコレクタ。
- Acquisition Unit：データコレクタをホストする専用のコンピュータ。通常は仮想マシンです。通常、このコンピュータは、監視対象の項目と同じデータセンター/VPC内にあります。
- データソース：ハードウェアまたはソフトウェアスタックと通信するためのモジュール。デバイスと通信するためにAUコンピュータで実行される設定とコードで構成されます。

Acquisition Unit の要件

インフラのデータコレクタ（ストレージ、 VM 、ポート、 EC2 など）から情報を取得するには、 Acquisition Unit （ AU ）をインストールする必要があります。Acquisition Unit をインストールする前に、オペレーティングシステム、 CPU 、メモリ、およびディスクスペースが要件を満たしていることを確認してください。

要件

コンポーネント	Linux 要件	Windows 要件

オペレーティングシステム	次のいずれかのライセンスバージョンを実行しているコンピュータ。 * CentOS（64ビット）：7.2～7.9、8.1～8.4、Stream 8、Stream 9 * AlmaLinux 9.3および9.4 * Debian (64ビット): 9と10 * openSUSE Leap 15.1～15.5 * Oracle Enterprise Linux（64ビット）：7.5～7.9、8.1～8.8 * Red Hat Enterprise Linux（64ビット）：7.2～7.9、8.1～8.10、9.1～9.4 ロッキー**9.0～9.4** *** SUSE Enterprise Linux Server 15、15 SP2～15 SP5** *** Ubuntu**サーバ：**18.04、20.04、22.04 LTS** *****上記のプラットフォームでの**SELinux** このコンピュータでは、他のアプリケーションレベルのソフトウェアを実行しないでください。専用のサーバを使用することを推奨します。 **SELinux**を使用している場合は、**Acquisition Unit**システムで次のコマンドを実行することを推奨します。 **sudo semanage fcontext -a -t usr_t "/opt/netapp/cloudinsights（/.）？"** sudo restorecon -R /opt/netapp/cloudinsights	次のいずれかのライセンスバージョンを実行しているコンピュータ。 * Microsoft Windows 10 64ビット * Microsoft Windows Server 2012 * Microsoft Windows Server 2012 R2 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows 11 このコンピュータでは、他のアプリケーションレベルのソフトウェアを実行しないでください。専用のサーバを使用することを推奨します。
CPU	2個のCPUコア	同じ
メモリ	8GB の RAM	同じ
使用可能なディスクスペース	50 GB（100 GBを推奨） Linuxの場合は、次の方法でディスクスペースを割り当てる必要があります。 /opt/netapp 10 GB（大規模環境では20 GB） /var/log/netapp 40 GB（大規模環境では80 GB） /tmpインストール中に1 GB以上の空き容量が必要です	50GB

ネットワーク	100 Mbps/1 Gbpsイーサネット接続、静的IPアドレス、およびAcquisition Unitから*。cloudinsights.c01.cloudinsights.com NetAppまたはデータインフラストラクチャインサイト環境（\https：//<environment_id>.c01.cloudinsights.c.com NetApp）へのポート80または443の接続が必要です。Acquisition Unitと各Data Collectorの間の要件については、の手順を参照してください"Data Collector"。インターネットアクセスにプロキシを使用する必要がある場合は、組織のプロキシの動作を理解し、Data Infrastructure Insightsが機能するために特定の例外を探す必要があります。たとえば、デフォルトでアクセスがブロックされ、特定のWebサイト/ドメインへのアクセスのみが例外で許可されていますか。その場合は、次のドメインを例外リストに追加する必要があります。*。NetApp .com詳細については、プロキシ"こちら（Linux）"またはを参照してください。"ここ（Windows）"	同じ
権限	Acquisition Unit サーバに対する sudo 権限 /tmp は EXEC 機能でマウントする必要があります。	Acquisition Unit サーバに対する管理者権限が必要です
ウィルススキャン		インストール時に、すべてのウィルススキャンソフトウェアを完全に無効にする必要があります。インストール後に、 Acquisition Unit ソフトウェアで使用するパスをウィルススキャンから除外する必要があります。

その他の推奨事項

- 正確な監査およびデータレポートを作成するためには、 * Network Time Protocol （ NTP ；ネットワークタイムプロトコル） * または * Simple Network Time Protocol （ SNTP ） * を使用して Acquisition Unit マシンの時間を同期することを強く推奨します。

サイジングについて

Data Infrastructure Insights Acquisition Unitの使用は、メモリが8GB、ディスクスペースが50GBしかないので開始できますが、大規模な環境の場合は次の点を自問してください。

次のことを期待していますか？

- この Acquisition Unit 上で、 2500 台を超える仮想マシン、または 10 台の大規模（ 2 ノード以上）の ONTAP クラスタ、 Symmetrix 、 HDS / HPE VSP/XP アレイを検出できるか？
- この Acquisition Unit に合計 75 個以上のデータコレクタを導入しますか？

上記の「はい」回答ごとに、 8 GB のメモリと 50 GB のディスク容量を AU に追加することをお勧めします。たとえば、「はい」と答えた場合、 150GB 以上のディスクスペースを備えた 24GB のメモリシステムを導入する必要があります。Linux の場合、ログの場所に追加するディスクスペース。

サイジングに関するその他の情報については、ネットアップサポートにお問い合わせください。

Federal Editionの追加要件

- Data Infrastructure Insights Federal EditionクラスタにAcquisition Unitをインストールする場合は、基盤となるオペレーティングシステムに十分なエントロピーがある必要があります。Linuxシステムでは、これは通常、_rng-tools_をインストールするか、ハードウェア乱数生成（RNG）を使用して行われます。Acquisition Unitマシンでこの要件が満たされていることを確認するのは、お客様の責任です。

Acquisition Unit の設定

Data Infrastructure Insightsは、ローカルサーバにインストールされている1つ以上のAcquisition Unitを使用してデバイスデータを収集します。各Acquisition Unitは複数のデータコレクタをホストでき、データコレクタはデバイスメトリックをData Infrastructure Insightsに送信して分析します。

ここでは、 Acquisition Unit を追加する方法と、プロキシを使用する環境で必要な追加の手順について説明します。

正確な監査およびデータレポートを作成するためには、 * Network Time Protocol （ NTP ；ネットワークタイムプロトコル） * または * Simple Network Time Protocol （ SNTP ） * を使用して Acquisition Unit マシンの時間を同期することを強く推奨します。

Data Infrastructure Insightsのセキュリティについては"こちらをご覧ください"、こちらをご覧ください。

Linux Acquisition Unit の追加

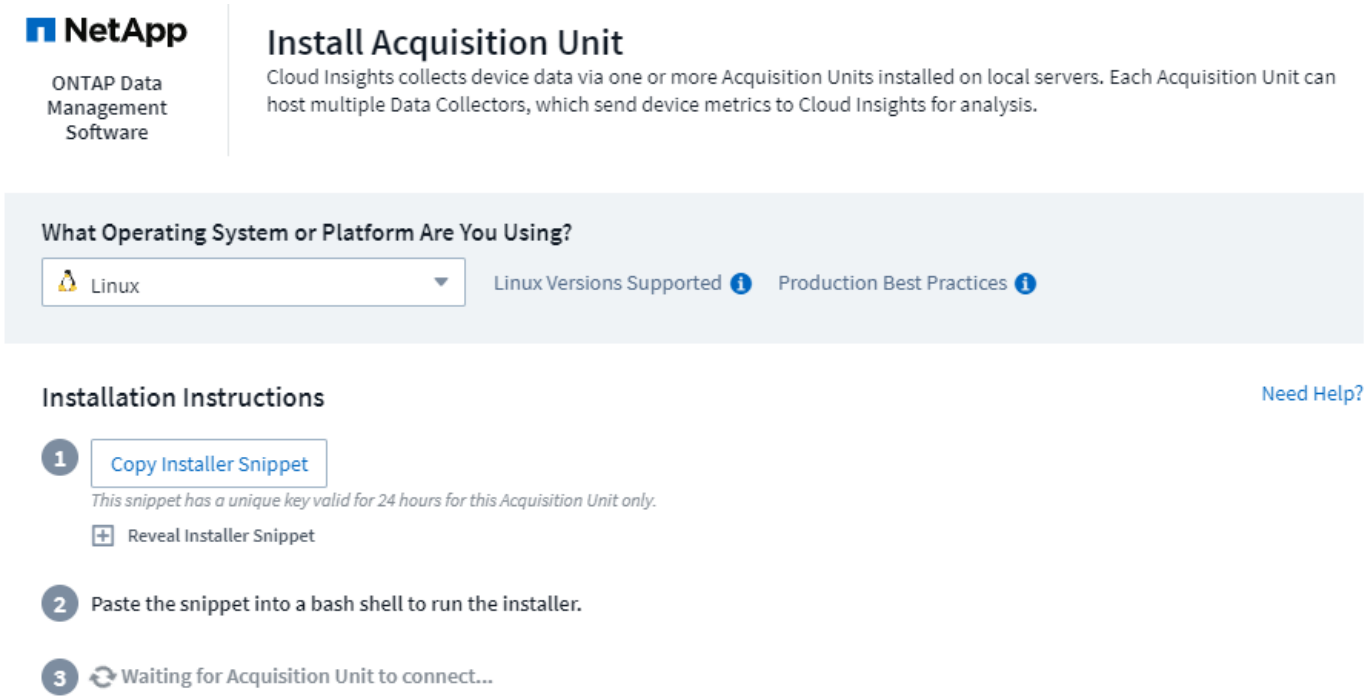
作業を開始する前に

- プロキシを使用するシステムの場合は、 Acquisition Unit をインストールする前にプロキシ環境変数を設定する必要があります。詳細については、を参照してください [プロキシ環境変数を設定しています]。

Linux Acquisition Unit のインストール手順

1. Data Infrastructure Insights環境に管理者またはアカウント所有者としてログインします。
2. [Observability]>[Collectors]>[Acquisition Units]>[+Acquisition Unit]

   [Install Acquisition Unit_Dialog] が表示されます。Linux を選択します。



1. Acquisition Unit をホストしているサーバまたは VM が推奨されるシステム要件を満たしていることを確認する。
2. サーバでサポートされているバージョンの Linux が実行されていることを確認します。サポートされているバージョンのリストについては、「サポートされている OS バージョン」（ i ）をクリックしてください。
3. ダイアログ内の Installation コマンドスニペットを、 Acquisition Unit をホストするサーバまたは VM のターミナルウィンドウにコピーします。
4. Bash シェルにコマンドを貼り付けて実行します。

完了後

- [Observability]>[Collectors]>[Acquisition Units]*をクリックして、Acquisition Unitのステータスを確認します。
- Acquisition Unit のログには、 /var/log/netapp/cloudInsights /acq/ acq.log からアクセスできます
- Acquisition Unit を制御するには、次のスクリプトを使用します。
  - cloudinsights-service.sh （ stop 、 start 、 restart 、 status を確認）
- Acquisition Unit をアンインストールするには、次のスクリプトを使用します。
  - cloudinsights-uninstall.sh

プロキシ環境変数を設定しています

プロキシを使用する環境では、 Acquisition Unit を追加する前にプロキシ環境変数を設定する必要があります。プロキシの設定手順については、_Add Acquisition Unit_dialogを参照してください。

1. [+ in_ プロキシサーバを使用しますか ?_] をクリックします
2. コマンドをテキストエディタにコピーし、必要に応じてプロキシ変数を設定します。

   注：プロキシユーザ名とパスワードのフィールドでは、特殊文字に関する制限に注意してください。 ユー

ザ名フィールドに入力できます。' ： ' 、 % 、 ' ！ ' パスワードフィールドに入力できます。

3. Bash シェルを使用して、端末で編集したコマンドを実行します。
4. Acquisition Unit ソフトウェアをインストールします。

プロキシ設定：

Acquisition Unitは、双方向認証と相互認証を使用してData Infrastructure Insightsサーバに接続します。認証するには、クライアント証明書をData Infrastructure Insightsサーバに渡す必要があります。そのためには、データを復号化せずにHTTPS要求をData Infrastructure Insightsサーバに転送するようにプロキシを設定する必要があります。

これを行う最も簡単な方法は、Data Infrastructure Insightsと通信するためにプロキシ/ファイアウォールでワイルドカード設定を指定することです。次に例を示します。

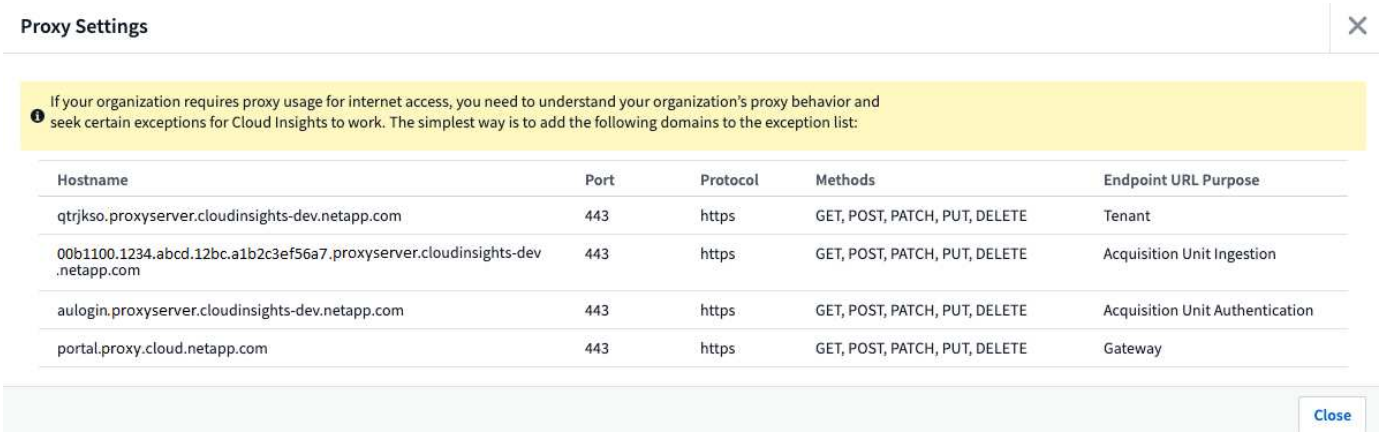
```
*.cloudinsights.netapp.com
```

ワイルドカードにアスタリスク（ * ）を使用するのは一般的ですが、プロキシ / ファイアウォールの設定では異なる形式を使用することがあります。プロキシのドキュメントで、ワイルドカードを正しく指定できることを確認してください。

プロキシ設定の詳細については、ネットアップのを参照してください "ナレッジベース（Knowledgbase）"。

プロキシ **URL** の表示

オンボーディング中にデータコレクタを選択するときに [* プロキシ設定 *] リンクをクリックするか、 [* ヘルプ > サポート *] ページの [_ プロキシ設定 _] の下のリンクをクリックすると、プロキシエンドポイントの URL を表示できます。次のようなテーブルが表示されます。



ワークロードセキュリティを使用している環境では、設定済みのエンドポイントURLもこのリストに表示されます。

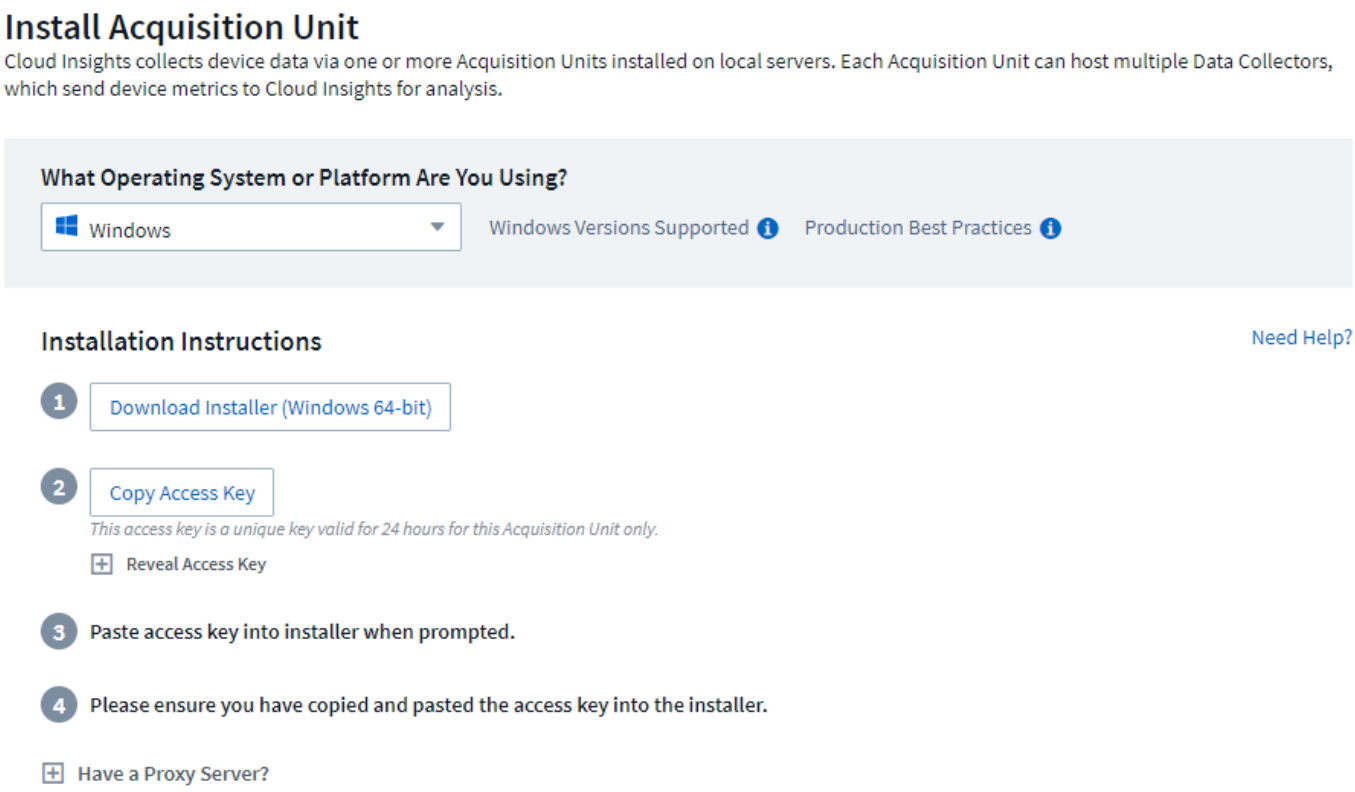
Windows Acquisition Unit の追加

Windows Acquisition Unit のインストールの手順

1. 管理者権限を持つユーザとして Acquisition Unit サーバ / VM にログインします。

2. そのサーバで、ブラウザウィンドウを開き、管理者またはアカウント所有者としてData Infrastructure Insights環境にログインします。
3. [Observability]>[Collectors]>[Acquisition Units]>[+Acquisition Unit]

   [Install Acquisition Unit_Dialog] が表示されます。Windows を選択します。



1. Acquisition Unit をホストしているサーバまたは VM が推奨されるシステム要件を満たしていることを確認する。
2. サーバでサポートされているバージョンの Windows が実行されていることを確認します。サポートされているバージョンのリストについては、「サポートされている OS バージョン」（ i ）をクリックしてください。
3. [インストーラのダウンロード（ Windows 64 ビット） *] ボタンをクリックします。
4. アクセスキーをコピーします。インストール中にこのファイルが必要になります。
5. Acquisition Unit のサーバ / VM で、ダウンロードしたインストーラを実行します。
6. プロンプトが表示されたら、アクセスキーをインストールウィザードに貼り付けます。
7. インストール中に、プロキシサーバーの設定が表示されます。

完了後

- [Observability]>[Collectors]>[Acquisition Units]*をクリックして、Acquisition Unitのステータスを確認します。
- Acquisition Unit のログには、 <install dir>\Cloud Insights \Acquisition Unit \log\acq.log からアクセスできます
- Acquisition Unit のステータスを確認するには、次のスクリプトを使用します。

```
cloudinsights-service.sh
```

プロキシ設定：

Acquisition Unitは、双方向認証と相互認証を使用してData Infrastructure Insightsサーバに接続します。認証するには、クライアント証明書をData Infrastructure Insightsサーバに渡す必要があります。そのためには、データを復号化せずにHTTPS要求をData Infrastructure Insightsサーバに転送するようにプロキシを設定する必要があります。

これを行う最も簡単な方法は、Data Infrastructure Insightsと通信するためにプロキシ/ファイアウォールでワイルドカード設定を指定することです。次に例を示します。

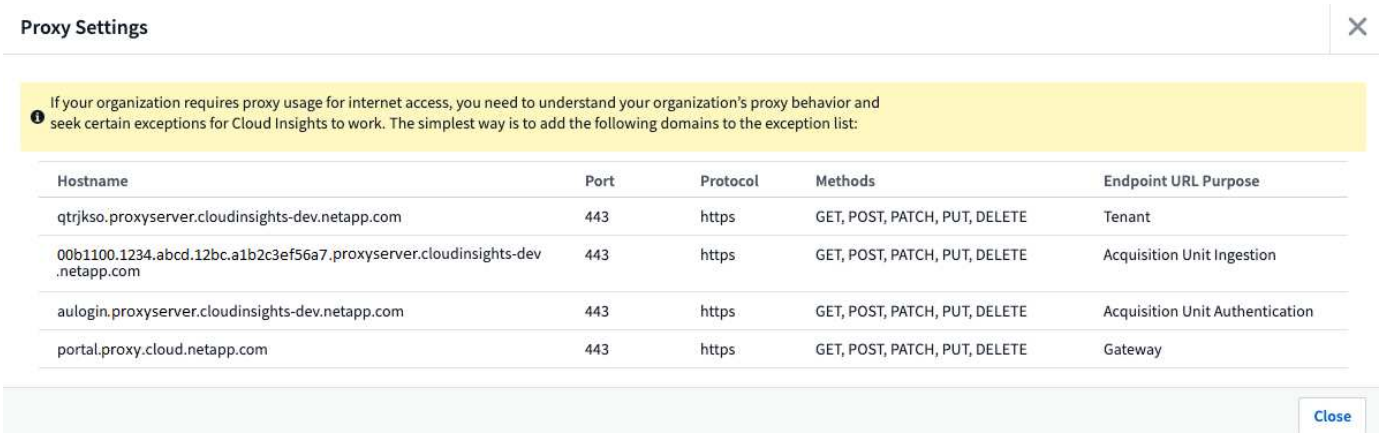
```
*.cloudinsights.netapp.com
```

ワイルドカードにアスタリスク（ * ）を使用するのは一般的ですが、プロキシ / ファイアウォールの設定では異なる形式を使用することがあります。プロキシのドキュメントで、ワイルドカードを正しく指定できることを確認してください。

プロキシ設定の詳細については、ネットアップのを参照してください "ナレッジベース（Knowledgbase）"。

プロキシ **URL** の表示

オンボーディング中にデータコレクタを選択するときに [* プロキシ設定 *] リンクをクリックするか、 [* ヘルプ > サポート *] ページの [_ プロキシ設定 _] の下のリンクをクリックすると、プロキシエンドポイントの URL を表示できます。次のようなテーブルが表示されます。



ワークロードセキュリティを使用している環境では、設定済みのエンドポイントURLもこのリストに表示されます。

Acquisition Unit のアンインストール

Acquisition Unit ソフトウェアをアンインストールするには、次の手順を実行します。

- Windows ： *

Windows * Acquisition Unitをアンインストールする場合は、次の手順を実行します。

1. Acquisition Unit のサーバー /VM で、 Control Panel を開いて、「プログラムのアンインストール」を選択します。削除するData Infrastructure Insights Acquisition Unitプログラムを選択します。
2. [アンインストール] をクリックし、画面の指示に従います。

- Linux ： *

Linux* Acquisition Unitをアンインストールする場合は、次の手順を実行します。

1. Acquisition Unit サーバ / VM で、次のコマンドを実行します。

```
 sudo cloudinsights-uninstall.sh -p
```

. アンインストールのヘルプについては、次のコマンドを実行します。

```
sudo cloudinsights-uninstall.sh --help
```

- WindowsおよびLinux：*
- AUのアンインストール後：
  1. Data Infrastructure Insightsで、**[Observability]>[Collectors]**に移動し、[Acquisition Units]*タブを選択します。
  2. アンインストールする Acquisition Unit の右側にある Options ボタンをクリックし、 _Delete_を 選択します。Acquisition Unit は、その Acquisition Unit にデータコレクタが割り当てられていない場合にのみ削除できます。

> ⓘ データコレクタが接続されているAcquisition Unit（AU）は削除できません。元のAUを削除する前に、AUのすべてのデータコレクタを別のAUに移動します（コレクタを編集して別のAUを選択するだけです）。

横に星印が付いたAcquisition Unitがデバイス解決に使用されています。このAUを削除する前に、デバイス解決に使用する別のAUを選択する必要があります。別のAUにカーソルを合わせ、「3つのドット」メニューを開き、「デバイス解像度に使用」を選択します。

Acquisition Unit の再インストール

Acquisition Unit を同じサーバ / VM に再インストールするには、次の手順を実行する必要があります。

作業を開始する前に

Acquisition Unit を再インストールするには、あらかじめ別のサーバ / VM で一時的な Acquisition Unit を設定しておく必要があります。

手順

1. Acquisition Unit サーバ /VM にログインし、 AU ソフトウェアをアンインストールします。
2. Data Infrastructure Insights環境にログインし、*オブザーバビリティ>コレクタ*に移動します。
3. 各データコレクタについて、右側の [オプション] メニューをクリックし、 *Edit* を選択します。一時収集ユニットにデータコレクタを割り当て、 * 保存 * をクリックします。

   同じタイプの複数のデータコレクタを選択し、 * 一括アクション * ボタンをクリックすることもできます。*Edit* を選択し、データコレクタを一時 Acquisition Unit に割り当てます。

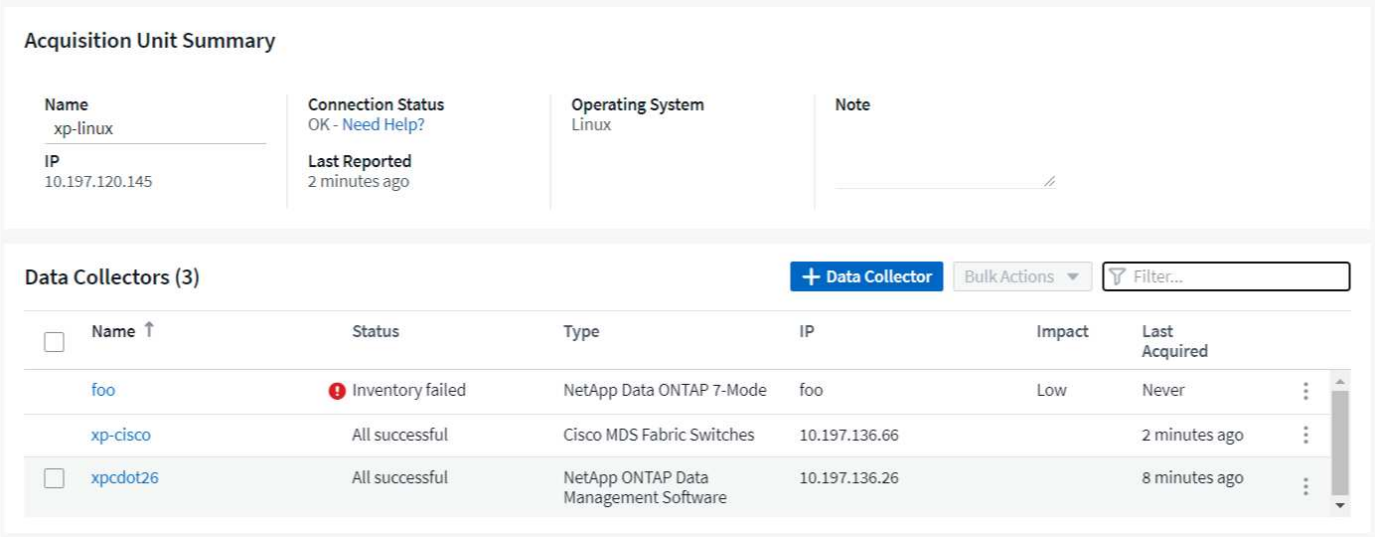
4. すべてのデータコレクタを一時的なAcquisition Unitに移動したら、**[Observability]>[Collectors]***に移動し、[Acquisition Units]*タブを選択します。
5. 再インストールする Acquisition Unit の右側にある Options ボタンをクリックし、 _Delete_を 選択します。Acquisition Unit は、その Acquisition Unit にデータコレクタが割り当てられていない場合にのみ削除できます。
6. Acquisition Unit ソフトウェアを元のサーバ / VM に再インストールできるようになりました。+ Acquisition Unit * をクリックし、上記の手順に従って Acquisition Unit をインストールします。
7. Acquisition Unit を再インストールしたら、データコレクタを Acquisition Unit に再び割り当てます。

AU 詳細を表示しています

Acquisition Unit （ AU ）の詳細ページには、 AU に関する有用な情報やトラブルシューティングに役立つ情報が表示されます。AU 詳細ページには、次のセクションがあります。

- 以下を示す * サマリ * セクション：
  - * Acquisition Unit の名前 * と IP *
  - AU の現在の接続 * Status *
  - * 最終報告 * データコレクタのポーリング時間に成功
  - AU マシンの * オペレーティング・システム *
  - AU の現在の * 注 * 。このフィールドには、 AU のコメントを入力します。このフィールドには、最後に追加されたメモが表示されます。
- 各データコレクタについて、 AU * Data Collectors * のテーブルが表示されます。
  - * 名前 *- このリンクをクリックすると、追加情報を使用してデータコレクタの詳細ページにドリルダウンできます
  - * Status * - 成功またはエラー情報
  - * タイプ * - ベンダー / モデル
  - * データコレクタの IP * アドレス

- 現在の * 影響 * レベル
- *Last Acquired * time ：データコレクタが最後に正常にポーリングされた時刻



データコレクタごとに、 [Three dots] メニューをクリックして、データコレクタの複製、編集、ポーリング、または削除を実行できます。このリストで複数のデータコレクタを選択して、それらに対して一括操作を実行することもできます。

Acquisition Unit を再起動するには、ページ上部の「 * Restart * 」ボタンをクリックします。接続に問題が発生した場合に、このボタンをドロップダウンして、 AU への * 接続の復元 * を試行します。

データを収集するためのエージェントの設定(Windows/Linux)

Data Infrastructure Insightsは、"Tegraf"統合データ収集のエージェントとしてを使用します。Telegraf はプラグインベースのサーバエージェントで、指標、イベント、ログの収集とレポートに使用できます。入力プラグインは、システム /OS に直接アクセスするか、サードパーティ API を呼び出すか、設定されたストリームをリスニングすることによって、エージェントに必要な情報を収集するために使用されます（例：） Kafka や StatsD など）を参照してください。出力プラグインは、収集されたメトリック、イベント、ログをエージェントからData Infrastructure Insightsに送信するために使用されます。

Data Infrastructure Insightsの現在のTelegrafバージョンは* 1.24.0 *です。

Kubernetesへのインストールの詳細については、を参照してください。 "NetApp Kubernetes Monitoring Operator" ページ

正確な監査およびデータレポートを作成するためには、 * Network Time Protocol （ NTP; ネットワークタイムプロトコル） * または * Simple Network Time Protocol （ SNTP ） * を使用して、 Agent マシンの時刻を同期することを強くお勧めします。

エージェントをインストールする前にインストールファイルを確認する場合は、の項を参照してください [チェックサムを検証する]。

エージェントをインストールしています

サービスデータコレクタをインストールしていて、エージェントをまだ設定していない場合は、最初に適切なオペレーティングシステム用のエージェントをインストールするように求められます。このトピックでは、Tegraf エージェントを次のオペレーティングシステムにインストールする手順について説明します。

- Windows の場合
- RHEL および CentOS
- Ubuntu と Debian

エージェントをインストールするには、使用しているプラットフォームに関係なく、まず次の手順を実行する必要があります。

1. エージェントに使用するホストにログインします。
2. Data Infrastructure Insights環境にログインし、*オブザーバビリティ>コレクタ*に移動します。
3. [**+Data Collector**] をクリックして、インストールするデータコレクタを選択します。
4. ホストに適したプラットフォームを選択（Windows、Linux）
5. プラットフォームごとに、残りの手順を実行します。

ホストにエージェントをインストールしたら、そのホストに再度エージェントをインストールする必要はありません。

サーバ/ VMにエージェントをインストールすると、Data Infrastructure Insightsは、設定したデータコレクタからの収集に加えて、そのシステムから指標を収集します。これらの指標はとして収集され"「ノード」指標"ます。

プロキシを使用している場合は、 Tegraf エージェントをインストールする前に、お使いのプラットフォームのプロキシの手順をお読みください。

ログの場所

Telegrafログメッセージは、stdoutから次のログファイルにリダイレクトされます。デフォルトでは、

- RHEL / CentOS：/var/log/telegraf/telegraf.log
- Ubuntu/Debian：/var/log/telegraf/telegraf.log
- Windows：C：\Program Files\telegraf\telegraf.log

Windows の場合

前提条件

- PowerShell がインストールされていること
- プロキシの背後にいる場合は、「Windows *プロキシ・サポートの構成」セクションの手順に従う必要があります。

Windows 向けプロキシサポートを設定しています

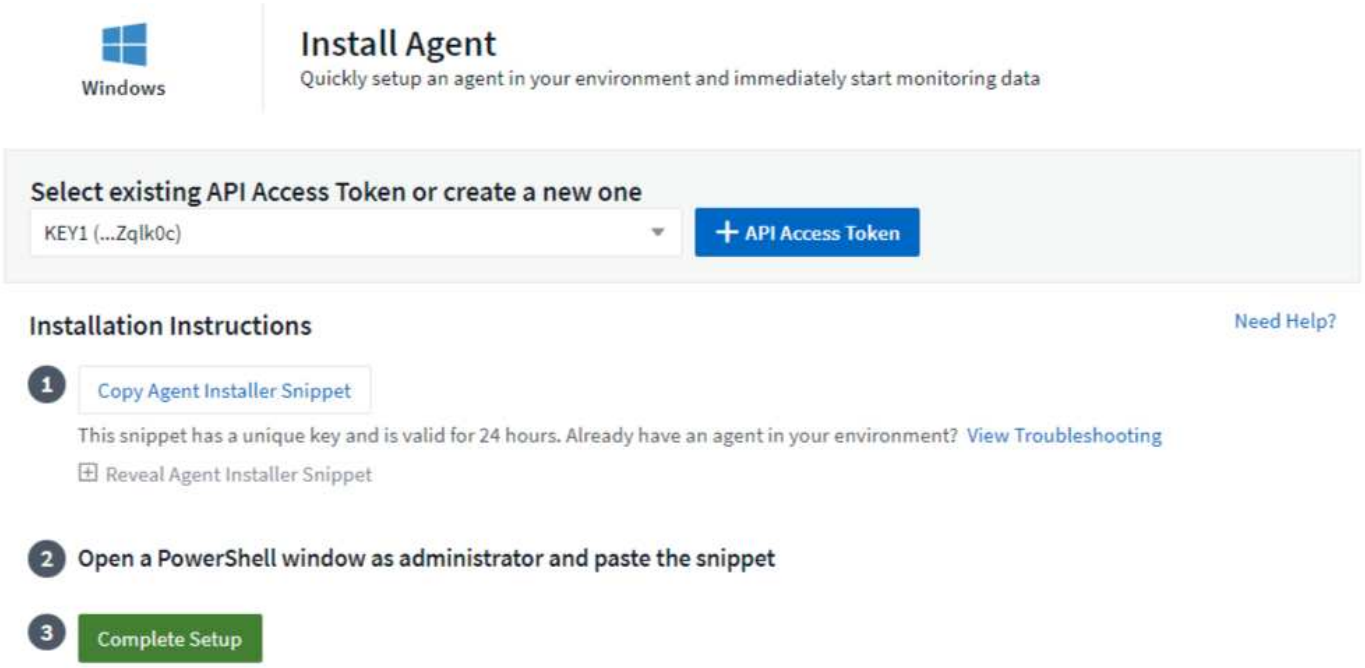
プロキシを使用する環境の場合は、をインストールする前にこのセクションをお読みください。

次の手順は '_http_proxy/https_proxy_environment 変数を設定するために必要なアクションの概要を示しています一部のプロキシ環境では '_no_proxy 環境変数も設定する必要があります

プロキシの背後にあるシステムの場合、 Telegraf エージェントをインストールする前に *https_proxy* および /or_http_proxy_environment 変数 * を設定するには、次の手順を実行します。

```
[System.Environment]::SetEnvironmentVariable("https_proxy",
"<proxy_server>:<proxy_port>",
[System.EnvironmentVariableTarget]::Machine)
```

エージェントをインストールしています



Windows にエージェントをインストールする手順：

1. エージェントアクセスキーを選択します。
2. エージェントのインストールダイアログからコマンドブロックをコピーします。クリップボードアイコンをクリックすると、コマンドをクリップボードに簡単にコピーできます。
3. PowerShell ウィンドウを開きます
4. コマンドを PowerShell ウィンドウに貼り付け、 Enter キーを押します。
5. コマンドは、適切なエージェントインストーラをダウンロードしてインストールし、デフォルト設定を行います。終了すると、エージェントサービスが再起動されます。コマンドには一意のキーがあり、 24 時間有効です。

6. [完了] または [続行] をクリックします

エージェントのインストール後、次のコマンドを使用してサービスを開始または停止できます。

```
Start-Service telegraf
Stop-Service telegraf
```

エージェントをアンインストールしています

Windows でエージェントをアンインストールするには、 PowerShell ウィンドウで次の手順を実行します。

1. Tegraf サービスを停止して削除します。

```
Stop-Service telegraf
sc.exe delete telegraf
```

2. 証明書を信頼ストアから削除します。

```
cd Cert:\CurrentUser\Root
//rm E5FB7B68C08B1CA902708584C274F8EFC7BE8ABC
rm 1A918038E8E127BB5C87A202DF173B97A05B4996
```

3. バイナリ、ログ、およびコンフィグレーションファイルを削除するには、 _C ： \Program Files\テレ グラムフォルダを削除します
4. レジストリから _SYSTEM\CurrentControlSet\Services\EventLog\Application\テレ グラムキーを削除します

Agent をアップグレードしています

テレグラムエージェントをアップグレードするには、次の手順に従います。

1. テレグラムサービスを停止および削除します。

```
Stop-Service telegraf
sc.exe delete telegraf
```

2. レジストリから _SYSTEM\CurrentControlSet\Services\EventLog\Application\テレ グラムキーを削除します
3. DELETE_C ： \Program Files\テレ グラム \テレ グラム af.conf_
4. DELETE_C ： \Program Files\テレ グラム \テレ グラム af.exe_
5. "新しいエージェントをインストールします"。

RHEL および CentOS

前提条件

- cURL 、 sudo 、 ping 、 sha256sum 、 openssl 、 dmidecode となります
- プロキシの背後にある場合は、「RHEL / CentOS *用のプロキシサポートの設定」セクションの手順に従う必要があります。

RHEL / CentOS でのプロキシサポートの設定

プロキシを使用する環境の場合は、をインストールする前にこのセクションをお読みください。

次の手順は '_http_proxy/https_proxy_environment 変数を設定するために必要なアクションの概要を示しています一部のプロキシ環境では '_no_proxy 環境変数も設定する必要があります

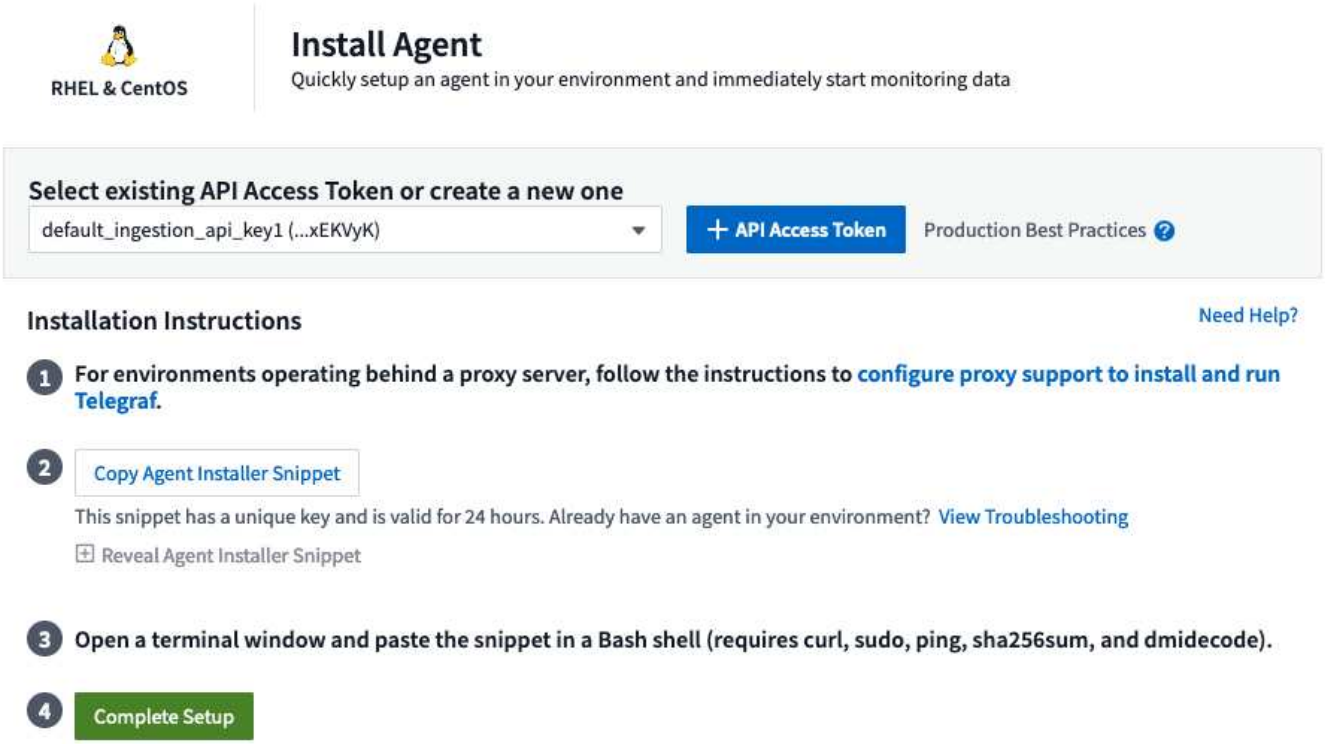
プロキシの背後にあるシステムの場合は、 Telegraf エージェントをインストールする前に、次の手順 * を実行します。

1. 現在のユーザの *https_proxy* 変数と _http_proxy_environment 変数を設定します。

```
 export https_proxy=<proxy_server>:<proxy_port>
. /etc/default/テレ グラム af_ を作成し、
_https_proxy_/or_http_proxy_variable の定義を挿入します。
```

```
https_proxy=<proxy_server>:<proxy_port>
```

エージェントをインストールしています



RHEL または **CentOS** にエージェントをインストールする手順：

1. エージェントアクセスキーを選択します。
2. エージェントのインストールダイアログからコマンドブロックをコピーします。クリップボードアイコンをクリックすると、コマンドをクリップボードに簡単にコピーできます。
3. Bash ウィンドウを開きます
4. Bash ウィンドウにコマンドを貼り付けて、 Enter キーを押します。
5. コマンドは、適切なエージェントインストーラをダウンロードしてインストールし、デフォルト設定を行います。終了すると、エージェントサービスが再起動されます。コマンドには一意のキーがあり、 24 時間有効です。
6. [完了] または [続行] をクリックします

エージェントのインストール後、次のコマンドを使用してサービスを開始または停止できます。

オペレーティングシステムで systemd （ CentOS 7+ および RHEL 7+ ）を使用している場合：

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

オペレーティングシステムで systemd （ CentOS 7+ および RHEL 7+ ）を使用していない場合：

```
sudo service telegraf start
sudo service telegraf stop
```

エージェントをアンインストールしています

Bash 端末で RHEL または CentOS のエージェントをアンインストールするには、次の手順を実行します。

1. Telegraf サービスを停止します。

```
systemctl stop telegraf (If your operating system is using systemd
(CentOS 7+ and RHEL 7+)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Tegraf エージェントを取り外します。

```
 yum remove telegraf
```

. 残っている設定ファイルまたはログファイルを削除します。

```
rm -rf /etc/telegraf*
rm -rf /var/log/telegraf*
```

Agent をアップグレードしています

テレグラムエージェントをアップグレードするには、次の手順に従います。

1. テレグラムサービスを停止します。

```
systemctl stop telegraf (If your operating system is using systemd
(CentOS 7+ and RHEL 7+)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. 前のテレグラムエージェントを削除します。

```
 yum remove telegraf
```

. xref:{relative_path}#rhel-and-centos["
新しいエージェントをインストールします"]。

Ubuntu と Debian

前提条件

- cURL 、 sudo 、 ping 、 sha256sum 、 openssl 、 dmidecode となります
- プロキシの背後にいる場合は、「Ubuntu / Debian *用のプロキシサポートの設定」セクションの手順に従う必要があります。

Ubuntu / Debian のプロキシサポートの設定

プロキシを使用する環境の場合は、をインストールする前にこのセクションをお読みください。

次の手順は '_http_proxy/https_proxy_environment 変数を設定するために必要なアクションの概要を示しています一部のプロキシ環境では '_no_proxy 環境変数も設定する必要があります

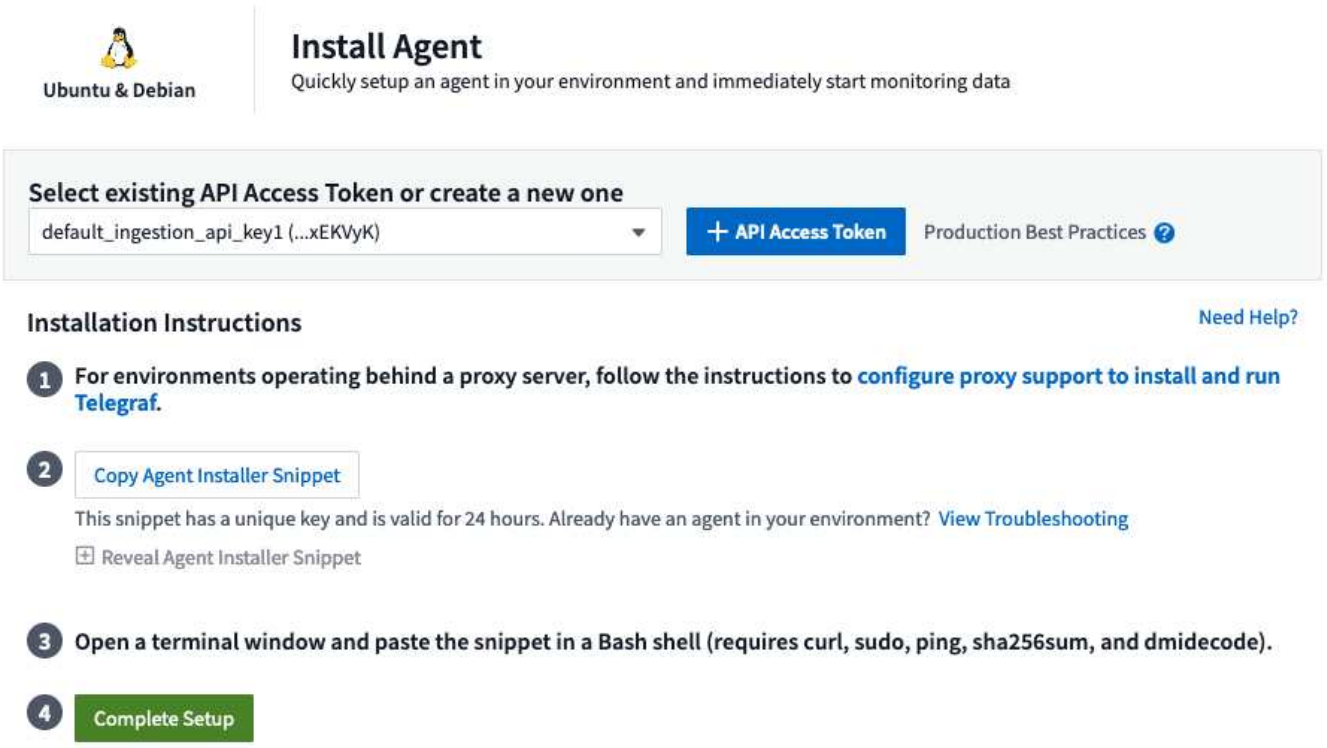
プロキシの背後にあるシステムの場合は、 Telegraf エージェントをインストールする前に、次の手順 * を実行します。

1. 現在のユーザの *https_proxy* 変数と _http_proxy_environment 変数を設定します。

```
 export https_proxy=<proxy_server>:<proxy_port>
. /etc/default/テレ グラムを作成し、 _https_proxy_/or_http_proxy_variable
以下の定義を挿入します。
```

```
https_proxy=<proxy_server>:<proxy_port>
```

エージェントをインストールしています



Debian または **Ubuntu** にエージェントをインストールする手順：

1. エージェントアクセスキーを選択します。
2. エージェントのインストールダイアログからコマンドブロックをコピーします。クリップボードアイコン

をクリックすると、コマンドをクリップボードに簡単にコピーできます。

3. Bash ウィンドウを開きます
4. Bash ウィンドウにコマンドを貼り付けて、 Enter キーを押します。
5. コマンドは、適切なエージェントインストーラをダウンロードしてインストールし、デフォルト設定を行います。終了すると、エージェントサービスが再起動されます。コマンドには一意のキーがあり、 24 時間有効です。
6. [完了] または [続行] をクリックします

エージェントのインストール後、次のコマンドを使用してサービスを開始または停止できます。

オペレーティング・システムが systemd を使用している場合：

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

オペレーティングシステムが systemd を使用していない場合は、次の手順を実行します。

```
sudo service telegraf start
sudo service telegraf stop
```

エージェントをアンインストールしています

Ubuntu または Debian でエージェントをアンインストールするには、 Bash ターミナルで次のコマンドを実行します。

1. Telegraf サービスを停止します。

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Tegraf エージェントを取り外します。

```
 dpkg -r telegraf
```

. 残っている設定ファイルまたはログファイルを削除します。

```
rm -rf /etc/telegraf*
rm -rf /var/log/telegraf*
```

Agent をアップグレードしています

テレグラムエージェントをアップグレードするには、次の手順に従います。

1. テレグラムサービスを停止します。

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. 前のテレグラムエージェントを削除します。

```
 dpkg -r telegraf
. xref:{relative_path}#ubuntu-and-
debian["新しいエージェントをインストールします"]。
```

チェックサムを検証する

Data Infrastructure Insightsエージェントインストーラは整合性チェックを実行しますが、ダウンロードしたアーティファクトをインストールまたは適用する前に独自の検証を実行することもできます。これを行うには、インストーラをダウンロードしてダウンロードしたパッケージのチェックサムを生成し、チェックサムをインストール手順に示されている値と比較します。

インストールせずにインストーラパッケージをダウンロードします

デフォルトのダウンロードおよびインストールではなく、ダウンロードのみの操作を実行するには、UIから取得したエージェントインストールコマンドを編集し、末尾の「インストール」オプションを削除します。

次の手順を実行します。

1. 指示に従ってエージェントインストーラスニペットをコピーします。
2. スニペットをコマンドウィンドウに貼り付ける代わりに、テキストエディタに貼り付けます。
3. コマンドから末尾の「--install」（Linux）または「-install」（Windows）を削除します。
4. コマンド全体をテキストエディタからコピーします。
5. 次に、コマンドウィンドウ（作業ディレクトリ内）に貼り付けて実行します。

Windows 以外（ Kubernetes の場合は次の例を使用します。実際のスクリプト名は異なる場合があります）

- Download and install （デフォルト）：

```
 installerName=cloudinsights-kubernetes.sh … && sudo -E -H
./$installerName --download --install
* ダウンロードのみ：
```

```
installerName=cloudinsights-kubernetes.sh … && sudo -E -H
./$installerName --download
```

Windows の場合

- Download and install （デフォルト）：

```
 !$($installerName=".\cloudinsights-windows.ps1") … -and
$(&$installerName -download -install)
* ダウンロードのみ：
```

```
!$($installerName=".\cloudinsights-windows.ps1") … -and
$(&$installerName -download)
```

download-onlyコマンドを実行すると、必要なすべてのアーティファクトがData Infrastructure Insightsから作業ディレクトリにダウンロードされます。アーティファクトには次のものがありますが、これらに限定することはできません。

- インストールスクリプト
- 環境ファイル
- YAMLファイル
- チェックサムファイル（末尾がSHA256.signedまたはSHA256.ps1）

インストールスクリプト、環境ファイル、 YAML ファイルは、目視検査を使用して検証できます。

チェックサム値を生成します

チェックサム値を生成するには、使用するプラットフォームに応じて次のコマンドを実行します。

- RHEL / Ubuntu：

```
 sha256sum <package_name>
* Windows の場合
```

```
Get-FileHash telegraf.zip -Algorithm SHA256 | Format-List
```

チェックサムを検証

チェックサムファイルから期待されるチェックサムを抽出する

- Windows 以外：

```
 openssl smime -verify -in telegraf*.sha256.signed -CAfile
netapp_cert.pem -purpose any -nosigs -noverify
* Windows の場合
```

```
(Get-Content telegraf.zip.sha256.ps1 -First 1).toUpper()
```

ダウンロードしたパッケージをインストールします

すべてのアーティファクトが正常に検証されたら、次のコマンドを実行してエージェントのインストールを開始できます。

Windows 以外：

```
 sudo -E -H ./<installation_script_name> --install
Windows の場合
```

```
.\cloudinsights-windows.ps1 -install
```

トラブルシューティング

エージェントの設定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
新しいプラグインを設定してTegrafを再起動すると、Tegrafが起動しない。ログには次のようなエラーが記録されています。 "[telegraf] Error running agent: Error loading config file /etc/telegraf/telegraf.d/cloudinsights-default.conf : plugin outputs.http:line <linenumber>: configuration specified the fields ["use_system_proxy"] but they were not used"	インストールされているTelegrafのバージョンが古い。このページの手順に従って、お使いのプラットフォームに対応するエージェント*をアップグレードしてください。
古いインストールでインストーラスクリプトを実行したが、エージェントがデータを送信していない	テレグラムエージェントをアンインストールし、インストールスクリプトを再実行します。お使いのプラットフォームに応じて、このページの*エージェントのアップグレード*の手順を実行します。

問題	次の操作を実行します
Data Infrastructure Insightsを使用してエージェントをインストール済み	ホスト /VM にエージェントがすでにインストールされている場合は、エージェントを再度インストールする必要はありません。この場合は、 Agent Installation （エージェントのインストール）画面で適切な Platform and Key （プラットフォームとキー）を選択し、 * Continue * （続行）または * Finish （完了） * をクリックします。
エージェントはすでにインストールされているが、Data Infrastructure Insightsインストーラを使用していない	以前のエージェントを削除し、Data Infrastructure Insights Agentのインストールを実行して、デフォルトの構成ファイルが正しく設定されていることを確認します。完了したら、 [* Continue * （続行）] または [* Finish （完了）] をクリックします。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

データコレクタの設定

Data Infrastructure Insights環境でData Collectorを構成して、データセンター内のデバイスからデータを収集します。

作業を開始する前に

- データの収集を開始する前に、 Acquisition Unit を設定しておく必要があります。
- データの収集元のデバイスのクレデンシャルが必要です。
- データの収集元のすべてのデバイスには、デバイスのネットワークアドレス、アカウント情報、およびパスワードが必要です。

手順

1. [Data Infrastructure Insights]メニューで、*[Observability]>[Collectors]*をクリックします。

   使用可能なデータコレクタがベンダー別に表示されます。

2. [+ Collector]*をクリックし、設定するデータコレクタを選択します。

   ダイアログボックスで、データコレクタを設定し、 Acquisition Unit を追加できます。

3. データコレクタの名前を入力します。
4. [詳細構成 *] をクリックして、追加の構成フィールドを追加します。すべてのデータコレクタで高度な設定が必要となるわけで
5. Test Configuration* をクリックして、データコレクタが正しく設定されていることを確認します。
6. [Add Collector]*をクリックして設定を保存し、Data Infrastructure Insightsテナントにデータコレクタを追加します。

サービスのデータがダッシュボードに表示されるか、クエリに使用できるようになるまで、ポーリング期間は最大 2 回かかる場合があります。

- 最初のインベントリポーリング：すぐに
- 第 1 回のパフォーマンスデータのポーリングでベースラインを確立：インベントリのポーリング直後
- 第 2 回パフォーマンスポーリング：第 1 回のパフォーマンスポーリングが完了してから 15 秒以内

ポーリングは、設定されたインベントリとパフォーマンスのポーリング間隔に従って続行されます。

データコレクタの収集ステータスの確認

データコレクタは、Data Infrastructure Insightsの主要な情報源であるため、実行状態を維持することが不可欠です。

データコレクタのステータスは、アセットページの右上に「 Acquired N minutes ago 」というメッセージとして表示されます。 N はアセットのデータコレクタの最新の取得時間を示します。取得日時も表示されます。

メッセージをクリックすると、データコレクタの名前、ステータス、および前回成功した収集時間を示すテーブルが表示されます。管理者としてサインインしている場合は、テーブルのデータコレクタ名のリンクをクリックすると、そのデータコレクタの詳細ページが表示されます。

設定済みデータコレクタの管理

[Installed Data Collectors]ページでは、Data Infrastructure Insights用に設定されたデータコレクタにアクセスできます。このページを使用して、既存のデータコレクタを変更できます。

手順

1. [Data Infrastructure Insights]メニューで、*[Observability]>[Collectors]*をクリックします。

   Available Data Collectors 画面が表示されます。

2. [インストール済みデータコレクタ *] をクリックします

   インストールされているすべてのデータコレクタのリストが表示されます。リストはコレクタを提供します
   名前、ステータス、コレクタがアクセスしているIPアドレス、およびデータが最後に取得された日時
   Aデバイスから。この画面で実行できる操作には、次のものがあります。

   - ポーリングの制御
   - データコレクタのクレデンシャルを
   - データコレクタのクローンを作成

Data Collector ポーリングの制御

データコレクタに変更を加えた後、すぐにポーリングして確認することができます
変更を加えたり、データコレクタのデータ収集を延期したりすることができます。
あなたが問題に取り組んでいる間、3日か5日。

手順

1. [Data Infrastructure Insights]メニューで、*[Observability]>[Collectors]*をクリックします。
2. [インストール済みデータコレクタ *] をクリックします
3. 変更する Data Collector の左側にあるチェックボックスをオンにします
4. ［ * 一括処理 * ］ をクリックして、実行するポーリングアクションを選択します。

   複数のデータコレクタに対して一括アクションを同時に実行できます。データを選択します
   をクリックし、* Bulk Action *メニューから実行するアクションを選択します。

データコレクタ情報の編集

既存のデータコレクタの設定情報を編集できます。

単一のデータコレクタを編集するには、次

1. [Data Infrastructure Insights]メニューで、*[Observability]>[Collectors]*をクリックして、インストールされているデータコレクタのリストを開きます。
2. 変更するデータコレクターの右にあるオプションメニューで、 * 編集 * をクリックします。

   [Edit Collector] ダイアログが開きます。

3. 変更内容を入力し、 * テスト構成 * をクリックして新しい構成をテストするか、 * 保存 * をクリックして構成を保存します。

複数のデータコレクタを編集することもできます。

1. 変更する各データコレクタの左側にあるチェックボックスをオンにします。
2. 「 * Bulk Actions * 」ボタンをクリックし、「 * Edit * 」を選択して、「 Edit Data Collector 」ダイアログを開きます。
3. 上記のようにフィールドを変更します。

   同じベンダーとモデルのデータコレクタを選択し、同じ Acquisition Unit に配置する必要があります。

   複数のデータコレクタを編集する場合、 Data Collector Name フィールドには「 Mixed 」と表示され、編集できません。ユーザー名やパスワードなどの他のフィールドには「混在」と表示され、編集できます。選択したデータコレクタ間で同じ値を共有するフィールドには、現在の値が表示され、編集できます。

   複数のデータコレクタを編集する場合、 * テスト設定 * ボタンは使用できません。

データコレクタのクローニング

クローン機能を使用すると、同じクレデンシャルを持つデータソースを簡単に追加できます
および属性を別のデータソースとして使用できます。クローニングを使用すると、複数のを簡単に構成できます
同じデバイスタイプのインスタンス。

手順

1. [Data Infrastructure Insights]メニューで、*[Observability]>[Collectors]*をクリックします。

2. [インストール済みデータコレクタ *] をクリックします。
3. コピーするデータコレクタの左側にあるチェックボックスをオンにします。
4. 選択したデータコレクターの右にあるオプションメニューで ' * クローン * をクリックします

   Clone Data Collector （クローンデータ収集）ダイアログが表示されます。

5. 必須フィールドに新しい情報を入力します。
6. [保存（ Save ）] をクリックします。

完了後

他のすべての属性と設定がクローニング処理によってコピーされ、新しいデータコレクタが作成されます。

データコレクタに対して一括操作を実行する

複数のデータコレクタの一部の情報を同時に編集できます。この機能を使用すると、複数のデータコレクタでポーリングの開始、ポーリングの延期、およびポーリングの再開を行うことができます。また、複数のデータコレクタを削除することもできます。

手順

1. [Data Infrastructure Insights]メニューで、*[Observability]>[Collectors]*をクリックします。
2. [インストール済みデータコレクタ *] をクリックします
3. 変更するデータコレクタの左側にあるチェックボックスをオンにします。
4. 右側のオプションメニューで、実行するオプションをクリックします。

完了後

選択した操作がデータコレクタで実行されます。データコレクタを削除するように選択すると、アクションを適合させる必要があるダイアログが表示されます。

データコレクタの問題の調査

データコレクタにエラーメッセージと「高」または「中」の影響がある場合は、データコレクタの概要ページにリンクされている情報を使用して、この問題を調査する必要があります。

次の手順に従って、失敗したデータコレクタの原因を確認します。データコレクタの障害メッセージは、[**Admin**] メニューおよび [*Installed Data Collectors] ページに表示されます。

手順

1. [**Admin**>*Data Collector*>*Installed Data Collectors] をクリックします。
2. [リンクされたデータコレクタの名前] をクリックして、 [概要] ページを開きます。
3. 概要ページのコメント領域で、同じ問題について調査している他のエンジニアのメモがある場合はその内容を確認します。
4. パフォーマンスのメッセージを確認します。
5. イベントタイムライングラフのセグメントにマウスポインタを合わせると、追加情報が表示されます。

6. デバイスのエラーメッセージを選択し、イベントタイムラインの下に表示された後、メッセージの右側に表示されるエラー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. この Data Collector 領域から報告されるデバイスでは、リストをフィルタして対象デバイスのみを表示したり、デバイスのリンクされた * 名前 * をクリックしてそのデバイスのアセットページを表示したりすることができます。
8. データコレクタの概要ページに戻ったら、ページの下部にある「最近の変更を表示」 * 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。

ダッシュボードギャラリーからインポートする

Data Infrastructure Insightsには、データに関するビジネスインサイトを提供するために推奨されるダッシュボードが多数用意されています。各ダッシュボードには、回答で特定の質問をしたり、現在環境で収集されているデータに関連する特定の問題を解決したりするためのウィジェットが含まれています。

ギャラリーからダッシュボードをインポートするには、次の操作を行います。

1. [ダッシュボード（Dashboards）]>[ダッシュボード（Dashboards）
2. [* + from Gallery （ギャラリーから * + ）] をクリックします

   推奨ダッシュボードのリストが表示されます。ダッシュボードには、解決に役立つ特定の質問の名前が付けられます。AWS 、ネットアップ、ストレージ、 VMware 、回答 その他

3. リストから 1 つ以上のダッシュボードを選択し、 * ダッシュボードの追加 * をクリックします。これらのダッシュボードがダッシュボードリストに表示されるようになりました。

推奨されるダッシュボードに加えて、現在のデータに関連しない追加のダッシュボード * をインポートすることもできます。たとえば、現在ストレージデータコレクタがインストールされていないが、将来の設定を計画している場合でも、ストレージに関連するダッシュボードをインポートできます。これらのダッシュボードは表示可能ですが、少なくとも 1 つのストレージデータコレクタが設定されるまでは、関連するデータは表示されません。

ダッシュボードギャラリーからのインポートは、管理者ロールまたはアカウント所有者ロールを持つユーザーが使用できます。

ユーザアカウントとロール

Data Infrastructure Insightsには、アカウント所有者、管理者、ユーザ、ゲストの4つのユーザアカウントロールが用意されています。各アカウントには、次の表に示す特定の権限レベルが割り当てられます。"招待済み"Data Infrastructure Insightsのユーザには特定のロールが割り当てられているか、または"シングルサインオン（ SSO ）許可"デフォルトのロールを使用してからサインインできます。SSO認証は、Data Infrastructure Insights Premium Editionの機能として使用できます。

アクセス許可レベル

ユーザアカウントを作成または変更するには、管理者権限を持つアカウントを使用します。各ユーザアカウントには、次の権限レベルからData Infrastructure Insightsの各機能のロールが割り当てられます。

ロール	オブザーバビリティ	ワークロードのセキュリティ	レポート作成	管理者
アカウント所有者	管理者と同じ	管理者と同じ	管理者と同じ	Administratorと同じで、SSO認証とアイデンティティフェデレーションの設定も管理できます。追加の所有者を割り当てることもできます。
管理者	すべてのオブザーバビリティ機能を実行できるだけでなく、データコレクタの管理も実行できます。	アラート、フォレンジック、データコレクタ、自動応答ポリシー、セキュリティ用APIトークンなど、すべてのセキュリティ機能を実行できます。 管理者は、他のユーザを招待することもできますが、割り当てることができるのはセキュリティロールのみです。	Reporting API トークンの管理、レポートの設定、レポートタスクのシャットダウンと再起動など、すべての管理タスクに加えて、すべてのUser/Author 関数を実行できます。 管理者は、他のユーザーを招待することもできますが、割り当てることができるのは Reporting ロールのみです。	他のユーザを招待できますが、オブザーバビリティロールのみを割り当てることができます。SSO設定を表示できますが、変更できません。APIアクセストークンを作成および管理できます。監査情報を表示できます。サブスクリプション情報、使用状況、履歴を表示できます。グローバルアラート通知およびサブスクリプション通知の受信者リストを管理できます。
ユーザ	ダッシュボード、クエリ、アラート、アノテーション、アノテーションルール、アプリケーションをサポートし、デバイス解決を管理できます。	アラートを表示および管理し、フォレンジックを表示できます。ユーザーロールは、アラートステータスの変更、メモの追加、スナップショットの手動作成、制限ユーザーアクセスの管理を行うことができます。	すべてのゲスト / コンシューマ機能を実行できるほか、レポートとダッシュボードの作成と管理も可能です。	使用不可

ロール	オブザーバビリティ	ワークロードのセキュリティ	レポート作成	管理者
ゲスト	アセットページ、ダッシュボード、アラートへの読み取り専用アクセスが可能で、クエリの表示と実行が可能です。	アラートおよびフォレンジックを表示できます。ゲストロールは、アラートステータスの変更、メモの追加、スナップショットの手動作成、ユーザーアクセスの制限を行うことはできません。	レポートの表示、スケジュール設定、実行、および言語やタイムゾーンなどの個人設定を行うことができます。ゲスト / コンシューマは、レポートの作成や管理タスクの実行はできません。	使用不可

ベストプラクティスとして、管理者権限を持つユーザの数を制限することを推奨します。アカウントの最大数は、ユーザアカウントまたはゲストアカウントです。

ユーザロール別の**Data Infrastructure Insights**権限

次の表に、各ユーザロールに付与されているData Infrastructure Insightsの権限を示します。

フィーチャー（ Feature ）	管理者/ アカウント所有者	ユーザ	ゲスト
Acquisition Unit ：追加 / 変更 / 削除	Y	N	N
アラート * ：作成 / 変更 / 削除	Y	Y	N
アラート * ：表示	Y	Y	Y
アノテーションルール：作成、実行、変更、削除	Y	Y	N
注釈：作成 / 修正 / 割り当て / 表示 / 削除 / 削除	Y	Y	N
API アクセス * ：作成 / 名前変更 / 無効化 / 無効化	Y	N	N
アプリケーション：作成 / 表示 / 変更 / 削除	Y	Y	N
アセットページ：変更	Y	Y	N
アセットページ：表示	Y	Y	Y
監査：表示	Y	N	N
クラウドコスト	Y	N	N
セキュリティ	Y	N	N
ダッシュボード：作成 / 変更 / 削除	Y	Y	N
ダッシュボード：表示	Y	Y	Y

データコレクタ：追加 / 変更 / ポーリング / 削除	Y	N	N
通知:表示	Y	Y	Y
通知:変更	Y	N	N
クエリ：作成 / 変更 / 削除	Y	Y	N
クエリ：表示 / 実行	Y	Y	Y
デバイス解決	Y	Y	N
レポート * ：表示 / 実行	Y	Y	Y
レポート * ：作成 / 変更 / 削除 / スケジュール	Y	Y	N
サブスクリプション：表示 / 変更	Y	N	N
ユーザー管理：招待 / 追加 / 変更 / 非アクティブ化	Y	N	N

- Premium Edition が必要です

ユーザーを招待してアカウントを作成する

新しいユーザアカウントを作成するには、BlueXPを使用します。ユーザはEメールで送信された招待状に応答できますが、BlueXPのアカウントをお持ちでない場合は、BlueXPにサインアップして招待を承諾する必要があります。

作業を開始する前に

- ユーザー名は、招待の電子メールアドレスです。
- 割り当てるユーザロールを理解します。
- パスワードは、サインアップの過程でユーザーによって定義されます。

手順

1. Data Infrastructure Insightsにログイン
2. メニューで、 [*Admin] > [User Management] をクリックします

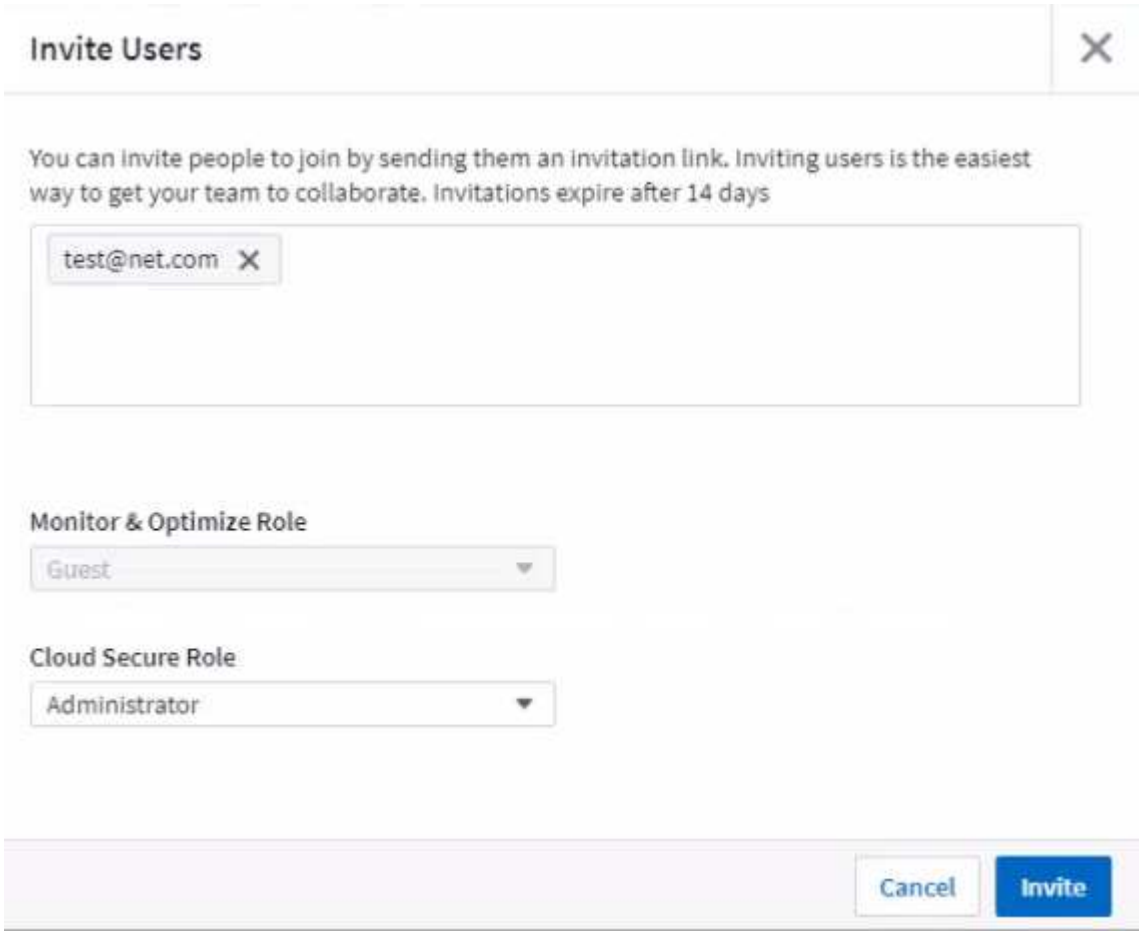
   User Management （ユーザー管理）画面が表示されます。画面には、システム上のすべてのアカウントのリストが表示されます。

3. [* + ユーザー *] をクリックします

   ユーザーの招待 * 画面が表示されます。

4. 招待状の電子メールアドレスまたは複数のアドレスを入力します。
   - 注： * 複数のアドレスを入力すると、すべて同じロールで作成されます。同じロールに設定できるユーザは複数だけです。
5. Data Infrastructure Insightsの各機能について、ユーザのロールを選択します。

選択できる機能とロールは、特定の管理者ロールでアクセスできる機能によって異なります。たとえば、レポートの管理者ロールのみを持っている場合、レポートの任意のロールにユーザーを割り当てることはできますが、観察能力またはセキュリティのロールを割り当てることはできません。



6. [* 招待 *] をクリックします

   招待がユーザーに送信されます。ユーザーは 14 日以内に招待を承諾する必要があります。招待を受諾すると、 NetApp Cloud Portal に送られ、招待状の E メールアドレスを使用してサインアップされます。そのEメールアドレスのアカウントをすでにお持ちの場合は、サインインするだけでData Infrastructure Insights環境にアクセスできます。

既存のユーザのロールを変更する

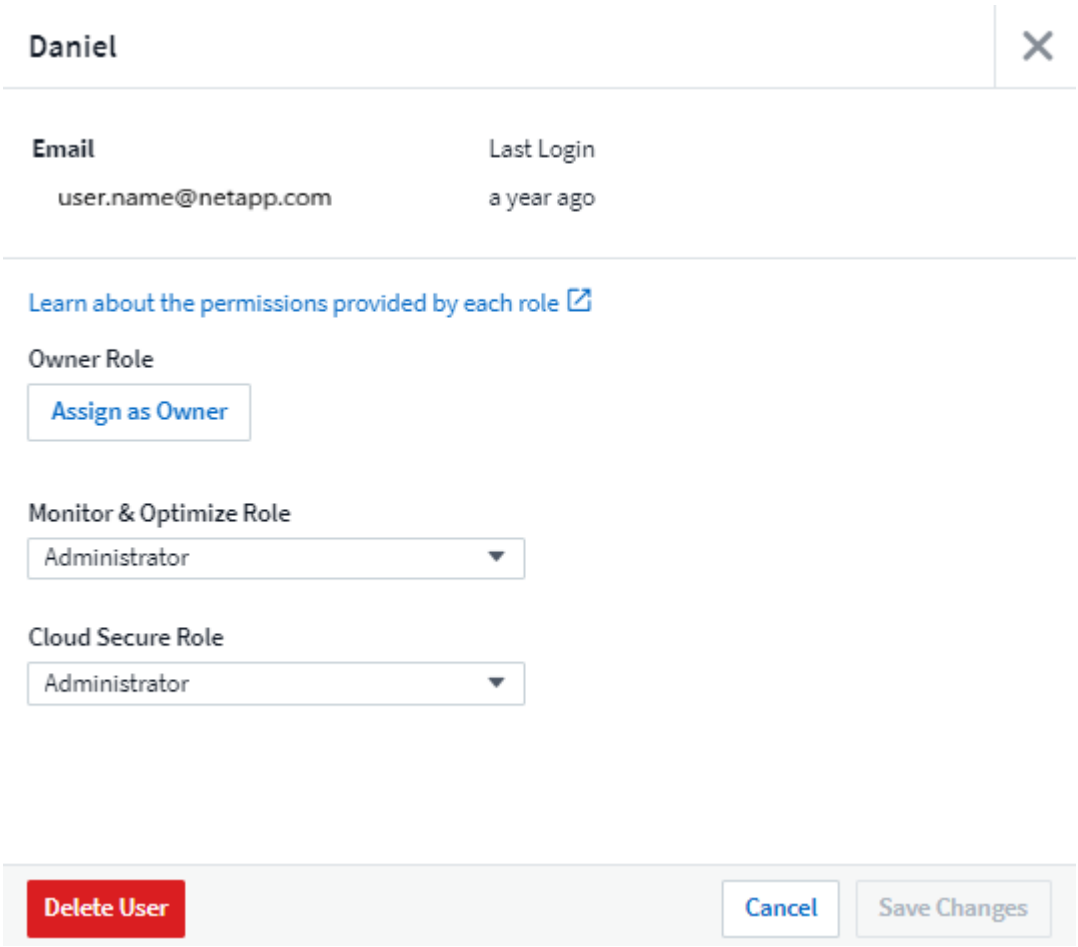
既存のユーザーの役割を変更し、 * セカンダリアカウント所有者 * として追加するには、次の手順を実行します。

1. [*Admin] > [User Management] をクリックします。画面には、システム上のすべてのアカウントのリストが表示されます。
2. 変更するアカウントのユーザ名をクリックします。
3. 必要に応じて、Data Infrastructure Insightsの各機能セットでユーザのロールを変更します。
4. 変更の保存 _ をクリックします。

セカンダリアカウント所有者を割り当てるには、次の手順に従います

アカウント所有者ロールを別のユーザーに割り当てるには、監視機能のアカウント所有者としてログインする必要があります。

1. [*Admin] > [User Management] をクリックします。
2. 変更するアカウントのユーザ名をクリックします。
3. [ユーザー] ダイアログで、 [所有者として割り当て] をクリックします。
4. 変更を保存します。



アカウント所有者はいくつでも設定できますが、所有者の役割は、選択したユーザーのみに制限することをお勧めします。

ユーザを削除します

管理者ロールを持つユーザーは ' ユーザーの名前をクリックして ' ダイアログの *Delete User* をクリックすることにより ' ユーザー (会社に所属していないユーザーなど) を削除できますこのユーザはData Infrastructure Insights環境から削除されます。

ユーザが作成したダッシュボードやクエリなどは、削除してもData Infrastructure Insights環境で引き続き使用できます。

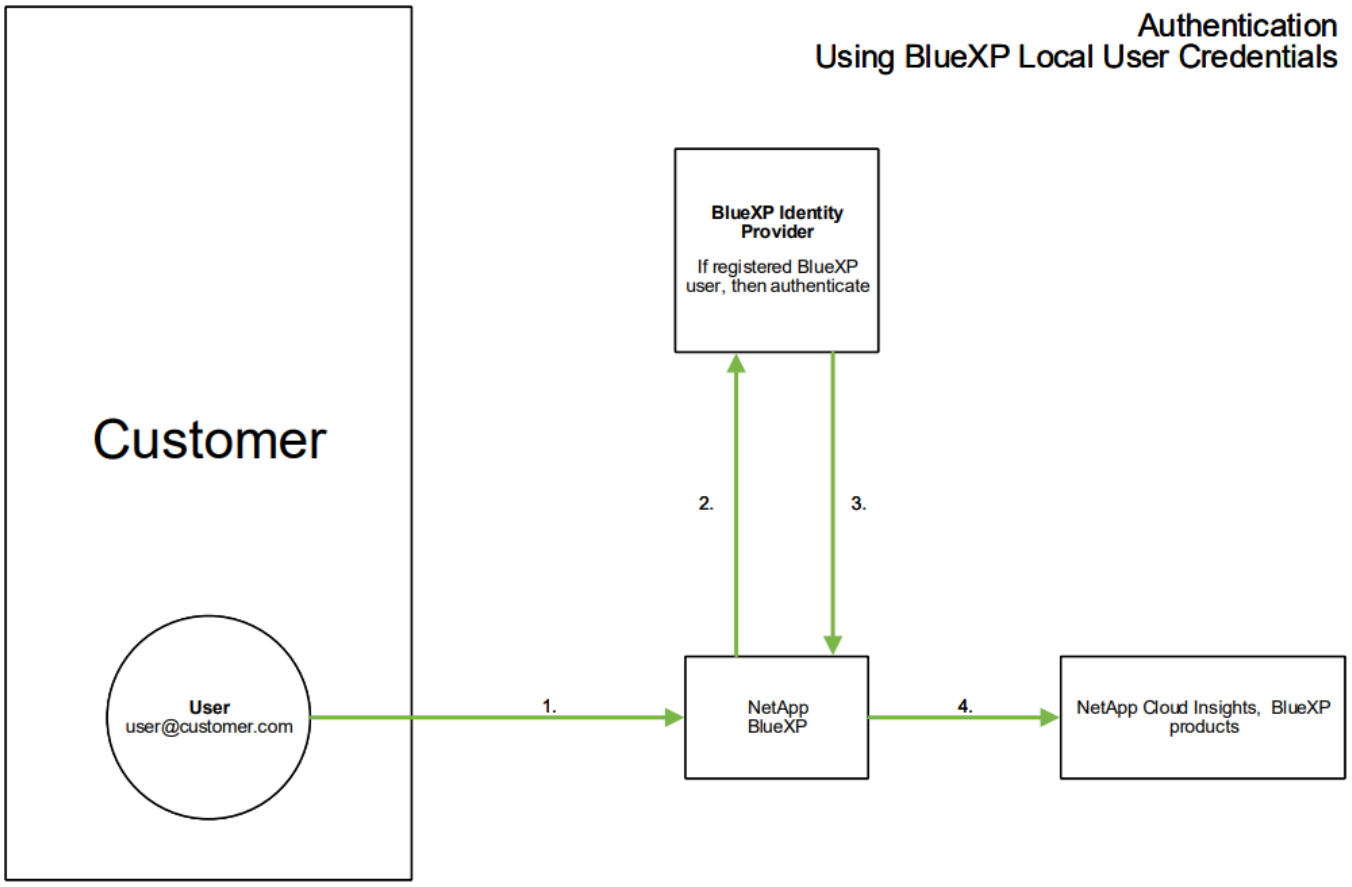
シングルサインオン（ SSO ）とアイデンティティフェデレーション

アイデンティティフェデレーションとは

アイデンティティフェデレーションを使用：

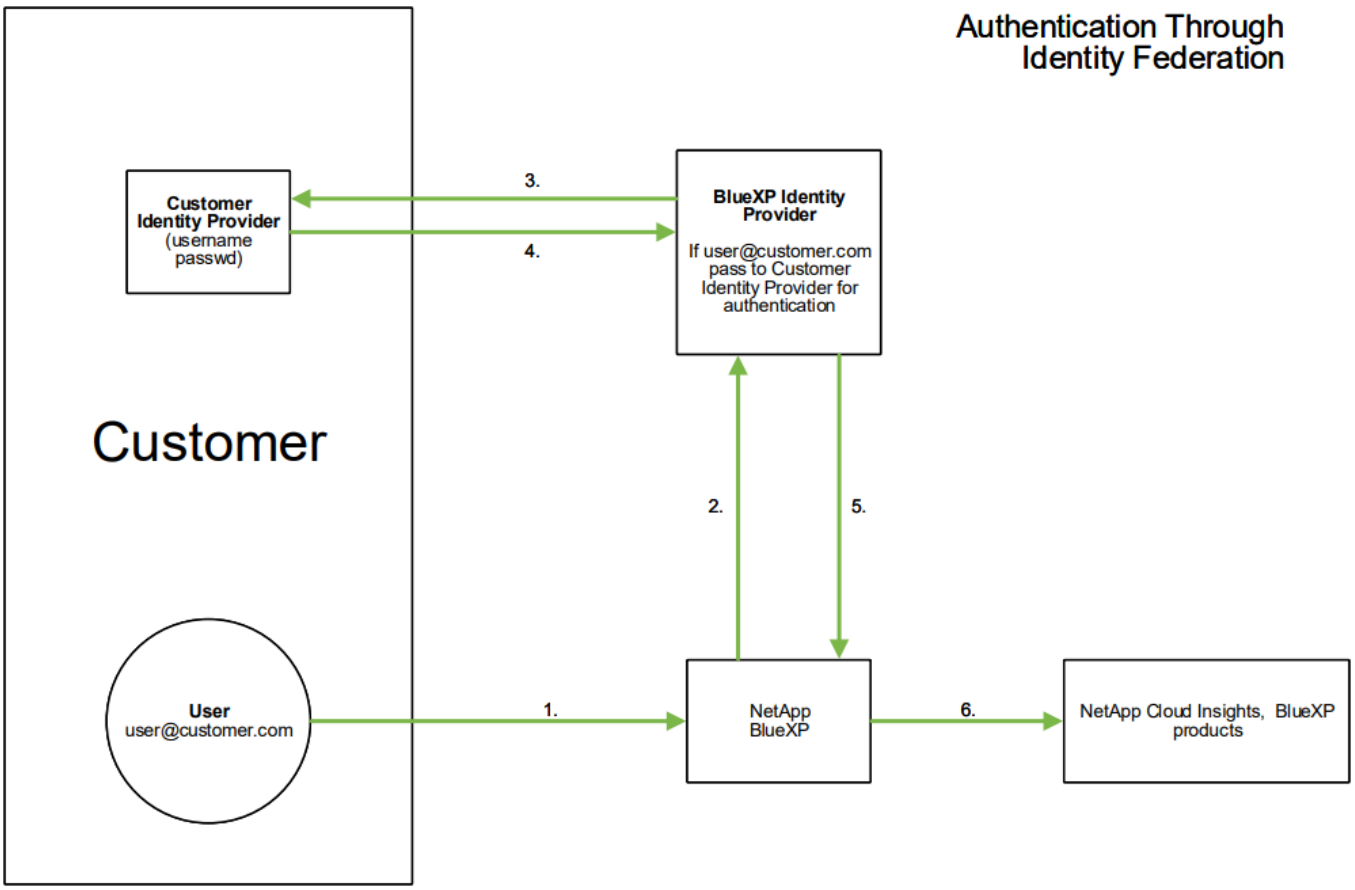
- 認証は、お客様の社内ディレクトリにあるお客様の資格情報を使用して、お客様のアイデンティティ管理システムに委任され、多要素認証（ MFA ）などの自動化ポリシーが適用されます。
- ユーザはすべてのNetApp BlueXPサービスに一度ログインします（シングルサインオン）。

ユーザアカウントは、すべてのクラウドサービスのNetApp BlueXPで管理されます。デフォルトでは、認証はBlueXPローカルユーザプロファイルを使用して行われます。このプロセスの概要を以下に示します。



ただし、お客様の中には、独自のアイデンティティプロバイダを使用して、データインフラ分析情報やその他のNetApp BlueXP サービスのユーザを認証したいと考えるお客様もいます。アイデンティティフェデレーションでは、NetApp BlueXPアカウントは社内ディレクトリのクレデンシャルを使用して認証されます。

次に、このプロセスの簡単な例を示します。



上の図では、ユーザがData Infrastructure Insightsにアクセスすると、そのユーザは認証のためにお客様のアイデンティティ管理システムに誘導されます。アカウントが認証されると、ユーザはData Infrastructure InsightsのテナントURLに移動します。

アイデンティティフェデレーションの有効

BlueXPはAuth0を使用してアイデンティティフェデレーションを実装し、Active Directoryフェデレーションサービス（ADFS）やMicrosoft Azure Active Directory（AD）などのサービスと統合します。アイデンティティフェデレーションを設定するには、 "BlueXPフェデレーションの手順"。

Data Infrastructure InsightsでSSOを使用するには、事前にBlueXP アイデンティティフェデレーションを設定する必要があります。

BlueXP でのアイデンティティフェデレーションの変更は、データインフラの分析情報だけでなく、すべてのNetApp BlueXP サービスにも適用されることを理解しておくことが重要です。この変更については、お客様が所有する各BlueXP製品のNetAppチームと話し合い、使用している設定がアイデンティティフェデレーションと連携していることを確認したり、アカウントの調整が必要な場合はその旨をお客様に伝えてください。お客様は、社内の SSO チームをアイデンティティフェデレーションの変更にも関与させる必要があります。

アイデンティティフェデレーションを有効にしたら、会社のアイデンティティプロバイダに対する変更（SAMLからMicrosoft ADへの移行など）には、ユーザのプロファイルを更新するためにBlueXPでトラブルシューティング/変更/対応が必要になる可能性があることを理解しておくことも重要です。

この問題またはその他のフェデレーションの問題については、次のURLでサポートチケットを開くことができます。 https://mysupport.netapp.com/site/help カテゴリ「bluexp.netapp.com」>「フェデレーションの問題」を選択します。

シングルサインオン（ **SSO** ）ユーザの自動プロビジョニング

管理者は、ユーザを招待するだけでなく、社内ドメイン内のすべてのユーザに対して*シングルサインオン（SSO）ユーザの自動プロビジョニング*によるData Infrastructure Insightsへのアクセスを有効にすることもできます。個別に招待する必要はありません。SSOが有効な場合は、同じドメインEメールアドレスを持つすべてのユーザが社内クレデンシャルを使用してData Infrastructure Insightsにログインできます。

> _SSOユーザ自動プロビジョニング_は、Data Infrastructure Insights Premium Editionで使用できます。Data Infrastructure Insightsで有効にするには、事前に構成する必要があります。SSOユーザ自動プロビジョニングの設定には、"アイデンティティフェデレーション"上記のセクションで説明したように、NetApp BlueXP を介した設定が含まれます。フェデレーションを使用すると、シングルサインオンユーザは、Security Assertion Markup Language 2.0（SAML）やOpenID Connect（OIDC）などのオープン標準を使用して、社内ディレクトリのクレデンシャルを使用してNetApp BlueXPアカウントにアクセスできます。

_SSOユーザ自動プロビジョニング_を設定するには、**[管理]>[ユーザ管理]***ページで、事前に**BlueXP**アイデンティティフェデレーションを設定しておく必要があります。バナーの[フェデレーションの設定]*リンクを選択して、BlueXPフェデレーションに進みます。設定が完了すると、Data Infrastructure Insightsの管理者はSSOユーザログインを有効にできます。管理者が _SSO ユーザーの自動プロビジョニング _ を有効にすると、すべての SSO ユーザー（ゲストやユーザーなど）にデフォルトの役割を選択します。SSO を使用してログインしたユーザには、このデフォルトロールが割り当てられます。

管理者が、デフォルトの SSO ロールから 1 人のユーザを昇格する場合（管理者に昇格する場合など）には、これは、ユーザの右側のメニューをクリックし、 _Assign Role_を 選択することにより、 [*Admin] > [User Management] ページで実行できます。この方法で明示的なロールが割り当てられたユーザは、_SSO User Auto-Provisioning_がその後無効になった場合でも、引き続きData Infrastructure Insightsにアクセスできます。

ユーザに昇格されたロールが不要になった場合は ' メニューをクリックしてユーザの削除を実行できますユーザがリストから削除されます。_SSO User Auto-Provisioning_が有効になっている場合、ユーザはデフォルトのロールでSSOを使用して引き続きData Infrastructure Insightsにログインできます。

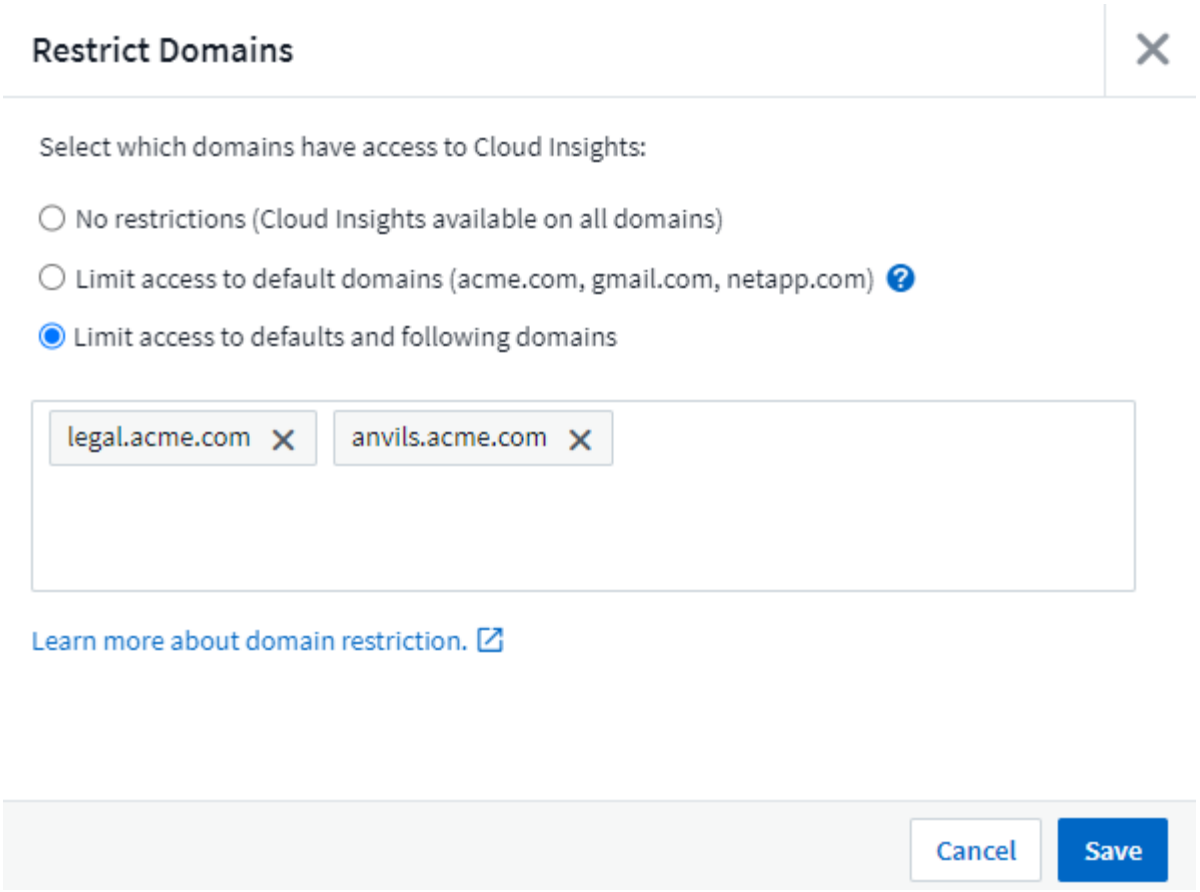
SSO ユーザーを非表示にするには、 * SSO ユーザーを表示 * チェックボックスをオフにします。

ただし、次のいずれかに該当する場合は、 _SSO ユーザの自動プロビジョニング _ を有効にしないでください。

- 組織にData Infrastructure Insightsのテナントが複数ある
- 組織では、フェデレーテッドドメインのすべてのユーザに、Data Infrastructure Insightsテナントへの一定レベルの自動アクセスを許可したくないと考えています。_ この時点では、グループを使用してこのオプションでのロールアクセスを制御することはできません。

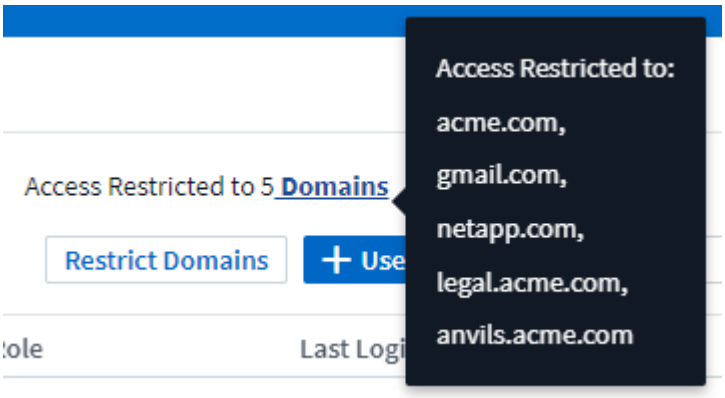
ドメインによるアクセスの制限

Data Infrastructure Insightsでは、指定したドメインのみにユーザアクセスを制限できます。[Admin]>[User Management]ページで、[Restrict Domains]を選択します。



次の選択肢が表示されます。

- 制限なし：ドメインに関係なく、ユーザは引き続きData Infrastructure Insightsにアクセスできます。
- デフォルトドメインへのアクセスを制限する：デフォルトドメインは、Data Infrastructure Insights環境のアカウント所有者が使用するドメインです。これらのドメインは常にアクセス可能です。
- 指定したデフォルトおよびドメインへのアクセスを制限します。デフォルトのドメインに加えて、Data Infrastructure Insights環境へのアクセスを許可するドメインをリストします。



Data Infrastructure Insightsのデータコレクタリスト

Data Infrastructure Insightsは、多数のベンダーやサービスが提供するさまざまなデータコレクタをサポートしています。

データコレクタは、次のタイプによって分類されます。

- インフラ：ストレージアレイ、スイッチ、ハイパーバイザー、バックアップデバイスなどのベンダーのデバイスから購入
- サービス： Kubernetes や Docker などのサービスから購入_ 連動 _ とも呼ばれます。

Data Infrastructure Insightsでサポートされているデータコレクタのアルファベット順リスト：

Data Collector	を入力します
"Amazon EC2 および EBS "	インフラ
"AWS S3をストレージとして使用"	インフラストラクチャ
"NetApp ONTAP 対応の Amazon FSX "	インフラ
"Apache "	サービス
"Azure NetApp Files の特長 "	インフラ
"Azure VM および VHD "	インフラ
"Brocade Network Advisor （ BNA ） "	インフラ
"Brocade ファイバチャネルスイッチ "	インフラ
"Brocade FOS REST "	インフラ
"Cisco MDS ファブリックスイッチ "	インフラ
"総領事 "	サービス
"Couchbase "	サービス
"CouchDB "	サービス
"Cohesity SmartFiles "	インフラ
"Dell EMC Data Domain の略 "	インフラ
"Dell EMC ECS の場合 "	インフラ
"Dell EMC PowerScale （旧 Isilon ） "	インフラ
"Dell EMC Isilon / PowerScale REST"	インフラ
"Dell EMC PowerStore"	インフラ
"Dell EMC RecoverPoint "	インフラ
"Dell EMC ScaleIO/PowerFlex "	インフラ
"Dell EMC Unity "	インフラ

Data Collector	を入力します
"Dell EMC Unisphere REST"	インフラ
"Dell EMC VMAX/PowerMax ファミリのデバイス "	インフラ
"Dell EMC VNX Block Storage の略 "	インフラ
"Dell EMC VNX ファイル "	インフラ
"Dell EMC VNX ユニファイド "	インフラ
"Dell EMC VPLEX "	インフラ
"Dell EMC XtremIO のインストール "	インフラ
"Dell XC シリーズ "	インフラ
"Docker です "	サービス
"Elasticsearch を指定します "	サービス
"フリップ "	サービス
"Fujitsu ETERNUS DX "	インフラ
"Google コンピューティングとストレージ "	インフラ
"Hadoop "	サービス
"HAProxy "	サービス
"日立コンテンツプラットフォーム（ HCP ）"	インフラ
"Hitachi Vantara Command Suite の略 "	インフラ
"Hitachi Vantara NAS Platform の略 "	インフラ
"Hitachi Ops Center の略 "	インフラ
"HP Enterprise Alletra 6000 （旧 Nimble ）ストレージ "	インフラ
"HP Enterprise Alletra 9000/Primera （旧 3PAR ）ストレージ "	インフラ
"HP Enterprise Command View の順にクリックします "	インフラ
"Huawei OceanStor および Dorado Devices "	インフラ
"IBM Cleversafe "	インフラ
"IBM CS シリーズ "	インフラ
"IBM PowerVM "	インフラ
"IBM SAN Volume Controller （ SVC ） "	インフラ
"IBM System Storage DS8000 シリーズ "	インフラ
"IBM XIV および A9000 ストレージ "	インフラ
"Infinidat InfiniBox "	インフラ
"Java "	サービス

Data Collector	を入力します
"カフカ "	サービス
"カパトール "	サービス
"キバナ "	サービス
"Kubernetes "	サービス
"Lenovo HX シリーズ "	インフラ
"Memcached "	サービス
"Microsoft Azure NetApp Files の略 "	インフラ
"Microsoft Hyper-V "	インフラ
"MongoDB "	サービス
"MySQL "	サービス
"NetApp Cloud Volumes ONTAP の略 "	インフラ
"ネットアップの AWS 向け Cloud Volume サービス "	インフラ
"ONTAP 9.9 以降でのネットアップクラウド接続 "	インフラ
"NetApp Data ONTAP 7-Mode "	インフラ
"NetApp E-Series "	インフラ
"NetApp EシリーズREST "	インフラ
"NetApp ONTAP 対応の Amazon FSX"	インフラ
"NetApp HCI 仮想センター "	インフラ
"NetApp ONTAP データ管理ソフトウェア "	インフラ
"NetApp ONTAP RESTコレクタ "	インフラ
"NetApp ONTAP Select の略 "	インフラ
"NetApp SolidFire オールフラッシュアレイ "	インフラ
"NetApp StorageGRID "	インフラ
"netstat "	サービス
"nginx "	サービス
"ノード "	サービス
"Nutanix NX シリーズ "	インフラ
"OpenStack の機能を使用 "	インフラ
"OpenZFS の場合 "	サービス
"Oracle ZFS Storage Appliance の略 "	インフラ
"PostgreSQL "	サービス
"Puppet Agent "	サービス
"Pure Storage FlashArray "	インフラ

Data Collector	を入力します
"Red Hat 仮想化 "	インフラ
"Redis "	サービス
"RethinkDB "	サービス
"RHELおよびCentOS "	サービス
"Rubrik CDMストレージ "	インフラ
"Ubuntu Debian "	サービス
"VMware vSphere の場合 "	インフラ
"Windows の場合 "	サービス
"Zookeeper の追加 "	サービス

Data Infrastructure Insightsのサブスクライブ

Data Infrastructure Insightsは、次の3つの簡単なステップで開始できます。

- でアカウントに登録します "* NetApp BlueXP *" ネットアップのクラウドサービスをすべて利用できるようになります。
- "* 無償トライアル *"Data Infrastructure Insightsのに登録して、利用可能な機能を確認してください。
- * Data Infrastructure Insightsにサブスクライブ*すると、"ネットアップの営業担当者"直接または経由でデータに中断なく継続的にアクセスできます。"AWS Marketplace"

登録プロセスでは、Data Infrastructure Insights環境をホストするグローバルリージョンを選択できます。詳細については、『Data Infrastructure Insights』をご覧"情報と地域"ください。

Data Infrastructure InsightsのBasicエディションとPremiumエディションで使用できる機能の完全な比較については、"データインフラ分析情報の価格設定"ページを参照してください。

Inactive Data Infrastructure Insights Basic Edition環境が削除され、そのリソースが再利用されます。連続する 30 日間のユーザアクティビティがない場合、 7 日間にわたってデータが取り込まれていない場合、環境は非アクティブとみなされます。Data Infrastructure Insightsは、環境が削除される4日前に通知を送信し、猶予期間を設定します。

Data Infrastructure Insightsの使用中に南京錠のアイコンが表示された場合は、現在のサブスクリプションでその機能を利用できないか、限定された形式で利用できないことを意味します。フルアクセスのためにその機能を購読してください。一部の機能は、サブスクライブする前にとして使用でき モジュールの評価 ます。

試用版

Data Infrastructure Insightsにサインアップして、環境がアクティブであれば、Data Infrastructure Insightsの30日間無償トライアルに参加できます。このトライアルでは、Data Infrastructure Insightsがお客様の環境で提供する機能を確認できます。

試用期間中は、いつでもData Infrastructure Insightsにサブスクライブできます。Data Infrastructure Insightsにサブスクライブすると、データへの中断のないアクセスと幅広い"* 製品サポート *"オプションが保証されます。

Data Infrastructure Insightsの無償トライアルが終了間近になると、バナーが表示されます。そのバナー内に_View Subscription_linkがあり、* Admin → Subscription *ページが開きます。管理者以外のユーザにはバナーが表示されますが、サブスクリプションページに移動することはできません。

Data Infrastructure Insightsの評価期間が4日以内に終了するように設定されていて、試用期間をさらに30日間延長できます。トライアルを延長できるのは 1 回だけです。トライアルの期限が切れている場合は延長できません。

AWS Marketplaceで試用

また、AWS Marketplaceで無料トライアルに登録することもできます。AWS Marketplaceの無償トライアルでは、33日間の試用期間でData Infrastructure Insightsにアクセスでき、最大499管理ユニット（MU）まで利用できます。

注：499 MUを超える値を設定すると、「違反」状態になります。トライアルが違反状態の間は、違反が解決されるまで、設定されているMUの数を減らすか、Data Infrastructure Insightsにサブスクライブすることで、一部のData Infrastructure Insights機能にアクセスできなくなります。

AWS Marketplaceの無償トライアルを延長することはできません。試用期間中はいつでも、* Admin → Subscription *ページからData Infrastructure Insights Basic Editionサブスクリプションにダウングレードしたり、Data Infrastructure Insightsの有料サブスクリプションに変更したりできます。

トライアル期間が終了した場合はどうなりますか？

無償トライアルの有効期限が切れていて、Data Infrastructure Insightsにまだサブスクライブしていない場合は、サブスクライブするまで機能が制限されます。データの取り込みが中止される場合があり、数週間後にデータ保持ポリシーに従ってデータが削除されます。

サブスクリプションの有効期限が切れた場合はどうなりますか？

Data Infrastructure Insightsのサブスクリプションをお持ちで、そのサブスクリプションの有効期限が切れている場合は、サブスクリプションを更新するために5日間の猶予期間が与えられます。Data Infrastructure Insightsのすべての機能は、この猶予期間中もアクティブなままです。

猶予期間が経過すると、更新するまでData Infrastructure Insightsの機能は一時停止されます。更新については、*[Admin]>[Subscription]*ページを参照するか、NetAppセールスにお問い合わせください。

猶予期間終了までに収集されたData Infrastructure Insightsデータは、猶予期間後30日間はそのまま維持されます。この時間内にサブスクリプションを更新すると、猶予期間が経過するまでのすべてのデータが利用可能になります。

サブスクリプション*の有効期限が切れた場合はどうなりますか？

Data Infrastructure Insightsのサブスクリプションをお持ちで、そのサブスクリプションの有効期限が切れている場合は、サブスクリプションを更新するために5日間の猶予期間が与えられます。Data Infrastructure Insightsのすべての機能は、この猶予期間中もアクティブなままです。

猶予期間が経過すると、更新するまでData Infrastructure Insightsの機能は一時停止されます。更新については、*[Admin]>[Subscription]*ページを参照するか、NetAppセールスにお問い合わせください。

Data Infrastructure Insightsのデータは、猶予期間後30日間そのまま維持されます。この時間内にサブスクリプションを更新すると、猶予期間が経過するまでのすべてのデータが利用可能になります。

モジュールの評価

また、*モジュール評価*もご利用いただけます。たとえば、インフラオブザーバビリティにすでにサブスクライブしていて、Kubernetesを環境に追加する場合は、NetApp Kubernetes監視オペレータのインストール時から、Kubernetesオブザーバビリティの30日間の評価が自動的に行われます。評価期間の終了時に、Kubernetes Observability Managed Unitの使用料金のみが請求されます。

評価後に新しいManaged Unit（MU）の使用料が請求されることに注意してください。そのため、適切な計画を立ててください。モジュールの評価が終了すると、サービスの中断を回避するためにMUを追加する必要があるかどうかが通知されます。

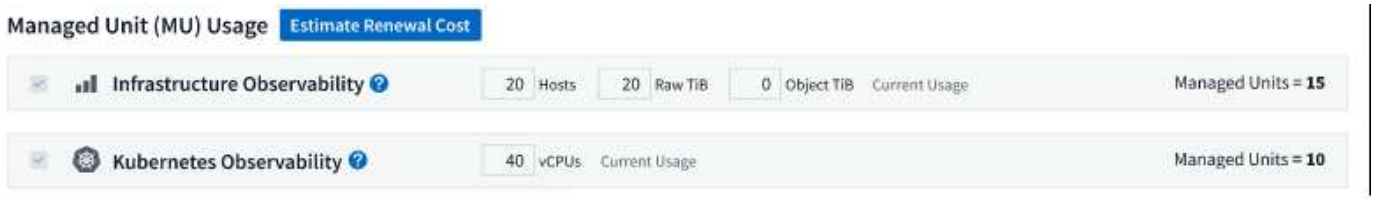
管理ユニットの使用状況は、**[管理]>[**サブスクリプション**]**ページの[使用状況]タブで監視できます。

画面"]

A_Module Evaluation_は_トライアルではありません_- Data Infrastructure Insightsサービスの無償トライアル期間をお客様に提供して、適切で購入可能であることを確認する場合は、タームトライアルを使用します。モジュールの評価方法は異なります。これは、有料サブスクリプションの直近数カ月間に使用していないData Infrastructure Insightsのモジュールを有料のお客様が試すことを許可する場合です。評価がアクティブな場合、新しく構成されたモジュールの料金だけが免除されます。お客様の作業環境はまだサブスクリプション期間中であり、無償トライアルに復帰していません。サブスクリプションは変更されていません。

試算ツール

モジュール評価中に、モジュールで消費されるリソースのMU使用量は変更されません。 ただし、(_Summary_tabの)* Estimator *を開いて、評価後にMUがどのように課金されるかを確認したり、将来必要になる可能性のあるMU数の「What if」シナリオでプレイしたりすることができます。Estimatorを終了して数値をリセットします。



モジュールの横にあるチェックボックスをオンにして、モジュール全体のMUを推定コストから追加または削除します。

Estimatorでは、現在のサブスクリプション期間を維持してライセンスを付与されたManaged Unitの数を増やすアドオンや、現在のサブスクリプションのときに購入する更新サブスクリプションの更新オプションのいず

れかのアドオンの番号がどのように積み重ねられているかを確認することもできます。 期間終了。

モジュール評価の対象となるのは、サブスクリプションごとに1回のみです。

サブスクリプションオプション

サブスクライブするには、*[管理]→[サブスクリプション]*に移動します。*Subscribe*ボタンに加えて、インストールされているデータコレクタを確認し、推定計測値を計算することができます。一般的な環境の場合は、セルフサービスのAWS Marketplaceボタンをクリックします。ご使用の環境に 1,000 台以上の管理対象ユニットが含まれている場合、または含まれる予定の場合は、ボリューム価格の対象となります。

オブザーバビリティ計測

データインフラの分析インフラのオブザーバビリティとKubernetesのオブザーバビリティは、* Managed Unit *ごとに計測されます。管理対象ユニットの使用量は、 * ホストまたは仮想マシン * の数と、インフラ環境で管理されている * フォーマットされていない容量 * の量に基づいて計算されます。

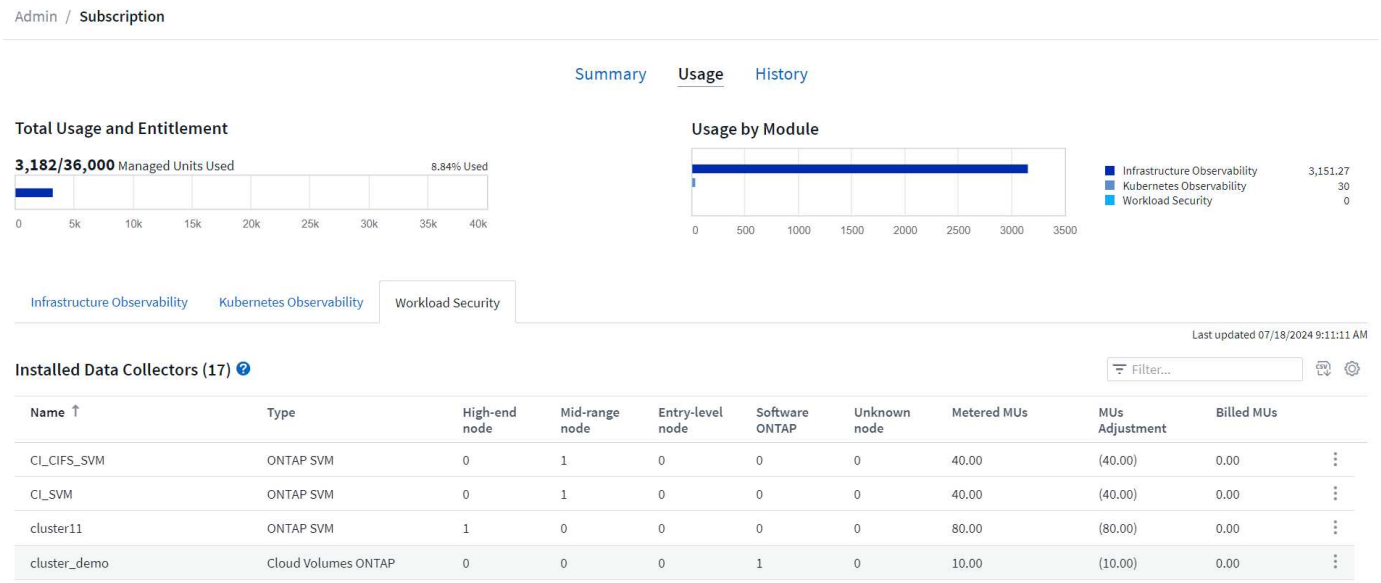
- 1 台の管理対象ユニット = 2 台のホスト（任意の仮想マシンまたは物理マシン）
- 1 管理ユニット = 物理ディスクまたは仮想ディスクのフォーマットされていない容量の 4TiB
- 1 Managed Unit = 40TiBの未フォーマット容量（AWS S3、Cohesity SmartFiles、Dell EMC Data Domain、Dell EMC ECS、Hitachi Content Platform、IBM Cleversafe、NetApp StorageGRID、 ルブリク
- 1 Managed Unit = KubernetesのvCPU 4台。
  - 1 Managed Unit（K8s）の調整=インフラでも監視されるノードまたはホスト×2

1 、 000 台以上の管理対象ユニットが含まれている、または含まれる予定の環境では、 * ボリューム価格設定 * の対象となり、ネットアップ営業に登録を依頼するように求められます。を参照してください 下 詳細：

ワークロードのセキュリティ計測

ワークロードのセキュリティは、オブザーバビリティの計測と同じアプローチを使用してクラスタごとに計測されます。

ワークロードセキュリティの使用状況は、**[管理者]>[サブスクリプション]***ページの[ワークロードセキュリティ]*タブで確認できます。



既存のワークロードセキュリティサブスクリプションでは、ノードの使用量がManaged Unitを消費しないように、MU使用量が調整されます。Data Infrastructure Insightsは、使用量を測定して、ライセンスされた使用量に確実に準拠します。

登録方法を教えてください。

管理ユニット数が 1 、 000 台未満の場合は、ネットアップ営業またはから登録できます セルフサブスクライブ AWS Marketplace 経由で提供

ネットアップの営業担当者にサブスクライブ

予想される管理ユニット数が 1,000 以上の場合は、をクリックします "* 販売担当者 * にお問い合わせください" ボタンをクリックして、ネットアップ営業チームに登録してください。

有償のサブスクリプションをデータインフラ分析環境に適用できるように、Data Infrastructure Insights のシリアル番号*を**NetApp**営業担当者に提出する必要があります。シリアル番号は、**Data Infrastructure Insights**のトライアル環境を一意に識別するもので、[Admin]>[Subscription]*ページで確認できます。

AWS Marketplace でセルフサブスクライブ

AWS Marketplaceサブスクリプションを既存のData Infrastructure Insightsトライアルアカウントに適用するには、アカウント所有者または管理者である必要があります。さらに、 Amazon Web Services （ AWS ）アカウントが必要です。

Amazon Marketplaceのリンクをクリックすると、AWS "データインフラの分析情報"サブスクリプションページが開き、サブスクリプションを完了できます。このページでは、計算ツールで入力した値が AWS のサブスクリプションページに入力されていないことに注意してください。管理対象ユニットの総数を入力する必要があります。

管理対象ユニットの総数を入力し、 12 か月または 36 か月のサブスクリプション期間を選択したら、「 * アカウントの設定 * 」をクリックしてサブスクリプションプロセスを終了します。

AWSのサブスクリプションプロセスが完了すると、現在のData Infrastructure Insights環境に戻ります。また

は、環境がアクティブでなくなった場合（ログアウトした場合など）は、NetApp BlueXPのサインインページに移動します。Data Infrastructure Insightsに再度サインインすると、お客様のサブスクリプションが有効になります。

AWS Marketplace のページで「 * アカウントの設定 * 」をクリックしてから、 AWS サブスクリプションの手続きを 1 時間以内に完了する必要があります。1 時間以内に完了しない場合は、もう一度「 * アカウントの設定 * 」をクリックして処理を完了する必要があります。

問題が発生し、サブスクリプションプロセスが正常に完了しない場合でも、環境にログインすると「トライアルバージョン」のバナーが表示されます。この場合は、 * Admin > Subscription * に移動して、契約プロセスを繰り返すことができます。

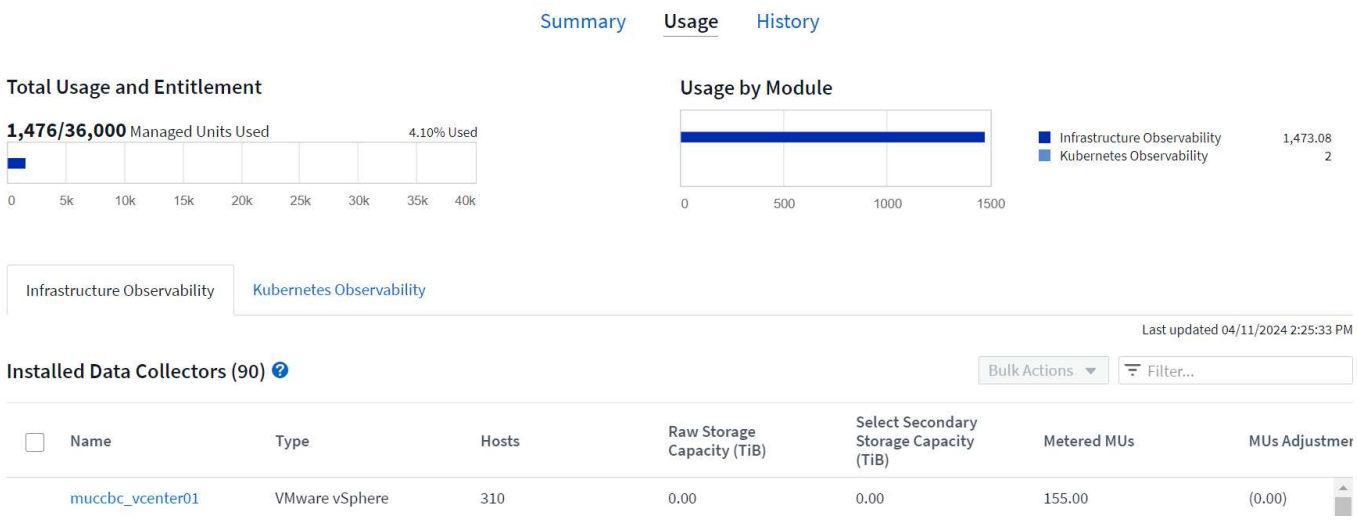
サブスクリプションステータスを表示します

サブスクリプションがアクティブになると、 [*Admin] > [Subscription] * ページからサブスクリプションのステータスと管理ユニットの使用状況を確認できます。

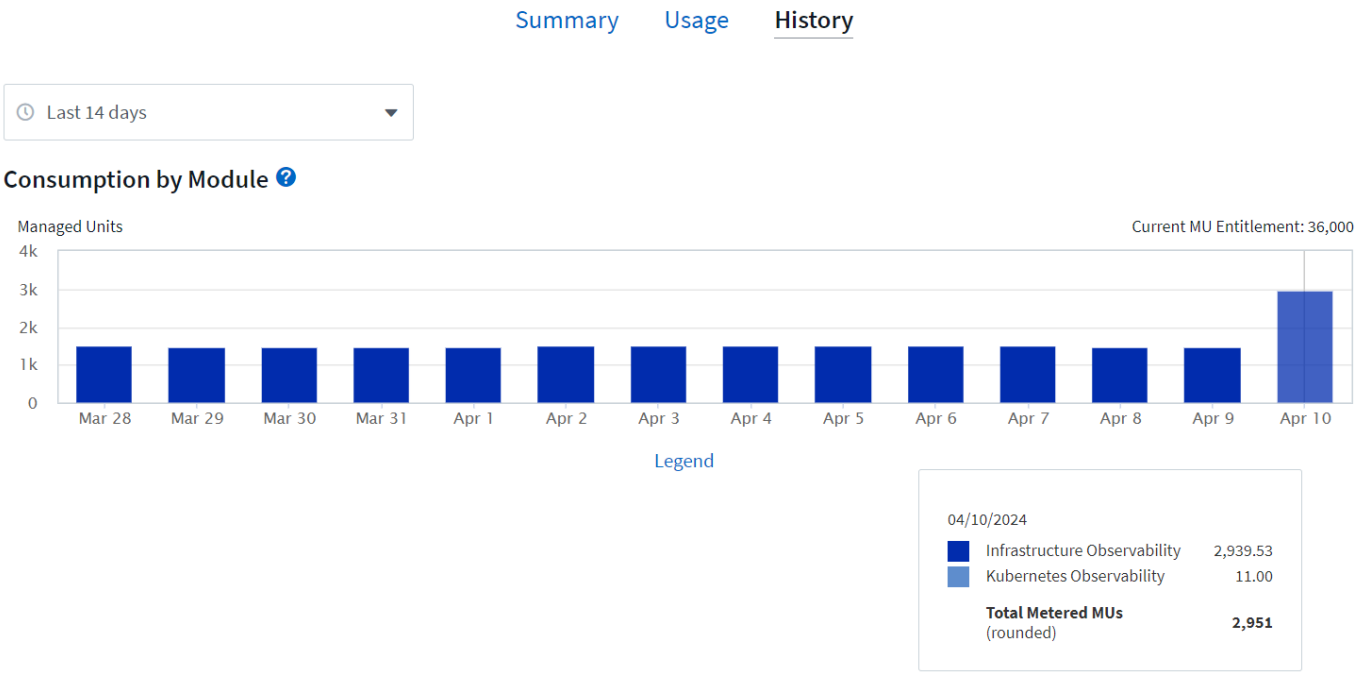
Subscription * Summary *タブには、次のような情報が表示されます。

- 現在のエディション
- サブスクリプションシリアル番号
- 現在のMUエンタイトルメント

[* Usage]タブには、現在のMUの使用状況と、その使用状況がデータコレクタ別に表示されます。



[History（履歴）]タブには、過去7～90日間のMU使用状況が表示されます。グラフの列にカーソルを合わせると、モジュール別の内訳（オブザーバビリティ、Kubernetesなど）が表示されます。



使用状況管理を表示します

[Usage Management]タブには、Managed Unitの使用状況の概要と、コレクタまたはKubernetesクラスタ別のManaged Unitの消費状況を示すタブが表示されます。

フォーマットされていない容量管理対象ユニット数は、環境内の合計物理容量を表し、最も近い管理対象ユニットに切り上げられます。

管理対象ユニットの合計は、サマリセクションのデータコレクタ数とは若干異なる場合があります。これは、管理対象ユニットの数が最も近い管理対象ユニットに切り上げられるためです。データコレクタリストのこれらの数値の合計は、ステータスセクションの管理対象ユニットの合計よりも少し高くなる場合があります。サマリセクションには、サブスクリプションの実際の管理ユニット数が表示されます。

利用状況がサブスクライブした金額に近づいている、または超過している場合は、データコレクタを削除するか、Kubernetesクラスタの監視を停止することで、使用量を減らすことができます。このリストの項目を削除するには、「3つのドット」メニューをクリックして_Delete_を選択します。

購読している使用量を超えた場合はどうなりますか？

管理下ユニットの使用率が総加入量の 80% 、 90% 、 100% を超えると、警告が表示されます。

* 使用量が * を超えた場合	* これは / 推奨される処置 : *
• 80% *	情報バナーが表示されます。対処は不要です。
• 90%*	警告バナーが表示されます。購読している管理ユニット数を増やすことができます。

* 使用量が * を超えた場合	* これは / 推奨される処置 : *
• 100%*	次のいずれかを実行するまで、エラーバナーが表示されます。 • データコレクタを削除して、Managed Unitの使用量がサブスクライブした量以下になるようにする • サブスクリプションを変更してManaged Unitの数を増やす

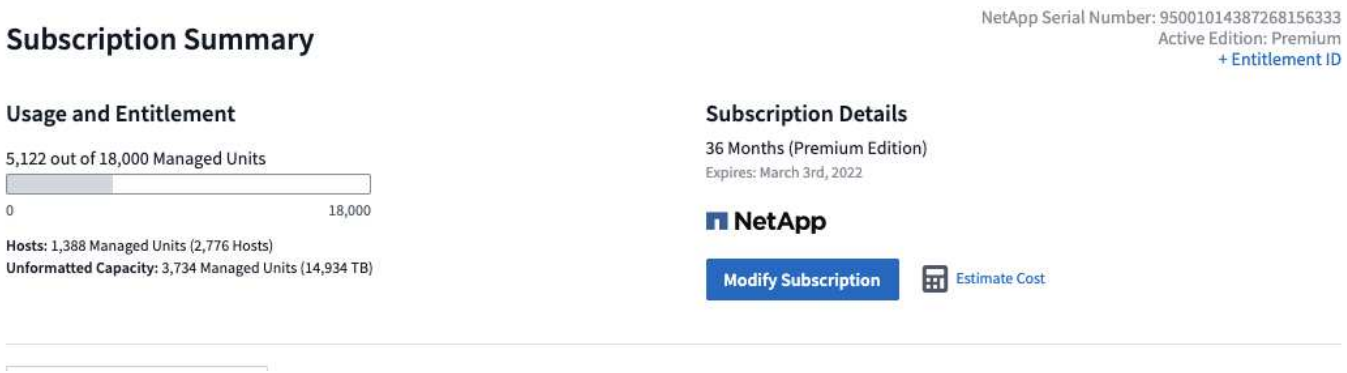
直接購読して、トライアルをスキップしてください

Data Infrastructure Insightsは "AWS Marketplace"、最初に試用環境を作成することなく、から直接サブスクライブすることもできます。サブスクリプションが完了し、環境がセットアップされると、すぐにサブスクライブされます。

エンタイトルメント ID の追加

Data Infrastructure Insightsにバンドルされている有効なNetApp製品を所有している場合は、その製品のシリアル番号を既存のData Infrastructure Insightsサブスクリプションに追加できます。たとえば、NetApp Astra Control Centerを購入した場合、Astra Control Centerライセンスのシリアル番号を使用してData Infrastructure Insightsでサブスクリプションを識別できます。Data Infrastructure Insightsでは、このエンタイトルメントID _を参照しています。

Data Infrastructure Insightsサブスクリプションに使用権IDを追加するには、*[Admin]>[Subscription]*ページで、[+Entitlement ID_]をクリックします。



オブザーバビリティ

ダッシュボードの作成

ダッシュボードの概要

Data Infrastructure Insightsでは、インフラデータの運用ビューを柔軟に作成できます。さまざまなウィジェットを使用してカスタムダッシュボードを作成し、それぞれのダッシュボードでデータの表示やグラフを柔軟に行うことができます。

これらのセクションの例は、説明のみを目的としたものであり、想定されるすべてのシナリオを網羅しているわけではありません。ここに記載されている概念や手順を参考にしながら、実際のニーズに応じたデータ用のダッシュボードを作成してください。

ダッシュボードの作成

新しいダッシュボードは次のどちらかの場所に作成します。

- * ダッシュボード > [+ 新しいダッシュボード] *
- * ダッシュボード > すべてのダッシュボードを表示 > * [+ ダッシュボード] * ボタンをクリックします

ダッシュボードコントロール

ダッシュボード画面には、次のような複数のコントロールがあります

- * 期間セレクタ * ：過去 15 分間から過去 30 日間、またはカスタムの期間である最大 31 日間のデータをダッシュボードに表示できます。ウィジェットごとにこのグローバルな期間を無効にすることができます。
- * 編集 * ボタン：これを選択すると編集モードが有効になり、ダッシュボードに変更を加えることができます。新しいダッシュボードは、デフォルトで編集モードで開きます。
- * 保存 * ボタン：ダッシュボードを保存または削除できます。

  [保存（ Save ）] をクリックする前に新しい名前を入力することで、現在のダッシュボードの名前を変更できます。

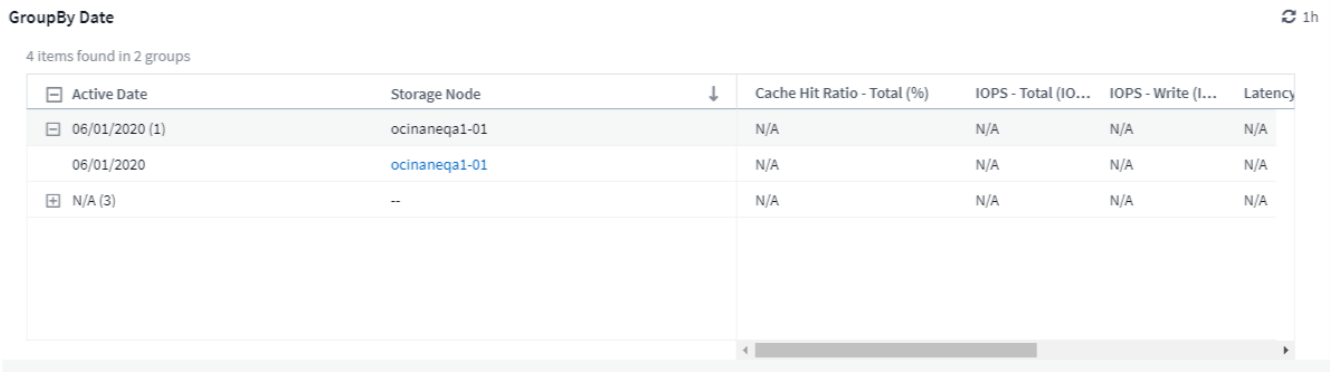
- * 表、グラフ、その他のウィジェットをいくつでもダッシュボードに追加できる [ウィジェットの追加] ボタン。

  ウィジェットは、サイズを変更したり、ダッシュボード内で別の位置に移動したりすることで、現在のニーズに合わせてデータを見やすくすることができます。

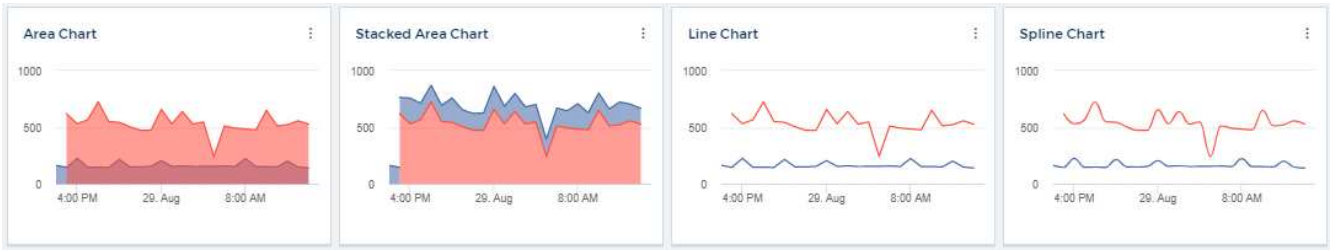
ウィジェットタイプ

次のタイプのウィジェットから選択できます。

- * 表ウィジェット *: 選択したフィルターや列に基づいてデータを表示する表。テーブルデータは、グループにまとめて、折りたたんだり展開したりすることができます。

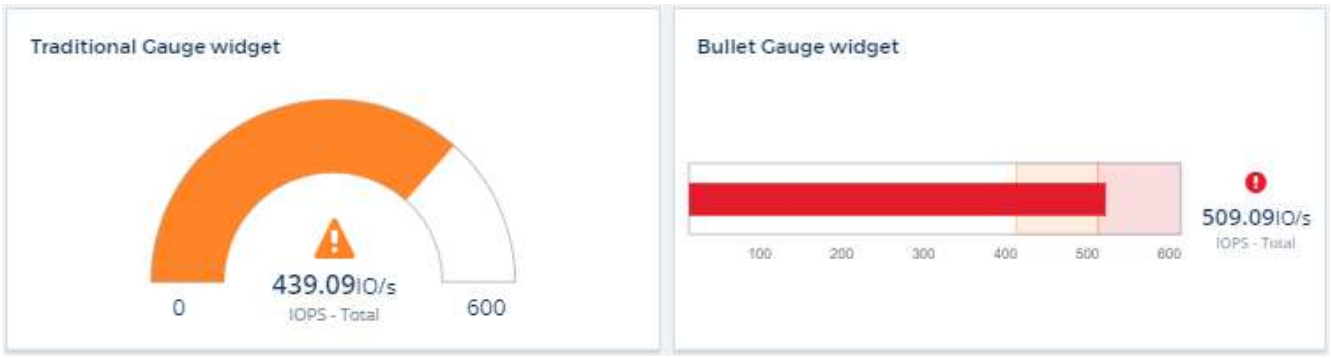


- * ライン、スプライン、エリア、積み上げ面グラフ * ：これらは、パフォーマンスやその他のデータを時系列で表示できる時系列グラフウィジェットです。

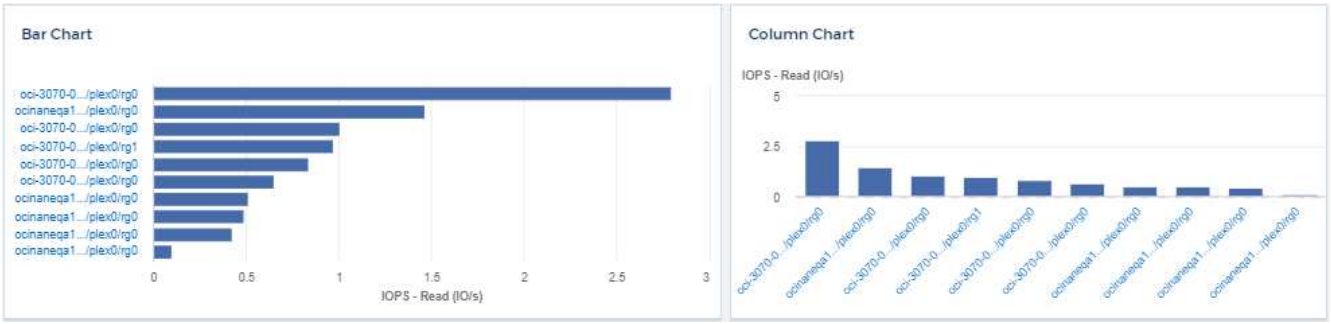


- * 単一値ウィジェット * ：カウンタから直接取得することも、クエリや式を使用して計算することもできる単一の値を表示するウィジェット。カラーの書式設定しきい値を定義して、値が予想範囲、警告範囲、または重要範囲のいずれであるかを表示できます。

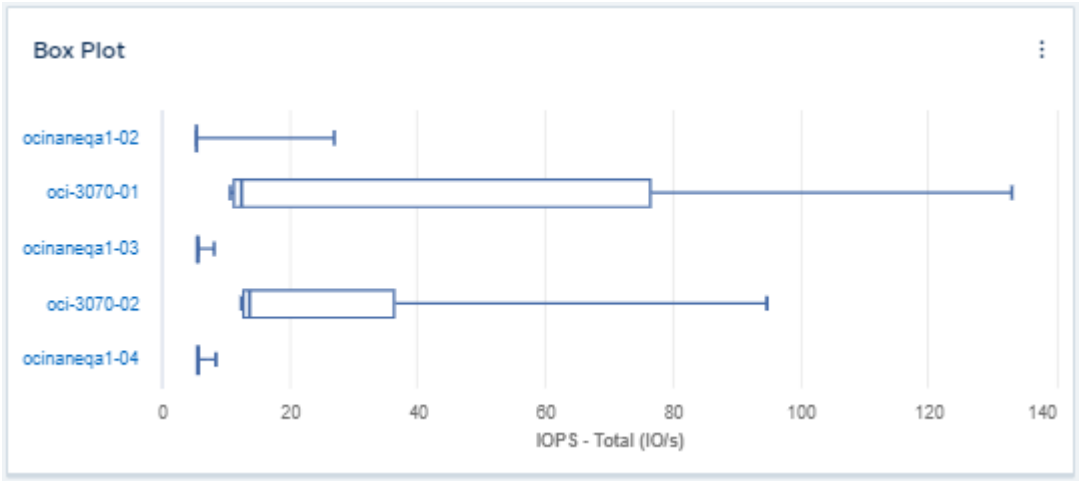
- * ゲージウィジェット * ：単一値のデータを従来の（固体）ゲージまたは箇条書きゲージに表示します。「警告」または「重大」の値に基づいた色で表示します "カスタマイズ"。



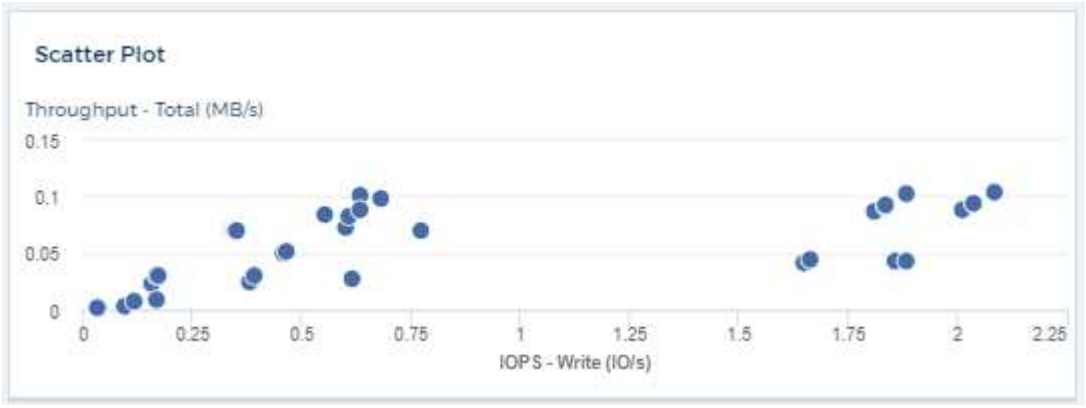
- * バー、棒グラフ * ：容量別のトップ 10 ストレージや IOPS 別の下位 5 ボリュームなど、上位または下位の N 値が表示されます。



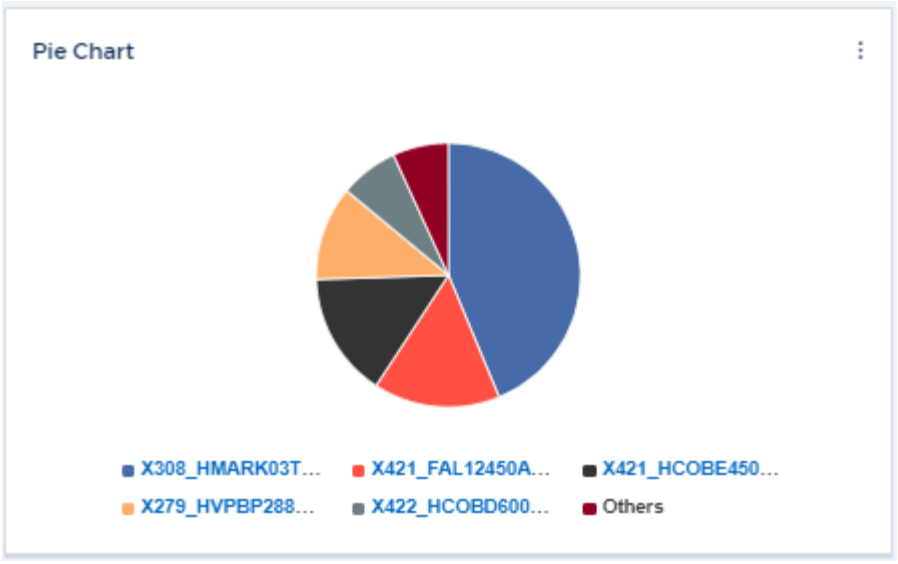
- * ボックスプロットグラフ * ： 1 つのグラフ内のデータの最小、最大、中央値、および下位四分位から上位四分位までの範囲のプロット。



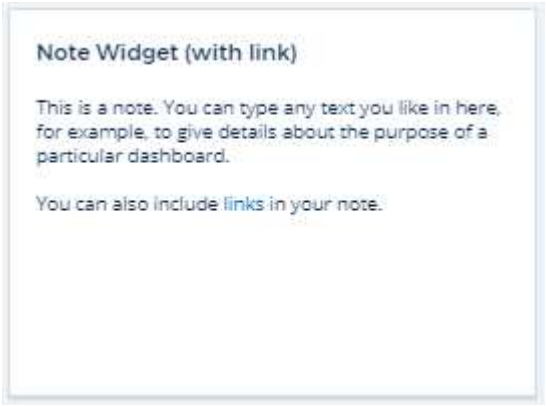
- * 散布図 * ：関連データを IOPS やレイテンシなどの点で出力します。この例では、スループットが高く IOPS が低いアセットをすばやく特定できます。



- * 円グラフ * ：データを全体の一部として表示するための従来の円グラフ。



- * メモウィジェット *: 最大 1000 文字のフリーテキスト。



- * アラート・テーブル * ：最新の 1 、 000 件のアラートを表示します。

これらの機能およびその他のダッシュボード機能の詳細については、 "ここをクリックしてください"。

ホームページとしてダッシュボードを設定する

環境の * ホームページ * として設定するダッシュボードは、次のいずれかの方法で選択できます。

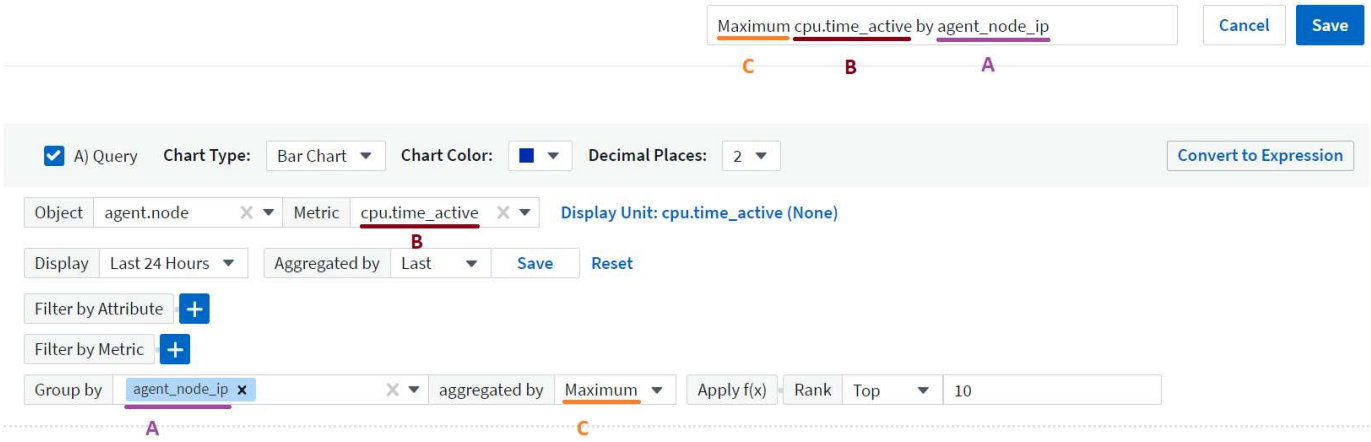
- [* Dashboards （ダッシュボード）] > [Show All Dashboards （すべてのダッシュボードを表示）] に移動して、環境内のダッシュボードのリストを表示します。目的のダッシュボードの右側にあるオプションメニューをクリックし、 * ホームページとして設定 * を選択します。
- リストからダッシュボードをクリックして、ダッシュボードを開きます。上部コーナーのドロップダウンメニューをクリックし、 * ホームページに設定 * を選択します。

ダッシュボードの機能

ダッシュボードとウィジェットでは、データの表示方法を柔軟に変更することができます。ここでは、カスタムダッシュボードを最大限に活用するのに役立つ概念をいくつか紹介します。

ウィジェットの命名

ウィジェットの名前は、最初のクエリで選択したオブジェクト、指標、または属性に基づいて自動的に付けられます。ウィジェットのグループ化も選択すると、「グループ化」属性が自動命名（集計方法とメトリック）に含まれます。



新しいオブジェクトまたはグループ化属性を選択すると、自動名称が更新されます。

自動ウィジェット名を使用しない場合は、単に新しい名前を入力します。

ウィジェットの配置とサイズ

ダッシュボードウィジェットは、それぞれのダッシュボードのニーズに応じて配置やサイジングを行うことができます。

ウィジェットの複製

ダッシュボード編集モードで、ウィジェットのメニューをクリックし、 * 複製 * を選択します。ウィジェットエディタが起動し、元のウィジェットの設定とウィジェット名に「 copy 」というサフィックスが付きます。必要な変更を簡単に加えて、新しいウィジェットを保存することができます。ウィジェットはダッシュボードの下部に配置され、必要に応じて配置することができます。すべての変更が完了したら、必ずダッシュボードを保存してください。

ウィジェット凡例を表示します

ダッシュボードのほとんどのウィジェットでは、凡例を表示または非表示にすることができます。ウィジェットの凡例の表示 / 非表示は、次のいずれかの方法で切り替えることができます。

- ダッシュボードを表示するときは、ウィジェットの * オプション * ボタンをクリックし、メニューから * 凡例を表示 * を選択します。

ウィジェットに表示されるデータが変わると、そのウィジェットの凡例が動的に更新されます。

凡例が表示されているときに、凡例が示すアセットのランディングページにアクセス可能な場合は、凡例がそのアセットページへのリンクとして表示されます。凡例に「すべて」と表示されている場合は、リンクをクリックすると、ウィジェットの最初のクエリに対応するクエリページが表示されます。

メトリックの変革

Data Infrastructure Insightsでは、ウィジェットの特定のメトリック(特に、Kubernetes、ONTAP Advanced Data、Telegrafプラグインなどの「カスタム」または統合メトリックと呼ばれるメトリック)にさまざまな* transform *オプションを提供しており、さまざまな方法でデータを表示できます。変換可能なメトリックをウィジェットに追加する場合は、ドロップダウンから次のトランスフォームの選択肢を選択できます。

なし
: データはそのまま表示され、操作は行われません。

レート
: 現在の値を前回の観察以降の時間範囲で割った値。

累計
: 前の値と現在の値の合計の累積値。

デルタ（ **Delta** ）
: 前回の観察値と現在の値の差。

デルタレート
: デルタ値を前回の観察からの時間範囲で割った値。

累積レート
: 累積値を前回の観察以降の時間範囲で割った値。

指標を変換しても、基盤となるデータ自体は変わりませんが、表示されるのはデータの表示方法だけです。

ダッシュボードウィジェットのクエリとフィルタ

クエリ

ダッシュボードウィジェットのクエリは、データ表示を管理するための強力なツールです。ここでは、ウィジェットのクエリに関する注意事項を示します。

一部のウィジェットでは、最大 5 つのクエリを設定できます。クエリごとに固有の折れ線などのグラフがウィジェットに出力されます。1 つのクエリに集計方法、グループ化、上位 / 下位などを設定しても、ウィジェットの他のクエリには影響しません。

目のアイコンをクリックすると、クエリが一時的に非表示になります。クエリの表示と非表示を切り替えると、ウィジェットに自動的に表示される情報が更新されます。これにより、ウィジェットの作成時に表示されるデータを個々のクエリで確認することができます。

次のタイプのウィジェットでは、複数のクエリを設定できます。

- 面グラフ
- 積み上げ面グラフ
- 折れ線グラフ
- スプライングラフ
- 単一値ウィジェット

残りのタイプのウィジェットでは、クエリを 1 つだけ設定できます。

- 表
- 棒グラフ
- ボックスプロット
- 散布図

ダッシュボードウィジェットのクエリでのフィルタリング

あなたのフィルターを最大限に活用するためにすることができるある事はここにある。

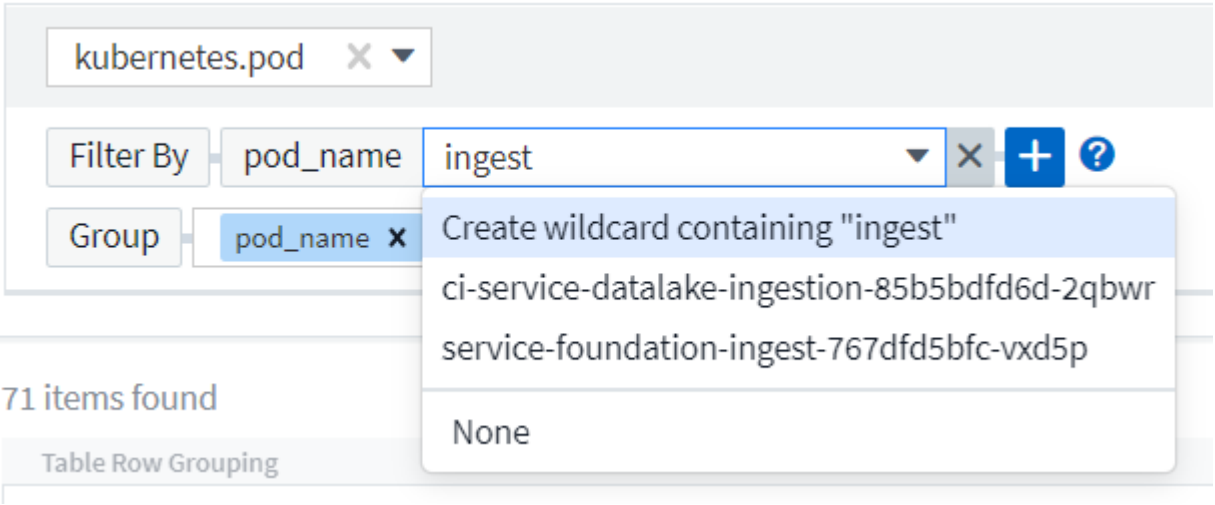
完全一致フィルタリング

フィルタ文字列を二重引用符で囲むと、 Insight では、最初と最後の引用符の間のすべての部分が完全に一致するものとして扱われます。引用符内の特殊文字または演算子は、リテラルとして扱われます。たとえば、「 * 」を指定した場合、リテラルアスタリスクである結果は返されますが、アスタリスクはワイルドカードとして扱われません。演算子 AND 、 OR 、および NOT は、二重引用符で囲まれた場合にもリテラル文字列として扱われます。

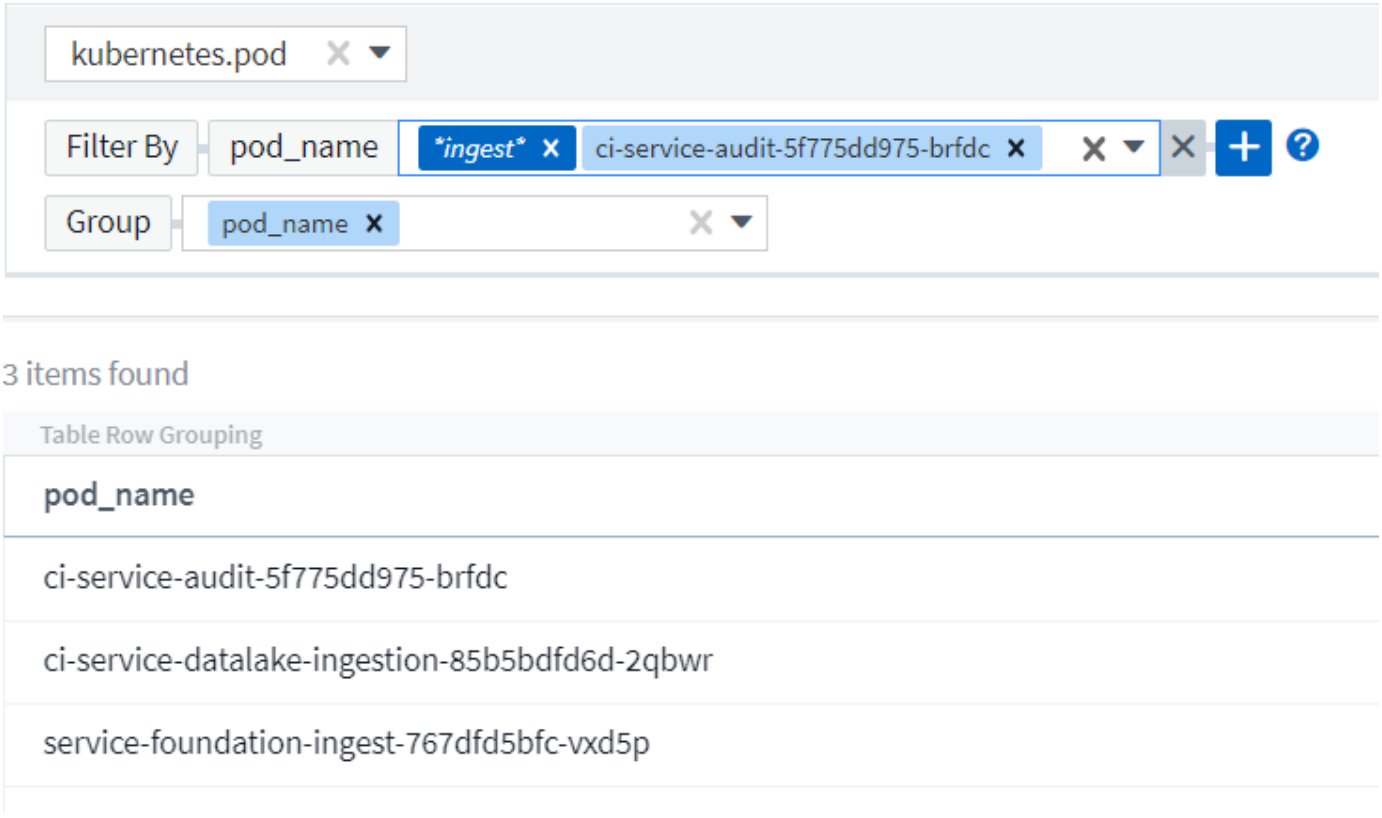
完全一致フィルタを使用して、ホスト名などの特定のリソースを検索できます。ホスト名「マーケティング」のみを検索し、「マーケティング 01 」、「マーケティングボストン」などを除外する場合は、名前「 marketing 」を二重引用符で囲みます。

ワイルドカードと式

クエリやダッシュボードウィジェットでテキストやリストの値をフィルタする場合、入力を開始すると、現在のテキストに基づいて * ワイルドカードフィルタ * を作成するオプションが表示されます。このオプションを選択すると、ワイルドカード式に一致するすべての結果が返されます。また、 NOT または OR を使用して *expressions * を作成することもできます。また、「 None 」オプションを選択して、フィールドで null 値をフィルタリングすることもできます。



ワイルドカードまたは式に基づくフィルタ（例 フィルタフィールドに濃い青で表示されます。リストから直接選択した項目は、水色で表示されます。



ワイルドカードおよび式フィルタリングは、テキストまたはリストでは機能しますが、数値、日付、またはブール値では機能しません。

コンテキストタイプアヘッド提案を使用した高度なテキストフィルタリング

ウィジェットクエリでのフィルタ処理は *contextual _* です。フィールドのフィルタ値または値を選択すると、そのクエリの他のフィルタには、そのフィルタに関連する値が表示されます。
たとえば ' 特定の *object_Name* にフィルタを設定した場合 '*Model* にフィルタを適用するフィールドには ' そのオブジェクト名に関連する値のみが表示されます

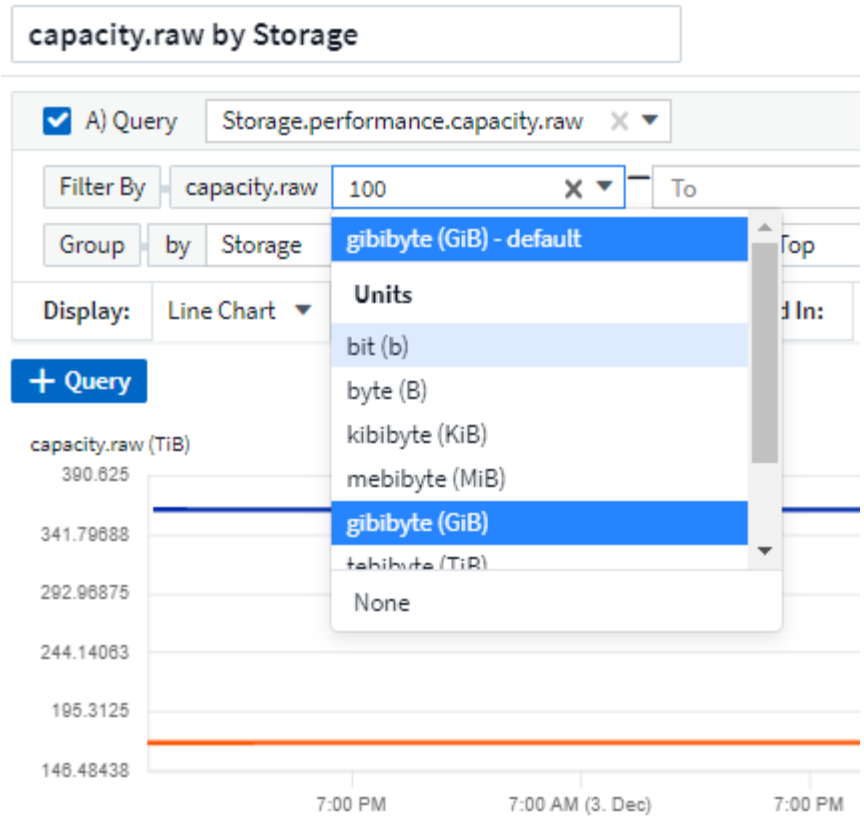
コンテキストフィルタリングでは、環境 ダッシュボードページの変数（テキストタイプの属性または注釈のみ）も使用できます。1 つの変数にファイラー値を選択すると、関連オブジェクトを使用する他のすべての変数には、それらの関連変数のコンテキストに基づいたフィルタ値のみが表示されます。

テキストフィルターのみがコンテキストに応じたタイプアヘッド候補を表示することに注意してください。日付、 Enum （ list ）などは先行入力候補を表示しません。つまり、列挙型フィールドにフィルタを設定し、他のテキストフィールドをコンテキストでフィルタリングすることができます。たとえば、データセンターなどの Enum フィールドの値を選択すると、他のフィルタにはそのデータセンターのモデル / 名前のみが表示されますが、逆の場合は表示されません。

選択した時間範囲には、フィルタに表示されたデータのコンテキストも表示されます。

フィルタの単位を選択します

フィルタフィールドに値を入力するときに、グラフに値を表示する単位を選択できます。たとえば、物理容量でフィルタして、 DEAFultGiB で表示するか、 TiB などの別の形式を選択できます。これは、ダッシュボードに TiB の値を示すグラフがいくつかあり、すべてのグラフで一貫した値を表示する場合に便利です。



その他のフィルタリングの詳細

フィルタをさらに絞り込むには、次のコマンドを使用します。

- アスタリスクを使用すると、すべての項目を検索できます。例：

```
vol*rhel
```

「 vol 」で始まり、「 rhel 」で終わるすべてのリソースを表示します。

- 疑問符を使用すると、特定の数の文字を検索できます。例：

```
BOS-PRD??-S12
```

BOS-PRD12-S12_,*BOS-PRD13-S12* などが表示されます。

- OR 演算子を使用すると、複数のエンティティを指定できます。例：

```
FAS2240 OR CX600 OR FAS3270
```

複数のストレージモデルを検出します。

- NOT 演算子を使用すると、検索結果からテキストを除外できます。例：

```
NOT EMC*
```

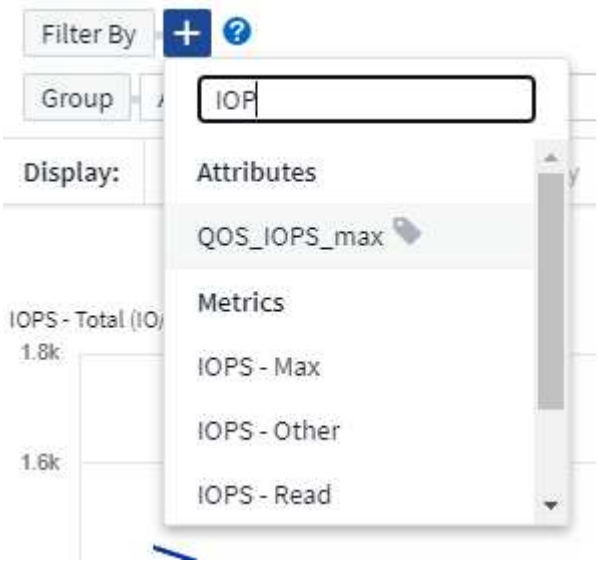
「 EMC 」で始まるものをすべて検索します。を使用できます

```
NOT *
```

値のないフィールドを表示します。

クエリとフィルタで返されるオブジェクトを特定する

クエリとフィルタで返されるオブジェクトは、次の図に示すようになります。「タグ」が割り当てられているオブジェクトはアノテーションであり、タグのないオブジェクトはパフォーマンスカウンタまたはオブジェクト属性です。



グループ化と集約

グループ化（ローリングアップ）

ウィジェットに表示されるデータは、取得中に収集されたデータポイントからグループ化（集計）されたものです。たとえば、ストレージ IOPS の経過を示す折れ線グラフでは、データセンターごとにグラフ線を表示してデータをすばやく比較できます。これらのデータをグループ化する方法はいくつかあります。

- * Average * ：収集されたデータの平均値の線を表示します。
- * 最大 * ：各行を基になるデータの *maximum* として表示します。
- * 最小 * ：各行を基になるデータの *minimum* として表示します。
- * 合計 * ：各行を基になるデータの *SUM*(合計) として表示します。
- * Count * ：指定した期間内にデータが報告されたオブジェクトの _count_of を表示します。ダッシュボードの時間範囲によって決定される_Entire Time Window_を選択できます。

手順

グループ化方法を設定するには、次の手順を実行します。

1. ウィジェットのクエリで、アセットのタイプと指標（ *Storage* など）と指標（ *Performance IOPS Total* など）を選択します。
2. **Group** の場合、集計方法（ *Average* など）を選択し、データを集計する属性またはメトリックを選択します（例： *Data Center* ）。

   ウィジェットが自動的に更新され、各データセンターのデータが表示されます。

また、基になるデータをグループ化してグラフや表にまとめることもできます。この場合は、ウィジェットのクエリごとに 1 つの線が表示されます。つまり、収集されたすべてのアセットについて、選択した指標または指標の平均、最小、最大、合計、または数が表示されます。

データが「すべて」でグループ化されているウィジェットの凡例をクリックすると、ウィジェットで使用されている最初のクエリの結果を示すクエリページが開きます。

クエリにフィルタを設定している場合は、フィルタされたデータに基づいてデータがグループ化されます。

ウィジェットを任意のフィールド（ *Model* など）でグループ化することを選択した場合でも、そのフィールドのデータをグラフまたは表に正しく表示するには、そのフィールドでフィルタ処理する必要があります。

データの集約

データポイントを分、時間、日などのバケットに集約して時系列のグラフ（行や領域など）をさらに調整し、そのデータを属性別（選択した場合）に集計することもできます。データポイントを、それぞれの平均、最大、最小、合計、またはカウント _ に従って集計することができます。

インターバルを長くすると、「集計間隔にはデータポイントが多すぎる」という警告が表示されることがあります。間隔が短い場合は、ダッシュボードの期間を 7 日に延長するとこのように表示されることがあります。この場合、選択する期間がより短いほど、集約間隔は一時的に長くなります。

棒グラフウィジェットおよび単一値ウィジェットでデータを集約することもできます。

ほとんどのアセットカウンタは、デフォルトでは *Average* に集計されます。一部のカウンタは、デフォルトで *Max* 、 *Min* 、または *Sum_By* に集計されます。たとえば、デフォルトでは、ポートエラーのアグリゲートは *_sum* になり、ストレージ *IOPS* のアグリゲートは *_Average* になります。

上 / 下の結果を表示しています

グラフウィジェットでは、集計されたデータの「上位」または「 * 下位」の結果を表示したり、表示される結果の数をドロップダウンリストから選択したりできます。表ウィジェットでは、任意の列でソートできます。

グラフウィジェットの上位 / 下位表示機能

グラフウィジェットでは、特定の属性でデータを集計することを選択すると、上位または下位の結果を表示することができます。ただし、 _All_attributes で集計することを選択した場合は、上位または下位の結果を選択することはできません。

表示する結果を選択するには、クエリの * Show * フィールドで * Top * または * Bottom * を選択し、表示されるリストから値を選択します。

表ウィジェットにエントリが表示されます

表ウィジェットでは、表に表示する結果の数を選択できます。表では、いずれかの列を基準に結果を昇順または降順でオンデマンドでソートすることができるため、上位または下位の結果を表示するオプションはありません。

クエリの * エントリの表示 * フィールドから値を選択すると、ダッシュボードのテーブルに表示する結果の数を選択できます。

表ウィジェットでのグループ化

表ウィジェット内のデータは使用可能な属性別にグループ化できるため、データの概要だけでなく、データの詳細も確認できます。表内の指標が集計され、各行を折りたためば全体のデータが見やすくなります。

表ウィジェットでは、設定した属性に基づいてデータをグループ化できます。たとえば、ストレージ IOPS の合計を、それらのストレージが配置されているデータセンター別にグループ化できます。また、仮想マシンをホストしているハイパーバイザー別にグループ化して表示することもできます。リストで各グループを展開すると、そのグループのアセットが表示されます。

グループ化は表ウィジェットタイプでのみ使用できます。

グループ化の例（集計の説明を含む）

表ウィジェットでは、データをグループ化して見やすくすることができます。

この例では、すべての VM をデータセンター別にグループ化して表示する表を作成します。

手順

1. ダッシュボードを作成または開き、 * 表 * ウィジェットを追加します。
2. このウィジェットのアセットタイプとして、 [Virtual Machine_] を選択します。
3. 列 Selector をクリックし、 *Hypervisor name_or_IOPS-Total* を選択します。

   表にこれらの列が表示されます。

4. IOPS がない VM は無視し、合計 IOPS が 1 を超える VM だけを表示するように設定します。[* Filter by * [+] *] ボタンをクリックして、 [*IOPS- Total _]* を選択します。*[on_any*] をクリックし、 [* 開始日] フィールドに * 1 * と入力します。[* から *] フィールドは空のままにします。Enter キーを押し、フィルタフィールドをクリックしてフィルタを適用します。

   これで、合計 IOPS が 1 以上の VM がすべて表示されます。この表にはグループ化はありません。すべての VM が表示されている。

5. [+]* でグループ化ボタンをクリックします。

   表示されている任意の属性またはアノテーションでグループ化できます。1 つのグループ内のすべての VM を表示するには、 *ALL* を選択します。

   パフォーマンス指標の列ヘッダーには、「 3 ドット」メニューが表示されます。このメニューには「 * 集計」オプションが含まれています。デフォルトの集計方法は *Average* です。つまり、このグループに表示されている数値は、グループ内の各 VM の合計 IOPS の平均値です。この列を平均 (*Average)* 、合計 *(Sum)* 、最小 *(Minimum)* 、または最大 *(Maximum_Maximum*) で集計することを選択できます。表示された列のうち、パフォーマンス指標を含むものはいずれも、個別に集計できます。

6. [*all*] をクリックし、 [_Hypervisor name _] を選択します。

   VM のリストがハイパーバイザーでグループ化されます。各ハイパーバイザーを展開すると、そのハイパーバイザーがホストしている VM を表示できます。

7. [保存（ Save ）] をクリックして、テーブルをダッシュボードに保存します。ウィジェットは必要に応じてサイズ変更または移動できます。
8. 保存 * をクリックしてダッシュボードを保存します。

パフォーマンスデータの集計

表ウィジェットにパフォーマンスデータの列（ *iops-Total* など）を含める場合は、データのグループ化を選択する際に、その列の集計方法を選択できます。デフォルトの集計方法では、グループ行の基になるデータの平均（ *avg*） が表示されます。データの合計値、最小値、最大値を表示することもできます。

ダッシュボードの時間範囲セレクタ

ダッシュボードデータの期間を選択できます。ダッシュボードのウィジェットには、選択した期間に関連するデータのみが表示されます。 次の期間を選択できます。

- 最後の 15 分
- 過去 30 分
- 最後の60分
- 過去2時間
- 過去 3 時間（デフォルト）
- 過去6時間
- 過去12時間
- 過去 24 時間
- 過去2日間

- 過去 3 日間
- 過去7日間
- 過去30日間
- カスタムの期間

  カスタム期間では、最大 31 日間連続で選択できます。この範囲に開始時間と終了時間を設定することもできます。デフォルトの開始時間は、最初に選択した日の午前 12 時、最後に選択した日のデフォルトの終了時間は午後 11 時 59 分です。* 適用 * をクリックすると、カスタムの時間範囲がダッシュボードに適用されます。

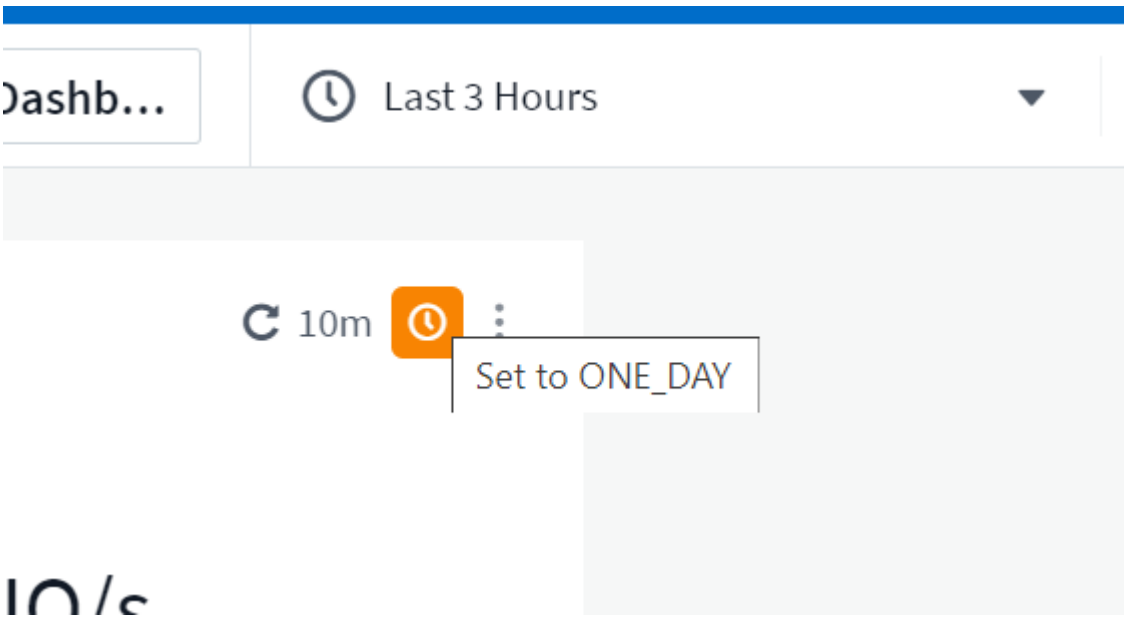
ウィジェットでのダッシュボード時間の無効化

メインのダッシュボードの期間設定をウィジェットごとに無効にすることができます。これらのウィジェットでは、ダッシュボードの期間ではなく、各ウィジェットに対して設定された期間に基づいてデータが表示されます。

ダッシュボードの時間を上書きしてウィジェットで独自の期間を使用するには、ウィジェットの編集モードで期間を選択し、ウィジェットをダッシュボードに保存します。

ウィジェットには、ダッシュボードで選択した期間に関係なく、ウィジェットに対して設定された期間に従ってデータが表示されます。

ウィジェットに対して設定した期間は、ダッシュボード上の他のウィジェットには影響しません。



第 **1** 軸と第 **2** 軸

グラフに表示されるデータには、指標ごとに使用する測定単位が異なります。たとえば、 IOPS の測定単位は 1 秒あたりの I/O 処理数（ IO/s ）であるのに対し、レイテンシは単純に時間（ミリ秒、マイクロ秒、秒など）で測定されます。これらの両方の指標を、 Y 軸で 1 つの値セットを示す 1 つの折れ線グラフに出力すると、レイテンシの数値（通常は数ミリ秒単位）が IOPS （通常は数千単位）と同じ目盛りで表示されるため、レイテンシの線が見えなくなります。

ただし、一次（左側）の Y 軸に測定単位を 1 つ設定し、二次（右側）の Y 軸にもう一方の測定単位を設定することで、両方のデータセットをわかりやすい 1 つのグラフにまとめることができます。これで、個々の指標がそれぞれの目盛りで出力されます。

手順

この例では、グラフウィジェットでの主軸と第 2 軸の概念を示します。

1. ダッシュボードを作成するか、開きます。折れ線グラフ、スプライングラフ、面グラフ、または積み上げ面グラフウィジェットをダッシュボードに追加します。
2. アセットのタイプ（例： *Storage* ）を選択し、最初の指標の *iops-Total* を選択します。必要なフィルタを設定し、必要に応じて集計方法を選択します。

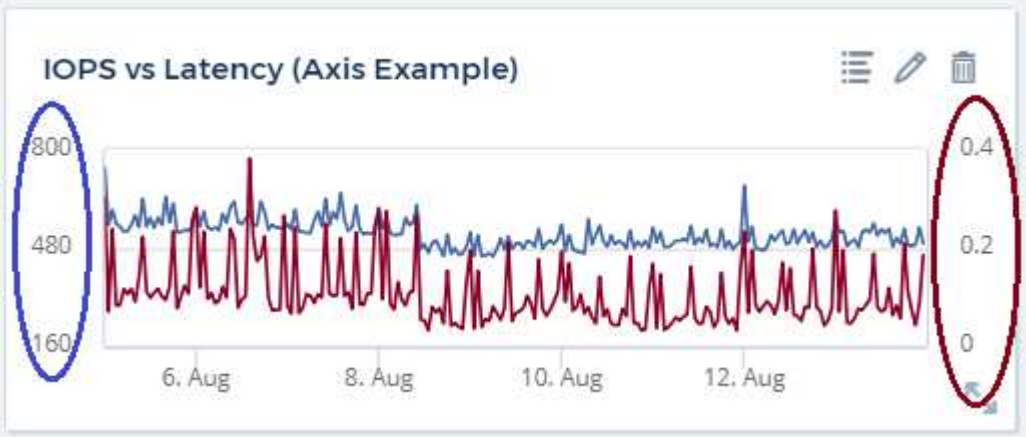
   折れ線グラフに IOPS の線が出力され、左側に目盛りが表示されます。

3. グラフに 2 行目を追加するには、 [+ クエリ] をクリックします。この行では、メトリックの _Latency - Total _ を選択します。

   グラフの下部にこの線が表示されます。これは、 IOPS の線と同じ目盛りで _ 描かれているためです。

4. レイテンシクエリで、 * Y 軸：セカンダリ * を選択します。

   これで Latency の線が Latency 用の目盛りでグラフの右側に表示されます。



ウィジェットの式

ダッシュボードでは、時系列ウィジェット（折れ線、スプライン、面、積み上げ面）の棒グラフ、棒グラフ、円グラフ、または表ウィジェットを使用して、選択した指標から式を作成し、それらの式の結果を単一のグラフ（ 表ウィジェット）。次の例では、式を使用して特定の問題を解決します。最初の例は、環境内のすべてのストレージアセットの合計 IOPS に占める読み取り IOPS の割合を表示するウィジェットです。2 つ目の例では、環境内で発生した「システム」または「オーバーヘッド」の IOPS を可視化しています。これらの IOPS は、データの読み取りや書き込みから直接ではありません。

式で変数を使用できます（例： *$var1 * 100* ）。

式の例：読み取り **IOPS** の割合

この例では、合計 IOPS に占める読み取り IOPS の割合をウィジェットに表示します。これは次の式と考えることができます。

```
Read Percentage = (Read IOPS / Total IOPS) x 100
```
このデータは、ダッシュボードに折れ線グラフで表示できます。これを行うには、次の手順を実行します。

手順

1. 新しいダッシュボードを作成するか、既存のダッシュボードを編集モードで開きます。
2. ダッシュボードにウィジェットを追加します。[* Area chart* （エリアグラフ * ）] を

   ウィジェットが編集モードで開きます。デフォルトでは、クエリは _IOPS-Total_For _Storage_Assets を表示します。必要に応じて、別のアセットタイプを選択します。

3. 右側の [式に変換] リンクをクリックします。

   現在のクエリが式モードに変換されます。式モードのときはアセットタイプを変更できません。式モードでは、リンクが * クエリに戻る * に変わります。いつでもクエリモードに切り替えるには、このボタンをクリックします。モードを切り替えるとフィールドがデフォルトにリセットされるので注意してください。

   ここでは、式モードのままにします。

4. IOPS - 合計 * 指標がアルファベット変数フィールド「 * A * 」に追加されました。「 * b * 」変数フィールドで * Select * をクリックし、 * iops-Read * を選択します。

   変数フィールドの後にある [+] ボタンをクリックすると、式に合計 5 つまでの英字変数を追加できます。IOPS 読み取りの割合の計算に必要なのは、合計 IOPS （「 * a * 」）と読み取り IOPS （「 * b * 」）のみです。

5. [**Expression**] フィールドでは、各変数に対応する文字を使用して式を作成します。読み取り IOPS の割合 = （読み取り IOPS / 合計 IOPS ） x 100 であることがわかっているので、次のように式を書きます。

   ```
   (b / a) * 100
   ```
   . *Label* フィールドは、式を識別します。ラベルを「 Read Percentage 」に変更するか、同様のわかりやすいものにします。
   . [単位 *] フィールドを "%" または "percent" に変更します。

   グラフに、選択したストレージデバイスの読み取り IOPS の割合が時系列で表示されます。必要に応じて、フィルタを設定するか、別の集計方法を選択できます。集計方法として [合計] を選択すると、すべてのパーセント値が一緒に追加され、 100% を超える可能性があることに注意してください。

6. グラフをダッシュボードに保存するには、 * 保存 * をクリックします。

式の例：システム **I/O**

例 2 ：データソースから収集した指標の中には、読み取り IOPS 、書き込み IOPS 、合計 IOPS があります。ただし、データソースで報告される IOPS の合計数には、「システム」 IOPS が含まれていることがあります。これらは、データの読み取りや書き込みとは直接関係のない I/O 処理です。このシステム I/O はオーバーヘッド I/O と考えることもできますが、適切なシステム運用には必要ですが、データの運用には直接関係しているわけではありません。

これらのシステム I/O を表示するには、収集によって報告された合計 IOPS から読み取り IOPS と書き込み IOPS を差し引きます。式は次のようになります。

```
System IOPS = Total IOPS - (Read IOPS + Write IOPS)
```

このデータは、ダッシュボードに折れ線グラフで表示できます。これを行うには、次の手順を実行します。

手順

1. 新しいダッシュボードを作成するか、既存のダッシュボードを編集モードで開きます。
2. ダッシュボードにウィジェットを追加します。「 * 線グラフ * 」を選択します。

   ウィジェットが編集モードで開きます。デフォルトでは、クエリは _IOPS-Total_For _Storage_Assets を表示します。必要に応じて、別のアセットタイプを選択します。

3. [集計] フィールドで、 [合計] を [すべて] で選択します。

   合計 IOPS の合計が線で表示されます。

4. [*Duplicate this Query*]アイコンをクリックして、クエリのコピーを作成します。

   重複するクエリが元のクエリの下に追加されます。

5. 2 番目のクエリで、 * 式に変換 * ボタンをクリックします。

   現在のクエリが式モードに変換されます。いつでもクエリモードに切り替えるには、 [クエリに戻る] をクリックします。モードを切り替えるとフィールドがデフォルトにリセットされるので注意してください。

   ここでは、式モードのままにします。

6. これで、 *iops-Total_metric* はアルファベット変数フィールド「 *A * 」に追加されました。*[_IOPS] - [Total*] をクリックして、 [*IOPS-Read*] に変更します。
7. 「 * b * 」変数フィールドで、 * Select * をクリックし、 *iops-Write*. を選択します。
8. [**Expression**] フィールドでは、各変数に対応する文字を使用して式を作成します。ここでは、単純に次のように式を記述します。

   ```
   a + b
   ```

   [表示] セクションで、この式の [グラフの領域 *] を選択します。

9. **Label** フィールドは、式を識別します。ラベルを「 System IOPS 」に変更するか、同様のわかりやすいものにします。

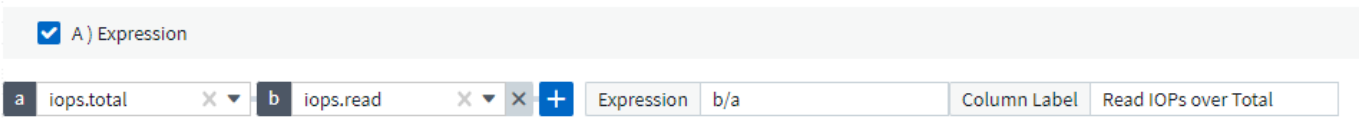
   合計 IOPS の折れ線グラフが表示され、その下に読み取り IOPS と書き込み IOPS を組み合わせた面グラフが表示されます。この 2 つのグラフの間が、データの読み取り処理や書き込み処理に直接関係していない IOPS を表します。これらはシステムの IOPS です。

10. グラフをダッシュボードに保存するには、 * 保存 * をクリックします。

式で変数を使用するには、変数名（例： *$var1 * 100* ）を入力します。式で使用できるのは数値変数のみです。

表ウィジェットの式

表ウィジェットでは、式の処理方法が少し異なります。1つの表ウィジェットに最大5つの式を設定でき、それぞれが新しい列として表に追加されます。各式には、計算を実行するための最大5つの値を含めることができます。列に意味のある名前を簡単に付けることができます。



変数（ **variables** ）

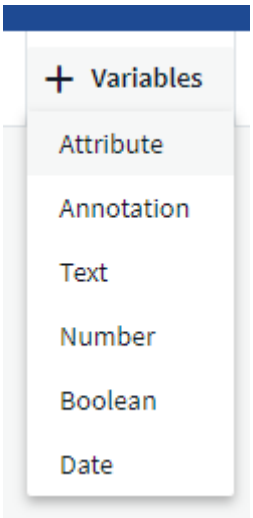
変数を使用すると、ダッシュボードの一部またはすべてのウィジェットに表示するデータを一度に変更できます。1 つ以上原因のウィジェットで共通の変数を使用するように設定すると、 1 箇所で変更を加え、各ウィジェットに表示されるデータが自動的に更新されます。

ダッシュボードの変数にはいくつかの種類があり、さまざまなフィールドで使用できます。また、命名規則もあります。ここでは、これらの概念について説明します。

変数の型

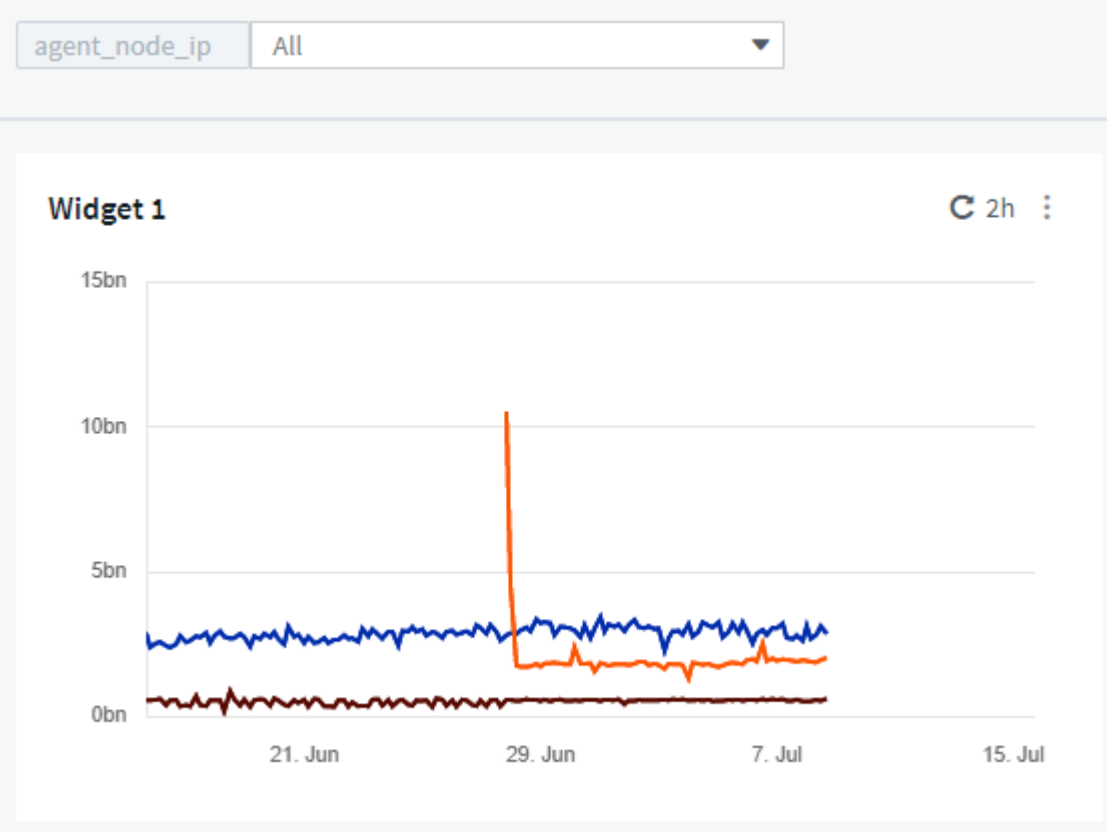
変数には、次のタイプがあります。

- * 属性 * ：オブジェクトの属性またはメトリックを使用してフィルタリングします
- * 注釈 * ：事前定義されたを使用します "アノテーション" ウィジェットデータをフィルタリングします。
- * Text * ：英数字の文字列。
- * 数値 * ：数値。ウィジェットフィールドに応じて、単独で使用することも、「 From 」または「 To 」値として使用することもできます。
- * Boolean * ： True / False 、 Yes / No などの値を持つフィールドに使用します。ブール変数の場合、選択肢は Yes 、 No 、 None 、 Any です。
- * 日付 *: 日付値。ウィジェットの構成に応じて、「 From 」または「 To 」の値として使用します。

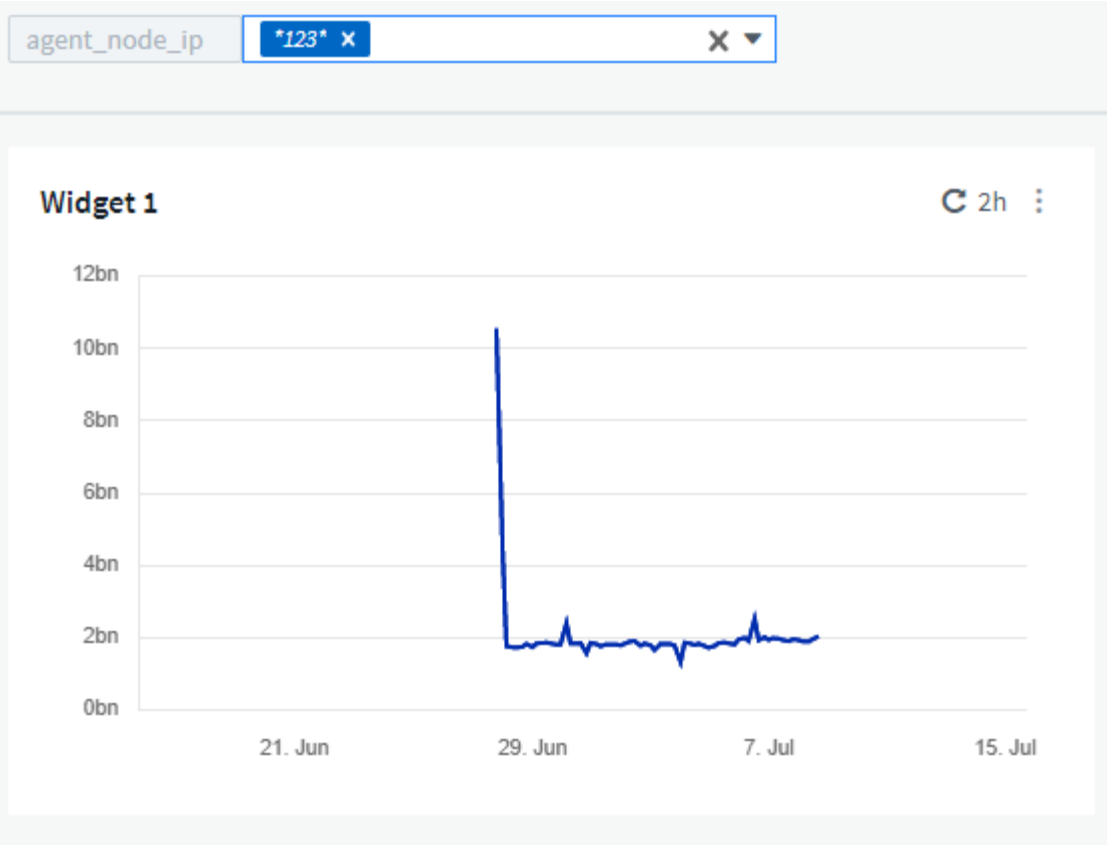


属性変数

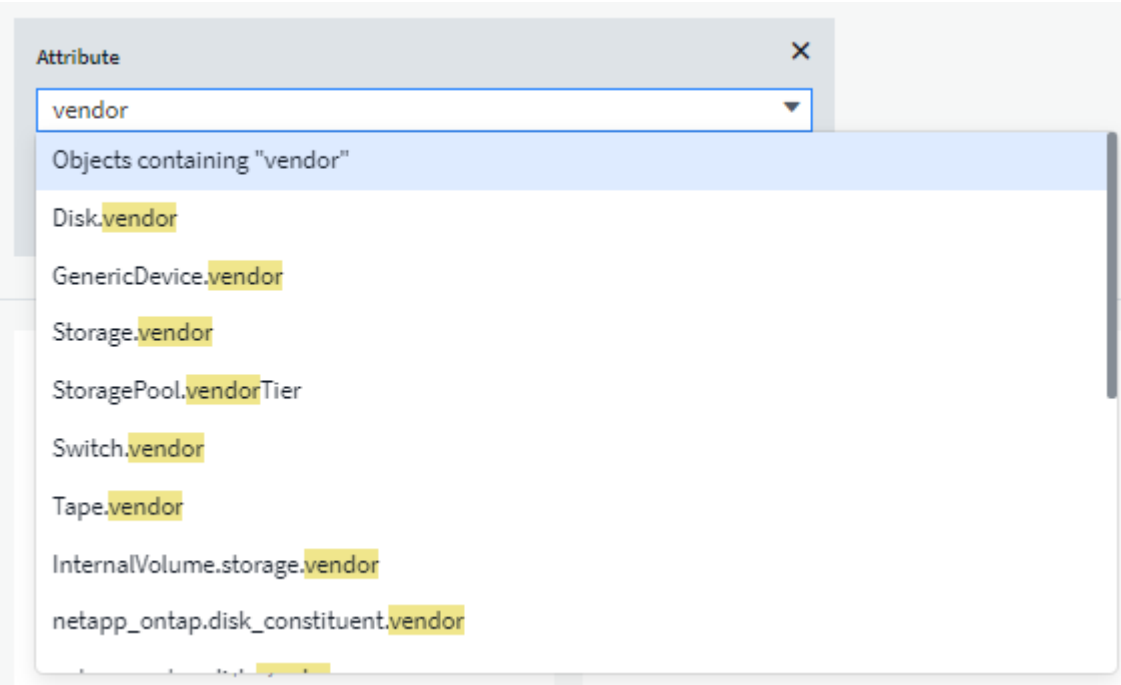
属性タイプ変数を選択すると、指定した属性値を含むウィジェットデータをフィルタできます。次の例は、エージェントノードの空きメモリの傾向を表示する折れ線ウィジェットを示しています。エージェントノード IP の変数を作成しました。現在、すべての IP を表示するように設定されています。



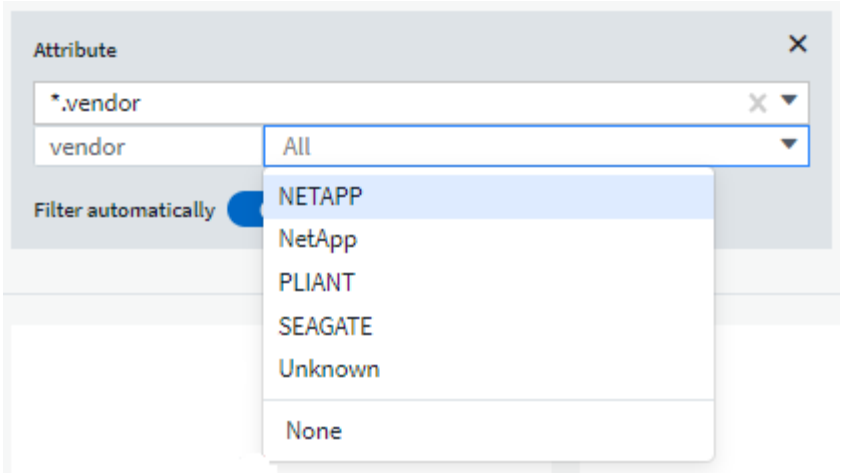
ただし、環境内の個々のサブネット上のノードだけを一時的に表示する場合は、その変数を特定のエージェントノード IP または IP に設定または変更できます。ここでは、「 123 」サブネット上のノードのみを表示しています。



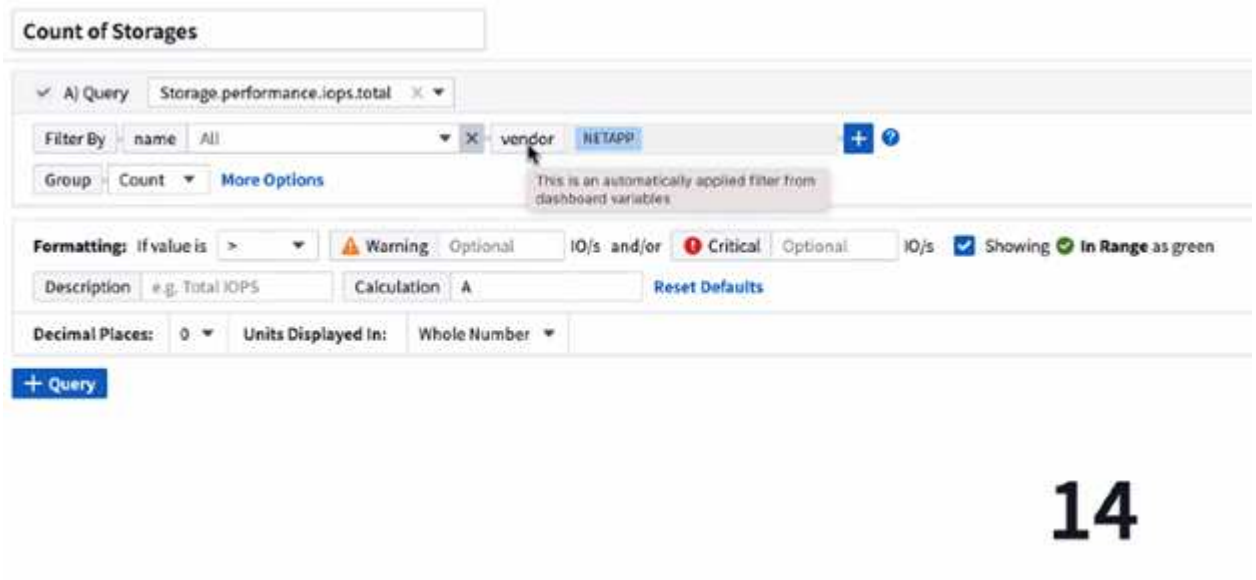
また、変数フィールドに「 vendor」 という属性を指定することにより、オブジェクトタイプに関係なく特定の属性で _all_objects をフィルタリングするように変数を設定することもできます。「*。」を入力する必要はありません。ワイルドカードオプションを選択した場合、Data Infrastructure Insightsが指定します。



変数値の選択肢のリストをドロップダウンすると、その結果がフィルタリングされ、ダッシュボード上のオブジェクトに基づいて使用可能なベンダーのみが表示されます。



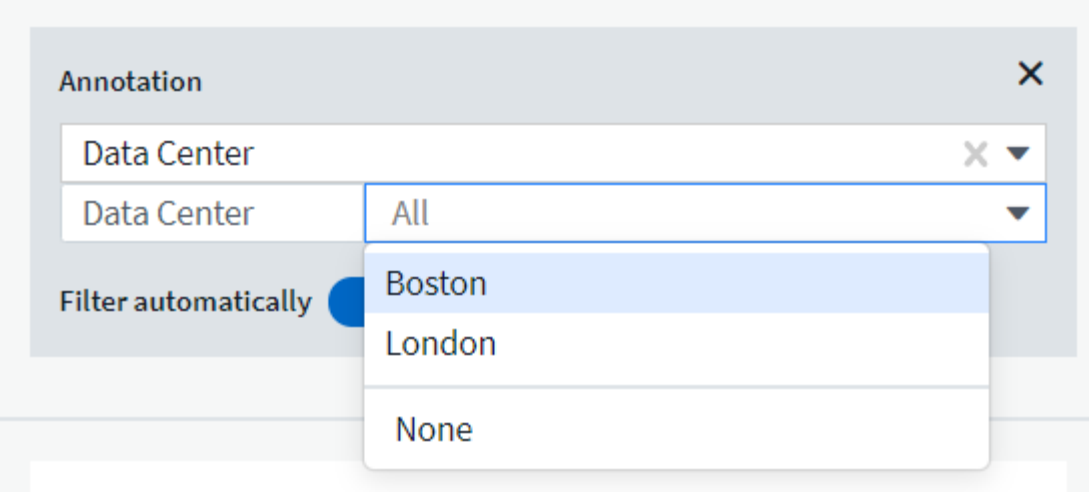
属性フィルタが関連するダッシュボードでウィジェットを編集すると（つまり、ウィジェットのオブジェクトに _*.vendor 属性 _ が含まれている）、属性フィルタが自動的に適用されていることがわかります。



変数の適用は、選択した属性データを変更するだけで簡単です。

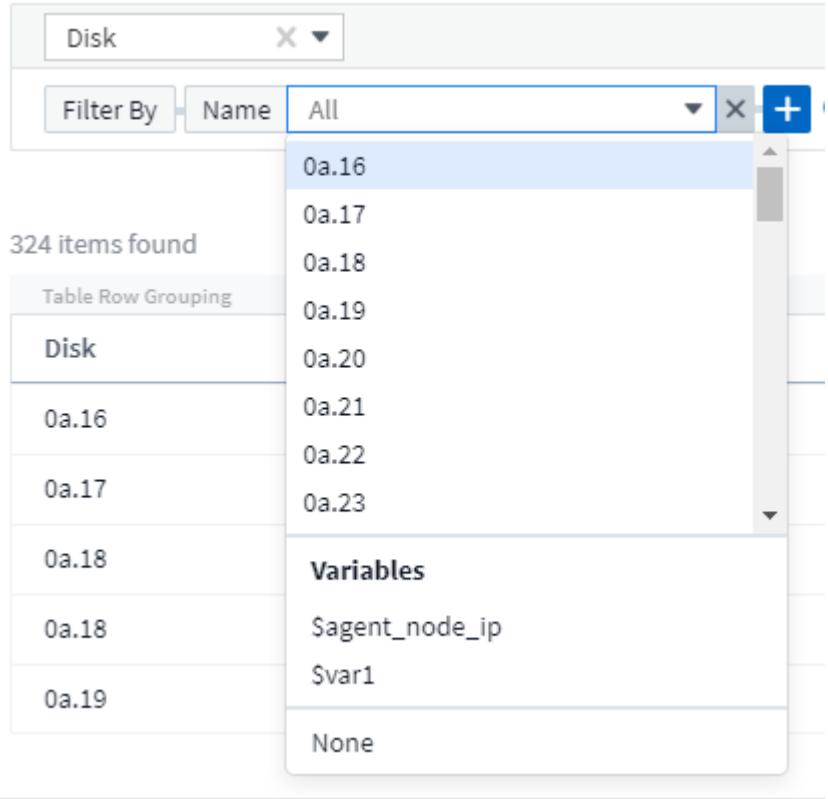
アノテーション変数

アノテーション変数を選択すると、そのアノテーションに関連付けられているオブジェクト（同じデータセンターに属するオブジェクトなど）をフィルタできます。



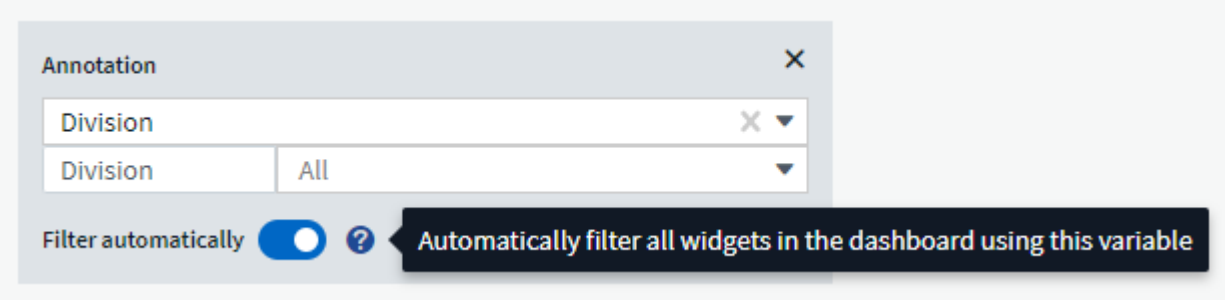
テキスト、数値、日付、またはブール変数

特定の属性に関連付けられていない汎用変数を作成するには、 *Text* 、 *Number* 、 *Boolean* 、または *Date_* の変数タイプを選択します。作成した変数は、ウィジェットフィルタフィールドで選択できます。ウィジェットでフィルタを設定する場合、フィルタに選択できる特定の値に加えて、ダッシュボード用に作成されたすべての変数がリストに表示されます。これらは、ドロップダウンの「変数」セクションの下にグループ化され、名前は「 $ 」で始まります。このフィルタで変数を選択すると、ダッシュボードの変数フィールドに入力した値を検索できます。フィルタでその変数を使用するウィジェットはすべて動的に更新されます。



変数フィルタスコープ（ **Variable Filter Scope** ）

アノテーション変数または属性変数をダッシュボードに追加すると、ダッシュボードの _ALL_widgets に変数を適用できるため、ダッシュボードのすべてのウィジェットで、変数に設定した値に基づいてフィルタされた結果が表示されます。



このように自動的にフィルタ処理できるのは属性変数とアノテーション変数だけです。Annotation または -Attribute 以外の変数は ' 自動的にフィルタできません個々のウィジェットで、これらのタイプの変数を使用するように設定する必要があります。

自動フィルタを無効にして、変数でウィジェットを設定したウィジェットのみを環境にするには、 [自動的にフィルタ] スライダをクリックして無効にします。

個々のウィジェットで変数を設定するには、ウィジェットを編集モードで開き、 _Filter by_field で特定のアノテーションまたは属性を選択します。アノテーション変数では、特定の値を 1 つ以上選択するか、変数名（先頭の「 $ 」で示されます）を選択することで、ダッシュボードレベルで変数を入力できます。同じ環境属性変数変数を設定したウィジェットでのみ、フィルタされた結果が表示されます。

変数でのフィルタ処理は _contextual _ です。変数のフィルタ値または値を選択すると、ページ上の他の変数には、そのフィルタに関連する値のみが表示されます。
たとえば、変数フィルタを特定のストレージモデルに設定すると、 Storage _Name _ でフィルタするように設定された変数には、そのモデルに関連する値のみが表示されます。

式で変数を使用するには、式の一部として変数名を入力します。たとえば、 *$var1 * 100* と入力します。式で使用できるのは数値変数のみです。式では、数値アノテーション変数または属性変数は使用できません。

変数でのフィルタ処理は _contextual _ です。変数のフィルタ値または値を選択すると、ページ上の他の変数には、そのフィルタに関連する値のみが表示されます。
たとえば、変数フィルタを特定のストレージモデルに設定すると、 Storage _Name _ でフィルタするように設定された変数には、そのモデルに関連する値のみが表示されます。

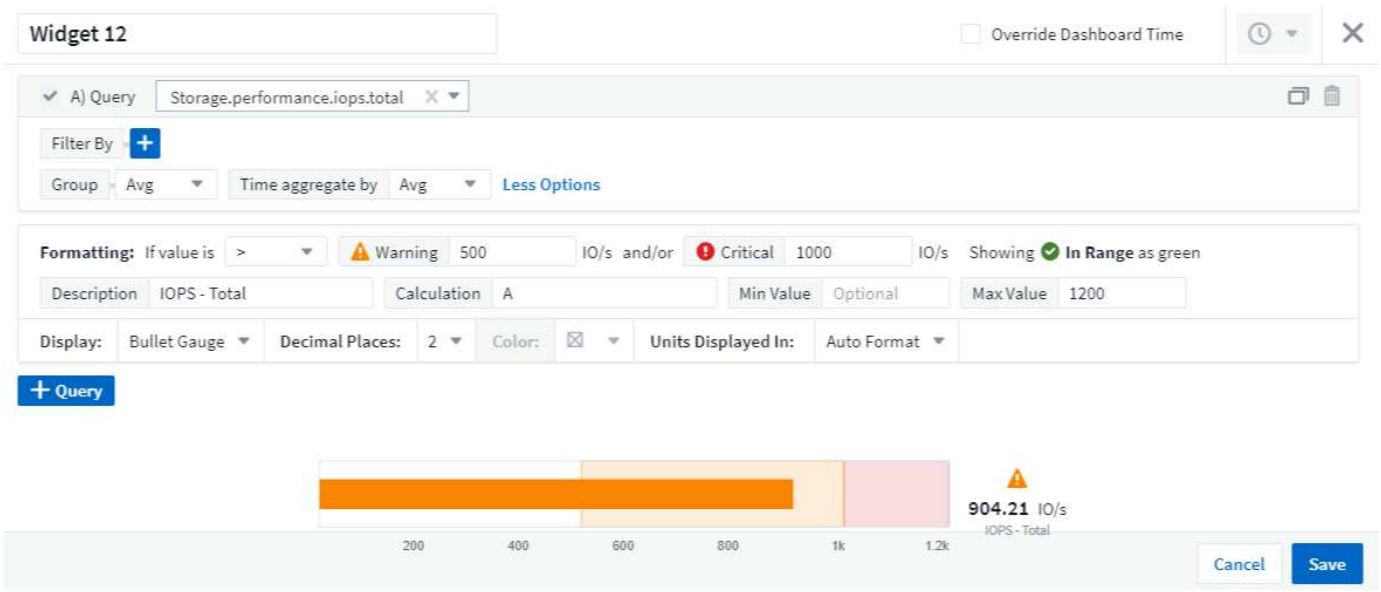
変数の命名規則

変数名：

- a~z 、 0~9 の数字、ピリオド（ . ）、アンダースコア（ _ ）、およびスペース（ . ）のみを使用してください。
- 20 文字以下にする必要があります。
- 大文字と小文字が区別されます。 $CityName と $cityname は変数によって異なります。
- 既存の変数名と同じにすることはできません。
- 空にすることはできません。

ゲージウィジェットの書式設定

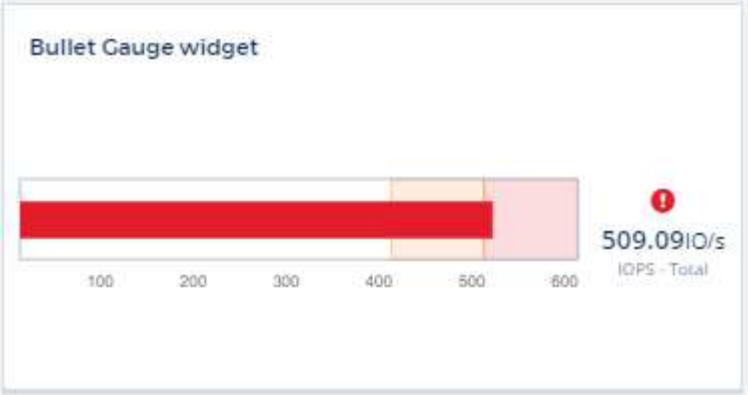
固体および箇条書きウィジェットでは、 *Warning* および / または _Critical_Levels のしきい値を設定し、指定したデータを明確に表現できます。



これらのウィジェットに書式を設定するには、次の手順を実行します。

1. しきい値より大きい（>）値と小さい（<）値のどちらを強調表示するかを選択します。この例では、しきい値レベル（ > ）より大きい値を強調表示します。
2. 「警告」しきい値の値を選択します。このレベルより大きい値がウィジェットに表示される場合は、ゲージがオレンジで表示されます。
3. 「クリティカル」しきい値の値を選択します。このレベルより大きい値原因を指定すると、ゲージが赤で表示されます。

必要に応じて、ゲージの最小値と最大値を選択できます。最小値を下回る値はゲージを表示しません。最大値を超えると、フルゲージが表示されます。最小値または最大値を選択しない場合は、ウィジェットの値に基づいて最適な最小値と最大値が選択されます。



単一値ウィジェットのフォーマット

単一値ウィジェットでは、警告（オレンジ）しきい値と重大（赤）しきい値の設定に加えて、「範囲内」（警告レベル未満）の値を緑または白の背景で表示するように選択できます。

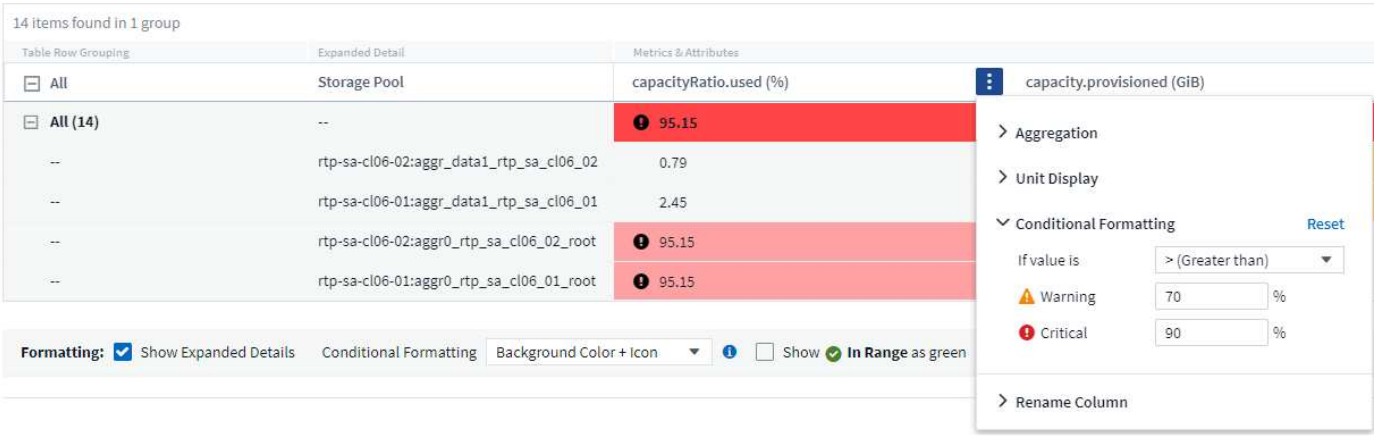
単一値ウィジェットまたはゲージウィジェットのリンクをクリックすると、ウィジェットの最初のクエリに対応するクエリページが表示されます。

表ウィジェットの書式設定

単一値ウィジェットやゲージウィジェットと同様に、表ウィジェットで条件付き書式を設定し、色や特殊アイコンでデータを強調表示することができます。

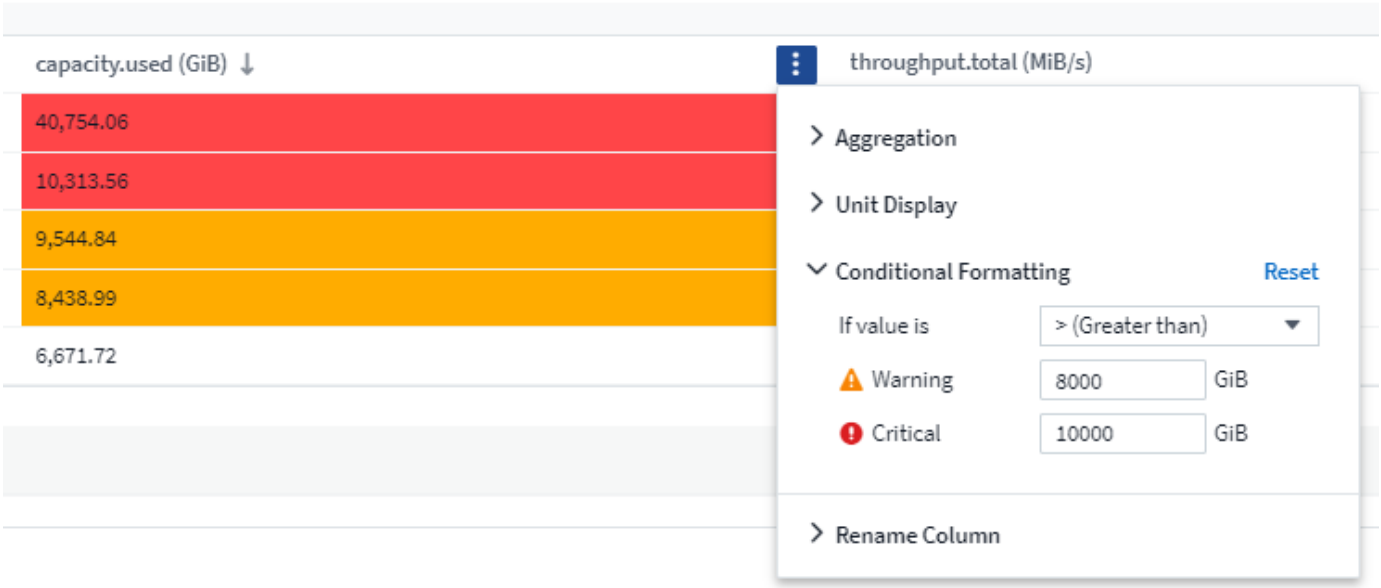
条件付き書式は、現在Data Infrastructure Insights Federal Editionでは使用できません。

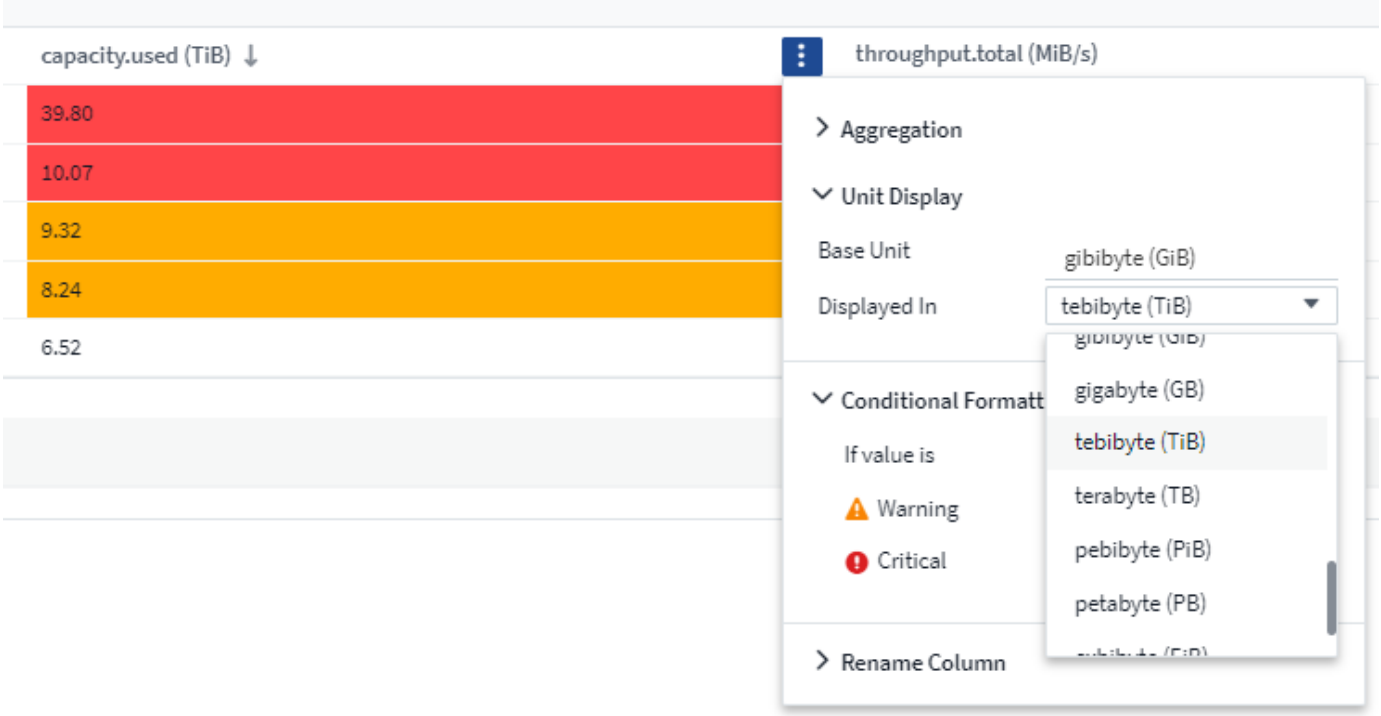
条件付き書式を使用すると、表ウィジェットで警告レベルと重大レベルのしきい値を設定して強調表示し、異常なデータポイントを瞬時に可視化できます。



条件付き書式は、表の各列に個別に設定されます。たとえば、容量列ではしきい値のセットを選択し、スループット列ではしきい値のセットを選択できます。

列の単位表示を変更しても、条件付き書式は維持され、値の変更が反映されます。以下の画像は、表示単位が異なる場合でも同じ条件付き書式を示しています。



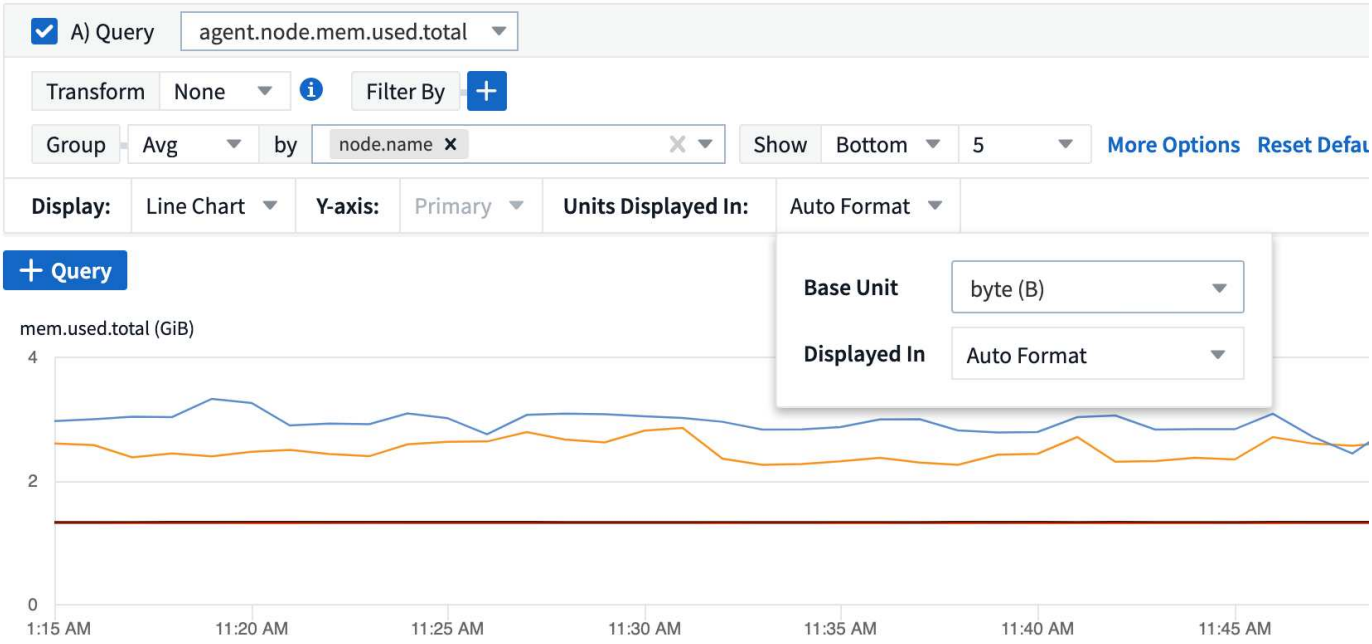


条件の書式を色、アイコン、またはその両方で表示するかどうかを選択できます。

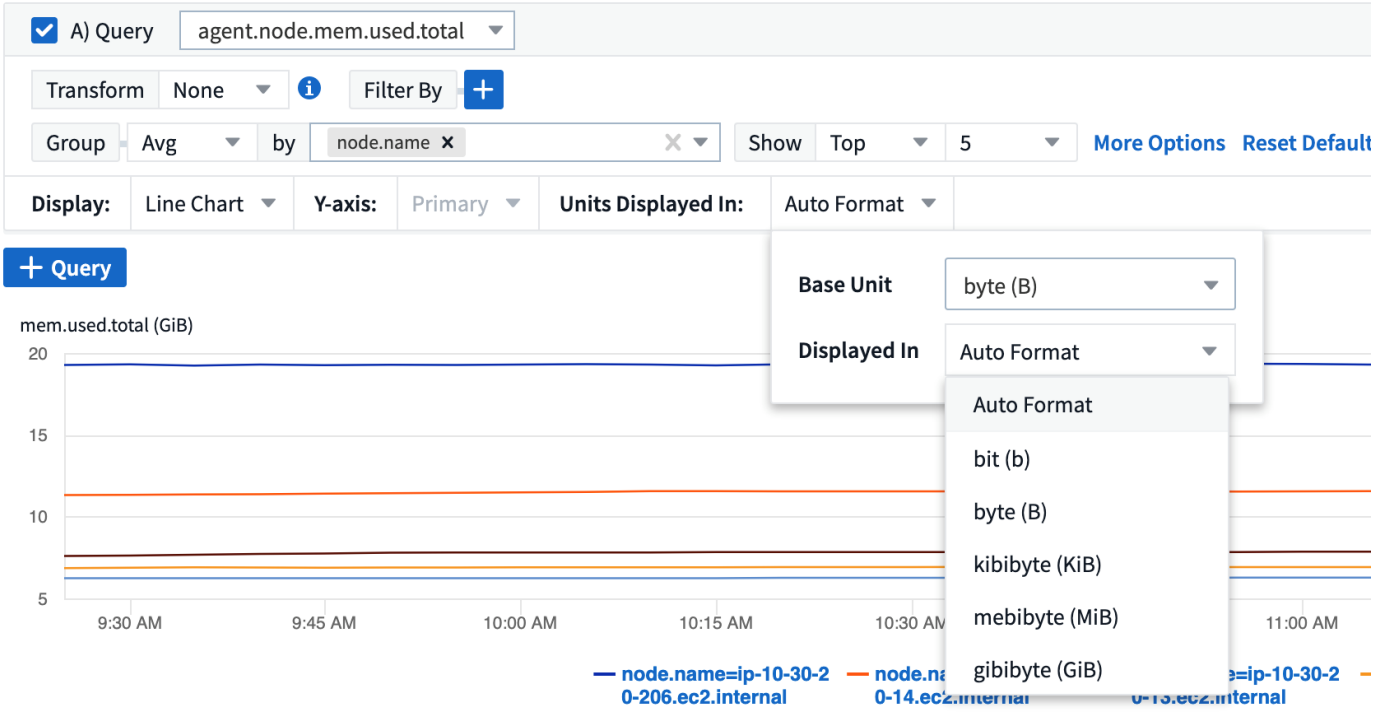
データ表示の単位を選択します

ダッシュボードのほとんどのウィジェットでは、値を表示する単位を指定できます。たとえば、*megabytes*、*thousands*、*percentage*、_milliseconds（ms）_などです。多くの場合、Data Infrastructure Insightsは取得するデータに最適な形式を認識しています。最適な形式がわからない場合は、目的の形式を設定できます。

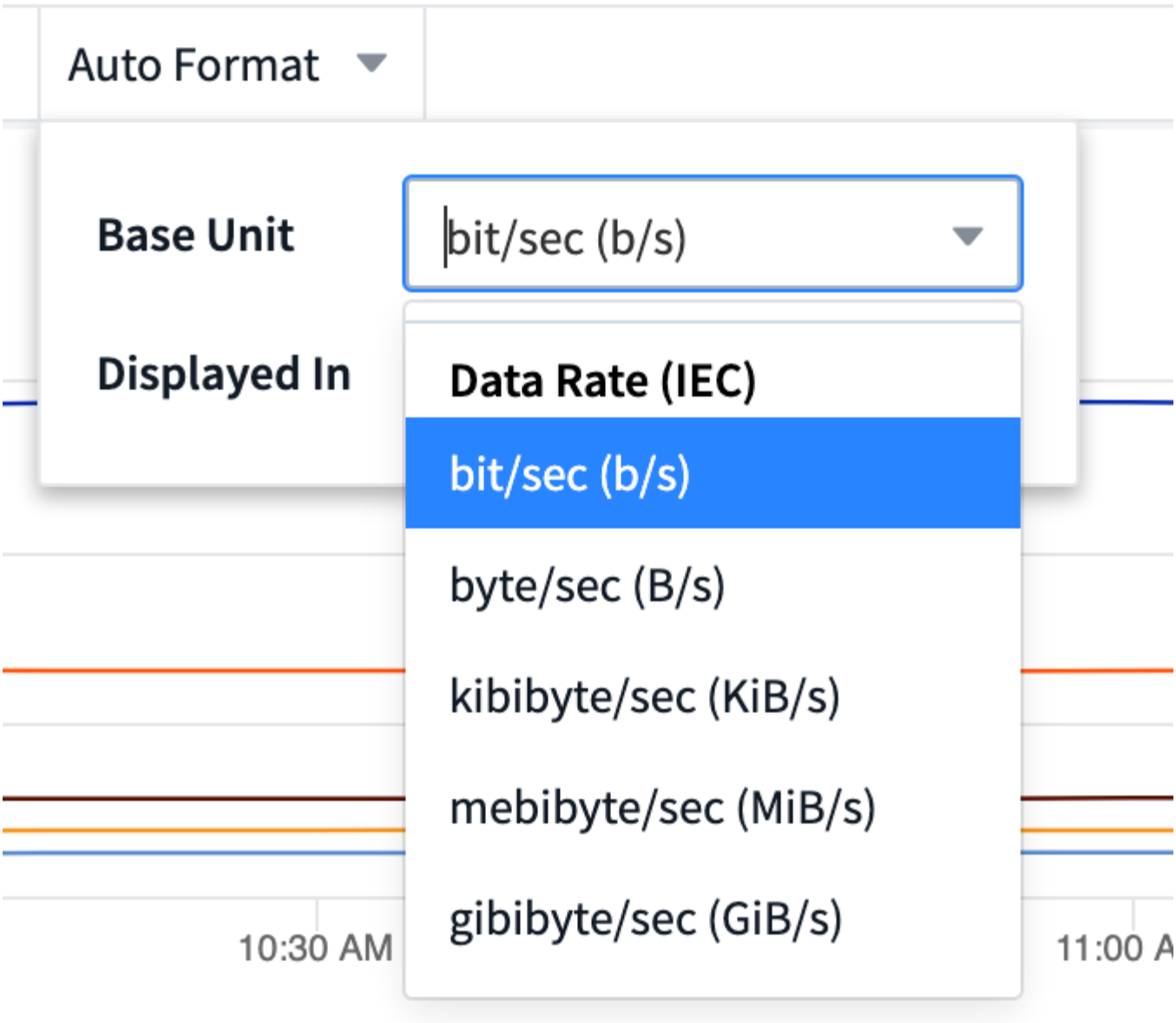
下の折れ線グラフの例では、ウィジェットに対して選択されたデータは *BYTS*(ベースの IEC データユニット : 下の表を参照) であることがわかっているため、ベースユニットは自動的に「バイト (B) 」として選択されます。ただし、データ値はギビバイト（GiB）として表示されるのに十分な大きさであるため、Data Infrastructure Insightsではデフォルトで自動的にGiBにフォーマットされます。グラフの Y 軸には表示単位が「 GiB 」と表示され、すべての値がその単位で表示されます。



グラフを別の単位で表示する場合は、値を表示する別の形式を選択できます。この例のベースユニットは _byte _ なので、ビット（ b ）、バイト（ B ）、キビバイト（ KiB ）、メビバイト（ MiB ）、ギビバイト（ GiB ）のいずれかの形式を選択できます。Y 軸ラベルと値は、選択した形式に応じて変更されます。



ベースユニットが不明な場合は、からユニットを割り当てることができます "使用可能な単位"をクリックするか、独自の情報を入力します。ベースユニットを割り当てたら、を選択して、サポートされている適切な形式のいずれかでデータを表示できます。



設定をクリアしてから、もう一度開始するには、 [* 初期設定にリセット *] をクリックします。

オートフォーマットについての単語

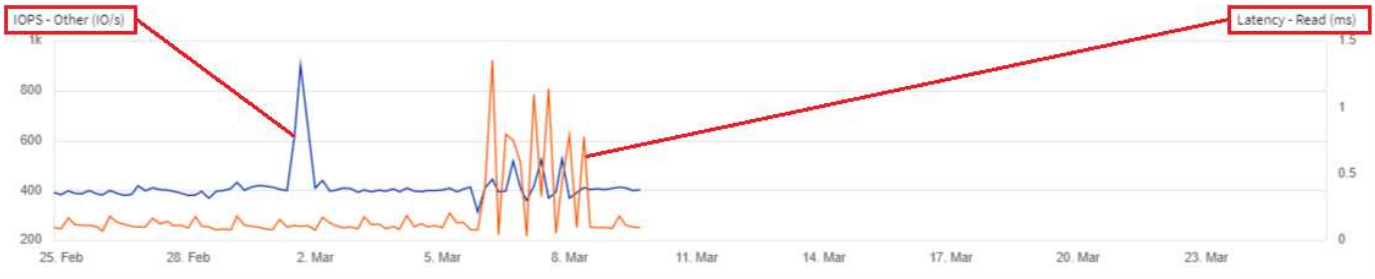
ほとんどの指標は、最小単位のデータコレクタによって報告されます。たとえば、 1 、 234 、 567,890 バイトのような整数で報告されます。デフォルトでは、Data Infrastructure Insightsは最も読みやすい表示に自動的に値の書式を設定します。たとえば、データ値 1,234,567,890 バイトは、自動的に 1.23_ギ ビバイトにフォーマットされます。メビバイト _ のように、別の形式で表示することもできます。それに応じて値が表示されます。

Data Infrastructure Insightsでは、米国英語の番号命名標準を使用しています。米国の「 10 億」は「 1000 万」に相当します。

複数のクエリを使用するウィジェット

2 つのクエリを含む時系列ウィジェット（直線、スプライン、面、積み上げ面）があり、両方が主 Y 軸をプロットしている場合、ベースユニットは Y 軸の上部に表示されません。 ただし、ウィジェットにプライマリ Y 軸に対するクエリとセカンダリ Y 軸に対するクエリがある場合は、それぞれのベースユニットが表示されま

す。



ウィジェットにクエリが 3 つ以上ある場合、ベースユニットは Y 軸に表示されません。

使用可能な単位

次の表は、カテゴリ別に使用可能なすべてのユニットを示しています。

* カテゴリ *	* 単位 *
通貨	セント ドルだ
データ（ IEC ）	ビット バイト キビバイト メビバイト ギビバイト テビバイト ペビバイト エクスビバイト
データ速度（ IEC ）	ビット/秒 バイト/秒 キビバイト/秒 メビバイト/秒 ギビバイト/秒 テビバイト/秒 ペビバイト/秒
データ (メートル)	キロバイト メガバイト ギガバイト テラバイト ペタバイト エクサバイト
データ速度（メートル単位）	キロバイト/秒 メガバイト/秒 ギガバイト/秒 テラバイト/秒 ペタバイト/秒 エクサバイト/秒

IEC	吉備 メビ ギビ テビ ペビ 元FBIだ
10 進数	整数 サウザンド ミリオン ビリオン 兆ドルです
割合	割合
時間	ナノ秒 マイクロ秒 ミリ秒 第二に 分 時間
温度	摂氏 華氏だ
頻度	ヘルツ キロヘルツ メガヘルツ ギガヘルツ
CPU	ナノコアだ マイクロコア ミリコア コア数 キロコア メガコア ジガコア テラコア ペタコレス エクサコア
スループット	1秒あたりのI/O処理数 処理数/秒 要求数/秒 読み取り/秒 書き込み/秒 処理数/分 読み取り/分 書き込み/分

TV モードと自動更新

ダッシュボードとアセットランディングページのウィジェットのデータは、選択した[Dashboard Time Range]で決定される更新間隔に従って自動更新されます。更新間隔は、ウィジェットが時系列（折れ線、スプライン、面、積み上げ面グラフ）であるか非時系列（その他すべてのグラフ）であるかに基づいています。

ダッシュボードの時間範囲	時系列の更新間隔	非タイムシリーズ更新間隔
最後の 15 分	10 秒	1 分
過去 30 分	15秒	1 分
最後の60分	15秒	1 分
過去2時間	30秒	5 分
過去3時間	30秒	5 分
過去6時間	1 分	5 分
過去12時間	5 分	10分だ
過去 24 時間	5 分	10分だ
過去2日間	10分だ	10分だ
過去 3 日間	15分だ	15分だ
過去7日間	1 時間	1 時間
過去30日間	2 時間	2 時間

各ウィジェットの右上に自動更新間隔が表示されます。

カスタムダッシュボードの期間では自動更新を使用できません。

- TV モード * と組み合わせて使用すると、自動更新により、ダッシュボードまたはアセットページにほぼリアルタイムでデータを表示できます。テレビモードでは、すっきりとしたディスプレイが提供されます。ナビゲーションメニューは非表示になっており、編集ボタンと同様に、データ表示用の画面のスペースが増えます。TVモードでは、Data Infrastructure Insightsの一般的なタイムアウトが無視され、手動でログアウトするか、認証セキュリティプロトコルによって自動的にログアウトするまで、ディスプレイはライブのままになります。

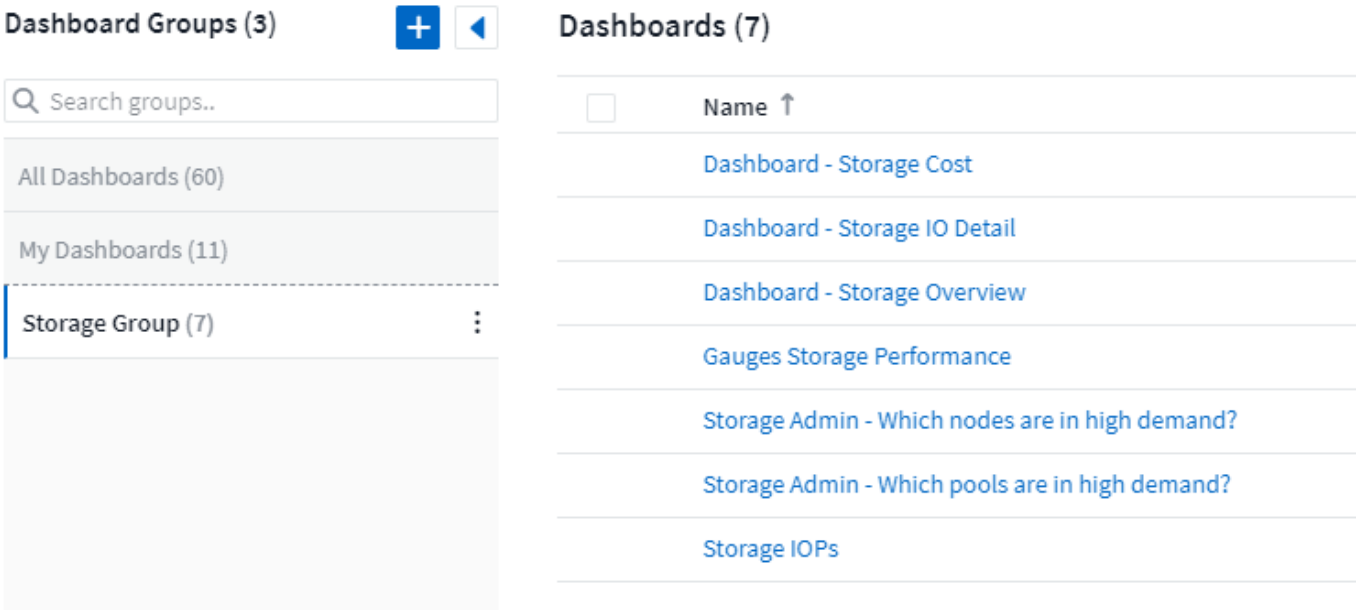
NetApp BlueXP には7日間のユーザログインタイムアウトが設定されているため、Data Infrastructure Insightsもそのイベントを使用してログアウトする必要があります。再度ログインするだけで、ダッシュボードは引き続き表示されます。

- TVモードを有効にするには、TVモードボタンをクリックします。
- TV モードを無効にするには、画面左上の * 終了 * ボタンをクリックします。

右上隅にある一時停止ボタンをクリックすると、自動更新を一時的に中断できます。一時停止中は、ダッシュボードの時間範囲フィールドに一時停止中のデータのアクティブな時間範囲が表示されます。自動更新が一時停止されている間も、データの取得と更新はまだ行われています。[再開] ボタンをクリックして、データの自動更新を続行します。

ダッシュボードグループ

グループ化を使用すると、関連するダッシュボードを表示および管理できます。たとえば、環境内のストレージ専用のダッシュボードグループを作成できます。ダッシュボードグループは、 [ダッシュボード（ *Dashboards ）]>[すべてのダッシュボードを表示（ Show All Dashboards ）] * ページで管理します。



デフォルトでは 2 つのグループが表示されます。

- * すべてのダッシュボード * には、所有者に関係なく、作成されたすべてのダッシュボードが表示されます。
- * My Dashboards * には、現在のユーザーが作成したダッシュボードのみが表示されます。

グループ名の横には、各グループに含まれるダッシュボードの数が表示されます。

新しいグループを作成するには、「 + 」「ダッシュボードグループの新規作成 * 」ボタンをクリックします。グループの名前を入力し、 * グループの作成 * をクリックします。空のグループがその名前で作成されます。

グループにダッシュボードを追加するには、 *All Dashboards_group* をクリックして、環境内のすべてのダッシュボードを表示します。所有しているダッシュボードのみを表示するには、 *[Click _ My Dashboards*] をクリックし、次のいずれかの操作を行います。

- 単一のダッシュボードを追加するには ' ダッシュボードの右側にあるメニューをクリックして ' グループに追加 (Add to Group_) を選択します
- グループに複数のダッシュボードを追加するには、各ダッシュボードの横にあるチェックボックスをクリックしてダッシュボードを選択し、 * Bulk Actions * ボタンをクリックして、 _ グループに追加 _ を選択します。

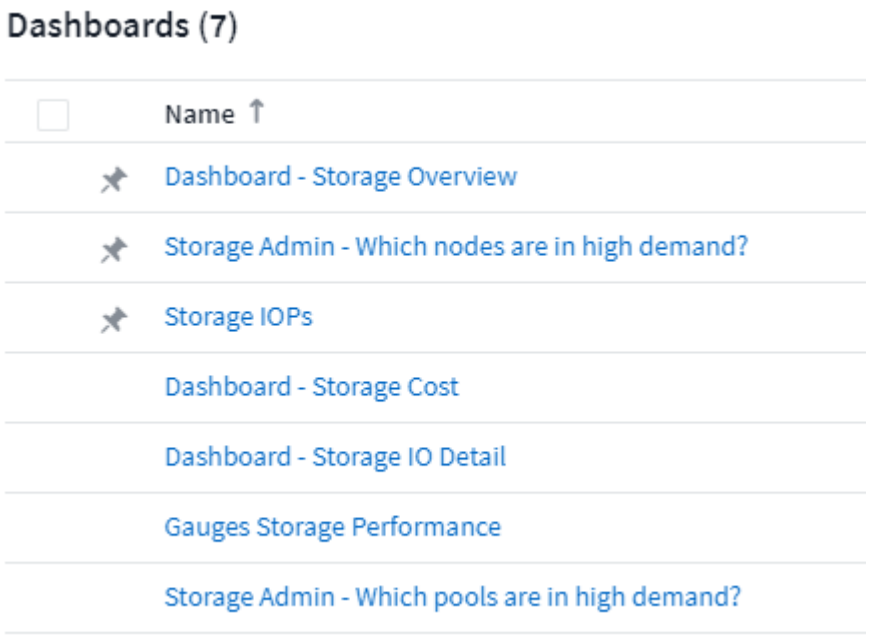
[グループから削除] を選択して ' 現在のグループからダッシュボードを削除する方法と同じ方法で ' 現在のグループからダッシュボードを削除しますダッシュボードは、 _All Dashboards_or_My Dashboards_group からは削除できません。

グループからダッシュボードを削除しても、Data Infrastructure Insightsからは削除されません。ダッシュボードを完全に削除するには ' ダッシュボードを選択して *Delete*(削除) をクリックしますこれにより、そのグループが属していたすべてのグループから削除され、どのユーザもそのグループを使用できなくなります。

お気に入りのダッシュボードをピン固定します

お気に入りのダッシュボードをダッシュボードリストの一番上に固定することで、ダッシュボードをさらに管理することができます。ダッシュボードを固定するには、任意のリストのダッシュボード上にカーソルを置いたときに表示されるサムタックボタンをクリックします。

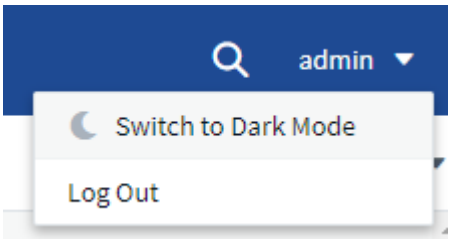
ダッシュボードのピン / ピン解除は ' ダッシュボードが属するグループに依存しない ' 個別のユーザー設定です



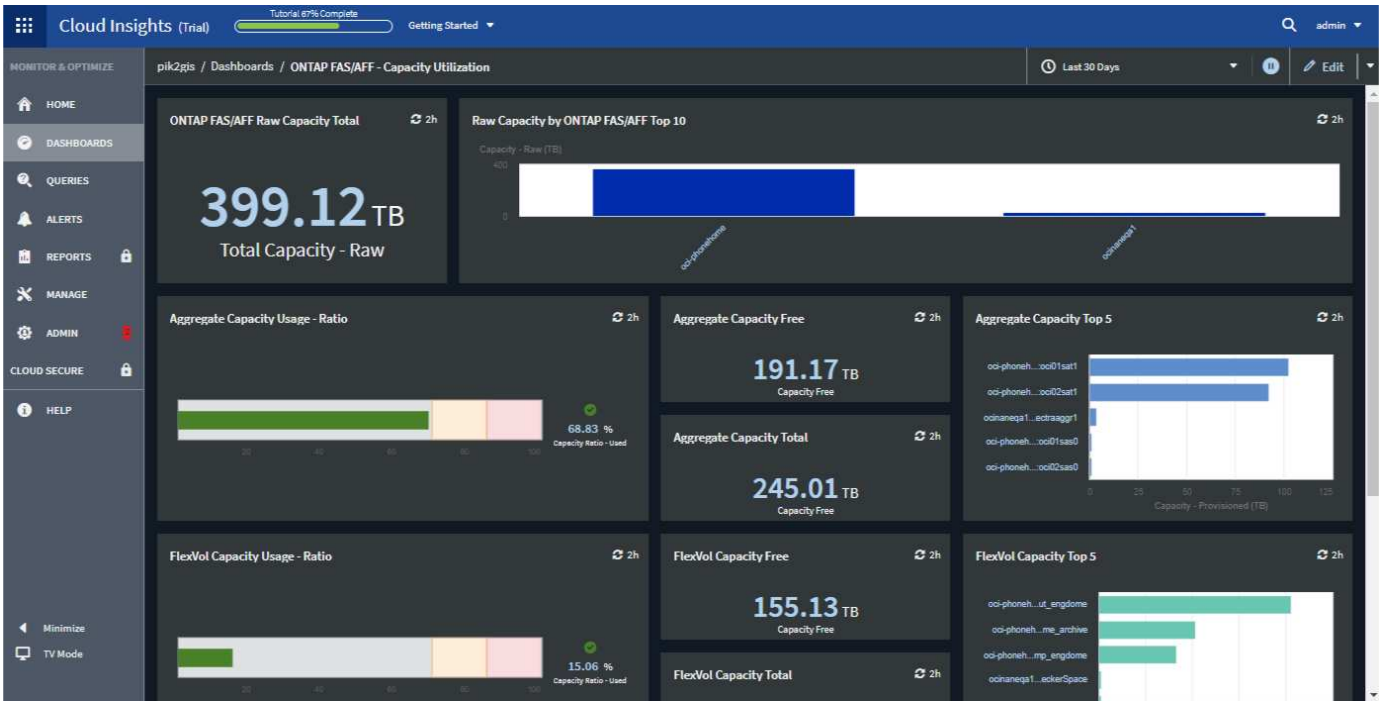
ダークテーマ

Data Infrastructure Insightsは、明るいテーマ（デフォルト）を使用して表示できます。このテーマでは、ほとんどの画面を暗いテキスト付きの明るい背景で表示します。暗いテーマでは、ほとんどの画面を暗いテキスト付きの暗い背景で表示します。

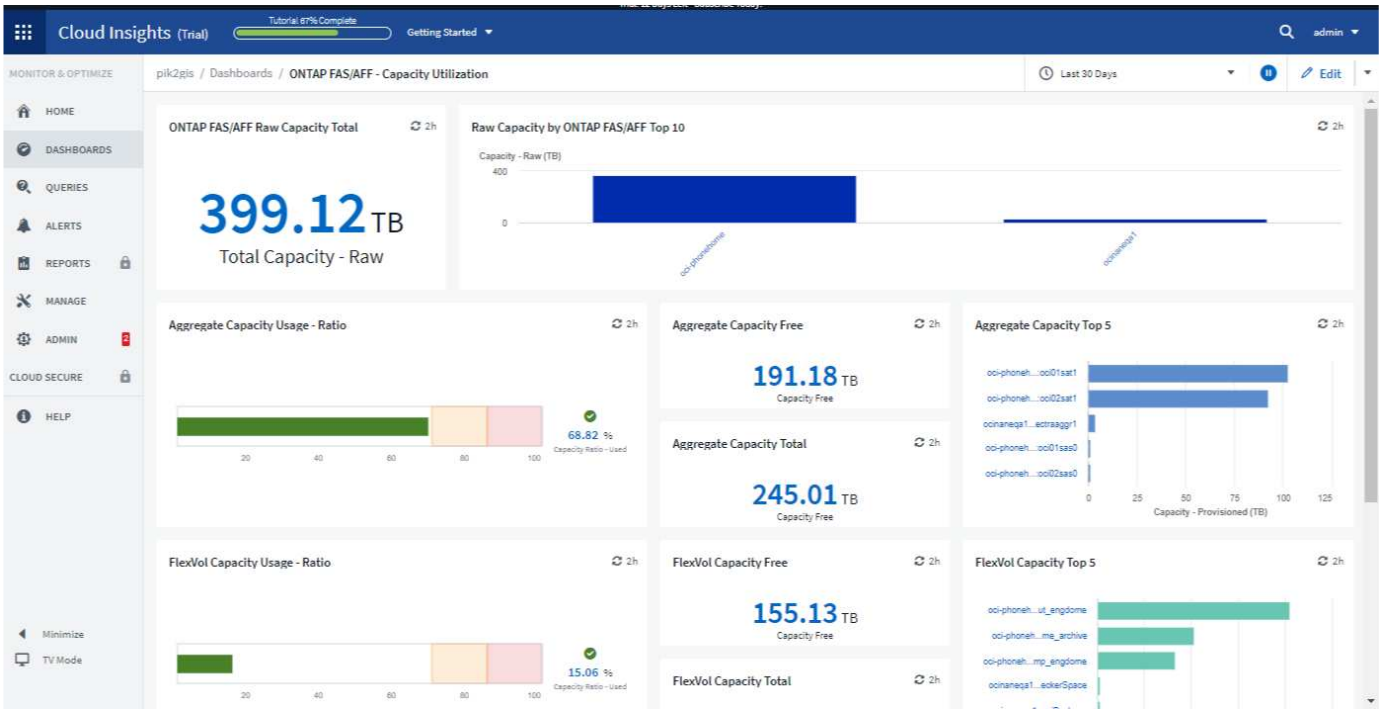
明るいテーマと暗いテーマを切り替えるには、画面の右上にあるユーザ名ボタンをクリックし、目的のテーマを選択します。



ダークテーマのダッシュボードビュー：



ライトテーマダッシュボードビュー：



一部のウィジェットグラフなどの画面領域では、暗いテーマで表示しているときでも、背景が明るい場合があります。

折れ線グラフの補間

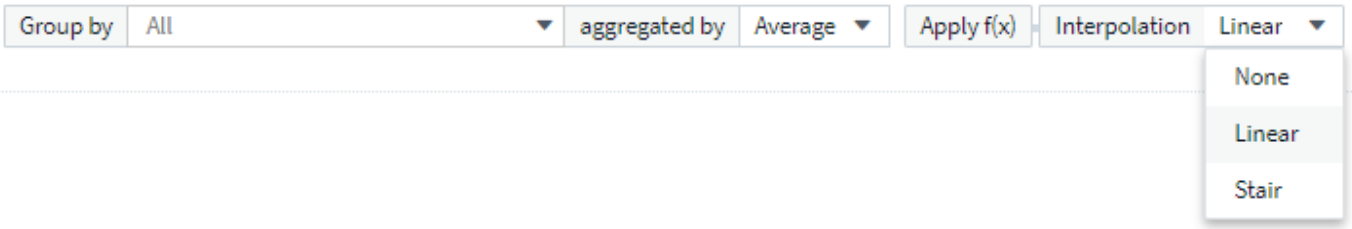
多くの場合、データコレクタがデータを異なる間隔でポーリングします。たとえば、データコレクタ A は 15 分ごとにポーリングし、データコレクタ B は 5 分ごとにポーリングします。折れ線グラフウィジェット（スプライングラフ、面グラフ、積み上げ面グラフも含む）で、複数のデータコレクタのこのデータを 1 行に集計している場合（たとえば、ウィジェットが「すべて」でグループ化されている場合）は、次のようになります。 また、 5 分ごとにデータを更新すると、コレクタ B からのデータが正確に表示され、コレクタ A からの

データにギャップが生じ、コレクタ A が再度ポーリングするまでアグリゲートに影響が及ぶ可能性があります。

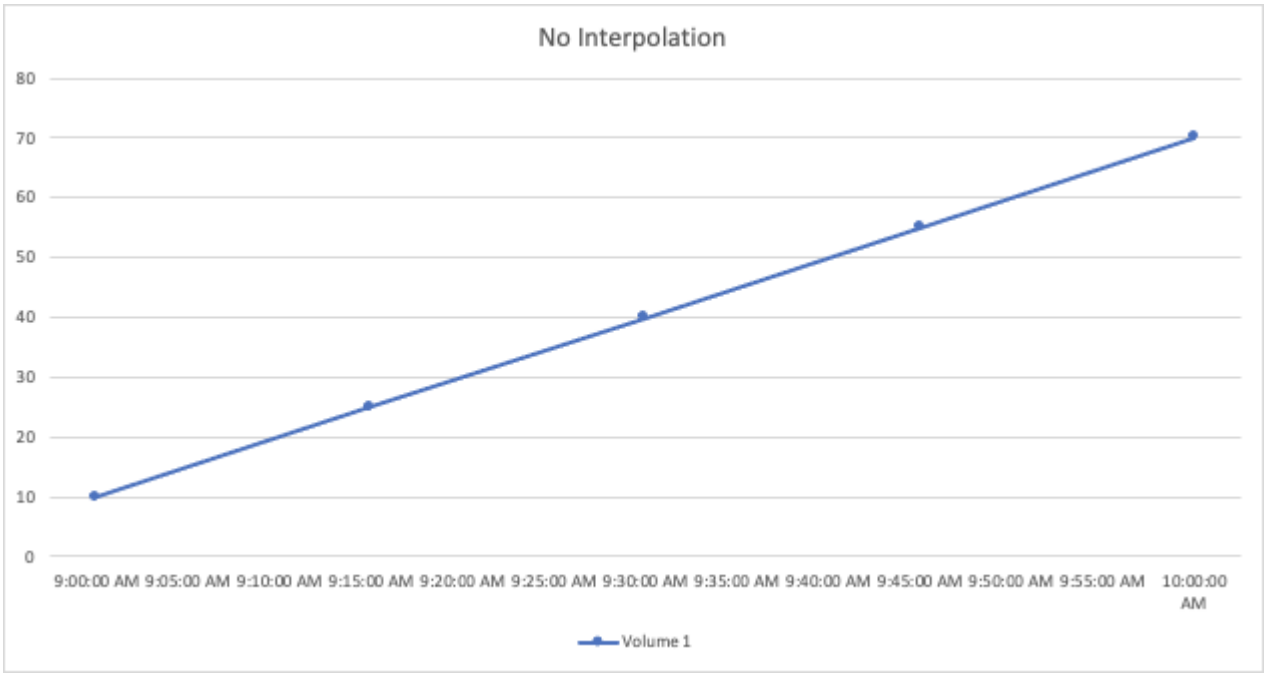
この問題を軽減するために、Data Infrastructure Insightsは集計時にデータを補間し、周囲のデータポイントを使用してデータコレクタが再度ポーリングを行うまでデータを「最善の推測」で評価します。ウィジェットのグループ化を調整することで、各データコレクタのオブジェクトデータをいつでも個別に表示できます。

補間法

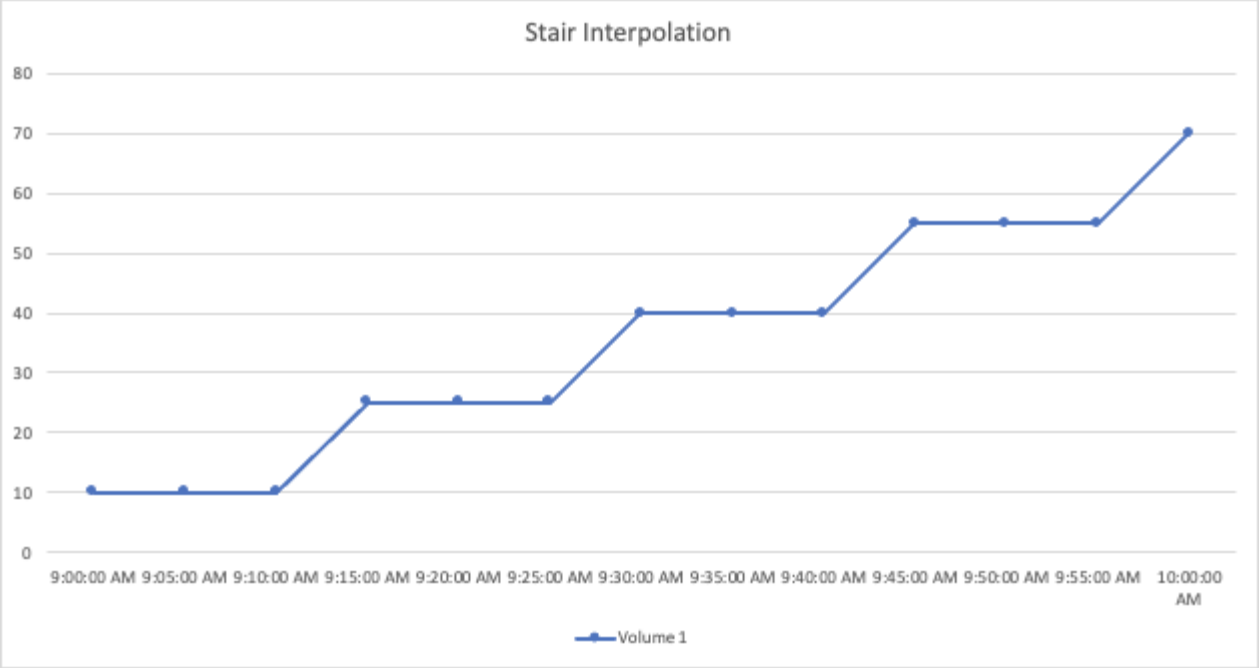
折れ線グラフ（スプライングラフ、面グラフ、積み上げ面グラフ）を作成または変更する場合、補間方法を 3 つのタイプのいずれかに設定できます。「グループ化」セクションで、目的の補間法を選択します。



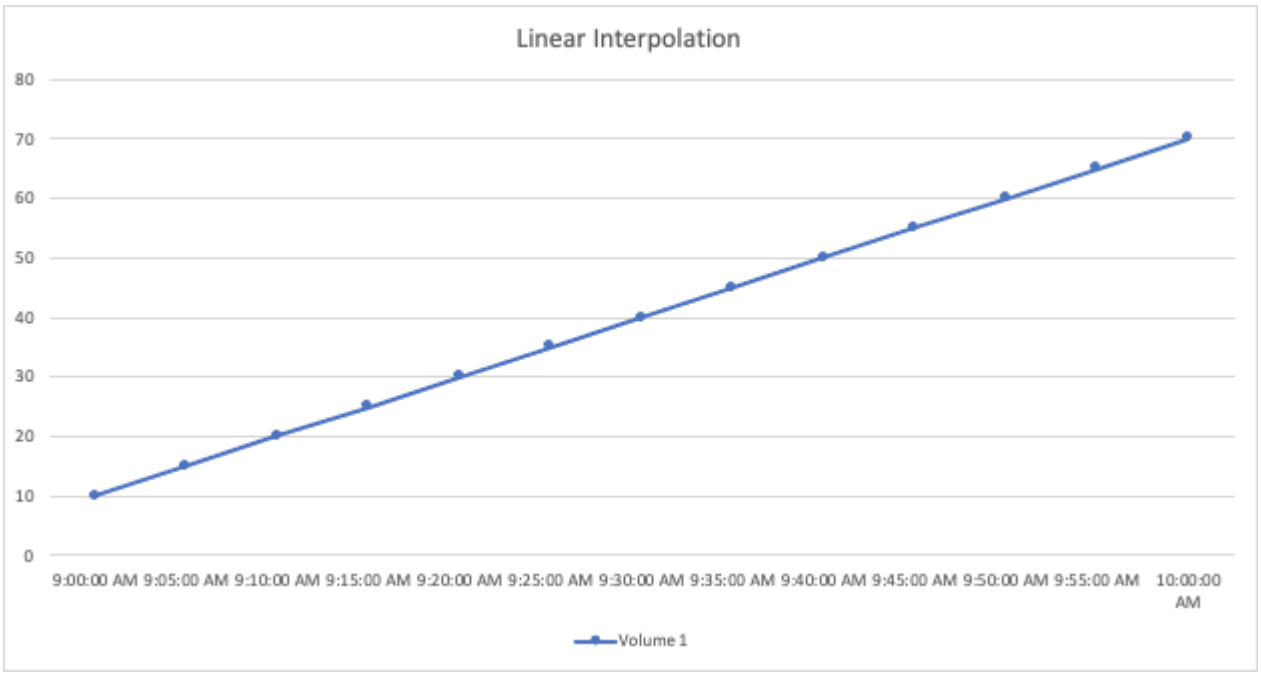
- * なし * ：何もしないでください。つまり、その間に点を生成しません。



- * 階段 * ：点は前の点の値から生成されます。直線では、これは典型的な「階段」のレイアウトとして表示されます。



- * 線形 * ： 2 点間の接続の値として点が生成されます。2 つのポイントを接続しているラインのように見え、追加の (補間された) データポイントを持つラインを生成します。



ダッシュボードの例

ダッシュボードの例：仮想マシンのパフォーマンス

現在、 IT 運用が直面している課題は多数あります。管理者は少ないリソースでより多くの成果を達成するよう求められており、動的なデータセンターを完全に可視化することは必須条件です。この例では、環境内の仮想マシン（ VM ）のパフォーマンスに関する運用状況を確認できるウィジェットを含むダッシュボードを作成する方法を紹介しま

す。この例で示す手順に従って、ウィジェットを作成して固有のニーズに対応することで、フロントエンド仮想マシンとバックエンドストレージのパフォーマンスの比較を可視化したり、 VM のレイテンシと I/O 要求の比較を表示したりできます。

このタスクについて

ここでは、以下を含む仮想マシンのパフォーマンス用ダッシュボードを作成します。

- VM 名とパフォーマンスデータをリストするテーブル
- VM のレイテンシをストレージのレイテンシと比較するグラフ
- VM の読み取り IOPS 、書き込み IOPS 、合計 IOPS を示すグラフ
- VM の最大スループットを示すグラフ

ここで紹介するのは基本的な例です。ダッシュボードをカスタマイズして、運用上のベストプラクティスに合わせて、選択したパフォーマンスデータを強調表示および比較することができます。

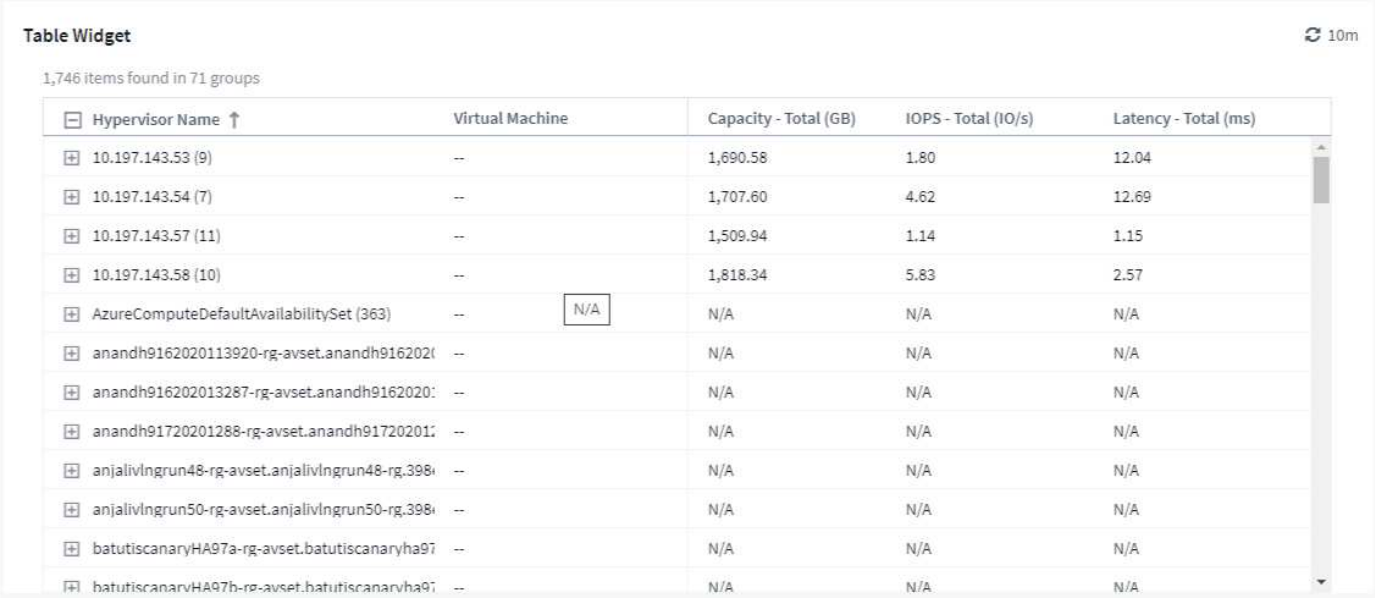
手順

1. 管理者権限を持つユーザとして Insight にログインします。
2. [* ダッシュボード *] メニューから、 [* [+ 新しいダッシュボード] *] を選択します。

   [新しいダッシュボード *] ページが開きます。

3. ページの上部に、「 VM Performance by Application 」など、ダッシュボードの一意の名前を入力します。
4. 「 * 保存 * 」をクリックして、ダッシュボードに新しい名前を付けて保存します。
5. 次に、ウィジェットを追加します。必要に応じて、 * 編集 * アイコンをクリックして編集モードを有効にします。
6. [ウィジェットの追加 * （ Add Widget * ）] アイコンをクリックし、 [* テーブル * （ * Table * ）] を選択して新しい表ウィジェットをダッシュボードに追加します。

   ウィジェットを編集（ Edit Widget ）ダイアログが開きます。環境内のすべてのストレージについて、デフォルトのデータが表示されます。



ダイアログ"]

1. このウィジェットをカスタマイズできます。上部の Name フィールドで「 Widget 1 」を削除し、「 Virtual Machine Performance table 」と入力します。
2. アセットのタイプドロップダウンをクリックし、「 Storage _To Virtual Machine _ 」を変更します。

   表のデータが更新され、環境内のすべての仮想マシンが表示されます。

3. 表に列をいくつか追加してみましょう。右側の歯車アイコンをクリックし、 _Hypervisor name _ 、 _IOPS - Total _ 、および _Latency - Total _ を選択します。検索結果に名前を入力して、目的のフィールドをすばやく表示することもできます。

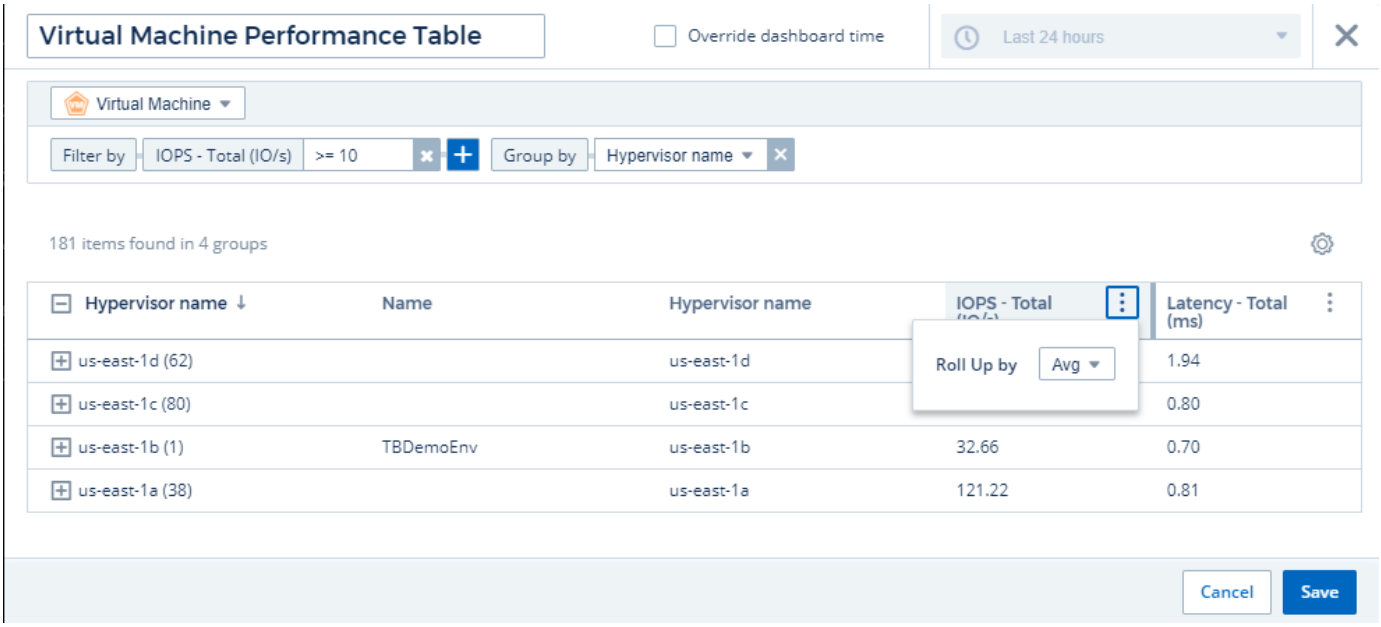
   これらの列が表に表示されます。これらの列のいずれかを使用してテーブルをソートできます。列はウィジェットに追加した順序で表示されます。

4. この演習では、あまり使用されていない VM は除外するため、合計 IOPS が 10 未満のものをフィルタで除外します。[* フィルタ基準] の横にある * [+] * ボタンをクリックし、 [_IOPS] - [合計] を選択します。任意の * をクリックし、 * 開始 * フィールドに「 10 」と入力します。[* から *] フィールドは空のままにします。フィルタフィールドをクリックするか、 Enter キーを押してフィルタを設定します。

   これで、合計 IOPS が 10 以上の VM のみが表に表示されます。

5. 結果をグループ化すると、表をさらに折りたたむことができます。[* Group by] の横にある [*] ボタンをクリックし、グループ化するフィールド（ _Application_or_Hypervisor name _ など）を選択します。グループ化が自動的に適用されます。

   これで、設定に従ってテーブルの行がグループ化されます。グループは必要に応じて展開または折りたたむことができます。グループ化された行には、各列の集計データが表示されます。一部の列では、その列の集計方法を選択できます。



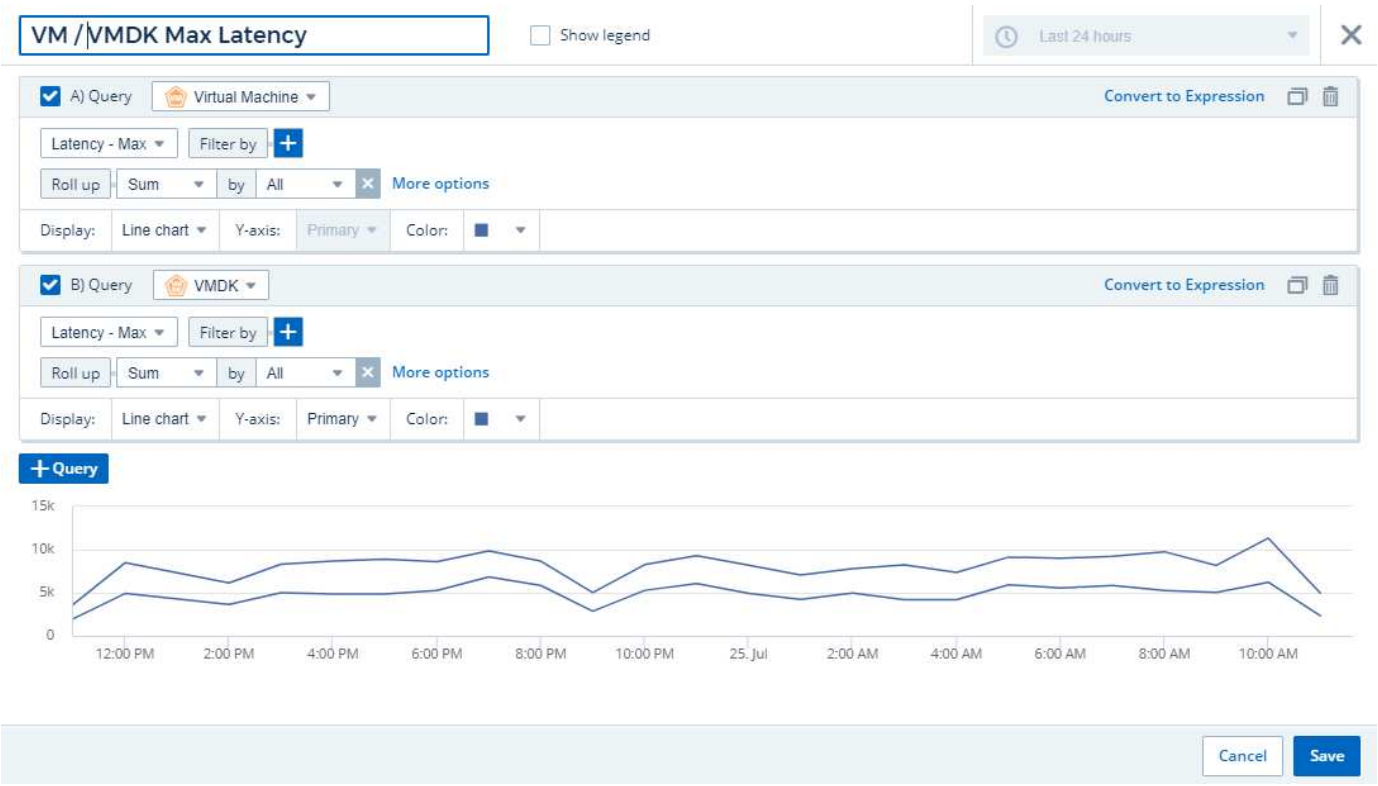
1. 目的に応じて表ウィジェットをカスタマイズしたら、「 * [保存] * 」ボタンをクリックします。

   表ウィジェットがダッシュボードに保存されます。

ダッシュボード上のウィジェットの右下をドラッグすると、ウィジェットのサイズを変更できます。すべての列が明確に表示されるようにウィジェットの幅を広げます。保存 * をクリックして、現在のダッシュボードを保存します。

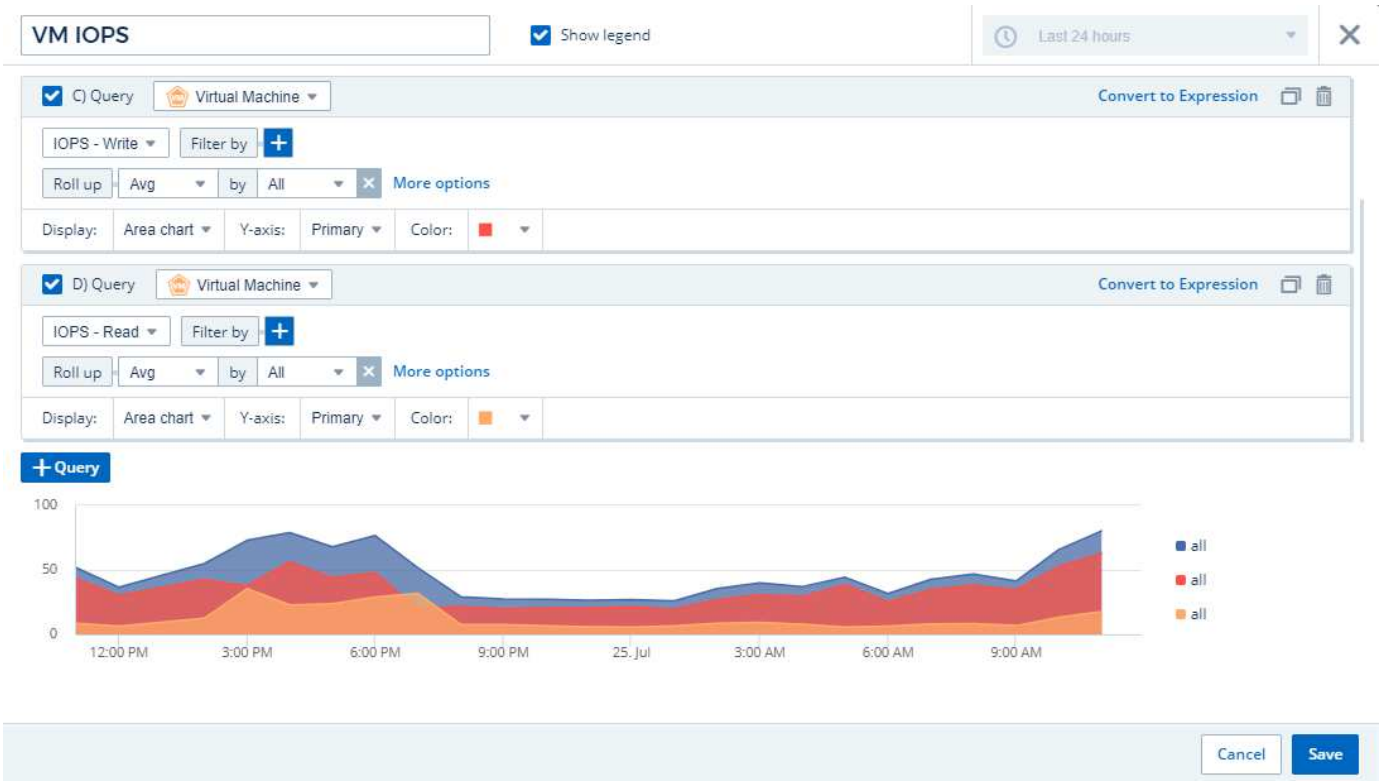
次に、 VM のパフォーマンスを表示するグラフをいくつか追加します。次に、 VM のレイテンシと VMDK のレイテンシを比較する折れ線グラフを作成します。

1. 必要に応じて、ダッシュボードの * 編集 * アイコンをクリックして編集モードを有効にします。
2. [ウィジェットの追加] アイコンをクリックし、 [折れ線グラフ _] を選択して、新しい折れ線グラフウィジェットをダッシュボードに追加します。
3. [ウィジェットを編集（ Edit Widget ）] ダイアログが開きます。このウィジェットに「 VM / VMDK 最大レイテンシ」と名前を付けます
4. 「 * Virtual Machine * 」を選択し、「 *Latency - Max* 」を選択します。任意のフィルターを設定するか、 * フィルターを * 空のままにします。「 * 集計」で、「 _ 合計 _ すべて _ 」を選択します。このデータを「 *Line Chart* 」として表示し、「 Y 軸」を「 *_Primary_* 」のままにします。
5. [+Query] * ボタンをクリックして、 2 行目を追加します。この行では、 *VMDK_or_Latency - Max* を選択します。任意のフィルターを設定するか、 * フィルターを * 空のままにします。「 * 集計」で、「 _ 合計 _ すべて _ 」を選択します。このデータを「 *Line Chart* 」として表示し、「 Y 軸」を「 *_Primary_* 」のままにします。
6. このウィジェットをダッシュボードに追加するには、「 * [保存] * 」をクリックします。



次に、 VM の読み取り IOPS 、書き込み IOPS 、合計 IOPS を 1 つのグラフに表示するグラフを追加します。

1. [ウィジェットの追加] アイコンをクリックし、 [エリアグラフ _] を選択して、新しい面グラフウィジェットをダッシュボードに追加します。
2. ウィジェットを編集（ Edit Widget ）ダイアログが開きます。このウィジェットに「 VM IOPS 」と名前を付けます。
3. 「 * Virtual Machine * 」を選択し、「 *IOPS-Total* 」を選択します。任意のフィルターを設定するか、 * フィルターを * 空のままにします。「 * 集計」で、「 _ 合計 _ すべて _ 」を選択します。このデータを *Area Chart* として表示し、 Leave *Y - Axis_as Primary_* として表示します。
4. [+Query] * ボタンをクリックして、 2 行目を追加します。この行では、 * Virtual Machine * を選択し、 *iops-Read* を選択します。
5. 3 番目のデータ行を追加するには、 [+Query] * ボタンをクリックします。この行では、 * Virtual Machine * を選択し、 *IOs-Write*. を選択します。
6. このウィジェットの凡例をダッシュボードに表示するには、 * 凡例を表示 * をクリックします。



1. このウィジェットをダッシュボードに追加するには、「 * [保存] * 」をクリックします。

次に、 VM に関連付けられているアプリケーションごとに VM のスループットを表示するグラフを追加します。これにはロールアップ機能を使用します。

1. [ウィジェットの追加] アイコンをクリックし、 [折れ線グラフ _] を選択して、新しい折れ線グラフウィジェットをダッシュボードに追加します。
2. ウィジェットを編集（ Edit Widget ）ダイアログが開きます。このウィジェットに「 VM throughput by Application 」と名前を付けます。
3. [仮想マシン] を選択し、 [スループット - 合計] を選択します。必要なフィルタを設定するか、フィルタを空のままにします。「ロールアップ」で「最大」を選択し、「アプリケーション」または「名前」で選択します。トップ 10 アプリケーションを表示します。このデータを折れ線グラフとして表示し、 Y 軸を [プライマリ] のままにします。
4. このウィジェットをダッシュボードに追加するには、「 * [保存] * 」をクリックします。

ダッシュボード上でウィジェットを移動するには、ウィジェット上部の任意の場所でマウスボタンを押したまま、新しい場所にドラッグします。

ウィジェットの右下をドラッグすると、ウィジェットのサイズを変更できます。

変更を行ったら、必ずダッシュボードを * [Save] * してください。

最後の VM パフォーマンスダッシュボードは次のようになります。

ダッシュボードとウィジェットのベストプラクティス

ここでは、ダッシュボードとウィジェットを最大限に活用するためのヒントやコツを紹介します。

適切な指標を見つける

Data Infrastructure Insightsは、データコレクタごとに異なる名前を使用してカウンタと指標を取得します。

ダッシュボードウィジェットの指標やカウンタを検索するときは、予期しない名前で指標が分類されることがあります。Data Infrastructure Insightsのドロップダウンリストは通常アルファベット順に表示されますが、必要と思われる用語がリストに表示されないことがあります。たとえば、ほとんどのリストで「 raw capacity 」は「 used capacity 」から離れた位置に表示されます。

- ベストプラクティス * ：[フィルタ条件] などのフィールドや列セレクタのような場所で検索機能を使用して、探しているものを検索します。たとえば、「 cap 」で検索すると、リストのどこに含まれているかに関係なく、名前に「 capacity 」が含まれているすべての指標が表示されます。これにより、必要な指標を短いリストから簡単に選択できるようになります。

以下は、指標を検索する際に有効なキーワードの例です。

検索する項目	次の検索も試してください。
CPU	プロセッサ
容量	使用済み容量 物理容量 プロビジョニングされた容量 ストレージプールの容量 <other asset type> の容量 書き込み済み容量

ディスク速度	最低のディスク速度 パフォーマンスが最も低いディスクタイプ
ホスト	ハイパーバイザー ホスト
ハイパーバイザー	ホスト ハイパーバイザーです
マイクロコード	ファームウェア
名前	エイリアス ハイパーバイザー名 ストレージ名 <other asset type> 名 単純な名前 リソース名 ファブリックエイリアス
読み取り / 書き込み	部分的なR/W 保留中の書き込み IOPS -書き込み 書き込み済み容量 レイテンシ-読み取り キャッシュ使用率-読み取り
仮想マシン	VM 仮想化されている

これは包括的なリストではありません。これらは検索キーワードの一例です。

適切な資産を見つける

ウィジェットで参照できるアセットは、アセットのタイプによってフィルタや検索に使用できます。

ダッシュボードとアセットページでは、ウィジェットの作成時に関連付けるアセットタイプによって、フィルタや列の追加が可能な他のアセットタイプカウンタが決まります。ウィジェットを作成する際は、次の点に注意してください。

アセットタイプ / カウンタ	フィルタ可能なアセット
仮想マシン	VMDK です
データストア	内部ボリューム VMDK です 仮想マシン ボリューム
ハイパーバイザー	仮想マシン ハイパーバイザーです ホスト
ホスト	内部ボリューム ボリューム クラスタホスト 仮想マシン

ファブリック	ポート

これは包括的なリストではありません。

- ベストプラクティス * ：リストに表示されない特定のアセットタイプでフィルタリングする場合は、別のアセットタイプを使用してクエリを作成してみてください。

散布図の例：軸を知る

散布図ウィジェットでカウンタの順序を変更すると、データを表示する軸が変更されます。

このタスクについて

この例では、 IOPS が低いにも関わらずレイテンシが高い低パフォーマンスの VM を示す散布図を作成します。

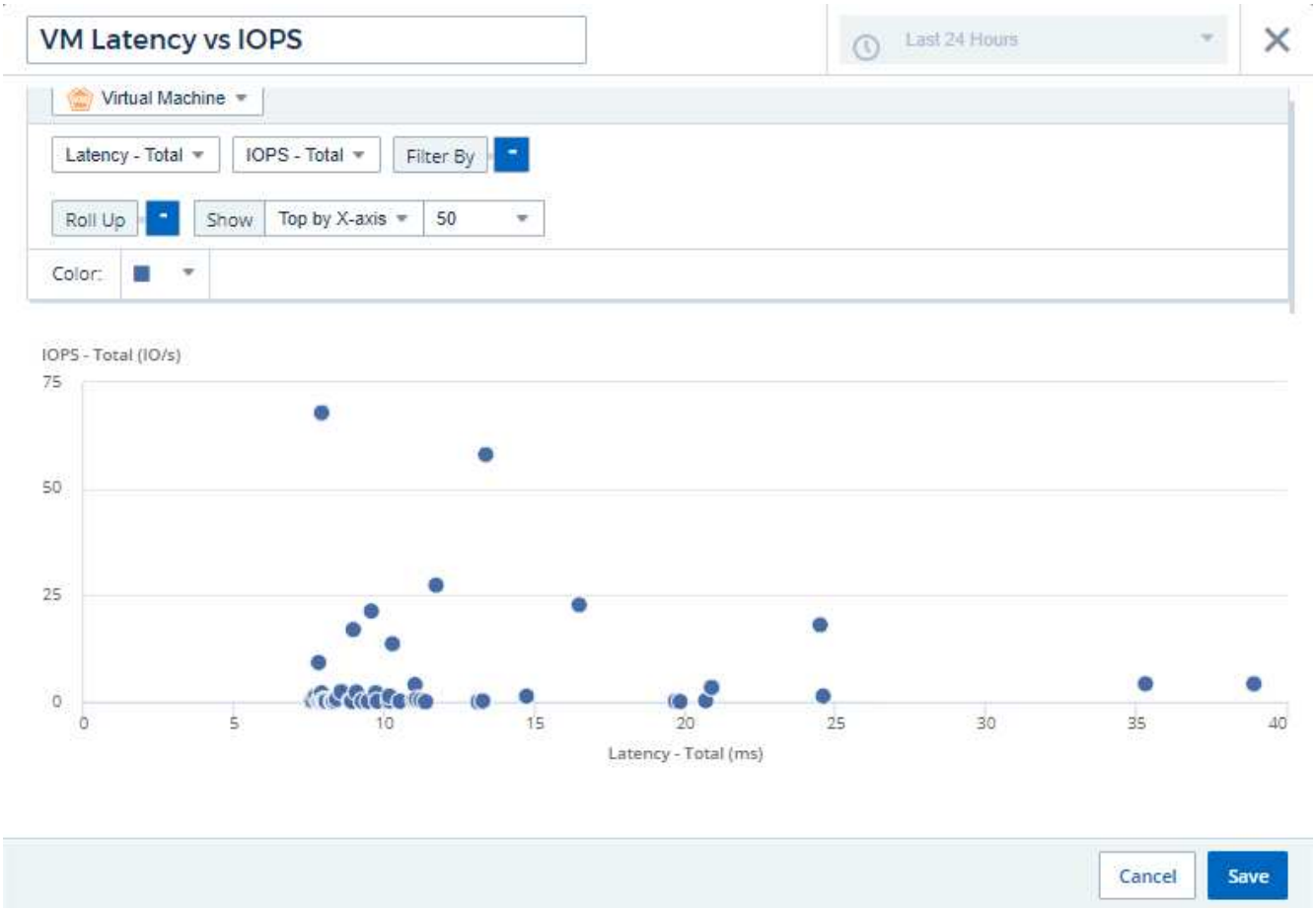
手順

1. ダッシュボードを編集モードで作成または開き、 * 散布図 * ウィジェットを追加します。
2. アセットのタイプを選択します。例： *Virtual Machine* 。
3. 出力する最初のカウンタを選択します。この例では、 _Latency - Total _ を選択します。

   _Latency - Total _ がグラフの X 軸に沿って表示されます。

4. プロットする 2 番目のカウンタを選択します。この例では、 *iops-Total* を選択します。

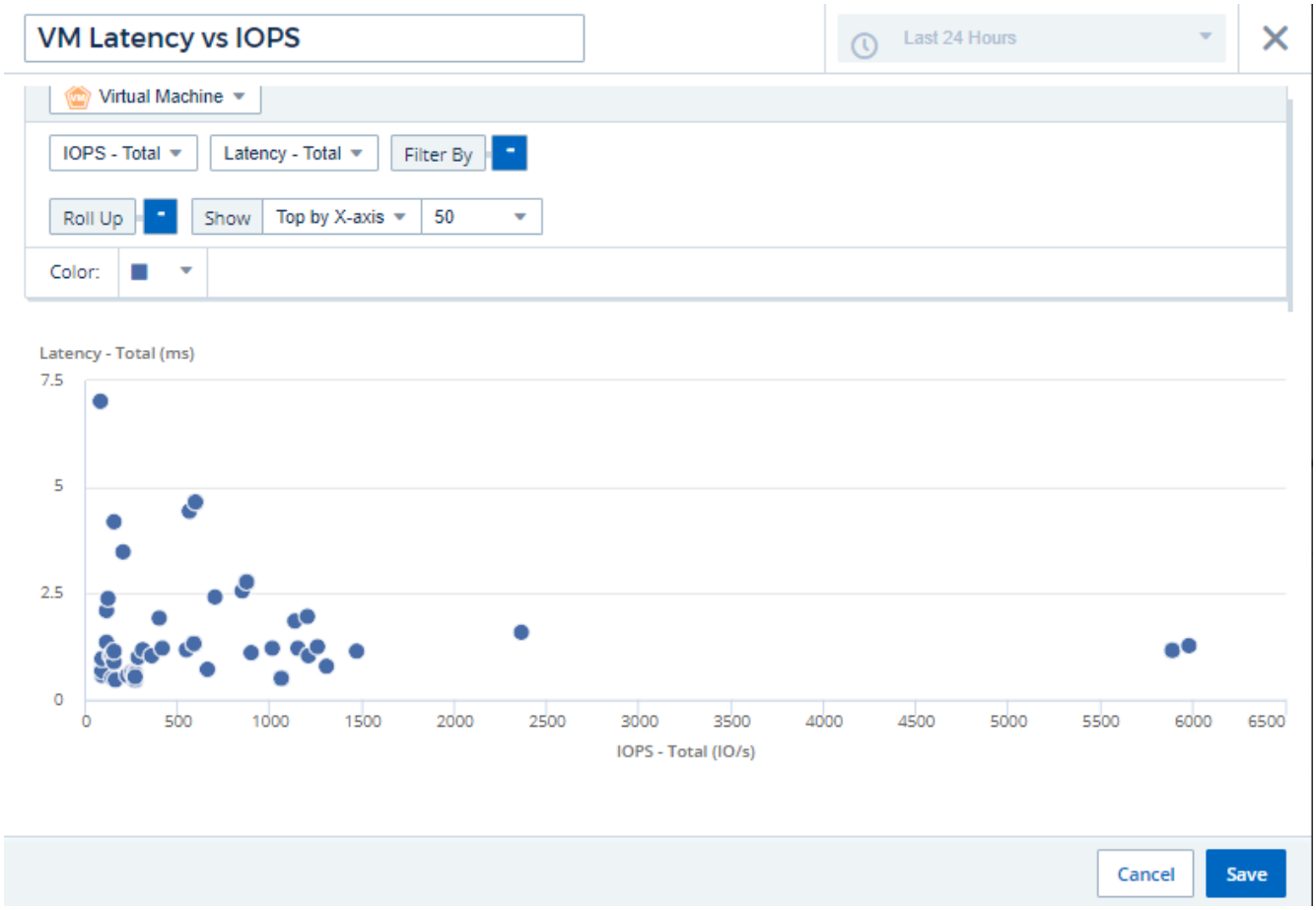
   _IOPS - Total _ がグラフの Y 軸に沿って表示されます。VM のレイテンシが高いほど、グラフの右側に表示されます。上位 X 軸 * の設定が最新であるため、レイテンシが高い上位 100 個の VM のみが表示されます。



5. 1 つ目のカウンタを *iops-Total* に、 2 つ目を _Latency - Total _ に設定して、カウンタの順序を逆にしています。

   _Latency - Total _ がグラフの Y 軸に沿って表示され、 _IOPS - Total _ が X 軸に沿って表示されるようになりました。今度は VM の IOPS が高いほど、グラフの右側に表示されます。

   「 X 軸上」の設定は変更されていないため、ウィジェットには、現在 X 軸に沿ってプロットされている上位 100 個の IOPS の高い VM が表示されます。



X 軸上の N 、 Y 軸上の N 、 X 軸下の N 、 Y 軸下の N 、または Y 軸下の N をグラフに表示するように選択できます。この例の最後のグラフには、合計 IOPS が高い上位 100 個の VM が表示されています。Y 軸上 * に変更すると、合計レイテンシが最も高い上位 100 個の VM が再びグラフに表示されます。

散布図では、ポイントをクリックすると、そのリソースのアセットページにドリルダウンできます。

クエリを使用した作業

クエリで使用するアセット

クエリを使用すると、ネットワークの監視やトラブルシューティングで環境内のアセットや指標を、ユーザが選択した条件（アノテーションなど）に基づいて細かいレベルで検索することができます。

アセットにアノテーションを自動的に割り当てるアノテーションルール _require_a クエリに注意してください。

環境内の物理または仮想インベントリアセット（および関連する指標）、または Kubernetes や ONTAP の高度なデータなどと統合されている指標を照会することができます。

在庫資産

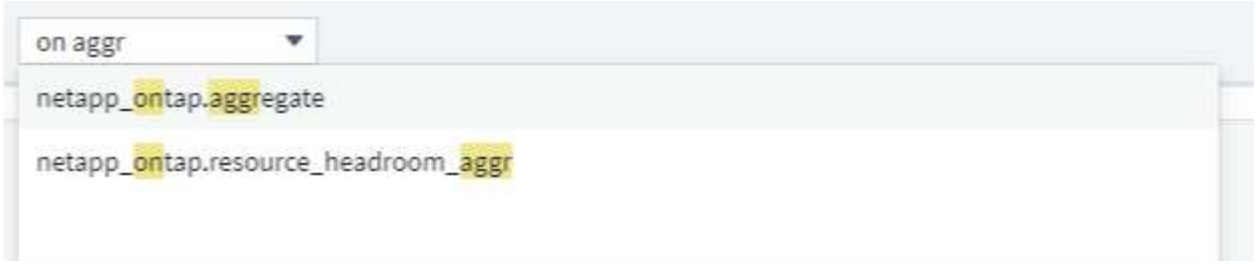
クエリ、ダッシュボードウィジェット、およびカスタムのアセットランディングページで使用できるアセットタイプは次のとおりです。フィルタ、式、表示に使用できるフィールドとカウンタは、アセットのタイプによ

って異なります。すべてのアセットをすべてのウィジェットタイプで使用できるわけではありません。

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

統合メトリック

インベントリ資産とその関連するパフォーマンス指標のクエリに加えて、 Kubernetes や Docker で生成された指標や ONTAP Advanced Metrics で提供された指標など、 * 統合データ * の指標も照会できます。



クエリの作成

クエリを使用すると、環境内のアセットを細かいレベルで検索できるため、必要なデータをフィルタして、目的のデータに基づいて結果をソートすることができます。

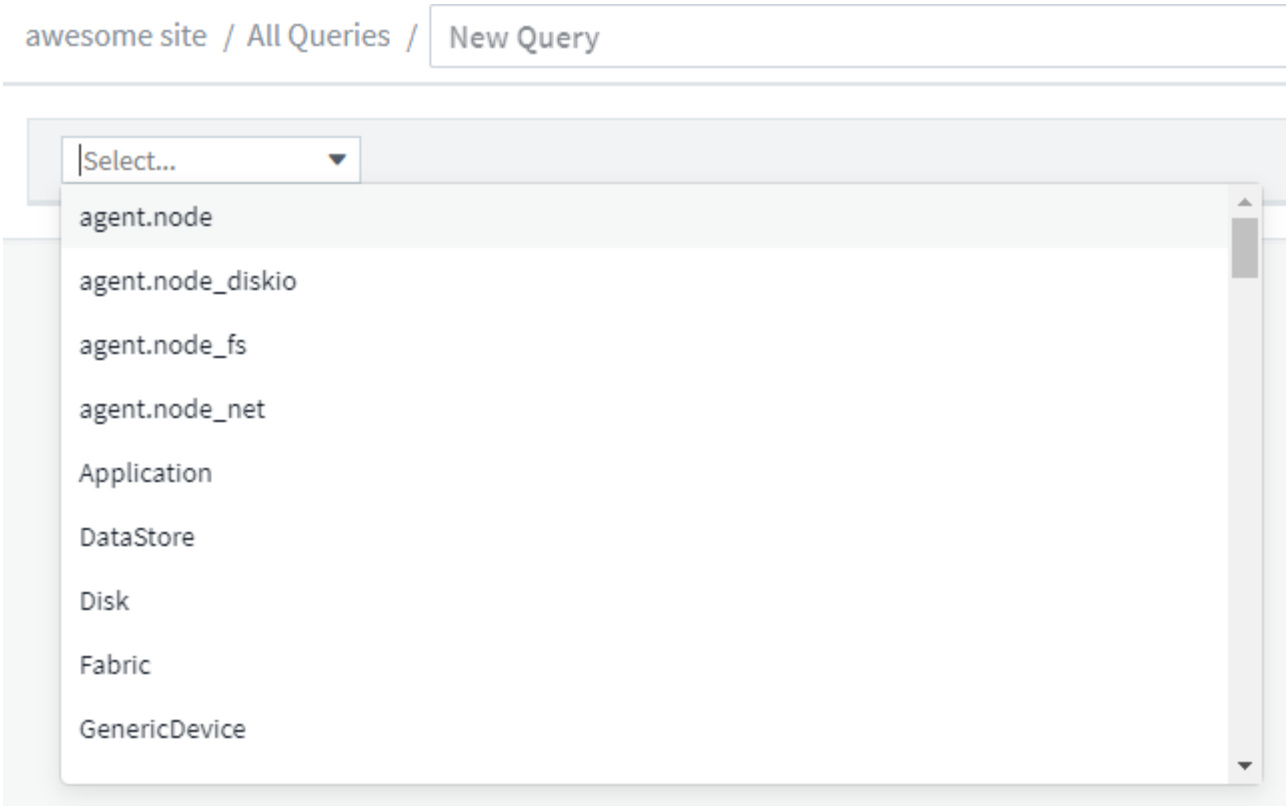
たとえば、 _VOLUMES _ のクエリを作成し、選択したボリュームに関連付けられている特定の _クエリ を検索するフィルタを追加し、選択したボリュームで「 Tier 1 」などの特定の _annotation_associated を検索するフィルタをもう 1 つ追加できます。 最後に、 _iops-Read （ IO/s ） _greater が 25 を超えるすべてのストレージを検索するフィルタを追加します。結果が表示されたら、クエリに関連付けられている各列で情報を昇順または降順にソートすることができます。

注：アセットを取得する新しいデータコレクタが追加された場合、またはアノテーションやアプリケーションの割り当てが行われた場合は、クエリにインデックスが付けられたあとに初めて、それらの新しいアセット、アノテーション、またはアプリケーションを照会できます。インデックス作成は、定期的にスケジュールされた間隔で、またはアノテーションルールの実行などの特定のイベント中に実行されます。

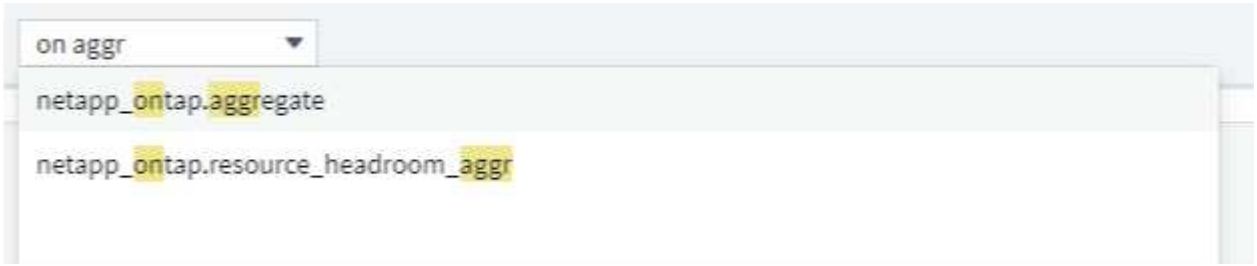
クエリの作成は非常に簡単です。

1. [クエリ] 、 [* + 新しいクエリ *] の順に移動します。
2. [選択 …] リストから、照会するオブジェクトタイプを選択する。リストをスクロールしたり、入力を開始して検索対象をすばやく見つけることができます。

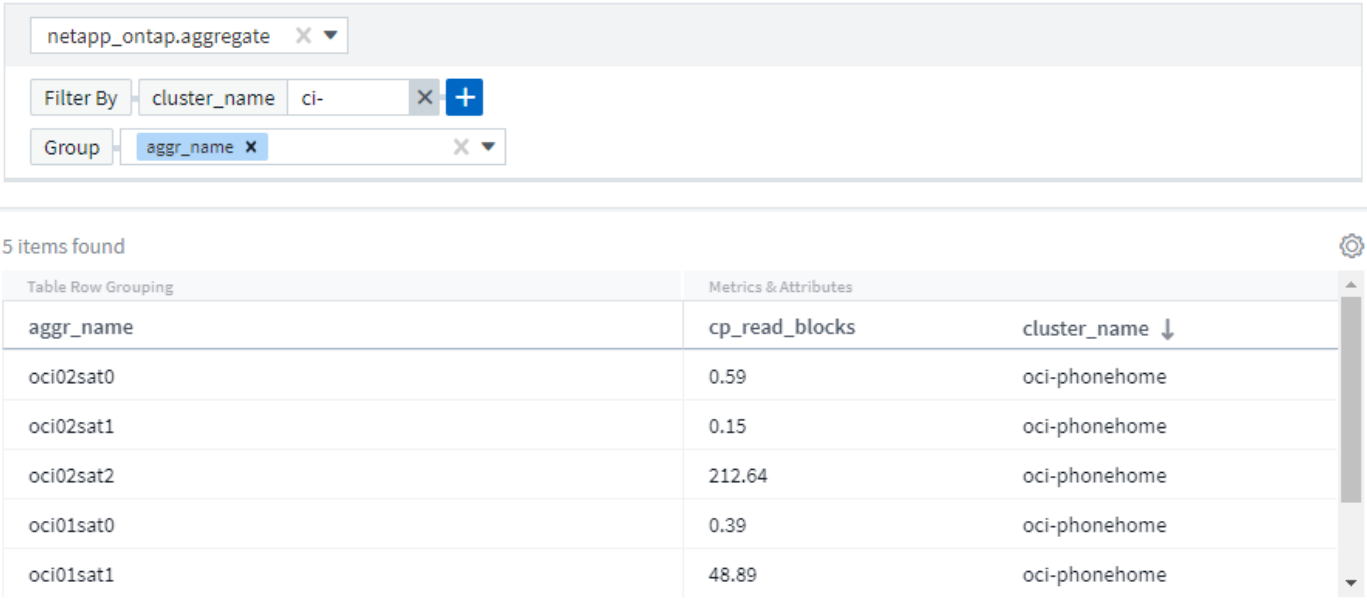
スクロールリスト：



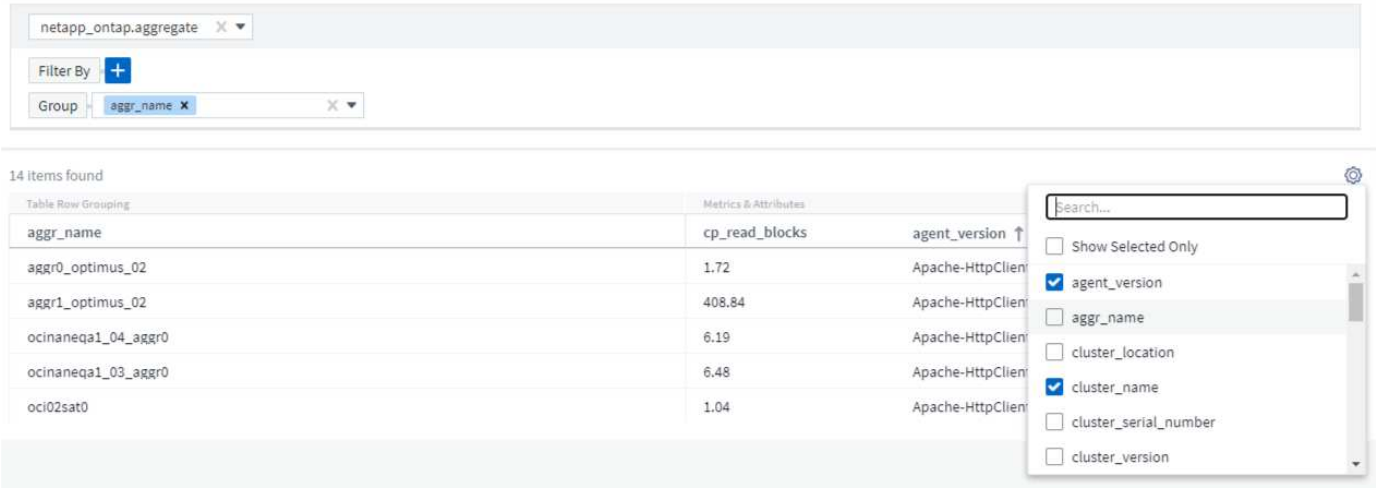
検索タイプ：



フィルタを追加して、 [* フィルタ条件 *] フィールドの [+] ボタンをクリックすると、クエリをさらに絞り込むことができます。
行をオブジェクトまたは属性でグループ化します。統合データ（ Kubernetes 、 ONTAP Advanced Metrics など）を使用する場合は、必要に応じて複数の属性でグループ化できます。



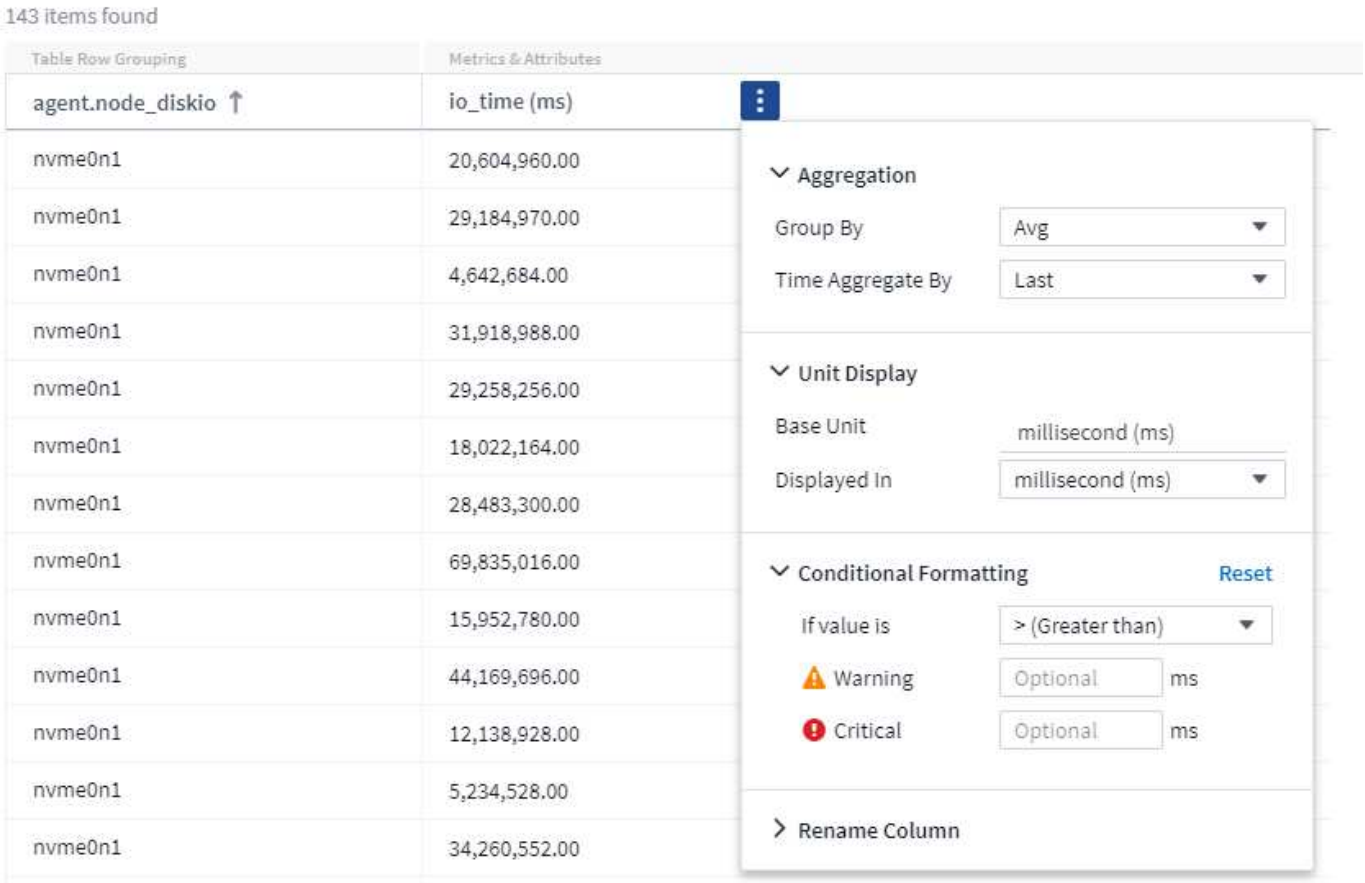
クエリ結果リストには、検索対象のオブジェクトタイプに応じていくつかのデフォルト列が表示されます。列を追加、削除、または変更するには、テーブルの右側にある歯車アイコンをクリックします。使用可能な列は、アセット / 指標タイプによって異なります。



[集計]、[単位]、[条件付き書式]の順に選択します

集計と単位

「値」列では、表示される値の集計方法を選択したり、それらの値を表示する単位を選択したりすることで、クエリ結果をさらに絞り込むことができます。これらのオプションは、列の上部にある「3つのドット」メニューを選択すると表示されます。



ページの結果には、集計、条件付き書式、単位表示、列名の変更が表示されます"]

単位（ **Units** ）

値を表示する単位を選択できます。たとえば、[Selected]列にraw容量が表示され、値の単位がGiBで表示されている場合は、[Unit Display]ドロップダウンから[TiB]を選択します。

集約

同様に、表示されている値が基になるデータから「Average」として集約されている場合、 ただし、すべての値の合計を表示する場合は、_Group by_drop（グループ化された値に合計を表示する場合）または_Time Aggregate by_drop（行の値に基礎となるデータの合計を表示する場合）から[Sum]を選択します。

グループ化されたデータポイントを_Avg、Max、Min、またはSum_で集計することができます。

個 々 の行データは、_Average、Last data point Acquired、Maximum、Minimum、またはSum_で集計できます。

条件付き書式

条件付き書式を使用すると、クエリ結果リストで警告レベルと重要レベルのしきい値を強調表示し、外れ値や例外的なデータポイントを即座に可視化できます。

条件付き書式は、列ごとに個別に設定されます。たとえば、容量列ではしきい値のセットを選択し、スループット列ではしきい値のセットを選択できます。

列名を変更します

列の名前を変更すると、[クエリ結果]リストに表示される名前が変更されます。クエリリストを.csvにエクスポートすると、新しい列名も結果のファイルに表示されます。

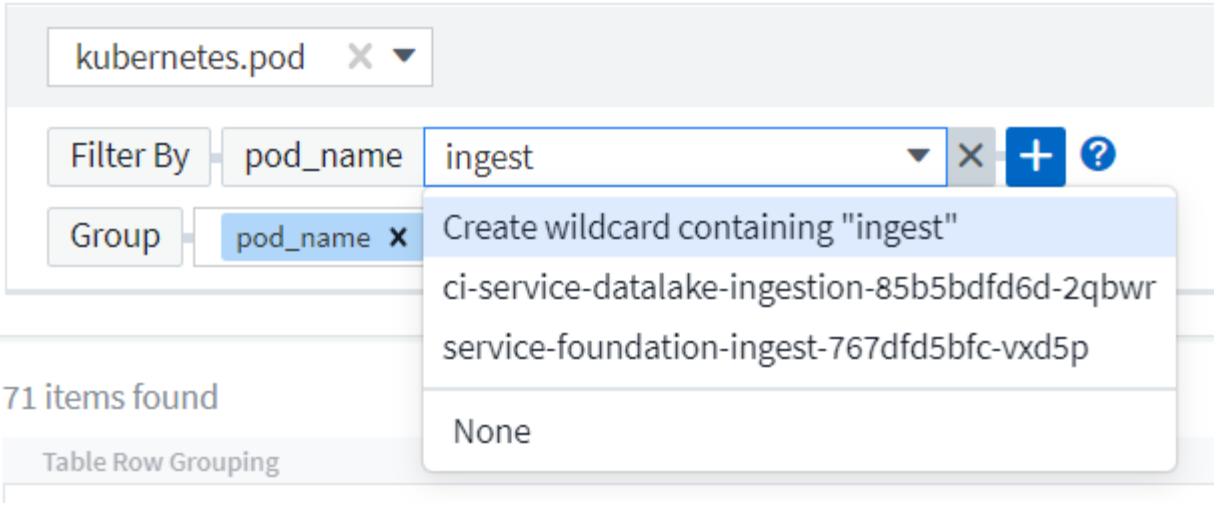
保存（**Save**）

目的の結果が表示されるようにクエリを設定したら、 * 保存 * ボタンをクリックして、クエリを保存して後で使用することができます。わかりやすい一意の名前を指定してください。

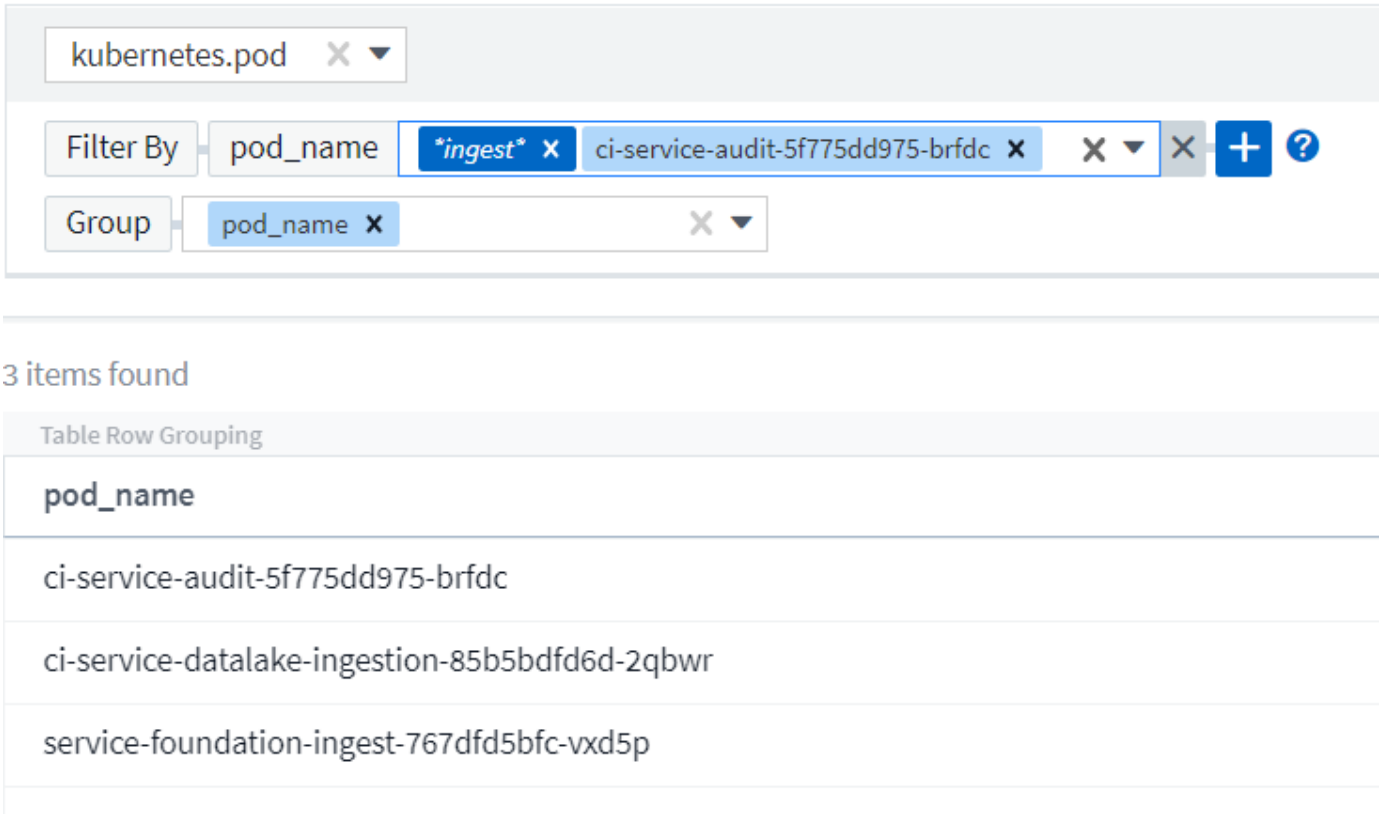
フィルタリングの詳細

ワイルドカードと式

クエリやダッシュボードウィジェットでテキストやリストの値をフィルタする場合、入力を開始すると、現在のテキストに基づいて * ワイルドカードフィルタ * を作成するオプションが表示されます。このオプションを選択すると、ワイルドカード式に一致するすべての結果が返されます。また、 NOT または OR を使用して *expressions * を作成することもできます。また、「 None 」オプションを選択して、フィールドで null 値をフィルタリングすることもできます。



ワイルドカードまたは式に基づくフィルタ（例 フィルタフィールドに濃い青で表示されます。リストから直接選択した項目は、水色で表示されます。



ワイルドカードおよび式フィルタリングは、テキストまたはリストでは機能しますが、数値、日付、またはブール値では機能しません。

フィルタの調整

次の方法でフィルタを絞り込むことができます。

フィルタ	機能	例	結果

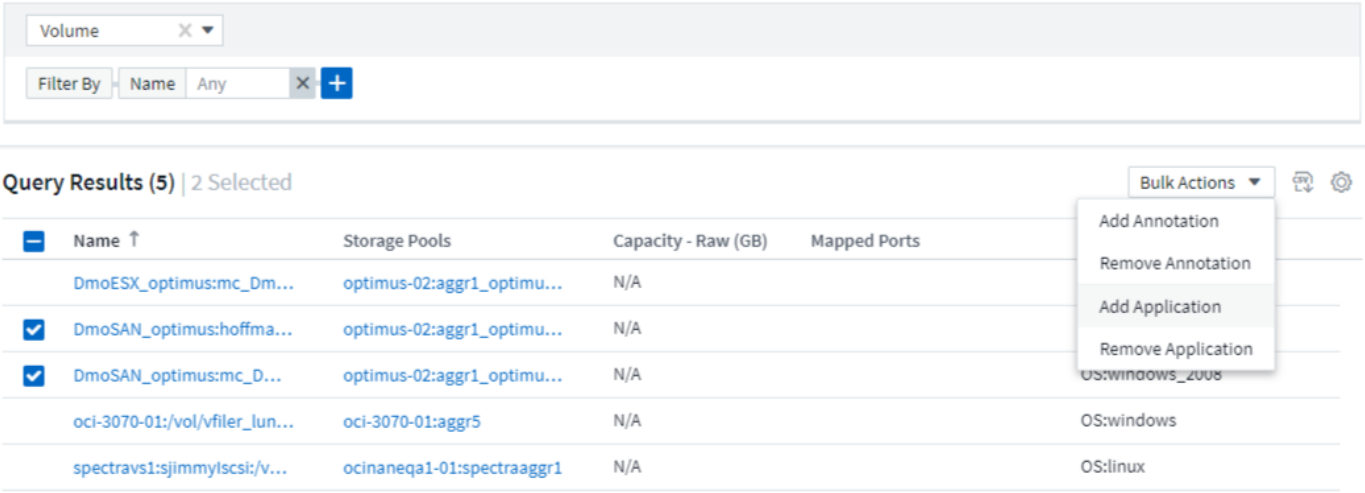
* （アスタリスク）	すべての項目を検索できます	ボリューム * RHEL	「 vol 」で始まるリソースをすべて返し、「 rhel 」で終わるリソースをすべて返します。
？（疑問符）	では、特定の数の文字を検索できます	BOS-PRD ？？ -S12	BOS-PRD ***12***-S12 、 BOS-PRD ***23***-S12 などを返します
または	複数のエンティティを指定できます	FAS2240 または CX600 または FAS3270	FAS2440 、 CX600 、または FAS3270 のいずれかを返します
ありません	検索結果からテキストを除外できます	EMC * ではありません	「 EMC 」で始まるものをすべて返します。
_ なし _	すべてのフィールドで NULL 値を検索します	_ なし _	ターゲットフィールドが空の場合に結果を返します
NOT *	_text-only_fields 内の NULL 値を検索します	NOT *	ターゲットフィールドが空の場合に結果を返します

フィルタ文字列を二重引用符で囲むと、 Insight では、最初と最後の引用符の間のすべての部分が完全に一致するものとして扱われます。引用符内の特殊文字または演算子は、リテラルとして扱われます。たとえば、「 * 」を指定した場合、リテラルアスタリスクである結果は返されますが、アスタリスクはワイルドカードとして扱われません。演算子 OR および NOT は、二重引用符で囲まれた場合にもリテラル文字列として扱われます。

クエリ結果が表示されたら、どうすればよいですか？

クエリを使用すると、アノテーションの追加やアセットへのアプリケーションの割り当てを簡単に行うことができます。インベントリアセットに割り当てることができるのは、アプリケーションやアノテーションだけです（ディスク、ストレージなど）。統合指標には、アノテーションやアプリケーションの割り当ては適用されません。

照会結果のアセットに注釈またはアプリケーションを割り当てるには、結果テーブルの左側にあるチェックボックス列を使用してアセットを選択し、右側の * 一括アクション * ボタンをクリックします。選択したアセットに適用するアクションを選択します。



アノテーションルールではクエリが必要です

を設定する場合 "アノテーションルール"を使用するには、各ルールに基礎となるクエリが必要です。しかし、前述のように、クエリは必要に応じて広範囲に、または限定されています。

クエリを表示する

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

手順

1. Data Infrastructure Insightsテナントにログインします。
2. [* クエリ *] をクリックし、 [* すべてのクエリを表示 *] を選択します。
   クエリの表示方法は次のいずれかの方法で変更できます。
3. フィルタボックスにテキストを入力すると、検索して特定のクエリを表示できます。
4. 列見出しで矢印をクリックすると、クエリの表内の列のソート順序を昇順（上矢印）または降順（下矢印）に変更できます。
5. 列のサイズを変更するには、列見出しの上にカーソルを合わせ、青いバーが表示されるまで動かします。バーの上にマウスを置き、左右にドラッグします。
6. 列を移動するには、列ヘッダーをクリックし、左右にドラッグします。

クエリ結果をスクロールするときは、Data Infrastructure Insightsが自動的にデータコレクタにポーリングを行うため、結果が変わる可能性があることに注意してください。これにより、一部の項目が表示されなくなったり、ソート方法によっては一部の項目が順序どおりに表示されない場合があります。

クエリ結果を **.csv** ファイルにエクスポートしています

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

手順

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

   [クエリ] ページが表示されます。

3. クエリをクリックします。
4. をクリックします ボタン"] クエリ結果を .csv ファイルにエクスポートします。

.csvへのエクスポートは、ダッシュボードテーブルウィジェットの「3つのドット」メニューや、ほとんどのランディングページのテーブルでも実行できます。

エクスポートされたデータには、現在表示されているフィルタ、列、および列名が反映されます。

メモ：アセット名にカンマが含まれている場合は、アセット名を引用符で囲んでエクスポートすることで、アセット名を維持しつつ適切な .csv 形式が保たれるようになりました。

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

これを回避するには、次の手順に従って .csv を Excel にインポートします。

1. Excel で新しいシートを開きます。
2. [データ] タブで、 [テキストから] を選択します。
3. 目的の .csv ファイルを見つけて、 [インポート] をクリックします。
4. インポートウィザードで、 [区切り記号] を選択し、 [次へ] をクリックします。
5. 区切り文字に「カンマ」を選択し、「次へ」をクリックします。
6. 必要な列を選択し、列データ形式として「テキスト」を選択します。
7. 完了をクリックします。

   オブジェクトが Excel で適切な形式で表示されることを確認します。

クエリの変更または削除

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

クエリーの変更

手順

1. をクリックし、[すべてのメトリッククエリ]*を選択します。

   [クエリ] ページが表示されます。

2. クエリ名をクリックします
3. クエリに条件を追加するには、[Columns]アイコンをクリックし、リストから指標または属性を選択します。

必要な変更をすべて行ったら、次のいずれかを実行します。

- 最初に使用した名前でクエリを保存するには、「 * 保存 * 」ボタンをクリックします。
- [保存 *] ボタンの横にあるドロップダウンをクリックし、 [名前を付けて保存 *] を選択してクエリを別の名前で保存します。元のクエリは上書きされません。
- 「 * 保存 * 」ボタンの横にあるドロップダウンをクリックし、「 * 名前の変更 * 」を選択して、最初に使用したクエリ名を変更します。これにより、元のクエリが上書きされます。
- [保存 *] ボタンの横にあるドロップダウンをクリックし、 [変更を破棄 *] を選択して、クエリーを最後に保存した変更に戻します。

クエリーの削除

クエリを削除するには、「 * クエリ * 」をクリックし、「 * すべてのクエリを表示 * 」を選択して、次のいずれかの操作を行います。

1. クエリの右側にある 3 つのドットメニューをクリックし、 * 削除 * をクリックします。
2. クエリ名をクリックし、 * 保存 * ドロップダウンメニューから * 削除 * を選択します。

テーブル値をコピーしています

テーブルの値をクリップボードにコピーして、検索ボックスやその他のアプリケーションで使用することができます。

このタスクについて

テーブルまたはクエリ結果からクリップボードに値をコピーする方法は 2 つあります。

手順

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

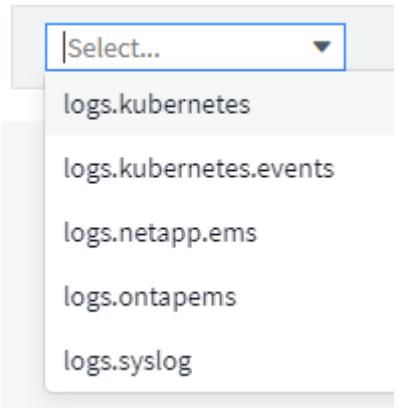
   このメソッドを使用してコピーできるのは、アセットへのリンクである値のみです。コピーアイコンは、単一の値（リスト以外）を含むフィールドのみに表示されます。

ログエクスプローラ

Data Infrastructure Insightsのログエクスプローラは、システムログを照会するための強力なツールです。検査に役立つだけでなく、ログクエリーをモニタに保存して、特定のログトリガーがアクティブになったときにアラートを生成することもできます。

ログの検索を開始するには、*[Log Queries]>[+New Log Query]*をクリックします。

リストから使用可能なログを選択します。

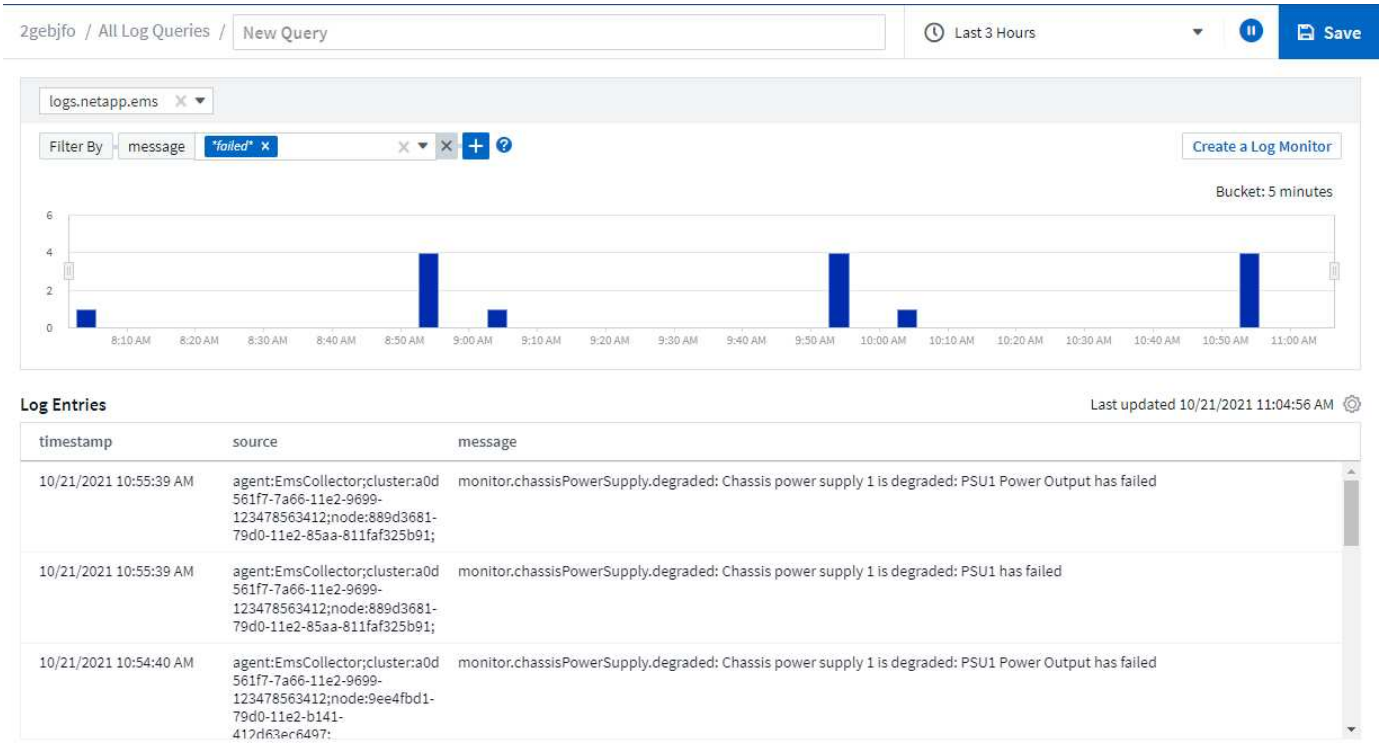


クエリに使用できるログの種類は環境によって異なります。ログタイプは、時間が経過すると追加される場合があります。

フィルタを設定して、クエリの結果をさらに絞り込むことができます。たとえば、障害を示すすべてのログ・メッセージを検索するには、「 failed 」という単語を含む *Messages* のフィルタを設定します。

フィルタフィールドには、必要なテキストの入力を開始できます。Data Infrastructure Insights では、入力時に文字列を含むワイルドカード検索を作成するよう求められます。

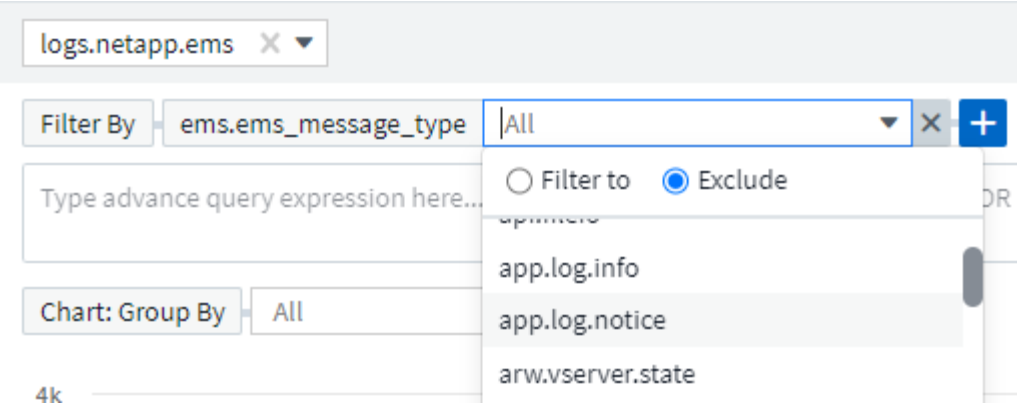
結果は、表示される各期間のログインスタンスの数を示すグラフに表示されます。グラフの下には、自分のログエントリが表示されます。グラフとエントリは、選択した期間に基づいて自動的に更新されます。



フィルタリング

含める/除外する

ログをフィルタリングするときは、入力した文字列を*含める*（「フィルタする」など）または*除外*にすることができます。除外された文字列は、完了したフィルタに「Not <string>」と表示されます。



ワイルドカードまたは式に基づくフィルタ（例 フィルタフィールドに濃い青で表示されます。リストから直接選択した項目は、水色で表示されます。

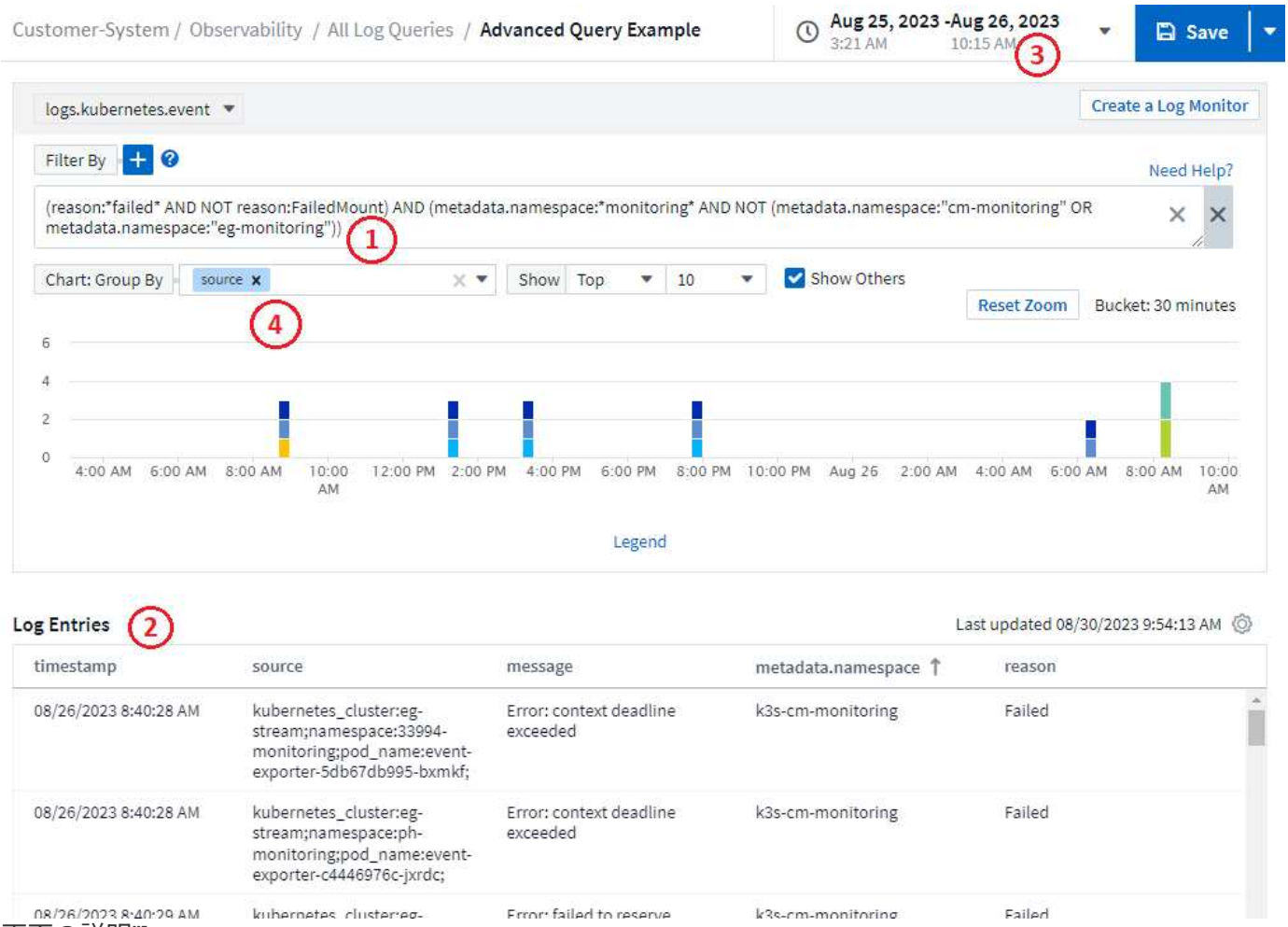
[ログモニタの作成] をクリックすると、現在のフィルタに基づいて新しいモニタを作成できます。

高度なフィルタリング

クエリやダッシュボードウィジェットでテキストやリストの値をフィルタする場合、入力を開始すると、現在のテキストに基づいて * ワイルドカードフィルタ * を作成するオプションが表示されます。このオプションを選択すると、ワイルドカード式に一致するすべての結果が返されます。NOT、AND、ORを使用して式を作成することもできます。また、[None]オプションを選択してnull値をフィルタリングすることもできます。

フィルタリングを構築するときは、クエリを早期に頻繁に保存するようにしてください。高度なクエリは「自由形式」の文字列エントリであり、ビルド中に解析ミスが発生する可能性があります。

この画面の画像を見てください。この画像は、_logs.kubernetes.event_logの高度なクエリのフィルタリングされた結果を示しています。このページでは多くのことが行われています。これについては、画像の下で説明します。

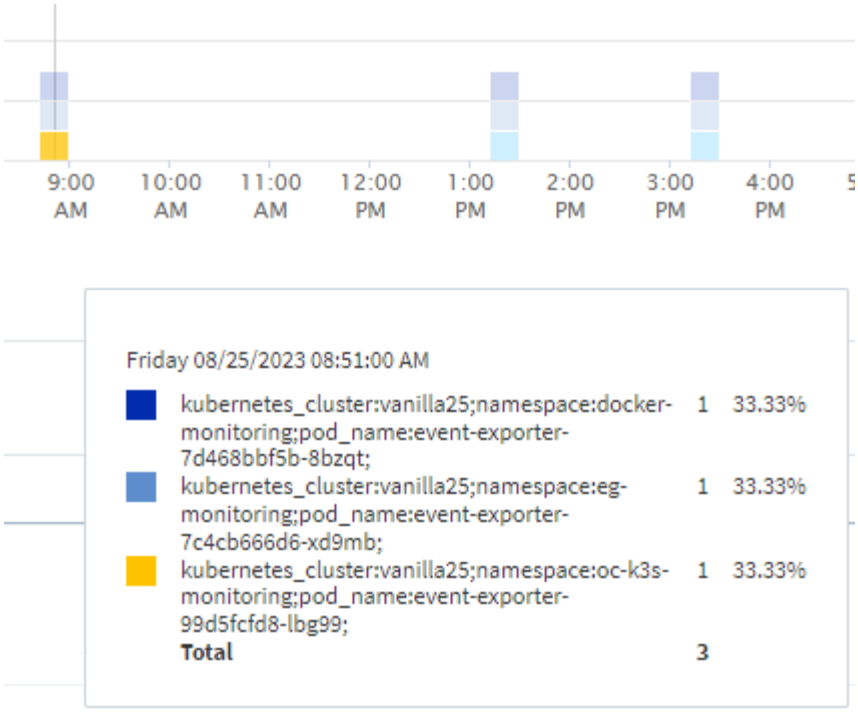


画面の説明"]

1. この高度なクエリー文字列フィルタは、次の項目に対して適用されます。
   - 「failed」という単語を含む_reason_のログエントリをフィルタリングしますが、特定の理由が「FailedMount」のログエントリはフィルタリングしません。
   - 「monitoring」という単語を含む_metadata.namespace_を含むエントリのいずれかを含めますが、「cm-monitoring」または「eg-monitoring」の特定の名前空間は除外します。

     上記の場合、"cm-monitoring"と"eg-monitoring"の両方にダッシュが含まれているため、文字列を二重引用符で囲む必要があります。そうしないと、解析エラーが表示されます。ダッシュ、スペースなどを含まない文字列は、引用符で囲む必要はありません。疑わしい場合は、文字列を引用符で囲みます。

2. 現在のフィルタの結果（[Filter By]の値や[Advanced Query]のフィルタなど）が結果リストに表示されます。リストは、表示されている任意の列でソートできます。追加の列を表示するには、「歯車」アイコンを選択します。
3. グラフが拡大され、特定の期間内に発生したログ結果のみが表示されるようになりました。ここに表示されている時間範囲は、現在のズームレベルを反映しています。[*Reset Zoom*]ボタンを選択して、ズームレベルを現在のData Infrastructure Insightsの時間範囲に戻します。
4. グラフの結果は、_source_fieldでグループ化されています。グラフには、各列の結果が色別にグループ化されて表示されます。グラフの列にカーソルを合わせると、特定のエントリに関する詳細が表示されます。



フィルタの調整

次の方法でフィルタを絞り込むことができます。

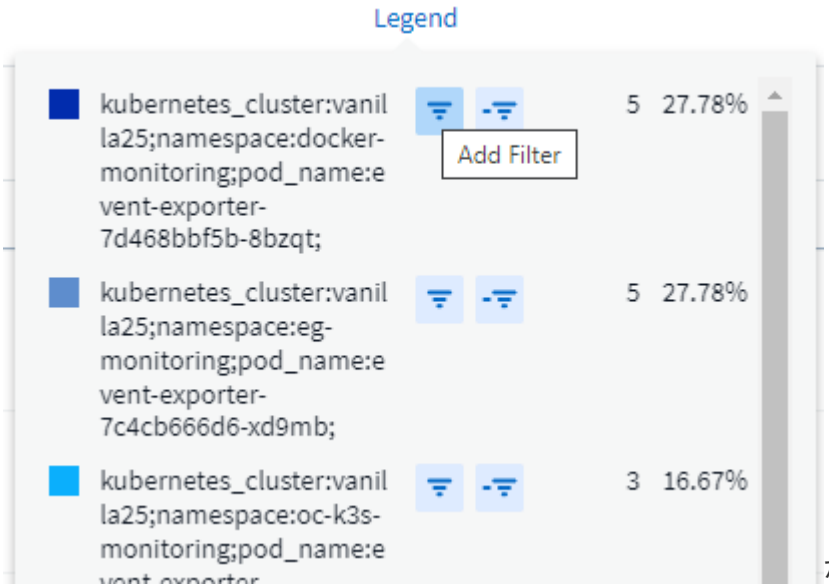
フィルタ	機能
* （アスタリスク）	すべての項目を検索できます
？（疑問符）	では、特定の数の文字を検索できます
または	複数のエンティティを指定できます
ありません	検索結果からテキストを除外できます
_ なし _	すべてのフィールドで NULL 値を検索します
NOT *	_text-only_fields 内の NULL 値を検索します

フィルタ文字列を二重引用符で囲むと、 Insight では、最初と最後の引用符の間のすべての部分が完全に一致するものとして扱われます。引用符内の特殊文字または演算子は、リテラルとして扱われます。たとえば、「 * 」を指定した場合、リテラルアスタリスクである結果は返されますが、アスタリスクはワイルドカードとして扱われません。演算子 OR および NOT は、二重引用符で囲まれた場合にもリテラル文字列として扱われます。

単純なフィルタと高度なクエリフィルタを組み合わせることができます。結果のフィルタは、2つのうちの「AND」になります。

グラフの凡例

グラフの下の_凡例_にもいくつかの驚きがあります。凡例に表示される結果ごとに（現在のフィルタに基づいて）、その行の結果のみを表示するオプション（フィルタの追加）、またはその行以外の結果を表示するオプション（除外フィルタの追加）があります。グラフと[ログエントリ]リストが更新され、選択した結果が表示されます。 このフィルタリングを削除するには、凡例をもう一度開き、[X]を選択して凡例ベースのフィルタをクリアします。

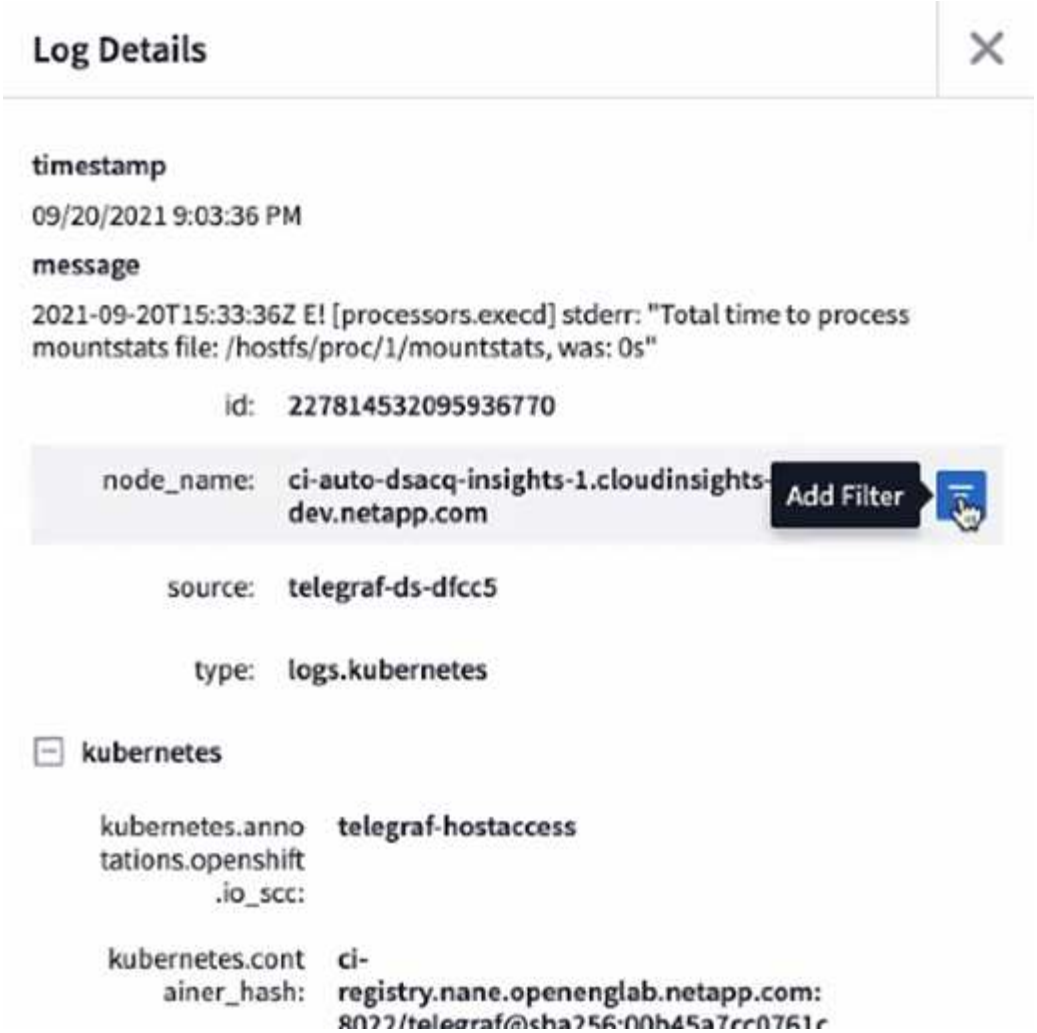


が表示されているAdvanced Queryの凡例"]

ログの詳細

リスト内のログエントリの任意の場所をクリックすると、そのエントリの詳細ペインが開きます。 ここでは、イベントに関する詳細を確認できます。

[フィルタの追加] をクリックして、選択したフィールドを現在のフィルタに追加します。ログエントリリストは、新しいフィルタに基づいて更新されます。



トラブルシューティング

ここでは、ログクエリに関する問題のトラブルシューティング方法を説明します。

* 問題： *	* これを試みなさい : *
ログクエリに「デバッグ」メッセージが表示されません	デバッグログのメッセージが収集されません。必要なメッセージをキャプチャするには、関連するメッセージの重大度を _INFORMATIONAL 、 ERROR 、 ALERT 、 EMERGENCY 、 _OR_NOTICE レベルに変更します。

分析

分析

分析情報を使用すると、リソースの使用状況や他のリソースへの影響、時間のかかる分析などを確認できます。

さまざまなインサイトをご利用いただけます。[Dashboards]>[Insights（インサイト）]に移動して、ダイビングを開始します。 アクティブなインサイト（現在発生しているインサイト）は、メインタブで表示するか、

非アクティブなインサイト（_Inactive Insights）タブで表示できます。非アクティブなインサイトとは、以前はアクティブだったものの、もう発生していないインサイトです。

Insightのタイプ

負荷のある共有リソース

影響の大きいワークロードは、共有リソース内の他のワークロードのパフォーマンスを低下させる可能性があります。これにより、共有リソースに負荷がかかります。Data Infrastructure Insightsは、リソースの飽和状態や環境への影響を調査するのに役立つツールを提供します。"詳細はこちら。"

Kubernetesネームスペースのスペースが不足しています

スペース不足Insightで実行されているKubernetesネームスペースのワークロードについて、スペース不足になる可能性がある状況をKubernetesネームスペースで確認できます。各スペースがフルになるまでの推定日数も示されます。 "詳細はこちら。"

ONTAP コールドストレージを再利用します

ONTAP コールドストレージの再利用_Insightは、ONTAP システム上のボリュームについて、コールド容量、潜在的なコスト/電力削減、推奨される対処方法に関するデータを提供します。 "詳細はこちら。"

これは_Preview_featureであり、改善が行われると時間の経過とともに変更される場合があります。"詳細はこちら。" Data Infrastructure Insightsプレビュー機能について

知見：ストレスのある共有リソース

影響の大きいワークロードは、共有リソース内の他のワークロードのパフォーマンスを低下させる可能性があります。これにより、共有リソースに負荷がかかります。Data Infrastructure Insightsは、リソースの飽和状態や環境への影響を調査するのに役立つツールを提供します。

用語集

ワークロードやリソースへの影響について話すときは、次の定義が役立ちます。

要求の厳しいワークロードとは、共有ストレージプール内の他のリソースに影響を与えていると現在特定されているワークロードのことです。これらのワークロードは IOPS を高め（など）、影響を受けるワークロードの IOPS を削減します。要求の厳しいワークロードは _ 高消費のワークロード _ と呼ばれることもあります。

「 Impacted Workload 」は、共有ストレージプール内の負荷の高いワークロードによる影響を受けます。このようなワークロードでは、要件の厳しいワークロードが原因で IOPS やレイテンシが低下しています。

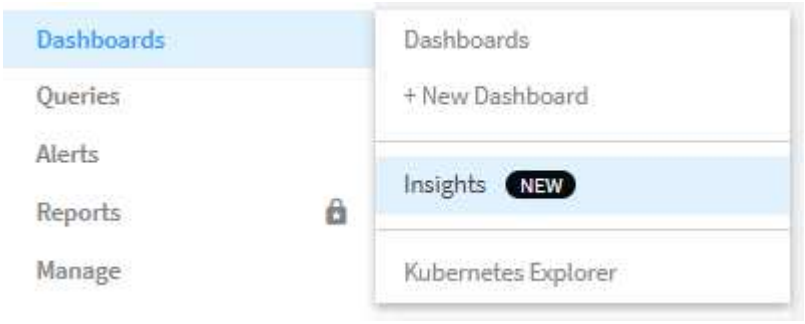
Data Infrastructure Insightsが業界をリードするコンピューティングワークロードを検出していない場合は、ボリュームまたは内部ボリューム自体がワークロードとして認識されることに注意してください。この環境は、要求の厳しいワークロードでも影響を受けやすいワークロードでも

- 共有リソースの飽和 * は、 *BASELINE* に影響する IOPS の比率です。
- ベースライン * は、検出された飽和状態に直前の 1 時間における各ワークロードのレポートされる最大データポイントです。

競合 * または飽和 * は、 IOPS が共有ストレージプール内の他のリソースまたはワークロードに影響していると判断された場合に発生します。

要件の厳しいワークロード

共有リソースで要件の厳しいワークロードや影響を受けるワークロードの調査を開始するには、**[Dashboards]>[Insights]***をクリックし、**[Stress]**[Insight]で*[Shared Resources]を選択します。



メニュー"]

Data Infrastructure Insightsには、飽和状態が検出されたワークロードのリストが表示されます。Data Infrastructure Insightsでは、少なくとも1つの_要求の厳しいリソース_*または*_影響を受けるリソース_が検出されたワークロードが表示されます。

ワークロードをクリックすると、そのワークロードの詳細ページが表示されます。上部チャートには、競合や飽和が発生している共有リソース（ストレージプールなど）のアクティビティが表示されます。

以下の 2 つのグラフは、要件の厳しいワークロードの影響を受けやすいワークロードを示しています。

各表の下には、競合に影響を及ぼすワークロードやリソースが表示されます。 リソース（ VM など）をクリックすると、そのリソースの詳細ページが開きます。ワークロードをクリックすると、関連するポッドを示すクエリページが開きます。リンクが空のクエリを開く場合は、影響を受けるポッドがアクティブな競合の一部でなくなっている可能性があります。クエリの時間範囲を変更して、ポッドリストを表示する時間範囲を大きくすることも、よりフォーカスした時間範囲にすることもできます。

飽和状態を解決するにはどうすればよいですか？

環境内の飽和の可能性を減らすか、または排除するために、いくつかの手順を実行できます。これらは、ページの「 * + 推奨を表示」リンクを展開することで表示されます。 いくつか試してみてください。

- 高 IOPS の利用者を移動

  「 Greedy 」ワークロードを、飽和状態になっていないストレージプールに移動します。ワークロードを移動する前に、これらのプールの階層と容量を評価して、不要なコストや追加の競合を回避することをお勧めします。

- Quality of Service （ QoS ；サービス品質）ポリシーを実装する

  使用可能な十分な空きリソースを確保するためにワークロードごとに QoS ポリシーを実装すると、ストレージプールの飽和を軽減できます。これは長期的な解決策です。

- リソースを追加する

  共有リソース（ストレージプールなど）が IOPS 飽和ポイントに達した場合、プールにディスクを追加するか、より高速なディスクを追加することで、飽和状態を緩和するための十分な空きリソースが確保されます。

最後に、 [* Insight Link* のコピー] をクリックして、ページの URL をクリップボードにコピーすると、同僚と簡単に共有できます。

分析情報：**Kubernetes**ネームスペースのスペースが不足しています

環境のスペース不足は、決して良い状況ではありません。Data Infrastructure Insights は、Kubernetes永続ボリュームがフルになるまでの時間を予測するのに役立ちます。

Space_Insightで実行されている_ Kubernetes名前空間を使用すると、容量不足のリスクがあるKubernetes名

前空間のワークロードを表示できます。各永続ボリュームがいっぱいになるまでに推定される残り日数を確認できます。

このInsightを表示するには、[* Dashboards > Insights（ダッシュボード>インサイト*）]に移動します。

Kubernetes Namespaces Running Out of Space (3)

Description	Estimated Days to Full	Workloads at Risk	Detected ↓
1 workload at risk on es	35	1	2 days ago
1 workload at risk on manager	24	1	2 days ago
2 workloads at risk on cloudinsights	1	2	2 days ago

ワークロードをクリックすると、Insightの詳細ページが開きます。 このページのグラフには、ワークロード容量のトレンドと次の表が表示されます。

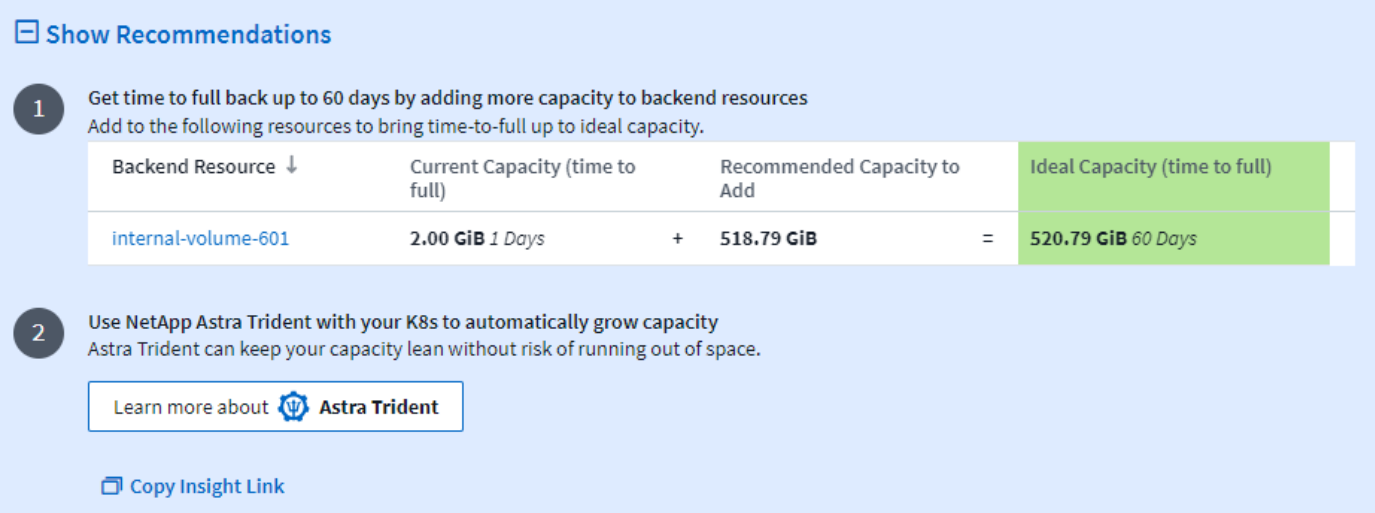
- ワークロード名
- 永続ボリュームが影響を受けます
- 予測フルまでの時間（日数）
- 永続ボリュームの容量
- バックエンドストレージリソースに影響し、現在の使用容量が合計容量を上回っています。このリンクをクリックすると、バックエンドボリュームの詳細なランディングページが表示されます。

Workloads at risk (2)

Workloads	Persistant Volume (pvClaim)	Time to Full (Days) ↓	Persistant Volume Capacity (GiB)	Backend Storage Resource (Capacity Used)	
⊞ multi (1)	pv1 (pvc1)	1	4.00	internal-volume-601	60.00% (3.00/5.00 GiB)
⊞ taskmanager (1)	pv1 (pvc1)	1	4.00	internal-volume-601	60.00% (3.00/5.00 GiB)

スペース不足になった場合はどうすればよいですか？

Insightのページで、「*+推奨事項を表示」をクリックして解決策を確認します。スペースが不足している場合の最も簡単なオプションは、常に容量を追加することです。Data Infrastructure Insightsは、追加するのに最適な容量を表示して、目標の60日間の予測に到達するまでの時間を短縮します。その他の推奨事項も表示されます。



また、このInsightへのリンクをコピーして、ページをブックマークに追加したり、チームと簡単に共有したりすることもできます。

分析情報：**ONTAP** コールドストレージの再利用

ONTAP コールドストレージの再利用_Insightは、ONTAP システム上のボリュームについて、コールド容量、潜在的なコスト/電力削減、推奨される対処方法に関するデータを提供します。

これらの分析情報を表示するには、*[Dashboards]>[Insights]*に移動し、_Reclaim ONTAP Cold Storage_Insightを確認します。このInsightでは、Data Infrastructure Insightsでコールドストレージが検出された場合にのみ、影響を受けるストレージが表示されます。検出されなかった場合は「すべてクリア」というメッセージが表示されます。

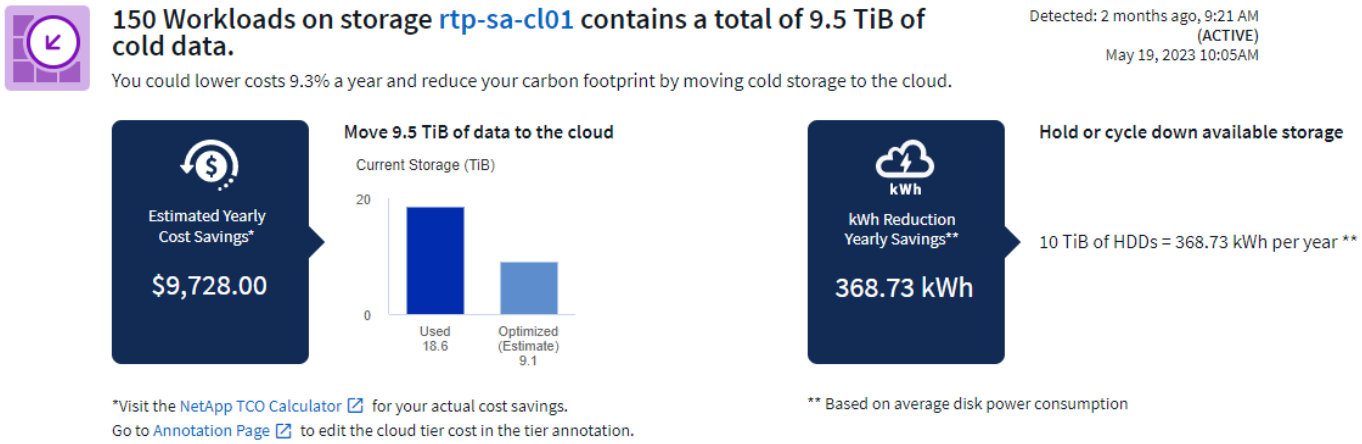
30日前に作成されたコールドデータは表示されません。

Reclaim ONTAP Cold Storage (3)

Description	Cold data storage(TiB)	Workloads with cold data	Detected
0.30 TiB of cold data on storage rtp-sa-cl04	0.30	45	an hour ago
1.22 TiB of cold data on storage umeng-aff300-01-02	1.22	84	16 days ago
11.62 TiB of cold data on storage rtp-sa-cl01	11.62	171	16 days ago

Insight概要 には、「コールド」として検出されたデータの量と、データが配置されているストレージがすぐに表示されます。このテーブルには、コールドデータを含むワークロードの数も表示されます。

リストからInsightを選択すると、詳細を示すページが開きます。これには、クラウドへのデータの移動や未使用ディスクのサイクルダウンに関する推奨事項、推奨事項の実装によって実現できる可能性のあるコスト削減と電力削減の予測などが含まれます。このページには、への便利なリンクも用意されています "ネットアップのTCO試算ツール" だからあなたは数字を試すことができます。



推奨事項

[Insight]ページで、*[推奨事項]*を展開して次のオプションを確認します。

- 未使用のワークロード（ゾンビ）を低コストのストレージ階層（HDD）に移動

  ゾンビフラグ、コールドストレージ、日数を使用して、最もコールドで最大のデータ量を特定し、低コストのストレージ階層（ハードディスクストレージを使用するストレージプールなど）にワークロードを移動します。が30日以上重大なIO要求を受信していない場合、ワークロードは「ゾンビ」とみなされます。

- 未使用のワークロードを削除

  使用されていないワークロードを確認し、アーカイブするかストレージシステムから削除することを検討してください。

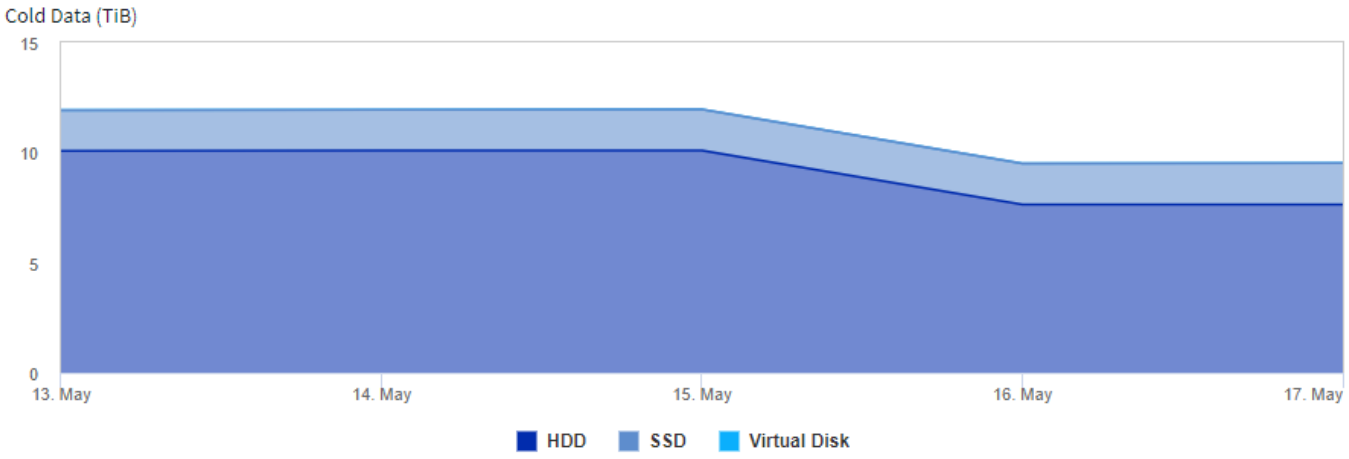
- ネットアップのFabric Pool解決策 を検討してみましょう

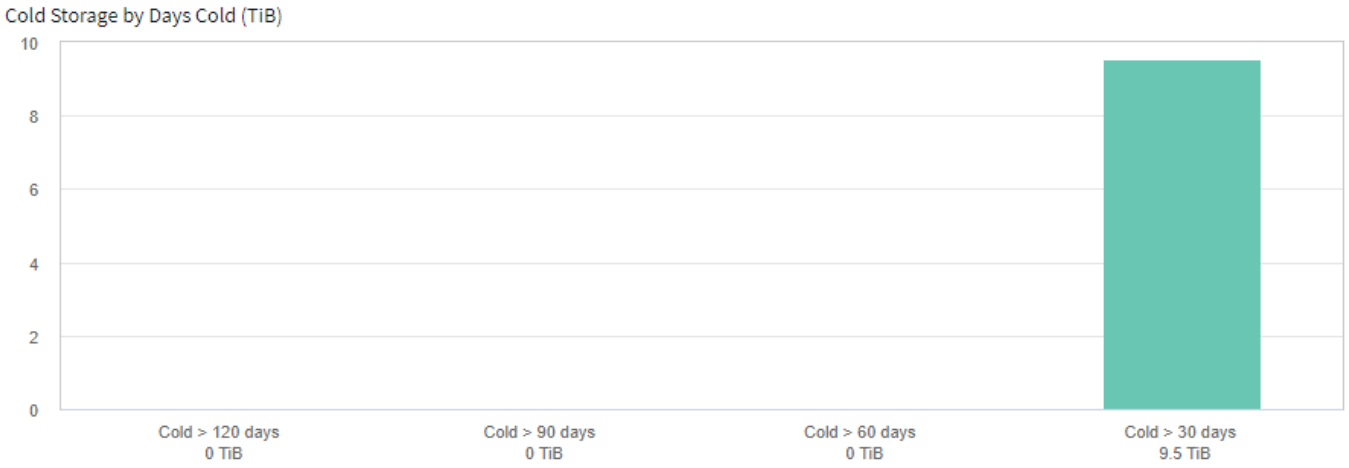
  ネットアップの "Fabric Pool解決策 の略" コールドデータを低コストのクラウドストレージに自動的に階層化することで、パフォーマンス階層の効率を高め、リモートデータ保護を実現します。

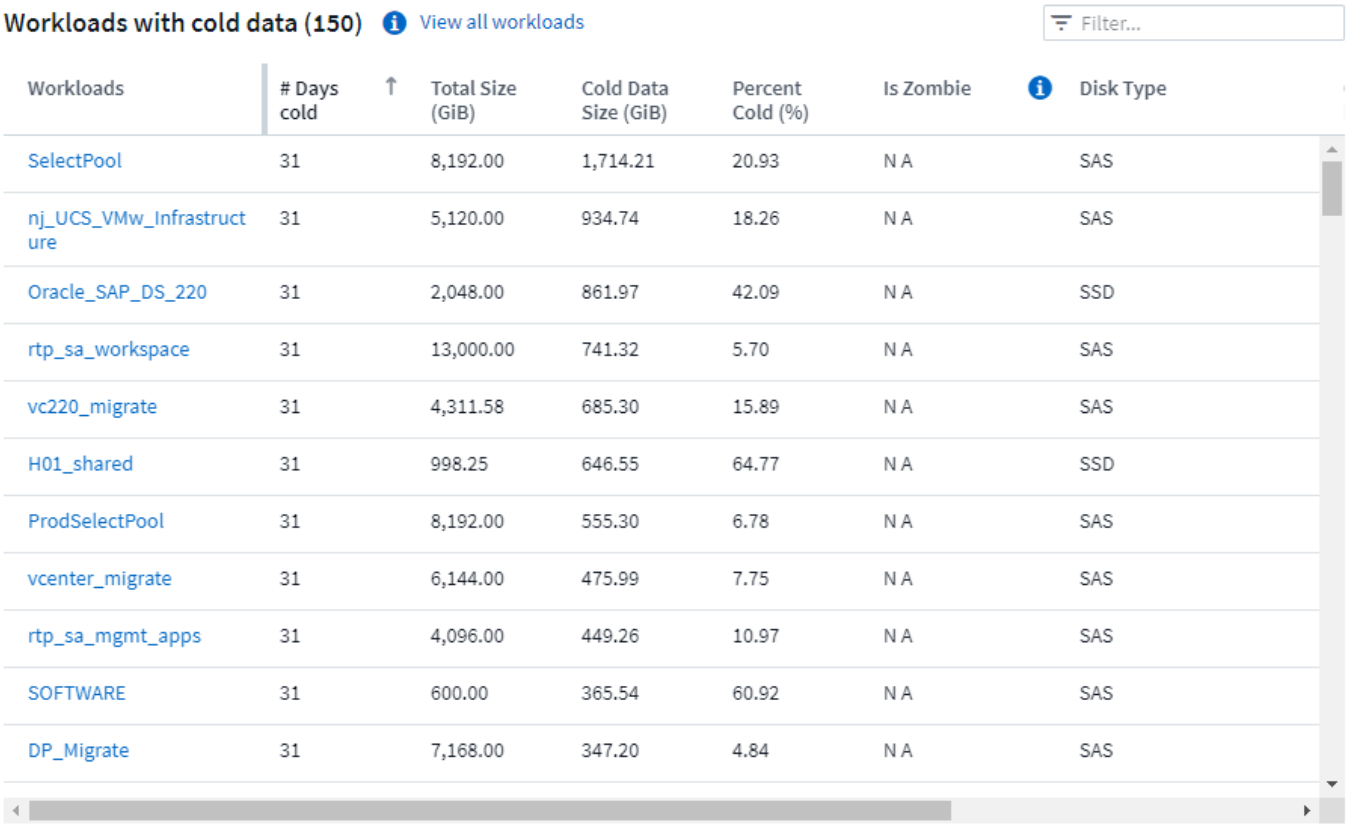
視覚化と探索

グラフと表にはトレンドに関する追加情報が表示されるほか、個 々 のワークロードにドリルダウンすることもできます。

Cluster Cold Storage Trend Show Details







Workloads with cold data (150) View all workloads

Filter...

Workloads	# Days cold	Total Size (GiB)	Cold Data Size (GiB)	Percent Cold (%)	Is Zombie	Disk Type
SelectPool	31	8,192.00	1,714.21	20.93	N A	SAS
nj_UCS_VMw_Infrastructure	31	5,120.00	934.74	18.26	N A	SAS
Oracle_SAP_DS_220	31	2,048.00	861.97	42.09	N A	SSD
rtp_sa_workspace	31	13,000.00	741.32	5.70	N A	SAS
vc220_migrate	31	4,311.58	685.30	15.89	N A	SAS
H01_shared	31	998.25	646.55	64.77	N A	SSD
ProdSelectPool	31	8,192.00	555.30	6.78	N A	SAS
vcenter_migrate	31	6,144.00	475.99	7.75	N A	SAS
rtp_sa_mgmt_apps	31	4,096.00	449.26	10.97	N A	SAS
SOFTWARE	31	600.00	365.54	60.92	N A	SAS
DP_Migrate	31	7,168.00	347.20	4.84	N A	SAS

監視とアラート

モニタとのアラート

監視を作成して、ネットワーク内のリソースに関連する問題についてユーザに通知するアラートをトリガーするしきい値を設定します。たとえば、多数のプロトコルのいずれかに対して _node write latency _ に対してアラートを送信するモニタを作成できます。

モニタとアラートはData Infrastructure Insightsのすべてのエディションで使用できますが、Basicエディションには次の条件が適用されます。一度にアクティブにできるカスタムモニタは最大**5**つまでです。**5**台を超えるモニタは、**_Paused _**状態に作成または移動されます。VMDK、仮想マシン、ホスト、データストアのメトリックモニタはサポートされていません。これらのメトリック用に作成されたモニタは一時停止され、Basic Editionにダウングレードすると再開できません。

監視を使用すると、ストレージ、 VM 、 EC2 、ポートなどの「インフラ」オブジェクトによって生成される指標や、 Kubernetes 、 ONTAP の高度な指標、 Telegraf プラグイン用に収集されたデータなどの「統合」データに対してしきい値を設定できます。これらの _ は、警告レベルまたは重大レベルのしきい値を超えたときにアラートを監視します。

また、警告レベル、重大レベル、または情報レベルのアラートをトリガーするモニタを作成して、指定された _ ログイベント _ が検出されたときに生成することもできます。

Data Infrastructure Insightsには、環境に応じて多数の機能もあり"システム定義のモニター"ます。

セキュリティのベストプラクティス

Data Infrastructure Insightsのアラートは、環境内のデータポイントやトレンドを特定するように設計されており、Data Infrastructure Insightsでは、アラート受信者として有効なEメールアドレスを入力できます。セキュアな環境で作業する場合は、通知を受け取っているユーザ、またはアラートへのアクセス権があるユーザを特に意識してください。

メトリックまたはログモニタ

1. [Data Infrastructure Insights]メニューで、*[Alerts]>[Manage Monitors]*をクリックします。

   [モニタ] リストページが表示され、現在設定されているモニタが表示されます。

2. 既存のモニタを変更するには、リストでモニタ名をクリックします。
3. モニタを追加するには、 *+ モニタ * をクリックします。

新しいモニタを追加すると、メトリックモニタまたはログモニタを作成するよう求められます。

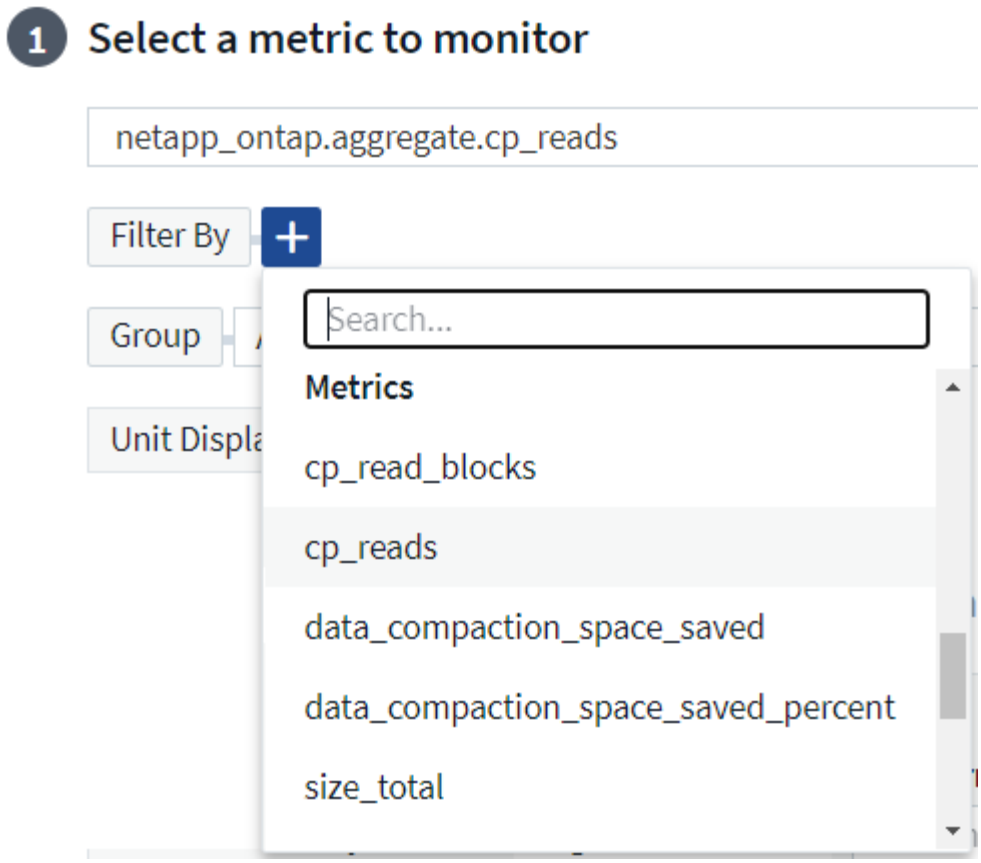
- _Metric _ は、インフラまたはパフォーマンスに関連するトリガーに関するアラートを監視します
- ログ関連のアクティビティに関するアラートを監視します

モニタタイプを選択すると、モニタ設定ダイアログが表示されます。構成は、作成するモニタのタイプによって異なります。

メートル法モニタ（ **Metric Monitor**

1. ドロップダウンで、監視するオブジェクトタイプと指標を検索して選択します。

フィルタを設定して、監視するオブジェクトの属性や指標を絞り込むことができます。



統合データ（ Kubernetes 、 ONTAP 高度なデータなど）を使用する場合、指標フィルタリングを使用すると、データ系列の集計値でフィルタが機能し、グラフからオブジェクト全体が削除されるのとは異なり、プロットされたデータ系列から個々のデータポイントや一致しないデータポイントが削除されます。

複数条件のモニタ（ IOPS > X 、レイテンシ > Y など）を作成するには、最初の条件をしきい値、 2 番目の条件をフィルタとして定義します。

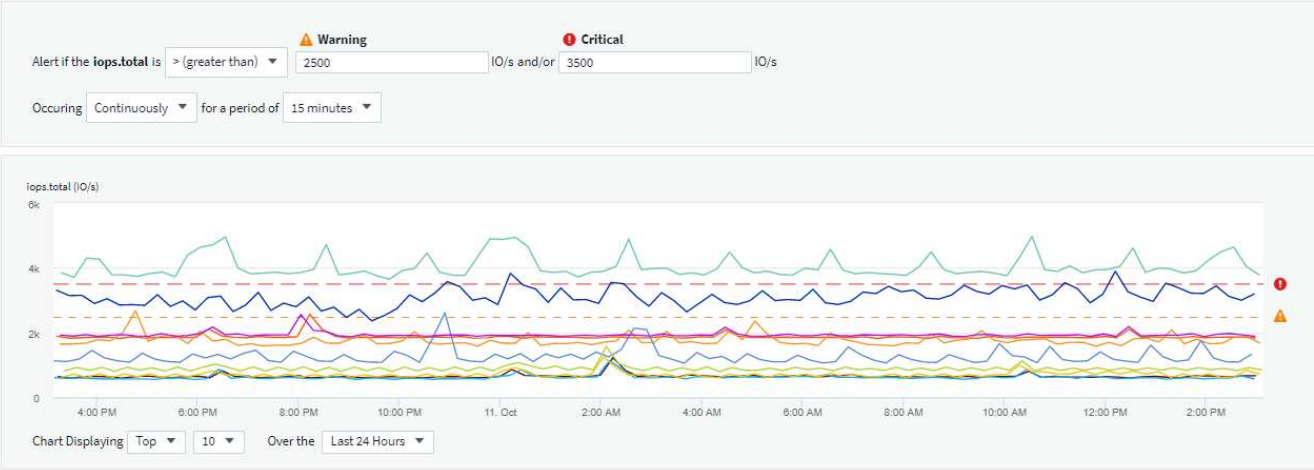
モニターの条件を定義します。

1. 監視するオブジェクトと指標を選択したら、警告レベルと重大レベルのしきい値、またはその両方を設定します。
2. _Warning_level には、この例に 200 を入力します。この警告レベルを示す破線がグラフの例に表示されます。
3. _Critical_level の場合は、 400 と入力します。このクリティカルレベルを示す破線がグラフの例に表示されます。

   このグラフには履歴データが表示されます。グラフ上の警告および重大レベルの線はモニタを視覚的に表しているため、モニタがアラートをトリガーするタイミングを簡単に確認できます。

4. 実行間隔には、 *15* 分 _ の間で _*Continuously* を選択します。

   しきい値を超えた時点でアラートをトリガーするか、しきい値が一定期間継続して違反になるまでアラートをトリガーするかを選択できます。この例では、合計 IOPS が警告レベルまたは重大レベルを超えるたびにアラートを表示する必要はありませんが、監視対象のオブジェクトがこれらのレベルの 1 つを 15 分以上継続して超えた場合にのみアラートを表示します。



アラート解決の動作を定義します

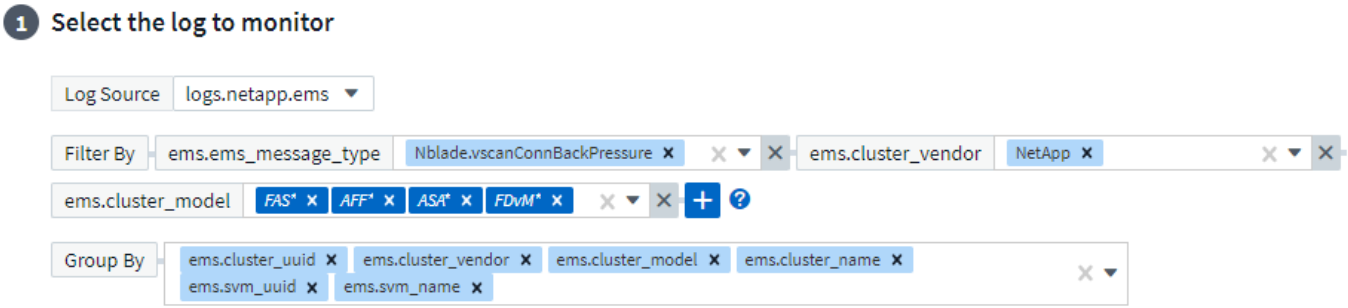
指標モニタのアラートの解決方法を選択できます。次の2つの選択肢が表示されます。

- メトリックが許容範囲に戻ったときに解決します。
- メトリックが、指定した時間（1分～7日）にわたって許容範囲内に収まった場合に解決します。

ログモニタ

*Log monitor * を作成する場合は、まず使用可能なログリストから、監視するログを選択します。次に、前述のように使用可能な属性に基づいてフィルタできます。1つ以上の「グループ化」属性を選択することもできます。

ログモニタフィルタを空にすることはできません。



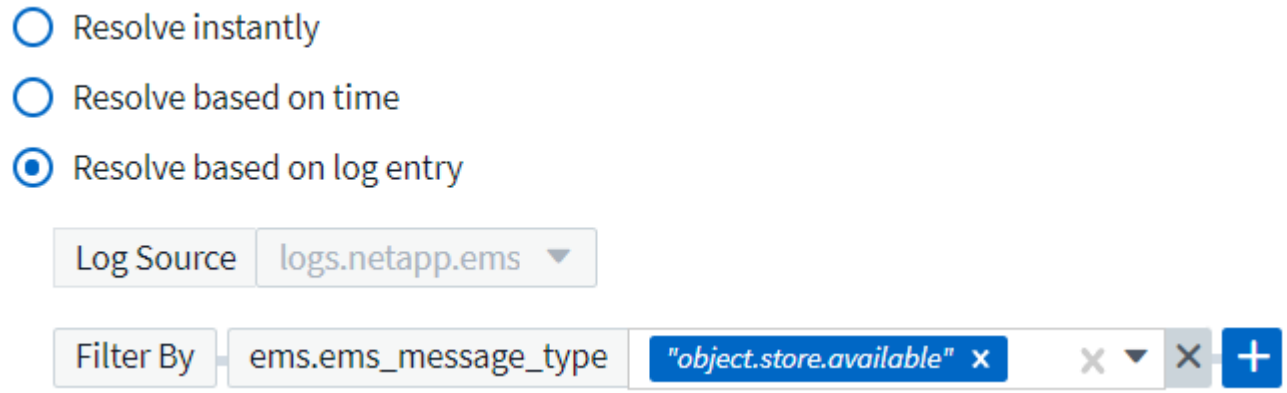
アラートの動作を定義します

上記で定義した条件が1回（即刻）発生した場合に、重大度レベル_Critical_、*Warning*、または_Informational_でアラートを生成したり、条件が2回以上発生するまでアラートを待機したりするようにモニタを作成できます。

アラート解決の動作を定義します

ログモニタのアラートの解決方法を選択できます。次の 3 つの選択肢があります。

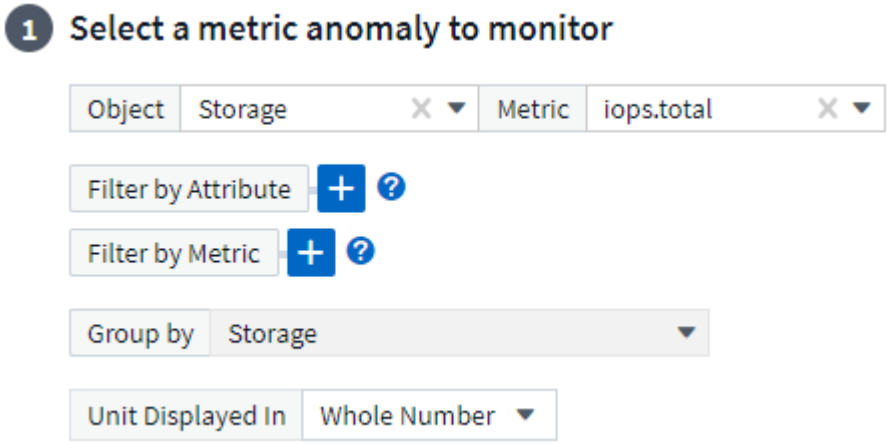
- * 即時解決 * ：このアラートは、対処不要で即座に解決されます
- * 時間に基づく解決 * ：アラートは指定した時間が経過すると解決されます
- * ログエントリに基づいて解決 * ：このアラートは、後続のログアクティビティが発生すると解決されます。たとえば、あるオブジェクトが「 available 」としてログされる場合などです。



異常検出モニタ

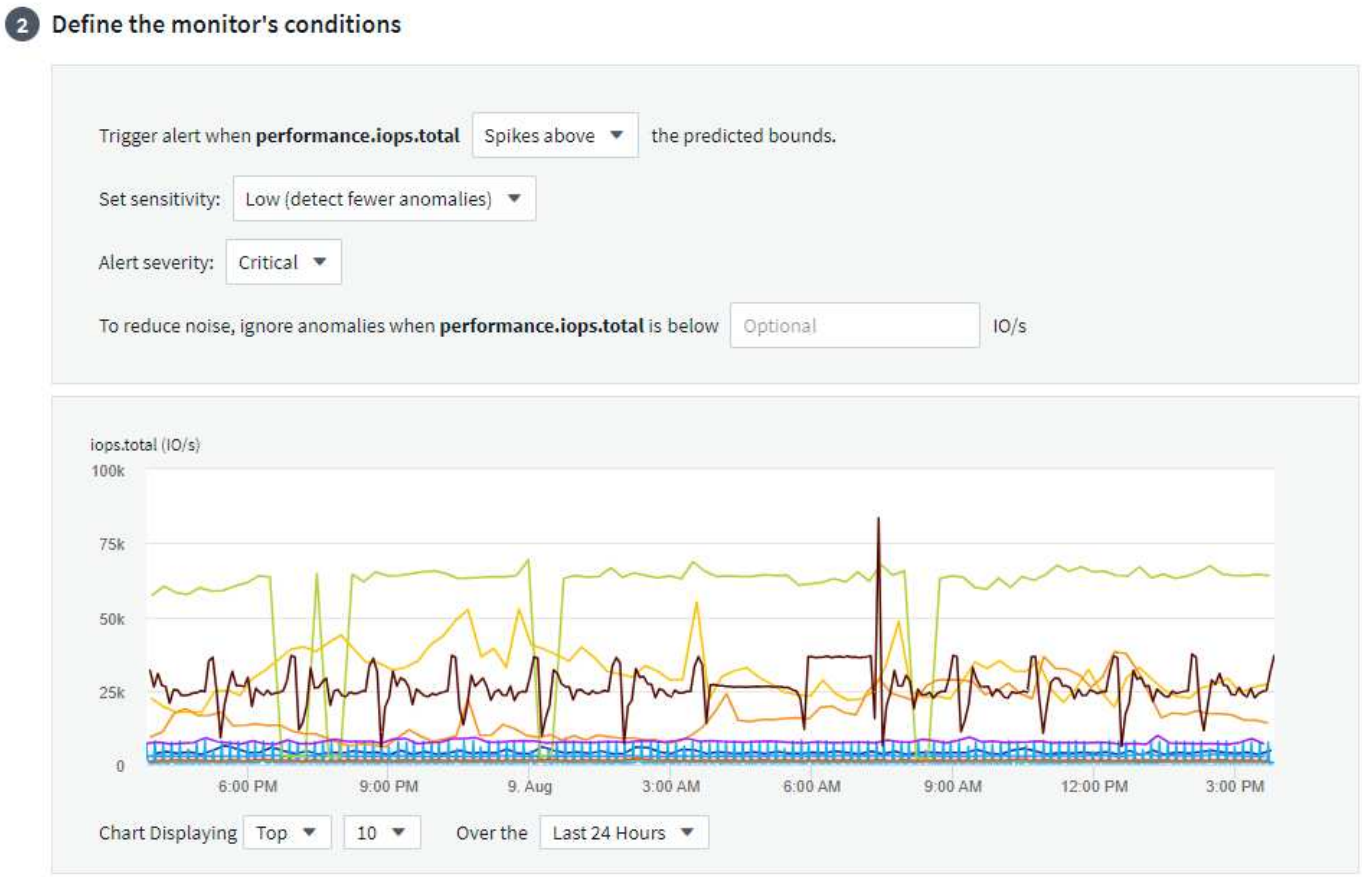
1. ドロップダウンで、監視するオブジェクトタイプと指標を検索して選択します。

フィルタを設定して、監視するオブジェクトの属性や指標を絞り込むことができます。



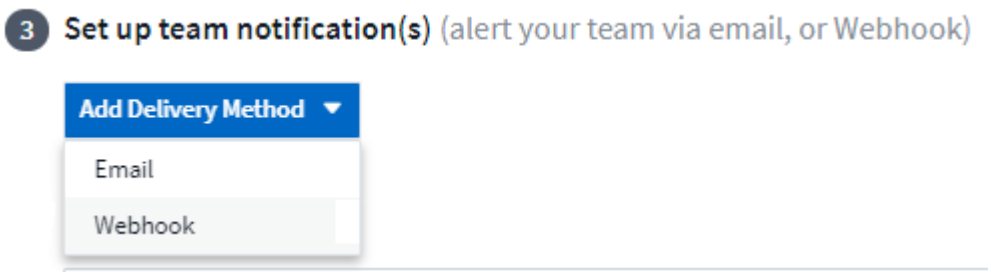
モニターの条件を定義します。

1. 監視するオブジェクトとメトリックを選択した後、異常が検出される条件を設定します。
    - 選択したメトリック*スパイクが予測された境界を超えている場合、*ドロップがそれらの境界を超えている場合、*スパイクが境界を超えている場合、または*スパイクが境界を下回っている場合に異常を検出するかどうかを選択します。
    - 検出の*感度*を設定します。低（検出される異常が少ない）、中、または*高*（検出される異常が多い）。
    - 警告をWither * Warning または Critical *に設定します。
    - 必要に応じて、選択したメトリックが設定したしきい値を下回った場合に異常を無視して、ノイズを低減するように選択できます。



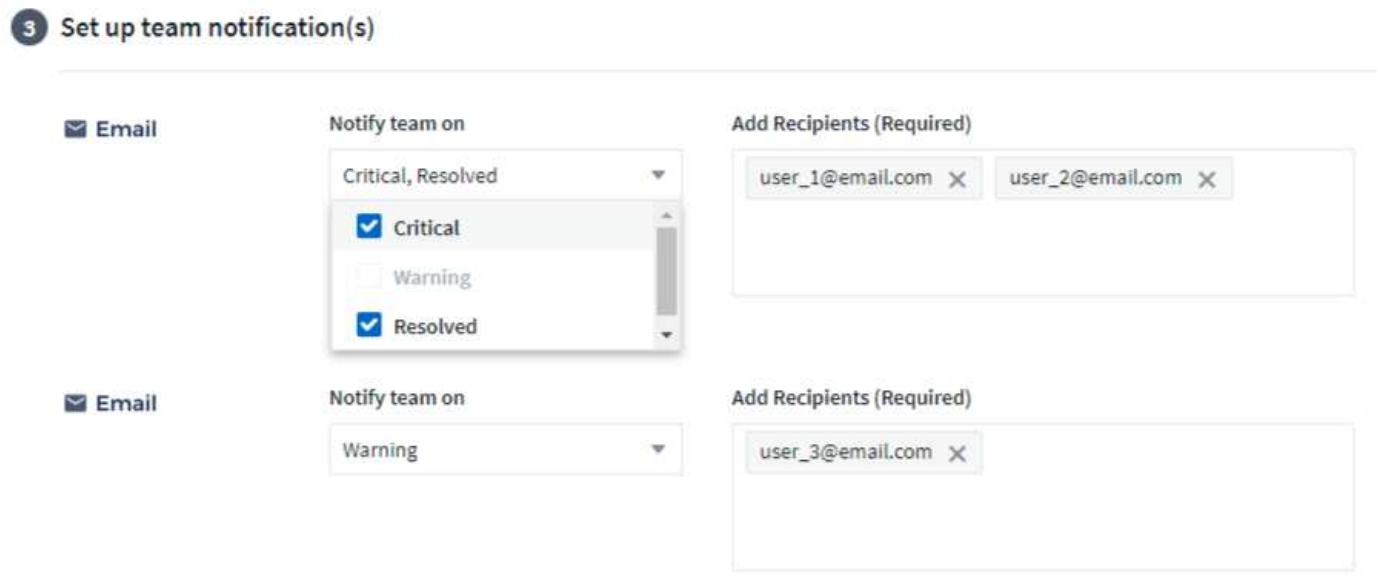
通知タイプと受信者を選択します

[チーム通知の設定] セクションでは、電子メールと Webhook のどちらでチームに通知するかを選択できます。



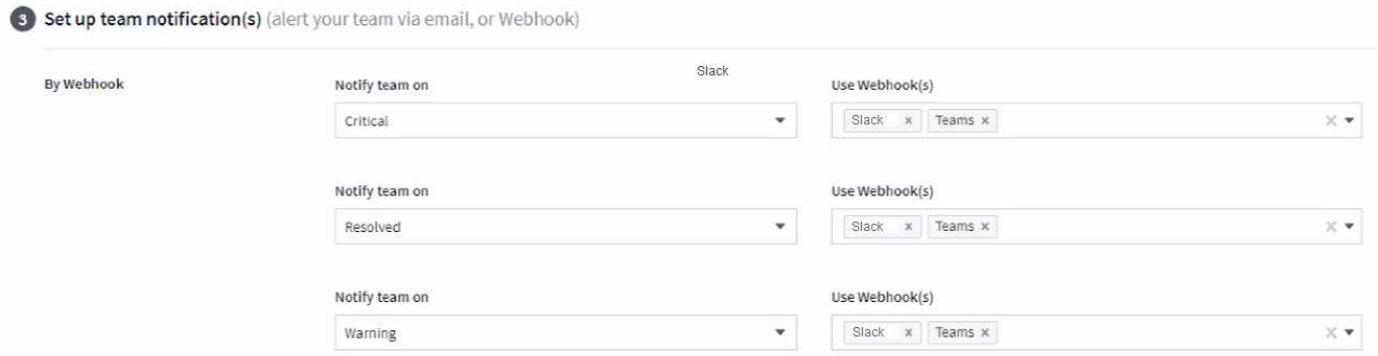
- 電子メールによる警告 :*

アラート通知の E メール受信者を指定します。必要に応じて、警告または重大なアラートの受信者を別々に選択することもできます。



- Webhook による警告 :*

アラート通知に使用する Web フックを指定します。必要に応じて、警告または重大なアラートに別のフックを選択できます。

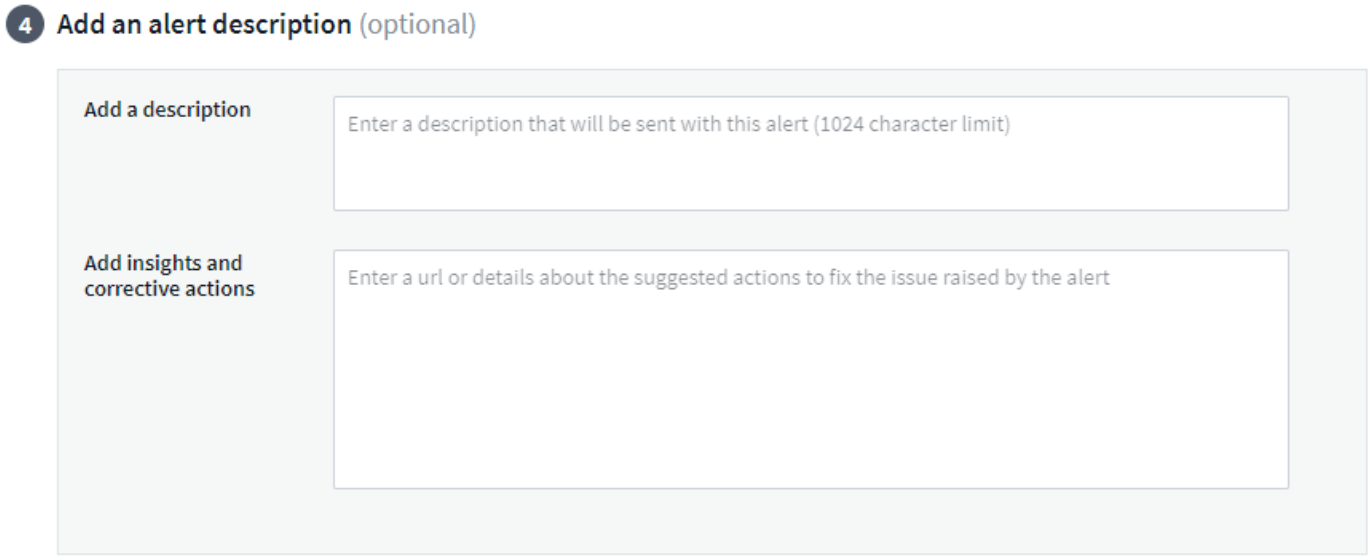


ONTAP データコレクタ通知は、クラスタ/データコレクタに関連する特定のモニタ通知よりも優先されます。Data Collector自体に設定した受信者リストには、データコレクタアラートが送信されます。アクティブなデータコレクタアラートがない場合は、監視用に生成されたアラートが特定の監視受信者に送信されます。

対処方法または追加情報を設定しています

オプションの概要を追加したり、追加のインサイトや修正アクションを追加したりするには、「 * アラート概要の追加 * 」セクションに入力します。概要は 1024 文字以内で指定し、アラートとともに送信されます。分析情報 / 対処方法のフィールドは最大 67,000 文字で、アラートランディングページの概要セクションに表示されます。

これらのフィールドには、アラートを修正したり対処したりするためのメモ、リンク、手順を入力できます。



モニタを保存します

1. 必要に応じて、モニタの概要を追加できます。
2. モニターにわかりやすい名前を付け、 * 保存 * をクリックします。

   新しいモニタがアクティブなモニタのリストに追加されます。

監視リスト

[Monitor] ページには、現在設定されているモニタが一覧表示され、次の情報が示されます

- モニタ名
- ステータス
- 監視対象のオブジェクト / 指標
- モニタの状態

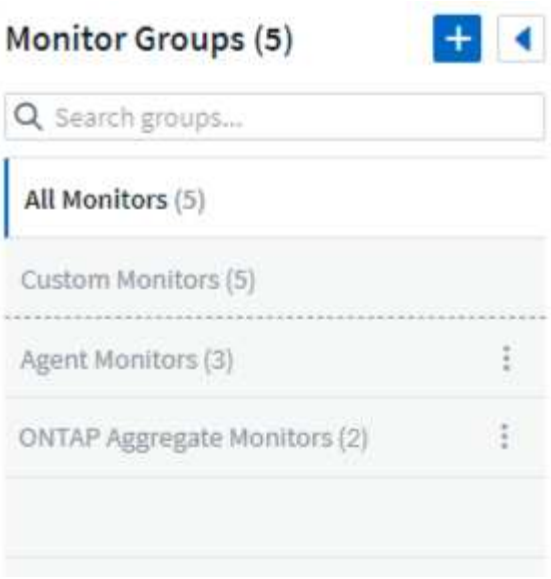
モニターの右側にあるメニューをクリックし、 * 一時停止 * を選択すると、オブジェクトタイプの監視を一時的に停止できます。モニタリングを再開する準備ができたら、 * Resume * （続行）をクリックします。

モニタをコピーするには、メニューから「 * Duplicate （複製） * 」を選択します。その後、新しいモニタを変更して、オブジェクト / 指標、フィルタ、条件、 E メール受信者などを変更できます

モニタが不要になった場合は、メニューから * Delete * を選択して削除できます。

グループを監視します

グループ化により、関連するモニタを表示および管理できます。たとえば、環境内のストレージ専用の監視グループを使用したり、特定の受信者リストに関連する監視を使用したりできます。



次のモニタグループが表示されます。グループ名の横には、グループに含まれるモニタの数が表示されます。

- * すべてのモニタ * にすべてのモニタが一覧表示されます。
- * カスタムモニター * には、ユーザーが作成したすべてのモニターが一覧表示されます。
- *一時停止中のモニター*には、Data Infrastructure Insightsによって一時停止されたシステムモニターが表示されます。
- Data Infrastructure Insightsには複数の*システム監視グループ*も表示され、"システム定義のモニタ "ONTAPインフラ監視やワークロード監視など、の1つ以上のグループが表示されます。

カスタムモニタは、一時停止、再開、削除、または別のグループへの移動が可能です。システム定義のモニタは一時停止および再開できますが、削除または移動することはできません。

一時停止したモニタ

このグループは、Data Infrastructure Insightsが1つ以上のモニタを一時停止している場合にのみ表示されます。モニタが過度のアラートまたは継続的なアラートを生成している場合、モニタが一時停止することがあります。モニタがカスタムモニタの場合は、継続的なアラートの発生を防止する条件を変更してから、モニタを再開します。問題 がサスペンションを引き起こしている状態が解消されると、モニタはサスペンド状態のモニタグループから削除されます。

システム定義のモニター

これらのグループには、監視に必要なデバイスやログの可用性が環境に含まれている限り、Data Infrastructure Insightsが提供する監視が表示されます。

システム定義のモニタは、変更、別のグループへの移動、または削除できません。ただし、システムモニタを複製して、複製を変更または移動することはできます。

システムモニタには、 ONTAP インフラストラクチャ（ストレージ、ボリュームなど）のモニタ、ワークロード（ログモニタなど）、またはその他のグループが含まれます。ネットアップでは、お客様のニーズと製品の機能を常に評価しており、必要に応じてシステムの監視やグループの更新や追加を行います。

必要に応じてモニタを含めるための独自のグループを作成できます。たとえば、すべてのストレージ関連モニタのグループを作成する場合などです。

新しいカスタムモニタグループを作成するには、「 + 」「新規モニタグループの作成 * 」ボタンをクリックします。グループの名前を入力し、 * グループの作成 * をクリックします。空のグループがその名前で作成されます。

モニタをグループに追加するには、 _all Monitors グループ（推奨）に移動し、次のいずれかの操作を行います。

- 単一のモニタを追加するには、モニタの右側にあるメニューをクリックし、 _ グループに追加 _ を選択します。モニタを追加するグループを選択します。
- モニタ名をクリックしてモニタの編集ビューを開き '*Associate to a monitor group* セクションでグループを選択します

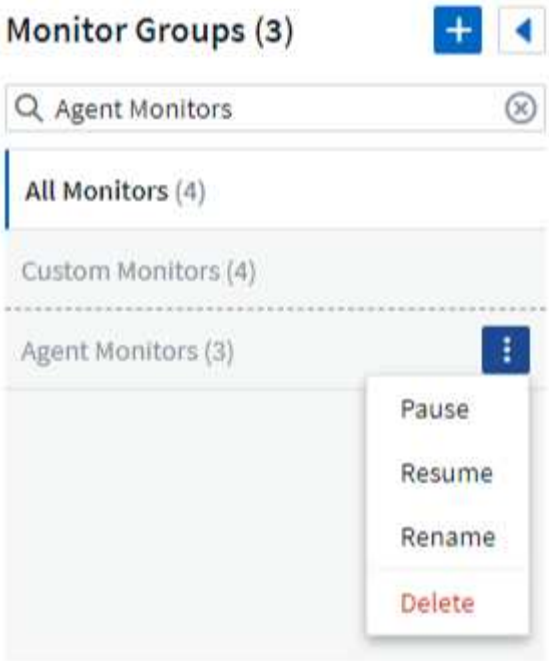
モニタを削除するには、グループをクリックし、メニューから「 _ グループから削除」を選択します。モニタを _all Monitors _ または _Custom Monitors _ グループから削除することはできませんこれらのグループからモニタを削除するには、モニタ自体を削除する必要があります。

グループからモニタを削除しても、そのモニタがData Infrastructure Insightsから削除されることはありません。モニタを完全に削除するには、モニタを選択し、 *Delete*(削除) をクリックします。これにより、その所有者であるグループからも削除され、どのユーザからも使用できなくなります。

同様にモニタを別のグループに移動するには '*Move to Group* を選択します

グループ内のすべてのモニタを一度に一時停止または再開するには、グループのメニューを選択し、 _Pause_or_Resume_を クリックします。

同じメニューを使用して、グループの名前変更または削除を行います。グループを削除しても、Data Infrastructure Insightsからモニタは削除されません。モニタは「すべてのモニタ」で引き続き使用できます。



システム定義のモニター

Data Infrastructure Insightsには、指標とログの両方について、システム定義の監視が多数含まれています。使用可能なシステムモニタは、環境内にあるデータコレクタによって異なります。そのため、Data Infrastructure Insightsで使用できるモニタは、データコレクタの追加や設定の変更に応じて変更される場合があります。

ページを表示して、Data Infrastructure Insightsに含まれるモニタの説明を確認"システム定義のモニター"します。

詳細情報

- "アラートの表示と非表示"

モニタからのアラートの表示と管理

Data Infrastructure Insightsには、超過した場合にアラートが表示され"監視対象のしきい値"ます。

監視とアラートは、Data Infrastructure Insights Standard Edition以上で利用できます。

アラートの表示と管理

アラートを表示および管理するには、次の手順を実行します。

1. [* Alerts] > [All Alerts] * ページに移動します。
2. 最新の 1 、 000 個までのアラートのリストが表示されます。フィールドの列ヘッダーをクリックすると、任意のフィールドでこのリストをソートできます。リストには、次の情報が表示されます。デフォルトでは、すべての列が表示されるわけではありません。歯車アイコンをクリックすると、表示する列を選択できます。

- * アラート ID* ：システムによって生成された一意のアラート ID
- * Triggered Time * ：該当するモニタがアラートをトリガーした時刻
- * 現在の重大度 *（アクティブなアラートタブ）：アクティブなアラートの現在の重大度
- * 重大度上位 *（解決済みアラートタブ）。解決前のアラートの最大重大度
- **Monitor** ：アラートをトリガーするように設定されたモニタ
- * triggered on * ：監視対象のしきい値に違反したオブジェクト
- * ステータス * ：現在のアラートステータス、 *New_or_in Process*
- * アクティブステータス * ： _Active_or_Resolved _
- * Condition * ：アラートをトリガーしたしきい値条件
- * Metric * ：監視対象のしきい値を超えたオブジェクトのメトリック
- **Monitor Status** ：アラートをトリガーしたモニタの現在のステータス
- * 対応処置あり * ：アラートで推奨される対処方法が提示されています。アラートページを開いて表示します。

アラートの右側にあるメニューをクリックし、次のいずれかを選択してアラートを管理できます。

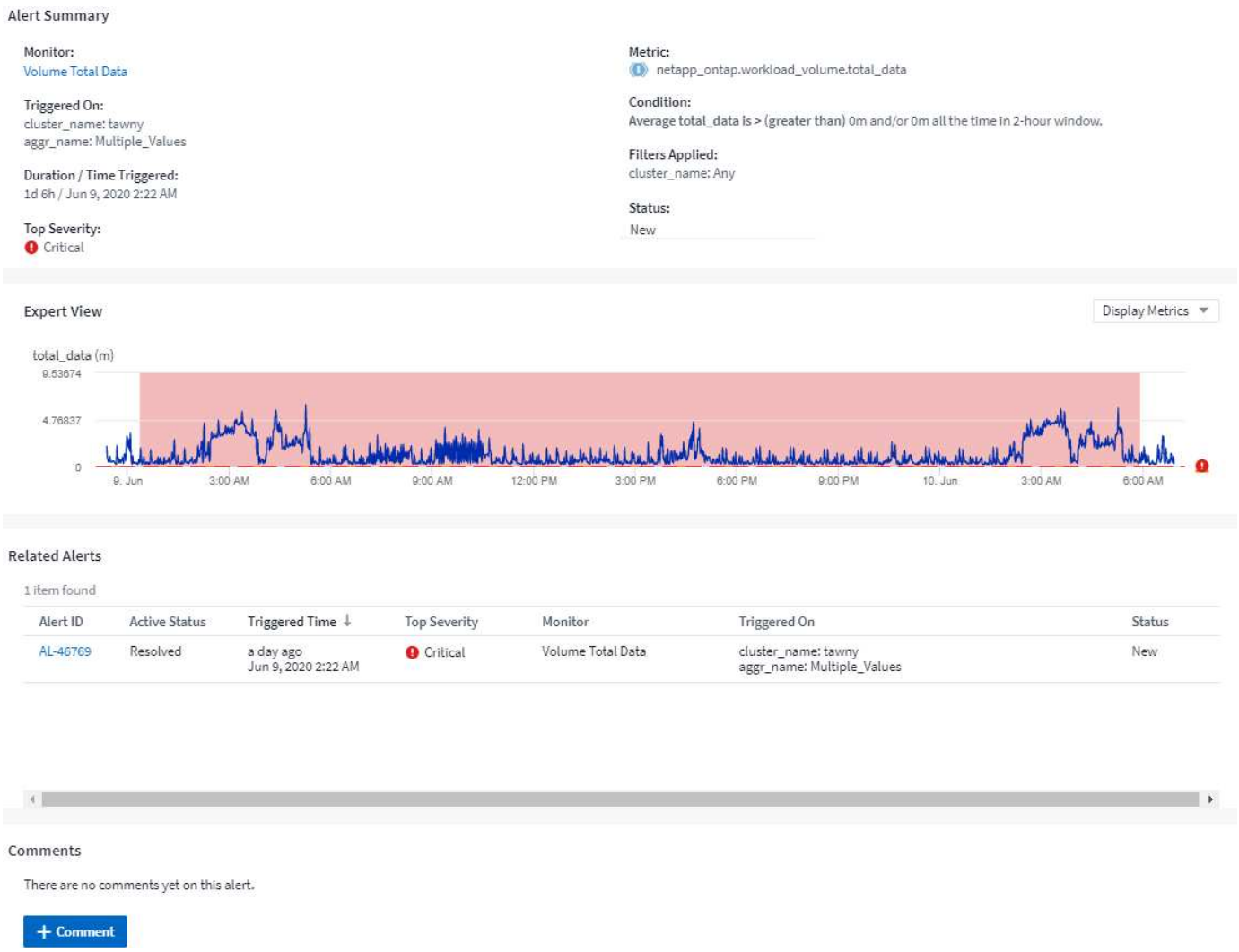
- * 処理中 * ：アラートが調査中であること、またはオープン状態を維持する必要があることを示します
- * Dismiss * を選択すると、アクティブなアラートのリストからアラートが削除されます。

各アラートの左側にあるチェックボックスをオンにして、 [選択したアラートステータスの変更] をクリックすると、複数のアラートを管理できます。

アラート ID をクリックすると、アラート詳細ページが開きます。

アラートの詳細ページ

Alert Detail ページには ' アラートの詳細情報が表示されますこれには 'a_Summary_'a_Expert View_Showing Graphs related to the object' any_related Assets_'_Comments_entered by alert 博士が含まれます



データが見つからない場合に警告します

Data Infrastructure Insightsなどのリアルタイムシステムでは、監視の分析をトリガーしてアラートを生成するかどうかを判断するには、次の2つの要素のいずれかを使用します。

- 次のデータポイントに到達します
- データポイントがなく、十分な時間を待っているときに起動するタイマー

データ到着が遅い場合や、データ到着がない場合と同様に、タイマーメカニズムを引き継ぐ必要があります。これは、「リアルタイム」でアラートをトリガーするためのデータ到着率が不十分であるためです。 そのため、質問は「分析ウィンドウを閉じて、何を確認するまでにどれくらい待つか」ということが一般的です。待機時間が長すぎると、アラートを生成するのに十分な時間がかかります。

長期的なデータ損失が発生する前の最後のデータポイントによって条件が違反されていることを通知する30分のウィンドウを備えたモニタがある場合、 この状態が持続していることをモニタが確認するために使用する他の情報を受信しなかったため、アラートが生成されます。

「 **Permanently Active** 」アラート

監視対象オブジェクトでは、条件を「常に * 」にするようにモニタを設定できます。たとえば、 IOPS>1 や Latency >0 などです。これらは頻繁に「テスト」モニターとして作成され、そして忘れられる。このような監視を実行すると、コンスティチュエントオブジェクトを永続的に開いたままにするアラートが作成されま

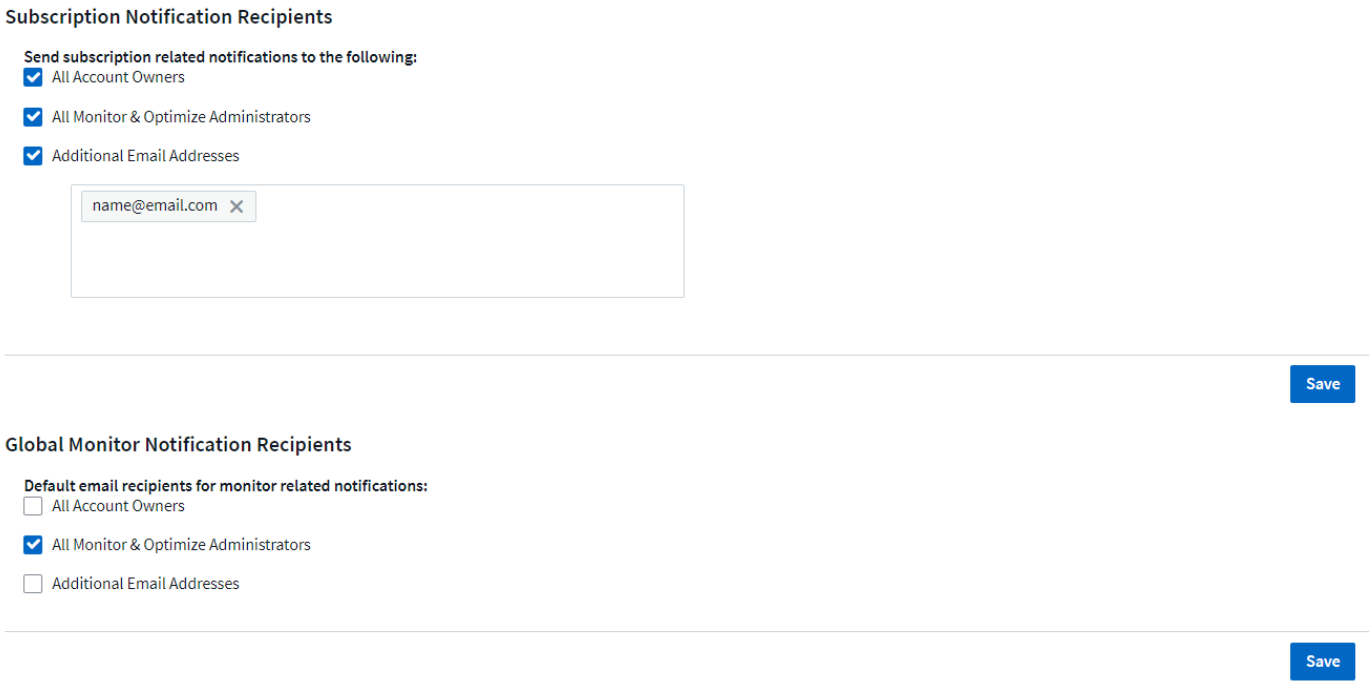
す。これにより、原因システムにかかる負荷や安定性の問題が時間の経過に

これを回避するために、Data Infrastructure Insightsは「永続的にアクティブな」アラートを7日後に自動的に閉じます。基本的なモニタ状態が (おそらく) 継続して存在し、新しいアラートがほぼ即座に発行されることに注意してください。しかし、この「常時アクティブ」アラートを閉じることで、他の状況で発生する可能性のあるシステム負荷が軽減されます。

電子メール通知を設定しています

サブスクリプション関連の通知用の E メールリストや、パフォーマンスポリシーのしきい値違反の通知を受け取る受信者のグローバル E メールリストを設定できます。

通知メール受信者の設定を行うには、 [*Admin] > [Notifications] ページに移動し、 [*Email*] タブを選択します。



サブスクリプション通知の受信者

サブスクリプション関連のイベント通知の受信者を設定するには、「サブスクリプション通知の受信者」セクションに移動します。
次の受信者のいずれかまたはすべてに、サブスクリプション関連イベントに関する E メール通知を送信するように選択できます。

- すべてのアカウント所有者
- すべての監視と最適化管理者
- 指定する追加の E メールアドレス

送信される通知の種類と実行できるユーザアクションの例を次に示します。

* 通知： *	* ユーザーアクション： *

トライアルまたはサブスクリプションが更新されました	でサブスクリプションの詳細を確認します "サブスクリプション。" ページ
サブスクリプションの有効期限は90日です サブスクリプションは30日後に期限切れになります	[Auto Renewal]が有効になっている場合、対処は不要です 連絡先 "ネットアップの営業担当者" をクリックして、サブスクリプションを更新します
トライアルは 2 日で終了します	からトライアルを更新します "サブスクリプション。" ページ試用版は 1 回更新できます。 連絡先 "ネットアップの営業担当者" をクリックして、サブスクリプションを購入します
トライアルまたはサブスクリプションの有効期限が切れています アカウントは48時間後にデータの収集を停止します アカウントは48時間後に削除されます	連絡先 "ネットアップの営業担当者" をクリックして、サブスクリプションを購入します

アラートのグローバル受信者リスト

アラートの E メール通知は、アラートに対するすべての対処方法についてアラート受信者リストに送信されます。アラート通知をグローバル受信者リストに送信することもできます。

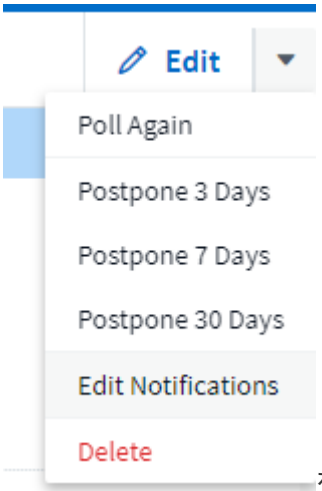
グローバルアラート受信者を設定するには、 [* Global Monitor Notification Recipients] セクションで目的の受信者を選択します。

モニタを作成または変更するときは、各モニタのグローバル受信者リストを常に上書きできます。

ONTAP データコレクタ通知は、クラスタ/データコレクタに関連する特定のモニタ通知よりも優先されます。Data Collector自体に設定した受信者リストには、データコレクタアラートが送信されます。アクティブなデータコレクタアラートがない場合は、監視用に生成されたアラートが特定の監視受信者に送信されます。

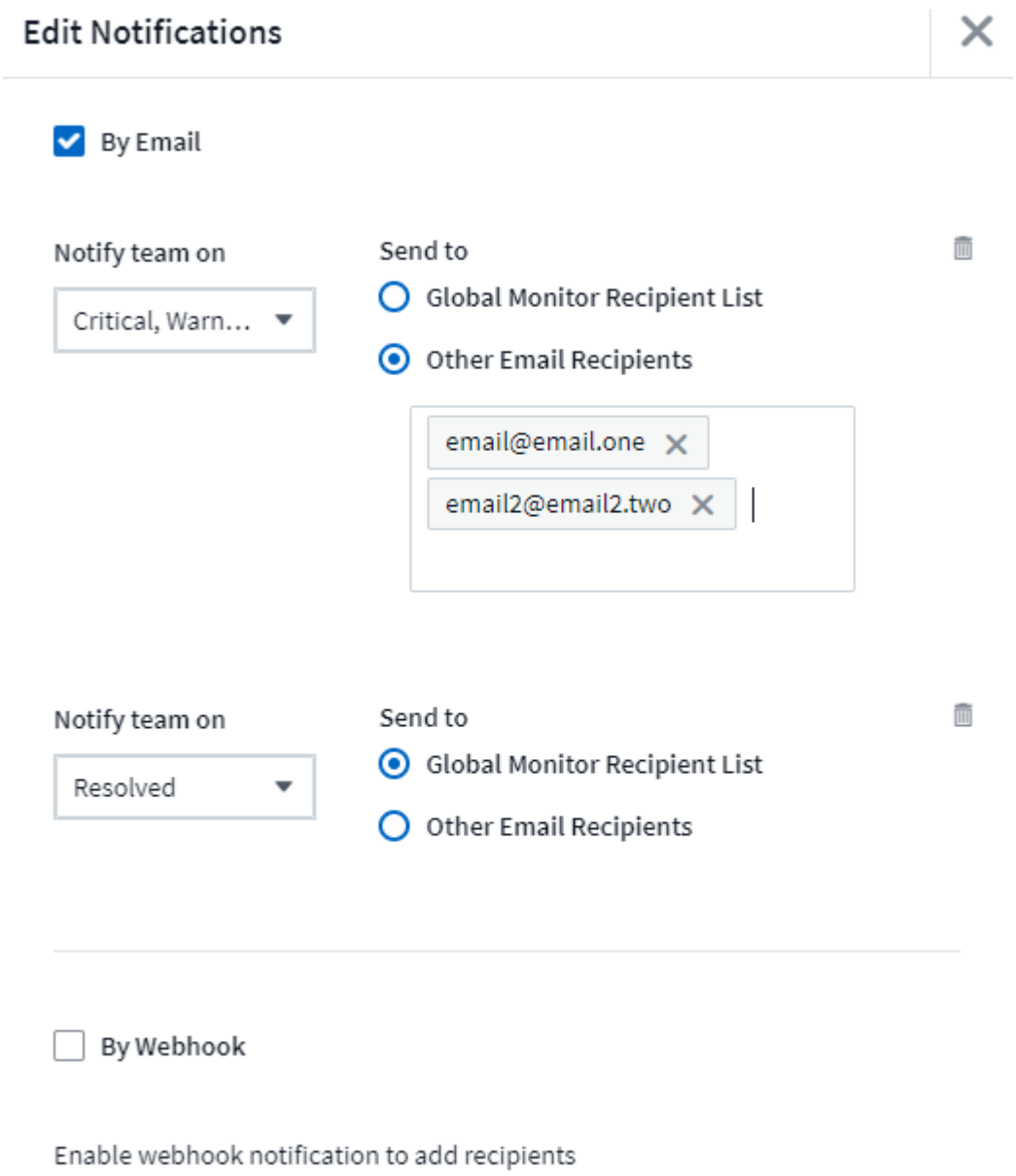
ONTAP の通知の編集

ONTAP クラスタの通知を変更するには、ストレージランディングページの右上のドロップダウンから[*Edit Notifications*]を選択します。



をクリックします"]

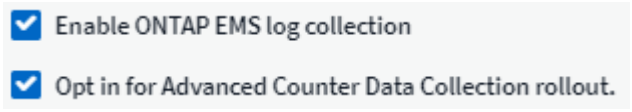
ここでは、重大、警告、情報、解決済みのアラートの通知を設定できます。各シナリオは、グローバル受信者リストまたは選択した他の受信者に通知できます。



システムモニタ

Data Infrastructure Insightsには、指標とログの両方について、システム定義の監視が多数含まれています。使用可能なシステムモニタは、環境内にあるデータコレクタによって異なります。そのため、Data Infrastructure Insightsで使用できるモニタは、データコレクタの追加や設定の変更に応じて変更される場合があります。

多くのシステムモニタは、デフォルトでIN_PAUSED_STATEになっています。システムモニタを有効にするには、モニタの_Resume_optionを選択します。Data Collectorで_Advanced Counter Data Collection_and_Enable ONTAP EMSログcollection_が有効になっていることを確認します。これらのオプションは、 ONTAP データコレクタの *Advanced Configuration* にあります。



モニタの説明

システム定義のモニタは、事前に定義されたメトリックと条件に加えて、デフォルトの説明と修正アクションで構成されています。これらは変更できません。システム定義モニタの通知受信者リストを変更できます。メトリック、条件、概要、および修正アクションを表示したり、受信者リストを変更したりするには、システム定義のモニタグループを開き、リスト内のモニタ名をクリックします。

システム定義のモニタグループは変更または削除できません。

以下のシステム定義モニタは、記載されたグループで使用できます。

- * ONTAP インフラストラクチャ * は、 ONTAP クラスタのインフラストラクチャ関連の問題を監視します。
- * ONTAP ワークロードの例 * には、ワークロード関連の問題のモニターが含まれています。
- 両方のグループのモニタのデフォルトは _Paused _ state です。

現在Data Infrastructure Insightsに含まれているシステム監視は次のとおりです。

メトリックモニタ

モニタ名	重大度	概要を監視します	対処方法

ファイバチャネルポートの利用率が高い	重要	ファイバチャネルプロトコルポートは、お客様のホストシステムと ONTAP LUN の間で SAN トラフィックを送受信するために使用されます。ポートの利用率が高い場合は、そして、これはボトルネックになり、最終的にはファイバチャネルプロトコルの負荷の影響を受けやすいパフォーマンスに影響を与えます。…警告アラートは、ネットワークトラフィックのバランスを取るために計画されたアクションを実行する必要があることを示します。…重大アラートは、サービスの中断が差し迫っていること、およびネットワークのバランスを取るための緊急措置を示します サービスの継続性を確保するためのトラフィック。	重大しきい値を超えた場合は、ただちに対処してサービスの中断を最小限に抑えることを検討してください。 1.利用率の低い別のFCPポートにワークロードを移動します。 2.特定のLUNのトラフィックは、ONTAPのQoSポリシーまたはホスト側の構成を使用して重要な作業のみに制限し、FCPポートの使用率を軽減します。 警告しきい値を超えている場合は、次の処理を計画してください。 1.より多くのFCPポートを設定して、データトラフィックを処理し、ポート利用率がより多くのポートに分散されるようにします。 2. 使用率の低い別の FCP ポートにワークロードを移動します。 3. ONTAP またはホスト側の設定で QoS ポリシーを使用して、特定の LUN のトラフィックを重要な処理のみに制限し、 FCP ポートの利用率を高めます。

LUN レイテンシが高くなっています	重要	LUN は、 I/O トラフィックを処理するオブジェクトで、多くの場合、データベースなどのパフォーマンス重視のアプリケーションによって駆動されます。LUN のレイテンシが高いと、アプリケーション自体が影響を受け、タスクを実行できなくなる可能性があります。…警告アラートは、 LUN を適切なノードまたはアグリゲートに移動するために計画的なアクションが必要であることを示しています。…重大アラートは、サービスの停止が差し迫っていること、および緊急時の措置を講じる必要があることを示してい サービスの継続性を確保します。次に、メディアタイプに基づく想定レイテンシを示します。これは、最大 1 ～ 2 ミリ秒の SSD 、最大 8 ～ 10 ミリ秒の SAS 、および 17 ～ 20 ミリ秒の SATA HDD です	重大しきい値を超えた場合は、サービスの中断を最小限に抑えるために次の操作を検討してください。 LUNまたはそのボリュームにQoSポリシーが関連付けられている場合は、そのしきい値制限を評価して、LUNワークロードが調整されているかどうかを確認します。 警告しきい値を超えている場合は、次の処理を計画してください。 1.アグリゲートの利用率も高い場合は、LUNを別のアグリゲートに移動します。 2. ノードの利用率が高い場合は、ボリュームを別のノードに移動するか、ノードのワークロードの合計を減らします。 3. LUN またはそのボリュームに QoS ポリシーが関連付けられている場合は、しきい値の制限を評価し、 LUN ワークロードが調整されているかどうかを検証します。

ネットワークポートの利用率が高い	重要	ネットワークポートは、NFS 、 CIFS 、および iSCSI のプロトコルトラフィックを受信して、お客様のホストシステムと ONTAP の間で転送するために使用されます。ポート利用率が高いとボトルネックになり、最終的には NFS のパフォーマンスに影響します。 CIFS と iSCSI のワークロード。警告アラートは、ネットワークトラフィックのバランスを取るために計画されたアクションを実行する必要があることを示しています。重要アラートは、サービスの中断が差し迫っていることを示しており、サービスの継続性を確保するためにネットワークトラフィックの負荷を分散するために緊急措置を講じる	重大しきい値を超えた場合は、サービスの中断を最小限に抑えるために、すぐに次の対処方法を検討してください。 1. ONTAPのQoSポリシーまたはホスト側の分析を使用して、特定のボリュームのトラフィックを重要な作業だけに制限し、ネットワークポートの使用率を低下させます。 2.使用率の低い別のネットワークポートを使用するように、1つまたは複数のボリュームを構成します。 警告しきい値を超えた場合は、すぐに次の対処方法を検討してください。 1.データトラフィックを処理するネットワークポートを追加して、ポート使用率がより多くのポートに分散されるようにします。 2. 利用率の低い別のネットワークポートを使用するように 1 つ以上のボリュームを構成します。

NVMe ネームスペースレイテンシが高です	重要	NVMe ネームスペースは、データベースなどのパフォーマンス重視のアプリケーションで I/O トラフィックを処理するオブジェクトです。NVMe ネームスペースのレイテンシが高いと、アプリケーション自体が影響を受けてタスクを実行できなくなる可能性があります。…警告アラートは、LUN を適切なノードまたはアグリゲートに移動するための計画的なアクションが必要であることを示しています。…重大アラートは、サービスの停止が迫っていること、および緊急時の措置を講じる必要があることを示しサービスの継続性を確保するため。	重大しきい値を超えた場合は、ただちに対処してサービスの中断を最小限に抑えることを検討してください。 NVMeネームスペースまたはそのボリュームにQoSポリシーが割り当てられている場合は、制限しきい値が原因でNVMeネームスペースのワークロードが調整されている場合に備えて評価します。 警告しきい値を超えている場合は、次の処理を検討してください。 1.アグリゲートの利用率も高い場合は、LUNを別のアグリゲートに移動します。 2. ノードの利用率が高い場合は、ボリュームを別のノードに移動するか、ノードのワークロードの合計を減らします。 3. NVMe ネームスペースまたはそのボリュームに QoS ポリシーが割り当てられている場合、 NVMe ネームスペースのワークロードが調整されている原因となった場合に備えて、ネームスペースまたはそのボリュームの制限のしきい値を評価します。

qtree 容量がフルです	重要	qtree とは、論理的に定義されたファイルシステムで、ボリューム内のルートディレクトリに特別なサブディレクトリとして作成できます。各 qtree には、ボリューム容量内でツリーに格納されるデータ量を制限するために、クォータポリシーによって定義されるデフォルトスペースクォータがあります。……警告アラートは、スペースを増やすために計画的な処理が必要であることを示します。…重大アラートは、サービスの停止が差し迫っていることを示しますサービスの継続性を確保するために、スペースを空けるために緊急措置を講じる必要があります。	重大しきい値を超えた場合は、ただちに対処してサービスの中断を最小限に抑えることを検討してください。 1.増加に対応するために、qtreeのスペースを増やします。 2.不要なデータを削除してスペースを解放します。 警告しきい値を超えている場合は、次のアクションをすぐに実行するように計画してください。 1.増加に対応するために、qtreeのスペースを増やします。 2. 不要なデータを削除してスペースを解放します。
qtree 容量ハードリミット	重要	qtree とは、論理的に定義されたファイルシステムで、ボリューム内のルートディレクトリに特別なサブディレクトリとして作成できます。各 qtree には、ボリューム内のユーザデータの増加を制御し、合計容量を超えないようにデータを格納するために使用される KB 単位のスペースクォータがあります。 qtree は、ユーザにアラートを提供するソフトストレージ容量クォータを維持し、合計容量に達する前にユーザにアラートを送信しますqtree 内の容量クォータ制限が超過したため、データを格納できなくなりました。qtree に格納されているデータ量を監視することで、ユーザに中断のないデータサービスを確実に提供できます。	重大しきい値を超えた場合は、サービスの中断を最小限に抑えるために、すぐに次の対処方法を検討してください。 1.増加に対応するために、ツリースペースのクォータを増やします 2.ツリー内の不要なデータを削除してスペースを解放するようにユーザーに指示します

qtree 容量のソフトリミット	警告	qtree とは、論理的に定義されたファイルシステムで、ボリューム内のルートディレクトリに特別なサブディレクトリとして作成できます。各 qtree には、ボリューム内のユーザデータの増加を制御し、その合計容量を超えないようにデータを格納するために使用できる、KB 単位のスペースクォータがあります。 qtree は、に到達する前にユーザにプロアクティブにアラートを提供するソフトストレージ容量クォータを維持します qtree 内の容量クォータの合計制限で、データを格納できなくなります。qtree に格納されているデータ量を監視することで、ユーザに中断のないデータサービスを確実に提供できます。	警告しきい値を超えた場合は、すぐに次の対処方法を検討してください。 1.ツリー・スペース・クォータを増加して'増加に対応します 2. ツリー内の不要なデータを削除してスペースを解放するようにユーザーに指示します。
qtree のファイル数のハードリミット	重要	qtree とは、論理的に定義されたファイルシステムで、ボリューム内のルートディレクトリに特別なサブディレクトリとして作成できます。各 qtree には、ボリューム内で管理可能なファイルシステムサイズを維持するために含めることができるファイル数のクォータがあります。… qtree は、ツリー内の新しいファイルが拒否されるハードファイル数のクォータを保持します。qtree 内のファイル数を監視すると、ユーザには中断のないデータサービスが確実に提供されます。	重大しきい値を超えた場合は、ただちに対処してサービスの中断を最小限に抑えることを検討してください。 1. qtreeのファイル数クォータを増やします。 2. qtree ファイルシステムから不要なファイルを削除します。

qtree のファイル数がソフトリミット	警告	qtree とは、論理的に定義されたファイルシステムで、ボリューム内のルートディレクトリに特別なサブディレクトリとして作成できます。各 qtree には、ボリューム内の管理可能なファイルシステムサイズを維持するために、格納できるファイル数のクォータがあります。… qtree は、ソフトファイル番号のクォータを保持し、 qtree および内のファイル数の上限に達する前にユーザにプロアクティブにアラートを送信します 追加のファイルを保存できません。qtree 内のファイル数を監視すると、ユーザには中断のないデータサービスが確実に提供されます。	警告しきい値を超えている場合は、次のアクションをすぐに実行するように計画してください。 1. qtreeのファイル数クォータを増やします。 2. qtree ファイルシステムから不要なファイルを削除します。

Snapshot リザーブスペースがフルです	重要	アプリケーションとお客様のデータを格納するには、ボリュームのストレージ容量が必要です。スナップショット予約領域と呼ばれる領域の一部はスナップショットの保存に使用され、データをローカルで保護できます。ONTAP ボリュームに格納される新規データや更新データが多いほど、使用される Snapshot 容量は増えますが、今後追加または更新されるデータに使用できる Snapshot ストレージ容量は少なくなります。ボリューム内の Snapshot データ容量が Snapshot リザーブスペースの合計に達すると、新しい Snapshot データを格納できなくなり、ボリューム内のデータの保護レベルが低下する可能性があります。ボリュームの使用済み Snapshot 容量を監視して、データサービスの継続性を確保します。	重大しきい値を超えた場合は、ただちに対処してサービスの中断を最小限に抑えることを検討してください。 1.スナップショット予約がいっぱいになったときにボリュームのデータスペースを使用するようにスナップショットを構成します。 2.古い不要なスナップショットをいくつか削除して、領域を解放します。 警告しきい値を超えている場合は、次のアクションをすぐに実行するように計画してください。 1.ボリューム内のスナップショット・リザーブ・スペースを拡張して'増加に対応します 2. スナップショット予約がいっぱいになったときにボリューム内のデータ領域を使用するようにスナップショットを設定します。

ストレージ容量の制限	重要	ストレージプール（アグリゲート）がいっぱいになると I/O 処理が低速化し、最後にストレージ停止インシデントが発生します。警告アラートは、最小限の空きスペースをリストアするために計画的な対処が必要であることを示しています。重大アラートは、サービスの停止が差し迫っていることを示しており、サービスの継続性を確保するためにスペースを解放するために緊急措置を講じる必要があることを示しています。	重大しきい値を超えた場合は、すぐに次の処理を検討してサービスの中断を最小限に抑えます。 1.重要でないボリュームのSnapshotを削除します。 2.不要なワークロードであり、ストレージコピーからリストアされる可能性のあるボリュームまたはLUNを削除します。… 警告しきい値を超えている場合は、次のアクションをすぐに計画してください。 1. 1つ以上のボリュームを別のストレージの場所に移動します。 2. ストレージ容量を追加します。 3. ストレージ効率の設定を変更するか、アクセス頻度の低いデータをクラウドストレージに階層化します。

ストレージパフォーマンスの制限	重要	ストレージシステムのパフォーマンスが上限に達すると、処理速度が低下し、レイテンシが増大し、ワークロードやアプリケーションで障害が発生する可能性があります。ONTAP は、ワークロードのストレージプールの使用率を評価し、パフォーマンスの消費率を推定します。…警告アラートは、ストレージプールの負荷を軽減するために、ワークロードのピークに対応できるだけの十分なストレージプールのパフォーマンスが確保されるように、計画されたアクションを実行する必要があることを示しますパフォーマンスの低下が切迫しており、サービスの継続性を確保するためにストレージプールの負荷を軽減するために緊急措置を講じる必要があります。	重大しきい値を超えた場合は、サービスの中断を最小限に抑えるために、すぐに次の対処方法を検討してください。 1. SnapshotやSnapMirrorレプリケーションなど、スケジュールされているタスクを中断します。 2.重要でないワークロードをアイドル状態にする… 警告しきい値を超えた場合は、すぐに次の処理を実行します。 1. 1つ以上のワークロードを別のストレージの場所に移動します。 2.ストレージノード（AFF）またはディスクシェルフ（FAS）を追加し、ワークロードを再配分します 3. ワークロード特性（ブロックサイズ、アプリケーションキャッシング）の変更

ユーザクォータ容量のハードリミット	重要	ONTAP は、ボリューム内のボリューム、ファイル、またはディレクトリにアクセスする権限を持つ UNIX または Windows システムのユーザを認識します。その結果、ユーザやユーザグループが使用する Linux または Windows システムのストレージ容量を ONTAP で設定できるようになります。ユーザまたはグループのポリシークォータによって、ユーザが自身のデータに使用できるスペース量が制限されます。このクォータのハードリミットにより、ボリューム内で使用されている容量が適切である場合に、合計容量クォータに達する前にユーザに通知できます。ユーザクォータまたはグループクォータに保存されているデータ量を監視することで、ユーザに中断のないデータサービスを確実に提供できます。	重大しきい値を超えた場合は、サービスの中断を最小限に抑えるために、すぐに次の対処方法を検討してください。 1.増加に対応するために、ユーザクォータまたはグループクォータのスペースを増やします。 2. 不要なデータを削除してスペースを解放するようにユーザまたはグループに指示します。

ユーザクォータ容量のソフトリミット	警告	ONTAP は、ボリューム内のボリューム、ファイル、またはディレクトリにアクセスできる権限を持つ UNIX または Windows システムのユーザを認識します。その結果、ユーザやユーザグループが使用する Linux または Windows システムのストレージ容量を ONTAP で設定できるようになります。ユーザまたはグループのポリシークォータによって、ユーザが自身のデータに使用できるスペース量が制限されます。このクォータのソフトリミットにより、ボリューム内で使用されている容量が合計容量クォータに達したときにユーザにプロアクティブな通知が可能になります。ユーザクォータまたはグループクォータに保存されているデータ量を監視することで、ユーザに中断のないデータサービスを確実に提供できます。	警告しきい値を超えている場合は、次のアクションをすぐに実行するように計画してください。 1.増加に対応するために、ユーザクォータまたはグループクォータのスペースを増やします。 2. 不要なデータを削除してスペースを解放します。

ボリュームの容量がフルです	重要	アプリケーションとお客様のデータを格納するには、ボリュームのストレージ容量が必要です。ONTAP ボリュームに格納されるデータが多いほど、以降のデータで使用できるストレージ容量は少なくなります。ボリューム内のデータストレージ容量が合計ストレージ容量に達すると、ストレージ容量の不足によりデータを格納できなくなる可能性があります。ボリュームの使用済みストレージ容量を監視して、データサービスの継続性を確保します。	重大しきい値を超えた場合は、サービスの中断を最小限に抑えるために、すぐに次の対処方法を検討してください。 1.拡張に対応できるようにボリュームのスペースを増やします。 2. 不要なデータを削除してスペースを解放します。 3. SnapshotコピーがSnapshotリザーブよりも多くのスペースを占有している場合は、古いSnapshotを削除するか、ボリュームSnapshotの自動削除を有効にします。…警告しきい値を超えている場合は、次のアクションをすぐに実行するように計画してください。 1.ボリュームの拡張に対応するために、ボリュームのスペースを増やします 2. SnapshotコピーがSnapshotリザーブよりも多くのスペースを占有する場合は、古いSnapshotを削除するか、ボリュームSnapshotの自動削除を有効にします。……

ボリュームの inode 制限	重要	ファイルを格納するボリュームでは、インデックスノード（ inode ）を使用してファイルメタデータが格納されます。ボリュームの inode 割り当てが使用されなくなった場合は、 これ以上ファイルを追加できません。…警告アラートは、使用可能な inode の数を増やすために計画的なアクションを実行する必要があることを示しています。重要なアラートは、ファイル制限の枯渇が差し迫っていることを示しており、サービスの継続性を確保するために緊急対策を講じる必要があることを示しています。	重大しきい値を超えた場合は、サービスの中断を最小限に抑えるために、すぐに次の対処方法を検討してください。 1.ボリュームのinodeの値を増やします。inode の値がすでに最大値に達している場合は、ファイルシステムのサイズが最大サイズを超えているため、ボリュームを複数のボリュームにスプリットします。 2. FlexGroupを使用すると、大規模なファイルシステムに対応できます。 警告しきい値を超えている場合は、次のアクションをすぐに実行するように計画してください。 1.ボリュームのinodeの値を増やします。inode の値がすでに最大値に達している場合は、ファイルシステムのサイズが最大サイズを超えているため、ボリュームを 2 つ以上のボリュームにスプリットします。 2. 大規模なファイルシステムに対応するために FlexGroup を使用する

ボリュームレイテンシが高くなっています	重要	ボリュームは、 I/O トラフィックを処理するオブジェクトで、多くの場合、 DevOps アプリケーション、ホームディレクトリ、データベースなどのパフォーマンス重視のアプリケーションによって駆動されます。ボリュームのレイテンシが高いと、アプリケーション自体に影響を及ぼし、タスクを実行できなくなる可能性があります。ボリュームのレイテンシを監視することは、アプリケーションの整合性を維持するうえで非常に重要です。メディアタイプに基づく想定レイテンシは、最大 1 ～ 2 ミリ秒、 SAS は最大 8 ～ 10 ミリ秒、 SATA HDD は 17 ～ 20 ミリ秒です	重大しきい値を超えた場合は、サービスの中断を最小限に抑えるために、すぐに次の対処方法を検討してください。 ボリュームにQoSポリシーが割り当てられている場合は、ボリュームのワークロードが調整される原因になっている場合に備えて、制限しきい値を評価します。 警告しきい値を超えた場合は、すぐに次の対処方法を検討してください。 1.アグリゲートの利用率も高い場合は、ボリュームを別のアグリゲートに移動します。 2. ボリュームに QoS ポリシーが割り当てられている場合、ボリュームワークロードが調整される原因となった場合に備えて、制限しきい値を評価します。 3. ノードの利用率が高い場合は、ボリュームを別のノードに移動するか、ノードの合計ワークロードを減らします。
モニタ名	重大度	概要を監視します	対処方法

ノードの高レイテンシ	警告 / 重大	ノードのレイテンシが、ノード上のアプリケーションのパフォーマンスに影響する可能性があるレベルに達しました。ノードのレイテンシが低いため、アプリケーションのパフォーマンスが安定します。メディアタイプに基づく想定レイテンシは次のとおりです。 SSD は最大 1 ～ 2 ミリ秒、 SAS は最大 8 ～ 10 ミリ秒、 SATA HDD は 17 ～ 20 ミリ秒。	重大しきい値を超えた場合は、サービスの中断を最小限に抑えるためにすぐに対処する必要があります。 1.スケジュールされたタスク、Snapshot、またはSnapMirrorレプリケーションを中断します 2. QoS制限により、優先度の低いワークロードの需要を抑制 3.重要でないワークロードを非アクティブ化します 警告しきい値を超えた場合の即時の対処を検討します。 1. 1つ以上のワークロードを別のストレージの場所に移動します 2. QoS制限により、優先度の低いワークロードの需要を抑制 3.ストレージノード（AFF）またはディスクシェルフ（FAS）を追加し、ワークロードを再配分します 4.ワークロードの特性（ブロックサイズ、アプリケーションのキャッシュなど）の変更

ノードのパフォーマンス制限	警告 / 重大	ノードのパフォーマンス使用率が、 IOS およびノードでサポートされているアプリケーションのパフォーマンスに影響する可能性があるレベルに達しました。ノードのパフォーマンス利用率が低いため、アプリケーションのパフォーマンスが安定します。	重大しきい値を超えた場合は、サービスの中断を最小限に抑えるためにすぐに対処する必要があります。 1.スケジュールされたタスク、Snapshot、またはSnapMirrorレプリケーションを中断します 2. QoS制限により、優先度の低いワークロードの需要を抑制 3.重要でないワークロードを非アクティブ化します 警告しきい値を超えた場合は、次の処理を検討してください。 1. 1つ以上のワークロードを別のストレージの場所に移動します 2. QoS制限により、優先度の低いワークロードの需要を抑制 3.ストレージノード（AFF）またはディスクシェルフ（FAS）を追加し、ワークロードを再配分します 4.ワークロードの特性（ブロックサイズ、アプリケーションのキャッシュなど）の変更

Storage VM のレイテンシが高くなっています	警告 / 重大	Storage VM （ SVM ）のレイテンシが Storage VM のアプリケーションのパフォーマンスに影響する可能性があるレベルに達しました。Storage VM のレイテンシが低いため、アプリケーションのパフォーマンスが安定します。メディアタイプに基づく想定レイテンシは次のとおりです。 SSD は最大 1 ～ 2 ミリ秒、 SAS は最大 8 ～ 10 ミリ秒、 SATA HDD は 17 ～ 20 ミリ秒。	重大しきい値を超えている場合は、QoSポリシーが割り当てられているStorage VMのボリュームのしきい値制限をすぐに評価して、ボリュームワークロードの調整の原因になっているかどうかを確認します 警告しきい値を超えた場合は、すぐに次の対応を検討してください。 1.アグリゲートの利用率も高い場合は、Storage VMの一部のボリュームを別のアグリゲートに移動します。 2. QoSポリシーが割り当てられているStorage VMのボリュームについて、しきい値制限が原因でボリュームワークロードが調整されている場合は評価します 3.ノードの利用率が高い場合は、Storage VMの一部のボリュームを別のノードに移動するか、ノードの総ワークロードを減らします
ユーザクォータのファイル数のハードリミット	重要	ボリューム内に作成されたファイル数が重大な制限に達したため、追加ファイルを作成できません。保存されたファイル数を監視することで、ユーザに中断のないデータサービスを確実に提供できます。	重大しきい値を超えた場合にサービスの中断を最小限に抑えるには、すぐに対処する必要があります。…次のアクションを実行することを検討してください。 1.特定のユーザのファイル数クォータを増やします 2.不要なファイルを削除して、特定のユーザーのファイルクォータへの負荷を軽減します

ユーザクォータのファイル数がソフトリミット	警告	ボリューム内に作成されたファイル数がクォータのしきい値に達し、重大な制限に近づいています。クォータが重大の上限に達した場合、追加のファイルを作成できません。ユーザが保存するファイル数を監視することで、ユーザに中断のないデータサービスが確実に提供されます。	警告しきい値を超えた場合の即時の対処を検討します。 1.特定のユーザクォータのファイル数クォータを増やします 2.不要なファイルを削除して、特定のユーザーのファイルクォータへの負荷を軽減します
ボリュームキャッシュミス率	警告 / 重大	ボリュームキャッシュミス率は、クライアントアプリケーションからの読み取り要求に対してキャッシュからではなくディスクからデータが返される割合です。これは、ボリュームが設定されたしきい値に達したことを意味します。	重大しきい値を超えた場合は、サービスの中断を最小限に抑えるためにすぐに対処する必要があります。 1.ボリュームのノードから一部のワークロードを移動してIO負荷を軽減します 2.ボリュームのノードにWAFLキャッシュがない場合は、Flash Cacheを購入して追加し、キャッシュを拡張します 3. QoS制限により、同じノード上で優先度の低いワークロードの負荷を軽減します 警告しきい値を超えた場合の即時の対処を検討します。 1.ボリュームのノードから一部のワークロードを移動してIO負荷を軽減します 2.ボリュームのノードにWAFLキャッシュがない場合は、Flash Cacheを購入して追加し、キャッシュを拡張します 3. QoS制限により、同じノード上で優先度の低いワークロードの負荷を軽減します 4.ワークロードの特性（ブロックサイズ、アプリケーションのキャッシュなど）の変更

ボリュームの qtree クォータオーバーコミット	警告 / 重大	ボリュームの qtree クォータオーバーコミットは、ボリュームが qtree クォータによってオーバーコミットされているとみなす割合を示します。ボリュームの qtree クォータの設定しきい値に達しました。ボリューム qtree クォータオーバーコミットを監視することで、ユーザに中断のないデータサービスが確実に提供されます。	重大しきい値を超えた場合は、サービスの中断を最小限に抑えるためにすぐに対処する必要があります。 1.ボリュームのスペースを増やします 2.不要なデータを削除します 警告しきい値を超えた場合は、ボリュームのスペースを増やすことを検討してください。

トップに戻る

ログモニタ

モニタ名	重大度	説明	対処方法
AWS クレデンシャルが初期化されて	情報	このイベントは、モジュールが初期化される前に、クラウドクレデンシャルスレッドから Amazon Web Services （ AWS ）の Identity and Access Management （ IAM ）ロールベースクレデンシャルにアクセスしようとした場合に発生します。	" クラウドクレデンシャルのスレッドとシステムの初期化が完了するまで待ちます。

クラウド階層に到達不能です	重要	ストレージノードからクラウド階層のオブジェクトストア API に接続することはできません。一部のデータにアクセスできません。	オンプレミス製品を使用している場合は、次の対処策を実施します。 …「 network interface show 」コマンドを使用して、クラスタ間 LIF がオンラインで機能していることを確認します。…デスティネーションノードのクラスタ間 LIF で「 ping 」コマンドを使用して、オブジェクトストアサーバへのネットワーク接続を確認します。…オブジェクトストアの設定が変更されていないことを確認します。ログインおよび接続の情報はです それでも有効です。問題が解決しない場合は、ネットアップのテクニカルサポートにお問い合わせください。 Cloud Volumes ONTAP を使用する場合は、次の対処方法を実行します。…オブジェクトストアの設定が変更されていないことを確認します。 ログイン情報と接続情報がまだ有効であることを確認してください。問題が有効でない場合は、ネットアップのテクニカルサポートにお問い合わせください。
ディスクがサービスを停止しています	情報	「このイベントは、ディスクが障害としてマークされているか、完全消去中であるか、 Maintenance Center に入力されたためにサービスから削除された場合に発生します。」	なし

FlexGroup 構成要素がフルです	重要	「 FlexGroup ボリューム内のコンスティチュエントがいっぱいになっているため、原因がサービスを停止する可能性があります。この場合も、 FlexGroup ボリュームでファイルを作成または拡張できます。ただし、コンスティチュエントに格納されているファイルを変更することはできません。その結果、 FlexGroup ボリュームに対して書き込み処理を実行しようとしたときに、ランダムなスペース不足エラーが発生することがあります。」	「 volume modify -files + X 」コマンドを使用して、 FlexGroup ボリュームに容量を追加することを推奨します。または、 FlexGroup ボリュームからファイルを削除することもできます。しかし、どのファイルがコンスティチュエントに置かれているかを特定するのは難しい」
FlexGroup コンスティチュエントがほぼフルです	警告	「 FlexGroup ボリューム内のコンスティチュエントのスペースがほとんどなくなると、原因によってサービスが停止する可能性があります。ファイルを作成して展開できます。ただし、コンスティチュエントのスペースが不足すると、コンスティチュエントにファイルを追加したり変更したりできなくなる可能性があります。	「 volume modify -files + X 」コマンドを使用して、 FlexGroup ボリュームに容量を追加することを推奨します。または、 FlexGroup ボリュームからファイルを削除することもできます。しかし、どのファイルがコンスティチュエントに置かれているかを特定するのは難しい」
FlexGroup コンスティチュエントの inode がほぼなくなっています	警告	「 FlexGroup ボリューム内のコンスティチュエントは inode がほとんどなくなっており、原因がサービスの停止を招く可能性があります。コンスティチュエントに平均よりも少ない作成要求が送信されます。FlexGroup ボリュームの全体的なパフォーマンスに影響することがあります。これは、 inode が多いコンスティチュエントに要求がルーティングされるためです。」	「 volume modify -files + X 」コマンドを使用して、 FlexGroup ボリュームに容量を追加することを推奨します。または、 FlexGroup ボリュームからファイルを削除することもできます。しかし、どのファイルがコンスティチュエントに置かれているかを特定するのは難しい」

FlexGroup コンスティチュエントの inode が不明です	重要	「 FlexGroup ボリュームのコンスティチュエントの inode が不足しており、原因によってサービスが停止する可能性があります。この構成要素には新しいファイルを作成できません。これにより、 FlexGroup ボリューム間でコンテンツが全体的に不均衡な状態に分散される可能性があります。」	「 volume modify -files +X 」コマンドを使用して、 FlexGroup ボリュームに容量を追加することを推奨します。または、 FlexGroup ボリュームからファイルを削除することもできます。しかし、どのファイルがコンスティチュエントに置かれているかを特定するのは難しい」
LUN はオフラインです	情報	このイベントは、 LUN が手動でオフラインになった場合に発生します。	LUN をオンラインに戻します。
メインユニットファンに障害が発生しました	警告	1 つ以上のメインユニットファンで障害が発生しました。システムは動作し続けます。しかし、状態が長く続くと、過熱によって自動シャットダウンがトリガーされることがあります。	" 障害が発生したファンを取り付け直します。エラーが解消されない場合は、交換します。
警告状態のメインユニットファン	情報	このイベントは、 1 つまたは複数のメインユニットファンが警告状態のときに発生します。	過熱を防ぐため、示されたファンを交換してください。
NVRAM バッテリ低下	警告	NVRAM バッテリ容量が非常に少なくなっています。バッテリの電力が不足すると、データが失われる可能性があります。…NetApp テクニカルサポートと設定済みの送信先（該当する場合）に、 AutoSupport または「 call home 」というメッセージが生成されて送信されます。AutoSupport メッセージが正常に配信されると、問題の特定と解決方法が大幅に改善されます。	「 system node environment sensors show 」コマンドを使用して、バッテリの現在のステータス、容量、および充電状態を表示します。バッテリを最近交換した場合や、システムが長時間にわたって動作していない場合は、次の対処方法を実行します。 バッテリを監視して、適切に充電されていることを確認してください。…バッテリの稼働時間が引き続きクリティカルなレベルを下回ると、ストレージシステムが自動的にシャットダウンする場合は、ネットアップテクニカルサポートにお問い合わせください。

サービスプロセッサが設定されていません	警告	「このイベントは毎週発生し、サービスプロセッサ（ SP ）の設定を通知するために使用されます。SP は、システムに組み込まれている物理デバイスであり、リモートアクセス機能とリモート管理機能を提供します。すべての機能を使用できるように SP を設定する必要があります。	次の対処方法を実行します。…「 system service-processor network modify 」コマンドを使用して SP を設定します。オプションで、 「 system service-processor network show 」コマンドを使用して、 SP の MAC アドレスを取得します。…「 system service-processor network show 」コマンドを使用して、 SP ネットワーク設定を確認します。「 system service-processor AutoSupport invoke 」コマンドを使用して、 SP から AutoSupport E メールを送信できることを確認します。 注 AutoSupport ：このコマンドを実行する前に、 ONTAP E メールホストと受信者を問題で設定する必要があります。
サービスプロセッサはオフラインです	重要	「すべての SP リカバリアクションが実行されていても、 ONTAP はサービスプロセッサ（ SP ）からハートビートを受信しなくなりました。ONTAP は、 SP なしでハードウェアの状態を監視できません。システムはシャットダウンして、ハードウェアの損傷やデータの損失を防ぎます。SP がオフラインになった場合にすぐに通知されるようにパニック・アラートを設定する	次の操作を実行して、システムの電源を再投入します。…コントローラをシャーシから引き出します。…コントローラをもう一度押し込みます。…コントローラをオンに戻します。問題が解決しない場合は、コントローラモジュールを交換します。

シェルフのファンに障害があります	重要	" シェルフの冷却ファンまたはファンモジュールに障害が発生しました。シェルフ内のディスクに十分な通気による冷却が確保されないと、ディスク障害が発生する可能性があります。」	次の対処方法を実行します。ファンモジュールが完全に装着され、固定されていることを確認します。 メモ：一部のディスクシェルフの電源装置モジュールにファンが内蔵されています。問題が解決しない場合は、ファンモジュールを交換してください。それでも問題が解決しない場合は、ネットアップのテクニカルサポートにお問い合わせください。
メインユニットファンの障害により、システムは動作できません	重要	「 1 つまたは複数のメインユニットファンで障害が発生し、システムの動作が中断しました。これにより、データが失われる可能性があります。	障害が発生したファンを交換します。
未割り当てディスク	情報	システムに未割り当てのディスクがあります - 容量が無駄になっており、構成の設定ミスや部分的な変更がシステムに適用されている可能性があります。	次の対処方法を実行します。「 disk show -n 」コマンドを使用して、どのディスクが割り当てられていないかを確認します。「 disk assign 」コマンドを使用して、ディスクをシステムに割り当てます。
アンチウイルスサーバビジー	警告	ウィルス対策サーバがビジーのため、新しいスキャン要求を受け入れることができません。	このメッセージが頻繁に表示される場合は、 SVM で生成されるウィルススキャンの負荷を処理できるだけの十分なウィルス対策サーバがあることを確認してください。

IAM ロールの AWS クレデンシャルの期限が切れました	重要	Cloud Volume ONTAP にアクセスできなくなりました。ID およびアクセス管理（ IAM ）ロールベースのクレデンシャルの期限が切れている。クレデンシャルは、 IAM ロールを使用して Amazon Web Services （ AWS ）メタデータサーバから取得され、 Amazon Simple Storage Service （ Amazon S3 ）への API 要求に署名するために使用されます。	次の手順を実行します。… AWS EC2 管理コンソールにログインします。…インスタンスページに移動します。… Cloud Volumes ONTAP 導入のインスタンスを探してその健常性を確認します。…インスタンスに関連付けられている AWS IAM ロールが有効であり、インスタンスに適切な権限が付与されていることを確認します。
IAM ロールの AWS クレデンシャルが見つかりません	重要	クラウドクレデンシャルスレッドで、 Amazon Web Services （ AWS ）の Identity and Access Management （ IAM ）ロールベースのクレデンシャルを AWS メタデータサーバから取得することはできません。クレデンシャルは、 Amazon Simple Storage Service （ Amazon S3 ）への API 要求への署名に使用されます。Cloud Volume ONTAP にアクセスできなくなりました。…	次の手順を実行します。… AWS EC2 管理コンソールにログインします。…インスタンスページに移動します。… Cloud Volumes ONTAP 導入のインスタンスを探してその健常性を確認します。…インスタンスに関連付けられている AWS IAM ロールが有効であり、インスタンスに適切な権限が付与されていることを確認します。
IAM ロールの AWS クレデンシャルが無効です	重要	ID およびアクセス管理（ IAM ）ロールベースのクレデンシャルが無効です。クレデンシャルは、 IAM ロールを使用して Amazon Web Services （ AWS ）メタデータサーバから取得され、 Amazon Simple Storage Service （ Amazon S3 ）への API 要求に署名するために使用されます。Cloud Volume ONTAP にアクセスできなくなりました。	次の手順を実行します。… AWS EC2 管理コンソールにログインします。…インスタンスページに移動します。… Cloud Volumes ONTAP 導入のインスタンスを探してその健常性を確認します。…インスタンスに関連付けられている AWS IAM ロールが有効であり、インスタンスに適切な権限が付与されていることを確認します。

AWS IAM ロールが見つかりません	重要	Identity and Access Management （ IAM ）ロールスレッドで、 AWS メタデータサーバに Amazon Web Services （ AWS ） IAM ロールが見つかりません。IAM ロールは、 Amazon Simple Storage Service （ Amazon S3 ）への API 要求の署名に使用するロールベースのクレデンシャルを取得する必要があります。Cloud Volume ONTAP にアクセスできなくなりました。…	次の手順を実行します。… AWS EC2 管理コンソールにログインします。…インスタンスページに移動します。… Cloud Volumes ONTAP 導入のインスタンスを探してその健常性を確認します。…インスタンスに関連付けられている AWS IAM ロールが有効であることを確認します。
AWS IAM ロールが無効です	重要	AWS メタデータサーバの Amazon Web Services （ AWS ） Identity and Access Management （ IAM ）ロールが無効です。Cloud Volume ONTAP にアクセスできなくなりました。…	次の手順を実行します。… AWS EC2 管理コンソールにログインします。…インスタンスページに移動します。… Cloud Volumes ONTAP 導入のインスタンスを探してその健常性を確認します。…インスタンスに関連付けられている AWS IAM ロールが有効であり、インスタンスに適切な権限が付与されていることを確認します。
AWS メタデータサーバに接続できませんでした	重要	Identity and Access Management （ IAM ）役割スレッドで、 Amazon Web Services （ AWS ）メタデータサーバとの通信リンクを確立できません。Amazon Simple Storage Service （ Amazon S3 ）への API 要求の署名に使用する AWS IAM ロールベースの必要なクレデンシャルを取得するために通信を確立する必要があります。Cloud Volume ONTAP にアクセスできなくなりました。…	次の手順を実行します。… AWS EC2 管理コンソールにログインします。…インスタンスページに移動します。… Cloud Volumes ONTAP 導入のインスタンスを探してその健全性を確認します。

FabricPool のスペース使用制限にほぼ達しました	警告	容量ライセンスのあるプロバイダが提供するオブジェクトストアでのクラスタ全体の FabricPool スペースの使用量が、ライセンスで許可された上限にほぼ達しています。	次の対処方法を実行します。…「 storage aggregate object-store show-space 」コマンドを使用して、各 FabricPool ストレージ階層で使用されているライセンス容量の割合を確認します。…「 volume snapshot delete 」コマンドを使用して、階層化ポリシー「 snapshot 」または「 backup 」が設定されたボリュームから Snapshot コピーを削除します。…新しいライセンスをインストールします クラスタ上でライセンス容量を拡張します。
FabricPool のスペース使用制限に達しました	重要	容量ライセンスプロバイダが提供するオブジェクトストアのFabricPoolスペース使用量が、クラスタ全体での合計でライセンスの上限に達しています。	次の対処方法を実行します。…「 storage aggregate object-store show-space 」コマンドを使用して、各 FabricPool ストレージ階層で使用されているライセンス容量の割合を確認します。…「 volume snapshot delete 」コマンドを使用して、階層化ポリシー「 snapshot 」または「 backup 」が設定されたボリュームから Snapshot コピーを削除します。…新しいライセンスをインストールします クラスタ上でライセンス容量を拡張します。

アグリゲートのギブバックに失敗しました	重要	ストレージフェイルオーバー（ SFO ）ギブバックの一環としてアグリゲートを移行したときに、デスティネーションノードがオブジェクトストアに到達できない場合に発生します。	次の対処方法を実行します。…「 network interface show 」コマンドを使用して、インタークラスタ LIF がオンラインで機能していることを確認します。…デスティネーションノードのクラスタ間 LIF で「 ping 」コマンドを使用して、オブジェクトストアサーバへのネットワーク接続を確認します。…「 aggregate object-store config show 」コマンドを使用して、オブジェクトストアの設定が変更されておらず、ログインおよび接続の情報が正確であることを確認してください。または、 このエラーを無効にするには、 giveback コマンドの「 require-partner-waiting 」パラメータに false を指定します。詳細やサポートについては、ネットアップテクニカルサポートにお問い合わせください。

HA インターコネクトが停止しています	警告	ハイアベイラビリティ（HA）インターコネクトが停止しています。フェイルオーバーを利用できない場合、サービスが停止するリスクがあります。	対処方法は、プラットフォームでサポートされている HA インターコネクトリンクの数と種類、およびインターコネクトが停止している理由によって異なります。…リンクがダウンしている場合 : … HA ペアの両方のコントローラが動作していることを確認します。外部接続リンクの場合は、相互接続ケーブルが正しく接続されていること、および小型フォームファクタプラガブル（ SFP ）が両方のコントローラに正しく装着されていることを確認します。内部接続されているリンクの場合は、リンクを無効にし、リンクを有効にします。一方は、「 IC LINK OFF 」コマンドと「 IC LINK ON 」コマンドを使用して行います。…リンクが無効になっている場合は、「 ic link on 」コマンドを使用してリンクを有効にします。…ピアが接続されていない場合は、「 ic link off 」コマンドと「 ic link on 」コマンドを使用して、一方のリンクを無効にし、再度有効にします。…問題が解決しない場合は、ネットアップのテクニカルサポートにお問い合わせください。

ユーザあたりの最大セッション数を超えました	警告	TCP 接続でのユーザあたりの最大許容セッション数を超えました。セッションを確立する要求は、一部のセッションが解放されるまで拒否されます。…	次の対処策を実行します。 …クライアントで実行されているすべてのアプリケーションを検査し、正常に動作していないアプリケーションを終了します。…クライアントを再起動します。…問題が新規または既存のアプリケーションによって発生しているかどうかを確認します。アプリケーションが新規の場合は、「 cifs option modify -max-opense-opense-file-per-tree 」コマンドを使用して、クライアントのしきい値を大きく設定します。 クライアントが想定どおりに動作していても、しきい値の上昇が必要となる場合があります。クライアントのしきい値を高く設定するには、advanced 権限が必要です。…問題が既存のアプリケーションに起因している場合は、クライアントに問題が存在する可能性があります。詳細またはサポートについては、ネットアップテクニカルサポートにお問い合わせください。

ファイルあたりの最大オープン回数を超えました	警告	TCP 接続でファイルを開くことができる最大回数を超えました。このファイルを開く要求は、ファイルの開いているインスタンスをいくつか閉じるまでは拒否されます。これは通常、異常なアプリケーション動作を示します。	次の修正アクションを実行します。この TCP 接続を使用してクライアントで実行されているアプリケーションを検査します。 クライアントが正しく動作していない可能性があります。クライアントを再起動します。クライアントが新規または既存のアプリケーションによって問題が発生しているかどうかを確認します。アプリケーションが新規である場合は、「 cifs option modify -max-opense -opense-file-per-tree 」コマンドを使用して、クライアントのしきい値を大きく設定します。 クライアントが想定どおりに動作していても、しきい値の上昇が必要となる場合があります。クライアントのしきい値を高く設定するには、 advanced 権限が必要です。…問題が既存のアプリケーションに起因している場合は、クライアントに問題が存在する可能性があります。詳細またはサポートについては、ネットアップテクニカルサポートにお問い合わせください。

NetBIOS 名が競合しています	重要	NetBIOS ネームサービスが、リモートマシンから名前登録要求に対して否定的な応答を受信しました。これは通常、NetBIOS 名またはエイリアスの競合が原因です。その結果、クライアントがデータにアクセスできなくなったり、クラスタ内の適切なデータを提供しているノードに接続できなくなったりすることがあります。	次のいずれかの修正処置を実行します。… NetBIOS 名またはエイリアスに競合がある場合、次のいずれかを実行します。…「 vserver cifs delete -aliases alias -vserver vserver 」コマンドを使用して、重複する NetBIOS エイリアスを削除します。…「 vserver cifs create -aliases alias -vserver vserver 」コマンドを使用して、重複する名前を削除し、新しい名前のエイリアスを追加して、 NetBIOS エイリアスの名前を変更します。… NetBIOS 名にエイリアスが設定されておらず、競合がある場合は、「 vserver cifs delete -vserver vserver 」コマンドと「 vserver cifs create -cifs -server netbiosname 」コマンドを使用して CIFS サーバの名前を変更します。 メモ： CIFS サーバを削除すると、データにアクセスできなくなる可能性があります。…リモートマシンの NetBIOS 名を削除するか、 NetBIOS 名を変更します。
NFSv4 ストアプールを使い果たしました	重要	NFSv4 ストアプールを使い果たしました。	NFS サーバが応答しなくなってから 10 分以上が経過した場合は、ネットアップテクニカルサポートにお問い合わせください。

登録済みのスキャンエンジンがありません	重要	Antivirus Connector は、スキャンエンジンが登録されていないことを ONTAP に通知しました。「 scan-mandatory 」オプションを有効にすると、原因データを使用できなくなることがあります。	次の対処方法を実行します。…アンチウイルスサーバーにインストールされているスキャンエンジンソフトウェアが ONTAP と互換性があることを確認します。スキャンエンジンソフトウェアが実行中で、ローカルループバックを介してアンチウイルスコネクタに接続するように設定されていることを確認します。
Vscan 接続なし	重要	ONTAP では、ウィルススキャン要求への対応に関する Vscan 接続はありません。「 scan-mandatory 」オプションを有効にすると、原因データを使用できなくなることがあります。	スキャナプールが正しく設定され、ウィルス対策サーバがアクティブで ONTAP に接続されていることを確認します。
ノードのルートボリュームのスペースが不足しています	重要	ルートボリュームのスペースが危険なほど少なくなっていることが検出されました。ノードが完全には動作していません。ノードで NFS アクセスと CIFS アクセスが制限されているため、クラスタ内でデータ LIF がフェイルオーバーされる可能性があります。管理機能は、ノードがルートボリューム上のスペースをクリアするためのローカルリカバリ手順に限定されます。	次の対処方法を実行します。…古い Snapshot コピーを削除してルートボリュームのスペースをクリアする、 /mrootDirectory から不要になったファイルを削除する、またはルートボリュームの容量を拡張する。…コントローラをリブートする…詳細やサポートについては、ネットアップのテクニカルサポートにお問い合わせください。
存在しない管理共有です	重要	vscan 問題：クライアントが、存在しない ONTAP_ADMIN$ 共有に接続しようとしました。	指定した SVM ID で Vscan が有効になっていることを確認してください。SVM で Vscan を有効にすると、 SVM 用に ONTAP_ADMIN$ 共有が自動的に作成されます。
NVMe ネームスペースのスペースが不足しています	重要	スペース不足が原因の書き込みエラーが原因で NVMe ネームスペースがオフラインになりました。	ボリュームにスペースを追加し、「 vserver nvme namespace modify 」コマンドを使用して NVMe ネームスペースをオンラインにします。

NVMF の猶予期間 - アクティブ	警告	このイベントは、 NVMe over Fabrics （ NVMe-oF ）プロトコルを使用していてライセンスの猶予期間がアクティブになっている場合に毎日発生します。NVMe-oF 機能には、ライセンスの猶予期間が終了したあとにライセンスが必要です。ライセンスの猶予期間が終了すると、 NVMe-oF 機能は無効になります。	営業担当者に連絡して NVMe-oF ライセンスを取得し、クラスタに追加するか、 NVMe-oF 構成のすべてのインスタンスをクラスタから削除してください。
NVMF の猶予期間 - 終了	警告	NVMe over Fabrics （ NVMe-oF ）ライセンスの猶予期間が終了し、 NVMe-oF 機能は無効になります。	営業担当者に連絡して NVMe-oF ライセンスを取得し、クラスタに追加してください。
NVMF の猶予期間 - 開始	警告	ONTAP 9.5 ソフトウェアへのアップグレード中に NVMe over Fabrics （ NVMe-oF ）設定が検出されました。NVMe-oF 機能を使用するには、ライセンスの猶予期間が終了したあとにライセンスが必要です。	営業担当者に連絡して NVMe-oF ライセンスを取得し、クラスタに追加してください。
オブジェクトストアのホスト解決不可	重要	オブジェクトストアサーバのホスト名を IP アドレスに解決できません。オブジェクトストアクライアントが IP アドレスに解決しないとオブジェクトストアサーバと通信できません。その結果、データにアクセスできなくなる可能性があります。	DNS 設定を調べて、ホスト名が IP アドレスで正しく設定されていることを確認します。

オブジェクトストアのクラスタ間 LIF が停止しています	重要	オブジェクトストアクライアントが、オブジェクトストアサーバと通信するための稼働している LIF を見つけることができません。クラスタ間 LIF が動作可能になるまで、このノードはオブジェクトストアクライアントトラフィックを許可しません。その結果、データにアクセスできなくなる可能性があります。	次の対処方法を実行します。…「 network interface show -role intercluster 」コマンドを使用して、クラスタ間 LIF のステータスを確認します。…クラスタ間 LIF が正しく設定されていて動作していることを確認します。…クラスタ間 LIF が設定されていない場合は、「 network interface create -role intercluster 」コマンドを使用して追加します。
オブジェクトストアシグネチャの不一致	重要	オブジェクトストアサーバに送信された要求の署名が、クライアントで計算された署名と一致しません。その結果、データにアクセスできなくなる可能性があります。	シークレットアクセスキーが正しく設定されていることを確認します。正しく設定されている場合は、ネットアップテクニカルサポートにお問い合わせください。
READDIR タイムアウト	重要	READDIR ファイル処理が、 WAFL で実行が許可されているタイムアウトを超えました。これは、ディレクトリが非常に大きく、スパースであるためです。対処方法を推奨します。	次の対処方法を実行します。…次の「diag」権限ノードシェルCLIコマンドを使用して、READDIRファイル操作が期限切れになった最近のディレクトリに固有の情報を検索します。 WAFL readdir notice show …ディレクトリがスパースとして表示されているかどうかを確認します。…ディレクトリがスパースとして表示されている場合は、ディレクトリの内容を新しいディレクトリにコピーしてディレクトリファイルのスパースを削除することをお勧めします。…ディレクトリがスパースとして示されておらず、ディレクトリが大きい場合は、ディレクトリ内のファイルエントリの数を減らすことでディレクトリファイルのサイズを小さくすることをお勧めします。

アグリゲートの再配置に失敗しました	重要	このイベントは、アグリゲートの再配置時にデスティネーションノードがオブジェクトストアに到達できない場合に発生します。	次の対処方法を実行します。…「 network interface show 」コマンドを使用して、インタークラスタ LIF がオンラインで機能していることを確認します。…デスティネーションノードのクラスタ間 LIF で「 ping 」コマンドを使用して、オブジェクトストアサーバへのネットワーク接続を確認します。…「 aggregate object-store config show 」コマンドを使用して、オブジェクトストアの設定が変更されておらず、ログインおよび接続の情報が正確であることを確認してください。または、再配置コマンドの「 override-destination-checks 」パラメータを使用してエラーを無効にすることもできます。詳細やサポートについては、ネットアップのテクニカルサポートにお問い合わせください。
シャドウコピーに失敗しました	重要	ボリュームシャドウコピーサービス（ VSS ）の実行に失敗しました。 VSS は、 Microsoft Server のバックアップおよびリストアサービス処理です。	イベントメッセージに表示される情報を使用して、次の項目を確認します。… Is shadow copy configuration enabled? …適切なライセンスがインストールされているか？…どの共有でシャドウコピー操作が実行されますか？共有名は正しいですか？共有パスは存在しますか？シャドウコピーセットとそのシャドウコピーの状態はどうなっていますか？

ストレージスイッチの電源装置に障害が発生しました	警告	クラスタスイッチに電源装置がありません。冗長性が低下し、停電が発生するリスクが高まります。	次の対処方法を実行します。クラスタスイッチに電力を供給する電源装置の電源がオンになっていることを確認します。電源コードが電源装置に接続されていることを確認します。問題が解決しない場合は、ネットアップのテクニカルサポートにお問い合わせください。
CIFS 認証が多すぎます	警告	多数の認証ネゴシエーションが同時に行われています。このクライアントからの新規セッション要求は 256 個あります。	クライアントが新しい接続要求を 256 個以上作成した理由を調べます。エラーの原因を特定するために、クライアントまたはアプリケーションのベンダーに問い合わせなければならない場合があります。
管理共有への権限のないユーザアクセス	警告	クライアントが ONTAP_ADMIN$ 共有に接続しようとしましたが、ログインしているユーザが許可されていません。	次の対処方法を実行します。…指定したユーザ名と IP アドレスがアクティブな Vscan スキャナプールの 1 つに設定されていることを確認します。… vserver vscan scanner pool show-active コマンドを使用して、現在アクティブなスキャナプールの設定を確認します。
ウイルスを検出しました	警告	Vscan サーバからストレージシステムにエラーが報告されました。通常は、ウイルスが検出されたことを示します。ただし、 Vscan サーバでその他のエラーが発生すると、このイベントを原因できます。ファイルへのクライアントアクセスは拒否されます。Vscan サーバは、設定に応じて、ファイルをクリーンアップするか、ファイルを隔離するか、または削除する可能性があります。	「 syslog 」イベントで報告された Vscan サーバのログを調べて、感染ファイルのクリーンアップ、隔離、削除が正常に完了したかどうかを確認します。削除できなかった場合は、システム管理者が手動でファイルを削除しなければならないことがあります。
ボリュームはオフラインです	情報	ボリュームがオフラインになりました。	ボリュームをオンラインに戻します。

ボリュームは制限状態です	情報	フレキシブルボリュームが制限されたことを示すイベントです。	ボリュームをオンラインに戻します。
Storage VMが停止しました	情報	このメッセージは、「vserver stop」処理が成功した場合に表示されます。	Storage VMでデータアクセスを開始するには、「vserver start」コマンドを使用します。
ノードのパニック	警告	このイベントはパニック状態になった場合に生成されます	ネットアップカスタマーサポートにお問い合わせください。

トップに戻る

ランサムウェア対策ログモニタ

モニタ名	重大度	説明	対処方法
Storage VM ランサムウェア対策監視が無効になっています	警告	Storage VM のランサムウェア対策監視は無効になっています。Storage VM を保護するには、ランサムウェア対策を有効にしてください。	なし
Storage VM ランサムウェア対策監視有効（ラーニングモード）	情報	Storage VM のランサムウェア対策監視は、学習モードで有効になっています。	なし
Volume Anti-Ransomware Monitoring を有効にしました	情報	ボリュームのランサムウェア対策監視が有効になっている。	なし
ボリュームのアンチランサムウェア監視が無効になっています	警告	ボリュームのランサムウェア対策監視は無効になっています。ランサムウェア対策を有効にしてボリュームを保護	なし
ボリュームのランサムウェア対策監視が有効（ラーニングモード）	情報	ボリュームのランサムウェア対策監視は、学習モードで有効になっています。	なし
ボリュームのアンチランサムウェア監視が一時停止されました（ラーニングモード）	警告	ボリュームのアンチランサムウェアモニタリングが学習モードで一時停止しています。	なし
ボリュームのアンチランサムウェアモニタリングが一時停止されました	警告	ボリュームのランサムウェア対策監視が一時停止されています。	なし
Volume Anti-Ransomware Monitoring Disabling の略	警告	ボリュームのアンチランサムウェア監視が無効になっています。	なし

ランサムウェアのアクティビティが検出され	重要	検出されたランサムウェアからデータを保護するために、元のデータをリストアするために使用できる Snapshot コピーが作成されました。システムによって AutoSupport または「コールホーム」メッセージが生成され、ネットアップテクニカルサポートおよび設定された宛先に送信されます。AutoSupport メッセージを使用すると、問題の特定と解決方法が向上します	ランサムウェアの活動を修復する方法については、「 final-document-name 」を参照してください。

トップに戻る

NetApp ONTAP モニタの **FSX**

モニタ名	しきい値	概要を監視します	対処方法
FSX ボリューム容量がフルです	警告 @>85% …重大 @>95%	アプリケーションとお客様のデータを格納するには、ボリュームのストレージ容量が必要です。ONTAP ボリュームに格納されるデータが多いほど、以降のデータで使用できるストレージ容量は少なくなります。ボリューム内のデータストレージ容量が合計ストレージ容量に達すると、ストレージ容量の不足によりデータを格納できなくなる可能性があります。ボリュームの使用済みストレージ容量を監視して、データサービスの継続性を確保します。	重大のしきい値を超えた場合にサービスの中断を最小限に抑えるには、即時アクションが必要です。 1.スペースを解放するために、不要になったデータを削除することを検討してください

FSX ボリューム高レイテンシ	警告@>1000 µ s…重大@>2000 µ s	ボリュームとは、多くの場合、 DevOps アプリケーション、ホームディレクトリ、データベースなどのパフォーマンス重視のアプリケーションによって I/O トラフィックを処理するオブジェクトです。ボリュームのレイテンシが高いと、アプリケーション自体に影響を及ぼし、タスクを実行できなくなる可能性があります。ボリュームのレイテンシを監視することは、アプリケーションの整合性を維持するうえで非常に重要です。	重大のしきい値を超えた場合にサービスの中断を最小限に抑えるには、即時アクションが必要です。 1.ボリュームに QoS ポリシーが割り当てられている場合は、ボリュームのワークロードが抑制される原因になった場合に制限しきい値を評価します。……警告しきい値を超えた場合には、すぐに次の処理を実行するよう計画してください。 1.ボリュームに QoS ポリシーが割り当てられている場合は、ボリュームのワークロードが調整される原因となった場合に備えて、制限のしきい値を評価します。… 2.ノードの利用率も高い場合は、ボリュームを別のノードに移動するか、ノードの合計ワークロードを減らしてください。
FSX ボリュームの inode 制限	警告 @>85% …重大 @>95%	ファイルを格納するボリュームでは、インデックスノード（ inode ）を使用してファイルメタデータが格納されます。ボリュームが inode の割り当てを使用しなくなると、そのボリュームにはこれ以上ファイルを追加できません。警告アラートは、使用可能な inode の数を増やすために計画的な処理が必要であることを示しています。重大アラートは、ファイル制限の枯渇が差し迫っていることを示し、サービスの継続性を確保するために inode を解放するための緊急対策を講じる必要があることを示しています	重大のしきい値を超えた場合にサービスの中断を最小限に抑えるには、即時アクションが必要です。 1.ボリュームの inode の値を増やすことを検討してください。inode の値がすでに最大値に達している場合は、ファイルシステムが最大サイズを超えているため、ボリュームを 2 つ以上のボリュームに分割することを検討してください。次の処理は、警告しきい値に違反した場合にすぐに実行されます。 1.ボリュームの inode の値を増やすことを検討してください。inode の値がすでに最大値に達している場合は、ファイルシステムの最大サイズを超えたためにボリュームを 2 つ以上のボリュームにスプリットすることを検討してください

FSX ボリュームの qtree クォータオーバーコミット	警告 @>95% …危険 @>100%	ボリュームの qtree クォータオーバーコミットは、ボリュームが qtree クォータによってオーバーコミットされているとみなす割合を示します。ボリュームの qtree クォータの設定しきい値に達しました。ボリューム qtree クォータオーバーコミットを監視することで、ユーザに中断のないデータサービスが確実に提供されます。	重大しきい値を超えた場合は、サービスの中断を最小限に抑えるためにすぐに対処する必要があります。 1.不要なデータを削除します。警告しきい値を超えた場合は、ボリュームの容量を増やすことを検討してください。
FSX Snapshot リザーブスペースがフルです	警告@>90%…重大@>95%	アプリケーションとお客様のデータを格納するには、ボリュームのストレージ容量が必要です。スナップショット予約領域と呼ばれる領域の一部はスナップショットの保存に使用され、データをローカルで保護できます。ONTAP ボリュームに格納される新規データや更新データが多いほど、使用される Snapshot 容量は増えますが、今後追加または更新されるデータに使用できる Snapshot ストレージ容量は少なくなります。ボリューム内の Snapshot データ容量が Snapshot リザーブの合計スペースに達すると、新しい Snapshot データを格納できなくなり、ボリューム内のデータの保護レベルが低下する可能性があります。ボリュームの使用済み Snapshot 容量を監視して、データサービスの継続性を確保します。	重大のしきい値を超えた場合にサービスの中断を最小限に抑えるには、即時アクションが必要です。 1.スナップショット予約がいっぱいになったときに、ボリューム内のデータ領域を使用するようにスナップショットを設定することを検討してください。 2.容量を解放するために不要になった古いスナップショットを削除することを検討してください……警告しきい値を超えた場合には、すぐに次のアクションを実行するよう計画してください。 …1.ボリューム内のスナップショット予約容量を増やして、増加に対応することを検討してください。 2.Snapshot リザーブがフルになったときにボリューム内のデータスペースを使用するように Snapshot を設定することを検討してください

FSX ボリュームキャッシュミス率	警告 @>95% …危険 @>100%	ボリュームキャッシュミス率は、クライアントアプリケーションからの読み取り要求に対してキャッシュからではなくディスクからデータが返される割合です。これは、ボリュームが設定されたしきい値に達したことを意味します。	重大しきい値を超えた場合は、サービスの中断を最小限に抑えるためにすぐに対処する必要があります。 1.ボリュームのノードから一部のワークロードを移動してIO負荷を軽減します 2. QoS制限により、同じノード上の優先度の低いワークロードの要求を下げます。警告しきい値を超えた場合は、すぐに対処することを検討します。 1.ボリュームのノードから一部のワークロードを移動してIO負荷を軽減します 2. QoS制限により、同じノード上で優先度の低いワークロードの負荷を軽減します 3.ワークロードの特性（ブロックサイズ、アプリケーションのキャッシュなど）の変更

トップに戻る

K8s モニタ

モニタ名	説明	対処方法	重大度/しきい値

永続ボリュームレイテンシが高い	高レイテンシの永続ボリュームは、アプリケーション自体に影響を及ぼし、タスクを実行できない可能性があることを意味します。アプリケーションの一貫したパフォーマンスを維持するには、永続ボリュームのレイテンシを監視することが重要です。メディアタイプに基づく想定レイテンシは、最大 1 ～ 2 ミリ秒、SAS は最大 8 ～ 10 ミリ秒、 SATA HDD は 17 ～ 20 ミリ秒です	即時アクション 重大しきい値を超えた場合は、ただちに対処してサービスの中断を最小限に抑えることを検討してください。 ボリュームにQoSポリシーが割り当てられている場合は、制限のしきい値が原因でボリュームのワークロードが調整されていないかどうかを評価します。 すぐに実行するアクション 警告しきい値を超えている場合は、すぐに次のアクションを計画してください。 1.ストレージプールの利用率も高い場合は、ボリュームを別のストレージプールに移動します。 2. ボリュームに QoS ポリシーが割り当てられている場合、ボリュームワークロードが調整される原因となった場合に備えて、制限しきい値を評価します。 3. コントローラの利用率が高い場合は、ボリュームを別のコントローラに移動するか、コントローラの総ワークロードを減らします。	警告@> 6、000 µ s 臨界@> 12、000 µ s
クラスタメモリ飽和度高	クラスタの割り当て可能メモリの飽和度が高くなっています。 クラスタのCPU飽和度は、メモリ使用量の合計をすべてのKubernetesノードの割り当て可能なメモリの合計で割った値です。	ノードを追加します。 スケジュールされていないノードを修正します。 適切なサイズのポッドでノードのメモリを解放	警告@> 80% 重大@> 90%
ポッドの接続に失敗しました	このアラートは、ポッドとのボリューム接続に失敗した場合に発生します。		警告

高い再送信レート	高いTCP再送信レート	ネットワークの輻輳を確認する-ネットワーク帯域幅を大量に消費するワークロードを特定します。 PodのCPU利用率が高いかどうかを確認します。 ハードウェアネットワークのパフォーマンスを確認します。	警告@> 10% 重大@> 25%
ノードファイルシステム容量上限	ノードファイルシステム容量上限	-アプリケーションファイル用の十分なスペースを確保するために、ノードディスクのサイズを拡張します。 -アプリケーションファイルの使用量を削減します。	警告@> 80% 重大@> 90%
ワークロードネットワークジッタ上限	高いTCPジッタ（レイテンシ/応答時間の変動が大きい）	ネットワークの輻輳を確認します。ネットワーク帯域幅を大量に消費するワークロードを特定します。 PodのCPU利用率が高いかどうかを確認します。 ハードウェアネットワークのパフォーマンスの確認	警告@> 30 ms CRITICAL @> 50 ms

永続的ボリュームのスループット	永続ボリュームの MBps のしきい値を使用して、永続ボリュームが事前に定義されたパフォーマンスの期待値を超えたときに管理者にアラートを送信し、他の永続ボリュームに影響を及ぼしている可能性があるこのモニタをアクティブにすると、SSD 上の永続的ボリュームの一般的なスループットプロファイルに適したアラートが生成されます。このモニタでは、環境内のすべての永続ボリュームを監視します。警告および重大のしきい値は、監視目標に基づいてこのモニタを複製し、ストレージクラスに適したしきい値を設定することで調整できます。さらに、環境内の永続ボリュームのサブセットを対象とすることもできます。	即時アクション 重大しきい値を超えた場合は、サービスの中断を最小限に抑えるための迅速な対処を計画してください。 1.ボリュームのQoS MBpsの上限を設定します。 2. ボリュームのワークロードを処理しているアプリケーションに異常がないかを確認します。 すぐに実行するアクション 警告しきい値を超えている場合は、次のアクションをすぐに実行するように計画してください。 1.ボリュームのQoS MBpsの上限を設定します。 2. ボリュームのワークロードを処理しているアプリケーションに異常がないかを確認します。	警告@> 10、000 MB/秒 重大@> 15、000 MB/秒
OOMが終了する危険性のあるコンテナ	コンテナのメモリ制限が低すぎます。コンテナが削除される可能性があります（Out of Memory Kill）。	コンテナメモリの上限を引き上げます。	警告@> 95%
ワークロード停止	ワークロードに正常なポッドがありません。		重大@< 1
永続的ボリューム要求のバインドに失敗しました	このアラートは、 PVC でバインディングが失敗した場合に発生します。		警告
リソースクォータのメモリ制限を超えようとしています	ネームスペースのメモリ制限がResourceQuotaを超えようとしています		警告@> 80% 重大@> 90%
ResourceQuotaのメモリ要求が超過しようとしています	ネームスペースのメモリ要求がResourceQuotaを超えようとしています		警告@> 80% 重大@> 90%
ノード作成に失敗しました	設定エラーのため、ノードをスケジュールできませんでした。	Kubernetesイベントログで、設定エラーの原因を確認します。	重要
永続的ボリュームの再生に失敗しました	ボリュームの自動再生に失敗しました。		警告@>0 B

コンテナのCPUスロットリング	コンテナのCPU制限が低すぎます。コンテナプロセスの速度が低下します。	コンテナのCPU制限を引き上げます。	警告@> 95% 重大@> 98%
サービスロードバランサを削除できませんでした			警告
永続ボリューム IOPS	永続ボリュームの IOPS しきい値を使用すると、永続ボリュームが事前に定義されたパフォーマンスの期待値を超えたときに管理者に通知することができます。このモニタをアクティブにすると、永続ボリュームの一般的な IOPS プロファイルに適したアラートが生成されます。このモニタでは、環境内のすべての永続ボリュームを監視します。警告および重大のしきい値は、このモニタを複製し、ワークロードに適したしきい値を設定することで、監視の目標に基づいて調整できます。	即時アクション 重大しきい値に違反した場合は、サービスの中断を最小限に抑えるための即時アクションを計画します。 1.ボリュームのQoS IOPS制限を導入します。 2. ボリュームのワークロードを処理しているアプリケーションに異常がないかを確認します。 すぐに実行するアクション 警告しきい値を超えている場合は、すぐに次のアクションを計画してください。 1.ボリュームのQoS IOPS制限を導入します。 2. ボリュームのワークロードを処理しているアプリケーションに異常がないかを確認します。	警告@> 20、000 IO/秒 重大@> 25、000 IO/秒
サービスロードバランサを更新できませんでした			警告
ポッドのマウントに失敗しました	このアラートは、ポッドでマウントに失敗したときに発生します。		警告
ノードPID圧力	（Linux）ノードで使用可能なプロセス識別子が削除しきい値を下回っています。	多数のプロセスを生成し、使用可能なプロセスIDのノードを枯渇させるポッドを検索して修正します。 プロセスを生成するポッドやコンテナからノードを保護するには、PodPidsLimitを設定します。	重大@>0

ポッドイメージのプルエラー	Kubernetesがポッドコンテナイメージを取得できませんでした。	-ポッド構成でポッドのイメージのスペルが正しいことを確認します。 -レジストリにイメージタグが存在することを確認してください。 -イメージレジストリのクレデンシャルを確認します。 -レジストリ接続の問題を確認します。 -公共のレジストリプロバイダーによって課されたレート制限に達していないことを確認します。	警告
ジョブの実行時間が長すぎます	ジョブの実行時間が長すぎます		警告@> 1時間 重大@> 5時間
ノードメモリ上限	ノードのメモリ使用率が高くなっています	ノードを追加します。 スケジュールされていないノードを修正します。 適切なサイズのポッドでノードのメモリを解放	警告@> 85% 重大@> 90%
ResourceQuotaのCPU制限を超えようとしています	ネームスペースのCPU制限がリソースクォータを超えようとしています		警告@> 80% 重大@> 90%
ポッドクラッシュループバックオフ	ポッドがクラッシュし、何度も再起動しようとしました。		重大@>3
ノードCPU高	ノードのCPU使用率が高くなっています。	ノードを追加します。 スケジュールされていないノードを修正します。 適切なサイズのポッドでノードのCPUを解放	警告@> 80% 重大@> 90%
ワークロードネットワークレイテンシのRTTが高い	高いTCP RTT（Round Trip Time）遅延	Check for Network congestion：ネットワーク帯域幅を大量に消費するワークロードを特定します。 PodのCPU利用率が高いかどうかを確認します。 ハードウェアネットワークのパフォーマンスを確認します。	警告@> 150 ms 重大@> 300 ms
ジョブ失敗	ノードのクラッシュまたはリブート、リソースの枯渇、ジョブのタイムアウト、またはポッドのスケジュール設定エラーが原因で、ジョブが正常に完了しませんでした。	Kubernetesイベントログで障害の原因を確認します。	警告@>1

永続的ボリュームが数日でフル	永続的ボリュームのスペースが数日後に不足します	-ボリュームサイズを大きくして、アプリケーションファイル用の十分な空き容量を確保します。 -アプリケーションに保存されるデータ量を削減します。	警告（8日未満） 重大（3日未満）
ノードのメモリ圧力	ノードのメモリが不足しています。使用可能なメモリが削除しきい値に達しました。	ノードを追加します。 スケジュールされていないノードを修正します。 適切なサイズのポッドでノードのメモリを解放	重大@>0
ノード-準備完了	ノードの準備が5分間完了していません	ノードに十分なCPU、メモリ、およびディスクリソースがあることを確認します。 ノードのネットワーク接続を確認してください。 Kubernetesイベントログで障害の原因を確認します。	重大@< 1
永続的ボリュームの容量が上限です	永続的ボリュームバックエンドの使用容量が多くなっています。	-ボリュームサイズを大きくして、アプリケーションファイル用の十分な空き容量を確保します。 -アプリケーションに保存されるデータ量を削減します。	警告@> 80% 重大@> 90%
サービスロードバランサを作成できませんでした	サービスロードバランサの作成に失敗しました		重要
ワークロードレプリカの不一致	現在、一部のポッドはDeploymentまたはDaemonSetで使用できません。		警告@>1
ResourceQuota CPU要求が超過しようとしています	ネームスペースのCPU要求がリソースクォータを超えようとしています		警告@> 80% 重大@> 90%
高い再送信レート	高いTCP再送信レート	ネットワークの輻輳を確認する-ネットワーク帯域幅を大量に消費するワークロードを特定します。 PodのCPU利用率が高いかどうかを確認します。 ハードウェアネットワークのパフォーマンスを確認します。	警告@> 10% 重大@> 25%

ノードディスク圧力	ノードのルートファイルシステムまたはイメージファイルシステムで使用可能なディスクスペースとinodeが削除しきい値を超えています。	-アプリケーションファイル用の十分なスペースを確保するために、ノードディスクのサイズを拡張します。 -アプリケーションファイルの使用量を削減します。	重大@>0
クラスタのCPU飽和度-上限	クラスタの割り当て可能なCPU使用率が高くなっています。 クラスタのCPU使用率は、CPU使用率の合計をすべてのKubernetesノードの割り当て可能なCPUの合計で割って算出されます。	ノードを追加します。 スケジュールされていないノードを修正します。 適切なサイズのポッドでノードのCPUを解放	警告@> 80% 重大@> 90%

トップに戻る

変更ログモニタ

モニタ名	重大度	概要を監視します
内部ボリュームが検出されました	情報	このメッセージは、内部ボリュームが検出された場合に表示されます。
内部ボリュームが変更されました	情報	このメッセージは、内部ボリュームが変更された場合に表示されます。
ストレージノードを検出	情報	このメッセージは、ストレージノードが検出された場合に表示されます。
ストレージノードが削除されました	情報	このメッセージは、ストレージノードが削除された場合に表示されます。
ストレージプールが検出されました	情報	このメッセージは、ストレージプールが検出された場合に表示されます。
Storage Virtual Machineを検出	情報	このメッセージは、Storage Virtual Machineが検出された場合に表示されます。
Storage Virtual Machineを変更	情報	このメッセージは、Storage Virtual Machineが変更された場合に表示されます。

トップに戻る

データ収集モニタ

モニタ名	説明	対処方法
Acquisition Unit のシャットダウン	Data Infrastructure Insights Acquisition Unitは、アップグレードの一環として定期的に再起動し、新機能を導入します。これは、一般的な環境で月に1回以下の頻度で発生します。Acquisition Unitがシャットダウンしたという警告アラートのすぐ後に、新しく再起動したAcquisition UnitがData Infrastructure Insightsへの登録を完了したことを示す解決策が表示されます。通常、このシャットダウンと登録のサイクルには5～15分かかります。	このアラートが頻繁に発生する場合や15分以上続く場合は、Acquisition Unit、ネットワーク、およびAUをインターネットに接続するプロキシをホストしているシステムの動作を確認してください。
コレクタでエラーが	データコレクタのポーリングで予期しない障害が発生しました。	Data Infrastructure Insightsのデータコレクタページにアクセスして、状況の詳細を確認してください。
コレクタ警告	このアラートは通常、データコレクタまたはターゲットシステムの設定に誤りがある場合に発生します。今後のアラートを防止するために、設定を再確認してください。また、データコレクタがすべてのデータを収集した、完了していないデータの取得が原因の可能性もあります。これは、データ収集中に状況が変化した場合に発生します（データ収集の開始時に存在する仮想マシンが、データ収集の実行中とキャプチャの前に削除された場合など）。	データコレクタまたはターゲットシステムの設定を確認します。 コレクタ警告のモニタは他のモニタタイプよりも多くのアラートを送信できるため、トラブルシューティングを行っていない限り、アラート受信者を設定しないことをお勧めします。

トップに戻る

セキュリティモニタ

モニタ名	しきい値	概要を監視します	対処方法

AutoSupport HTTPS 転送が無効です	警告@<1>	AutoSupport は、転送プロトコルとして HTTPS 、 HTTP 、 SMTP をサポートしています。AutoSupport メッセージは機密性が高いため、ネットアップでは、AutoSupport メッセージをネットアップサポートに送信する際のデフォルト転送プロトコルとして HTTPS を使用することを強く推奨しています。	AutoSupport メッセージの転送プロトコルとしてHTTPSを設定するには、次のONTAP コマンドを実行します。…system node AutoSupport modify -transport https
SSH用のクラスタのセキュアでない暗号	警告@<1>	SSHでセキュアでない暗号（たとえば、*CBCで始まる暗号）が使用されていることを示します。	CBC暗号を削除するには、次のONTAP コマンドを実行します。…security ssh remove -vserver <admin vserver>-ciphers aes256-cbc、aes192-cbc、aes128-cbc、3des-cbc
クラスタでログインバナーが無効になりました	警告@<1>	ONTAP システムにアクセスするユーザに対してログインバナーが無効になっていることを示します。ログインバナーを表示すると、システムに期待されるアクセス方法や使用方法を設定するのに役立ちます。	クラスタにログインバナーを設定するには、次のONTAP コマンドを実行します。…security login banner modify -vserver <admin SVM>-message "権限のあるユーザだけがアクセスできます"
クラスタピア通信が暗号化されていません	警告@<1>	ディザスタリカバリ、キャッシング、またはバックアップのためにデータをレプリケートする場合は、ONTAP クラスタから別のクラスタにデータを転送するときに、そのデータを保護する必要があります。ソースとデスティネーションの両方のクラスタで暗号化を設定する必要があります。	ONTAP 9.6よりも前に作成されたクラスタピア関係に対して暗号化を有効にするには、ソースとデスティネーションのクラスタを9.6にアップグレードする必要があります。その後、「cluster peer modify」コマンドを使用して、クラスタピアリング暗号化を使用するようにソースとデスティネーション両方のクラスタピアを変更します。詳細については、『ONTAP 9セキュリティ設定ガイド』を参照してください。

デフォルトのローカル管理者ユーザが有効です	警告@>0	ロックコマンドを使用して、不要なデフォルトの管理ユーザ（組み込み）アカウントをロック（無効化）することを推奨します。これらは主に、パスワードが更新または変更されていないデフォルトアカウントです。	組み込みの「admin」アカウントをロックするには、次のONTAP コマンドを実行します。…security login lock-username admin
FIPSモードが無効になりました	警告@<1>	FIPS 140-2への準拠を有効にすると、TLSv1とSSLv3は無効になり、TLSv1.1とTLSv1.2のみが引き続き有効になります。ONTAP では、FIPS 140-2準拠モードが有効な場合、TLSv1とSSLv3を有効にすることはできません。	クラスタでFIPS 140-2準拠モードを有効にするには、次のONTAP コマンドをadvanced権限モードで実行します。…security config modify -interface SSL -is-fips-enabled true
ログ転送が暗号化されていない	警告@<1>	セキュリティ違反の影響が1つのシステムまたは解決策 に限定されるように、syslog情報のオフロードが必要です。そのため、syslog情報を安全なストレージまたは保持場所に安全にオフロードすることを推奨します。	ログの転送先を作成したあとにプロトコルを変更することはできません。暗号化されたプロトコルに変更するには、次のONTAP コマンドを使用して、ログの転送先を削除して再作成します。…cluster log-forwarding create -destination <destination ip>-protocol tcp-encrypted
MD5ハッシュ化パスワード	警告@>0	ONTAP ユーザアカウントのパスワードには、より安全なSHA-512ハッシュ関数を使用することを推奨します。安全性の低いMD5ハッシュ関数を使用するアカウントは、SHA-512ハッシュ関数に移行する必要があります。	ユーザに解決策 MD5ハッシュ関数を使用するパスワードでアカウントをロックするには、次のONTAP コマンドを実行します。…security login lock -vserver *-username *-hash-function MD5
NTPサーバが設定されていません	警告@<1>	クラスタにNTPサーバが設定されていないことを示します。冗長性と最適なサービスを実現するために、最低3台のNTPサーバをクラスタに関連付けることを推奨します。	NTPサーバをクラスタに関連付けるには、次のONTAPコマンドを実行します。 cluster time-service ntp server create -server <ntp server host name or ip address>の略

NTPサーバ数が不足しています	警告@<3.	クラスタに設定されているNTPサーバが3台未満であることを示します。冗長性と最適なサービスを実現するために、最低3台のNTPサーバをクラスタに関連付けることを推奨します。	クラスタにNTPサーバを関連付けるには、次のONTAP コマンドを実行します。…cluster time-service ntp server create -server <ntp server host name or ip address>
リモートシェルが有効です	警告@>0	リモートシェルは、ONTAP 解決策 へのコマンドラインアクセスを確立するためのセキュアな方法ではありません。セキュアなリモートアクセスのために、リモートシェルを無効にする必要があります。	ネットアップでは、セキュアなリモートアクセスのためにSecure Shell（SSH）を推奨しています。クラスタでリモートシェルを無効にするには、advanced権限モードで次のONTAP コマンドを実行します。…security protocol modify -application rsh -enabled false
Storage VM監査ログが無効になりました	警告@<1>	SVMで監査ログが無効になっていることを示します。	SVMの監査ログを設定するには、次のONTAP コマンドを実行します。…vserver audit enable -vserver <svm>
SSH用のStorage VMのセキュアでない暗号	警告@<1>	SSHでセキュアでない暗号（たとえば、*CBCで始まる暗号）が使用されていることを示します。	CBC暗号を削除するには、次のONTAP コマンドを実行します。…security ssh remove -vserver <vserver>-ciphers aes256-cbc、aes192-cbc、aes128-cbc、3des-cbc
Storage VMのログインバナーが無効になっています	警告@<1>	システムでSVMにアクセスするユーザに対してログインバナーが無効になっていることを示します。ログインバナーを表示すると、システムに期待されるアクセス方法や使用方法を設定するのに役立ちます。	クラスタにログインバナーを設定するには、次のONTAP コマンドを実行します。…security login banner modify -vserver <svm>-message "権限のあるユーザだけがアクセスできます"

Telnetプロトコルが有効です	警告@>0	Telnetは、ONTAP 解決策へのコマンドラインアクセスを確立するためのセキュアな方法ではありません。セキュアなリモートアクセスのためにTelnetを無効にする必要があります。	ネットアップでは、セキュアなリモートアクセスのために Secure Shell （ SSH ）を推奨しています。 クラスタでTelnetを無効にするには、次のONTAP コマンドをadvanced権限モードで実行します。…security protocol modify -application telnet -enabled false

トップに戻る

データ保護モニタ

モニタ名	しきい値	概要を監視します	対処方法
LUN Snapshotコピー用の十分なスペースがありません	（contains _luns = Yes ）Warning @> 95%…Critical @> 100%	アプリケーションとお客様のデータを格納するには、ボリュームのストレージ容量が必要です。スナップショット予約領域と呼ばれる領域の一部はスナップショットの保存に使用され、データをローカルで保護できます。ONTAP ボリュームに格納される新規データや更新データが多いほど、使用される Snapshot 容量は増えますが、今後追加または更新されるデータに使用できる Snapshot ストレージ容量は少なくなります。ボリューム内のSnapshotデータ容量がSnapshotリザーブスペースの合計に達すると、新しいSnapshotデータを格納できなくなり、ボリューム内のLUN内のデータの保護レベルが低下する可能性があります。ボリュームの使用済み Snapshot 容量を監視して、データサービスの継続性を確保します。	即時アクション 重大しきい値を超えた場合は、ただちに対処してサービスの中断を最小限に抑えることを検討してください。 1.スナップショット予約がいっぱいになったときにボリュームのデータスペースを使用するようにスナップショットを構成します。 2. 古い不要なスナップショットをいくつか削除して、領域を解放します。 すぐに実行するアクション 警告しきい値を超えている場合は、次のアクションをすぐに実行するように計画してください。 1.ボリューム内のスナップショット・リザーブ・スペースを拡張して’増加に対応します 2. スナップショット予約がいっぱいになったときにボリューム内のデータ領域を使用するようにスナップショットを設定します。

SnapMirror関係の遅延	警告@>150%…重大@>300%	SnapMirror関係の遅延は、Snapshotのタイムスタンプとデスティネーションシステムの時間の差です。lag_time_ percentは、SnapMirrorポリシーのスケジュール間隔に対する遅延時間の比率です。遅延時間がスケジュール間隔と等しい場合、lag_time_パーセントは100%になります。SnapMirrorポリシーにスケジュールが設定されていない場合、lag_time_ percentは計算されません。	snapmirror showコマンドを使用して、SnapMirrorのステータスを監視します。snapmirror show-historyコマンドを使用して、SnapMirror転送の履歴を確認します

トップに戻る

Cloud Volume（CVO）モニタ

モニタ名	CI の重大度	概要を監視します	対処方法
CVO Disk Out of Service』を参照してください	情報	「このイベントは、ディスクが障害としてマークされているか、完全消去中であるか、Maintenance Center に入力されたためにサービスから削除された場合に発生します。」	なし

ストレージプールのCVOギブバックに失敗しました	重要	ストレージフェイルオーバー（ SFO ）ギブバックの一環としてアグリゲートを移行したときに、デスティネーションノードがオブジェクトストアに到達できない場合に発生します。	次の対処方法を実行します。 「 network interface show 」コマンドを使用して、インタークラスタ LIF がオンラインで機能していることを確認します。 デスティネーションノードのクラスタ間LIFで「ping」コマンドを使用して、オブジェクトストアサーバへのネットワーク接続を確認してください。 aggregate object-store config showコマンドを使用して、オブジェクトストアの設定が変更されておらず、ログインおよび接続の情報がまだ正確であることを確認してください。 また、 giveback コマンドの「 require-partner-waiting 」パラメータに false を指定して、エラーを無効にすることもできます。 詳細またはサポートについては、ネットアップテクニカルサポートにお問い合わせください。

CVO HAインターコネクトが停止しています	警告	ハイアベイラビリティ（HA）インターコネクトが停止しています。フェイルオーバーを利用できない場合、サービスが停止するリスクがあります。	対処方法は、プラットフォームでサポートされている HA インターコネクトリンクの数と種類、およびインターコネクトが停止している理由によって異なります。 リンクがダウンしている場合： HAペアの両方のコントローラが動作していることを確認します。 外部接続リンクの場合は、インターコネクトケーブルが正しく接続されていることと、Small Form-Factor Pluggable（SFP）がある場合は、両方のコントローラに正しく取り付けられていることを確認してください。 内部接続リンクの場合は、「ic link off」コマンドと「ic link on」コマンドを使用して、一方のリンクを無効にし、再度有効にします。 リンクが無効になっている場合は、「ic link on」コマンドを使用してリンクを有効にします。 ピアが接続されていない場合は、「IC link off」コマンドと「IC link on」コマンドを使用して、一方のリンクをディセーブルにし、再度イネーブルにします。 問題が解決しない場合は、ネットアップテクニカルサポートにお問い合わせください。

ユーザあたりのCVOの最大セッション数を超えました	警告	TCP 接続でのユーザあたりの最大許容セッション数を超えました。セッションを確立する要求は、一部のセッションが解放されるまで拒否されます。	次の対処方法を実行します。 クライアントで実行されているすべてのアプリケーションを調べて、正常に動作していないアプリケーションを終了します。 クライアントをリブートします。 問題の原因が新規または既存のアプリケーションかどうかを確認します。 アプリケーションが新規の場合は、「 cifs option modify -max-opense -opense-same -file-per -tree 」コマンドを使用して、クライアントのしきい値を高く設定します。クライアントが想定どおりに動作していても、しきい値の上昇が必要となる場合があります。クライアントのしきい値を高く設定するには、advanced 権限が必要です。 既存のアプリケーションが問題 の原因である場合は、クライアントに問題がある可能性があります。詳細またはサポートについては、ネットアップテクニカルサポートにお問い合わせください。

CVO NetBIOS名が競合しています	重要	NetBIOS ネームサービスが、リモートマシンから名前登録要求に対して否定的な応答を受信しました。これは通常、NetBIOS 名またはエイリアスの競合が原因です。その結果、クライアントがデータにアクセスできなくなったり、クラスタ内の適切なデータを提供しているノードに接続できなくなったりすることがあります。	次のいずれかの対処方法を実行します。 NetBIOS名またはエイリアスが競合している場合は、次のいずれかを実行します。 「vserver cifs delete-aliases alias -vserver vserver」コマンドを使用して、重複するNetBIOSエイリアスを削除します。 「vserver cifs create -aliases alias alias -vserver vserver」コマンドを使用して、重複する名前を削除し、新しい名前のエイリアスを追加してNetBIOSエイリアスの名前を変更します。 エイリアスが設定されておらず、NetBIOS名に競合がある場合は、「vserver cifs delete -vserver vserver」コマンドと「vserver cifs create -cifs -server netbiosname」コマンドを使用してCIFSサーバの名前を変更します。 メモ： CIFS サーバを削除すると、データにアクセスできなくなる可能性があります。 NetBIOS名を削除するか、リモートマシンのNetBIOS名を変更します。
CVO NFSv4のストアプールを使い果たしました	重要	NFSv4 ストアプールを使い果たしました。	NFS サーバが応答しなくなってから 10 分以上が経過した場合は、ネットアップテクニカルサポートにお問い合わせください。
CVOノードのパニック	警告	このイベントはパニック状態になった場合に生成されます	ネットアップカスタマーサポートにお問い合わせください。

CVOノードのルートボリュームのスペースが不足しています	重要	ルートボリュームのスペースが危険なほど少なくなっていることが検出されました。ノードが完全には動作していません。ノードで NFS アクセスと CIFS アクセスが制限されているため、クラスタ内でデータ LIF がフェイルオーバーされる可能性があります。管理機能は、ノードがルートボリューム上のスペースをクリアするためのローカルリカバリ手順に限定されます。	次の対処方法を実行します。 古い Snapshot コピーを削除するか、/mrootdirectory から不要になったファイルを削除するか、またはルートボリュームの容量を拡張して、ルートボリュームのスペースをクリアします。 コントローラをリブートします。 詳細またはサポートについては、ネットアップテクニカルサポートにお問い合わせください。
CVOが存在しない管理者共有です	重要	vscan 問題：クライアントが、存在しない ONTAP_ADMIN$ 共有に接続しようとしました。	指定した SVM ID で Vscan が有効になっていることを確認してください。SVM で Vscan を有効にすると、 SVM 用に ONTAP_ADMIN$ 共有が自動的に作成されます。
CVOオブジェクトストアのホスト解決不可	重要	オブジェクトストアサーバのホスト名を IP アドレスに解決できません。オブジェクトストアクライアントが IP アドレスに解決しないとオブジェクトストアサーバと通信できません。その結果、データにアクセスできなくなる可能性があります。	DNS 設定を調べて、ホスト名が IP アドレスで正しく設定されていることを確認します。

CVOオブジェクトストアのクラスタ間LIFが停止しています	重要	オブジェクトストアクライアントが、オブジェクトストアサーバと通信するための稼働している LIF を見つけることができません。クラスタ間 LIF が動作可能になるまで、このノードはオブジェクトストアクライアントトラフィックを許可しません。その結果、データにアクセスできなくなる可能性があります。	次の対処方法を実行します。 「 network interface show -role intercluster 」コマンドを使用して、クラスタ間 LIF のステータスを確認します。 クラスタ間LIFが正しく設定され、動作していることを確認してください。 インタークラスタLIFが設定されていない場合は、「network interface create -role intercluster」コマンドを使用して追加します。
CVOオブジェクトストアシグネチャの不一致	重要	オブジェクトストアサーバに送信された要求の署名が、クライアントで計算された署名と一致しません。その結果、データにアクセスできなくなる可能性があります。	シークレットアクセスキーが正しく設定されていることを確認します。正しく設定されている場合は、ネットアップテクニカルサポートにお問い合わせください。
CVO QoS監視メモリの最大化	重要	QoS サブシステムの動的メモリが現在のプラットフォームハードウェアの上限に達しました。一部の QoS 機能は、制限された容量で動作する場合があります。	いくつかのアクティブなワークロードまたはストリームを削除してメモリを解放してください。アクティブなワークロードを判別するには、「statistics show -object workloads counter ops」コマンドを使用します。アクティブなワークロードに対する処理がゼロ以外の処理を示しています。次に、「workload delete <workloads name>」コマンドを複数回使用して、特定のワークロードを削除します。または、「stream delete-workload <workload name>*」コマンドを使用して、アクティブなワークロードから関連するストリームを削除します。

CVO READDIRタイムアウト	重要	READDIR ファイル処理が、 WAFL で実行が許可されているタイムアウトを超えました。これは、ディレクトリが非常に大きく、スパースであるためです。対処方法を推奨します。	次の対処方法を実行します。 次の「diag」権限ノードシェルCLIコマンドを使用して、READDIRファイル操作が期限切れになった最近のディレクトリに固有の情報を検索します。WAFL readdir notice show ディレクトリがスパースと表示されているかどうかを確認します。 ディレクトリがスパースとして示されている場合は、ディレクトリの内容を新しいディレクトリにコピーして、ディレクトリファイルの sparsess を削除することをお勧めします。 ディレクトリがスパースとして示されておらず、ディレクトリが大きい場合は、ディレクトリ内のファイルエントリの数を減らすことでディレクトリファイルのサイズを縮小することを推奨します。

ストレージプールのCVOの再配置に失敗しました	重要	このイベントは、アグリゲートの再配置時にデスティネーションノードがオブジェクトストアに到達できない場合に発生します。	次の対処方法を実行します。 「 network interface show 」コマンドを使用して、インタークラスタ LIF がオンラインで機能していることを確認します。 デスティネーションノードのクラスタ間LIFで「ping」コマンドを使用して、オブジェクトストアサーバへのネットワーク接続を確認してください。 aggregate object-store config showコマンドを使用して、オブジェクトストアの設定が変更されておらず、ログインおよび接続の情報がまだ正確であることを確認してください。 また、再配置コマンドの「 override -destination -checks 」パラメータを使用して、このエラーを無視することもできます。 詳細またはサポートについては、ネットアップテクニカルサポートにお問い合わせください。

CVOシャドウコピーが失敗しました	重要	ボリュームシャドウコピーサービス（ VSS ）の実行に失敗しました。 VSS は、 Microsoft Server のバックアップおよびリストアサービス処理です。	イベントメッセージに表示された情報を使用して、次の点を確認します。 シャドウコピーの設定が有効かどうか 適切なライセンスがインストールされているか。 どの共有でシャドウコピー処理が実行されますか。 共有名は正しいですか？ 共有パスが存在するか。 シャドウコピーセットとそのシャドウコピーの状態
CVO Storage VMが停止されました	情報	このメッセージは、「vserver stop」処理が成功した場合に表示されます。	Storage VMでデータアクセスを開始するには、「vserver start」コマンドを使用します。
CVOにCIFS認証が多すぎます	警告	多数の認証ネゴシエーションが同時に行われています。このクライアントからの新規セッション要求は 256 個あります。	クライアントが新しい接続要求を 256 個以上作成した理由を調べます。エラーの原因を特定するために、クライアントまたはアプリケーションのベンダーに問い合わせなければならない場合があります。
CVOの未割り当てディスク	情報	システムに未割り当てのディスクがあります - 容量が無駄になっており、構成の設定ミスや部分的な変更がシステムに適用されている可能性があります。	次の対処方法を実行します。 disk show -n コマンドを使用して、割り当てが解除されたディスクを確認します。 disk assignコマンドを使用して、ディスクをシステムに割り当てます。

CVO：管理者共有への不正なユーザアクセス	警告	クライアントが ONTAP_ADMIN$ 共有に接続しようとしましたが、ログインしているユーザが許可されていません。	次の対処方法を実行します。 指定したユーザ名と IP アドレスがアクティブな Vscan スキャナプールの 1 つに設定されていることを確認してください。 vserver vscan scanner-pool show-activeコマンドを使用して、現在アクティブなスキャナプールの設定を確認します。
CVO Virus Detected.（CVOウイルスが検出	警告	Vscan サーバからストレージシステムにエラーが報告されました。通常は、ウイルスが検出されたことを示します。ただし、 Vscan サーバで発生したその他のエラーではこのイベントを原因 処理できます。 ファイルへのクライアントアクセスが拒否されました。Vscan サーバは、設定に応じて、ファイルをクリーンアップするか、ファイルを隔離するか、または削除する可能性があります。	「 syslog 」イベントで報告された Vscan サーバのログを調べて、感染ファイルのクリーンアップ、隔離、削除が正常に完了したかどうかを確認します。削除できなかった場合は、システム管理者が手動でファイルを削除しなければならないことがあります。
CVO Volumeオフライン	情報	ボリュームがオフラインになりました。	ボリュームをオンラインに戻します。
CVO Volumeは制限付きです	情報	フレキシブルボリュームが制限されたことを示すイベントです。	ボリュームをオンラインに戻します。

トップに戻る

ビジネス継続性（**SMBC**）メディエーターログモニタ用**SnapMirror**

モニタ名	重大度	概要を監視します	対処方法
ONTAP メディエーターが追加されました	情報	このメッセージは、ONTAP メディエーターがクラスタに追加された場合に表示されます。	なし

ONTAP メディエーターにアクセスできません	重要	このメッセージは、ONTAP メディエーターが転用された場合、またはメディエーターパッケージがメディエーターサーバにインストールされなくなった場合に表示されます。そのため、SnapMirrorフェイルオーバーを実行できません。	「snapmirror mediator remove」コマンドを使用して、現在のONTAP メディエーターの設定を削除します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。
ONTAP メディエーターが削除されました	情報	このメッセージは、ONTAP メディエーターがクラスタから削除された場合に表示されます。	なし
ONTAP メディエーターに到達できません	警告	このメッセージは、クラスタでONTAP メディエーターに到達できない場合に表示されます。そのため、SnapMirrorフェイルオーバーを実行できません。	「network ping」コマンドと「network traceroute」コマンドを使用して、ONTAP メディエーターへのネットワーク接続を確認します。問題 が解除されない場合は、「snapmirror mediator remove」コマンドを使用して現在のONTAP メディエーターの設定を削除します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。
SMBC CA証明書期限切れ	重要	このメッセージは、ONTAP メディエーター認証局（CA）証明書の有効期限が切れた場合に表示されます。そのため、ONTAP メディエーターへの以降のすべての通信を行うことができません。	「snapmirror mediator remove」コマンドを使用して、現在のONTAP メディエーターの設定を削除します。ONTAP メディエーターサーバで新しいCA証明書を更新します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。

SMBC CA証明書の有効期限が切れて	警告	このメッセージは、ONTAP メディエーター認証局（CA）証明書の有効期限が30日以内になった場合に表示されます。	この証明書の有効期限が切れる前に、「snapmirror mediator remove」コマンドを使用して現在のONTAP メディエーターの設定を削除します。ONTAP メディエーターサーバで新しいCA証明書を更新します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。
SMBCクライアント証明書期限切れ	重要	このメッセージは、ONTAP メディエータークライアント証明書の有効期限が切れた場合に表示されます。そのため、ONTAP メディエーターへの以降のすべての通信を行うことができません。	「snapmirror mediator remove」コマンドを使用して、現在のONTAP メディエーターの設定を削除します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。
SMBCクライアント証明書の有効期限が切れて	警告	このメッセージは、ONTAP メディエータークライアント証明書の有効期限が30日以内に切れると表示されます。	この証明書の有効期限が切れる前に、「snapmirror mediator remove」コマンドを使用して現在のONTAP メディエーターの設定を削除します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。

SMBC関係が同期されていません 注：UMにはこの機能はありません	重要	このメッセージは、SnapMirror for Business Continuity（SMBC）関係のステータスが「In-Sync」から「Out-of-sync」に変わると表示されます。このRPO = 0のため、データ保護は中断されます。	ソースボリュームとデスティネーションボリュームの間のネットワーク接続を確認します。デスティネーションで「snapmirror show」コマンドを使用し、ソースで「snapmirror list-destinations」コマンドを使用して、SMBC関係のステータスを監視します。自動再同期では、関係のステータスが「同期中」に戻ります。再同期に失敗した場合は、クラスタ内のすべてのノードがクォーラムにあること、および正常な状態であることを確認します。
SMBCサーバ証明書期限切れ	重要	このメッセージは、ONTAP メディエーターサーバ証明書の有効期限が切れた場合に表示されます。そのため、ONTAP メディエーターへの以降のすべての通信を行うことができません。	「snapmirror mediator remove」コマンドを使用して、現在のONTAP メディエーターの設定を削除します。ONTAP メディエーターサーバで新しいサーバ証明書を更新します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。
SMBCサーバ証明書の有効期限が切れて	警告	このメッセージは、ONTAP メディエーターサーバ証明書の有効期限が30日以内になった場合に表示されます。	この証明書の有効期限が切れる前に、「snapmirror mediator remove」コマンドを使用して現在のONTAP メディエーターの設定を削除します。ONTAP メディエーターサーバで新しいサーバ証明書を更新します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。

トップに戻る

その他の電源、ハートビート、およびその他のシステムモニタ

モニタ名	重大度	概要を監視します	対処方法
ディスクシェルフの電源装置が検出されました	情報	このメッセージは、電源装置をディスクシェルフに追加した場合に表示されます。	なし
ディスクシェルフの電源装置が取り外されました	情報	このメッセージは、電源装置をディスクシェルフから取り外すと表示されます。	なし
MetroCluster の自動計画外スイッチオーバーが無効になりました	重要	このメッセージは、自動計画外スイッチオーバー機能が無効になっている場合に表示されます。	クラスタ内の各ノードで「MetroCluster modify -node -name <nodename> -automatic -switchover -onfailure true」コマンドを実行して、自動スイッチオーバーを有効にします。
MetroCluster ストレージブリッジに到達不能	重要	ストレージブリッジに管理ネットワーク経由でアクセスできません	1）ブリッジをSNMPで監視している場合は、「network interface show」コマンドを使用して、ノード管理LIFが動作していることを確認します。「network ping」コマンドを使用して、ブリッジがアクティブであることを確認します。 2)ブリッジがインバンドで監視されている場合は、ブリッジへのファブリックケーブル接続を確認し、ブリッジの電源が入っていることを確認します。
MetroCluster ブリッジの温度が異常-重大を下回っています	重要	ファイバチャネルブリッジのセンサーが重大しきい値を下回っている温度を報告しています。	1)ストレージブリッジのファンの動作ステータスを確認します。 2)ブリッジが推奨される温度条件で動作していることを確認します。
MetroCluster ブリッジの温度が異常-重大を超えています	重要	ファイバチャネルブリッジのセンサーが重大しきい値を超えている温度を報告しています。	1）ストレージブリッジのシャーシ温度センサーの動作ステータスを確認するには、コマンド「storage bridge show -Cooling」を使用します。 2)ストレージブリッジが推奨される温度条件で動作していることを確認します。

モニタ名	重大度	概要を監視します	対処方法
MetroCluster アグリゲートが残っています	警告	アグリゲートはスイッチバック時にリストアされませんでした。	1）コマンド「aggr show」を使用して、アグリゲートの状態を確認します。 2）アグリゲートがオンラインの場合、コマンド「MetroCluster switchback」を使用して、アグリゲートを元の所有者に戻します。
MetroCluster パートナー間のすべてのリンクが停止しています	重要	RDMAインターコネクトアダプタとクラスタ間LIFがピアクラスタへの接続を切断しているか、ピアクラスタが停止しています。	1）クラスタ間LIFが動作していることを確認します。インタークラスタLIFが停止している場合は修復します。 2）「cluster peer ping」コマンドを使用して、ピアクラスタが稼働していることを確認します。ピアクラスタが停止している場合は、『MetroClusterディザスタリカバリガイド』を参照してください。 3) Fabric MetroCluster の場合は、バックエンドファブリックISLが稼働していることを確認します。バックエンドファブリックISLが停止している場合は、ISLを修復します。 4）非ファブリックMetroCluster 構成の場合は、RDMAインターコネクトアダプタ間のケーブル接続が正しいことを確認します。リンクがダウンしている場合は、ケーブル接続を再設定します。

モニタ名	重大度	概要を監視します	対処方法
MetroCluster パートナーにピアリングネットワーク経由で到達できません	重要	ピアクラスタへの接続が切断されています。	1)ポートが正しいネットワーク/スイッチに接続されていることを確認します。 2）クラスタ間LIFがピアクラスタに接続されていることを確認 3) cluster peer pingコマンドを使用して、ピアクラスタが稼働中であることを確認します。ピアクラスタが停止している場合は、『MetroCluster ディザスタリカバリガイド』を参照してください。
MetroCluster スイッチ間のすべてのリンクが停止しています	重要	ストレージスイッチのすべてのスイッチ間リンク（ISL）が停止しています。	1）ストレージスイッチのバックエンドファブリックISLを修復します。 2）パートナースイッチが稼働し、ISLが動作していることを確認します。 3) xWDMデバイスなどの中間機器が動作していることを確認します。
MetroCluster ノードからストレージスタックへのSASリンクが停止しています	警告	SASアダプタまたは接続されているケーブルに問題がある可能性があります。	1. SASアダプタがオンラインで、実行中であることを確認します。 2.物理的なケーブル接続がしっかりと接続され、動作していることを確認し、必要に応じてケーブルを交換します。 3. SASアダプタがディスクシェルフに接続されている場合は、IOMとディスクが適切に装着されていることを確認します。
MetroClusterFCイニシエータリンクガテイシシテイル	重要	FCイニシエータアダプタに障害が発生しています。	1. FCイニシエータリンクが改ざんされていないことを確認します。 2.コマンド「system node run -node local-command storage show adapter」を使用して、FCイニシエータアダプタの動作ステータスを確認します。

モニタ名	重大度	概要を監視します	対処方法
FC-VIインターコネクトリンクが停止しています	重要	FC-VIポート上の物理リンクがオフラインです。	1. FC-VIリンクが改ざんされていないことを確認します。 2.コマンド「MetroCluster interconnect adapter show」を使用して、FC-VIアダプタの物理ステータスが「up」になっていることを確認します。 3.ファブリックスイッチを含む構成の場合は、正しくケーブル接続され、設定されていることを確認します。
MetroCluster のスペアディスクが残っています	警告	スペアディスクはスイッチバック中にリストアされませんでした。	ディスクで障害が発生していない場合は、コマンド「MetroCluster switchback」を使用してディスクを元の所有者に戻します。
MetroCluster ストレージブリッジのポートが停止しています	重要	ストレージブリッジのポートはオフラインです。	1）コマンド「storage bridge show -ports」を使用して、ストレージブリッジのポートの動作ステータスを確認します。 2)ポートへの論理接続と物理接続を確認します。
MetroCluster ストレージスイッチのファンに障害が発生しました	重要	ストレージスイッチのファンで障害が発生しました。	1）コマンドstorage switch show -Coolingを使用して、スイッチのファンが正しく動作していることを確認します。 2)ファンFRUが正しく挿入され、動作していることを確認します。
MetroCluster ストレージスイッチに到達不能です	重要	ストレージスイッチに管理ネットワーク経由でアクセスできません。	1）「network interface show」コマンドを使用して、ノード管理LIFが動作していることを確認します。 2)「network ping」コマンドを使用して、スイッチが有効であることを確認します。 3)スイッチにログインした後、SNMP経由でスイッチにアクセスできることを確認します。

モニタ名	重大度	概要を監視します	対処方法
MetroCluster スイッチの電源装置に障害が発生しました	重要	ストレージスイッチの電源装置が正常に動作していません。	1）コマンド「storage switch show -error-switch -name <swtich name> 」を使用して、エラーの詳細を確認します。 2)コマンド「storage switch show power-switch-name <switch name> 」を使用して、障害のある電源装置ユニットを特定します。 3)電源装置のunitisがストレージスイッチのシャーシに正しく挿入され、完全に動作していることを確認します。
MetroCluster スイッチの温度センサーに障害が発生しました	重要	Fibre Channelスイッチのセンサーに障害が発生しました。	1）コマンドstorage switch show -Coolingを使用して、ストレージスイッチの温度センサーの動作ステータスを確認します。 2)スイッチが推奨される温度条件で動作していることを確認します。
MetroCluster スイッチの温度が異常です	重要	Fibre Channelスイッチの温度センサーが異常な温度を報告しました。	1）コマンドstorage switch show -Coolingを使用して、ストレージスイッチの温度センサーの動作ステータスを確認します。 2)スイッチが推奨される温度条件で動作していることを確認します。
Service Processor Heartbeat Missedの略	情報	このメッセージは、ONTAP がサービスプロセッサ（SP）から想定される「ハートビート」信号を受信しなかった場合に表示されます。このメッセージに加えて、SPからのログファイルがデバッグのために送信されます。ONTAP はSPをリセットして通信を回復しようとします。SPのリブート中は、最大2分間はSPを使用できません。	ネットアップテクニカルサポートにお問い合わせください。

モニタ名	重大度	概要を監視します	対処方法
サービスプロセッサハートビートを停止しました	警告	このメッセージは、ONTAP がサービスプロセッサ（SP）からハートビートを受信しなくなった場合に表示されます。ハードウェアの設計によっては、システムは引き続きデータを提供することも、データ損失やハードウェアの破損を防ぐためにシャットダウンすることもあります。システムはデータを提供し続けますが、SPが動作していない可能性があるため、システムは停止しているアプライアンス、ブートエラー、またはOpen Firmware（OFW）のPower-on Self-Test（POST）エラーの通知を送信できません。システムが設定されている場合は、AutoSupport （「コールホーム」）メッセージを生成してネットアップテクニカルサポートおよび設定された宛先に送信します。AutoSupport メッセージが正常に配信されると、問題の特定と解決方法が大幅に改善されます。	システムがシャットダウンした場合は、ハード電源の再投入を試みます。コントローラをシャーシから引き出し、押し込んでから、システムの電源を入れます。電源再投入後も問題が解決しない場合、または注意が必要なその他の状況については、ネットアップテクニカルサポートにお問い合わせください。

トップに戻る

詳細情報

- "アラートの表示と非表示"

webhook を使用した通知

Webhook を使用すると、ユーザーはカスタマイズされた webhook チャネルを使用して、さまざまなアプリケーションにアラート通知を送信できます。

多くの商用アプリケーションでは、標準入力インターフェイスとして Webhook がサポートされています。たとえば、 Slack 、 PagerDuty 、 Teams 、および Discord は、すべてのウェブフックをサポートしています。Data Infrastructure Insightsは、カスタマイズ可能な汎用Webhookチャネルをサポートすることで、これらの配信チャネルの多くをサポートできます。Web フックの情報は、これらのアプリケーション Web サイトに掲載されています。たとえば、Slackには"この便利なガイドです"次のような機能があります。

複数の Web フックチャネルを作成できます。各チャネルは異なる目的に合わせて、アプリケーションや受信者などを個別に指定できます

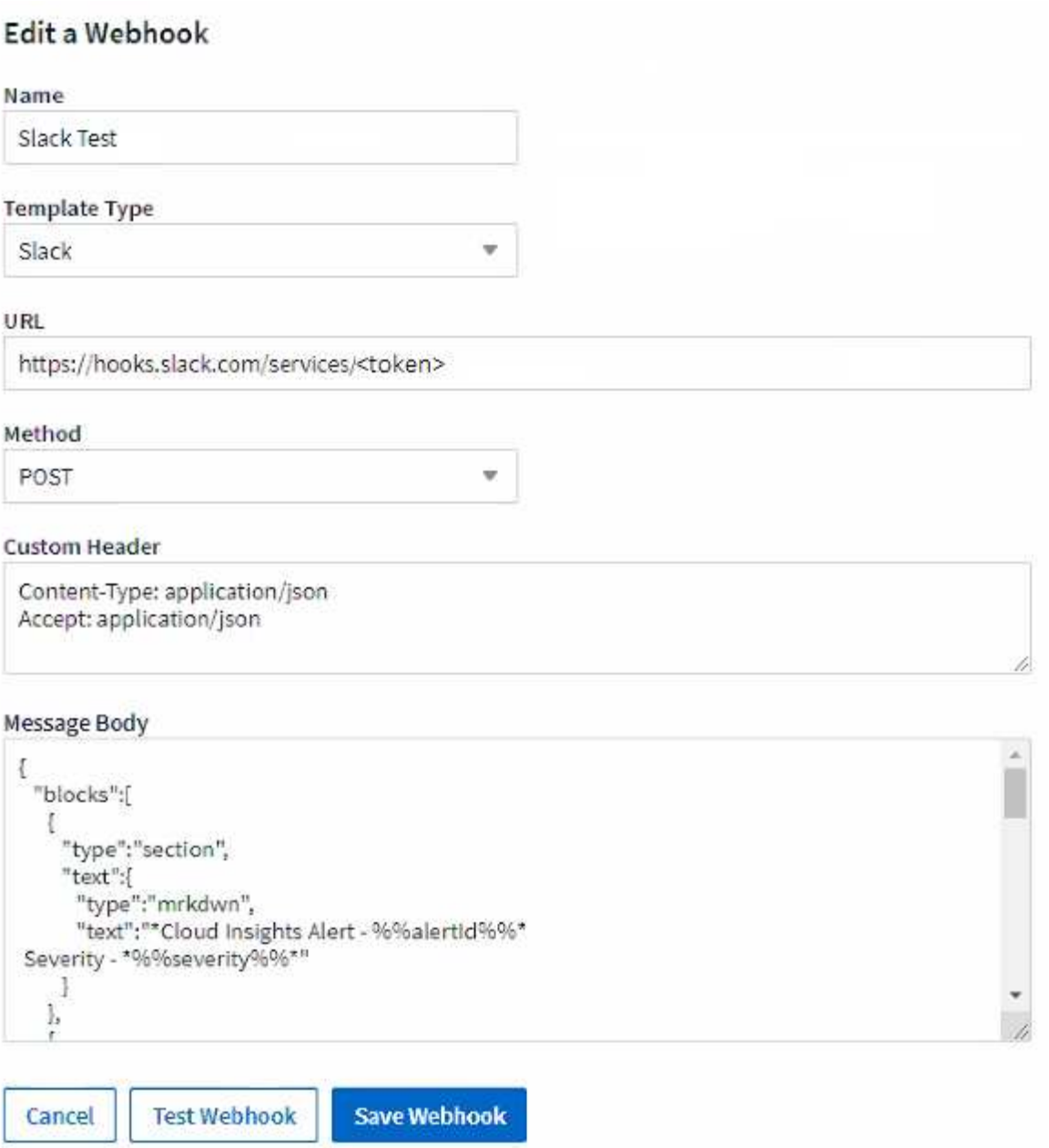
webhook チャネルインスタンスは、次の要素で構成されています。

名前	一意の名前
URL	URLパラメータとともに_ http://または https://_プレフィックスを含むWebhookターゲットURL
メソッド	GET 、 POST-DEFAULT は POST です
カスタムヘッダー	ここで任意のカスタムヘッダー行を指定します
メッセージ本文	メッセージの本文をここに入力します
デフォルトのアラートパラメータ	に、 webhook のデフォルトパラメータを示します
カスタムパラメータとシークレット	カスタムパラメータとシークレットを使用すると、一意のパラメータとパスワードなどのセキュアな要素を追加できます

Webhook の作成

Data Infrastructure InsightsのWebhookを作成するには、* Admin > Notifications に移動し、 Webhooks *タブを選択します。

次の図は、 Slack 用に設定された webhook の例を示しています。



各フィールドに適切な情報を入力し、完了したら[保存]をクリックします。

また、[Webフックのテスト]ボタンをクリックして、接続をテストすることもできます。これにより、選択されたメソッドに従って、定義されたURLに「Message Body」（置換なし）が送信されます。

Data Infrastructure InsightsのWebhookは、多数のデフォルトパラメータで構成されています。また、独自のカスタムパラメータまたはシークレットを作成することもできます。

Default Alert Parameters

Name	Description
%%alertDescription%%	Alert description
%%alertId%%	Alert ID
%%alertRelativeUrl%%	Relative URL to the Alert page. To build alert link use https://%%cloudInsightsHostName%%%%alertRelativeUrl%%
%%metricName%%	Monitored metric
%%monitorName%%	Monitor name
%%objectType%%	Monitored object type
%%severity%%	Alert severity level
%%alertCondition%%	Alert condition
%%triggerTime%%	Alert trigger time in GMT ('Tue, 27 Oct 2020 01:20:30 GMT')
%%triggerTimeEpoch%%	Alert trigger time in Epoch format (milliseconds)
%%triggeredOn%%	Triggered On (key:value pairs separated by commas)
%%value%%	Metric value that triggered the alert
%%cloudInsightsLogoUrl%%	Cloud Insights logo URL
%%cloudInsightsHostname%%	Cloud Insights Hostname (concatenate with relative URL to build alert link)

Custom Parameters and Secrets

Name	Value	Description
No Data Available		

+ Parameter

パラメータ：パラメータとは何ですか？また、パラメータの使用方法を教えてください。

アラートパラメータは、アラートごとに動的に設定される値です。たとえば、 %%TriggeredOn%% の _Parameter はアラートがトリガーされたオブジェクトで置き換えられます。

このセクションでは、置換は「Test Webhook」ボタンをクリックしたときに_not_performedになります。このボタンは、_%_substitionsを示すペイロードを送信しますが、これらをデータに置き換えません。

カスタムパラメータとシークレット

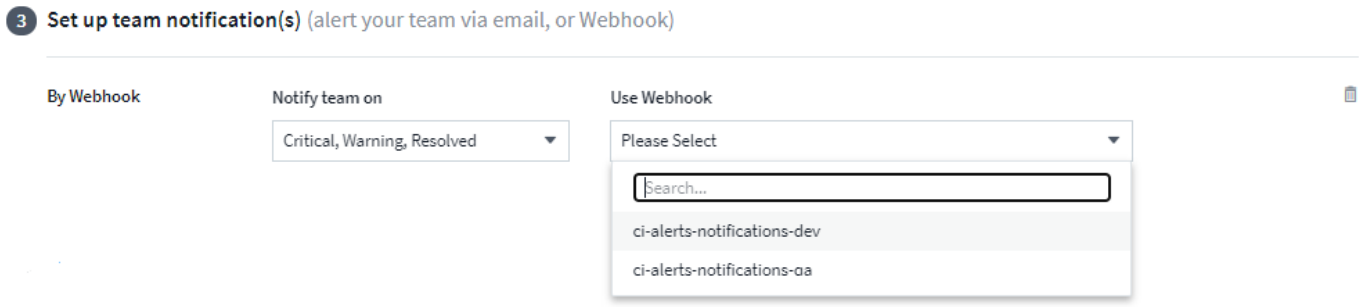
このセクションでは、任意のカスタムパラメータやシークレットを追加できます。セキュリティ上の理由から、シークレットが定義されている場合は、 webhook 作成者だけがこの webhook チャネルを変更できます。他のユーザに対しては読み取り専用です。URL/ ヘッダーのシークレットは、 %%<secret_name>%%_ として使用できます。

Webhookリストページ

Webhookのリストページには、Name、Created By、Created On、Status、Secure、 およびLast Reportedフィールド。

モニタで **[Webhook Notification]** を選択します

で webhook 通知を選択します "モニタ"をクリックして、 [* Alerts] > [Manage Monitors * （モニタの管理）] に移動し、目的のモニタを選択するか、新しいモニタを追加します。[チーム通知の設定] セクションで、配信方法として [*Webhook*] を選択します。警告レベル（重大、警告、解決済み）を選択し、目的のウェブフックを選択します。



Webhook の例：

のウェブフック "Slack"
のウェブフック "PagerDuty"
のウェブフック "チーム"
のウェブフック "切断"

アノテーションの使用

アノテーションの定義

Data Infrastructure Insightsでデータの追跡方法を企業の要件に合わせてカスタマイズするときは、アノテーションと呼ばれる特殊なメモを定義してアセットに割り当てることができます。

アセットの終了日、データセンター、建物の場所、ストレージ階層、ボリュームのサービスレベルなどの情報をアノテーションに割り当てることができます。

環境の監視にアノテーションを使用すると、次の作業に役立ちます。

- すべてのアノテーションタイプの定義を作成または編集する。

- アセットページを表示し、各アセットを 1 つ以上のアノテーションに関連付ける。

  たとえば、リースしているアセットのリース期限が 2 カ月以内の場合、終了日のアノテーションを適用すると、これにより、他のユーザがそのアセットを長期間使用できないようにすることができます。

- ルールを作成して、同じタイプの複数のアセットにアノテーションを自動的に適用する。
- アノテーションに基づいてアセットをフィルタする。

デフォルトのアノテーションタイプ

Data Infrastructure Insightsには、デフォルトのアノテーションタイプがいくつかあります。これらのアノテーションを使用して、データをフィルタまたはグループ化できます。

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

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

次の表に、Data Infrastructure Insightsが提供するアノテーションタイプを示します。

アノテーションタイプ	説明	を入力します
エイリアス	リソースのフレンドリ名	テキスト（ Text ）
コンピュートリソースグループ	Host and VM File Systems データコレクタで使用されるグループ割り当て	リスト
データセンター	物理的な場所	リスト
ホット	使用頻度が高いデバイスが定期的に、または容量のしきい値に達しています	ブール値
注	リソースに関連付けられているコメント	テスト
サービスレベル	リソースに割り当てることができる一連のサポート対象サービスレベル。内部ボリューム、 qtree 、およびボリュームの番号付きのオプションのリストが用意されています。サービスレベルを編集して、各レベルのパフォーマンスポリシーを設定できます。	リスト
日没	そのデバイスに新しい割り当てを実行できないしきい値。計画的な移行や保留中のネットワークの変更に役立ちます。	日付
スイッチレベル	スイッチのカテゴリを設定するための事前定義されたオプション。通常、これらの指定はデバイスのライフサイクルを通して維持されますが、編集することもできます。スイッチに対してのみ設定できます。	リスト

階層	を使用すると、環境内のさまざまなサービスレベルを定義できます。階層では、必要な速度などのレベルを定義できます（例： Gold や Silver ）。この機能は、内部ボリューム、 qtree 、ストレージアレイ、ストレージプール、およびボリュームに対してのみ使用できます。	リスト
違反の重大度	違反（ホストポートの欠落や冗長性の欠如など）のランク（例： Major ）。重要度の高い順に階層化されています。	リスト

エイリアス、データセンター、ホット、サービスレベル、サンセット、 [Switch Level]、[Tier]、および[Violation Severity]はシステムレベルのアノテーションで、削除や名前変更はできません。変更できるのは割り当てられている値のみです。

カスタムアノテーションの作成

アノテーションを使用すると、ビジネスニーズに合わせて、ビジネス固有のカスタムデータをアセットに追加できます。Data Infrastructure Insightsには一連のアノテーションがデフォルトで用意されていますが、別の方法でデータを表示したい場合もあります。カスタムアノテーションのデータは、ストレージのメーカー、ボリューム数、パフォーマンス統計など、すでに収集されたデバイスの補足データになります。アノテーションを使用して追加したデータは、Data Infrastructure Insightsでは検出されません。

手順

1. [Data Infrastructure Insights]メニューで、*[管理]>[アノテーション]*をクリックします。

   アノテーションページにアノテーションのリストが表示されます。

2. 「 * + 追加」をクリックします。
3. アノテーションの * Name * と * 概要 * を入力します。

   これらのフィールドには、 255 文字まで入力できます。

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

アノテーションタイプ

ブール値

選択肢が yes と no のドロップダウンリストを作成しますたとえば、「 Direct Attached 」アノテーションはブーリアンです。

日付

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

リスト

次のいずれかを作成します。

- 固定のドロップダウンリスト

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

ません。

- 可変のドロップダウンリスト

  このリストを作成するときに [オンザフライで新しい値を追加] オプションを選択すると、他のユーザーがこのアノテーションタイプをデバイスに割り当てるときに、リストに値を追加できます。

番号

アノテーションを割り当てるユーザが数値を入力できるフィールドを作成します。たとえば、アノテーションタイプが「 floor 」の場合は、値タイプとして「 number 」を選択し、フロア番号を入力できます。

テキスト（ **Text** ）

自由形式のテキストを許可するフィールドを作成します。たとえば、アノテーションタイプとして「 Language 」と入力し、値のタイプとして「 Text 」を選択し、言語を値として入力できます。

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

1. アノテーションタイプとして List を選択した場合は、次の手順を実行します。
   a. アセットページでアノテーションの値を追加して柔軟なリストを作成できるようにするには、「 * オンザフライで新しい値を追加」を選択します。

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

   b. 値と概要を*値*および*概要*フィールドに入力します。
   c. 値を追加するには、 **[Add]** をクリックします。
   d. 「ゴミ箱」アイコンをクリックして値を削除します。
2. [保存（ Save ）] をクリックします。

アノテーションがアノテーションページのリストに表示されます。

完了後

UI では、アノテーションがすぐに使用可能になります。

アノテーションの使用

アノテーションを作成し、監視対象のアセットに割り当てる。アノテーションは、物理的な場所、終了日、ストレージ階層、ボリュームのサービスレベルなど、アセットに関する情報を提供するメモです。

アノテーションの定義

アノテーションを使用すると、ビジネスニーズに合わせて、ビジネス固有のカスタムデータをアセットに追加できます。Data Infrastructure Insightsには、アセットのライフサイクル（開始日や終了日）、建物やデータセンターの場所、階層など、一連のデフォルトのアノテーションが用意されていますが、別の方法でデータを表示したい場合もあります。

カスタムアノテーションのデータは、スイッチのメーカー、ポートの数、パフォーマンス統計など、すでに収集されたデバイスの補足データになります。アノテーションを使用して追加したデータは、Data Infrastructure Insightsでは検出されません。

作業を開始する前に

- 環境のデータを関連付ける必要がある業界固有の用語をリストします。
- 環境のデータを関連付ける必要がある会社固有の用語をリストします。
- 使用できるデフォルトのアノテーションタイプがないかどうかを特定します。
- 作成する必要があるカスタムアノテーションを特定します。アセットに割り当てる前に、アノテーションを作成する必要があります。

アノテーションを作成するには、次の手順を実行します。

手順

1. [Data Infrastructure Insights]メニューで、*[Observability]>[Enrich]>[Annotations]*をクリックします。
2. [* + 注釈 * （ * + Annotation * ）] をクリックして、新しい注釈を作成する。
3. 名前（ Name ）、アノテートアイテム（概要）を入力し、新しいアノテートアイテムに入力します。

   たとえば、次のように入力して、データセンター 4 のアセットの物理的な場所を定義するテキストアノテーションを作成します。

   - アノテーションの名前（「 Location 」など）を入力します。
   - 「 Physical location is Data Center 4 」など、アノテーションの説明に使用する概要を入力します。
   - アノテーションの「 type 」を入力します（「 Text 」など）。

アセットへのアノテーションの手動割り当て

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

作業を開始する前に

- 割り当てるアノテーションを作成しておく必要があります。

手順

1. Data Infrastructure Insights環境にログインします。
2. アノテーションを適用するアセットを選択します。
   - アセットを検索するには、クエリ、ダッシュボードウィジェットから選択、または検索します。目的のアセットが見つかったら、リンクをクリックしてアセットのランディングページを開きます。

3. アセットページの [ユーザーデータ] セクションで、 [**+Annotation**] をクリックします。
4. [注釈の追加] ダイアログボックスが表示されます。
5. リストからアノテーションを選択します。
6. 値をクリックし、選択したアノテーションのタイプに応じて次のいずれかを実行します。
    - アノテーションタイプがリスト、日付、またはブーリアンの場合は、値をリストから選択します。
    - アノテーションタイプがテキストの場合は、値を入力します。
7. [保存（ Save ）] をクリックします。

アノテーションを割り当てたあとに値を変更する場合は、アノテーションフィールドをクリックして別の値を選択します。
fly_option で _Add 新規値を選択したリストタイプのアノテーションの場合は ' 既存の値を選択するだけでなく ' 新しい値を入力できます

アノテーションルールを使用してアノテーションを割り当てる

定義した条件に基づいてアセットにアノテーションを自動的に割り当てるには、アノテーションルールを設定します。Data Infrastructure Insightsは、これらのルールに基づいてアセットにアノテーションを割り当てます。Data Infrastructure Insightsには、2つのデフォルトのアノテーションルールも用意されています。これらのルールは、ニーズに合わせて変更したり、不要な場合は削除したりできます。

アノテーションルールの作成

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

作業を開始する前に

アノテーションルールのクエリを作成しておく必要があります。

このタスクについて

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

手順

1. [管理（ Manage ）] > [注釈ルール（ Annotation rules ）] をクリック

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

2. 「 * + 追加」をクリックします。
3. 次の手順を実行します。
    a. [* 名前 *] ボックスに、ルールを説明する一意の名前を入力します。

        この名前はアノテーションルールページに表示されます。

    b. * クエリ * をクリックし、アセットへのアノテーションの適用に使用するクエリを選択します。
    c. [* Annotation*] をクリックし、適用する注釈を選択します。

d. * 値 * をクリックし、アノテーションの値を選択します。

   たとえば、 Birthday のアノテーションを選択した場合は、日付の値を指定します。

e. [保存（ Save ）] をクリックします。

f. すべてのルールをすぐに実行する場合は、 * すべてのルールを実行 * をクリックします。それ以外の場合、ルールは定期的に実行されます。

アノテーションルールの作成

アノテーションルールを使用すると、定義した条件に基づいて複数のアセットにアノテーションを自動的に適用できます。Data Infrastructure Insightsは、これらのルールに基づいてアセットにアノテーションを割り当てます。個々のアセットページで手動で設定したアノテーションは、 Cloud Insight でアノテーションルールが評価されるときにルールベースのアノテーションよりも優先されます。

作業を開始する前に

アノテーションルールのクエリを作成しておく必要があります。

手順

1. [Data Infrastructure Insights]メニューで、*[管理]>[アノテーションルール]*をクリックします。
2. 新しいアノテーションルールを追加するには、「 * + ルール * 」をクリックします。

   [Add Rule] ダイアログが表示されます。

3. 次の手順を実行します。
   a. [* 名前 *] ボックスに、ルールを説明する一意の名前を入力します。

      名前がアノテーションルールページに表示されます。

   b. [Query]*をクリックし、Data Infrastructure Insightsがアノテーションを適用するアセットを特定するために使用するクエリを選択します。
   c. [* Annotation*] をクリックし、適用する注釈を選択します。
   d. * 値 * をクリックし、アノテーションの値を選択します。

      たとえば、 Birthday のアノテーションを選択した場合は、日付の値を指定します。

   e. [保存（ Save ）] をクリックします。
   f. すべてのルールをすぐに実行する場合は、 * すべてのルールを実行 * をクリックします。それ以外の場合、ルールは定期的に実行されます。

> ⓘ 大規模なData Infrastructure Insights環境で、アノテーションルールの実行に時間がかかることがあります。これは、インデクサが最初に実行され、ルールを実行する前に完了する必要があるためです。インデクサは、データ内の新規または更新されたオブジェクトやカウンタを検索またはフィルタリングする機能をData Infrastructure Insightsに提供します。ルールエンジンは、インデクサが更新を完了するまで待機してから、ルールを適用します。

アノテーションルールの変更

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

手順

1. [Data Infrastructure Insights]メニューで、*[管理]>[アノテーションルール]*をクリックします。

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

2. 変更するアノテーションルールを選択します。

   アノテーションルールは、フィルタボックスに値を入力してフィルタすることも、ページ番号をクリックして各ページで参照することもできます。

3. 変更するルールのメニューアイコンをクリックします。
4. [編集（ Edit ）] をクリックします。

   Edit Rule ダイアログが表示されます。

5. アノテーションルールの名前、アノテーション、値、またはクエリを変更します。

ルールの順序を変更する

アノテーションルールは、ルールリストの一番上から一番下まで処理されます。ルールの処理順序を変更するには、次の手順を実行します。

手順

1. 移動するルールのメニューアイコンをクリックします。
2. 目的の場所にルールが表示されるまで、必要に応じて [上へ移動] または [下へ移動] をクリックします。

アセット上で同じアノテーションを更新する複数のルールを実行している場合は、最初のルール（上から下に実行）によってアノテーションが適用され、アセットが更新されます。2番目のルールは適用されますが、前のルールですでに設定されているアノテーションは変更されません。

アノテーションルールを削除する

使用されなくなったアノテーションルールを削除できます。

手順

1. [Data Infrastructure Insights]メニューで、*[管理]>[アノテーションルール]*をクリックします。

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

2. 削除するアノテーションルールを選択します。

   アノテーションルールは、フィルタボックスに値を入力してフィルタすることも、ページ番号をクリックして各ページで参照することもできます。

3. 削除するルールのメニューアイコンをクリックします。

4. [削除（ Delete ）] をクリックします。

   ルールを削除するかどうかを確認するメッセージが表示されます。

5. [OK] をクリックします。

アノテーションのインポート

Data Infrastructure Insightsには、CSVファイルからアノテーションやアプリケーションをインポートし、指定したオブジェクトに割り当てるためのAPIが含まれています。

Data Infrastructure Insights APIは、* Data Infrastructure Insights Premium Edition *で利用できます。

インポート中です

[*Admin] > [API Access] リンクには、が含まれています "ドキュメント" * Assets / Import * API の場合。このドキュメントでは、 .csv ファイルの形式について説明しています。

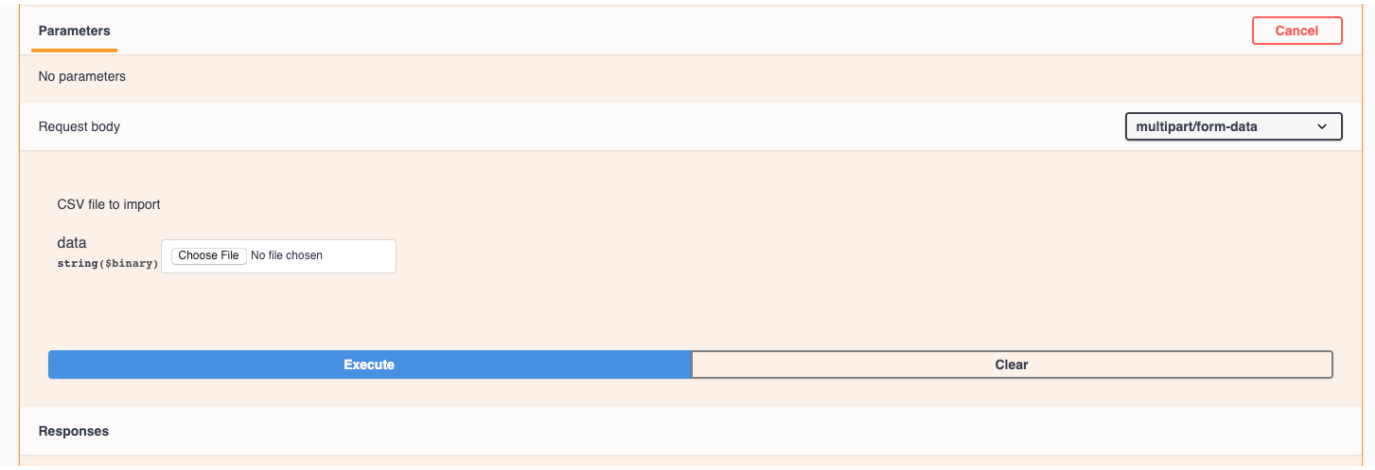
.csv ファイル形式の略

CSV ファイルの一般的な形式は次のとおりです。ファイルの 1 行目では、インポートフィールドを定義し、フィールドの順序を指定します。次に、アノテーションまたはアプリケーションごとに個別の行を表示します。すべてのフィールドを定義する必要はありません。ただし、後続の注釈行は、定義行と同じ順序に従う必要があります。

```
 [Object Type] , [Object Name or ID] , Annotation Type [, Annotation
Type,  ...] [, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]
```

`.csv` ファイルの例については、 `API` のドキュメントを参照してください。

API スワッガー自体から .csv ファイルからアノテーションをインポートして割り当てることができます。使用するファイルを選択し、 _Execute_Button をクリックします。



インポートビヘイビア

インポート処理では、インポートするオブジェクトとオブジェクトタイプに応じて、データの追加、マージ、または置換が行われます。インポート時には、次の動作に注意してください。

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

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

- アノテーション値が空の場合、そのアノテーションはオブジェクトから削除されます。継承された注釈は影響を受けません。
- 日付タイプのアノテーション値は、 UNIX 時間（ミリ秒）で指定する必要があります。
- ボリュームまたは内部ボリュームのアノテーションでは、オブジェクト名はストレージ名とボリューム名を組み合わせたもので、区切り文字として使用されます。たとえば、 < ストレージ名 >-> < ボリューム名 > のように指定します
- オブジェクト名にカンマが含まれている場合は、名前全体を二重引用符で囲む必要があります。たとえば、「 Netapp1 ！」、「 NetApp 2 」、「 -> 023F_ 」のように入力します
- ストレージ、スイッチ、ポートにアノテーションを接続している場合は、「アプリケーション」列は無視されます。
- テナント、基幹業務、ビジネスユニット、プロジェクトのいずれかまたは両方がビジネスエンティティになります。すべてのビジネスエンティティと同様に、いずれの値も空にすることができます。

次のオブジェクトタイプに注釈を付けることができます。

オブジェクトタイプ	名前またはキー
ホスト	ID\-><id> または <Name>
VM	ID\-><id> または < 名前 >

ストレージプール	ID\-><id> または <Storage Name> <Storage Pool Name>
内部ボリューム	ID\-><id> または <Storage Name>-> <Internal Volume Name>
ボリューム	ID\-><id> または <Storage Name>-> <Volume Name>
ストレージ	ID\-><id> または <Name>
スイッチ	ID\-><id> または <Name>
ポート	ID\-><id> または <WWN>
qtree	ID\-><id> または <Storage Name> <Internal Volume Name>\-><qtree Name>
共有	ID\-><id> または <Storage Name> <Internal Volume Name>\-><Share Name>-><Protocol> [\-><qtree 名（デフォルト qtree の場合はオプション） >]

アプリケーションの操作

アプリケーションごとにアセットの使用状況を追跡する

環境で実行されているアプリケーションに関連付けられているデータを追跡するには、まずそれらのアプリケーションを定義し、適切なアセットに関連付ける必要があります。アプリケーションを関連付けることができるアセットは、ホスト、仮想マシン、ボリューム、内部ボリューム、 qtree 、 共有、ハイパーバイザー：

ここでは、マーケティングチームが Exchange E メールに使用する仮想マシンの使用状況を追跡する例を示します。

環境で使用されているアプリケーションを特定し、各アプリケーションを使用してグループまたはビジネスユニットをメモするには、次のような表を作成します。

テナント	基幹業務部門	ビジネスユニット	プロジェクト	アプリケーション
ネットアップ	データストレージ	法律	特許	Oracle Identity Manager 、 Oracle On Demand 、 PatentBuy
ネットアップ	データストレージ	マーケティング	セールスイベント	Exchange 、 Oracle 共有データベース、 BlastOff Event Planner

次の表は、マーケティングチームが Exchange アプリケーションを使用していることを示しています。ストレージの追加がいつ必要になるかを予測できるように、 Exchange の仮想マシンの使用率を追跡したいと考えています。 Exchange アプリケーションをマーケティング部門のすべての仮想マシンに関連付けることができます。

1. Exchange という名前のアプリケーションを作成します
2. [クエリ] 、 [新規クエリ] の順に移動して、仮想マシンの新しいクエリを作成します (必要に応じて、既

存の VM クエリを選択します) 。

マーケティングチームの VM のすべてに文字列「 * mkt * 」を含む名前があると仮定して、「 mkt 」の VM 名をフィルタリングするクエリを作成します。

3. VM を選択します。
4. *Bulk Actions > Add Applications * を使用して、 VM を _Exchange_application に関連付けます。
5. 目的のアプリケーションを選択し、 * 保存 * をクリックします。
6. 完了したら、 * クエリを保存 * します。

アプリケーションの作成

環境で実行されている特定のアプリケーションに関連付けられているデータを追跡するには、 Cloud Insights でアプリケーションを定義します。

作業を開始する前に

アプリケーションをビジネスエンティティに関連付ける場合は、アプリケーションを定義する前にビジネスエンティティを作成する必要があります。

このタスクについて

Cloud Insights を使用すると、アプリケーションに関連付けられているアセットのデータを追跡して、使用状況やコストレポートなどの情報を確認できます。

手順

1. Cloud Insightsメニューで、* Observability > Enrich > Applications *をクリックします。選択

   [アプリケーションの追加]ダイアログボックスが表示されます。

2. アプリケーションの一意の名前を入力します。
3. アプリケーションの優先度を選択します。
4. [保存（ Save ）] をクリックします。

アプリケーションを定義したら、アセットに割り当てることができます。

アセットへのアプリケーションの割り当て

この手順では、例としてアプリケーションをホストに割り当てます。アプリケーションには、ホスト、仮想マシン、ボリューム、または内部ボリュームを割り当てることができます。

手順

1. アプリケーションに割り当てるアセットを選択します。
2. [* クエリ] 、 [新しいクエリ] の順にクリックし、 [ホスト] を検索します。
3. アプリケーションに関連付けるホストの左側にあるチェックボックスをオンにします。
4. [一括操作]>[アプリケーションの追加 *] をクリックします。
5. アセットを割り当てるアプリケーションを選択します。

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

関連するアセットが大量にある環境では、それらのアセットへのアプリケーションの割り当ての継承に数分かかることがあります。関連するアセットが多数ある場合は、継承の時間を長くしてください。

完了後

アプリケーションにホストを割り当てたら、残りのアセットをアプリケーションに割り当てることができます。アプリケーションのランディング・ページにアクセスするには、 * Manage > Application * をクリックして、作成したアプリケーションを選択します。

自動デバイス解決

自動デバイス解決の概要

Data Infrastructure Insightsで監視するデバイスをすべて特定する必要があります。環境のパフォーマンスとインベントリを正確に追跡するには、識別が必要です。通常、環境で検出されたデバイスの大部分は、 *Automatic Device Resolution* で識別されます。

データコレクタを設定すると、スイッチ、ストレージアレイ、ハイパーバイザーや VM の仮想インフラなど、環境内のデバイスが特定されます。ただし、通常は環境内のすべてのデバイスが識別されるわけではありません。

データコレクタタイプのデバイスを設定したら、デバイス解決ルールを利用して環境内の残りの不明なデバイスを特定することを推奨します。デバイス解決は、次のデバイスタイプとして不明なデバイスの解決に役立ちます。

- 物理ホスト
- ストレージアレイ
- テープ

デバイス解決後も不明なままのデバイスは汎用デバイスとみなされるため、クエリやダッシュボードに表示することもできます。

似た属性の新しいデバイスが以降に環境に追加されると、作成したルールに基づいて自動的に識別されます。場合によっては、Data Infrastructure Insightsで検出されなかったデバイスについては、デバイス解決ルールを無視して手動で識別することもできます。

デバイスの識別が完了していないと、次のような問題が発生する可能性

- 不完全なパスです
- マルチパス接続が識別されない
- アプリケーションをグループ化できない
- 正確なトポロジが表示されない
- Data Warehouse や Reporting で正確なデータが表示されない

デバイス解決機能（ [管理]>[デバイス解決] ）には、次のタブがあります。各タブは、デバイス解決の計画および結果の表示に役割を果たします。

- * Fibre Channel identify * には、自動デバイス解決で解決されなかったファイバ・チャネル・デバイスの WWN およびポート情報のリストが含まれます。識別されたデバイスの割合も表示されます。
- * IP Address identify * には、自動デバイス解決で識別されなかった CIFS 共有および NFS 共有にアクセスするデバイスのリストが表示されます。識別されたデバイスの割合も表示されます。
- * 自動解決ルール * には、ファイバ・チャネル・デバイス解決を実行する際に実行されるルールのリストが含まれます。これらのルールは、識別されないファイバチャネルデバイスを解決するために作成します。
- * 環境設定 * には、環境に合わせてデバイスの解像度をカスタマイズするための設定オプションが用意されています。

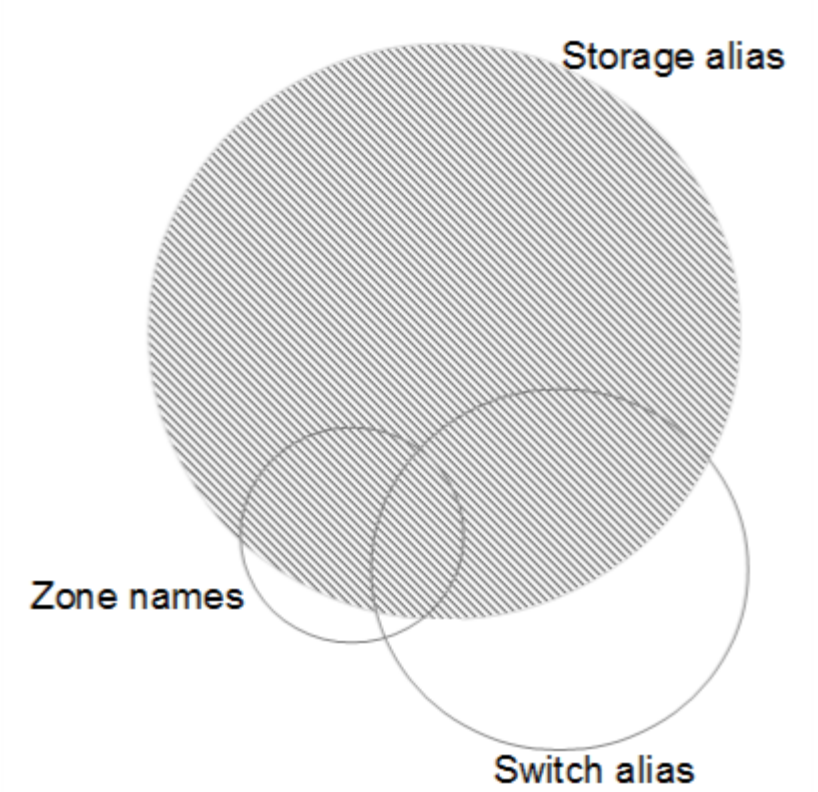
作業を開始する前に

デバイスを識別するルールを定義する前に、環境がどのように設定されているかを理解しておく必要があります。環境についての知識が多いほど、デバイスの識別が容易になります。

正確なルールを作成するには、次のような回答の質問が必要です。

- ゾーンやホストの命名基準がある場合、それらはどの程度正確であるか。
- スイッチエイリアスやストレージエイリアスを使用している場合、それらがホスト名と一致しているかどうか。
- 命名規則はどれくらいの頻度で変更されますか？
- 買収や合併によって命名規則が変わっていないかどうか。

環境を分析することで、どのような命名基準があり、その信頼性がどの程度であるかを特定できるようになります。たとえば、収集した情報から、次の図のような状況であることがわかったとします。



この例では、ストレージエイリアスで最も多くのデバイスを表すことができます。ストレージエイリアスを使用してホストを識別するルールを最初に記述し、次にスイッチエイリアスを使用するルール、最後にゾーンエイリアスを使用するルールを作成します。ゾーンエイリアスやスイッチエイリアスと重なっている部分のデバイスについても、ストレージエイリアスのルールで識別できるため、ゾーンエイリアスやスイッチエイリアスに必要なルールは少なくて済みます。

デバイスを識別する手順

環境内のデバイスを識別する一般的なワークフローを次に示します。識別は反復的なプロセスであり、ルールの計画や調整が何度も必要になることがあります。

- 研究環境
- ルールを計画する
- ルールを作成 / 改訂します
- 結果を確認します
- 追加のルールを作成するか、デバイスを手動で識別します
- 完了しました

未識別のデバイス（通常は不明または汎用デバイス）が環境にあり、その後、ポーリング時にこれらのデバイスを識別するデータソースを設定すると、それらのデバイスは表示されなくなり、汎用デバイスとしてカウントされなくなります。

関連：
"デバイス解決ルールの作成"
"ファイバチャネルのデバイス解決"
"IP デバイス解決"

"デバイス解決のプリファレンスの設定"

デバイス解決ルール

Data Infrastructure Insightsで現在自動識別されていないホスト、ストレージ、テープを識別するためのデバイス解決ルールを作成します。作成したルールにより、環境内の既存のデバイスが識別されるほか、環境に追加された同様のデバイスも識別されます。

デバイス解決ルールの作成

ルールを作成するときは、最初に、ルールの実行対象となる情報のソース、情報の抽出に使用する方法、およびルールの結果に DNS ルックアップを適用するかどうかを特定します。

デバイスの識別に使用するソース	*ホストのSRMエイリアス *ホスト名またはテープ名が埋め込まれたストレージエイリアス *ホスト名またはテープ名が埋め込まれたスイッチエイリアス *ホスト名が埋め込まれたゾーン名
ソースからデバイス名を抽出する方法	*そのまま（SRMから名前を抽出） *区切り文字 *正規表現
DNS ルックアップ	ホスト名の検証に DNS を使用するかどうかを指定します

ルールは、 ［ 自動解決ルール ］ タブで作成します。以下に、ルールの作成プロセスについて説明します。

手順

1. **[Manage] > [Device Resolution]** をクリックします
2. 自動解決ルール * タブで、 * + ホストルール * または * + テープルール * をクリックします。

   [* 解決ルール * （ Resolution Rule ）] 画面が表示されます。

   正規表現の作成に関するヘルプと例については、 _View matching_criteria リンクをクリックしてください。

3. [* タイプ] リストで、識別するデバイスを選択します。

   ホストまたはテープを選択できます。

4. [* ソース *] リストで、ホストの識別に使用するソースを選択します。

   選択したソースに応じて、Data Infrastructure Insightsには次の応答が表示されます。

   a. *ゾーン*には、Data Infrastructure Insightsで識別する必要があるゾーンとWWNを示します。
   b. * SRM *には、Data Infrastructure Insightsで識別する必要がある未識別のエイリアスが一覧表示されます。
   c. *ストレージエイリアス*には、Data Infrastructure Insightsで識別する必要があるストレージエイリア

スとWWNが表示されます。

d. *スイッチのエイリアス*には、Data Infrastructure Insightsで識別する必要があるスイッチのエイリアスが表示されます。

5. メソッド * リストで、ホストの識別に使用する方法を選択します。

ソース	メソッド
SRM の場合	そのままで、デリミタ、正規表現を使用します
ストレージエイリアス	デリミタ、正規表現
スイッチエイリアス	デリミタ、正規表現
ゾーン	デリミタ、正規表現

◦ Delimiters を使用するルールの場合は、デリミタとホスト名の最小文字数を指定する必要があります。ホスト名の最小文字数は、Data Infrastructure Insightsがホストを識別するために使用する文字数です。Data Infrastructure Insightsでは、これ以上長いホスト名に対してのみDNSルックアップが実行されます。

delimiters を使用するルールの場合、入力文字列は区切り文字でトークン化され、ホスト名候補のリストは、隣接するトークンを複数組み合わせて作成されます。リストは、最大から最小にソートされます。たとえば '*vipsnq03_hba3_emc3_12ep0* の入力 sring の場合 ' リストは次のようになります

- vipsnq03_hba3_emc3_12ep0
- vipsnq03_hba3_emc3
- hba3 emc3_12ep0
- vipsnq03_hba3
- emc3_12ep0
- hba3_emc3
- vipsnq03.
- 12ep0
- emcs3
- hba3

◦ 正規表現を使用するルールでは、正規表現、形式、および大文字と小文字の区別を選択する必要があります。

6. すべてのルールを実行するには、 * Run AR * をクリックします。または、ボタンの下矢印をクリックして、作成したルール（および前回の AR のフル実行後に作成された他のルール）を実行します。

ルールの実行結果は、 * FC identify * タブに表示されます。

自動デバイス解決の更新を開始しています

デバイス解決の更新では、前回の完全な自動デバイス解決の実行後に手動で行った変更がコミットされます。更新を実行すると、デバイス解決設定に対する新しい手動のエントリのみをコミットして実行できます。完全なデバイス解決は実行されません。

手順

1. Data Infrastructure Insights Web UIにログインします。
2. [**Manage] > [Device Resolution**] をクリックします
3. [* デバイス解決 *] 画面で、 [* AR の実行] ボタンの下矢印をクリックします。
4. アップデートを開始するには、 * アップデート * をクリックします。

ルールに基づく手動識別

この機能は、不明なホスト、ストレージ、テープデバイスを解決するために特定のルールまたはルールのリストを（ 1 回だけ順序変更の有無に関係なく）実行する場合に使用します。

作業を開始する前に

識別されていないデバイスが多数あり、他のデバイスを正しく識別した複数のルールがある場合。

ソースにホスト名またはデバイス名の一部だけが含まれている場合は、正規表現のルールを使用して欠落しているテキストを追加するように形式を変更します。

手順

1. Data Infrastructure Insights Web UIにログインします。
2. [**Manage] > [Device Resolution**] をクリックします
3. Fibre Channel identify * タブをクリックします。

   デバイスとその解決ステータスが表示されます。

4. 識別されていない複数のデバイスを選択
5. をクリックし、[ホスト解決の設定]または[テープ解決の設定]*を選択します。

   識別画面が表示され、デバイスを正しく識別したすべてのルールのリストが表示されます。

6. ルールの順序を、ニーズに合った順序に変更します。

   ルールの順序は識別画面で変更されますが、グローバルには変更されません。

7. ニーズに合った方法を選択します。

Data Infrastructure Insightsでは、ホスト解決プロセスが表示されている順序（上部から順に）で実行されます。

適用されるルールが検出されると、ルールの名前がルールの列に表示され、手動で識別されます。

関連：
"ファイバチャネルのデバイス解決"
"IP デバイス解決"
"デバイス解決のプリファレンスの設定"

ファイバチャネルデバイスの解決

Fibre Channel identify （ファイバチャネル識別）画面には、自動デバイス解決でホストが識別されていないファイバチャネルデバイスの WWN と WWPN が表示されます。こ

の画面には、手動デバイス解決で解決されたデバイスも表示されます。

手動解決で解決されたデバイスのステータスは *OK* で、デバイスの識別に使用されたルールを識別します。欠落しているデバイスのステータスは *Unidentified* です。識別から除外されたデバイスのステータスは、_Excluded _ です。このページには、デバイスの識別範囲の合計が表示されます。

一括操作を実行するには、 Fibre Channel 識別画面の左側で複数のデバイスを選択します。1 つのデバイス上でアクションを実行するには、デバイスの上にカーソルを移動し、リストの右端にある _identified_or_Unidentified_buttons を選択します。

_Total Coverage_link には、特定されたデバイスの数、または構成に使用可能なデバイスの数のリストが表示されます。

- SRM エイリアス
- ストレージエイリアス
- スイッチエイリアス
- ゾーン
- ユーザ定義

ファイバチャネルデバイスを手動で追加する

Data Infrastructure Insightsにファイバチャネルデバイスを手動で追加するには、デバイス解決の[Fibre Channel Identify]タブにある_Manual Add_機能を使用します。このプロセスは、今後検出されることが予想されるデバイスの事前識別に使用される場合があります。

作業を開始する前に

システムにデバイス識別情報を追加するには、 WWN または IP アドレスとデバイス名を確認しておく必要があります。

このタスクについて

ホスト、ストレージ、テープ、または不明なファイバチャネルデバイスを手動で追加できます。

手順

1. Data Infrastructure Insights Web UIにログイン
2. [**Manage] > [Device Resolution**] をクリックします
3. Fibre Channel identify * タブをクリックします。
4. [* 追加（ Add * ）] ボタンをクリックします。

   [* デバイスの追加 *] ダイアログが表示されます

5. WWN または IP アドレスとデバイス名を入力し、デバイスタイプを選択します。

   入力したデバイスは、 Fibre Channel identify タブのデバイスのリストに追加されます。ルールは *Manual* と指定されます。

.csv ファイルからファイバチャネルデバイスの識別情報をインポートしています

ファイバチャネルデバイスの識別情報は、.csvファイルのデバイスのリストを使用して、Data Infrastructure Insightsのデバイス解決に手動でインポートできます。

1. 作業を開始する前に

デバイスの識別情報をデバイス解決に直接インポートするには、正しい形式の .csv ファイルが必要です。ファイバチャネルデバイスの .csv ファイルには、次の情報が必要です。

WWN	IP	名前	を入力します

データフィールドは、次の例に示すように、引用符で囲む必要があります。

```
"WWN","IP","Name","Type"
"WWN:2693","ADDRESS2693|IP2693","NAME-2693","HOST"
"WWN:997","ADDRESS997|IP997","NAME-997","HOST"
"WWN:1860","ADDRESS1860|IP1860","NAME-1860","HOST"
```

ベストプラクティスとして、最初にファイバチャネル識別情報を .csv ファイルにエクスポートし、そのファイルに必要な変更を加えてから、ファイルをファイバチャネル識別情報にインポートすることを推奨します。これにより、必要な列が適切な順序で配置されます。

ファイバ・チャネル識別情報をインポートするには ' 次の手順

1. Data Infrastructure Insights Web UIにログインします。
2. [**Manage] > [Device Resolution**] をクリックします
3. Fibre Channel identify * タブを選択します。
4. [識別]>[ファイルから識別] ボタンをクリックします。
5. インポートする .csv ファイルが格納されているフォルダに移動し、目的のファイルを選択します。

   入力したデバイスは、ファイバチャネル識別タブのデバイスのリストに追加されます。「規則」は「手動」と識別されます。

.csv ファイルへのファイバチャネルデバイス識別情報のエクスポート

Data Infrastructure Insightsのデバイス解決機能から、ファイバチャネルデバイスの既存の識別情報を.csvファイルにエクスポートできます。エクスポートしたデバイス識別情報を変更してData Infrastructure Insightsに再度インポートすると、最初に識別情報をエクスポートしたデバイスと類似したデバイスの識別に使用できます。

このタスクについて

このシナリオは、 .csv ファイルで簡単に編集できる属性がデバイスに似ている場合に使用し、その後システムにインポートし直すことができます。

ファイバチャネルデバイスの識別情報を .csv ファイルにエクスポートすると、次の情報がこの順序でファイルに格納されます。

WWN	IP	名前	を入力します

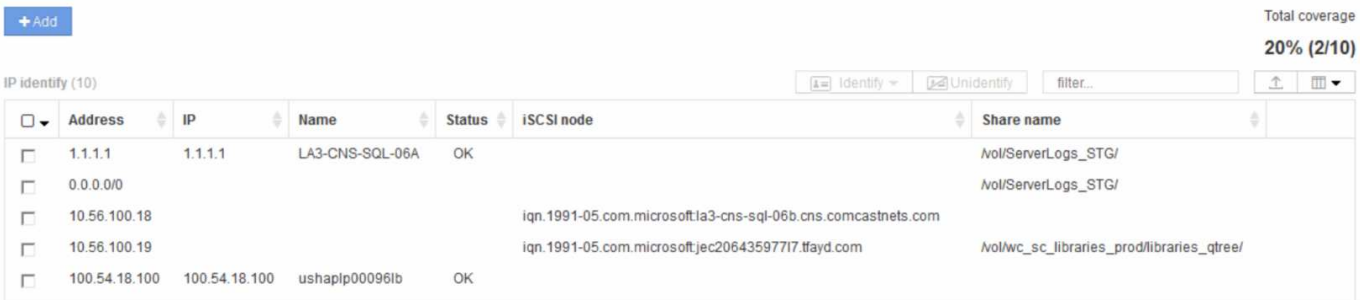
手順

1. Data Infrastructure Insights Web UIにログインします。
2. [**Manage] > [Device Resolution**] をクリックします
3. Fibre Channel identify * タブを選択します。
4. 識別情報をエクスポートする 1 つ以上のファイバチャネルデバイスを選択します。
5. [* Export*] をクリックします ボタン"] ボタンを押します。

関連：
"IP デバイス解決"
"デバイス解決ルールの作成"
"デバイス解決のプリファレンスの設定"

IP デバイスの解決

IP の識別画面には、自動デバイス解決または手動デバイス解決によって識別された iSCSI 共有と CIFS 共有または NFS 共有が表示されます。また、未識別のデバイスも表示されます。画面には、デバイスの IP アドレス、名前、ステータス、 iSCSI ノード、および共有名が表示されます。識別に成功したデバイスの割合も表示されます。



IP デバイスを手動で追加する

[IP Identify]画面の手動追加機能を使用して、IPデバイスをData Infrastructure Insightsに手動で追加できます。

手順

1. Data Infrastructure Insights Web UIにログインします。
2. [**Manage] > [Device resolution**] をクリックします
3. [IP Address identify *] タブをクリックします。
4. [* 追加（ Add * ）] ボタンをクリックします。

   Add Device ダイアログが表示されます

5. アドレス、 IP アドレス、および一意のデバイス名を入力します。

結果

入力したデバイスは、 [IP Address Identify （ IP アドレスの識別）] タブのデバイスのリストに追加されます。

.csv ファイルからの **IP** デバイス識別情報のインポート

IP デバイスの識別情報を、 .csv ファイルのデバイス識別情報のリストを使用して手動でデバイス解決機能にインポートできます。

1. 作業を開始する前に

デバイスの識別情報をデバイス解決機能に直接インポートするには、正しい形式の .csv ファイルが必要です。IP デバイスの .csv ファイルには、次の情報が必要です。

住所	IP	名前

データフィールドは、次の例に示すように、引用符で囲む必要があります。

```
"Address","IP","Name"
"ADDRESS6447","IP6447","NAME-6447"
"ADDRESS3211","IP3211","NAME-3211"
"ADDRESS593","IP593","NAME-593"
```

ベストプラクティスとして、まず IP アドレス識別情報を .csv ファイルにエクスポートし、そのファイルに必要な変更を加えてから、そのファイルを IP アドレス識別にインポートすることをお勧めします。これにより、必要な列が適切な順序で配置されます。

IP デバイス識別情報の **.csv** ファイルへのエクスポート

Data Infrastructure Insightsのデバイス解決機能から、既存のIPデバイスの識別情報を.csvファイルにエクスポートできます。エクスポートしたデバイス識別情報を変更してData Infrastructure Insightsに再度インポートすると、最初に識別情報をエクスポートしたデバイスと類似したデバイスの識別に使用できます。

このタスクについて

。
このシナリオは、 .csv ファイルで簡単に編集できる属性がデバイスに似ている場合に使用し、その後システムにインポートし直すことができます。

IP デバイスの識別情報を .csv ファイルにエクスポートすると、次の情報がこの順序でファイルに格納されます。

住所	IP	名前

手順

1. Data Infrastructure Insights Web UIにログインします。
2. [**Manage] > [Device Resolution**] をクリックします
3. [IP Address identify *] タブを選択します。
4. 識別情報をエクスポートする IP デバイスを選択します。

5. [* Export*] をクリックします ボタン"] ボタンを押します。

関連：
"ファイバチャネルデバイスの解決"
"デバイス解決ルールの作成"
"デバイス解決のプリファレンスの設定"

[環境設定] タブでオプションを設定します

デバイス解決のプリファレンスタブでは、自動解決スケジュールの作成、識別情報を含めるストレージベンダーやテープベンダーの指定、および DNS 検索オプションの設定を行うことができます。

自動解決スケジュール

自動デバイス解決を実行するスケジュールを指定できます。

オプション	説明
間隔	曜日、時間、または分単位で自動デバイス解決を実行する場合は、このオプションを使用します。
毎日	このオプションは、自動デバイス解決を特定の時刻に毎日実行する場合に使用します。
手動で実行する	このオプションは、自動デバイス解決を手動でのみ実行する場合に使用します。
環境が変化するたびに	このオプションは、環境に変更があったときに自動デバイス解決を実行する場合に使用します。

manually_manually__ を指定すると、毎晩の自動デバイス解決が無効になります。

DNS の処理オプション

DNS の処理オプションでは、次の機能を選択できます。

- DNS ルックアップの結果の処理を有効にすると、解決されたデバイスに付加する DNS 名のリストを追加できます。
- Auto resolution of IPs ：を選択すると、 NFS 共有にアクセスする iSCSI イニシエータおよびホストについて、 DNS ルックアップを使用した自動ホスト解決を有効にできます。指定しない場合は、 FC ベースの解決のみが実行されます。
- ホスト名にアンダースコアを使用できるようにすることも、標準のポートエイリアスの代わりに「接続先」のエイリアスを使用することもできます。

ストレージやテープの特定のベンダーを含めるか、除外します

ストレージやテープの特定のベンダーを自動解決の対象に含めたり除外したりできます。レガシーホストとなり、新しい環境から除外する必要があることがわかっているホストがある場合などは、特定のベンダーを除外することができます。除外したベンダーを再度追加することもできます。

テープのデバイス解決ルールは、 WWN のベンダーがテープ専用に設定されている WWN でのみ機能します。ベンダーの環境設定では、その WWN のベンダーがテープ専用に設定されています。

次も参照してください。 "正規表現の例"

正規表現の例

ソースの命名方法として正規表現の手法を選択している場合は、正規表現の例を参考に、Data Infrastructure Insightsの自動解決方法で使用する独自の式を作成できます。

正規表現の形式

Data Infrastructure Insightsの自動解決の正規表現を作成する場合、_format_という名前のフィールドに値を入力して出力形式を設定できます。

デフォルトの設定は \1 です。これは、正規表現に一致するゾーン名が、正規表現で作成される最初の変数の内容に置き換えられることを意味します。正規表現では、かっこで囲まれた記述で変数の値が作成されます。かっこで囲まれた記述が複数ある場合、変数は左から右に数値で参照されます。変数は、任意の順序で出力形式で使用できます。定数テキストは、書式フィールドに追加することによって、出力に挿入することもできます。

たとえば、このゾーンの命名規則には、次のようなゾーン名があります。

```
 [Zone number]_[data center]_[hostname]_[device type]_[interface number]
* S123_Miami_hostname1_filer_FC1 のように入力します
* S14_Tampa_hostname2_switch_fc4
* S3991_Boston_hostname3_windows2K_FC0
* S44_Raleigh_hostname4_Solaris_FC1
```

出力形式は次のようになります。

```
 [hostname]-[data center]-[device type]
そのためには、ホスト名、データセンター、およびデバイスタイプのフィールドを変数に取り込み、それらを使用して出力する必要があります。正規表現は次のようになります。
```

```
 .*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
かっこが 3 組あるため、変数 \1 、 \2 、および \3 が入力されます。
```

この場合、次の形式で出力を受け取ることができます。

```
 \2-\1-\3
出力は次のようになります。
```

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

変数間のハイフンは、出力に一定のテキストを挿入した例を示します。

例

例 **1** ：ゾーン名の例

この例では、正規表現を使用してゾーン名からホスト名を抽出します。次のようなゾーン名がある場合は、正規表現を作成できます。

- S0032_myComputer1Name - HBA0
- S0434_myComputer1Name - HBA1
- S0432_myComputer1Name - HBA3

ホスト名を取り込むための正規表現は次のようになります。

```
 S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
```
これは、先頭の文字が「 `S` 」で、そのあとに任意の桁数の数字、アンダースコア、英数字のホスト名（ `myComputer1Name` ）、アンダースコアまたはハイフン、大文字の「 `HBA` 」、 `1` 桁の数字（ `0~9` ）の順に続くすべてのゾーンに一致します。ホスト名のみが変数 `*\1*` に格納されます。

正規表現は次のように構成要素に分割できます。

- 「 S 」はゾーン名の先頭の文字を表します。これは、ゾーン名の先頭にある「 S 」にのみ一致します。
- 角かっこで囲まれた文字 [0-9] は、「 S 」のあとの文字が 0~9 の数字でなければならないことを示します。
- + 記号は、前の角かっこ内の情報が 1 回以上存在している必要があることを示します。
- （アンダースコア）は、「 S 」のあとの数字の直後に続くゾーン名の文字がアンダースコアでなければならないことを意味します。この例のゾーンの命名規則では、ゾーン名とホスト名の区切りにアンダースコアが使用されています。
- 必須のアンダースコアのあとにあるかっこは、そのかっこで囲まれたパターンが変数 \1 に格納されることを示します。
- 角かっこで囲まれた文字 [a-zA-Z0-9] は、すべての英字（大文字と小文字の両方）と数字に一致することを示します。
- 角かっこのあとの「 * 」（アスタリスク）は、角かっこで囲まれた文字の 0 回以上の繰り返しを示します。
- 角かっこで囲まれた文字 [__]（アンダースコアとダッシュ）は、英数字のパターンのあとにアンダースコアまたはダッシュが必要であることを示します。

- 正規表現内の文字列「 HBA 」は、この文字列そのものがゾーン名に含まれている必要があることを示します。
- 最後の角かっこで囲まれた文字 [0-9] は、 0~9 の 1 桁の数字に一致します。

例 **2**

この例では、最初のアンダースコアのあとの「 E 」から 2 番目ののの前までの部分を照合し、それよりも前とあとの部分は省いています。

- ゾーン： * Z_E2FHDBS01_E1NETAPP
- ホスト名： * E2FHDBS01
- RegExp ： * 。 * ？ _ （ E. * ？） _ 。 * ？

例**3.**

正規表現の最後のセクションの前後にあるかっこ（）は、どの部分がホスト名であるかを識別します。「 VSAN3 」の部分がホスト名である場合は、 _ （ [a-zA-Z0-9] ） . * となります

ゾーン： A_VSAN3_SR48KENT_A_CX2578_SPA0

ホスト名： SR48KENT

- RegExp ： * _[a-zA-Z0-9]+_ （ [a-zA-Z0-9] ） . *

例 **4** は、複雑な命名パターンを示しています

次のようなゾーン名がある場合は、正規表現を作成できます。

- myComputerName123 ： HBA1_Symm1_FA3
- myComputerName123-HBA2_Symm1_FA5
- myComputerName123-HBA3_Symm1_FA7

これらを取り込むために使用できる正規表現は次のとおりです。

```
([a-zA-Z0-9]*)_.*
```

この式で評価された変数 `\1` には、 `_myComputerName123_` だけが含まれます。

正規表現は次のように構成要素に分割できます。

- かっこは、そのかっこで囲まれたパターンが変数 \1 に格納されることを示します。
- 角かっこで囲まれた文字 [a-zA-Z0-9] は、任意の英字（大文字と小文字の両方）と数字に一致することを示します。
- 角かっこのあとの「 * 」（アスタリスク）は、角かっこで囲まれた文字の 0 回以上の繰り返しを示します。
- 正規表現内の文字（アンダースコア）は、その前の角かっこの部分で照合された英数字の文字列の直後に続くゾーン名の文字がアンダースコアでなければならないことを意味します。

- 。（ピリオド）は、任意の文字（ワイルドカード）に一致します。
- 「*」（アスタリスク）は、その前のピリオド（ワイルドカード）が 0 回以上続くことを示します。

  つまり、「.*」の組み合わせは任意の文字数の任意の文字を表します。

例 **5** ：パターンがないゾーン名の例

次のようなゾーン名がある場合は、正規表現を作成できます。

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

これらを取り込むために使用できる正規表現は次のとおりです。

```
(.*?)_.*
```

変数 `\1` には、 `_myComputerName_` （ `1` つ目のゾーン名の例）または `_myComputerName123_` （ `2` つ目のゾーン名の例）が格納されます。したがって、この正規表現は、最初のアンダースコアの前のすべての部分に一致します。

正規表現は次のように構成要素に分割できます。

- かっこは、そのかっこで囲まれたパターンが変数 \1 に格納されることを示します。
- 「.*」（ピリオドとアスタリスク）は、任意の文字数の任意の文字に一致します。
- 角かっこのあとの「*」（アスタリスク）は、角かっこで囲まれた文字の 0 回以上の繰り返しを示します。
- 。文字は、最短一致を示します。これにより、最後のアンダースコアではなく、最初のアンダースコアでの照合が強制的に停止されます。
- 文字「_.*」は、最初のアンダースコア以降のすべての文字に一致します。

例 **6** ：パターンを含むコンピュータ名の例

次のようなゾーン名がある場合は、正規表現を作成できます。

- storage1_Switch1_myComputerName123A_A1_FC1を参照してください
- storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

これらを取り込むために使用できる正規表現は次のとおりです。

```
.*?_.*?_([a-zA-Z0-9]*[ABT])_.*
```

このゾーンの命名規則には特定のパターンがあるため、上記の式を使用できます。この式は「 `A` 」、「 `B` 」、または「 `T` 」のいずれかで終わるすべてのホスト名（この例では「 `myComputerName` 」）に一致し、そのホスト名を変数 `\1` に格納します。

正規表現は次のように構成要素に分割できます。

- 「 . * 」（ピリオドとアスタリスク）は、任意の文字数の任意の文字に一致します。
- 。文字は、最短一致を示します。これにより、最後のアンダースコアではなく、最初のアンダースコアでの照合が強制的に停止されます。
- アンダースコア文字は、ゾーン名の最初のアンダースコアに一致します。
- したがって、最初の ***.?combination*** は、最初のゾーン名の例では、 ***Storage1*** という文字と一致します。
- 2 番目の .*?*combination* は最初のゾーンと同じように動作しますが、最初のゾーン名の例では *Switch1* と一致します。
- かっこは、そのかっこで囲まれたパターンが変数 \1 に格納されることを示します。
- 角かっこで囲まれた文字 [a-zA-Z0-9] は、任意の英字（大文字と小文字の両方）と数字に一致することを示します。
- 角かっこのあとの「 * 」（アスタリスク）は、角かっこで囲まれた文字の 0 回以上の繰り返しを示します。
- 正規表現内の角かっこで囲まれた文字 [ABT] は、ゾーン名に含まれる「 A 」、「 B 」、または「 T 」のいずれか 1 文字に一致します
- かっこのあとの（アンダースコア）は、 [ABT] で照合された文字のあとにアンダースコアが必要であることを示します。
- 「 . * 」（ピリオドとアスタリスク）は、任意の文字数の任意の文字に一致します。

その結果、次のいずれかの英数字文字列を含む変数 \1 が原因されます。

- 前に任意の数の英数字と 2 つのアンダースコアがある
- 後ろにアンダースコア（および任意の数の英数字）がある。
- 3 番目のアンダースコアの前に、 A 、 B 、または T の最後の文字を使用した。

例**7.**

ゾーン： myComputerName123_HBA1_Symm1_FA1

ホスト名： myComputerName123

- RegExp ： * （ [a-zA-Z0-9]+ ） _ 。 *

例**8**

この例では、最初ののの前のすべての部分を検出します。

ゾーン： MyComputerName_HBA1_Symm1_FA1

MyComputerName123_HBA1_Symm1_FA1

Hostname ： MyComputerName

正規表現：（ .* ？） _ 。 *

例**9**

この例では、最初のののあとから2番目ののの前までのすべての部分を検出します。

- ゾーン： * Z_MyComputerName_StorageName
- ホスト名： * MyComputerName
- RegExp ：*。*？_（*？）_。*？

例**10**

この例では、ゾーンの例から「 MyComputerName123 」を抽出します。

ゾーン： Storage1_Switch1_MyComputerName123A_A1_FC1

storage2_Switch2_MyComputerName123B_A2_FC2

Storage3_Switch3_MyComputerName123T_A3_FC3

ホスト名： MyComputerName123

- RegExp ：*。*。_。*？_（[a-zA-Z0-9]+）* [ABT] _。*

例**11**

ゾーン： Storage1_Switch1_MyComputerName123A_A1_FC1

ホスト名： MyComputerName123A

- RegExp ：*。*。_。*？_（[a-zA-Z0-9]+）_。*？_

例**12**

角かっこ * の内側にある ^ （キャレット） * は、その式の否定を表します。たとえば、 [^Ff] は大文字の F と小文字の F を除くすべての文字に一致し、 [^a-z] は小文字の a~z を除くすべての文字に一致します。上の例の場合は、 _ 以外の文字に一致します。format ステートメントは、出力ホスト名にを追加します。

- ゾーン： * mhs_apps44_d_a_10a0_0429
- ホスト名： * mhs-apps44-d
- RegExp：**()_([AB]).* Data Infrastructure Insights**の形式：**\1-\2([^_])_()_([^_]).** Data Infrastructure Insightsの形式：\1-\2-\3

例**13**

この例では、ストレージエイリアスの区切りにが使用されています。この場合、が文字列で実際に使用されており、式の一部ではないことを示すために、を使用する必要があります。

- ストレージエイリアス： * \Hosts\E2DOC01C1\E2DOC01N1

ホスト名： E2DOC01N1

- RegExp ：*\\。*？\\。*？\\（.*？）

例14

この例では、ゾーンの例から「PD-RV-W-AD-2」を抽出します。

- ゾーン： * PD_D-RV-W-AD-2_01
- ホスト名： * pd-RV-W-AD-2
- RegExp ： * [^-] + - （ . * - \d+ ） . *

例15

この例では、形式の設定でホスト名に「 US-BV- 」を追加しています。

ゾーン： SRV_USBVM11_F1

ホスト名： US-BV-M11

- RegExp ： * SRV_USBV （ [a-zA-Z0-9]+ ） _F [12]
- フォーマット： * US-BV-\1

アセットページ情報

アセットページの概要

アセットページには、アセットの現在のステータスの概要と、アセットと関連するアセットに関する追加情報へのリンクが表示されます。

アセットページのタイプ

Data Infrastructure Insightsには、次のアセットのアセットページが用意されています。

- 仮想マシン
- Storage Virtual Machine （ SVM ）
- ボリューム
- 内部ボリューム
- ホスト（ハイパーバイザーを含む）
- ストレージプール
- ストレージ
- データストア
- アプリケーション
- ストレージノード
- qtree
- ディスク
- VMDK です

- ポート
- スイッチ
- ファブリック

表示データの時間範囲を変更する

アセットページにはデフォルトでは過去 24 時間のデータが表示されますが、他の一定の期間やカスタムの期間を選択して、その範囲のデータを表示することができます。

アセットの種類に関係なく、すべてのアセットページに表示されるオプションを使用して、データを表示する期間を変更することができます。時間範囲を変更するには、トップバーに表示されている時間範囲をクリックし、次の時間セグメントから選択します。

- 最後の 15 分
- 過去 30 分
- 最後の60分
- 過去2時間
- 過去 3 時間（デフォルト）
- 過去6時間
- 過去12時間
- 過去 24 時間
- 過去2日間
- 過去 3 日間
- 過去7日間
- 過去30日間
- カスタムの期間

カスタム期間では、最大 31 日間連続で選択できます。この範囲に開始時間と終了時間を設定することもできます。デフォルトの開始時間は、最初に選択した日の午前 12 時、最後に選択した日のデフォルトの終了時間は午後 11 時 59 分です。適用をクリックすると、カスタムの期間がアセットページに適用されます。

アセットページの概要セクションの情報、およびページの表やカスタムウィジェットの情報は、選択した期間に基づいて自動的に更新されます。現在のリフレッシュレートは、[Summary]セクションの右上隅、およびページ上の関連するテーブルまたはウィジェットに表示されます。

カスタムウィジェットを追加します

任意のアセットページに独自のウィジェットを追加できます。 追加したウィジェットは、そのタイプのすべてのオブジェクトのアセットページに表示されます。たとえば、ストレージアセットページにカスタムウィジェットを追加すると、そのウィジェットがすべてのストレージアセットのアセットページに表示されます。

コンテキスト内のオブジェクトのフィルタリング

アセットのランディングページでウィジェットを設定するときに、 _incontext_filters を

設定すると、現在のアセットに直接関連するオブジェクトのみを表示できます。デフォルトでは、ウィジェットを追加すると、環境内で選択したタイプの _ALL_OBJECTS が表示されます。コンテキスト内フィルタを使用すると、現在のアセットに関連するデータのみを表示できます。

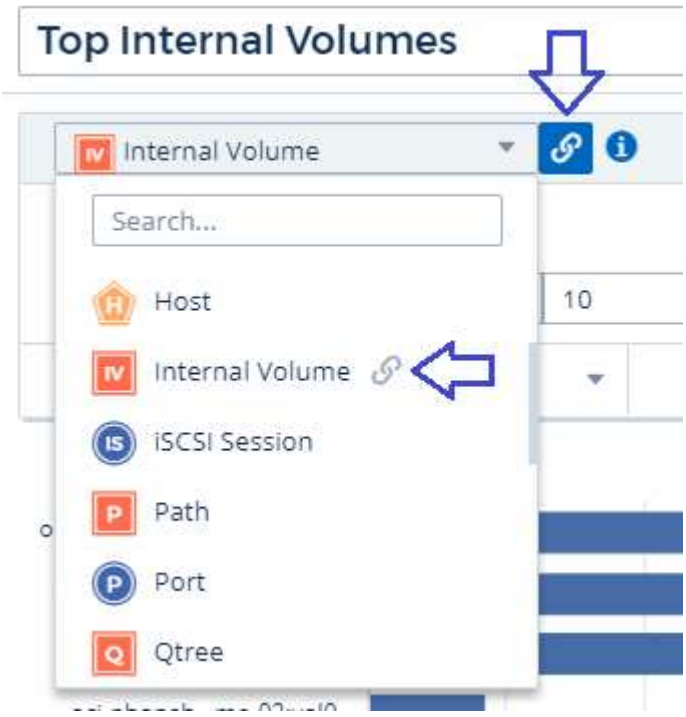
ほとんどのアセットランディングページでは、現在のアセットに関連するオブジェクトをフィルタできます。フィルタのドロップダウンでは、リンクアイコンが表示されるオブジェクトタイプを現在のアセットに合わせてフィルタリングできます。

たとえば、ストレージアセットページで棒グラフウィジェットを追加すると、そのストレージの内部ボリュームのみの上位 IOPS を表示できます。デフォルトでは、ウィジェットを追加すると、環境内の _all_internal ボリュームが表示されます。

現在のストレージアセット上の内部ボリュームのみを表示するには、次の手順を実行します。

手順

1. 任意の * ストレージ * アセットのアセットページを開きます。
2. 編集 * をクリックして、アセットページを編集モードで開きます。
3. [ウィジェットを追加（ Add Widget ）] をクリックし、 [バーチャート _ （ *Bar Chart* ）] を
4. 棒グラフに表示するオブジェクトタイプとして「 * 内部ボリューム * 」を選択します。内部ボリュームのオブジェクトタイプの横にリンクアイコンが表示されていることを確認します。「リンク済み」アイコンはデフォルトで有効になっています。



5. [*IOPS] - [Total*] を選択して、追加のフィルタを設定します。
6. 横にある [X] をクリックして、 [**Roll Up**] フィールドを折りたたみます。[* Show *] フィールドが表示されます。
7. トップ 10 を表示することを選択します。

8. ウィジェットを保存します。

   棒グラフには、現在のストレージアセットにある内部ボリュームのみが表示されます。

すべてのストレージオブジェクトのアセットページにウィジェットが表示されます。ウィジェットでコンテキスト内リンクが有効になっている場合は、現在表示されているストレージアセットに関連する内部ボリュームのデータが棒グラフに表示されます。

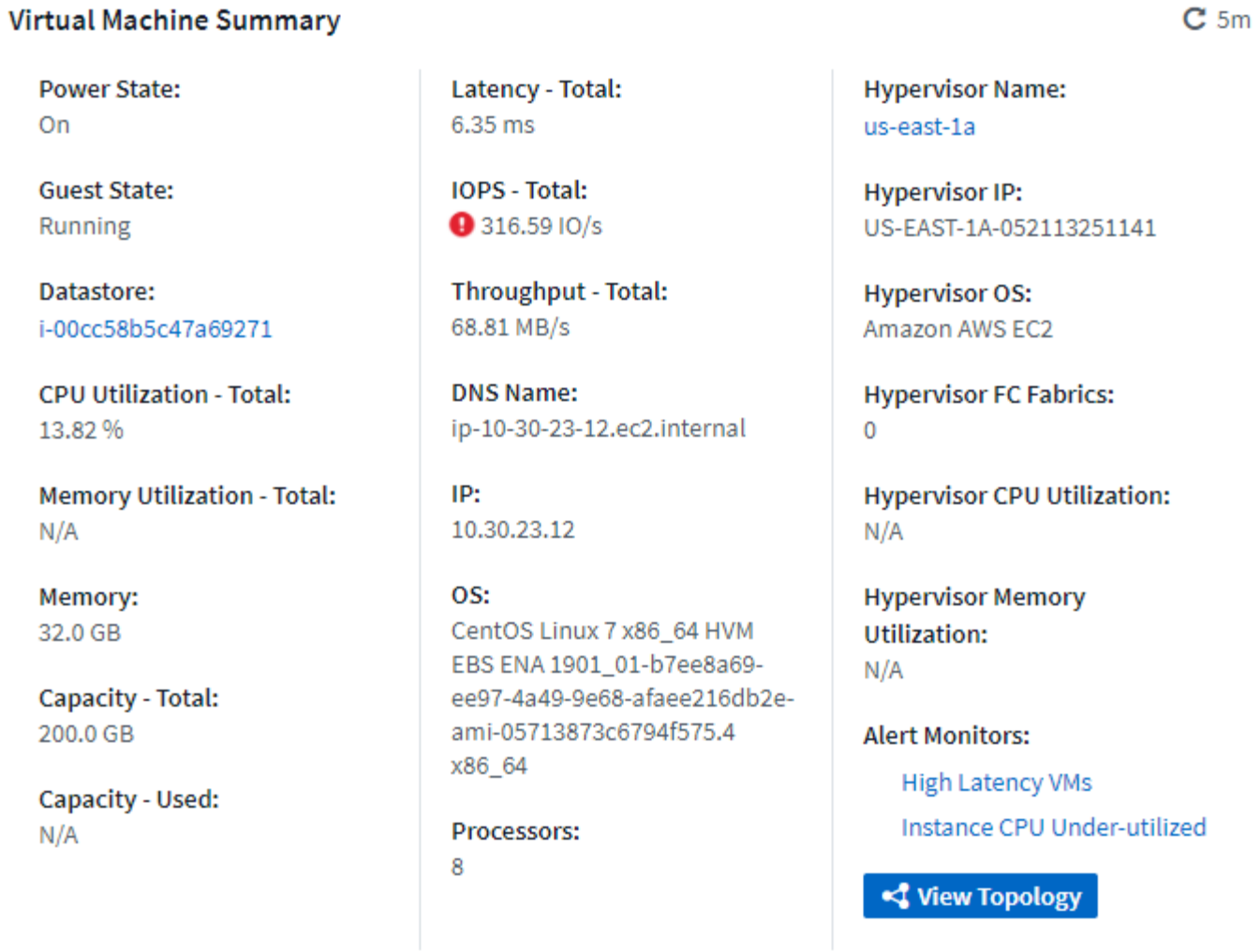
オブジェクトデータのリンクを解除するには、ウィジェットを編集し、オブジェクトタイプの横にあるリンクアイコンをクリックします。リンクが無効になり、環境内の_all_objectsのデータがグラフに表示されます。

を使用することもできます "* ウィジェットの特殊な変数 *" をクリックすると、ランディングページにアセット関連の情報が表示されます。

アセットページの概要セクション

アセットページの概要セクションには、原因の指標やパフォーマンスポリシーなど、アセットに関する全般的な情報が表示されます。潜在的な問題領域は赤い丸で示されます。

概要セクションの情報、およびアセットページの表やカスタムウィジェットの情報は、選択した期間に基づいて自動的に更新されます。現在のリフレッシュレートは、[Summary]セクション、テーブル、およびカスタムウィジェットの右上隅に表示されます。



注：「概要」セクションに表示される情報は、表示しているアセットのタイプによって異なります。

いずれかのアセットのリンクをクリックすると、対応するアセットページを表示できます。たとえば、ストレージノードを表示している場合、リンクをクリックすると、関連付けられているストレージのアセットページを表示できます。

アセットに関連付けられている指標を表示できます。指標の横に赤い丸が表示されている場合、診断や解決を要する潜在的な問題があることを示しています。

一部のストレージアセットについて、ボリュームの容量の表示が 100% を超えることがあります。これは、ボリュームの容量に関するメタデータが使用済み容量としてアセットから報告されるためです。

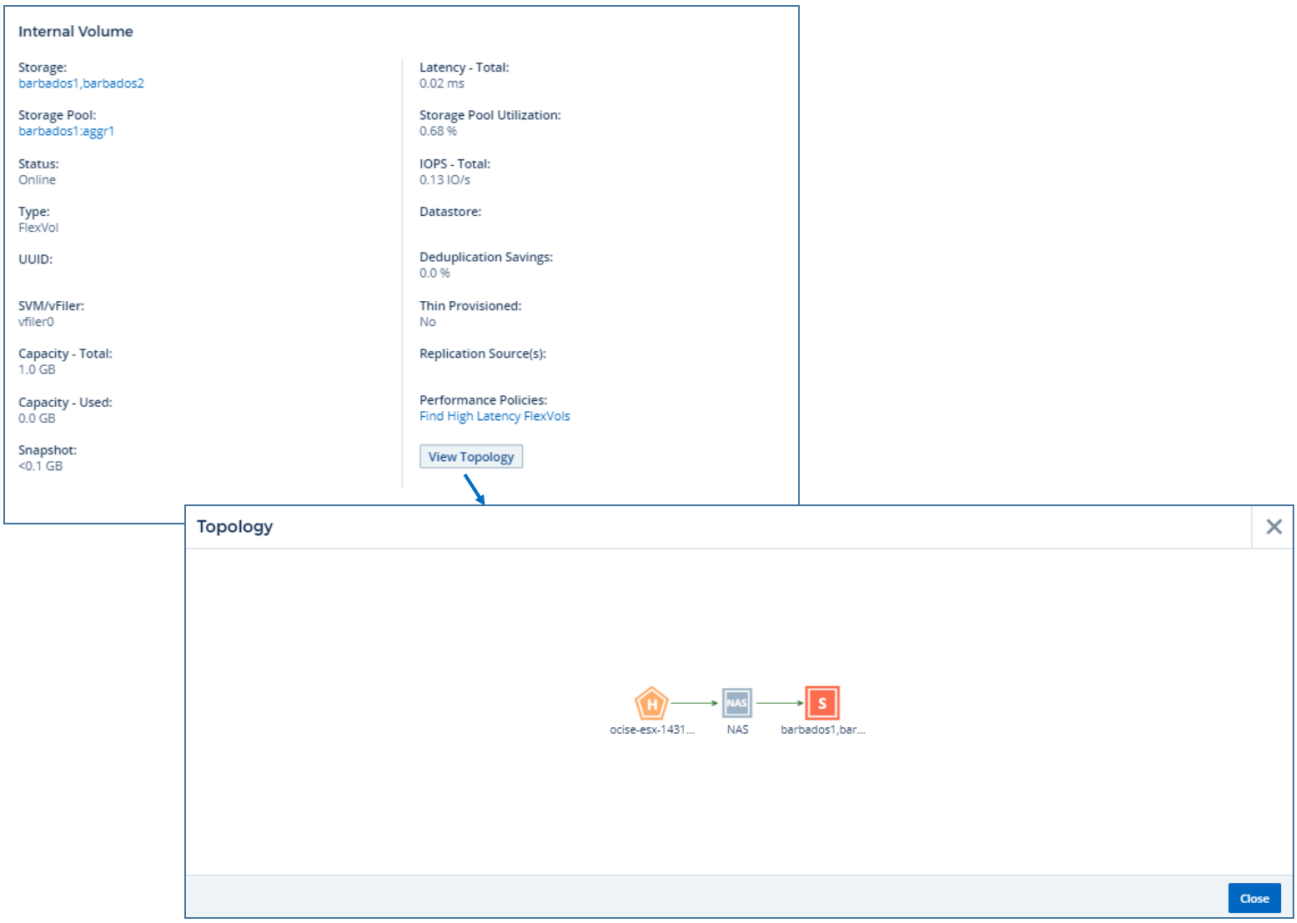
該当する場合は、アラートのリンクをクリックして、アセットに関連付けられているアラートとモニタを表示できます。

トポロジ

一部のアセットページでは、概要セクションにアセットとその接続のトポロジを表示するためのリンクが表示されます。

トポロジは次のアセットタイプで使用できます。

- アプリケーション
- ディスク
- ファブリック
- ホスト
- 内部ボリューム
- ポート
- スイッチ
- 仮想マシン
- VMDK です
- ボリューム



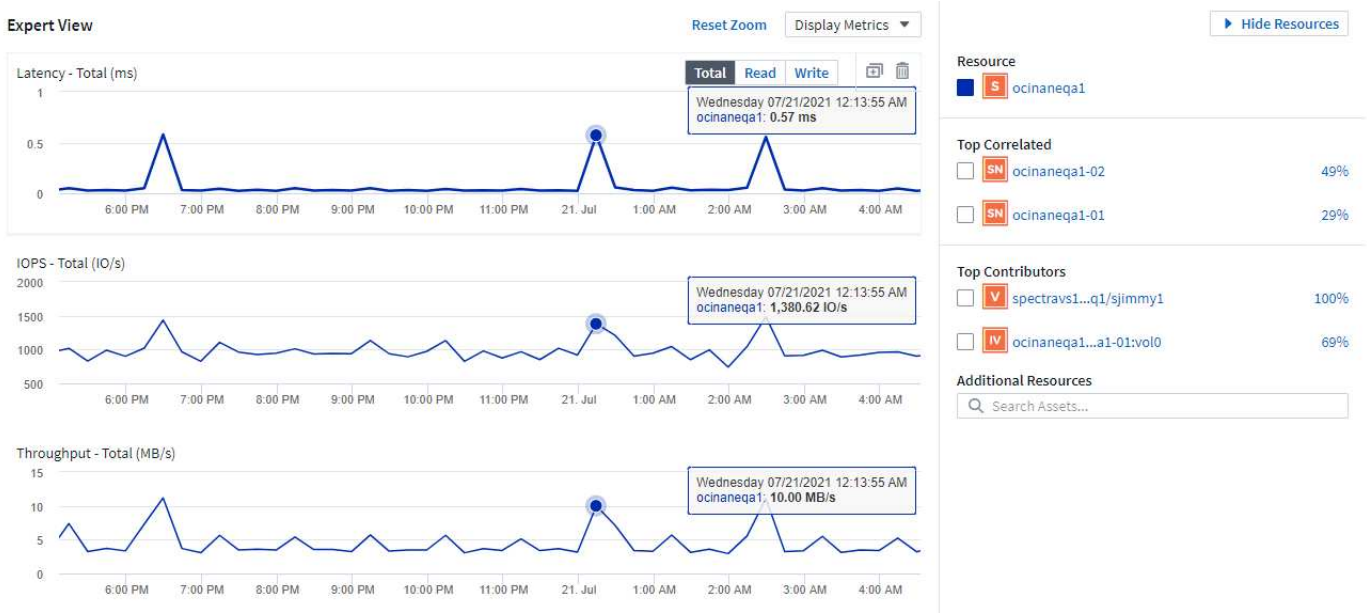
エキスパートビュー

アセットページのエキスパートビューセクションでは、任意の数の該当する指標に基づ

いてベースアセットのパフォーマンスサンプルを表示でき、選択した期間のパフォーマンスチャートと関連するアセットを参照できます。 グラフのデータは、データコレクタがポーリングを行い、更新されたデータが取得されると自動的に更新されます。

[エキスパートビュー（ **Expert View** ）] セクションの使用

ストレージアセットページの Expert View セクションの例を次に示します。



選択した期間について、パフォーマンスチャートで表示する指標を選択することができます。[Display Metrics_] ドロップダウンをクリックし、表示されたメトリックから選択します。

リソースセクションには、ベースアセットの名前とパフォーマンスチャートでの色が表示されます。「上位相関 * 」セクションにパフォーマンスチャートに表示したいアセットが含まれていない場合は、「その他のリソース」セクションの「アセットの検索」ボックスを使用してアセットを検索し、パフォーマンスチャートに追加できます。リソースを追加すると、 [追加リソース] セクションにリソースが表示されます。

ベースアセットに関連するアセットがある場合、それらのアセットもリソースセクションに次のカテゴリ別に表示されます。

- 関連性が高い

  1 つ以上のパフォーマンス指標との関連性が高いアセット（割合）がベースアセットに表示されます。

- 上位貢献者

  ベースアセットへの影響が大きいアセットが表示されます。

- ワークロードの競合

  ホスト、ネットワーク、ストレージなど、他の共有リソースに影響を及ぼすアセットと影響を受けるアセットが表示されます。このようなリソースを_greeding_/degraded_resourcesと呼ぶこともあります。

エキスパートビューのアラート

また、アセットランディングページのエキスパートビューセクションには、アラートをトリガーした時間と期間、およびアラートをトリガーした監視条件が表示されます。

エキスパートビューの指標の定義

アセットページのエキスパートビューセクションには、アセットに対して選択した期間に関する複数の指標が表示されます。各指標は独自のパフォーマンスチャートに表示されます。確認が必要なデータに応じて、チャートに表示する指標や関連するアセットを追加したり削除したりできます。選択できる指標はアセットのタイプによって異なります。

* メートル法 *	* 概要 *
BB クレジットのゼロ受信、転送	サンプリング期間中に受信 / 送信のバッファ間クレジット数がゼロになった回数。この指標は、接続されたポートで提供できるクレジットを使い果たしたために転送が中止された回数を表します。
BB クレジットのゼロ期間の転送	サンプリング期間中に送信 BB クレジットがゼロになっていた時間（ミリ秒）。
キャッシュヒット率（合計、読み取り、書き込み）	キャッシュにヒットする要求の割合。ボリュームへのアクセス数に対するヒット数の割合が高いほど、パフォーマンスが高くなります。この列は、キャッシュヒット情報を収集しないストレージアレイについては空になります。
キャッシュ使用率（合計）	キャッシュにヒットするキャッシュ要求の合計割合
クラス 3 は破棄されます	ファイバチャネルのクラス 3 データ転送が破棄された回数。
CPU 利用率（合計）	使用可能な合計（すべての仮想 CPU ）に対する使用中のアクティブな CPU リソースの割合。
CRC エラーです	サンプリング期間中にポートで無効な Cyclic Redundancy Check （ CRC ；巡回冗長検査）が検出されたフレーム数
フレームレート	転送フレームレート（ 1 秒あたりのフレーム数）。

フレームサイズ平均（ Rx 、 Tx ）	フレームサイズに対するトラフィックの比率。この指標から、ファブリック内にフレームのオーバーヘッドがないかどうかを特定できます。
フレームサイズが長すぎます	ファイバチャネルの長すぎるデータ転送フレームの数。
フレームサイズが短すぎます	ファイバチャネルの短すぎるデータ転送フレームの数。
I/O 密度（合計、読み取り、書き込み）	ボリューム、内部ボリューム、またはストレージ要素の使用済み容量（データソースの最新のインベントリポーリングから取得）で IOPS を割った値。1 秒間の TB あたりの I/O 処理数で測定されます。
IOPS （合計、読み取り、書き込み）	I/O チャネルまたはそのチャネルの一部を通過する読み取り / 書き込み I/O サービス要求の単位時間あたりの数（ 1 秒あたりの I/O 数で測定）
IP スループット（合計、読み取り、書き込み）	合計： IP データの転送および受信速度の合計。 1 秒あたりのメガバイト数で示されます。
読み取り： IP スループット（受信）：	IP データを受信した平均レート（ 1 秒あたりのメガバイト数）。
書き込み： IP スループット（送信）：	IP データが 1 秒あたりのメガバイト数で送信された平均レート。
レイテンシ（合計、読み取り、書き込み）	Latency （ R&W ）：一定の時間内にデータが仮想マシンに対して読み取りまたは書き込みされるレート。1 秒あたりのメガバイト数で測定されます。
レイテンシ	データストア内の仮想マシンからの平均応答時間。
上位のレイテンシ：	データストア内の仮想マシンからの最大応答時間。
リンク障害です	サンプリング期間中にポートで検出されたリンク障害の数。
リンクリセット Rx 、 Tx	サンプリング期間中に受信または送信されたリセットリンクの数。この指標は、このポートに対して接続されたポートから発行されたリンクリセットの数を表します。
メモリ使用率（合計）	ホストで使用されるメモリのしきい値。
部分的 R/W （合計） %	RAID 5 、 RAID 1/0 、または RAID 0 の LUN において、読み取り / 書き込み処理がディスクモジュールのストライプ境界を越えた合計回数。通常、ストライプを越えると、各 LUN で追加の I/O が必要になるため、ストライプを越えることは効果がありませんこの割合が低いほど、ストライプ要素のサイズは効率的であり、ボリューム（ネットアップの LUN ）のアライメントは不適切であることを示します。CLARiX については、ストライプを越えた回数を IOPS の合計で割った値が示されます。
ポートエラーです	サンプリング期間中または一定の期間に検出されたポートエラーのレポート。

信号損失回数	信号損失エラーの数。信号損失エラーが発生した場合は、電気的接続がなく、物理的な問題があります。
スワップレート（合計レート、インレート、アウトレート）	サンプリング期間中にディスクとアクティブメモリの間にスワップイン速度、スワップアウト速度、またはその両方が発生した速度。これは環境仮想マシンのカウンタです。
同期損失の数	同期損失エラーの数同期損失エラーが発生した場合、ハードウェアはトラフィックを認識できないか、ロックオンされません。すべての機器のデータ速度が同じでないか、光接続または物理接続の品質が低下している可能性があります。このエラーが発生するたびにポートの再同期が必要になるため、システムのパフォーマンスに影響します。単位は KB/ 秒です
スループット（合計、読み取り、書き込み）	I/O サービス要求への応答として一定の時間内に送受信されたデータのレート（ 1 秒あたりの MB で測定）。
タイムアウト廃棄フレーム数 - Tx	送信フレームがタイムアウトで破棄された回数。
トラフィック速度（合計、読み取り、書き込み）	サンプリング期間中に送受信されたトラフィックの量（ 1 秒あたりのメビバイト数）。
トラフィック利用率（合計、読み取り、書き込み）	サンプリング期間中の送受信トラフィックの比率、受信 / 送信 / 合計容量に対するトラフィックの比率。
利用率（合計、読み取り、書き込み）	送信（ Tx ）と受信（ Rx ）に使用できる帯域幅の割合。
書き込み保留（合計）	保留中の書き込み I/O サービス要求の数。

[エキスパートビュー（ **Expert View** ） **]** セクションの使用

エキスパートビューのセクションでは、選択した期間中に適用可能な任意の数の指標に基づいてアセットのパフォーマンスチャートを表示し、関連するアセットを追加してアセットと関連するアセットのパフォーマンスをさまざまな期間で比較および比較できます。

手順

1. 次のいずれかの方法でアセットページを検索します。
   - 特定のアセットを検索して選択します。
   - ダッシュボードウィジェットからアセットを選択します。
   - 一連のアセットを照会し、結果リストから 1 つ選択します。

     アセットページが表示されます。デフォルトでは、パフォーマンスチャートには、アセットページで選択した期間についての 2 つの指標のデータが表示されます。たとえば、ストレージの場合は、レイテンシと合計 IOPS がデフォルトで表示されます。リソースセクションには、リソースの名前とその他のリソースセクションが表示されます。ここでは、アセットを検索できます。アセットによっては、関連性の高いアセット、影響のあるリソース、 Greedy リソース、 Dedgraded セクションにアセットが表示されることもあります。これらのセクションに関連するアセットがない場合、それらのアセットは表示されません。

2. 指標のパフォーマンスチャートを追加するには、 [* Display Metrics] をクリックし、表示する指標を選択します。

選択した指標ごとに個別のグラフが表示されます。グラフには、選択した期間のデータが表示されます。期間を変更するには、アセットページの右上にある別の期間をクリックするか、グラフを拡大します。

[Display Metrics] をクリックして、グラフの選択を解除します。エキスパートビューからは、その指標のパフォーマンスチャートが削除されます。

3. グラフにカーソルを合わせ、アセットに応じて次のいずれかをクリックすると、そのグラフに表示される指標データを変更できます。

   ◦ 読み取り、書き込み、合計のいずれかです

   ◦ Tx 、 Rx 、または Total

     デフォルトは合計です。

   グラフ上でカーソルをドラッグしてデータポイントを選択すると、選択した期間における指標の値の変化を確認できます。

4. リソースセクションでは、関連するアセットをパフォーマンスチャートに追加できます。

   ◦ 関連するアセットを「上位の関連項目 * 」、「上位の寄与者 * 」、「 Greedy * 」、「 Degraded 」の各セクションで選択することで、そのアセットのデータを選択した各指標のパフォーマンスチャートに追加できます。

     アセットを選択すると、そのアセットのグラフ上のデータポイントと同じ色のブロックがアセットの横に表示されます。

5. [リソースを隠す] をクリックすると、 [その他のリソース] ペインが非表示になります。[* リソース] をクリックしてペインを表示します。

   ◦ 表示されているアセットの名前をクリックすると、そのアセットページを表示できます。また、ベースアセットに対する関連性または影響度を示す数値をクリックすると、ベースアセットとアセットの関連性の詳細が表示されます。

     たとえば、関連性が高いアセットの横にある関連性の数値をクリックすると、ベースアセットとの関連性についてタイプ別に比較した情報メッセージが表示されます。

   ◦ 関連性が高いセクションに比較のためにパフォーマンスチャートに表示するアセットが含まれていない場合は、 [その他のリソース] セクションの [アセットの検索] ボックスを使用して他のアセットを検索できます。

選択したアセットは、 [リソースの追加] セクションに表示されます。アセットに関する情報を表示する必要がなくなった場合は、ゴミ箱アイコンをクリックして削除します。

User Data セクション

アセットページの User Data セクションには、アプリケーションやアノテーションなどのユーザ定義データが表示されます。データの変更も可能です。

User Data セクションを使用してアプリケーションを割り当てまたは変更する

環境で実行しているアプリケーションを特定のアセット（ホスト、仮想マシン、ボリューム、内部ボリューム、 qtree 、 ハイパーバイザーを含む）。User Data セクションでは、アセットに割り当てられているアプリケーションを追加、変更、または削除できます。これらのアセットタイプにボリュームを除くすべてのタイプ

を対象に、複数のアプリケーションを割り当てることができます。

手順

1. 次のいずれかの方法でアセットページを検索します。
   a. アセットのリストを照会し、リストから 1 つ選択します。
   b. ダッシュボードで、アセット名を確認してクリックします。
   c. 検索を実行し、結果からアセットを選択します。

      アセットページが表示されます。ページの User Data セクションには、現在割り当てられているアプリケーションまたはアノテーションが表示されます。

割り当てられているアプリケーションを変更したり、アプリケーションやその他のアプリケーションを割り当てるには、 * Application * リストをドロップダウンして、アセットに割り当てるアプリケーションを選択します。アプリケーションを検索するにはを入力し、リストからアプリケーションを選択します。

アプリケーションを削除するには、アプリケーションリストをドロップダウンし、アプリケーションのチェックを解除します。

User Data セクションを使用して、注釈を割り当てまたは変更する

Data Infrastructure Insightsでデータの追跡方法を企業の要件に合わせてカスタマイズする場合は、アノテーションと呼ばれる特殊なメモを定義してアセットに割り当てることができます。アセットページの User Data セクションには、アセットに割り当てられているアノテーションが表示されます。また、そのアセットに割り当てるアノテーションを変更することもできます。

手順

1. アセットにアノテーションを追加するには、アセットページの User Data セクションで、 * + Annotation * をクリックします。
2. リストからアノテーションを選択します。
3. 値をクリックし、選択したアノテーションのタイプに応じて次のいずれかを実行します。
   a. アノテーションタイプがリスト、日付、またはブーリアンの場合は、値をリストから選択します。
   b. アノテーションタイプがテキストの場合は、値を入力します。
4. [保存] をクリックします .

アセットにアノテーションが割り当てられ、クエリでアノテーションに基づいてアセットをフィルタできるようになります。

アノテーションを割り当てたあとに値を変更する場合は、アノテーションリストをドロップダウンして別の値を入力します。

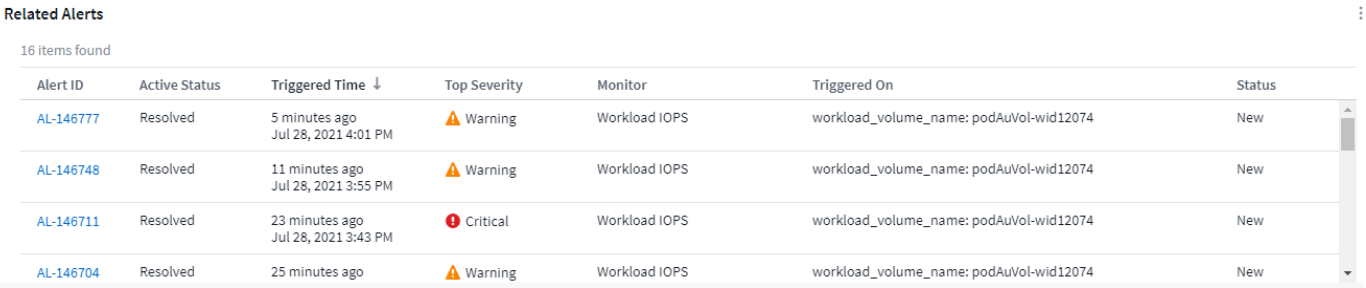
fly_option で新しい値を追加するために _Add を選択したリストタイプのアノテーションの場合は ' 既存の値を選択するだけでなく ' 新しい値を追加することもできます

Asset Page Related Alerts セクション

アセットページの関連アラートセクションでは、アセットに割り当てられたモニタを実行した結果、環境で発生したアラートを確認できます。では、設定した条件に基づいて

アラートが生成されます。予想される影響を特定し、問題の影響とルート原因を分析できるため、迅速かつ効果的に修正できます。

次の例は、アセットページに表示される一般的な関連アラートのセクションを示しています。



Related Alerts セクションでは、アセットに割り当てられた監視条件の結果としてネットワークで発生するアラートを表示および管理できます。

手順

- 次のいずれかの方法でアセットページを検索します。
  - 検索領域にアセットの名前を入力し、リストからアセットを選択します。
  - ダッシュボードウィジェットで、アセットの名前をクリックします。
  - 一連のアセットを照会し、結果リストからオンを選択します。

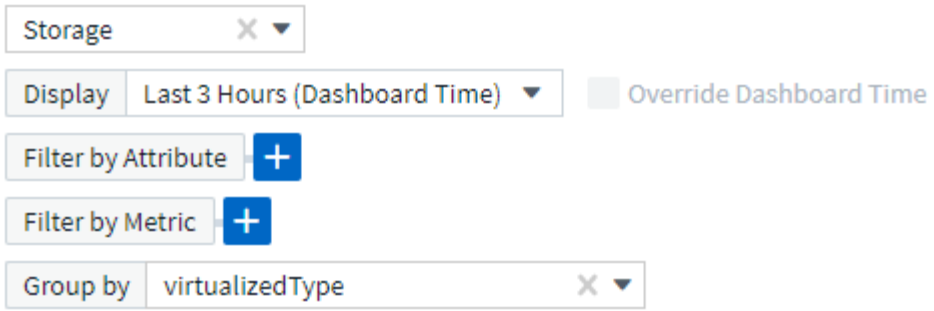
アセットページが表示されます。関連アラートセクションには、アラートがトリガーされた時刻と、アラートの現在のステータス、およびアラートをトリガーしたモニタが表示されます。アラート ID をクリックすると、アラートのランディングページを開いて詳しい調査を行うことができます。

ストレージ仮想化

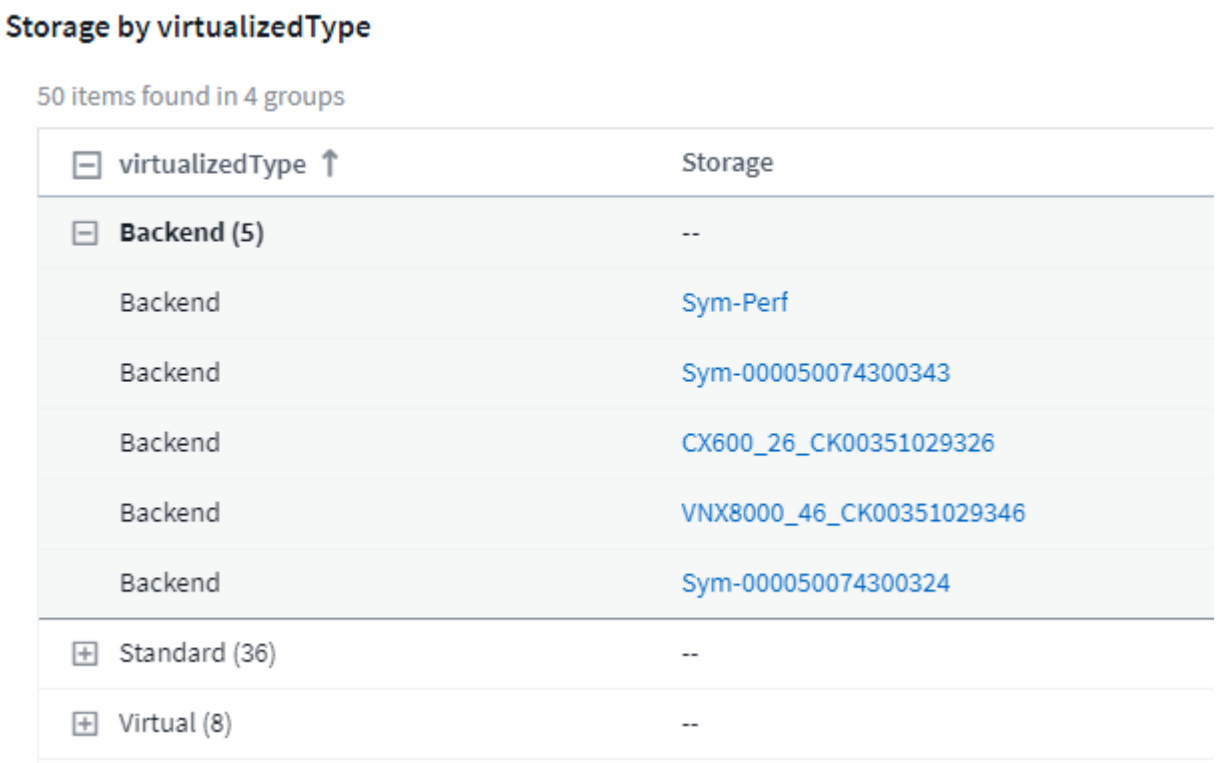
Data Infrastructure Insightsでは、ローカルストレージがあるストレージアレイと、他のストレージアレイが仮想化されているストレージアレイを区別できます。これにより、コストを関連付け、フロントエンドからインフラのバックエンドまで、パフォーマンスを区別することができます。

テーブルウィジェットでの仮想化

ストレージ仮想化を確認する最も簡単な方法の1つは、[Virtualized]タイプを示すダッシュボード表ウィジェットを作成することです。ウィジェットのクエリを作成するときは、グループ化またはフィルタに「virtualizedType」を追加するだけです。

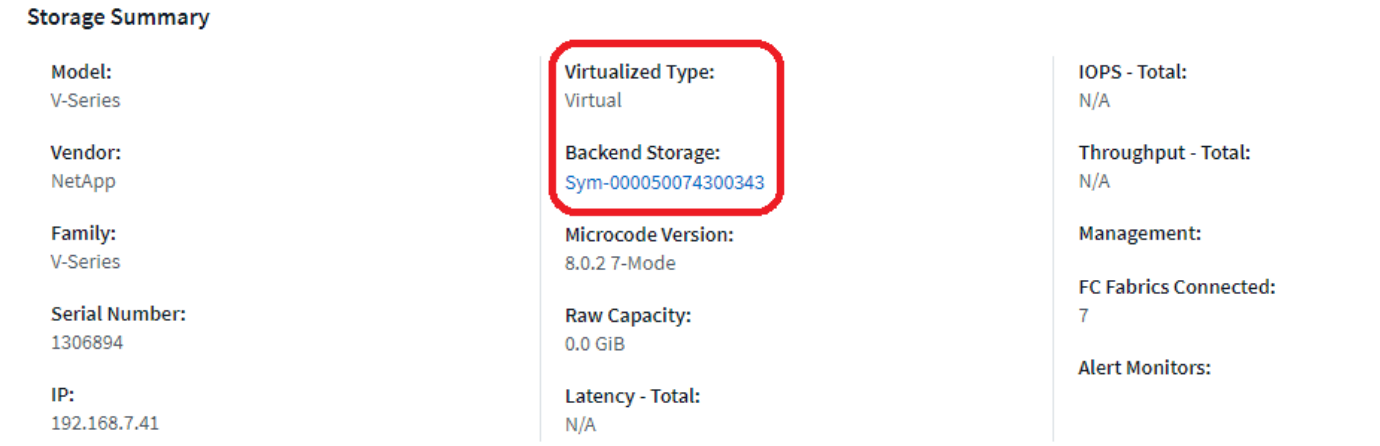


表示される表ウィジェットには、環境内の_Standard_、*Backend*、および_Virtual _ストレージが表示されます。



ランディング・ページには仮想化された情報が表示される

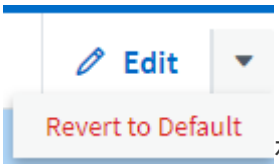
ストレージ、ボリューム、内部ボリューム、ディスクのランディングページでは、関連する仮想化情報を確認できます。たとえば、以下のストレージランディングページを見ると、これが仮想ストレージであり、どのバックエンドストレージシステムが適用されているかがわかります。ランディングページの関連テーブルにも、必要に応じて仮想化情報が表示されます。



既存のランディングページとダッシュボード

現在の環境でカスタマイズされたランディングページやダッシュボードを使用している場合、デフォルトではすべての仮想化情報が自動的に表示されるわけではないことに注意してください。ただし、任意のカスタマイズされたダッシュボードまたはランディングページ（カスタマイズを再実装する必要があります）に戻すことも、必要な仮想化の属性や指標を含めるように関連するウィジェットを変更することもできます。

カスタムダッシュボードまたはランディングページ画面の右上隅にある_revert to default_を使用できます。



ボタン"]

資産とアラートを検索するためのヒントとヒント

監視対象環境内のデータやオブジェクトを検索する場合は、複数の検索手法を使用できます。

- * ワイルドカード検索 *

  文字を使用して、複数文字のワイルドカード検索を実行できます。たとえば、 *applic * n* は *application* を返します。

- * フレーズ検索 *

  フレーズは、「 VNX LUN 5 」などの二重引用符で囲まれた単語のグループです。二重引用符を使用して、名前または属性にスペースを含むドキュメントを検索できます。

- * 論理演算子 *

  論理演算子 OR 、 AND 、 NOT を使用すると、複数のキーワードを組み合わせて複雑なクエリを作成できます。

  または

  OR 演算子は、デフォルトの結合演算子です。

2 つのキーワードの間にブール演算子がない場合は、 OR 演算子が使用されます。

OR 演算子は、 2 つのキーワードをリンクし、どちらかの条件がドキュメントに存在する場合に一致するドキュメントを検索します。

たとえば、 *storage* や *NetApp_searches* と指定すると、 *_storage_or_NetApp._* を含むドキュメントが検索されます。

一致するキーワードの数が多いドキュメントほどスコアが高くなります。

および

AND 演算子を使用すると、両方の検索語が 1 つのドキュメント内に存在するドキュメントを検索できます。たとえば、 *storage* と *NetApp_searches* は、 *_storage* と *NetApp* の両方を含むドキュメントを検索します。

との代わりに、記号 * & * を使用できます。

ありません

NOT 演算子を使用すると、 NOT のあとのキーワードを含むすべてのドキュメントが検索結果から除外されます。たとえば、 *storage NOT NetApp_searches* を指定すると、 *_storage* のみを含み、かつ *NetApp* でないドキュメントが検索されます。

NOT という単語の代わりに、記号 * ！ * を使用できます。

検索では大文字と小文字は区別されません。

インデックスキーワードを使用して検索します

インデックスキーワードの数が多い検索では、スコアが高くなります。

検索文字列は、スペースで複数の検索キーワードに分けて表示されます。たとえば、「 storage aurora netapp 」という検索文字列は、「 storage 」、「 aurora 」、「 netapp 」の 3 つのキーワードに分けられ、3 つのキーワードをすべて使用して検索が実行されます。これらのキーワードのほとんどに一致するドキュメントのスコアが最も高くなります。入力する情報が多いほど、検索結果の方が適しています。たとえば、ストレージを名前やモデルで検索できます。

検索結果は、カテゴリごとに上位 3 件まで表示されます。想定しているオブジェクトが見つからない場合は、検索文字列にキーワードを追加して検索結果を絞り込むことができます。

次の表に、検索文字列に追加できるインデックスキーワードのリストを示します。

カテゴリ	インデックスキーワード
ストレージ	"ストレージ" 名前 ベンダー モデル

カテゴリ	インデックスキーワード
ストレージプール	"ストレージプール" 名前 ストレージの名前 ストレージのIPアドレス ストレージのシリアル番号 ストレージベンダー ストレージモデル 関連付けられているすべての内部ボリュームの名前 関連付けられているすべてのディスクの名前
内部ボリューム	"内部ボリューム" 名前 ストレージの名前 ストレージのIPアドレス ストレージのシリアル番号 ストレージベンダー ストレージモデル ストレージプールの名前 関連付けられているすべての共有の名前 関連付けられているすべてのアプリケーションの名前
ボリューム	"ボリューム" 名前 ラベル すべての内部ボリュームの名前 ストレージプールの名前 ストレージの名前 ストレージのIPアドレス ストレージのシリアル番号 ストレージベンダー ストレージモデル
ストレージノード	"ストレージノード" 名前 ストレージの名前 ストレージのIPアドレス ストレージのシリアル番号 ストレージベンダー ストレージモデル
ホスト	"ホスト" 名前 IP アドレス 関連付けられているすべてのアプリケーションの名前
データストア	"データストア" 名前 Virtual Center IPの略 すべてのボリュームの名前 すべての内部ボリュームの名前

カテゴリ	インデックスキーワード
仮想マシン	「仮想マシン」 名前 DNS名 IP アドレス ホストの名前 ホストのIPアドレス すべてのデータストアの名前 関連付けられているすべてのアプリケーションの名前
スイッチ（標準と NPV ）	"スイッチ" IP アドレス WWN 名前 シリアル番号 モデル ドメインID ファブリックの名前 ファブリックのWWN
アプリケーション	"アプリケーション" 名前 テナント 基幹業務部門 ビジネスユニット プロジェクト
テープ	"テープ" IP アドレス 名前 シリアル番号 ベンダー
ポート	"ポート" WWN 名前
ファブリック	"ファブリック" WWN 名前
Storage Virtual Machine （ SVM ）	"ストレージ仮想マシン" 名前 UUID

レポート作成

Data Infrastructure Insightsレポートの概要

Data Infrastructure Insightsのレポート機能は、事前定義済みのレポートを表示したり、カスタムレポートを作成したりできるビジネスインテリジェンスツールです。

レポート機能はData Infrastructure Insightsで使用でき"Premium Edition の場合"ます。

Data Infrastructure Insightsのレポート作成機能では、次のタスクを実行できます。

- 事前定義済みのレポートを実行します
- カスタムレポートを作成する
- レポートの形式と配信方法をカスタマイズする
- レポートが自動的に実行されるようにスケジュールを設定する
- レポートを E メールで送信
- データのしきい値を色で表します

Data Infrastructure Insights Reportingでは、チャージバック、消費分析、予測などの領域に関するカスタムレポートを生成でき、次のような質問に対する回答に役立ちます。

- 所有しているインベントリ
- インベントリの場所
- アセットの使用者
- ビジネスユニットに割り当てられているストレージのチャージバック
- ストレージ容量の追加購入が必要になるまでの期間
- ビジネスユニットが適切なストレージ階層に配置されているか。
- 1 カ月、 1 四半期、 1 年のストレージ割り当ての変化

データインフラの分析情報レポートへのアクセス

Data Infrastructure Insights Reportingにアクセスするには、メニューの*[レポート]*リンクをクリックします。

Reporting インターフェイスに移動します。Data Infrastructure Insightsでは、レポートエンジンにIBM Cognos Analyticsを使用しています。

ETL とは

Reporting では、「 Data Warehouse 」と「 ETL 」という用語が使用されます。ETL は、「抽出、変換、読み込み」の略です。ETLプロセスでは、Data Infrastructure Insightsで収集されたデータが取得され、レポートで使用する形式に変換されます。「 Data Warehouse 」は、レポートに使用できる収集データを表します。

ETL プロセスは、次の個別プロセスで構成されます。

- * Extract *：Data Infrastructure Insightsからデータを取得
- 変換：Data Infrastructure Insightsから抽出されるデータにビジネスロジックのルールや機能を適用します。
- * ロード *: 変換されたデータをデータウェアハウスに保存して、レポート作成に使用します。

Data Infrastructure Insights Reportingのユーザロール

Data Infrastructure Insights Premium Edition with Reportingを使用している場合は、環境内のすべてのData Infrastructure Insightsユーザが、レポートアプリケーション（Cognosなど）へのシングルサインオン（SSO）ログインも利用できます。メニューの * Reports

* リンクをクリックすると、自動的に Reporting にログインします。

Reportingユーザのロールは、Data Infrastructure Insightsのユーザロールによって決まります。

Data Infrastructure Insightsロール	Reporting ロール	レポート権限
ゲスト	消費者	レポートの表示、スケジュール設定、実行、および言語やタイムゾーンなどの個人設定を行うことができます。消費者は、レポートの作成や管理タスクの実行はできません。
ユーザ	作成者	すべてのコンシューマ機能を実行できるだけでなく、レポートやダッシュボードの作成と管理も可能です。
管理者	管理者	作成者のすべての機能だけでなく、レポートの設定や、レポートタスクのシャットダウンと再起動などのすべての管理タスクも実行できます。

次の表は、各 Reporting ロールで使用できる機能を示しています。

フィーチャー（ Feature ）	消費者	作成者	管理者
[チームコンテンツ] タブでレポートを表示します	はい。	はい。	はい。
レポートを実行する	はい。	はい。	はい。
レポートのスケジュールを設定する	はい。	はい。	はい。
外部ファイルをアップロードします	いいえ	はい。	はい。
ジョブを作成します	いいえ	はい。	はい。
ストーリーを作成します	いいえ	はい。	はい。
レポートを作成します	いいえ	はい。	はい。
パッケージとデータモジュールを作成します	いいえ	はい。	はい。
管理タスクを実行	いいえ	いいえ	はい。
HTMLアイテムを追加/編集します	いいえ	いいえ	はい。
HTMLアイテムを使用してレポートを実行します	はい。	はい。	はい。
カスタムSQLを追加/編集します	いいえ	いいえ	はい。

カスタムSQLを使用してレポートを実行します	はい。	はい。	はい。

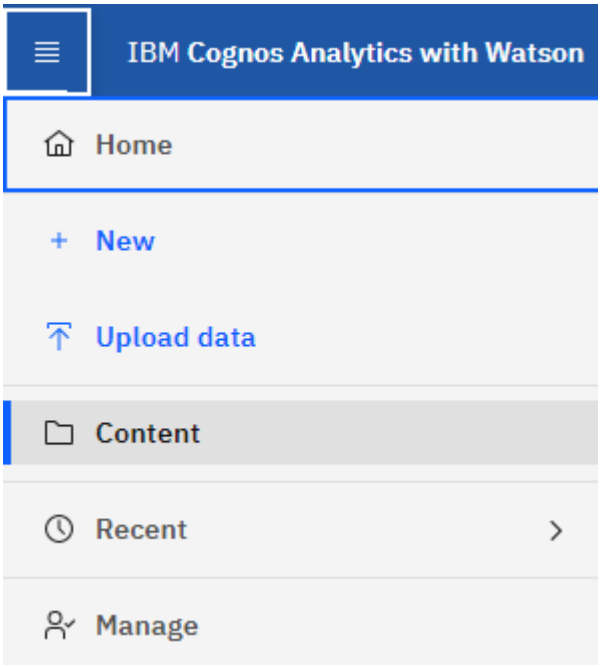
Reporting （ Cognos ） E メールの設定

Data Infrastructure Insights Reporting（Cognosアプリケーション）でユーザのEメール設定を変更した場合、それらの設定は現在のセッション_のACTIVE_ONLYになります。Cognos からログアウトして再度ログインすると、 E メールの設定がリセットされます。

SSO を有効にするために既存の環境を準備するには、どのような手順を実行する必要がありますか。

レポートを確実に保持するには、次の手順を使用して、 *My Content_to _Team Content* からすべてのレポートを移行します。この作業は、環境で SSO を有効にする前に行う必要があります。

1. [メニュー]>[コンテンツ]*に移動します



1. **Team Content**に新しいフォルダを作成します
   a. 複数のユーザーが作成されている場合は、重複した名前でレポートを上書きしないように、ユーザーごとに個別のフォルダを作成してください
2. マイコンテンツ _ に移動します
3. 保持するすべてのレポートを選択します。
4. メニューの右上隅で、 [コピーまたは移動] を選択します。
5. *Team Content* で新しく作成したフォルダに移動します
6. [コピー先] または [移動先] ボタンを使用して、新しく作成したフォルダにレポートを貼り付けます
7. CognosでSSOが有効になったら、アカウントの作成に使用したEメールアドレスでData Infrastructure Insightsにログインします。
8. Cognos 内の *Team Content_folder* に移動し、以前に保存したレポートを *_My Content* にコピーまたは移動します。

事前定義済みのレポートを簡単に作成

Data Infrastructure Insights Reportingには、レポート作成に関する一般的な要件に対処する事前定義済みのレポートが含まれており、関係者がストレージインフラに関する十分な情報に基づいて意思決定を下すために必要な重要な分析情報を提供します。

レポート機能はData Infrastructure Insightsで使用でき"Premium Edition の場合"ます。

Data Infrastructure Insights Reporting Portalから事前定義済みのレポートを生成したり、他のユーザにEメールで送信したり、変更したりできます。複数のレポートを使用して、デバイス、ビジネスエンティティ、または階層でフィルタリングできます。このレポートツールは、 IBM Cognos をベースとしたツールで、さまざまなデータ表示オプションが用意されています。

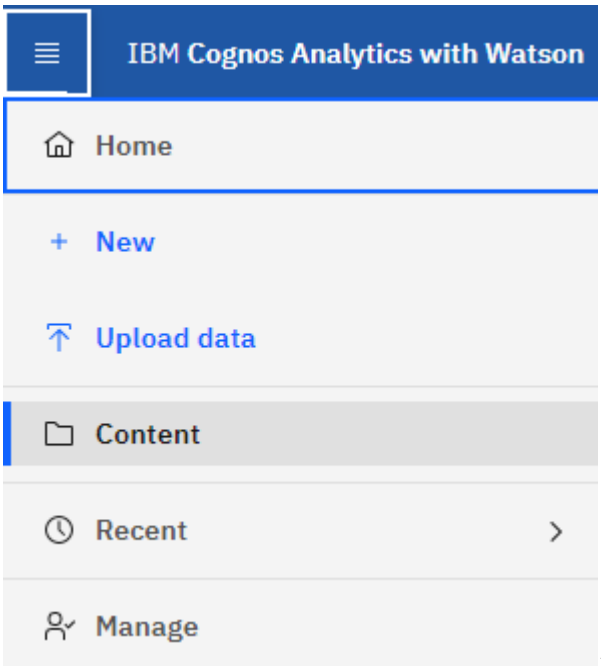
事前定義済みのレポートには、インベントリ、ストレージ容量、チャージバック、パフォーマンス、ストレージ効率、 クラウドコストのデータを活用できます。これらの事前定義済みレポートを変更して、変更内容を保存できます。

HTML 、 PDF 、 CSV 、 XML などのさまざまな形式でレポートを生成できます。 Excel などです。

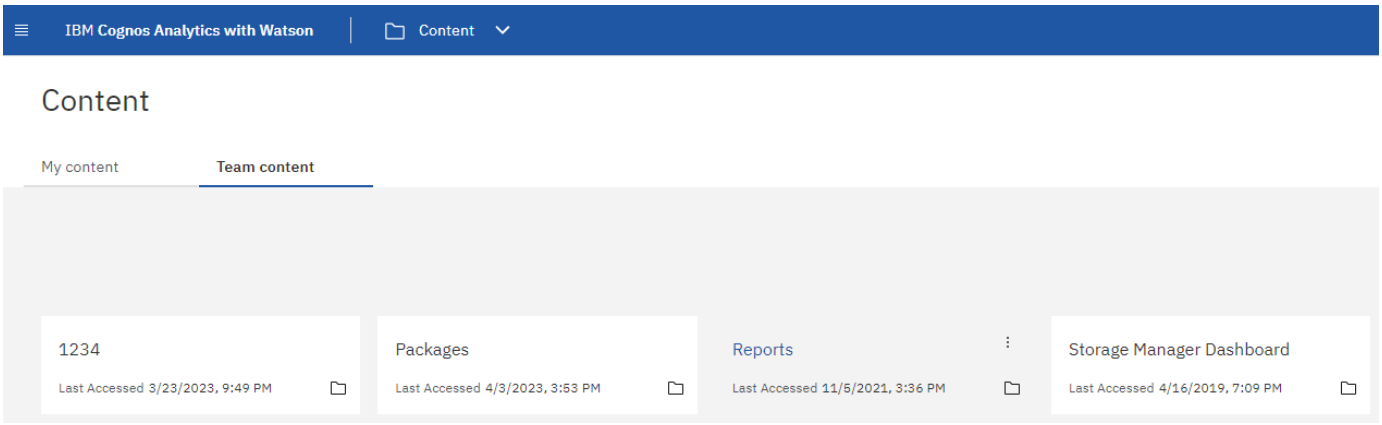
事前定義済みレポートに移動します

Reportingポータルを開くと、Data Infrastructure Insightsのレポートに必要な情報のタイプを選択するための出発点として_Team Content_フォルダが使用されます。

1. 左側のナビゲーションペインで、*コンテンツ>チームコンテンツ*を選択します。
2. 事前定義済みのレポートにアクセスするには、*[レポート]*を選択します。



メニュー"]



事前定義済みのレポートを使用した回答に関する一般的な質問への

次の事前定義済みレポートは、 * チームコンテンツ > レポート * で使用できます。

アプリケーションサービスレベルの容量とパフォーマンス

Application Service Level Capacity and Performance レポートには、アプリケーションの概要が表示されます。この情報は、キャパシティプランニングや移行計画に使用できます。

チャージバック

Chargeback レポートには、ストレージ容量のチャージバックとアカウンタビリティの情報がホスト、アプリケーション、およびビジネスエンティティ別に表示され、現在のデータと履歴データの両方が含まれます。

データが二重に収集されないようにするために、 ESX サーバを対象から除外し、 VM のみを監視してください。

データソース

Data Sources レポートには、サイトにインストールされているすべてのデータソース、データソースのステータス（ success / failure ）、およびステータスメッセージが表示されます。このレポートには、データソースのどこで問題が発生したかに関する情報が記載されていますデータソースが正常に機能しないと、レポートの精度と製品の可用性全般が低下します。

ESX と **VM** のパフォーマンス

ESX と VM のパフォーマンス比較レポートには、 ESX サーバと VM の平均および最大の IOPS 、スループット、レイテンシ、利用率が表示されます。データが二重に収集されないようにするために、 ESX サーバを対象から除外し、 VM のみを監視してください。
このレポートの最新版は、 NetApp Storage Automation Store から入手できます。

ファブリックの概要

Fabric Summary レポートには、ポート数、ファームウェアバージョン、ライセンスステータスなど、スイッチとスイッチの情報が表示されます。このレポートには NPV スイッチポートは含まれません。

ホストの **HBA**

Host HBAs レポートには、環境内のホストの概要と、 HBA のベンダー、モデル、ファームウェアバージョン、および HBA が接続されているスイッチのファームウェアレベルが表示されます。このレポートを使用し

て、スイッチまたは HBA のファームウェアのアップグレードを計画する際にファームウェアの互換性を分析できます。

ホストのサービスレベルの容量とパフォーマンス

Host Service Level Capacity and Performance レポートには、ブロック専用アプリケーションのホスト別のストレージ利用率の概要が表示されます。

ホストサマリ

Host Summary レポートには、選択した各ホストのストレージ利用率の概要と、 Fibre Channel ホストおよび iSCSI ホストの情報が表示されます。このレポートを使用して、ポートとパス、 Fibre Channel と iSCSI の容量、および違反数を比較できます。

ライセンスの詳細

License Details レポートには、すべてのサイトで、ライセンスが付与されているリソースの数が表示されます。このレポートには、すべてのサイトでの実際のライセンス数の合計も表示されます。この合計には、複数のサーバで管理されるストレージアレイが重複してカウントされることがあります。

マップ済みだがマスクされていないボリューム

Mapped but not Masked Volumes レポートには、 LUN は特定のホストにマッピングされているが、そのホストに対してマスクされていないボリュームが表示されます。このようなボリュームは、マスクが解除された、運用を終了した LUN である可能性があります。マスクされていないボリュームにはどのホストからもアクセスできるため、データが破損しやすくなります。

ネットアップの容量とパフォーマンス

NetApp Capacity and Performance レポートには、割り当て済み容量、使用済み容量、コミット済み容量のグローバルデータ、および容量のトレンドとパフォーマンスデータが表示されます。

スコアカード

スコアカードレポートには、Data Infrastructure Insightsで取得したすべての資産の概要と全般的なステータスが表示されます。ステータスは、緑色、黄色、赤色のフラグで示されます。

- 緑は正常な状態を示します
- 黄色は、環境内に潜在的な問題があることを示します
- 赤は、注意が必要な問題を示します

レポート内のすべてのフィールドの説明は、レポートに付属のデータディクショナリに記載されています。

ストレージサマリ

Storage Summary レポートには、 raw 、割り当て済み、ストレージプール、およびボリュームについて、使用済み容量と未使用の容量のデータの概要が表示されます。このレポートは、検出されたすべてのストレージの概要を示します。

VM の容量とパフォーマンス

仮想マシン（ VM ）環境とその使用容量が表示されます。VM の電源がオフになっている場合など、一部のデ

ータを表示するには、 VM ツールを有効にする必要があります。

VM パス

VM Paths レポートは、仮想マシンが実行されているホスト、どのホストがどの共有ボリュームにアクセスしているか、アクティブなアクセスパスが何であるか、および容量の割り当てと使用量がどのようなものであるかについて、データストアの容量データとパフォーマンスの指標を提供します。

HDS 容量（シンプール別）

HDS Capacity by Thin Pool レポートには、シンプロビジョニングされたストレージプールで使用可能な容量が表示されます。

ネットアップ容量 - アグリゲート別

NetApp Capacity by Aggregate レポートには、アグリゲートの合計 raw スペース、合計スペース、使用済みスペース、使用可能なスペース、およびコミット済みスペースが表示されます。

シックアレイ別の Symmetrix 容量

Symmetrix Capacity by Thick Array レポートには、 raw 容量、使用可能な容量、空き容量、マッピングされた容量、マスクされた容量が表示されます。 合計空き容量を確認します。

シン・プール別の Symmetrix 容量

Symmetrix Capacity by Thin Pool レポートには、 raw 容量、使用可能な容量、使用済み容量、空き容量、使用済みの割合が表示されます。 サブスクライブ済み容量およびサブスクリプション率：

アレイ別の XIV 容量

XIV Capacity by Array レポートには、アレイの使用済み容量と未使用の容量が表示されます。

XIV Capacity by Pool の対比を表示します

XIV Capacity by Pool レポートには、ストレージプールの使用済み容量と未使用の容量が表示されます。

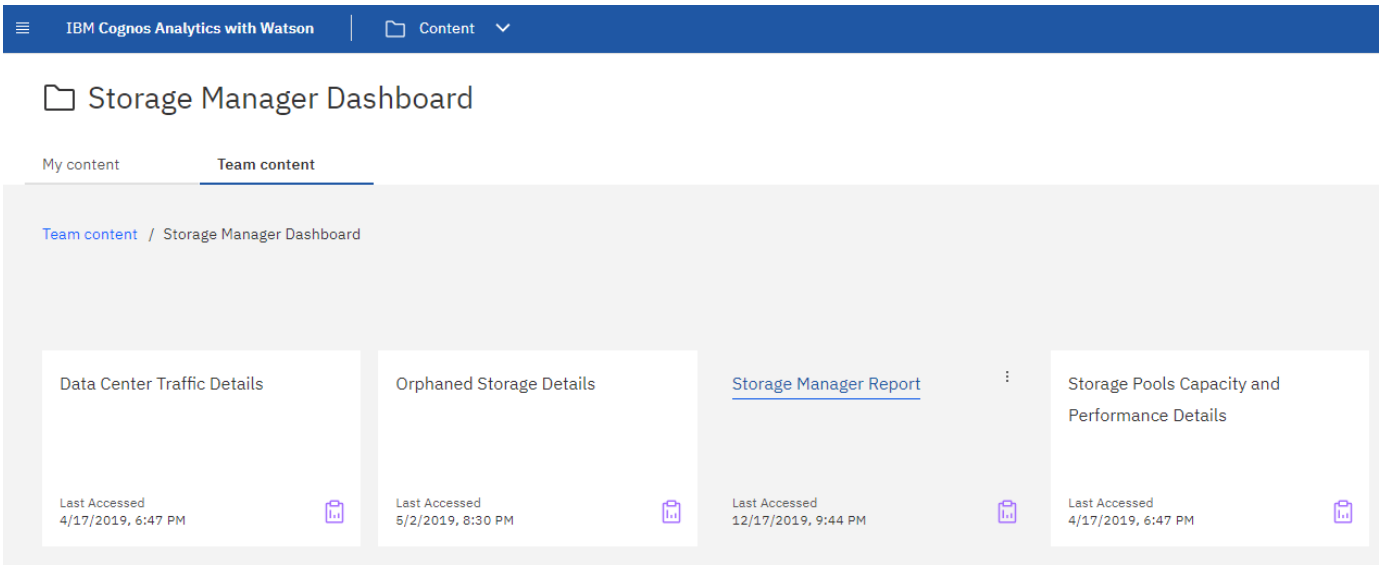
Storage Manager のダッシュボード

Storage Manager Dashboard では、一定期間のリソース使用量をまとめて表示し、許容範囲および過去何日間かのアクティビティと比較することができます。ストレージサービスの主要なパフォーマンス指標だけが表示されるため、データセンターの管理方法についての決定を下すことができます。

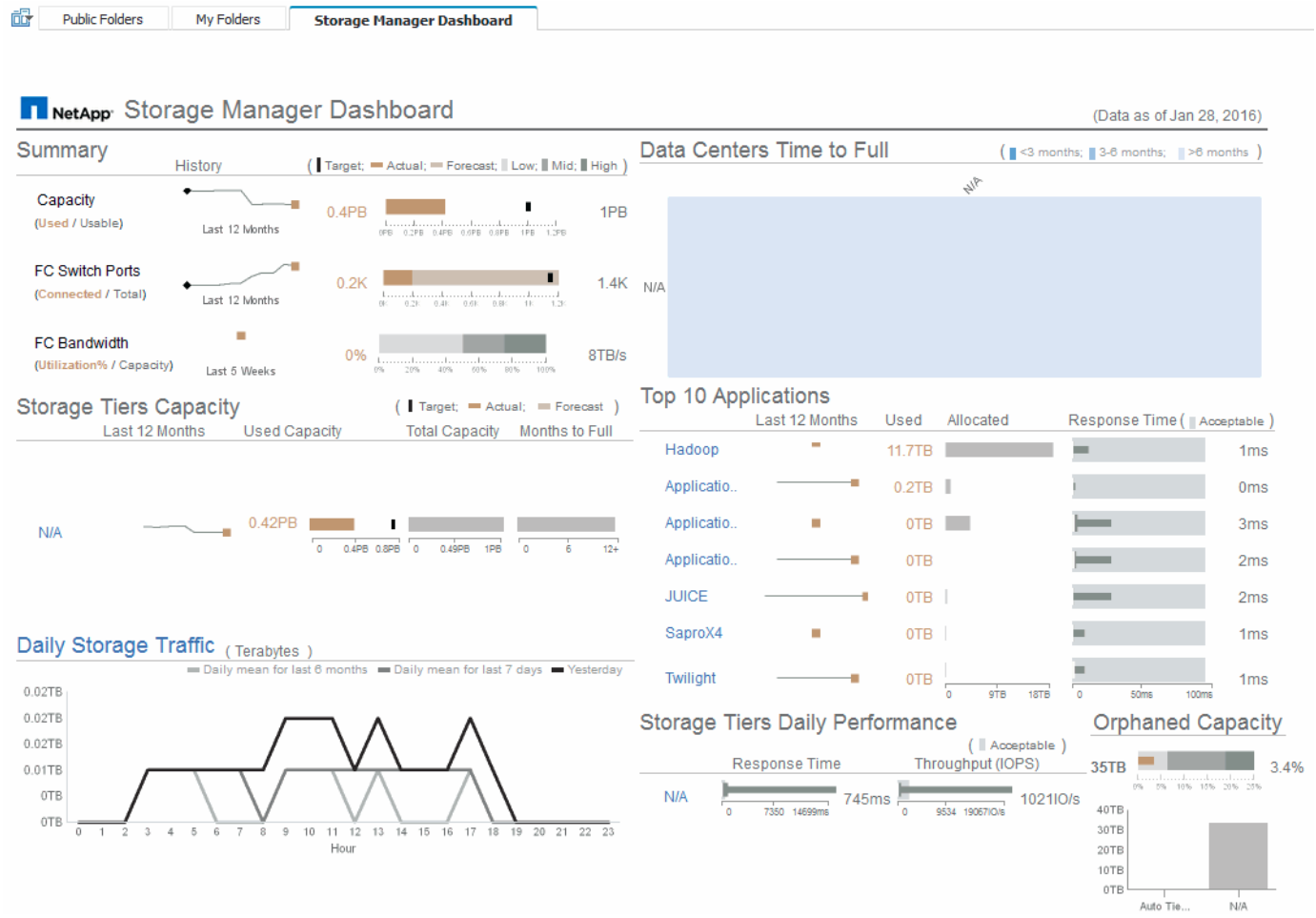
レポート機能はData Infrastructure Insightsで使用でき"Premium Edition の場合"ます。

まとめ

チームコンテンツから* Storage Manager Dashboard *を選択すると、トラフィックとストレージに関する情報を提供する複数のレポートが表示されます。



Storage Manager Report *は、ストレージ環境のさまざまな側面に関するコンテキスト情報を含む7つのコンポーネントで構成されています。ストレージサービスの要素をドリルダウンして、最も関心のあるセクションについて詳細な分析を実施できます。



このコンポーネントには、使用済みのストレージ容量と使用可能なストレージ容量、スイッチポートの総数と接続されているスイッチポートの数、接続されているスイッチポートの合計利用率と総帯域幅、および一定期間にわたるこれらのトレンドが表示されます。実際の使用率を低、中、高の範囲と比較して表示でき、予測と実際の使用量をターゲットに基づいて比較できます。容量とスイッチポートについては、このターゲットを設

定できます。予測は、現在の増加率と設定した日付による外挿によって算出されます。将来使用日に基づいて予測された使用済み容量がターゲットを超えると、容量の横にアラート（赤い丸）が表示されます。

ストレージ階層容量

このコンポーネントには、使用済みの階層容量と階層に割り当てられた容量が表示され、 12 カ月間での使用済み容量の増減と容量の上限に到達するまでの月数が表示されます。容量の使用状況は、実際の使用量に対して提供された値、使用量予測、および容量のターゲットとともに表示されます。これらの値を設定できます。将来使用日に基づいて予測された使用済み容量がターゲットを超えると、階層の横にアラート（赤い丸）が表示されます。

いずれかの階層をクリックすると、 Storage Pools Capacity and Performance Details レポートを表示できます。このレポートには、空き容量と使用済み容量、上限に到達するまでの日数、および選択した階層内のすべてのプールのパフォーマンス（ IOPS と応答時間）の詳細が表示されます。また、このレポート内のいずれかのストレージまたはストレージプール名をクリックすると、リソースの現在の状態をまとめたアセットページを表示できます。

日次ストレージトラフィック

このコンポーネントには、環境のパフォーマンス、増加率、変更率、潜在的な問題が過去 6 カ月間と比較してどのように発生しているかが表示されます。また、平均トラフィックと過去 7 日間および前日のトラフィックの比較も表示されます。周期的（過去 7 日間）な変化と季節的（過去 6 カ月間）な変化の両方を示す情報が提供されるため、インフラのパフォーマンスについての異常を可視化できます。

タイトル（ Daily Storage Traffic ）をクリックすると、 Storage Traffic Details レポートを表示できます。このレポートには、各ストレージシステムについて、前日のストレージトラフィックの 1 時間ごとのヒートマップが表示されます。レポート内のいずれかのストレージ名をクリックすると、リソースの現在の状態をまとめたアセットページが表示されます。

データセンターがフルになるまでの時間

このコンポーネントには、すべてのデータセンターとすべての階層が表示され、が予測した増加率に基づいて、各データセンターにどのくらいの容量が残っているかがストレージの階層ごとに表示されます。階層の容量レベルは青で表示され、色が暗くなるほど、その場所の階層が上限に到達するまでの時間が少なくなります。

階層のセクションをクリックすると、 Storage Pools Days to Full Details レポートを表示できます。このレポートには、合計容量、空き容量、選択した階層とデータセンター内のすべてのプールが上限に到達するまでの日数が表示されます。レポート内のいずれかのストレージまたはストレージプール名をクリックすると、リソースの現在の状態をまとめたアセットページが表示されます。

上位 **10** 個のアプリケーション

このコンポーネントには、使用済み容量に基づく上位 10 個のアプリケーションが表示されます。この領域には、階層によるデータの割り当てに関係なく、インフラの現在の使用済み容量と共有状況が表示されます。過去 7 日間のユーザエクスペリエンスを可視化して、応答時間が許容可能な（または許容できない）範囲にあるかどうかを確認できます。

また、アプリケーションがパフォーマンスのサービスレベル目標（ SLO ）を満たしているかどうかを示すトレンドも表示されます。前週の最小応答時間、最初の四分位数、 3 番目の四分位数、および最大応答時間を表示できます。中央値は、許容可能な SLO に対して表示され、設定可能です。応答時間の中央値が許容可能な SLO 範囲に含まれていない場合は、アプリケーションの横にアラート（赤い丸）が表示されます。アプリケーションをクリックすると、リソースの現在の状態をまとめたアセットページを表示できます。

ストレージ階層の日次パフォーマンス

このコンポーネントには、過去 7 日間の応答時間と IOPS についての階層のパフォーマンスの概要が表示されます。このパフォーマンスは、ユーザが設定可能な SLO と比較したものです。これにより、階層の統合、階層から提供されるワークロードの再調整、または特定の階層に関する問題の特定の機会があるかどうかを確認できます。応答時間の中央値または IOPS の中央値が許容可能な SLO 範囲に含まれていない場合は、階層の横にアラート（赤い丸）が表示されます。

階層名をクリックすると、 Storage Pools Capacity and Performance Details レポートを表示できます。このレポートには、空き容量と使用済み容量、上限に到達するまでの日数、および選択した階層内のすべてのプールのパフォーマンス（ IOPS と応答時間）の詳細が表示されます。レポート内のいずれかのストレージまたはストレージプールをクリックすると、リソースの現在の状態をまとめたアセットページが表示されます。

孤立容量

このコンポーネントには、孤立容量の合計と階層別の孤立容量が表示されます。使用可能な総容量の許容範囲と比較され、孤立している実際の容量が表示されます。孤立容量には、設定に起因するものとパフォーマンスに起因するものがあります。設定に起因する孤立ストレージは、ホストにストレージが割り当てられている場合に該当します。ただし、設定が正しく実行されていないため、ホストはストレージにアクセスできません。パフォーマンスに起因する孤立ストレージは、ホストがアクセスするようにストレージが正しく設定されている場合に該当します。ただし、ストレージトラフィックが発生していません。

水平の積み上げ棒は許容範囲を示します。グレーの色が暗くなるほど、許容できない状況になります。実際の状況は、孤立している実際の容量を示す細いブロンズバーとともに表示されます。

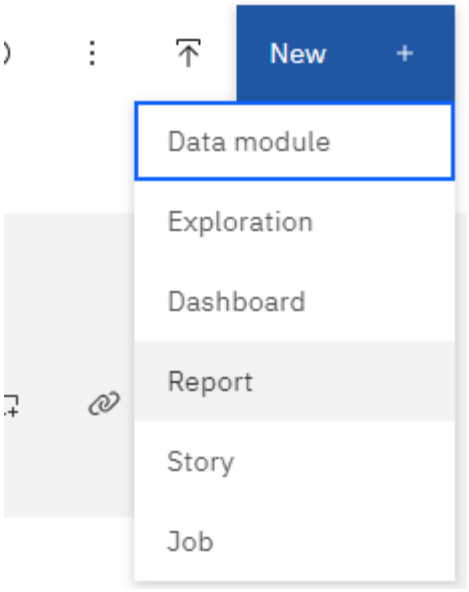
階層をクリックすると、 Orphaned Storage Details レポートを表示できます。このレポートには、選択した階層について、設定およびパフォーマンスが原因で孤立していると特定されたすべてのボリュームが表示されます。このレポート内のいずれかのストレージ、ストレージプール、またはボリュームをクリックすると、リソースの現在の状態をまとめたアセットページが表示されます。

レポートの作成（例）

この例の手順を使用して、複数のデータセンター内のストレージプールとストレージプールの物理容量に関するシンプルなレポートを生成します。

手順

1. [メニュー]>[コンテンツ]>[チームコンテンツ]>[レポート]*に移動します
2. 画面の右上で、*[新規+]*を選択します
3. [レポート]*を選択します



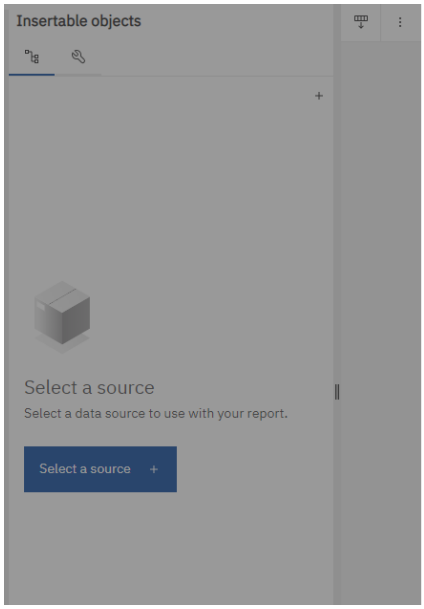
4. [Templates]タブで、[*blank*]を選択します

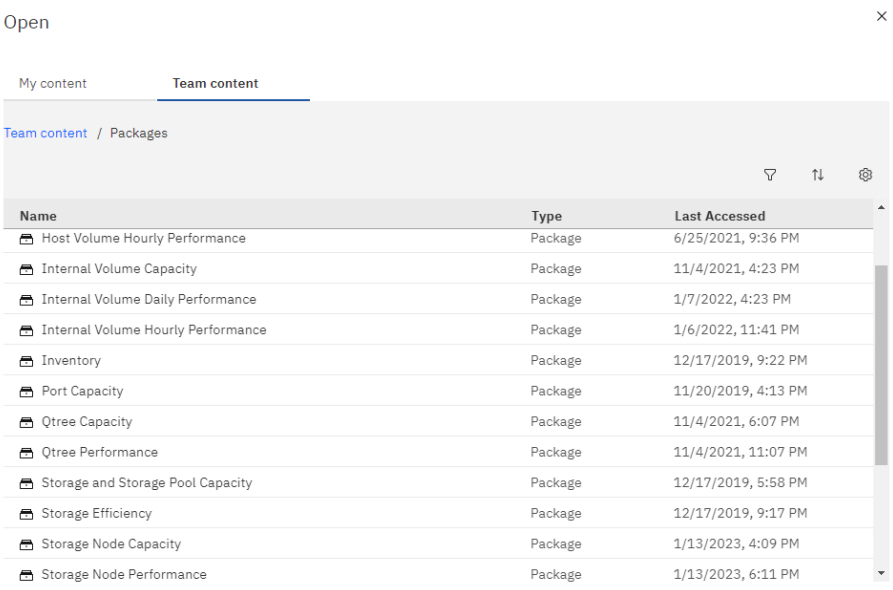
   [ソース] タブと [データ] タブが表示されます

5. 開く*ソースを選択+*
6. チームコンテンツ*で、*パッケージ*を開きます

   利用可能なパッケージのリストが表示されます。

7. [ストレージとストレージプールの容量]*を選択します





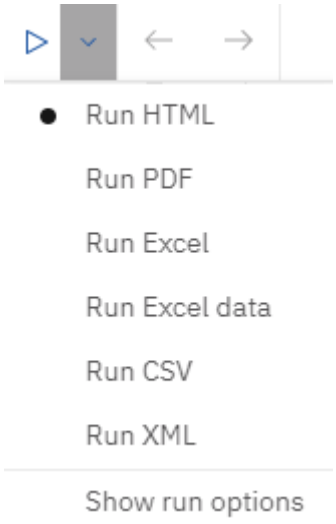
8. [開く]*を選択します

   レポートで使用できるスタイルが表示されます。

9. [リスト]*を選択します

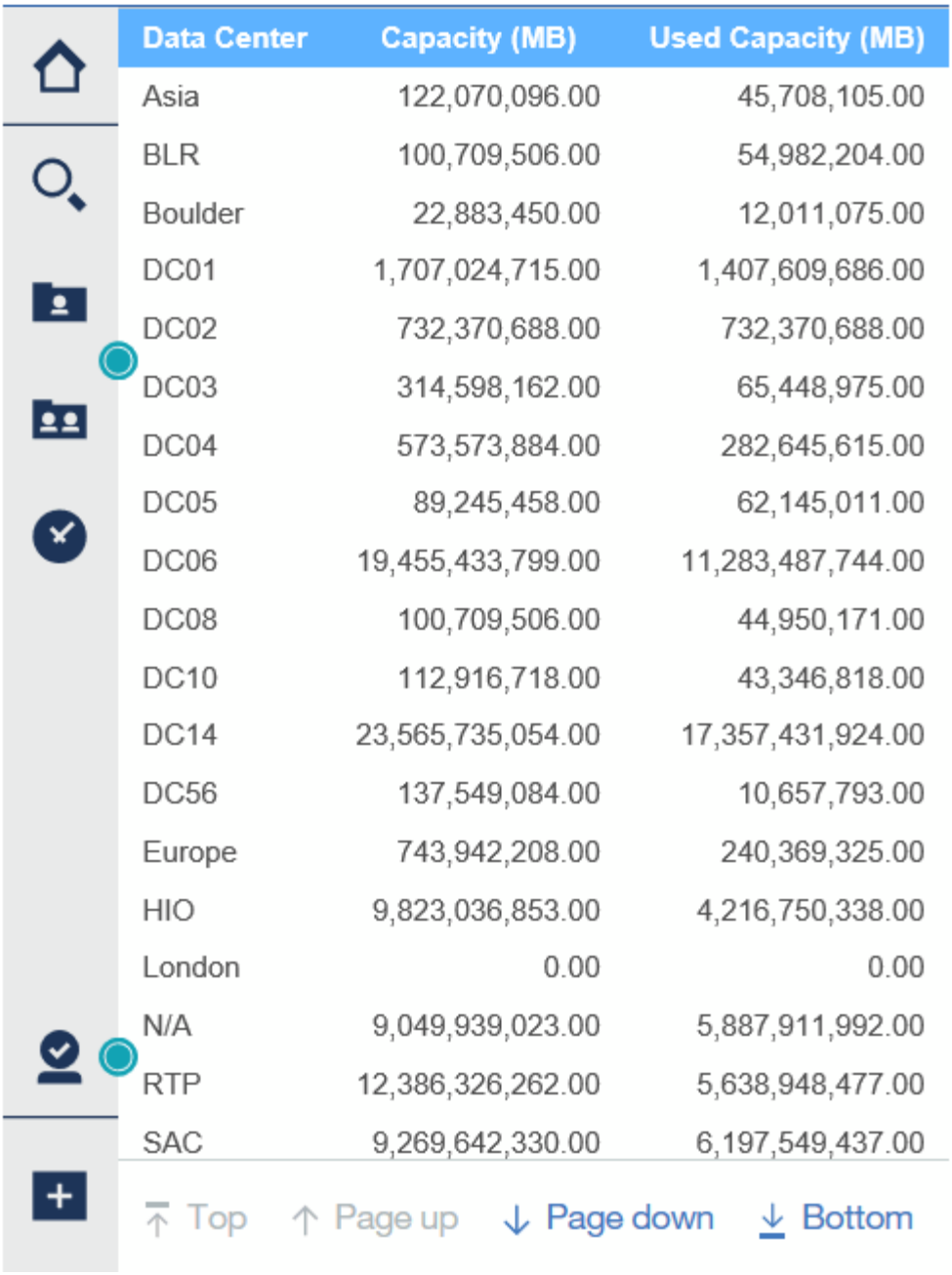
   リストとクエリに適切な名前を追加します

10. 「 * OK 」を選択します
11. 物理容量 _ を展開します
12. データセンターを最も低いレベルに拡張します
13. レポート口蓋に *Data Center* をドラッグします。
14. を展開します
15. レポート口蓋に _Capacity （ MB ） _ をドラッグします。
16. 使用容量（ MB ） _ をレポート口蓋にドラッグします。
17. [実行]メニューから出力タイプを選択して、レポートを実行します。



結果

次のようなレポートが作成されます。



Data Center	Capacity (MB)	Used Capacity (MB)
Asia	122,070,096.00	45,708,105.00
BLR	100,709,506.00	54,982,204.00
Boulder	22,883,450.00	12,011,075.00
DC01	1,707,024,715.00	1,407,609,686.00
DC02	732,370,688.00	732,370,688.00
DC03	314,598,162.00	65,448,975.00
DC04	573,573,884.00	282,645,615.00
DC05	89,245,458.00	62,145,011.00
DC06	19,455,433,799.00	11,283,487,744.00
DC08	100,709,506.00	44,950,171.00
DC10	112,916,718.00	43,346,818.00
DC14	23,565,735,054.00	17,357,431,924.00
DC56	137,549,084.00	10,657,793.00
Europe	743,942,208.00	240,369,325.00
HIO	9,823,036,853.00	4,216,750,338.00
London	0.00	0.00
N/A	9,049,939,023.00	5,887,911,992.00
RTP	12,386,326,262.00	5,638,948,477.00
SAC	9,269,642,330.00	6,197,549,437.00

レポートの管理

レポートの出力形式と配信のカスタマイズ、レポートのプロパティまたはスケジュールの設定、およびレポートの電子メール送信を行うことができます。

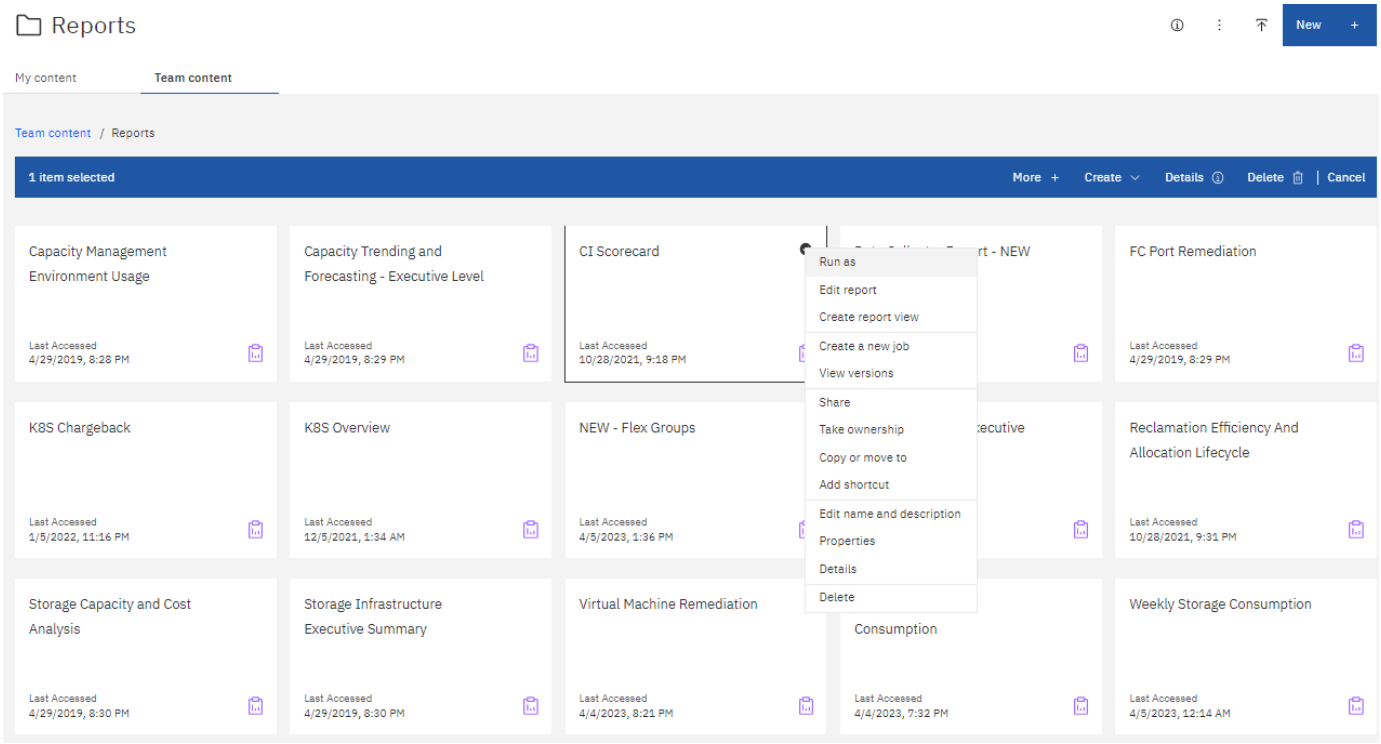
レポート機能はData Infrastructure Insightsで使用でき"Premium Edition の場合"ます。

レポートの出力形式と配信方法のカスタマイズ

レポートの形式と配信方法をカスタマイズできます。

1. Data Infrastructure Insights Reportingポータルで、*[メニュー]>[コンテンツ]>[マイコンテンツ/チームコンテンツ]*に移動します。カスタマイズするレポートの上にマウスを置き、「3つのドット」メニューを開き

ます。

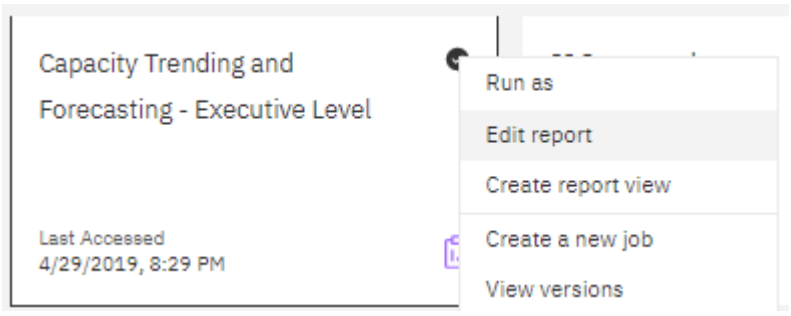


1. [プロパティ] 、 [スケジュール] の順にクリックします
2. 次のオプションを設定できます。
   - レポートを実行するスケジュール。
   - レポートの形式と配信（保存、印刷、電子メール）、およびレポートの言語には*オプション*を選択します。
3. [保存]*をクリックして、選択した内容を使用してレポートを作成します。

レポートをクリップボードにコピーしています

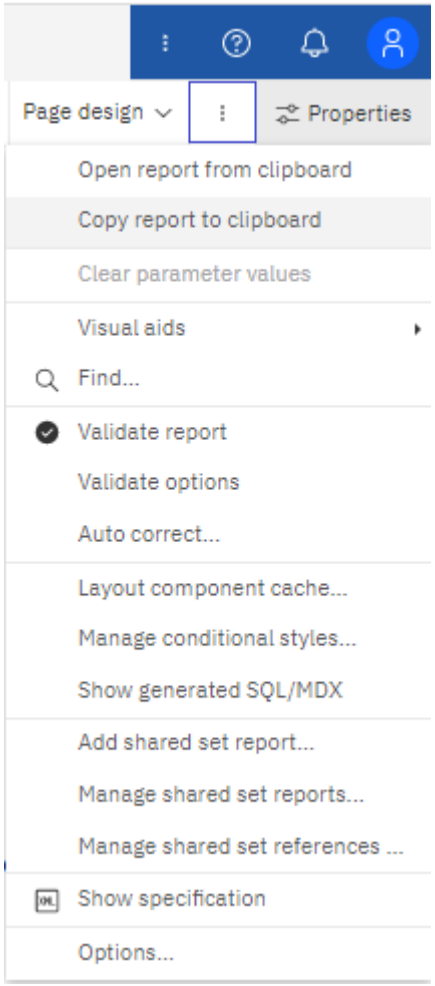
レポートをクリップボードにコピーするには、次の手順を実行します。

1. コピー元のレポートを選択します（*[メニュー]>[コンテンツ]>[マイコンテンツ]または[チームコンテンツ]）。
2. レポートのドロップダウンメニューから[*Edit report*]を選択します



3. 画面の右上にある「プロパティ」の横にある「3つのドット」メニューを開きます。

4. [レポートをクリップボードにコピー]*を選択します。

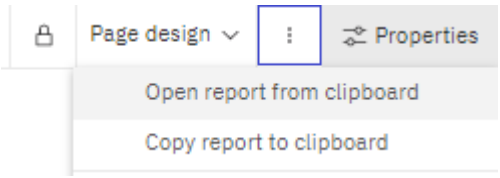


クリップボードからレポートを開く

以前クリップボードにコピーされたレポート仕様を開くことができます。

このタスクについて
最初に、新しいレポートを作成するか、コピーしたレポートで置き換える既存のレポートを開きます。新しいレポートの手順は次のとおりです。

1. [メニュー]>[+新規]>[レポート]*を選択し、空白のレポートを作成します。
2. 画面の右上にある「プロパティ」の横にある「3つのドット」メニューを開きます。
3. [クリップボードからレポートを開く]*を選択します。



1. コピーしたコードをウィンドウに貼り付け、* OK *を選択します。
2. フロッピーディスクのアイコンを選択して、レポートを保存します。

3. レポートの保存場所（*My Content*、*Team Content*、または新しいフォルダを作成）を選択します。
4. 新しいレポートにわかりやすい名前を付け、*[保存]*を選択します。

既存のレポートの編集

デフォルトの場所にあるファイルを編集すると、次回のレポートカタログの更新時にレポートが上書きされるリスクがあることに注意してください。編集したレポートは新しい名前で保存するか、デフォルト以外の場所に保存することをお勧めします。

トラブルシューティング

ここでは、レポートに関する問題のトラブルシューティング方法を示します。

* 問題： *	* これを試みなさい : *
レポートを E メールで送信するようにスケジュール設定すると、ログインしているユーザの名前が E メールの「宛先」フィールドに事前に入力されます。ただし、名前は「 firstname lastname 」（名、スペース、姓）の形式になっています。これは有効な E メールアドレスではないため、スケジュールされたレポートの実行時に E メールを送信できません。	レポートを E メールで送信するようにスケジュールする場合は、事前に入力された名前をクリアし、正しい形式で正しい形式の有効な E メールアドレスを [宛先] フィールドに入力します。

カスタムレポートの作成

レポートオーサリングツールを使用してカスタムレポートを作成できます。作成したレポートは、保存して定期的に実行できます。レポートの結果は、自分や他のユーザに E メールで自動送信できます。

レポート機能はData Infrastructure Insightsで使用でき"Premium Edition の場合"ます。

このセクションの例では、次のプロセスを示します。これらのプロセスは、Data Infrastructure Insights Reportingデータモデルで使用できます。

- レポートで回答する質問を特定しています
- 結果をサポートするために必要なデータを決定する
- レポートのデータ要素を選択しています

カスタムレポートを設計する前に、いくつかの前提条件となるタスクを完了しておく必要があります。これらの作業を完了しないと、不正確または不完全なレポートが生成される可能性があります。

たとえば、デバイスの識別プロセスを完了していないと、正確な容量レポートが生成されません。また、アノテーション（階層、ビジネスユニット、データセンターなど）の設定が完了していないと、ドメイン全体でデータが正確にレポートされなかったり、一部のデータに「 N/A 」と表示されたりする可能性があります。

レポートを設計する前に、次の作業を完了してください。

- すべてを設定します "データコレクタ" 適切です。
- 環境内のデバイスとリソースにアノテーション（階層、データセンター、ビジネスユニットなど）を入力

します。Data Infrastructure Insights Reportingでは履歴情報が収集されるため、レポートを生成する前にアノテーションを安定させておくと便利です。

レポート作成プロセス

カスタム（「アドホック」とも呼ばれる）レポートを作成するプロセスには、いくつかのタスクが含まれます。

- レポートの結果を計画します。
- 結果をサポートするデータを特定します。
- データが格納されているデータモデル（ Chargeback データモデル、 Inventory データモデルなど）を選択します。
- レポートのデータ要素を選択します。
- 必要に応じて、レポート結果の書式設定、並べ替え、フィルタリングを行います。

カスタムレポートの結果を計画する

レポートオーサリングツールを開く前に、必要な結果についてレポートで計画することができます。レポートオーサリングツールでは、レポートを簡単に作成でき、詳細な計画は必要ないかもしれませんが、レポートを必用としている担当者にレポートの要件について確認しておくことを推奨します。

- 回答の正確な質問を特定します。例：
  - 残りの容量
  - ビジネスユニットあたりのチャージバックコスト
  - 階層別の容量 - 各ビジネスユニットが適切なストレージ階層に配置されているか
  - 必要な電力と冷却コストを予測するにはどうすればよいですか。（リソースにアノテーションを追加することで、カスタマイズしたメタデータを追加）
- 回答をサポートするために必要なデータ要素を特定します。
- 回答に表示するデータ間の関係を特定します。「容量に関連するポートを表示したい」など、問題に論理的でない関係を含めないでください。
- データに必要な計算があれば特定します。
- 結果を制限するために必要なフィルタリングのタイプを決定します。
- 現在のデータまたは履歴データのどちらを使用する必要があるかを判断します。
- レポートにアクセス権を設定してデータの閲覧を特定のユーザに制限する必要があるかどうかを判断します。
- レポートの配布方法を特定します。たとえば、設定されたスケジュールで電子メールで送信するか、チームコンテンツフォルダ領域に含める必要がありますか？
- レポートの管理者を決定します。これは、設計の複雑さに影響する可能性があります。
- レポートのモックアップを作成します。

レポートの設計に関するヒント

レポートを設計するときは、いくつかのヒントが役立つことがあります。

- 現在のデータと履歴データのどちらを使用する必要があるかを判断します。

  ほとんどのレポートでは、Data Infrastructure Insightsで利用可能な最新データに関するレポートのみを作成する必要があります。

- Data Infrastructure Insights Reportingでは、容量とパフォーマンスに関する履歴情報は提供されますが、インベントリに関する情報は提供されません。
- すべてのユーザにすべてのデータが表示されますが、データを特定のユーザに制限しなければならない場合もあります。

  ユーザごとに情報を分割するには、レポートを作成し、レポートにアクセス権限を設定します。

レポートデータモデル

Data Infrastructure Insightsには複数のデータモデルが含まれており、事前定義されたレポートを選択することも、独自のカスタムレポートを作成することもできます。

各データモデルにはシンプルなデータマートと高度なデータマートが含まれています。

- シンプルなデータマートを使用すると、最もよく使用されるデータ要素に簡単にアクセスできます。このデータマートには、 Data Warehouse データの最新の Snapshot だけが含まれており、履歴データは含まれていません。
- 高度なデータマートは、シンプルなデータマートに含まれるすべての値と詳細を提供し、履歴データ値へのアクセスを含みます。

Capacityデータモデル

ストレージ容量、ファイルシステム利用率、内部ボリュームの容量、ポート容量、 qtree 容量に関する回答の情報を表示します。 仮想マシン（ VM ）の容量が必要です。Capacity データモデルは、複数の容量データモデルをまとめたコンテナです。このデータモデルを使用して、さまざまなタイプの情報を収集したレポートを作成できます。

Storage and Storage Pool Capacity データモデル

ストレージとストレージプール、および物理ストレージプールと仮想ストレージプールの両方のデータについて、ストレージ容量のリソース計画に関する回答の情報を確認できます。このシンプルなデータモデルを使用すると、フロアの容量に関連する回答の質問や、一定期間にわたる階層別およびデータセンター別のストレージプールの使用容量に関する情報を確認できます。
容量に関するレポートを初めて作成する場合は、シンプルでターゲットが限定されたこのデータモデルを使用してください。このデータモデルを使用すると、次のような回答の情報を確認できます。

- 物理ストレージの容量しきい値の 80% に達するまでの予測日
- 特定の階層のアレイ上の物理ストレージ容量
- メーカー、ファミリー、およびデータセンター別のストレージ容量
- すべての階層のアレイにおけるストレージ利用率のトレンド
- 利用率が最も高い上位 10 個のストレージシステム
- ストレージプールのストレージ利用率のトレンド
- 割り当て済みの容量

- 割り当て可能な容量

File System Utilization データモデル

このデータモデルを使用すると、ファイルシステムレベルでホスト別の容量利用率を確認できます。管理者は、ファイルシステムごとの割り当て済み容量と使用済み容量、およびファイルシステムタイプを確認したり、ファイルシステムタイプ別のトレンドを特定したりできます。このデータモデルを使用すると、次の情報を回答で確認できます。

- ファイルシステムのサイズ
- データはどこに保管され、どのようにアクセスされるか（ローカル、 SAN など）。
- ファイルシステム容量の過去の傾向は何ですか。そして、これに基づいて、将来のニーズにどのような対応を期待できますか？

Internal Volume Capacity データモデル

一定期間にわたる内部ボリュームの使用済み容量、割り当て済みの容量、および使用容量に関する回答の情報を確認できます。

- 利用率が事前に定義されたしきい値を上回っている内部ボリューム
- トレンドに基づいて容量が不足する危険がある内部ボリュームはどれですか？
  8 内部ボリュームの使用済み容量と割り当て済み容量の比較

Port Capacity データモデル

一定期間にわたるスイッチポートの接続、ポートのステータス、およびポートの速度に関する回答の情報を確認できます。次のような回答 の質問は、新しいスイッチの購入を計画するのに役立ちます。
（データセンター、スイッチベンダー、ポート速度に応じて）リソース（ポート）の可用性を予測するポート消費予測を作成するには、どうすればよいですか。

- 容量不足になり、データ速度、データセンター、ベンダー、ホストポートとストレージポートの数が提供される可能性があるポートはどれですか？
- 一定期間にわたるスイッチポートの容量のトレンド
- ポートの速度
- 必要なポート容量のタイプ、および特定のポートタイプまたはベンダーで容量が不足しそうな組織
- いつまでに容量を購入して利用可能にするべきか

Qtree Capacity データモデル

一定期間にわたる qtree 利用率のトレンドを（使用済み容量と割り当て済み容量の比較などのデータを使用して）確認できます。ビジネスエンティティ、アプリケーション、階層、サービスレベルなど、さまざまなディメンション別に情報を表示できます。このデータモデルを使用すると、次の情報を回答で確認できます。

- アプリケーションまたはビジネスエンティティごとに設定されている制限値に対する qtree の使用済み容量
- キャパシティプランニングを実施するための使用済み容量と空き容量のトレンド
- 使用容量が最も多いビジネスエンティティ

- 使用容量が最も多いアプリケーション

VM Capacity データモデル

仮想環境とその使用容量を報告できます。このデータモデルを使用すると、 VM とデータストアの一定期間にわたる使用容量の変化を報告できます。このデータモデルは、シンプロビジョニングと仮想マシンのチャージバックデータも提供します。

- VM とデータストアにプロビジョニングされた容量に基づいて容量のチャージバックを決定する方法
- VM で使用されていない容量、およびそのうちの空き容量、孤立している容量、その他の状態の容量
- 消費傾向に基づいて何を購入する必要がありますか？
- ストレージのシンプロビジョニングと重複排除のテクノロジを使用することで達成される Storage Efficiency による削減効果

VM Capacity データモデルの容量は、仮想ディスク（ VMDK ）から取得されます。つまり、 VM Capacity データモデルを使用した場合の VM のプロビジョニング済みサイズは、その VM の仮想ディスクのサイズです。これは、Data Infrastructure Insightsの[Virtual Machines]ビューに表示されるプロビジョニング済み容量とは異なります。この容量には、VM自体のプロビジョニング済みサイズが表示されます。

Volume Capacity データモデル

環境内のボリュームのすべての要素を分析し、ベンダー、モデル、階層、サービスレベル、およびデータセンター別にデータを整理できます。

孤立ボリューム、未使用ボリューム、および保護ボリューム（レプリケーションに使用）に関連する容量を表示できます。また、さまざまなボリュームテクノロジ（ iSCSI または FC ）を表示したり、アレイの仮想化の問題について仮想ボリュームと非仮想ボリュームを比較したりすることもできます。

このデータモデルを使用すると、次のような回答の情報を確認できます。

- 利用率が事前に定義されたしきい値を上回っているボリューム
- 孤立ボリューム容量のデータセンターにおけるトレンド
- 仮想化またはシンプロビジョニングされているデータセンター容量
- レプリケーション用に予約する必要があるデータセンター容量

Chargeback データモデル

ストレージリソース（ボリューム、内部ボリューム、 qtree ）の使用済み容量と割り当て済み容量に関する回答の情報を確認できます。このデータモデルは、ストレージ容量のチャージバックとアカウンタビリティの情報をホスト、アプリケーション、およびビジネスエンティティ別に提供します。現在のデータと履歴データの両方が含まれます。レポートデータは、サービスレベルとストレージ階層で分類できます。

このデータモデルを使用すると、ビジネスエンティティで使用されている容量を検出することでチャージバックレポートを生成できます。このデータモデルでは、複数のプロトコル（ NAS 、 SAN 、 FC 、 iSCSI など）についてのレポートをまとめて作成できます。

- 内部ボリュームがないストレージの場合、チャージバックレポートにはボリューム別のチャージバックが表示されます。
- 内部ボリュームがあるストレージの場合：

- ビジネスエンティティがボリュームに割り当てられている場合、チャージバックレポートにはボリューム別のチャージバックが表示されます。
- ビジネスエンティティがボリュームではなく qtree に割り当てられている場合、チャージバックレポートには qtree 別のチャージバックが表示されます。
- ビジネスエンティティがボリュームにも qtree にも割り当てられていない場合、チャージバックレポートには内部ボリュームが表示されます。
- ボリューム別、 qtree 別、または内部ボリューム別のチャージバックを表示するかどうかは内部ボリュームごとに決定されるため、同じストレージプール内の別々の内部ボリュームで異なるレベルのチャージバックが表示される可能性があります。

容量ファクトはデフォルトの期間後にパージされます。詳細については、 Data Warehouse のプロセスを参照してください。

Chargeback データモデルを使用するレポートには、 Storage Capacity データモデルを使用するレポートとは異なる値が表示される場合があります。

- ネットアップストレージシステムでないストレージアレイの場合、両方のデータモデルのデータは同じです。
- NetApp および Celerra のストレージシステムの場合、 Chargeback データモデルは（ボリューム、内部ボリューム、または qtree の） 1 つのレイヤを使用して料金を請求し、 Storage Capacity データモデルは（ボリュームと内部ボリュームの）複数のレイヤを使用して料金を加算します。

Inventory データモデル

ホスト、ストレージシステム、スイッチ、ディスク、テープなどのインベントリリソースに関する回答の質問にお答えします。 qtree 、クォータ、仮想マシンとサーバ、および汎用デバイスです。Inventory データモデルには、レプリケーション、 FC パス、 iSCSI パス、 NFS パス、および違反に関する情報を表示するサブマートが複数含まれています。Inventory データモデルには履歴データは含まれません。このデータを使用して回答で確認できる情報

- 所有しているアセットとその場所
- アセットの使用者
- 所有しているデバイスの種類と、デバイスのコンポーネントを教えてください。
- OS あたりのホスト数とホスト上のポート数
- 各データセンターには、ベンダーごとにどのようなストレージアレイがありますか。
- 各データセンターには、ベンダーあたりいくつのスイッチがありますか。
- ライセンスが設定されていないポートの数
- 使用しているベンダーのテープ、および各テープのポート数。レポートの作成を開始する前に、特定されたすべての汎用デバイスを再確認します。
- ホストとストレージボリュームまたはテープ間のパス
- 汎用デバイスとストレージボリュームまたはテープ間のパス
- データセンターごとの各タイプの違反数
- レプリケートされた各ボリュームの、ソースボリュームとターゲットボリューム
- Fibre Channel ホストの HBA とスイッチとの間にファームウェアの互換性の問題またはポート速度の不一致があるか

Performance データモデル

ボリューム、アプリケーションボリューム、内部ボリューム、スイッチ、アプリケーションのパフォーマンスに関する回答の質問に回答できます。 VM 、 VMDK 、 ESX と VM 、ホスト、およびアプリケーションノードです。これらのレポートの多くは、_Hourly_data、_Daily_data、またはその両方です。このデータモデルを使用すると、回答に複数のタイプのパフォーマンス管理に関する情報を記載したレポートを作成できます。

- 特定の期間に使用またはアクセスされていないボリュームまたは内部ボリューム
- アプリケーション用のストレージ（未使用）に関する潜在的な構成ミスを特定できるか？
- アプリケーションの全体的なアクセス動作パターン
- 特定のアプリケーションに階層型ボリュームが適切に割り当てられているか
- アプリケーションのパフォーマンスに影響を与えずに、実行中のアプリケーションに安価なストレージを使用できますか？
- 現在設定されているストレージへのアクセスが多いアプリケーション

スイッチパフォーマンスのテーブルを使用すると、次の情報を取得できます。

- 接続されたポート経由でホストトラフィックが分散されているか。
- 多数のエラーが発生しているスイッチまたはポート
- ポートパフォーマンスに基づいて最も使用されているスイッチはどれですか？
- 使用率の低いスイッチのうち、ポートのパフォーマンスに基づくものは何ですか。
- ポートのパフォーマンスに基づくホストのトレンド分析スループット
- 特定の 1 つのホスト、ストレージシステム、テープ、またはスイッチの過去 X 日間のパフォーマンス利用率
- 特定のスイッチでトラフィックを生成しているデバイス（たとえば、利用率の高いスイッチを使用しているデバイス）
- 環境内の特定のビジネスユニットのスループット

ディスクパフォーマンスのテーブルを使用すると、次の情報を取得できます。

- ディスクのパフォーマンスデータに基づく、指定されたストレージプールのスループット
- 最も使用されているストレージプール
- 特定のストレージのディスク利用率の平均
- ディスクパフォーマンスデータに基づくストレージシステムまたはストレージプールの使用状況のトレンド
- 特定のストレージプールのディスク使用率のトレンド

VM と VMDK のパフォーマンスのテーブルを使用すると、次の情報を取得できます。

- 仮想環境のパフォーマンスが最適化されているか
- 最も高いワークロードを報告している VMDK
- 異なるデータストアにマッピングされた VM から報告されたパフォーマンスを使用して、階層化の再決定を行うにはどうすればよいですか。

パフォーマンスデータモデルには、階層の妥当性、アプリケーション用のストレージの構成ミス、およびボリュームと内部ボリュームの最終アクセス時刻を特定するための情報が含まれています。このデータモデルは、応答時間、 IOPS 、スループット、保留中の書き込み数、アクセスステータスなどのデータを提供します。

Storage Efficiency データモデル

一定期間にわたるストレージの削減率と可能性を追跡できます。このデータモデルには、プロビジョニング済み容量のデータだけでなく、使用済みまたは消費済みの容量（物理的な測定値）も格納されます。たとえば、シンプロビジョニングが有効な場合、Data Infrastructure Insightsにはデバイスから消費された容量が表示されます。また、このモデルを使用して、重複排除が有効な場合の効率を判断することもできます。Storage Efficiency データマートを使用すると、回答に関するさまざまな情報を確認できます。

- シンプロビジョニングと重複排除を実装した場合の Storage Efficiency による削減効果
- データセンター全体でのストレージ削減量
- 過去の容量のトレンドに基づいて、ストレージを追加購入する必要があるのはいつですか？
- シンプロビジョニングや重複排除などのテクノロジを有効にした場合の容量の増加
- ストレージ容量にリスクがありますか？

データモデルのファクトテーブルとディメンションテーブル

各データモデルには、ファクトテーブルとディメンションテーブルの両方が含まれています。

- ファクトテーブル：量、物理容量、使用可能な容量など、測定されたデータが含まれます。ディメンションテーブルへの外部キーが含まれます。
- ディメンションテーブル：データセンターやビジネスユニットなど、ファクトに関する説明が含まれます。ディメンションはデータを分類する構造であり、多くの場合、複数の階層で構成されます。ディメンション属性は、ディメンション値の説明に役立ちます。

（レポート内の列に表示される）複数のディメンション属性を使用して、データモデルに含まれる各ディメンションのデータをアクセスするレポートを作成します。

データモデル要素で使用される色

データモデル要素の色には意味があります。

- 黄色のアセット：測定値を表します。
- 黄色以外のアセット：属性を表します。これらの値は集計されません。

1 つのレポートで複数のデータモデルを使用する

通常は、レポートごとに 1 つのデータモデルを使用します。ただし、複数のデータモデルのデータを結合したレポートを作成することができます。

複数のデータモデルのデータを結合したレポートを作成するには、ベースとして使用するデータモデルを 1 つ選択し、追加のデータマートからデータを収集する SQL クエリを作成します。SQL の Join 機能を使用して、複数のクエリのデータを 1 つのクエリに結合し、レポートの作成に使用できます。

たとえば、各ストレージアレイの現在の容量を確認し、アレイのカスタムアノテーションを取得するとします。このレポートは、 Storage Capacity データモデルを使用して作成できます。Current Capacity テーブルとディメンションテーブルの要素を使用し、別途 SQL クエリを追加して Inventory データモデルのアノテーシ

ョン情報にアクセスします。最後に、ストレージ名と結合条件を使用して Inventory のストレージデータを Storage Dimension テーブルにリンクして、データを結合します。

API 経由で Reporting Database にアクセスします

Data Infrastructure Insightsの強力なAPIを使用すると、Cognos Reporting環境を介さずに、Data Infrastructure Insights Reportingデータベースに直接クエリを実行できます。

このドキュメントでは、Data Infrastructure Insights Premiumエディションで利用できるData Infrastructure Insightsのレポート機能について説明します。

OData

Data Infrastructure Insights Reporting APIは、（Open Data Protocol）標準に従って"OData v4 の"Reportingデータベースを照会します。詳細または詳細については、ODataをご覧ください"このチュートリアルでは"。

すべての要求は、URL_\https://<Data Infrastructure Insights URL>/rest/v1/dwh-management/odata_で始まります。

apiKey を生成します

詳細については、をご覧ください"データインフラ分析情報API"。

API キーを生成するには、次の手順を実行します。

- Data Infrastructure Insights環境にログインし、*[Admin]>[API Access]*を選択します。
- [+API Access Token] をクリックします。
- 名前と概要を入力します。
- タイプには、 Data Warehouse _ を選択します。
- 権限を読み取り / 書き込みに設定します。
- 要望の有効期限を設定します。
- [保存] をクリックし、 * キーをコピーして安全な場所に保存します。あとでフルキーにアクセスすることはできません。

APIkeysはに適しています 同期または非同期_。

テーブルの直接クエリ

API キーを配置した状態で、 Reporting データベースの直接クエリを実行できるようになりました。長いURLは、\https://<Data Infrastructure Insightsの完全なURL >/rest/v1/dwh-management/odata/ではなく、表示目的で\https://…/odata/に単純化できます。

次のような簡単なクエリを試してください

- https://<Dataインフラ分析情報のURL>/reset/v1/dwh-management/odata/dwh_custom
- https://<Dataインフラ分析情報のURL>/rest /v1/dwh-management/odata/dwh_inventory
- https://<Dataインフラ分析情報のURL>/rest /v1/dwh-management/odata/dwh_inventory/storage

- https://<Dataインフラ分析情報のURL>/rest /v1/dwh-management/odata/dwh_inventory/disk
- https://…/odata/dwh_custom/custom_queries

REST API の例

すべての呼び出しのURLは_\https://<Data Infrastructure Insights URL>/rest/v1/dwh-management/odata_です。

- get/{schema}/**-レポートデータベースからデータを取得します。

形式：*https://<Data Infrastructure Insights <schema_name>/<query>*

例

```
 https://<domain>/rest/v1/dwh-
management/odata/dwh_inventory/fabric?$count=true&$orderby=name
```

結果


```
{
   "@odata.context": "$metadata#fabric",
   "@odata.count": 2,
   "value": [
       {
           "id": 851,
           "identifier": "10:00:50:EB:1A:40:3B:44",
           "wwn": "10:00:50:EB:1A:40:3B:44",
           "name": "10:00:50:EB:1A:40:3B:44",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941716"
       },
       {
           "id": 852,
           "identifier": "10:00:50:EB:1A:40:44:0C",
           "wwn": "10:00:50:EB:1A:40:44:0C",
           "name": "10:00:50:EB:1A:40:44:0C",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941836"
        }
    ]
}
```

役に立つヒント

Reporting API クエリを使用する場合は、次の点に注意してください。

- クエリペイロードには有効な JSON 文字列を指定する必要があります
- クエリペイロードは 1 行に含める必要があります
- 二重引用符はエスケープする必要があります。
- タブは \t としてサポートされています
- コメントは避けてください
- 小文字のテーブル名がサポートされています

さらに、

- 2 つのヘッダーが必要です。
  - 「 X-CloudInsights - apiKey 」という名前を付けます。
  - 属性値「 <apiKey> 」

APIキーは、お客様のData Infrastructure Insights環境に固有のものです。

同期か非同期か

デフォルトでは、APIコマンドは_synchronous_modeで動作します。つまり、要求を送信するとすぐに応答が返されます。ただし、クエリの実行に時間がかかることがあり、要求がタイムアウトする可能性があります。これを回避するには、request_asynchronously _を実行します。非同期モードでは、要求は実行の監視に使用するURLを返します。URLは準備ができたら結果を返します。

非同期モードでクエリを実行するには、ヘッダーを追加します。 **`Prefer: respond-async`** 要求に。実行が成功すると、応答に次のヘッダーが含まれます。

```
Status Code: 202 (which means ACCEPTED)
preference-applied: respond-async
location: https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncStatus/<token>
```

ロケーションURLを照会すると、応答の準備ができていない場合は同じヘッダーが返され、応答の準備ができている場合はステータス200が返されます。応答コンテンツのタイプはtextで、元のクエリのhttpステータスとメタデータが含まれ、その後に元のクエリの結果が続きます。

```
HTTP/1.1 200 OK
 OData-Version: 4.0
 Content-Type: application/json;odata.metadata=minimal
 oDataResponseSizeCounted: true

 { <JSON_RESPONSE> }
```

すべての非同期クエリのリストと、準備ができているものを表示するには、次のコマンドを使用します。

```
 GET https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncList
```
応答の形式は次のとおりです。

```
{
   "queries" : [
       {
           "Query": "https://<Data Infrastructure Insights
URL>/rest/v1/dwh-
management/odata/dwh_custom/heavy_left_join3?$count=true",
           "Location": "https://<Data Infrastructure Insights
URL>/rest/v1/dwh-management/odata/dwh_custom/asyncStatus/<token>",
           "Finished": false
       }
   ]
}
```

レポート用に履歴データを保持する方法

Data Infrastructure Insightsでは、次の表に示すように、履歴データが保持され、データマートおよびデータの単位に基づいてReportingで使用されます。

データマート	測定されたオブジェクト	精度	保持期間
Performance データマート	ボリュームと内部ボリューム	毎時	14 日
Performance データマート	ボリュームと内部ボリューム	毎日	13 カ月
Performance データマート	アプリケーション	毎時	13 カ月
Performance データマート	ホスト	毎時	13 カ月
Performance データマート	ポートのスイッチパフォーマンス	毎時	35日
Performance データマート	ホスト、ストレージ、およびテープのスイッチパフォーマンス	毎時	13 カ月
Performance データマート	ストレージノード	毎時	14 日
Performance データマート	ストレージノード	毎日	13 カ月

Performance データマート	VM パフォーマンス	毎時	14 日
Performance データマート	VM パフォーマンス	毎日	13 カ月
Performance データマート	ハイパーバイザーのパフォーマンス	毎時	35日
Performance データマート	ハイパーバイザーのパフォーマンス	毎日	13 カ月
Performance データマート	VMDKのパフォーマンス	毎時	35日
Performance データマート	VMDKのパフォーマンス	毎日	13 カ月
Performance データマート	ディスクパフォーマンス	毎時	14 日
Performance データマート	ディスクパフォーマンス	毎日	13 カ月
Capacity データマート	すべて（個々のボリュームを除く）	毎日	13 カ月
Capacity データマート	すべて（個々のボリュームを除く）	月の代表日	14 カ月以上
Inventory データマート	個々のボリューム	現在の状態	1 日（または次の ETL まで）

Data Infrastructure Insightsのレポートスキーマ図

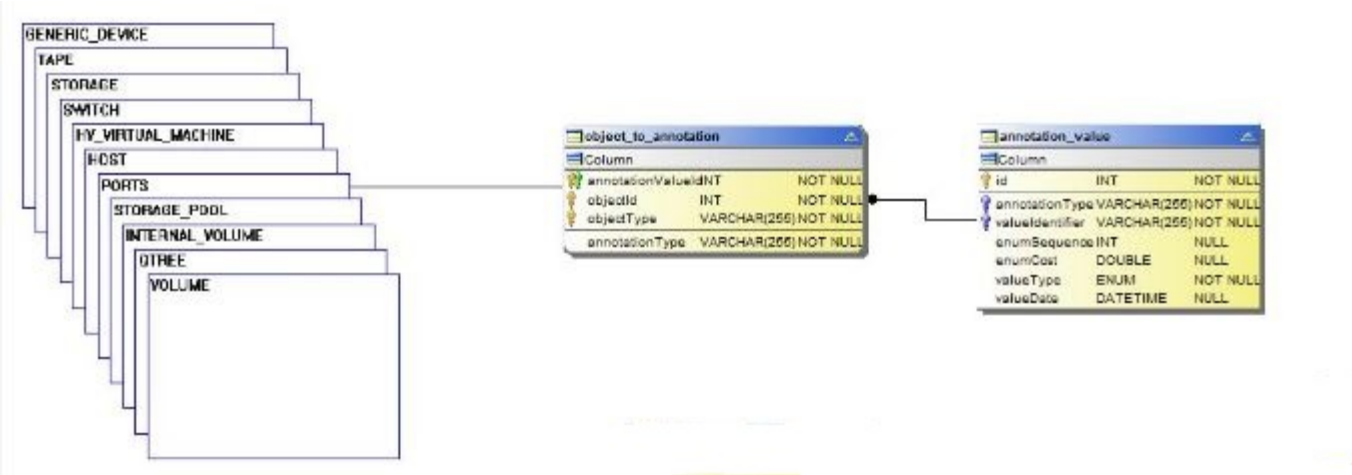
このドキュメントでは、 Reporting Database のスキーマ図を示します。を含むファイルをダウンロードすることもできます "スキーマテーブル"。

レポート機能はData Infrastructure Insightsで使用でき"Premium Edition の場合"ます。

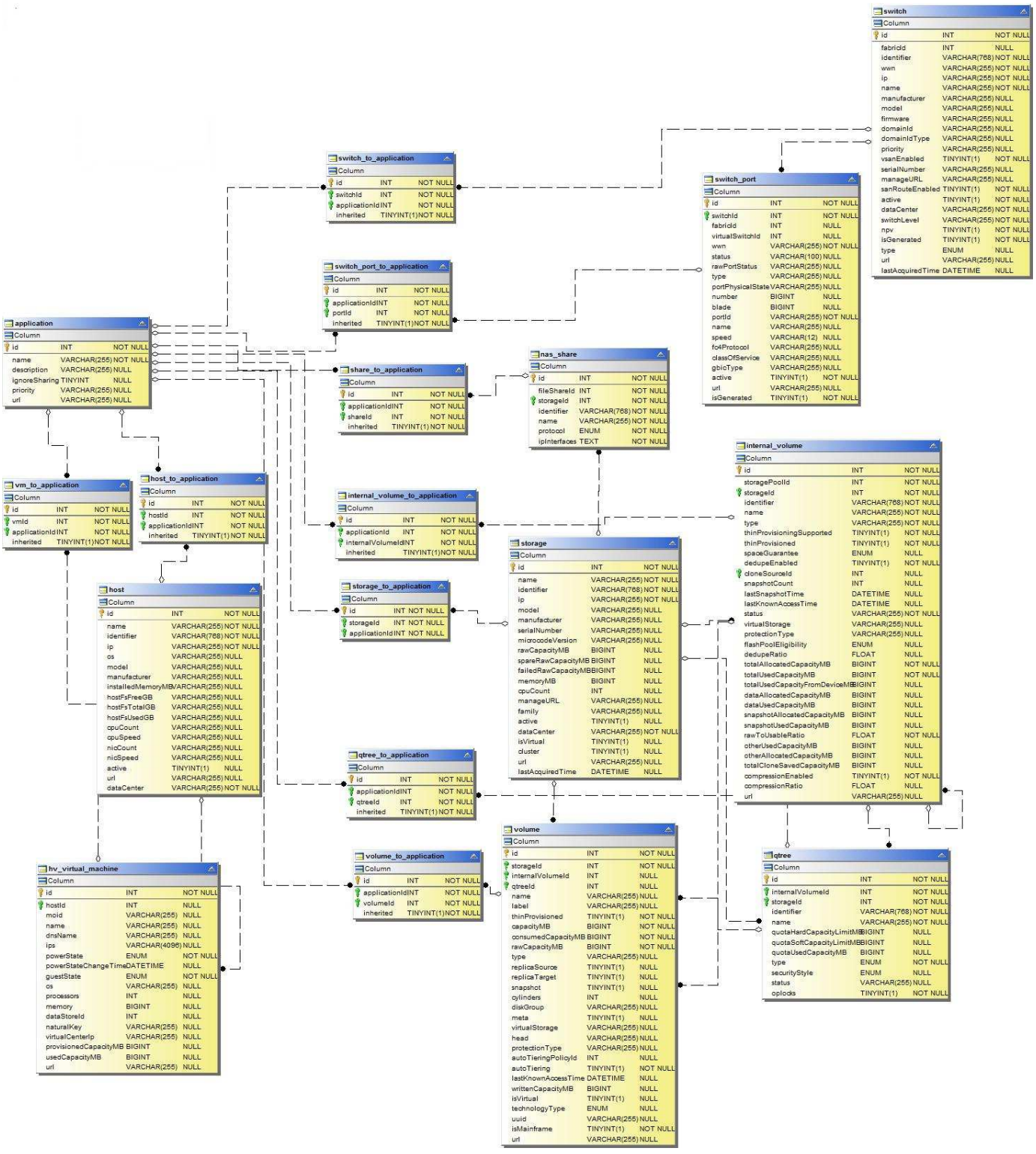
Inventory Datamart のサービスです

次の図は、インベントリデータマートを説明しています。

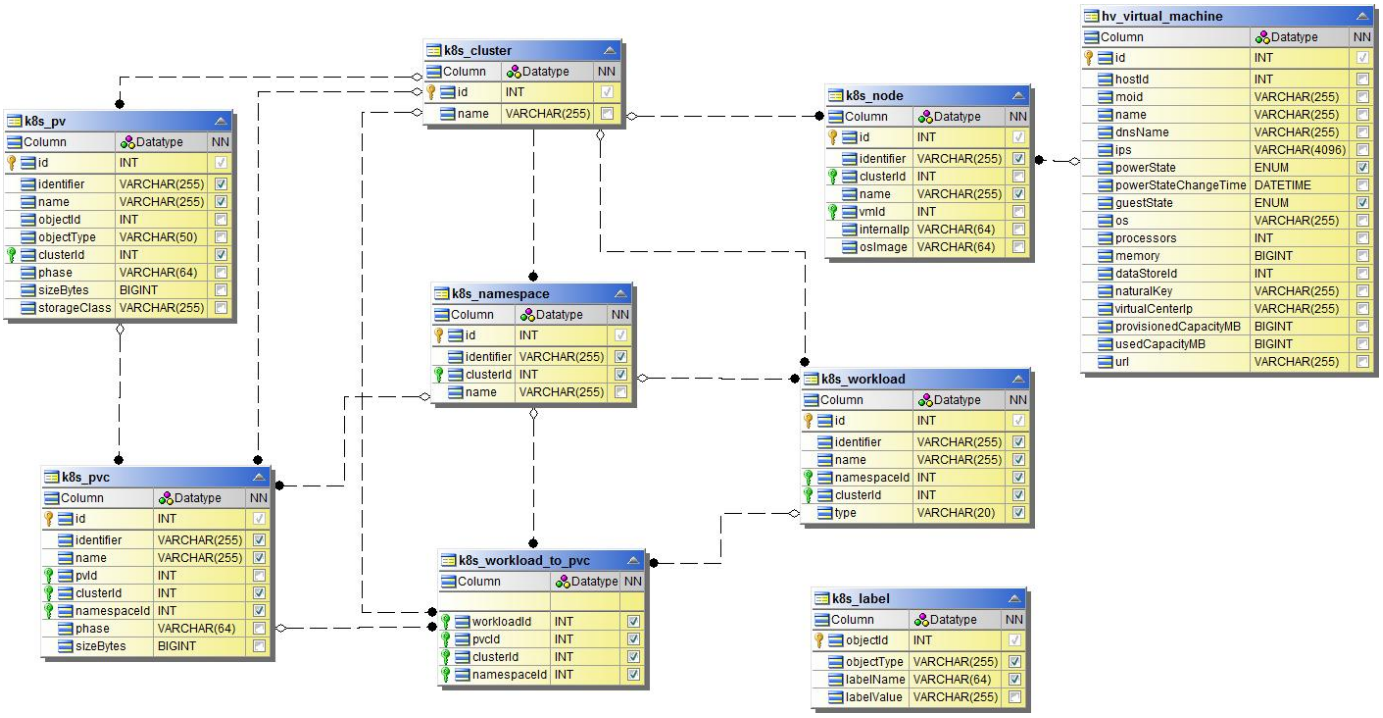
注釈


GENERIC_DEVICE
TAPE
STORAGE
SWITCH
HV_VIRTUAL_MACHINE
HOST
PORTS
STORAGE_POOL
INTERNAL_VOLUME
OTHER
VOLUME
object_to_annotation
Column
annotationValueId INT NOT NULL
objectId INT NOT NULL
objectType VARCHAR(255) NOT NULL
annotationType VARCHAR(255) NOT NULL
annotation_value
Column
id INT NOT NULL
annotationType VARCHAR(255) NOT NULL
valueIdentifier VARCHAR(255) NOT NULL
enumSequence INT NULL
enumCost DOUBLE NULL
valueType ENUM NOT NULL
valueDate DATETIME NULL

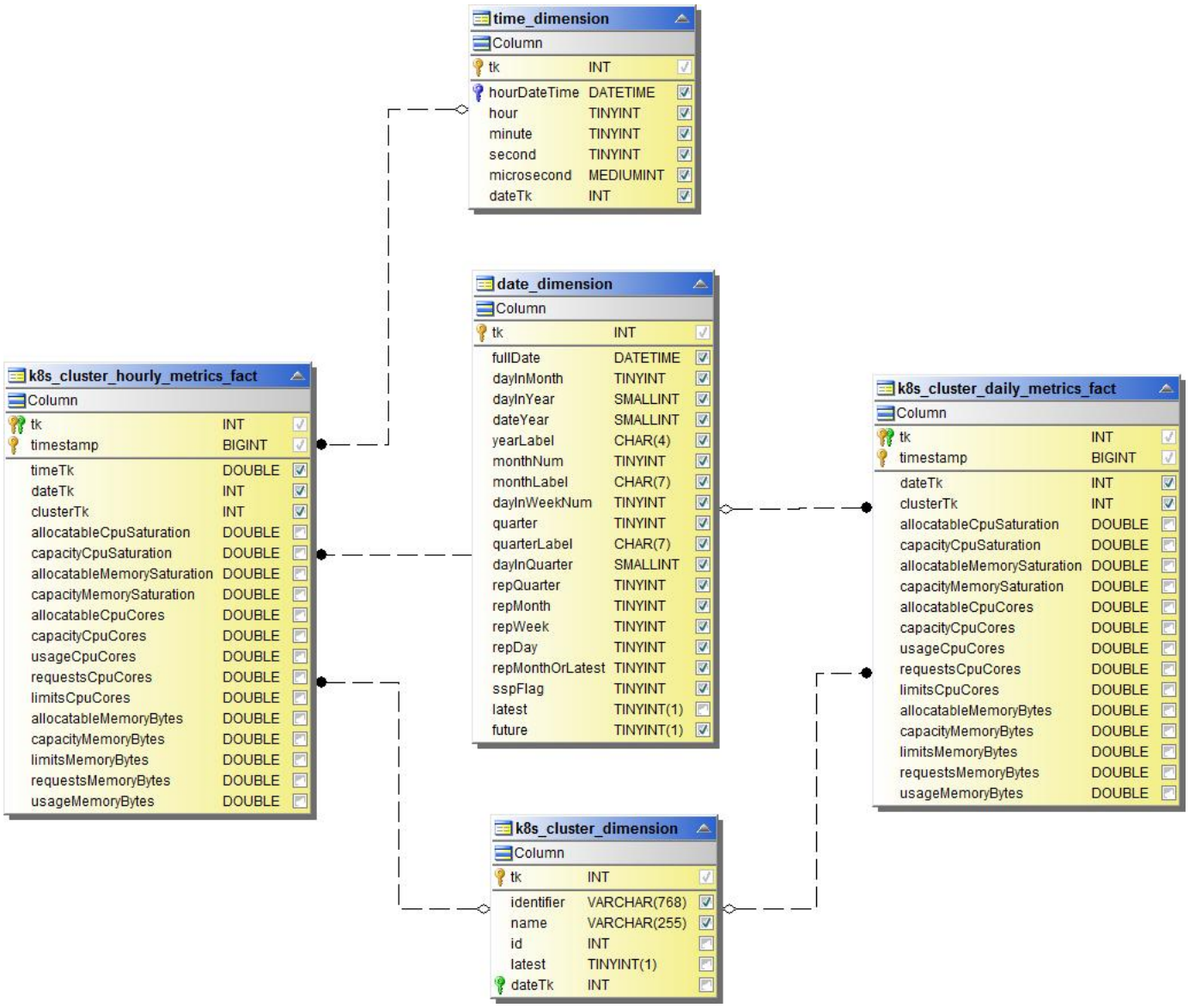
アプリケーション



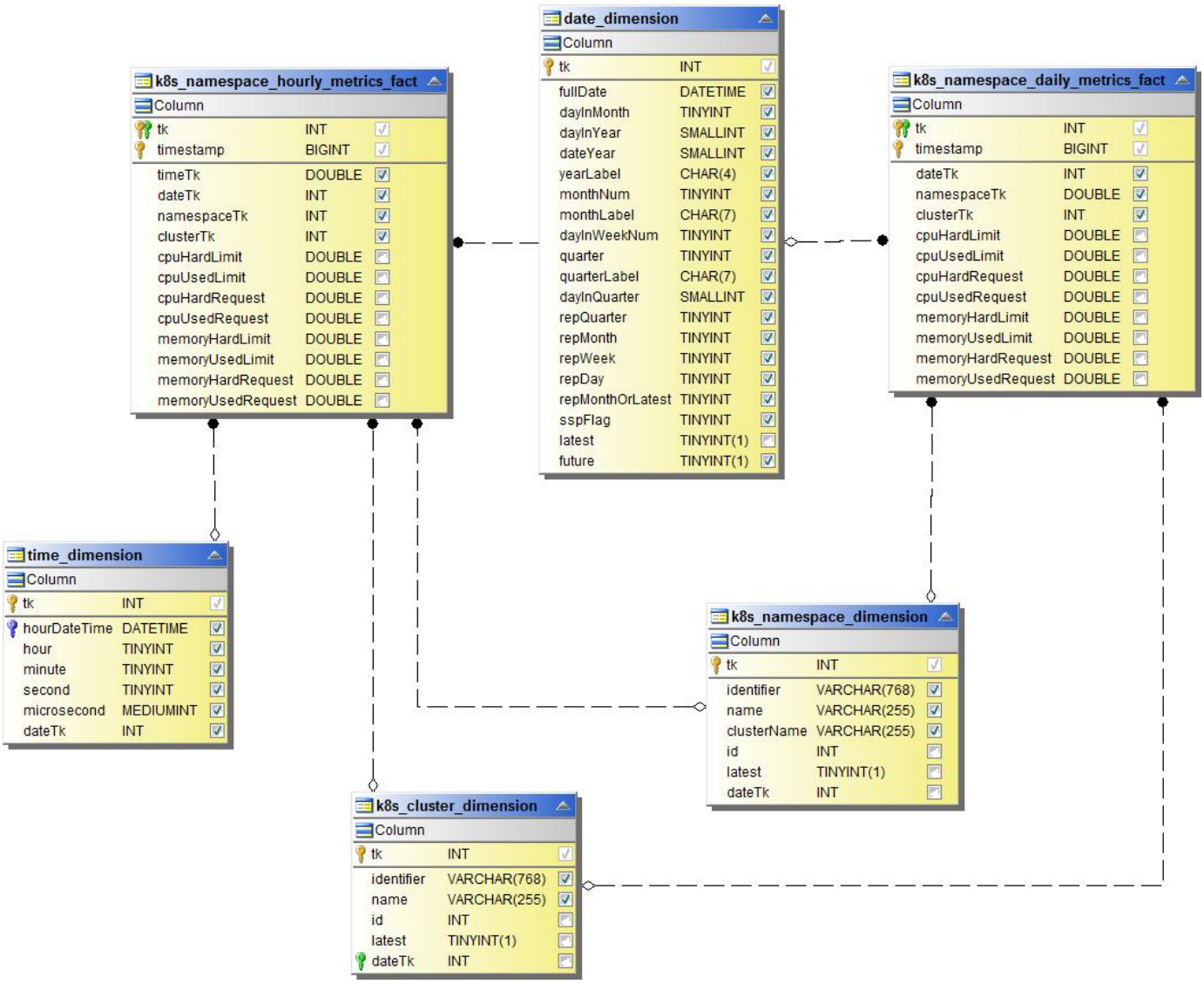
Kubernetes指標



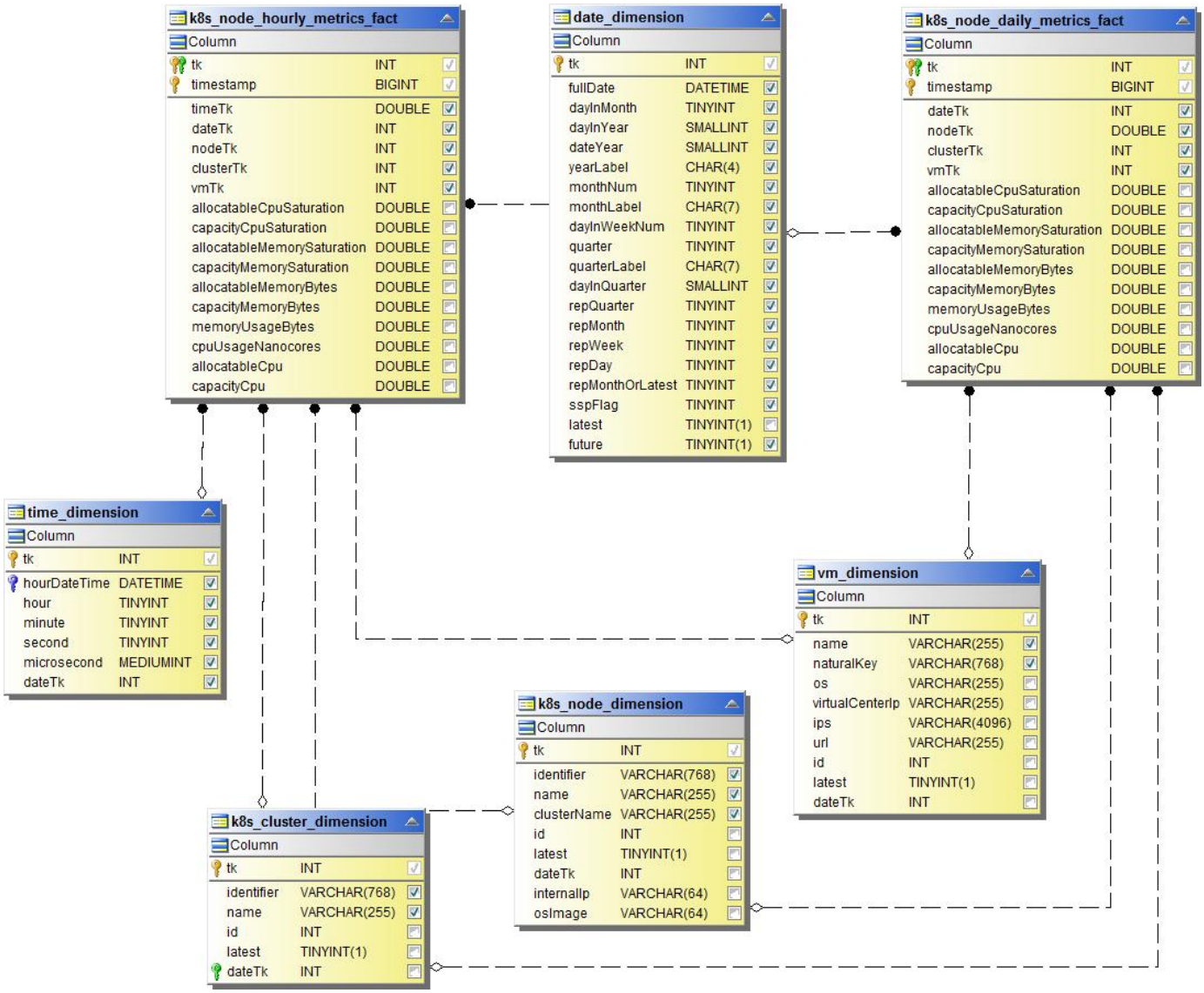
Kubernetes Cluster Metricsファクト



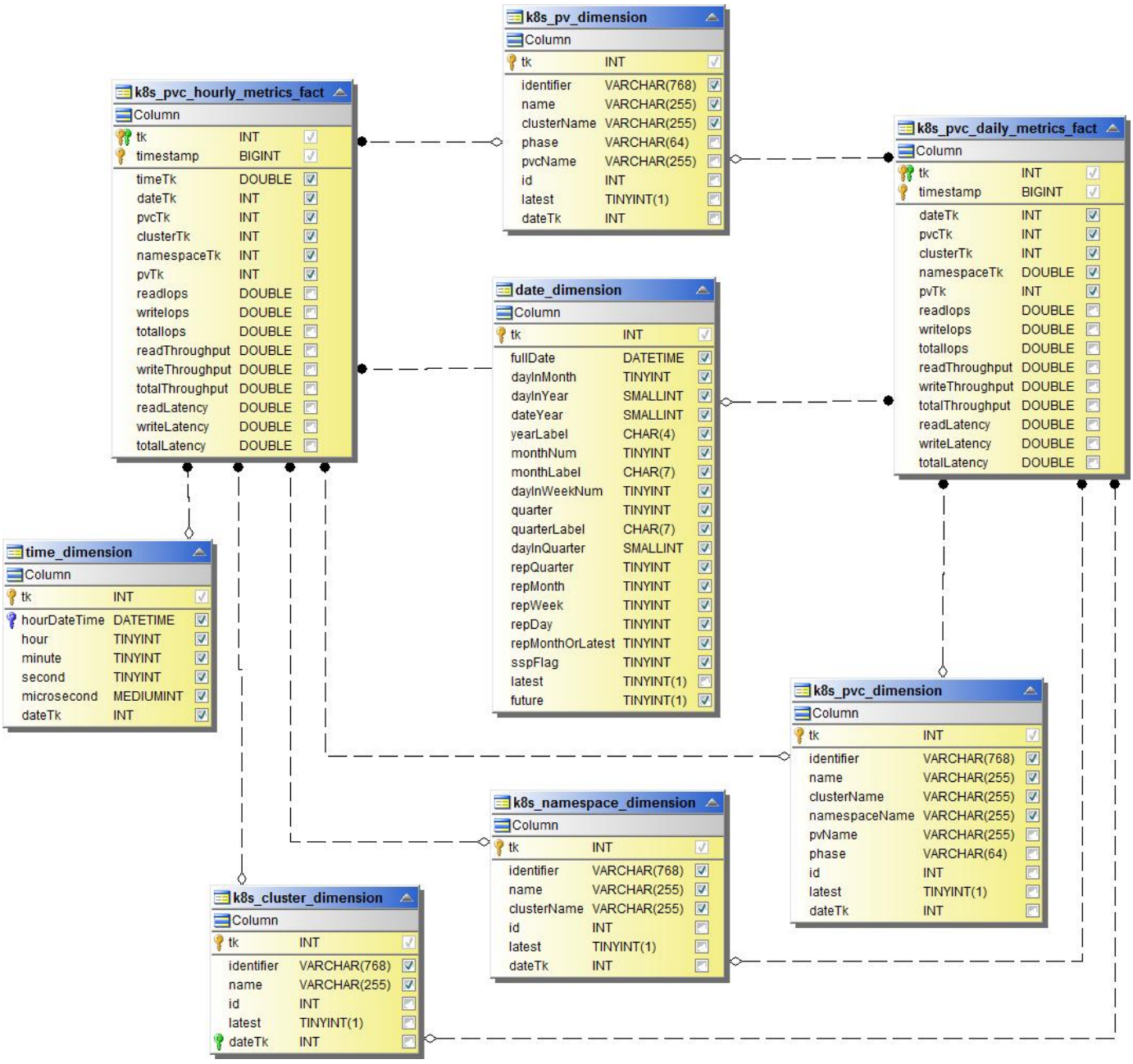
Kubernetes Namespace Metricsファクト



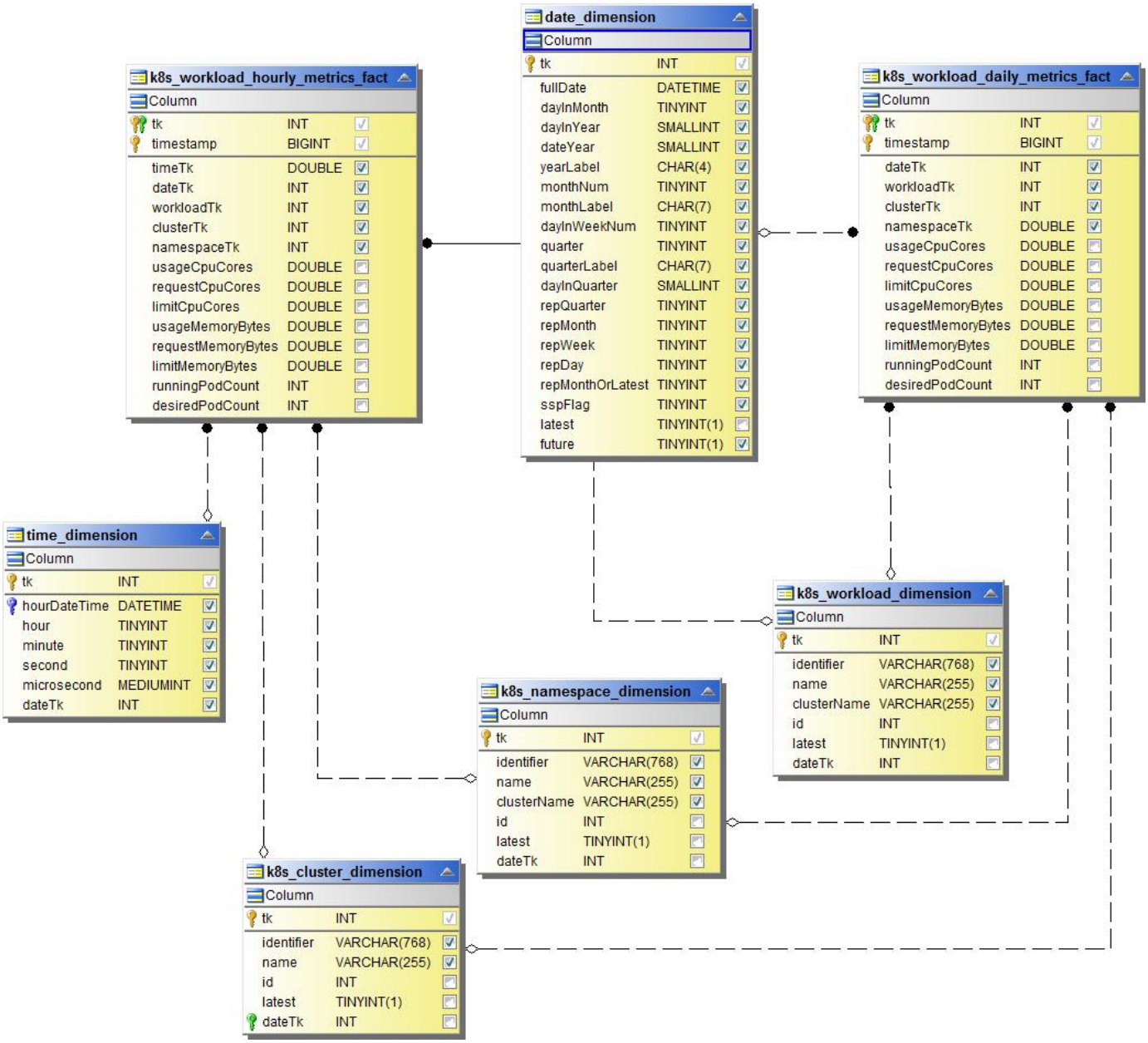
Kubernetes Node Metricsファクト



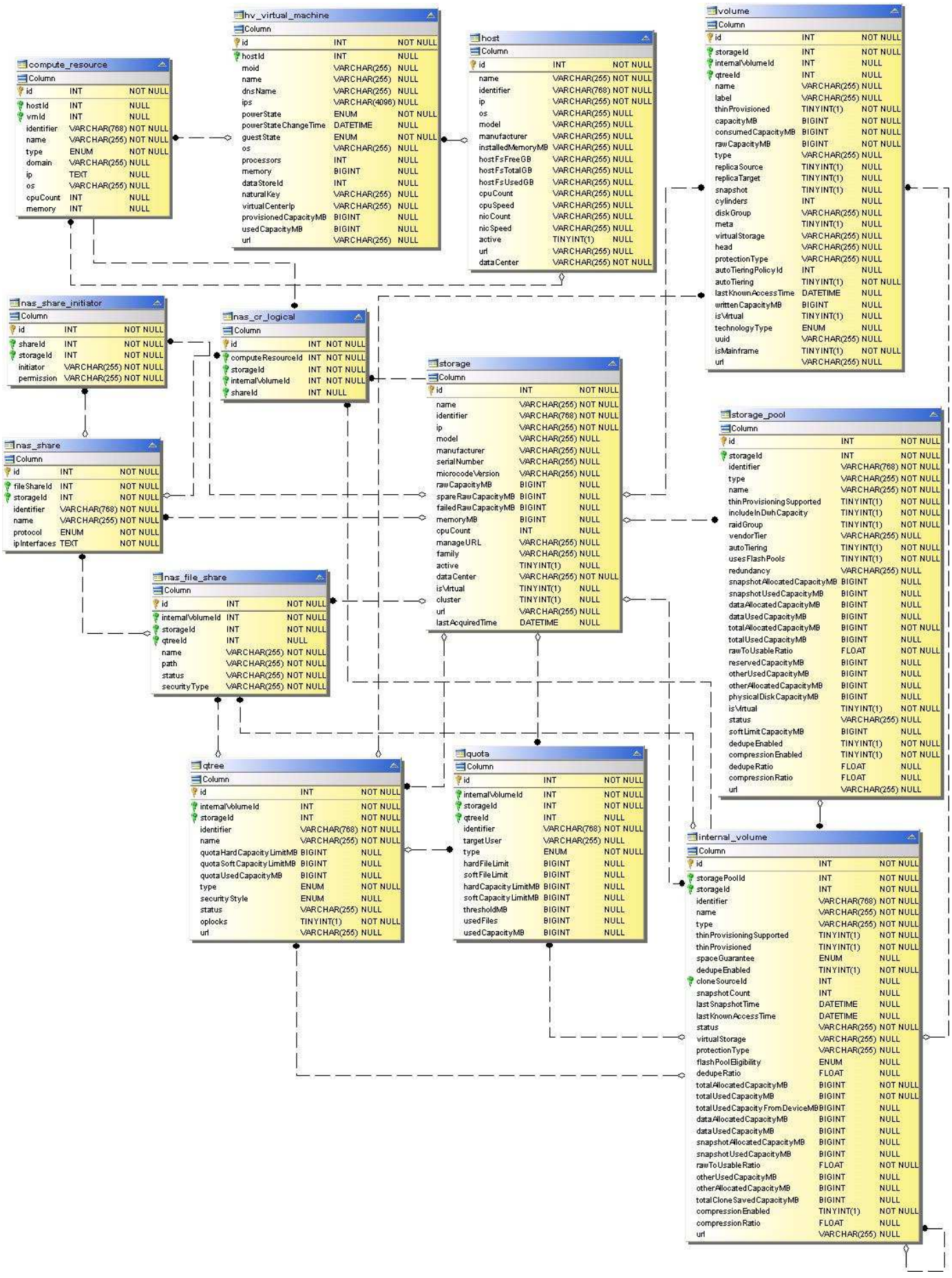
Kubernetes PVC Metricsファクト



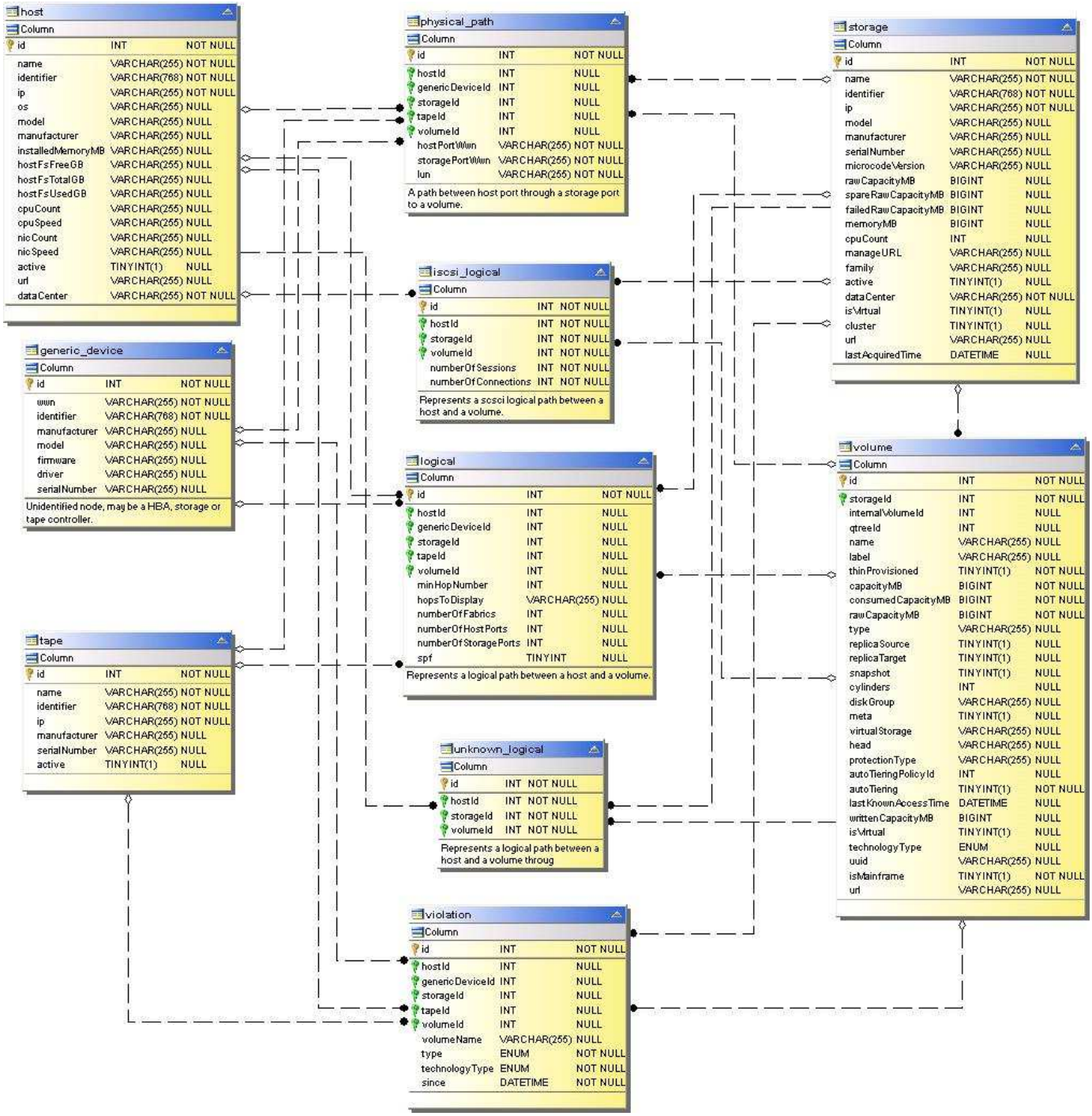
Kubernetes Workload Metricsファクト


date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
sspFlag TINYINT
latest TINYINT(1)
future TINYINT(1)
k8s_workload_hourly_metrics_fact
Column
tk INT
timestamp BIGINT
timeTk DOUBLE
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk INT
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
k8s_workload_daily_metrics_fact
Column
tk INT
timestamp BIGINT
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk DOUBLE
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT
k8s_workload_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_namespace_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_cluster_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT

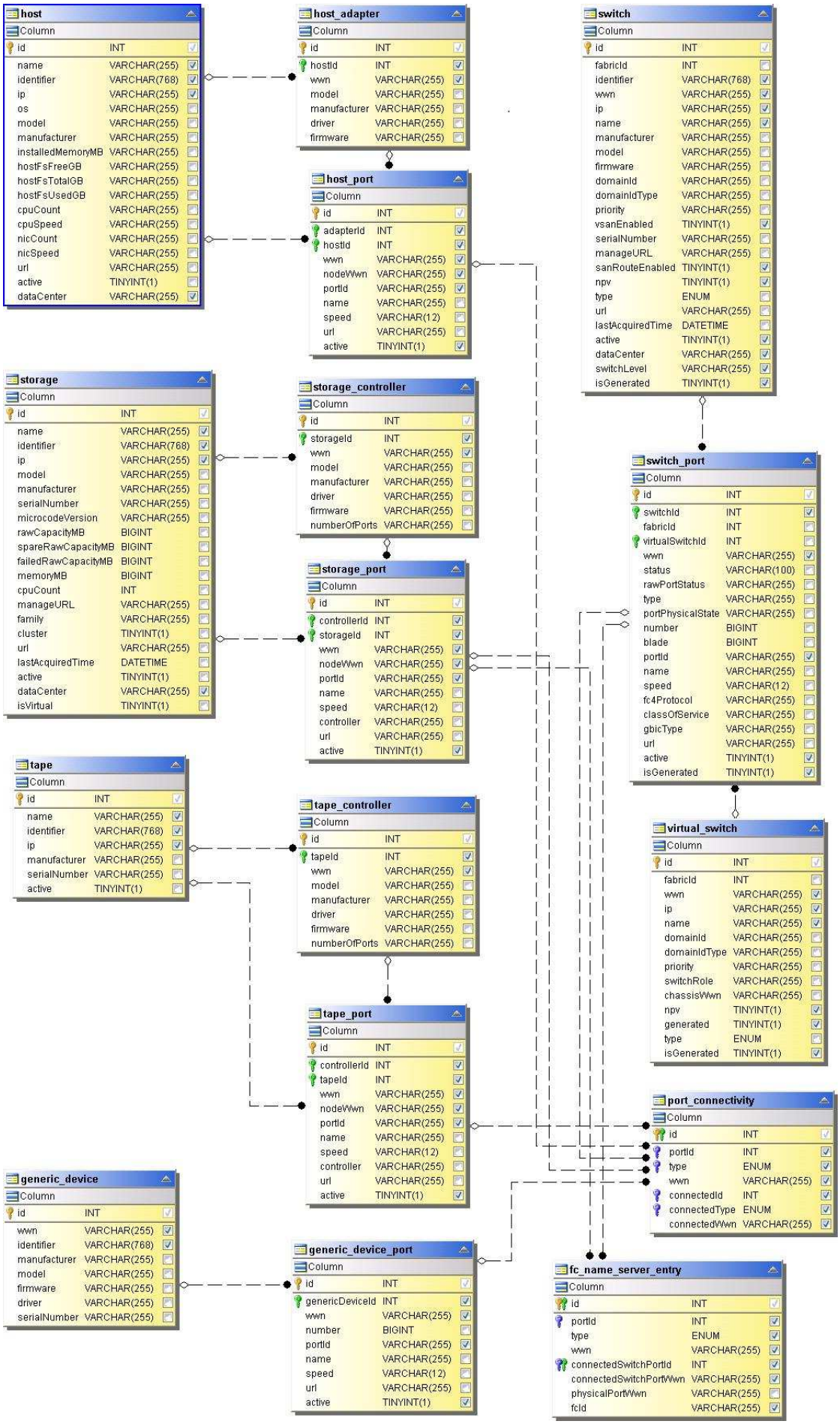
NAS


compute_resource
Column
id INT NOT NULL
hostId INT NULL
vmId INT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type ENUM NOT NULL
domain VARCHAR(255) NULL
ip TEXT NULL
os VARCHAR(255) NULL
cpuCount INT NULL
memory INT NULL
hv_virtual_machine
Column
id INT NOT NULL
hostId INT NULL
moid VARCHAR(255) NULL
name VARCHAR(255) NULL
dnsName VARCHAR(255) NULL
ips VARCHAR(4096) NULL
powerState ENUM NOT NULL
powerStateChangeTime DATETIME NULL
guestState ENUM NOT NULL
os VARCHAR(255) NULL
processors INT NULL
memory BIGINT NULL
dataStoreId INT NULL
naturalKey VARCHAR(255) NULL
virtualCenterIp VARCHAR(255) NULL
provisionedCapacityMB BIGINT NULL
usedCapacityMB BIGINT NULL
url VARCHAR(255) NULL
host
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
os VARCHAR(255) NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
installedMemoryMB VARCHAR(255) NULL
hostFsFreeGB VARCHAR(255) NULL
hostFsTotalGB VARCHAR(255) NULL
hostFsUsedGB VARCHAR(255) NULL
cpuCount VARCHAR(255) NULL
cpuSpeed VARCHAR(255) NULL
nicCount VARCHAR(255) NULL
nicSpeed VARCHAR(255) NULL
active TINYINT(1) NULL
url VARCHAR(255) NULL
dataCenter VARCHAR(255) NOT NULL
volume
Column
id INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NULL
qtreeId INT NULL
name VARCHAR(255) NULL
label VARCHAR(255) NULL
thinProvisioned TINYINT(1) NOT NULL
capacityMB BIGINT NOT NULL
consumedCapacityMB BIGINT NOT NULL
rawCapacityMB BIGINT NOT NULL
type VARCHAR(255) NULL
replicaSource TINYINT(1) NULL
replicaTarget TINYINT(1) NULL
snapshot TINYINT(1) NULL
cylinders INT NULL
diskGroup VARCHAR(255) NULL
meta TINYINT(1) NULL
virtualStorage VARCHAR(255) NULL
head VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
autoTieringPolicyId INT NULL
autoTiering TINYINT(1) NOT NULL
lastKnownAccessTime DATETIME NULL
writtenCapacityMB BIGINT NULL
isVirtual TINYINT(1) NULL
technologyType ENUM NULL
uuid VARCHAR(255) NULL
isMainframe TINYINT(1) NOT NULL
url VARCHAR(255) NULL
nas_share_initiator
Column
id INT NOT NULL
shareId INT NOT NULL
storageId INT NOT NULL
initiator VARCHAR(255) NOT NULL
permission VARCHAR(255) NOT NULL
nas_cr_logical
Column
id INT NOT NULL
computeResourceId INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NOT NULL
shareId INT NULL
storage
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
serialNumber VARCHAR(255) NULL
microcodeVersion VARCHAR(255) NULL
rawCapacityMB BIGINT NULL
spareRawCapacityMB BIGINT NULL
failedRawCapacityMB BIGINT NULL
memoryMB BIGINT NULL
cpuCount INT NULL
manageURL VARCHAR(255) NULL
family VARCHAR(255) NULL
active TINYINT(1) NULL
dataCenter VARCHAR(255) NOT NULL
isVirtual TINYINT(1) NULL
cluster TINYINT(1) NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
storage_pool
Column
id INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
type VARCHAR(255) NOT NULL
name VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
includeInDuhCapacity TINYINT(1) NOT NULL
raidGroup TINYINT(1) NOT NULL
vendorTier VARCHAR(255) NULL
autoTiering TINYINT(1) NOT NULL
usesFlashPools TINYINT(1) NOT NULL
redundancy VARCHAR(255) NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
reservedCapacityMB BIGINT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
physicalDiskCapacityMB BIGINT NULL
isVirtual TINYINT(1) NOT NULL
status VARCHAR(255) NULL
softLimitCapacityMB BIGINT NULL
dedupeEnabled TINYINT(1) NOT NULL
compressionEnabled TINYINT(1) NOT NULL
dedupeRatio FLOAT NULL
compressionRatio FLOAT NULL
url VARCHAR(255) NULL
nas_share
Column
id INT NOT NULL
fileShareId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
protocol ENUM NOT NULL
ipInterfaces TEXT NOT NULL
nas_file_share
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
name VARCHAR(255) NOT NULL
path VARCHAR(255) NOT NULL
status VARCHAR(255) NOT NULL
securityType VARCHAR(255) NOT NULL
qtree
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
quotaHardCapacityLimitMB BIGINT NULL
quotaSoftCapacityLimitMB BIGINT NULL
quotaUsedCapacityMB BIGINT NULL
type ENUM NOT NULL
securityStyle ENUM NULL
status VARCHAR(255) NULL
oplocks TINYINT(1) NOT NULL
url VARCHAR(255) NULL
quota
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
identifier VARCHAR(768) NOT NULL
targetUser VARCHAR(255) NULL
type ENUM NOT NULL
hardFileLimit BIGINT NULL
softFileLimit BIGINT NULL
hardCapacityLimitMB BIGINT NULL
softCapacityLimitMB BIGINT NULL
thresholdMB BIGINT NULL
usedFiles BIGINT NULL
usedCapacityMB BIGINT NULL
internal_volume
Column
id INT NOT NULL
storagePoolId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
thinProvisioned TINYINT(1) NOT NULL
spaceGuarantee ENUM NULL
dedupeEnabled TINYINT(1) NOT NULL
cloneSourceId INT NULL
snapshotCount INT NULL
lastSnapshotTime DATETIME NULL
lastKnownAccessTime DATETIME NULL
status VARCHAR(255) NOT NULL
virtualStorage VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
flashPoolEligibility ENUM NULL
dedupeRatio FLOAT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NOT NULL
totalUsedCapacityFromDeviceMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
totalCloneSavedCapacityMB BIGINT NULL
compressionEnabled TINYINT(1) NOT NULL
compressionRatio FLOAT NULL
url VARCHAR(255) NULL

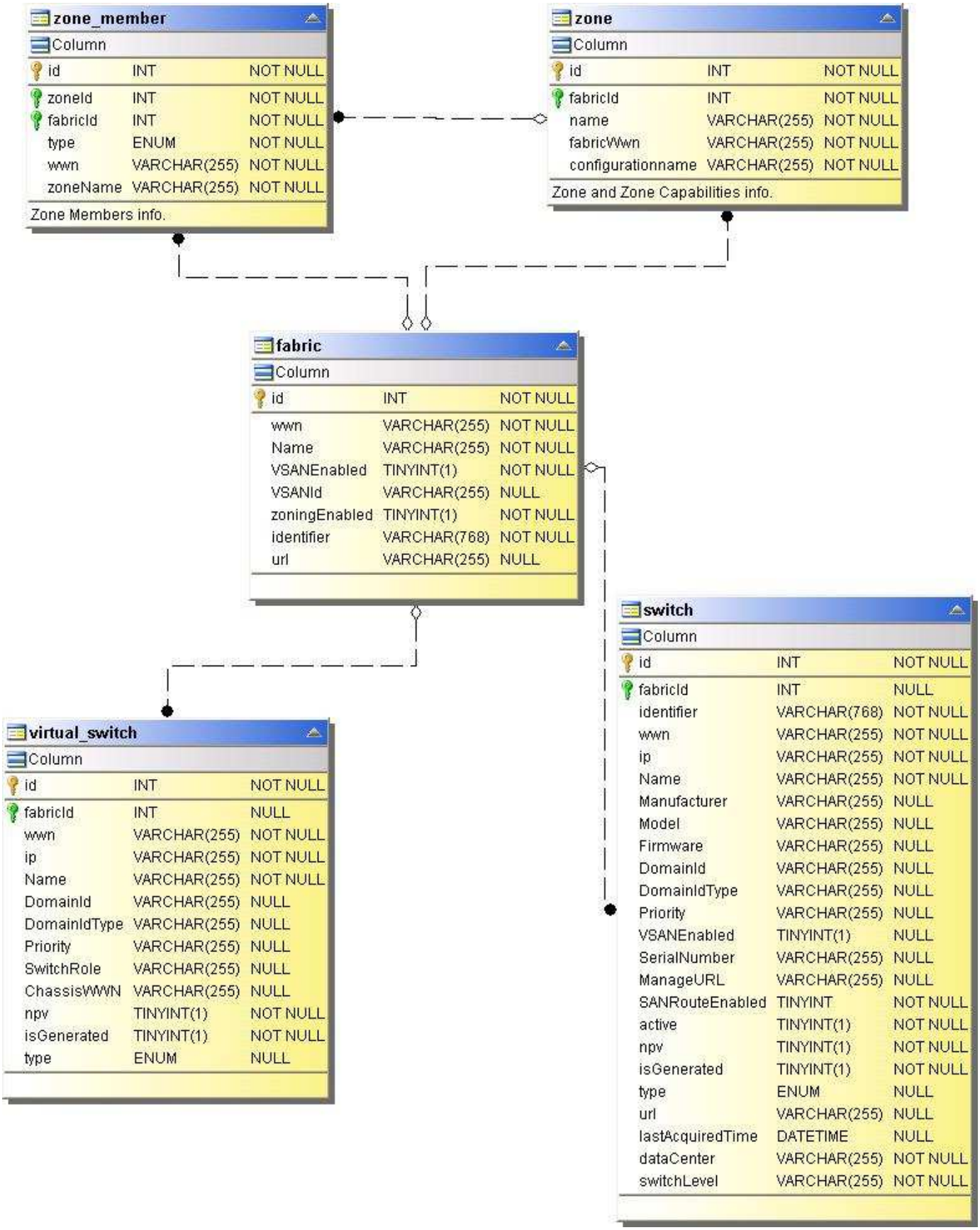
パスと違反

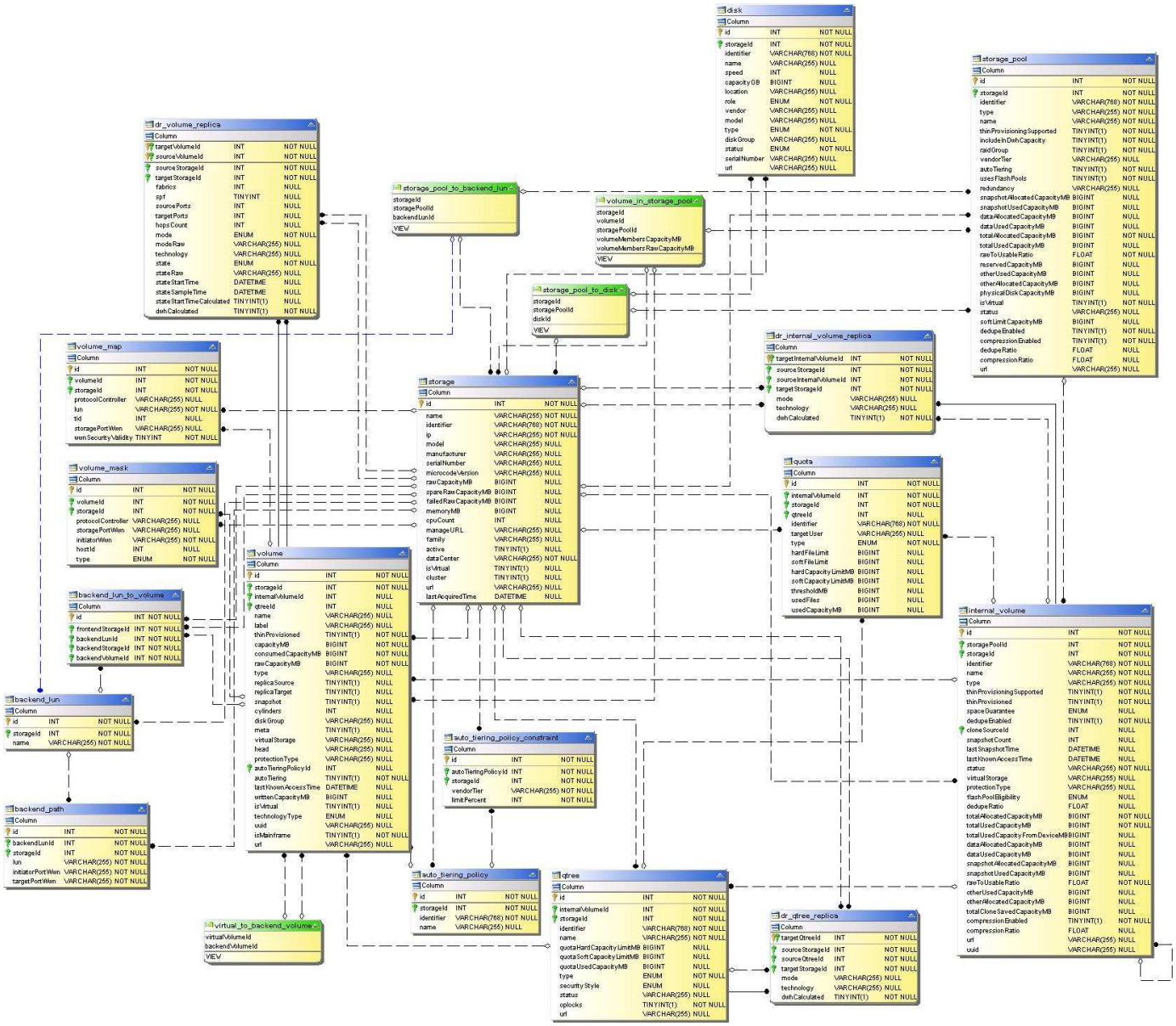

host
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
os VARCHAR(255) NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
installedMemoryMB VARCHAR(255) NULL
hostFsFreeGB VARCHAR(255) NULL
hostFsTotalGB VARCHAR(255) NULL
hostFsUsedGB VARCHAR(255) NULL
cpuCount VARCHAR(255) NULL
cpuSpeed VARCHAR(255) NULL
nicCount VARCHAR(255) NULL
nicSpeed VARCHAR(255) NULL
active TINYINT(1) NULL
url VARCHAR(255) NULL
dataCenter VARCHAR(255) NOT NULL
physical_path
Column
id INT NOT NULL
hostId INT NULL
genericDeviceId INT NULL
storageId INT NULL
tapeId INT NULL
volumeId INT NULL
hostPortWwn VARCHAR(255) NOT NULL
storagePortWwn VARCHAR(255) NOT NULL
lun VARCHAR(255) NOT NULL
A path between host port through a storage port to a volume.
storage
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
serialNumber VARCHAR(255) NULL
microcodeVersion VARCHAR(255) NULL
rawCapacityMB BIGINT NULL
spareRawCapacityMB BIGINT NULL
failedRawCapacityMB BIGINT NULL
memoryMB BIGINT NULL
cpuCount INT NULL
manageURL VARCHAR(255) NULL
family VARCHAR(255) NULL
active TINYINT(1) NULL
dataCenter VARCHAR(255) NOT NULL
isVirtual TINYINT(1) NULL
cluster TINYINT(1) NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
iscsi_logical
Column
id INT NOT NULL
hostId INT NOT NULL
storageId INT NOT NULL
volumeId INT NOT NULL
numberOfSessions INT NOT NULL
numberOfConnections INT NOT NULL
Represents a scsci logical path between a host and a volume.
generic_device
Column
id INT NOT NULL
wwn VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
manufacturer VARCHAR(255) NULL
model VARCHAR(255) NULL
firmware VARCHAR(255) NULL
driver VARCHAR(255) NULL
serialNumber VARCHAR(255) NULL
Unidentified node, may be a HBA, storage or tape controller.
logical
Column
id INT NOT NULL
hostId INT NULL
genericDeviceId INT NULL
storageId INT NULL
tapeId INT NULL
volumeId INT NULL
minHopNumber INT NULL
hopsToDisplay VARCHAR(255) NULL
numberOfFabrics INT NULL
numberOfHostPorts INT NULL
numberOfStoragePorts INT NULL
spf TINYINT NULL
Represents a logical path between a host and a volume.
volume
Column
id INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NULL
qtreeId INT NULL
name VARCHAR(255) NULL
label VARCHAR(255) NULL
thinProvisioned TINYINT(1) NOT NULL
capacityMB BIGINT NOT NULL
consumedCapacityMB BIGINT NOT NULL
rawCapacityMB BIGINT NOT NULL
type VARCHAR(255) NULL
replicaSource TINYINT(1) NULL
replicaTarget TINYINT(1) NULL
snapshot TINYINT(1) NULL
cylinders INT NULL
diskGroup VARCHAR(255) NULL
meta TINYINT(1) NULL
virtualStorage VARCHAR(255) NULL
head VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
autoTieringPolicyId INT NULL
autoTiering TINYINT(1) NOT NULL
lastKnownAccessTime DATETIME NULL
writtenCapacityMB BIGINT NULL
isVirtual TINYINT(1) NULL
technologyType ENUM NULL
uuid VARCHAR(255) NULL
isMainframe TINYINT(1) NOT NULL
url VARCHAR(255) NULL
tape
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
manufacturer VARCHAR(255) NULL
serialNumber VARCHAR(255) NULL
active TINYINT(1) NULL
unknown_logical
Column
id INT NOT NULL
hostId INT NOT NULL
storageId INT NOT NULL
volumeId INT NOT NULL
Represents a logical path between a host and a volume throug
violation
Column
id INT NOT NULL
hostId INT NULL
genericDeviceId INT NULL
storageId INT NULL
tapeId INT NULL
volumeId INT NULL
volumeName VARCHAR(255) NULL
type ENUM NOT NULL
technologyType ENUM NOT NULL
since DATETIME NOT NULL

ポート接続

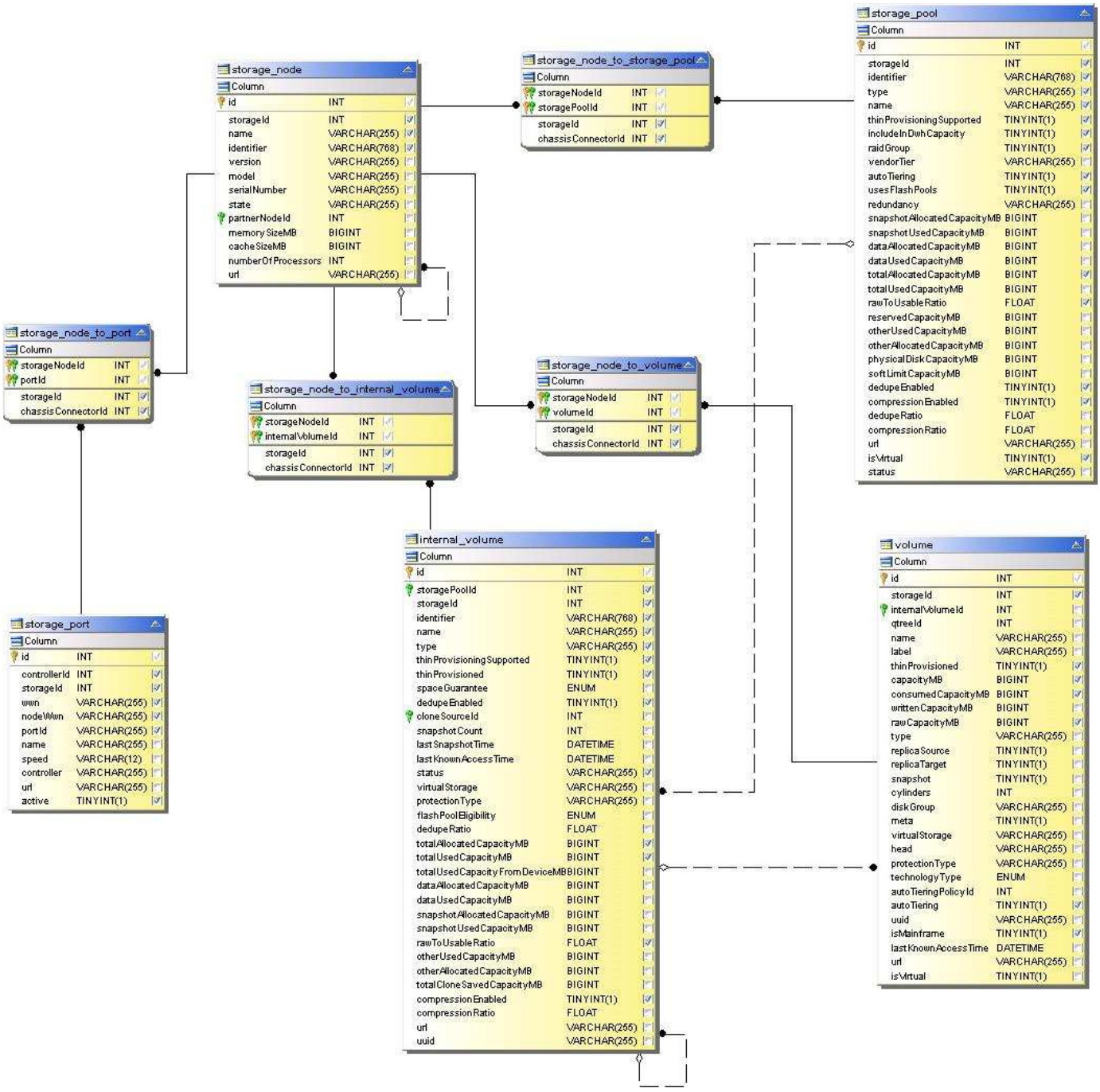

host
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
os VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
installedMemoryMB VARCHAR(255)
hostFsFreeGB VARCHAR(255)
hostFsTotalGB VARCHAR(255)
hostFsUsedGB VARCHAR(255)
cpuCount VARCHAR(255)
cpuSpeed VARCHAR(255)
nicCount VARCHAR(255)
nicSpeed VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
dataCenter VARCHAR(255)
host_adapter
Column
id INT
hostId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
host_port
Column
id INT
adapterId INT
hostId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
switch
Column
id INT
fabricId INT
identifier VARCHAR(768)
wwn VARCHAR(255)
ip VARCHAR(255)
name VARCHAR(255)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
vsanEnabled TINYINT(1)
serialNumber VARCHAR(255)
manageURL VARCHAR(255)
sanRouteEnabled TINYINT(1)
npv TINYINT(1)
type ENUM
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
switchLevel VARCHAR(255)
isGenerated TINYINT(1)
storage
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
rawCapacityMB BIGINT
spareRawCapacityMB BIGINT
failedRawCapacityMB BIGINT
memoryMB BIGINT
cpuCount INT
manageURL VARCHAR(255)
family VARCHAR(255)
cluster TINYINT(1)
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
isVirtual TINYINT(1)
storage_controller
Column
id INT
storageId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
storage_port
Column
id INT
controllerId INT
storageId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
switch_port
Column
id INT
switchId INT
fabricId INT
virtualSwitchId INT
wwn VARCHAR(255)
status VARCHAR(100)
rawPortStatus VARCHAR(255)
type VARCHAR(255)
portPhysicalState VARCHAR(255)
number BIGINT
blade BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
fc4Protocol VARCHAR(255)
classOfService VARCHAR(255)
gbicType VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
isGenerated TINYINT(1)
tape
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
active TINYINT(1)
tape_controller
Column
id INT
tapeId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
tape_port
Column
id INT
controllerId INT
tapeId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
virtual_switch
Column
id INT
fabricId INT
wwn VARCHAR(255)
ip VARCHAR(255)
name VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
switchRole VARCHAR(255)
chassisWwn VARCHAR(255)
npv TINYINT(1)
generated TINYINT(1)
type ENUM
isGenerated TINYINT(1)
port_connectivity
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedId INT
connectedType ENUM
connectedWwn VARCHAR(255)
generic_device
Column
id INT
wwn VARCHAR(255)
identifier VARCHAR(768)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
driver VARCHAR(255)
serialNumber VARCHAR(255)
generic_device_port
Column
id INT
genericDeviceId INT
wwn VARCHAR(255)
number BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
fc_name_server_entry
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedSwitchPortId INT
connectedSwitchPortWwn VARCHAR(255)
physicalPortWwn VARCHAR(255)
fcId VARCHAR(255)

SAN ファブリック

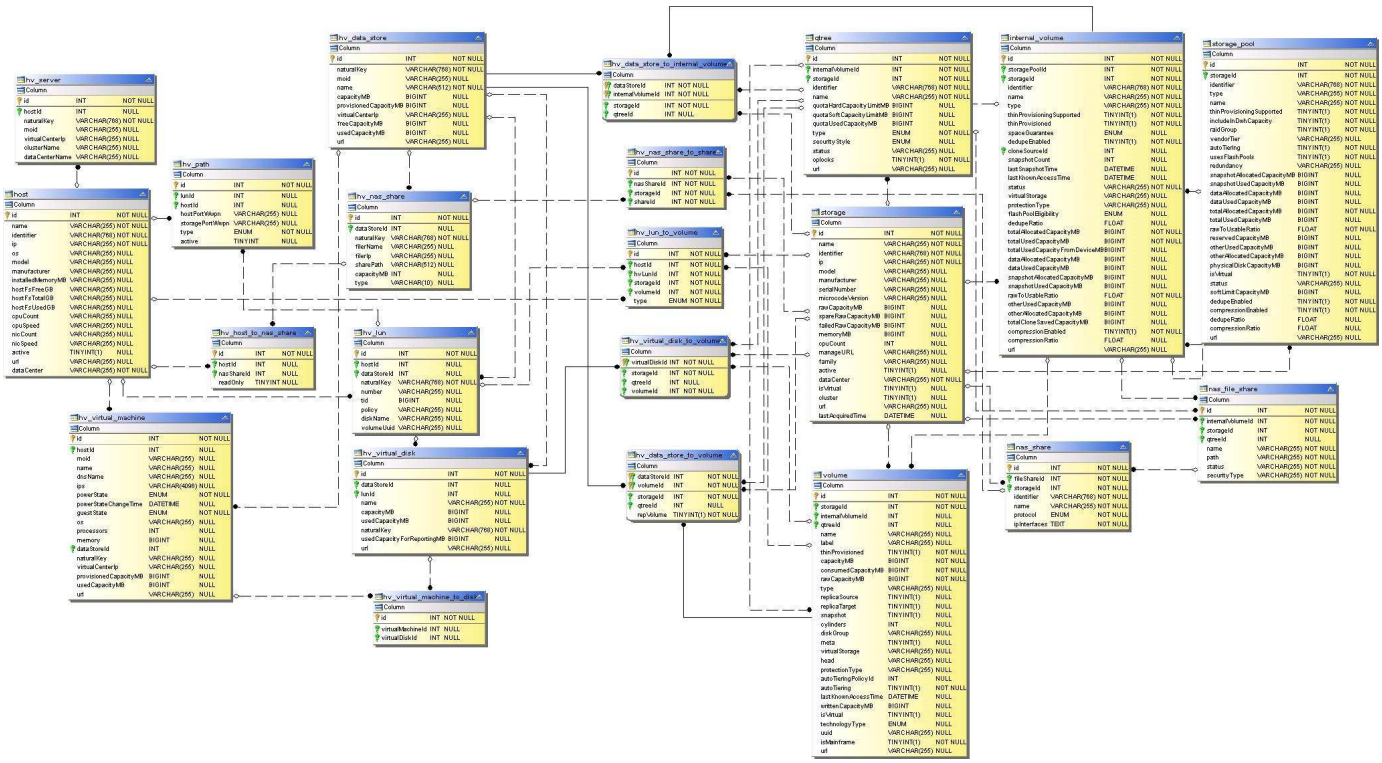

zone_member
Column
id INT NOT NULL
zoneId INT NOT NULL
fabricId INT NOT NULL
type ENUM NOT NULL
wwn VARCHAR(255) NOT NULL
zoneName VARCHAR(255) NOT NULL
Zone Members info.
zone
Column
id INT NOT NULL
fabricId INT NOT NULL
name VARCHAR(255) NOT NULL
fabricWwn VARCHAR(255) NOT NULL
configurationname VARCHAR(255) NOT NULL
Zone and Zone Capabilities info.
fabric
Column
id INT NOT NULL
wwn VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
VSANEnabled TINYINT(1) NOT NULL
VSANId VARCHAR(255) NULL
zoningEnabled TINYINT(1) NOT NULL
identifier VARCHAR(768) NOT NULL
url VARCHAR(255) NULL
virtual_switch
Column
id INT NOT NULL
fabricId INT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
SwitchRole VARCHAR(255) NULL
ChassisWWN VARCHAR(255) NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL
switch
Column
id INT NOT NULL
fabricId INT NULL
identifier VARCHAR(768) NOT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
Manufacturer VARCHAR(255) NULL
Model VARCHAR(255) NULL
Firmware VARCHAR(255) NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
VSANEnabled TINYINT(1) NULL
SerialNumber VARCHAR(255) NULL
ManageURL VARCHAR(255) NULL
SANRouteEnabled TINYINT NOT NULL
active TINYINT(1) NOT NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
dataCenter VARCHAR(255) NOT NULL
switchLevel VARCHAR(255) NOT NULL


disk
storage_pool
dr_volume_replica
storage_pool_to_backend_lun
volume_in_storage_pool
storage_pool_to_disk
volume_map
dr_internal_volume_replica
storage
volume_mask
quota
volume
backend_lun_to_volume
internal_volume
backend_lun
auto_tiering_policy_constraint
backend_path
auto_tiering_policy
qtree
dr_qtree_replica
virtual_to_backend_volume

ストレージノード


storage_node
Column
id INT
storageId INT
name VARCHAR(255)
identifier VARCHAR(768)
version VARCHAR(255)
model VARCHAR(255)
serialNumber VARCHAR(255)
state VARCHAR(255)
partnerNodeId INT
memorySizeMB BIGINT
cacheSizeMB BIGINT
numberOfProcessors INT
url VARCHAR(255)
storage_node_to_storage_pool
Column
storageNodeId INT
storagePoolId INT
storageId INT
chassisConnectorId INT
storage_pool
Column
id INT
storageId INT
identifier VARCHAR(768)
type VARCHAR(255)
name VARCHAR(255)
thinProvisioningSupported TINYINT(1)
includeInDwhCapacity TINYINT(1)
raidGroup TINYINT(1)
vendorTier VARCHAR(255)
autoTiering TINYINT(1)
usesFlashPools TINYINT(1)
redundancy VARCHAR(255)
snapshotAllocatedCapacityMB BIGINT
snapshotUsedCapacityMB BIGINT
dataAllocatedCapacityMB BIGINT
dataUsedCapacityMB BIGINT
totalAllocatedCapacityMB BIGINT
totalUsedCapacityMB BIGINT
rawToUsableRatio FLOAT
reservedCapacityMB BIGINT
otherUsedCapacityMB BIGINT
otherAllocatedCapacityMB BIGINT
physicalDiskCapacityMB BIGINT
softLimitCapacityMB BIGINT
dedupeEnabled TINYINT(1)
compressionEnabled TINYINT(1)
dedupeRatio FLOAT
compressionRatio FLOAT
url VARCHAR(255)
isVirtual TINYINT(1)
status VARCHAR(255)
storage_node_to_port
Column
storageNodeId INT
portId INT
storageId INT
chassisConnectorId INT
storage_node_to_internal_volume
Column
storageNodeId INT
internalVolumeId INT
storageId INT
chassisConnectorId INT
storage_node_to_volume
Column
storageNodeId INT
volumeId INT
storageId INT
chassisConnectorId INT
internal_volume
Column
id INT
storagePoolId INT
storageId INT
identifier VARCHAR(768)
name VARCHAR(255)
type VARCHAR(255)
thinProvisioningSupported TINYINT(1)
thinProvisioned TINYINT(1)
spaceGuarantee ENUM
dedupeEnabled TINYINT(1)
cloneSourceId INT
snapshotCount INT
lastSnapshotTime DATETIME
lastKnownAccessTime DATETIME
status VARCHAR(255)
virtualStorage VARCHAR(255)
protectionType VARCHAR(255)
flashPoolEligibility ENUM
dedupeRatio FLOAT
totalAllocatedCapacityMB BIGINT
totalUsedCapacityMB BIGINT
totalUsedCapacityFromDeviceMB BIGINT
dataAllocatedCapacityMB BIGINT
dataUsedCapacityMB BIGINT
snapshotAllocatedCapacityMB BIGINT
snapshotUsedCapacityMB BIGINT
rawToUsableRatio FLOAT
otherUsedCapacityMB BIGINT
otherAllocatedCapacityMB BIGINT
totalCloneSavedCapacityMB BIGINT
compressionEnabled TINYINT(1)
compressionRatio FLOAT
url VARCHAR(255)
uuid VARCHAR(255)
volume
Column
id INT
storageId INT
internalVolumeId INT
qtreeId INT
name VARCHAR(255)
label VARCHAR(255)
thinProvisioned TINYINT(1)
capacityMB BIGINT
consumedCapacityMB BIGINT
writtenCapacityMB BIGINT
rawCapacityMB BIGINT
type VARCHAR(255)
replicaSource TINYINT(1)
replicaTarget TINYINT(1)
snapshot TINYINT(1)
cylinders INT
diskGroup VARCHAR(255)
meta TINYINT(1)
virtualStorage VARCHAR(255)
head VARCHAR(255)
protectionType VARCHAR(255)
technologyType ENUM
autoTieringPolicyId INT
autoTiering TINYINT(1)
uuid VARCHAR(255)
isMainframe TINYINT(1)
lastKnownAccessTime DATETIME
url VARCHAR(255)
isVirtual TINYINT(1)
storage_port
Column
id INT
controllerId INT
storageId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)

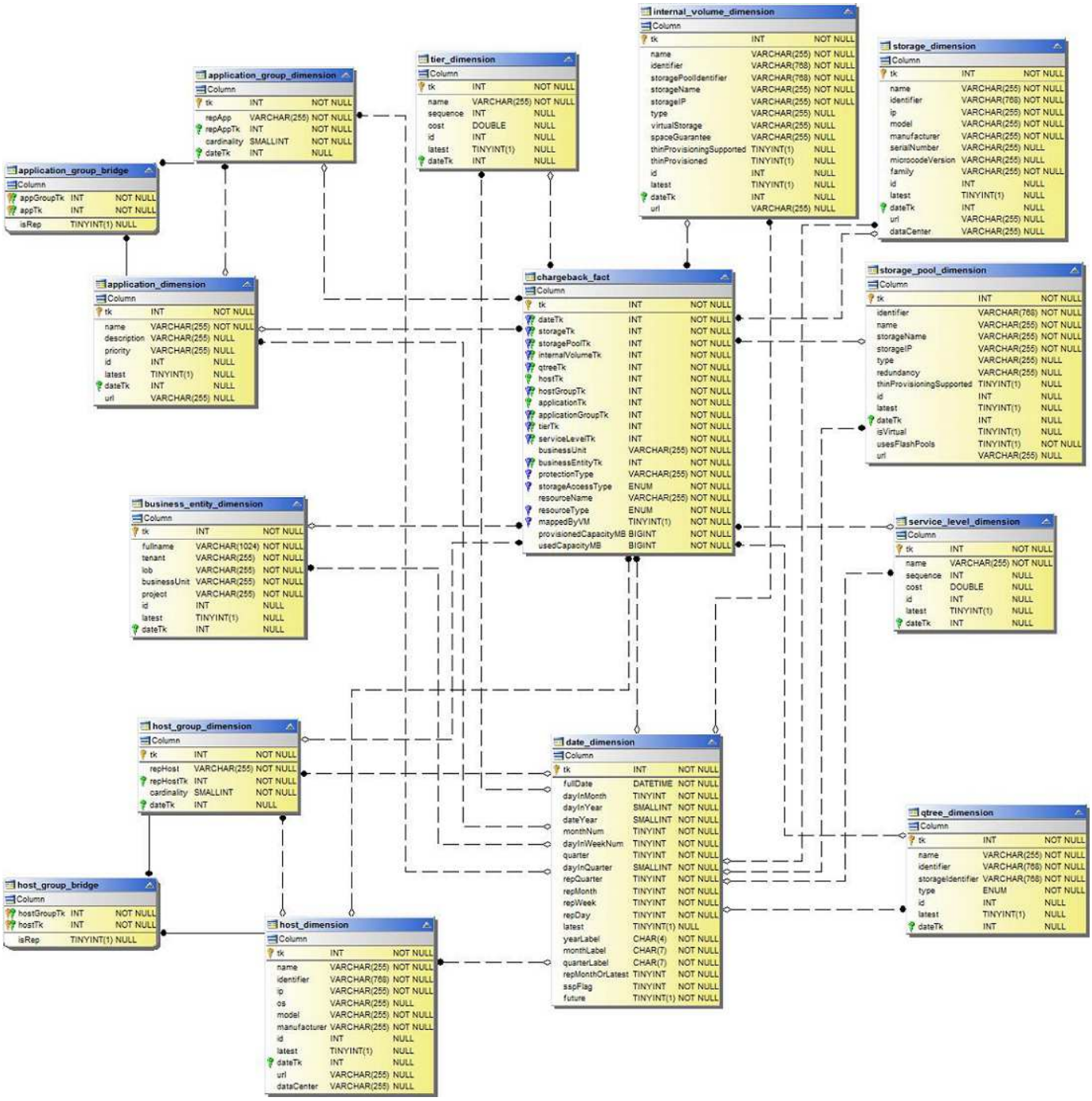
VM



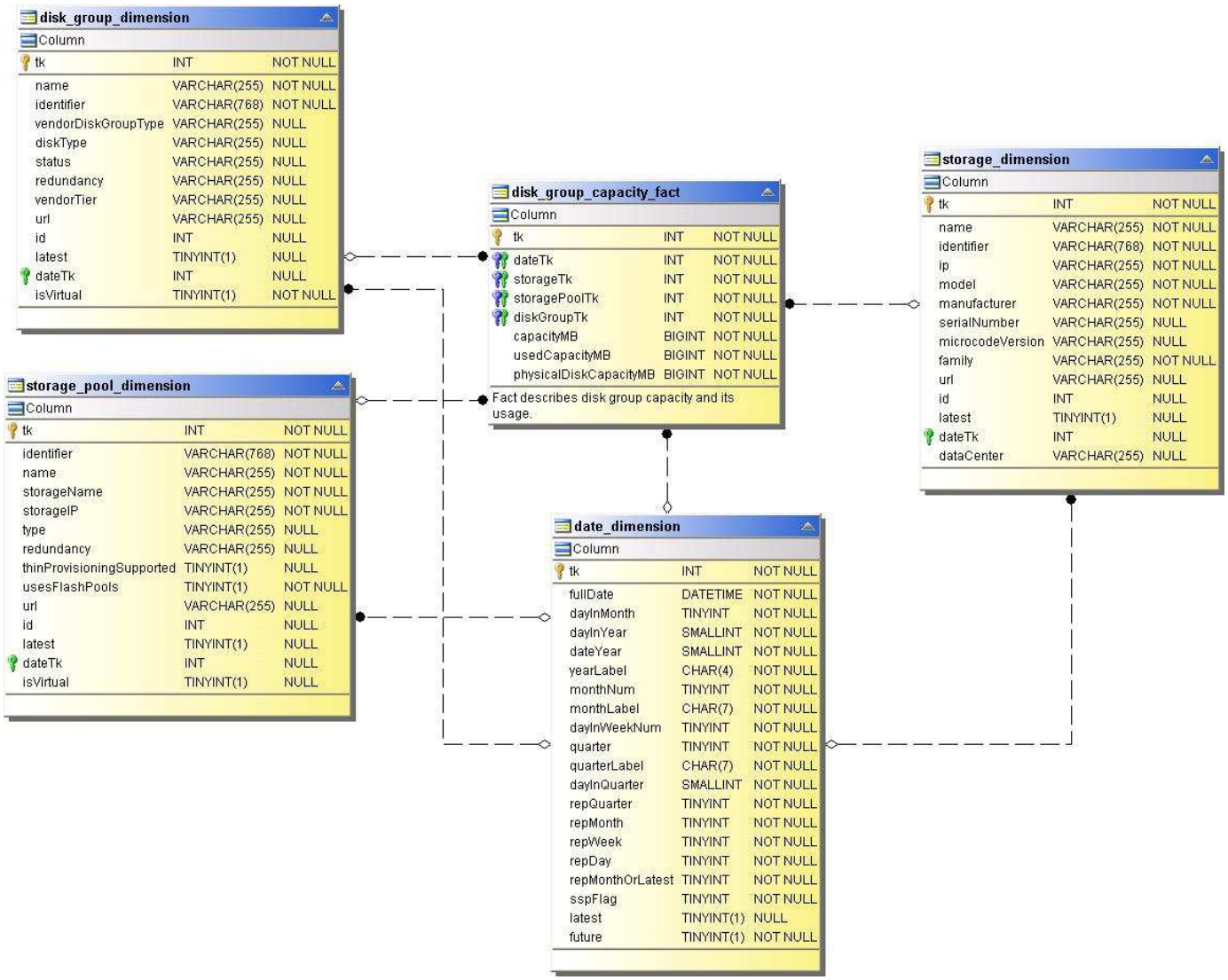
Capacity Datamartの略

次の図は、容量データマートを示しています。

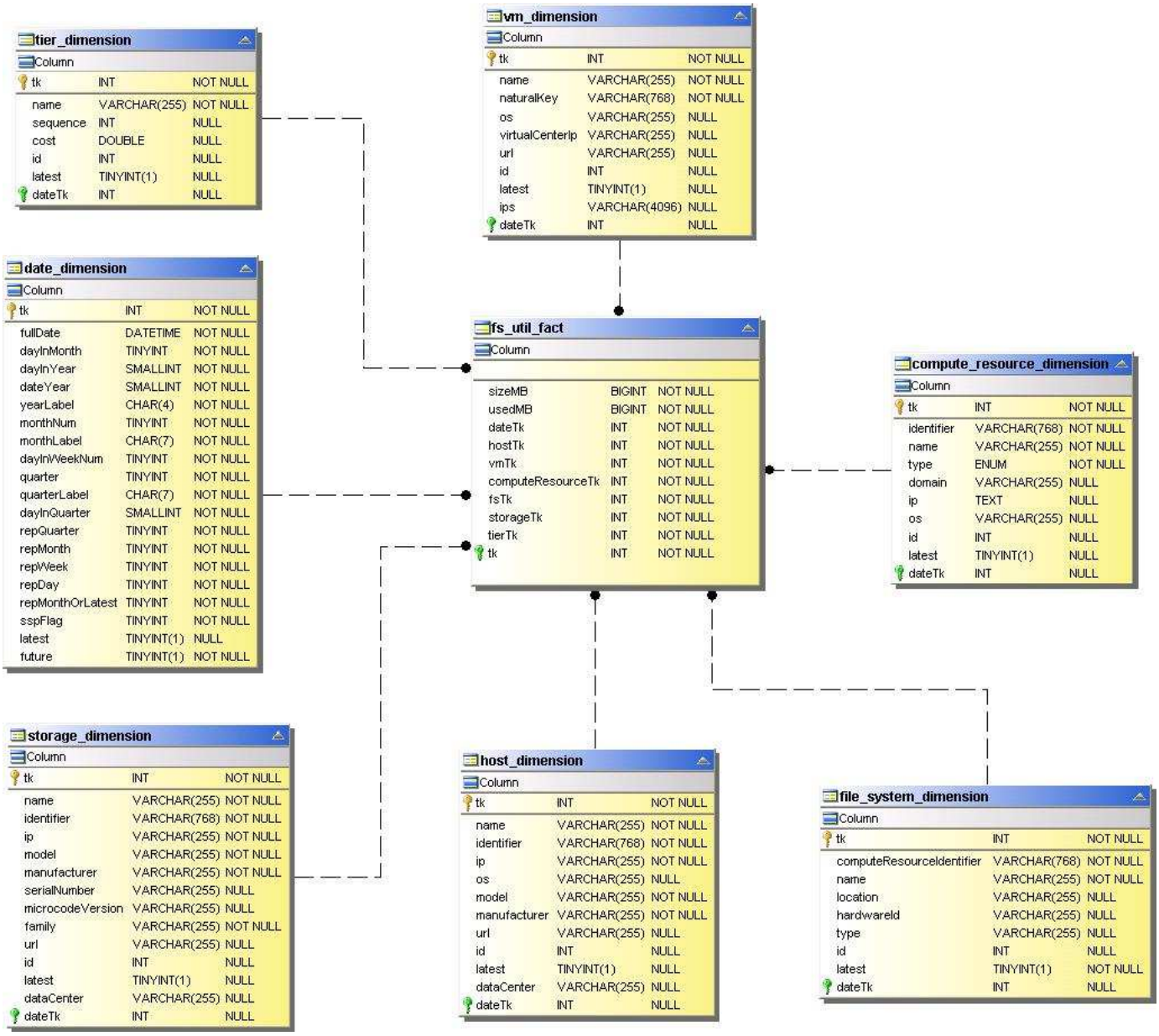
チャージバック



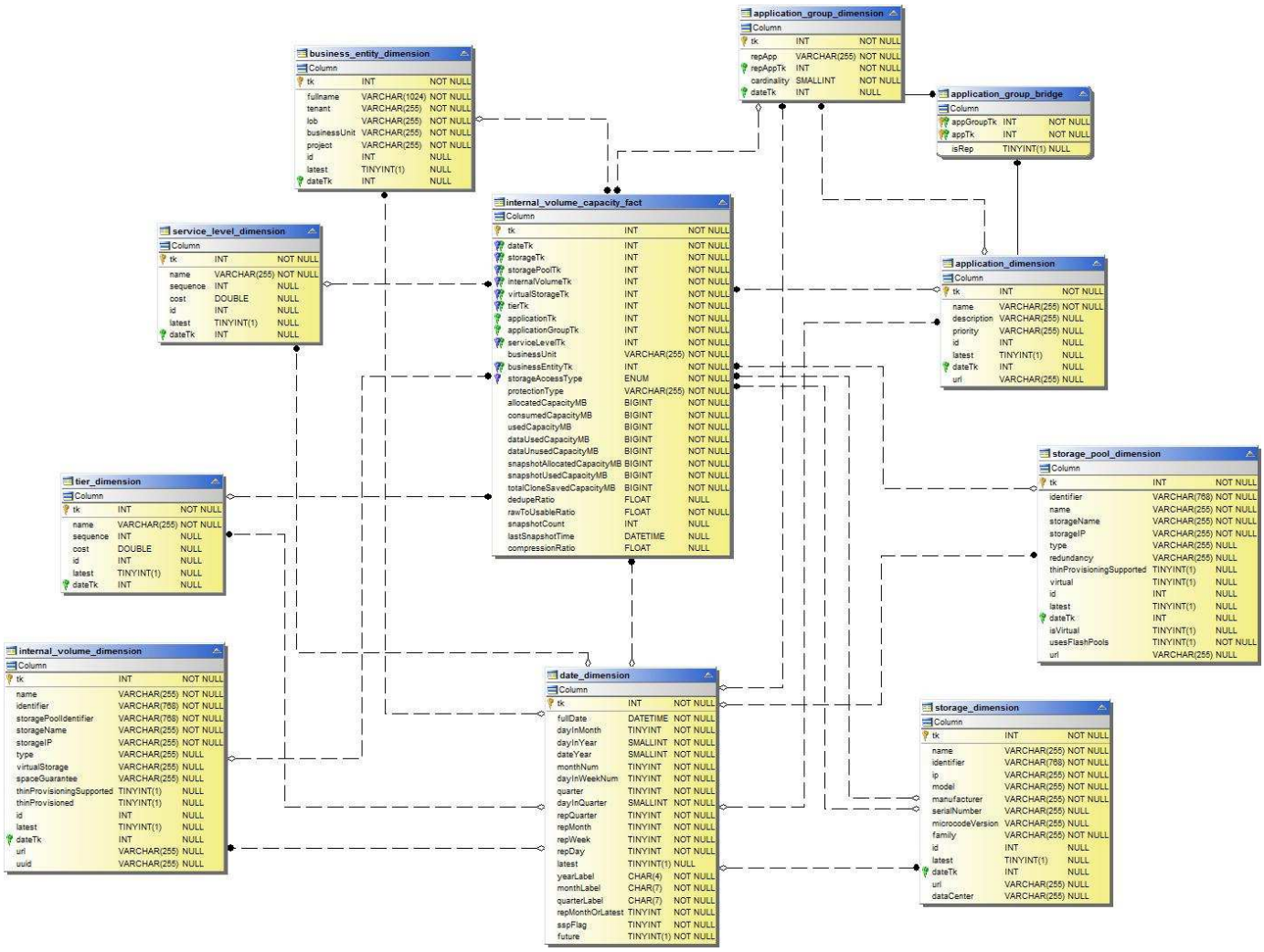
ディスクグループの容量



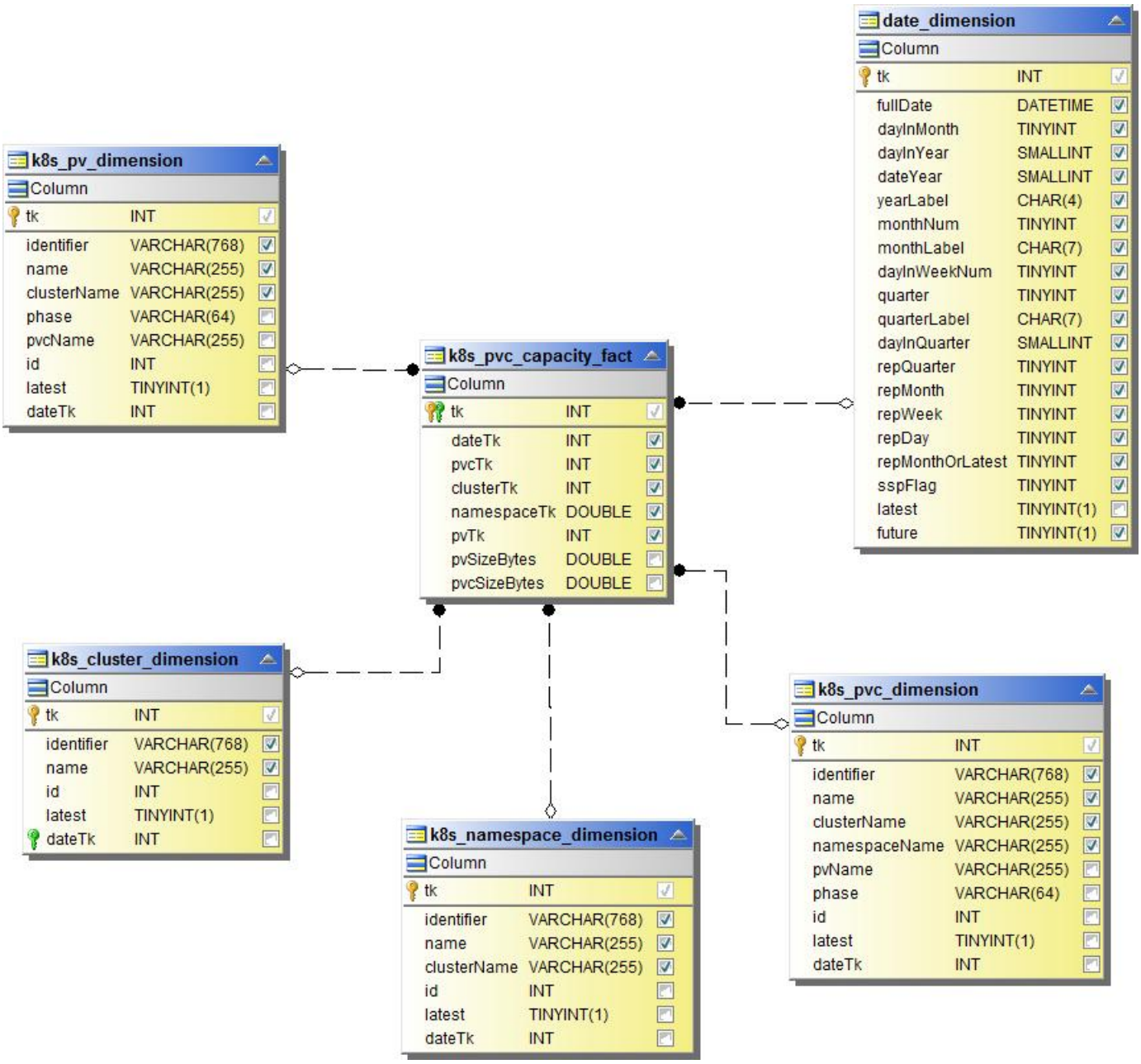
ファイルシステムの利用率


tier_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
sequence INT NULL
cost DOUBLE NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
vm_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
naturalKey VARCHAR(768) NOT NULL
os VARCHAR(255) NULL
virtualCenterIp VARCHAR(255) NULL
url VARCHAR(255) NULL
id INT NULL
latest TINYINT(1) NULL
ips VARCHAR(4096) NULL
dateTk INT NULL
date_dimension
Column
tk INT NOT NULL
fullDate DATETIME NOT NULL
dayInMonth TINYINT NOT NULL
dayInYear SMALLINT NOT NULL
dateYear SMALLINT NOT NULL
yearLabel CHAR(4) NOT NULL
monthNum TINYINT NOT NULL
monthLabel CHAR(7) NOT NULL
dayInWeekNum TINYINT NOT NULL
quarter TINYINT NOT NULL
quarterLabel CHAR(7) NOT NULL
dayInQuarter SMALLINT NOT NULL
repQuarter TINYINT NOT NULL
repMonth TINYINT NOT NULL
repWeek TINYINT NOT NULL
repDay TINYINT NOT NULL
repMonthOrLatest TINYINT NOT NULL
sspFlag TINYINT NOT NULL
latest TINYINT(1) NULL
future TINYINT(1) NOT NULL
fs_util_fact
Column
sizeMB BIGINT NOT NULL
usedMB BIGINT NOT NULL
dateTk INT NOT NULL
hostTk INT NOT NULL
vmTk INT NOT NULL
computeResourceTk INT NOT NULL
fsTk INT NOT NULL
storageTk INT NOT NULL
tierTk INT NOT NULL
tk INT NOT NULL
compute_resource_dimension
Column
tk INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type ENUM NOT NULL
domain VARCHAR(255) NULL
ip TEXT NULL
os VARCHAR(255) NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
storage_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
model VARCHAR(255) NOT NULL
manufacturer VARCHAR(255) NOT NULL
serialNumber VARCHAR(255) NULL
microcodeVersion VARCHAR(255) NULL
family VARCHAR(255) NOT NULL
url VARCHAR(255) NULL
id INT NULL
latest TINYINT(1) NULL
dataCenter VARCHAR(255) NULL
dateTk INT NULL
host_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
os VARCHAR(255) NULL
model VARCHAR(255) NOT NULL
manufacturer VARCHAR(255) NOT NULL
url VARCHAR(255) NULL
id INT NULL
latest TINYINT(1) NULL
dataCenter VARCHAR(255) NULL
dateTk INT NULL
file_system_dimension
Column
tk INT NOT NULL
computeResourceIdentifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
location VARCHAR(255) NULL
hardwareId VARCHAR(255) NULL
type VARCHAR(255) NULL
id INT NULL
latest TINYINT(1) NOT NULL
dateTk INT NULL

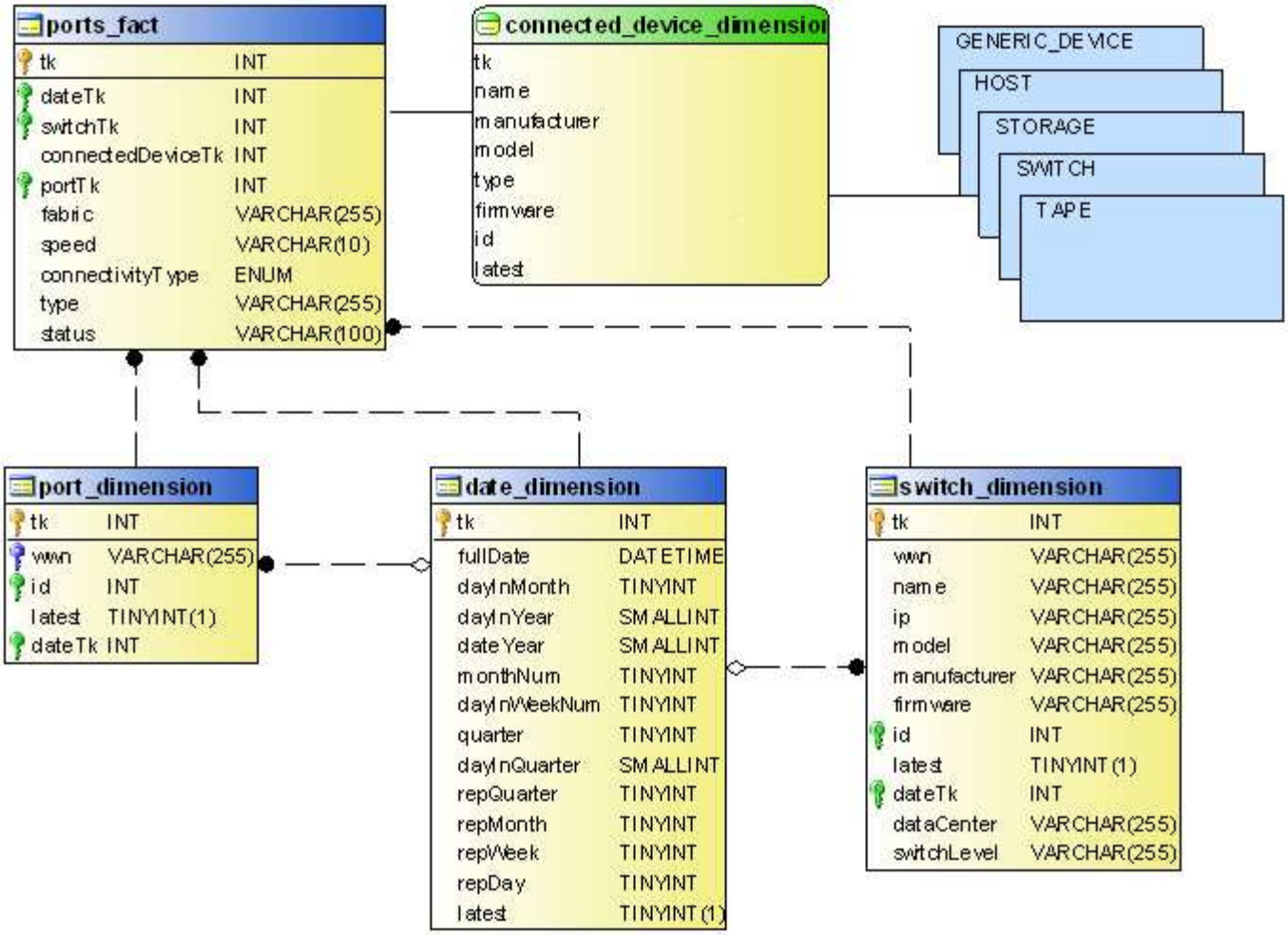
内部ボリューム容量



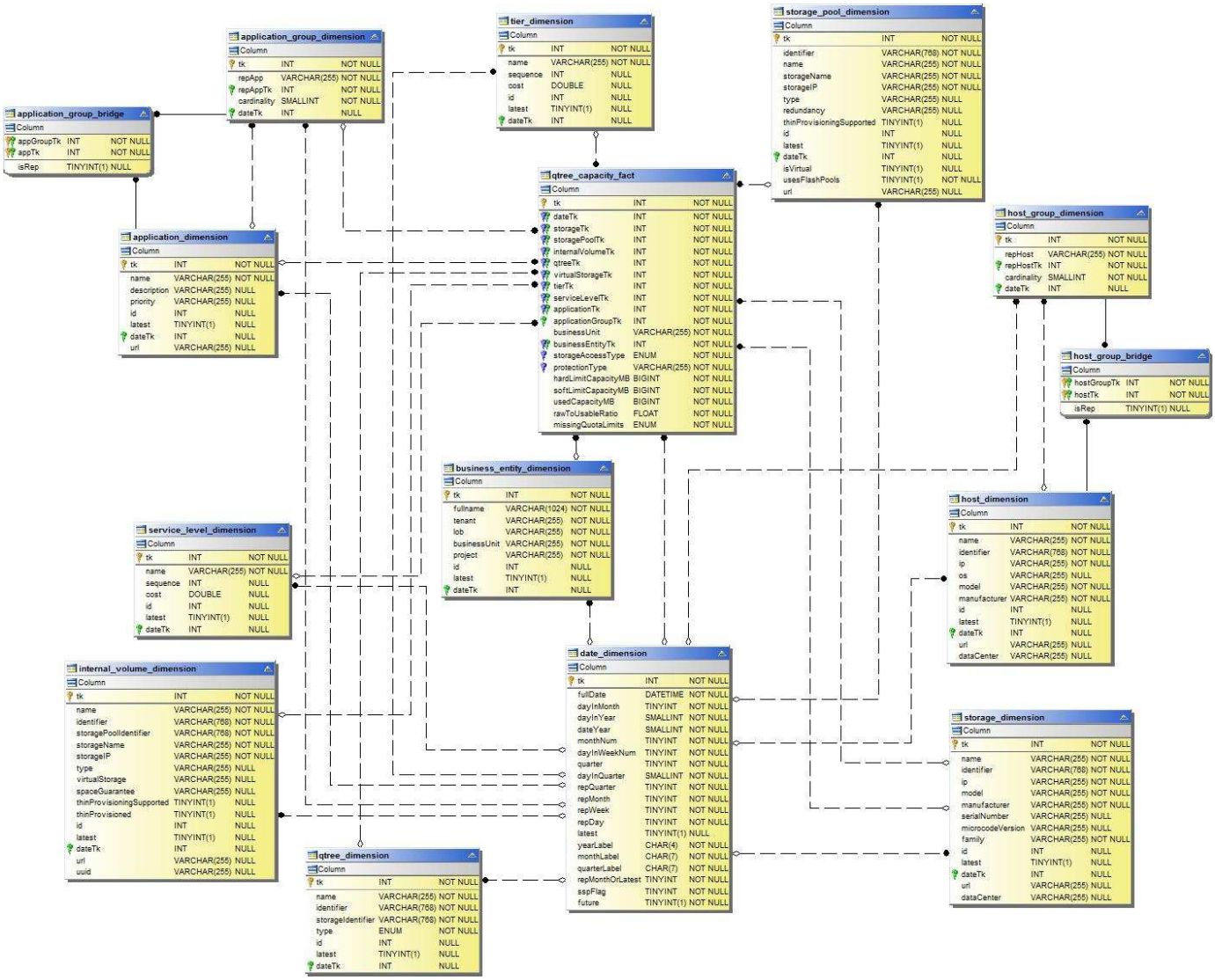
Kubernetes PVの容量


k8s_pv_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
phase VARCHAR(64)
pvcName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_pvc_capacity_fact
Column
tk INT
dateTk INT
pvcTk INT
clusterTk INT
namespaceTk DOUBLE
pvTk INT
pvSizeBytes DOUBLE
pvcSizeBytes DOUBLE
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
sspFlag TINYINT
latest TINYINT(1)
future TINYINT(1)
k8s_cluster_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_namespace_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_pvc_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
namespaceName VARCHAR(255)
pvName VARCHAR(255)
phase VARCHAR(64)
id INT
latest TINYINT(1)
dateTk INT

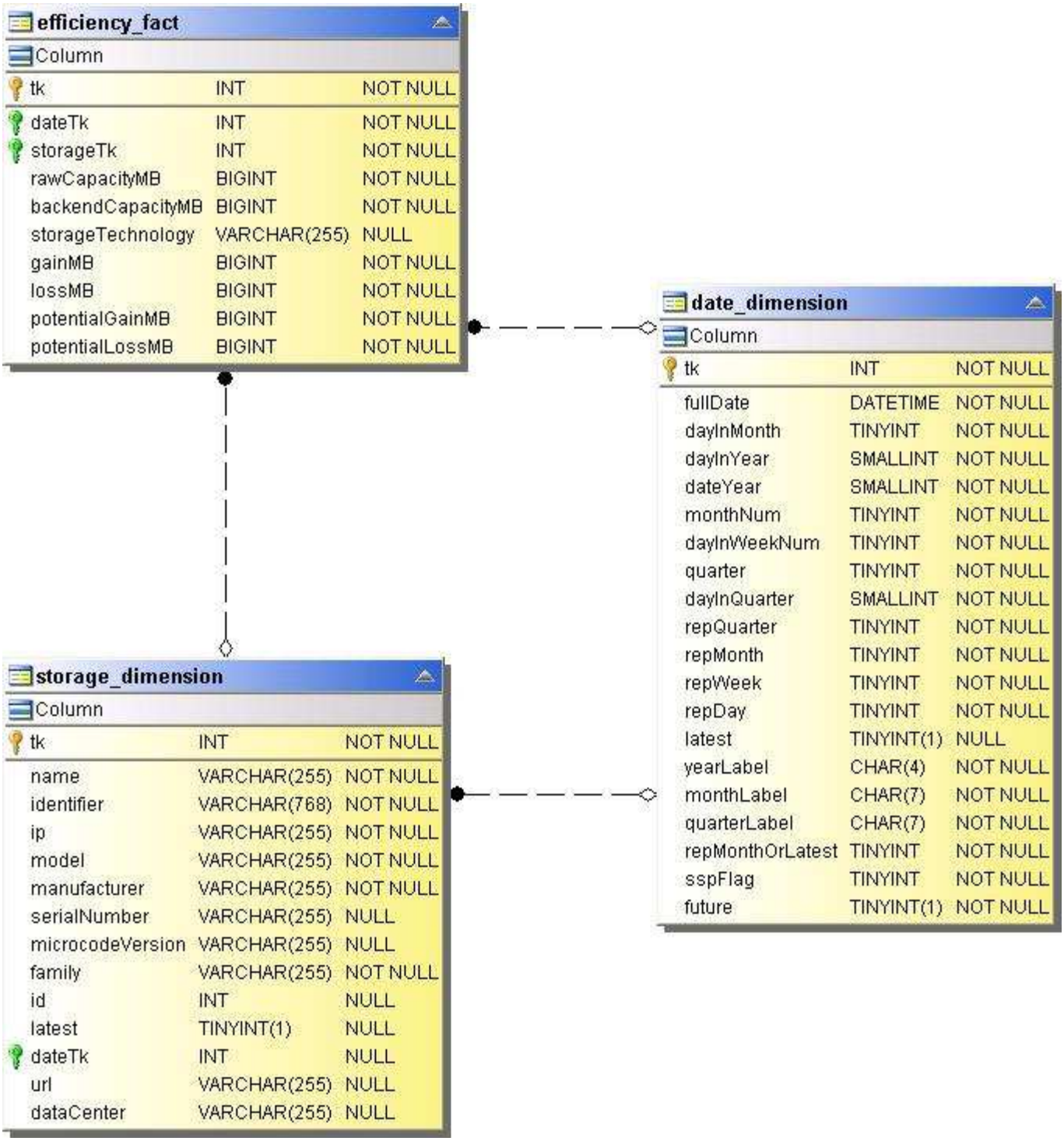
ポートの容量


ports_fact
tk INT
dateTk INT
switchTk INT
connectedDeviceTk INT
portTk INT
fabric VARCHAR(255)
speed VARCHAR(10)
connectivityType ENUM
type VARCHAR(255)
status VARCHAR(100)
connected_device_dimensio
tk
name
manufacturer
model
type
firmware
id
latest
GENERIC_DEVICE
HOST
STORAGE
SWITCH
TAPE
port_dimension
tk INT
wwn VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
date_dimension
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
monthNum TINYINT
dayInWeekNum TINYINT
quarter TINYINT
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
latest TINYINT(1)
switch_dimension
tk INT
wwn VARCHAR(255)
name VARCHAR(255)
ip VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
firmware VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
dataCenter VARCHAR(255)
switchLevel VARCHAR(255)

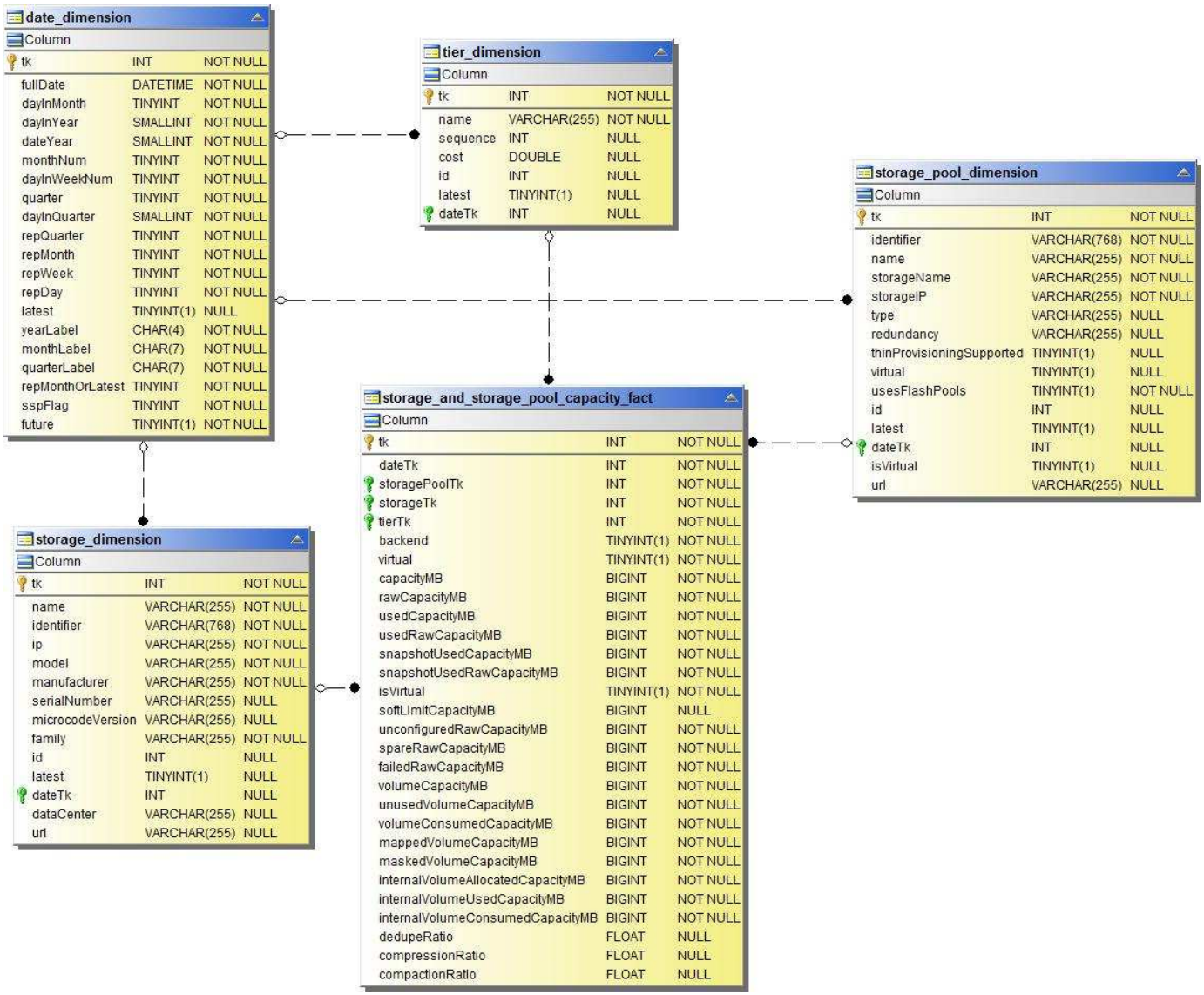
qtree 容量



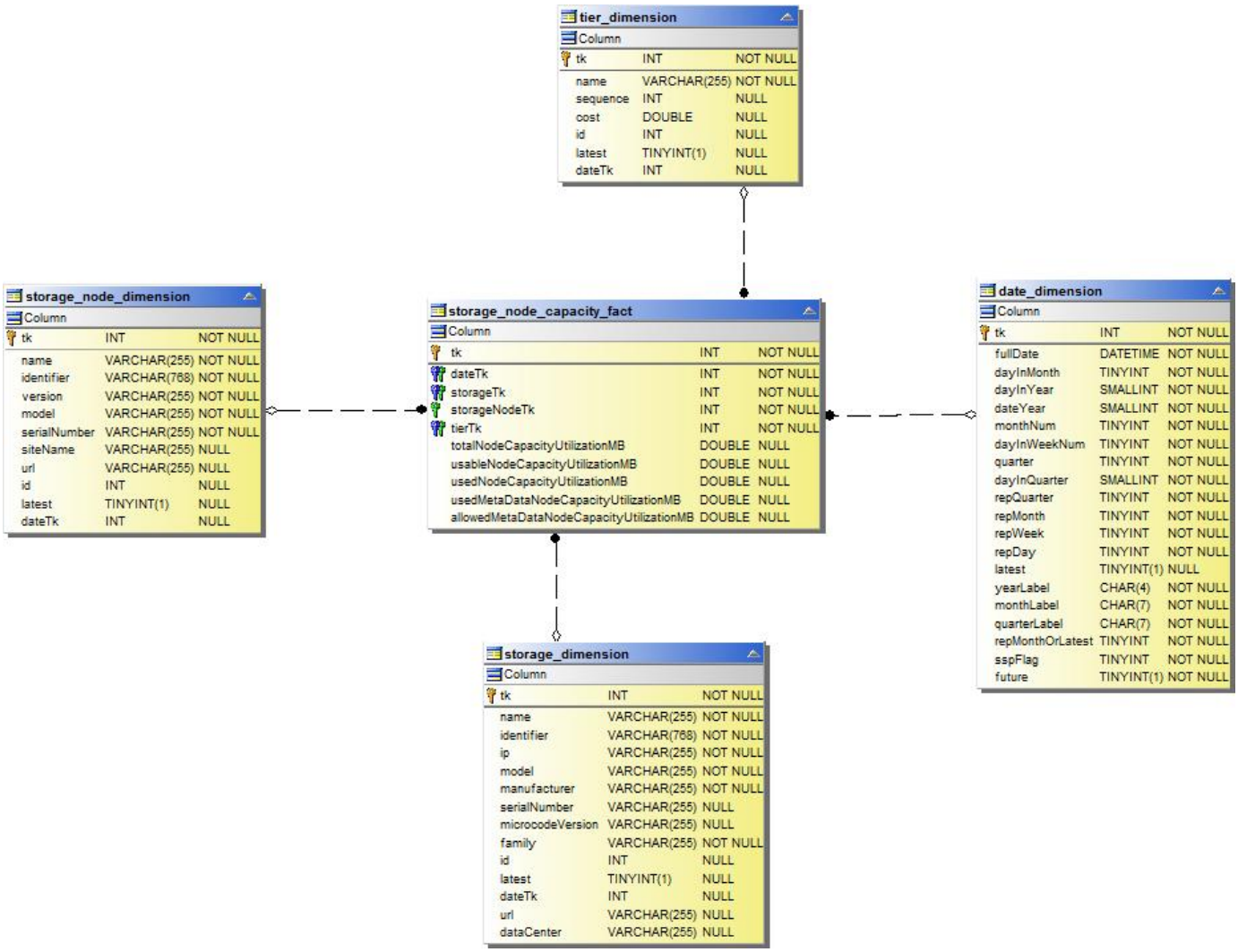
ストレージ容量の削減比率



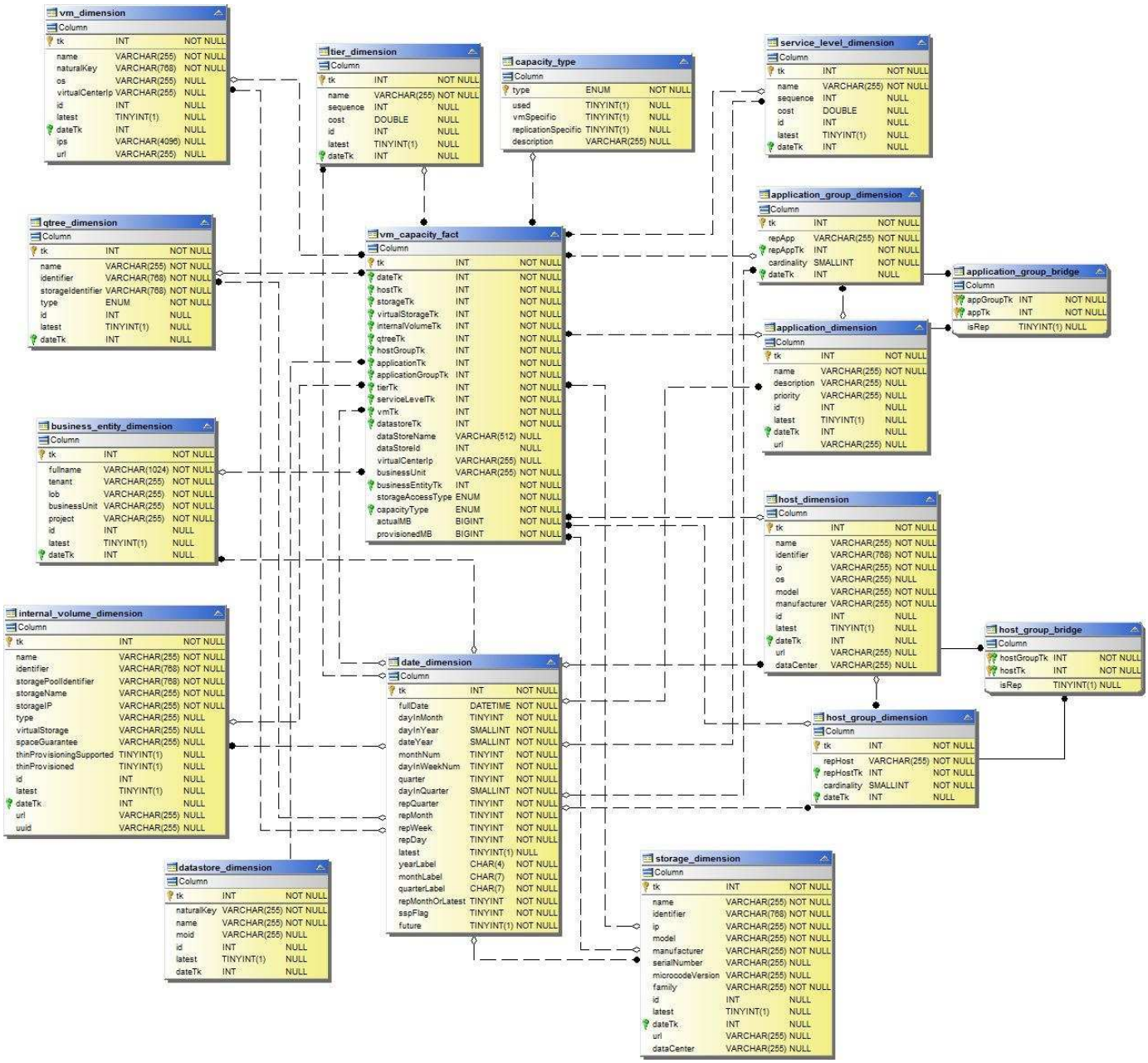
ストレージおよびストレージプールの容量



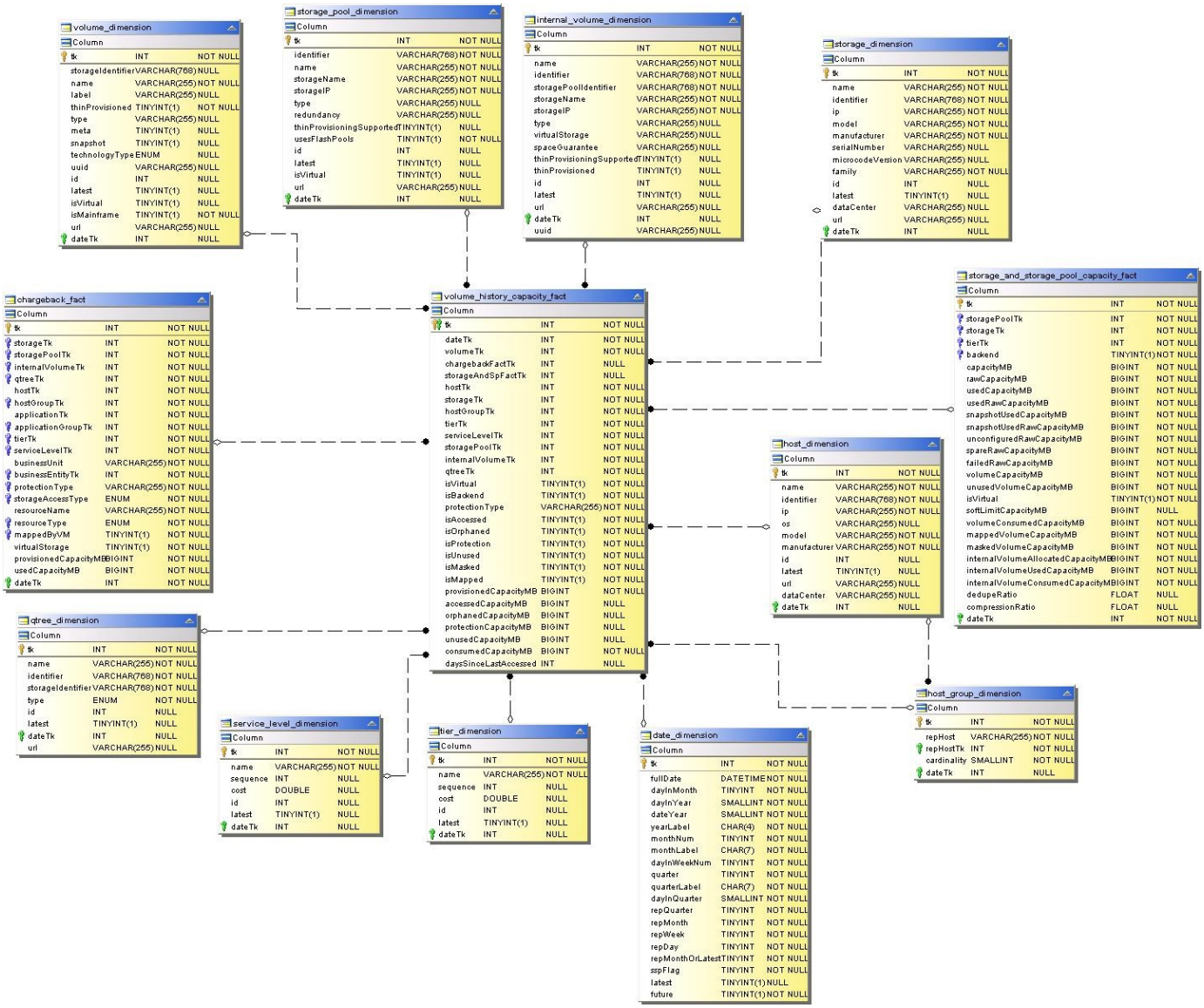
ストレージノードの容量


tier_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
sequence INT NULL
cost DOUBLE NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
storage_node_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
version VARCHAR(255) NOT NULL
model VARCHAR(255) NOT NULL
serialNumber VARCHAR(255) NOT NULL
siteName VARCHAR(255) NULL
url VARCHAR(255) NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
storage_node_capacity_fact
Column
tk INT NOT NULL
dateTk INT NOT NULL
storageTk INT NOT NULL
storageNodeTk INT NOT NULL
tierTk INT NOT NULL
totalNodeCapacityUtilizationMB DOUBLE NULL
usableNodeCapacityUtilizationMB DOUBLE NULL
usedNodeCapacityUtilizationMB DOUBLE NULL
usedMetaDataNodeCapacityUtilizationMB DOUBLE NULL
allowedMetaDataNodeCapacityUtilizationMB DOUBLE NULL
date_dimension
Column
tk INT NOT NULL
fullDate DATETIME NOT NULL
dayInMonth TINYINT NOT NULL
dayInYear SMALLINT NOT NULL
dateYear SMALLINT NOT NULL
monthNum TINYINT NOT NULL
dayInWeekNum TINYINT NOT NULL
quarter TINYINT NOT NULL
dayInQuarter SMALLINT NOT NULL
repQuarter TINYINT NOT NULL
repMonth TINYINT NOT NULL
repWeek TINYINT NOT NULL
repDay TINYINT NOT NULL
latest TINYINT(1) NULL
yearLabel CHAR(4) NOT NULL
monthLabel CHAR(7) NOT NULL
quarterLabel CHAR(7) NOT NULL
repMonthOrLatest TINYINT NOT NULL
sspFlag TINYINT NOT NULL
future TINYINT(1) NOT NULL
storage_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
model VARCHAR(255) NOT NULL
manufacturer VARCHAR(255) NOT NULL
serialNumber VARCHAR(255) NULL
microcodeVersion VARCHAR(255) NULL
family VARCHAR(255) NOT NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
url VARCHAR(255) NULL
dataCenter VARCHAR(255) NULL

VM 容量


vm_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
naturalKey VARCHAR(768) NOT NULL
os VARCHAR(255) NULL
virtualCenterIp VARCHAR(255) NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
ips VARCHAR(4096) NULL
url VARCHAR(255) NULL
tier_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
sequence INT NULL
cost DOUBLE NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
capacity_type
Column
type ENUM NOT NULL
used TINYINT(1) NULL
vmSpecific TINYINT(1) NULL
replicationSpecific TINYINT(1) NULL
description VARCHAR(255) NULL
service_level_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
sequence INT NULL
cost DOUBLE NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
application_group_dimension
Column
tk INT NOT NULL
repApp VARCHAR(255) NOT NULL
repAppTk INT NOT NULL
cardinality SMALLINT NOT NULL
dateTk INT NULL
application_group_bridge
Column
appGroupTk INT NOT NULL
appTk INT NOT NULL
isRep TINYINT(1) NULL
qtree_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
storageIdentifier VARCHAR(768) NOT NULL
type ENUM NOT NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
vm_capacity_fact
Column
tk INT NOT NULL
dateTk INT NOT NULL
hostTk INT NOT NULL
storageTk INT NOT NULL
virtualStorageTk INT NOT NULL
internalVolumeTk INT NOT NULL
qtreeTk INT NOT NULL
hostGroupTk INT NOT NULL
applicationTk INT NOT NULL
applicationGroupTk INT NOT NULL
tierTk INT NOT NULL
serviceLevelTk INT NOT NULL
vmTk INT NOT NULL
datastoreTk INT NOT NULL
dataStoreName VARCHAR(512) NULL
dataStoreId INT NULL
virtualCenterIp VARCHAR(255) NULL
businessUnit VARCHAR(255) NOT NULL
businessEntityTk INT NOT NULL
storageAccessType ENUM NOT NULL
capacityType ENUM NOT NULL
actualMB BIGINT NOT NULL
provisionedMB BIGINT NOT NULL
application_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
description VARCHAR(255) NULL
priority VARCHAR(255) NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
url VARCHAR(255) NULL
business_entity_dimension
Column
tk INT NOT NULL
fullname VARCHAR(1024) NOT NULL
tenant VARCHAR(255) NOT NULL
lob VARCHAR(255) NOT NULL
businessUnit VARCHAR(255) NOT NULL
project VARCHAR(255) NOT NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
host_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
os VARCHAR(255) NULL
model VARCHAR(255) NOT NULL
manufacturer VARCHAR(255) NOT NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
url VARCHAR(255) NULL
dataCenter VARCHAR(255) NULL
internal_volume_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
storagePoolIdentifier VARCHAR(768) NOT NULL
storageName VARCHAR(255) NOT NULL
storageIP VARCHAR(255) NOT NULL
type VARCHAR(255) NULL
virtualStorage VARCHAR(255) NULL
spaceGuarantee VARCHAR(255) NULL
thinProvisioningSupported TINYINT(1) NULL
thinProvisioned TINYINT(1) NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
url VARCHAR(255) NULL
uuid VARCHAR(255) NULL
date_dimension
Column
tk INT NOT NULL
fullDate DATETIME NOT NULL
dayInMonth TINYINT NOT NULL
dayInYear SMALLINT NOT NULL
dateYear SMALLINT NOT NULL
monthNum TINYINT NOT NULL
dayInWeekNum TINYINT NOT NULL
quarter TINYINT NOT NULL
dayInQuarter SMALLINT NOT NULL
repQuarter TINYINT NOT NULL
repMonth TINYINT NOT NULL
repWeek TINYINT NOT NULL
repDay TINYINT NOT NULL
latest TINYINT(1) NULL
yearLabel CHAR(4) NOT NULL
monthLabel CHAR(7) NOT NULL
quarterLabel CHAR(7) NOT NULL
repMonthOrLatest TINYINT NOT NULL
sspFlag TINYINT NOT NULL
future TINYINT(1) NOT NULL
host_group_bridge
Column
hostGroupTk INT NOT NULL
hostTk INT NOT NULL
isRep TINYINT(1) NULL
host_group_dimension
Column
tk INT NOT NULL
repHost VARCHAR(255) NOT NULL
repHostTk INT NOT NULL
cardinality SMALLINT NOT NULL
dateTk INT NULL
datastore_dimension
Column
tk INT NOT NULL
naturalKey VARCHAR(255) NOT NULL
name VARCHAR(255) NOT NULL
moid VARCHAR(255) NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
storage_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
model VARCHAR(255) NOT NULL
manufacturer VARCHAR(255) NOT NULL
serialNumber VARCHAR(255) NULL
microcodeVersion VARCHAR(255) NULL
family VARCHAR(255) NOT NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
url VARCHAR(255) NULL
dataCenter VARCHAR(255) NULL

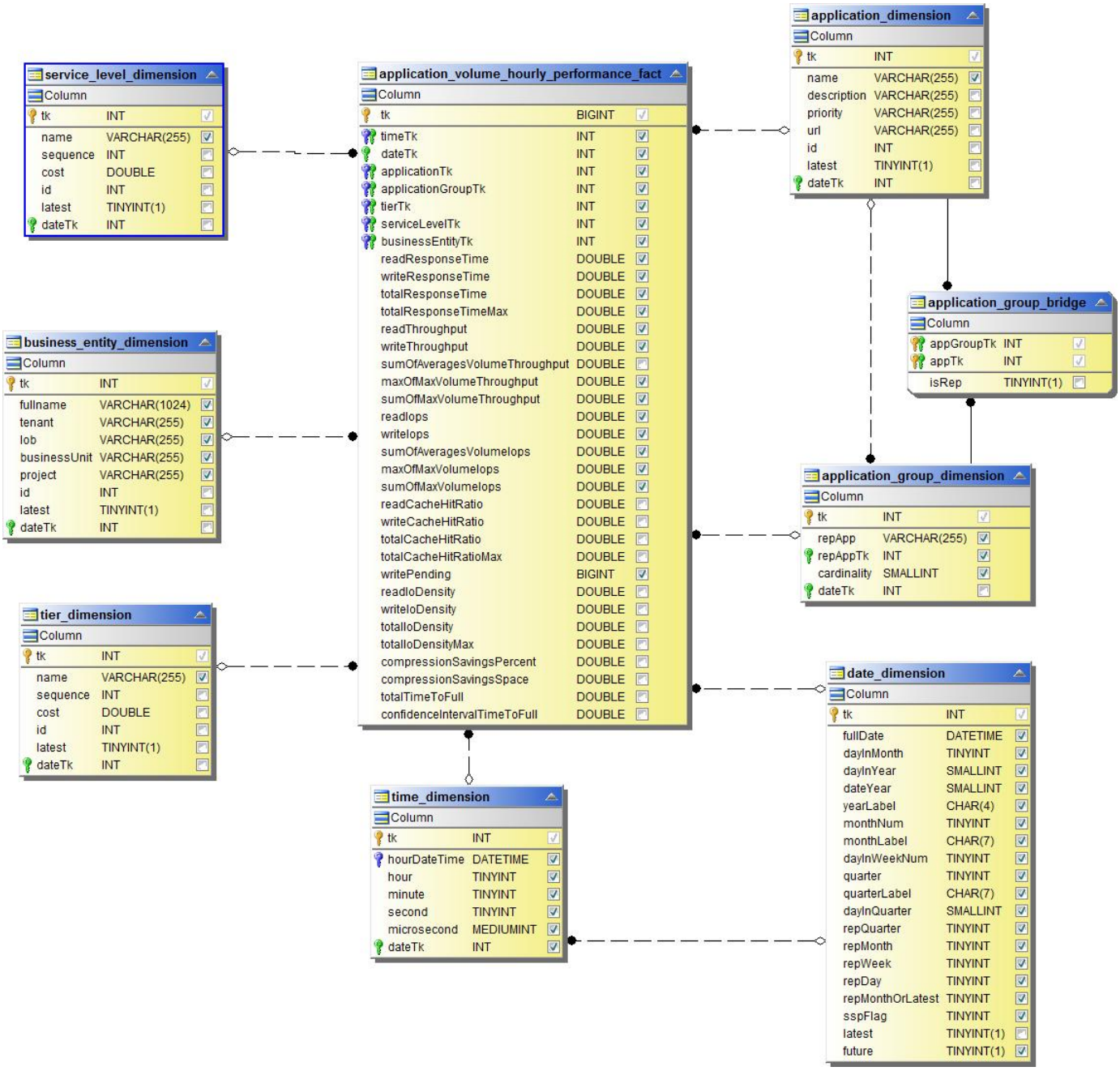
ボリューム容量



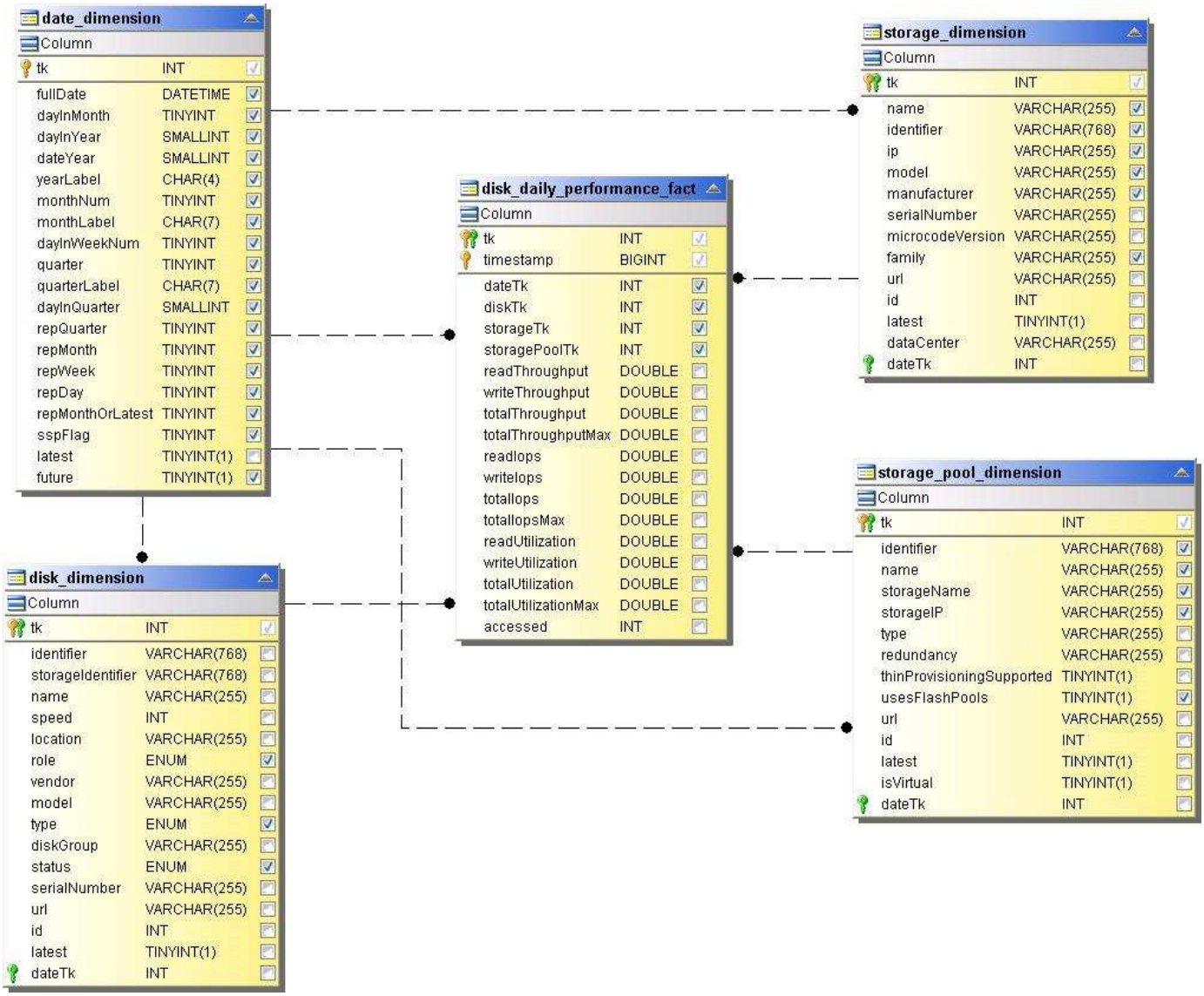
パフォーマンスデータマート

次の図は、パフォーマンスデータマートを説明しています。

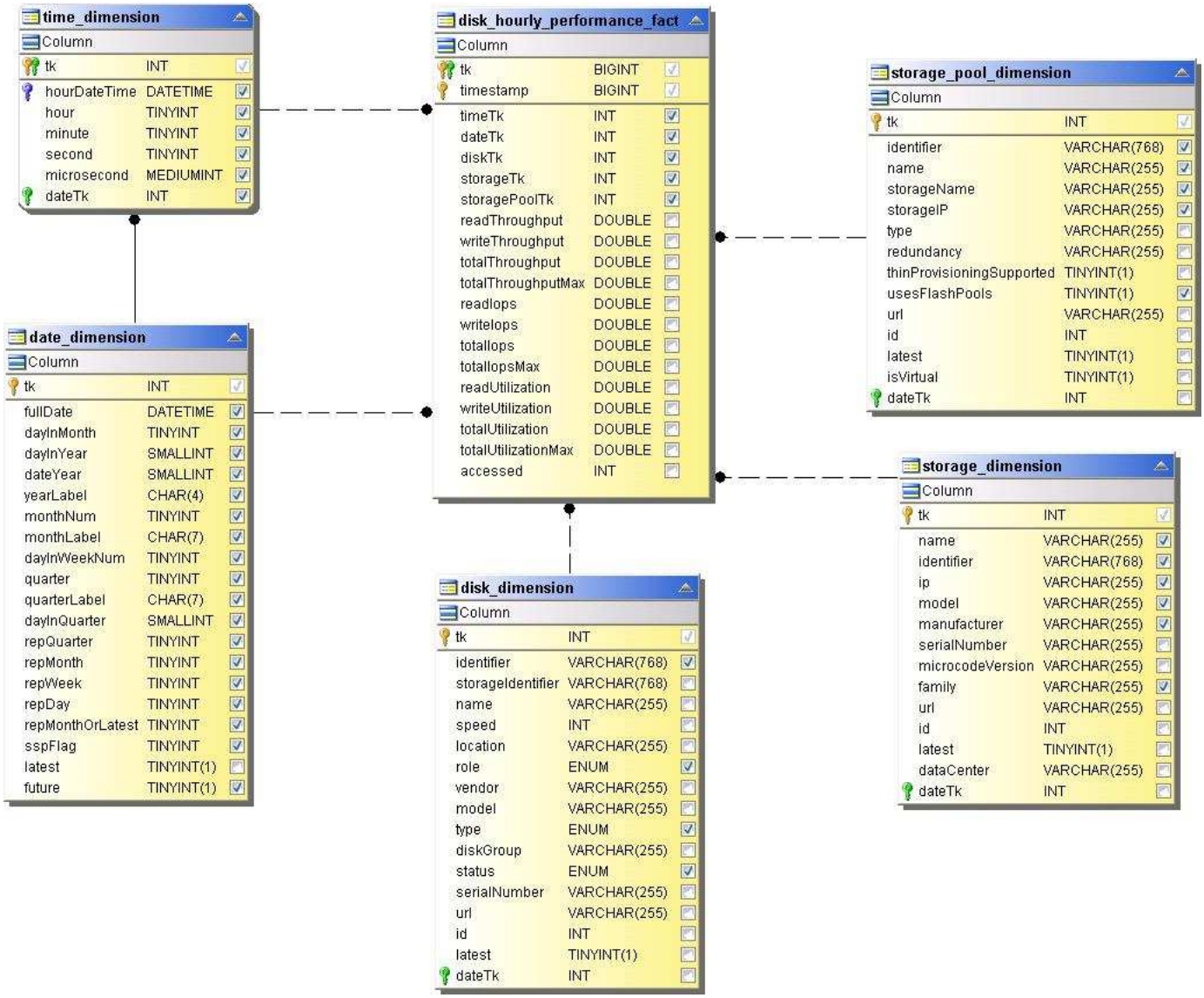
アプリケーションボリューム毎時パフォーマンス



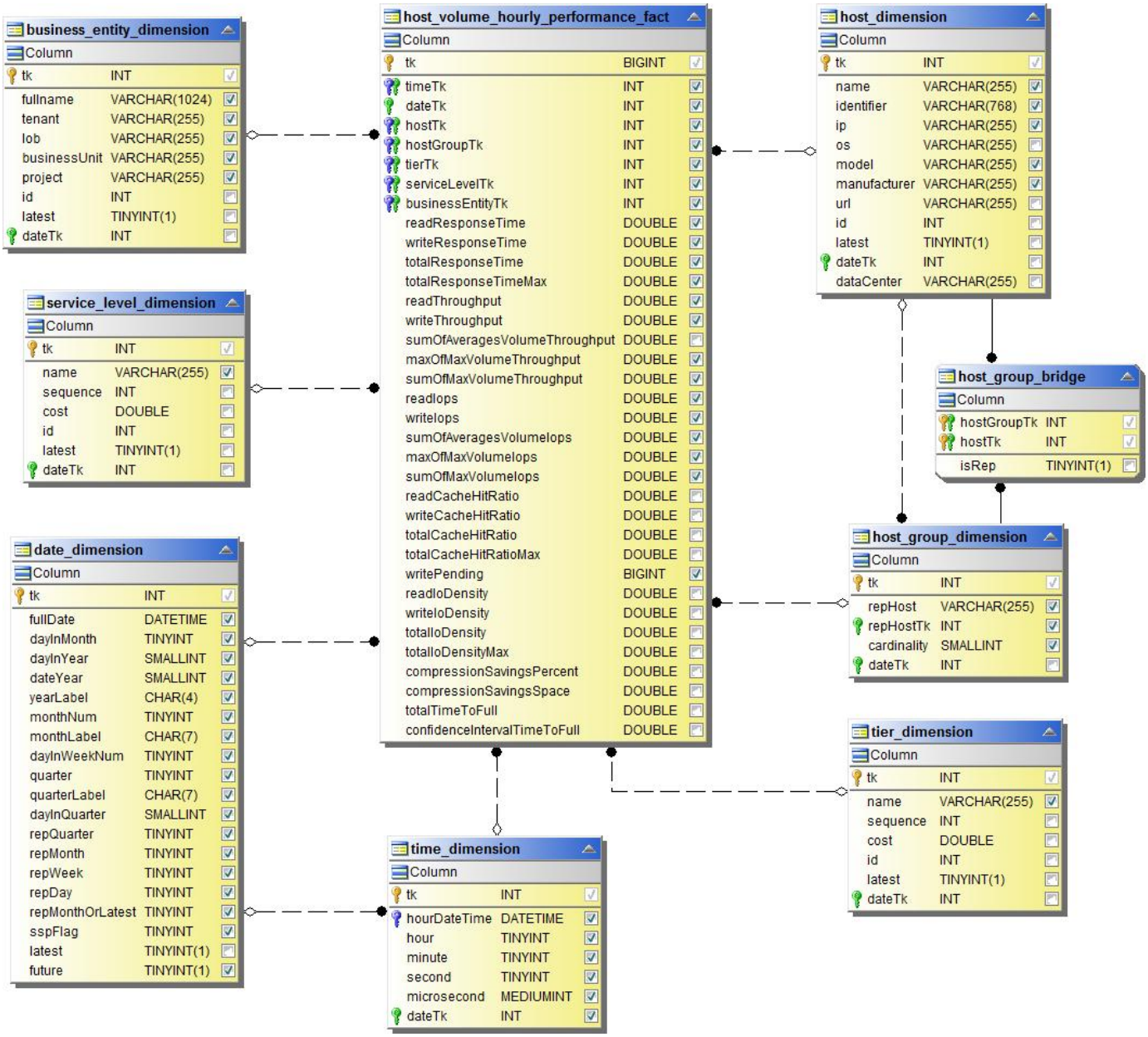
ディスクの日次パフォーマンス



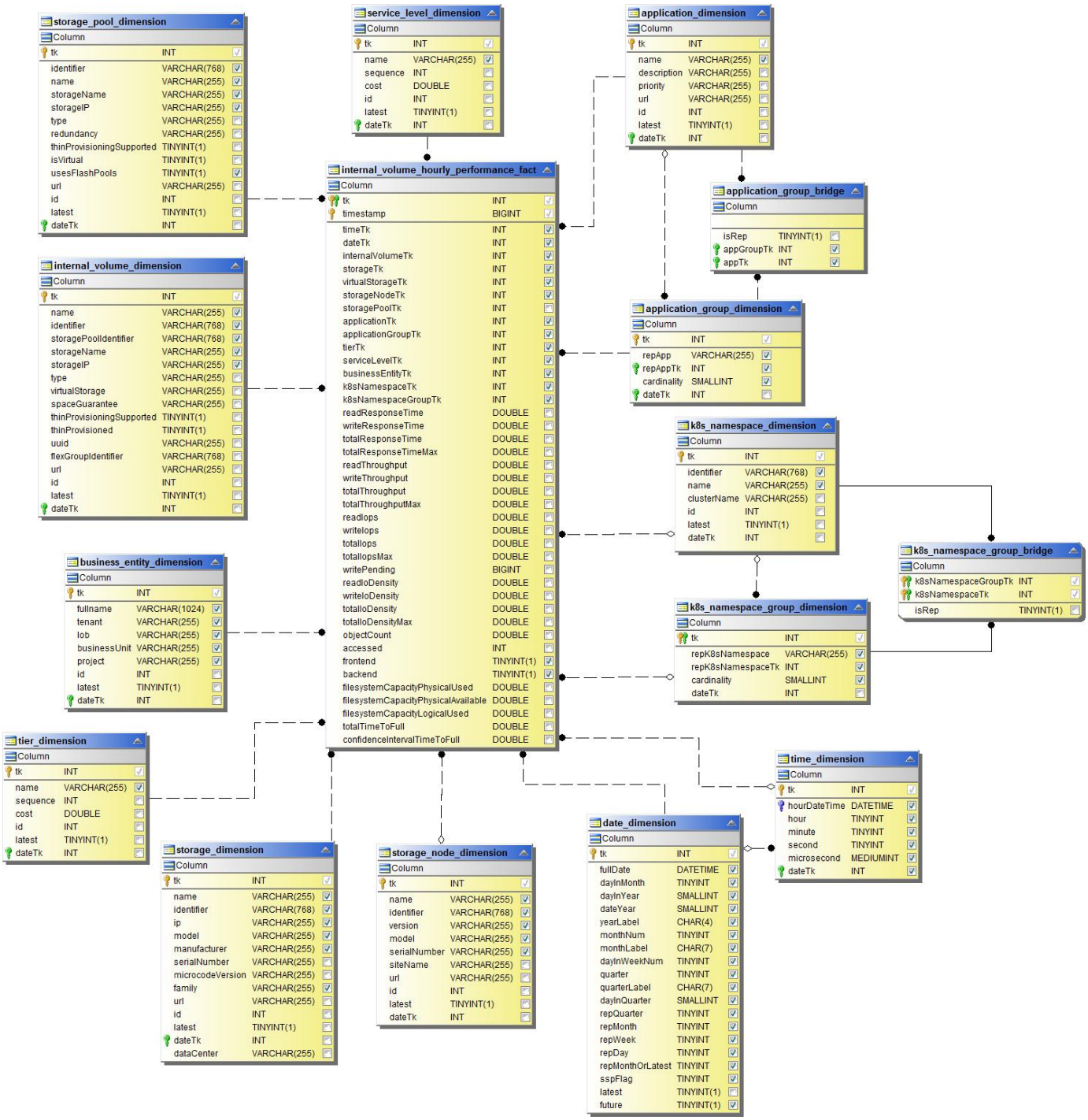
Disk Hourly Performance の **2** つの機能が



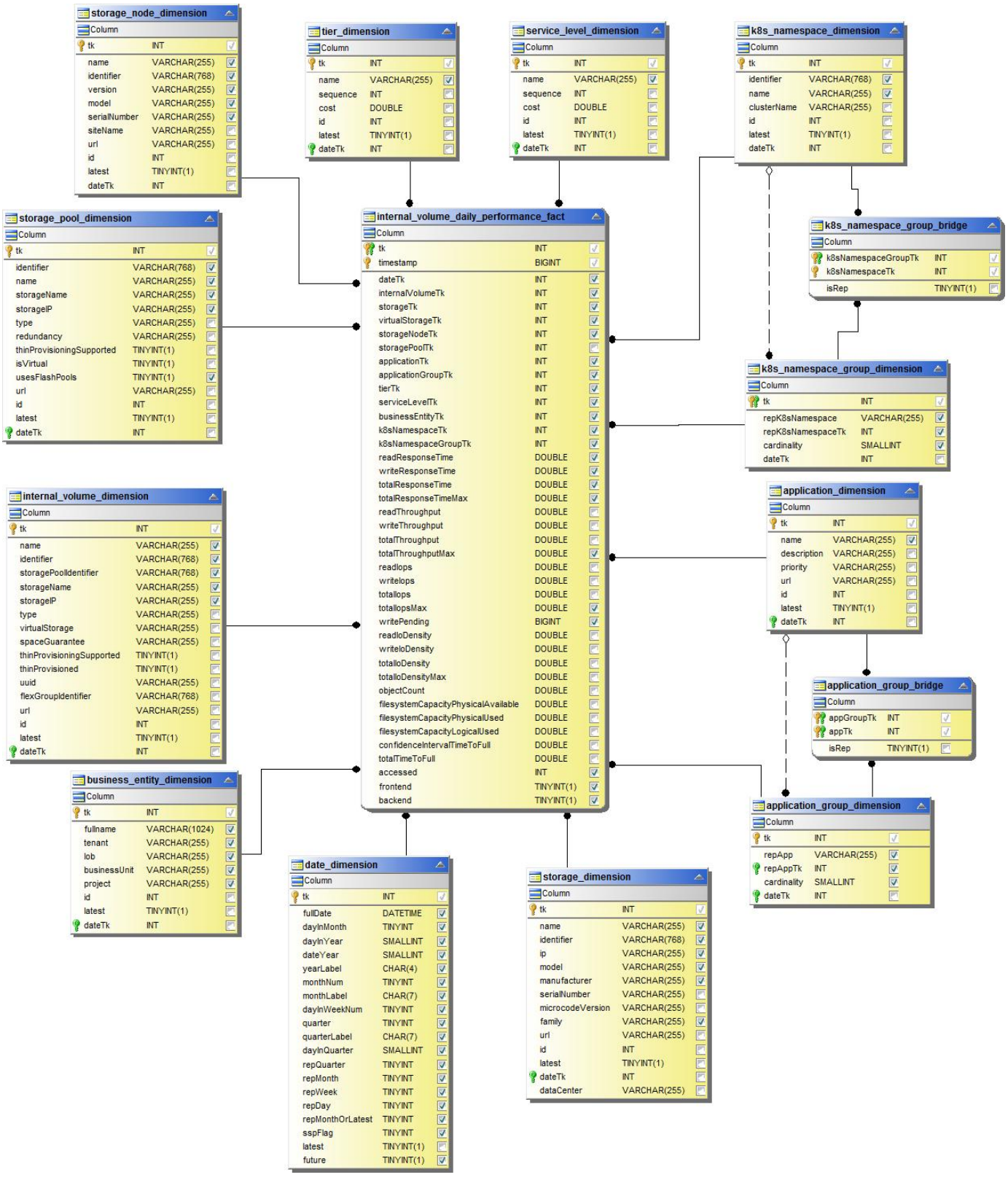
Host Hourly Performanceの略



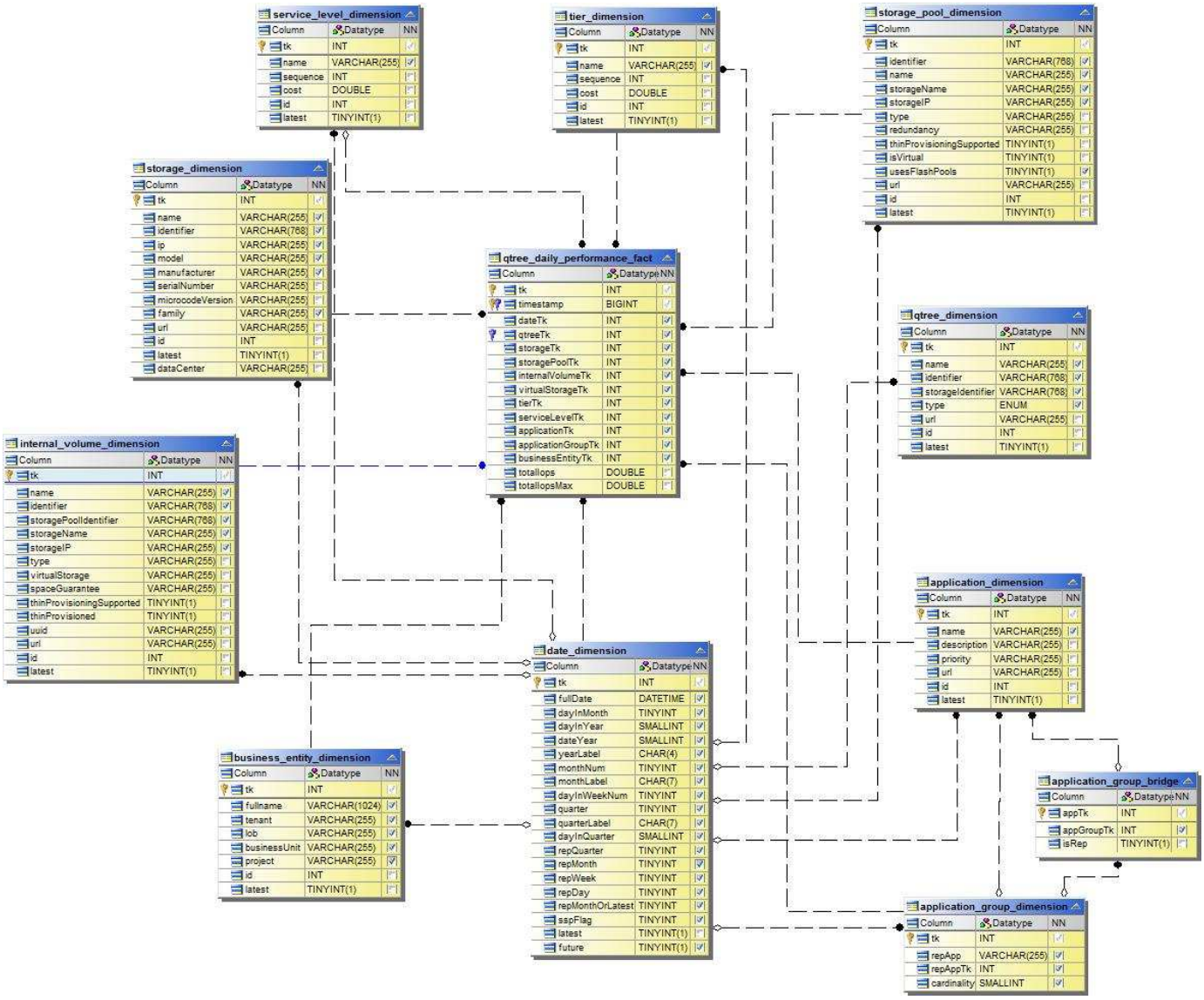
内部ボリューム毎時パフォーマンス



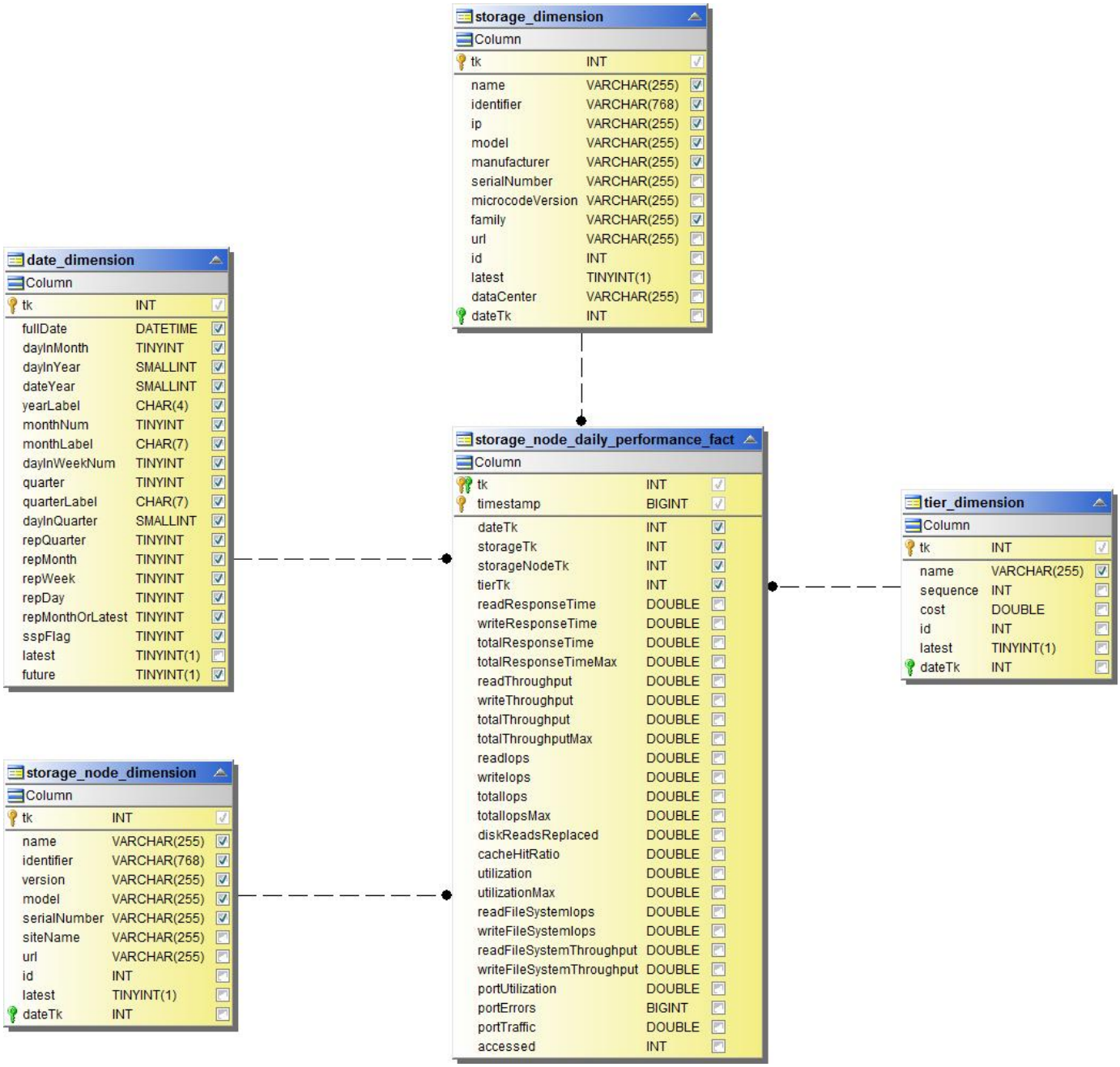
内部ボリュームの日次パフォーマンス



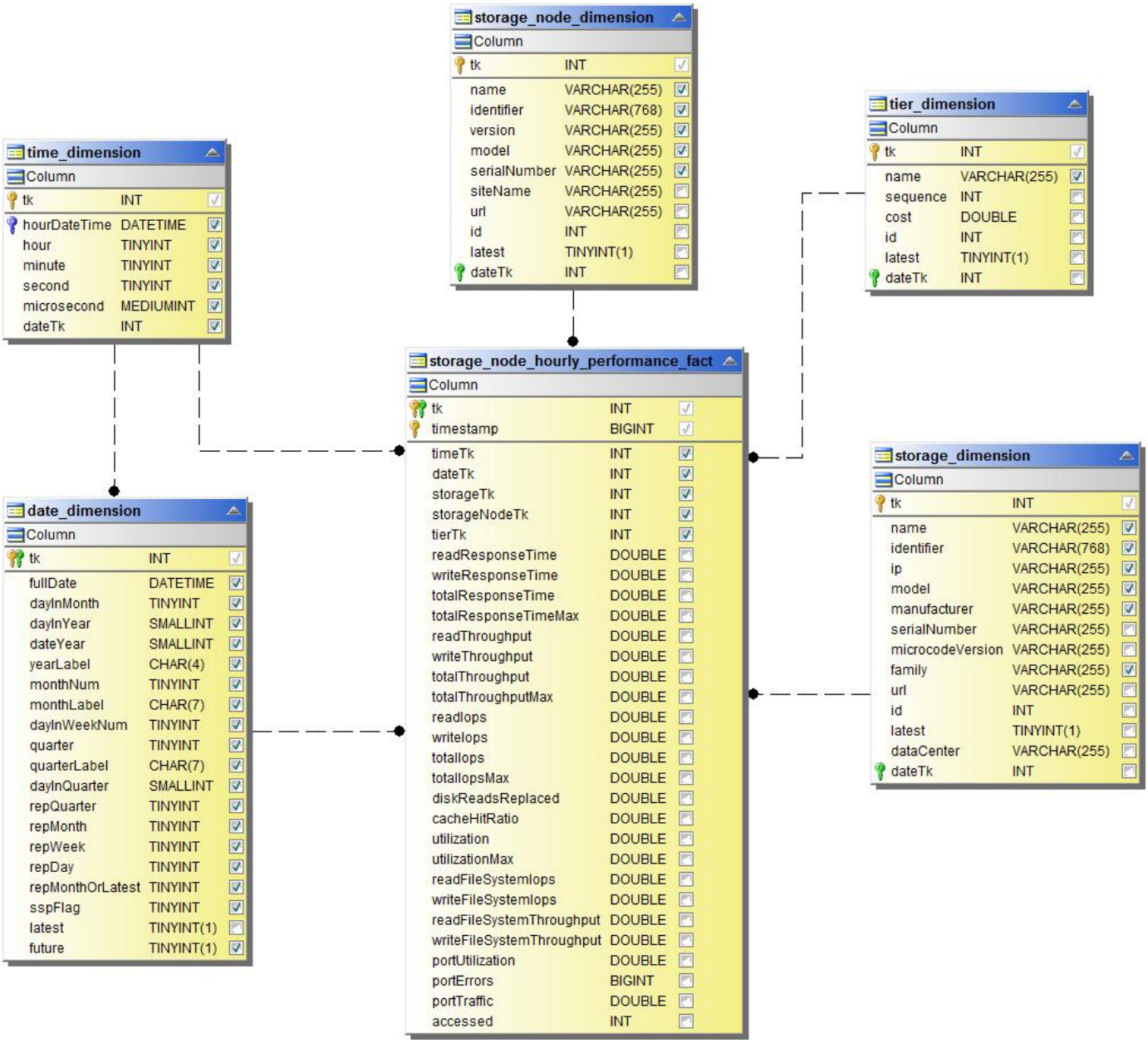
qtree ：日次パフォーマンス



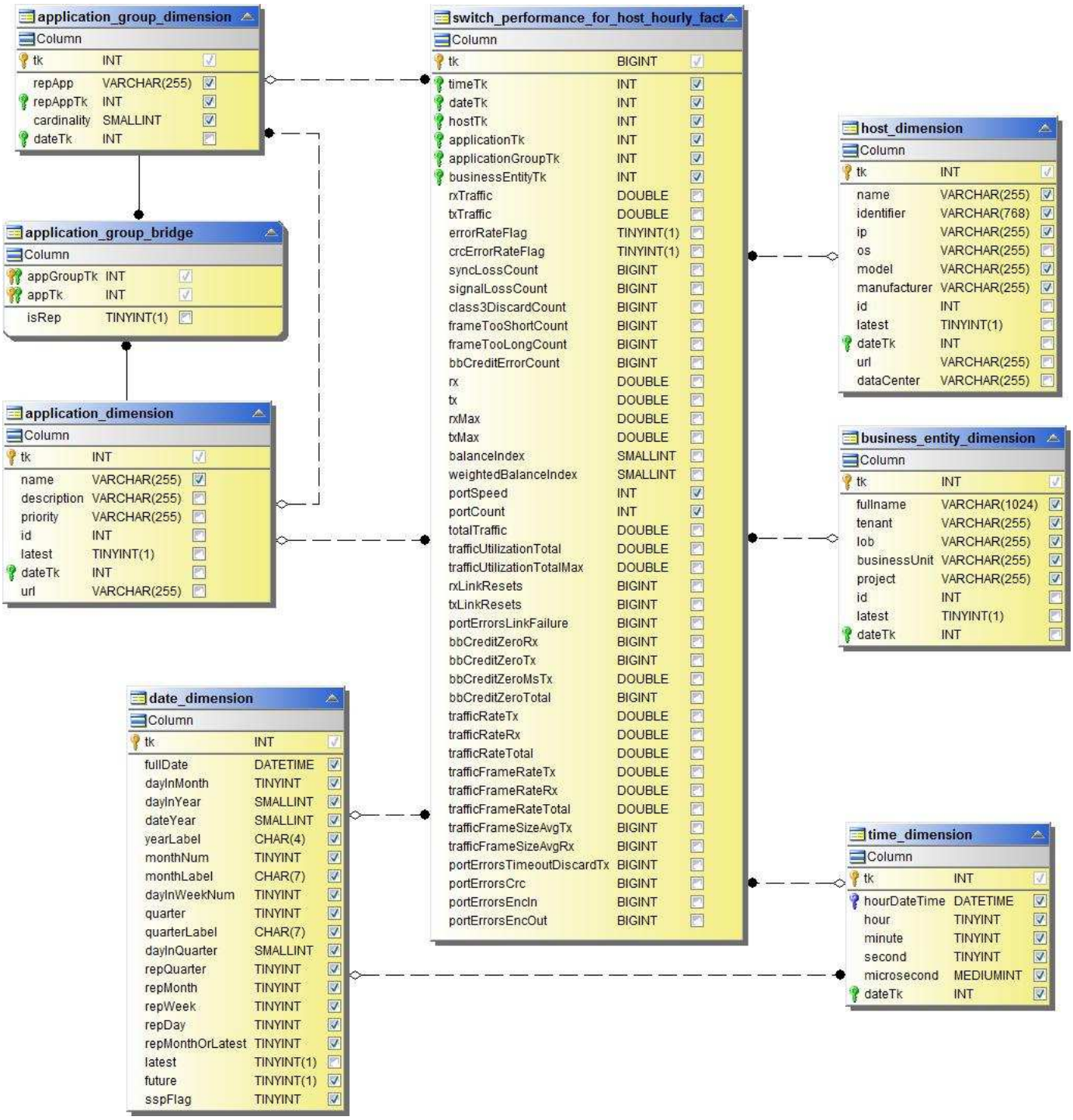
ストレージノードの日次パフォーマンス



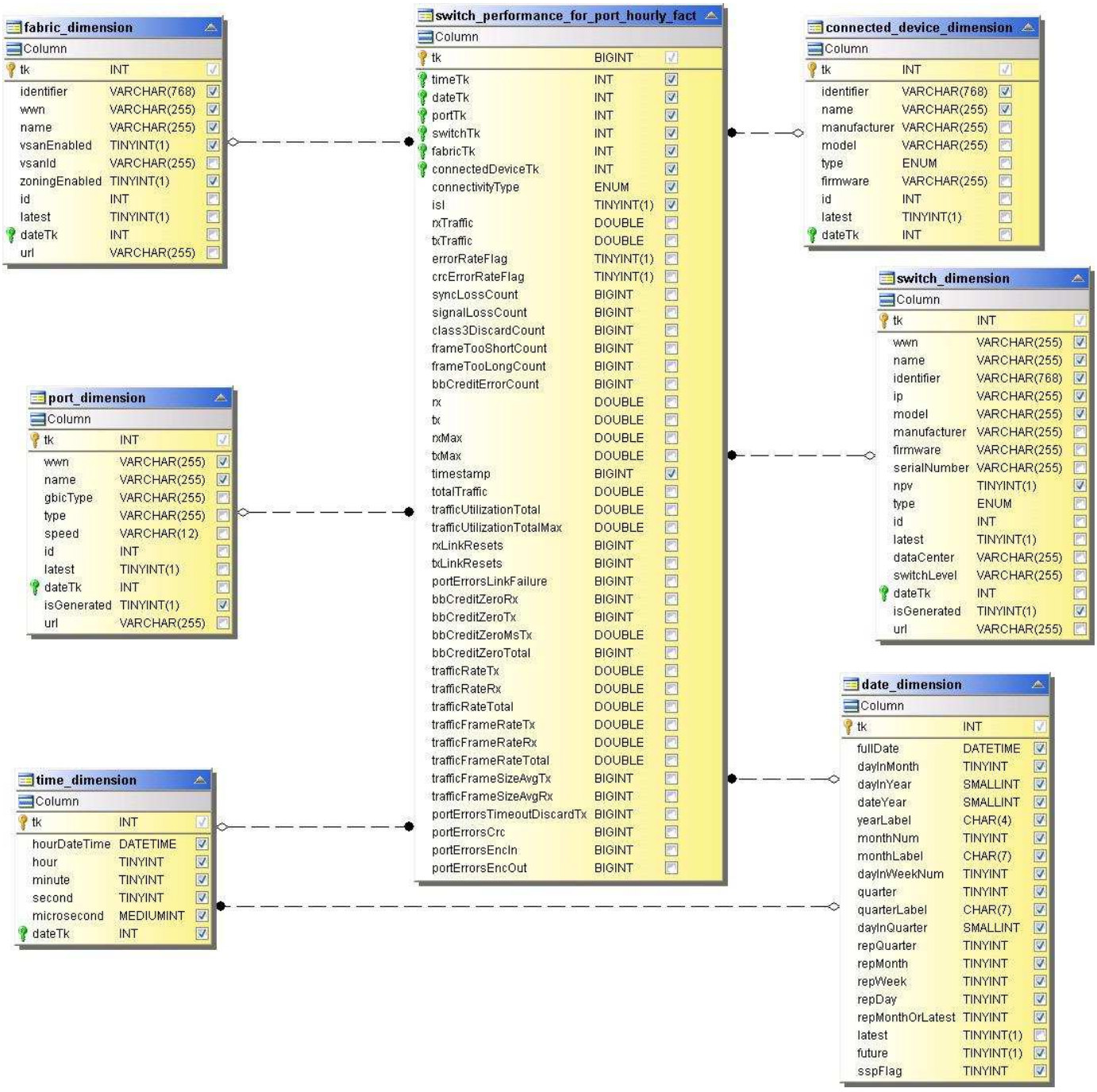
Storage Node Hourly Performance の略



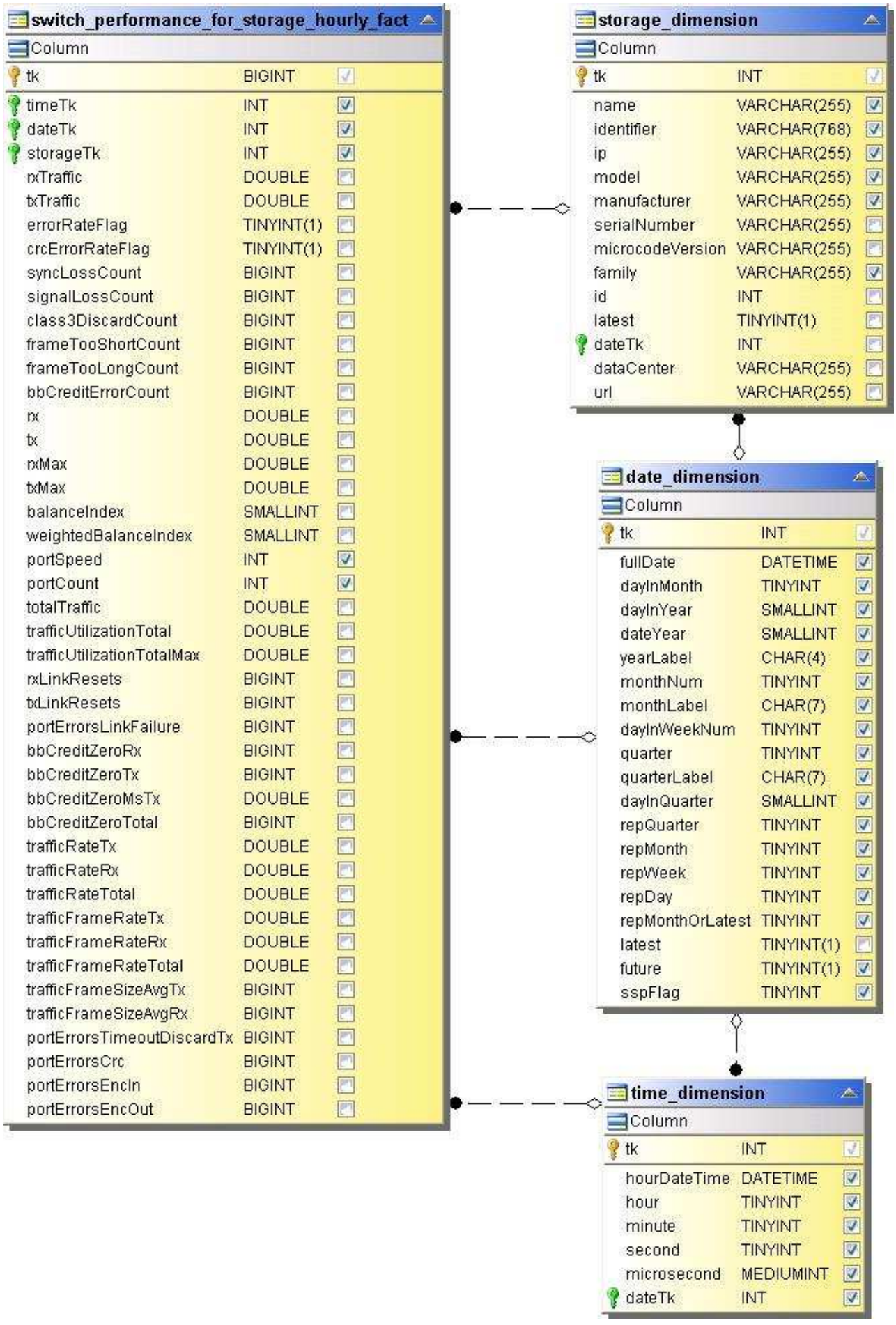
Switch Hourly Performance for Host



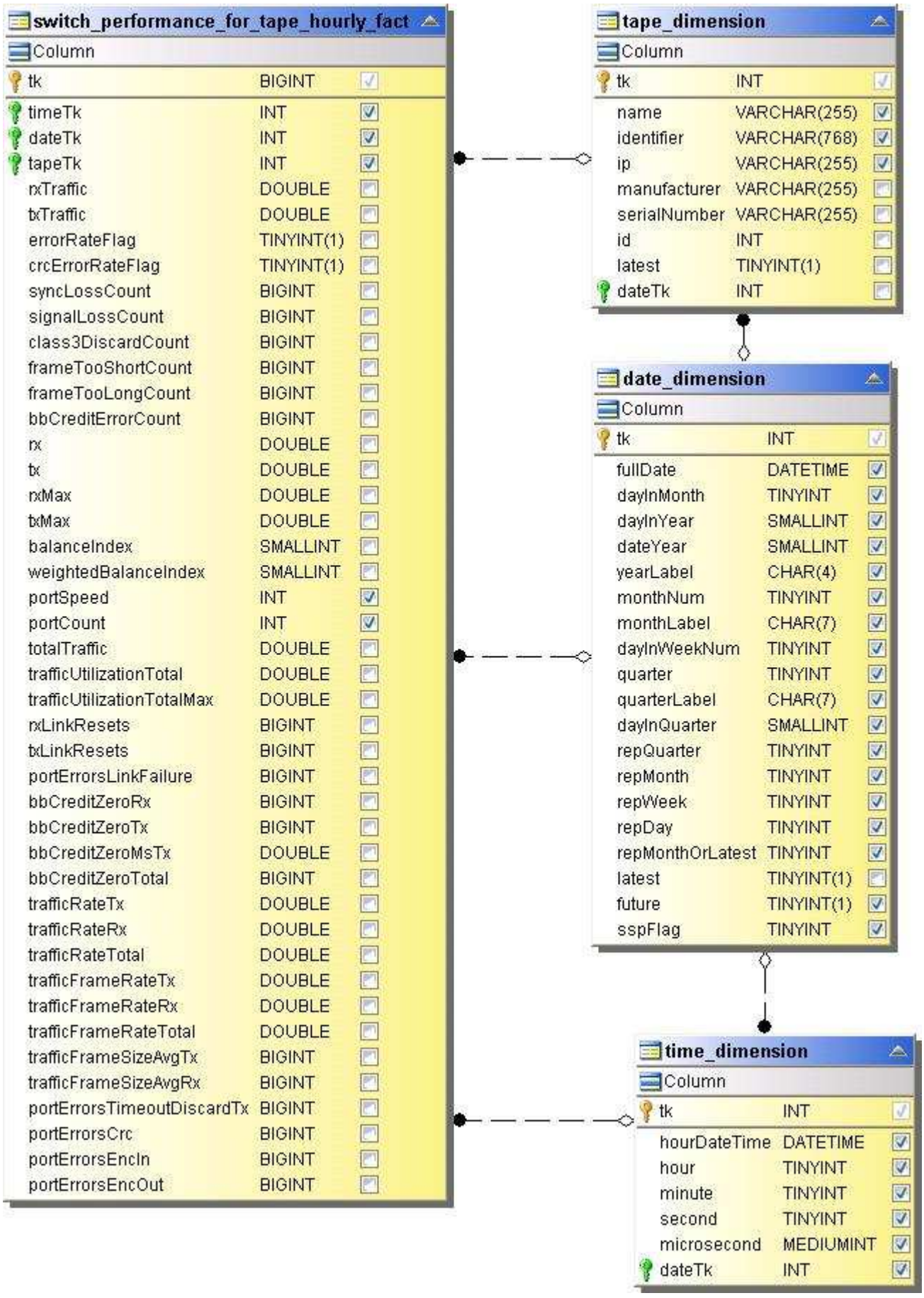
Switch Hourly Performance for Port



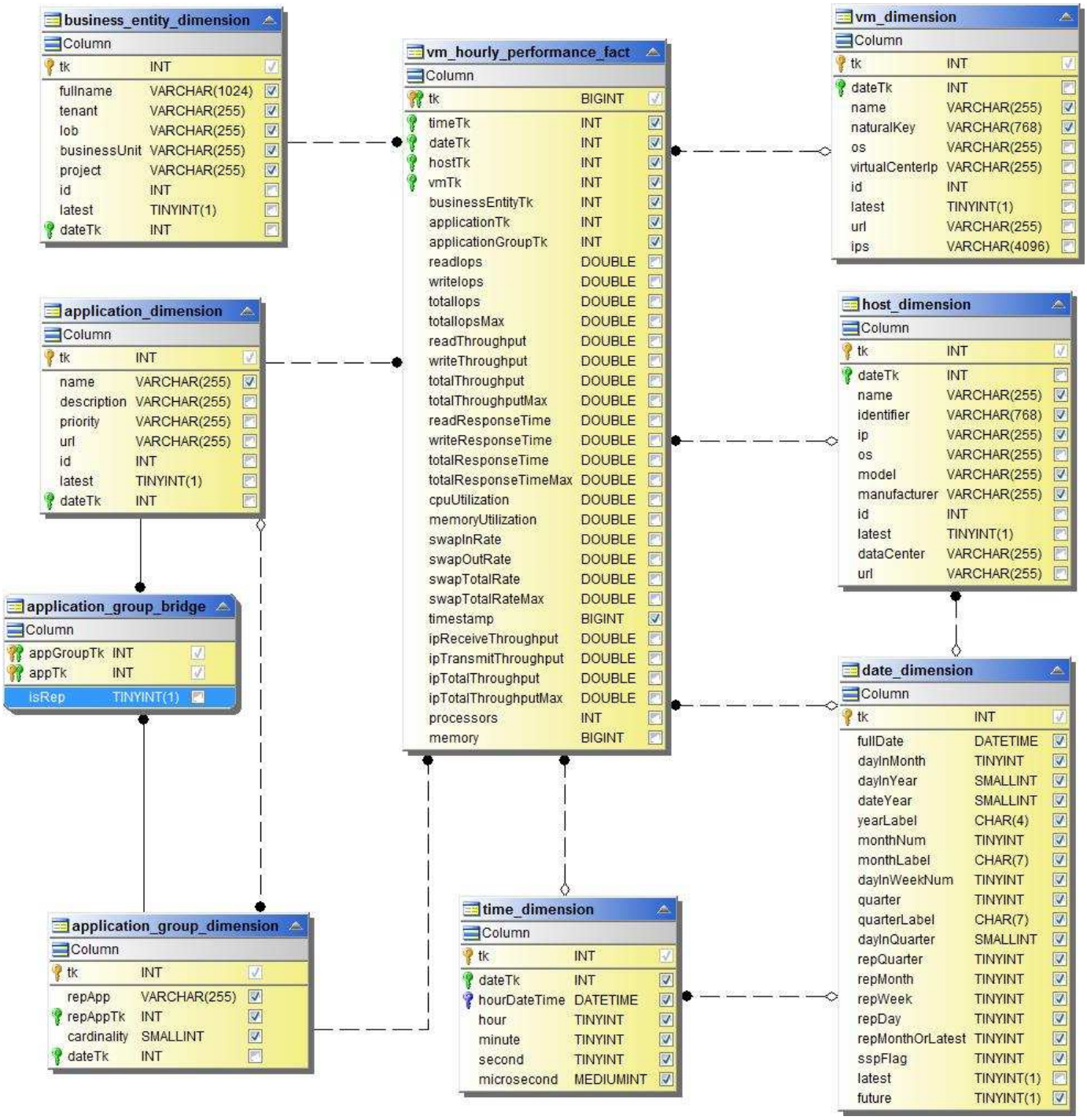
Switch Hourly Performance for Storage の略


switch_performance_for_storage_hourly_fact
Column
tk BIGINT
timeTk INT
dateTk INT
storageTk INT
rxTraffic DOUBLE
txTraffic DOUBLE
errorRateFlag TINYINT(1)
crcErrorRateFlag TINYINT(1)
syncLossCount BIGINT
signalLossCount BIGINT
class3DiscardCount BIGINT
frameTooShortCount BIGINT
frameTooLongCount BIGINT
bbCreditErrorCount BIGINT
rx DOUBLE
tx DOUBLE
rxMax DOUBLE
txMax DOUBLE
balanceIndex SMALLINT
weightedBalanceIndex SMALLINT
portSpeed INT
portCount INT
totalTraffic DOUBLE
trafficUtilizationTotal DOUBLE
trafficUtilizationTotalMax DOUBLE
rxLinkResets BIGINT
txLinkResets BIGINT
portErrorsLinkFailure BIGINT
bbCreditZeroRx BIGINT
bbCreditZeroTx BIGINT
bbCreditZeroMsTx DOUBLE
bbCreditZeroTotal BIGINT
trafficRateTx DOUBLE
trafficRateRx DOUBLE
trafficRateTotal DOUBLE
trafficFrameRateTx DOUBLE
trafficFrameRateRx DOUBLE
trafficFrameRateTotal DOUBLE
trafficFrameSizeAvgTx BIGINT
trafficFrameSizeAvgRx BIGINT
portErrorsTimeoutDiscardTx BIGINT
portErrorsCrc BIGINT
portErrorsEncIn BIGINT
portErrorsEncOut BIGINT
storage_dimension
Column
tk INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
family VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
dataCenter VARCHAR(255)
url VARCHAR(255)
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
latest TINYINT(1)
future TINYINT(1)
sspFlag TINYINT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT

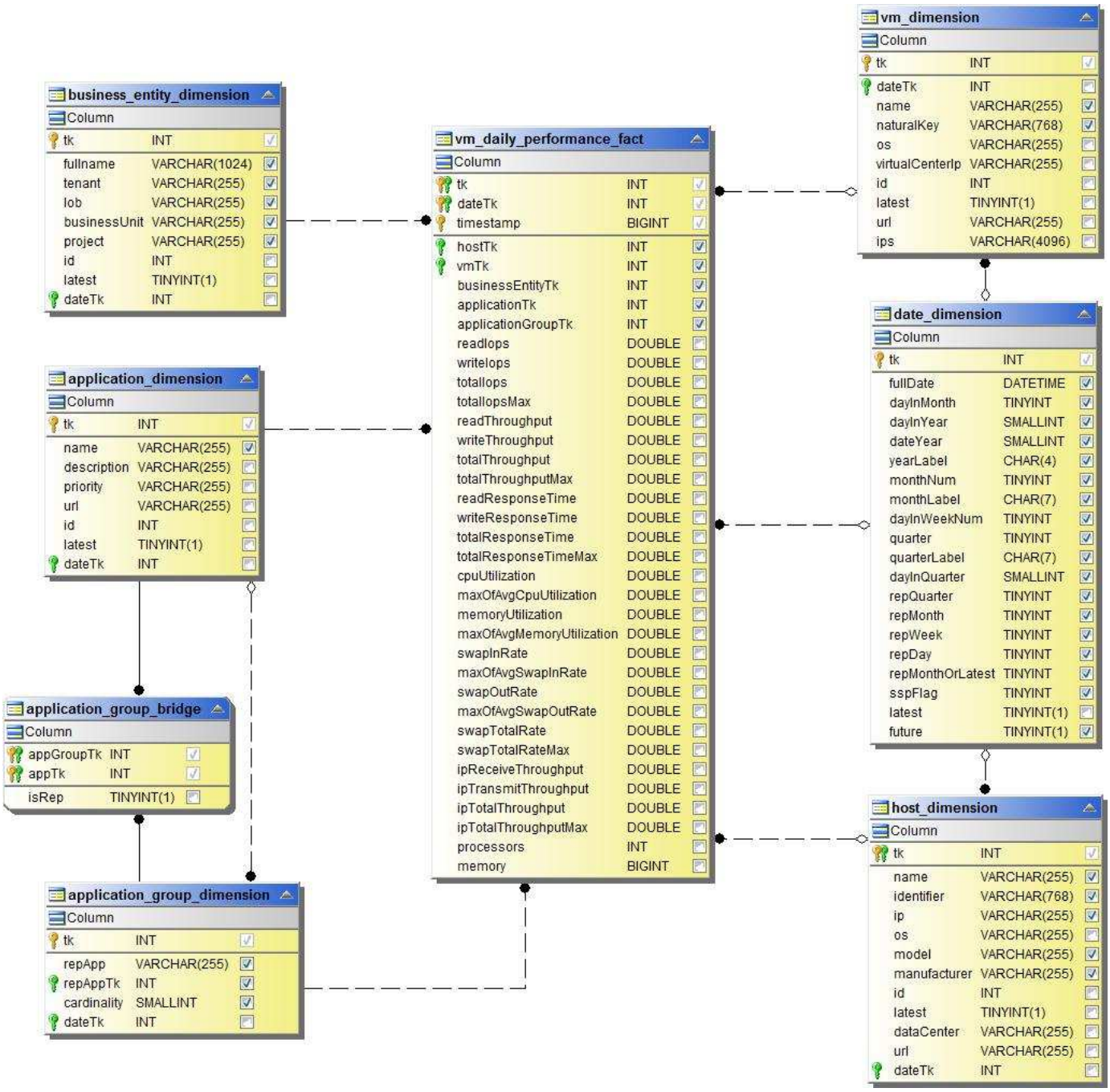
Switch Hourly Performance for Tape



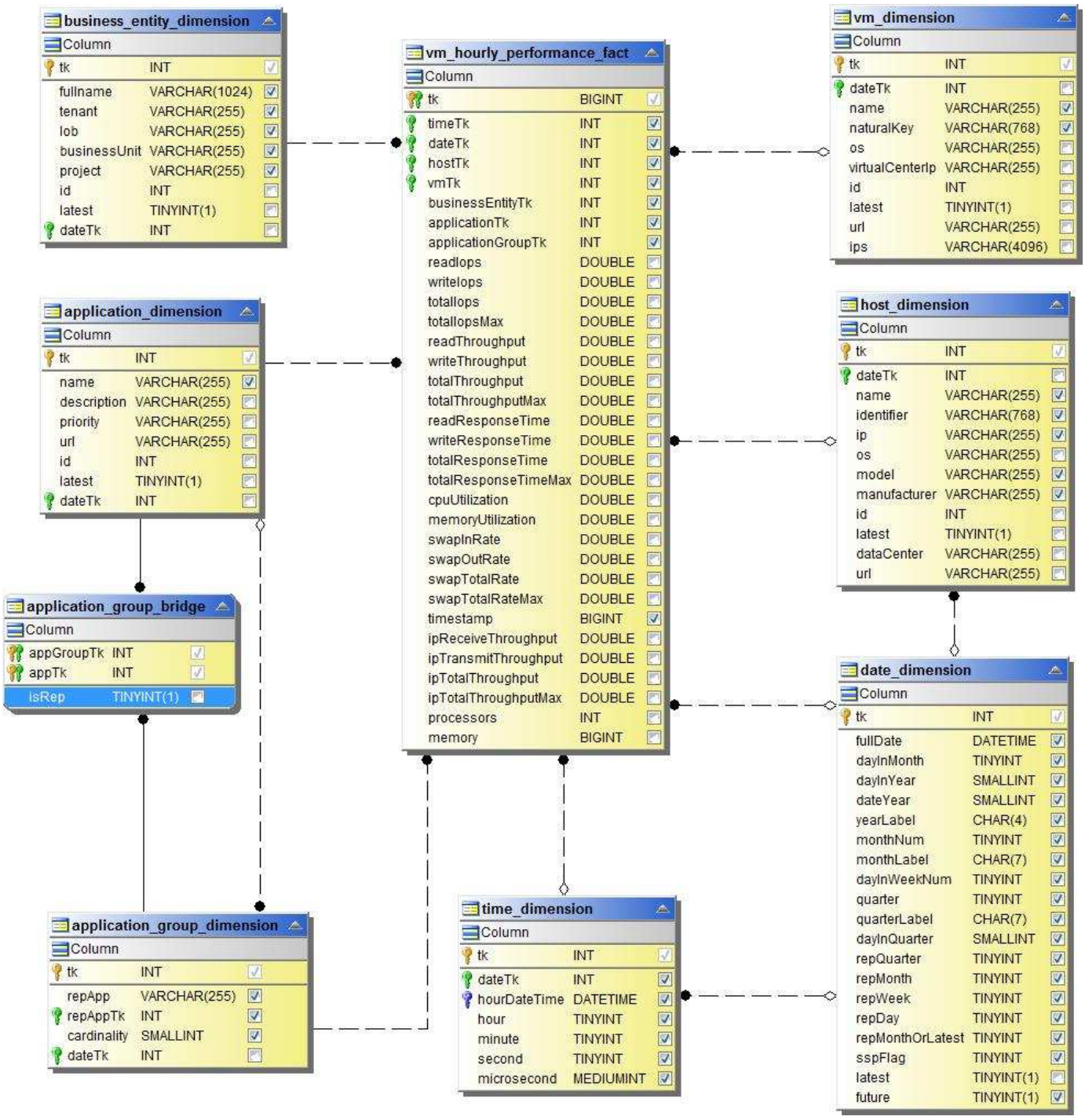
VM パフォーマンス



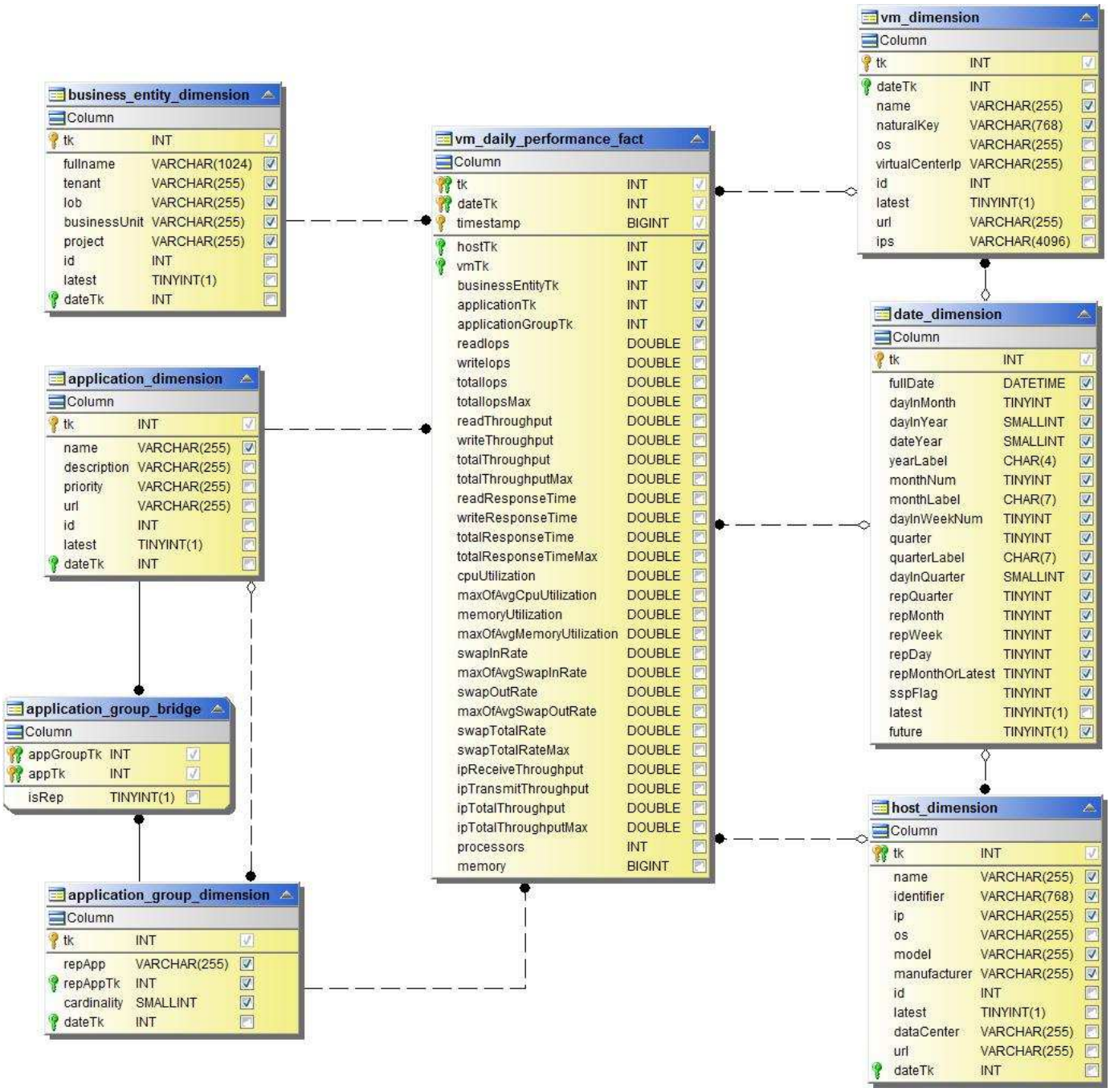
ホストの **VM** の日次パフォーマンス



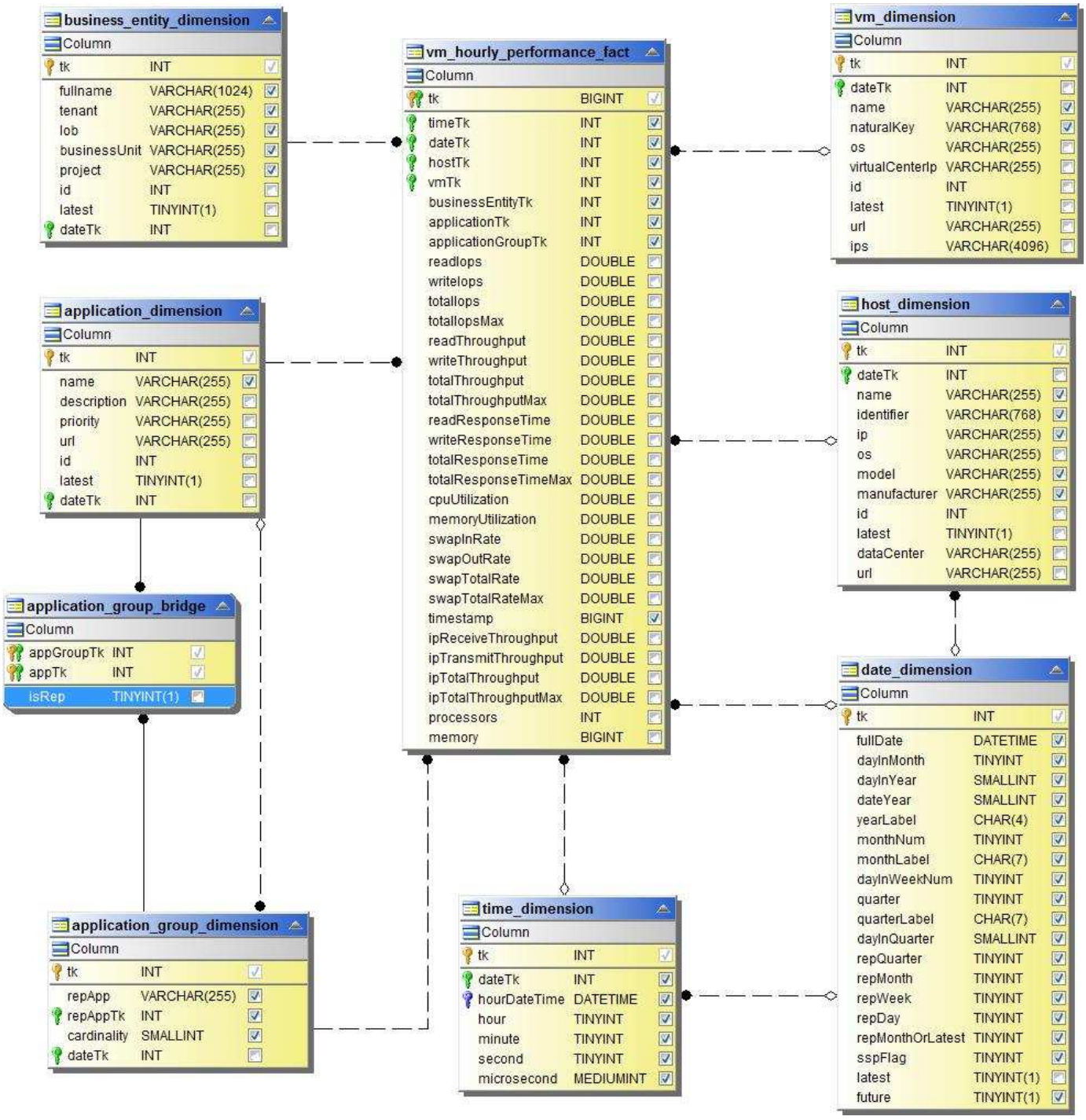
ホストの **VM 1** 時間ごとのパフォーマンス



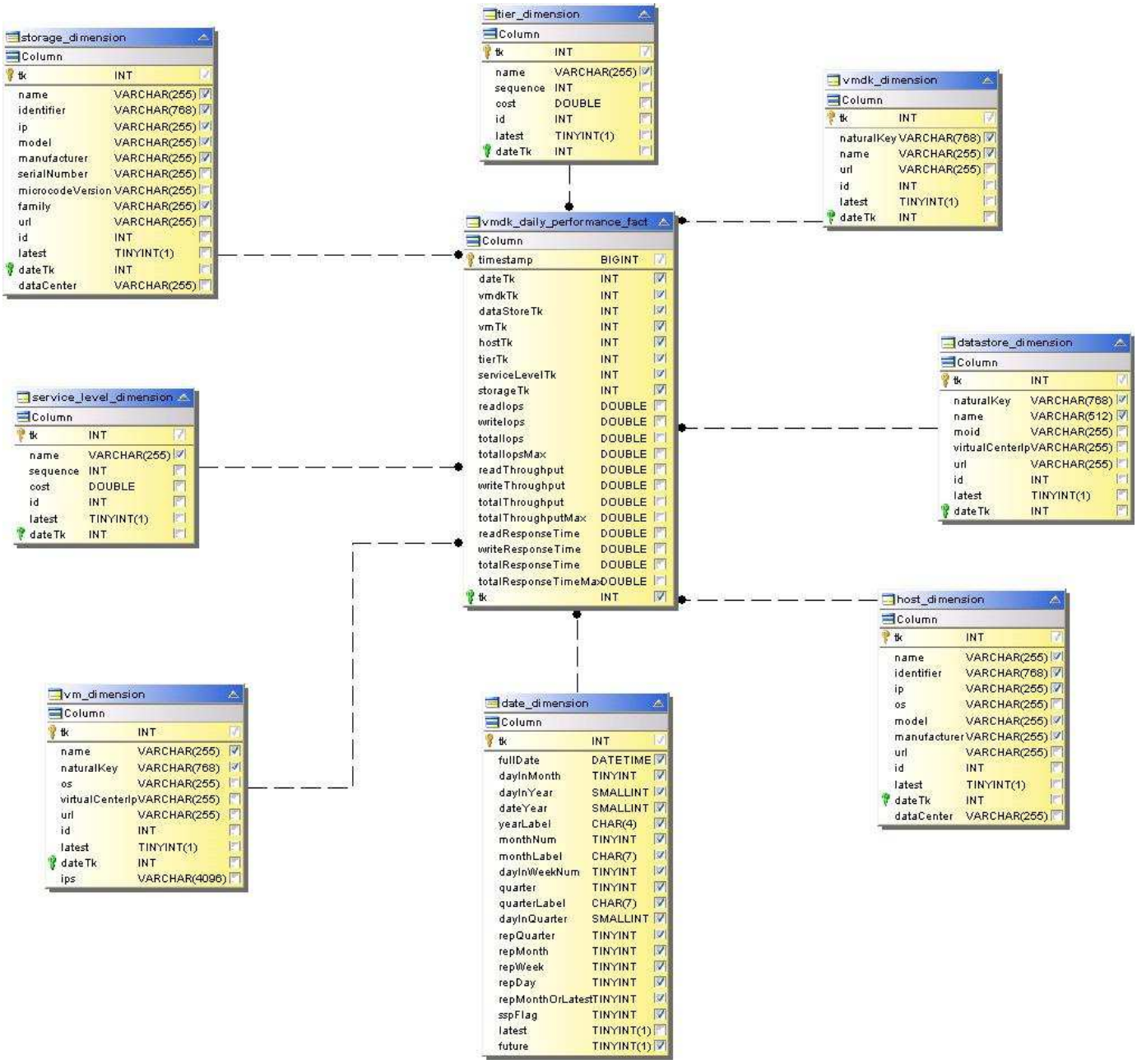
ホストの **VM** の日次パフォーマンス



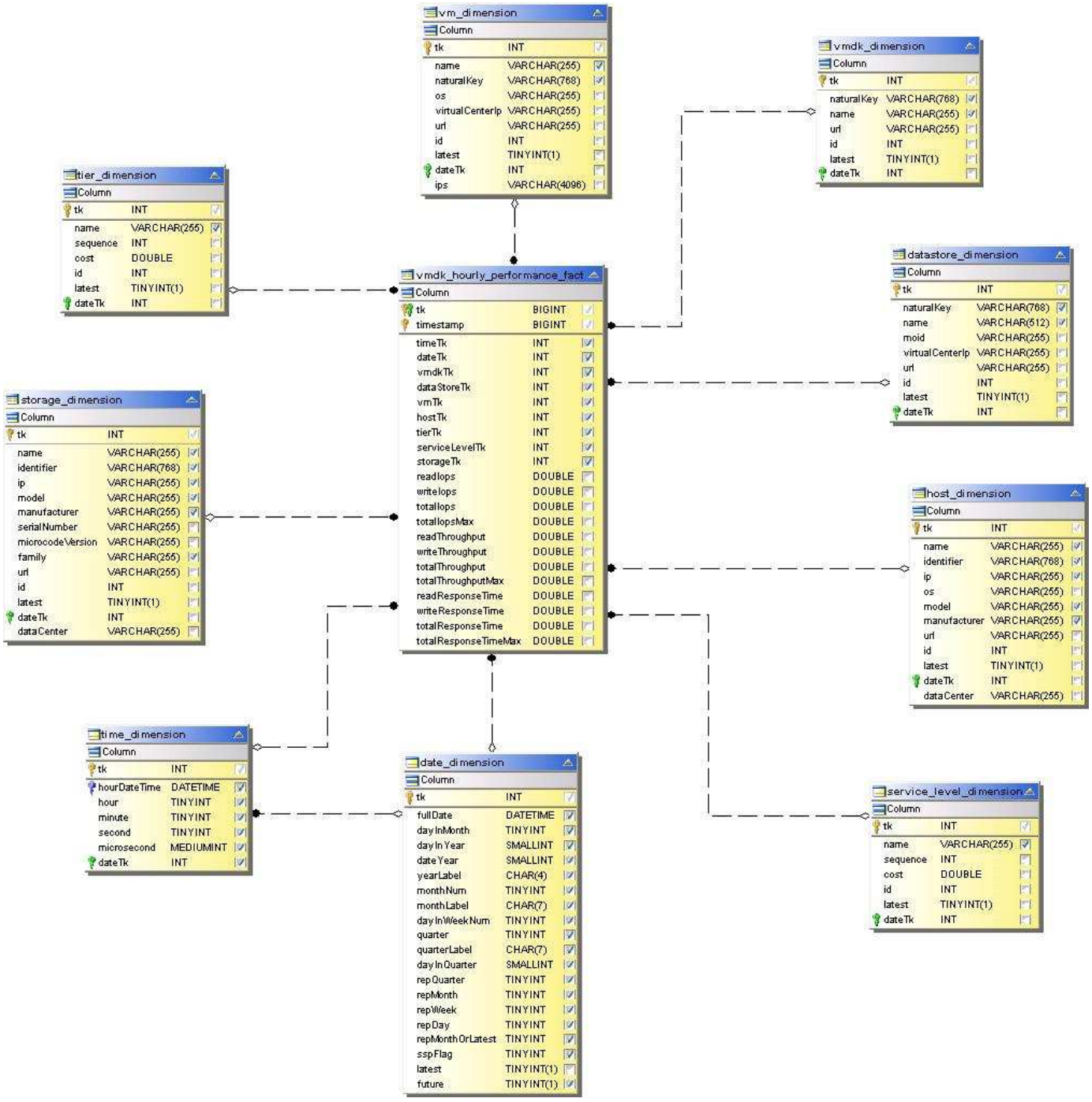
ホストの **VM 1** 時間ごとのパフォーマンス



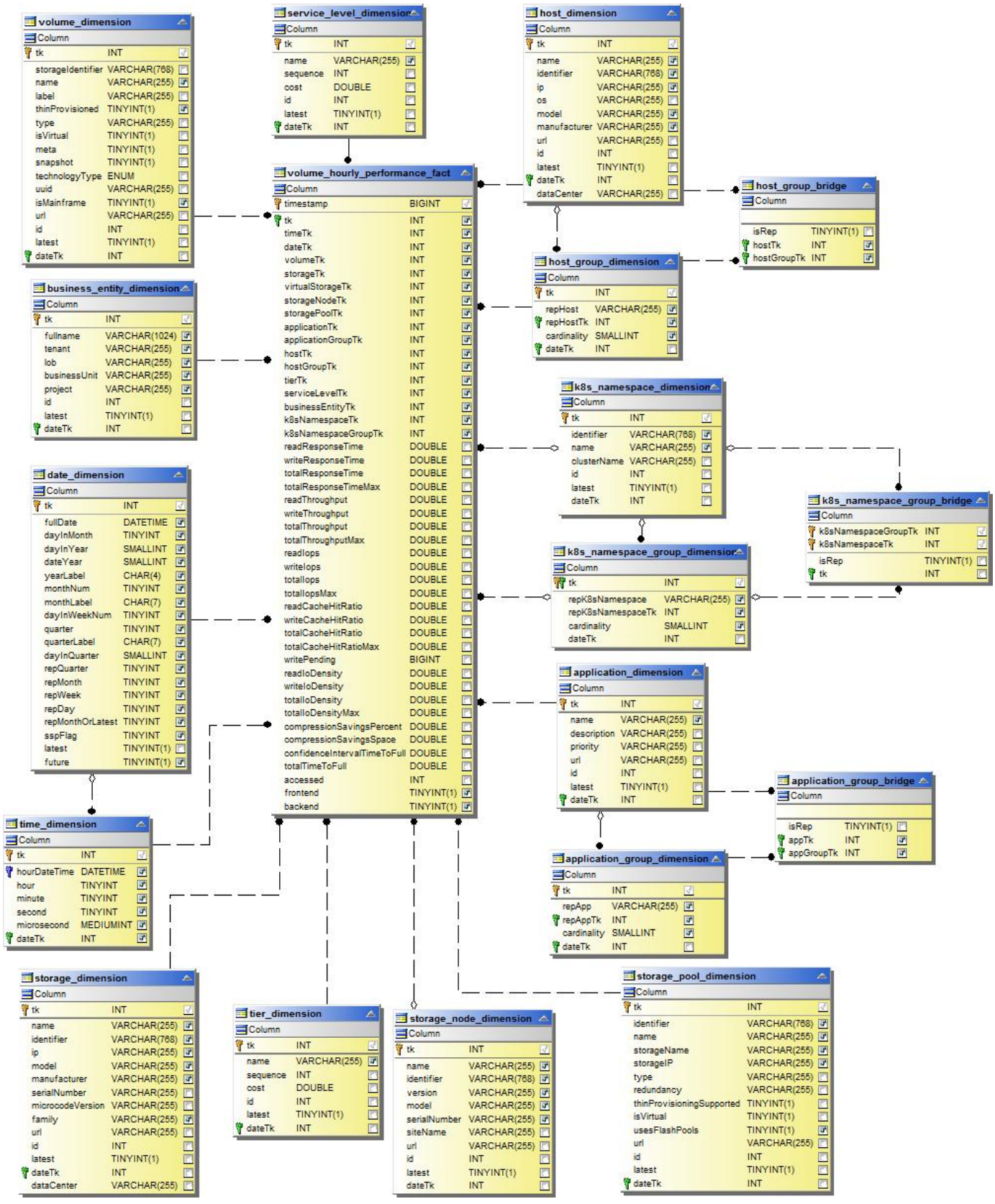
VMDK の日次パフォーマンス



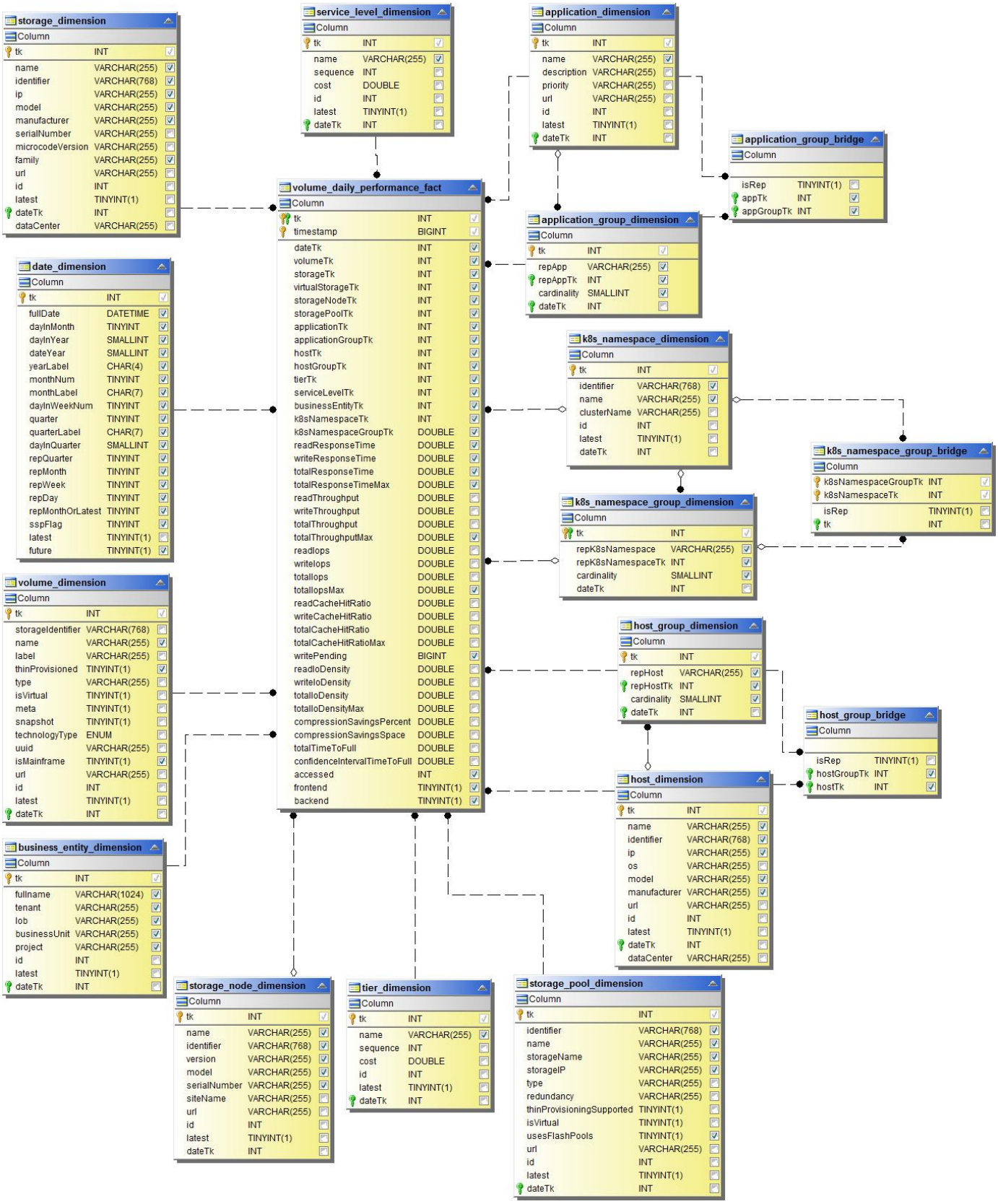
VMDK 毎時パフォーマンス



1 時間ごとのボリュームパフォーマンス



ボリュームの日次パフォーマンス



レポート作成のためのデータインフラ分析情報スキーマ

ここでは、Data Infrastructure Insightsのレポート作成の参考として、スキーマの表と図を示します。

"* スキーマテーブル *" .pdf 形式で指定します。リンクをクリックして開くか、右クリックして「 _ 名前を付けて保存 …_ 」を選択してダウンロードします。

"* スキーマ図 *"

レポート機能はData Infrastructure Insightsで使用でき"Premium Edition の場合"ます。

Kubernetes

Kubernetes クラスタの概要

Data Infrastructure Insights Kubernetes Explorerは、Kubernetesクラスタの全体的な健全性と使用状況を表示するための強力なツールであり、調査領域に簡単にドリルダウンできます。

[Dashboards]>[Kubernetes Explorer]をクリックすると、[Kubernetes Cluster]リストページが開きます。この概要ページには、環境内のKubernetesクラスタの表が含まれています。

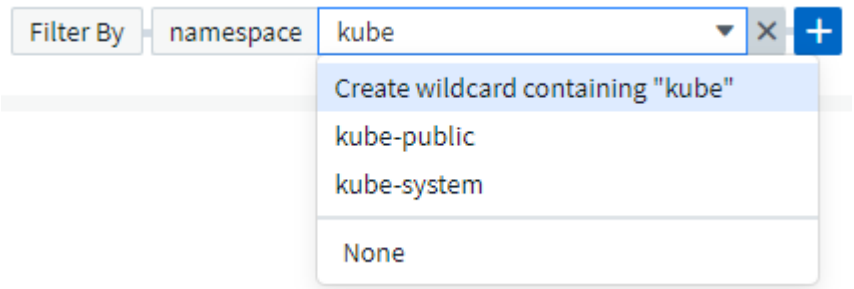
クラスタリスト

クラスタリストには、環境内の各クラスタについて次の情報が表示されます。

- クラスタ*名*。クラスタ名をクリックすると、が開きます "* 詳細ページ *" をクリックします。
- *彩度*パーセンテージ。Overall Saturation（全体飽和）は、CPU、メモリ、またはストレージの飽和度の最大値です。
- クラスタ内のノード数*。この番号をクリックすると、Node listページが開きます。
- クラスタ内の* Pod*の数。この番号をクリックすると、ポッドリストページが開きます。
- クラスタ内のネームスペースの数*。この番号をクリックすると、名前空間リストページが開きます。
- クラスタ内のワークロードの数*。この数値をクリックすると、ワークロードリストページが開きます。

フィルタを調整しています

フィルタ処理中に、入力を開始すると、現在のテキストに基づいて * ワイルドカードフィルタ * を作成するオプションが表示されます。このオプションを選択すると、ワイルドカード式に一致するすべての結果が返されます。NOTまたはANDを使用して*式*を作成することもできます。また、「なし」オプションを選択してフィールド内のnull値をフィルタリングすることもできます。



ワイルドカードまたは式に基づくフィルタ（例 フィルタフィールドには、「なし」などは濃い青で表示されます。リストから直接選択した項目は、水色で表示されます。

Kubernetes フィルタはコンテキストに応じて表示されます。つまり、特定のノードページ上にある場合、pod _name フィルタはそのノードに関連するポッドのみをリストします。さらに、特定のネームスペースにフィルタを適用すると、名前空間の名前空間ではポッドのみが表示されます。

ワイルドカードおよび式フィルタリングは、テキストまたはリストでは機能しますが、数値、日付、またはブール値では機能しません。

NetApp Kubernetes監視オペレータをインストールまたはアップグレードする前に

をインストールまたはアップグレードする前に、この情報をお読みください。 "Kubernetes監視オペレータ"。

コンポーネント	要件
Kubernetes のバージョン	Kubernetes v1.20以上：
Kubernetesディストリビューション	AWS Elastic Kubernetes Service（EKS） Azure Kubernetes Service （ AKS ） Google Kubernetes Engine （ GKE ） Red Hat OpenShift のサービスです Rancher Kubernetes Engine （ RKE ） VMware Tanzu の
Linux OS	Data Infrastructure Insightsでは、Arm64アーキテクチャで実行されているノードはサポートされません。ネットワーク監視：Linuxカーネルバージョン4.18.0以上を実行している必要があります。Photon OSはサポートされていません。
ラベル	Data Infrastructure Insightsは、Kubernetesノードセレクタを指定して、これらのプラットフォームで次のKubernetesラベルを検索することで、Linuxを実行しているKubernetesノードの監視をサポートします。Kubernetes v1.20以降：Kubernetes .io/os=linux Rancher + cattle.ioをオーケストレーション/Kubernetesプラットフォーム：cattle.io/os=linux
コマンド	curlコマンドとkubectlコマンドが使用可能である必要があります。;最良の結果を得るには、これらのコマンドをパスに追加してください。

コンポーネント	要件
接続性	kubectl CLIはターゲットのKubernetesクラスタと通信するように設定されており、Data Infrastructure Insights環境にインターネット接続されています。インストール中にプロキシの背後にいる場合は、「オペレータのインストール」のセクションに記載されている手順に従ってください"プロキシサポートを設定しています"。監査およびデータレポートを正確に作成するには、Network Time Protocol（NTP；ネットワークタイムプロトコル）またはSimple Network Time Protocol（SNTP；簡易ネットワークタイムプロトコル）を使用してAgentマシンの時刻を同期します。
その他	OpenShift 4.6以降を実行している場合は、"OpenShift の手順" さらに、これらの前提条件が満たされていることを確認します。
APIトークン	Operatorを再デプロイする場合(つまり、Operatorを更新または置換する場合)は、新しいAPIトークンを作成する必要はありません。前のトークンを再利用できます。

始める前に注意すべき重要事項

を使用してを実行する場合 プロキシを使用してください カスタムリポジトリまたはを使用しているOpenShiftを参照してください。

また、 権限。

プロキシサポートを設定しています

環境にプロキシを使用してNetApp Kubernetes Monitoring Operatorをインストールする方法は2つあります。同じプロキシシステムでも、別のプロキシシステムでもかまいません。

- インストールコードスニペット（「curl」を使用）の実行中に、スニペットが実行されるシステムをData Infrastructure Insights環境に接続するために必要なプロキシ
- ターゲットのKubernetesクラスタがData Infrastructure Insights環境と通信するために必要なプロキシ

これらのいずれかまたは両方にプロキシを使用する場合、NetApp Kubernetesオペレーティングモニタをインストールするには、まずプロキシがデータインフラストラクチャインサイト環境との良好な通信を許可するように設定されていることを確認する必要があります。たとえば、Operatorをインストールするサーバ/ VMからData Infrastructure Insightsにアクセスし、Data Infrastructure Insightsからバイナリをダウンロードできるようにする必要があります。

NetApp Kubernetes Operating Monitorのインストールに使用するプロキシとして、オペレータをインストールする前に、_http_proxy/https_proxy_environment変数を設定します。一部のプロキシ環境では'_no_proxy環境変数も設定する必要があります

変数を設定するには、NetApp Kubernetes Monitoring Operatorをインストールする前に、システムで次の手順を実行します。

1. 現在のユーザの *https_proxy* 変数と _http_proxy_environment 変数を設定します。

a. セットアップするプロキシに認証（ユーザ名/パスワード）がない場合は、次のコマンドを実行します。

```
 export https_proxy=<proxy_server>:<proxy_port>
```

.. セットアップするプロキシに認証（ユーザ名/パスワード）が設定されている場合は、次のコマンドを実行します。

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_port>
```

KubernetesクラスタがData Infrastructure Insights環境と通信するために使用するプロキシの場合は、これらの手順をすべて読んでからNetApp Kubernetes監視オペレータをインストールします。

NetApp Kubernetes Monitoring Operatorを導入する前に、operator-config.yamlでAgentConfigurationのプロキシセクションを設定します。

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

カスタムまたはプライベートの**Docker**リポジトリを使用する

デフォルトでは、NetApp Kubernetes監視オペレータは、データインフラのインサイトリポジトリからコンテナイメージを取得します。監視のターゲットとして使用されているKubernetesクラスタがあり、カスタムまたはプライベートのDockerリポジトリまたはコンテナレジストリからのみコンテナイメージを取得するようにそのクラスタが設定されている場合は、NetApp Kubernetes Monitoring Operatorで必要なコンテナへのアク

セスを設定する必要があります。

NetApp Monitoring Operatorのインストールタイルから[Image Pull Snippet]を実行します。このコマンドを実行すると、Data Infrastructure Insightsリポジトリにログインし、オペレータが必要とするすべてのイメージを取得して、Data Infrastructure Insightsリポジトリからログアウトします。プロンプトが表示されたら、指定したリポジトリの一時パスワードを入力します。このコマンドは、オプション機能を含む、オペレータが使用するすべてのイメージをダウンロードします。これらの画像がどの機能に使用されるかについては、以下を参照してください。

Core Operator Functionality and Kubernetes Monitoringの略

- ネットアップによる監視
- kube-rbac-proxyの略
- kube-state-metricsの略
- テレグラフ
- distroless-root-user

イベントログ

- Fluent-bit
- kubernetes-event-exporterの略

ネットワークのパフォーマンスとマップ

- ci-net-observerの略

社内のポリシーに従って、オペレータ用の Docker イメージをプライベート / ローカル / エンタープライズ Docker リポジトリにプッシュします。リポジトリ内のこれらのイメージへのイメージタグとディレクトリパスが、Data Infrastructure Insightsリポジトリ内のイメージタグとディレクトリパスと一致していることを確認します。

operator-deployment.yamlでmonitoring-operatorデプロイメントを編集し、プライベートDockerリポジトリを使用するようにすべてのイメージ参照を変更します。

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

operator-config.yamlのAgentConfigurationを編集して、新しいDockerリポジトリの場所を反映します。プライベートリポジトリ用に新しいimagePullSecretを作成します。詳細については、_ https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/_を参照してください

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation for
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository[using a custom or private docker repository].
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

OpenShift の手順

OpenShift 4.6以降で実行している場合は、_runPrivileged_settingを有効にするには、_operator-config.yaml_でAgentConfigurationを編集する必要があります。

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

OpenShiftは、一部のKubernetesコンポーネントへのアクセスをブロックする可能性のある追加のセキュリティレベルを実装する場合があります。

権限

監視しているクラスタにClusterRoleがないカスタムリソースが含まれている場合、 "表示するアグリゲート" イベントログを使用してこれらのリソースを監視するには、オペレータにこれらのリソースへのアクセスを手動で許可する必要があります。

1. edit_operator -additional-permissions.yaml_インストール前、またはインストール後にresource_ClusterRole/<namespace>-additional-permissions_を編集します。
2. 動詞["get","watch","list"]を使用して、目的のapiGroupsとリソースの新しいルールを作成します。「\https://kubernetes.io/docs/reference/access-authn-authz/rbac/」を参照
3. クラスタに変更を適用します。

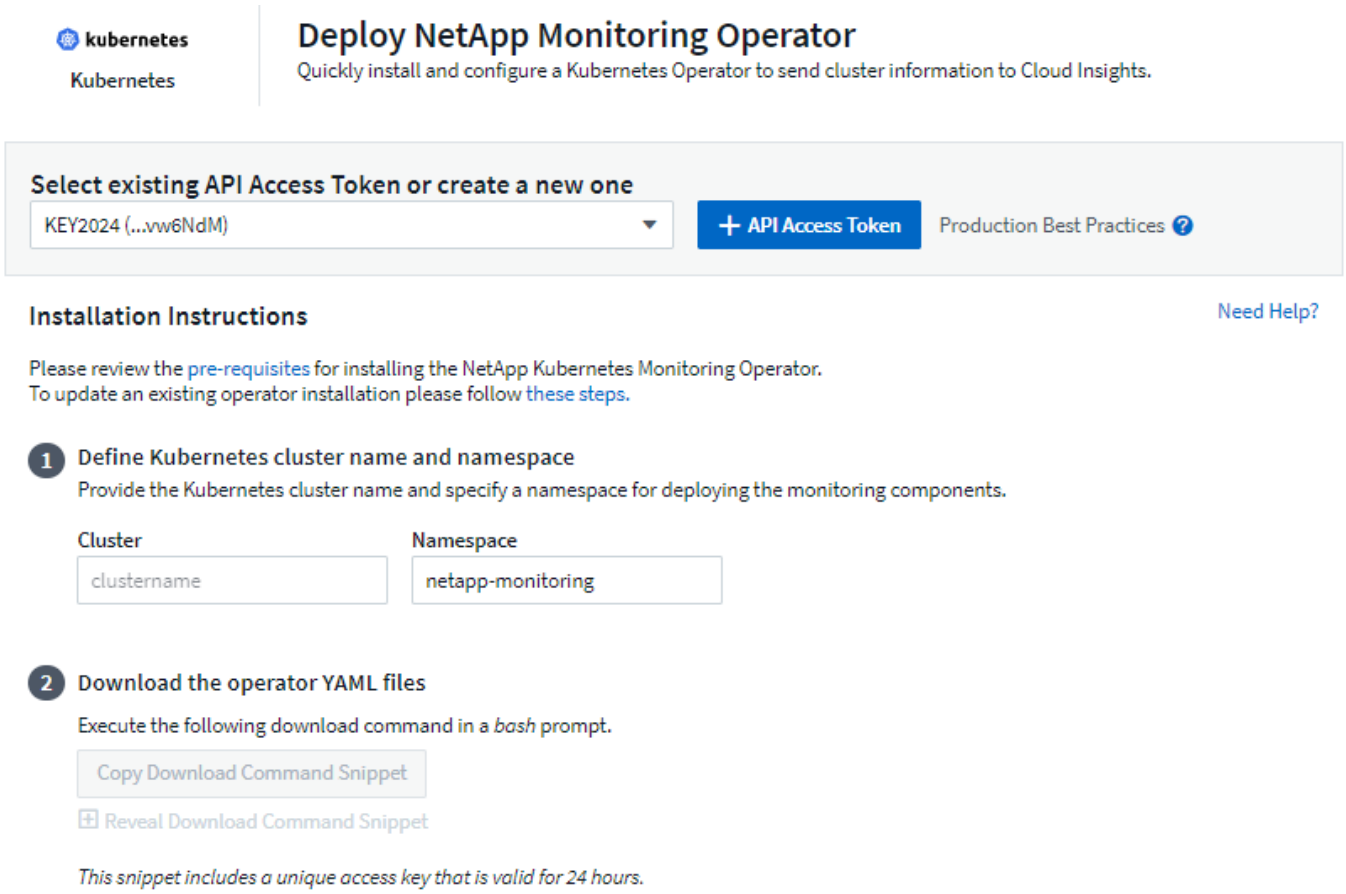
Kubernetes Monitoring Operatorのインストールと設定

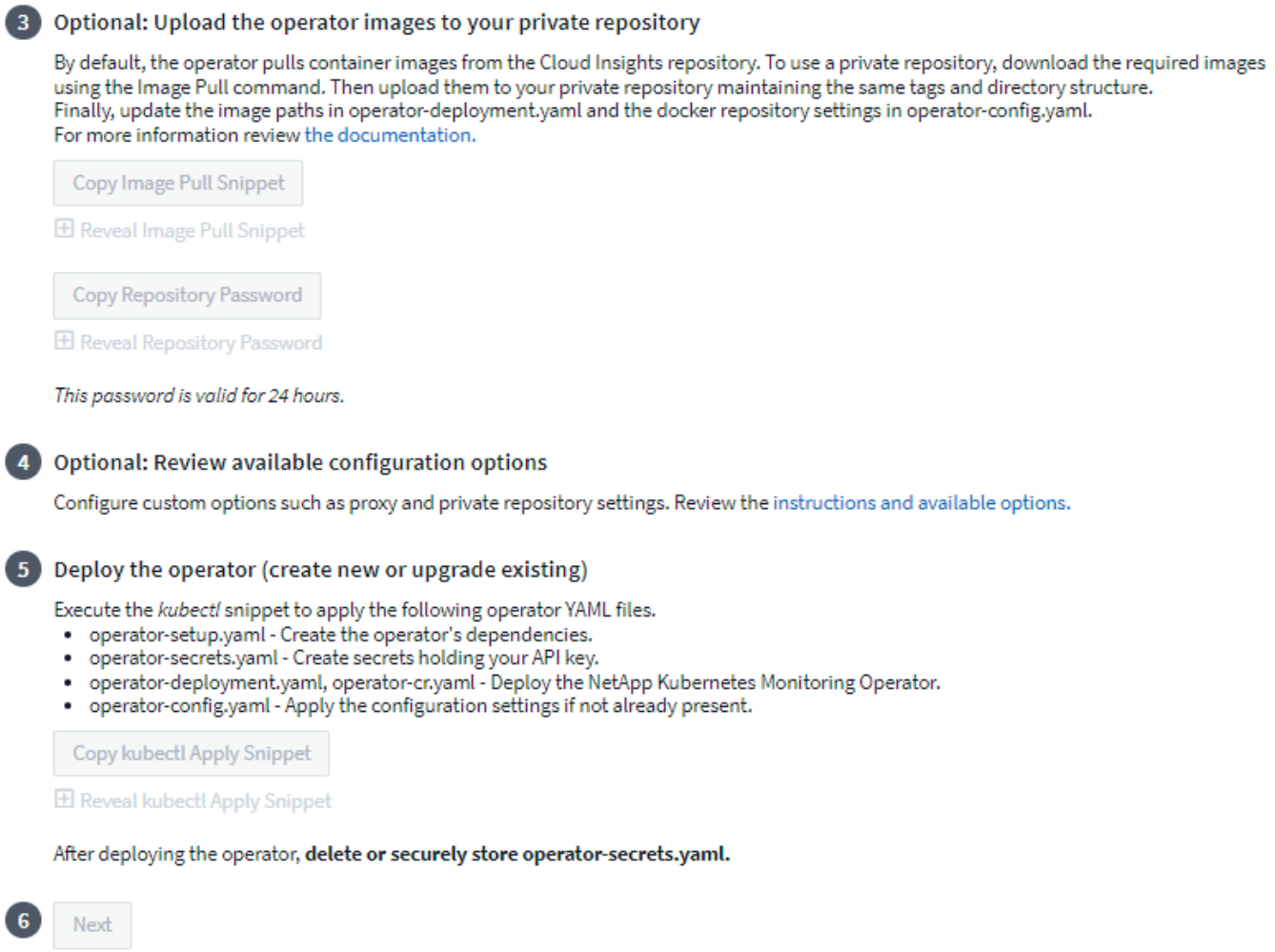
Data Infrastructure Insightsは、Kubernetesコレクション向けの「Kubernetes Monitoring Operator」を提供しています。新しいオペレータを導入するには、* Kubernetes > Collectors >+ Kubernetes Collector *に移動します。

Kubernetes Monitoring Operatorをインストールする前に

を参照してください "前提条件" Kubernetes Monitoring Operatorをインストールまたはアップグレードする前のドキュメント。

Kubernetes Monitoring Operatorのインストール





Kubernetesに**Kubernetes Monitoring Operator**エージェントをインストールする手順は次のとおりです。

1. 一意のクラスタ名およびネームスペースを入力してください。実行中の場合 をアップグレードして 以前のKubernetes Operatorで、同じクラスタ名とネームスペースを使用します。
2. これらを入力すると、ダウンロードコマンドスニペットをクリップボードにコピーできます。
3. スニペットを a_bash_window に貼り付け、実行します。Operatorインストールファイルがダウンロードされます。スニペットには固有のキーがあり、24時間有効です。
4. カスタムリポジトリまたはプライベートリポジトリがある場合は、オプションのImage Pullスニペットをコピーし、a_bash_shellに貼り付けて実行します。画像がプルされたら、プライベートリポジトリにコピーします。必ず同じタグとフォルダ構造を維持してください。_operator-deployment.yaml_のパスと_operator-config.yaml_のDockerリポジトリ設定を更新します。
5. 必要に応じて、プロキシやプライベートリポジトリの設定など、使用可能な設定オプションを確認します。あなたはについてもっと読むことができます "設定オプション"。
6. 準備ができたら、kubectl Applyスニペットをコピーしてダウンロードし、実行してOperatorをデプロイします。
7. インストールが自動的に開始されます。完了したら、[*Next*]ボタンをクリックします。
8. インストールが完了したら、[*Next*]ボタンをクリックします。また、_operator-secrets.yaml_fileを削除するか、安全に保存してください。

プロキシを使用している場合は、 プロキシを設定します。

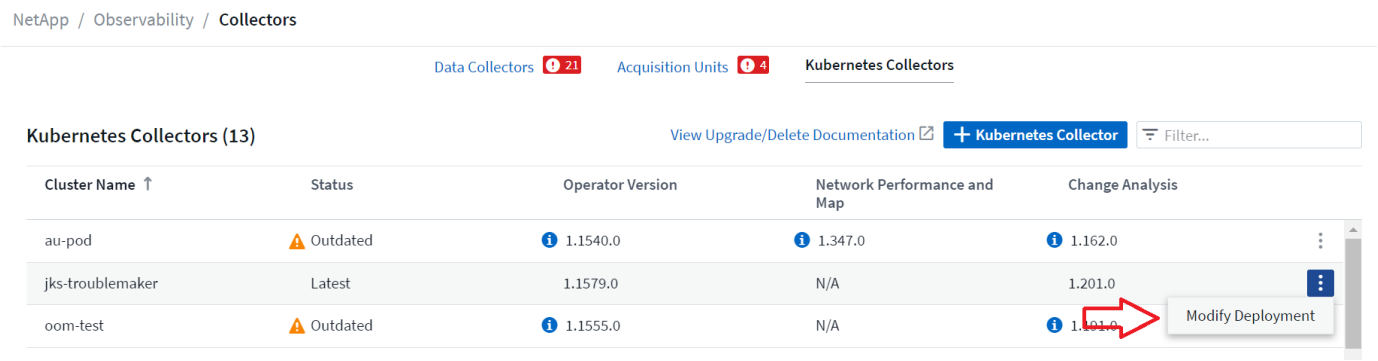
カスタムリポジトリをお持ちの場合は、 カスタム/プライベートDockerリポジトリを使用する。

Kubernetes監視コンポーネント

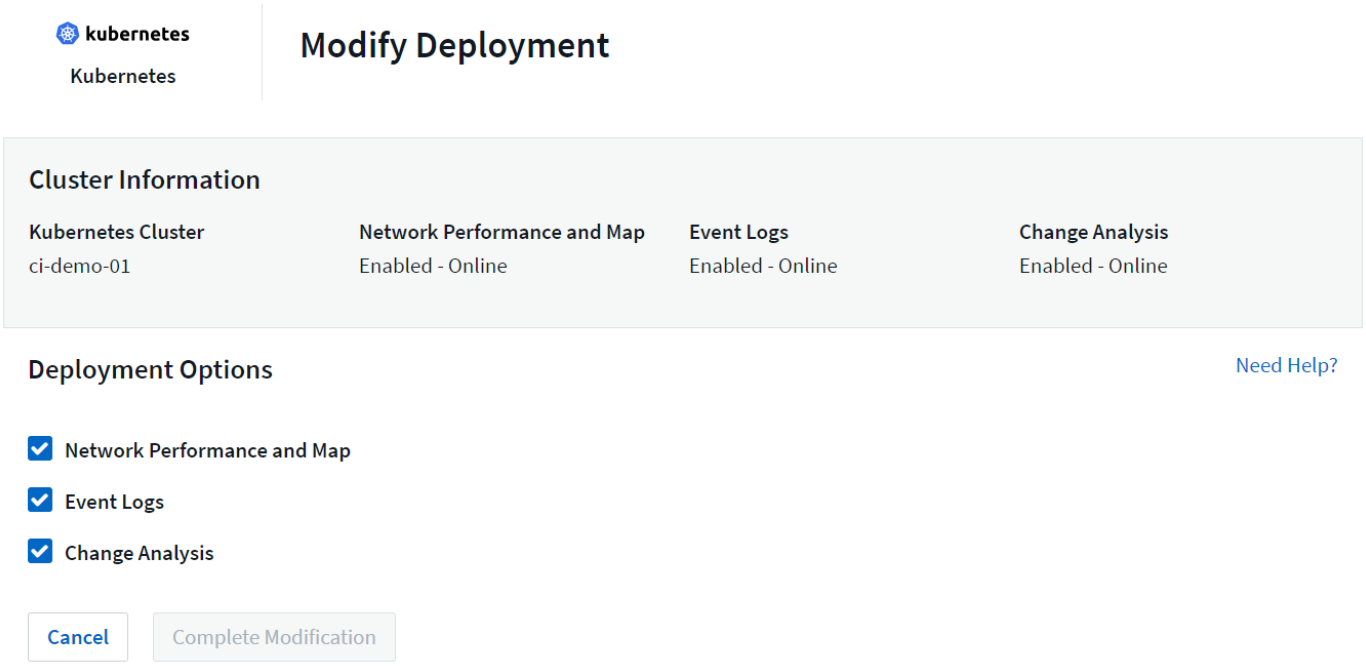
Data Infrastructure Insights Kubernetes Monitoringは、次の4つの監視コンポーネントで構成されます。

- クラスタ指標
- ネットワークパフォーマンスとマップ（オプション）
- イベントログ（オプション）
- 変更分析（オプション）

上記のオプションコンポーネントは、各Kubernetesコレクタに対してデフォルトで有効になっています。特定のコレクタ用のコンポーネントが必要ないと判断した場合は、* Kubernetes > Collectors *に移動し、画面右側のコレクタの「three dots」メニューから_Modify Deployment_を選択して無効にできます。



画面には各コンポーネントの現在の状態が表示され、必要に応じてそのコレクタのコンポーネントを無効または有効にすることができます。



をアップグレードして

最新の**Kubernetes Monitoring Operator**へのアップグレード

既存のOperatorにAgentConfigurationが存在するかどうかを確認します（ネームスペースがdefault_netapp-monitoring_でない場合は、適切なネームスペースに置き換えてください）。

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-monitoring-
configuration
AgentConfigurationが存在する場合：
```

- をインストールします 既存の演算子の上にある最新の演算子。
  - 確認してください 最新のコンテナイメージを取得します カスタムリポジトリを使用している場合。

AgentConfigurationが存在しない場合は、次の手順を実行します。

- クラスタ名がData Infrastructure Insightsで認識される名前であることをメモします（ネームスペースがデフォルトのNetApp監視機能でない場合は、適切なネームスペースで置き換えてください）。

  ```
   kubectl -n netapp-monitoring get agent -o
  jsonpath='{.items[0].spec.cluster-name}'
  * 既存の
  Operatorのバックアップを作成します（ネームスペースがデフォルトのネットアップ監視機能になっていない場合は、適切なネームスペースで置き換えてください）。
  ```

  ```
   kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
  * <<to-remove-the-kubernetes-monitoring-operator,をアンインストールします>>
  既存の演算子。
  * <<installing-the-kubernetes-monitoring-operator,をインストールします>>
  最新の演算子。
  ```

  - 同じクラスタ名を使用してください。
  - 最新のOperator YAMLファイルをダウンロードしたら、展開する前に、agent_backup.yamlにあるカスタマイズをダウンロードしたoperator-config.yamlに移植します。
  - 確認してください 最新のコンテナイメージを取得します カスタムリポジトリを使用している場合。

Kubernetes Monitoring Operatorの停止と起動

Kubernetes Monitoring Operatorを停止するには：

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Kubernetes Monitoring Operatorを起動するには：
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

アンインストール中です

Kubernetes Monitoring Operatorを削除するには

Kubernetes Monitoring Operatorのデフォルトのネームスペースは「netapp-monitoring」です。 独自のネームスペースを設定した場合は、それらのネームスペースと、以降のすべてのコマンドおよびファイルを置き換えます。

新しいバージョンの監視オペレータは、次のコマンドを使用してアンインストールできます。

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

監視オペレータが専用のネームスペースに配置されている場合は、ネームスペースを削除します。

```
 kubectl delete ns <NAMESPACE>
```
最初のコマンドが「リソースが見つかりません」を返した場合は、次の手順に従って古いバージョンの監視オペレータをアンインストールします。

次の各コマンドを順番に実行します。現在のインストール状況によっては、これらのコマンドの一部で「オブジェクトが見つかりません」というメッセージが返される場合があります。これらのメッセージは無視してかまいません。

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

セキュリティコンテキスト制約が事前に作成されている場合は、次の手順を実行します。

```
kubectl delete scc telegraf-hostaccess
```

Kubeステートメトリックについて

NetApp Kubernetes Monitoring Operatorは、他のインスタンスとの競合を回避するために独自のkube-state-metricsをインストールします。

Kube-State-Metricsの詳細については、を参照してください。 "このページです"。

オペレータの設定/カスタマイズ

これらのセクションでは、オペレータ設定のカスタマイズ、プロキシの操作、カスタムまたはプライベートDockerリポジトリの使用、OpenShiftの操作について説明します。

設定オプション

最も一般的に変更される設定は、_AgentConfiguration_customリソースで構成できます。オペレータを配備する前に、_operator-config.yaml_fileを編集して、このリソースを編集できます。このファイルには、コメントアウトされた設定例が含まれています。のリストを参照してください "使用可能な設定" 演算子の最新バージョン。

オペレータが配備された後で、次のコマンドを使用してこのリソースを編集することもできます。

```
kubectl -n netapp-monitoring edit AgentConfiguration
```

展開したオペレータのバージョンが`AgentConfiguration`をサポートしているかどうかを確認するには、次のコマンドを実行します。

```
kubectl get crd agentconfigurations.monitoring.netapp.com
```

「`Error from server (NotFound)`」というメッセージが表示された場合は、`AgentConfiguration`を使用する前にオペレータをアップグレードする必要があります。

プロキシサポートを設定しています

Kubernetes Monitoring Operatorをインストールするために、環境内でプロキシを使用できる場所は2つあります。同じプロキシシステムでも、別のプロキシシステムでもかまいません。

- インストールコードスニペット（「curl」を使用）の実行中に、スニペットが実行されるシステムをData Infrastructure Insights環境に接続するために必要なプロキシ
- ターゲットのKubernetesクラスタがData Infrastructure Insights環境と通信するために必要なプロキシ

これらのいずれかまたは両方にプロキシを使用する場合、Kubernetes Operating Monitorをインストールするには、まず、Data Infrastructure Insights環境との通信が良好になるようにプロキシが設定されていることを確認する必要があります。プロキシがあり、Operatorをインストールするサーバ/ VMからData Infrastructure Insightsにアクセスできる場合は、プロキシが適切に設定されている可能性があります。

Kubernetes Operating Monitorのインストールに使用するプロキシについては、Operatorをインストールする前に、_http_proxy/https_proxy_environment変数を設定します。一部のプロキシ環境では'_no_proxy環境変数も設定する必要があります

変数を設定するには、Kubernetes Monitoring Operatorをインストールする前に、システム*で次の手順を実行します。

1. 現在のユーザの *https_proxy* 変数と _http_proxy_environment 変数を設定します。
   a. セットアップするプロキシに認証（ユーザ名/パスワード）がない場合は、次のコマンドを実行します。

```
 export https_proxy=<proxy_server>:<proxy_port>
```

. . セットアップするプロキシに認証（ユーザ名/パスワード）が設定されている場合は、次のコマンドを実行します。

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

KubernetesクラスタがData Infrastructure Insights環境と通信するために使用するプロキシの場合は、以下の手順をすべて読んでからKubernetes Monitoring Operatorをインストールします。

Kubernetes Monitoring Operatorをデプロイする前に、operator-config.yamlのAgentConfigurationのプロキシセクションを設定します。

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

カスタムまたはプライベートの**Docker**リポジトリを使用する

Kubernetes監視オペレータは、デフォルトで、Data Infrastructure Insightsリポジトリからコンテナイメージを取得します。監視のターゲットとして使用されているKubernetesクラスタがあり、そのクラスタがカスタムまたはプライベートのDockerリポジトリまたはコンテナレジストリからコンテナイメージのみをプルするように構成されている場合は、Kubernetes Monitoring Operatorが必要とするコンテナへのアクセスを設定する必要があります。

NetApp Monitoring Operatorのインストールタイルから[Image Pull Snippet]を実行します。このコマンドを実行すると、Data Infrastructure Insightsリポジトリにログインし、オペレータが必要とするすべてのイメージを取得して、Data Infrastructure Insightsリポジトリからログアウトします。プロンプトが表示されたら、指定したリポジトリの一時パスワードを入力します。このコマンドは、オプション機能を含む、オペレータが使用するすべてのイメージをダウンロードします。これらの画像がどの機能に使用されるかについては、以下を参照してください。

Core Operator Functionality and Kubernetes Monitoringの略

- ネットアップによる監視
- ci-kube-rbac-proxy
- CI-KSM
- CI-テレグラフ
- distroless-root-user

イベントログ

- CI-fluent-bit
- ci-kubernetes-event-exporter

ネットワークのパフォーマンスとマップ

- ci-net-observerの略

社内のポリシーに従って、オペレータ用の Docker イメージをプライベート / ローカル / エンタープライズ Docker リポジトリにプッシュします。リポジトリ内のこれらのイメージへのイメージタグとディレクトリパスが、Data Infrastructure Insightsリポジトリ内のイメージタグとディレクトリパスと一致していることを確認します。

operator-deployment.yamlでmonitoring-operatorデプロイメントを編集し、プライベートDockerリポジトリを使用するようにすべてのイメージ参照を変更します。

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

operator-config.yamlのAgentConfigurationを編集して、新しいDockerリポジトリの場所を反映します。プライベートリポジトリ用に新しいimagePullSecretを作成します。詳細については、_ https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/_を参照してください

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here:
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

OpenShift の手順

OpenShift 4.6以降で実行している場合は、_runPrivileged_settingを有効にするには、_operator-config.yaml_でAgentConfigurationを編集する必要があります。

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

OpenShiftは、一部のKubernetesコンポーネントへのアクセスをブロックする可能性のある追加のセキュリテ

ィレベルを実装する場合があります。

秘密に関する注意事項

Kubernetes Monitoring Operatorのシークレットをクラスタ全体で表示する権限を削除するには、インストール前に_operator-setup.yaml_fileから次のリソースを削除します。

```
 ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-clusterrolebinding
```

アップグレードの場合は、クラスタからリソースも削除します。

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

変更分析が有効になっている場合は、_AgentConfiguration_or_operator -config.yaml_を変更して、変更管理セクションのコメントを解除し、変更管理セクションの下に_kindsToIgnoreFromWatch：'"secrets"'_を含めます。この行の一重引用符と二重引用符の存在と位置に注意してください。

```
# change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Kubernetes のチェックサムの検証

Data Infrastructure Insightsエージェントインストーラは整合性チェックを実行しますが、ダウンロードしたアーティファクトをインストールまたは適用する前に独自の検証を実行することもできます。デフォルトのダウンロードおよびインストールではなく、ダウンロードのみの操作を実行するには、 UI から取得したエージェントインストールコマンドを編集し、末尾の「インストール」オプションを削除します。

次の手順を実行します。

1. 指示に従ってエージェントインストーラスニペットをコピーします。
2. スニペットをコマンドウィンドウに貼り付ける代わりに、テキストエディタに貼り付けます。
3. コマンドから末尾の「--install」を削除します。
4. コマンド全体をテキストエディタからコピーします。

5. 次に、コマンドウィンドウ（作業ディレクトリ内）に貼り付けて実行します。
   - Download and install （デフォルト）：

```
 installerName=cloudinsights-rhel_centos.sh … && sudo -E -H
./$installerName --download --install
```

** ダウンロードのみ：

```
installerName=cloudinsights-rhel_centos.sh … && sudo -E -H
./$installerName --download
```

download-onlyコマンドを実行すると、必要なすべてのアーティファクトがData Infrastructure Insightsから作業ディレクトリにダウンロードされます。アーティファクトには次のものがありますが、これらに限定することはできません。

- インストールスクリプト
- 環境ファイル
- YAMLファイル
- 署名済みチェックサムファイル（ SHA256 署名）
- 署名の検証に使用する PEM ファイル（ NetApp_cert.pem ）

インストールスクリプト、環境ファイル、 YAML ファイルは、目視検査を使用して検証できます。

PEM ファイルは、フィンガープリントが次のようになっていることを確認することで検証できます。

```
 1A918038E8E127BB5C87A202DF173B97A05B4996
```

具体的には、

```
 openssl x509 -fingerprint -sha1 -noout -inform pem -in netapp_cert.pem
```

署名済みチェックサムファイルは、 `PEM` ファイルを使用して確認できます。

```
 openssl smime -verify -in sha256.signed -CAfile netapp_cert.pem -purpose
any
```

すべてのアーティファクトが正常に検証されたら、次のコマンドを実行してエージェントのインストールを開始できます。

```
sudo -E -H ./<installation_script_name> --install
```

公差と接線（**Tolerations and Taints**）

NetApp-ci-telegraf-ds_、*NetApp-CI-fluent-bit-ds*、および_NetApp-CI-net-observer-l4-DS_DaemonSetsは、すべてのノードのデータを正しく収集するために、クラスタ内のすべてのノードでポッドをスケジュールする必要があります。オペレータは、いくつかの既知の*テイント*に耐えられるように設定されています。ノードにカスタムのtaintsを設定して、すべてのノードでポッドが実行されないようにしている場合は、それらのtaintsに* toleration *を作成できます "（*AgentConfiguration*）をクリックします"。クラスタ内のすべてのノードにカスタムテイントを適用した場合は、オペレータの導入に必要な許容範囲を追加して、オペレータポッドをスケジュールおよび実行できるようにする必要があります。

Kubernetesの詳細はこちらをご覧ください "塗料および耐性"。

に戻ります "* NetApp Kubernetes監視オペレータのインストール*ページ"

トラブルシューティング

Kubernetes Monitoring Operatorの設定で問題が発生した場合に試すべきこと：

問題	次の操作を実行します
Kubernetes 永続ボリュームと対応するバックエンドストレージデバイスの間にハイパーリンク / 接続がありません。My Kubernetes Persistent Volume がストレージサーバのホスト名を使用して設定されます。	手順に従って既存の Tegraf エージェントをアンインストールし、最新の Tegraf エージェントを再インストールします。Telegrafバージョン2.0以降を使用しており、KubernetesクラスタストレージがData Infrastructure Insightsによってアクティブに監視されている必要があります。

問題	次の操作を実行します
ログに次のようなメッセージが表示されます。 E0901 15:21:39.962145 1 reflector.go:178]k8s.io/kube-state-metrics/internal/store/builder.go:352:リストに失敗しました*v1.MutatingWebhookConfiguration:サーバーは要求されたリソースを見つけることができませんでした E0901 15:21:43.168161 1 reflector.go:178]k8s.io/kube-state-metrics/internal/store/builder.go:352:リストに失敗しました*v1 Lease:サーバーは要求されたリソースを見つけることができませんでした(GET leases.coordination.k8s.io) など	これらのメッセージは、1.20より前のバージョンのKubernetesでkube-state-metricsバージョン2.0.0以上を実行している場合に発生する可能性があります。 Kubernetesのバージョンを取得するには： *kubectl*バージョン kube-state-metricsバージョンを取得するには、次の手順を実行します。 *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* これらのメッセージが発生しないように、ユーザはkube-state-metrics展開を変更して、次のリースを無効にすることができます。 *mutatingwebhookconfigurations* 検証webhookconfigurations_ *volumeattachments*リソース 具体的には、次のCLI引数を使用できます。 resources=certificatesigningrequests, configmaps, cronjobs, daemonsets, deployments, endpoints, horizontalpodautoscalers, ingresses, jobs, limitranges, namespaces, networkpolicies, poddisruptionbudgets, pods, ReplicaSets, replicationcontrollasses, resourcequotases, secrets, resourcequotases, secrets, services, storage, storefuls. デフォルトのリソースリストは次のとおりです。 certificatesigningrequests, configmaps, cronjobs, daemonsets, deployments, endpoints, horizontalpododautoscalers, ingresses, jobs, leases, limitranges, mutatingwebhookconfiguration, namespaces, networkpersistentvolumes, poddisruptionbudgets, pers, persistentresets, pondsets, podsets, postresets, replicassess, replicastess, replicatess, replicastorets, replicast 検証Webhook構成’ボリューム添付ファイル"\y"ケンショウ:Webhookコウセイ’ボリュームアタッチメント

問題	次の操作を実行します
Telegrafから次のようなエラーメッセージが表示されますが、Telegrafは起動して実行されます。 10月11日14:23:41 IP-172-31-39-47 systemd[1]: InfluxDBにメトリックを報告するプラグイン駆動のサーバーエージェントを起動しました。 10 月 11 日 14 ： 23 ： 41 IP-172-41-39-47 テレグラム [1827] ： time="2021 - 10-11T14 ： 23 ： 41Z" level= error msg=" キャッシュディレクトリの作成に失敗しました。/etc/telegraf/.cache/snowflake 、err:mkdir /etc/telegraf/.ca CHE：権限が拒否されました。無視\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 10月11日14：23：41 IP-172-31-39-47 telegraf [1827] ：time="2021-10-11T14：23：41Z" level=error msg="failed to open.無視されます。/etc/telegraf/.cache/snowflake/ocsp_response_cache.jsonを開きます。no such ファイルまたはディレクトリ\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 10月11日14:23:41 IP-172-31-39-47 telegraf [1827]: 2021-10-11T14:23:41Z I! Telegraf 1.19.3 を起動しています	これは問題と呼ばれています。 を参照してください "この GitHub の記事" 詳細：Tegraf が起動して動作している限り、ユーザはこのエラーメッセージを無視できます。
Kubernetesで、Telegrafポッドが次のエラーを報告しています。 "mountstats情報の処理中にエラーが発生しました ：mountstatsファイルを開けませんでした ：/hostfs/proc/1/mountstats、エラー ：open/hostfs/proc/1/mountstats：権限が拒否されました"	SELinuxを有効にして強制すると、TelegrafポッドがKubernetesノードの/proc/1/mountstatsファイルにアクセスできなくなる可能性があります。この制限を克服するには、agentconfigurationを編集し、runPrivileged設定を有効にします。詳細については、 "OpenShift の手順"。
Kubernetesで、Telegraf ReplicaSetポッドが次のエラーを報告しています。 [プラグインのinputs.prometheus]エラー：keypair /etc/kubernetes/pki/etcd/server.crtをロードできませんでした：/etc/kubernetes/pki/etcd/server.key：open /etc/kubernetes/pki/etcd/server.crt：該当するファイルまたはディレクトリはありません	Telegraf ReplicaSet ポッドは、マスターまたは etcd 用に指定されたノード上で実行することを目的としています。これらのノードのいずれかで ReplicaSet ポッドが実行されていない場合は、これらのエラーが発生します。マスター / etcd ノードに汚染があるかどうかを確認します。その場合は、 Telegraf ReplicaSet 、テレグラム af-RS に必要な忍容を追加します。 たとえば、ReplicaSet… kubectl edit rs telegraf-rs 仕様に適切な公差を追加します。次に、 ReplicaSet ポッドを再起動します。

問題	次の操作を実行します
PSP/PSA環境があります。これはモニタリングオペレータに影響しますか？	KubernetesクラスタがPod Security Policy（PSP）またはPod Security Admission（PSA）を使用して実行されている場合は、最新のKubernetes Monitoring Operatorにアップグレードする必要があります。PSP/PSAをサポートしている現在のオペレータにアップグレードするには、次の手順に従います。 1. をアンインストールします 以前の監視オペレータ： kubectl delete agent agent-monitoring-netapp-n netapp-monitoring kubectlによってネットアップによる監視が削除されます kubectlはCRD agents.monitoring.netapp.comを削除します kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 2. をインストールします モニタリングオペレータの最新バージョン。
Operatorを展開しようとして問題が発生しましたが、PSP/PSAを使用しています。	1.次のコマンドを使用してエージェントを編集します。 kubectl -n <name-space>編集エージェント 2.「security-policy-enabled」を「false」に設定します。これにより、PodセキュリティポリシーとPodセキュリティアドミッションが無効になり、オペレータが展開できるようになります。次のコマンドを使用して確認します。 kubectl get psp（Pod Security Policy removedを表示する必要があります） kubectl get all -n <namespace>
grep -i psp (should show that nothing is found)	「ImagePullBackoff」エラーが発生しました
これらのエラーは、カスタムまたはプライベートのDockerリポジトリがあり、Kubernetes Monitoring Operatorを適切に認識するように設定していない場合に表示されることがあります。 詳細はこちら カスタム/プライベートリポジトリの設定について	監視オペレータの配置に問題 を使用していますが、現在のドキュメントでは解決できません。

問題	次の操作を実行します
次のコマンドの出力をキャプチャまたはメモし、テクニカルサポートチームに連絡します。 `kubectl -n netapp-monitoring get all` `kubectl -n netapp-monitoring describe all` `kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true` `kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true`	Operator名前空間のNet-Observer（ワークロードマップ）ポッドがCrashLoopBackOffにある
これらのポッドは、Network ObservabilityのWorkload Mapデータコレクタに対応しています。以下をお試しください。 •いずれかのポッドのログをチェックして、カーネルの最小バージョンを確認します。例： --- {"ci-tenant-id"："your-tenant-id"、"collector-cluster"："your-k8s-cluster-name"、"environment"："prod"、"level"："error"、"msg"："検証に失敗しました。理由：カーネルバージョン3.10.0が最小カーネルバージョン4.18.0よりも小さい、"time"："2022-11-09T08:23:08Z"} --- •Net-Observerポッドを使用するには、Linuxカーネルのバージョンが4.18.0以上である必要があります。「uname -r」コマンドを使用してカーネルのバージョンを確認し、4.18.0以上であることを確認します	PodはOperatorネームスペース（デフォルト：netapp-monitoring）で実行されているが、Queriesのワークロードマップまたは Kubernetes指標のデータがUIに表示されない
K8Sクラスタのノードの時間設定を確認します。監査およびデータレポートを正確に作成するには、Network Time Protocol（NTP；ネットワークタイムプロトコル）またはSimple Network Time Protocol（SNTP；簡易ネットワークタイムプロトコル）を使用してAgentマシンの時刻を同期することを強く推奨します。	Operator名前空間の一部のnet-observerポッドがPending状態です

問題	次の操作を実行します
net-observerはデーモンセットであり、Kubernetesクラスタの各ノードでポッドを実行します。 •保留状態のポッドをメモし、CPUまたはメモリのリソース問題が発生しているかどうかを確認します。必要なメモリとCPUがノードにあることを確認します。	Kubernetes Monitoring Operatorをインストールした直後にログに次のようなメッセージが表示されます。 [プラグインのinputs.prometheus]エラー：\http://kube-state-metricsへの要求エラー。<namespace>.svc.cluster.local：8080/metrics：get\ http://kube-state-metrics <namespace>.svc.cluster.local：8080/metrics：dial tcp：lookup kube-state-metrics 。<namespace>.svc.cluster.local：該当するホストはありません。
このメッセージが表示されるのは、通常、_KSM_PODが起動する前に、新しいオペレータがインストールされ、_テレ グラム-RS_PODが稼働している場合のみです。これらのメッセージは、すべてのポッドが実行されると停止します。	クラスタに存在するKubernetes CronJobsについて収集された指標が表示されません。
Kubernetesのバージョンを確認します（ `kubectl version`）。 v1.20.x以下の場合、これは想定される制限です。 Kubernetes Monitoring Operatorで導入されたkube-state-metricsリリースでは、v1.cronjobのみがサポートされます。 Kubernetes 1.20.x以前では、cronjobリソースはv1beta.cronjobにあります。その結果、kube-state-metricsはcronjobリソースを見つけることができません。	オペレータのインストール後、telegraf-DSポッドがCrashLoopBackOffに入り、PODログに「su：Authentication failure」と表示されます。
_AgentConfiguration_のtelegrafセクションを編集し、set_dockerMetricCollectionEnabled_をfalseに設定します。詳細については、オペレータのを参照して"設定オプション"ください。注: Data Infrastructure Insights Federal Editionを使用している場合、_su_の使用が制限されているユーザーはDockerメトリクスを収集できません。Dockerソケットにアクセスするには、telegrafコンテナをrootとして実行するか、_su_を使用してtelegrafユーザーをDockerグループに追加する必要があるためです。Dockerメトリック収集と_su_の使用はデフォルトで有効になっています。両方を無効にするには、_AgentConfiguration_fileの_telegraf.docker_entryを削除します。…spec:…telegraf:… -name：docker run-mode： -DaemonSet 置換： -key：docker_unix_sock_placeholder 値：unix：//run/docker.sock……	Telegrafログに次のようなエラーメッセージが繰り返し表示されます。 来い! [agent]出力への書き込み中にエラーが発生しました。http：Post "\https：//<tenant_url>/rest/v1/lake/ingest/influxdb"：context deadline exceeded (Client. ヘッダー待機中にタイムアウトを超過しました）
_AgentConfiguration_およびincrease_outputTimeout_のtelegrafセクションを10秒に編集します。詳細については、オペレータのを参照してください "設定オプション"。	一部のイベントログの_involvedobject_dataが見つかりません。
次の手順を実行していることを確認してください： "権限" 上記のセクション。	2つの監視オペレータポッド（netapp-ci-monitoring-operator-pod <pod>とmonitoring-operator-pod）が実行されているのはなぜ<pod>ですか？

問題	次の操作を実行します
2023年10月12日付けで、Data Infrastructure Insightsは、ユーザへのサービス向上のためにオペレータをリファクタリングしました。これらの変更を完全に採用するには古いオペレータを削除します。、とが必要です。新しいものを取り付ける	Kubernetesイベントが予期せずData Infrastructure Insightsに報告されなくなりました。
event-exporterポッドの名前を取得します。 `kubectl -n netapp-monitoring get pods`	grep event-exporter
awk '{print $1}'	sed 's/event-exporter./event-exporter/` 「netapp-ci-event-exporter」または「event-exporter」のいずれかにする必要があります。 次に、監視エージェントを編集します。 `kubectl -n netapp-monitoring edit agent`をクリックし、log_fileの値を設定して、前の手順で見つけた適切なイベントエクスポータポッド名を反映します。 具体的には、log_fileは「/var/log/containers/netapp-ci-event-exporter.log」または「/var/log/containers/event-exporter 。**log**」のいずれかに設定する必要があります。 **….** **fluent-bit:** **…** **- name: event-exporter-ci** **substitutions:** **- key: LOG_FILE** **values:** **- /var/log/containers/netapp-ci-event-exporter**.log … …. 別の方法として、 をアンインストールします および再インストール エージェント。
リソースが不足しているため、Kubernetes Monitoring Operatorによってデプロイされたポッドがクラッシュしています。	Kubernetes Monitoring Operatorを参照 "設定オプション" 必要に応じてCPUやメモリの制限を増やします。
イメージがないか無効な設定が原因で、netapp-ci-kube-state-metricsポッドが起動しないか準備完了状態になりました。これでStatefulSetが停止し、設定の変更がnetapp-ci-kube-state-metricsポッドに適用されなくなりました。	StatefulSetは "切断" 状態。設定の問題を修正したら、netapp-ci-kube-state-metricsポッドをバウンスします。
NetApp-ci-kube-state-metricsポッドがKubernetes Operatorのアップグレード実行後に起動せず、ErrImagePullがスローされる（イメージをプルできない）。	ポッドを手動でリセットしてみてください。

問題	次の操作を実行します
Kubernetesクラスタの[Log Analysis]で、「Event discarded as being older then maxEventAgeSeconds」というメッセージが確認されています。	Operator_agentconfiguration_を変更し、*event-exporter-maxEventAgeSeconds*（60秒）、*event-exporter-kubeQPS*（100）、および_event-exporter-kubeBurst_（500）を増やします。これらの設定オプションの詳細については、を参照してください。 "設定オプション" ページ
Telegrafが警告するか、ロック可能なメモリが不足しているためにクラッシュします。	基盤となるオペレーティングシステム/ノードでTelegrafのロック可能メモリの制限を増やしてみてください。制限値を増やすことができない場合は'NKMOエージェントの構成を変更して'_unprotected_to_true_に設定します これにより、Telegrafはロックされたメモリページを予約しないように指示します。復号化されたシークレットがディスクにスワップアウトされる可能性があるため、セキュリティリスクが発生する可能性がありますが、ロックされたメモリを予約できない環境では実行できます。_unprotected_configurationオプションの詳細については、 "設定オプション" ページ

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Kubernetes監視オペレータの設定オプション

。 "Kubernetes監視オペレータ" 設定はカスタマイズできます。

次の表に、_AgentConfiguration_ファイルに使用できるオプションを示します。

コンポーネント	オプション	説明
エージェント		オペレータがインストールできるすべてのコンポーネントに共通の設定オプション。これらは「グローバル」オプションと見なすことができます。
	dockerrepo	Data Infrastructure Insights Dockerリポジトリと比較して、お客様のプライベートDockerリポジトリからイメージを取得するためのdockerRepoオーバーライド。デフォルトはData Infrastructure Insights Dockerリポジトリ
	dockerImagePullSecretの略	オプション:顧客のプライベートリポジトリのシークレット
	クラスタ名	すべてのお客様のクラスタ間でクラスタを一意に識別するフリーテキストフィールド。これは、Data Infrastructure Insightsのテナント全体で一意である必要があります。デフォルトでは、UIで[Cluster Name]フィールドに入力します

コンポーネント	オプション	説明
	プロキシ の形式で入力し プロキシ： サーバ： ポート： ユーザ名： パスワード： NoProxy： isTelegrafProxyEnabled： isAuProxyEnabled： isFluentbitProxyEnabled： isCollectorProxyEnabled ：	プロキシを設定する場合はオプションです。これは通常、顧客の法人代理店です。
テレグラフ		オペレータのTelegrafインストールをカスタマイズできる設定オプション
	collectionInterval	指標収集間隔（秒）（最大=60秒）
	dsCpuLimit	Telegraf DSのCPU制限
	dsMemLimit	Telegraf DSのメモリ制限
	dsCpuRequest	Telegraf DSのCPU要求
	dsMemRequest	Telegraf DSのメモリ要求
	rsCpuLimit	Telegraf RSのCPU制限
	rsMemLimit	Telegraf RSのメモリ制限
	rsCpuRequest	Telegraf RSのCPU要求
	rsMemRequest	テレグラフRSのメモリ要求
	runPrivileged	特権モードでTelegrafコンテナを実行します。KubernetesノードでSELinuxが有効になっている場合は、このをtrueに設定します
	バッチサイズ	を参照してください "Telegraf設定ドキュメント"
	BufferLimit	を参照してください "Telegraf設定ドキュメント"
	RoundIntervalの略	を参照してください "Telegraf設定ドキュメント"
	collectionJitter	を参照してください "Telegraf設定ドキュメント"
	精度	を参照してください "Telegraf設定ドキュメント"
	flushInterval（フラッシュ間隔）	を参照してください "Telegraf設定ドキュメント"
	FlushJitter（フラッシュジッタ	を参照してください "Telegraf設定ドキュメント"
	outputTimeout	を参照してください "Telegraf設定ドキュメント"
	dsTolerations	Telegraf-DS追加の許容値。

コンポーネント	オプション	説明
	rsTolerations	Telegraf-RS追加許容値。
	skipProcessorsAfterAggregators	を参照してください "Telegraf設定ドキュメント"
	保護なし	を参照してください "既知のTelegraf問題" 。Setting_unprotected_はKubernetes Monitoring OperatorにTelegrafを `--unprotected` フラグ。
kube-state-metricsの略		Operatorのkube状態メトリックのインストールをカスタマイズできる設定オプション
	cpuLimit	kube-state-metricsデプロイメントのCPU制限
	memLimit	kube-state-metrics展開のメモリ制限
	cpuRequest	kube state metrics deploymentのCPU要求
	MemRequestの略	KUBE状態メトリクス展開のためのMEM要求
	リソース	キャプチャするリソースをカンマで区切ったリスト。例：cronjobs、デーモンセット、配置、入力、ジョブ、ネームスペース、ノード、persistentvolumeclaims、persistentvolumes、pods、ReplicaSets、resourcequotas、services、statefulsets
	許容範囲	kube-state-metrics追加の許容値。
	ラベル	kube-state-metricsでキャプチャするリソースをカンマで区切ったリスト 例：cronjobs=[*]、daemonsets=[*]、deployments=[*]、ingresses=[*]、jobs=[*]、namespaces=[*]、nodes=[*]、 persistentvolumeclaims=[*]、persistentvolumes=[*]、pods=[*]、ReplicaSets=[*]、resourcequotas=[*]、services=[*]、statefulsets=[*]
ログ		オペレータのログ収集とインストールをカスタマイズできる設定オプション
	readFromHead	true / false。fluentビットがheadからログを読み取る必要があります
	タイムアウト	タイムアウト（秒）
	DNSMode（DNSMode）	TCP / UDP、DNSのモード
	Fluent-bit-tolerationsの略	FLUENT-BIT-DSの追加許容値。
	event-exporter-tolerationsの略	イベントエクスポータの追加許容値。
	event-exporter-maxEventAgeSeconds	イベントエクスポータの最大イベント経過時間。 を参照してください https://github.com/jkroepke/resmoio-kubernetes-event-exporter

コンポーネント	オプション	説明
	runPrivileged	Fluent Bitの起動に失敗し、データベースのオープン/作成を試みた場合は、runPrivilegedをtrueに設定します。
ワークロードマップ		作業負荷マップの収集とオペレータのインストールをカスタマイズできる設定オプション
	cpuLimit	ネットオブザーバーDSのCPU制限
	memLimit	ネットオブザーバDSのメモリ制限
	cpuRequest	ネットオブザーバーDSのCPU要求
	MemRequestの略	ネットオブザーバーDSのMEM要求
	metricAggregationInterval	メトリック集約間隔（秒単位）
	bpfPollIntervalの略	BPFポーリング間隔（秒単位）
	enableDNSLookup	trueまたはfalse、DNSルックアップを有効にします
	L4 -公差	NET-OBSERVER-L4-DS追加許容値。
	runPrivileged	true/false - KubernetesノードでSELinuxが有効になっている場合は、runPrivilegedをtrueに設定します。
変更管理		Kubernetes Change Management and Analysisの構成オプション
	cpuLimit	change-observer-watch-rsのCPU制限
	memLimit	change-observer-watch-rsのメモリ制限
	cpuRequest	change-observer-watch-rsのCPU要求
	MemRequestの略	change-observer-watch-rsのMEM要求
	failureDeclarationIntervalMins	ワークロードの導入に失敗した場合に障害が発生したとマークされる間隔（分）
	deployAggrIntervalSeconds	ワークロード導入を実行中のイベントが送信される頻度
	nonWorkloadAggrIntervalSeconds	ワークロード以外の導入環境を組み合わせて送信する頻度
	termsToRedact	値が編集される環境名およびデータマップで使用される一連の正規表現 用語の例：「pwd」、「password」、「token」、「apiKey」、「api-key」、 "JWT"
	AdditionalKindsToWatch	コレクターが監視するデフォルトの種類のセットから、監視する追加の種類のコンマ区切りリスト
	kindsToIgnoreFromWatch	コレクタが監視するデフォルトの種類のセットから、監視対象から無視する種類のコンマ区切りのリスト
	logRecordAggrIntervalSeconds	コレクタからCIにログレコードを送信する頻度

コンポーネント	オプション	説明
	ウォッチトレランス	change-observer-watch-ds追加の許容値。省略された単一行形式のみ。 例：「｛key：taint1、operator：exists、effect：NoSchedule｝、｛key：taint2、operator：exists、effect：NoExecute｝」

サンプルの**AgentConfiguration**ファイル

以下は、Sample_AgentConfiguration_ファイルです。

```
apiVersion: monitoring.netapp.com/v1alpha1
kind: AgentConfiguration
metadata:
  name: netapp-ci-monitoring-configuration
  namespace: "netapp-monitoring"
  labels:
    installed-by: nkmo-netapp-monitoring

spec:
  # # You can modify the following fields to configure the operator.
  # # Optional settings are commented out and include default values for
reference
  # #   To update them, uncomment the line, change the value, and apply
the updated AgentConfiguration.
  agent:
    # # [Required Field] A uniquely identifiable user-friendly
clustername.
    # # clusterName must be unique across all clusters in your Data
Infrastructure Insights environment.
    clusterName: "my_cluster"

    # # Proxy settings. The proxy that the operator should use to send
metrics to Data Infrastructure Insights.
    # # Please see documentation here: https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#configuring-proxy-
support
    # proxy:
    #   server:
    #   port:
    #   noproxy:
    #   username:
    #   password:
    #   isTelegrafProxyEnabled:
    #   isFluentbitProxyEnabled:
    #   isCollectorsProxyEnabled:
```

```
    # # [Required Field] By default, the operator uses the CI repository.
    # # To use a private repository, change this field to your repository
name.
    # # Please see documentation here: https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
    dockerRepo: 'docker.c01.cloudinsights.netapp.com'
    # # [Required Field] The name of the imagePullSecret for dockerRepo.
    # # If you are using a private repository, change this field from
'netapp-ci-docker' to the name of your secret.
    dockerImagePullSecret: 'netapp-ci-docker'

    # # Allow the operator to automatically rotate its ApiKey before
expiration.
    # tokenRotationEnabled: 'true'
    # # Number of days before expiration that the ApiKey should be
rotated. This must be less than the total ApiKey duration.
    # tokenRotationThresholdDays: '30'

  telegraf:
    # # Settings to fine-tune metrics data collection. Telegraf config
names are included in parenthesis.
    # # See
https://github.com/influxdata/telegraf/blob/master/docs/CONFIGURATION.md#a
gent

    # # The default time telegraf will wait between inputs for all plugins
(interval). Max=60
    # collectionInterval: '60s'
    # # Maximum number of records per output that telegraf will write in
one batch (metric_batch_size).
    # batchSize: '10000'
    # # Maximum number of records per output that telegraf will cache
pending a successful write (metric_buffer_limit).
    # bufferLimit: '150000'
    # # Collect metrics on multiples of interval (round_interval).
    # roundInterval: 'true'
    # # Each plugin waits a random amount of time between the scheduled
collection time and that time + collection_jitter before collecting inputs
(collection_jitter).
    # collectionJitter: '0s'
    # # Collected metrics are rounded to the precision specified. When set
to "0s" precision will be set by the units specified by interval
(precision).
    # precision: '0s'
```

```
    # # Time telegraf will wait between writing outputs (flush_interval).
Max=collectionInterval
    # flushInterval: '60s'
    # # Each output waits a random amount of time between the scheduled
write time and that time + flush_jitter before writing outputs
(flush_jitter).
    # flushJitter: '0s'
    # # Timeout for writing to outputs (timeout).
    # outputTimeout: '5s'

    # # telegraf-ds CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # dsCpuLimit: '750m'
    # dsMemLimit: '800Mi'
    # dsCpuRequest: '100m'
    # dsMemRequest: '500Mi'

    # # telegraf-rs CPU/Mem limits and requests.
    # rsCpuLimit: '3'
    # rsMemLimit: '4Gi'
    # rsCpuRequest: '100m'
    # rsMemRequest: '500Mi'

    # # Skip second run of processors after aggregators
    # skipProcessorsAfterAggregators: 'true'

    # # telegraf additional tolerations. Use the following abbreviated
single line format only.
    # # Inspect telegraf-rs/-ds to view tolerations which are always
present.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # dsTolerations: ''
    # rsTolerations: ''


    # If telegraf warns of insufficient lockable memory, try increasing
the limit of lockable memory for Telegraf in the underlying operating
system/node.  If increasing the limit is not an option, set this to true
to instruct Telegraf to not attempt to reserve locked memory pages.  While
this might pose a security risk as decrypted secrets might be swapped out
to disk, it allows for execution in environments where reserving locked
memory is not possible.
    # unprotected: 'false'
```

```
    # # Set runPrivileged to true if SELinux is enabled on your Kubernetes
nodes.
    # runPrivileged: 'false'

    # # Collect container Block IO metrics.
    # dsBlockIOEnabled: 'true'

    # # Collect NFS IO metrics.
    # dsNfsIOEnabled: 'true'

    # # Collect kubernetes.system_container metrics and objects in the
kube-system|cattle-system namespaces for managed kubernetes clusters (EKS,
AKS, GKE, managed Rancher).  Set this to true if you want collect these
metrics.
    # managedK8sSystemMetricCollectionEnabled: 'false'

    # # Collect kubernetes.pod_volume (pod ephemeral storage) metrics.
Set this to true if you want to collect these metrics.
    # podVolumeMetricCollectionEnabled: 'false'

    # # Declare Rancher cluster as managed.  Set this to true if your
Rancher cluster is managed as opposed to on-premise.
    # isManagedRancher: 'false'

    # # If telegraf-rs fails to start due to being unable to find the etcd
crt and key, manually specify the appropriate path here.
    # rsHostEtcdCrt: ''
    # rsHostEtcdKey: ''

  # kube-state-metrics:
    # # kube-state-metrics CPU/Mem limits and requests.
    # cpuLimit: '500m'
    # memLimit: '1Gi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    # # Comma-separated list of resources to enable.
    # # See resources in https://github.com/kubernetes/kube-state-
metrics/blob/main/docs/cli-arguments.md
    # resources:
'cronjobs,daemonsets,deployments,ingresses,jobs,namespaces,nodes,persisten
tvolumeclaims,persistentvolumes,pods,replicasets,resourcequotas,services,s
tatefulsets'

    # # Comma-separated list of metrics to enable.
    # # See metric-allowlist in https://github.com/kubernetes/kube-state-
metrics/blob/main/docs/cli-arguments.md
```

```
    # metrics:
'kube_cronjob_created,kube_cronjob_status_active,kube_cronjob_labels,kube_
daemonset_created,kube_daemonset_status_current_number_scheduled,kube_daem
onset_status_desired_number_scheduled,kube_daemonset_status_number_availab
le,kube_daemonset_status_number_misscheduled,kube_daemonset_status_number_
ready,kube_daemonset_status_number_unavailable,kube_daemonset_status_obser
ved_generation,kube_daemonset_status_updated_number_scheduled,kube_daemons
et_metadata_generation,kube_daemonset_labels,kube_deployment_status_replic
as,kube_deployment_status_replicas_available,kube_deployment_status_replic
as_unavailable,kube_deployment_status_replicas_updated,kube_deployment_sta
tus_observed_generation,kube_deployment_spec_replicas,kube_deployment_spec
_paused,kube_deployment_spec_strategy_rollingupdate_max_unavailable,kube_d
eployment_spec_strategy_rollingupdate_max_surge,kube_deployment_metadata_g
eneration,kube_deployment_labels,kube_deployment_created,kube_job_created,
kube_job_owner,kube_job_status_active,kube_job_status_succeeded,kube_job_s
tatus_failed,kube_job_labels,kube_job_status_start_time,kube_job_status_co
mpletion_time,kube_namespace_created,kube_namespace_labels,kube_namespace_
status_phase,kube_node_info,kube_node_labels,kube_node_role,kube_node_spec
_unschedulable,kube_node_created,kube_persistentvolume_capacity_bytes,kube
_persistentvolume_status_phase,kube_persistentvolume_labels,kube_persisten
tvolume_info,kube_persistentvolume_claim_ref,kube_persistentvolumeclaim_ac
cess_mode,kube_persistentvolumeclaim_info,kube_persistentvolumeclaim_label
s,kube_persistentvolumeclaim_resource_requests_storage_bytes,kube_persiste
ntvolumeclaim_status_phase,kube_pod_info,kube_pod_start_time,kube_pod_comp
letion_time,kube_pod_owner,kube_pod_labels,kube_pod_status_phase,kube_pod_
status_ready,kube_pod_status_scheduled,kube_pod_container_info,kube_pod_co
ntainer_status_waiting,kube_pod_container_status_waiting_reason,kube_pod_c
ontainer_status_running,kube_pod_container_state_started,kube_pod_containe
r_status_terminated,kube_pod_container_status_terminated_reason,kube_pod_c
ontainer_status_last_terminated_reason,kube_pod_container_status_ready,kub
e_pod_container_status_restarts_total,kube_pod_overhead_cpu_cores,kube_pod
_overhead_memory_bytes,kube_pod_created,kube_pod_deletion_timestamp,kube_p
od_init_container_info,kube_pod_init_container_status_waiting,kube_pod_ini
t_container_status_waiting_reason,kube_pod_init_container_status_running,k
ube_pod_init_container_status_terminated,kube_pod_init_container_status_te
rminated_reason,kube_pod_init_container_status_last_terminated_reason,kube
_pod_init_container_status_ready,kube_pod_init_container_status_restarts_t
otal,kube_pod_status_scheduled_time,kube_pod_status_unschedulable,kube_pod
_spec_volumes_persistentvolumeclaims_readonly,kube_pod_container_resource_
requests_cpu_cores,kube_pod_container_resource_requests_memory_bytes,kube_
pod_container_resource_requests_storage_bytes,kube_pod_container_resource_
requests_ephemeral_storage_bytes,kube_pod_container_resource_limits_cpu_co
res,kube_pod_container_resource_limits_memory_bytes,kube_pod_container_res
ource_limits_storage_bytes,kube_pod_container_resource_limits_ephemeral_st
orage_bytes,kube_pod_init_container_resource_limits_cpu_cores,kube_pod_ini
t_container_resource_limits_memory_bytes,kube_pod_init_container_resource_
```

```
limits_storage_bytes,kube_pod_init_container_resource_limits_ephemeral_sto
rage_bytes,kube_pod_init_container_resource_requests_cpu_cores,kube_pod_in
it_container_resource_requests_memory_bytes,kube_pod_init_container_resour
ce_requests_storage_bytes,kube_pod_init_container_resource_requests_epheme
ral_storage_bytes,kube_replicaset_status_replicas,kube_replicaset_status_r
eady_replicas,kube_replicaset_status_observed_generation,kube_replicaset_s
pec_replicas,kube_replicaset_metadata_generation,kube_replicaset_labels,ku
be_replicaset_created,kube_replicaset_owner,kube_resourcequota,kube_resour
cequota_created,kube_service_info,kube_service_labels,kube_service_created
,kube_service_spec_type,kube_statefulset_status_replicas,kube_statefulset_
status_replicas_current,kube_statefulset_status_replicas_ready,kube_statef
ulset_status_replicas_updated,kube_statefulset_status_observed_generation,
kube_statefulset_replicas,kube_statefulset_metadata_generation,kube_statef
ulset_created,kube_statefulset_labels,kube_statefulset_status_current_revi
sion,kube_statefulset_status_update_revision,kube_node_status_capacity,kub
e_node_status_allocatable,kube_node_status_condition,kube_pod_container_re
source_requests,kube_pod_container_resource_limits,kube_pod_init_container
_resource_limits,kube_pod_init_container_resource_requests'

    # # Comma-separated list of Kubernetes label keys that will be used in
the resources' labels metric.
    # # See metric-labels-allowlist in https://github.com/kubernetes/kube-
state-metrics/blob/main/docs/cli-arguments.md
    # labels:
'cronjobs=[*],daemonsets=[*],deployments=[*],ingresses=[*],jobs=[*],namesp
aces=[*],nodes=[*],persistentvolumeclaims=[*],persistentvolumes=[*],pods=[
*],replicasets=[*],resourcequotas=[*],services=[*],statefulsets=[*]'

    # # kube-state-metrics additional tolerations. Use the following
abbreviated single line format only.
    # # No tolerations are applied by default
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # tolerations: ''

    # # kube-state-metrics shards.  Increase the number of shards for
larger clusters if telegraf RS pod(s) experience collection timeouts
    # shards: '2'

  # # Settings for the Events Log feature.
  # logs:
    # # Set runPrivileged to true if Fluent Bit fails to start, trying to
open/create its database.
    # runPrivileged: 'false'

    # # If Fluent Bit should read new files from the head, not tail.
```

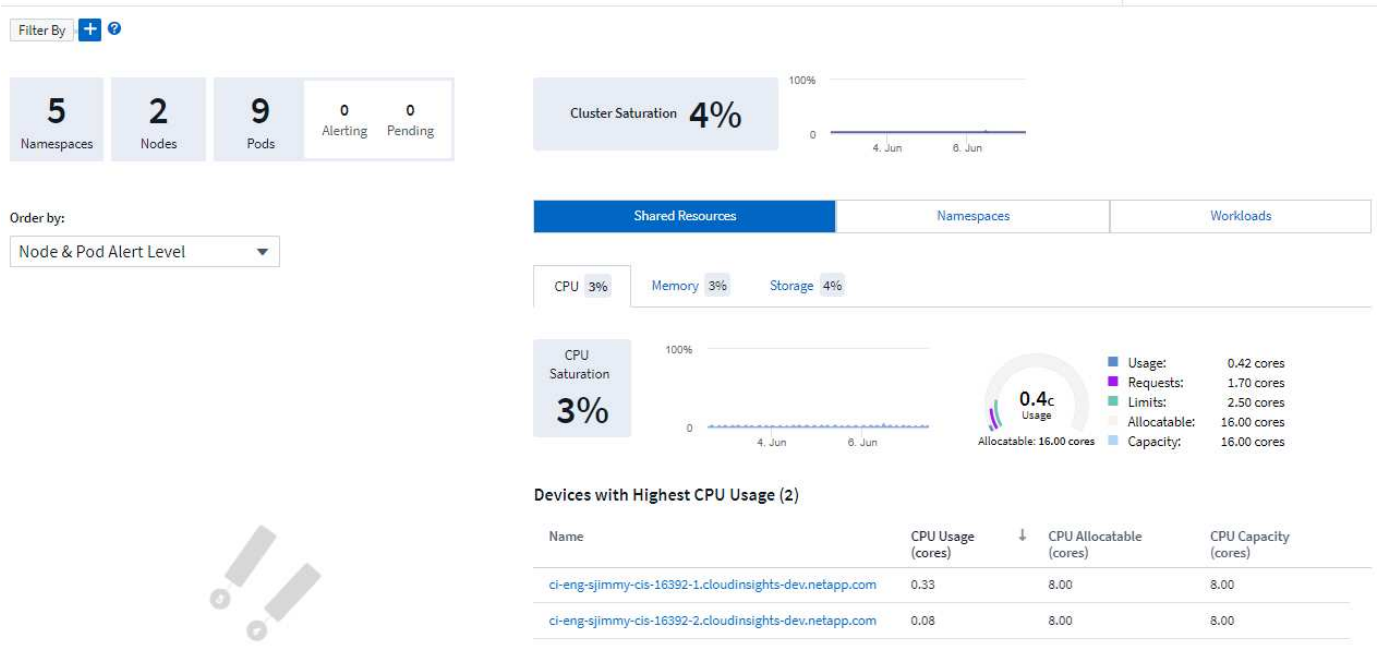
```
    # # See Read_from_Head in
https://docs.fluentbit.io/manual/pipeline/inputs/tail
    # readFromHead: "true"

    # # Network protocol that Fluent Bit should use for DNS: "UDP" or
"TCP".
    # dnsMode: "UDP"

    # # DNS resolver that Fluent Bit should use: "LEGACY" or "ASYNC"
    # fluentBitDNSResolver: "LEGACY"

    # # Logs additional tolerations. Use the following abbreviated single
line format only.
    # # Inspect fluent-bit-ds to view tolerations which are always
present. No tolerations are applied by default for event-exporter.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # fluent-bit-tolerations: ''
    # event-exporter-tolerations: ''

    # # event-exporter CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # event-exporter-cpuLimit: '500m'
    # event-exporter-memLimit: '1Gi'
    # event-exporter-cpuRequest: '50m'
    # event-exporter-memRequest: '100Mi'

    # # event-exporter max event age.
    # # See https://github.com/jkroepke/resmoio-kubernetes-event-exporter
    # event-exporter-maxEventAgeSeconds: '10'

    # # event-exporter client-side throttling
    # # Set kubeBurst to roughly match your events per minute and
kubeQPS=kubeBurst/5
    # # See https://github.com/resmoio/kubernetes-event-
exporter#troubleshoot-events-discarded-warning
    # event-exporter-kubeQPS: 20
    # event-exporter-kubeBurst: 100

    # # fluent-bit CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # fluent-bit-cpuLimit: '500m'
    # fluent-bit-memLimit: '1Gi'
    # fluent-bit-cpuRequest: '50m'
```

```
    # fluent-bit-memRequest: '100Mi'

  # # Settings for the Network Performance and Map feature.
  # workload-map:
    # # netapp-ci-net-observer-l4-ds CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # cpuLimit: '500m'
    # memLimit: '500Mi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    # # Metric aggregation interval in seconds. Min=30, Max=120
    # metricAggregationInterval: '60'

    # # Interval for bpf polling. Min=3, Max=15
    # bpfPollInterval: '8'

    # # Enable performing reverse DNS lookups on observed IPs.
    # enableDNSLookup: 'true'

    # # netapp-ci-net-observer-l4-ds additional tolerations. Use the
following abbreviated single line format only.
    # # Inspect netapp-ci-net-observer-l4-ds to view tolerations which are
always present.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # l4-tolerations: ''

    # # Set runPrivileged to true if SELinux is enabled on your Kubernetes
nodes.
    # # Note: In OpenShift environments, this is set to true
automatically.
    # runPrivileged: 'false'

  # change-management:
    # # change-observer-watch-rs CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # cpuLimit: '1'
    # memLimit: '1Gi'
    # cpuRequest: '500m'
    # memRequest: '500Mi'

    # # Interval in minutes after which a non-successful deployment of a
workload will be marked as failed
```

```
    # failureDeclarationIntervalMins: '30'

    # # Frequency at which workload deployment in-progress events are sent
    # deployAggrIntervalSeconds: '300'

    # # Frequency at which non-workload deployments are combined and sent
    # nonWorkloadAggrIntervalSeconds: '15'

    # # A set of regular expressions used in env names and data maps whose
value will be redacted
    # termsToRedact: '"pwd", "password", "token", "apikey", "api-key",
"api_key", "jwt", "accesskey", "access_key", "access-key", "ca-file",
"key-file", "cert", "cafile", "keyfile", "tls", "crt", "salt",
".dockerconfigjson", "auth", "secret"'

    # # A comma separated list of additional kinds to watch from the
default set of kinds watched by the collector
    # # Each kind will have to be prefixed by its apigroup
    # # Example: '"authorization.k8s.io.subjectaccessreviews"'
    # additionalKindsToWatch: ''

    # # A comma separated list of additional field paths whose diff is
ignored as part of change analytics. This list in addition to the default
set of field paths ignored by the collector.
    # # Example: '"metadata.specTime", "data.status"'
    # additionalFieldsDiffToIgnore: ''

    # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
    # # Each kind will have to be prefixed by its apigroup
    # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
    # kindsToIgnoreFromWatch: ''

    # # Frequency with which log records are sent to CI from the collector
    # logRecordAggrIntervalSeconds: '20'

    # # change-observer-watch-ds additional tolerations. Use the following
abbreviated single line format only.
    # # Inspect change-observer-watch-ds to view tolerations which are
always present.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # watch-tolerations: ''
```

Kubernetes クラスタの詳細ページ

Kubernetesクラスタの詳細ページには、Kubernetesクラスタの概要が表示されます。



ネームスペース、ノード、およびポッドの数

ページ上部のカウントには、クラスタ内のネームスペース、ノード、ポッドの総数、および現在アラート中および保留中のPopdの数が表示されます。

共有リソースと飽和

詳細ページの右上には、クラスタが現在の割合で飽和状態になっているかどうかのグラフと、その期間の最新の傾向が表示されます。クラスタの飽和は、各時点でのCPU、メモリ、またはストレージの飽和状態の最大値です。

その下には、CPU、メモリ、ストレージのタブがデフォルトで*共有リソース*の使用状況として表示されます。各タブには、時間の経過に伴う飽和度と傾向が表示され、使用状況の詳細も表示されます。ストレージの場合、この値はバックエンドとファイルシステムの飽和度の大きい方で、それぞれ独立して計算されます。

使用率が最も高いデバイスが下部の表に表示されます。リンクをクリックすると、これらのデバイスを確認できます。

ネームスペース

[ネームスペース]タブには、Kubernetes環境内のすべてのネームスペースのリストが表示されます。このタブには、CPUとメモリの使用状況、および各ネームスペース内のワークロードの数が表示されます。名前のリンクをクリックして、各ネームスペースを確認します。

Shared Resources | Namespaces | Workloads

Namespaces (5)

Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Workload Count
netapp-monitoring	0.25	0.38	4
kube-system	0.01	0.03	3
kube-public	0.00	0.00	0
kube-node-lease	0.00	0.00	0
default	0.00	<0.01	1

ワークロード

同様に、各ネームスペースのワークロードのリストがワークロードタブに表示され、CPUとメモリの使用量も表示されます。ネームスペースリンクをクリックすると、ドリルでそれぞれが実行されます。

Shared Resources | Namespaces | Workloads

Workloads (8)

Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Namespace
telegraf-rs-lf9gg	0.24	0.24	netapp-monitoring
telegraf-ds-k957c	0.01	0.10	netapp-monitoring
nginx	0.00	<0.01	default
monitoring-operator-6fcf4755ff-p2cs6	<0.01	0.02	netapp-monitoring
metrics-server-7b4f8b595-f7j9f	<0.01	0.01	kube-system
local-path-provisioner-64d457c485-289gx	<0.01	0.01	kube-system
kube-state-metrics-7995866f8c-t8c49	<0.01	0.01	netapp-monitoring
coredns-5d69dc75db-nkw5p	<0.01	0.01	kube-system

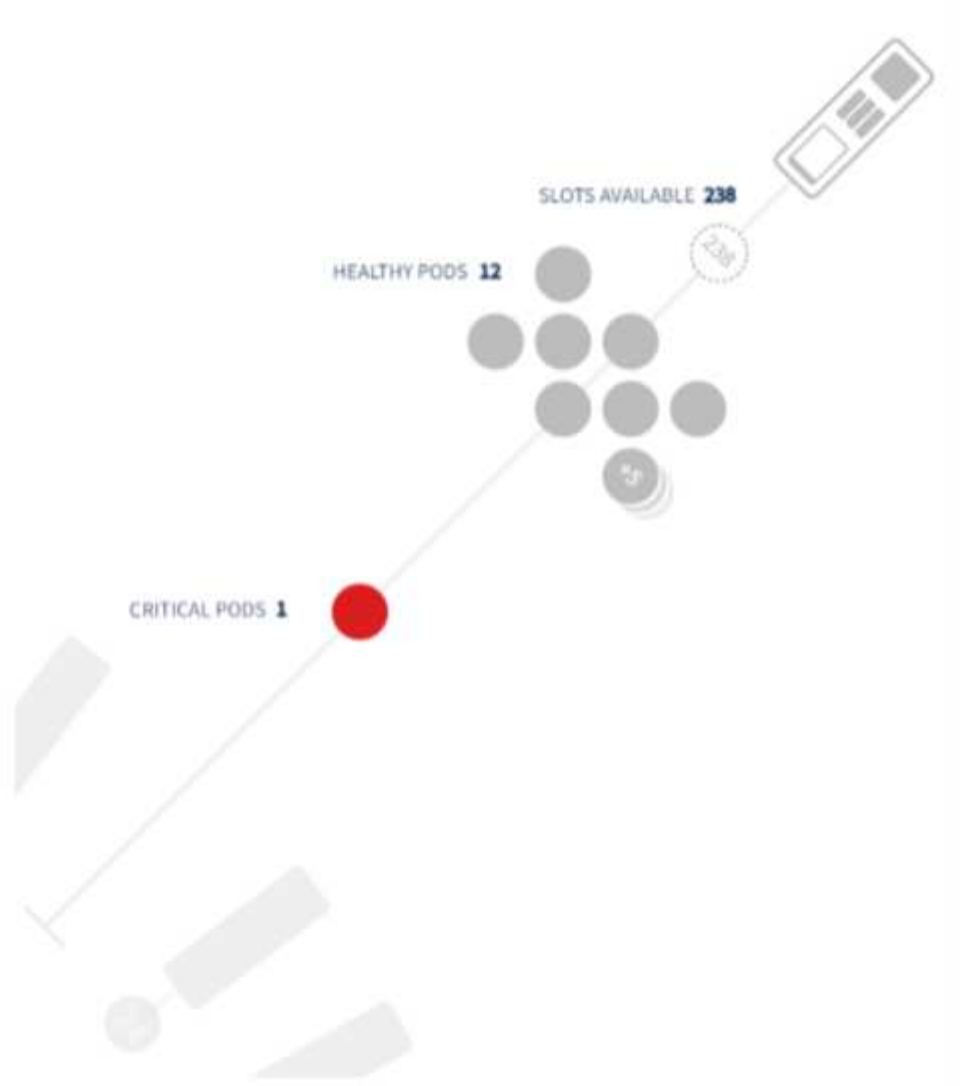
クラスタ「ホイール」

クラスタの「ホイール」セクションでは、ノードとポッドの健全性を一目で確認できます。詳細については、ドリルで確認できます。クラスタのノード数がページのこの領域に表示される数を超えている場合は、使用可能なボタンを使用してホイールを回すことができます。

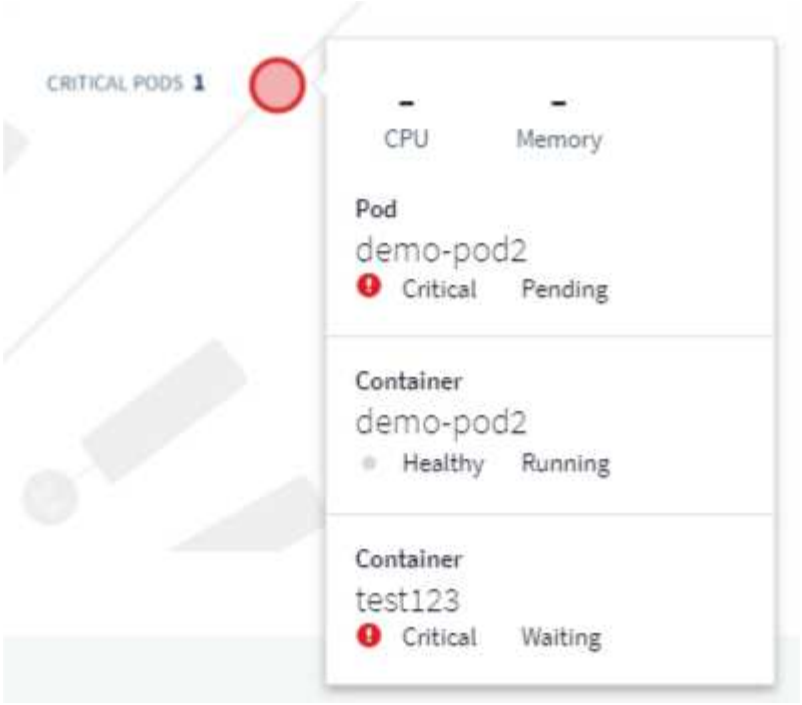
アラートのポッドまたはノードは赤で表示されます。「警告」の領域はオレンジで表示されます。スケジュールされていないポッド（未接続）は、クラスタ「 Wheel 」の下部コーナーに表示されます。

ポッド（円）またはノード（バー）にカーソルを合わせると、ノードのビューが拡張されます。

そのビューでポッドまたはノードをクリックすると、展開されたノードビューが拡大表示されます。



ここから、エレメントにカーソルを合わせると、そのエレメントの詳細を表示できます。たとえば、この例で重要なポッドにカーソルを合わせると、そのポッドに関する詳細が表示されます。



ファイルシステム、メモリ、および CPU の情報を表示するには、 Node 要素にカーソルを合わせます。

ゲージに関する注意

メモリと CPU のゲージには、 *allocatable capacity* と _total の容量 _ に関連して _Used_in が表示されるので、 3 色が表示されます。

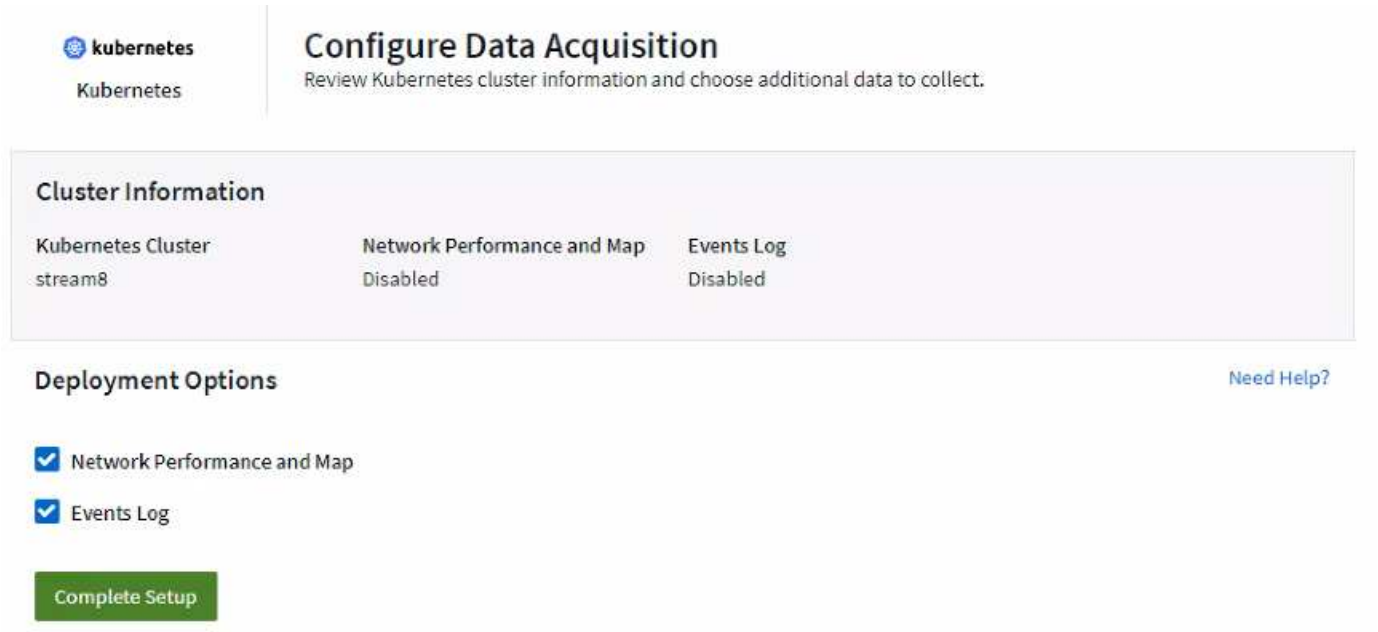
Kubernetes Network Performance Monitoring and Mapの略

KubernetesのNetwork Performance Monitoring and Map機能は、サービス（ワークロードとも呼ばれます）間の依存関係をマッピングすることでトラブルシューティングを簡易化し、ネットワークパフォーマンスのレイテンシや異常をリアルタイムで可視化して、ユーザに影響を与える前にパフォーマンスの問題を特定します。
この機能は、Kubernetesのトラフィックフローを分析、監査することで全体的なコストを削減するのに役立ちます。

主な特長：
•ワークロードマップは、Kubernetesワークロードの依存関係とフローを示し、ネットワークとパフォーマンスの問題を明らかにします。
•Kubernetesポッド、ワークロード、ノード間のネットワークトラフィックを監視し、トラフィックとレイテンシの問題の原因を特定します。
•入力、出力、リージョン間、ゾーン間のネットワークトラフィックを分析することで、全体的なコストを削減します。

前提条件

Kubernetes Network Performance Monitoring and Mapを使用する前に、を設定しておく必要があります "NetApp Kubernetes Monitoring Operator" このオプションを有効にします。オペレータの配備中に、[ネットワークパフォーマンスとマップ]チェックボックスをオンにして有効にします。このオプションを有効にするには、Kubernetesランディングページに移動して[Modify Deployment]を選択します。



モニタ

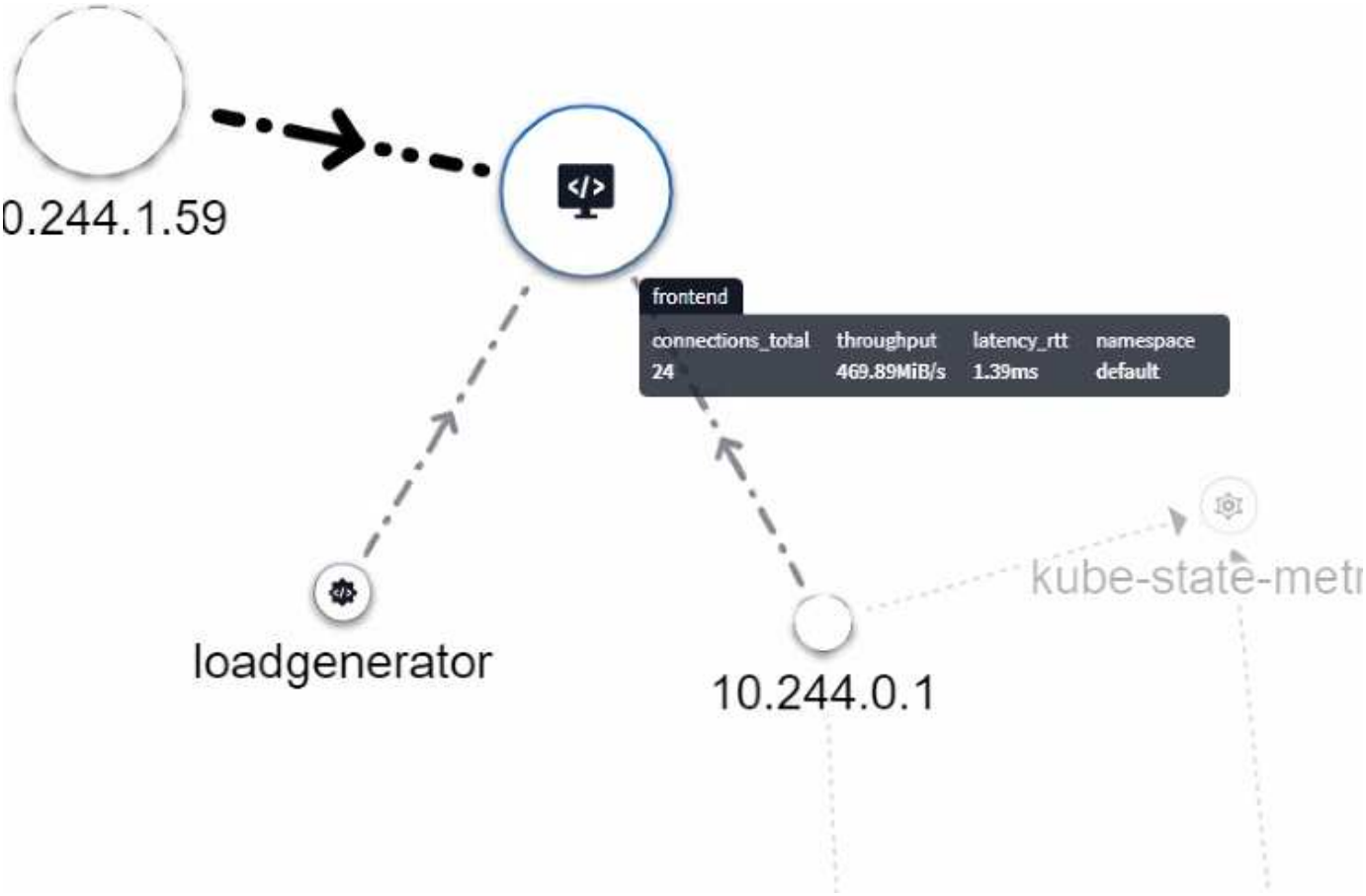
ワークロードマップは、を使用し"モニタ"て情報を取得します。Data Infrastructure Insightsには、多数のデフォルトKubernetesモニタが用意されています（デフォルトでは、これらのモニタは_Paused_になっている場合があります）。必要なモニタを_Resume_(つまり有効化)することも、ワークロードマップでも使用されるKubernetesオブジェクト用のカスタムモニタを作成することもできます。

Data Infrastructure Insightsの指標アラートは、以下のいずれかのオブジェクトタイプに対して作成できます。データがデフォルトのオブジェクトタイプでグループ化されていることを確認します。

- kubernetes.workload
- kubernetes.daemonset
- kubernetes.deployment
- kubernetes.cronjob
- kutability.job
- kubernetes.replicaset
- kubernetes.statefulset
- Kubernetesポッド
- kubernetes.network_traffic_l4

地図

マップには、サービス/ワークロードとそれらの相互関係が表示されます。矢印は交通の方向を示しています。ワークロードにカーソルを合わせると、そのワークロードの概要情報が表示されます（次の例を参照）。



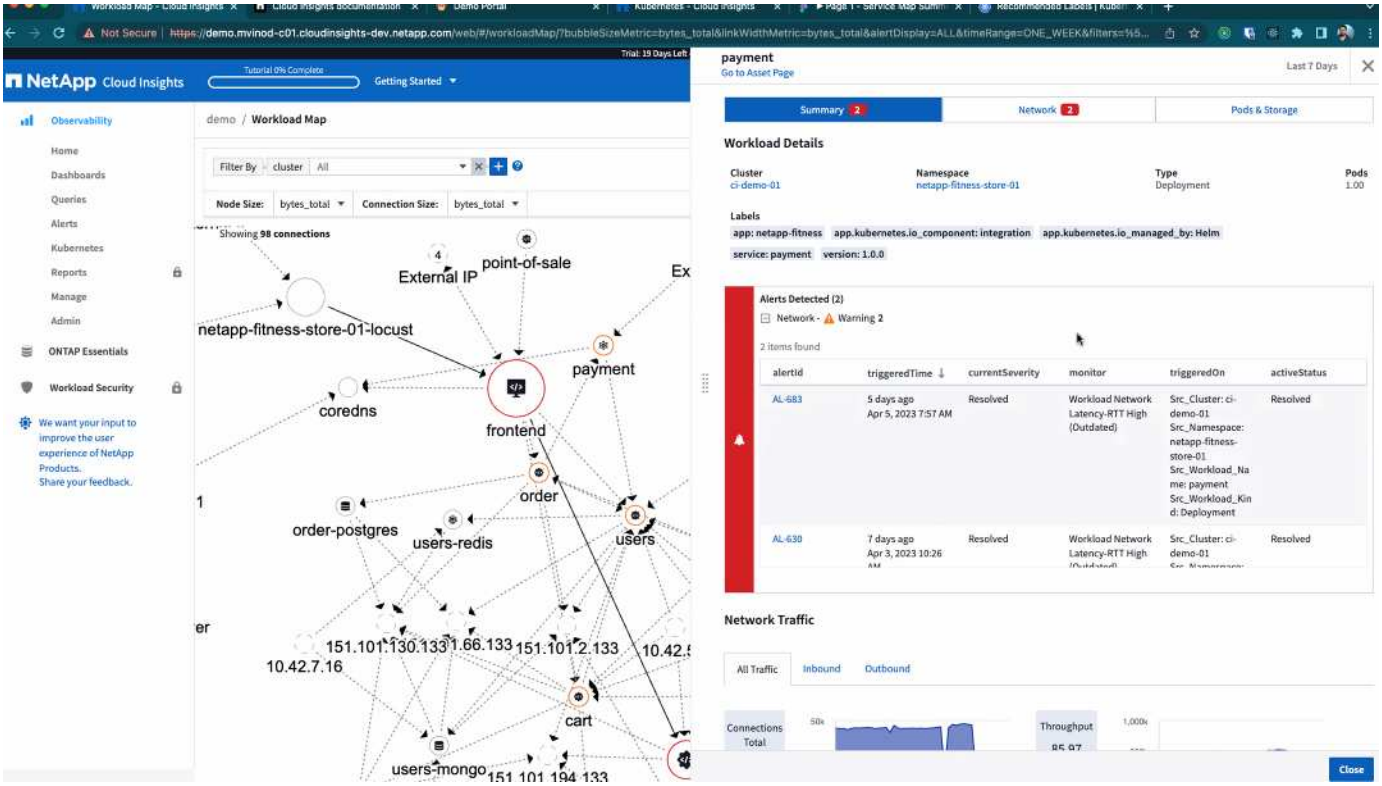
円の中のアイコンは、さまざまなサービスタイプを表します。アイコンは、基になるオブジェクトにがある場合にのみ表示されます ラベル。

各円のサイズはノードサイズを示します。これらのサイズは相対的なものであることに注意してください。ブラウザのズームレベルまたは画面サイズは、実際の円のサイズに影響を与える可能性があります。 同様に、トラフィックラインスタイルでは、接続サイズが一目でわかるようになっています。太字の実線は交通量が多く、点線は交通量が少ないです。

円の中の数字は、サービスによって現在処理されている外部接続の数です。

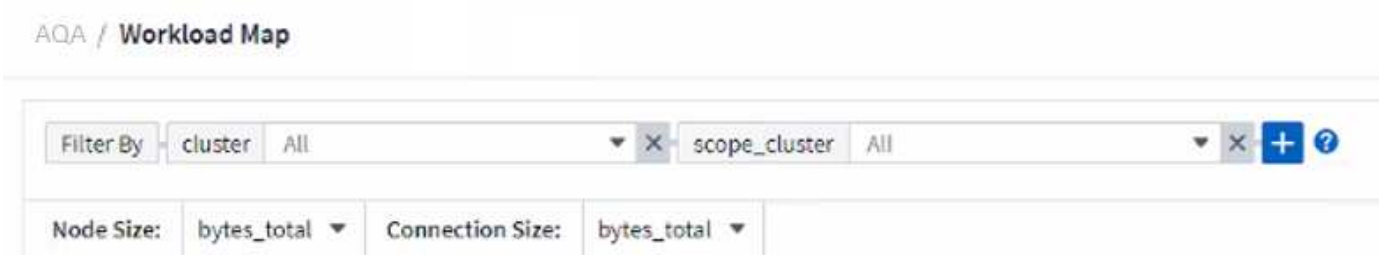
ワークロードの詳細とアラート

色の円は、ワークロードに関する警告レベルまたは重大レベルのアラートを示します。 円にカーソルを合わせると問題 の概要が表示されます。円をクリックすると、より詳細なスライドアウトパネルが開きます。

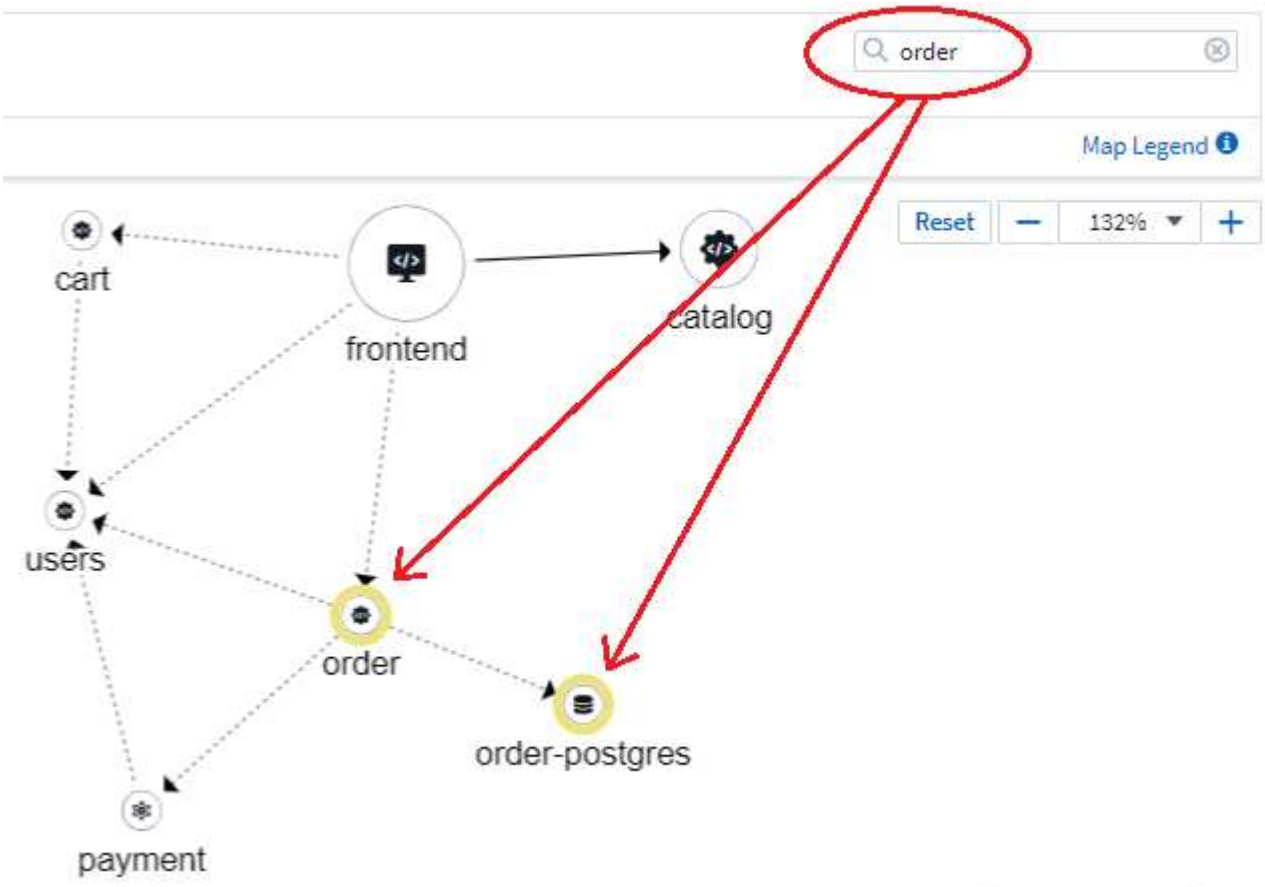


検索とフィルタ

Data Infrastructure Insightsの他の機能と同様に、必要なオブジェクトやワークロードの属性に絞り込むフィルタを簡単に設定できます。



同様に、_Find_フィールドに文字列を入力すると、一致するワークロードがハイライトされます。



ワークロードラベル

表示されるワークロードのタイプ（円のアイコンなど）をマップで識別するには、ワークロードラベルが必要です。 ラベルは次のように導出されます。

- 一般的な用語で実行されているサービス/アプリケーションの名前
- ソースがポッドの場合：
  - ラベルはポッドのワークロードラベルから取得されます
  - ワークロードの想定されるラベル：app.kubernetes.io/component
  - ラベル名参照： https://kubernetes.io/docs/concepts/overview/working-with-objects/common-labels/
  - 推奨ラベル：
    - フロントエンド

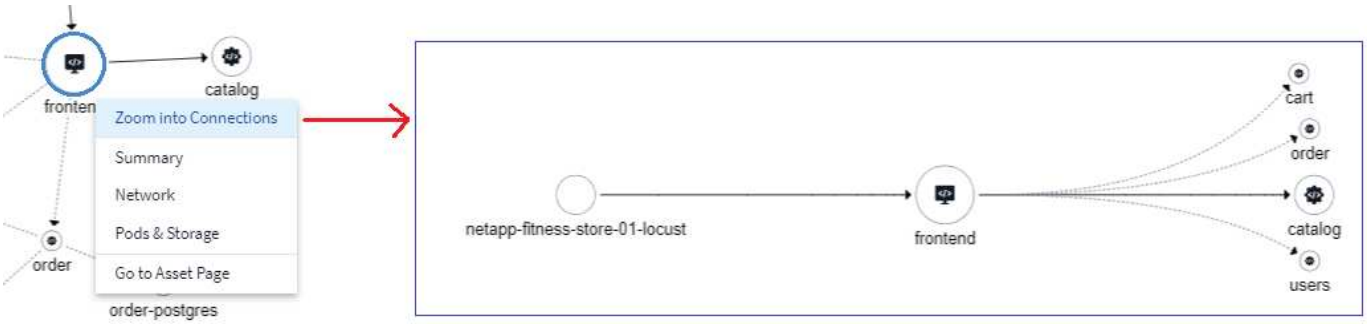
- バックエンド
- データベース
- キャッシュ
- キュー
- カフカ

- ソースがKubernetesクラスタの外部にある場合は、次の手順を実行します。
  - Data Infrastructure Insightsは、DNS解決名を解析してサービスタイプを抽出しようとします。

    たとえば、DNS解決名が_s3.eu-north-1.amazonaws.comの場合、解決された名前はサービスタイプとしてget_s3_に解析されます。

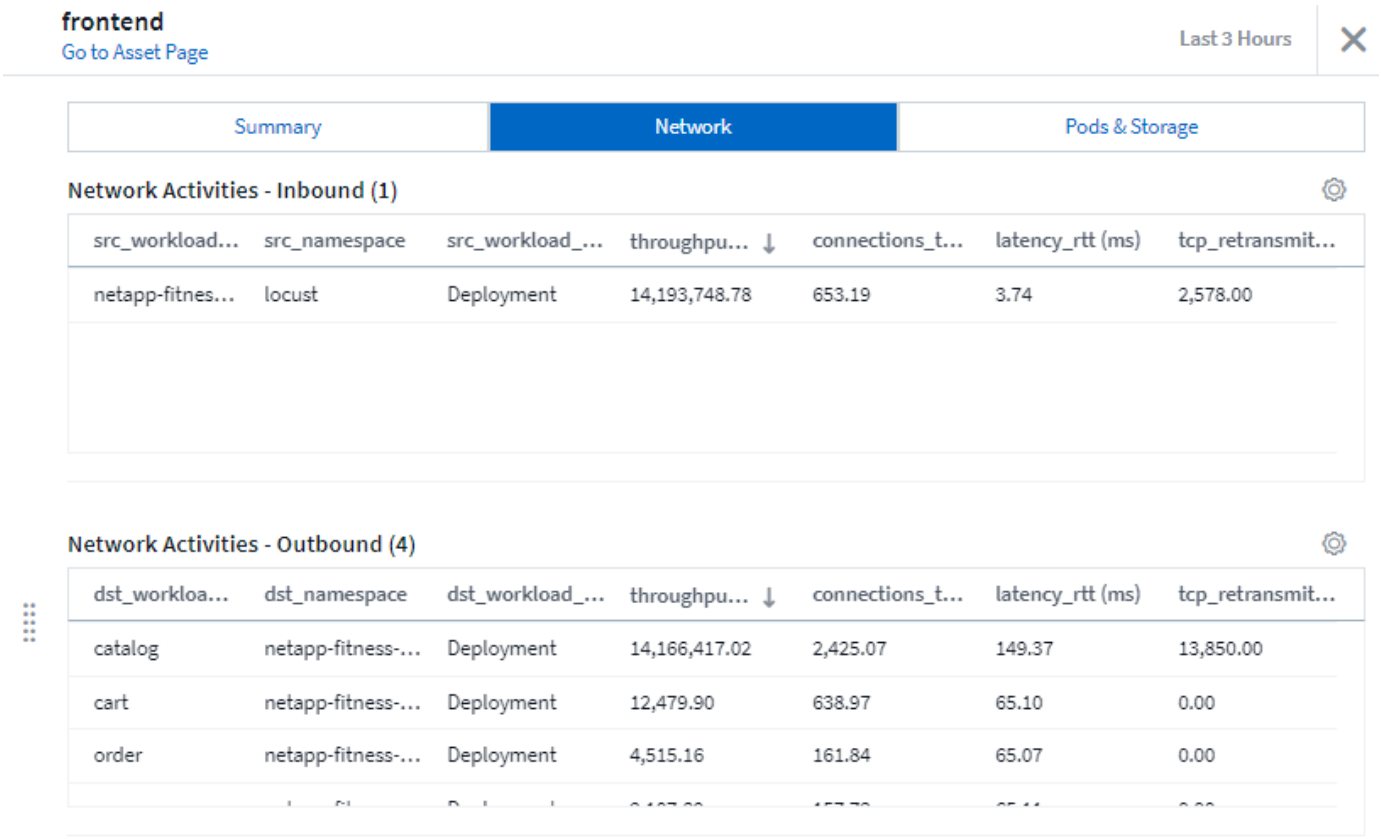
深海に潜る

ワークロードを右クリックすると、さらに詳しく調べるための追加のオプションが表示されます。たとえば、ここからズームインして、そのワークロードの接続を表示できます。

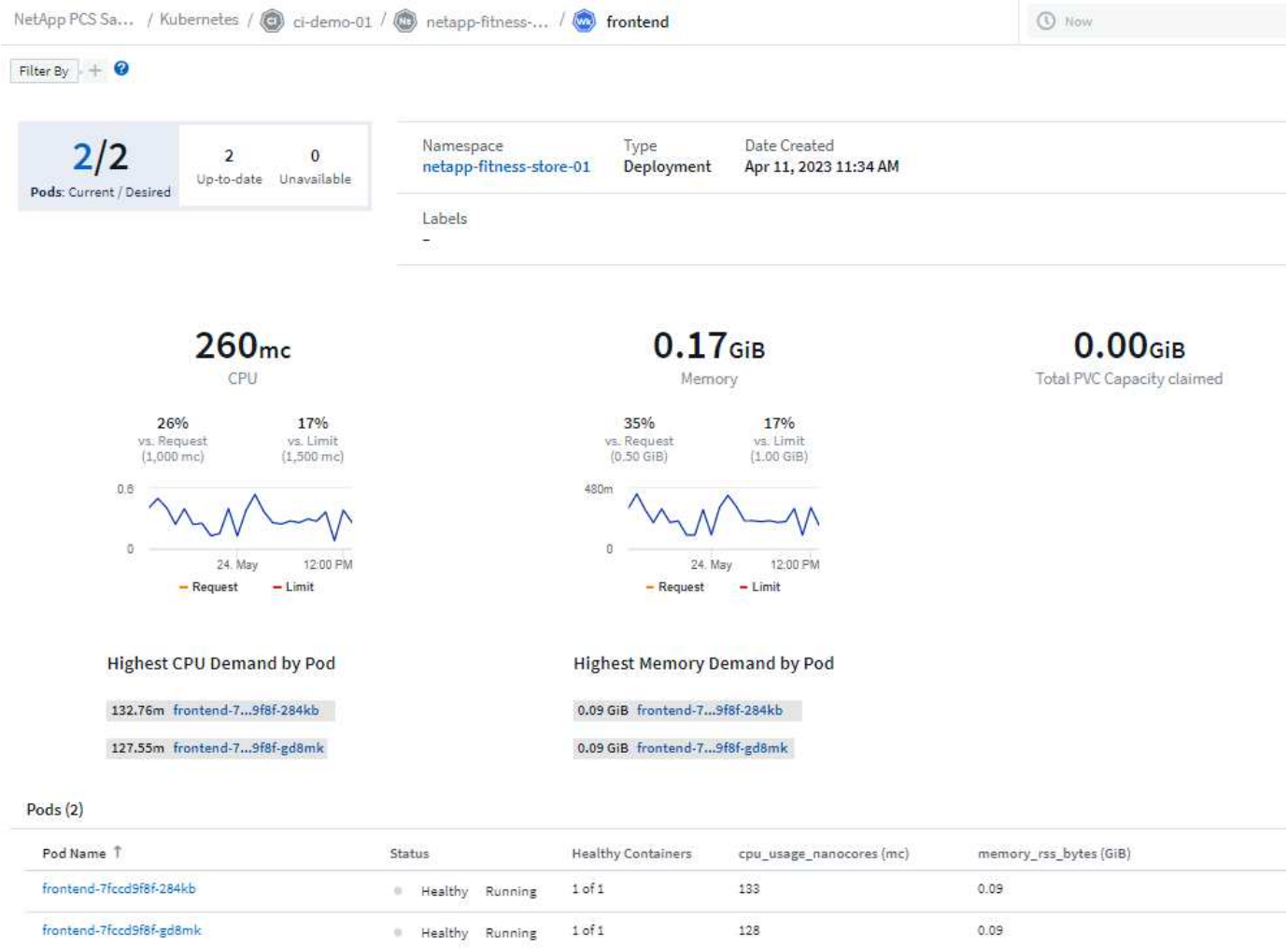


を右クリックすると、ワークロードの接続が表示されます"]

または、詳細スライドアウトパネルを開いて、*Summary*、*Network*、または_Pod & Storage_タブを直接表示することもできます。



最後に、[*Go to Asset Page*]を選択すると、ワークロードの詳細なアセットランディングページが開きます。



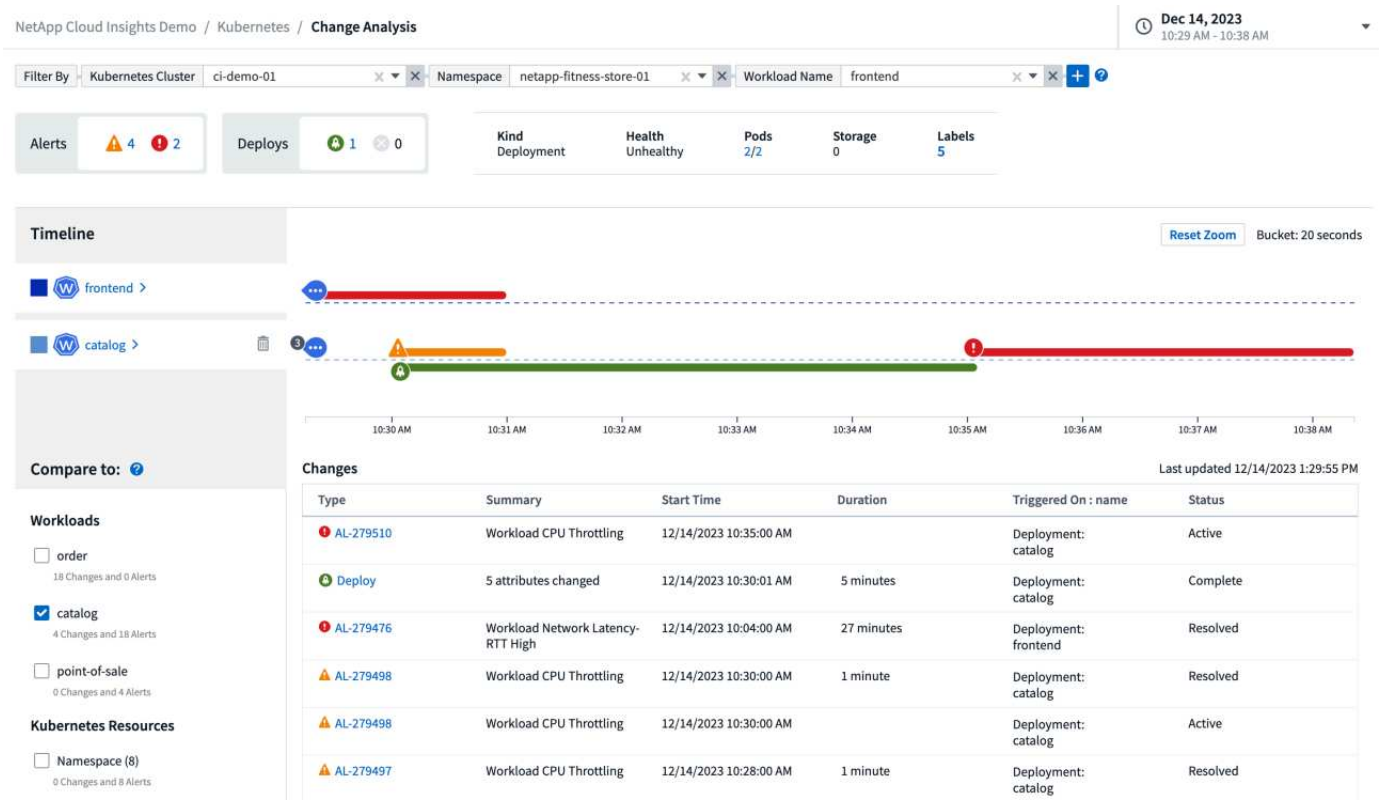
Kubernetesの変更分析

Kubernetes Change Analyticsを使用すると、Kubernetes環境に対する最近の変更をオールインワンビューで確認できます。アラートと導入ステータスをすぐに確認できます。変更分析を使用すると、導入と設定の変更をすべて追跡し、Kubernetesのサービス、インフラ、クラスタの健全性とパフォーマンスに関連付けることができます。

変更分析はどのように役立ちますか？

- マルチテナントKubernetes環境では、設定ミスが原因でシステムが停止する可能性があります。Change Analyticsでは、ワークロードの健全性と構成の変更を1つのペインで表示して関連付けることができます。これは、動的なKubernetes環境のトラブルシューティングに役立ちます。

Kubernetes Change Analyticsを表示するには、* Kubernetes > Change Analysis *に移動します。



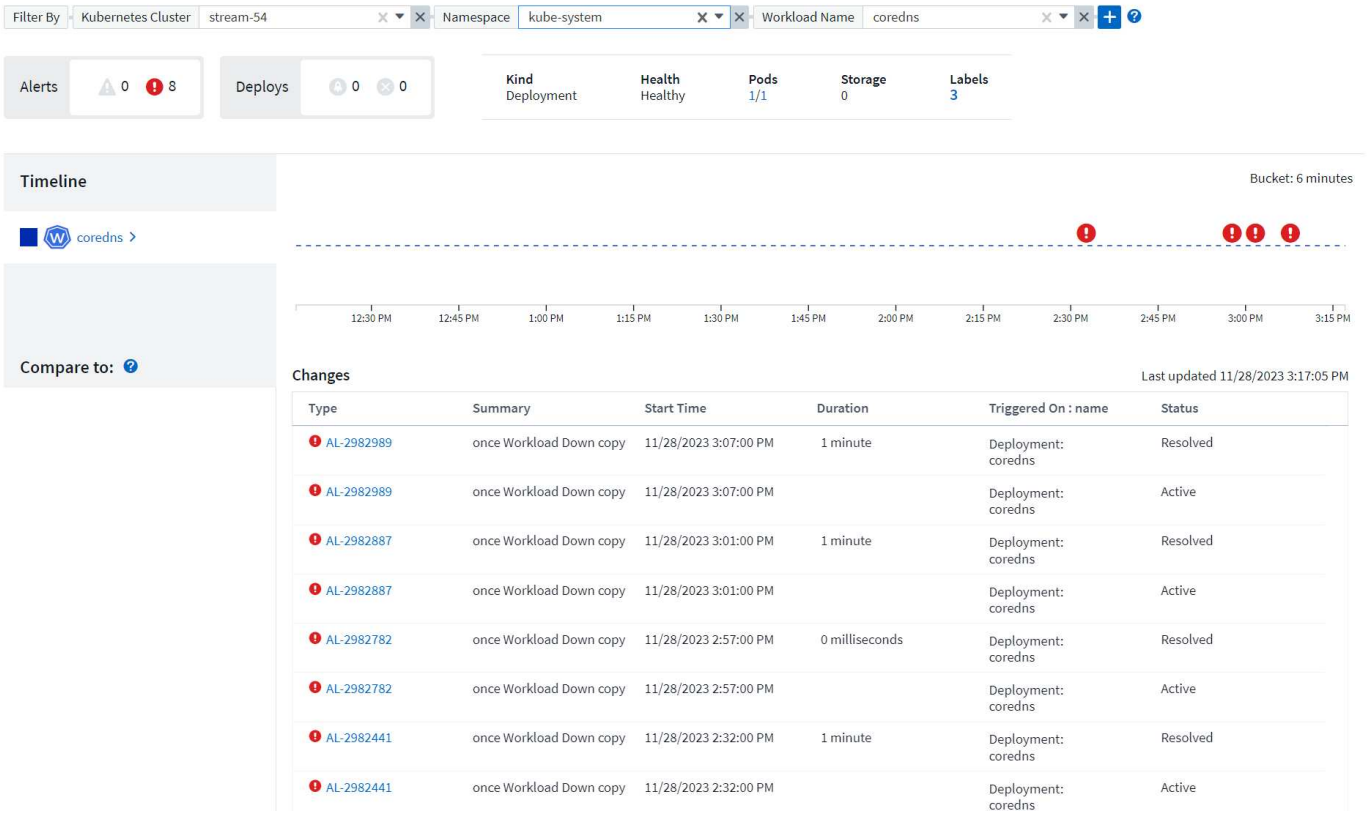
。

このページは、現在選択されているData Infrastructure Insightsの期間に基づいて自動的に更新されます。時間範囲が小さいほど、画面の更新頻度が高くなります。

フィルタリング

Data Infrastructure Insightsのすべての機能と同様に、変更リストは直感的にフィルタリングできます。ページ上部で、Kubernetesクラスタ、ネームスペース、ワークロードの値を入力または選択したり、[+]ボタンを選択して独自のフィルタを追加したりできます。

特定のクラスタ、ネームスペース、ワークロードにフィルタを適用して（設定した他のフィルタと一緒に）、そのクラスタ上のそのネームスペース内のそのワークロードに対する導入とアラートのタイムラインが表示されます。さらに拡大するには、グラフをクリックしてドラッグし、より具体的な時間範囲にフォーカスします。

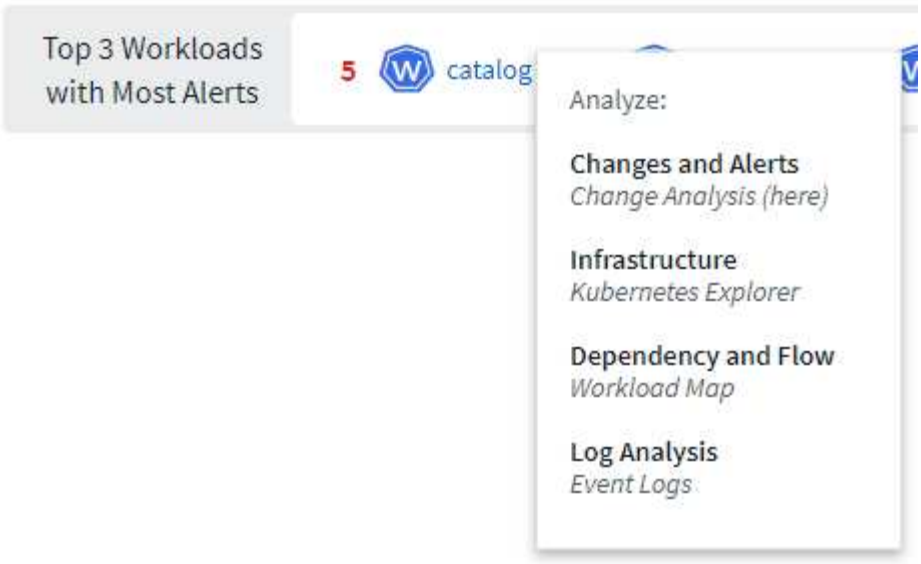


クイックステータス

フィルタリングエリアの下には、いくつかの高レベルインジケータがあります。左側にはアラートの数（WarningおよびCritical）が表示されます。この数には、_Active_alertsと_Resolved_alertsが含まれます。Only_Active_alertsを表示するには、「Status」のフィルタを設定し、「Active」を選択します。

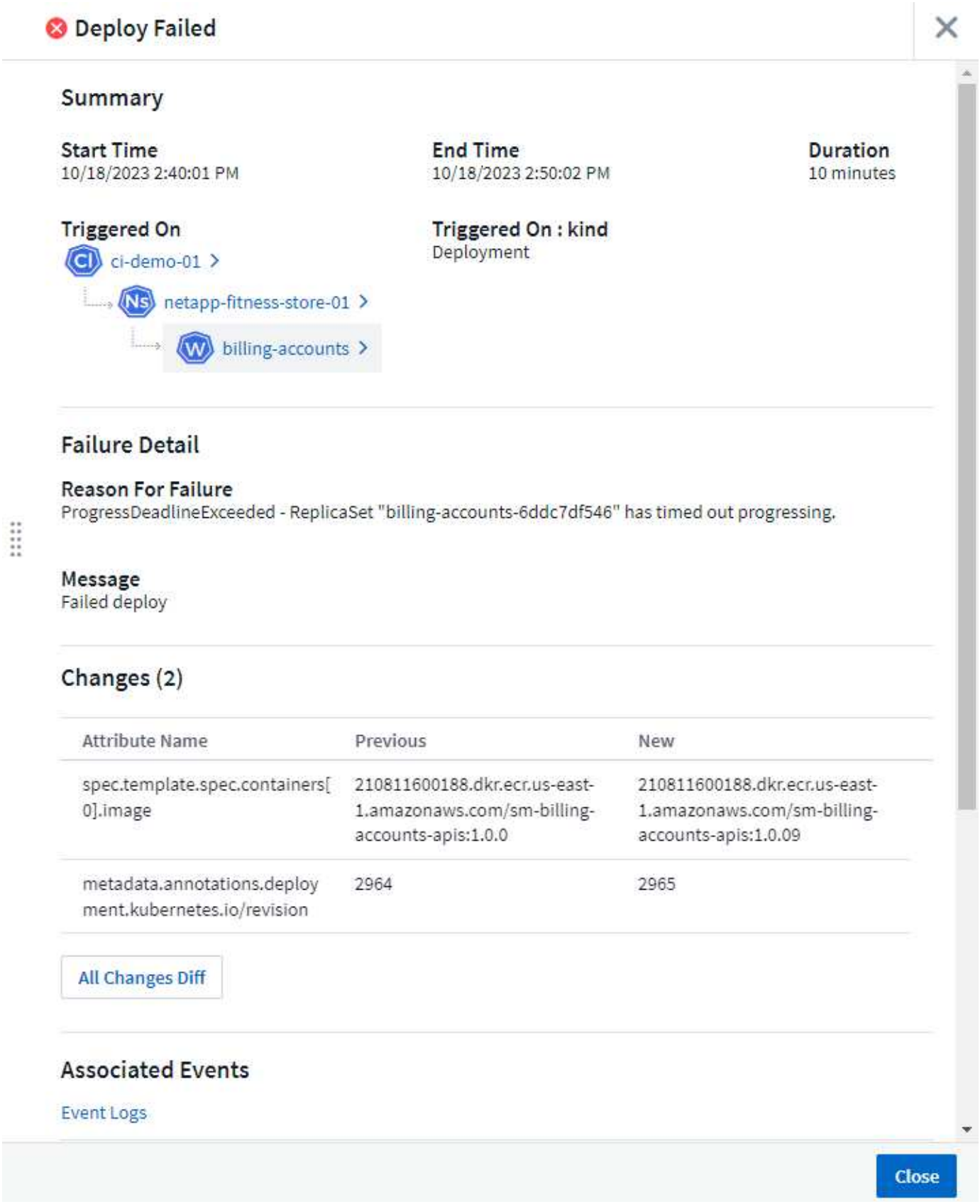
導入ステータスもここに表示されます。繰り返しになりますが、デフォルトでは、*Started*、*complete*、および_Failed_deploymentsの数が表示されます。Failed_Deploymentsのみを表示するには、[Status]のフィルタを設定し、[Failed]を選択します。

次にアラートが最も多い上位3つのワークロードが表示されます。各ワークロードの横にある赤の数字は、そのワークロードに関連するアラートの数を示します。ワークロードのリンクをクリックして、インフラ（Kubernetes Explorer）、依存関係（ワークロードマップ）、またはログ分析（イベントログ）を確認します。



詳細パネル

リストで変更を選択すると、変更を詳細に説明するパネルが開きます。たとえば、失敗したDeployを選択すると、Deployの概要、開始時刻と終了時刻、期間、および導入がトリガーされた場所、およびそれらのリソースを確認するためのリンクが表示されます。また、失敗の理由、関連する変更、関連するイベントも表示されます。



同様にアラートを選択すると、アラートをトリガーしたモニタやアラートのタイムラインを示すグラフなど、アラートの詳細が表示されます。

ONTAP の基礎知識

ONTAP Essentialsは、ONTAP のインベントリとワークロードの詳細な概要を提供するダッシュボードとワークフローのセットです。ONTAP Essentialsで作業するときに使用される次の用語が表示されることがあります。

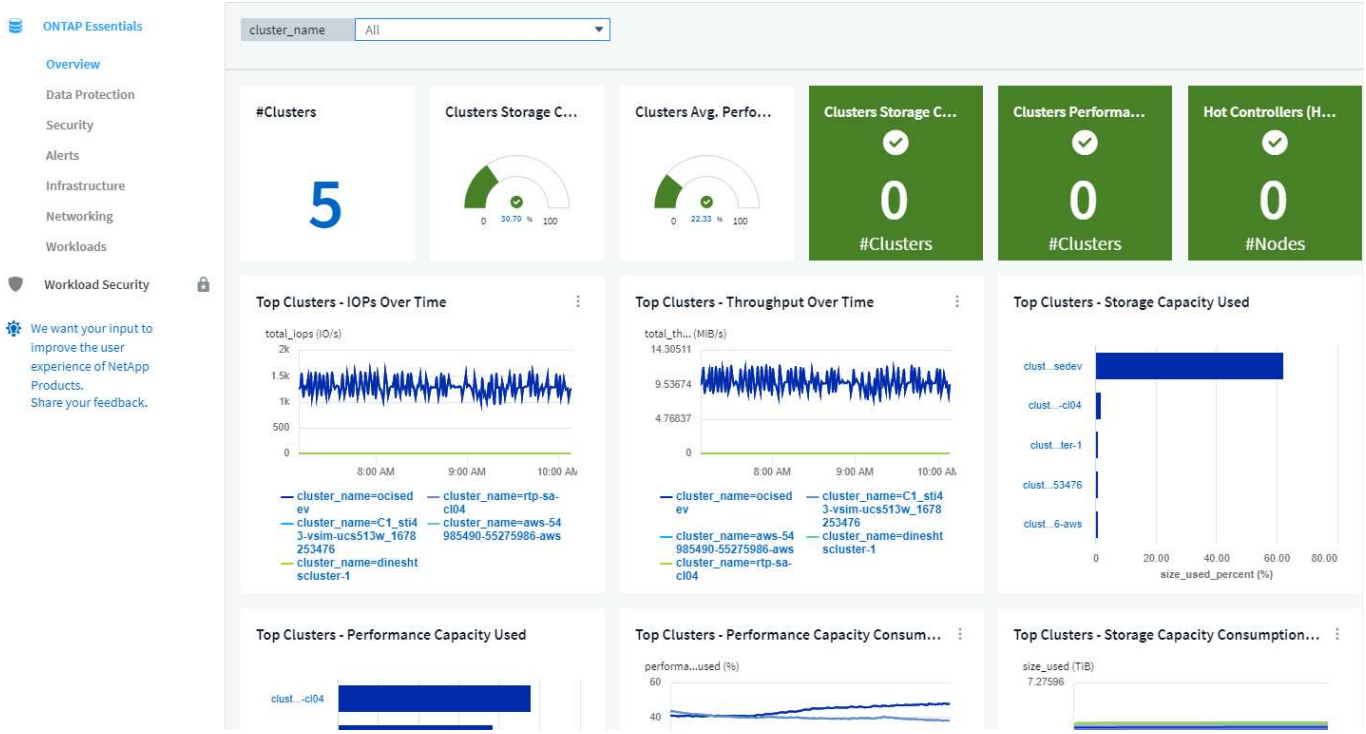
- インフラ/インベントリ：ユーザデータにストレージ/ネットワークサービスを提供するオブジェクト
- Workloads：ユーザにデータの読み取り/書き込みのインターフェイスを提供するオブジェクト。
- データ保護：ネットアップのデータ保護テクノロジを使用して保護できるオブジェクト

ONTAP に関連するその他の用語と定義については、を参照してください "ONTAP データコレクタ" ドキュメント

ONTAP Essentialsには、過去7日間に収集されたデータを含む、最低1つの動作中のONTAP データコレクタが必要です。

概要

データインフラのインサイトのメインメニューから*「ONTAP Essentials」*を選択して、データインフラの詳細を確認してください。



概要*ダッシュボードには、環境内のクラスタ数や全体的な容量とパフォーマンスの割合など、役立つ情報が表示されます。また、ストレージ容量またはパフォーマンス容量がスペース不足になるまでの想定日数に関する予測データも表示されます。また、インフラ内にCPU使用率が65%を超えて稼働しているコントローラがある場合（フェイルオーバー時にクラスタがリスクにさらされる可能性があるため）、ONTAP Essentialsでは「ホット」コントローラと表示されます。

情報グラフは、時間の経過に伴うパフォーマンスの確認や、容量使用率の内訳を提供します。これらのグラフ

やデータポイントは、調査や調査の開始点として使用できます。

注：「フルまでの日数」に0（ゼロ）を指定すると、フルまでの日数が90日を超えたと推定されます。つまり、システムがすぐにスペース不足になる危険性はありません。

データ保護

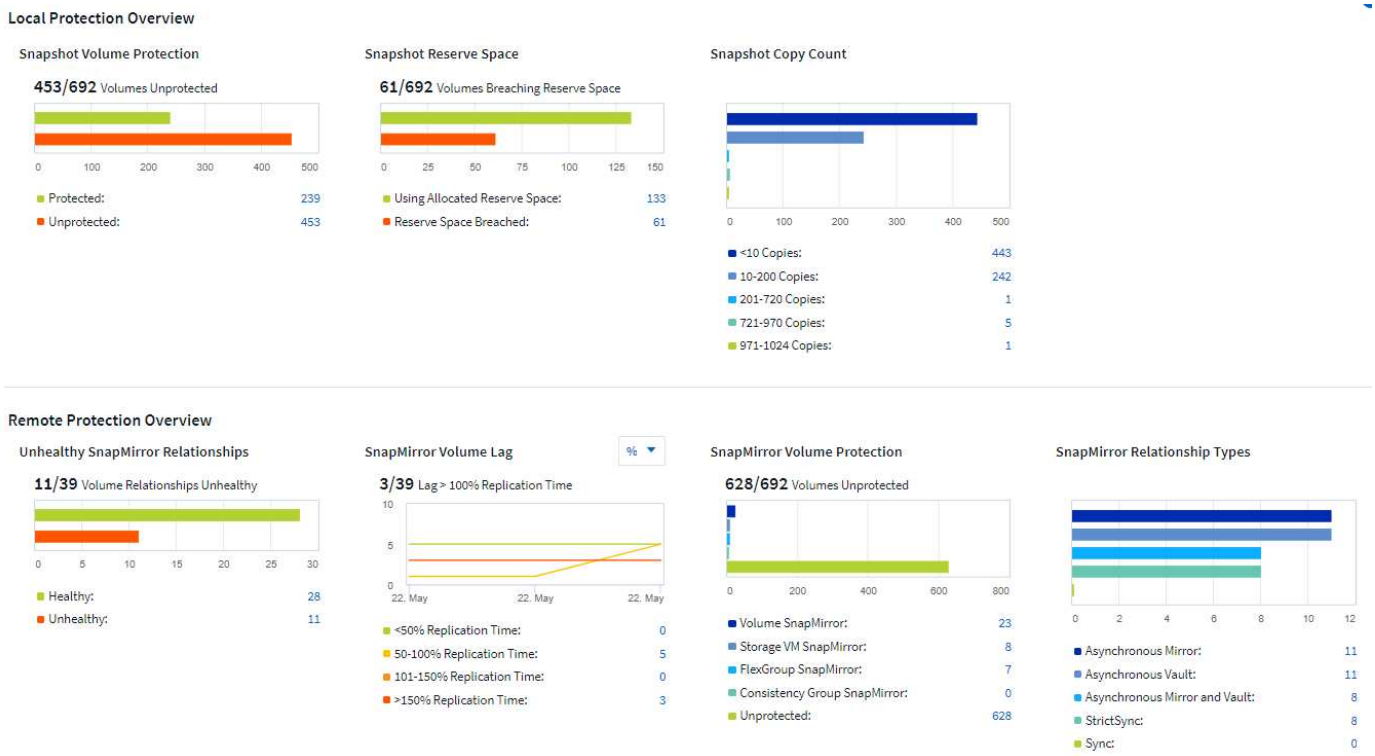
[データ保護]ページには、* Snapshotコピー*または* SnapMirrorポリシー*で保護されているボリュームのステータスが表示されます。

[*Local Protection Overview*]セクションのグラフには、Snapshotコピーで保護されているボリュームに関する次の情報が表示されます。

- Snapshotコピーで保護されているボリュームと保護されていないボリュームの数。
- Snapshotコピー用のリザーブスペースを使用しているボリューム、または超過しているボリュームの数。
- Snapshotコピー数の特定の範囲（コピー数が10個未満、10~200個など）にあるボリュームの数。

[*Remote Protection Overview*]セクションのグラフには、SnapMirrorポリシーで保護されているボリュームに関する情報が表示されます。

- 正常なSnapMirror関係と正常でないSnapMirror関係の数。
- 遅延ステータスに基づくRecovery Point Objective（RPO；目標復旧時点）の遅延が発生しているSnapMirror関係の数。
- SnapMirrorボリューム保護タイプで保護される関係の数（ボリュームSnapMirror、SVMDR関係、FlexGroup SnapMirror関係、SnapMirrorビジネス継続性（SMBC）整合性グループ関係、保護されていないボリュームなど）。
- SnapMirror関係タイプ（非同期ミラー、非同期バックアップ、非同期ミラーバックアップ、StrictSync、Syncなど）で保護されている関係の数。



ウィジェットには、ローカルとリモートの概要が表示されます"]

ページ下部の_Clusters_gridには、次の項目に関する詳細が表示されます。

- ボリュームがSnapshotで保護されていません。
- ボリュームがSnapshotリザーブスペースを超過しています。
- SnapMirrorポリシーで保護されていないボリューム、およびSnapMirror関係で遅延が発生しています。
- 正常でないSnapMirror関係。

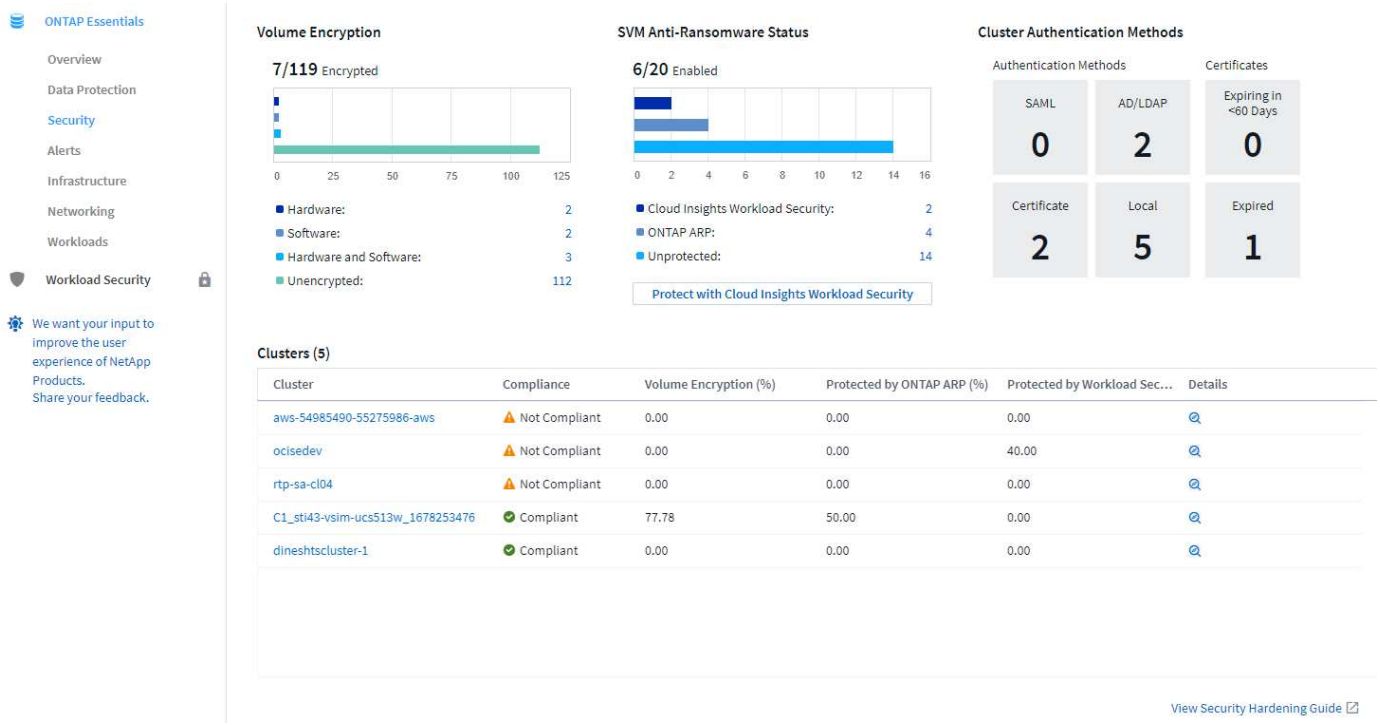
Clusters (6)

Cluster	Volumes Not Protected by Snapshots ↓	Volumes Breaching Snapshot Reserve Space	Volumes Not Protected by SnapMirror	SnapMirror Relationships Experiencing Lag	Unhealthy SnapMirror Relationships
rtp-sa-cl01	304	1	393	0	1
umeng-aff300-01-02	123	20	160	1	3
annapook-vsim12	7	4	7	0	3
C1_sti11-vsim-ucs574m_168327	0	0	0	0	0
C1_sti43-vsim-ucs513w_167825	0	0	0	0	0
ci-cs-fas8060-01-02	0	0	0	0	0

セキュリティ

[Security Dashboard]には、現在のセキュリティ状況が瞬時に表示され、ハードウェアとソフトウェアのボリューム暗号化、ランサムウェア対策ステータス、クラスタ認証方式のチャートが表示されます。セキュリティ基準は、で定義された推奨事項に基づいて評価されます "* ONTAP 9向けネットアップセキュリティ強化ガイド*"。

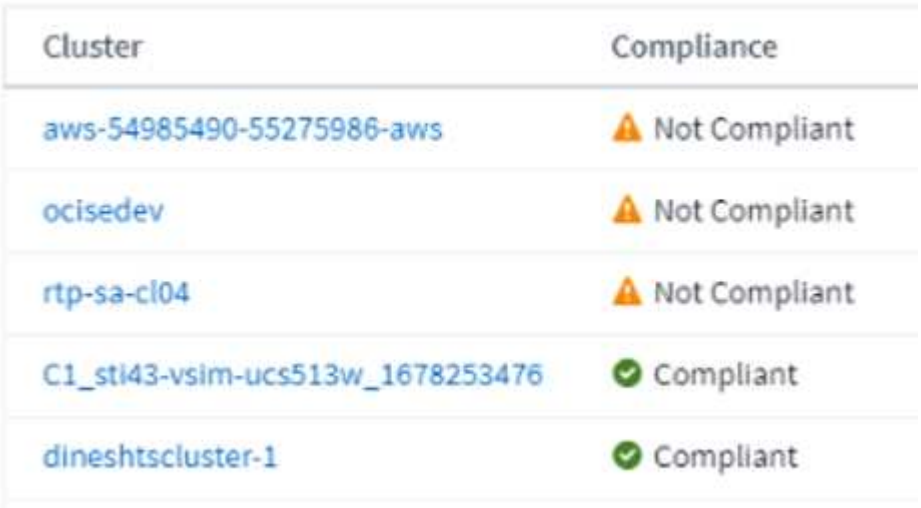
暗号化やランサムウェア対策の中から必要なものを選択して、環境を詳しく調べます。



ONTAP Essentialsのセキュリティダッシュボードは、環境を監視して、クラスタのコンプライアンスステータスを判断します。を参照してください "クラスタ準拠カテゴリ" をクリックしてください。ONTAP Essentialsでは、次のモニタを使用してコンプライアンスを判断します。

モニタ名	属性名（**[Cluster Details]**に表示）	属性準拠値
FIPSモードが無効になりました	FIPS モード	有効
SSH用のクラスタのセキュアでない暗号	Secure SSH設定	はい。
Telnetプロトコルが有効です	Telnet	無効
リモートシェルが有効です	リモートシェル（ Remote Shell ）	無効
デフォルトのローカル管理者ユーザが有効です	デフォルトの管理ユーザ	無効
MD5ハッシュ化パスワード	MD5が使用中です	いいえ
クラスタピア通信が暗号化されていません	クラスタピアリング	暗号化/ピアなし
AutoSupport HTTPS転送が無効です	HTTPSを使用するAutoSupport	はい。
NTPサーバが設定されていません	Network Time Protocol の略	を設定します
NTPサーバ数が不足しています	Network Time Protocol の略	を設定します
クラスタでログインバナーが無効になりました	ログインバナー	有効
ログ転送が暗号化されていない	ログ転送が暗号化されました	はい。

上記のモニタが無効になっている場合は、クラスタの詳細で対応するセキュリティ準拠属性の値が「Not checked」と表示されることに注意してください。

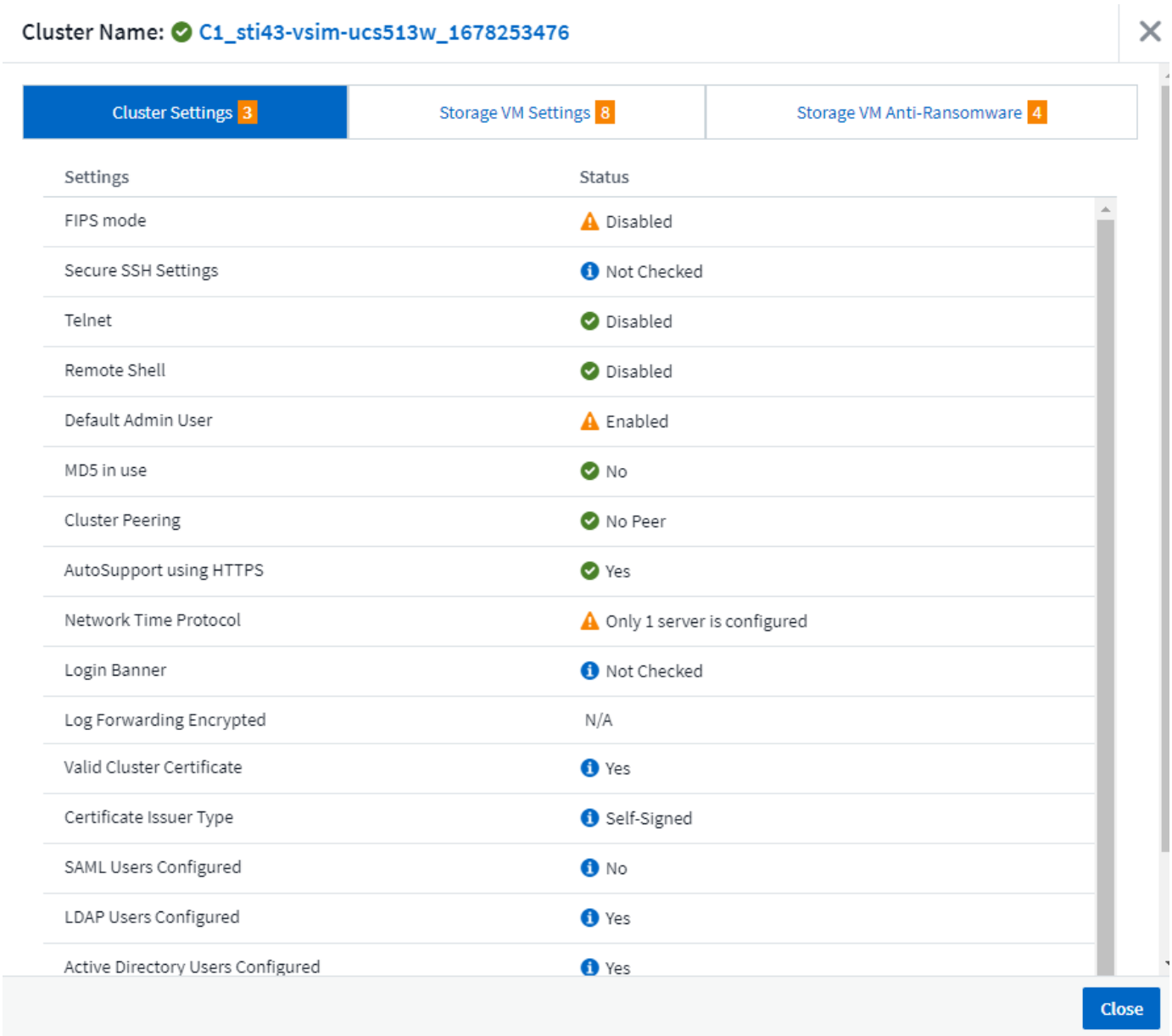


SVMの場合、[Security]ダッシュボードでは次のモニタが表示されます。

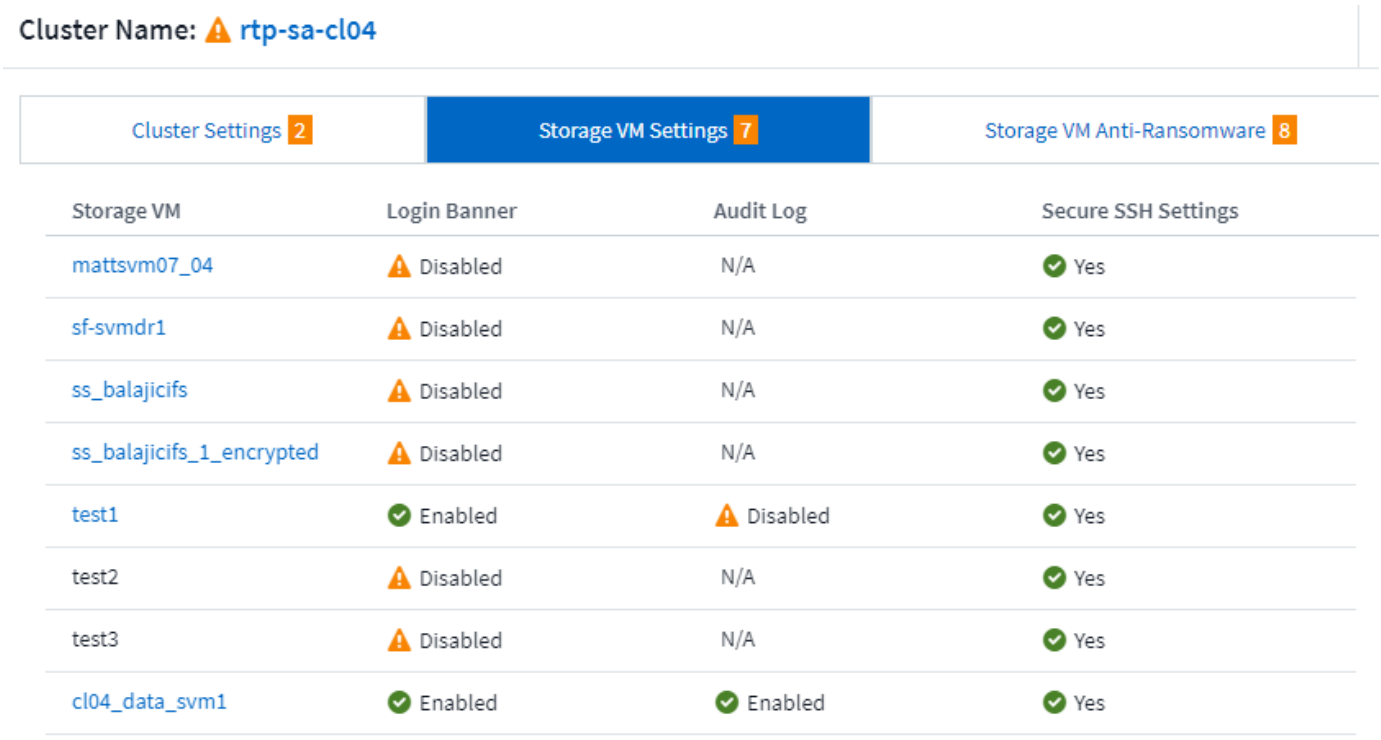
モニタ名	属性名（**Storage VM**設定に表示）	属性準拠値
SSH用のStorage VMのセキュアでない暗号	Secure SSH設定	はい。
Storage VMのログインバナーが無効になっています	ログインバナー	有効
Storage VM監査ログが無効になりました	監査ログ	有効

クラスタリストで、各クラスタの[*View Details*]を選択してスライドアウトパネルを開き、_Cluster、Storage VM、_or_Anti-Ransomware_の現在の設定を確認します。

クラスタの詳細には、接続ステータスや証明書情報などがあります。



Storage VMの詳細には、監査とSSHの情報が表示されます。

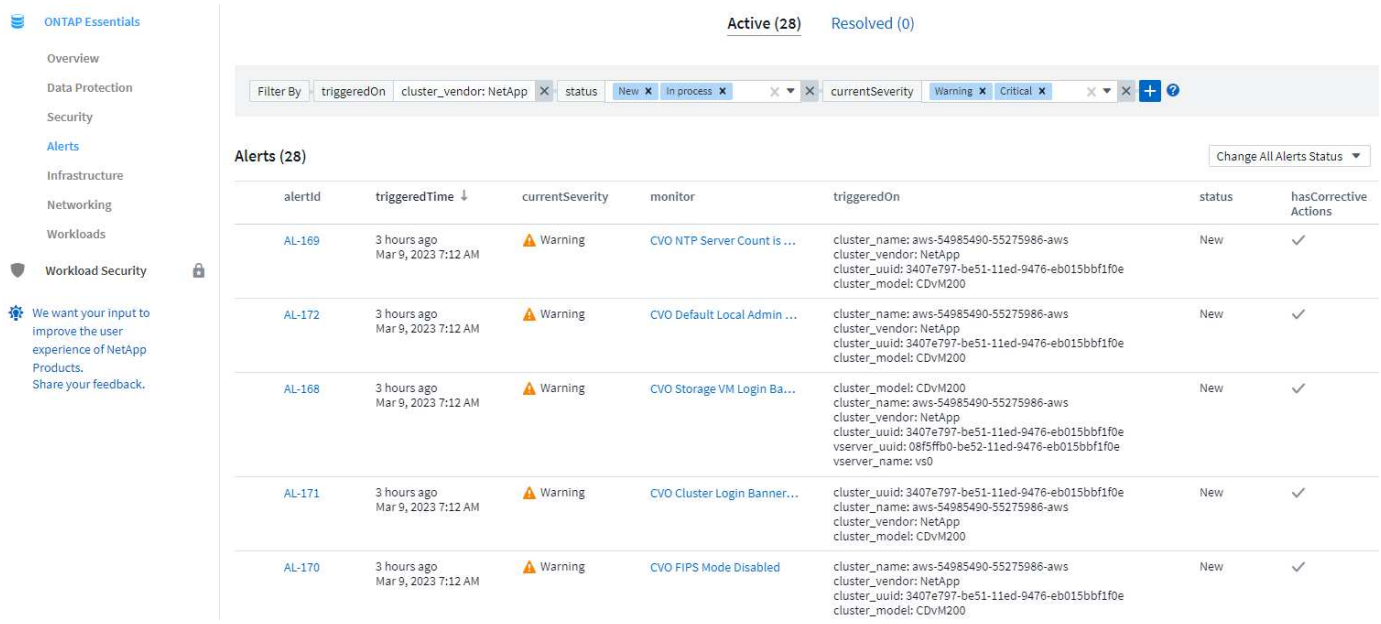


タブ"]

ランサムウェア対策の詳細では、Storage VMがONTAPのランサムウェア対策とデータインフラ分析情報のワークロードセキュリティのどちらで保護されているかを確認できます。ONTAP の[ARP]列には、ONTAP システムで設定されているONTAPのオンボードランサムウェア対策の現在のステータスが表示されます。Data Infrastructure Insightsワークロードセキュリティを有効にするには、列の[保護]を選択します。

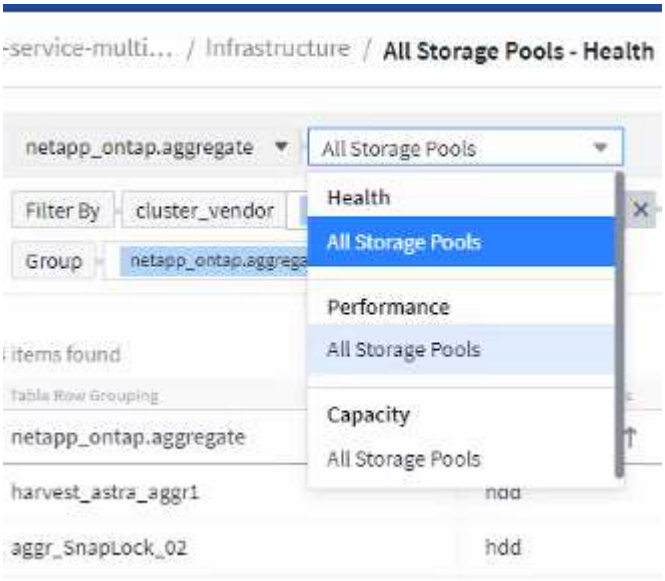
アラート

ここでは、環境内のアクティブなアラートを表示し、潜在的な問題をすばやく詳細に把握できます。解決済みのアラートを表示するには、_Resolvedタブを選択します。

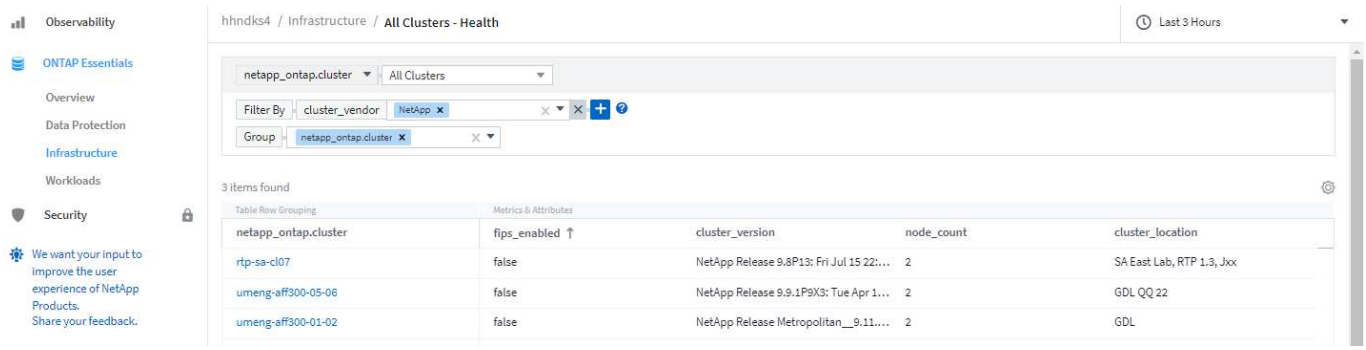


インフラ

ONTAP Essential* Infrastructure *ページでは、すべての基本的なONTAP オブジェクトに対して事前に構築された（さらにカスタマイズ可能な）クエリーを使用して、クラスタの正常性とパフォーマンスを確認できます。確認するオブジェクトタイプ（クラスタ、ストレージプールなど）を選択し、健常性とパフォーマンスのどちらの情報を表示するかを選択します。フィルタを設定して、個々のシステムの詳細を調べます。

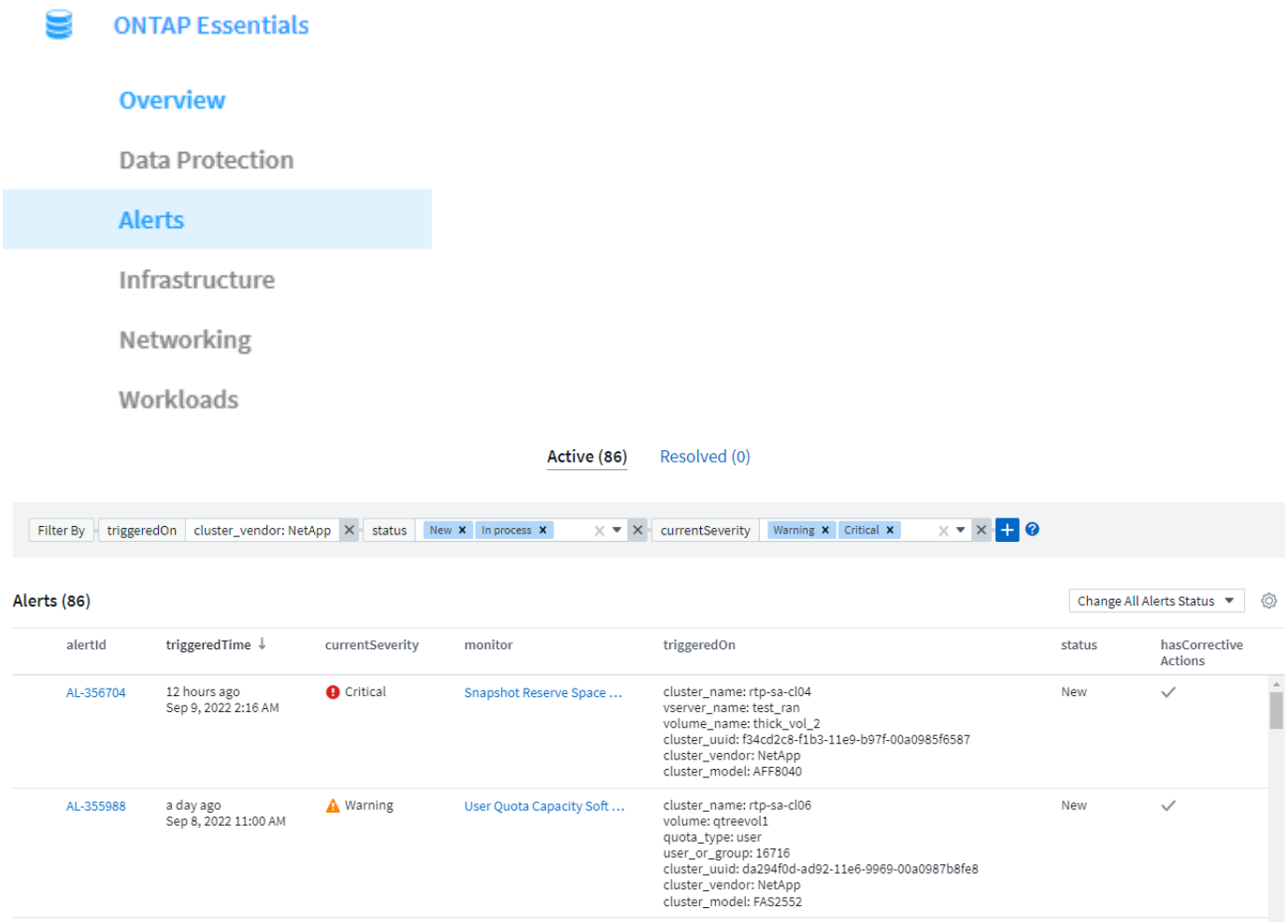


クラスタの健常性を示すインフラのページ：



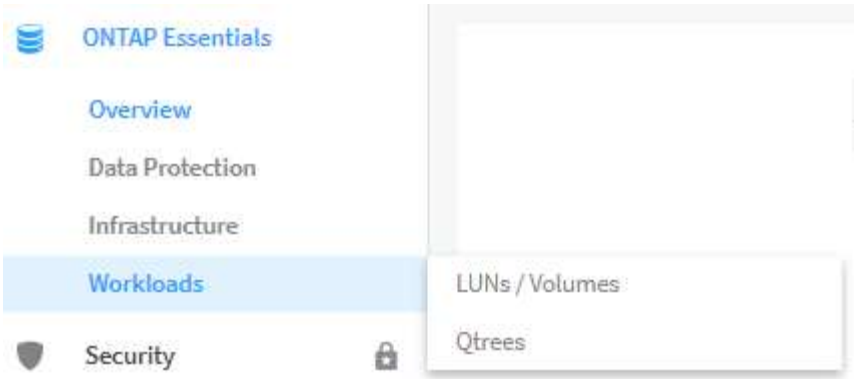
ネットワーキング

ONTAP Essentialsネットワーキングでは、FC、NVMe FC、イーサネット、およびiSCSIインフラストラクチャを確認できます。このページでは、クラスタ内のポートやクラスタ内のノードを確認できます。



ワークロード

環境内のLUN /ボリューム、NFSまたはSMB共有、またはqtreeのワークロードを表示して確認できます。



netapp_ontap.lun | All LUNs

Filter By | cluster_vendor | NetApp

Group | netapp_ontap.lun

13 items found

Table Row Grouping	Metrics & Attributes								
netapp_ontap.lun	total_late... ↑	total_iops (IO/s)	total_through...	size (B)	size_used (B)	volume	vserver_name	aggregate_name	node
/vol/ste/ste	0.00	0.00	0.00	53,694,627,840....	0.00	ste	vs_test	umeng_aff300...	ui
/vol/kubebug/kubebuglun1	0.00	0.00	0.00	85,905,637,376....	1,489,985,536.00	kubebug	vs_test	umeng_aff300...	ui
/vol/trident_pvc_3ef5a87c_4149_44e8_8113...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_3e...	vs_test	umeng_aff300...	ui
/vol/trident_pvc_0bf4ffd4_3f11_4d63_aa01_...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_0b...	vs_test	umeng_aff300...	ui
/vol/NSLM_VOL_LUN_1597772263794/matts...	0.00	0.00	0.00	1,073,741,824.00	0.00	NSLM_VOL_LU...	VMware_test	aggr_data_01_...	rt
/vol/mattlun12345/mattlun12345	0.00	0.00	0.00	1,073,741,824.00	0.00	mattlun12345	VMware_test	aggr_data_01_...	rt
/vol/kubebug1/kubebuglun2	0.00	0.00	0.00	85,904,826,368....	0.00	kubebug1	vs_test	umeng_aff300...	ui
/vol/trident_pvc_d66d7f51_a623_4fc3_8cda...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_d6...	vs_test	umeng_aff300...	ui
/vol/Rah/Rah	0.00	0.00	0.00	57,576,960.00	0.00	Rah	vs_test	umeng_aff300...	ui
/vol/chap_test_lun_vol/chap_test_lun	0.00	0.00	0.00	107,374,182,40...	0.00	chap_test_lun_...	VMware_test	aggr_data_01_...	rt
/vol/windows_iscsi_example/windows_iscsi...	0.00	0.00	1.04	1,073,741,824.00	10,911,744.00	windows_iscsi...	VMware_test	aggr_data_01_...	rt
/vol/vol_test/lun1	0.04	0.10	0.00	1,073,741,824.00	0.00	vol_test	vs_test	umeng_aff300...	ui
/vol/osc_iscsi_vol01/osc_iscsi_vol01	2.11	116.83	2,737,374.33	4,398,046,511,1...	2,535,381,008,3...	osc_iscsi_vol01	osc	umeng_aff300...	ui

管理およびその他のタスク

データインフラ分析情報API

Data Infrastructure Insights APIを使用すると、NetAppのお客様や独立系ソフトウェアベンダー（ISV）は、データインフラの分析情報をCMDBやその他のチケット発行システムなどの他のアプリケーションと統合できます。

Data Infrastructure InsightsのAPIは、現在のエディションに基づいて使用できます。

APIタイプ	基本	標準	Premium サービス
Acquisition Unit の略	✔	✔	✔
データ収集	✔	✔	✔
アラート		✔	✔
資産		✔	✔
データの取り込み		✔	✔
ログの取り込み		✔	✔

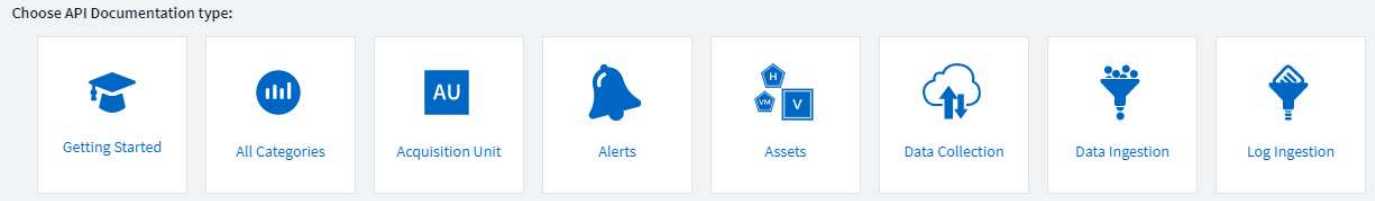
さらに、Data Infrastructure Insights"機能セットのロール"がアクセス可能なAPIを決定します。ユーザロールとゲストロールの権限は、管理者ロールよりも少なくなります。たとえば、 Monitor と Optimize で Administrator ロールを割り当てていても、 Reporting で User ロールを割り当てている場合は、 Data Warehouse を除くすべての API タイプを管理できます。

API アクセスの要件

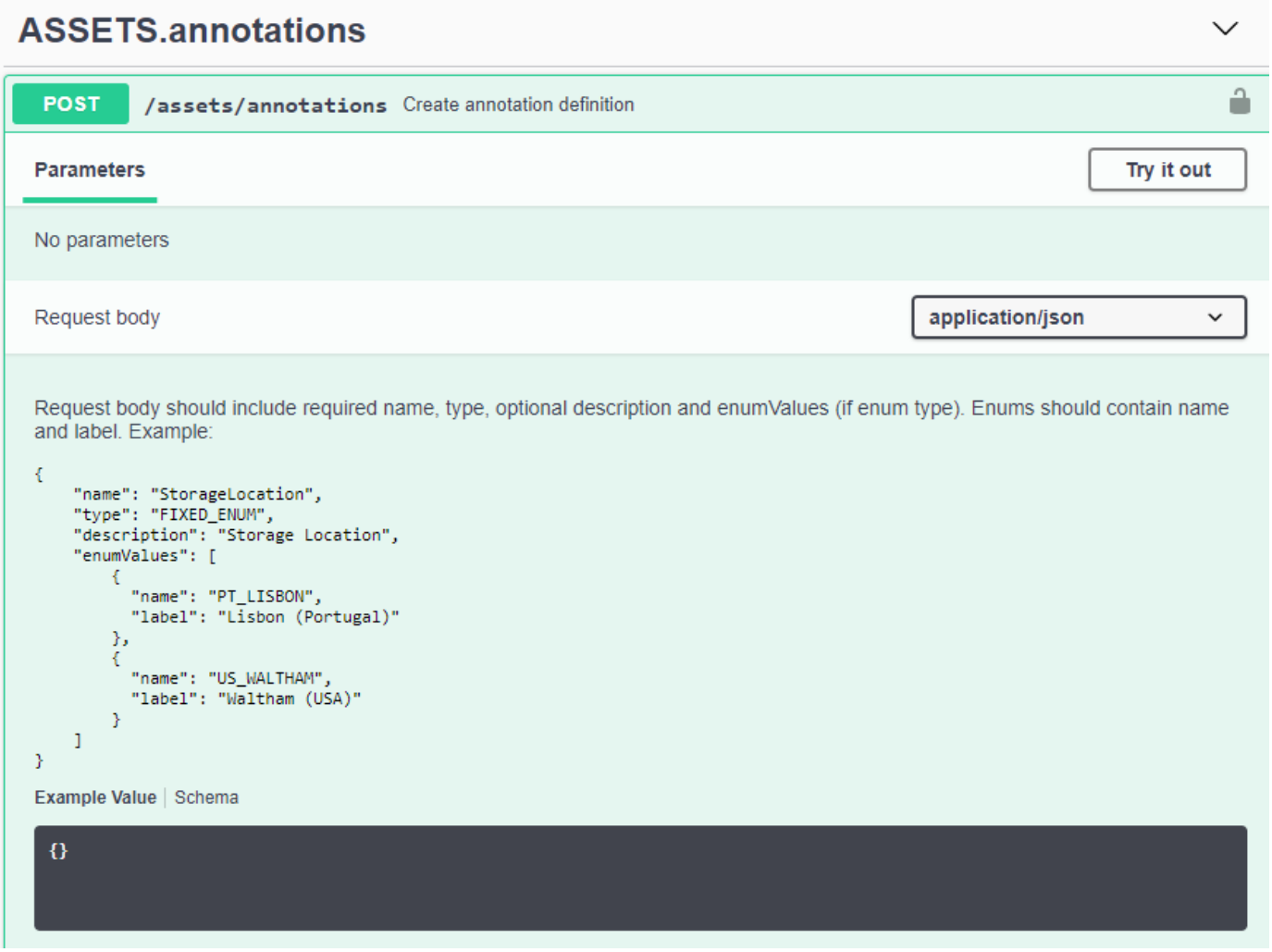
- API アクセストークンモデルを使用してアクセスが許可されます。
- APIトークン管理は、管理者ロールを持つData Infrastructure Insightsユーザによって実行されます。

API ドキュメント（ Swagger ）

最新のAPI情報は、Data Infrastructure Insightsにログインし、**[Admin]>[API Access]***に移動すると確認できます。**[API Documentation]** リンクをクリックします。



API ドキュメントは Swagger ベースです。 API の簡単な概要情報と使用方法を提供しており、環境内で試すことができます。ユーザロールやData Infrastructure Insightsのエディションによっては、使用できるAPIタイプが異なる場合があります。



API アクセストークン

Data Infrastructure Insights APIを使用する前に、1つ以上の* APIアクセストークン*を作成する必要があります。アクセストークンは、指定された API タイプに使用され、読み取り権限と書き込み権限を付与できます。各アクセストークンの有効期限を設定することもできます。指定したタイプの API はすべて、アクセストークンに対して有効です。各トークンはユーザ名またはパスワードを無効にします。

アクセストークンを作成するには：

- **[Admin] > [API Access]** をクリックします
- [*+API アクセストークン *] をクリックします
  - トークン名を入力します
  - API タイプを選択します
  - この API アクセスに付与する権限を指定します
  - トークン有効期限を指定します

トークンは、クリップボードにコピーして作成プロセス中に保存する場合にのみ使用できます。トークンは作成後に取得できないため、トークンをコピーして安全な場所に保存することを強くお勧めします。トークン作成画面を閉じる前に、 [API アクセストークンのコピー *] ボタンをクリックするよう求められます。

トークンを無効化、有効化、および取り消しできます。無効になっているトークンを有効にできます。

トークンを使用すると、お客様の観点から API への汎用アクセスが許可され、独自のテナントの範囲内で API へのアクセスが管理されます。お客様の管理者は、Data Infrastructure Insightsのバックエンド担当者が直接関与することなく、これらのトークンを許可または取り消しできます。

アプリケーションは、ユーザがアクセスの認証と許可に成功した後、ターゲット API を呼び出すときにアクセストークンをクレデンシャルとして渡します。渡されたトークンは、 API にアクセスするためのトークンのベアラーが許可されていることを API に通知し、許可中に許可されたスコープによって指定された特定のアクションを実行します。

アクセストークンが渡される HTTP ヘッダーは * X-CloudInsights - apiKey ： * です。

たとえば、次のようにしてストレージアセットを取得します。

```
 curl https://<tenant_host_name>/rest/v1/assets/storages -H 'X-
CloudInsights-ApiKey:<API_Access_Token>'
```

_<API_Access_Token>_ は、 API アクセスの作成時に保存したトークンです。

使用するAPIに固有の例については、swaggerページを参照してください。

APIタイプ

Data Infrastructure Insights APIはカテゴリベースであり、現在次のタイプが含まれています。

- アセットタイプには、アセット、クエリ、および検索 API が含まれます。
  - アセット：最上位のオブジェクトを列挙し、特定のオブジェクトまたはオブジェクト階層を取得します。
  - クエリ：Data Infrastructure Insightsのクエリを取得して管理します。
  - インポート：アノテーションまたはアプリケーションをインポートしてオブジェクトに割り当てます
  - 検索：オブジェクトの一意の ID またはフルネームを知らずに、特定のオブジェクトを検索します。
- データ収集タイプは、データコレクタを取得および管理するために使用します。
- データの取り込みタイプは、 Telegraf エージェントなどの取り込みデータとカスタムメトリックを取得および管理するために使用されます
- ログの取り込みは、ログデータの取得と管理に使用されます

これ以外のタイプや API は、時間の経過とともに使用できるようになる可能性があります。最新の API 情報は、で確認できます "API Swagger のドキュメント"。

ユーザがアクセスできるAPIタイプは、"ユーザロール"Data Infrastructure Insightsの各機能セット（監視、ワークロードセキュリティ、レポート）にあるAPIタイプによっても異なります。

在庫移動

このセクションでは、Data Infrastructure Insightsオブジェクトの階層を横断する方法について説明します。

トップレベルオブジェクト

個々のオブジェクトは、一意の URL （ JSON では「 self 」）によって要求に示され、オブジェクトタイプと内部 ID を知る必要があります一部のトップレベルオブジェクト（ホスト、ストレージなど）については、 REST API を使用して完全なコレクションにアクセスできます。

API URL の一般的な形式は次のとおりです。

```
 https://<tenant>/rest/v1/<type>/<object>
```

たとえば、 _mysite.c01.cloudinsights.netapp.com_ という名前のテナントからすべてのストレージを取得する場合、要求の URL は次のようになります。

```
https://mysite.c01.cloudinsights.netapp.com/rest/v1/assets/storages
```

子および関連オブジェクト

ストレージなどの最上位のオブジェクトを使用して、他の子や関連オブジェクトをトラバースできます。たとえば、特定のストレージのすべてのディスクを取得するには、ストレージの「 self 」 URL を「 /disks 」に連結します。次に例を示します。

```
https://<tenant>/rest/v1/assets/storages/4537/disks
```

展開します

多くの API コマンドでは、関連オブジェクトのオブジェクトや URL に関する追加情報を提供する * expand * パラメータがサポートされています。

共通の展開パラメータの 1 つは _expands_です応答には、オブジェクトに対して使用可能なすべての特定の展開のリストが含まれています。

たとえば、次のように要求したとします。

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=_expands
```

API は、オブジェクトに対して使用可能なすべての拡張を次のように返します。

```
{
      "id": "1247936",
        "self": "/rest/v1/assets/storages/1247936",
        "name": "amsprdclu01",
        "simpleName": "amsprdclu01",
        "naturalKey": "5DF483F0-1729-11DC-9A79-123478563412",
        "ip": "10.64.0.132",
        "serialNumber": "1-80-000011",
        "model": "FAS3270,FAS6290",
        "vendor": "NetApp",
        "microcodeVersion": "8.1.3 clustered Data ONTAP",
        "capacity": {
          "description": "Storage Capacity",
          "unitType": "MB",
          "total": {
            "value": 8.23185105E8
          },
          "storagePools": {
            "value": 5.43220974E8
          }
        },
        "isActive": true,
        "createTime": "2013-05-07T16:52:21-0700",
        "family": "FAS3200,FAS6200",
        "managementUrl": null,
        "virtualizedType": "STANDARD",
        "protocols":
        [
          "NAS",
          "NFS",
          "CIFS",
          "FC",
          "ISCSI"
        ],
        "_expands": {
          "performance": {
            "url": "/rest/v1/assets/storages/1247936/performance",
            "name": "Performance Data"
          },
          "storageNodes": {
            "url": "/rest/v1/assets/storages/1247936/storageNodes",
            "name": "Storage Storage Nodes"
          },
          "storagePools": {
            "url": "/rest/v1/assets/storages/1247936/storagePools",
            "name": "Storage Storage Pools"
          },
          "storageResources": {
            "url": "/rest/v1/assets/storages/1247936/storageResources",
            "name": "Storage Storage Resources"
          },
          "internalVolumes": {
            "url": "/rest/v1/assets/storages/1247936/internalVolumes",
            "name": "Storage Internal Volumes"
          },
          "volumes": {
            "url": "/rest/v1/assets/storages/1247936/volumes",
            "name": "Storage Volumes"
          },
          "disks": {
            "url": "/rest/v1/assets/storages/1247936/disks",
            "name": "Disks"
          },
          "datasources": {
            "url": "/rest/v1/assets/storages/1247936/datasources",
            "name": "Storage Datasources"
          },
          "ports": {
            "url": "/rest/v1/assets/storages/1247936/ports",
            "name": "Storage Ports"
          },
          "annotations": {
            "url": "/rest/v1/assets/storages/1247936/annotations",
            "name": "Storage Annotations"
          },
          "qtrees": {
            "url": "/rest/v1/assets/storages/1247936/qtrees",
            "name": "Qtrees"
          },
```

各展開には、データ、 URL 、またはその両方が含まれます。expand パラメータでは、次のような複数の属性とネストされた属性がサポートされます。

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=performance,storageR
esources.storage
```

`Expand` を使用すると、関連するデータを `1` 回の応答で大量に取り込むことができます。ネットアップでは、一度に大量の情報を要求しないことを推奨しています。これにより、原因のパフォーマンスが低下する可能性があります。

これを防止するために、トップレベルのコレクションに対する要求は展開できません。たとえば、すべてのストレージオブジェクトの拡張データを一度に要求することはできません。クライアントは、オブジェクトのリストを取得し、特定のオブジェクトを選択して拡張する必要があります。

パフォーマンスデータ

パフォーマンスデータは、さまざまなデバイスにわたって個別のサンプルとして収集されます。Data Infrastructure Insightsでは、パフォーマンスサンプルが1時間ごと（デフォルト）に集計され、要約されます。

この API を使用すると、サンプルと集計データの両方にアクセスできます。パフォーマンスデータが格納されたオブジェクトの場合、パフォーマンスの概要は *expand = performion.*パフォーマンス履歴の時系列は、Nested_expand= perform中 .history_ で確認できます。

パフォーマンスデータオブジェクトには次のようなものがあります。

- ストレージパフォーマンス
- StoragePoolPerformance の各ノードでパフォーマンスが
- PortPerformance の 2 つのグループ
- ディスクパフォーマンス

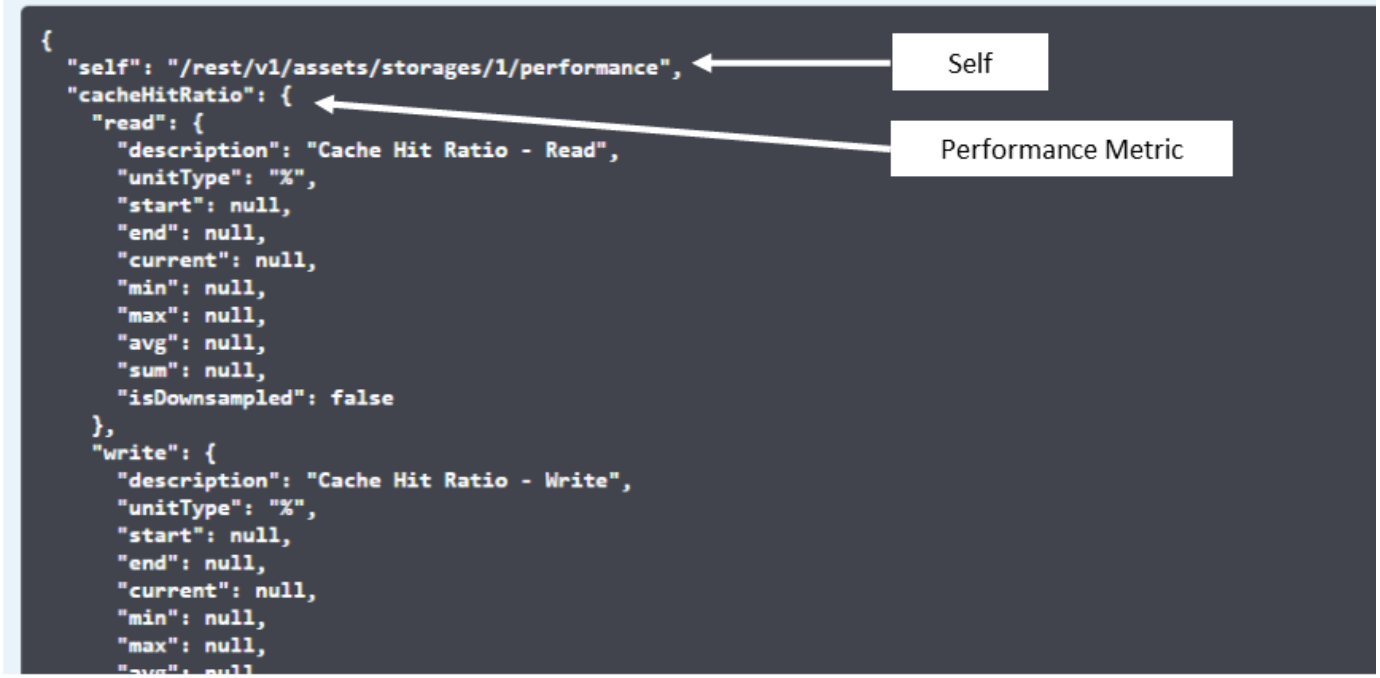
パフォーマンスメトリックには、概要 とタイプがあり、パフォーマンスサマリーのコレクションが含まれています。たとえば、 Latency 、 Traffic 、 Rate などです。

パフォーマンスサマリーには、 1 つのパフォーマンスカウンタから特定の期間（ 1 時間、 24 時間、 3 日間など）にわたって計算された概要、ユニット、サンプル開始時間、サンプル終了時間、および要約された値（現在、最小、最大、平均など）のコレクションが含まれます。

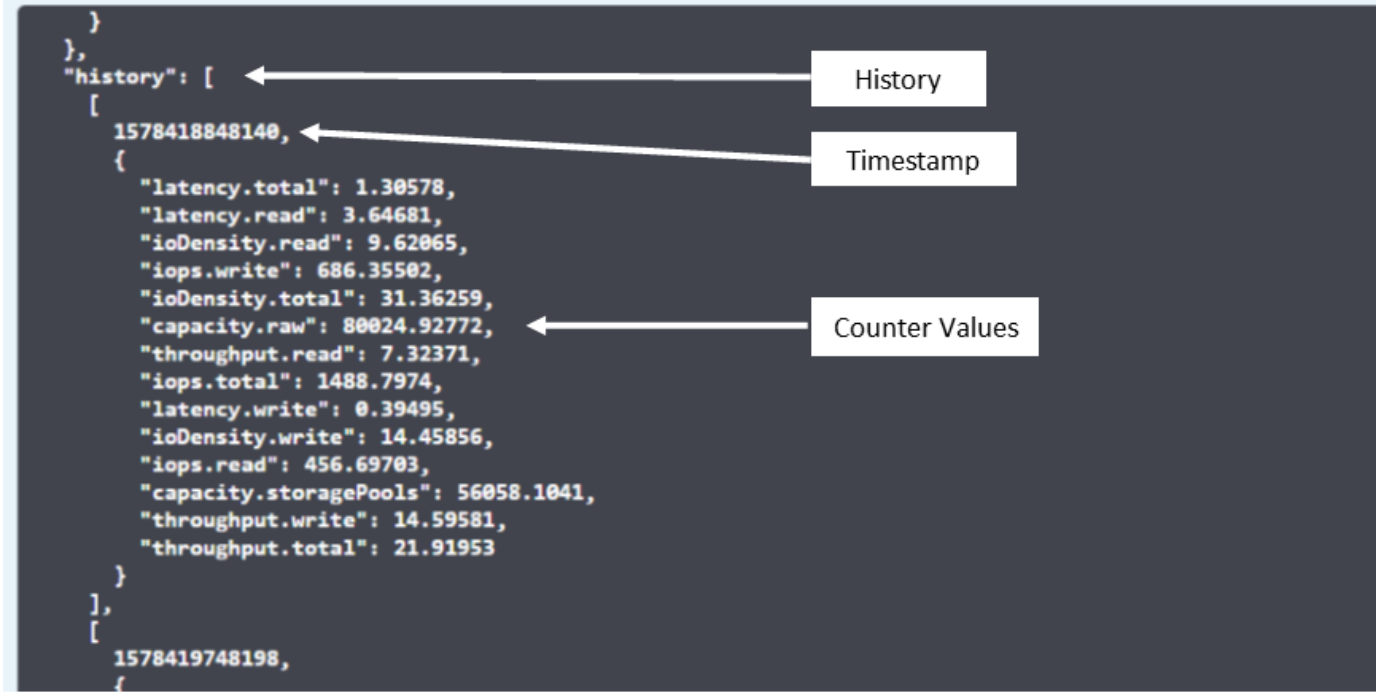
https://tenant.cloudinsights.netapp.com/rest/v1/assets/storages/1/performance?expand=history

Details

Response body



Response body



結果の Performance Data ディクショナリには、次のキーがあります。

- 「 self 」は、オブジェクトの一意の URL です

- 「 history 」は、タイムスタンプとカウンタ値のマップのペアのリストです
- 他のすべてのディクショナリキー（「 diskThroughput 」など）は、パフォーマンスメトリックの名前です。

パフォーマンスデータのオブジェクトタイプごとに、一意のパフォーマンス指標のセットがあります。たとえば、仮想マシンのパフォーマンスオブジェクトは、パフォーマンスメトリックとして「 diskThroughput 」をサポートします。サポートされている各パフォーマンスメトリックは、メトリックディクショナリに示されている特定の「パフォーマンスカテゴリ」です。Data Infrastructure Insightsは、本ドキュメントで後述する複数のパフォーマンス指標タイプをサポートしています。各パフォーマンスメトリックディクショナリには、このパフォーマンスメトリックの判読可能な概要である「概要」フィールドと、パフォーマンスサマリーカウンタエントリのセットも含まれます。

Performance Summary カウンタは、パフォーマンスカウンタの要約です。これは、カウンタの一般的な集計値であり、最新の測定値、要約データの時間範囲、カウンタの単位タイプ、データのしきい値なども表示します。しきい値のみオプションで、残りの属性は必須です。

パフォーマンス要約は、次のタイプのカウンタで使用できます。

- Read –読み取り処理の概要
- Write –書き込み処理の概要です
- Total –すべての処理の概要。読み取りと書き込みの単純な合計よりも高くなる場合があり、それ以外の処理も含まれる場合があります。
- Total Max –すべての処理の概要。指定した期間内の最大合計値です。

オブジェクトのパフォーマンス指標

API は、環境内のオブジェクトについて、次のような詳細な指標を返すことができます。

- IOPS （ 1 秒あたりの入出力要求の数）、レイテンシ、スループットなどのストレージパフォーマンス指標。
- スイッチのパフォーマンス指標：トラフィック利用率、 BB クレジットゼロデータ、ポートエラーなど。

を参照してください "API Swagger のドキュメント" 各オブジェクトタイプの指標に関する情報が表示されます。

パフォーマンス履歴データ

履歴データは、タイムスタンプとカウンタマップのペアのリストとしてパフォーマンスデータに表示されます。

履歴カウンタの名前は、パフォーマンス指標オブジェクトの名前に基づいて決まります。たとえば、仮想マシンのパフォーマンスオブジェクトは「 diskThroughput 」をサポートしているため、履歴マップには「 diskThroughput 」、「 diskThroughput 」、「 diskThroughput 」、「 diskThroughput 」、「 diskThroughput total 」という名前のキーが含まれます。

timestamp は UNIX の時間形式です。

ディスクのパフォーマンスデータの JSON の例を次に示します。

```
"performance": {
    "self": "/rest/v1/assets/disks/4013931/performance",
    "iops": {
      "performanceCategory": "IOPS",
      "description": "Disk IOPS",
      "read": {
        "description": "Disk Read Iops",
        "unitType": "IO/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 1,
        "min": 0,
        "max": 6,
        "avg": 0.5532
      },
  […]
     "total": {
        "description": "Disk Total Throughput",
        "unitType": "MB/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 0,
        "min": 0,
        "max": 2,
        "avg": 0.1702
      }
    },
    "history":
    [
      [
        1399300412690,
        {
          "utilization.total": 12,
          "iops.total": 26,
          "iops.write": 22,
          "iops.read": 4,
          "throughput.read": 0,
          "utilization.read": 2.12,
          "throughput.total": 5,
          "utilization.write": 10.24,
          "throughput.write": 5
```


容量属性を持つオブジェクト

容量の属性を持つオブジェクトは、基本的なデータ型と CapacityItem を使用して表現します。

CapacityItem

CapacityItem は、容量の単一の論理ユニットです。親オブジェクトで定義された単位には「値」と「高しきい値」があります。また、容量値の構成方法を説明するオプションの内訳マップもサポートしています。たとえば、 100TB の StoragePool の総容量は、 1 、 000 の CapacityItem になります。この内訳では、「データ」に 60 TB 、「スナップショット」に 40 TB が割り当てられています。

注

「 highThreshold 」は、対応するメトリックのシステム定義のしきい値を表します。このしきい値を使用すると、クライアントは、許容範囲外の設定された値に関するアラートや視覚的なキューを生成できます。

次に、複数の容量カウンタがある StoragePools の容量を示します。

[検索（ **Search** ）] を使用してオブジェクトを検索する

検索 API は、システムへのシンプルなエントリポイントです。API に対する唯一の入力パラメータは自由形式の文字列であり、結果の JSON には分類された結果のリストが含まれています。タイプは、ストレージ、ホスト、データストアなど、インベントリのアセットタイプによって異なります。各タイプには、検索条件に一致するタイプのオブジェクトのリストが含まれます。

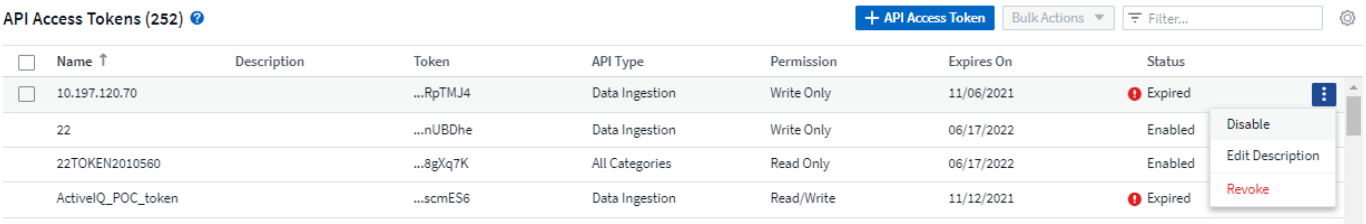
Data Infrastructure Insightsは拡張可能な（オープンな）ソリューションで、サードパーティのオーケストレーションシステム、ビジネス管理システム、変更管理システム、チケット発行システム、カスタムCMDB統合との統合を可能にします。

Cloud Insight の RESTful API は、データのシンプルかつ効果的な移動を可能にし、ユーザがデータにシームレスにアクセスできるようにする統合の主要なポイントです。

API トークンの無効化または取り消し

API トークンを一時的に無効にするには、 API トークンリストページで API の「 3 つのドット」メニューをクリックし、 *Disable* を選択します。 トークンは ' 同じメニューを使用して *'Enable* を選択していつでも再度有効にできます

API トークンを完全に削除するには、メニューから「 Revoke 」を選択します。取り消されたトークンは再度有効にすることはできません。新しいトークンを作成する必要があります。



期限切れの API アクセストークンの回転

API アクセストークンには有効期限があります。API アクセストークンの期限が切れると、ユーザは新しいトークン（ TYPE_Data Ingestion _ with Read/Write パーミッション）を生成し、期限切れのトークンではなく、新しく生成されたトークンを使用するように Telegraf を再設定する必要があります。以下の手順では、その方法について詳しく説明します。

Kubernetes

これらのコマンドでは、デフォルトのネームスペースである「 NetApp-monitoring 」が使用されていることに注意してください。 独自のネームスペースを設定した場合は、それらのネームスペースと、以降のすべてのコマンドおよびファイルを置き換えます。

注：最新のNetApp Kubernetes Monitoring Operatorがインストールされ、更新可能なAPIアクセストークンを使用している場合、期限切れになるトークンは自動的に新規または更新されたAPIアクセストークンに置き換えられます。 以下に示す手動手順を実行する必要はありません。

- NetApp Kubernetes Monitoring Operatorを編集します。

```
 kubectl -n netapp-monitoring edit agent agent-monitoring-netapp
* 古いAPIトークンを新しいAPIトークンに置き換えて、_spec.output-sink.api-key_valueを変更します。
```

```
spec:
…
  output-sink:
  - api-key:<NEW_API_TOKEN>
```

RHEL / CentOS と **Debian/Ubuntu**

- Telegraf 構成ファイルを編集し、古い API トークンのすべてのインスタンスを新しい API トークンに置き換えます。

```
 sudo sed -i.bkup 's/<OLD_API_TOKEN>/<NEW_API_TOKEN>/g'
/etc/telegraf/telegraf.d/*.conf
* Tegraf を再起動します。
```

```
sudo systemctl restart telegraf
```

Windows の場合

- 各 Tegraf コンフィギュレーションファイルを *C ： \Program Files\Telegra\Telegraf .d* で、古い API トークンのすべてのインスタンスを新しい API トークンに置き換えます。

```
cp <plugin>.conf <plugin>.conf.bkup
(Get-Content <plugin>.conf).Replace('<OLD_API_TOKEN>',
'<NEW_API_TOKEN>') | Set-Content <plugin>.conf
```

- Tegraf を再起動します。

```
Stop-Service telegraf
Start-Service telegraf
```

環境の監視

監査

予想される変更（追跡用）と予想外の変更（トラブルシューティング用）の両方を特定するために、Data Infrastructure Insightsのシステムイベントとユーザアクティビティの監査証跡を表示できます。

監査済みイベントの表示

[監査] ページを表示するには、メニューの [管理者] 、 [監査 *] の順にクリックします。監査ページが表示され、各監査エントリについて次の詳細が示されます。

- * Time * - イベントまたはアクティビティの日付と時刻
- * ユーザー * - アクティビティを開始したユーザー
- ロール- Data Infrastructure Insightsにおけるユーザのロール（ゲスト、ユーザ、管理者）
- *ip * - イベントに関連付けられた IP アドレス
- * アクション * - ログイン、作成、更新などのアクティビティのタイプ
- * カテゴリ * - アクティビティのカテゴリ
- * Details * - アクティビティの詳細

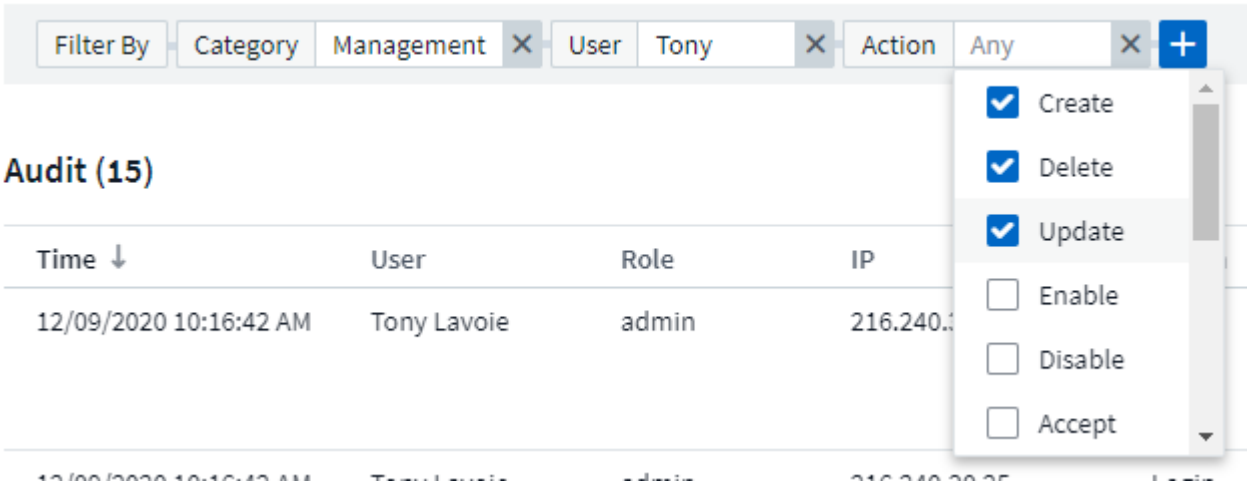
監査エントリの表示

監査エントリを表示する方法はいくつかあります。

- 特定の期間（ 1 時間、 24 時間、 3 日など）を選択することで、監査エントリを表示できます。
- 列見出しで矢印をクリックすると、エントリのソート順序を昇順（上矢印）または降順（下矢印）に変更できます。

  デフォルトでは、エントリが降順に表示されます。

- フィルタフィールドを使用して、テーブルに必要なエントリのみを表示できます。[+] ボタンをクリックして、フィルタを追加します。



フィルタリングの詳細

次のいずれかを使用して、フィルタを絞り込むことができます。

フィルタ	機能	例	結果
* （アスタリスク）	すべての項目を検索できます	ボリューム * RHEL	「 vol 」で始まるリソースをすべて返し、「 rhel 」で終わるリソースをすべて返します。
？（疑問符）	では、特定の数の文字を検索できます	BOS-PRD ？？ -S12	BOS-PRD ***12***-S12 、 BOS-PRD ***23***-S12 などを返します
または	複数のエンティティを指定できます	FAS2240 または CX600 または FAS3270	FAS2440 、 CX600 、または FAS3270 のいずれかを返します
ありません	検索結果からテキストを除外できます	EMC * ではありません	「 EMC 」で始まるものをすべて返します。
_ なし _	選択されているフィールドで空白 / NULL / なしを検索します	_ なし _	ターゲットフィールドが空でない場合に結果を返します

NOT *	_None_above と同様に ' このフォームを使用して _text-only_fields 内の NULL 値を検索することもできます	NOT *	ターゲットフィールドが空でない場合に結果を返します。
""	完全一致を検索します	「 NetApp * 」	完全に一致するリテラル文字列 _netapp * _ を含む結果を返します

フィルタ文字列を二重引用符で囲むと、 Insight では、最初と最後の引用符の間のすべての部分が完全に一致するものとして扱われます。引用符内の特殊文字または演算子は、リテラルとして扱われます。たとえば、「 * 」を指定した場合、リテラルアスタリスクである結果は返されますが、アスタリスクはワイルドカードとして扱われません。演算子 OR および NOT は、二重引用符で囲まれた場合にもリテラル文字列として扱われます。

監査済みイベントとアクション

Data Infrastructure Insightsで監査されるイベントとアクションは、大きく次の領域に分類できます。

- * ユーザーアカウント * ：ログイン、ログアウト、ロール変更など

  例：*User * Tony Lavoie * 10.1.120.15* 、ユーザエージェント *Mozilla/5.0*（*Windows NT 10.0*、*Win64*、*x64*）*AppleWebKit/537.36*（*KHTML*、*Gecko*など）*Chrome/85.0.4183.121 Safari/537.36* 、ログイン方法 *BlueXP Portal Login**

- * Acquisition Unit * ：作成、削除など

  例： _ Acquisition Unit * AU-Boston-1 * removed_.

- * Data Collector * ：追加、削除、変更、延期 / 再開、 Acquisition Unit の変更、 スタート / ストップなど

  例： *Datasource * FlexPod Lab * Removed* 、 *vendor * netapp* * 、 *model * ONTAP Data Management Software* * 、 *IP * 192.168.106.5* * 。

- * アプリケーション *: 追加、オブジェクトへの割り当て、削除など

  例： _ 内部ボリューム * ocisedev ： t1appSVM01 ： t1appFlexVol01 * がアプリケーション * Test App_* に追加されました。

- * アノテーション * ：追加、割り当て、削除、アノテーションルールアクション、アノテーション値の変更、 など

  例： *Annotation Value * Boston * added to annotation type * SalesOffice** 。

- * クエリ * ：追加、削除など

  例： _Query * TL Sales Query * が追加されました _ 。

- * モニター * ：追加、削除など

  例： Monitor_Aggr サイズ -CI アラート通知 Dev_Updated

- * 通知 * ：電子メールの変更など

  例： Recipient_ci -alerts-notifications-dl_created

監査イベントのエクスポート

監査表示の結果を .csv ファイルにエクスポートして、データを分析したり、別のアプリケーションにインポートしたりできます。

手順

1. [監査] ページで、目的の時間範囲と任意のフィルタを設定します。Data Infrastructure Insightsでは、設定したフィルタリングと時間範囲に一致する監査エントリのみがエクスポートされます。
2. [*Export*] ボタンをクリックします ボタン"] をクリックします。

表示される監査イベントは、最大 10 、 000 行までの .csv ファイルにエクスポートされます。

監査データの保持

Data Infrastructure Insightsが監査データを保持する時間は、お客様のエディションによって異なります。

- Basic Edition ：監査データは 30 日間保持されます
- Standard Edition および Premium Editions ：監査データは 1 年と 1 日の間保持されます

保持期限よりも古い監査エントリは自動的にパージされます。ユーザによる操作は不要です。

トラブルシューティング

ここでは、監査に関する問題のトラブルシューティングに関する提案を示します。

* 問題： *	* これを試みなさい : *
モニターがエクスポートされたことを示す監査メッセージが表示されます。	カスタムモニタ構成のエクスポートは、通常、ネットアップのエンジニアが新機能の開発およびテストに使用します。このメッセージが表示されない場合は、監査対象のアクションで指定されたユーザーのアクションを調査するか、サポートに問い合わせてください。

Active IQ

ネットアップ "Active IQ" ハードウェア / ソフトウェアシステム向けに、ネットアップのお客様に一連の視覚化機能、分析機能、サポート関連サービスを提供します。Active IQが報告するデータは、システム問題のトラブルシューティングを強化するとともに、デバイスに関する最適化と予測分析の情報も提供します。

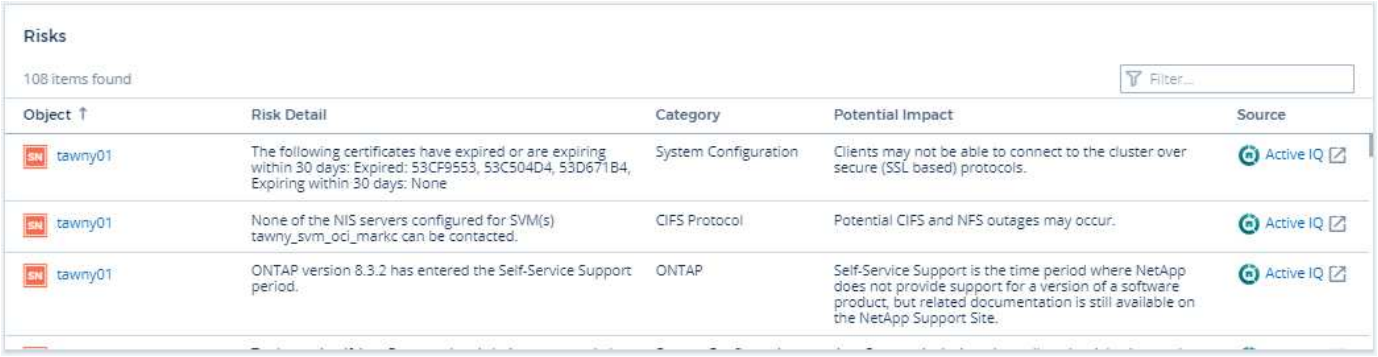
ActiveIQは、Data Infrastructure Insights Federal Editionでは使用できません。

Data Infrastructure Insightsは、Active IQによって監視およびレポートされるすべてのNetApp clustered Data ONTAPストレージシステムについて、*リスク*を収集します。ストレージシステムについて報告されたリスクは、Data Infrastructure Insightsによって、それらのデバイスからのデータ収集の一環として自動的に収集さ

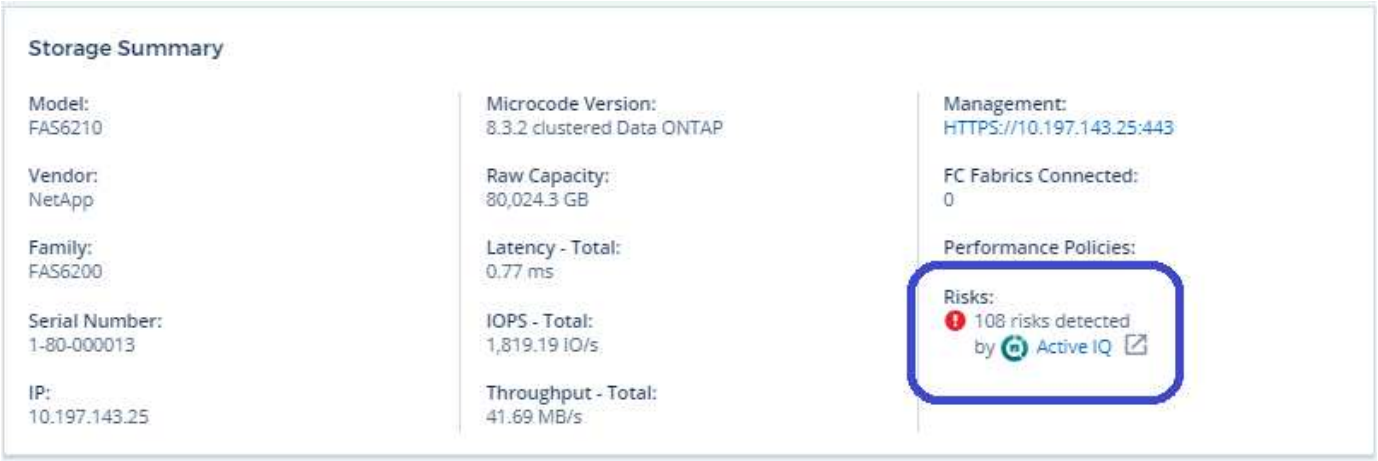
れます。Active IQリスク情報を収集するには、適切なデータコレクタをData Infrastructure Insightsに追加する必要があります。

Data Infrastructure Insightsには、Active IQで監視およびレポートされていないONTAPシステムのリスクデータは表示されません。

レポートされるリスクは、Data Infrastructure Insightsの_storage_and_storage node_assetランディングページの「リスク」の表に表示されます。この表には、リスクの詳細、リスクのカテゴリ、潜在的な影響が表示されます。また、ストレージノードのすべてのリスクをまとめた Active IQ ページへのリンクも表示されます（ネットアップサポートアカウントのサインインが必要です）。



ランディングページの概要ウィジェットにも報告されたリスクの数が表示され、該当する Active IQ ページへのリンクが表示されます。a_storage_landing ページの数は、基盤となるすべてのストレージノードのリスクの合計です。



Active IQ ページを開きます

Active IQ ページへのリンクをクリックして、現在 Active IQ アカウントにサインインしていない場合は、次の手順を実行してストレージノードの Active IQ ページを表示する必要があります。

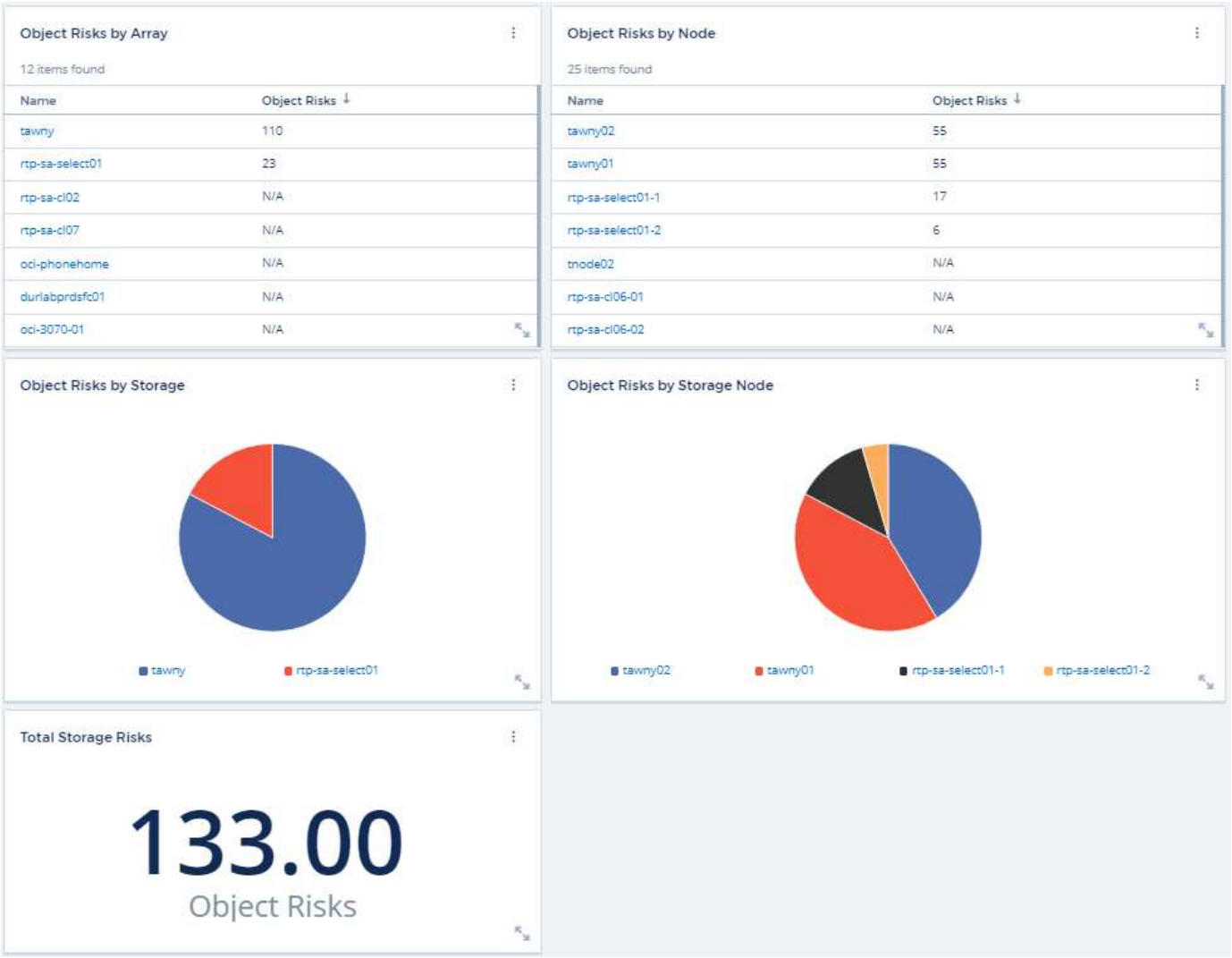
1. [Data Infrastructure Insights Summary]ウィジェットまたは[Risks]テーブルで、Active IQリンクをクリックします。
2. ネットアップサポートアカウントにサインインします。Active IQ のストレージノードのページに直接移動します。

リスクを照会しています

Data Infrastructure Insightsでは、ストレージまたはストレージノードのクエリに* monitoring.count *列を追加できます。返される結果にActive IQ監視対象のストレージシステムが含まれる場合は、monitor.count列にストレージシステムまたはノードのリスク数が表示されます。

ダッシュボード

ウィジェット（円グラフ、表ウィジェット、棒グラフ、列、散布図、 および単一価値ウィジェット）：
Active IQ によって監視される NetApp clustered Data ONTAP システムのストレージノードとストレージノードのオブジェクトリスクを可視化します。これらのウィジェットでは、「オブジェクトリスク」を列または指標として選択できます。各ウィジェットでは、ストレージノードまたはストレージノードがオブジェクトとなります。



ワークロードのセキュリティ

ストレージワークロードのセキュリティについて

データインフラに関するインサイトStorage Workload Security（旧称Cloud Secure）は、内部の脅威に関する実用的な情報に基づいてデータを保護します。ハイブリッドクラウド環境全体にわたるすべての企業データへのアクセスを一元的に可視化および制御できるため、セキュリティとコンプライアンスの目標を確実に達成できます。

Data Infrastructure Insights Federal Editionでは、ワークロードセキュリティは利用できません。

可視性

オンプレミスまたはクラウドに保存されている重要な企業データへのユーザアクセスを一元的に可視化し、制御できます。

データのアクセスと管理をタイムリーかつ正確に可視化できないツールや手動プロセスを置き換えます。ワークロードセキュリティは、クラウドストレージシステムとオンプレミスストレージシステムの両方で独自に動作し、悪意のあるユーザの行動をリアルタイムで警告します。

保護

高度な機械学習と異常検出機能により、悪意のあるユーザや悪意のあるユーザによる組織データの不正使用を防止します。

高度な機械学習とユーザの動作に関する異常検出によって、異常なデータアクセスをユーザに警告します。

コンプライアンス

オンプレミスまたはクラウドに保存されている重要な企業データへのユーザデータアクセスを監査することで、企業のコンプライアンスを確保します。

はじめに

ワークロードセキュリティの導入

Workload Securityを使用してユーザアクティビティを監視する前に、設定タスクを完了する必要があります。

ワークロードセキュリティシステムは、エージェントを使用して、ストレージシステムからアクセスデータとディレクトリサービスサーバからユーザ情報を収集します。

データの収集を開始する前に、次の項目を設定する必要があります。

タスク	関連情報

エージェントを設定します	"エージェントの要件" "エージェントを追加します" "* ビデオ * ：エージェントの配備"
ユーザディレクトリコネクタを設定します	"ユーザーディレクトリコネクターを追加します" "* ビデオ * ： Active Directory 接続"
データコレクタを設定する	[ワークロードセキュリティ]>[コレクタ]をクリックします。 設定するデータコレクタをクリックします。 ドキュメントの **Data Collector Vendor Reference** セクションを参照してください。 " ビデオ * ： **ONTAP SVM** 接続"
ユーザーアカウントを作成します	"ユーザアカウントを管理する"
トラブルシューティング	"* ビデオ * ：トラブルシューティング"

ワークロードセキュリティは、他のツールとも統合できます。 例： "このガイドを参照してください" Splunk と統合し、

ワークロードセキュリティエージェントの要件

実行する必要があります "エージェントをインストールします" データコレクタから情報を取得します。Agent をインストールする前に、お使いの環境がオペレーティングシステム、 CPU 、メモリ、およびディスクスペースの要件を満たしていることを確認してください。

コンポーネント	**Linux** 要件
オペレーティングシステム	次のいずれかのライセンスバージョンを実行しているコンピュータ。* CentOS 8 Stream（64ビット）、SELinux * openSUSE LEAP 15.3～15.5（64ビット）* Oracle Linux 8.6-8.8、9.1～9.2（64ビット）* Red Hat Enterprise Linux 8.6～8.8、9.1～9.2（64ビット）、SELinux * Rocky 9.2（64ビット）、SELinux * SUSE Linux Enterprise Server 15 SP3～15 SP3（64ビット）* Ubuntu 20.04 LTSおよび22.04 LTS（64ビット）このコンピューターでは、他のアプリケーションレベルのソフトウェアを実行しないでください。専用のサーバを使用することを推奨します。
コマンド	インストールには「unzip」が必要です。また、インストール、スクリプトの実行、およびアンインストールには、「sudo su–」コマンドが必要です。
CPU	4 個の CPU コア
メモリ	16GB の RAM

コンポーネント	**Linux** 要件
使用可能なディスクスペース	ディスクスペースは次の方法で割り当てる必要があります。 /opt/netapp 36 GB（ファイルシステム作成後に35 GB以上の空きスペース） 注:ファイルシステムを作成できるように、少し余分なディスク領域を割り当てることをお勧めします。ファイルシステムに35GB以上の空きスペースがあることを確認します。 /optがNASストレージからマウントされたフォルダである場合は、ローカルユーザーがこのフォルダにアクセスできることを確認してください。ローカルユーザにこのフォルダへのアクセス権がない場合、エージェントまたはデータコレクタのインストールが失敗する可能性があります。を参照してください "トラブルシューティング" 詳細については、を参照してください。
ネットワーク	100 Mbps~1 Gbpsイーサネット接続、静的IPアドレス、すべてのデバイスへのIP接続、およびワークロードセキュリティインスタンスへの必要なポート（80または443）

注：ワークロードセキュリティエージェントは、Data Infrastructure Insights Acquisition Unitやエージェントと同じマシンにインストールできます。ただし、これらを別々のマシンにインストールすることを推奨します。これらが同じマシンにインストールされている場合は、次のようにディスク領域を割り当ててください。

使用可能なディスクスペース	50～55 GB Linuxの場合は、次の方法でディスクスペースを割り当てる必要があります。 /opt/ネットアップ25~30GB /var/log/netapp 25GB

その他の推奨事項

- ONTAP システムとエージェントマシンの両方の時刻を、 *Network Time Protocol （ NTP; ネットワークタイムプロトコル） * または *Simple Network Time Protocol （ SNTP ） * を使用して同期することを強くお勧めします。

Cloud Network Access Rules の略

USベースの*ワークロード・セキュリティー環境の場合：

プロトコル	ポート	ソース	宛先	説明
TCP	443年	ワークロードセキュリティエージェント	<site_name>.cs01.cloudinsights.netapp.com <site_name>.c01.cloudinsights.netapp.com <site_name>.c02.cloudinsights.netapp.com	データインフラの分析情報へのアクセス

プロトコル	ポート	ソース	宛先	説明
TCP	443年	ワークロードセキュリティエージェント	gateway.c01.cloudinsights.netapp.com agentlogin.cs01.cloudinsights.netapp.com	認証サービスへのアクセス

欧州*ベースのワークロード・セキュリティー環境の場合：

プロトコル	ポート	ソース	宛先	説明
TCP	443年	ワークロードセキュリティエージェント	<site_name>.cs01-eu-1.cloudinsights.netapp.com <site_name>.c01-eu-1.cloudinsights.netapp.com <site_name>.c02-eu-1.cloudinsights.netapp.com	データインフラの分析情報へのアクセス
TCP	443年	ワークロードセキュリティエージェント	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-eu-1.cloudinsights.netapp.com	認証サービスへのアクセス

APACベースの*ワークロード・セキュリティ環境の場合：

プロトコル	ポート	ソース	宛先	説明
TCP	443年	ワークロードセキュリティエージェント	<site_name>.cs01-ap-1.cloudinsights.netapp.com <site_name>.c01-ap-1.cloudinsights.netapp.com <site_name>.c02-ap-1.cloudinsights.netapp.com	データインフラの分析情報へのアクセス
TCP	443年	ワークロードセキュリティエージェント	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-ap-1.cloudinsights.netapp.com	認証サービスへのアクセス

ネットワーク内ルール

プロトコル	ポート	ソース	宛先	説明
TCP	389（LDAP） 636（LDAPS / START-TLS）	ワークロードセキュリティエージェント	LDAP サーバ URL	LDAP に接続します
TCP	443年	ワークロードセキュリティエージェント	クラスタまたはSVMの管理IPアドレス（SVMコレクタの設定に応じて）	ONTAP との API 通信
TCP	35000~55000	SVM データ LIF の IP アドレス	ワークロードセキュリティエージェント	FPolicyイベントのONTAPからワークロードセキュリティエージェントへの通信。ONTAPがイベントをワークロードセキュリティエージェントに送信するには、これらのポートをワークロードセキュリティエージェントに対して開いておく必要があります。これには、ワークロードセキュリティエージェント自体のファイアウォールも含まれます（存在する場合）。これらのポートをすべて予約する必要はありませんが、予約するポートはこの範囲内である必要があります。最初に最大100個のポートを予約し、必要に応じて増やすことをお勧めします。
TCP	7.	ワークロードセキュリティエージェント	SVM データ LIF の IP アドレス	エージェントからSVMのデータLIFへのエコー
SSH	22.	ワークロードセキュリティエージェント	クラスタ管理	CIFS / SMBユーザブロックに必要です。

システムのサイジング

を参照してください "イベントレートチェッカー" サイジングに関する情報のドキュメント

ワークロードセキュリティエージェントのインストール

ワークロードセキュリティ（旧Cloud Secure ）は、1つ以上のエージェントを使用してユーザアクティビティデータを収集します。エージェントは環境内のデバイスに接続し、分析のためにワークロードセキュリティSaaSレイヤに送信されるデータを収集します。を参照してください "エージェントの要件" エージェント VM を設定します。

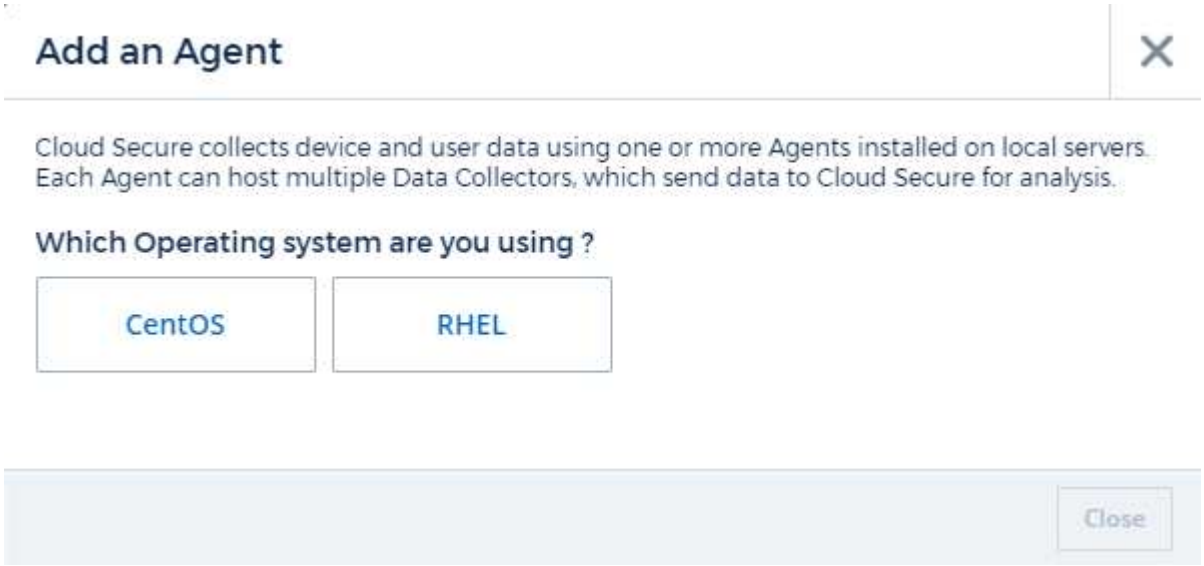
作業を開始する前に

- インストール、スクリプトの実行、アンインストールには sudo 権限が必要です。
- エージェントのインストール中に、ローカルのuser_cssys_とローカルのgroup_cssys_がマシン上に作成されます。権限設定でローカルユーザの作成が許可されておらず、Active Directoryが必要な場合は、Active Directoryサーバにusername_csys_という名前のユーザを作成する必要があります。
- Data Infrastructure Insightsのセキュリティについては"こちらをご覧ください"、こちらをご覧ください。

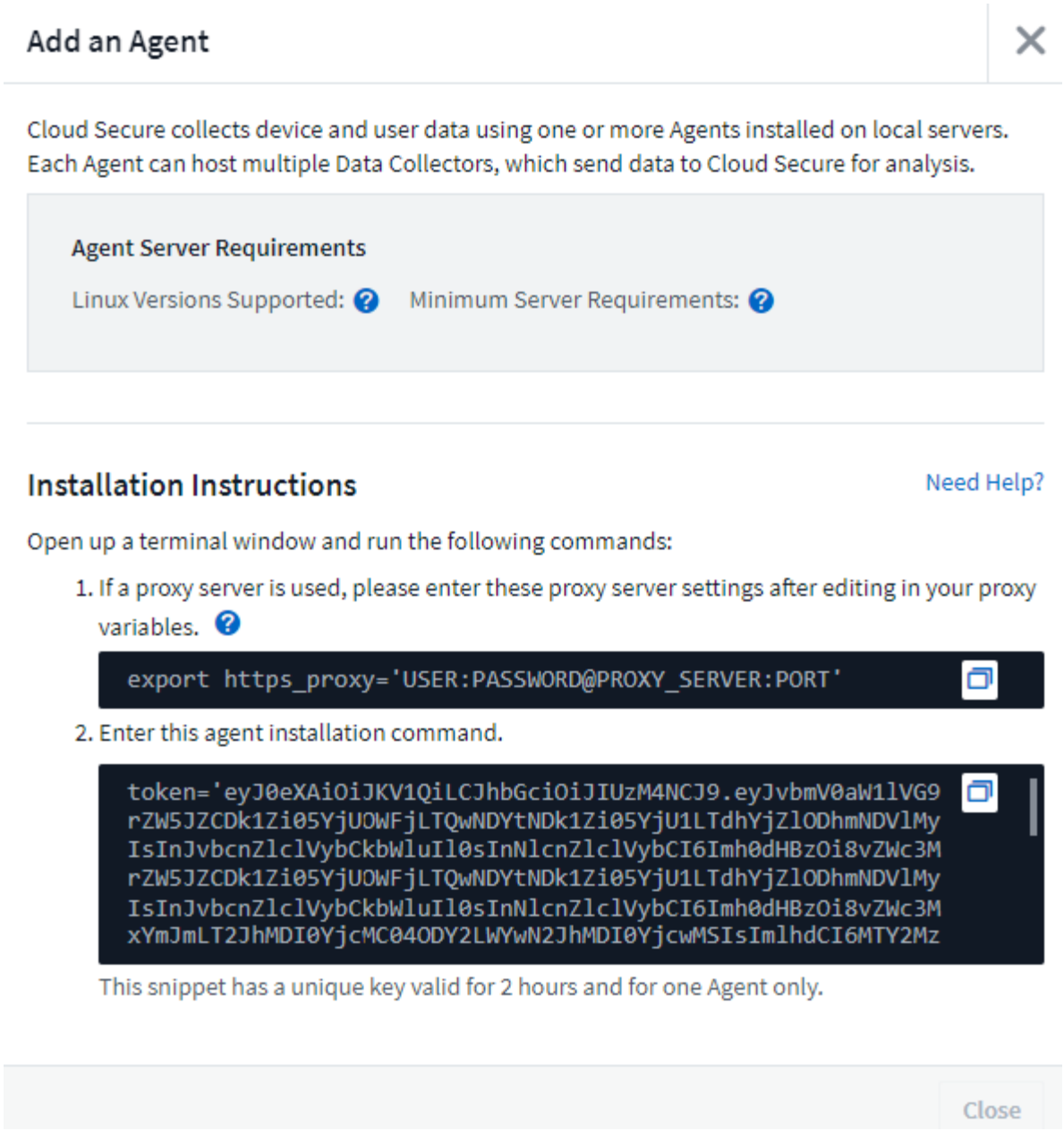
エージェントをインストールする手順

1. ワークロードセキュリティ環境に管理者またはアカウント所有者としてログインします。
2. [Collectors]>[Agents]>[+Agent]を選択します。

   [エージェントの追加] ページが表示されます。



3. エージェントサーバが最小システム要件を満たしていることを確認します。
4. エージェントサーバでサポートされているバージョンの Linux が実行されていることを確認するには、 _ サポートされているバージョン（ i ） _ をクリックします。
5. ネットワークでプロキシサーバを使用している場合は、プロキシセクションの指示に従ってプロキシサーバの詳細を設定してください。



6. [クリップボードにコピー] アイコンをクリックして、インストールコマンドをコピーします。
7. ターミナルウィンドウでインストールコマンドを実行します。
8. インストールが正常に完了すると、次のメッセージが表示されます。

完了後

1. を設定する必要があります "User Directory Collector の略 "。
2. 1 つ以上のデータコレクタを設定する必要があります。

ネットワーク構成：

ローカルシステムで次のコマンドを実行して、ワークロードセキュリティで使用されるポートを開きます。ポート範囲に関するセキュリティ上の問題がある場合は、 *35000 ： 35100* のように小さいポート範囲を使用できます。各 SVM は 2 つのポートを使用します。

手順

1. `sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp`
2. `sudo firewall-cmd --reload`

プラットフォームに応じて、次の手順を実行します。

- CentOS 7.x/RHEL 7.x * ：
  1. `sudo iptables-save | grep 35000`

出力例：

```
 -A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack
-ctstate NEW,UNTRACKED -j ACCEPT
* CentOS 8.x / RHEL 8.x * ：
```

1. `sudo firewall-cmd --zone=public --list-ports | grep 35000` （CentOS 8の場合）

出力例：

```
35000-55000/tcp
```

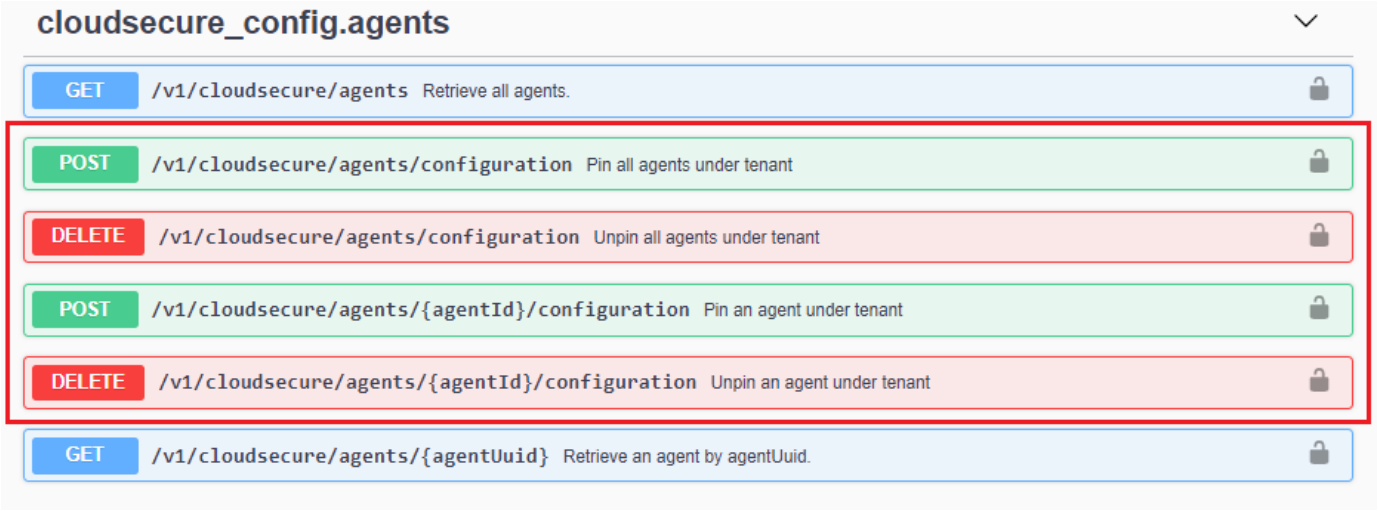
現在のバージョンでエージェントを「固定」する

デフォルトでは、Data Infrastructure Insights Workload Securityはエージェントを自動的に更新します。お客様によっては、自動更新を一時停止したい場合があります。これにより、次のいずれかが発生するまで、Agentは現在のバージョンのままになります。

- カスタマーはエージェントの自動更新を再開します。
- 30日が過ぎました。30日間は、エージェントが一時停止された日ではなく、最新のエージェント更新の日に開始されます。

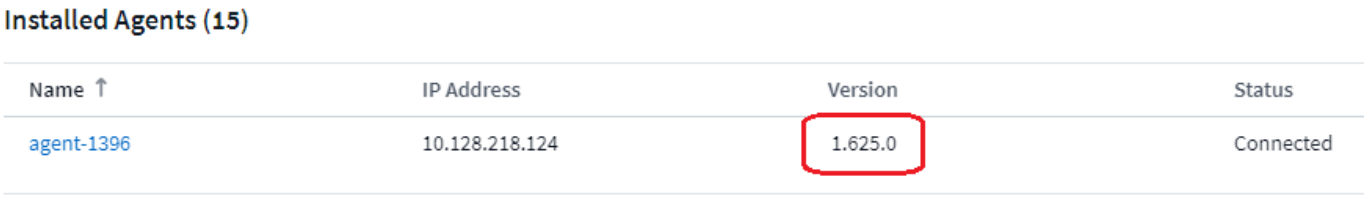
これらのいずれの場合も、エージェントは次回のワークロードセキュリティ更新時に更新されます。

エージェントの自動更新を一時停止または再開するには、_cloudsecure_config.agents_APIを使用します。



一時停止または再開のアクションが有効になるまで、最大5分かかることがあります。

現在のエージェントのバージョンは、*ワークロードセキュリティ>コレクタ*ページの*エージェント*タブで確認できます。



エージェントエラーのトラブルシューティング

既知の問題とその解決策を次の表に示します。

問題	解決策：
エージェントのインストール時に /opt/NetApp/cloudsecure/agent/logs/agent.log フォルダが作成されず、 install.log ファイルに関連情報が記録されません。	このエラーは、エージェントのブートストラップ中に発生します。ロガーが初期化される前に発生するため、エラーはログファイルに記録されません。エラーは標準出力にリダイレクトされ、 `journalctl -u cloudsecure-agent.service`コマンドを使用してサービスログに表示されます。このコマンドは、問題の詳細なトラブルシューティングに使用できます。est
「この Linux ディストリビューションはサポートされていません。インストールを終了しています。	このエラーは、サポートされていないシステムにAgentをインストールしようとしたときに表示されます。を参照してください "エージェントの要件"。
エージェントのインストールが次のエラーで失敗しました： "-bash：unzip：コマンドが見つかりません"	unzip をインストールし、インストールコマンドを再度実行します。Yum がマシンにインストールされている場合は、「 yum install unzip 」を実行して解凍ソフトウェアをインストールしてください。 その後、 Agent インストール UI からコマンドをコピーして CLI に貼り付け、再度インストールを実行します。

問題	解決策：
エージェントがインストールされ、実行されていました。しかし、エージェントは突然停止しました。	Agent マシンに SSH 接続します。を使用して、エージェントサービスのステータスを確認します `sudo systemctl status cloudsecure-agent.service`。 1.ログに「Failed to start Workload Security daemon service」というメッセージが表示されるかどうかを確認します。 2. cssys ユーザが Agent マシンに存在するかどうかを確認します。次のコマンドを root 権限で 1 つずつ実行し、 cssys ユーザとグループが存在するかどうかを確認します。 `sudo id cssys` `sudo groups cssys` 3.何も存在しない場合は、中央集中型の監視ポリシーによってcssysユーザが削除されている可能性があります。 4. 次のコマンドを実行して、 cssys のユーザとグループを手動で作成します。 `sudo useradd cssys` `sudo groupadd cssys` 5.次のコマンドを実行して、エージェントサービスを再起動します。 `sudo systemctl restart cloudsecure-agent.service` 6.まだ実行されていない場合は、他のトラブルシューティングオプションを確認してください。
エージェントには50個を超えるデータコレクタを追加できません。	エージェントに追加できるデータコレクタは 50 個までです。Active Directory 、 SVM 、その他のコレクタなど、すべてのコレクタタイプを組み合わせて使用できます。
Agent is in not_connected 状態であることが UI に表示されます。	エージェントを再起動する手順。 1. エージェントマシンに SSH 接続します。 2.その後、次のコマンドを実行してエージェントサービスを再起動します。 `sudo systemctl restart cloudsecure-agent.service` 3.からエージェントサービスのステータスを確認します `sudo systemctl status cloudsecure-agent.service`。 4. エージェントは接続状態になります。
エージェント VM が Zscaler プロキシの背後にあり、エージェントのインストールに失敗しています。ZscalerプロキシのSSL検査により、ワークロードセキュリティ証明書はZscaler CAによって署名されたため、エージェントが通信を信頼していないと表示されます。	*.cloudinsights.netapp.com URL の Zscaler プロキシで SSL 検査をディセーブルにします。ZscalerがSSLを検査して証明書を置き換えた場合、Workload Securityは機能しません。

問題	解決策：
エージェントのインストール中に、解凍後にインストールがハングします。	「 chmod 755 -rf 」コマンドが失敗しています。 このコマンドは、別のユーザに属する作業ディレクトリ内のファイルを含む root 以外の sudo ユーザがエージェントのインストールコマンドを実行している場合は失敗し、それらのファイルの権限を変更することはできません。失敗した chmod コマンドのため、残りのインストールは実行されません。 1.「cloudsecure」という名前の新しいディレクトリを作成します。 2.そのディレクトリに移動します。 3.完全な「トークン=……」をコピーして貼り付けます。 … ./cloudsecure-agent-install.sh "インストールコマンドを入力し、Enterキーを押します。 4.インストールを続行できるはずです。
エージェントがまだ SaaS に接続できない場合は、ネットアップサポートでケースをオープンしてください。Data Infrastructure Insightsのシリアル番号を提供してケースをオープンし、記録したとおりにログをケースに添付します。	ログをケースに添付するには、次の手順に従います。 1. root権限で以下のスクリプトを実行し、出力ファイル(cloudsecure-agent-symptions.zip)を共有します。 A /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 以下のコマンドをroot権限で1つずつ実行し、出力を共有します。 A ID csys B グループcsys c. Cat /etc/os-release
cloudsecure-agent-symptom-collector.shスクリプトが次のエラーで失敗します。 [root@machine tmp]#/opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh サービスログを収集しています アプリケーションログを収集しています エージェント設定を収集しています サービスステータスのスナップショットを取得しています エージェントディレクトリ構造のスナップショットを取得しています …… 。 …… 。 /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh行52:zip:コマンドが見つかりません エラー：/tmp/ cloudsecure-agent-symptoms.zipを作成できませんでした	ZIPツールがインストールされていません。 コマンド「yum install zip」を実行してzipツールをインストールします。 次に、cloudsecure-agent-symptom-collector.shを再度実行します。

問題	解決策：
エージェントのインストールに失敗し、useradd：Cannot create directory/home/cssysというメッセージが表示されます	このエラーは、権限がないためにユーザのログインディレクトリを/homeの下に作成できない場合に発生することがあります。 回避策では、次のコマンドを使用してcsysユーザを作成し、ログインディレクトリを手動で追加します。 *sudo useradd user_name -m -d home_DIR* -m：ユーザのホームディレクトリが存在しない場合は作成します。 -d：新しいユーザは'ユーザのログイン・ディレクトリの値としてhome_DIRを使用して作成されます たとえば、_sudo useradd cssys-m-d/cssys_ はuser_cssys_を追加し、rootの下にそのログインディレクトリを作成します。
エージェントはインストール後に実行されていません。 _systemctl status cloudsecure-agent.service_には、次の情報が表示されます。 [root@demo ~]# systemctl status cloudsecure-agent.service agent.service–Workload Security Agent Daemon Service（ワークロードセキュリティエージェントデーモンサービス） loaded: loaded(/usr/lib/systemd/system/cloudsecure-agent.service;有効;ベンダープリセット:無効) アクティブ:アクティブ化(自動再起動)(結果:終了コード) Since Tue 2021-08-03 21:12:26 PDT;2 s ago プロセス：25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent（code=exited status=126） メインPID：25889（コード=終了、ステータス= 126）、 Aug 03 21:12:26 demo systemd[1]：cloudsecure-agent.service: main process exited、code=exited、status=126/n/a Aug 03 21:12:26 demo systemd[1]：Unit cloudsecure-agent.service entered failed state. 8月03日21：12：26デモシステムd[1]：cloudsecure-agent.serviceが失敗しました。	これは'_cssys_userにインストール権限がないために失敗することがあります /opt/netappがNFSマウントで、_cssys_userがこのフォルダにアクセスできない場合、インストールは失敗します。_cssys_は、マウントされた共有にアクセスする権限がない可能性があるワークロードセキュリティインストーラによって作成されたローカルユーザです。 これを確認するには、_cssys_userを使用して/opt/netapp/cloudsecure/agent/bin/cloudsecure-agentにアクセスします。 「Permission denied」が返された場合、インストール許可は表示されません。 マウントされたフォルダではなく、マシンのローカルディレクトリにインストールします。

問題	解決策：
エージェントは最初にプロキシサーバを介して接続され、エージェントのインストール時にプロキシが設定されました。これでプロキシサーバが変更されました。エージェントのプロキシ設定はどのように変更できますか。	agent.propertiesを編集して、プロキシの詳細を追加できます。次の手順を実行します。 1.プロパティファイルを含むフォルダに変更します。 CD /opt/netapp/cloudsecure/conf 2.お気に入りのテキストエディタを使用して、_agent.properties_ファイルを開いて編集します。 3.次の行を追加または変更します。 agent_proxy_host = scspa1950329001.vm.netapp.com AGENT_PROXY_PORT = 80 agent_proxy_user = pxuser AGENT_PROXY_PASSWORD = pass1234 4.ファイルを保存します。 5.エージェントを再起動します。 sudo systemctl restart cloudsecure-agent.service

ワークロードセキュリティエージェントの削除

ワークロードセキュリティエージェントを削除する場合は、そのエージェントに関連付けられているすべてのデータコレクタを先に削除する必要があります。

エージェントの削除

エージェントを削除すると、そのエージェントに関連付けられているすべてのデータコレクタが削除されます。別のエージェントでデータコレクタを設定する場合は、 Agent を削除する前に、 Data Collector 設定のバックアップを作成する必要があります。

作業を開始する前に

1. ワークロードセキュリティポータルから、エージェントに関連付けられているすべてのデータコレクタが削除されていることを確認します。

   注：関連するすべてのコレクタが停止状態にある場合は、この手順を無視してください。

エージェントを削除する手順：

1. エージェント VM に SSH 接続し、次のコマンドを実行します。プロンプトが表示されたら、「 y 」と入力して続行します。

```
sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
uninstall.sh
Uninstall CloudSecure Agent? [y|N]:
```

2. [Workload Security]>[Collectors]>[Agents]*をクリックします。

   設定されたエージェントのリストが表示されます。

3. 削除するエージェントのオプションメニューをクリックします。
4. [削除（ Delete ）] をクリックします。

   [エージェントの削除 *] ページが表示されます。

5. 削除を確認するには、 * Delete * をクリックします。

Active Directory （ AD ）ユーザディレクトリコレクタの設定

ワークロードセキュリティは、Active Directoryサーバからユーザ属性を収集するように設定できます。

作業を開始する前に

- このタスクを実行するには、Data Infrastructure Insightsの管理者またはアカウント所有者である必要があります。
- Active Directory サーバをホストしているサーバの IP アドレスを確認しておく必要があります。
- ユーザディレクトリコネクタを設定する前に、エージェントを設定する必要があります。

ユーザーディレクトリコレクタの設定手順

1. [Workload Security]メニューで、次のいずれかをクリックします。
   [Collectors]>[User Directory Collector]>[+ User Directory Collector]*を選択し、[Active Directory]*を選択します。

   [Add User Directory] 画面が表示されます。

次の表に必要なデータを入力して、 User Directory Collector を設定します。

名前	説明
名前	ユーザディレクトリの一意の名前。例： *GlobalADCollector*
エージェント	リストから設定済みエージェントを選択します
サーバの IP / ドメイン名	Active Directory をホストしているサーバの IP アドレスまたは完全修飾ドメイン名（ FQDN ）

フォレスト名	ディレクトリ構造のフォレストレベル。 フォレスト名では、次の両方の形式を使用できます。 *x.y.z*⇒ドメイン名をSVMと同じように直接指定します。[例：hq.companyname.com] *dc=x*、*dc=y*、*dc=z*⇒相対識別名[例：dc=hq 、dc=companyname、dc=com] または、次のように指定できます。 *OU=engineering*、*DC=hq*、*DC=companyname*、*DC=com*[特定のOU engineeringでフィルタする] *CN=username*、*OU=engineering*、*DC=companyname*、*DC=netapp*、*DC=com*[OU <engineering>から<username>を使用して特定のユーザだけを取得する場合] *CN=Acrobat*ユーザー、*CN=Users*、*DC=HQ* 、*DC=companyname*、*DC=com*、*O=companyname* 、*L=Boston*、*S=MA*、*C=US*[その組織のユーザー内のすべてのAcrobatユーザーを取得するには] 信頼されたActive Directoryドメインもサポートされます。
バインド DN	ディレクトリの検索が許可されています。たとえば、*username@companyname.com* や *username@domainname.com* などです また、Domain Read Only権限が必要です。 ユーザは、セキュリティグループ_Read-Only Domain Controllers_のメンバーである必要があります。
バインドパスワード	ディレクトリサーバのパスワード（バインド DN で使用されるユーザ名のパスワード）
プロトコル	LDAP 、 ldaps 、 ldap-start-TLS
ポート	ポートを選択します

Active Directory でデフォルトの属性名が変更されている場合は ' 次の Directory Server 必須属性を入力しますほとんどの場合、これらの属性名は Active Directory で _not_modified となります。この場合、デフォルトの属性名をそのまま使用できます。

属性（ Attributes ）	ディレクトリサーバの属性名
表示名	名前
SID	objectSID を指定します
ユーザ名	sAMAccountName

次の属性を追加するには、オプション属性を含めるをクリックします。

属性（ Attributes ）	ディレクトリサーバの属性名

E メールアドレス	メール
電話番号	電話番号
ロール	タイトル
国名	共同
状態	状態
部門	部門
写真	サムネイル写真
ManagerDN	マネージャー
グループ	所属グループ

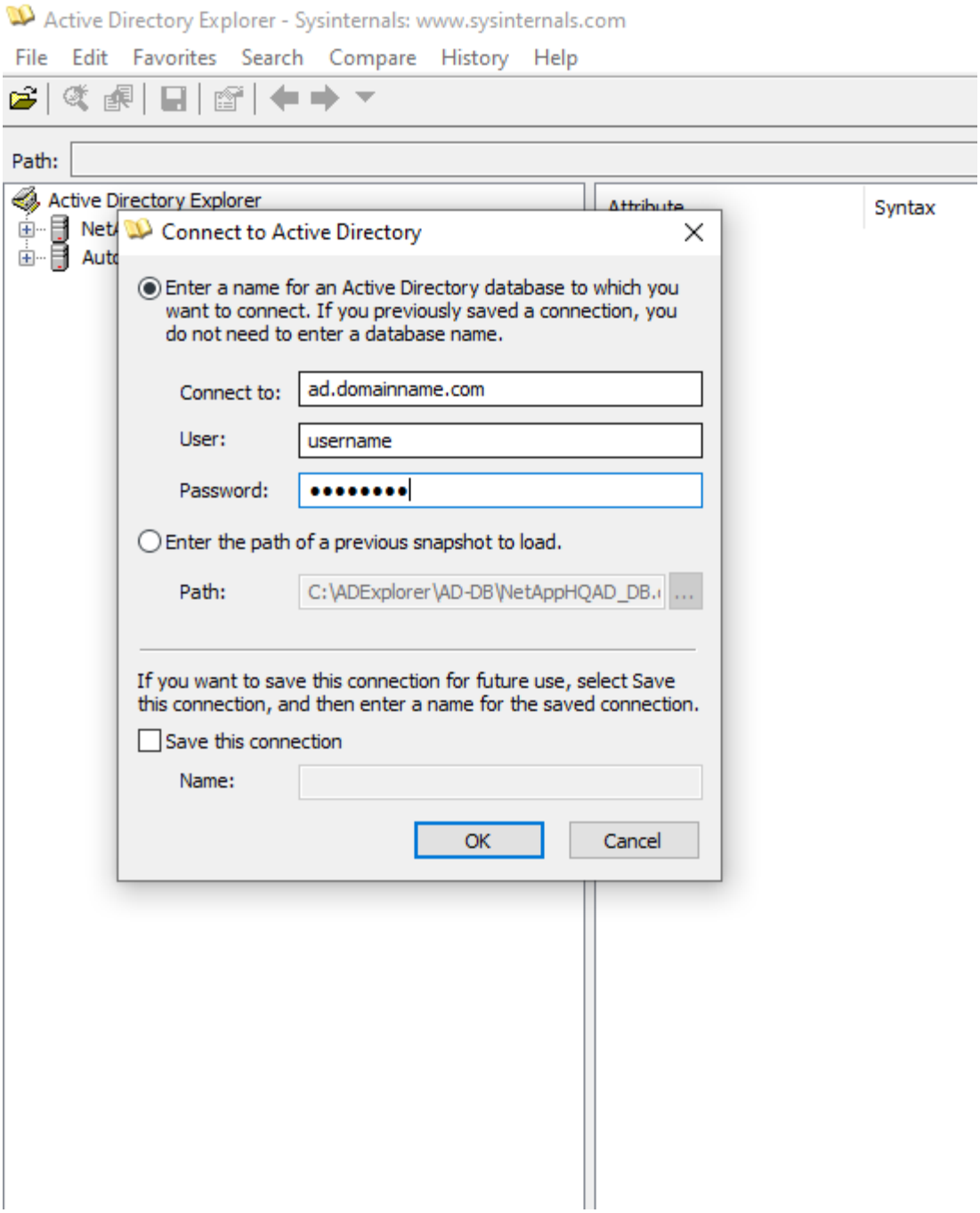
ユーザディレクトリコレクタ設定のテスト

LDAP ユーザ権限および属性定義は、次の手順で検証できます。

- 次のコマンドを使用して、ワークロードセキュリティのLDAPユーザ権限を検証します。

```
ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p
389 -D Administrator@netapp.com -W
```

- AD Explorer を使用して、 AD データベースのナビゲート、オブジェクトのプロパティと属性の表示、権限の表示、オブジェクトのスキーマの表示、高度な検索の実行を行い、保存して再実行することができます。
  - をインストールします "AD エクスプローラ" AD サーバに接続できる任意の Windows マシン。
  - AD ディレクトリサーバのユーザ名とパスワードを使用して AD サーバに接続します。



ユーザディレクトリコレクタ設定エラーのトラブルシューティング

次の表に、コレクタの設定時に発生する可能性のある既知の問題と解決策を示します。

問題	解決策：
ユーザディレクトリコネクタを追加すると、「エラー」状態になります。「 Invalid credentials provided for LDAP server 」 (LDAP サーバーの資格情報が無効です) というエラーが表示されます	入力したユーザ名またはパスワードが正しくありません。を編集し、正しいユーザ名とパスワードを入力します。

問題	解決策：
ユーザディレクトリコネクタを追加すると、「エラー」状態になります。「 DN=DC=HQ,DC=domainname,DC=com に対応するオブジェクトをフォレスト名として提供できませんでした」というエラーが表示されます。	指定したフォレスト名が正しくありません。正しいフォレスト名を編集して入力します。
ドメインユーザーのオプションの属性は、[ワークロードセキュリティユーザープロファイル]ページに表示されません。	これは、 CloudSecure で追加されたオプション属性の名前と Active Directory の実際の属性名が一致しないことが原因である可能性があります。正しいオプションの属性名を編集して入力します。
データコレクタでエラーが発生し、「 LDAP ユーザを取得できませんでした。失敗の理由：サーバに接続できません。接続が null です "	_Restart_Button をクリックして、コレクタを再起動します。
ユーザディレクトリコネクタを追加すると、「エラー」状態になります。	必須フィールドに有効な値（ Server 、 forest-name 、 bind-dn 、 bind-Password ）が指定されていることを確認してください。 bind-DN 入力が常に「 Administrator@<domain_forest_name> 」またはドメイン管理者権限を持つユーザーアカウントとして提供されていることを確認してください。
ユーザディレクトリコネクタを追加すると、「再試行中」の状態になります。「 Unable to define state of the collector 、 reason TCP command [Connect (localhost:35012, None, List() 、 some (,seconds),true)] failed because of java.net.ConnectionException:Connection refused 」というエラーが表示されます。	AD サーバに指定された IP または FQDN が正しくありません。を編集し、正しい IP アドレスまたは FQDN を指定します。
ユーザディレクトリコネクタを追加すると、「エラー」状態になります。「 LDAP 接続の確立に失敗しました」というエラーが表示されます。	AD サーバに指定された IP または FQDN が正しくありません。を編集し、正しい IP アドレスまたは FQDN を指定します。
ユーザディレクトリコネクタを追加すると、「エラー」状態になります。「設定をロードできませんでした。理由：データソースの設定でエラーが発生しました。具体的な理由： /connector/conf/application.conf ： 70 ： ldap.ldap-port には number ではなく string 型があります。	指定したポートの値が正しくありません。デフォルトのポート値または AD サーバの正しいポート番号を使用してみてください。
必須属性から始めて、機能しました。オプションの属性を追加した後、オプションの属性データは AD から取得されません。	これは、 CloudSecure で追加されたオプションの属性と Active Directory の実際の属性名が一致しないことが原因である可能性があります。正しい必須またはオプションの属性名を編集して入力します。
コレクタの再起動後、 AD 同期はいつ行われますか？	コレクタの再起動後すぐに AD 同期が行われます。約 15 分で約 30 万人のユーザデータが取得され、 12 時間ごとに自動的に更新されます。
ユーザーデータは、 AD から CloudSecure に同期されます。データを削除するタイミング	更新がない場合、ユーザデータは 13 カ月間保持されます。テナントが削除されると、データは削除されます。

問題	解決策：
ユーザーディレクトリコネクタが「エラー」状態になります。" コネクタでエラーが発生しました。サービス名： usersLDAP 。失敗の理由： LDAP ユーザを取得できませんでした。失敗の理由： 80090308 ： LdapErr: DSID-0C090453 、 comment: AcceptSecurityContext error 、 data 52e 、 v3839	指定したフォレスト名が正しくありません。正しいフォレスト名を指定する方法については、上記を参照してください。
電話番号がユーザプロファイルページに入力されていません。	これは、多くの場合、 Active Directory の属性マッピングの問題が原因です。 1. Active Directory からユーザの情報を取得している特定の Active Directory コレクタを編集します。 2. オプション属性の下に、 Active Directory 属性「 telephonenumber 」にマッピングされたフィールド名「 Telephone Number 」があることに注意してください。 4. ここでは、前述の Active Directory エクスプローラツールを使用して、 Active Directory を参照し、正しい属性名を確認してください。 3. Active Directory に、実際にユーザの電話番号を持つ「 telephonenumber 」という名前の属性があることを確認します。 5. ここでは、 Active Directory で「 phonenumber 」に変更されたとします。 6. CloudSecure User Directory コレクタを編集します。オプションの属性セクションで、「 telephonenumber 」を「 phonenumber 」に置き換えます。 7. Active Directory コレクタを保存すると、コレクタが再起動してユーザの電話番号が取得され、ユーザプロファイルページにも同じ番号が表示されます。
Active Directory（AD）サーバで暗号化証明書（SSL）が有効になっている場合、Workload Security User Directory CollectorはADサーバに接続できません。	ユーザーディレクトリコレクタを設定する前に、 AD サーバーの暗号化を無効にします。 ユーザの詳細情報が取得されてから 13 カ月間表示されます。 ユーザーの詳細を取得した後に AD サーバーが切断された場合、新しく追加された AD 内のユーザーは取得されません。再度取得するには、ユーザディレクトリコレクタをADに接続する必要があります。
Active DirectoryのデータはCloudInsightsのセキュリティに存在します。 CloudInsightsからすべてのユーザ情報を削除する必要がある。	CloudInsights SecurityからActive Directoryユーザー情報のみを削除することはできません。ユーザを削除するには、テナント全体を削除する必要があります。

LDAP Directory Server Collector の設定

ワークロードセキュリティを設定して、LDAPディレクトリサーバからユーザ属性を収集します。

作業を開始する前に

- このタスクを実行するには、Data Infrastructure Insightsの管理者またはアカウント所有者である必要があります。
- LDAP ディレクトリサーバをホストしているサーバの IP アドレスを確認しておく必要があります。
- LDAP ディレクトリコネクタを設定する前に、エージェントを設定する必要があります。

ユーザーディレクトリコレクタの設定手順

1. [Workload Security]メニューで、次のいずれかをクリックします。
   [Collectors]>[User Directory Collector]>[+ User Directory Collector]*を選択し、[LDAP Directory Server]*を選択します。

   [Add User Directory] 画面が表示されます。

次の表に必要なデータを入力して、 User Directory Collector を設定します。

名前	説明
名前	ユーザディレクトリの一意の名前。たとえば、「 *GlobalLDAPCollector* 」と入力します
エージェント	リストから設定済みエージェントを選択します
サーバの IP / ドメイン名	LDAP ディレクトリサーバをホストするサーバの IP アドレスまたは完全修飾ドメイン名（ FQDN ）
ベース検索	LDAPサーバの検索ベース 検索ベースでは、次の両方の形式を使用できます。 *x.y.z*⇒ドメイン名をSVMと同じように直接指定します。[例：hq.companyname.com] *dc=x*、*dc=y*、*dc=z*⇒相対識別名[例：dc=hq、dc=companyname、dc=com] または、次のように指定できます。 *OU=engineering*、*DC=hq*、*DC=companyname*、*DC=com*[特定のOU engineeringでフィルタする] *CN=username*、*OU=engineering*、*DC=companyname*、*DC=netapp*、*DC=com*[OU <engineering>から<username>を使用して特定のユーザだけを取得する場合] *CN=Acrobat*ユーザー、*CN=Users*、*DC=HQ*、*DC=companyname*、*DC=com*、*O=companyname*、*L=Boston*、*S=MA*、*C=US*[その組織のユーザー内のすべてのAcrobatユーザーを取得するには]

バインド DN	ディレクトリの検索が許可されています。例：uid=ldapuser、cn=users、cn=accounts、dc=domain、dc=companyname、dc=com uid=john、cn=users、cn=accounts、dc=dorp、dc=company、dc=com（ユーザjohn@dorp.company.comの場合） dorp.company.com
アカウント	ユーザ
— ジョン	— アンナ
バインドパスワード	ディレクトリサーバのパスワード（バインド DN で使用されるユーザ名のパスワード）
プロトコル	LDAP 、 ldaps 、 ldap-start-TLS
ポート	ポートを選択します

LDAP ディレクトリサーバでデフォルトの属性名が変更されている場合は ' 次の Directory Server 必須属性を入力しますこれらの属性名のほとんどは、 LDAP ディレクトリサーバで _not_modified となります。この場合、デフォルトの属性名をそのまま使用できます。

属性（ Attributes ）	ディレクトリサーバの属性名
表示名	名前
UNIX ID	uidNumber
ユーザ名	UID

次の属性を追加するには、オプション属性を含めるをクリックします。

属性（ Attributes ）	ディレクトリサーバの属性名
E メールアドレス	メール
電話番号	電話番号
ロール	タイトル
国名	共同
状態	状態
部門	部門番号
写真	写真
ManagerDN	マネージャー
グループ	所属グループ

ユーザディレクトリコレクタ設定のテスト

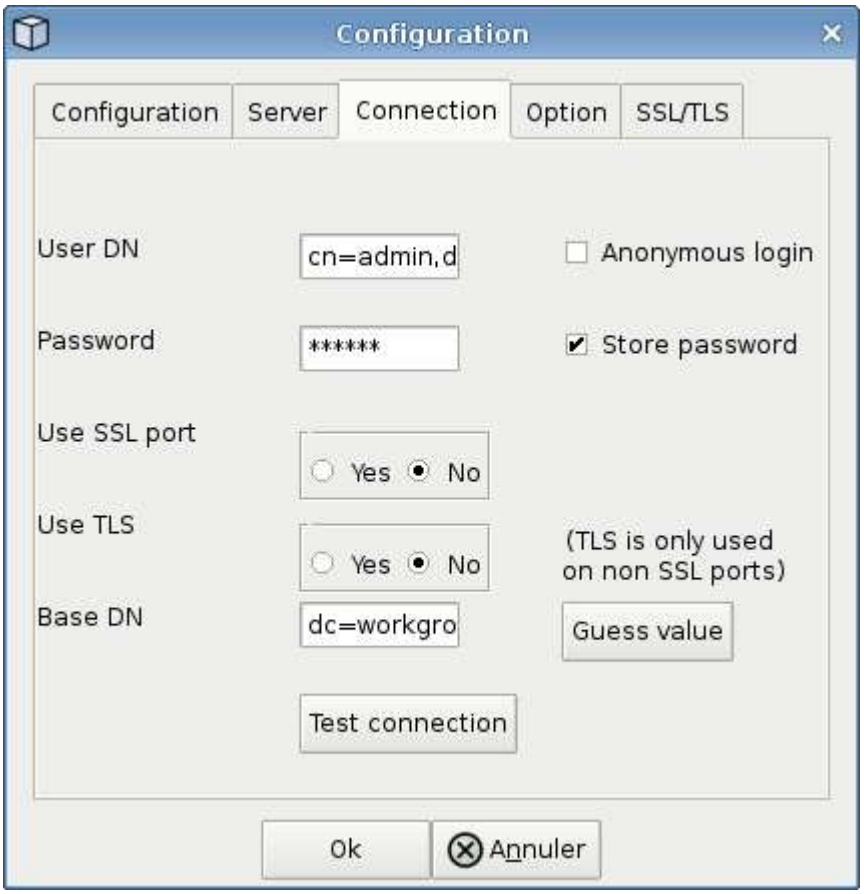
LDAP ユーザ権限および属性定義は、次の手順で検証できます。

- 次のコマンドを使用して、ワークロードセキュリティのLDAPユーザ権限を検証します。

```
 ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
```

* LDAP エクスプローラを使用して、 LDAP データベースの移動、オブジェクトのプロパティと属性の表示、権限の表示、オブジェクトのスキーマの表示、高度な検索の実行を行い、保存して再実行することができます。

- LDAP Explorer をインストールします (http://ldaptool.sourceforge.net/）またはJava LDAPエクスプローラ (http://jxplorer.org/）LDAPサーバに接続できるすべてのWindowsマシンで使用します。
- LDAPディレクトリサーバのユーザ名/パスワードを使用してLDAPサーバに接続します。



LDAP ディレクトリコレクタ設定エラーのトラブルシューティング

次の表に、コレクタの設定時に発生する可能性のある既知の問題と解決策を示します。

問題	解決策：
LDAP Directory Connector を追加すると、「 Error 」状態になります。「 Invalid credentials provided for LDAP server 」 (LDAP サーバーの資格情報が無効です) というエラーが表示されます	指定したバインド DN またはバインドパスワードまたは検索ベースが正しくありません。を編集し、正しい情報を入力します。

問題	解決策：
LDAP Directory Connector を追加すると、「 Error 」状態になります。「 DN=DC=HQ,DC=domainname,DC=com に対応するオブジェクトをフォレスト名として提供できませんでした」というエラーが表示されます。	入力された検索ベースが正しくありません正しいフォレスト名を編集して入力します。
ドメインユーザーのオプションの属性は、[ワークロードセキュリティユーザープロファイル]ページに表示されません。	これは、 CloudSecure で追加されたオプション属性の名前と Active Directory の実際の属性名が一致しないことが原因である可能性があります。フィールドでは大文字と小文字が区別されます正しいオプションの属性名を編集して入力します。
データコレクタでエラーが発生し、「 LDAP ユーザを取得できませんでした。失敗の理由：サーバに接続できません。接続が null です "	_Restart_Button をクリックして、コレクタを再起動します。
LDAP Directory Connector を追加すると、「 Error 」状態になります。	必須フィールドに有効な値（ Server 、 forest-name 、 bind-dn 、 bind-Password ）が指定されていることを確認してください。 bind-DN 入力が常に uid=ldapuser,cn=Users,cn=account,dc=domain,dc=companyname,dc=com として提供されていることを確認します。
LDAP Directory Connector を追加すると、「再試行中」の状態になります。「 Failed to Determine the health of the collector したがって retrying again 」というエラーが表示されます。	正しいサーバ IP と検索ベースが提供されていることを確認します ////
LDAPディレクトリの追加中に、次のエラーが表示されます。 「Failed to determine the health of the collector within 2 retries、try restarting the collector again（Error Code：AGENT008）」	正しいサーバ IP と検索ベースが提供されていることを確認します
LDAP Directory Connector を追加すると、「再試行中」の状態になります。「 Unable to define state of the collector 、 reason TCP command [Connect (localhost:35012, None, List() 、 some (,seconds),true)] failed because of java.net.ConnectionException:Connection refused 」というエラーが表示されます。	AD サーバに指定された IP または FQDN が正しくありません。を編集し、正しい IP アドレスまたは FQDN を指定します。 ////
LDAP Directory Connector を追加すると、「 Error 」状態になります。「 LDAP 接続の確立に失敗しました」というエラーが表示されます。	LDAP サーバに対して指定された IP または FQDN が正しくありません。を編集し、正しい IP アドレスまたは FQDN を指定します。 または 指定したポートの値が正しくありません。LDAP サーバのデフォルトのポート値または正しいポート番号を使用してみてください。

問題	解決策：
LDAP Directory Connector を追加すると、「 Error 」状態になります。「設定をロードできませんでした。理由：データソースの設定でエラーが発生しました。具体的な理由： /connector/conf/application.conf ： 70 ： ldap.ldap-port には number ではなく string 型があります。	指定したポートの値が正しくありません。デフォルトのポート値または AD サーバの正しいポート番号を使用してみてください。
必須属性から始めて、機能しました。オプションの属性を追加した後、オプションの属性データは AD から取得されません。	これは、 CloudSecure で追加されたオプションの属性と Active Directory の実際の属性名が一致しないことが原因である可能性があります。正しい必須またはオプションの属性名を編集して入力します。
コレクタの再起動後、 LDAP 同期はいつ行われますか。	コレクタが再起動するとすぐに LDAP 同期が実行されます。約 15 分で約 30 万人のユーザデータが取得され、 12 時間ごとに自動的に更新されます。
ユーザデータは LDAP から CloudSecure に同期されます。データを削除するタイミング	更新がない場合、ユーザデータは 13 カ月間保持されます。テナントが削除されると、データは削除されます。
LDAP Directory Connector により、「 Error 」状態になります。" コネクタでエラーが発生しました。サービス名： usersLDAP 。失敗の理由： LDAP ユーザを取得できませんでした。失敗の理由： 80090308 ： LdapErr: DSID-0C090453 、 comment: AcceptSecurityContext error 、 data 52e 、 v3839	指定したフォレスト名が正しくありません。正しいフォレスト名を指定する方法については、上記を参照してください。
電話番号がユーザプロファイルページに入力されていません。	これは、多くの場合、 Active Directory の属性マッピングの問題が原因です。 1. Active Directory からユーザの情報を取得している特定の Active Directory コレクタを編集します。 2. オプション属性の下に、 Active Directory 属性「 telephonenumber 」にマッピングされたフィールド名「 Telephone Number 」があることに注意してください。 4. ここでは、前述の Active Directory エクスプローラツールを使用して LDAP ディレクトリサーバを参照し、正しい属性名を確認してください。 3. LDAP ディレクトリに、実際にユーザの電話番号を持つ「 telephonenumber 」という名前の属性があることを確認します。 5. ここでは、 LDAP ディレクトリで「 phonenumber 」に変更されたとします。 6. CloudSecure User Directory コレクタを編集します。オプションの属性セクションで、「 telephonenumber 」を「 phonenumber 」に置き換えます。 7. Active Directory コレクタを保存すると、コレクタが再起動してユーザの電話番号が取得され、ユーザプロファイルページにも同じ番号が表示されます。

問題	解決策：
Active Directory（AD）サーバで暗号化証明書（SSL）が有効になっている場合、Workload Security User Directory CollectorはADサーバに接続できません。	ユーザーディレクトリコレクタを設定する前に、 AD サーバーの暗号化を無効にします。 ユーザの詳細情報が取得されてから 13 カ月間表示されます。 ユーザーの詳細を取得した後に AD サーバーが切断された場合、新しく追加された AD 内のユーザーは取得されません。再度取得するには、ユーザディレクトリコレクタが AD に接続されている必要があります。

ONTAP SVM Data Collector の設定

ワークロードセキュリティでは、データコレクタを使用して、デバイスからファイルとユーザのアクセスデータを収集します。

作業を開始する前に

- このデータコレクタは、次の機能でサポートされています。
  - Data ONTAP 9.2 以降のバージョン最高のパフォーマンスを得るには、9.13.1よりも新しいバージョンのData ONTAPを使用してください。
  - SMBプロトコルバージョン3.1以前。
  - ONTAP 9.151以降を搭載したNFS 4.1以前のバージョン。
  - FlexGroup は ONTAP 9.4 以降のバージョンでサポートされます
  - ONTAP Select がサポートされています
- サポートされるのはデータタイプの SVM のみです。Infinite Volume を備えた SVM はサポートされません。
- SVM には複数のサブタイプがあります。このうち、サポートされるのは_DEFAULT_、*SYNC_SOURE*、および_SYNC_destination_のみです。
- エージェント "を設定する必要があります" データコレクタを設定する前に、
- ユーザディレクトリコネクタが正しく設定されていることを確認します。正しく設定されていないと、イベントはエンコードされたユーザ名で表示され、 Active Directory に保存されているユーザの実際の名前ではなく、 [Activity Forensics] ページに表示されます。
- •ONTAP永続ストアは9.14.1以降でサポートされています。
- 最適なパフォーマンスを実現するには、 FPolicy サーバをストレージシステムと同じサブネットに設定する必要があります。
- 次のどちらかの方法で SVM を追加する必要があります。
  - クラスタ IP 、 SVM 名、およびクラスタ管理のユーザ名とパスワードを使用する。これは推奨される方法です。
    - SVM 名は ONTAP に表示されるとおりに指定する必要があり、大文字と小文字が区別されます。
  - SVM SVM 管理 IP 、ユーザ名、およびパスワードを使用する
  - フル管理者のクラスタ / SVM 管理ユーザ名とパスワードを使用できない場合は、に記載されている権限よりも少ないカスタムユーザを作成できます 「権限に関する注意事項」 セクションを参照してください。このカスタムユーザは、 SVM アクセスまたはクラスタアクセス用に作成できます。

- 以下の「権限に関する注意」セクションで説明されているように、少なくともcsroleの権限を持つロールを持つADユーザを使用することもできます。も参照してください "ONTAP のドキュメント"。

- 次のコマンドを実行して、 SVM に正しいアプリケーションが設定されていることを確認します。

```
clustershell::> security login show -vserver <vservername> -user-or
-group-name <username>
```

出力例：

```
Vserver: svmname
                                                                Second
User/Group                  Authentication                 Acct   Authentication
Name           Application  Method        Role Name        Locked Method
-------------- -----------  ------------  ---------------- ------ --------------
vsadmin        http         password      vsadmin          no     none
vsadmin        ontapi       password      vsadmin          no     none
vsadmin        ssh          password      vsadmin          no     none
3 entries were displayed.
```

- SVMにCIFSサーバが設定されていることを確認します。
  クラスタシェル：：> `vserver cifs show`

  Vserver 名、 CIFS サーバ名、およびその他のフィールドが返されます。

- SVM の vsadmin ユーザのパスワードを設定します。カスタムユーザまたはクラスタ管理者ユーザを使用する場合は、この手順を省略します。
  クラスタシェル：：> `security login password -username vsadmin -vserver svmname`

- SVM の vsadmin ユーザの外部アクセスのロックを解除します。カスタムユーザまたはクラスタ管理者ユーザを使用する場合は、この手順を省略します。
  クラスタシェル：：> `security login unlock -username vsadmin -vserver svmname`

- データ LIF のファイアウォールポリシーが「 GMT 」（「 data 」ではない）に設定されていることを確認します。専用の管理 LIF を使用して SVM を追加する場合は、この手順を省略してください。
  クラスタシェル：：> `network interface modify -lif <SVM_data_LIF_name> -firewall -policy mgmt`

- ファイアウォールが有効になっている場合は、 Data ONTAP データコレクタを使用してポートの TCP トラフィックを許可する例外を定義する必要があります。

  を参照してください "エージェントの要件" を参照してください。この環境オンプレミスエージェントおよびクラウドにインストールされたエージェント。

- Cloud ONTAP SVM を監視するために AWS EC2 インスタンスにエージェントがインストールされている場合は、そのエージェントとストレージが同じ VPC 内に存在する必要があります。これらの VPC が個別の VPC 内にある場合は、 VPC 間に有効なルートが必要です。

ユーザアクセスブロックの前提条件

次の点に注意してください。 "ユーザアクセスブロック"：

この機能を使用するには、クラスタレベルのクレデンシャルが必要です。

クラスタ管理者のクレデンシャルを使用している場合、新しい権限は不要です。

ユーザに付与された権限でカスタムユーザ（_csuser_など）を使用している場合は、次の手順に従ってワークロードセキュリティにユーザをブロックする権限を付与します。

クラスタクレデンシャルを持つ csuser の場合、 ONTAP コマンドラインから次の手順を実行します。

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

アクセス権に関する注意事項

クラスタ管理**IP**を使用して追加する場合の権限：

クラスタ管理管理者ユーザがワークロードセキュリティを使用してONTAP SVMデータコレクタにアクセスできない場合は、次のコマンドに示すロールを持つ「csuser」という新しいユーザを作成できます。Cluster Management IPを使用するようにWorkload Securityデータコレクタを設定する場合は、「csuser」のユーザ名とパスワードを使用します。

新しいユーザを作成するには、クラスタ管理者のユーザ名とパスワードを使用して ONTAP にログインし、ONTAP サーバで次のコマンドを実行します。

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
```

SVM管理**IP** *を使用して追加する場合の権限：

クラスタ管理管理者ユーザがワークロードセキュリティを使用してONTAP SVMデータコレクタにアクセスできない場合は、次のコマンドに示すロールを持つ「csuser」という新しいユーザを作成できます。Workload SecurityデータコレクタでSVM管理IPを使用するように設定する場合は、「csuser」のユーザ名とパスワードを使用します。

新しいユーザを作成するには、クラスタ管理者のユーザ名とパスワードを使用して ONTAP にログインし、ONTAP サーバで次のコマンドを実行します。これらのコマンドをテキストエディタにコピーし、<vservername> を SVM 名に置き換えてから、 ONTAP で次のコマンドを実行します。

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
```

ONTAP Autonomous Ransomware Protectionの権限とONTAPへのアクセス拒否

クラスタ管理者のクレデンシャルを使用している場合、新しい権限は不要です。

ユーザに付与された権限でカスタムユーザ（_csuser_など）を使用している場合は、次の手順に従ってワークロードセキュリティにアクセス許可を付与し、ONTAP からARP関連情報を収集します。

詳細については、 "ONTAPアクセス拒否との統合"

および "ONTAP によるランサムウェア対策との統合"

データコレクタを設定します

設定の手順

1. Data Infrastructure Insights環境に管理者またはアカウント所有者としてログインします。
2. [Workload Security]>[Collectors]>[+Data Collectors]*をクリックします。

   使用可能なデータコレクタが表示されます。
3. NetApp SVM のタイルにカーソルを合わせ、 * + Monitor * をクリックします。

   ONTAP SVM の設定ページが表示されます。各フィールドに必要なデータを入力します。

フィールド	説明
名前	Data Collector の一意の名前
エージェント	リストから設定済みエージェントを選択します。
管理 IP 経由で接続：	クラスタ IP または SVM 管理 IP を選択します
クラスタ / SVM 管理 IP アドレス	上記の選択に応じて、クラスタまたは SVM の IP アドレス。
SVM 名	SVM の名前（このフィールドはクラスタ IP 経由で接続する場合は必須です）

ユーザ名	SVM /クラスタにアクセスするためのユーザ名 クラスタIPを使用して追加する場合のオプションは次のとおりです。 1.クラスタ管理者 2.「csuser」 3. csuserと同様の役割を持つADユーザ。 SVM IPを使用して追加する場合のオプションは次のとおりです。 4. vsadmin 5.「csuser」 6.AD - csuserと同様のロールを持つユーザ名。
パスワード	上記のユーザ名のパスワード
共有 / ボリュームをフィルタリングします	イベントコレクションに共有 / ボリュームを含めるか除外するかを選択します
除外または対象に含める共有名を入力します	イベント収集の対象から除外または対象に含める（必要に応じて）共有をカンマで区切ったリスト
除外または対象に含めるボリュームの完全な名前を入力します	イベント収集の対象から除外または対象に含めるボリュームをカンマで区切ったリスト
フォルダアクセスを監視します	オンにすると、フォルダアクセス監視のイベントが有効になります。このオプションを選択しなくても、フォルダの作成 / 名前変更および削除が監視されることに注意してください。これを有効にすると、監視されるイベントの数が増えます。
ONTAP 送信バッファサイズを設定します	ONTAP FPolicy 送信バッファのサイズを設定します。9.8p7 より前のバージョンの ONTAP を使用していて、 Performance 問題が表示された場合、 ONTAP 送信バッファサイズを変更して ONTAP のパフォーマンスを向上させることができます。このオプションが表示されない場合は、ネットアップサポートにお問い合わせください。

完了後

- Installed Data Collectors ページで、各コレクタの右側にあるオプションメニューを使用してデータコレクタを編集します。データコレクタを再起動したり、データコレクタ設定の属性を編集したりできます。

Metro Clusterの推奨構成

Metro Clusterの推奨事項は次のとおりです。

1. 2つのデータコレクタをソースSVMに、別のデータコレクタをデスティネーションSVMに接続します。
2. データコレクタは、*Cluster IP*.によって接続する必要があります。
3. あるデータコレクタを実行する必要がある時点であれば、別のデータコレクタでエラーが発生します。

   現在の「実行中」のSVMのデータコレクタは、_RUNNING _と表示されます。現在の「停止」されているSVM
   データコレクタには_Error_と表示されます。

4. スイッチオーバーが発生すると、データコレクタの状態が「Running」から「Error」に変わり、その逆も

同様です。

5. データコレクタがError状態からRunning状態に移行するまでに最大2分かかります。

サービスポリシー

ONTAP バージョン9.9..1のサービスポリシーを使用してData Source Collectorに接続するには、Data Service_data-NFS_、および/or _data-cifs_が 必要です。

例

```
Testcluster-1::*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

9.6.1より前のバージョンのONTAP では、_data -fpolicy-client_need not be set」を実行します。

Data Collectorの再生-一時停止

2つの新しい操作がコレクタのkebabメニューに表示されるようになりました(一時停止と再開)。

Data Collectorがin_running_stateの場合は、収集を一時停止できます。コレクターの「3つのドット」メニューを開き、一時停止を選択します。コレクタが一時停止している間は、ONTAPからデータが収集されず、コレクタからONTAPにデータが送信されません。つまり、ONTAPからデータコレクタへ、およびそこからデータインフラストラクチャインサイトへのFPolicyイベントは流れません。

コレクタの一時停止中に新しいボリュームなどがONTAPに作成されると、ワークロードセキュリティでデータが収集されず、それらのボリュームなどがダッシュボードやテーブルに反映されないことに注意してください。

次の事項に注意してください。

- スナップショットのパージは、一時停止中のコレクタに設定されている設定に従って実行されません。
- 一時停止したコレクタでEMSイベント（ONTAP ARPなど）は処理されません。つまり、ONTAPがランサムウェア攻撃を特定した場合、データインフラ分析情報ワークロードセキュリティはそのイベントを取得できません。
- 一時停止中のコレクタについては、ヘルス通知Eメールは送信されません。
- 一時停止中のコレクタでは'手動または自動のアクション(スナップショットやユーザーブロックなど)はサポートされません
- エージェントまたはコレクタのアップグレード、エージェントVMの再起動/再起動、またはエージェントサービスの再起動時に、一時停止したコレクタは_Paused_stateのままになります。
- データコレクタが_Error_stateの場合、コレクタを_Paused_stateに変更することはできません。Pauseボタンは'コレクタの状態が_running_の場合にのみ有効になります
- エージェントが切断されている場合、コレクタを_Paused_stateに変更することはできません。コレクタが_stopped_stateになり、Pauseボタンが無効になります。

永続的ストア

永続的ストアは、ONTAP 9.14.1以降でサポートされます。ボリューム名の手順はONTAP 9.14~9.15では異なります。

永続ストアを有効にするには、コレクタの編集/追加ページでチェックボックスをオンにします。チェックボックスを選択すると、ボリューム名を受け入れるためのテキストフィールドが表示されます。永続的ストアを有効にするには、ボリューム名は必須フィールドです。

- ONTAP 9.14.1では、この機能を有効にする前にボリュームを作成し、_Volume Name_フィールドに同じ名前を指定する必要があります。推奨されるボリュームサイズは16GBです。
- ONTAP 9.15.1では、_Volume Name_フィールドに指定した名前を使用して、16GBのサイズでボリュームが自動的に作成されます。

Persistent Storeには特定の権限が必要です（これらの一部またはすべてがすでに存在する場合があります）。

クラスタモード：

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <cluster-name>
```

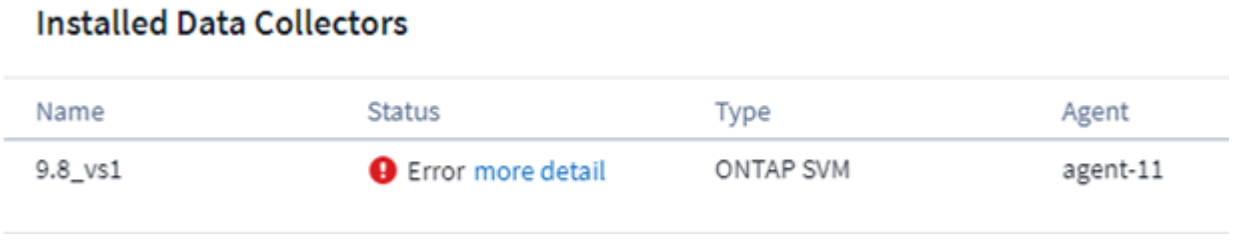
SVMモード：

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <vserver-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <vserver-name>
```

トラブルシューティング

既知の問題とその解決策を次の表に示します。

エラーの場合は、 *Status_column* で *_more detail* をクリックしてエラーの詳細を確認します。



問題	解決策：
Data Collector はしばらくの間実行され、ランダムな時刻の後に停止します。 "Error message: connector is in error state" というエラーメッセージが表示されます。サービス名： audit 。エラーの理由：外部 FPolicy サーバが過負荷状態です。」	ONTAP からのイベントレートは、 [エージェント] ボックスで処理できるイベントレートよりもはるかに高くなっています。そのため、接続が終了しました。 切断が発生したときに、 CloudSecure でピークトラフィックを確認します。これは、 * CloudSecure > Activity Forensics > All Activity * ページで確認できます。 集約されたトラフィックのピークが [エージェント] ボックスで処理できるトラフィックよりも大きい場合は、 [エージェント] ボックスでのコレクタ展開のサイズ設定方法に関する [イベントレートチェッカー] ページを参照してください。 2021年3月4日より前にAgentがAgentボックスにインストールされている場合は、Agentボックスで次のコマンドを実行します。 echo 'net.core.rmem_max=838608'>>/etc/sysctl.conf echo 'net.ipv4.tcp_rmem=4096 2097152 838608'>>/etc/sysctl.conf sysctl -p サイズ変更後にUIからコレクタを再起動します。

問題	解決策：
コレクタから「 No local IP address found on the Connector that can reach the data interfaces of the SVM 」というエラーメッセージが報告されます。	その理由としては、 ONTAP 側のネットワーク問題が考えられます。次の手順を実行してください。 1. SVMデータLIFまたは管理LIFに、SVMからの接続をブロックしているファイアウォールがないことを確認します。 2. クラスタ管理 IP を使用して SVM を追加する場合、 Agent VM から SVM のデータ LIF と管理 LIF に ping できることを確認します。問題が発生した場合は、 LIF のゲートウェイ、ネットマスク、およびルートを確認してください。 また、クラスタ管理 IP を使用して SSH 経由でクラスタにログインし、エージェント IP に ping を実行することもできます。エージェントIPがping可能であることを確認します。 *network ping -vserver <vserver name>-destination <Agent IP>-lif <Lif Name>-show-detail* pingできない場合は、ONTAPのネットワーク設定が正しいことを確認して、エージェントマシンにpingできるようにします。 3. クラスタ IP 経由で接続しようとしたが動作しない場合は、 SVM IP 経由で直接接続してみます。SVM IP を使用して接続する手順については、上記を参照してください。 4. SVM の IP と vsadmin のクレデンシャルを使用してコレクタを追加するときに、 SVM の LIF で Data plus Mgmt ロールが有効になっていることを確認します。この場合、 SVM LIF に ping することは可能ですが、 SVM LIF への SSH は機能しません。 「はい」の場合は、 SVM 管理のみの LIF を作成し、この SVM 管理のみの LIF を使用して接続してみてください。 5. まだ機能しない場合は、新しい SVM LIF を作成し、その LIF を介して接続します。サブネットマスクが正しく設定されていることを確認します。 6.高度なデバッグ: a）ONTAPでパケットトレースを開始します。 b）CloudSecure UIからSVMにデータコレクタを接続してみます。 c)エラーが表示されるまで待ちます。ONTAP でパケットトレースを停止します。 d）ONTAPからパケットトレースを開きます。この場所で入手できます \ *https：//<cluster_mgmt_ip>/spi /<clustername>/etc/log/packet_traces/*

問題	解決策：
メッセージ： "[hostname:<IP Address>] の ONTAP タイプを特定できませんでした。理由：ストレージシステム <IP アドレス > への接続エラー：ホストに到達できません（ホストに到達できません） "	1. 正しい SVM IP 管理アドレスまたはクラスタ管理 IP が指定されていることを確認します。 2. 接続する SVM またはクラスタに SSH で接続します。接続が完了したら、 SVM またはクラスタ名が正しいことを確認してください。
エラーメッセージ：「コネクタにエラーがあります。service.name ：監査。失敗の理由：外部 FPolicy サーバが終了しました。」	1. 多くの場合、ファイアウォールがエージェントマシンの必要なポートをブロックしています。エージェントマシンが SVM から接続するために、ポート範囲 35000-55000/TCP を開いていることを確認します。また、 ONTAP 側からエージェントマシンへの通信をブロックするファイアウォールが有効になっていないことを確認します。 2. [エージェント] ボックスに次のコマンドを入力し、ポート範囲が開いていることを確認します。 _sudo iptables -save

問題	解決策：
grep 3500 *_ 出力例は次のようになります。 *-a in_public_allow -p tcp -m tcp — dport 35000 -m conntrack -ctstate new -j accept* 3.SVMにログインし、次のコマンドを入力して、ONTAPとの通信をブロックするファイアウォールが設定されていないことを確認します。 *system services firewall show _* *_system services firewall policy show _* "ファイアウォールコマンドをチェックしてください"を選択します。 *ONTAP* *4.* 監視する *SVM / クラスタに SSH* で接続します。*SVMデータLIFから[Agent]ボックスにpingを送信し（CIFSプロトコルとNFSプロトコルをサポート）、pingが動作していることを確認します。* *_network ping -vserver <vserver name>-destination <Agent IP>-lif <Lif Name>-show-detail* pingできない場合は、ONTAPのネットワーク設定が正しいことを確認して、エージェントマシンにpingできるようにします。 5. 1 つの SVM を 2 つのデータコレクタを使用してテナントに 2 回追加すると、このエラーが表示されます。UI を使用して、いずれかのデータコレクタを削除します。次に、 UI を使用して他のデータコレクタを再起動します。次に、データコレクタのステータスが「 running 」と表示され、 SVM からのイベントの受信が開始されます。 基本的に、テナントでは、 1 つのデータコレクタで 1 つの SVM を追加します。1 つの SVM を 2 つのデータコレクタを使用して 2 回追加しないで 6.同じSVMが2つの異なるワークロードセキュリティ環境（テナント）に追加された場合は、最後の1つが常に成功します。2 つ目のコレクタは、独自の IP アドレスで FPolicy を設定し、最初の IP アドレスから開始します。そのため、最初のデータ収集ツールはイベントの受信を停止し、その「監査」サービスはエラー状態になります。 これを回避するには、各 SVM を 1 つの環境に設定します。 7.このエラーは、サービスポリシーが正しく設定されていない場合にも発生する可能性がありま	アクティビティページにイベントは表示されません。

問題	解決策：
1. ONTAP コレクタが「実行中」の状態かどうかを確認します。「はい」の場合は、一部のファイルを開いて、 CIFS クライアント VM 上で一部の CIFS イベントが生成されていることを確認します。 2. アクティビティが表示されない場合は、 SVM にログインして次のコマンドを入力してください。 *source fpolicy*<SVM> event log show -source fpolicy_ fpolicyに関連するエラーがないことを確認してください。 3. アクティビティが表示されない場合は、 SVM にログインしてください。次のコマンドを入力します。 <SVM> fpolicy show _ プレフィックスが「cloudsecure_」であるという名前のFPolicyポリシーが設定され、ステータスが「on」になっているかどうかを確認します。設定されていないと、 Agent が SVM でコマンドを実行できない可能性が高くなります。ページの先頭に記載されているすべての前提条件を満たしていることを確認してください。	SVM Data Collector がエラー状態で、エラーメッセージ「 Agent failed to connect to the collector 」
1. エージェントが過負荷になっており、データソースコレクタに接続できない可能性が高い。 2. エージェントに接続されているデータソースコレクタの数を確認します。 3. UI の ［All Activity ］ ページでデータフローレートを確認します。 4. 1 秒あたりのアクティビティ数が非常に多い場合は、別のエージェントをインストールし、一部のデータソースコレクタを新しいエージェントに移動します。	SVM Data Collector で、「 fpolicy.server.connectError: Node failed to establish a connection with the FPolicy server "12.195.15.146" （ reason ： Select Timed Out" ）」というエラーメッセージが表示される
SVM / クラスタでファイアウォールが有効になっています。そのため、 FPolicy エンジンは FPolicy サーバに接続できません。 詳細情報の取得に使用できるONTAPのCLIは次のとおりです。 event log show -source fpolicyでエラーを表示します event log show -source fpolicy -fields event、action、詳細を表示する説明。 "ファイアウォールコマンドをチェックしてください"を選択します。 ONTAP	エラーメッセージ : 「コネクタはエラー状態です。サービス名： audit 。失敗の理由： SVM で有効なデータインターフェイスが見つかりません（ロール：データ、データプロトコル： NFS か CIFS か、両方、ステータス：稼働）。」
動作インターフェイス（データプロトコルおよびデータプロトコルとして CIFS / NFS が設定されている）があることを確認してください。	データコレクタが Error 状態になり、しばらくしてから running 状態になり、 Error に戻ります。このサイクルが繰り返されます。

問題	解決策：
これは通常、次のシナリオで発生します。 1.複数のデータコレクタが追加されています。 2.このような動作を示すデータコレクタには、これらのデータコレクタにSVMが1つ追加されます。つまり、 2 つ以上のデータコレクタが 1 つの SVM に接続されます。 3. 1つのデータコレクタが1つのSVMにのみ接続されることを確認します。 4.同じSVMに接続されている他のデータコレクタを削除します。	コネクタでエラーが発生しています。サービス名：audit 。失敗の理由：（ SVM SVM 名のポリシー）を設定できませんでした。理由： 'fpolicy.scope-modify ： "federy" 内の 'shares-to-include' 要素に無効な値が指定されています
共有名は、引用符を付けずに指定する必要があります。ONTAP SVM DSC 設定を編集して共有名を修正します。 Include および exclude shares _ は、長い共有名のリストを対象としたものではありません。対象に含める共有や除外する共有が大量にある場合は、ボリュームでフィルタリングします。	クラスタに未使用の既存のポリシーがあります。ワークロードセキュリティをインストールする前に、これらのワークロードに対して何を行う必要がありますか？
切断状態の場合でも、既存の未使用の FPolicy 設定をすべて削除することを推奨します。ワークロードセキュリティで、プレフィックス「cloudsecure_」を付けてFPolicyを作成します。その他の未使用の FPolicy 設定はすべて削除できます。 fpolicy listを表示するCLIコマンド： *fpolicy show* FPolicy設定を削除する手順は次のとおりです。 *fpolicy disable -vserver <svmname>-policy-name <policy_name>* *fpolicy policy scope delete -vserver <svmname>-policy-name <policy_name>* *fpolicy policy delete -vserver <svmname>-policy-name <policy_name>* *fpolicy policy event delete -vserver <svmname>-event-name <event_list>* *fpolicy policy external-engine delete -vserver <svmname>-engine-name <engine_name>*	ワークロードセキュリティを有効にすると、ONTAP のパフォーマンスが低下します。レイテンシは一時的に上昇し、IOPSは散発的に低下します。
ワークロードセキュリティでONTAPを使用しているときに、ONTAPでレイテンシの問題が発生することがあります。これには、次のようないくつかの理由が考えられます。 "1372994"、 "1415152"、 "1438207"、 "1479704"、 "1354659"。これらの問題はすべてONTAP 9.13.1以降で解決されています。これらのいずれかのバージョンを使用することを強く推奨します。	データコレクタでエラーが発生し、次のエラーメッセージが表示されます。 「エラー：コネクタがエラー状態です。サービス名：audit 。失敗の理由： SVM svm_backup でポリシーを設定できませんでした。理由： ZAPI フィールド：イベントに対して値が指定されていません。「

問題	解決策：
NFS サービスのみが設定された新しい SVM から開始します。 ワークロードのセキュリティにONTAP SVMのデータコレクタを追加します。ワークロードセキュリティでONTAP SVMデータコレクタを追加する際、CIFSはSVMで許可されるプロトコルとして設定されます。 ワークロードセキュリティのデータコレクタでエラーが表示されるまで待ちます。 SVMでCIFSサーバが設定されていないため、左側にあるエラーはワークロードのセキュリティに表示されます。 ONTAP SVM データコレクタを編集し、許可されたプロトコルとして CIFS のチェックを解除します。データコレクタを保存します。NFS プロトコルのみが有効な状態で実行が開始されます。	Data Collectorに次のエラーメッセージが表示されます。 「Error：Failed to determine the health of the collector within 2 retries、try restarting the collector again（Error Code：AGENT008）」
1.データコレクタページで、エラーが表示されているデータコレクタの右にスクロールし、3つのドットメニューをクリックします。選択した編集 _ 。 データコレクタのパスワードをもう一度入力します。 [Save] ボタンを押して、データコレクタを保存します。 Data Collector が再起動し、エラーが解決されます。 2.エージェントマシンに十分なCPUまたはRAMヘッドルームがない場合があります。そのため、DSCが故障しています。 マシンのエージェントに追加されているデータコレクタの数を確認してください。 20を超える場合は、エージェントマシンのCPUとRAM容量を増やしてください。 CPUとRAMが増加すると、DSCは初期化状態になり、その後自動的に実行状態になります。 のサイジングガイドを参照してください "このページです"。	SVMモードが選択されている場合、Data Collectorはエラーアウトしています。

それでも問題が解決しない場合は、 [ヘルプ]>[サポート *] ページに記載されているサポートリンクにアクセスしてください。

NetApp ONTAP コレクタ用のCloud Volumes ONTAP とAmazon FSXの設定

ワークロードセキュリティでは、データコレクタを使用して、デバイスからファイルとユーザのアクセスデータを収集します。

Cloud Volumes ONTAP ストレージ構成

ワークロードセキュリティエージェントをホストするシングルノード/ HA AWSインスタンスの設定については、OnCommand Cloud Volumes ONTAP のドキュメントを参照してください。
https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html

設定が完了したら、次の手順に従って SVM をセットアップします。
https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html

サポート対象プラットフォーム

- Cloud Volumes ONTAP は、利用可能なすべてのクラウドサービスプロバイダで利用できます。たとえば、Amazon、Azure、Google Cloudなどです。
- ONTAP Amazon FSXの略

Agent Machine Configuration の略

エージェントマシンは、クラウドサービスプロバイダのそれぞれのサブネットで設定する必要があります。ネットワークアクセスの詳細については、[エージェントの要件]を参照してください。

以下は、AWSでエージェントをインストールする手順です。クラウドサービスプロバイダに応じて、AzureまたはGoogle Cloudでインストールのために同等の手順を実行できます。

AWSでワークロードセキュリティエージェントとして使用するマシンを設定するには、次の手順を実行します。

ワークロードセキュリティエージェントとして使用するマシンを構成するには、次の手順を実行します。

手順

1. AWS コンソールにログインし、 EC2-Instances ページに移動して、 *Launch instance* を選択します。
2. このページに記載されているバージョンに応じて、 RHEL または CentOS AMI を選択します。
https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html
3. Cloud ONTAP インスタンスが存在する VPC とサブネットを選択します。
4. 割り当てられたリソースとして、 [T2.xlarge _ （ 4 vCPU と 16 GB RAM ）] を選択します。
    a. EC2 インスタンスを作成します。
5. YUM パッケージマネージャを使用して、必要な Linux パッケージをインストールします。
    a. Linux パッケージのインストール _wget_or_unzip_native 。

ワークロードセキュリティエージェントをインストールします

1. Data Infrastructure Insights環境に管理者またはアカウント所有者としてログインします。
2. **[Collectors]***に移動し、[Agents]*タブをクリックします。
3. [*+Agent] をクリックし、ターゲットプラットフォームとして RHEL を指定します。
4. [エージェントインストール] コマンドをコピーします。
5. ログインしている RHEL EC2 インスタンスに Agent Installation コマンドを貼り付けます。
これにより、ワークロードセキュリティエージェントがインストールされ、すべてのが提供されます "エージェントの前提条件" 達成された。

詳細な手順については、次のリンクを参照してください。
https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

トラブルシューティング

既知の問題とその解決策を次の表に示します。

問題	解決策：
「Workload Security: Failed to Determine ONTAP type for Amazon FxSN data collector」というエラーがData Collectorに表示されます。 お客様が新しいAmazon FSxNデータコレクタをワークロードセキュリティに追加できません。 エージェントからのポート443上のFSxNクラスタへの接続がタイムアウトしました。ファイアウォールとAWSセキュリティグループでは、通信を許可するために必要なルールが有効になっています。エージェントはすでに導入されており、同じAWSアカウントにも存在します。同じエージェントを使用して、残りのネットアップデバイス（およびすべてのデバイスが動作）を接続および監視します。	この問題 を解決するには、fsxadmin LIFネットワークセグメントをエージェントのセキュリティルールに追加します。 ポートについて不明な場合は、すべてのポートを許可します。

ユーザ管理

ワークロードセキュリティユーザアカウントは、Cloud Insights を使用して管理されます。

Cloud Insights には、アカウント所有者、管理者、ユーザ、ゲストの 4 つのユーザアカウントレベルがあります。各アカウントには、特定の権限レベルが割り当てられます。管理者権限を持つユーザアカウントは、ユーザを作成または変更し、各ユーザに次のいずれかのワークロードセキュリティロールを割り当てることができます。

ロール	ワークロードセキュリティアクセス
管理者	アラート、フォレンジック、データコレクタ、自動応答ポリシー、ワークロードセキュリティ用APIなど、すべてのワークロードセキュリティ機能を実行できます。 管理者は、他のユーザーを招待することもできますが、割り当てられるのはワークロードセキュリティロールのみです。
ユーザ	アラートを表示および管理し、フォレンジックを表示できます。ユーザーロールは、アラートステータスの変更、メモの追加、スナップショットの手動作成、ユーザーアクセスの制限を行うことができます。
ゲスト	アラートおよびフォレンジックを表示できます。ゲストロールは、アラートステータスの変更、メモの追加、スナップショットの手動作成、ユーザーアクセスの制限を行うことはできません。

手順

1. Workload Securityにログインします
2. メニューで、 [*Admin] > [User Management] をクリックします

Cloud Insights の User Management ページに転送されます。

3. 各ユーザに必要なロールを選択します。

新しいユーザを追加する際には、目的のロール（通常はユーザまたはゲスト）を選択します。

ユーザアカウントとロールの詳細については、 Cloud Insights を参照してください "ユーザロール" ドキュメント

SVMイベントレートチェッカー（エージェントサイジングガイド）

イベントレートチェッカーは、 ONTAP SVM データコレクタをインストールする前に、 SVM での NFS / SMB の組み合わせイベントレートを確認するために使用します。これにより、エージェントマシンで監視可能な SVM 1 の数が表示されます。イベントレートチェッカーは、セキュリティ環境の計画に役立つサイジングガイドとして使用します。

Agentは最大50個のデータコレクタをサポートできます。

要件

- クラスタIP
- クラスタ管理者のユーザ名とパスワード

このスクリプトを実行するときは、イベント速度を確認する SVM で ONTAP SVM Data Collector を実行していない必要があります。

手順

1. CloudSecure の指示に従って、 Agent をインストールします。
2. エージェントをインストールしたら、 sudo ユーザとして _server_data_rate_checker.sh_script を実行します。

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. このスクリプトを使用するには、 Linux マシンに _sshpass_to
をインストールする必要があります。インストール方法は 2 種類あります。
```

a. 次のコマンドを実行します。

```
 linux_prompt> yum install sshpass
.. 表示されない場合は、 Web から Linux マシンに sshpass_to
をダウンロードし、次のコマンドを実行します。
```

```
linux_prompt> rpm -i sshpass
```

3. プロンプトが表示されたら、正しい値を指定します。例については、以下を参照してください。
4. スクリプトの実行には約 5 分かかります。
5. 実行が完了すると、 SVM からイベントレートが出力されます。コンソールの出力では、 SVM ごとのイベントレートを確認できます。

```
“Svm svm_rate is generating 100 events/sec”.
```

各 ONTAP SVM データコレクタを 1 つの SVM に関連付けることができます。つまり、各データコレクタは、 1 つの SVM が生成するイベント数を受け取ることができます。

次の事項に注意してください。

a）この表は、一般的なサイジングガイドとして使用します。コアまたはメモリの数を増やして、サポートされるデータコレクタの数を増やすことができます（最大50個のデータコレクタ）。

Agent Machine Configuration の略	SVM データコレクタの数	エージェントマシンが処理できる最大イベントレート
4 コア、 16GB	10 個のデータコレクタ	20K イベント / 秒
4コア、32GB	データコレクタ 20 個	20K イベント / 秒

b ）合計イベント数を計算するには、そのエージェントのすべての SVM に対して生成されたイベントを追加します。

c) スクリプトがピーク時に実行されない場合、またはピークトラフィックが予測しにくい場合は、 30% のイベントレートバッファを維持します。

B+C は A 未満でなければなりません。そうしないと、 Agent マシンはモニタできません。

つまり、 1 台のエージェントマシンに追加できるデータコレクタの数は、次の式に準拠する必要があります。

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
```

を参照してください
xref:{relative_path}concept_cs_agent_requirements.html["エージェントの要件"]
ページで、その他の前提条件と要件を確認してください。

例

ここでは、 1 秒あたり 100 、 200 、および 300 のイベントレートを生成する SMS が 3 つあるとします。

式を適用します。

```
 (100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored
via one agent box.
```

コンソール出力は、エージェントマシンの現在の作業ディレクトリにあるファイル名 *fpolicy_stat_<SVM 名 >.log* で確認できます。

次の場合、スクリプトから間違った結果が返されることがあります。

- クレデンシャル、 IP 、または SVM 名が正しくない。
- 同じ名前、シーケンス番号などの既存の FPolicy にはエラーが発生します。
- 実行中はスクリプトは突然停止します。

スクリプトの実行例を次に示します。

```
[root@ci-cs-data agent]#
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
------------------------------
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

```
------------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

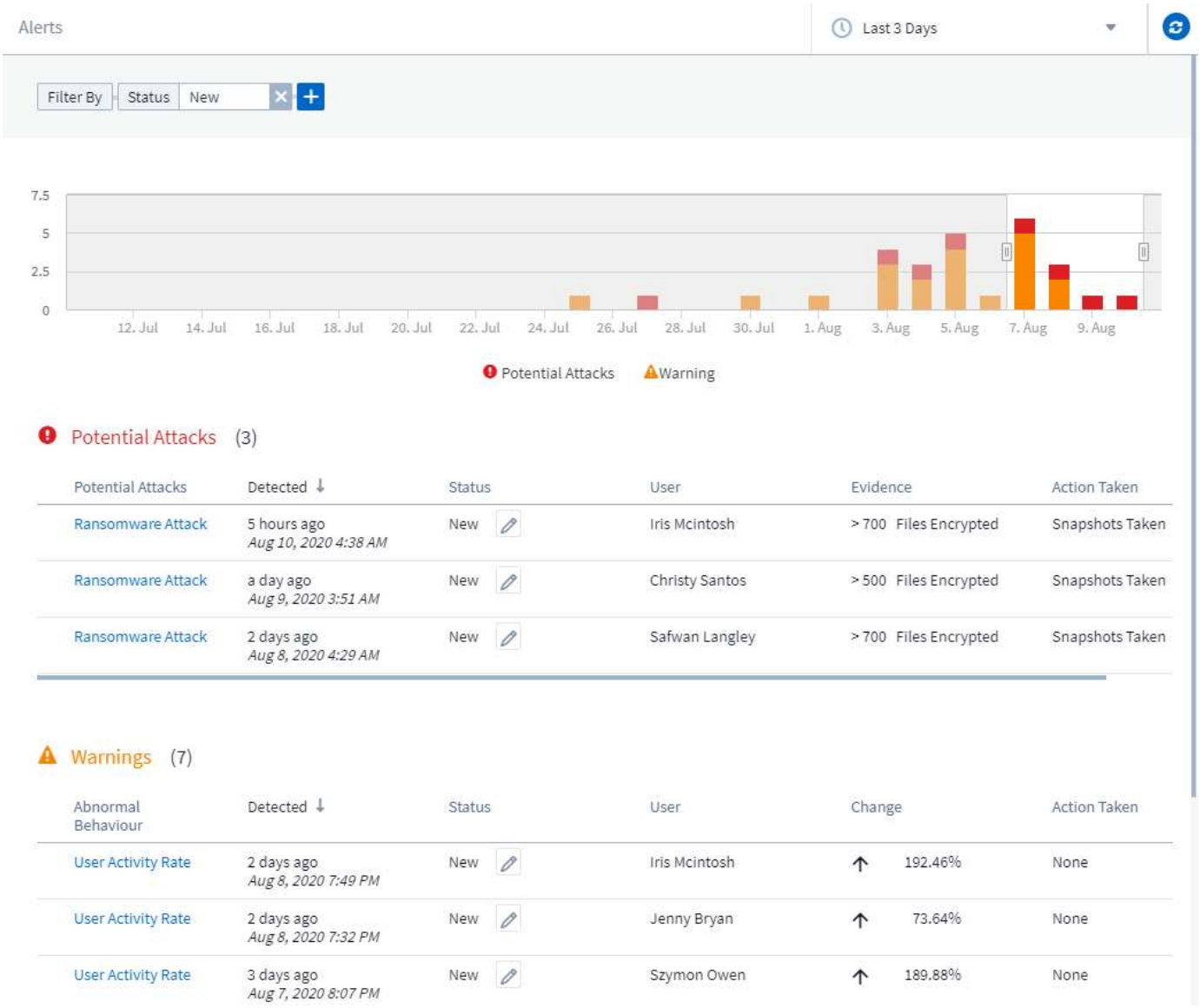
```
[root@ci-cs-data agent]#
```

トラブルシューティング

質問	回答
ワークロードセキュリティ用にすでに設定されているSVMに対してこのスクリプトを実行した場合、SVMの既存のfpolicy設定だけを使用するのか、それとも一時的なfpolicyを設定してプロセスを実行するのか。	ワークロードセキュリティがすでに設定されているSVMであっても、イベントレートチェッカーは問題なく実行できます。影響はありません。
スクリプトを実行できるSVMの数を増やすことはできますか。	はい。スクリプトを編集して、 SVM の最大数を 5 から任意の数に変更するだけです。
SVMの数を増やすと、スクリプトの実行時間は長くなりますか。	いいえSVM の数を増やした場合でも、スクリプトは最大 5 分間実行されます。
スクリプトを実行できるSVMの数を増やすことはできますか。	はい。スクリプトを編集して、 SVM の最大数を 5 から任意の望ましい数に変更する必要があります。
SVMの数を増やすと、スクリプトの実行時間は長くなりますか。	いいえSVM の数を増やした場合でも、スクリプトは最大 5 分間実行されます。
既存のエージェントでEvent Rate Checkerを実行するとどうなりますか？	既存のエージェントに対してイベントレートチェッカーを実行する原因 と、SVMのレイテンシが増加する可能性があります。この増加は、イベントレートチェッカーの実行中は一時的なものです。

アラート

[ワークロードセキュリティアラート]ページには、最近の攻撃や警告のタイムラインが表示され、各問題 の詳細を表示できます。



アラート

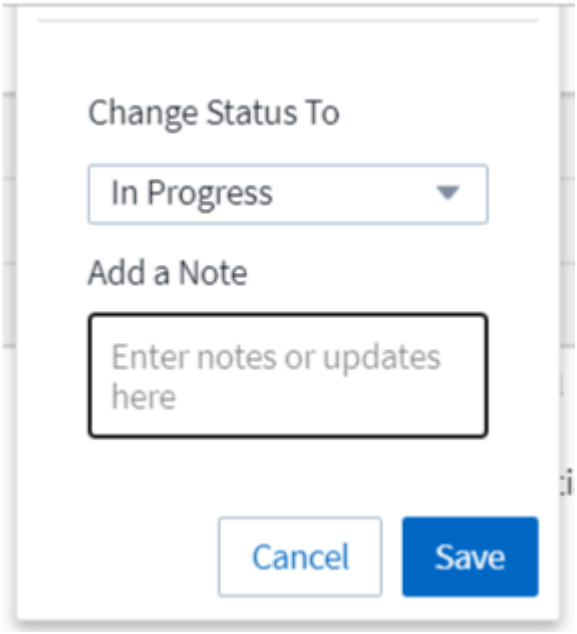
アラートリストには、選択した期間内に発生した攻撃および警告の総数、およびその期間内に発生した攻撃または警告のリストがグラフで表示されます。期間を変更するには、グラフの開始時間と終了時間のスライダを調整します。

アラートごとに次の情報が表示されます。

- 潜在的な攻撃 :*
- 潜在的な攻撃の種類（ランサムウェアや破壊行為など）
- 潜在的な攻撃が検出された日時 _

- アラートの *Status* ：
  - * 新規 * ：新しいアラートのデフォルトです。
  - * 進行中 * ：アラートはチームメンバーまたはメンバーによって調査中です。
  - * 解決済み * ：アラートはチームメンバーによって解決済みとマークされています。
  - * 却下 * ：アラートは誤検知または予期される動作として却下されました。

    管理者は、アラートのステータスを変更し、調査に役立つメモを追加できます。



- アラートをトリガーした動作のユーザー（ *User* ）
- 攻撃の _ 証拠 _ （多数のファイルが暗号化された場合など）
- アクションの実行 _ （スナップショットが作成された場合など）
- 警告 :*
- 警告をトリガーした異常な動作 _
- 動作が検出された日付と時刻 _
- アラートの *Status* （新規、進行中など）
- アラートをトリガーした動作のユーザー（ *User* ）
- 概要 of the *Chang* （ファイルアクセスが異常に増加している場合など）
- 実行されたアクション _

フィルタオプション（ **Filter Options** ）

アラートは次の方法でフィルタできます。

- アラートの *Status*
- 特定のテキスト（ *Note.*

- _ 攻撃 / 警告 _ のタイプ
- 警告 / 警告をトリガーしたアクションのユーザー _

[Alert Details] ページ

アラートリストページのアラートリンクをクリックすると、そのアラートの詳細ページを開くことができます。アラートの詳細は、攻撃またはアラートのタイプによって異なる場合があります。たとえば、ランサムウェア攻撃の詳細ページには、次のような情報が表示される場合があります。

サマリセクション：

- 攻撃の種類（ランサムウェア、被害者）とアラートID（ワークロードセキュリティが割り当て）
- 攻撃が検出された日時
- 実行された処理（自動スナップショットの作成など）。Snapshot の時刻は概要セクションのすぐ下に表示されます）
- ステータス（新規、進行中など）

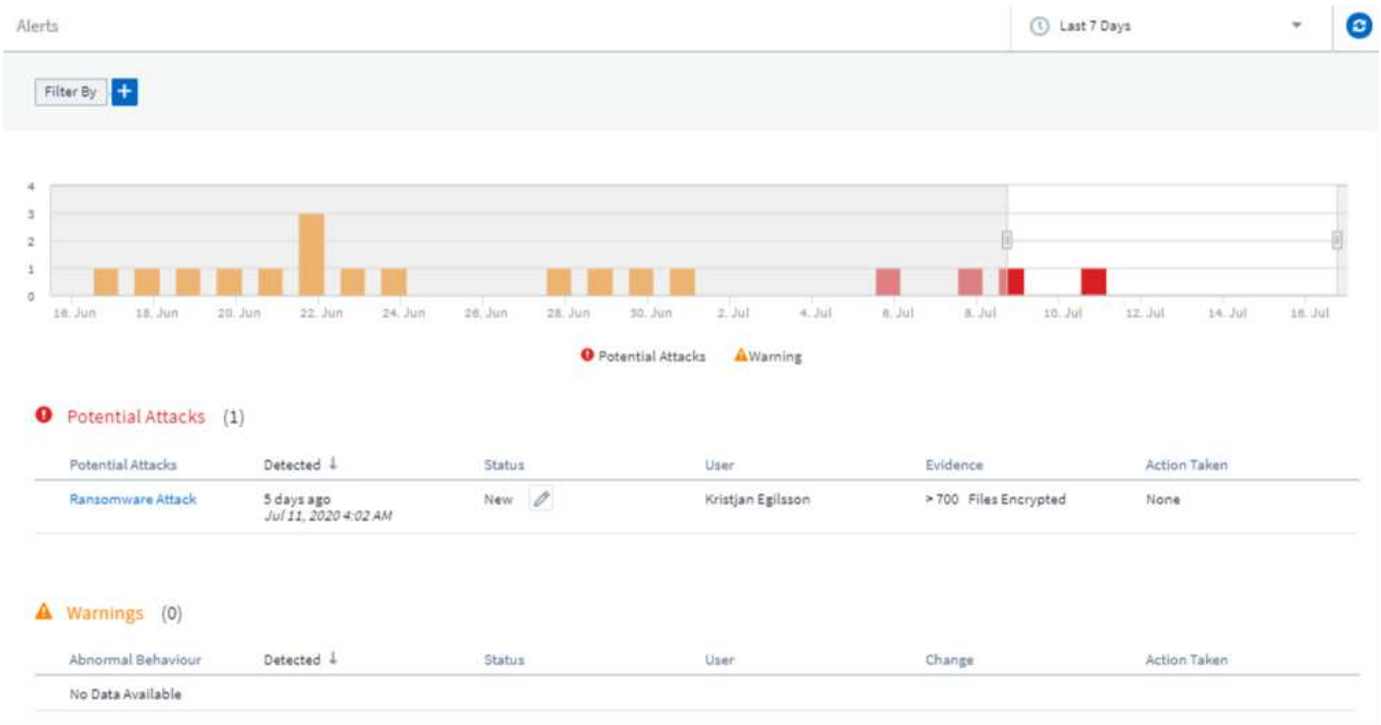
［ 攻撃結果 ］ セクション：

- 影響を受けるボリュームとファイルの数
- 検出の概要
- 攻撃中のファイルアクティビティを示すグラフ

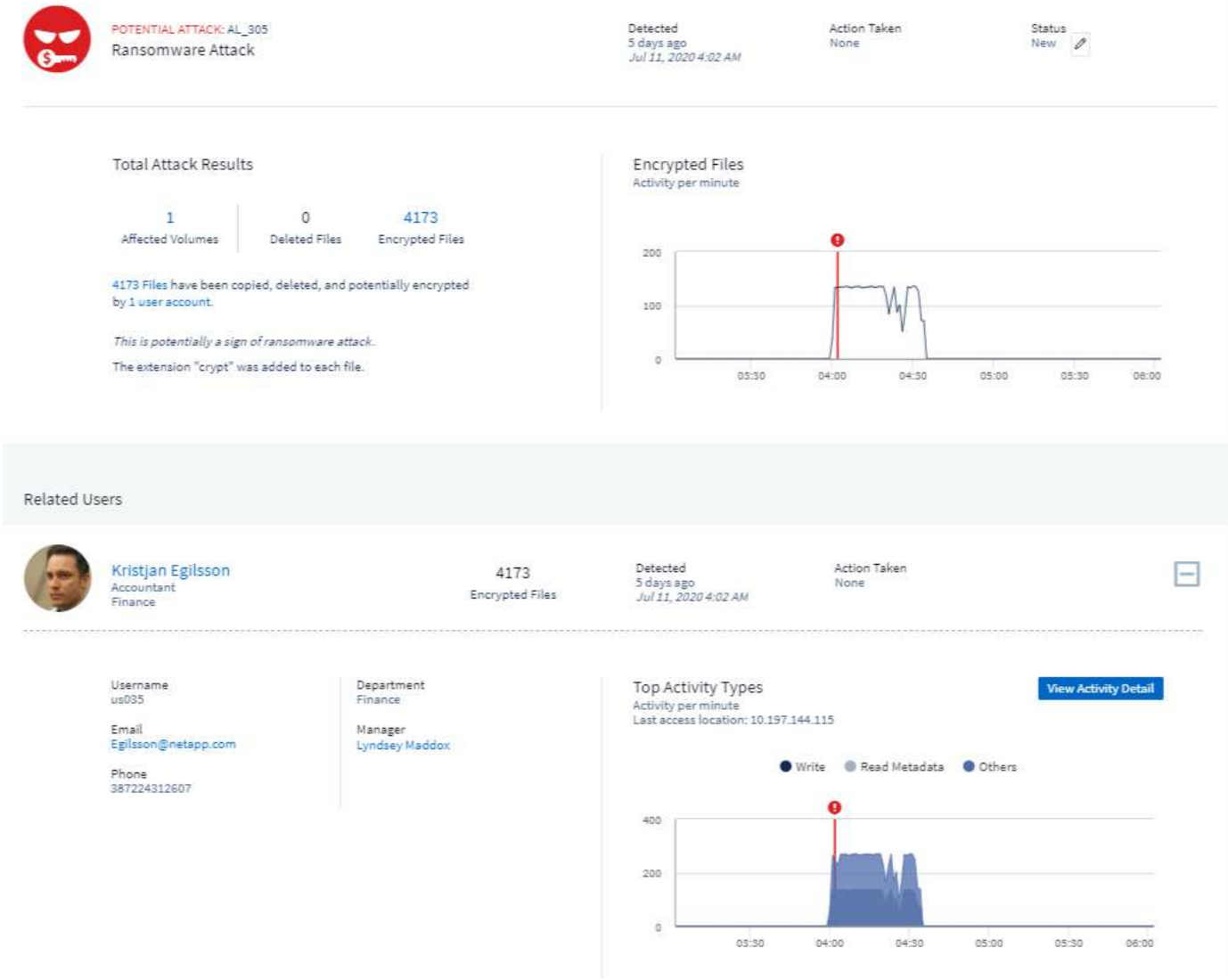
[関連ユーザー **]** セクション：

このセクションでは、潜在的な攻撃に関与するユーザーの詳細を示します。ユーザーの上位アクティビティのグラフも含まれます。

アラートページ（この例ではランサムウェア攻撃の可能性があります）：



詳細ページ（この例ではランサムウェア攻撃の可能性を示しています）：

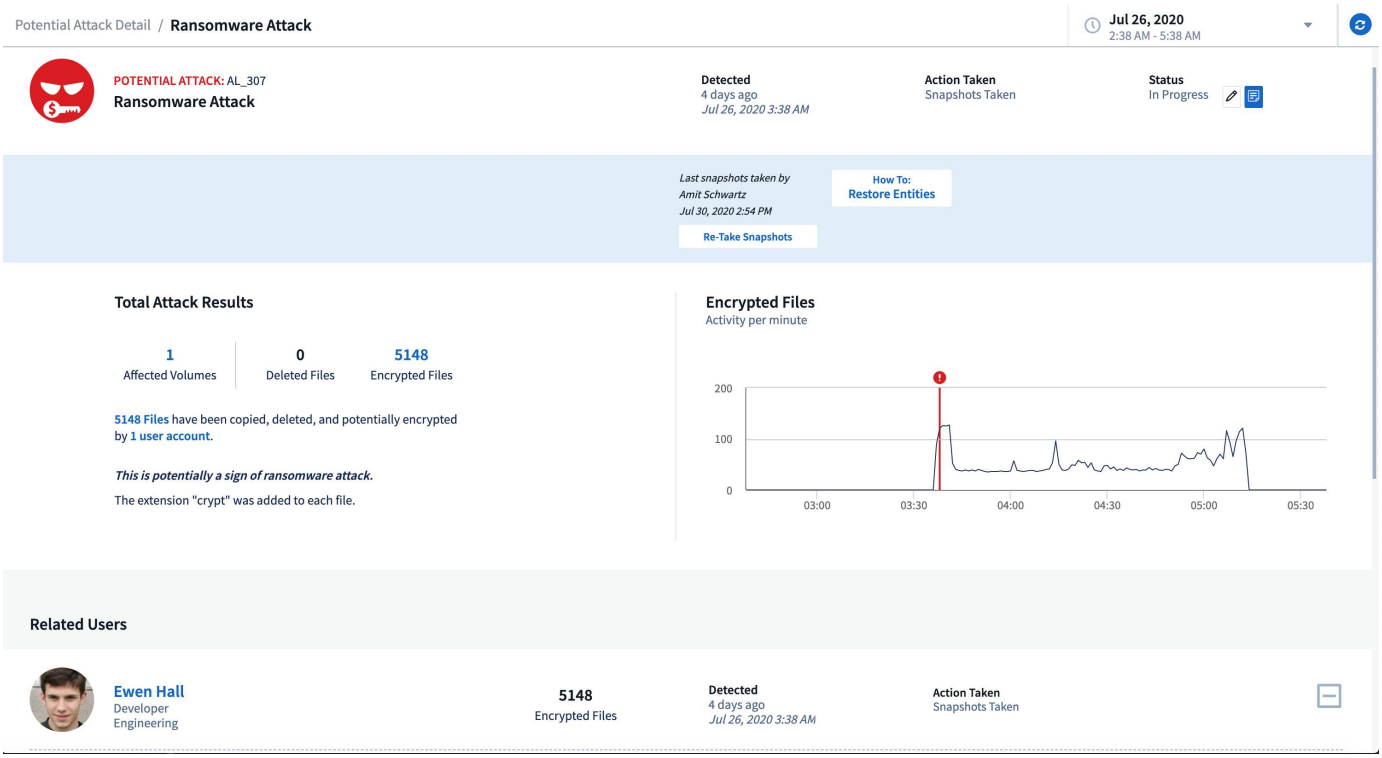


Snapshot_Actionを実行します

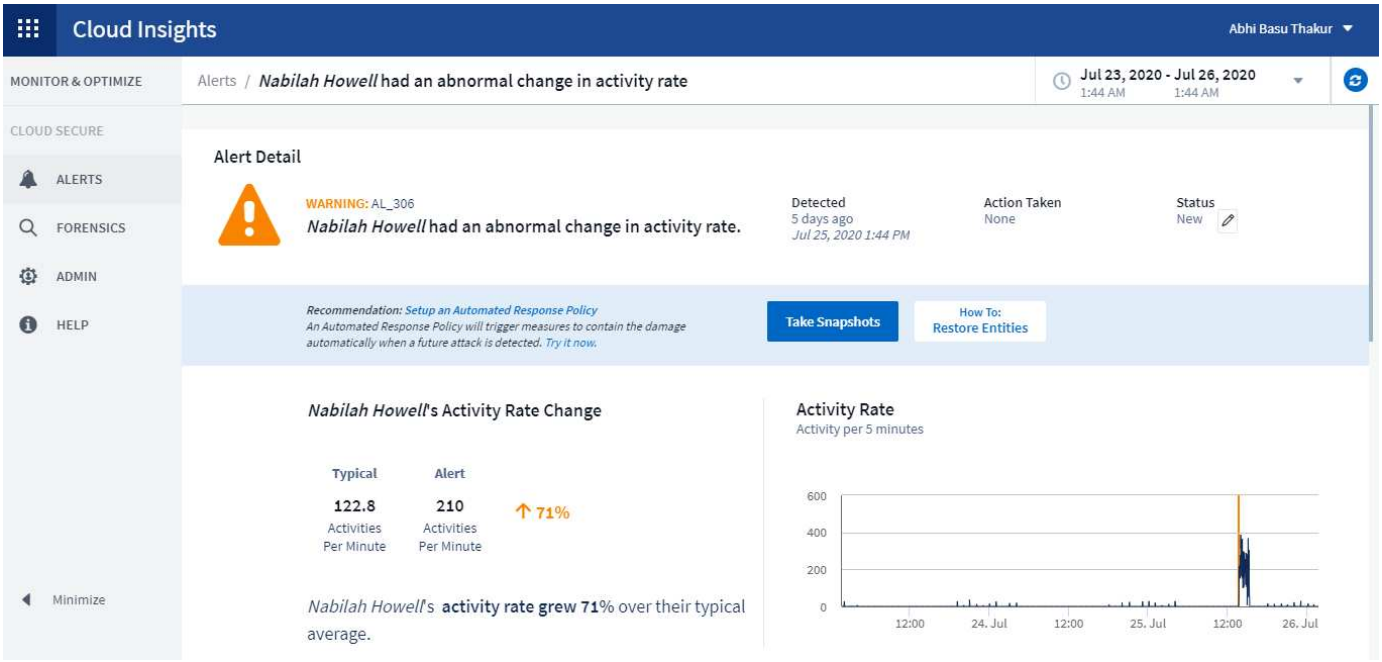
ワークロードセキュリティは、悪意のあるアクティビティが検出されたときにスナップショットを自動的に取得することでデータを保護し、データを安全にバックアップします。

を定義できます "自動応答ポリシー" ランサムウェア攻撃やその他の異常なユーザアクティビティが検出されるとスナップショットが作成されます。
アラートページから手動で Snapshot を作成することもできます。

自動 Snapshot の作成：



手動スナップショット：



アラート通知

アラートの E メール通知は、アラートに対するすべての対処方法についてアラート受信者リストに送信されます。アラート受信者を設定するには、 [*Admin] > [Notifications] をクリックし、受信者ごとに電子メールアドレスを入力します。

保持ポリシー

アラートと警告は 13 カ月間保持されます。13 カ月を経過したアラートと警告は削除されます。

ワークロードセキュリティ環境を削除すると、その環境に関連付けられているすべてのデータも削除されます。

トラブルシューティング

問題	次の操作を実行します
ONTAP では、 1 日に 1 時間ごとに Snapshot が作成される場合があります。ワークロードセキュリティ（WS）スナップショットは影響しますか。WSスナップショットは時間単位のスナップショットを作成しますか。デフォルトの時間単位の Snapshot は停止しますか？	ワークロードセキュリティスナップショットは、1時間ごとのスナップショットには影響しません。WSスナップショットは時間単位のスナップショット領域を使用しないため、以前と同様に継続する必要があります。デフォルトの時間単位 Snapshot は停止しません。
ONTAP で Snapshot 数が上限に達した場合、どうなるかを確認します。	最大Snapshot数に達すると、以降のSnapshot作成が失敗し、Snapshotがフルであることを示すエラーメッセージがワークロードセキュリティに表示されます。 最も古い Snapshot を削除するには、 Snapshot ポリシーを定義する必要があります。定義しないと、 Snapshot は作成されません。 ONTAP 9.3 以前では、ボリュームに格納できる Snapshot コピーは最大 255 個です。ONTAP 9.4 以降では、ボリュームに格納できる Snapshot コピーは最大 1023 個です。 の詳細については、 ONTAP のマニュアルを参照してください "Snapshot 削除ポリシーを設定しています"。
ワークロードセキュリティでSnapshotをまったく作成できません。	スナップショットの作成に使用されているロールに、「https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html#a-note-about-permissions[proper rights assigned」リンクがあることを確認します。 スナップショットを作成するための適切なアクセス権を持つ_csrole_が作成されていることを確認します。 security login role create -vserver <vservername>-role csrole -cmddirname "volume snapshot"-access all
ワークロードセキュリティから削除されたSVMでSnapshotを再度追加した場合、古いアラートに対してSnapshotが失敗します。SVM が再び追加されたあとに発生する新しいアラートについては、 Snapshot が作成されます。	これはまれなシナリオです。この問題が発生した場合は、 ONTAP にログインし、古いアラートに対して手動で Snapshot を作成してください。
_Alert Details_page では、 _Take Snapshot_Button の下に「 Last Attempt failed 」エラーが表示されます。 エラーにカーソルを合わせると、「 invoke API command has timed out for the data collector with id 」というメッセージが表示されます。	これは、SVMのLIFがONTAP で_disabled_stateである場合に、SVM管理IPを使用してワークロードセキュリティにデータコレクタが追加されたときに発生することがあります。 ONTAP で特定のLIFを有効にし、ワークロードセキュリティからtrigger _Take Snapshotを手動で作成します。Snapshot 処理が成功します。

フォレンジック

法医学 - すべての活動

すべてのアクティビティページは'ワークロードセキュリティ環境でエンティティに対して実行されるアクションを理解するのに役立ちます

すべてのアクティビティデータを確認しています

- Forensics > Activity Forensics * をクリックし、 * All Activity * タブをクリックして、 All Activity ページにアクセスします。
  このページでは、環境内のアクティビティの概要を説明します。次の情報が強調表示されます。
- グラフには、 _ アクティビティ履歴 _ （選択したグローバル時間範囲に基づいて、 1 分あたり 5 分あたり / 10 分あたりにアクセス）が表示されます。

  グラフの四角形をドラッグすると、グラフをズームできます。ページ全体がロードされ、ズームした時間範囲が表示されます。ズームインすると、ユーザーがズームアウトできるボタンが表示されます。
- アクティビティタイプ _ のチャート。アクティビティタイプ別にアクティビティ履歴データを取得するには、対応する X 軸ラベルリンクをクリックします。
- エンティティタイプ _ 上のアクティビティのグラフ。エンティティタイプ別にアクティビティ履歴データを取得するには、対応する X 軸ラベルリンクをクリックします。
- すべての Activity_data のリスト

すべてのアクティビティ *_table には、次の情報が表示されます。デフォルトでは、すべての列が表示されるわけではありません。歯車アイコンをクリックすると、表示する列を選択できます。

- エンティティがアクセスされた時間（年、月、日、最終アクセス時刻を含む）。
- へのリンクでエンティティにアクセスした * user * "ユーザ情報"。
- ユーザーが実行した * アクティビティ * 。サポートされるタイプは次のとおりです
  - * グループ所有権の変更 * - グループ所有権はファイルまたはフォルダに変更されています。グループの所有権の詳細については、を参照してください "リンクをクリックしてください"
  - * 所有者の変更 * - ファイルまたはフォルダの所有権が別のユーザーに変更されています。
  - * アクセス権の変更 * - ファイルまたはフォルダのアクセス権が変更されました。
  - * 作成 * - ファイルまたはフォルダを作成します。
  - * 削除 * - ファイルまたはフォルダを削除します。フォルダを削除すると、そのフォルダおよびサブフォルダ内のすべてのファイルについて、 _delete_events が取得されます。
  - * 読み取り *- ファイルが読み取られています。
  - * 読み取りメタデータ * - フォルダ監視オプションを有効にした場合のみ。Windows でフォルダを開くか、 Linux のフォルダ内で「 ls 」を実行すると、が生成されます。
  - * 名前の変更 * - ファイルまたはフォルダの名前を変更します。
  - * Write * - データはファイルに書き込まれます。
  - * メタデータの書き込み * - ファイルのメタデータが書き込まれます。たとえば、権限が変更された場

合などです。

- * その他の変更 * - 上記に記載されていないその他のイベント。マッピングされていないイベントはすべて、「その他の変更」アクティビティタイプにマッピングされます。ファイルおよびフォルダに適用されます。

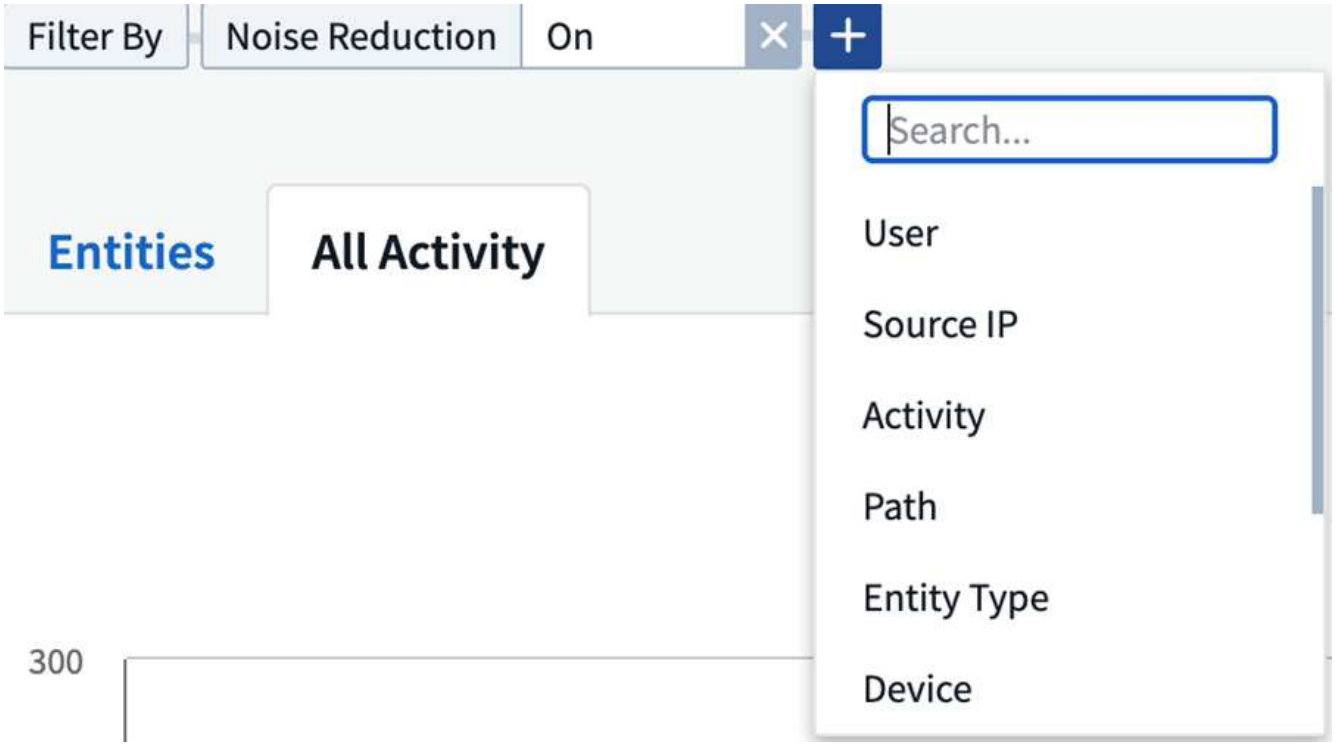
- へのリンクを持つエンティティへの * パス * "エンティティ詳細データ"
- エンティティタイプ * （エンティティ（ファイル）拡張子（ .doc 、 .docx 、 .tmp など）
- エンティティが存在する * デバイス *
- イベントの取得に使用される * プロトコル * 。
- 元のファイルの名前を変更したときに名前変更イベントに使用された * 元のパス * 。デフォルトでは、この列はテーブルに表示されません。列セレクタを使用して、この列をテーブルに追加します。
- エンティティが存在するボリューム * 。デフォルトでは、この列はテーブルに表示されません。列セレクタを使用して、この列をテーブルに追加します。

フォレンジックアクティビティ履歴データのフィルタリング

データのフィルタリングに使用できる方法は 2 つあります。

1. テーブルのフィールドにカーソルを合わせ、表示されるフィルタアイコンをクリックします。この値は、top_Filter by_list の適切なフィルタに追加されます。
2. 次のフィールドに「 _Filter By_field 」と入力して、データをフィルタリングします。

   [+]* ボタンをクリックして、 [フィルタ基準] ウィジェットから適切なフィルタを選択します。



   検索テキストを入力します

   Enter キーを押すか、フィルタボックスの外側をクリックしてフィルタを適用します。

フォレンジックアクティビティデータは、次のフィールドでフィルタできます。

- * アクティビティ * タイプ。
- * エンティティがアクセスされたソース IP * 。有効な送信元 IP アドレスを二重引用符で囲んで指定する必要があります（例：「 10.1.1.1 」）。 「 10.1.1.* 」、「 10.1.. 」などの不完全な IP は機能しません。
- * プロトコル * 。プロトコル固有のアクティビティを取得します。
- * アクティビティを実行しているユーザーのユーザー名 * 。フィルタリングするユーザ名を正確に指定する必要があります。部分的なユーザ名で検索したり、プレフィックスやサフィックスの付いたユーザ名の一部を検索したりすることはできません。
- * ユーザーが過去 2 時間に作成したファイルをフィルタリングするためのノイズリダクション * 。また、ユーザがアクセスする一時ファイル（ .tmp ファイルなど）をフィルタするためにも使用されます。
- アクティビティを実行しているユーザーの*ドメイン*。フィルタするには、* exact domain を指定する必要があります。部分ドメイン、または部分ドメインの先頭または末尾にワイルドカード(**")**が付いている部分ドメインを検索することはできません。_None_を指定すると、見つからないドメインを検索できます。

次のフィールドには、特別なフィルタルールが適用されます。

- エンティティタイプ（エンティティ（ファイル）拡張子を使用）-引用符で正確なエンティティタイプを指定することをお勧めします。例：「txt」_。
- エンティティのパス-ディレクトリパスフィルタ（/で終わるパス文字列）のパス*は、より高速な結果を得るために、最大4つのディレクトリの深さが推奨されます。例：*/home/userX/nested1/nested2/_or*"/home/userX/nested1/nested2/"_。詳細については、次の表を参照してください。
- *ユーザー*アクティビティの実行-引用符で正確なユーザーを指定することをお勧めします。たとえば、_"Administrator"_などです。
- * エンティティが存在するデバイス * （ SVM ）
- * 体積 * エンティティが存在する場所
- 元のファイルの名前を変更したときに名前変更イベントに使用された * 元のパス * 。

フィルタリングを行う場合、上記のフィールドは次のようになります。

- 正確な値は引用符で囲む必要があります。例： "searchtext"
- ワイルドカード文字列には引用符は含まれていません。例： searchtext 、 * searchtext * は、 'earchtext ' を含む文字列をフィルタします。
- プレフィックスが付いた文字列、たとえば searchtext* は、「 earchtext 」で始まる文字列を検索します。

アクティビティフォレンジックフィルタの例：

ユーザが適用したフィルタ式	予想される結果	パフォーマンス評価	コメント（**Comment**）
path=/home/userX/nested1/nested2/または/home/userX/nested1/nested2/*または"/home/userX/nested1/nested2/"	指定したディレクトリの下にあるすべてのファイルとフォルダの再帰的検索	高速	最大4つのディレクトリの検索が高速になります。
path=/home/userX/nested1/または/home/userX/nested1/*または/home/userX/nested1/	指定したディレクトリの下にあるすべてのファイルとフォルダの再帰的検索	高速	最大4つのディレクトリの検索が高速になります。
path=/home/userX/nested1/test *または/home/userX/nested1/test	指定されたパス正規表現の下にあるすべてのファイルおよびフォルダの再帰的検索（test *はファイルまたはディレクトリ、あるいはその両方を意味する）	遅い	ディレクトリ+ファイル正規表現検索は、ディレクトリ検索と比較して検索に時間がかかります。
path=/home/userX/nested1/nested2/nested3/or /home/userX/nested1/nested2/nested3/* or "/home/userX/nested1/nested2/nested3/"	指定したディレクトリの下にあるすべてのファイルとフォルダの再帰的検索	遅い	4つ以上のディレクトリ検索は、検索に時間がかかります。
パス=* userX/nested1/test *	指定されたワイルドカードパス文字列の下にあるすべてのファイルおよびフォルダの再帰的検索（test *はファイルまたはディレクトリ、あるいはその両方を意味します）	最も遅い	先頭のワイルドカード検索は、最も低速な検索です。
その他のパスベース以外のフィルタ。UserとEntity Typeのフィルタは引用符で囲むことをお勧めします。例：User="Administrator" Entity Type="txt"		高速	

注：

1. 選択した時間範囲が3日を超える場合、[すべてのアクティビティ]アイコンの横に表示されるアクティビティ数は30分に四捨五入されます。たとえば、_ 9月1日10：15 ~ 9月7日10：15 AM_の時間範囲には、9月1日10：00 ~ 9月7日10：30のアクティビティ数が表示されます。
2. 同様に、[Activity Types]、[Activity on Entity Types]、[Activity History]グラフに表示されるカウントメトリックは、選択した期間が3日を超える場合は30分に切り捨てられます。

フォレンジックアクティビティ履歴データのソート

アクティビティ履歴データは、_Time、User、Source IP、Activity、_and_Entity Type _でソートできます。デフォルトでは、テーブルは descending _Time_order でソートされます。つまり、最新のデータが最初に表示されます。_Device_Field と _Protocol_fields に対してソートが無効になっています。

非同期エクスポートのユーザガイド

概要

Storage Workload Securityの非同期エクスポート機能は、大規模なデータエクスポートを処理するように設計されています。

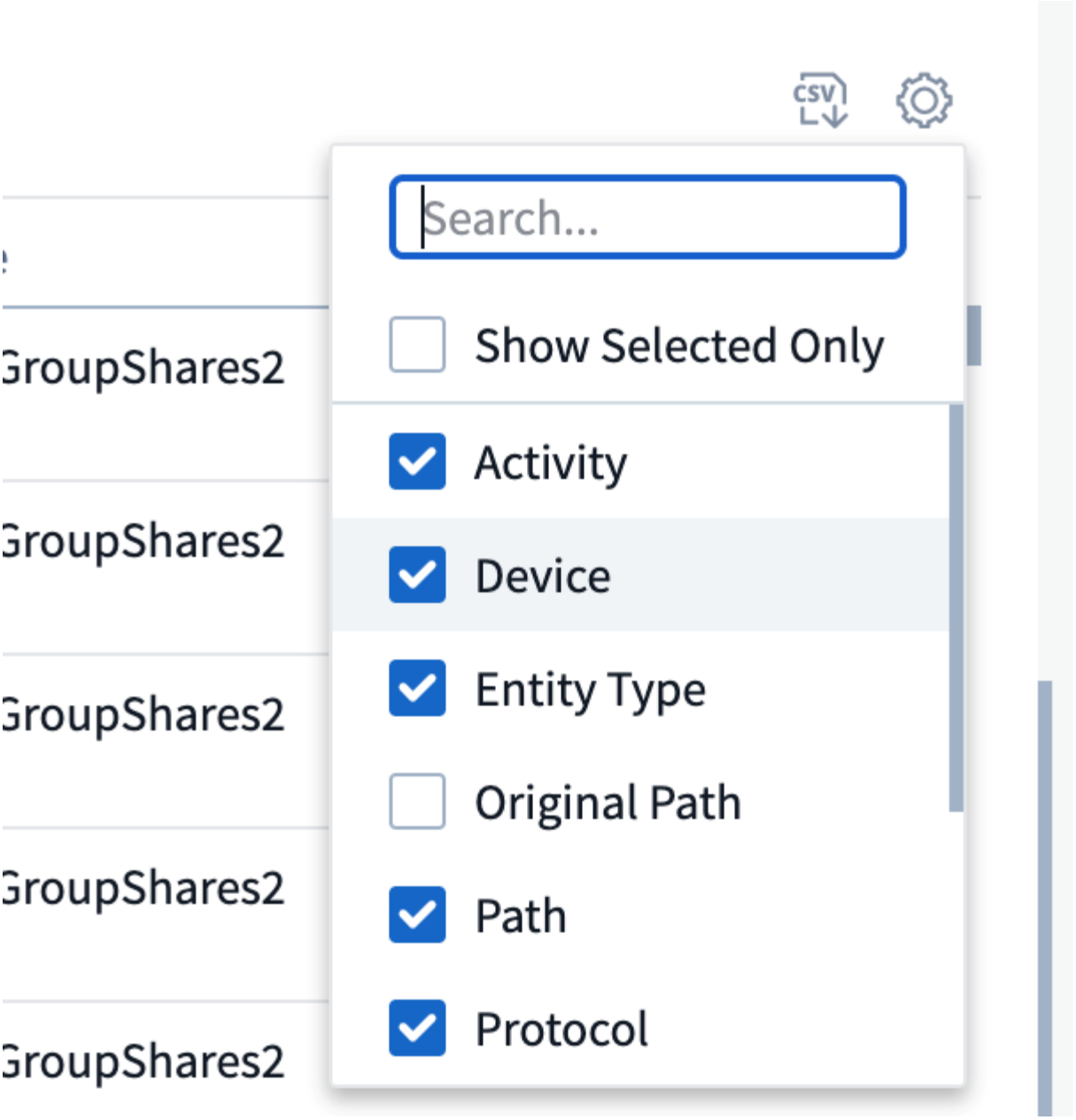
ステップバイステップガイド：非同期エクスポートを使用したデータのエクスポート

1. エクスポートの開始：エクスポートの所要時間とフィルタを選択し、エクスポートボタンをクリックします。
2. エクスポートが完了するのを待ちます：処理時間は数分から数時間の範囲で指定できます。フォレンジックページを数回更新する必要がある場合があります。エクスポートジョブが完了すると、[Download last export CSV file]ボタンが有効になります。
3. ダウンロード:「最後に作成したエクスポートファイルをダウンロード」ボタンをクリックして、エクスポートされたデータを.zip形式で取得します。このデータは、ユーザーが別の非同期エクスポートを開始するまで、または3日が経過するまで（いずれか早い方）ダウンロードできます。このボタンは、別の非同期エクスポートが開始されるまで有効のままです。
4. 制限事項：
    - 非同期ダウンロードの数は、現在、ユーザあたり1つ、テナントあたり3つに制限されています。
    - エクスポートされるデータは、最大100万レコードに制限されます。

APIを介してフォレンジックデータを抽出するサンプルスクリプトは、NetAppエージェントの_/opt/apl/cloudsecure/agent/export-script /_にあります。スクリプトの詳細については、この場所にあるreadmeを参照してください。

すべてのアクティビティの列を選択します

すべての activity テーブルには ' デフォルトで SELECT カラムが表示されます列を追加、削除、または変更するには、テーブルの右側にある歯車アイコンをクリックし、使用可能な列のリストから選択します。



アクティビティ履歴の保持

アクティビティ履歴は、アクティブなワークロードセキュリティ環境で13カ月間保持されます。

Forensicsページのフィルタの適用性

フィルタ	機能	例	これらのフィルタに適用可能	これらのフィルタには適用されません	結果
* （アスタリスク）	すべての項目を検索できます	Auto * 03172022 検索テキストにハイフンまたはアンダースコアが含まれている場合は、角かっこで式を指定します。例：SVM-123の検索には（SVM*）を使用します。	ユーザー、パス、エンティティタイプ、デバイス、ボリューム、元のパス		"Auto"で始まり、"03172022"で終わるすべてのリソースを返します。
？（疑問符）	では、特定の数の文字を検索できます	AutoSabotageUser1_03172022	ユーザー、エンティティタイプ、デバイス、ボリューム		AutoSabotageUser1_03172022A、AutoSabotageUser1_03172022B、AutoSabotageUser1_03172025などを返します
または	複数のエンティティを指定できます	AutoSabotageUser1_03172022またはAutoRansomUser4_03162022	ユーザー、ドメイン、パス、エンティティタイプ、元のパス		AutoSabotageUser1_03172022またはAutoRansomUser4_03162022のいずれかを返します
ありません	検索結果からテキストを除外できます	AutoRansomUser4_03162022ではありません	ユーザー、ドメイン、パス、エンティティタイプ、元のパス	デバイス	"AutoRansomUser4_03162022 "で始まるものをすべて返します。
なし	すべてのフィールドで NULL 値を検索します	なし	ドメイン		ターゲットフィールドが空の場合に結果を返します

パス/元のパスの検索

検索結果に/が含まれている場合と含まれていない場合は異なります

/AutoDir1/AutoFile	動作します
AutoDir1/AutoFileです	壊れています
/AutoDir1/AutoFile（Dir1）	dir1部分部分文字列が機能しない
"/AutoDir1/AutoFile032420222022"	完全検索が実行されます
Auto * 03242022	壊れています

AutoSabotageUser1_03172022	壊れています
/AutoDir1/AutoFile03242022または/AutoDir1/AutoFile03242022	動作します
/AutoDir1/AutoFile03242022ではありません	動作します
NOT / AutoDir1	動作します
/AutoFile03242022はありません	壊れています
*	すべてのエントリを表示します

ローカルルート**SVM**ユーザアクティビティの変更

ローカルルートSVMユーザが何らかのアクティビティを実行している場合、NFS共有がマウントされているクライアントのIPがユーザ名で考慮されるようになりました。フォレンジックアクティビティとユーザアクティビティの両方のページで、root@<ip-address-of-the-client>と表示されます。

例：

- SVM-1がワークロードセキュリティによって監視されていて、そのSVMのrootユーザがIPアドレスが10.197.12.40のクライアントに共有をマウントした場合、フォレンジックアクティビティページに表示されるユーザ名は_root@10.197.12.40_になります。
- IPアドレスが10.197.12.41の別のクライアントに同じSVM-1がマウントされている場合、フォレンジックアクティビティページに表示されるユーザ名は_root@10.197.12.41_になります。

*•これは、NFS rootユーザーのアクティビティをIPアドレスごとに分離するために行われます。以前は、すべてのアクティビティは_root_userによってのみ実行され、IPの区別はありませんでした。

トラブルシューティング

問題	試してみてください
[All Activities]テーブルの[User]列には、ユーザ名が次のように表示されます。 LDAP：HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” または 「LDAP：デフォルト：80038003」	考えられる原因は次のとおりです。 1.ユーザディレクトリコレクタがまだ設定されていません。追加するには、**[**ワークロードセキュリティ**]>[**コレクタ**]>[**ユーザディレクトリコレクタ**]***に移動し、[+ユーザディレクトリコレクタ]*をクリックします。Active Directory_or_LDAP ディレクトリサーバー_ を選択します。 2. ユーザディレクトリコレクタは設定されていますが、停止しているか、エラー状態です。[コレクタ]>[ユーザディレクトリコレクタ]*に移動し、ステータスを確認してください。を参照してください "User Directory Collector のトラブルシューティング" トラブルシューティングのヒントについては、ドキュメントのセクションを参照してください。 適切に設定すると、 24 時間以内に名前が自動的に解決されます。 それでも解決されない場合は、正しい User Data Collector を追加しているかどうかを確認します。追加した Active Directory / LDAP ディレクトリサーバにユーザが実際に含まれていることを確認します。

一部の NFS イベントが UI に表示されません。	次の点を確認します。 1. POSIX属性が設定されたADサーバのユーザディレクトリコレクタが、UIからunixid属性を有効にして実行されている必要があります。 2. NFSアクセスを実行しているすべてのユーザは、UIからユーザページで検索したときに表示されます 3. rawイベント（ユーザがまだ検出されていないイベント）はNFSではサポートされていません 4. NFSエクスポートへの匿名アクセスは監視されません。 5. NFSバージョンがNFS4.1未満で使用されていることを確認します。
Forensics_All Activity_or_Entities_pagesのフィルタにアスタリスク(*)などのワイルドカード文字を含む文字を入力すると、ページのロードに時間がかかります。	検索文字列にアスタリスク（*）を付けると、すべてが検索されます。ただし、*<*searchTerm*> or *<*searchTerm*>*_のような先頭のワイルドカード文字列は、クエリに時間がかかります。パフォーマンスを向上させるには、代わりに<searchTerm>*という形式でプレフィックス文字列を使用します（つまり、検索用語としてアスタリスク***()_after_a***を追加します）。例： testvolume_or_* test * volume__ではなく、文字列_testvolume *_を使用します。ディレクトリ検索を使用して、指定したフォルダの下にあるすべてのアクティビティを再帰的に表示します(階層検索)。たとえば、/path1/path2/path3/or "/path1/path2/path3/"は、すべてのアクティビティを/path1/path2/path3の下に再帰的に表示します。または、[すべてのアクティビティ]タブの[フィルタに追加]オプションを使用します。
パスフィルタを使用すると、「Request failed with status code 500/503」というエラーが発生します。	レコードのフィルタリングには、より小さい日付範囲を使用してみてください。
_path_filterを使用すると、Forensic UIでデータのロードに時間がかかります。	ディレクトリパスフィルタ(/で終わるパス文字列)より高速な結果を得るには、最大4つのディレクトリの深さが推奨されます。たとえば、ディレクトリパスが/Aaa/Bbb/Ccc/Dddの場合は、/Aaa/Bbb/Ccc/Ddd/または「/Aaa/Bbb/Ccc/Ddd/」を検索して、データをより高速にロードしてみてください。

フォレンジックエンティティページ

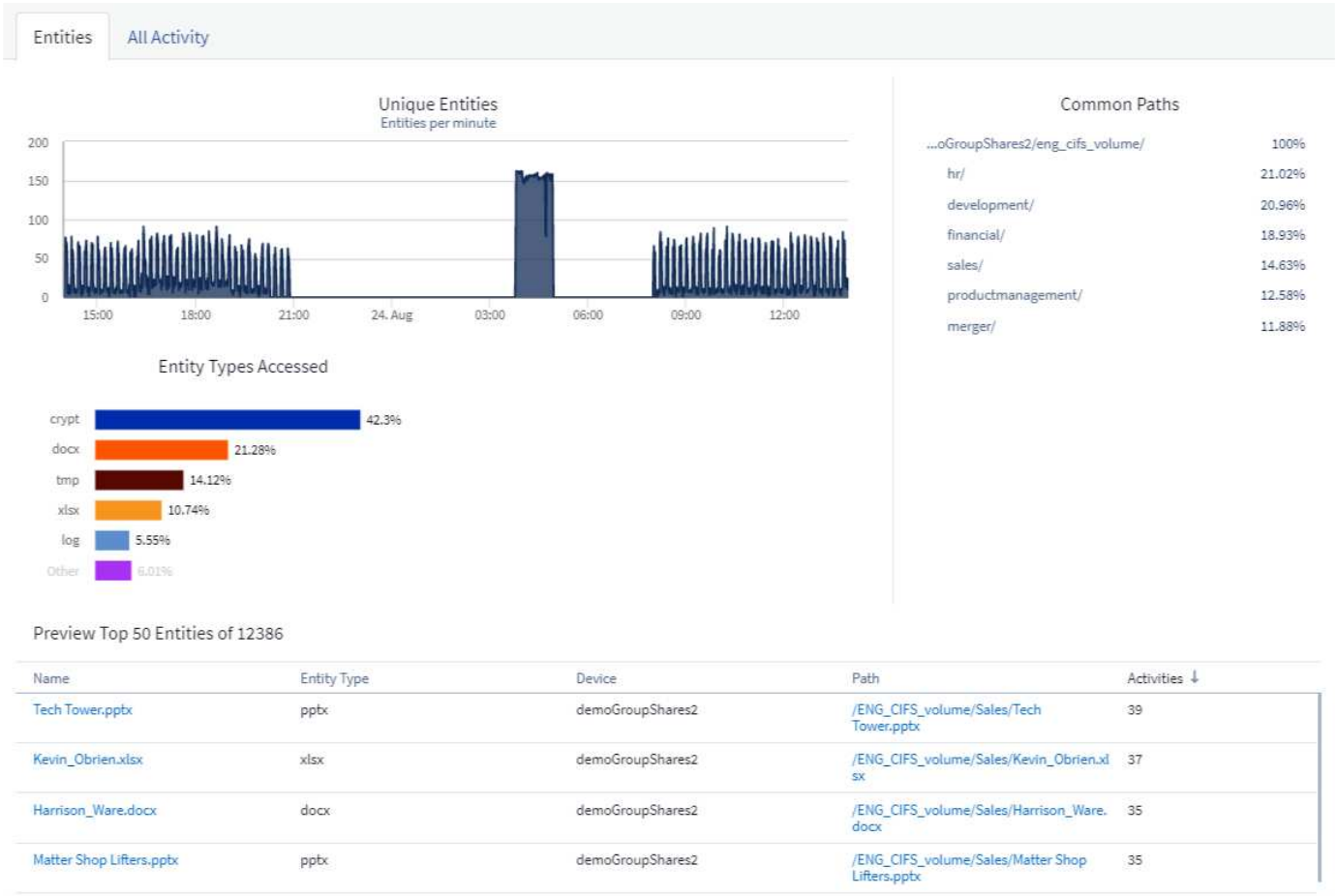
フォレンジックエンティティページには、環境内のエンティティアクティビティに関する詳細情報が表示されます。

エンティティ情報の検査

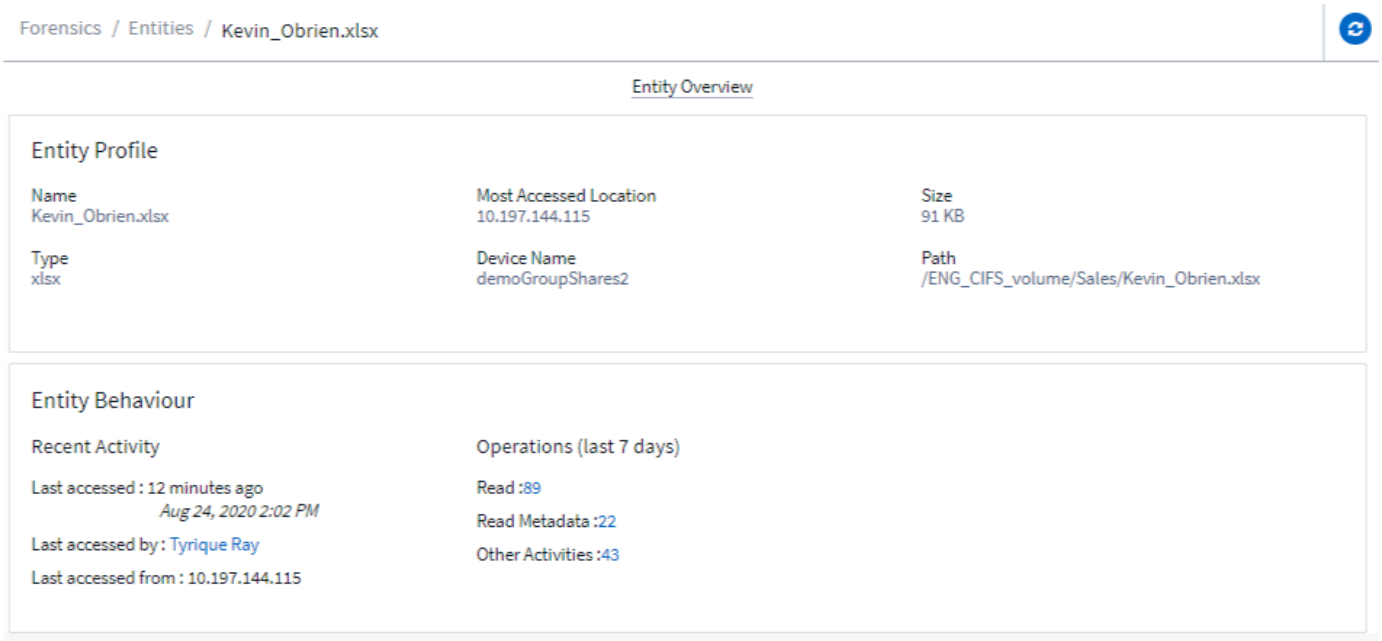
- Forensics > Activity Forensics * をクリックし、 *Entities* タブをクリックして Entities ページにアクセスします。

このページには、環境内のエンティティアクティビティの概要が表示され、次の情報が強調表示されます。
* 1分あたりの_unique Entities_accessedを示すグラフ
*アクセスされたエンティティタイプ_のグラフ

*_Common Paths_の内訳
*エンティティの総数のうち_Top 50 Entities_outのリスト



リスト内のエンティティをクリックすると、エンティティの概要ページが開き、エンティティのプロファイルに名前、タイプ、デバイス名、最もアクセスされる場所の IP 、パスなどの詳細、およびユーザ、 IP 、 エンティティが最後にアクセスされた時刻です。



Forensic User の概要

各ユーザーの情報については、「ユーザー概要」を参照してください。これらのビューを使用して、ユーザの特性、関連付けられたエンティティ、および最近のアクティビティを把握できます。

ユーザプロファイル

ユーザプロファイル情報には、ユーザの連絡先情報と場所が含まれます。プロファイルには次の情報が表示されます。

- ユーザの名前
- ユーザの E メールアドレス
- ユーザーのマネージャー
- ユーザの電話連絡先
- ユーザの場所

ユーザの動作

ユーザの動作情報には、最近実行したアクティビティと処理が含まれます。これには次の情報が含まれ

- 最近のアクティビティ
  - 最終アクセス場所
  - アクティビティグラフ
  - アラート
- 過去 7 日間の処理
  - 処理数

更新間隔

ユーザーリストは 12 時間ごとに更新されます。

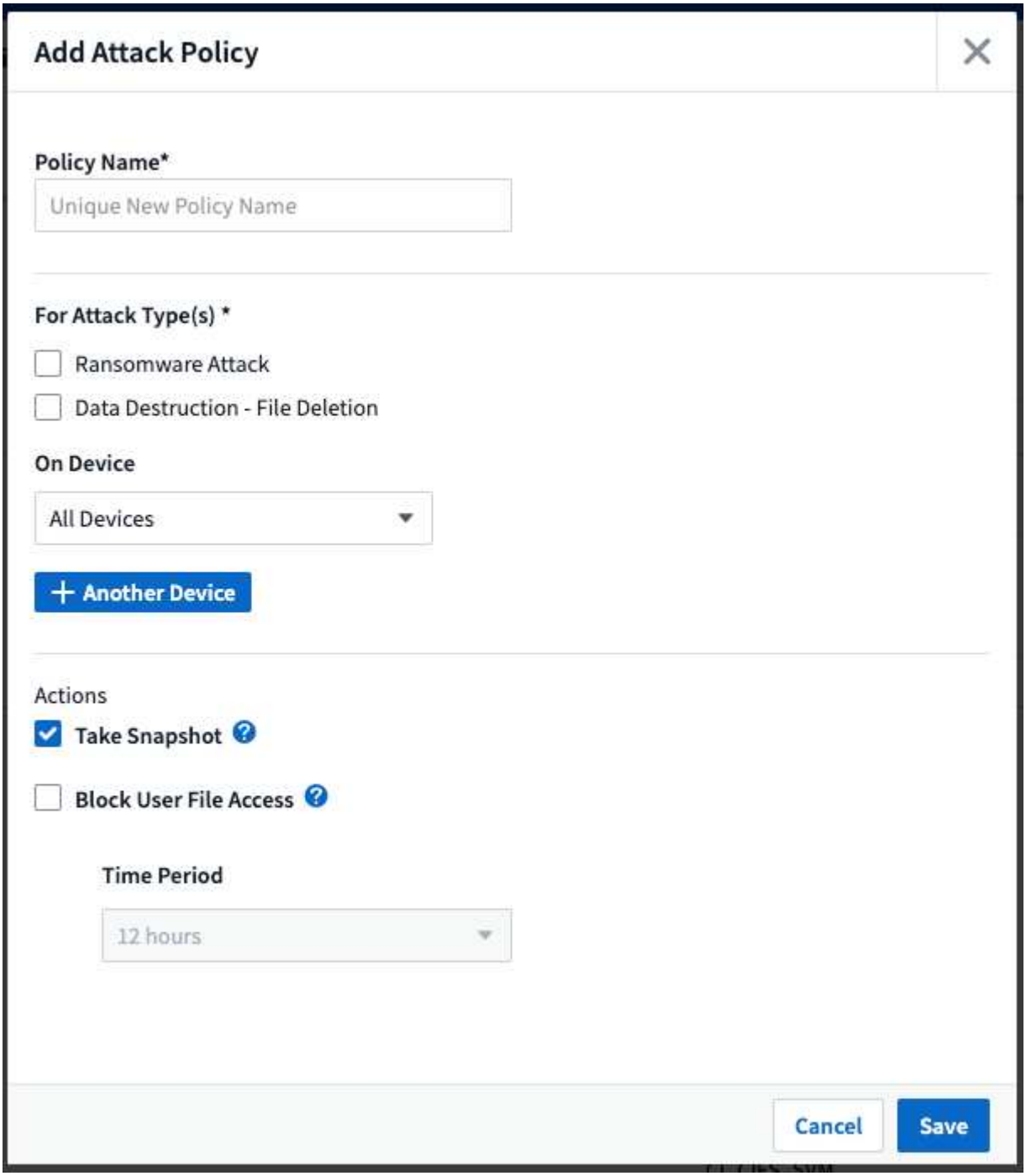
保持ポリシー

再更新されない場合、ユーザリストは 13 カ月間保持されます。13 カ月を過ぎると、データは削除されます。ワークロードセキュリティ環境を削除すると、その環境に関連付けられているすべてのデータが削除されます。

自動応答ポリシー

応答ポリシーは、スナップショットの作成や、攻撃や異常なユーザ動作が発生した場合のユーザアクセスの制限などのアクションをトリガーします。

特定のデバイスまたはすべてのデバイスにポリシーを設定できます。応答ポリシーを設定するには、* Admin > Automated Response Policies を選択し、適切な+ Policy *ボタンをクリックします。攻撃または警告のポリシーを作成できます。



ポリシーは一意の名前で保存する必要があります。

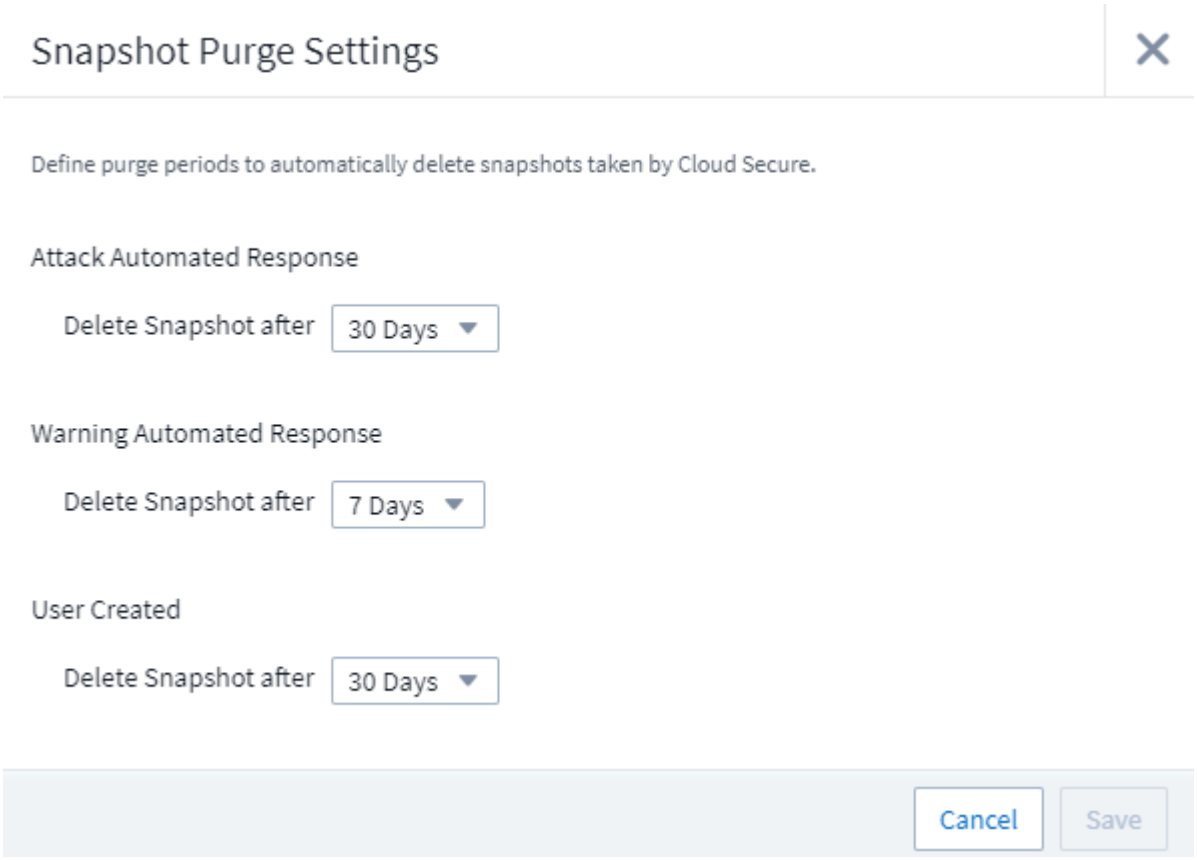
自動応答アクションを無効にする（例： Take Snapshot ）には、アクションをチェック解除してポリシーを保存するだけです。

指定されたデバイス（または選択されている場合はすべてのデバイス）に対してアラートがトリガーされると、自動応答ポリシーによってデータのスナップショットが作成されます。Snapshot のステータスは、で確認できます "アラートの詳細ページ"。

を参照してください "ユーザアクセスの制限" IP によるユーザアクセスの制限の詳細については、ページを参照してください。

自動応答ポリシーを変更または一時停止するには、ポリシーのドロップダウンメニューでオプションを選択します。

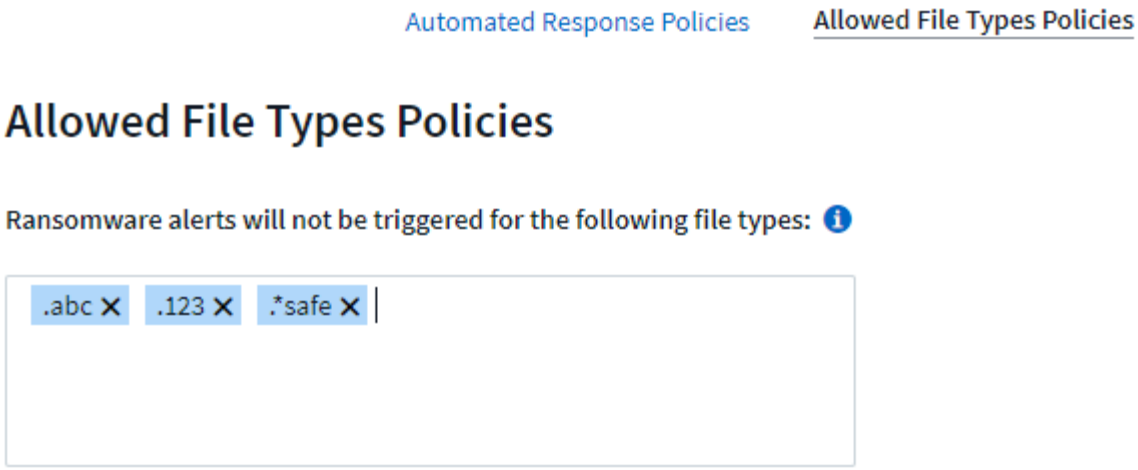
ワークロードセキュリティでは、Snapshotの削除設定に基づいて、Snapshotが1日に1回自動的に削除されます。



許可されたファイルタイプポリシー

既知のファイル拡張子に対するランサムウェア攻撃が検出され、[Alerts]画面でアラートが生成されている場合は、そのファイル拡張子を_allowedファイルtypes_listに追加して不要なアラートを防ぐことができます。

[Workload Security]>[Policies]*に移動し、[_Allowed File Type Policies]タブに移動します。



一度_allowedファイルtypes_listに追加されると、その許可されたファイルタイプに対してランサムウェア攻撃アラートは生成されません。_allowed File types_policyはランサムウェアの検出にのみ適用されることに注意してください。

たとえば、*test.txt_*という名前のファイルが*_test.txt.abc_*に変更され、.abc_拡張子によってランサムウェア攻撃が検出された場合、*.abc_*拡張子を*_allowed*ファイル*types_list*に追加できます。リストに追加されると、拡張子が.abc_のファイルに対するランサムウェア攻撃は生成されなくなります。

許可されるファイルタイプには、完全一致（例：".abc"）または式（例：".**type**"、"**.type**"、または"**type**"）を指定できます。タイプ「. a * c」、「. p * f」の式はサポートされていません。

ONTAP によるランサムウェア対策との統合

ONTAP の自律的ランサムウェア対策（ARP）機能は、NAS（NFSおよびSMB）環境におけるワークロード分析を使用して、ランサムウェア攻撃を示す可能性のある異常なインファイルアクティビティをプロアクティブに検出して警告します。

ARPに関する詳細およびライセンス要件については、を参照してください "こちらをご覧ください"。

ワークロードセキュリティは、ONTAP と統合してARPイベントを受信し、追加の分析と自動応答レイヤを提供します。

ワークロードセキュリティは、ONTAP からARPイベントを受信し、次の処理を行います。

1. ボリューム暗号化イベントとユーザアクティビティを関連付けて、破損の原因となっているユーザを特定します。
2. 自動応答ポリシーを実装する（定義されている場合）
3. フォレンジック機能を提供：
    - お客様がデータ侵害の調査を実施できるようにします。
    - 影響を受けたファイルを特定し、迅速なリカバリとデータ侵害の調査に役立ちます。

前提条件

1. 最小ONTAP バージョン：9.11.1
2. ARPが有効なボリューム。ARPをイネーブルにする方法の詳細は、を参照してください "こちらをご覧ください"。 ARPは、OnCommand システムマネージャを介して有効にする必要があります。ワークロードセキュリティでARPを有効にすることはできませ
3. ワークロードセキュリティコレクタはクラスタIPを介して追加する必要があります。
4. この機能を使用するには、クラスタレベルのクレデンシャルが必要です。つまり、SVMを追加するときはクラスタレベルのクレデンシャルを使用する必要があります。

ユーザ権限が必要です

クラスタ管理者のクレデンシャルを使用している場合、新しい権限は不要です。

ユーザに付与された権限でカスタムユーザ（_csuser_など）を使用している場合は、次の手順に従ってワークロードセキュリティにアクセス許可を付与し、ONTAP からARP関連情報を収集します。

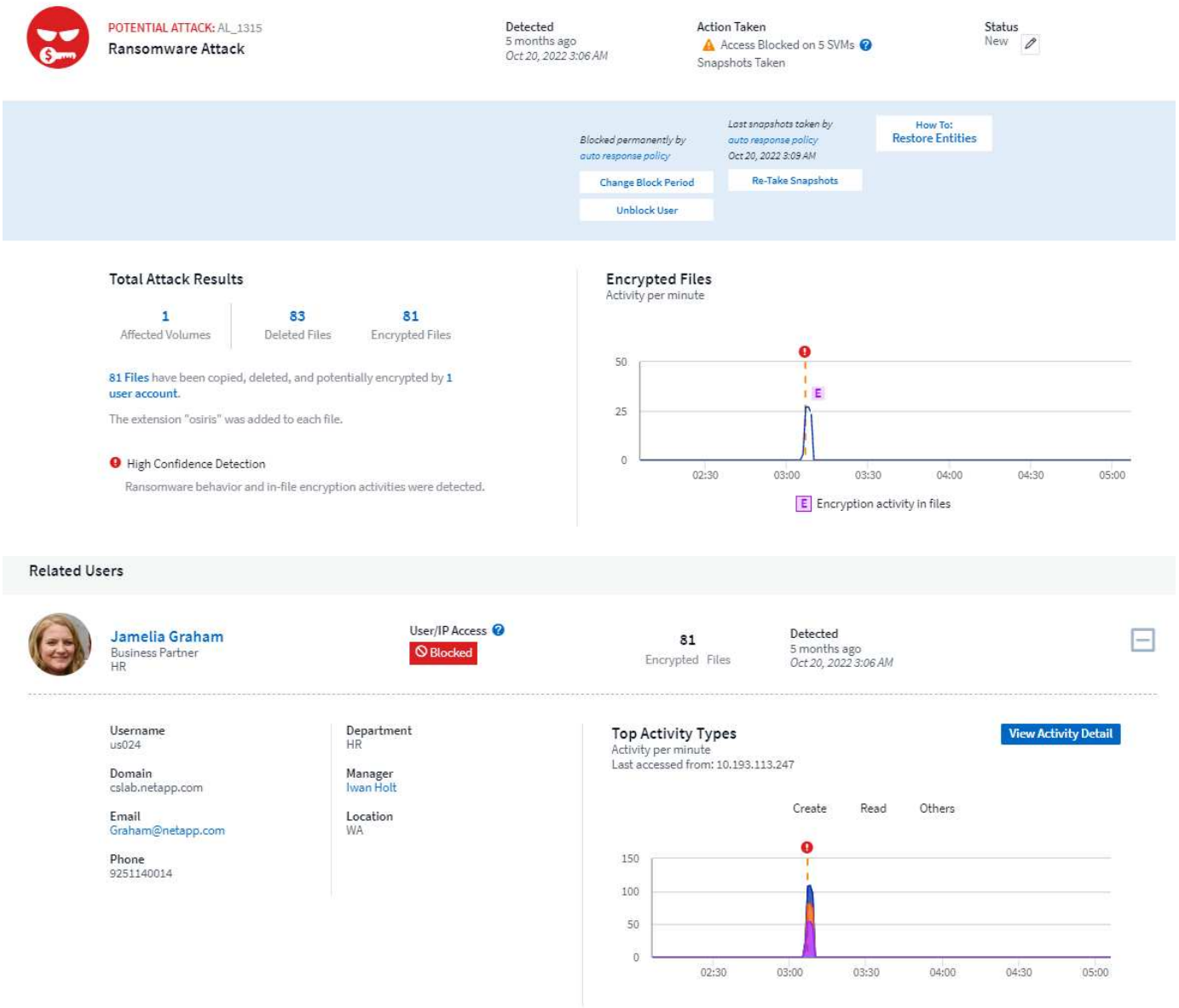
クラスタクレデンシャルを使用する_csuser_withの場合、ONTAP コマンドラインから次の操作を実行します。

```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly  -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

その他の設定について詳しくは、こちらをご覧ください "ONTAP 権限"。

アラートの例

ARPイベントにより生成されたアラートの例を次に示します。



信頼性の高いバナーは、攻撃がランサムウェアの挙動とファイル暗号化のアクティビティを示していることを示しています。
暗号化ファイルのグラフには、ARP解決策 によってボリューム暗号化アクティビティが検出されたタイムスタンプが示されます。

制限

SVMがワークロードセキュリティで監視されていないものの、ONTAP によって生成されたARPイベントがある場合、ワークロードセキュリティはイベントを受信して表示します。ただし、アラートに関連するフォレンジック情報およびユーザーマッピングはキャプチャまたは表示されません。

トラブルシューティング

既知の問題とその解決策を次の表に示します。

問題	解決策：
電子メールアラートは、攻撃が検出されてから24時間後に受信されます。UIでは、その24時間前にData Infrastructure Insights Workload SecurityがEメールを受信するとアラートが表示されます。	ONTAPがData Infrastructure Insights Workload Security（ワークロードセキュリティ）に_Ransomware Detected_Eventを送信すると、Eメールが送信されます。イベントには、攻撃のリストとタイムスタンプが含まれます。Workload Security UIには、攻撃を受けた最初のファイルのアラートタイムスタンプが表示されます。ONTAPは、一定数のファイルがエンコードされると、_Ransomware Detected_EventをData Infrastructure Insightsに送信します。そのため、UIにアラートが表示される時間とEメールが送信される時間が異なる場合があります。

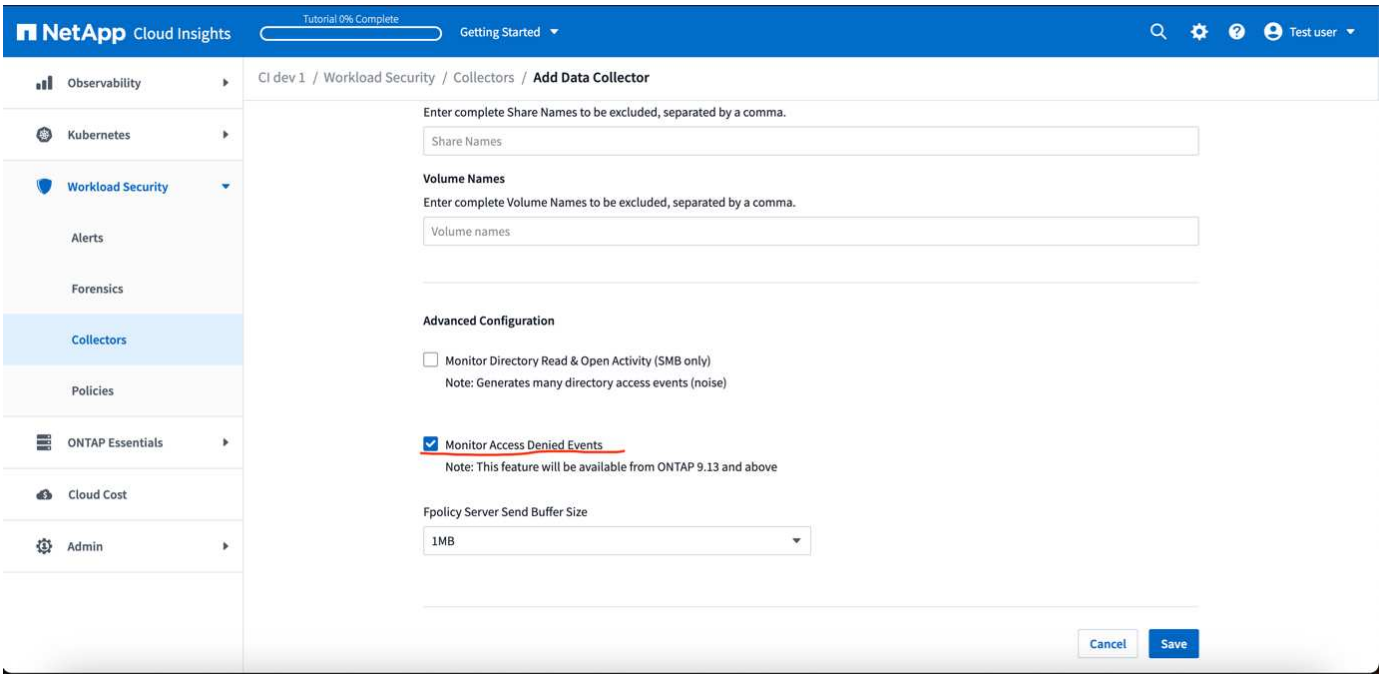
ONTAPアクセス拒否との統合

ONTAPアクセス拒否機能は、NAS環境（NFSおよびSMB）のワークロード分析を使用して、失敗したファイル処理（権限のない処理を実行しようとしているユーザなど）をプロアクティブに検出して警告します。これらのファイル操作の失敗の通知は、特にセキュリティ関連の障害の場合には、初期段階でのインサイダー攻撃のブロックにさらに役立ちます。

データインフラストラクチャインサイトワークロードセキュリティは、ONTAPと統合してアクセス拒否イベントを受信し、追加の分析および自動応答レイヤを提供します。

前提条件

- ONTAPの最小バージョン：9.13.0
- ワークロードセキュリティ管理者は、新しいコレクタの追加時または既存のコレクタの編集時に、[Advanced Configuration]の下にある[*Monitor Access Denied Events*]チェックボックスをオンにして、アクセス拒否機能を有効にする必要があります。



ユーザ権限が必要です

クラスタ管理資格情報を使用してData Collectorを追加する場合、新しい権限は必要ありません。

ユーザに付与された権限を持つカスタムユーザ（_csuser_など）を使用してコレクタを追加する場合は、次の手順に従って、ONTAPでアクセス拒否イベントに登録するために必要な権限をワークロードセキュリティに付与します。

CSUSER WITH_CLUSTER_CREDENTIALの場合は、ONTAPコマンドラインから次のコマンドを実行します。_csrestrole_はカスタムロールで、_csuser_はONTAPカスタムユーザです。

```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

csuser with _svm_credentialsの場合は、ONTAPコマンドラインから次のコマンドを実行します。

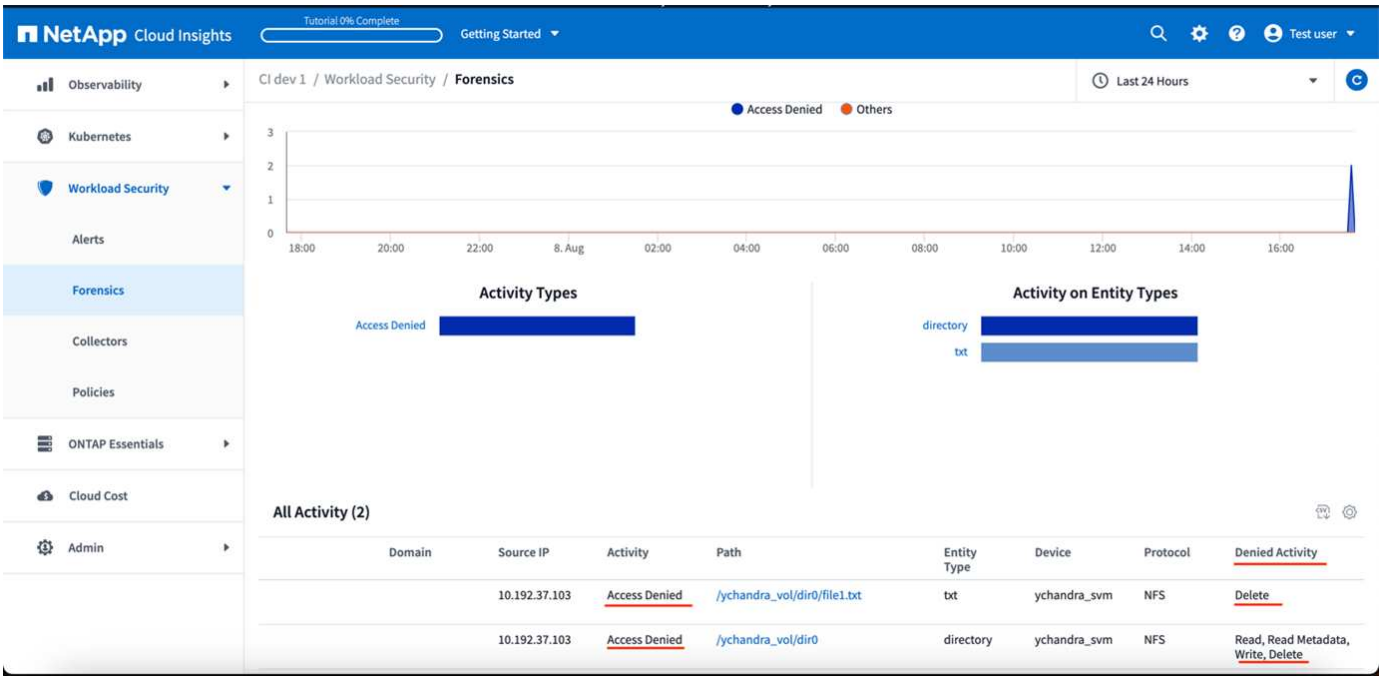
```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

その他の設定について詳しくは、こちらをご覧ください "ONTAP 権限"。

アクセス拒否イベント

ONTAPシステムからイベントが取得されると、[ワークロードセキュリティフォレンジック]ページにアクセス

拒否イベントが表示されます。表示される情報に加えて、歯車アイコンから_desired Activity_columnをテーブルに追加することで、特定の操作で不足しているユーザー権限を表示できます。



ユーザアクセスをブロックしています

攻撃が検出されると、ワークロードセキュリティは、ファイルシステムへのユーザーアクセスをブロックすることで攻撃を停止できます。アクセスは、自動応答ポリシーを使用して自動的にブロックするか、アラートまたはユーザの詳細ページから手動でブロックできます。

ユーザアクセスをブロックする場合は、ブロック期間を定義する必要があります。選択した期間が終了すると、ユーザアクセスが自動的にリストアされます。
アクセスブロックは、SMBプロトコルとNFSプロトコルの両方でサポートされています。

SMBおよびホストマシンのIPアドレスに対してユーザが直接ブロックされているため、NFSに対して攻撃がブロックされます。これらのマシンのIPアドレスは、ワークロードセキュリティで監視されているいずれかのStorage Virtual Machine（SVM）へのアクセスがブロックされます。

たとえば、ワークロードセキュリティでは10個のSVMを管理し、自動応答ポリシーでは4つのSVMを設定するとします。攻撃の原因が4つのSVMのいずれかである場合、10個のSVMすべてでユーザのアクセスがブロックされます。元の SVM では引き続き Snapshot が作成されます。

SMB用に設定されたSVMが4つあり、NFS用に設定されたSVMが残り2つのSVMがNFSとSMB両方に対して設定されている場合、4つのSVMのいずれかで攻撃が発生すると、すべてのSVMがブロックされます。

ユーザアクセスブロックの前提条件

この機能を使用するには、クラスタレベルのクレデンシャルが必要です。

クラスタ管理者のクレデンシャルを使用している場合、新しい権限は不要です。

ユーザに付与された権限でカスタムユーザ（_csuser_など）を使用している場合は、次の手順に従ってワークロードセキュリティにユーザをブロックする権限を付与します。

クラスタクレデンシャルを持つ csuser の場合、 ONTAP コマンドラインから次の手順を実行します。

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

の[Permissions]セクションを確認してください。 "ONTAP SVM Data Collector の設定" ページも参照してください。

機能を有効にする方法

- [Workload Security]で、**[Workload Security]>[Policies]>[Automated Response Policies]***に移動します。 **[**+ Attack Policy]*を選択します。
- [_Block User File Access]を選択（チェック）します。

自動ユーザアクセスブロックの設定方法

- 新しい攻撃ポリシーを作成するか、既存の攻撃ポリシーを編集します。
- 攻撃ポリシーを監視する SVM を選択します。
- [ユーザーファイルアクセスをブロックする]チェックボックスをオンにします。この機能は、このオプションを選択すると有効になります。
- [Time Period]で、ブロッキングを適用する時間を選択します。
- 自動ユーザブロッキングをテストするには、を使用して攻撃をシミュレートします "シミュレートされたスクリプト"。

システム内にブロックされているユーザーがいるかどうかを確認する方法

- アラートリストページでは、ユーザがブロックされた場合に画面上部のバナーが表示されます。
- バナーをクリックすると、[Users]ページが表示され、ブロックされているユーザのリストが表示されます。
- [Users]ページには、「User/IP Access」という名前のカラムがあります。この列には、ユーザブロッキングの現在の状態が表示されます。

ユーザアクセスを手動で制限および管理します

- アラートの詳細画面またはユーザの詳細画面に移動して、これらの画面からユーザを手動でブロックまた

は復元できます。

ユーザアクセス制限履歴

［アラートの詳細とユーザーの詳細］ページのユーザーパネルで、ユーザーのアクセス制限履歴（時間、アクション（ブロック、ブロック解除）、期間、実行されたアクション）の監査を表示できます。 手動/自動、およびNFSの影響を受けるIP。

機能を無効にする方法

この機能はいつでも無効にできます。システム内に制限のあるユーザがいる場合は、アクセスを先にリストアする必要があります。

- [Workload Security]で、**[Workload Security]>[Policies]>[Automated Response Policies]***に移動します。 **[**+ Attack Policy]*を選択します。
- [_Block User File Access]の選択を解除します（オフにします）。

この機能はすべてのページで非表示になります。

NFSのIPを手動でリストア

ワークロードセキュリティトライアルの期限が切れた場合、またはエージェント/コレクタがダウンした場合に、ONTAP からIPを手動で復元するには、次の手順を実行します。

1. SVM のすべてのエクスポートポリシーをリストします。

```
contrail-qa-fas8020::> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0         default         1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm1         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm3         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
4 entries were displayed.
```

2. 「cloudsecure_rule」をクライアント一致として持つSVMのすべてのポリシーのルールを削除するには、対応するRuleIndexを指定します。通常、ワークロードのセキュリティルールは1になります。

```
 contrail-qa-fas8020::*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
```

.
ワークロードセキュリティルールが削除されていることを確認します（確認のためのオプションの手順）。

```
contrail-qa-fas8020::*> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- --------------------
---------
svm0         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
2 entries were displayed.
```

SMBのユーザを手動でリストア

ワークロードセキュリティトライアルの期限が切れた場合、またはエージェント/コレクタがダウンした場合に、ONTAP からユーザーを手動で復元するには、次の手順を実行します。

ワークロードセキュリティでブロックされたユーザーのリストは、ユーザーリストページから取得できます。

1. cluster_admin_credentialsを使用してONTAP クラスタ（ユーザのブロックを解除する場所）にログインします。（Amazon FSXの場合、FSXクレデンシャルを使用してログインします）。
2. 次のコマンドを実行して、すべてのSVMのSMBワークロードセキュリティでブロックされているすべてのユーザを表示します。

```
vserver name-mapping show -direction win-unix -replacement " "
```

```
Vserver:   <vservername>
Direction: win-unix
Position Hostname         IP Address/Mask
-------- ---------------- ----------------
1       -                -                    Pattern: CSLAB\\US040
                                          Replacement:
2       -                -                    Pattern: CSLAB\\US030
                                          Replacement:
2 entries were displayed.
```

上記の出力では、2人のユーザーがドメインCSLABでブロックされました（US030、US040）。

1. 上記の出力から位置を特定したら、次のコマンドを実行してユーザーのブロックを解除します。

```
 vserver name-mapping delete -direction win-unix -position <position>
```

. コマンドを実行して、ユーザがブロックされていないことを確認します。

```
vserver name-mapping show -direction win-unix -replacement " "
```

以前にブロックしたユーザに対しては、エントリは表示されません。

トラブルシューティング

問題	試してみてください
一部のユーザーは制限されていませんが、攻撃があります。	1. SVMのData CollectorとAgentがin_running_stateであることを確認します。Data CollectorとAgentが停止している場合、ワークロードセキュリティはコマンドを送信できません。 2. これは、ユーザが以前に使用されていない新しい IP を持つマシンからストレージにアクセスした可能性があるためです。 制限は、ユーザがストレージにアクセスする際に使用するホストの IP アドレスを介して行われます。UI （ Alert Details > Access Limitation History for this User > Affected IP ）で、制限されている IP アドレスのリストを確認します。IP が制限された IP と異なるホストからストレージにアクセスしている場合、ユーザは制限されていない IP を介してストレージにアクセスできます。IP が制限されているホストからアクセスしようとすると、ストレージにアクセスできなくなります。
[Restrict Access] を手動でクリックすると、「このユーザの IP アドレスはすでに制限されています」というメッセージが表示されます。	制限する IP はすでに別のユーザから制限されています。
ポリシーを変更できませんでした。理由：このコマンドは許可されていません。	csuserを使用している場合は、上記のようにユーザに権限が与えられているかどうかを確認します。

問題	試してみてください
NFSのユーザ（IPアドレス）ブロックが機能しますが、SMB / CIFSの場合、次のエラーメッセージが表示されます。「SIDからドメイン名への変換に失敗しました。理由タイムアウト：ソケットが確立されていません」	これは、is_csuser_doesにsshを実行する権限がありません。（クラスタレベルで接続してから、ユーザがsshを実行できることを確認してください）。_csuser_roleには、これらの権限が必要です。 https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking クラスタクレデンシャルを使用する_csuser_withの場合、ONTAP コマンドラインから次の操作を実行します。 security login role create -role csrole -cmddirname "vserver export-policy rule"-access all security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname "vserver cifs session"-access all security login role create -role csrole -cmddirname "vserver services access-check authentication translate"-access all security login role create -role csrole -cmddirname "vserver name-mapping"-access all _csuser_を使用せず、クラスタレベルのadminユーザを使用している場合は、adminユーザにONTAPに対するssh権限があることを確認してください。
エラーメッセージ_SID変換に失敗しました。_Reason：255：Error：command failed：not authorized for that command_エラー：*"access-check" is not a recognized command*、when a user should have been blocked.	これは、_csuser_に正しい権限がない場合に発生する可能性があります。詳細については、を参照してください "ユーザアクセスブロックの前提条件" 。権限を適用したら、ONTAPデータコレクタとユーザディレクトリデータコレクタを再起動することをお勧めします。必要な権限コマンドを次に示します。---- security login role create -role csrole -cmddirname "vserver export-policy rule"-access all security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname "vserver cifs session"-access all security login role create -role csrole csrole -cmddirname "vserver services access-check authentication translate"-access role create -role csrole -cmddirname "vserver name-mapping"-access all ----

ワークロードのセキュリティ：攻撃のシミュレーション

このページの手順を使用して、付属のランサムウェアシミュレーションスクリプトを使用して、ワークロードセキュリティをテストまたは実証する攻撃をシミュレートできます。

始める前に注意してください

- ランサムウェアシミュレーションスクリプトは Linux でのみ動作します。
- このスクリプトは、Workload Securityエージェントのインストールファイルとともに提供されます。ワークロードセキュリティエージェントがインストールされているすべてのマシンで使用できます。
- このスクリプトは、Workload Securityエージェントマシン自体で実行できます。他のLinuxマシンを準備する必要はありません。ただし、スクリプトを別のシステムで実行する場合は、スクリプトをコピーしてそこで実行するだけです。

サンプルファイルを **1** 、 **000** 個以上用意してください

このスクリプトは、暗号化するファイルが格納されたフォルダを含む SVM で実行する必要があります。フォルダとサブフォルダには、少なくとも 1 、 000 個のファイルを含めることをお勧めします。ファイルは空にできません。
ファイルを作成したり、同じユーザを使用して暗号化したりしないでください。ワークロードセキュリティでは、これはリスクの低いアクティビティとみなされるため、アラートは生成されません（つまり、同じユーザが作成したファイルを変更した場合）。

手順については、以下を参照してください "プログラムによって空でないファイルを作成します"。

シミュレータを実行する前のガイドライン：

1. 暗号化されたファイルが空でないことを確認します。
2. 必ず50を超えるファイルを暗号化してください。少数のファイルは無視されます。
3. 同じユーザで何度も攻撃を実行しないでください。数回後、ワークロードセキュリティはこのユーザの動作を学習し、それがユーザの通常の動作であると想定します。
4. 同じユーザが作成したファイルは暗号化しないでください。ユーザが作成したばかりのファイルを変更しても、リスクのあるアクティビティとは見なされません。別のユーザが作成したファイルを使用するか、ファイルの作成から暗号化まで数時間かかります。

システムを準備

まず、ターゲットボリュームをマシンにマウントします。NFS マウントまたは CIFS エクスポートをマウントできます。

Linux で NFS エクスポートをマウントするには、次の手順を実行

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

NFS バージョン 4.1 はマウントしないでください。 FPolicy ではサポートされていません。

Linux で CIFS をマウントするには、次の手順を

```
 mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```
次に、 `Data Collector` をセットアップします。

1. ワークロードセキュリティエージェントがまだ構成されていない場合は構成します。
2. SVM データコレクタが設定されていない場合は設定します。

ランサムウェアシミュレータスクリプトを実行します

1. ワークロードセキュリティエージェントマシンにログイン（ssh）します。
2. /opt/NetApp/cloudsecure/agent/install_に 移動します
3. パラメータを指定せずにシミュレータスクリプトを呼び出し、使用状況を確認します。

```
# pwd
/opt/netapp/cloudsecure/agent/install
# ./ransomware_simulator.sh
Error: Invalid directory  provided.
Usage: ./ransomware_simulator.sh [-e] [-d] [-i <input_directory>]
       -e to encrypt files (default)
       -d to restore files
       -i <input_directory> - Files under the directory to be encrypted
```

```
Encrypt command example: ./ransomware_simulator.sh -e -i
/mnt/audit/reports/
Decrypt command example: ./ransomware_simulator.sh -d -i
/mnt/audit/reports/
```

テストファイルを暗号化します

ファイルを暗号化するには、次のコマンドを実行します。

```
# ./ransomware_simulator.sh -e -i /root/for/
Encryption key is saved in /opt/netapp/cloudsecure/cloudsecure-agent-
1.251.0/install/encryption-key,
which can be used for restoring the files.
Encrypted /root/for/File000.txt
Encrypted /root/for/File001.txt
Encrypted /root/for/File002.txt
...
```

ファイルをリストアします

復号化するには、次のコマンドを実行します。

```
[root@scspa2527575001 install]# ./ransomware_simulator.sh -d -i /root/for/
File /root/for/File000.txt is restored.
File /root/for/File001.txt is restored.
File /root/for/File002.txt is restored.
...
```

スクリプトを複数回実行します

ユーザがランサムウェア攻撃を受けた場合は、別のユーザに切り替えて攻撃を受けます。
Workload Securityはユーザの動作を学習し、同じユーザに対してランサムウェア攻撃が繰り返し発生してもアラートを生成しません。

プログラムでファイルを作成します

ファイルを作成する前に、データコレクタの処理を停止または一時停止する必要があります。
データコレクタをエージェントに追加する前に、次の手順を実行します。データコレクタをすでに追加している場合は、データコレクタを編集し、無効なパスワードを入力して保存します。これにより、データコレクタが一時的にエラー状態になります。注意：元のパスワードを必ずメモしてください。

推奨されるオプションは次のとおりです。 "コレクターの一時停止" ファイルを作成する前に。]

シミュレーションを実行する前に、暗号化するファイルを追加する必要があります。暗号化するファイルを手動でターゲットフォルダにコピーするか、スクリプト（以下の例を参照）を使用してプログラムでファイルを作成することができます。どちらの方法を使用した場合も、 1 、 000 個以上のファイルをコピーしてください。

プログラムでファイルを作成する場合は、次の手順を実行します。

1. [エージェント] ボックスにログインします。
2. Filer の SVM から Agent マシンに NFS エクスポートをマウントします。CD をそのフォルダに移動します。
3. このフォルダに、 createfiles.sh という名前のファイルを作成します
4. 次の行をそのファイルにコピーします。

```
for i in {000..1000}
do
   echo hello > "File${i}.txt"
done
echo 3 > /proc/sys/vm/drop_caches ; sync
```

5. ファイルを保存します。

6. ファイルに対する実行権限を確認します。

```
 chmod 777 ./createfiles.sh
. スクリプトを実行します。
```

```
./createfiles.sh
```

現在のフォルダには 1000 個のファイルが作成されます。

7. データコレクタを再度有効にします

手順 1 でデータコレクタを無効にした場合は、データコレクタを編集し、正しいパスワードを入力して保存します。データコレクタが running 状態であることを確認します。

8. これらの手順を実行する前にコレクタを一時停止した場合は、 "コレクタの再開"。

アラート、警告、およびエージェント / データソースコレクタの状態に関する電子メール通知の設定

ワークロードセキュリティアラートの受信者を設定するには、[*Admin]>[Notifications]をクリックし、受信者ごとに適切なセクションに電子メールアドレスを入力します。

潜在的な攻撃アラートと警告

Attack_alert 通知を送信するには、 _Send Potential Attack Alerts_Section に受信者の電子メールアドレスを入力します。
アラートに対するすべてのアクションについて、 E メール通知がアラート受信者リストに送信されます。

警告通知を送信するには、 _ 警告通知の送信 _ セクションに受信者の電子メールアドレスを入力します。

エージェントおよび **Data Collector** のヘルスモニタリング

通知を使用して、エージェントとデータソースの状態を監視できます。

エージェントまたはデータソースコレクタが機能していない場合に通知を受信するには、 _Data Collection Health Alerts_Section に受信者の電子メールアドレスを入力します。

次の事項に注意してください。

- ヘルスアラートは、エージェント / コレクタが少なくとも 1 時間レポートを停止した後にのみ送信されます。
- エージェントまたはデータコレクタが長時間切断されている場合でも、指定された 24 時間以内に目的の受信者に送信される電子メール通知は 1 通だけです。
- エージェントに障害が発生した場合は、 1 つのアラートが送信されます（コレクタごとに送信されるアラートではありません）。E メールには影響を受けるすべての SVM のリストが記載されます。

- Active Directory による収集エラーは警告として報告されますが、ランサムウェアによる検出には影響しません。
- [はじめに] セットアップリストに、新しい _ 電子メール通知の構成 _ 段階が追加されました。

エージェントおよび**Data Collector**のアップグレード通知を受信しています

- [Data Collection Health Alerts]にEメールIDを入力します。
- [Enable upgrade notifications]チェックボックスが有効になります。
- エージェントおよびData CollectorのアップグレードのEメール通知は、予定されているアップグレードの1日前にEメールIDに送信されます。

トラブルシューティング

* 問題： *	* これを試みなさい：*
「Data Collector Health Alerts」にEメールIDが表示されていますが、通知を受信していません。	通知メールは、NetApp Data Infrastructure Insightsドメイン（*accounts@service.clou dinsights.jp NetApp .com*）から送信されます。一部の企業は、外部ドメインからの受信メールをブロックします。NetApp Data Infrastructure Insightsドメインからの外部通知がホワイトリストに登録されていることを確認します。

ワークロードセキュリティ**API**

ワークロードセキュリティAPIにより、ネットアップのお客様と独立系ソフトウェアベンダー（ISV）は、ワークロードセキュリティをCMDBや他のチケット発行システムなどの他のアプリケーションと統合できます。

API アクセスの要件：

- API アクセストークンモデルを使用してアクセスが許可されます。
- APIトークン管理は、管理者ロールを持つワークロードセキュリティユーザが実行します。

API ドキュメント（ **Swagger** ）

最新のAPI情報は、Workload Securityにログインし、* Admin > API Access に移動することで確認できます。**[API Documentation]** リンクをクリックします。
API ドキュメントは Swagger ベースです。 API の簡単な概要情報と使用方法を提供しており、環境内で試すことができます。

Forensics Activity APIを呼び出す場合は、cloudsecure_forensics.activities.* v2 * APIを使用します。このAPIに複数の呼び出しを行う場合は、呼び出しが並列ではなく連続して実行されるようにしてください。複数の並行呼び出しが発生すると、APIがタイムアウトする可能性があります。

API アクセストークン

ワークロードセキュリティAPIを使用する前に、1つ以上の* APIアクセストークン*を作成する必要があります。アクセストークンは読み取り権限を付与します。各アクセストークンの有効期限を設定することもできます。

アクセストークンを作成するには：

- [**Admin] > [API Access**] をクリックします
- [*+API アクセストークン *] をクリックします
- 「 * トークン名 * 」と入力します
- トークンの有効期限 * を指定します

> トークンは、クリップボードにコピーして作成プロセス中に保存する場合にのみ使用できます。トークンは作成後に取得できないため、トークンをコピーして安全な場所に保存することを強くお勧めします。トークンの作成画面を閉じる前に、 [API アクセストークンのコピー] ボタンをクリックするよう求められます。

トークンを無効化、有効化、および取り消しできます。無効になっているトークンを有効にできます。

トークンを使用すると、お客様の観点から API への汎用アクセスが許可され、環境の範囲内で API へのアクセスが管理されます。

アプリケーションは、ユーザがアクセスの認証と許可に成功した後、ターゲット API を呼び出すときにアクセストークンをクレデンシャルとして渡します。渡されたトークンは、トークンのベアラに対して API へのアクセスが許可されていることを API に通知し、許可中に付与されたスコープに基づいて特定のアクションを実行します。

アクセストークンが渡される HTTP ヘッダーは * X-CloudInsights - apiKey ： * です

たとえば、次のようにしてストレージアセットを取得します。

```
 curl https://<tenant_host_name>/rest/v1/cloudsecure/activities -H 'X-
CloudInsights-ApiKey: <API_Access_Token>'
```

_<API_Access_Token> _ は、 API アクセスキーの作成時に保存したトークンです。

詳細については、 _API Documentation_link の * Admin > API Access * を参照してください。

API経由でデータを抽出するスクリプト

ワークロードセキュリティエージェントには、要求された時間範囲を小さなバッチに分割することで、v2 APIへの並行呼び出しを容易にするエクスポートスクリプトが含まれています。

スクリプトは_/ opt/ NetApp / cloudsecure/agent/export-script_にあります。使用方法については、同じディレクトリにあるREADMEファイルを参照してください。

スクリプトを呼び出すコマンドの例を次に示します。

```
python3 data-export.py --tenant_url <tenant
id>.cs01.cloudinsights.netapp.com --access_key %ACCESS_KEY% --path_filter
"<dir path>" --user_name "<user>" --from_time "01-08-2024 00:00:00"
--to_time "31-08-2024 23:59:59" --iteration_interval 12 --num_workers 3
```

キーパラメータ:-: `--iteration_interval 12`要求された時間範囲を12時間の間隔に分割します。 `--num_workers 3`-: 3つのスレッドを使用して、これらの間隔を並行してフェッチします。

トラブルシューティング

Data Infrastructure Insightsの一般的な問題のトラブルシューティング

ここでは、Data Infrastructure Insightsのトラブルシューティングに関する推奨事項を紹介します。

も参照してください "Linux Acquisition Unit の問題のトラブルシューティング" および "Windows Acquisition Unit の問題のトラブルシューティング"。

ログインの問題

* 問題： *	* これを試みなさい：*
Data Infrastructure Insightsは6時間ごとに自動的にログアウト	これは、ブラウザのサードパーティのCookieが無効になっているためです。ユーザーは、ブラウザを設定してすべてのサードパーティのCookieを有効にするか、より狭い例外リストを使用してData Infrastructure Insights用のCookieを有効にすることができます。例:ブラウザの設定を開く[すべてのCookieを許可する]オプションを選択します。または[サードパーティクッキーをブロック]を選択し、*[*.] auth0.com* _および[*.] NetApp .com _に例外を追加します。Microsoft Edgeでは、Chromeと同じ形式の例外が適用されます。Firefoxでは、Cookie例外は単に_auth0.comおよび_netapp.comとして指定されます。
BlueXPアカウントを持っていますが、BlueXPにログインできません。	からチケットを開き https://mysupport.netapp.com/site/helpます。カテゴリ「blueXP.netapp.com」>「Account/Login Issues」または「bluexp.netapp.com」>「Federation Issues」を選択します。これらは、BlueXPの問題や質問に特化したものです。Data Infrastructure Insightsテクニカルサポートのその他の問題については、にお問い合わせください"ネットアップサポート"。
Data Infrastructure Insightsに招待されましたが、「権限がありません」というメッセージが表示されます。	BlueXPアカウントにサインアップしたこと、またはBlueXPでSSOログインを使用していることを確認します。BlueXP プロファイルのEメールアドレスが、Data Infrastructure InsightsのようこそEメールに表示されているEメールアドレスと一致していることを確認します。E メールが一致しない場合は、正しい E メールアドレスで新しい招待状をリクエストします。

* 問題： *	* これを試みなさい：*
BlueXP からログアウトし、Data Infrastructure Insightsから自動的にログアウトしました。	NetAppクラウドサービス全体でシングルサインオン（SSO）を実行すると、Data Infrastructure Insights のすべてのセッションがログアウトされます。複数のData Infrastructure Insightsアカウントにアクセスできる場合は、いずれかのアカウントからログアウトすると、アクティブなセッションがすべてログアウトされます。ログインし直して、アカウントにアクセスします。
数日後に自動的にログアウトされました。	NetApp Cloudアカウントでは、数日ごとに再認証が必要です（現在のBlueXPの設定は7日です）。ログインし直して、アカウントにアクセスします。
「ログインを許可されていません」というエラーメッセージが表示されます。	アカウント管理者に問い合わせて、Data Infrastructure Insightsへのアクセス権を確認してください。BlueXP プロファイルのEメールアドレスが、Data Infrastructure Insightsのようこそメールに表示されているEメールアドレスと一致していることを確認する
その他のログインエラーです	Chrome で incognito モードを試すか、ブラウザの履歴、クッキー、およびキャッシュをクリアします。別のブラウザプロファイル（例 Chrome - ユーザーを追加します）。

その他の問題

質問：	回答 ：
qtreeのハードクォータがクエリに正しく表示されていますが、ソフトクォータがボリュームの合計容量として表示されています。正解ですか？	設定されたクォータとして表示されるのは、手動で設定するかTridentで設定したハードクォータのみです。ハードクォータを指定しない場合、qtreeの容量は内部ボリュームの容量になります。
同じqtreeにソフトクォータとハードクォータの両方を手動で設定していますが、表示される合計容量はハードクォータです。Is that correct？	○（ハードクォータが指定されている場合は、合計容量として表示されます）
Cognosのレポートスケジュールの時間を入力すると、スケジュールの時間に「m」が余分に表示されることがあります。たとえば、時刻を「02:15 PM」と入力すると、「02:15 PMM」（またはPMM）という余分な文字が追加されます。外をクリックすると、「2:15 AM」に変わります。 レポートを保存することはできますが、保存したレポートを再度開くと、スケジュール時刻にAMとPMのどちらを入力したかに関係なく、スケジュール時刻はAM（午前）と表示されます。	「AM」または「PM」の文字を完全に入力しないように注意して、スケジュール時刻を再入力します。「AM」は「A」、「PM」は「P」と入力するだけで十分です。余分な文字が表示されない場合は、スケジュール時刻が正しく設定されます。

リソース

その他のトラブルシューティングのヒントについては、を参照してください "ネットアップナレッジベース"

（サポートサインインが必要です）。

その他のサポート情報については、Data Infrastructure Insightsのページを参照して"サポート"ください。

Data Infrastructure Insightsのアクティブなサブスクリプションをお持ちの場合は、次のサポートオプションをご利用いただけます。

"電話"
"サポートチケット"

詳細については、を参照して "Data Infrastructure Insightsサポートドキュメント"ください。

Linux での Acquisition Unit の問題のトラブルシューティング

ここでは、 Linux サーバの Acquisition Unit に関する問題のトラブルシューティングについて説明します。

* 問題： *	* これを試みなさい : *
[Acquisition Units]タブの*[Observability]>[Collectors]*ページにあるAUのステータスには、[Certificate Expired]または[Certificate Revoked]と表示されます。	AU の右側にあるメニューをクリックし、 * Restore Connection * （接続の復元）を選択します。指示に従ってAcquisition Unitをリストアします。 1. Acquisition Unit（AU）サービスを停止します。*Copy Stop command* ボタンをクリックすると、コマンドをクリップボードに簡単にコピーし、このコマンドを Acquisition Unit マシンのコマンドプロンプトに貼り付けることができます。 2. AU の /var/lib/netapp/cloudinsite/acq/conf_folder に「 token 」という名前のファイルを作成します。 3. *Copy Token_button* をクリックし ' 作成したファイルにこのトークンを貼り付けます *4. AU* サービスを再起動します。*_Copy Restart command* ボタンをクリックし、 AU のコマンドプロンプトにコマンドを貼り付けます。
Acquisition Unitサーバサービスの開始時に権限が拒否されました	AUをSELinuxにインストールしている場合は、SEを_permissive_modeに設定する必要があります。Enforcing_modeはサポートされていませんSELinuxをPermissiveモードに設定したら、AUサービスを再起動します。 "詳細はこちら。"。
サーバ要件が満たされていません	Acquisition Unit サーバまたは VM が次の条件を満たしていることを確認します "要件"

ネットワーク要件が満たされていません	Acquisition Unitサーバ/ VMが、NetAppポート443経由で<environment-name>接続を介してData Infrastructure Insights環境（ssl.c01.cloudinsights.ssl.com）にアクセスできることを確認します。次のコマンドを試してみてください。*ping <environment-name> NetApp NetApp <environment-name>.c01.cloudinsights.cloudinsights.c01.cloudinsights.c01.cloudinsights.c01.cloudinsights.c01.cloudinsights.c01.cloudinsights.com*<environment-name><environment-name> NetApp NetApp
プロキシサーバが正しく設定されていません	プロキシの設定を確認し、必要に応じて Acquisition Unit ソフトウェアをアンインストールして再インストールして、正しいプロキシの設定を入力します。 1. 「カール」を試してみます。 プロキシに関する "man curl " 情報 / ドキュメントを参照してください — preproxy 、 --proxy-* (curl では多数のプロキシ設定がサポートされているため、これはワイルドカード "*" です) 。 2. 「 wget 」を試します。 プロキシオプションについては、ドキュメントを参照してください。
Acquisition Serviceの開始中にCredentialエラーが発生し、Data Infrastructure InsightsでAcquisition Unitのインストールが失敗しました（acq.logに表示されます）。	これは、プロキシのクレデンシャルに特殊文字が含まれていることが原因で発生することがあります。AU （ _sudo cloudInsights - uninstall.sh ）をアンインストールし、特殊文字を使用せずに再インストールします。
Linux ：見つからないライブラリ / ファイルが見つかりません	Linux Acquisition Unit サーバ / VM に必要なライブラリがすべてあることを確認します。たとえば、サーバに *unzip_library* がインストールされている必要があります。*_unzip_library* をインストールするには、*Acquisition Unit* のインストールスクリプトを実行する前に、 *command* * sudo yum install unzip * _ を実行します
権限の問題	sudo 権限を持つユーザとしてログインしていることを確認します
収集が実行されていません	/opt/netapp/cloudinsights/acq/logs（Linux）からacq.logを収集します。 取得サービスを再起動します。sudo cloudinsights-service.sh acquisitionを再起動します
データ収集の問題：	Data Collector のランディングページで [Send Error Report] ボタンをクリックして、エラーレポートを送信します

ステータス：ハートビート失敗	Acquisition Unit（AU）は、リースを更新するために60秒ごとにハートビートをData Infrastructure Insightsに送信します。ネットワークの問題やData Infrastructure Insightsの応答がないためにハートビートコールが失敗した場合、AUのリース時間は更新されません。AUのリース期限が切れると、Data Infrastructure Insightsのステータスは「Heartbeat Failed」と表示されます。トラブルシューティングの手順： Acquisition Unit サーバと CloudInsights 間のネットワーク接続を確認します。Acquisition Unit サービスが実行されているかどうかを確認します。サービスが実行されていない場合は、サービスを開始します。Acquisition Unit のログ（ /var/log/netapp/cloudInsights /acq/acq.log ）でエラーがないかどうかを確認します。
「ハートビートエラー：」というメッセージが表示される	このエラーは、ネットワークの中断によってAcquisition UnitとData Infrastructure Insights環境の間の通信が1分以上中断される場合に発生することがあります。AUとData Infrastructure Insightsの間の接続が安定してアクティブであることを確認します。
Acquisition Unitを再インストールすると、「ValueError：File context for /opt/netapp/cloudinsights（/.*）？」と表示されるすでに定義されています」。	SELinuxを搭載したシステムでは、このエラーメッセージは `cloudinsights-uninstall.sh -p` が実行されました。Acquisition Unitを再インストールします。コマンドの実行 `semanage fcontext -d -t usr_t "/opt/netapp/cloudinsights(/.*)?"` 問題を修正し、メッセージを削除する必要があります。

プロキシとファイアウォールに関する考慮事項

インターネットアクセスにプロキシを使用する必要がある場合は、組織のプロキシの動作を理解し、Data Infrastructure Insightsが機能するために特定の例外を探す必要があります。次の事項に注意してください。

- まず、組織はデフォルトでアクセスをブロックしていますか。また、特定の Web サイト / ドメインへのアクセスのみを例外として許可していますか。その場合は、次のドメインを例外リストに追加する必要があります。

  ```
  *.cloudinsights.netapp.com
  ```

  Data Infrastructure Insights Acquisition Unitのほか、WebブラウザでのData Infrastructure Insightsの操作はすべて、そのドメイン名を持つホストに送信されます。

- 次に、一部のプロキシは、NetAppから生成されないデジタル証明書でデータインフラストラクチャインサイトのWebサイトを偽装することで、TLS/SSL検査を実行しようとします。Data Infrastructure Insights Acquisition Unitのセキュリティモデルは、これらのテクノロジと根本的に互換性がありません。Data Infrastructure Insights Acquisition UnitがData Infrastructure Insightsに正常にログインしてデータ検出を行えるようにするには、この機能以外の上記のドメイン名も必要です。

トラフィック検査用にプロキシが設定されている場合は、プロキシ構成の例外リストにData Infrastructure Insights環境を追加する必要があります。この例外リストの形式と設定は、プロキシの環境やツールによって

異なりますが、一般に、AUがこれらのサーバと適切に通信できるように、Data Infrastructure Insightsサーバのurlをこの例外リストに追加する必要があります。

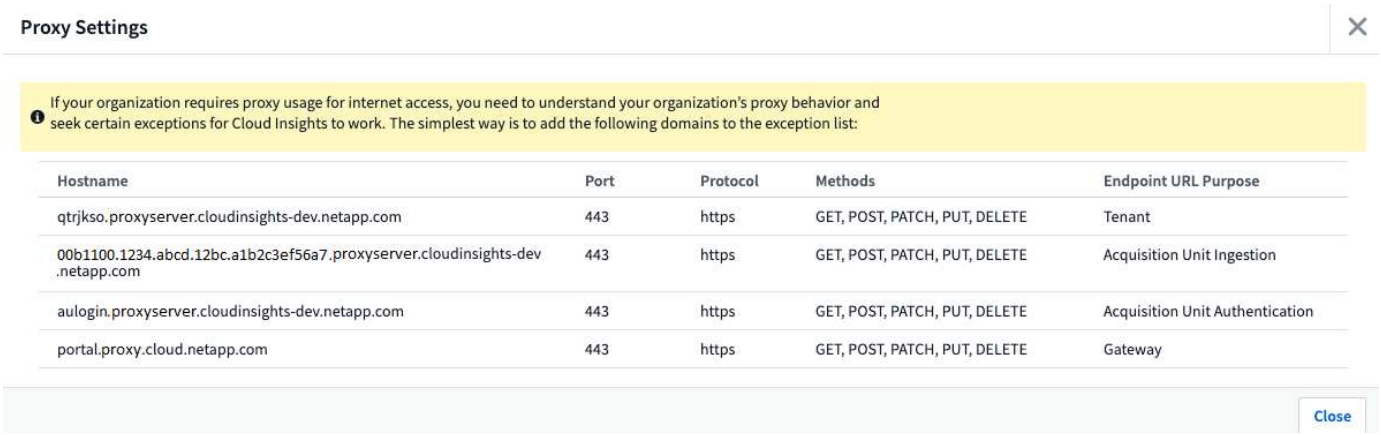
最も簡単な方法は、Data Infrastructure Insightsドメイン自体を例外リストに追加することです。

```
*.cloudinsights.netapp.com
```

プロキシがトラフィック検査用に設定されていない場合は、例外リストが必要な場合と必要でない場合があります。Data Infrastructure Insightsを例外リストに追加する必要があるかどうかわからない場合、またはプロキシやファイアウォールの構成が原因でData Infrastructure Insightsのインストールや実行に問題がある場合は、プロキシ管理チームに相談して、プロキシによるSSL代行受信の処理を設定してください。

プロキシエンドポイントの表示

プロキシエンドポイントを表示するには、オンボーディング中にデータコレクタを選択するときに * Proxy Settings * リンクをクリックするか、 * Help > Support * ページの *Proxy Settings_* のリンクをクリックします。次のようなテーブルが表示されます。ワークロードセキュリティを使用している環境では、設定済みのエンドポイントURLもこのリストに表示されます。



リソース

その他のトラブルシューティングのヒントについては、を参照してください "ネットアップナレッジベース"（サポートサインインが必要です）。

その他のサポート情報については、Data Infrastructure Insightsのページを参照して"サポート"ください。

Windows での Acquisition Unit の問題のトラブルシューティング

ここでは、 Windows サーバの Acquisition Unit に関する問題のトラブルシューティング方法を示します。

* 問題： *	* これを試みなさい : *

[Acquisition Units]タブの*[Observability]>[Collectors]*ページにあるAUのステータスには、[Certificate Expired]または[Certificate Revoked]と表示されます。	AU の右側にあるメニューをクリックし、 * Restore Connection *（接続の復元）を選択します。指示に従ってAcquisition Unitをリストアします。 1. Acquisition Unit（AU）サービスを停止します。*Copy Stop command* ボタンをクリックすると、コマンドをクリップボードに簡単にコピーし、このコマンドを Acquisition Unit マシンのコマンドプロンプトに貼り付けることができます。 2. AU の *c ： \Program Files\Cloud Insights \Acquisition Unit\conf_folder* に *"token"* という名前のファイルを作成します。 *3. _Copy Token_button* をクリックし ' 作成したファイルにこのトークンを貼り付けます *4. AU* サービスを再起動します。*_Copy Restart command* ボタンをクリックし、 AU のコマンドプロンプトにコマンドを貼り付けます。
サーバ要件が満たされていません	Acquisition Unit サーバまたは VM が次の条件を満たしていることを確認します "要件"
ネットワーク要件が満たされていません	Acquisition Unitサーバ/ VMが、NetAppポート443経由で<environment-name>接続を介してData Infrastructure Insights環境（ssl.c01.cloudinsights.ssl.com）にアクセスできることを確認します。次のコマンドを試してみてください。*ping <environment-name> NetApp NetApp <environment-name>.c01.cloudinsights.cloudinsights.c01.cloudinsights.c01.cloudinsights.c01.cloudinsights.c01.cloudinsights.com*<environment-name><environment-name> NetApp NetApp
プロキシサーバが正しく設定されていません	プロキシの設定を確認し、必要に応じて Acquisition Unit ソフトウェアをアンインストールして再インストールして、正しいプロキシの設定を入力します。 1. 「カール」を試してみます。 プロキシに関する "man curl " 情報 / ドキュメントを参照してください — preproxy 、 --proxy-* (curl では多数のプロキシ設定がサポートされているため、これはワイルドカード "*" です) 。 2. 「 wget 」を試します。 プロキシオプションについては、ドキュメントを参照してください。
Acquisition Serviceの開始中にCredentialエラーが発生し、Data Infrastructure InsightsでAcquisition Unitのインストールが失敗しました（acq.logに表示されます）。	これは、プロキシのクレデンシャルに特殊文字が含まれていることが原因で発生することがあります。AU（ _sudo cloudInsights - uninstall.sh ）をアンインストールし、特殊文字を使用せずに再インストールします。
権限の問題	管理者権限を持つユーザとしてログインしていることを確認してください

収集が実行されていません	情報は、 acq.log の _<install directory >\Cloud Insights \Acquisition Unit \log_folder にあります。Windows サービスを使用して取得を再開します
データ収集の問題：	Data Collector のランディングページで [Send Error Report] ボタンをクリックして、エラーレポートを送信します
ステータス：ハートビート失敗	Acquisition Unit（AU）は、リースを更新するために60秒ごとにハートビートをData Infrastructure Insightsに送信します。ネットワークの問題やData Infrastructure Insightsの応答がないためにハートビートコールが失敗した場合、AUのリース時間は更新されません。AUのリース期限が切れると、Data Infrastructure Insightsのステータスは「Heartbeat Failed」と表示されます。トラブルシューティングの手順： * Acquisition Unit サーバと CloudInsights 間のネットワーク接続を確認します。* Acquisition Unit サービスが実行されているかどうかを確認します。サービスが実行されていない場合は、サービスを開始します。* Acquisition Unit のログ（ <Install dir> ： \Program Files\Cloud Insights \Acquisition Unit \log\acq.log ）でエラーがないかどうかを確認します。
「 Heartbeat Error: message 」が表示されています	このエラーは、ネットワークの中断によってAcquisition UnitとData Infrastructure Insights環境の間の通信が1分以上中断される場合に発生することがあります。AUとData Infrastructure Insightsの間の接続が安定してアクティブであることを確認します。

プロキシとファイアウォールに関する考慮事項

インターネットアクセスにプロキシを使用する必要がある場合は、組織のプロキシの動作を理解し、Data Infrastructure Insightsが機能するために特定の例外を探す必要があります。次の事項に注意してください。

- まず、組織はデフォルトでアクセスをブロックしていますか。また、特定の Web サイト / ドメインへのアクセスのみを例外として許可していますか。その場合は、次のドメインを例外リストに追加する必要があります。

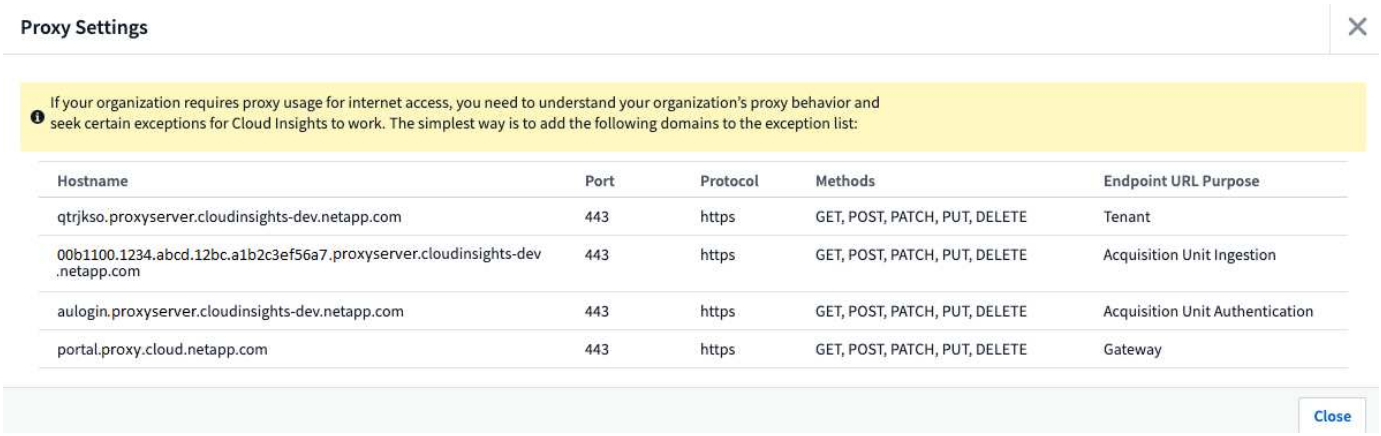
  ```
  *.cloudinsights.netapp.com
  ```

  Data Infrastructure Insights Acquisition Unitのほか、WebブラウザでのData Infrastructure Insightsの操作はすべて、そのドメイン名を持つホストに送信されます。

- 次に、一部のプロキシは、NetAppから生成されないデジタル証明書でデータインフラストラクチャインサイトのWebサイトを偽装することで、TLS/SSL検査を実行しようとします。Data Infrastructure Insights Acquisition Unitのセキュリティモデルは、これらのテクノロジと根本的に互換性がありません。Data Infrastructure Insights Acquisition UnitがData Infrastructure Insightsに正常にログインしてデータ検出を行えるようにするには、この機能以外の上記のドメイン名も必要です。

プロキシエンドポイントの表示

プロキシエンドポイントを表示するには、オンボーディング中にデータコレクタを選択するときに * Proxy Settings * リンクをクリックするか、 * Help > Support * ページの *Proxy Settings_* のリンクをクリックします。次のようなテーブルが表示されます。ワークロードセキュリティを使用している環境では、設定済みのエンドポイントURLもこのリストに表示されます。



リソース

その他のトラブルシューティングのヒントについては、を参照してください "ネットアップナレッジベース"（サポートサインインが必要です）。

その他のサポート情報については、Data Infrastructure Insightsのページを参照して"サポート"ください。

データコレクタの問題の調査

データコレクタにエラーメッセージと「高」または「中」の影響がある場合は、データコレクタの概要ページにリンクされている情報を使用して、この問題を調査する必要があります。

次の手順に従って、失敗したデータコレクタの原因を確認します。データコレクタの障害メッセージは、[**Admin**] メニューおよび [*Installed Data Collectors] ページに表示されます。

手順

1. [**Admin**>*Data Collector*>*Installed Data Collectors] をクリックします。
2. [リンクされたデータコレクタの名前] をクリックして、 [概要] ページを開きます。
3. 概要ページのコメント領域で、同じ問題について調査している他のエンジニアのメモがある場合はその内容を確認します。
4. パフォーマンスのメッセージを確認します。
5. イベントタイムライングラフのセグメントにマウスポインタを合わせると、追加情報が表示されます。
6. デバイスのエラーメッセージを選択し、イベントタイムラインの下に表示された後、メッセージの右側に表示されるエラー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. この Data Collector 領域から報告されるデバイスでは、リストをフィルタして対象デバイスのみを表示したり、デバイスのリンクされた * 名前 * をクリックしてそのデバイスのアセットページを表示したりすることができます。
8. データコレクタの概要ページに戻ったら、ページの下部にある「最近の変更を表示」 * 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。

Data Infrastructure Insights Data Collectorサポートマトリックス

Data Collector Support Matrixには、ベンダーやモデルの情報など、Data Infrastructure Insightsでサポートされるデータコレクタのリファレンスが記載されています。

HP Enterprise 3PAR/Alletra 9000/Primera StoreServストレージ

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
HPE Alletra 9080 HPE_3PAR 20450 HPE_3PAR 20800 HPE_3PAR 20850 HPE_3PAR 20850_R2 HPE_3PAR 7200c HPE_3PAR 7400 HPE_3PAR 7440c HPE_3PAR 7450c HPE_3PAR 8200 HPE_3PAR 8400 HPE_3PAR 8440 HPE_3PAR 8450 HPE_3PAR 9450 HPE_3PAR A630 HPE_3PAR A650 HPE_3PAR A670 HP_3PAR 20800 HP_3PAR 7200 HP_3PAR 7200c HP_3PAR 7400 HP_3PAR 7400c HP_3PAR 7450c HP_3PAR 8200 HP_3PAR 8400 InServ F400 InServ T400 InServ T800 InServ V400	3.1.1（MU1） 3.1.2（MU3） 3.1.3（MU1） 3.1.3（MU2） 3.1.3（MU3） 3.2.1（MU3） 3.2.1（MU5） 3.2.2 3.2.2（MU2） 3.2.2（MU4） 3.2.2（MU6） 3.3.1（MU1） 3.3.1（MU2） 3.3.1（MU5） 3.3.2 3.3.2（MU1） 4.4.1リリースタイプ：標準サポートリリース 4.5.11リリースタイプ：延長サポートリリース 4.5.3リリースタイプ：延長サポートリリース 4.5.7リリースタイプ：延長サポートリリース 9.5.8リリースタイプ：延長サポートリリース

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		UUID	実施しました	SSH	
		使用済み容量	実施しました	SSH	
プロダクト	カテゴリ	仮想ーチャー/属性（**Feature/Attribute**）	実施しました	使用するプロトコル	追加情報ジ仮想化デバイスですか？
	ボリュームマップ	LUN	実施しました	SSH	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	SSH	
		ストレージポート	実施しました	SSH	
		を入力します	ギャップ	SSH	
	ボリュームマスク	イニシエータ	実施しました	SSH	
		Protocol Controller（プロトコルコントローラ）	実施しました	SSH	
		ストレージポート	実施しました	SSH	
		を入力します	ギャップ	SSH	
	ボリューム参照	名前	実施しました	SSH	
		ストレージIP	実施しました	SSH	
	WWNエイリアス	ホストのエイリアス	実施しました	SSH	
		オブジェクトタイプ（ Object Type ）	実施しました	SSH	
		ソース	実施しました	SSH	
		WWN	実施しました	SSH	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					てのディスクでの読み取り/書き込み）（MB/秒）
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			実施しました	SMI-Sの使用	
	ボリューム	キャッシュヒット率読み取り	実施しました	SMI-Sの使用	
		キャッシュヒット率の合計	実施しました	SMI-Sの使用	
		キャッシュヒット率書き込み	実施しました	SMI-Sの使用	
		物理容量	実施しました	SMI-Sの使用	
		合計容量	実施しました	SMI-Sの使用	
		使用済み容量	実施しました	SMI-Sの使用	
		使用容量の比率	実施しました	SMI-Sの使用	
		容量比率の書き込み	実施しました	SMI-Sの使用	
		IOPS読み取り	実施しました	SMI-Sの使用	ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました	SMI-Sの使用	
		IOPS -書き込み	実施しました	SMI-Sの使用	
		レイテンシ読み取り	実施しました	SMI-Sの使用	
		レイテンシ合計	実施しました	SMI-Sの使用	
		レイテンシライト	実施しました	SMI-Sの使用	
		部分ブロック率	実施しました	SMI-Sの使用	
		スループット読み取り	実施しました	SMI-Sの使用	
		合計スループット	実施しました	SMI-Sの使用	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	SMI-Sの使用	
		書き込み保留中です	実施しました	SMI-Sの使用	合計書き込み保留中です

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
3PAR SMI-Sの2つのタイプがあります	SMI-Sの使用	HTTP / HTTPS	5988/5989		正しいです	正しいです	正しいです	正しいです
3PAR CLIの場合	SSH	SSH	22.		正しいです	いいえ	正しいです	正しいです

トップに戻る

Amazon AWS EC2

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン
2014-10-01

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		ションID			
	仮想マシンディスク	OID	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		VirtualDisk OID	実施しました	HTTPS	
		仮想マシンOID	実施しました	HTTPS	
	ホスト	ホストOS	実施しました	HTTPS	
		IPS	実施しました	HTTPS	
		製造元	実施しました	HTTPS	
		名前	実施しました	HTTPS	
		OID	実施しました	HTTPS	
	情報	API概要 の略	実施しました	HTTPS	
		API名	実施しました	HTTPS	
		APIのバージョン	実施しました	HTTPS	
		データソース名	実施しました	HTTPS	情報
		日付	実施しました	HTTPS	
		発信者ID	実施しました	HTTPS	
		Originatorキー	実施しました	HTTPS	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

					てのディスクでの読み取り/書き込み）（MB/秒）
プロダクト	カテゴリ	フィーチャー/属性ルール（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			実施しました	HTTPS	
	VM	合計容量	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		使用容量の比率	実施しました	HTTPS	
		合計CPU利用率	実施しました	HTTPS	
		IOPS読み取り	実施しました	HTTPS	ディスク上の読み取りIOPSの数
		diskIops.total	実施しました	HTTPS	
		ディスクIOPS書き込み	実施しました	HTTPS	
		レイテンシ読み取り	実施しました	HTTPS	
		レイテンシ合計	実施しました	HTTPS	
		レイテンシライト	実施しました	HTTPS	
		ディスクスループット読み込み	実施しました	HTTPS	
		スループット読み取り	実施しました	HTTPS	ディスクの合計スループット読み取り
		ディスクスループット書き込み	実施しました	HTTPS	
		IPスループット読み込み	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	IPスループットの合計
		ipThroughput書き込み	実施しました	HTTPS	
		合計メモリ利用率	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
EC2 APIの場合	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

Amazon AWS S3

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
S3	2010-08-01

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					のディスクの合計）
プロダクト	カテゴリ	仮想ーチャー/属性（**Feature/Attribute**）	実施しましたまたは	使用するプロトコル	追加情報ジ仮想化デバイスですか？
	ストレージプール	DWH容量に含める	実施しました	HTTPS	ACQからcotnrolまでの間には、DWH容量に興味深いストロークプールがあります
		名前	実施しました	HTTPS	
		物理ディスク容量（MB）	実施しました	HTTPS	ストレージプールの物理容量として使用されます
		RAID グループ	実施しました	HTTPS	このストレージプールがRAIDグループかどうかを示します
		使用可能な物理比率	実施しました	HTTPS	使用可能容量から物理容量への変換率
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニングがサポートされます	実施しました	HTTPS	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		合計割り当て済み容量	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？
パフォーマンス	内部ボリューム	合計容量	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		使用容量の比率	実施しました	HTTPS	
		合計オブジェクト数	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
S3 API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

Microsoft Azure NetApp Files の略

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン	モデル
2019-06-01	Azure NetApp Files の特長

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					のディスクの合計）
プロダクト	カテゴリ	仮想ーチャー/属性（**Feature/Attribute**）	実施しましたまたは	使用するプロトコル	追加情報ジ仮想化デバイスですか？
	ストレージプール	データの割り当て容量	ギャップ	HTTPS	データに割り当てられている容量
		データの使用容量	実施しました	HTTPS	
		DWH容量に含める	実施しました	HTTPS	ACQからcotnrolまでの間には、DWH容量に興味深いストロークプールがあります
		名前	実施しました	HTTPS	
		物理ディスク容量（MB）	実施しました	HTTPS	ストレージプールの物理容量として使用されます
		RAID グループ	実施しました	HTTPS	このストレージプールがRAIDグループかどうかを示します
		使用可能な物理比率	実施しました	HTTPS	使用可能容量から物理容量への変換率
		ステータス	実施しました	HTTPS	
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニングがサポートされます	実施しました	HTTPS	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		合計割り当て済み容量	実施しました	HTTPS	
		合計使用容量	実施しました	HTTPS	合計容量（MB）
		を入力します	ギャップ	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

		合計データ容量	実施しました		
		データの使用容量	実施しました		
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		Snapshot使用容量	実施しました		
	StoragePoolディスク	IOPS読み取り	実施しました		ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました		
		IOPS -書き込み	実施しました		
		スループット読み取り	実施しました		
		合計スループット	実施しました		ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました		

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Azure NetApp Files REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

Brocade ファイバチャネルスイッチ

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
178.0 183.0 Brocade 200E Brocade 300E Brocade 3900 Brocade 4024 Embedded Brocade 48000 Brocade 5000 Brocade 5100 Brocade 5300 Brocade 5480エンベデッド Brocade 6505 Brocade 6510 Brocade 6520 Brocade 6548 Brocade 7800 Brocade 7840 Brocade DCX Brocade DCX-4Sバックボーン Brocade DCX8510-4 Brocade DCX8510-8 Brocade G610 Brocade G620 Brocade G630 Brocade G720 Brocade M5424エンベデッド Brocade X6-4 Brocade X6-8 Brocade X7-4 Brocade X7-8	V5.3.2c V6.2.1b V6.2.2G v6.3.2 V6.4.1a V6.4.2 V6.4.2a v7.0.0 v7.0.1b v7.1.0c v7.3.0c V7.3.1d V7.4.1d V7.4.1f V7.4.2a V7.4.2c V7.4.2D V7.4.2G V7.4.2G_CVR_824494_01 V7.4.2h V7.4.2j1 v8.0.2a v8.0.2c v8.0.2D v8.1.2G v8.1.2j v8.1.2k v8.2.0 v8.2.0b v8.2.1c v8.2.1d v8.2.2a v8.2.2b v8.2.2c v8.2.2D v8.2.2d4 v8.2.3 v8.2.3a v8.2.3A1 v8.2.3b v8.2.3c v8.2.3C1 v9.0.0b v9.0.1a v9.0.1b4 v9.0.1c v9.0.1d v9.0.1e v9.0.1e1 v9.1.0b v9.1.1 v9.1.1_01 v9.1.1b

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		Type ）			
		ソース	実施しました	SSH	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		WWN	実施しました	SSH	
	ゾーン	ゾーン名	実施しました	SSH	
	ゾーンメンバー	を入力します	ギャップ	SSH	
		WWN	実施しました	SSH	
	ゾーニング機能	アクティブな構成	実施しました	SSH	
		コンフィギュレーション名（Configuration Name）	実施しました	SSH	
		デフォルトのゾーニング動作	実施しました	SSH	
		WWN	実施しました	SSH	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

					棄
		ポートエラー	実施しました	SNMP	合計ポートエラー数
プロダクト	カテゴリ	フィーチャー/属性ラベル（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			実施しました	SNMP	
		合計トラフィックフレームレート	実施しました	SNMP	
		トラフィックフレームレート	実施しました	SNMP	
		平均フレームサイズ	実施しました	SNMP	トラフィックの平均フレームサイズ
		Tx Frames（送信フレーム）	実施しました	SNMP	トラフィックの平均フレームサイズ
		トラフィックレート	実施しました	SNMP	
		合計トラフィックレート	実施しました	SNMP	
		トラフィックレート	実施しました	SNMP	
		トラフィック利用率	実施しました	SNMP	
		トラフィック利用率	実施しました	SNMP	合計トラフィック使用率
		トラフィック利用率	実施しました	SNMP	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Brocade SNMP	SNMP	SNMPv1、SNMPv2、SNMPv3	161		正しいです	正しいです	正しいです	正しいです
Brocade SSH	SSH	SSH	22.		いいえ	いいえ	正しいです	正しいです
データソースウィザードの設定	手動入力				正しいです	正しいです	正しいです	正しいです

トップに戻る

Brocade Network Advisor HTTP

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン	モデル	ファームウェアバージョン
14.4.1 14.4.3 14.4.4 14.4.5	Brocade 5300 Brocade 6510 Brocade 6520 Brocade 6548 Brocade DCX 8510-8 Brocade G620 DS-6620B EMC Connectrix ED-DCX8510-8B	v7.2.1a V7.3.1a V7.4.1b V7.4.2D v8.2.3b v8.2.3c v9.0.1a v9.0.1b v9.0.1e1

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		WWN	実施しました	HTTP/S	
	ゾーン	ゾーン名	実施しました	HTTP/S	
プロダクト	カテゴリー	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
	ゾーンメンバー	WWN を入力します	ギャップ	HTTP/S	
		WWN	実施しました	HTTP/S	
	ゾーニング機能	アクティブな構成	実施しました	HTTP/S	
		コンフィギュレーション名（Configuration Name）	実施しました	HTTP/S	
		WWN	実施しました	HTTP/S	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス	ポート	BBクレジットゼロ合計	実施しました	HTTP/S	
		BBクレジット	実施しました	HTTP/S	
		BBクレジットがゼロになります	実施しました	HTTP/S	
		portErrors.class3破棄	実施しました	HTTP/S	
		portErrors.crc	実施しました	HTTP/S	
		ポートエラー	実施しました	HTTP/S	
		ポートエラー	実施しました	HTTP/S	短いフレームによるポートエラーです
		portErrors.linkFailure	実施しました	HTTP/S	ポートエラーリンク障害
		ポートエラー	実施しました	HTTP/S	ポートエラー信号損失
		ポートエラー	実施しました	HTTP/S	ポートエラー同期が失われました
		ポートエラー	実施しました	HTTP/S	ポートエラータイムアウトの破棄
		ポートエラー	実施しました	HTTP/S	合計ポートエラー数
		トラフィックレート	実施しました	HTTP/S	
		合計トラフィックレート	実施しました	HTTP/S	
		トラフィックレート	実施しました	HTTP/S	
		トラフィック利用率	実施しました	HTTP/S	
		トラフィック利用率	実施しました	HTTP/S	合計トラフィック使用率
		トラフィック利用率	実施しました	HTTP/S	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Brocade Network Advisor REST API	HTTP / HTTPS	HTTP / HTTPS	80対443		正しいです	正しいです	正しいです	正しいです

トップに戻る

Brocade FOS REST

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
Brocade 6505 Brocade G720 Brocade X6-8	v8.2.3c v8.2.3C1 v9.0.1e1 v9.1.1b

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		WWN	実施しました	HTTPS	
	ゾーン	ゾーン名	実施しました	HTTPS	
プロダクト	カテゴリー	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
	ゾーンメンバー	を入力します WWN	ギャップ	HTTPS	
		WWN	実施しました	HTTPS	
	ゾーニング機能	アクティブな構成	実施しました	HTTPS	
		コンフィギュレーション名（Configuration Name）	実施しました	HTTPS	
		デフォルトのゾーニング動作	実施しました	HTTPS	
		WWN	実施しました	HTTPS	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

		合計トラフィックフレームレート	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）レート	ステータス	使用するプロトコル	追加情報
			実施しました	HTTPS	
		平均フレームサイズ	実施しました	HTTPS	トラフィックの平均フレームサイズ
		Tx Frames（送信フレーム）	実施しました	HTTPS	トラフィックの平均フレームサイズ
		トラフィックレート	実施しました	HTTPS	
		合計トラフィックレート	実施しました	HTTPS	
		トラフィックレート	実施しました	HTTPS	
		トラフィック利用率	実施しました	HTTPS	
		トラフィック利用率	実施しました	HTTPS	合計トラフィック使用率
		トラフィック利用率	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Brocade FOS REST API	HTTPS		443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

Cisco MDS / Nexusファブリックスイッチ

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
8978-E04	3.3（1c）
CN1610	4.1（3a）
DS-C9124-2-K9	5.0（1a）
DS-C9124-K9	5.0（3）N2（3.11e）
DS-C9132T-K9	5.0（3）N2（3.23 o）
DS-C9134-K9	5.0（3）N2（4.01d）
DS-C9148-16P-K9	5.0（3）N2（4.04e）
DS-C9148-32P-K9	5.0（3）N2（4.13e）
DS-C9148-48P-K9	5.0（3）N2（4.13i）
DS-C9148S-K9	5.0（3）N2（4.21e）
DS-C9148T-K9	5.0（3）N2（4.21j）
DS-C9222I-K9	5.0（3）N2（4.21k）
DS-C9250I-K9	5.0（3）N2（4.22c）
DS-C9396S-K9	5.0（8）
DS-C9396T-K9	5.2（2D）
DS-C9506	5.2（3）N2（2.28g）
DS-C9509	5.2（6a）
DS-C9513	5.2（8）
DS-C9706	5.2（8b）
DS-C9710	5.2（8c）
DS-C9718	5.2（8d）
DS-HP-8GFC-K9	5.2（8F）
DS-HP-FC-K9	5.2（8g）
N5K-C5548UP	5.2（8時間）
N5K-C5596UP	5.2（8i）
N5K-C56128P	6.2（1）
N5K-C5696Q	6.2（11）
UCS-FI-6248UP	6.2（11b）
UCS-FI-6296UP	6.2（11c）
UCS-FI-6332	6.2（11e）
UCS-FI-6332-16UP	6.2（13）
UCS-FI-6454	6.2（13a）
	6.2（15）
	6.2（17）
	6.2（19）
	6.2（21）
	6.2（23）
	6.2（25）
	6.2（27）
	6.2（29）
	6.2（31）
	6.2（33）
	6.2（5）
	6.2（5a）
	6.2（7）
	6.2（9）
	6.2（9a）
	6.2（9C）
	7.3（0）D1（1）
	7.3（0）DY（1）
	7.3(1) DY（1）
	7.3（1）N1（1）
	7.3（13）N1（1）
	7.3（6）N1（1）

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		オブジェクトタイプ（ Object Type ）	実施しました	SNMP	
プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
		WWN	実施しました	SNMP	
	ゾーン	ゾーン名	実施しました	SNMP	
		ゾーンタイプ	実施しました	SNMP	
	ゾーンメンバー	を入力します	ギャップ	SNMP	
		WWN	実施しました	SNMP	
	ゾーニング機能	アクティブな構成	実施しました	SNMP	
		コンフィギュレーション名（Configuration Name）	実施しました	SNMP	
		デフォルトのゾーニング動作	実施しました	SNMP	
		コントロールのマージ	実施しました	SNMP	
		WWN	実施しました	SNMP	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					
700					

		合計トラフィックフレームレート	実施しました	SNMP	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		レート	実施しました	SNMP	
		平均フレームサイズ	実施しました	SNMP	トラフィックの平均フレームサイズ
		Tx Frames（送信フレーム）	実施しました	SNMP	トラフィックの平均フレームサイズ
		トラフィックレート	実施しました	SNMP	
		合計トラフィックレート	実施しました	SNMP	
		トラフィックレート	実施しました	SNMP	
		トラフィック利用率	実施しました	SNMP	
		トラフィック利用率	実施しました	SNMP	合計トラフィック使用率
		トラフィック利用率	実施しました	SNMP	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Cisco SNMP	SNMP	SNMPv1（インベントリのみ）、SNMP v2、SNMP v3	161		正しいです	正しいです	正しいです	正しいです

トップに戻る

凝集性

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
C2500 C2505 C4000コンピューティングノード C4600 C5036 C5066 C6025 C6035 C6055 PXG1 UCS-C240M5H10	6.5.1f_release-20210913_13f6a4bf 6.5.1f_u1_release-20211027_9e4e40cb 6.6.0d_u6_release-20221204_c03629f0 6.8.1_release-20220807_6c9115ef 6.8.1_U1_RELEASE - 20221022_6f58ed2a 6.8.1_U2_RELEASE - 20230412_5ced2ed3 6.8.1_U3_RELEASE - 20230509_1e641b74 7.0_U1_RELEASE-20230222_8995f044

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		合計割り当て済み容量	実施しました		
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		合計使用容量	実施しました		合計容量（MB）
		ホットスポット	ギャップ		
		仮想	実施しました		ストレージ仮想化デバイスですか？
		暗号化	実施しました		

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

					込み）（MB/秒）
プロダクト	IOPSの合計 カテゴリ	実施しました フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	レイテンシライト 追加情報
	実施しました			利用率の合計	実施しました
			StoragePoolディスク	IOPS読み取り	実施しました
		ディスク上の読み取りIOPSの数		IOPS -書き込み	実施しました
				スループット読み取り	実施しました
				スループット書き込み	実施しました
				合計スループット	実施しました
		ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）		IOPSの合計	実施しました

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Cohesity REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

EMC Celerra（SSH）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
NS-480FC NSX VG8 VNX5200 VNX5300 VNX5400 VNX5600 VNX7600	5.5.38-1 6.0.65-2 7.1.76-4 7.1.79-8 7.1.83-2 8.1.21-266 8.1.21-303 8.1.9-155

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		合計割り当て済み容量	実施しました	SSH	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報 合計容量（MB）
		合計使用容量	実施しました	SSH	
		ボリューム	ギャップ	SSH	
		仮想	実施しました	SSH	ストレージ仮想化デバイスですか？

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Celerra CLIの場合	SSH	SSH			正しいです	いいえ	正しいです	正しいです

トップに戻る

EMC CLARiX（NaviCLI）

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン	モデル	ファームウェアバージョン
6.23 6.26 6.28 7.30 7.32 7.33	AX4-5F8 CX3-20f CX3-40f CX4-480 VNX5100 VNX5200 VNX5300 VNX5400 VNX5500 VNX5600 VNX5700 VNX5800 VNX7600 VNX8000	04.28.000.5.710 04.30.000.5.525 05.32.000.5.218 05.32.000.5.219 05.32.000.5.221 05.32.000.5.225 05.32.000.5.249 05.33.000.5.074 05.33.009.5.155 05.33.009.5.184 05.33.009.5.186 05.33.009.5.218 05.33.009.5.231 05.33.009.5.236 05.33.009.5.238 05.33.009.6.305 05.33.021.5.256 05.33.021.5.266 2.23.50.5.710 3.26.20.5.011 3.26.40.5.029

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		ニング			
		を入力します	ギャップ	CLI の使用	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		UUID	実施しました	CLI の使用	
		使用済み容量	実施しました	CLI の使用	
	ボリュームマップ	LUN	実施しました	CLI の使用	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	CLI の使用	
		ストレージポート	実施しました	CLI の使用	
		を入力します	ギャップ	CLI の使用	
	ボリュームマスク	イニシエータ	実施しました	CLI の使用	
		Protocol Controller（プロトコルコントローラ）	実施しました	CLI の使用	
		ストレージポート	実施しました	CLI の使用	
		を入力します	ギャップ	CLI の使用	
	ボリュームメンバー	容量	実施しました	CLI の使用	Snapshotの使用容量（MB単位）
		名前	実施しました	CLI の使用	
		ランク	実施しました	CLI の使用	
		合計物理容量	実施しました	CLI の使用	合計物理容量（アレイ上のすべてのディスクの合計）
		冗長性	実施しました	CLI の使用	冗長性レベル
		ストレージプールID	実施しました	CLI の使用	
		使用済み容量	実施しました	CLI の使用	
	WWNエイリアス	ホストのエイリアス	実施しました	CLI の使用	
		IP	実施しました	CLI の使用	
		オブジェクトタイプ（ Object Type ）	実施しました	CLI の使用	
		ソース	実施しました	CLI の使用	
		WWN	実施しました	CLI の使用	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		き込み			
		読み取り利用率	実施しました	CLI の使用	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		利用率の合計	実施しました	CLI の使用	
		利用率ライト	実施しました	CLI の使用	
	ボリューム	キャッシュヒット率読み取り	実施しました	CLI の使用	
		キャッシュヒット率の合計	実施しました	CLI の使用	
		キャッシュヒット率書き込み	実施しました	CLI の使用	
		物理容量	実施しました	CLI の使用	
		合計容量	実施しました	CLI の使用	
		使用済み容量	実施しました	CLI の使用	
		使用容量の比率	実施しました	CLI の使用	
		IOPS読み取り	実施しました	CLI の使用	ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました	CLI の使用	
		IOPS -書き込み	実施しました	CLI の使用	
		レイテンシ読み取り	実施しました	CLI の使用	
		レイテンシ合計	実施しました	CLI の使用	
		レイテンシライト	実施しました	CLI の使用	
		部分ブロック率	実施しました	CLI の使用	
		スループット読み取り	実施しました	CLI の使用	
		合計スループット	実施しました	CLI の使用	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	CLI の使用	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Navi CLIの場合	CLI の使用		6389、2162、2163、443（HTTPS）/ 80（HTTP）		正しいです	正しいです	正しいです	いいえ

トップに戻る

EMC Data Domain（SSH）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
DD VE DD2200 DD2500 DD3300 DD4200 DD6300 DD6800 DD6900 DD7200 DD9300 DD9400 DD9500 DD9800 DD990 DD9900	6.1.2.051-633576 6.1.2.20-606786 6.1.2.50-632120 6.2.0.30-629757 6.2.0.35-635767 6.2.1.30-663869 6.2.1.40-671977 6.2.1.60-686365 7.10.0.0-1017741 7.10.1.0-1042928 7.2.0.30-663847 7.2.0.50-671975 7.2.0.60-682124 7.2.0.70-686759 7.2.0.90-692270 7.6.0.20-689174 7.6.0.30-690691 7.7.0.7-1007134 7.7.1.10-1011247 7.7.2.011-1011427 7.7.2.10-1011249 7.7.3.0-1011963 7.7.4.0-1017976 7.7.5.1-1040473 7.7.5.11-1046187 7.8.0.0-1008134

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		使用可能な物理比率	実施しました	SSH	使用可能容量から物理容量への変換率
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			実施しました	SSH	
		シンプロビジョニングがサポートされます	実施しました	SSH	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		合計割り当て済み容量	実施しました	SSH	
		合計使用容量	実施しました	SSH	合計容量（MB）
		を入力します	ギャップ	SSH	
		仮想	実施しました	SSH	ストレージ仮想化デバイスですか？

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Data Domain CLIの略	SSH	SSH	22.		正しいです	正しいです	正しいです	正しいです

トップに戻る

EMC ECS

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
ECS の場合	3.6.1.1 3.6.1.3 3.6.2.1 3.6.2.4 3.7.0.0 3.7.0.3 3.7.0.4 3.7.0.5 3.8.0.1 3.8.0.2

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		ノードの使用可能容量利用率（MB）	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（FeatureAttribute）	ステータス	使用するプロトコル	追加情報
		使用容量（MB）	実施しました	HTTPS	
	ストレージプール	DWH容量に含める	実施しました	HTTPS	ACQからcotnrolまでの間には、DWH容量に興味深いストロークプールがあります
		名前	実施しました	HTTPS	
		物理ディスク容量（MB）	実施しました	HTTPS	ストレージプールの物理容量として使用されます
		RAID グループ	実施しました	HTTPS	このストレージプールがRAIDグループかどうかを示します
		使用可能な物理比率	実施しました	HTTPS	使用可能容量から物理容量への変換率
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニングがサポートされます	実施しました	HTTPS	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		合計割り当て済み容量	実施しました	HTTPS	
		合計使用容量	実施しました	HTTPS	合計容量（MB）
		を入力します	ギャップ	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

					てのディスクでの読み取り/書き込み）（MB/秒）
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			実施しました	HTTPS	
	StoragePoolディスク	プロビジョニング済み容量	実施しました	HTTPS	
		物理容量	実施しました	HTTPS	
		合計容量	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		オーバーコミット容量率です	実施しました	HTTPS	時系列で報告されます
		使用容量の比率	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
EMC ECS REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

Dell EMC IsilonとPowerScale REST

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
A200 A2000 A300 の比較 A3000 F200 F600 F800 F900 H400 H500 NL410 S210 X210 X400 X410	9.1.0.11 9.1.0.6 9.2.1.10 9.2.1.11 9.2.1.12 9.2.1.16 9.2.1.19 9.2.1.21 9.2.1.6 9.2.1.7 9.2.1.9 9.4.0.11 9.4.0.12 9.4.0.13 9.4.0.14 9.4.0.5 9.4.0.7 9.5.0.3 v8.0.0.4 v8.0.0.6 v8.0.0.7 v8.1.2.0 v8.2.2.0

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					（MB単位）
		Snapshotの使用容量	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			実施しました	HTTPS	
		シンプロビジョニングがサポートされます	実施しました	HTTPS	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		合計割り当て済み容量	実施しました	HTTPS	
		合計使用容量	実施しました	HTTPS	合計容量（MB）
		を入力します	ギャップ	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		利用率の合計	実施しました	HTTPS	
	StoragePoolディスク	プロビジョニング済み容量	実施しました	HTTPS	
		物理容量	実施しました	HTTPS	
		合計容量	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		オーバーコミット容量率です	実施しました	HTTPS	時系列で報告されます
		使用容量の比率	実施しました	HTTPS	
		合計データ容量	実施しました	HTTPS	
		データの使用容量	実施しました	HTTPS	
		IOPS読み取り	実施しました	HTTPS	ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました	HTTPS	
		IOPS -書き込み	実施しました	HTTPS	
		その他の合計容量	実施しました	HTTPS	
		その他の使用容量	実施しました	HTTPS	
		Snapshotのリザーブ容量	実施しました	HTTPS	
		Snapshotの使用容量	実施しました	HTTPS	
		Snapshotの使用容量の比率	実施しました	HTTPS	時系列で報告されます
		スループット読み取り	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
EMC Isilon およびPowerScale REST API	HTTPS		443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

Dell EMC Isilon / PowerScale（CLI）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
A200 A2000 A300 の比較 F200 F800 F900 H400 H500 H600 H700 NL400 NL410 S210 X200 X210 X400 X410	9.1.0.10 9.1.0.12 9.1.0.16 9.1.0.18 9.1.0.19 9.1.0.7 9.2.1.11 9.2.1.13 9.2.1.15 9.2.1.22 9.2.1.7 9.2.1.9 9.3.0.3 9.4.0.0 9.4.0.10 9.4.0.12 9.4.0.13 9.4.0.14 9.4.0.6 9.4.0.7 v7.1.1.8 v7.2.0.5 v7.2.1.3 v7.2.1.6 v8.0.0.4 v8.0.0.6 v8.0.0.7 v8.0.1.1 v8.1.2.0 v8.2.2.0

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		合計割り当て済み容量	実施しました	SSH	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		合計使用容量	実施しました	SSH	合計容量（MB）
		ボリューム	ギャップ	SSH	
		仮想	実施しました	SSH	ストレージ仮想化デバイスですか？

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					込み）（MB/秒）
		スループット書き込み	実施しました	SSH	
プロダクト	カテゴリ	スイッチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		利用率の合計	実施しました	SSH	
	StoragePoolディスク	プロビジョニング済み容量	実施しました	SSH	
		物理容量	実施しました	SSH	
		合計容量	実施しました	SSH	
		使用済み容量	実施しました	SSH	
		オーバーコミット容量率です	実施しました	SSH	時系列で報告されます
		使用容量の比率	実施しました	SSH	
		合計データ容量	実施しました	SSH	
		データの使用容量	実施しました	SSH	
		Snapshotのリザーブ容量	実施しました	SSH	
		Snapshotの使用容量	実施しました	SSH	
		Snapshotの使用容量の比率	実施しました	SSH	時系列で報告されます

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Isilon SSH	SSH	SSH	22.		正しいです	いいえ	正しいです	正しいです

トップに戻る

EMC PowerStore REST

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
PowerStore 1000T PowerStore 1200T PowerStore 3000T PowerStore 3200T PowerStore 5000T PowerStore 5000倍 PowerStore 9000T PowerStore 9200T	2.0.1.3 2.1.1.0 2.1.1.1 3.0.0.1 3.2.0.0 3.2.0.1 3.2.1.0

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

	ク				
		Protocol Controller（プロトコルコントローラ）	実施しました		
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		ゾーン	実施しました		
			ギャップ		
	WWNエイリアス	ホストのエイリアス	実施しました		
		オブジェクトタイプ（ Object Type ）	実施しました		
		ソース	実施しました		
		WWN	実施しました		

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

			合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）		き込み
プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
	実施しました				利用率の合計
	実施しました			StoragePoolディスク	圧縮による総削減量
	実施しました				IOPS読み取り
	実施しました		ディスク上の読み取りIOPSの数		IOPSの合計
	実施しました				IOPS -書き込み
	実施しました				スループット読み取り
	実施しました				合計スループット
	実施しました		ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）		スループット書き込み
	実施しました			ボリューム	物理容量
	実施しました				合計容量
	実施しました				使用済み容量
	実施しました				使用容量の比率
	実施しました				IOPS読み取り
	実施しました		ディスク上の読み取りIOPSの数		IOPSの合計
	実施しました				IOPS -書き込み
	実施しました				レイテンシ読み取り
	実施しました				レイテンシ合計
	実施しました				レイテンシライト
	実施しました				スループット読み取り
	実施しました				合計スループット
	実施しました		ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）		スループット書き込み

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
EMC PowerStore REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

EMC RecoverPoint（HTTP）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
RecoverPoint	5.1.P1（175年頃） 5.1.SP4.P1（H.89） 5.1.SP4.P2（H.101） 5.1.SP4.P3（H.109） 5.1.SP4.P4（H.97）

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

					のディスクの合計）
プロダクト	カテゴリ	仮想チャー/属性（**Feature/Attribute**）	実施しました	使用するプロトコル	追加情報ジ仮想化デバイスですか？
	ストレージノード	メモリサイズ	ギャップ	HTTPS	デバイスメモリ（MB単位）
		モデル	実施しました	HTTPS	
		名前	実施しました	HTTPS	
		プロセッサ数	実施しました	HTTPS	デバイスCPU
		シリアル番号	実施しました	HTTPS	
		状態	実施しました	HTTPS	デバイスの状態を説明するフリーテキスト
		UUID	実施しました	HTTPS	
		バージョン	実施しました	HTTPS	ソフトウェアバージョン
	ストレージ同期	モード	実施しました	HTTPS	
		モード列挙	実施しました	HTTPS	
		ソースストレージ	実施しました	HTTPS	
		ソースボリューム	実施しました	HTTPS	
		状態	実施しました	HTTPS	デバイスの状態を説明するフリーテキスト
		状態の列挙	実施しました	HTTPS	
		ターゲットストレージ	実施しました	HTTPS	
		ターゲットボリューム	実施しました	HTTPS	
		テクノロジ	実施しました	HTTPS	ストレージ効率化の原因となるテクノロジが変化しています

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
RecoverPoint REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

EMC ScaleIOおよびPowerFlex REST

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
ScaleIO	R2_6.11000.113 R2_6.11000.115 R3_0.1400.101 R3_5.1200.104 R3_6.500.113 R3_6.700.103

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		合計使用容量	実施しました	HTTPS	合計容量（MB）
		を入力します	ギャップ	HTTPS	
プロダクト	カテゴリ	仮想ーチャー/属性（**Feature/Attribute**）	実施しました	使用するプロトコル	追加情報ジ仮想化デバイスですか？
	ボリューム	容量	実施しました	HTTPS	Snapshotの使用容量（MB単位）
		ジャンクションパス	実施しました	HTTPS	
		名前	実施しました	HTTPS	
		合計物理容量	実施しました	HTTPS	合計物理容量（アレイ上のすべてのディスクの合計）
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニング	実施しました	HTTPS	
		UUID	実施しました	HTTPS	
		ホストIP	実施しました	HTTPS	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		ト			合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		IOPSの合計	実施しました		
	ボリューム	物理容量	実施しました		
		合計容量	実施しました		
		IOPS読み取り	実施しました		ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました		
		IOPS -書き込み	実施しました		
		スループット読み取り	実施しました		
		合計スループット	実施しました		ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました		

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
EMC ScaleIOおよびPowerFlex REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

EMC Symmetrix CLI

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン	モデル	ファームウェアバージョン
v10.0.0.0 v10.0.1.0 V7.6.2.67 V8.3.0.22 V8.3.0.6 V8.4.0.7 V8.4.0.9 v9.1.0.18 v9.1.0.5 v9.1.0.6 v9.2.0.0 v9.2.1.0 v9.2.1.1 v9.2.1.2 v9.2.2.0 v9.2.3.0 v9.2.3.1 v9.2.3.4 v9.2.3.5 v9.2.3.6 v9.2.4.1 v9.2.4.2	DMX3-24 DMX4-24 PMax2000 PowerMax_2000 PowerMax_8000 VMAX-1 VMAX100K VMAX10K VMAX200K VMAX250F VMAX400K VMAX40K VMAX450F VMAX850F VMAX950F	5773.198.142（168D0000）ビルド5 5876.272.177（16F40000）ビルド39 5876.286.194（16F40000）ビルド115 5876.309.196（16F40000）ビルド162 5977.1131.1131（17590000）ビルド551 5977.1151.1151（17590000）ビルド45 5977.1151.1151（17590000）ビルド59 5977.1151.1151（17590000）ビルド60 5977.1151.1151（17590000）ビルド9 5978.479.479（175A0000）ビルド195 5978.711.711（175A0000）ビルド113 5978.711.711（175A0000）ビルド139 5978.711.711（175A0000）ビルド149 5978.711.711（175A0000）ビルド194 5978.711.711（175A0000）ビルド196 5978.711.711（175A0000）ビルド220 5978.711.711（175A0000）ビルド239 5978.711.711（175A0000）ビルド252 5978.711.711（175A0000）ビルド267 5978.711.711（175A0000）ビルド278 5978.711.711（175A0000）ビルド287 5978.711.711（175A0000）ビルド335 5978.711.711（175A0000）ビルド365 5978.711.711（175A0000）ビルド366 5978.711.711（175A0000）ビルド388 5978.711.711（175A0000）ビルド416 5978.711.711（175A0000）ビルド436

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		トコルコントローラ）			
プロダクト	カテゴリ	ストレージポート/フィーチャー/属性（Feature/Attribute）の	実施しました/ステータス/ギャップ	使用するプロトコル	追加情報
	ボリュームメンバー	自動階層化	実施しました		このストレージプールが他のプールとの自動階層化に参加しているかどうかを示します
		容量	実施しました		Snapshotの使用容量（MB単位）
		シリンダ	実施しました		
		名前	実施しました		
		ランク	実施しました		
		合計物理容量	実施しました		合計物理容量（アレイ上のすべてのディスクの合計）
		冗長性	実施しました		冗長性レベル
		ストレージプールID	実施しました		
		UUID	実施しました		
		使用済み容量	実施しました		
	ボリューム参照	名前	実施しました		
		ストレージIP	実施しました		
	WWNエイリアス	ホストのエイリアス	実施しました		
		オブジェクトタイプ（ Object Type ）	実施しました		
		ソース	実施しました		
		WWN	実施しました		

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					てのディスクでの読み取り/書き込み）（MB/秒）
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			実施しました		
	ボリューム	キャッシュヒット率読み取り	実施しました		
		キャッシュヒット率の合計	実施しました		
		キャッシュヒット率書き込み	実施しました		
		物理容量	実施しました		
		合計容量	実施しました		
		使用済み容量	実施しました		
		書き込み済み容量	実施しました		
		使用容量の比率	実施しました		
		容量比率の書き込み	実施しました		
		IOPS読み取り	実施しました		ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました		
		IOPS -書き込み	実施しました		
		レイテンシ読み取り	実施しました		
		レイテンシ合計	実施しました		
		レイテンシライト	実施しました		
		スループット読み取り	実施しました		
		合計スループット	実施しました		ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました		
		書き込み保留中です	実施しました		合計書き込み保留中です

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
SYMCLI	CLI の使用		2707		正しいです	正しいです	正しいです	正しいです
Symmetrix SMI-S	SMI-Sの使用	HTTP / HTTPS	5988/5989		正しいです	いいえ	いいえ	正しいです

トップに戻る

Dell Unisphere REST

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン	モデル	ファームウェアバージョン
v10.0.0.5 v10.0.1.3 v9.2.1.6 v9.2.3.20 v9.2.3.22 v9.2.3.4 v9.2.4.1	PowerMax_2000 PowerMax_2500 PowerMax_8000 VMAX250F VMAX950F	5978.479.479ビルド350 5978.711.711ビルド252 5978.711.711ビルド278ビルド278 5978.711.711ビルド287 5978.711.711ビルド329ビルド329 5978.711.711ビルド365 5978.711.711ビルド365 5978.711.711ビルド376 5978.711.711ビルド388ビルド388 5978.711.711ビルド416 5978.711.711ビルド435 5978.711.711ビルド448 5978.711.711ビルド461ビルド461 5978.711.711ビルド481ビルド481 5978.711.711ビルド484 5978.711.711ビルド484ビルド484 5978.711.711ビルド502 6079.125.0ビルド53ビルド53 6079.175.0ビルド0

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		トコルコントローラ）			
プロダクト	カテゴリ	ストレージポート	実施しました	HTTPS	
		フィーチャー/属性（**Feature/Attribute**）を入力します	スケータス	使用するプロトコル	追加情報
			ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	WWNエイリアス	ホストのエイリアス	実施しました	HTTPS	
		オブジェクトタイプ（ Object Type ）	実施しました	HTTPS	
		ソース	実施しました	HTTPS	
		WWN	実施しました	HTTPS	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					のディスクでの読み取り/書き込み）（MB/秒）
プロダクト	カテゴリ スループット書き込み	フィーチャー/属性実施Feature/Attribute）	ステータス HTTPS	使用するプロトコル	追加情報 利用率の合計
	実施しました	HTTPS		ボリューム	物理容量
	実施しました	HTTPS			合計容量
	実施しました	HTTPS			使用済み容量
	実施しました	HTTPS			使用容量の比率
	実施しました	HTTPS			容量比率の書き込み
	実施しました	HTTPS			IOPS読み取り
	実施しました	HTTPS	ディスク上の読み取りIOPSの数		IOPSの合計
	実施しました	HTTPS			IOPS -書き込み
	実施しました	HTTPS			レイテンシ読み取り
	実施しました	HTTPS			レイテンシ合計
	実施しました	HTTPS			レイテンシライト
	実施しました	HTTPS			スループット読み取り
	実施しました	HTTPS			合計スループット
	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）		スループット書き込み

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Dell Unisphere API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

EMC VNX（SSH）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
VNX5300 VNX5400 VNX5700 VNX5800	05.33.009.5.231 7.1.76-4 7.1.80-3 8.1.9-232

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					合計）
		使用済み容量	実施しました	SSH	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		冗長性	実施しました	SSH	冗長性レベル
		ディスクタイプ	使用できません	SSH	
	ボリュームマップ	LUN	実施しました	SSH	バックエンドLUNの名前
		ストレージポート	実施しました	SSH	
		Protocol Controller（プロトコルコントローラ）	実施しました	SSH	
		を入力します	ギャップ	SSH	
	ボリュームマスク	ストレージポート	実施しました	SSH	
		イニシエータ	実施しました	SSH	
		Protocol Controller（プロトコルコントローラ）	実施しました	SSH	
		を入力します	ギャップ	SSH	
	WWNエイリアス	ソース	実施しました	SSH	
		ホストのエイリアス	実施しました	SSH	
		WWN	実施しました	SSH	
		オブジェクトタイプ（ Object Type ）	実施しました	SSH	
		IP	実施しました	SSH	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

		き込み			
		読み取り利用率	実施しました	SSH	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		利用率の合計	実施しました	SSH	
		利用率ライト	実施しました	SSH	
	ストレージ	失敗した物理容量	実施しました	SSH	
		物理容量	実施しました	SSH	
		スペアの物理容量	実施しました	SSH	スペアディスクのraw容量（スペアであるすべてのディスクの合計）
		ストレージプールの容量	実施しました	SSH	
		IOPS：その他	実施しました	SSH	
		IOPS読み取り	実施しました	SSH	ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました	SSH	
		IOPS -書き込み	実施しました	SSH	
		レイテンシ読み取り	実施しました	SSH	
		レイテンシ合計	実施しました	SSH	
		レイテンシライト	実施しました	SSH	
		スループット読み取り	実施しました	SSH	
		合計スループット	実施しました	SSH	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	SSH	
	ストレージノード	IOPS読み取り	実施しました	SSH	ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました	SSH	
		IOPS -書き込み	実施しました	SSH	
		利用率の合計	実施しました	SSH	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
VNX SSH およびCLI	SSH	SSH	22.		正しいです	いいえ	正しいです	正しいです

トップに戻る

EMC VNXeおよびUnity Unisphere（CLI）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
Unity 300 Unity 300F Unity 350F Unity 380 Unity 380F Unity 400 Unity 400F Unity 450F Unity 480F Unity 500 Unity 550F Unity 600 Unity 600F ユニティ650F ユニティ680F ユニティ880 VNXe3200	3.1.17.10223906 3.1.17.10229825 4.1.2.9257522 4.2.1.9535982 4.2.3.9670635 4.5.1.0.5.001 5.0.2.0.5.009 5.0.6.0.5.008 5.0.8.0.5.007 5.1.2.0.5.007 5.1.3.0.5.003 5.2.1.0.5.013 5.2.2.0.5.004 5.2.2.0.6.201 5.3.0.0.5.120

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		ルID			
		シンプロビジョニング	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		UUID	実施しました	HTTPS	
		仮想化済み容量	実施しました	HTTPS	
	ボリュームマップ	LUN	実施しました	HTTPS	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）		スループット書き込み
プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）		使用するプロトコル	追加情報
	実施しました	HTTPS		ボリューム	物理容量
	実施しました	HTTPS			合計容量
	実施しました	HTTPS			使用済み容量
	実施しました	HTTPS			使用容量の比率
	実施しました	HTTPS			IOPS読み取り
	実施しました	HTTPS	ディスク上の読み取りIOPSの数		IOPSの合計
	実施しました	HTTPS			IOPS -書き込み
	実施しました	HTTPS			レイテンシ合計
	実施しました	HTTPS			スループット読み取り
	実施しました	HTTPS			合計スループット
	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）		スループット書き込み

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
VNXeとUnisphere CLI	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

EMC VPLEX

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
VPLEX	5.4.1.00.00.07 5.4.1.01.00.05 6.2.0.03.00.02 6.2.0.04.00.07 6.2.0.05.00.11 6.2.0.07.00.02

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					
860					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		ニング			
		UUID	実施しました	HTTP/S	
プロダクト	カテゴリ	仮想ーチャー/属性（**Feature/Attribute**）	実施しました	使用するプロトコル	追加情報ジ仮想化デバイスですか？
	ボリュームマップ	LUN	実施しました	HTTP/S	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTP/S	
		ストレージポート	実施しました	HTTP/S	
		を入力します	ギャップ	HTTP/S	
	ボリュームマスク	イニシエータ	実施しました	HTTP/S	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTP/S	
		ストレージポート	実施しました	HTTP/S	
		を入力します	ギャップ	HTTP/S	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

					込み）（MB/秒）
		スループット書き込み	実施しました	SSH	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		利用率の合計	実施しました	SSH	
	StoragePoolディスク	プロビジョニング済み容量	実施しました	SSH	
		合計容量	実施しました	SSH	
		使用済み容量	実施しました	SSH	
		オーバーコミット容量率です	実施しました	SSH	時系列で報告されます
		使用容量の比率	実施しました	SSH	
		その他の合計容量	実施しました	SSH	
		その他の使用容量	実施しました	SSH	
	ボリューム	物理容量	実施しました	SSH	
		合計容量	実施しました	SSH	
		IOPSの合計	実施しました	SSH	
		レイテンシ読み取り	実施しました	SSH	
		レイテンシ合計	実施しました	SSH	
		レイテンシライト	実施しました	SSH	
		スループット読み取り	実施しました	SSH	
		合計スループット	実施しました	SSH	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	SSH	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
EMC VPLEX CLI	SSH	SSH	22.		正しいです	正しいです	正しいです	正しいです

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
EMC VPLEX API	HTTP / HTTPS	HTTP / HTTPS	80対443		正しいです	正しいです	正しいです	正しいです

トップに戻る

EMC XtremIO（HTTP）

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン	モデル	ファームウェアバージョン
6.2.1 6.2.2 6.3.1 6.3.2 6.3.3 6.4.0	1ブリック、125TB 1ブリック、24TB 1ブリック、26TB ブリック×1、31TB 1ブリック、62TB 1ブリック、8TB 10TB×1 20TB×1 40TB×1 ブリック×2、52TB ブリック×2、62TB ブリック×2、76TB ブリック×2、83TB 10TB×2 20TB×2 40TB×2 3ブリック、251TB 3ブリック、283TB 4ブリック、125TB 4ブリック、503TB 4ブリック、628TB 4ブリック、754TB 20TB×4 40TB×4 20TB×6	4.0.27-1 4.0.31-11 6.1.0-99_X2 6.3.3-8_X2 6.4.0-22_X2 6.4.0-36_hotfix_2_X2

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	テクノロジフィーチャー/属性（**Feature/Attribute**）	実施しましたステータス	HTTPS使用するプロトコル	ストレージ効率追加情報となるテクノロジが変化しています
	ボリューム	容量	実施しました	HTTPS	Snapshotの使用容量（MB単位）
		ディスクサイズ	実施しました	HTTPS	ディスクサイズのカンマ区切りリスト（GB）
		ディスク速度	実施しました	HTTPS	ディスク速度のカンマ区切りリスト（rpm）
		ディスクタイプ	使用できません	HTTPS	
		名前	実施しました	HTTPS	
		合計物理容量	実施しました	HTTPS	合計物理容量（アレイ上のすべてのディスクの合計）
		冗長性	実施しました	HTTPS	冗長性レベル
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニング	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
		UUID	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？
	ボリュームマップ	LUN	実施しました	HTTPS	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

					てのディスクでの読み取り/書き込み）（MB/秒）
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			実施しました	HTTPS	
	StoragePoolディスク	プロビジョニング済み容量	実施しました	HTTPS	
		物理容量	実施しました	HTTPS	
		合計容量	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		オーバーコミット容量率です	実施しました	HTTPS	時系列で報告されます
		使用容量の比率	実施しました	HTTPS	
		合計データ容量	実施しました	HTTPS	
		データの使用容量	実施しました	HTTPS	
	ボリューム	物理容量	実施しました	HTTPS	
		合計容量	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		使用容量の比率	実施しました	HTTPS	
		IOPS読み取り	実施しました	HTTPS	ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました	HTTPS	
		IOPS -書き込み	実施しました	HTTPS	
		レイテンシ読み取り	実施しました	HTTPS	
		レイテンシ合計	実施しました	HTTPS	
		レイテンシライト	実施しました	HTTPS	
		部分ブロック率	実施しました	HTTPS	
		スループット読み取り	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
EMC XtremIO REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

NetApp E-Series

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
2、600 2660 2680 2702 2704 2、800 B 2804 2806 3000 5480 5486 5488 5504 5564 5600 5700 5、700 B 6000	08.40.60.01 8.10.14.0 8.20.11.0 8.20.27.0 8.20.30.0 8.20.5.0 8.20.8.0 8.25.14.0 8.25.6.0 8.30.1.0 8.40.0.1 8.40.0.3 8.40.20.0 8.40.30.3 8.40.40.0 8.40.0.0 8.40.60.1 8.40.60.2 8.40.60.3 8.42.20.0 8.50.0.3 8.50.0.4 8.51.0.0 8.52.0.0 8.52.0.1 8.53.0.1 8.53.0.4 8.62.0.0 8.62.0.2 8.63.0.2 8.70.0.3 8.71.2.0 8.71.3.0 8.72.0.0 8.72.1.0 8.72.2.0 8.73.0.0 8.74.0.0 8.74.1.0 8.74.2.0 8.74.3.0 8.75.0.0

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					か？
		書き込み済み容量	実施しました	RMI	ホストによって
プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
	ボリュームマップ	LUN	実施しました	RMI	ボリュームに書き込まれた合計容量（MB） バックエンドLUNの名前
		ストレージポート	実施しました	RMI	
		を入力します	ギャップ	RMI	
	ボリュームマスク	イニシエータ	実施しました	RMI	
		ストレージポート	実施しました	RMI	
		を入力します	ギャップ	RMI	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		き込み			
		読み取り利用率	実施しました	RMI	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		利用率の合計	実施しました	RMI	
		利用率ライト	実施しました	RMI	
	ボリューム	キャッシュヒット率読み取り	実施しました	RMI	
		キャッシュヒット率の合計	実施しました	RMI	
		キャッシュヒット率書き込み	実施しました	RMI	
		物理容量	実施しました	RMI	
		合計容量	実施しました	RMI	
		使用済み容量	実施しました	RMI	
		書き込み済み容量	実施しました	RMI	
		使用容量の比率	実施しました	RMI	
		容量比率の書き込み	実施しました	RMI	
		IOPS読み取り	実施しました	RMI	ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました	RMI	
		IOPS -書き込み	実施しました	RMI	
		レイテンシ読み取り	実施しました	RMI	
		レイテンシ合計	実施しました	RMI	
		レイテンシライト	実施しました	RMI	
		スループット読み取り	実施しました	RMI	
		合計スループット	実施しました	RMI	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	RMI	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
SANtricity APIの略	RMI	TCP			正しいです	正しいです	いいえ	いいえ

トップに戻る

Google Cloudコンピューティング

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン
V1

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		IPS	実施しました	HTTPS	
		製造元	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
		名前	実施しました	HTTPS	
		OID	実施しました	HTTPS	
	情報	API概要 の略	実施しました	HTTPS	
		API名	実施しました	HTTPS	
		APIのバージョン	実施しました	HTTPS	
		データソース名	実施しました	HTTPS	情報
		日付	実施しました	HTTPS	
		発信者ID	実施しました	HTTPS	
		Originatorキー	実施しました	HTTPS	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

					てのディスクでの読み取り/書き込み）（MB/秒）
プロダクト	カテゴリ	フィーチャー/属性ルール（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			実施しました	HTTPS	
	VM	合計容量	実施しました	HTTPS	
		合計CPU利用率	実施しました	HTTPS	
		IOPS読み取り	実施しました	HTTPS	ディスク上の読み取りIOPSの数
		diskIops.total	実施しました	HTTPS	
		ディスクIOPS書き込み	実施しました	HTTPS	
		レイテンシ合計	実施しました	HTTPS	
		ディスクスループット読み込み	実施しました	HTTPS	
		スループット読み取り	実施しました	HTTPS	ディスクの合計スループット読み取り
		ディスクスループット書き込み	実施しました	HTTPS	
		IPスループット読み込み	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	IPスループットの合計
		ipThroughput書き込み	実施しました	HTTPS	
		合計メモリ利用率	実施しました	HTTPS	
		swapRate.inRate	実施しました	HTTPS	
		スワップレート	実施しました	HTTPS	
		合計スワップレート	実施しました	HTTPS	
		待機時間をスケジュールします	実施しました	HTTPS	スケジュールされた時間の待機時間（パーセント）

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Google Compute Platform REST API	HTTPS		443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

HDS HCP（HTTPS）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
Hitachi Content Platform の略	9.3.7.2 9.5.0.121

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
	ストレージノード	名前	実施しました	HTTPS	
		UUID	実施しました	HTTPS	
	ストレージプール	DWH容量に含める	実施しました	HTTPS	ACQからcotnrolまでの間には、DWH容量に興味深いストロークプールがあります
		名前	実施しました	HTTPS	
		物理ディスク容量（MB）	実施しました	HTTPS	ストレージプールの物理容量として使用されます
		RAID グループ	実施しました	HTTPS	このストレージプールがRAIDグループかどうかを示します
		使用可能な物理比率	実施しました	HTTPS	使用可能容量から物理容量への変換率
		ソフトリミット（MB）	実施しました	HTTPS	ボリュームの作成またはサイズ変更処理で定義される論理ボリュームサイズ
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニングがサポートされます	実施しました	HTTPS	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		合計割り当て済み容量	実施しました	HTTPS	
		合計使用容量	実施しました	HTTPS	合計容量（MB）
		を入力します	ギャップ	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
					込み）（MB/秒）
		スループット書き込み	実施しました		
		利用率の合計	実施しました		
	StoragePoolディスク	合計容量	実施しました		
		使用容量の比率	実施しました		
		プロビジョニング済み容量	実施しました		
		使用済み容量	実施しました		
		物理容量	実施しました		
		容量のソフトリミット	実施しました		
		オーバーコミット容量率です	実施しました		時系列で報告されます

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
HDS HCP REST API	HTTPS	HTTPS	9 -90だ		正しいです	正しいです	正しいです	正しいです

トップに戻る

HiCommand Device Managerの略

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン	モデル	ファームウェアバージョン
7.6.1 8.7.7 8.8.1 8.8.3 8.8.5	DF850MH DF850S HM800 HM850 P9500 RAID 700 RAID 800 VSP5000 XP24000 XP7	0983/A-H 0988/H-S DKC：60-08-22 DKC：60-08-65 DKC：70-06-46 DKC：70-06-67-00/00 DKC：80-06-80 DKC：80-06-82-00/00 DKC：80-06-86-00/00 DKC：80-06-87 DKC：80-06-88-00/00 DKC：80-06-91 DKC：80-06-91-00/00 DKC：80-06-93-00/00 DKC：83-05-45-40/00 DKC：83-05-45-60/00 DKC：83-05-46-60/00 DKC：83-05-47-60/00 DKC：83-05-48-40/00 DKC：83-05-48-60/00 DKC：88-08-08-60/00 DKC：88-08-09-60/00 DKC：90-08-81-00/00 DKC：90-08-83-00/01 SVP：60-08-21/00 SVP：60-08-54/00 SVP：70-06-32/00 SVP：70-06-51/00 SVP：80-06-76/02 SVP：80-06-78/00 SVP：80-06-81/00 SVP：80-06-82/00 SVP：80-06-83/00 SVP：80-06-86/00 SVP：80-06-88/00 SVP：83-05-49-40/00 SVP：83-05-49-60/00 SVP：83-05-50-60/00 SVP：83-05-51-60/00 SVP：83-05-52-40/00 SVP：83-05-52-60/00 SVP：88-08-10-60/00 SVP：88-08-11-60/00 SVP：90-08-81/00 SVP：90-08-83/00

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		シンプロビジョニング	実施しました	HDS XML API	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			ギャップ	HDS XML API	
		使用済み容量	実施しました	HDS XML API	
		仮想	実施しました	HDS XML API	ストレージ仮想化デバイスですか？
	ボリュームマップ	LUN	実施しました	HDS XML API	バックエンドLUNの名前
		マスキングが必要です	実施しました	HDS XML API	
		Protocol Controller（プロトコルコントローラ）	実施しました	HDS XML API	
		ストレージポート	実施しました	HDS XML API	
	ボリュームマスク	イニシエータ	実施しました	HDS XML API	
		Protocol Controller（プロトコルコントローラ）	実施しました	HDS XML API	
		ストレージポート	実施しました	HDS XML API	
	ボリュームメンバー	名前	実施しました	HDS XML API	
		ストレージプールID	実施しました	HDS XML API	
		ランク	実施しました	HDS XML API	
		シリンダ	実施しました	HDS XML API	
		容量	実施しました	HDS XML API	Snapshotの使用容量（MB単位）
		合計物理容量	実施しました	HDS XML API	合計物理容量（アレイ上のすべてのディスクの合計）
		使用済み容量	実施しました	HDS XML API	
	WWNエイリアス	ホストのエイリアス	実施しました	HDS XML API	
		オブジェクトタイプ（ Object Type ）	実施しました	HDS XML API	
		ソース	実施しました	HDS XML API	
		WWN	実施しました	HDS XML API	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

				ト/CLI	
		容量のソフトリミット	実施しました	エクスポート/CLI	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		容量率です	実施しました	エクスポート/CLI	時系列で報告されます
	ボリューム	レイテンシ合計	実施しました	エクスポート/CLI	
		IOPS読み取り	実施しました	エクスポート/CLI	ディスク上の読み取りIOPSの数
		レイテンシ読み取り	実施しました	エクスポート/CLI	
		キャッシュヒット率読み取り	実施しました	エクスポート/CLI	
		IOPS -書き込み	実施しました	エクスポート/CLI	
		キャッシュヒット率の合計	実施しました	エクスポート/CLI	
		キャッシュヒット率書き込み	実施しました	エクスポート/CLI	
		スループット読み取り	実施しました	エクスポート/CLI	
		スループット書き込み	実施しました	エクスポート/CLI	
		合計スループット	実施しました	エクスポート/CLI	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		IOPSの合計	実施しました	エクスポート/CLI	
		レイテンシライト	実施しました	エクスポート/CLI	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
エクスポートユーティリティ（USPV）/SNM CLI（AMS）	エクスポート/CLI				いいえ	いいえ	いいえ	いいえ
HiCommand Device Manager XML API	HDS XML API	HTTP / HTTPS	2001年		正しいです	正しいです	正しいです	正しいです

トップに戻る

Hitachi Ops Center の略

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
VSP 5100 VSP 5500 VSP F1500 VSP F600 VSP G800	80-06-92-00/00:01-65-03/05 83-05-46-60/00：01-65-03/05 83-05-47-40/00：01-65-03/05 83-05-48-40/00：01-65-03/05 90-08-81-00/00：01-65-03/05 90-08-82-00/00：01-65-03/05

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		ターゲットストレージ	実施しました		
		テクノロジ	実施しました		ストレージ効率化の情報
プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
	ボリューム	容量	実施しました		Snapshotの使用容量（MB単位）
		ジャンクションパス	実施しました		
		名前	実施しました		
		保護タイプ	実施しました		
		合計物理容量	実施しました		合計物理容量（アレイ上のすべてのディスクの合計）
		ストレージプールID	実施しました		
		シンプロビジョニング	実施しました		
		を入力します	ギャップ		
		使用済み容量	実施しました		
		圧縮が有効になりました	実施しました		
	ボリュームマップ	LUN	実施しました		バックエンドLUNの名前
		マスキングが必要です	実施しました		
		Protocol Controller（プロトコルコントローラ）	実施しました		
		ストレージポート	実施しました		
		を入力します	ギャップ		
	ボリュームマスク	イニシエータ	実施しました		
		Protocol Controller（プロトコルコントローラ）	実施しました		
		ストレージポート	実施しました		
		を入力します	ギャップ		

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

ト	ト				合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		IOPSの合計	実施しました		
	StoragePoolディスク	合計容量	実施しました		
		使用容量の比率	実施しました		
		プロビジョニング済み容量	実施しました		
		使用済み容量	実施しました		
		物理容量	実施しました		
		容量のソフトリミット	実施しました		
		オーバーコミット容量率です	実施しました		時系列で報告されます

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Hitachi Ops Center REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

HDS HNAS（CLI）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
G600 G800 HNAS 4080 HNAS 4100 N800	13.9.6918.05 14.5.7413.01 14.6.7520.04

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					を説明するフリーテキスト
		メモリサイズ	ギャップ	SSH	デバイスメモリ
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報（MB単位）
		プロセッサ数	実施しました	SSH	デバイスCPU
	ストレージプール	ストレージプールID	実施しました	SSH	
		名前	実施しました	SSH	
		を入力します	ギャップ	SSH	
		シンプロビジョニングがサポートされます	実施しました	SSH	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		DWH容量に含める	実施しました	SSH	ACQからcotnrolまでの間には、DWH容量に興味深いストロークプールがあります
		重複排除が有効です	実施しました	SSH	ストレージプールで重複排除が有効になっている
		仮想	実施しました	SSH	ストレージ仮想化デバイスですか？
		RAID グループ	実施しました	SSH	このストレージプールがRAIDグループかどうかを示します
		Snapshotの使用容量	実施しました	SSH	
		データの使用容量	実施しました	SSH	
		合計使用容量	実施しました	SSH	合計容量（MB）
		合計割り当て済み容量	実施しました	SSH	
		使用可能な物理比率	実施しました	SSH	使用可能容量から物理容量への変換率

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
HDS HNAS CLI	SSH	SSH	22.		正しいです	正しいです	正しいです	正しいです

トップに戻る

HPE Nimble / Alletra 6000ストレージ

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン	モデル	ファームウェアバージョン
V1	6030 AF1000 AF20Q AF3000 AF40 AF5000 CS1000 CS300 CS3000 CS500 CS5000 HF20 HF20H HF40 HF60	5.0.10.0-742719 -オプション 5.0.7.0-604814 -オプト 5.0.8.0-677726 -オプション 5.2.1.1000-1017822 -オプション 5.2.1.400-796142-opt 5.2.1.600-841103 -オプト 5.2.1.700-882343 -opt 5.2.1.800-930936 -オプション 5.2.1.900-1003439 -オプション 6.0.0.300-956221-OPT 6.0.0.400-991061 -オプト 6.1.1.200-1020304 -オプション 6.1.1.300-1028597 -オプション

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					化デバイスですか？
プロダクト	カテゴリ	圧縮が有効になりました	実施しましたステータス	HTTPS使用するプロトコル	追加情報
		フィーチャー/属性（Feature/Attribute）	実施しました	HTTPS	
	ボリュームマップ	LUN	実施しました	HTTPS	バックエンドLUNの名前
		マスキングが必要です	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	WWNエイリアス	ホストのエイリアス	実施しました	HTTPS	
		オブジェクトタイプ（ Object Type ）	実施しました	HTTPS	
		ソース	実施しました	HTTPS	
		WWN	実施しました	HTTPS	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					のディスクでの読み取り/書き込み）（MB/秒）
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			実施しました	HTTPS	
	ボリューム	物理容量	実施しました	HTTPS	
		合計容量	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		使用容量の比率	実施しました	HTTPS	
		圧縮による総削減量	実施しました	HTTPS	
		圧縮による削減スペース	実施しました	HTTPS	
		IOPS読み取り	実施しました	HTTPS	ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました	HTTPS	
		IOPS -書き込み	実施しました	HTTPS	
		レイテンシ読み取り	実施しました	HTTPS	
		レイテンシ合計	実施しました	HTTPS	
		レイテンシライト	実施しました	HTTPS	
		スループット読み取り	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
HP Nimble REST API	HTTPS	HTTPS	5392		正しいです	いいえ	正しいです	正しいです

トップに戻る

HUAWEI OceanStor（REST / HTTPS）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
5300 V5 5500 V3 5500 V5 5800 V3 Dorado 5000 V6 SAS Dorado 6000 V3 Dorado 6000 V6 NVMe	V300R001C01 V300R002C10 V300R006C20 V300R006C50 V500R007C10 V500R007C30 V600R003C00 V600R005C03

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		合計使用容量	実施しました	HTTPS	合計容量（MB）
		を入力します	ギャップ	HTTPS	
プロダクト	カテゴリ	仮想ーチャー/属性（**Feature/Attribute**）	実施しました	使用するプロトコル	追加情報ジ仮想化デバイスですか？
	ボリューム	容量	実施しました	HTTPS	Snapshotの使用容量（MB単位）
		ジャンクションパス	実施しました	HTTPS	
		名前	実施しました	HTTPS	
		合計物理容量	実施しました	HTTPS	合計物理容量（アレイ上のすべてのディスクの合計）
		冗長性	実施しました	HTTPS	冗長性レベル
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニング	実施しました	HTTPS	
		UUID	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？
	ボリュームマップ	LUN	実施しました	HTTPS	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

		IOPSの合計	実施しました	HTTPS	
		レイテンシライト	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		書き込み率の合計	実施しました	HTTPS	
	ボリューム	キャッシュヒット率読み取り	実施しました	HTTPS	
		キャッシュヒット率の合計	実施しました	HTTPS	
		キャッシュヒット率書き込み	実施しました	HTTPS	
		物理容量	実施しました	HTTPS	
		合計容量	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		使用容量の比率	実施しました	HTTPS	
		IOPS読み取り	実施しました	HTTPS	ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました	HTTPS	
		IOPS -書き込み	実施しました	HTTPS	
		レイテンシ読み取り	実施しました	HTTPS	
		レイテンシ合計	実施しました	HTTPS	
		レイテンシライト	実施しました	HTTPS	
		スループット読み取り	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Huawei OceanStor REST API	HTTPS	HTTPS	8088年		正しいです	正しいです	正しいです	正しいです

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Huawei OceanStor パフォーマンスREST API	HTTPS	HTTPS	8088年		正しいです	いいえ	正しいです	正しいです

トップに戻る

IBM Cleversafe

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		UUID	実施しました	HTTPS	
		バージョン	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	ソフトウェアバージョン 追加情報
		管理IPアドレス	実施しました	HTTPS	
	ストレージプール	DWH容量に含める	実施しました	HTTPS	ACQからcotnrolまでの間には、DWH容量に興味深いストロークプールがあります
		名前	実施しました	HTTPS	
		物理ディスク容量（MB）	実施しました	HTTPS	ストレージプールの物理容量として使用されます
		RAID グループ	実施しました	HTTPS	このストレージプールがRAIDグループかどうかを示します
		使用可能な物理比率	実施しました	HTTPS	使用可能容量から物理容量への変換率
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニングがサポートされます	実施しました	HTTPS	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		合計割り当て済み容量	実施しました	HTTPS	
		合計使用容量	実施しました	HTTPS	合計容量（MB）
		を入力します	ギャップ	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
IBM Cleversafe REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

IBM DS 8K（DSCLI）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
2107-951 2107-961 2107-985 2107-996	7.6.31.4250 7.7.51.1400 7.8.57.18 7.9.21.91 7.9.32.126

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		Protocol Controller（プロトコルコントローラ）	実施しました	DSNI	
プロダクト	カテゴリ	フィーチャー/属性ドレベル（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
			実施しました	DSNI	
	WWNエイリアス	ホストのエイリアス	実施しました	DSNI	
		ホストOS	実施しました	DSNI	
		オブジェクトタイプ（ Object Type ）	実施しました	DSNI	
		ソース	実施しました	DSNI	
		WWN	実施しました	DSNI	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		書き込み			
		読み取り利用率	実施しました	DSNI	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		利用率の合計	実施しました	DSNI	
		利用率ライト	実施しました	DSNI	
	ボリューム	キャッシュヒット率読み取り	実施しました	DSNI	
		キャッシュヒット率の合計	実施しました	DSNI	
		キャッシュヒット率書き込み	実施しました	DSNI	
		物理容量	実施しました	DSNI	
		合計容量	実施しました	DSNI	
		IOPS読み取り	実施しました	DSNI	ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました	DSNI	
		IOPS -書き込み	実施しました	DSNI	
		レイテンシ読み取り	実施しました	DSNI	
		レイテンシ合計	実施しました	DSNI	
		レイテンシライト	実施しました	DSNI	
		スループット読み取り	実施しました	DSNI	
		合計スループット	実施しました	DSNI	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	DSNI	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
データソースウィザードの設定	手動入力				正しいです	正しいです	正しいです	正しいです

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
IBM DS CLI	DSNI	DSNI			正しいです	正しいです	正しいです	正しいです

トップに戻る

IBM PowerVM（SSH）

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		プロセッサ	実施しました	SSH	
	仮想マシンディスク	OID	実施しました	SSH	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		VirtualDisk OID	実施しました	SSH	
		仮想マシンOID	実施しました	SSH	
	ホスト	ホストのCPU数	実施しました	SSH	
		ホストインストールメモリ	実施しました	SSH	
		ホストモデル	実施しました	SSH	
		NIC数	実施しました	SSH	
		IPS	実施しました	SSH	
		製造元	実施しました	SSH	
		名前	実施しました	SSH	
		OID	実施しました	SSH	
		プラットフォームタイプ	実施しました	SSH	
	情報	データソース名	実施しました	SSH	情報
		日付	実施しました	SSH	
		発信者ID	実施しました	SSH	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
IBM Hardware Management Console SSHアクセス	SSH	SSH	22.		正しいです	いいえ	正しいです	正しいです

トップに戻る

IBM SVC（CLI）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
2072-12F	1.5.2.7
2072-12G	1.6.1.2
2072-2N4	1.6.1.4
2072-324	1.6.1.5
2072-3H4	7.5.0.11
2072-3N4	7.5.0.12
2076-124	7.7.1.8
2076-12F	7.8.1.14
2076-224	7.8.1.6
2076-24F	7.8.1.8
2076-24G	8.2.1.10
2076-624	8.2.1.11
2076-724	8.2.1.14
2076-824	8.2.1.9
2076-AF6	8.3.1.1
2076 - AFF	8.3.1.2
2077-24F	8.3.1.5
2077-424	8.3.1.6
2078-12F	8.3.1.7
2078-224	8.3.1.9
2078-24c	8.4.0.10
2078-24F	8.4.0.11
2078-324	8.4.0.6
2078-424	8.4.0.7
2078-4H4	8.4.0.8
2078-92G	8.4.0.9
2078-AF3	8.5.0.5
4657-924	8.5.0.6
4662-12G	8.5.0.7
4662-6H2	8.5.0.8
4666-AH8	8.5.0.9
9843-AE2	8.5.2.2
9843-AE3	8.5.3.1
9846-AG8	8.5.4.0
9848-AE2	
9848-AF7	
9848-AF8	
9848-AG8	
SVC（サービス）	

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		書き込み済み容量	実施しました	SSH	ホストによってこのボリュームに書き込まれた合計容量（MB）
プロダクト	カテゴリ	フィーチャー/属性 Feature/Attribute	ステータス	使用するプロトコル	追加情報
		圧縮が有効になった	実施しました	SSH	
		暗号化	実施しました	SSH	
	ボリュームマップ	LUN	実施しました	SSH	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	SSH	
		ストレージポート	実施しました	SSH	
	ボリュームマスク	イニシエータ	実施しました	SSH	
		Protocol Controller（プロトコルコントローラ）	実施しました	SSH	
		ストレージポート	実施しました	SSH	
		を入力します	ギャップ	SSH	
	WWNエイリアス	ホストのエイリアス	実施しました	SSH	
		オブジェクトタイプ（ Object Type ）	実施しました	SSH	
		ソース	実施しました	SSH	
		WWN	実施しました	SSH	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		き込み			
		読み取り利用率	実施しました	SSH	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		利用率の合計	実施しました	SSH	
		利用率ライト	実施しました	SSH	
	ボリューム	キャッシュヒット率読み取り	実施しました	SSH	
		キャッシュヒット率の合計	実施しました	SSH	
		キャッシュヒット率書き込み	実施しました	SSH	
		物理容量	実施しました	SSH	
		合計容量	実施しました	SSH	
		使用済み容量	実施しました	SSH	
		書き込み済み容量	実施しました	SSH	
		使用容量の比率	実施しました	SSH	
		容量比率の書き込み	実施しました	SSH	
		IOPS読み取り	実施しました	SSH	ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました	SSH	
		IOPS -書き込み	実施しました	SSH	
		レイテンシ読み取り	実施しました	SSH	
		レイテンシ合計	実施しました	SSH	
		レイテンシライト	実施しました	SSH	
		スループット読み取り	実施しました	SSH	
		合計スループット	実施しました	SSH	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	SSH	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
IBM SVC CLI	SSH	SSH	22.		正しいです	いいえ	正しいです	正しいです

トップに戻る

IBM XIVおよびA9000（XIVCLI）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
415 A14	10.2.4.e 12.3.2.c

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					
990					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		合計使用容量	実施しました	XIV CLIの	合計容量（MB）
		を入力します	ギャップ	XIV CLIの	
プロダクト	カテゴリ	仮想ーチャー/属性（**Feature/Attribute**）	実施しました	使用するプロトコル	追加情報ジ仮想化デバイスですか？
	ボリューム	容量	実施しました	XIV CLIの	Snapshotの使用容量（MB単位）
		ディスクグループ	実施しました	XIV CLIの	ディスクグループタイプ
		ディスクタイプ	使用できません	XIV CLIの	
		名前	実施しました	XIV CLIの	
		qtree ID	実施しました	XIV CLIの	qtreeの一意のID
		合計物理容量	実施しました	XIV CLIの	合計物理容量（アレイ上のすべてのディスクの合計）
		冗長性	実施しました	XIV CLIの	冗長性レベル
		ストレージプールID	実施しました	XIV CLIの	
		シンプロビジョニング	実施しました	XIV CLIの	
		を入力します	ギャップ	XIV CLIの	
		使用済み容量	実施しました	XIV CLIの	
		圧縮が有効になりました	実施しました	XIV CLIの	
	ボリュームマップ	LUN	実施しました	XIV CLIの	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	XIV CLIの	
	ボリュームマスク	イニシエータ	実施しました	XIV CLIの	
		Protocol Controller（プロトコルコントローラ）	実施しました	XIV CLIの	
	WWNエイリアス	ホストのエイリアス	実施しました	XIV CLIの	
		ホストOS	実施しました	XIV CLIの	
		オブジェクトタイプ（ Object Type ）	実施しました	XIV CLIの	
		ソース	実施しました	XIV CLIの	
		WWN	実施しました	XIV CLIの	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

		使用済み容量	実施しました	DSNI	
		物理容量	実施しました	DSNI	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		容量率です	実施しました	DSNI	時系列で報告されます
	ボリューム	レイテンシ合計	実施しました	DSNI	
		レイテンシ読み取り	実施しました	DSNI	
		IOPS -書き込み	実施しました	DSNI	
		圧縮による削減スペース	実施しました	DSNI	
		スループット読み取り	実施しました	DSNI	
		IOPSの合計	実施しました	DSNI	
		レイテンシライト	実施しました	DSNI	
		IOPS読み取り	実施しました	DSNI	ディスク上の読み取りIOPSの数
		キャッシュヒット率読み取り	実施しました	DSNI	
		圧縮による総削減量	実施しました	DSNI	
		キャッシュヒット率の合計	実施しました	DSNI	
		キャッシュヒット率書き込み	実施しました	DSNI	
		スループット書き込み	実施しました	DSNI	
		合計スループット	実施しました	DSNI	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
IBM DS CLI	DSNI	DSNI			正しいです	正しいです	正しいです	正しいです
IBM XIV CLIの	XIV CLIの	TCP	7778年だ		正しいです	いいえ	正しいです	いいえ

トップに戻る

Infinidat Infinibox（HTTP）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
F6230 F6240 F6303 F6304	6.0.31.0 7.0.14.20

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		トコルコントローラ）			
プロダクト	カテゴリ	を入力します フィーチャー/属性（Feature/Attribute）	ギャップ ステータス 実施しました	HTTPS 使用するプロトコル HTTPS	追加情報
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
		ストレージポート	実施しました	HTTPS	
	WWNエイリアス	ソース	実施しました	HTTPS	
		ホストのエイリアス	実施しました	HTTPS	
		WWN	実施しました	HTTPS	
		オブジェクトタイプ（ Object Type ）	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Infinidat REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

Microsoft Azureコンピューティング

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン
2018-06-01

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		IPS	実施しました	HTTPS	
		製造元	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
		名前	実施しました	HTTPS	
		OID	実施しました	HTTPS	
	情報	API概要 の略	実施しました	HTTPS	
		API名	実施しました	HTTPS	
		APIのバージョン	実施しました	HTTPS	
		データソース名	実施しました	HTTPS	情報
		日付	実施しました	HTTPS	
		発信者ID	実施しました	HTTPS	
		Originatorキー	実施しました	HTTPS	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス	データストア	プロビジョニング済み容量	実施しました	HTTPS	
		合計容量	実施しました	HTTPS	
		オーバーコミット容量率です	実施しました	HTTPS	時系列で報告されます
	仮想ディスク	合計容量	実施しました	HTTPS	
		IOPS読み取り	実施しました	HTTPS	ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました	HTTPS	
		IOPS -書き込み	実施しました	HTTPS	
		スループット読み取り	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	
	VM	合計CPU利用率	実施しました	HTTPS	
		IOPS読み取り	実施しました	HTTPS	ディスク上の読み取りIOPSの数
		diskIops.total	実施しました	HTTPS	
		ディスクIOPS書き込み	実施しました	HTTPS	
		ディスクスループット読み込み	実施しました	HTTPS	
		スループット読み取り	実施しました	HTTPS	ディスクの合計スループット読み取り
		ディスクスループット書き込み	実施しました	HTTPS	
		IPスループット読み込み	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	IPスループットの合計
		ipThroughput書き込み	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Microsoft Azure Compute REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

Microsoft Hyper-V

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					
1012					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		使用済み容量	実施しました	WMI	
	仮想マシンディスク	OID	実施しました	WMI	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		VirtualDisk OID	実施しました	WMI	
		仮想マシンOID	実施しました	WMI	
	ホスト	ホストのCPU数	実施しました	WMI	
		ホストのCPU速度	実施しました	WMI	
		ホストドメイン	実施しました	WMI	
		ホストインストールメモリ	実施しました	WMI	
		ホストモデル	実施しました	WMI	
		NIC数	実施しました	WMI	
		NIC速度	実施しました	WMI	
		IPS	実施しました	WMI	
		製造元	実施しました	WMI	
		名前	実施しました	WMI	
		OID	実施しました	WMI	
		プラットフォームタイプ	実施しました	WMI	
	iSCSIノード	ホストのエイリアス	実施しました	WMI	
		ノード名	実施しました	WMI	
		OID	実施しました	WMI	
		を入力します	ギャップ	WMI	
	情報	データソース名	実施しました	WMI	情報
		日付	実施しました	WMI	
		発信者ID	実施しました	WMI	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					
1016					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					てのディスクでの読み取り/書き込み）（MB/秒）
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			実施しました	WS-Management	
	VM	合計容量	実施しました	WS-Management	
		使用済み容量	実施しました	WS-Management	
		使用容量の比率	実施しました	WS-Management	
		合計CPU利用率	実施しました	WS-Management	
		IOPS読み取り	実施しました	WS-Management	ディスク上の読み取りIOPSの数
		diskIops.total	実施しました	WS-Management	
		ディスクIOPS書き込み	実施しました	WS-Management	
		レイテンシ合計	実施しました	WS-Management	
		ディスクスループット読み込み	実施しました	WS-Management	
		スループット読み取り	実施しました	WS-Management	ディスクの合計スループット読み取り
		ディスクスループット書き込み	実施しました	WS-Management	
		IPスループット読み込み	実施しました	WS-Management	
		合計スループット	実施しました	WS-Management	IPスループットの合計
		ipThroughput書き込み	実施しました	WS-Management	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
PowerShell	WS-Management	HTTP	5985		正しいです	いいえ	いいえ	正しいです

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
WMI	WMI	WMI	一三五		正しいです	いいえ	正しいです	正しいです

トップに戻る

NetApp 7-Mode

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン	モデル	ファームウェアバージョン
1.12 1.14 1.17 1.19 1.20 1.21	FAS2040 FAS2050 FAS2220 FAS2240-2 FAS2240-4 FAS2520 FAS2554 FAS3140 FAS3160 FAS3210 FAS3220 FAS3240 FAS3250 FAS3270 FAS6240 FAS6290 FAS8020 FAS8040 FAS8060 FAS8080 N6070 N6240 V3240	7.3.6 8.1.1 7-Mode 8.1.3P2 7-Mode 8.1.4P1 7-Mode 8.1.4P10 7-Mode 8.1.4P9D18 7-Mode 8.2.1 7-Mode 8.2.2 7-Mode 8.2.3 7-Mode 8.2.3P2 7-Mode 8.2.3P3 7-Mode 8.2.4 7-Mode 8.2.4P2 7-Mode 8.2.4P4 7-Mode 8.2.4P5 7-Mode 8.2.4P6 7-Mode 8.2.5 7-Mode 8.2.5P1 7-Mode 8.2.5P2 7-Mode 8.2.5P4 7-Mode 8.2.5P5 7-Mode 8.2P3 7-Mode 8.2P4 7-Mode Data ONTAPリリース7.3.3 Data ONTAPリリース7.3.4 Data ONTAPリリース8.2.5 7-Mode

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					
1020					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		ルID			
		シンプロビジョニング	実施しました		
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		を入力します	ギャップ		
		仮想容量	実施しました		
	ボリュームマップ	LUN	実施しました		バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました		
		を入力します	ギャップ		
	ボリュームマスク	イニシエータ	実施しました		
		Protocol Controller（プロトコルコントローラ）	実施しました		
		ストレージポート	実施しました		
		を入力します	ギャップ		

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		き込み			
		読み取り利用率	実施しました		
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		利用率の合計	実施しました		
		利用率ライト	実施しました		
	ボリューム	物理容量	実施しました		
		合計容量	実施しました		
		使用済み容量	実施しました		
		使用容量の比率	実施しました		
		IO密度読み取り	実施しました		
		IO密度の合計	実施しました		
		書き込みI/O密度	実施しました		
		IOPS読み取り	実施しました		ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました		
		IOPS -書き込み	実施しました		
		レイテンシ読み取り	実施しました		
		レイテンシ合計	実施しました		
		レイテンシライト	実施しました		
		部分ブロック率	実施しました		
		スループット読み取り	実施しました		
		合計スループット	実施しました		ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました		
		書き込み保留中です	実施しました		合計書き込み保留中です

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
NetApp 7-Mode ZAPI	ZAPI	ZAPI			正しいです	正しいです	正しいです	正しいです

トップに戻る

NetApp Cloud Volumes Service の略

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
AWS Cloud Volumes	V1

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					
1040					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		失敗した物理容量	実施しました		障害が発生したディスクの物理容量（障害が発生したディスクの合計）
プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
	ストレージプール	ストレージプールID	実施しました		
		名前	実施しました		
		を入力します	ギャップ		
		シンプロビジョニングがサポートされます	実施しました		この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		DWH容量に含める	実施しました		ACQからcotnrolまでの間には、DWH容量に興味深いストロークプールがあります
		仮想	実施しました		ストレージ仮想化デバイスですか？
		RAID グループ	実施しました		このストレージプールがRAIDグループかどうかを示します
		Snapshotの使用容量	実施しました		
		データの使用容量	実施しました		
		データの割り当て容量	ギャップ		データに割り当てられている容量
		合計使用容量	実施しました		合計容量（MB）
		合計割り当て済み容量	実施しました		
		物理ディスク容量（MB）	実施しました		ストレージプールの物理容量として使用されます
		使用可能な物理比率	実施しました		使用可能容量から物理容量への変換率

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Cloud Volumes Service REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

NetApp ONTAP 対応の Amazon FSX

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
FSX for ONTAP の略	Data ONTAP

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		トコルコントローラ）			
プロダクト	カテゴリ	ストレージポート/フィーチャー/属性（Feature/Attribute）を入力します	実施しましたステータス	HTTPS使用するプロトコル	追加情報
			ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
パフォーマンス	ストレージ	障害ディスク	実施しました	HTTPS	
	ストレージノード	キャッシュヒット率の合計	実施しました	HTTPS	
		読み取られたディスクの合計数	実施しました	HTTPS	
		利用率の合計	実施しました	HTTPS	
	qtree		実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
NetApp ONTAP API	HTTP / HTTPS	HTTP / HTTPS	80対443		正しいです	正しいです	正しいです	正しいです

トップに戻る

NetApp clustered Data ONTAP 8.1.1+

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
AFF-A150 AFF-A200 AFF-A220 AFF-A250 AFF-A300 AFF-A320 AFF-A400 AFF-A700 AFF-A700s AFF-A800 AFF-A900 AFF-C190 AFF-C250 AFF-C400 AFF-C800 AFF8020 AFF8040 AFF8060の場合 AFF8080 CDvM100 CDvM200 DM5000H FAS2240-2 FAS2240-4 FAS2520 FAS2552 FAS2554 FAS2620 FAS2650 FAS2720 FAS2750 FAS3220 FAS3250 FAS3270 FAS500f FAS6210 FAS6220 FAS8020 FAS8040 FAS8060 FAS8080 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FASDvM300 シムボックス V6240	8.2.3P5 8.3.0 8.3.1 8.3.1P2 8.3.2 8.3.2P12 8.3.2P2 8.3.2P5 9.0.1 9.1.0 9.1.0P1 9.1.0P10 9.1.0P11 9.1.0P12 9.1.0P14 9.1.0P15 9.1.0P17 9.1.0P19 9.1.0P20 9.1.0P5 9.1.0P7 9.1.0P8 9.10.0 9.10.1 9.10.1P1 9.10.1P10 9.10.1P11 9.10.1P12 9.10.1P13 9.10.1P2 9.10.1P3 9.10.1P4 9.10.1P5 9.10.1P6 9.10.1P7 9.10.1P8 9.10.1P9 9.11.0P1 9.11.1 9.11.1P1 9.11.1P10 9.11.1P2 9.11.1P3 9.11.1P4 9.11.1P5 9.11.1P6 9.11.1P7 9.11.1P8 9.11.1P9 9.11.1X12 9.11.1X26 9.12.1: 9.12.1P1 9.12.1P2

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		QoS制限IOPS	実施しました	HTTPS	
		QoS制限MBps	実施しました	HTTPS	
		QoS制限（物理）	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		ポリシー	実施しました	HTTPS	
	ボリュームマップ	LUN	実施しました	HTTPS	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					
1082					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					てのディスクでの読み取り/書き込み）（MB/秒）
プロダクト	カテゴリ	フィーチャー/属性ルFeature/Attribute）	ステータス実施しました	使用するプロトコルTTPS	追加情報
	ボリューム	物理容量	実施しました	HTTPS	
		合計容量	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		使用容量の比率	実施しました	HTTPS	
		IO密度読み取り	実施しました	HTTPS	
		IO密度の合計	実施しました	HTTPS	
		書き込みI/O密度	実施しました	HTTPS	
		IOPS読み取り	実施しました	HTTPS	ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました	HTTPS	
		IOPS -書き込み	実施しました	HTTPS	
		レイテンシ読み取り	実施しました	HTTPS	
		レイテンシ合計	実施しました	HTTPS	
		レイテンシライト	実施しました	HTTPS	
		部分ブロック率	実施しました	HTTPS	
		スループット読み取り	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
NetApp ONTAP API	HTTP / HTTPS	HTTP / HTTPS	80対443		正しいです	正しいです	正しいです	正しいです

トップに戻る

NetApp SolidFire 8.1+

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
H410S-2 H610S-2 H610S-4 SF19210 のサポート SF2405 のように指定する SF38410 SF4805 SF9605 SF9608 FCN001 H300S H410S-0 H410S-1 H410S-2 H500S H610S-1 H610S-2 H610S-4 H610S2 SF19210 のサポート SF38410 SF4805 SF9605	11.1.0.72 11.5.0.63 11.7.0.76 11.8.0.23 12.0.0.333 12.2.0.777 12.3.0.958 12.3.1.103 12.3.1.165 12.3.2.3 12.5.0.897 12.7.0.380

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					
1092					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		トIOPS			
		QoS制限IOPS	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
		QoS最小IOPS	実施しました	HTTPS	
		QoSポリシー（**QoS**）	実施しました	HTTPS	
	ボリュームマップ	LUN	実施しました	HTTPS	バックエンドLUNの名前
		マスキングが必要です	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					
1100					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		果				
		その他の合計容量	実施しました	HTTPS		
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報	
		その他の使用容量	実施しました	HTTPS		
	ボリューム	物理容量	実施しました	HTTPS		
		合計容量	実施しました	HTTPS		
		使用済み容量	実施しました	HTTPS		
		使用容量の比率	実施しました	HTTPS		
		圧縮による総削減量	実施しました	HTTPS		
		IOPS読み取り	実施しました	HTTPS	ディスク上の読み取りIOPSの数	
		IOPSの合計	実施しました	HTTPS		
		IOPS -書き込み	実施しました	HTTPS		
		レイテンシ読み取り	実施しました	HTTPS		
		レイテンシ合計	実施しました	HTTPS		
		レイテンシライト	実施しました	HTTPS		
		部分ブロック率	実施しました	HTTPS		
		スループット読み取り	実施しました	HTTPS		
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）	
		スループット書き込み	実施しました	HTTPS		
		利用率の合計	実施しました	HTTPS		

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
SolidFire REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

NetApp StorageGRID（HTTPS）

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン	モデル	ファームウェアバージョン
3.0 3.2 3.3 3.4 3.5.	Webスケール	11.2.0 11.4.0 11.4.0.3 11.4.0.4 11.5.0.1 11.5.0.11 11.5.0.2 11.5.0.3 11.5.0.6 11.5.0.7 11.5.0.8 11.5.0.9 11.6.0 11.6.0.1 11.6.0.10 11.6.0.2 11.6.0.4 11.6.0.5 11.6.0.7 11.6.0.8 11.6.0.9 11.7.0

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					
1106					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		量利用率（MB）			
		ノード-使用済み容量-使用済みメタデータ（MB）	実施しました	HTTPS	
プロダクト	カテゴリ	ユニティ（属性（Feature/Attribute）名	ステータス	使用するプロトコル	追加情報
			実施しました	HTTPS	
	ストレージプール	DWH容量に含める	実施しました	HTTPS	ACQからcotnrolまでの間には、DWH容量に興味深いストロークプールがあります
		名前	実施しました	HTTPS	
		物理ディスク容量（MB）	実施しました	HTTPS	ストレージプールの物理容量として使用されます
		RAID グループ	実施しました	HTTPS	このストレージプールがRAIDグループかどうかを示します
		使用可能な物理比率	実施しました	HTTPS	使用可能容量から物理容量への変換率
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニングがサポートされます	実施しました	HTTPS	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		合計割り当て済み容量	実施しました	HTTPS	
		合計使用容量	実施しました	HTTPS	合計容量（MB）
		を入力します	ギャップ	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

								のディスクの合計）
プロダクト	カテゴリ	ストレージプールの容量	実施しました	使用するプロトコル	追加情報			
		物理容量	実施しました					
	ストレージノード	ノード容量利用率-許容されるメタデータ	実施しました					
		ノードの容量利用率-合計	実施しました					
		ノード-使用可能容量利用率	実施しました					
		ノード使用容量利用率	実施しました					
		ノード-容量使用状況-使用済みメタデータ	実施しました					
		スループット読み取り	実施しました					
		合計スループット	実施しました					ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました					
	StoragePoolディスク	プロビジョニング済み容量	実施しました					
物理容量		実施しました			合計容量			
実施しました				使用済み容量	実施しました			
			オーバーコミット容量率です	実施しました				
時系列で報告されます		使用容量の比率	実施しました					

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
StorageGRID REST API	HTTPS	HTTPS	443年		正しいです	いいえ	正しいです	正しいです

トップに戻る

Nutanixストレージ（REST）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
HPE DL360-8 G10 NX-3060-G6 NX-3170-G6 NX-8035-G6 NX-8150-G7 HPE DL360-8 G10 HPE DL380-12 G10 NX-3060-G5 NX-3170-G7 NX-5155-G6 NX-8035-G6 NX-8035-G7 NX-8150-G7 NX-8150-G8	6.5.1.6 6.5.2 6.5.2.5 6.5.2.6 6.5.2.7 6.5.3 6.5.3.1

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		合計割り当て済み容量	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）を入力します	ステータス	使用するプロトコル	追加情報
		合計使用容量	実施しました	HTTPS	合計容量（MB）
			ギャップ	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？
	ボリューム	容量	実施しました	HTTPS	Snapshotの使用容量（MB単位）
		ジャンクションパス	実施しました	HTTPS	
		名前	実施しました	HTTPS	
		qtree ID	実施しました	HTTPS	qtreeの一意のID
		合計物理容量	実施しました	HTTPS	合計物理容量（アレイ上のすべてのディスクの合計）
		冗長性	実施しました	HTTPS	冗長性レベル
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニング	実施しました	HTTPS	
		UUID	実施しました	HTTPS	
	ボリュームマップ	LUN	実施しました	HTTPS	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実施しました	HTTPS	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTPS	
		ストレージポート	実施しました	HTTPS	
		を入力します	ギャップ	HTTPS	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

			てのディスクでの読み取り/書き込み）（MB/秒）		
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
	実施しました	HTTPS		StoragePoolディスク	レイテンシライト
	実施しました	HTTPS			IOPS読み取り
	実施しました	HTTPS	ディスク上の読み取りIOPSの数		IOPSの合計
	実施しました	HTTPS			IOPS -書き込み
	実施しました	HTTPS			スループット読み取り
	実施しました	HTTPS			合計スループット
	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）		スループット書き込み
	実施しました	HTTPS		ボリューム	IOPS読み取り
	実施しました	HTTPS	ディスク上の読み取りIOPSの数		IOPSの合計
	実施しました	HTTPS			IOPS -書き込み
	実施しました	HTTPS			レイテンシ読み取り
	実施しました	HTTPS			レイテンシ合計
	実施しました	HTTPS			レイテンシライト
	実施しました	HTTPS			スループット読み取り
	実施しました	HTTPS			合計スループット
	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）		スループット書き込み

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Nutanix REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

OpenStack（REST API / SSH）

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		アス			
		ノード名	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		OID	実施しました	HTTPS	
		ホスト	ギャップ	HTTPS	
	情報	データソース名	実施しました	HTTPS	情報
		日付	実施しました	HTTPS	
		発信者ID	実施しました	HTTPS	
		Originatorキー	実施しました	HTTPS	
パフォーマンス	データストア	合計容量	実施しました		
		使用容量の比率	実施しました		
		プロビジョニング済み容量	実施しました		
		使用済み容量	実施しました		
		オーバーコミット容量率です	実施しました		時系列で報告されます
	ホスト	合計CPU利用率	実施しました		
		合計メモリ利用率	実施しました		
	仮想ディスク	レイテンシ読み取り	実施しました		
		レイテンシ合計	実施しました		
		レイテンシライト	実施しました		

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
OpenStack REST API	HTTPS	HTTPS	443年		正しいです	いいえ	正しいです	正しいです
OpenStack SSH	SSH	SSH	22.		正しいです	いいえ	正しいです	正しいです

トップに戻る

Oracle ZFS（HTTPS）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
Sun ZFS Storage 7330 Sun ZFS Storage 7335 Sun ZFS Storage 7350 Sun ZFS Storage 7370 Sun ZFS Storage 7420 Sun ZFS Storage 7430 Sun ZFS Storage 7450	1-1.1 1-1.2 1-1.3 1 ~ 1.34 1-1.4 2013.06.05.6.12 2013.06.05.6.15 2013.06.05.7.21 2013.06.05.7.24 2013.06.05.7.25 2013.06.05.7.26 2013.06.05.8.0 2013.06.05.8.26 2013.06.05.8.29 2013.06.05.8.35 2013.06.05.8.37 2013.06.05.8.47 2013.06.05.8.50 2013.06.05.8.53 2013.06.05.8.6 2013.06.05.8.7

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					
1132					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

					アレイ上のすべてのディスクの合計）
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		使用済み容量	実施しました	HTTP/S	
		冗長性	実施しました	HTTP/S	冗長性レベル
	ボリュームマップ	LUN	実施しました	HTTP/S	バックエンドLUNの名前
		ストレージポート	実施しました	HTTP/S	
		マスキングが必要です	実施しました	HTTP/S	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTP/S	
		を入力します	ギャップ	HTTP/S	
	ボリュームマスク	ストレージポート	実施しました	HTTP/S	
		イニシエータ	実施しました	HTTP/S	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTP/S	
		を入力します	ギャップ	HTTP/S	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

					込み）（MB/秒）
		スループット書き込み	実施しました		
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		利用率の合計	実施しました		
	ストレージノードデータ	キーを押します	実施しました		
		サーバID	実施しました		
		スループット読み取り	実施しました		
		スループット書き込み	実施しました		
		合計スループット	実施しました		ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		IOPS読み取り	実施しました		ディスク上の読み取りIOPSの数
		IOPS -書き込み	実施しました		
		IOPSの合計	実施しました		
		キャッシュヒット率の合計	実施しました		
		利用率の合計	実施しました		
	StoragePoolディスク	IOPSの合計	実施しました		
		合計容量	実施しました		
		使用容量の比率	実施しました		
		合計データ容量	実施しました		
		プロビジョニング済み容量	実施しました		
		データの使用容量	実施しました		
		使用済み容量	実施しました		
		その他の使用容量	実施しました		
		物理容量	実施しました		
		オーバーコミット容量率です	実施しました		時系列で報告されます
		Snapshotの使用容量	実施しました		
		Snapshotの使用容量の比率	実施しました		時系列で報告されます

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Oracle ZFS REST API	HTTP / HTTPS	HTTP / HTTPS	215だ		正しいです	正しいです	正しいです	正しいです

トップに戻る

Pure Storage FlashArray（HTTP）

このデータコレクタでサポートされるモデルとバージョン：

モデル	ファームウェアバージョン
DFSC1 FA-420 FA-450 FA-C40R3 FA-C60 FA-C60R3 FA-X10R2 FA-X10R3 FA-X20R2 FA-X20R3 FA-X50R2 FA-X50R3 FA-X70R2 FA-X70R3 FA-X90R2 FA-X90R3 FA-XL130 FA-XL170 fa-m10r2 FA-M20 fa-m20r2 FA-M50 fa-m50r2 FA-M70 fa-m70r2 FA-x70	4.8.8 5.3.14 5.3.15 5.3.17 5.3.18 5.3.20 5.3.21 5.3.6 5.3.8 6.1.10 6.1.11 6.1.13 6.1.14 6.1.15 6.1.17 6.1.18 6.1.19 6.1.21 6.1.22 6.1.23 6.1.5 6.2.13 6.2.7 6.2.9 6.3.10 6.3.11 6.3.12 6.3.2 6.3.5 6.3.6 6.3.7 6.3.9 6.4.3 6.4.4 6.4.5

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		を入力します	ギャップ	HTTP/S	
		使用済み容量	実施しました	HTTP/S	
プロダクト	カテゴリ	仮想ーチャー/属性（**Feature/Attribute**）	実施しました	使用するプロトコル	追加情報ジ仮想化デバイスですか？
	ボリュームマップ	LUN	実施しました	HTTP/S	バックエンドLUNの名前
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTP/S	
		ストレージポート	実施しました	HTTP/S	
		を入力します	ギャップ	HTTP/S	
	ボリュームマスク	イニシエータ	実施しました	HTTP/S	
		Protocol Controller（プロトコルコントローラ）	実施しました	HTTP/S	
		ストレージポート	実施しました	HTTP/S	
		を入力します	ギャップ	HTTP/S	
	WWNエイリアス	ホストのエイリアス	実施しました	HTTP/S	
		オブジェクトタイプ（ Object Type ）	実施しました	HTTP/S	
		ソース	実施しました	HTTP/S	
		WWN	実施しました	HTTP/S	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		量			
		Snapshotの使用容量	実施しました		
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		Snapshotの使用容量の比率	実施しました		時系列で報告されます
	ボリューム	物理容量	実施しました		
		合計容量	実施しました		
		使用済み容量	実施しました		
		使用容量の比率	実施しました		
		IOPS読み取り	実施しました		ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました		
		IOPS -書き込み	実施しました		
		レイテンシ読み取り	実施しました		
		レイテンシ合計	実施しました		
		レイテンシライト	実施しました		
		スループット読み取り	実施しました		
		合計スループット	実施しました		ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました		

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Pure Storage REST API	HTTP / HTTPS	HTTP / HTTPS	80対443		正しいです	正しいです	正しいです	正しいです

トップに戻る

Red Hat RHV（REST）

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		MOID	実施しました	HTTP/S		
	仮想マシンディスク	OID	実施しました	HTTP/S		
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報	
		仮想マシンOID	実施しました	HTTP/S		
		VirtualDisk OID	実施しました	HTTP/S		
	ホスト	OID	実施しました	HTTP/S		
		名前	実施しました	HTTP/S		
		IPS	実施しました	HTTP/S		
		プラットフォームタイプ	実施しました	HTTP/S		
		ホストインストールメモリ	実施しました	HTTP/S		
		製造元	実施しました	HTTP/S		
		ホストモデル	実施しました	HTTP/S		
		ホストのCPU数	実施しました	HTTP/S		
		ホストのCPU速度	実施しました	HTTP/S		
		NIC数	実施しました	HTTP/S		
		NIC速度	実施しました	HTTP/S		
	iSCSIノード	OID	実施しました	HTTP/S		
		ノード名	実施しました	HTTP/S		
		を入力します	ギャップ	HTTP/S		
	情報	データソース名	実施しました	HTTP/S	情報	
		発信者ID	実施しました	HTTP/S		
		日付	実施しました	HTTP/S		

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Red Hat RHEV REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

Rubrikストレージ

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン	ファームウェアバージョン
V5.3	5.3.3-p1-19391 6.0.3-p3-13584 7.0.2-p4-15876 7.0.3-p1-15949 8.0.3-p2-22743

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		能容量利用率（MB）			
		ノードの使用容量利用率（MB）	実施しました	HTTPS	
プロダクト	カテゴリ	クライアント属性（Feature/Attribute）名	ステータス	使用するプロトコル	追加情報
			実施しました	HTTPS	
	ストレージプール	データの使用容量	実施しました	HTTPS	
		DWH容量に含める	実施しました	HTTPS	ACQからcotnrolまでの間には、DWH容量に興味深いストロークプールがあります
		名前	実施しました	HTTPS	
		その他の使用容量（MB）	実施しました	HTTPS	データとSnapshot以外の容量
		物理ディスク容量（MB）	実施しました	HTTPS	ストレージプールの物理容量として使用されます
		RAID グループ	実施しました	HTTPS	このストレージプールがRAIDグループかどうかを示します
		使用可能な物理比率	実施しました	HTTPS	使用可能容量から物理容量への変換率
		Snapshotの使用容量	実施しました	HTTPS	
		ストレージプールID	実施しました	HTTPS	
		シンプロビジョニングがサポートされます	実施しました	HTTPS	この内部ボリュームで、上のボリュームレイヤのシンプロビジョニングがサポートされているかどうか
		合計割り当て済み容量	実施しました	HTTPS	
		合計使用容量	実施しました	HTTPS	合計容量（MB）
		を入力します	ギャップ	HTTPS	
		仮想	実施しました	HTTPS	ストレージ仮想化デバイスですか？
		実効使用容量	実施しました	HTTPS	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

					込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		利用率の合計	実施しました	HTTPS	
	StoragePoolディスク	物理容量	実施しました	HTTPS	
		合計容量	実施しました	HTTPS	
		使用済み容量	実施しました	HTTPS	
		使用容量の比率	実施しました	HTTPS	
		データの使用容量	実施しました	HTTPS	
		IOPS読み取り	実施しました	HTTPS	ディスク上の読み取りIOPSの数
		IOPSの合計	実施しました	HTTPS	
		IOPS -書き込み	実施しました	HTTPS	
		その他の使用容量	実施しました	HTTPS	
		Snapshotの使用容量	実施しました	HTTPS	
		スループット読み取り	実施しました	HTTPS	
		合計スループット	実施しました	HTTPS	ディスクの平均合計速度（すべてのディスクでの読み取り/書き込み）（MB/秒）
		スループット書き込み	実施しました	HTTPS	

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
Rubrikストレージ REST API	HTTPS	HTTPS	443年		正しいです	正しいです	正しいです	正しいです

トップに戻る

NetApp HCI 仮想センター

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン
VMware vCenter Server 6.7.0ビルド10244857 VMware vCenter Server 6.7.0ビルド14368073 VMware vCenter Server 7.0.3ビルド19234570 VMware vCenter Server 7.0.3ビルド- 20150588 VMware vCenter Server 7.0.3ビルド-20395099 VMware vCenter Server 7.0.3ビルド-20990077 VMware vCenter Server 7.0.3ビルド-21477706 VMware vCenter Server 7.0.3ビルド-21784236 VMware vCenter Server 8.0.1ビルド-21815093

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		使用済み容量	実施しました	Web サービス	
	仮想マシンディスク	OID	実施しました	Web サービス	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		VirtualDisk OID	実施しました	Web サービス	
		仮想マシンOID	実施しました	Web サービス	
	ホスト	ホストのCPU数	実施しました	Web サービス	
		ホストのCPU速度	実施しました	Web サービス	
		ホストドメイン	実施しました	Web サービス	
		ホストインストールメモリ	実施しました	Web サービス	
		ホストモデル	実施しました	Web サービス	
		NIC数	実施しました	Web サービス	
		NIC速度	実施しました	Web サービス	
		IPS	実施しました	Web サービス	
		製造元	実施しました	Web サービス	
		名前	実施しました	Web サービス	
		OID	実施しました	Web サービス	
		プラットフォームタイプ	実施しました	Web サービス	
	iSCSIノード	ホストのエイリアス	実施しました	Web サービス	
		ノード名	実施しました	Web サービス	
		OID	実施しました	Web サービス	
		を入力します	ギャップ	Web サービス	
	情報	API概要 の略	実施しました	Web サービス	
		API名	実施しました	Web サービス	
		APIのバージョン	実施しました	Web サービス	
		クライアントAPI名	実施しました	Web サービス	
		クライアントAPIバージョン	実施しました	Web サービス	
		データソース名	実施しました	Web サービス	情報
		日付	実施しました	Web サービス	
		発信者ID	実施しました	Web サービス	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		swapRate.inRate	実施しました	Web サービス	
		スワップレート	実施しました	Web サービス	
プロダクト	カテゴリ	フィーチャー/属性詳細（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
			実施しました	Web サービス	
		待機時間をスケジュールします	実施しました	Web サービス	スケジュールされた時間の待機時間（パーセント）

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
VMware REST API	Web サービス	HTTP / HTTPS	80対443		正しいです	正しいです	正しいです	正しいです

トップに戻る

AWS 上の VMware Cloud

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン
VMware vCenter Server 7.0.3ビルド20532039 VMware vCenter Server 7.0.3ビルド20870699 VMware vCenter Server 8.0.0 build-21709157

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		MOID	実施しました	Web サービス	
	仮想マシンディスク	OID	実施しました	Web サービス	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		仮想マシンOID	実施しました	Web サービス	
		VirtualDisk OID	実施しました	Web サービス	
	ホスト	OID	実施しました	Web サービス	
		名前	実施しました	Web サービス	
		IPS	実施しました	Web サービス	
		ホストドメイン	実施しました	Web サービス	
		プラットフォームタイプ	実施しました	Web サービス	
		ホストインストールメモリ	実施しました	Web サービス	
		製造元	実施しました	Web サービス	
		ホストモデル	実施しました	Web サービス	
		ホストのCPU数	実施しました	Web サービス	
		ホストのCPU速度	実施しました	Web サービス	
		NIC数	実施しました	Web サービス	
		NIC速度	実施しました	Web サービス	
	情報	データソース名	実施しました	Web サービス	情報
		発信者ID	実施しました	Web サービス	
		日付	実施しました	Web サービス	
		API名	実施しました	Web サービス	
		APIのバージョン	実施しました	Web サービス	
		API概要 の略	実施しました	Web サービス	
		クライアントAPI名	実施しました	Web サービス	
		クライアントAPIバージョン	実施しました	Web サービス	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		待機時間をスケジュールします	実施しました	Web サービス	スケジュールされた時間の待機時間（パーセント）
プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
		disk.ops.total	実施しました	Web サービス	
		合計スワップレート	実施しました	Web サービス	
		スループット読み取り	実施しました	Web サービス	ディスクの合計スループット読み取り

このデータコレクタで使用される管理API：

API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
VMware REST API	Web サービス	HTTP / HTTPS	80対443		正しいです	正しいです	正しいです	正しいです

トップに戻る

VMware vSphere（Webサービス）

このデータコレクタでサポートされるモデルとバージョン：

APIのバージョン
VMware ESXi 6.0.0ビルド10719132
VMware ESXi 6.0.0ビルド-2494585
VMware ESXi 6.0.0ビルド5572656
VMware ESXi 6.0.0ビルド9313334
VMware ESXi 6.5.0ビルド14990892
VMware ESXi 6.5.0ビルド5969303
VMware ESXi 7.0.0ビルド15843807
VMware ESXi 7.0.3ビルド20036589
VMware ESXi 7.0.3ビルド20328353
VMware ESXi 7.0.3ビルド20842708
VMware vCenter Server 5.0.0ビルド3073236
VMware vCenter Server 5.0.0ビルド455964
VMware vCenter Server 5.0.0ビルド623373
VMware vCenter Server 5.1.0ビルド3814779
VMware vCenter Server 5.5.0ビルド1750787
VMware vCenter Server 5.5.0ビルド-2442329
VMware vCenter Server 5.5.0ビルド3000241
VMware vCenter Server 5.5.0ビルド3252642
VMware vCenter Server 5.5.0ビルド3721164
VMware vCenter Server 5.5.0ビルド4180647
VMware vCenter Server 5.5.0ビルド6516310
VMware vCenter Server 5.5.0ビルド-9911218
VMware vCenter Server 6.0.0ビルド13638472
VMware vCenter Server 6.0.0ビルド14510545
VMware vCenter Server 6.0.0ビルド2776511
VMware vCenter Server 6.0.0ビルド3634793
VMware vCenter Server 6.0.0ビルド3634794
VMware vCenter Server 6.0.0 build-5960847
VMware vCenter Server 6.0.0ビルド-7924803
VMware vCenter Server 6.0.0ビルド8803875
VMware vCenter Server 6.0.0ビルド9313458
VMware vCenter Server 6.5.0ビルド10964411
VMware vCenter Server 6.5.0ビルド15679215
VMware vCenter Server 6.5.0ビルド17590285
VMware vCenter Server 6.5.0ビルド17994927
VMware vCenter Server 6.5.0ビルド18499837
VMware vCenter Server 6.5.0ビルド-18711281
VMware vCenter Server 6.5.0ビルド19261680
VMware vCenter Server 6.5.0ビルド20510539
VMware vCenter Server 6.5.0ビルド7119157
VMware vCenter Server 6.7.0ビルド10244857
VMware vCenter Server 6.7.0ビルド11727113
VMware vCenter Server 6.7.0ビルド13007421
VMware vCenter Server 6.7.0ビルド13639324
VMware vCenter Server 6.7.0ビルド14368073
VMware vCenter Server 6.7.0ビルド15129973
VMware vCenter Server 6.7.0ビルド15679289
VMware vCenter Server 6.7.0ビルド17137327
VMware vCenter Server 6.7.0ビルド18010599
VMware vCenter Server 6.7.0ビルド18485185
VMware vCenter Server 6.7.0ビルド- 18831049
VMware vCenter Server 6.7.0ビルド19299595
VMware vCenter Server 6.7.0ビルド-19832247
VMware vCenter Server 6.7.0ビルド-19832280

このデータコレクタでサポートされる製品：

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
基礎					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		使用済み容量	実施しました	Web サービス	
	仮想マシンディスク	OID	実施しました	Web サービス	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		VirtualDisk OID	実施しました	Web サービス	
		仮想マシンOID	実施しました	Web サービス	
	ホスト	ホストのCPU数	実施しました	Web サービス	
		ホストのCPU速度	実施しました	Web サービス	
		ホストドメイン	実施しました	Web サービス	
		ホストインストールメモリ	実施しました	Web サービス	
		ホストモデル	実施しました	Web サービス	
		NIC数	実施しました	Web サービス	
		NIC速度	実施しました	Web サービス	
		IPS	実施しました	Web サービス	
		製造元	実施しました	Web サービス	
		名前	実施しました	Web サービス	
		OID	実施しました	Web サービス	
		プラットフォームタイプ	実施しました	Web サービス	
	iSCSIノード	ホストのエイリアス	実施しました	Web サービス	
		ノード名	実施しました	Web サービス	
		OID	実施しました	Web サービス	
		を入力します	ギャップ	Web サービス	
	情報	API概要 の略	実施しました	Web サービス	
		API名	実施しました	Web サービス	
		APIのバージョン	実施しました	Web サービス	
		クライアントAPI名	実施しました	Web サービス	
		クライアントAPIバージョン	実施しました	Web サービス	
		データソース名	実施しました	Web サービス	情報
		日付	実施しました	Web サービス	
		発信者ID	実施しました	Web サービス	

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報
パフォーマンス					

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

プロダクト	カテゴリ	フィーチャー/属性（**Feature/Attribute**）	ステータス	使用するプロトコル	追加情報

		ト			の合計
		ipThroughput書き込み	実施しました	Web サービス	
プロダクト	カテゴリ	フィーチャー/属性（Feature/Attribute）	ステータス	使用するプロトコル	追加情報
		合計メモリ利用率	実施しました	Web サービス	
		swapRate.inRate	実施しました	Web サービス	
		スワップレート	実施しました	Web サービス	
		合計スワップレート	実施しました	Web サービス	
		待機時間をスケジュールします	実施しました	Web サービス	スケジュールされた時間の待機時間（パーセント）

このデータコレクタで使用される管理API：

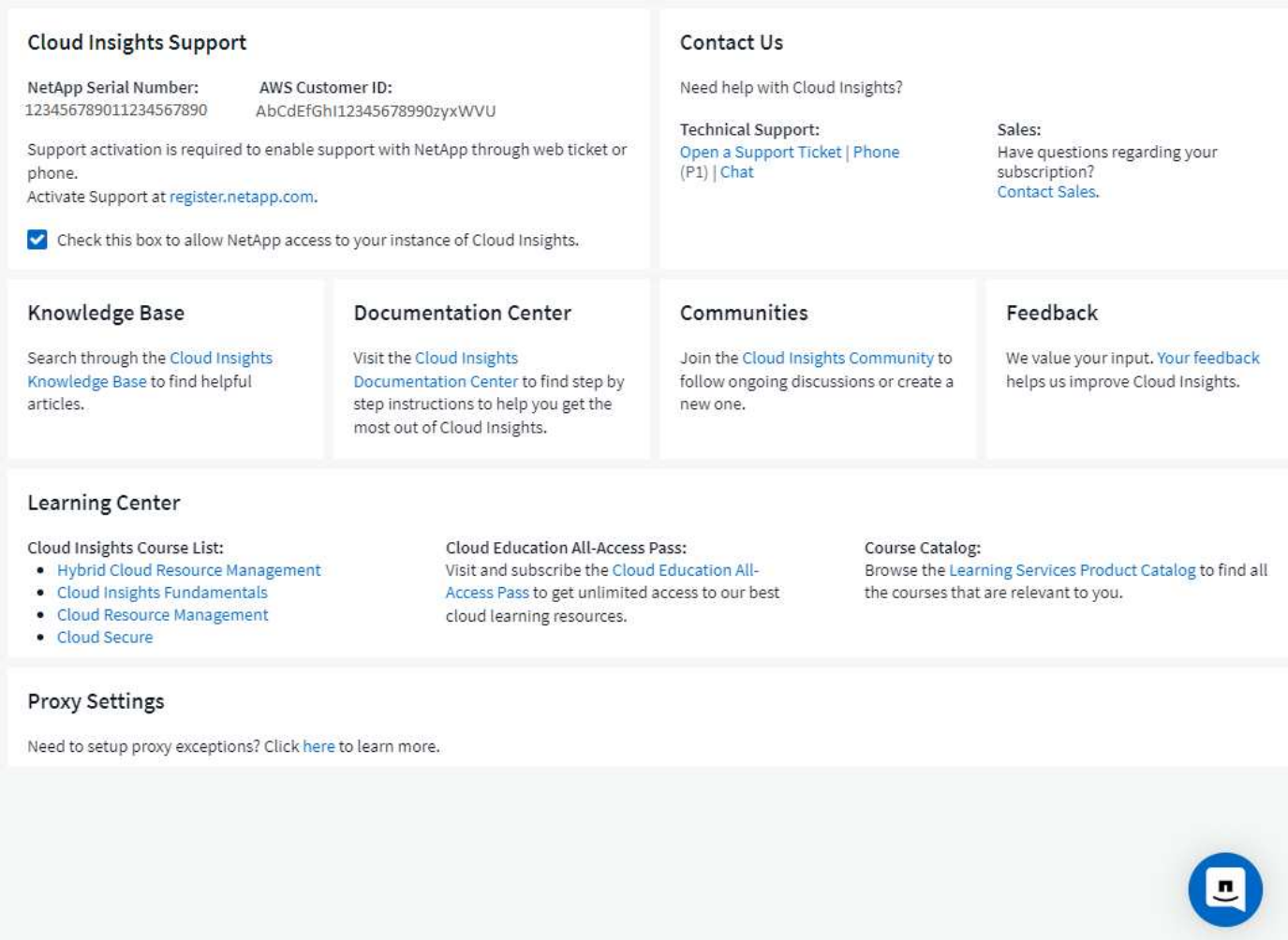
API	使用するプロトコル	使用するトランスポート層プロトコル	使用されている着信ポート	使用されている発信ポート	認証をサポートします	「読み取り専用」のクレデンシャルのみ必要です	暗号化をサポートします	ファイアウォール対応（静的ポート）
VMware REST API	Web サービス	HTTP / HTTPS	80対443		正しいです	正しいです	正しいです	正しいです

トップに戻る

リファレンス&サポート

サポートをリクエストしています

Data Infrastructure Insightsでサポートオプションにアクセスするには、*[ヘルプ]>[サポート]*をクリックします。利用可能なサポートオプションは、Data Infrastructure Insightsのエディションによって異なります。



サポート資格をアクティブ化しています

Data Infrastructure Insightsは、トライアルモードでの実行時にセルフサービスとEメールによるサポートを提供します。サービスに登録したら、サポート資格をアクティブ化することを強くお勧めします。サポートエンタイトルメントをアクティブにすると、オンラインチャット、 Web チケット発行システム、および電話でテクニカルサポートにアクセスできます。登録が完了するまで、デフォルトのサポートモードはセルフサービスです。詳細以下を参照してください。

初回のサブスクリプションプロセスでは、Data Infrastructure Insightsインスタンスが「950」で始まる20桁のNetAppシリアル番号を生成します。このNetAppシリアル番号は、アカウントに関連付けられたData Infrastructure Insightsのサブスクリプションを表します。サポート利用資格を有効にするには、ネットアップのシリアル番号を登録する必要があります。サポート登録には、次の 2 つのオプションがあります。

1. NetApp Support Site（ NSS ）の SSO アカウントをすでにお持ちのユーザ（現在ネットアップのお客様な

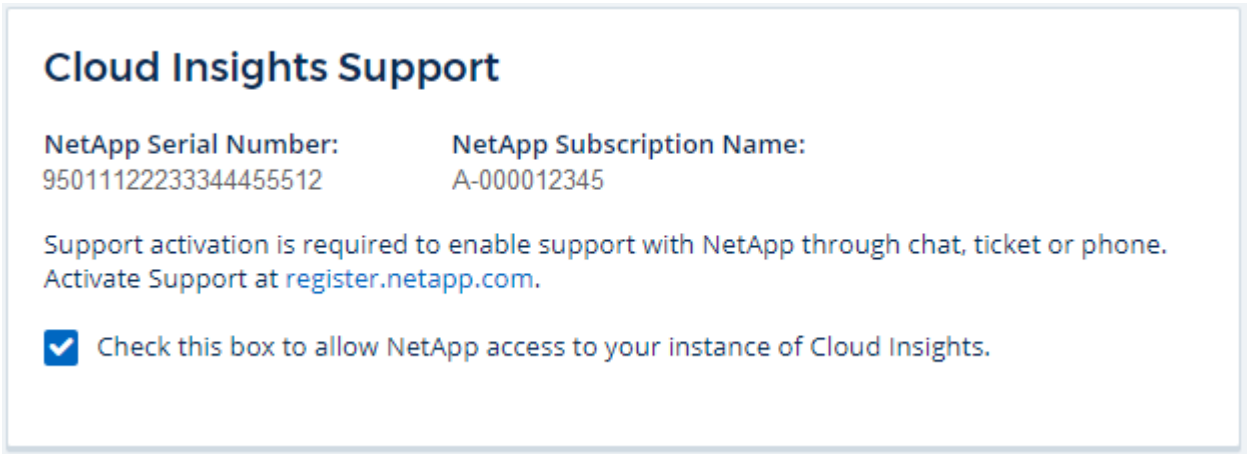
ど）

2. NetApp Support Site（ NSS ）の SSO アカウントがない新しいネットアップのお客様

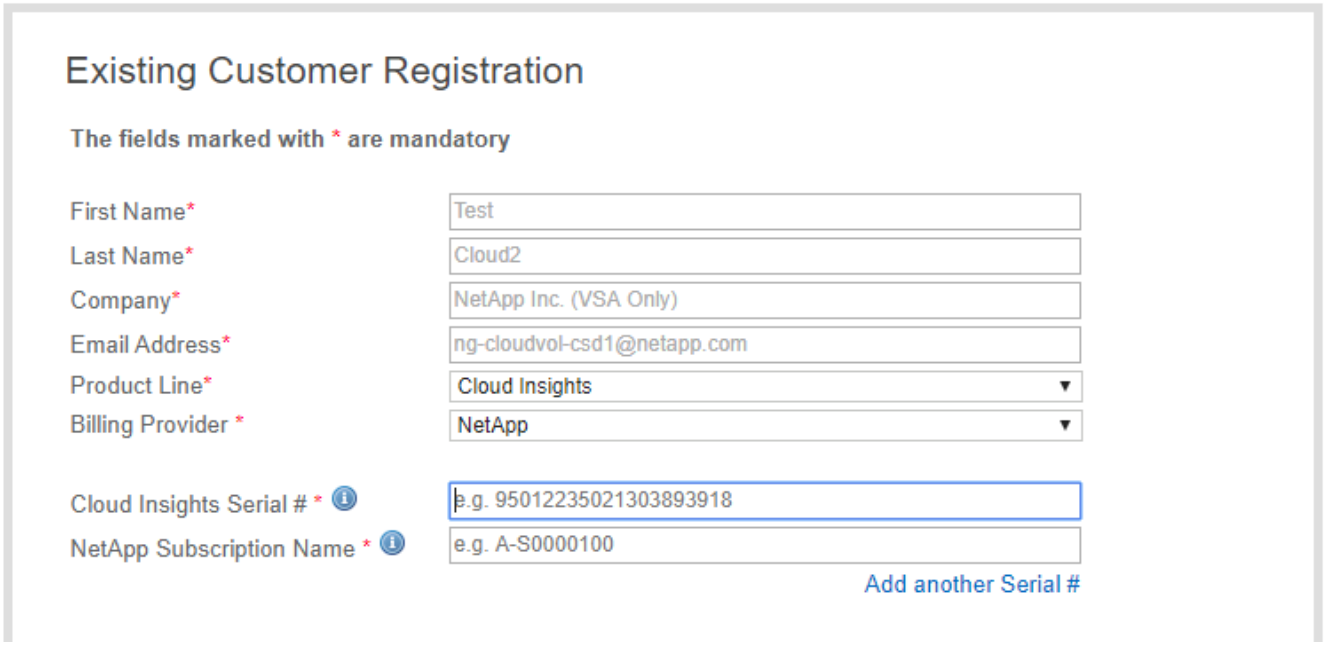
オプション **1** ：**NetApp Support Site**（ **NSS** ）の **SSO** アカウントを事前にお持ちのユーザ向けの手順

手順

1. ネットアップ登録用 Web サイトにアクセスします https://register.netapp.com
2. [I am already registered as NetApp Customer]を選択し、製品ラインとして[_Data Infrastructure Insights _]を選択します。課金プロバイダ（NetAppまたはAWS）を選択し、Data Infrastructure Insightsユーザインターフェイスの[Help]>[Support]メニューを参照してシリアル番号、NetAppサブスクリプション名、またはAWSカスタマーIDを入力します。



3. 既存の顧客登録フォームに入力し、 *Submit * をクリックします。

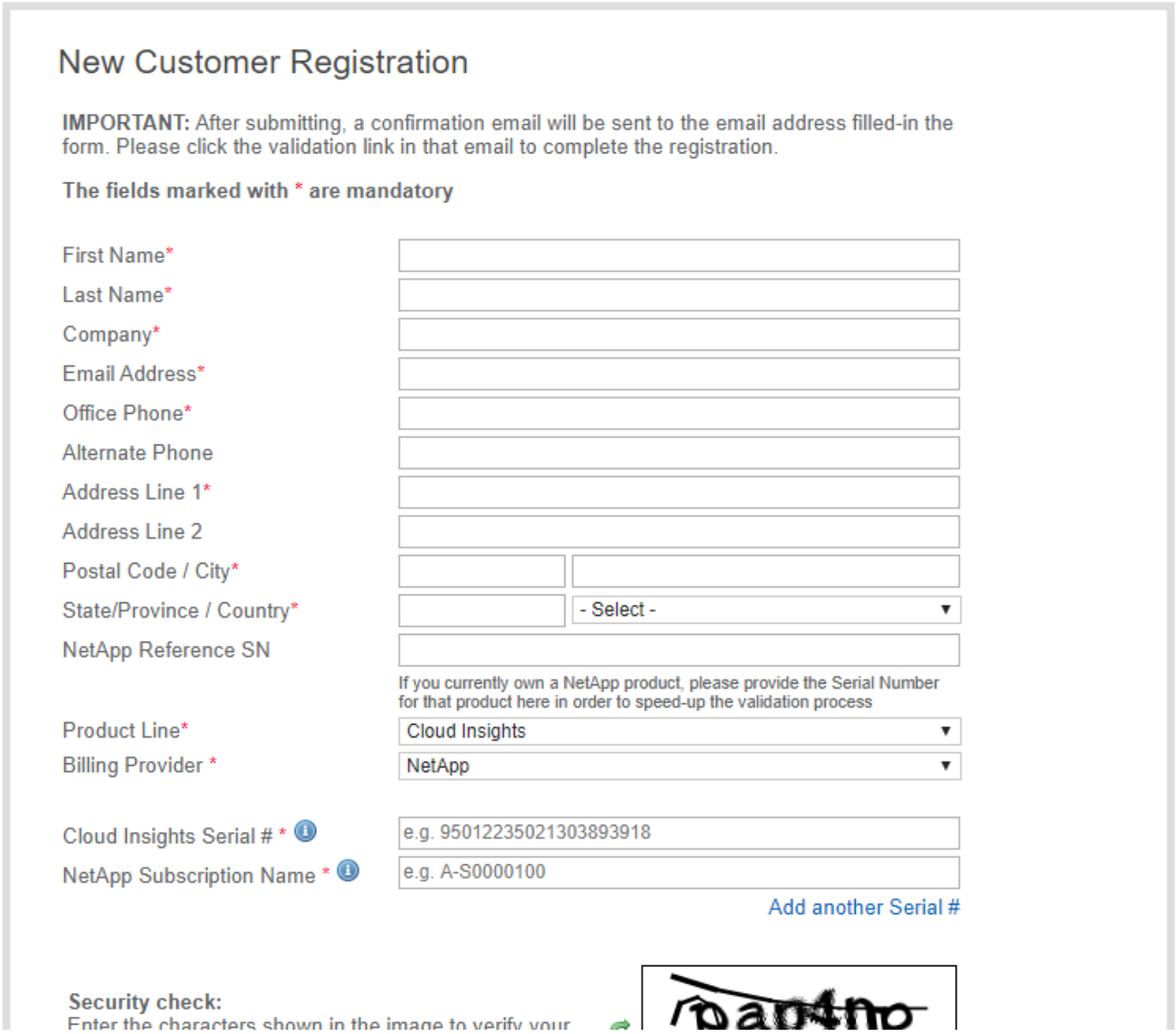


4. エラーが発生しない場合は、「登録が正常に送信されました」ページが表示されます。登録に使用されたNSS SSO ユーザ名に関連付けられた電子メールアドレスには、数分以内に「お使いの製品は現在サポート対象です」という電子メールが送信されます。
5. Data Infrastructure Insights NetAppのシリアル番号の登録は1回のみです。

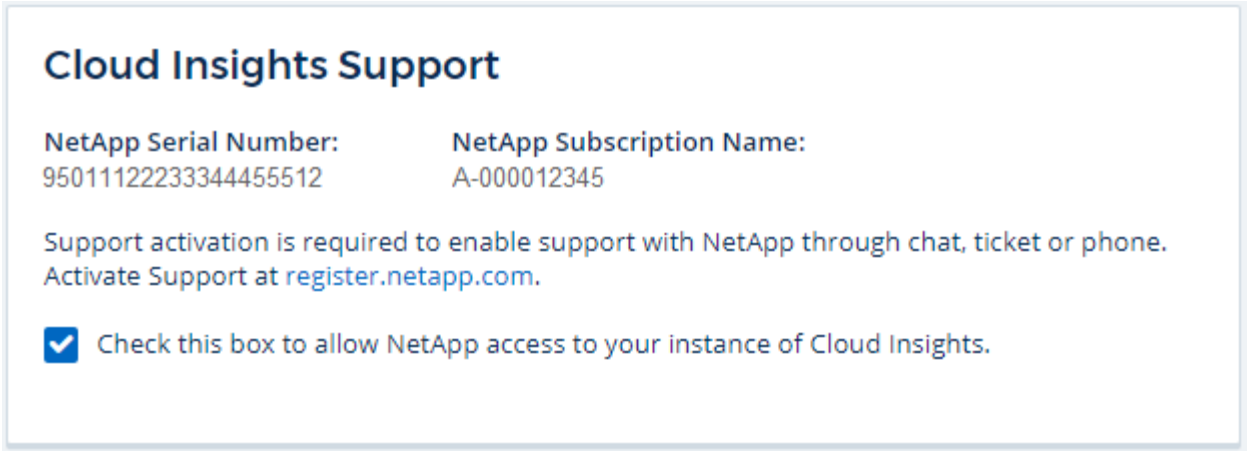
オプション 2 ：**NetApp Support Site**（ **NSS** ）の **SSO** アカウントがない新しいネットアップのお客様向けの手順

手順

1. ネットアップ登録用 Web サイトにアクセスします https://register.netapp.com
2. 「 I am not a registered NetApp Customer 」を選択し、以下の例のフォームに必要な情報を入力します。



1. 製品ラインとして「_Data Infrastructure Insights」を選択します。課金プロバイダ（NetAppまたはAWS）を選択し、Data Infrastructure Insightsユーザインターフェイスの[Help]>[Support]メニューを参照してシリアル番号、NetAppサブスクリプション名、またはAWSカスタマーIDを入力します。



2. エラーが発生しない場合は、「登録が正常に送信されました」ページが表示されます。登録に使用されたNSS SSO ユーザ名に関連付けられた電子メールアドレスには、「お使いの製品はサポート対象です」という電子メールが数時間以内に送信されます。
3. ネットアップの新規のお客様の場合は、NetApp Support Site（ NSS ）のユーザアカウントを作成して、今後の登録や、テクニカルサポートチャットや Web チケット発行用のサポートポータルにアクセスする必要があります。このリンクはにあります https://mysupport.netapp.com/eservice/public/now.do。新たに登録したData Infrastructure Insightsのシリアル番号を入力すると、プロセスを円滑に進めることができます。
4. これは、Data Infrastructure Insights NetAppのシリアル番号の1回限りの登録です。

サポート情報の入手方法

NetAppは、データインフラの分析情報をさまざまな方法でサポートします。ナレッジベース（ KB ）記事やネットアップコミュニティなど、幅広いセルフサポートオプションを 24 時間 365 日ご利用いただけます。Data Infrastructure Insightsのいずれかのエディション（Basic *、Standard、Premium）に登録しているユーザは、電話またはWebチケット発行を通じてテクニカルサポートを利用できます。Web チケットとケース管理には、NetApp Support Site（ NSS ）の SSO アカウントが必要です。

*すべてのネットアップストレージシステムが少なくともPremiumサポートレベル以上であれば、Basicエディションでサポートを利用できます。

セルフサービスサポート：

これらのサポートオプションはトライアルモードで利用でき、 24 時間 365 日無料でご利用いただけます。

- * https://kb。NetApp .com /スペシャル：検索？query=cloud + insights [KnowledgeBase]*

+このセクションのリンクをクリックすると、NetAppナレッジベースに移動し、関連記事やハウツーなどを検索できます。

- "ドキュメント"

  [Documentation] リンクをクリックすると、このドキュメントセンターに移動します。

- "コミュニティ"

  コミュニティリンクをクリックすると、NetApp Data Infrastructure Insightsのコミュニティに移動し、他のユーザやエキスパートと交流できます。

xref:./"* フィードバック *"データインフラの分析情報を改善するためのリンクもあります。

サブスクリプションサポート

上記のセルフサポートオプションに加えて、Data Infrastructure Insightsのサブスクリプションを契約しているか、監視対象のNetApp製品やサービスに対して有償サポートを利用している場合は、NetAppサポートエンジニアと協力して問題を解決できます。

に登録する必要があります サポートを有効にします ネットアップのクラウド製品の場合：登録は、ネットアップのにアクセスしてください "クラウドデータサービスサポート登録"。

NetAppサポートエンジニアがサポートセッション中にデータインフラ分析環境にアクセスできるようにするには、チェックボックスをオンにすることを強く推奨します。これにより、エンジニアが問題のトラブルシューティングを行い、問題を迅速に解決できるようになります。問題が解決されるか、サポートセッションが終了したら、チェックボックスをオフにできます。

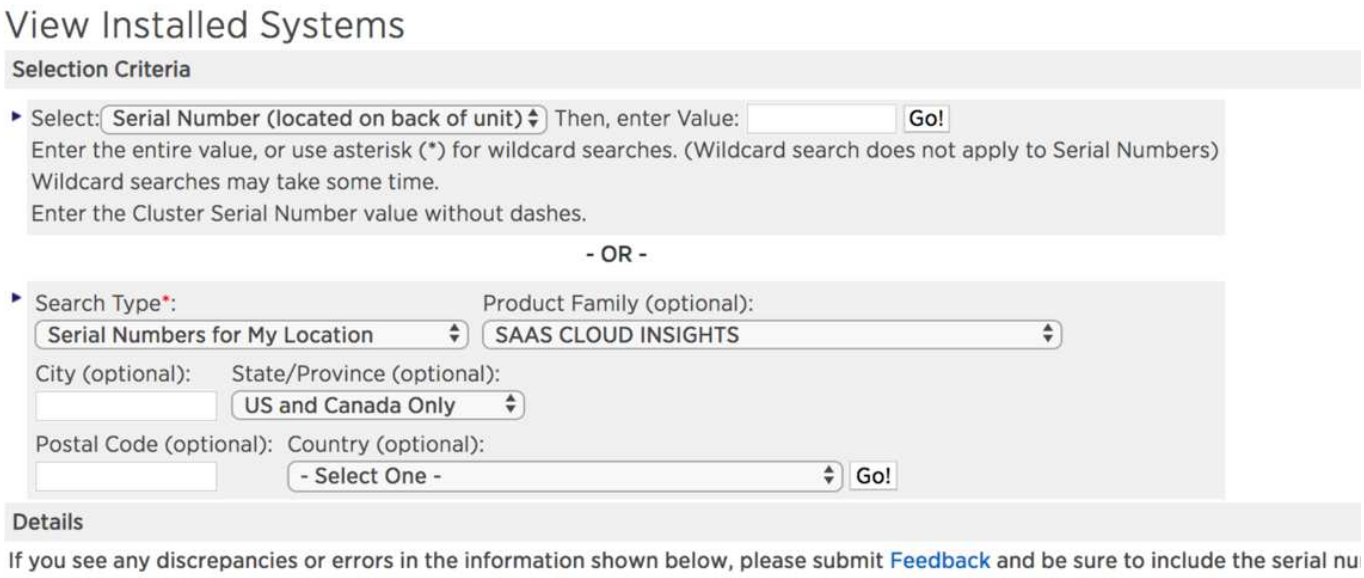
サポートは次のいずれかの方法でリクエストできます。以下のサポートオプションを利用するには、Data Infrastructure Insightsのアクティブなサブスクリプションが必要です。

- "* 電話 *"
- "* サポートチケット *"
- チャット- NetAppサポート担当者に連絡してサポートを受けます（平日のみ）。チャットは、Data Infrastructure Insights画面の右上にある* Help（ヘルプ）> Live Chat（ライブチャット）*メニューオプションで利用できます。

をクリックして、セールスサポートをリクエストすることもできます "* 販売担当者 * にお問い合わせください" リンク

Data Infrastructure Insightsのシリアル番号は、サービス内で*[ヘルプ]>[サポート]*メニューから確認できます。サービスへのアクセスで問題が発生し、以前にNetAppにシリアル番号を登録したことがある場合は、NetAppサポートサイトでData Infrastructure Insightsのシリアル番号のリストを次のように確認することもできます。

- mysupport.netapp.com にログインします
- [Products]>[My Products]メニュータブで、製品ファミリーの[SaaS Data Infrastructure Insights]を使用して登録済みのすべてのシリアル番号を確認します。



Data Infrastructure Insights Data Collectorサポートマトリックス

サポートされているデータコレクタの情報と詳細は、で表示またはダウンロードできます* Data Infrastructure Insights Data Collector Support Matrix *、role=。

ラーニングセンター

サブスクリプションに関係なく、*[ヘルプ]>[サポート]*をクリックすると、データインフラのインサイトを最大限に活用するために役立つNetApp Universityのいくつかのコースにアクセスできます。チェックアウト！

Data Collector Reference - Infrastructure （データコレクターリファレンス - インフラストラクチャ

Vendor-Specific Reference

このセクションのトピックでは、ベンダー別のリファレンス情報を提供します。ほとんどの場合、データコレクタの設定は簡単です。場合によっては、データコレクタを適切に設定するために追加情報またはコマンドが必要になることがあります。

左側のメニューで * VENDOR * をクリックすると、そのデータコレクタの情報が表示されます。

Amazon EC2 データコレクタの設定

Data Infrastructure Insightsは、Amazon EC2データコレクタを使用して、EC2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

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。

- 次のいずれかが必要です。

- IAM ロール認証を使用している場合は、 Amazon EC2 クラウドアカウント用の * IAM ロール * 。IAM ロールは、 Acquisition Unit が AWS インスタンスにインストールされている場合にのみ適用されます。
- IAM Access Key 認証を使用している場合は、 Amazon EC2 クラウドアカウントの * IAM Access Key * ID と Secret Access Key 。

- 「組織のリスト」権限が必要です
- ポート 443 HTTPS
- EC2 インスタンスは、仮想マシンまたは（自然に）ホストとしてレポートできます。EBS ボリュームは、 VM で使用されている仮想ディスクと、仮想ディスクの容量を提供するデータストアの両方として報告できます。

アクセスキーは、アクセスキー ID （ AKIAIOSFODNN7EXAMPLE など）とシークレットアクセスキー（ wJalrXUtil/K7MDENG/bPxRfiCYEXAMPLEKEY など）で構成されます。Amazon EC2 SDK 、 REST 、またはクエリ API の処理を使用している場合は、アクセスキーを使用して EC2 にプログラム経由の要求に署名します。これらのキーは、 Amazon の契約に付属しています。

設定

次の表に従って、データコレクタフィールドにデータを入力します。

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。の詳細については、以下を参照してください IAM ロール。
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 が API 要求を課金することを理解している	このチェックボックスをオンにすると、Data Infrastructure Insights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できます。

詳細設定

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）	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。「含める」が選択されている場合、タグキーフィールドを空にすることはできません。

フィールド	説明
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）	デフォルトは 1800 です。
CloudWatch Agent Metrics 名前空間	データの収集元である EC2/EBS のネームスペース。このネームスペースのデフォルトの指標の名前を変更すると、名前を変更したデータをData Infrastructure Insightsで収集できなくなる可能性があります。メトリック名はデフォルトのままにしておくことを推奨します。

IAM Access Key

アクセスキーは、 IAM ユーザまたは AWS アカウントの root ユーザの長期的なクレデンシャルです。アクセスキーは、プログラムによる AWS CLI または AWS API への要求に（直接または AWS SDK を使用して）署名するために使用します。

アクセスキーは、アクセスキー ID とシークレットアクセスキーの 2 つの部分で構成されます。IAM Role _authentication ではなく、 _IAM Access Key _authentication を使用する場合は、要求の認証にアクセスキー ID とシークレットアクセスキーの両方を一緒に使用する必要があります。詳細については、の Amazon のドキュメントを参照してください "アクセスキー"。

IAM ロール

IAM Access Key 認証ではなく、 _IAM Role_authentication 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割り当てられてい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。

詳細については、 Amazon ドキュメントを参照してください "IAM ロール"。

注： IAM ロールは、 AWS インスタンスで Acquisition Unit を実行している場合にのみ使用できます。

Amazonのタグを**Data Infrastructure Insights**のアノテーションにマッピング

Amazon EC2データコレクタには、EC2で設定されたタグを使用してData Infrastructure Insightsのアノテーションを入力できるオプションがあります。アノテーションには EC2 タグとまったく同じ名前を付ける必要が

あります。Data Infrastructure Insights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「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コレクタ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で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、Data Infrastructure Insights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、Data Infrastructure Insightsで「owner」という名前のアノテーションを作成し、EC2で「owner」、「Owner」、「owner」という名前のタグを作成すると、「owner」のEC2のすべてのバリエーションがCloud Insightの「owner」アノテーションにマッピングされます。

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 の子アカウントから収集しています

Data Infrastructure Insightsでは、1つのAWSデータコレクタ内でAWSの子アカウントを収集できます。この収集の設定は、 AWS 環境で実行されます。

- 各子アカウントに AWS ロールを設定して、メインアカウント 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する必要があります。
- 各子アカウントには、同じ文字列としてロール名を設定する必要があります。
- このロール名の文字列をData Infrastructure Insights 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。
- コレクタがインストールされているアカウントには、_delegateアクセス権administrator_deligate Privilegesが必要です。詳細については、"AWSのドキュメント"を参照してください。

ベストプラクティス： AWS Predefined_AmazonEC2ReadOnlyAccess_policy を EC2 メインアカウントに割り当てることを強く推奨します。また、データソースで設定したユーザが AWS に照会するには、少なくとも、 Predefined_AWSOrganizationReadOnlyAccess_policy を割り当てる必要があります。

Data Infrastructure InsightsがAWSの子アカウントからデータを収集できるように環境を構成する方法については、以下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"

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

NetApp ONTAP データコレクタ用の Amazon FSX

このデータコレクタは、 Amazon FSX for NetApp ONTAP 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。このデータコレクタは、Data Infrastructure Insightsサービスのリージョン全体で段階的に利用できるようになります。Data Infrastructure Insights環境にこのコレクタのアイコンが表示されない場合は、営業担当者にお問い合わせください。

このData Infrastructure Insightsコレクタには、*Filesystem-Scoped_role*を持つ*ONTAP*ユーザが必要です。"ロールとルール"使用可能なオプションについては、*AWS*のドキュメントを参照してください。現時点では、*AWS*は*Filesystem Scope*を使用するユーザロールの*1*種類（*_fsxadmin*）のみをサポートしています。これは、Data Infrastructure Insightsコレクタに使用する適切なロールです。また、ユーザには、http、ontapi、sshの3つのアプリケーションすべてが割り当てられている必要があります。

用語集

Data Infrastructure Insightsは、FSx - NetAppデータコレクタ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。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	**Data Infrastructure Insights**の用語
クラスタ	ストレージ
LUN	ボリューム
ボリューム	内部ボリューム

FSX - ネットアップの用語

FSx-NetApp 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。

ストレージ

- model –このクラスタ内で一意のディスクリートモデル名をカンマで区切って指定します。
- ベンダー–AWS
- Serial Number –アレイのシリアル番号。
- IP –一般に、データソースで設定されている IP またはホスト名です。
- 物理容量–FSXファイルシステムに割り当てられているすべてのSSDストレージの2つの合計。
- レイテンシ–読み取りと書き込みの両方について、ワークロードが直面しているホストの状況が表示されます。理想的なのは、Data Infrastructure Insightsがこの価値を直接提供していることですが、そうではないことがよくあります。Data Infrastructure Insights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約されたもの。管理–デバイスの管理インターフェイスのハイパーリンクが含まれている可能性があります。インベントリレポートの一部として、Data Infrastructure Insights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。

- storage –このプールのストレージアレイの場所。必須。
- Type –可能性のリストから説明的な値を入力します。最も一般的な構成は、「集約」または「 RAID グループ」です。
- 容量–使用済みの論理容量、使用可能な容量、および合計論理容量の値と、これらの要素で使用されている割合の値が表示されます。
- IOPS–このストレージプールに割り当てられているすべてのボリュームの合計IOPS。
- Throughput–このストレージプールに割り当てられているすべてのボリュームの合計スループット。

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。

- 「fsxadmin」ロールのアカウントにアクセスできる必要があります。このアカウントには、ssh、ontapi、httpの3つのアプリケーションが割り当てられています。
- アカウントの詳細には、ユーザ名とパスワードが含まれます。
- ポートの要件：443

設定

フィールド	説明
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

Advanced Metricsの**2**つのパラメータ

このデータコレクタは、NetApp ONTAP ストレージのFSXから次の高度な指標を収集します。

- FPolicy の
- NFSv3
- NFSv3：ノード
- NFSv4
- NFSv4_1
- nfsv4_1：ノード
- NFSv4：ノード
- policy_groupを開きます
- qtree
- ボリューム
- Workload _volume

FSx CLIコマンドとAPIコマンドは、Data Infrastructure Insights ZAPIで収集されない一部の容量値を取得するため、Data Infrastructure Insightsでは特定の容量値（ストレージプールの値など）がFSx自体と異なる場合があることに注意してください。

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。

在庫

問題	次の操作を実行します
401 HTTP 応答または 13003 ZAPI エラーコードを受信し、 ZAPI から「 Insufficient privileges 」または「 Not authorized for this command 」が返される	ユーザ名とパスワード、およびユーザの権限と権限を確認してください。
ZAPI から「 cluster role is not cluster_mgmt LIF 」が返される	AU はクラスタ管理 IP と通信する必要があります。IP を確認し、必要に応じて別の IP に変更してください
ZAPI コマンドの再試行後に失敗する	AU でクラスタとの通信に問題があります。ネットワーク、ポート番号、および IP アドレスを確認してください。また、 AU マシンのコマンドラインからもコマンドを実行しようとします。
AU が HTTP 経由で ZAPI に接続できませんでした	ZAPI ポートでプレーンテキストが受け入れるかどうかを確認します。AU が SSL ソケットにプレーンテキストを送信しようとすると、通信に失敗します。
SSLException で通信が失敗します	AU が Filer 上のプレーンテキストポートに SSL を送信しようとしています。ZAPI ポートで SSL を受け入れるか、別のポートを使用するかを確認します。
追加の接続エラー： ZAPI応答のエラーコード13001：「database is not open」 ZAPIエラーコードが60で、応答に「API did not finish on time」が含まれている ZAPIの応答に「initialize_session () returned NULL environment」が含まれる ZAPIエラーコードが14007で、応答に「Node is not healthy」が含まれている	ネットワーク、ポート番号、および IP アドレスを確認してください。また、 AU マシンのコマンドラインからもコマンドを実行しようとします。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Azure コンピューティングデータコレクタの設定

Data Infrastructure 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 OAuth 2.0 リダイレクト URI （ login.microsoftonline.com ）
- Azure Management Rest IP （ management.azure.com ）
- Azure Resource Manager IP （ management.core.windows.net ）
- 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 サービスプリンシパルの認証キー（ユーザパスワード）
- Data Infrastructure Insightsの検出用に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てAzureにアプリケーションを登録すると、Data Infrastructure 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取得されます。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

次の表に従って、データコレクタ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

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。「含める」が選択されている場合、タグキー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。

フィールド	説明
パフォーマンスポーリング間隔（秒）	デフォルトは300です

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Broadcom

Brocade Network Advisor データコレクタ

Data Infrastructure Insightsは、Brocadeネットワークアドバイザのデータコレクタを使用して、Brocadeスイッチ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。

用語集

Data Infrastructure Insightsは、Brocadeネットワークアドバイザ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。Data Infrastructure Insights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	**Data Infrastructure Insights**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
Logical Switch の略	Logical Switch の略

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。

要件

このデータコレクタを設定するには、次のものが必要です。

- Data Infrastructure Insights Acquisition Unitは、BNAサーバのTCPポート443への接続を開始します。BNAサーバはバージョン 14.2.1 以降を実行している必要があります。
- Brocade Network Advisor サーバの IP アドレス
- 管理者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	説明
Brocade Network Advisor サーバ IP	Network Advisor サーバの IP アドレス

フィールド	説明
ユーザ名	スイッチのユーザ名
ユーザ名	管理者のユーザ名
パスワード	管理者パスワード

高度な設定

フィールド	説明
接続タイプ	HTTPS （デフォルトポート 443 ）または HTTP （デフォルトポート 80 ）
接続ポートを上書きします	空白の場合は、 [Connection Type] フィールドでデフォルトのポートを使用します。それ以外の場合は、使用する接続ポートを入力します
パスワード	スイッチのパスワード
インベントリのポーリング間隔（分）	デフォルトは40です
Report Access Gateway の略	Access Gateway モードにデバイスを含める場合にオンにします
パフォーマンスポーリング間隔（秒）	デフォルトは 1800 です。

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。

在庫

問題	次の操作を実行します
複数のノードが Access Gateway ポートにログインしているというメッセージを受信するか、データコレクタが Access Gateway デバイスを検出できません。	NPV デバイスが正しく動作していること、および接続されているすべての WWN が必要であることを確認します。NPV デバイスを直接取得しないでください。代わりに、コアファブリックスイッチを取得すると NPV デバイスデータが収集されます。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Brocade FC スイッチデータコレクタ

Data Infrastructure Insights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またはブランド名が変更されたスイッチデバイスのインベントリを検出します。FC スイッチとアクセスゲートウェイの両方のモードのデバイスがサポートされます。

用語集

Data Infrastructure Insightsでは、Brocade FCスイッチ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。Data Infrastructure Insights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	**Data Infrastructure Insights**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
仮想ボリューム	ボリューム
LSANゾーン	IVR ゾーン

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。

要件

- Data Infrastructure Insights Acquisition Unit（AU）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接続が確立されている必要があります。[Discover all switches in the fabric]チェックボックスを選択すると、Data Infrastructure Insightsによって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。
- SNMP のパフォーマンスのポーリング用に、ファブリック内のすべてのスイッチでポート 161 および 162 を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	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
SNMP	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 ユーザ名
SNMP パスワード	SNMP パスワード

高度な設定

フィールド	説明
ファブリック名	データコレクタによって報告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。
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15です。
除外されたデバイス	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
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です。
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です。
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

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。

在庫

問題	次の操作を実行します
Brocadeデータソースのインベントリの取得が次のエラーで失敗します。 <date> <time>エラー[com.onaro.sanscreen.acquisition.framework.datasource.BaseDataSource]エラー2 / 2：<datasource name>[内部エラー]-デバイス<IP>のモデルを生成できません。プロンプトの検出エラー（ [Device name < name >] ：デバイス <IP> のモデルを生成できません。エラー検出プロンプト）	問題 は、デフォルトのタイムアウトである 5 秒を超えてプロンプトが表示されるまでに Brocade スイッチが時間がかかりすぎる場合に発生することがあります。Data Infrastructure Insightsのデータコレクタ のAdvanced Configuration設定で、_SSHバナー待機タイムアウト（秒）_の値を大きくしてみてください。
エラー：「Data Infrastructure Insights Received Invalid Chassis Role」	このデータソースで設定されているユーザにシャーシのロールの権限が付与されていることを確認します。
エラー：「シャーシの IP アドレスが一致しません」	シャーシの IP アドレスを使用するようにデータソース構成を変更します。
複数のノードが Access Gateway ポートにログインしているというメッセージを受信します	NPV デバイスが正しく動作していること、および接続されているすべての WWN が必要であることを確認します。NPV デバイスを直接取得しないでください。代わりに、コアファブリックスイッチを取得すると NPV デバイスデータが収集されます。
パフォーマンスの収集が失敗し、「Timed out during sending SNMP request」というメッセージが表示されます。	クエリー変数およびスイッチの設定によっては、一部のクエリーがデフォルトのタイムアウトを超える場合があります。 "詳細はこちら。"。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Brocade FOS RESTデータコレクタ

Data Infrastructure Insightsでは、Brocade FOS RESTコレクタを使用して、FabricOS（FOS）ファームウェア8.2以降を実行しているBrocadeスイッチデバイスのインベントリとパフォーマンスを検出します。

注意：FOSのデフォルトの「ユーザー」レベルでは、Data Infrastructure Insightsでデバイスのすべての論理的側面を表示するには不十分です。「シャーシロール」が有効になっているユーザーアカウントと、スイッチに設定されているすべての仮想ファブリックに対する権限が必要です。

FOSデバイスへのSSHセッションでData Infrastructure Insightsを使用するための「最小権限」ユーザアカウントを作成する方法の例を次に示します。

userconfig — add NetAppCIUser -r user -l 1-128 -c user -p QWERTY！

これにより、ユーザ「NetAppCIUser」、パスワード「QWERTY！」が作成されます。このユーザには、128個の可能なすべての仮想ファブリック（-l）で「ユーザ」ロール（-r）が割り当てられます。このユーザには、必要な「シャーシ」ロール（-c）が追加で割り当てられ、ユーザレベルのアクセス権が割り当てられています。

デフォルトでは、このコレクタは、スイッチが属するすべてのファブリックの一部であるすべてのFOSデバイスの検出を試みます。

用語集

Data Infrastructure Insightsでは、Brocade FOS REST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。Data Infrastructure Insights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	**Data Infrastructure Insights**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

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。

要件

- ファブリック内のすべてのスイッチへのTCP接続が確立されている必要があります。このデータコレクタタイプは、ファブリック内の各デバイスに対してHTTPとHTTPSの両方をシームレスに試行します。[Discover all switches in the fabric_]チェックボックスを選択すると、Data Infrastructure Insightsはファブリック内のすべてのスイッチを識別しますが、検出するにはこれらの追加スイッチへのTCP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。デバイスのWebインターフェイスを使用してアクセスを確認できます。

設定

フィールド	説明
スイッチ IP	FOS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

高度な設定

フィールド	説明
除外されたデバイス	ポーリングの対象から除外するデバイスのIPv4アドレス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）	インベントリのポーリング間隔。デフォルトは60です。
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。

フィールド	説明
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。
接続タイプ	HTTPまたはHTTPS。
この設定は、デバイスごとに最初に使用するプロトコルCIが変更されるだけであることに注意してください。デフォルトが失敗した場合、CIは自動的に反対のプロトコルを試行します。	TCP ポートを上書きします
デフォルトを使用しない場合は、ポートを指定します。	パフォーマンスポーリング間隔（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。

在庫

問題	次の操作を実行します
テスト機能は、プロトコルにアクセスできないことを警告します。	特定のBrocade FOS 8.2以降のデバイスは、HTTPまたはHTTPSでのみ通信します。スイッチにデジタル証明書がインストールされている場合、暗号化されていないHTTPとHTTPSで通信しようとすると、スイッチはHTTPエラーをスローします。テスト機能はHTTPとHTTPSの両方との通信を試行します。一方のプロトコルが成功したことをテストで確認した場合、もう一方のプロトコルが失敗したことを心配する必要はありません。コレクタは収集中に両方のプロトコルを試行し、どちらも機能しない場合にのみ失敗します。
エラー：「Data Infrastructure Insights Received Invalid Chassis Role」	このデータソースで設定されているユーザにシャーシのロールの権限が付与されていることを確認します。
エラー：「シャーシの IP アドレスが一致しません」	シャーシの IP アドレスを使用するようにデータソース構成を変更します。
403 Forbiddenでインベントリが失敗する	これは、単に不正な資格情報であるか、十分に強力でないロールを使用しようとしていることを示している可能性があります。「ユーザー」レベルのユーザーには、必要な「シャーシロール」権限がないか、デフォルト以外の仮想ファブリックへのアクセスを表示する権限がないことに注意してください。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Cisco MDS ファブリックスイッチデータコレクタ

Data Infrastructure Insightsでは、Cisco MDSファブリックスイッチデータコレクタを使用して、Cisco MDSファブリックスイッチおよび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。

また、このデータコレクタを使用して、 NPV モードで実行されている多くのモデルの Cisco デバイスを検出できます。

用語集

Data Infrastructure Insightsでは、Cisco FCスイッチ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。Data Infrastructure Insights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	**Data Infrastructure Insights**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

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。

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

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	V1 、 V2 、または V3 を選択します。パフォーマンスの収集には 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
除外されたデバイス	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
含まれるデバイス	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
First Alias Type （最初のエイリアスタイプ	エイリアスの解決で最初に優先する情報を指定します。次のいずれかを選択します。 デバイス**Alais *** これは、ポート**WWN**（**pWWN**）のフレンドリ名であり、必要に応じてすべてのコンフィギュレーションコマンドで使用できます。**Cisco MDS 9000** ファミリのすべてのスイッチは、 **Distributed Device Alias Services** （デバイスエイリアス）をサポートしています。 * なし * エイリアスは報告しないでください。 *ポート概要 * ポートのリストでポートを識別するための概要。 *ゾーンエイリアス（すべて） 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。
2 番目のエイリアスタイプ	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

フィールド	説明
3 番目のエイリアスタイプ	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）

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。

在庫

問題	次の操作を実行します
エラー：シャーシを検出できませんでした - スイッチが検出されていません	•IPを設定してデバイスにpingを実行します •Cisco Device Manager GUIを使用してデバイスにログインします •CLIを使用してデバイスにログインします •SNMP Walkを実行してみます
エラー：デバイスが Cisco MDS スイッチではありません	•デバイスに設定されているデータソースIPが正しいことを確認します •Cisco Device Manager GUIを使用してデバイスにログインします •CLIを使用してデバイスにログインします
エラー：Data Infrastructure Insightsがスイッチのwwnを取得できません。	このスイッチは FC スイッチまたは FCoE スイッチではない可能性があり、サポートされていない場合もあります。データソースに設定された IP / FQDN が、本当に FC / FCoE スイッチであることを確認してください。
エラー：複数のノードが NPV スイッチポートにログインしています	NPV スイッチの直接取得をディセーブルにします
エラー：スイッチに接続できませんでした	•デバイスが起動していることを確認します •IPアドレスとリスニングポートを確認します •デバイスにpingを実行します •Cisco Device Manager GUIを使用してデバイスにログインします •CLIを使用してデバイスにログインします •SNMP Walkを実行します

パフォーマンス

問題	次の操作を実行します
エラー： Performance acquisition not supported by SNMP v1	•データソースを編集し、スイッチパフォーマンスを無効にします •SNMP v2以上を使用するように、データソースとスイッチの設定を変更します

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Cohesity SmartFilesデータコレクタ

このREST APIベースのコレクタはCohesityクラスタを取得し、「ビュー」（Data Infrastructure Insightsの内部ボリューム）、各種ノードを検出し、パフォーマンス指標を収集します。

設定

フィールド	説明
Cohesity Cluster IPの略	CohesityクラスタのIPアドレス
ユーザ名	Cohesityクラスタのユーザ名
パスワード	Cohesityクラスタ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	CohesityクラスタとのTCP通信に使用するポート
インベントリポーリング間隔（分）	インベントリのポーリング間隔。デフォルトは60分です。
パフォーマンスポーリング間隔（分）	パフォーマンスのポーリング間隔デフォルトは900秒です。

トラブルシューティング

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

デル

Dell EMC XC シリーズデータコレクタ

Data Infrastructure Insightsは、このデータコレクタを使用して、Dell EMC XCシリーズストレージアレイのインベントリとパフォーマンスの情報を検出します。

設定

フィールド	説明
プリズム外部 IP アドレス	XCサーバのIPアドレス
ユーザ名	XC サーバーのユーザー名
パスワード	XC サーバのパスワード

高度な設定

フィールド	説明
TCPポート	XC サーバーとの TCP 通信に使用されるポート
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。
パフォーマンスポーリング間隔（分）	パフォーマンスのポーリング間隔デフォルトは300秒です。

トラブルシューティング

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Dell EMC

Dell EMC Data Domain データコレクタ

このデータコレクタは、 Dell EMC Data Domain 重複排除ストレージシステムからインベントリとパフォーマンスの情報を収集します。このデータコレクタを設定するには、特定の設定手順と使用に関する推奨事項に従う必要があります。

用語集

Data Infrastructure Insightsは、Data Domain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。Data Infrastructure Insights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	**Data Infrastructure Insights**の用語
ディスク	ディスク
配列	ストレージ
FC ポート	ポート
File System の略	内部ボリューム
クォータ	クォータ
NFS 共有および CIFS 共有	ファイル共有

注意：これらは一般的な用語のマッピングのみであり、このデータ照合のすべてのケースを表しているわけで

はありません。

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。

- 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）	インベントリのポーリング間隔。デフォルトは20です。
SSHポート	SSH サービスポート

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

EMC ECS データコレクタの設定

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クラスタのIPアドレスまたはホスト名、およびユーザ名とパスワードが必要です。

Dell EMC ECSでは、raw TBから管理ユニットへの異なるレートが使用されます。未フォーマットのECS容量の40 TBごとに、1として課金されます "管理ユニット (MU)"。

用語集

Data Infrastructure Insightsは、ECS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	**Data Infrastructure Insights**の用語
クラスタ	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

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。

要件

- ECSクラスタのIPアドレスまたはホスト名
- ECSシステムのユーザ名とパスワード
- ポート4443（HTTPS）。 ECSシステムのTCPポート4443へのアウトバウンド接続が必要です。

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ユーザーID	ECSのユーザ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）	デフォルトは360分です。

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。

在庫

問題	次の操作を実行します
エラー：ユーザ認証に失敗しました。	このデバイスのクレデンシャルが正しいことを確認してください。

パフォーマンス

問題	次の操作を実行します
エラー：十分なデータが収集されていません。	•ログファイルの収集タイムスタンプを確認し、それに応じてポーリング間隔を変更します •長時間待ちます
エラー：パフォーマンスのポーリング間隔が長すぎます。	ログファイル $ ｛ logfile ｝ の収集タイムスタンプを確認し、それに応じてポーリング間隔を変更してください

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Dell EMC PowerScale データコレクタ

Data Infrastructure Insightsは、Dell EMC PowerScale（以前のIsilon）SSHデータコレクタを使用して、PowerScale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のデータを取得します。

用語集

Data Infrastructure Insights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。Data Infrastructure Insights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	**Data Infrastructure Insights**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

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。

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。

- PowerScale ストレージへの管理者権限
- PowerScale クラスタの IP アドレス
- ポート 22 への SSH アクセス

設定

フィールド	説明
IP アドレス	PowerScale クラスタの IP アドレスまたは完全修飾ドメイン名

フィールド	説明
ユーザ名	PowerScale クラスタのユーザ名
パスワード	PowerScale 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）	インベントリのポーリング間隔。デフォルトは20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です。
SSHポート	SSH サービスポートデフォルトは22です。

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。

在庫

問題	次の操作を実行します
「 Invalid login credentials 」というエラーメッセージが表示されます。「 Commands not enabled for role-based administration require root user access 」	*ユーザーがデバイス上で次のコマンドを実行する権限を持っていることを確認します。 > isiバージョンosrelease > isi status -q > isi status -n > isiデバイス-d %s > isiライセンス *ウィザードで使用されている認証情報がデバイスの認証情報と一致することを確認します
「 Command <Your Command> run failed with permission ： <your current permisse> 」というエラーメッセージが表示されて「 Internal Error 」が表示されます。sudo コマンド run permission 問題」	ユーザにデバイスで次のコマンドを実行するための sudo 権限があることを確認します

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Dell EMC Isilon / PowerScale RESTデータコレクタ

Data Infrastructure Insightsは、Dell EMC Isilon / PowerScale RESTデータコレクタを使用して、Dell EMC IsilonまたはPowerScaleストレージからインベントリおよびパフォーマンスデータを取得します。このコレクタは、OneFS 8.0.0以降を実行しているアレイをサポートします。

用語集

Data Infrastructure Insights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。Data

Infrastructure Insights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	**Data Infrastructure Insights**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
OneFSファイルシステム	内部ボリューム
OneFSファイルシステム	ストレージプール
qtree	qtree

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。

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。

- ユーザアカウントとパスワード。このアカウントは、adminまたはrootである必要はありませんが、サービスアカウントに相当数の読み取り専用権限を付与する必要があります。以下の表を参照してください
- Dell EMC Isilon / PowerScaleクラスタのIPアドレス/完全修飾ドメイン名
- ポート8080へのHTTPSアクセス
- OneFS 8.0.0以降を実行しているIsilon/PowerScaleクラスタ

権限名	説明	**R**（読み取り）または**RW**（読み取りと書き込み）
ISI_PRIV_LOGI_PAPI	プラットフォームAPI	R
ISI_PRIV_SYS_TIME	時間	R
ISI_PRIV_AUTH	認証	R
ISI_PRIV_ROLE	権限	R
ISI_PRIV_devicesのことです	デバイス	R
ISI_PRIV_EVENT	イベント	R
ISI_PRIV_HDFS	HDFS	R
ISI_PRIV_NDMP	NDMP	R
ISI_PRIV_NETWORK	ネットワーク	R
ISI_PRIV_NFS	NFS	R
ISI_PRIV_PAPI_CONFIG	プラットフォームAPIを設定します	R
ISI_PRIV_quota（ISI_PRIV_quota）	クォータ	R

権限名	説明	**R**（読み取り）または**RW**（読み取りと書き込み）
ISI_PRIV_SmartPools	SmartPools	R
ISI_PRIV_SMB	SMB	R
ISI_PRIV_STATISTICS	統計情報	R
ISI_PRIV_SWIFT	Swift	R
ISI_PRIV_JOB_ENGINE	ジョブエンジン	R

設定

フィールド	説明
IsilonのIPアドレス	Isilon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	Isilonのユーザ名
パスワード	Isilon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8080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20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です。

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。

在庫

問題	次の操作を実行します
「 Invalid login credentials 」というエラーメッセージが表示されます。「 Commands not enabled for role-based administration require root user access 」	*ユーザーがデバイス上で次のコマンドを実行する権限を持っていることを確認します。 > isiバージョンosrelease > isi status -q > isi status -n > isiデバイス-d %s > isiライセンス *ウィザードで使用されている認証情報がデバイスの認証情報と一致することを確認します
「 Command <Your Command> run failed with permission ： <your current permisse> 」というエラーメッセージが表示されて「 Internal Error 」が表示されます。sudo コマンド run permission 問題」	ユーザにデバイスで次のコマンドを実行するための sudo 権限があることを確認します

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Dell EMC PowerStore データコレクタ

EMC PowerStore データ・コレクタは '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。

EMC PowerStore データ・コレクタは 'PowerStore 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Data Infrastructure Insightsには、各PowerStoreクラスタのストレージアレイが表示され、そのクラスタのノードとストレージポートのインベントリデータが収集されます。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。

用語集

Data Infrastructure Insights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。Data Infrastructure Insights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	**Data Infrastructure Insights**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

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。

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。

- 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

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。

Cloud Insight の PowerStore パフォーマンスコレクションは、 PowerStore の 5 分間のきめ細かいソースデータを利用しています。そのため、Data Infrastructure Insights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。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Dell EMC RecoverPoint データコレクタ

EMC RecoverPoint データコレクタの主な用途は、 RecoverPoint ストレージアプライアンスによって促進されるボリューム間レプリケーション関係を検出することです。このコレクタは、 RecoverPoint アプライアンス自体も検出します。Dell/EMC では、 VM 用の VMware バックアップ解決策 「 RecoverPoint for VMS 」を販売していますが、このコレクタではサポートされていません

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。

EMC RecoverPoint データコレクタは、 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。Data Infrastructure Insights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

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。

- 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

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）	インベントリのポーリング間隔。デフォルトは20分です。
除外クラスタ	ポーリング時に対象から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。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Dell EMC ScaleIO/PowerFlexデータコレクタ

ScaleIO/PowerFlexデータコレクタは、ScaleIOおよびPowerFlexストレージからインベントリ情報を収集します。このデータコレクタを設定するには、ScaleIO/PowerFlexゲートウェイアドレス、および管理者ユーザー名とパスワードが必要です。

用語集

Data Infrastructure Insightsは、ScaleIO/PowerFlex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。Data Infrastructure Insights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	**Data Infrastructure Insights**の用語
MDM （ Meta Data Manager ）クラスタ	ストレージ
SDS（ScaleIO/PowerFlexデータサーバー）	ストレージノード
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
デバイス	ディスク

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。

要件

- Admin ユーザアカウントへの読み取り専用アクセス
- ポート要件： HTTPS ポート 443

設定

フィールド	説明
ScaleIO/PowerFlexゲートウェイ	ScaleIO/PowerFlexゲートウェイのIPアドレスまたはFQDN（カンマ（,）またはセミコロン（;）で区切ったもの
ユーザ名	ScaleIO/PowerFlexデバイスへのログインに使用する管理者ユーザー名
パスワード	ScaleIO/PowerFlex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

Inventory チェックボックスをクリックして、インベントリ収集を有効にします。

フィールド	説明
HTTPSポート	443年
インベントリのポーリング間隔（分）	デフォルトは60です。
接続タイムアウト（秒）	デフォルトは60です。

トラブルシューティング

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

EMC Unity データコレクタの設定

Dell EMC Unity （旧 VNXe ）データコレクタは、 VNXe 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。Data Infrastructure Insightsは現在、iSCSIプロトコルとNASプロトコルをサポートしています。

要件

- Unity 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 Unity 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、 Acquisition Unit から Unity への HTTPS 接続を開始できる必要があります。
- Unity デバイスの IP アドレスまたは完全修飾ドメイン名
- データコレクタで使用するためには、読み取り専用ユーザが少なくとも 1 人必要です。
- ポート 443 での HTTPS が必要です

- EMC Unity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、Data Infrastructure Insights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しません。

用語集

Data Infrastructure Insightsは、Unity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。Data Infrastructure Insights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	**Data Infrastructure Insights**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
全般的なiSCSIブロック情報、VMware VMFS	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

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
Unity ストレージ	Unity 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	Unity デバイスのユーザ名
パスワード	Unity デバイスのパスワード
実行可能 UEMCLI への完全パス	_uemcli.exe_executable を含むフォルダへの完全パス

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分です
Unity CLI ポート	Unity CLI に使用するポート
パフォーマンスのポーリング間隔（秒）	デフォルトは300です。

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。

在庫

問題	次の操作を実行します
「 Failed to execute external utility 」というエラーメッセージが表示され、「 Failed to find Unisphere executable uemcli 」	正しい**IP**アドレス、ユーザー名、パスワードを確認します。 Unisphere CLIがData Infrastructure Insights Acquisition Unitにインストールされていることを確認します。*データソース構成でUnisphere CLIのインストールディレクトリが正しいことを確認します。*データソースの構成でVNXeのIPが正しいことを確認します。Data Infrastructure Insights Acquisition UnitでCMDを開き、設定されているインストールディレクトリ$ {INSTALLDIRに移動します。次のように入力して、 VNXe デバイスとの接続を試みます。 uemcli -d <your ip>-u <your ID>/sys/general show

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Dell EMC VMAX および **PowerMax** ファミリのデバイスデータコレクタ

Data Infrastructure Insightsは、Solutions Enablerのsymcliコマンドと環境内の既存のSolutions Enablerサーバを使用して、EMC VMAXおよびPowerMaxストレージアレイを検出します。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 VMAX/PowerMax ストレージアレイに接続できます。

要件

このデータコレクタを設定する前に、Data Infrastructure Insightsが既存のSolutions Enablerサーバのポート2707にTCP接続されていることを確認する必要があります。Data Infrastructure Insightsは、このサーバからの「symcfg list」出力に示されるように、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 Acquisition Unit サーバにインストールされている必要があります。 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が必要です。
- 適切に設定された {installdir}\EMC\SYMAPI\config\netcnfg ファイルが必要です。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。
- 管理用 Solutions Enabler サーバの IP アドレス
- 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
- UNISPHERE for VMAX アプリケーションを実行して、 SMI-S プロバイダのインストールで管理される EMC VMAX および PowerMax ストレージアレイの統計を収集する必要があります
- パフォーマンスのためのアクセスの検証：Acquisition UnitのWebブラウザで、_\ https：//<SMI-S Hostname or IP>：5989/ecomconfig_に移動します。「SMI-S Hostname or IP」は、SMI-SサーバのIPアドレスまたはホスト名です。このURLは'EMC SMI-S（ECOM）サービスの管理ポータル用であり'ログイン・ポップアップが表示されます

- 権限はSolutions Enablerサーバのデーモン構成ファイルで宣言する必要があります。通常は次の場所にあります。*/var/symapi/config/demon _users*

  次に、適切なciscysアクセス権を持つサンプルファイルを示します。

```
root@cernciaukc101:/root
14:11:25 # tail /var/symapi/config/daemon_users
###
###     Refer to the storrdfd(3) man page for additional details.
###
###     As noted above, only authorized users can perform stordaemon
control
###     operations (e.g., shutdown).
##############################################################################
########
# smith         storrdfd
cisys storapid <all>
```

用語集

Data Infrastructure Insightsでは、EMC VMAX / PowerMaxデータソース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	**Data Infrastructure Insights**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

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。

設定

注： SMI-Sユーザ認証が有効になっていない場合、Data Infrastructure Insightsデータコレクタのデフォルト値は無視されます。

フィールド	説明
サービス名	_netcnfG_file で指定されたサービス名
CLI の完全パス	Symmetrix CLI を含むフォルダへのフル・パス

フィールド	説明
SMI-S ホストの IP アドレス	SMI-S ホストの IP アドレス

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。
インベントリフィルタデバイスリスト	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
接続のキャッシュ	接続キャッシュ方法の選択： * local は 'Solutions Enabler サーバ上で Cloud Insights 取得サービスが実行されていることを意味しますこのサーバは ' 検出対象の Symmetrix アレイにファイバ・チャネルで接続されており ' 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このオプションは、一部の Remote Acquisition Unit （ RAU ）構成で使用されます。* REMOTE_CACHED はデフォルトの設定であり、ほとんどの状況でこのオプションを使用します。このオプションでは、 NETCNFG ファイルの設定に基づいて、 IP を使用して Solutions Enabler サーバに接続します。サーバは検出対象の Symmetrix アレイにファイバチャネルで接続されていて、ゲートキーパーボリュームにアクセスできる必要があります。* REMOTE_CACHED オプションで CLI コマンドが失敗する場合は、 REMOTE オプションを使用します。データ収集プロセスが遅くなることに注意してください（数時間から場合によっては数日かかることがあります）。検出対象の Symmetrix アレイにファイバチャネルで接続された Solutions Enabler サーバへの IP 接続には、引き続き NETCNFG ファイルの設定が使用されます。*注：*この設定では、「symcfg list」の出力でREMOTEと表示されているアレイに対するData Infrastructure Insightsの動作は変更されません。Data Infrastructure Insightsは、このコマンドでLOCALと表示されているデバイスのデータのみを収集します。
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。使用されているデフォルトのポートも表示されます。
SMIS-Port をオーバーライドします	空白の場合は、 [Connection Type] フィールドでデフォルトのポートを使用します。それ以外の場合は、使用する接続ポートを入力します
SMI-S ユーザー名	SMI-S プロバイダホストのユーザ名
SMI-S のパスワード	SMI-S プロバイダホストのユーザ名

フィールド	説明
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）
リストを指定するには、「除外」または「含める」を選択します	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

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
エラー：要求されている機能のライセンスがありません	SYMAPI サーバ・ライセンスをインストールします
エラー：デバイスが見つかりませんでした	SymmetrixデバイスがSolutions Enablerサーバによって管理されるように構成されていることを確認します - symcfg list -vを実行して’構成されているSymmetrixデバイスのリストを表示します
エラー：要求されたネットワークサービスがサービスファイルで見つかりませんでした	Solutions Enabler サービス名が Solutions Enabler 用の netcnfg ファイルとして定義されていることを確認します。このファイルは通常 'Solutions Enabler クライアントのインストールの SYMAPI\config\ にあります
エラー：リモートクライアント / サーバハンドシェイクに失敗しました	検出しようとしている Solutions Enabler ホストの最新の storsrvd.log * ファイルを確認します
エラー：クライアント証明書の共通名が無効です	Solutions Enabler サーバの _hosts_file を編集して、Acquisition Unit のホスト名が Solutions Enabler サーバの storsrvd.log で報告された IP アドレスに解決されるようにします。
エラー：機能がメモリを取得できませんでした	Solutions Enabler を実行するための十分な空きメモリがシステムにあることを確認してください
エラー： Solutions Enabler は必要なすべてのデータを提供できませんでした。	Solutions Enabler の正常性ステータスとロードプロファイルを調査します
エラー： •Solutions Enablerサーバ8.xからSolutions Enabler 7.xを使用して収集した場合、CLIコマンドsymcfg list -tdevが誤ったデータを返すことがあります •Solutions Enabler 8.1.0以前でSolutions Enabler 8.3以降からSolutions Enabler 8.1.0以前を使用して収集した場合、CLIコマンド「symcfg list-srp」から誤ったデータが返されることがあります。	Solutions Enabler のメジャーリリースが同じであることを確認してください

問題	次の操作を実行します
「unknown code」というメッセージが表示され、データ収集エラーが発生しました。	Solutions Enablerサーバのデーモン構成ファイルで権限が宣言されていない場合は、このメッセージが表示されることがあります（を参照） 要件 上記を参照 ）。これは、SEクライアントのバージョンがSEサーバのバージョンと一致していることを前提としています。 このエラーは'Solutions Enablerコマンドを実行する_cisys_userが/var/symapi/config/demon _users構成ファイルで必要なデーモン権限で構成されていない場合にも発生することがあります これを修正するには、/var/symapi/config/demonファイルを編集し、cisysユーザにstorapidデーモンに対して指定された<all> 権限があることを確認します。 例 14:11:25 #tail /var/symapi/config/demonユーザーな…何だ? cisys storapid <all>の略

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Dell EMC VNX Block Storage （ NaviCLI ）データコレクタ

Data Infrastructure Insightsは、Dell EMC VNX Block Storage（NaviSec）データコレクタ（旧CLARiX）を使用して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。

用語集

Data Infrastructure Insightsは、EMC VNX Block Storage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。Data Infrastructure Insights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	**Data Infrastructure Insights**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
このプール 'RAID グループ	ストレージプール
LUN	ボリューム

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

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。

- 各 VNX ブロックストレージプロセッサの IP アドレス
- VNX ブロックストレージ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
- NaviseccliがData Infrastructure Insights AUにインストールされていること
- アクセスの検証：ユーザー名とパスワードを使用して、Data Infrastructure Insights AUから各アレイに対してnaviseccliを実行します。
- ポート要件： 80 、 443
- naviseccli 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
- パフォーマンスを収集するには、統計のログを有効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>コマンド

設定

フィールド	説明
VNX Block Storage の IP アドレス	VNX ブロックストレージの IP アドレスまたは完全修飾ドメイン名
ユーザ名	VNX ブロック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	VNX ブロック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 から naviseccli.exe へのパス	_naviseccli.exe_executable を含むフォルダへの完全パス

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分です。
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。
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秒です。

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。

在庫

問題	次の操作を実行します
エラー： • エージェントが実行されてい • naviseccliが見つかりませんでした • コマンドを実行できませんでした	• Navisphere CLIがCloud Insight Acquisition Unitにインストールされていることを確認する • データコレクタ設定ウィザードで[Use secure client]オプションが選択されておらず、セキュアでないバージョンのNavisphere CLIがインストールされていません。 • データコレクタ構成でNavisphere CLIのインストールディレクトリが正しいことを確認する • データコレクタ構成でVNXブロックストレージのIPが正しいことを確認します。 • Data Infrastructure Insights Acquisition Unitから： ◦ CMDを開きます。 ◦ 設定したインストールディレクトリにディレクトリを変更します。 ◦ 「navicli -h {ip} getagent」と入力して、VNXブロックストレージデバイスとの接続を試行します（{ip}を実際のIPに置き換えます）。
エラー： 4.29 emc235848 emc241018 getAll Failed to parse host alias info	これは ' アレイ自体のホスト・イニシエータ・データベースの問題が FLARE 29 によって破損したことが原因で発生する可能性がありますEMC ナレッジベースの記事 emc235848 、 emc241018 を参照してください。チェックすることもできます https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128
エラー：メタデータ LUN を取得できません。java -jar navicli.jar の実行中にエラーが発生しました	• セキュアクライアントを使用するようにデータコレクタの設定を変更する（推奨） • navicli.exeまたはnaviseccli.exeへのCLIパスにnavicli.jarをインストールします。 • 注：navicli.jarはEMC Navisphereバージョン6.26で廃止されました • navicli.jarは\http://powerlink.emc.comから入手できます。
エラー：ストレージプールから、設定された IP アドレスのサービスプロセッサのディスクが報告されません	サービスプロセッサの両方の IP をカンマで区切ってデータコレクタを設定します

問題	次の操作を実行します
エラー：リビジョン不一致エラー	• これは通常、VNXブロックストレージデバイスのファームウェアの更新が原因で発生しますが、NaviCLI.exeのインストールは更新されません。ファームウェアが異なる複数のデバイスがあっても、インストールされている CLI が 1 つだけ（ファームウェアバージョンが異なる）の場合にも、この問題が発生する可能性があります。 • デバイスとホストの両方で同じバージョンのソフトウェアが実行されていることを確認します。 ◦ Data Infrastructure Insights Acquisition Unit で、コマンドラインウィンドウを開く ◦ 設定したインストールディレクトリにディレクトリを変更します。 ◦ 「navicli -h <ip> getagent」と入力して、CLARiXデバイスとの接続を確立します。 ◦ 最初の2行でバージョン番号を探します。例：エージェントリビジョン：6.16.2(0.1) ◦ 最初の行のバージョンを探して比較します。例： Navisphere CLI Revision 6.07.00.04.07
エラー：サポート対象外の構成 - Fibre Channel ポートがありません	デバイスにファイバチャネルポートが設定されていない。現在サポートされているのは FC 構成のみです。 このバージョン / ファームウェアがサポートされていることを確認してください。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Dell EMC VNX File （旧 Celerra Unified Storage System ）データコレクタ

このデータコレクタは、 VNX File Storage System からインベントリ情報を取得します。この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

Data Infrastructure Insightsは、VNX File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。Data Infrastructure Insights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	**Data Infrastructure Insights**の用語
Celerra Network Server/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

ベンダー / モデルの用語	**Data Infrastructure Insights**の用語
データムーバー	コントローラ
データムーバー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

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。

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。

- 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
VNX ファイルの IP アドレス	VNX File 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	VNX File デバイスへのログインに使用する名前
パスワード	VNX File 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）	インベントリのポーリング間隔。デフォルトは20分です。

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。

在庫

問題	次の操作を実行します
エラー： DART の更新の実行中は処理を続行できません	Possible 解決策：データコレクタを一時停止し、DART のアップグレードが完了するのを待ってから、別の取得要求を実行します。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Dell EMC VNX Unified データコレクタの設定

Dell EMC VNX Unified （ SSH ）データコレクタを設定するには、 Control Station 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

Data Infrastructure Insights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。Data Infrastructure Insights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	**Data Infrastructure Insights**の用語
ディスク	ディスク
ディスクフォルダ	ディスクグループ
ファイルシステム	内部ボリューム
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
ストレージプール、 RAID グループ	ストレージプール
LUN	ボリューム
データムーバー	コントローラ
データムーバー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

要件

VNX （ SSH ）データコレクタを構成するには、次のものが必要です。

- VNX IP アドレスと資格情報を Celerra Control Station に追加します。
- 読み取り専用のユーザ名とパスワード
- データコレクタは 'DART OS NAS ヘッドを使用して ' バックエンド・アレイに対して NaviCLI/naviseccli コマンドを実行できます

設定

フィールド	説明
VNX IP アドレス	VNX Control Station の IP アドレスまたは完全修飾ドメイン名
ユーザ名	VNX Control Station のユーザー名
パスワード	VNX Control Station 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40分です。
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秒です。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

EMC VPLEXデータコレクタの設定

このデータコレクタは、EMC VPLEX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、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。

VPLEXクラスタからData Infrastructure Insightsのパフォーマンス収集を行うには、Data Infrastructure InsightsがSCPベースのファイルコピーを介して取得する.csvファイルとログを取り込むために、パフォーマンスアーカイブサービスが動作している必要があります。VPLEX ファームウェアのアップグレード / 管理ステーションの更新の多くが、この機能を動作不能にすることが確認されています。このようなアップグレードを計画しているお客様は、計画しているアップグレードによってこの機能が動作不能になる場合は、 Dell/EMC に事前に問い合わせてください。問題が発生した場合、パフォーマンスの可視性のギャップを最小限に抑えるために、どのように IT を再有効化できますか。Cloud InsightのVPLEXパフォーマンスコードは、各ポーリングで想定されるすべてのファイルが存在するかどうか、およびファイルが適切に更新されているかどうかを評価します。不足しているファイルや古いファイルがある場合、Data Infrastructure Insightsはパフォーマンス収集の失敗をログに記録します。

用語集

Data Infrastructure Insightstは、VPLEX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	**Data Infrastructure Insights**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、システムエクステント	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

ベンダー / モデルの用語	**Data Infrastructure Insights**の用語
ITL	バックエンドパス

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。

要件

- VPLEX Management Console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。

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に使用するパスワード
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。デフォルトは443です。
インベントリポーリング間隔（分）	デフォルトは20分です。
接続の再試行回数	デフォルトは3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600秒です。
再試行回数	デフォルトは2です。

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。

在庫

問題	次の操作を実行します
エラー：ユーザ認証に失敗しました。	このデバイスのクレデンシャルが正しいことを確認してください。

パフォーマンス

問題	次の操作を実行します
エラー：バージョン 5.3 より前の VPLEX パフォーマンスはサポートされていません。	VPLEX を 5.3 以上にアップグレードします
エラー：十分なデータが収集されていません。	•ログファイルの収集タイムスタンプを確認し、それに応じてポーリング間隔を変更します •長時間待ちます
エラー：恒久的なログファイルは更新されていません。	永続ログファイルの更新を有効にするには、 EMC サポートにお問い合わせください
エラー：パフォーマンスのポーリング間隔が長すぎます。	ログファイル $ ｛ logfile ｝ の収集タイムスタンプを確認し、それに応じてポーリング間隔を変更してください
エラー： VPLEX Management Console のパフォーマンスリモートの IP アドレスが設定されていません。	データソースを編集して、 VPLEX Management Console のパフォーマンスリモート IP アドレスを設定します。
エラー：ディレクタからパフォーマンスデータが報告されていません	•システムパフォーマンスモニタが正しく動作していることを確認します •システムパフォーマンスモニタログファイルの更新を有効にするには、EMCサポートにお問い合わせください

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Dell EMC XtremIO データコレクタ

EMC XtremIO データコレクタは、 EMC XtremIO ストレージシステム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

EMC XtremIO （ HTTP ）データコレクタを設定するには、次のものが必要です。

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

用語集

Data Infrastructure Insightsは、EMC XtremIO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。Data Infrastructure Insights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	**Data Infrastructure Insights**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
ターゲット FC イニシエータ	ボリュームマスク

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

- XtremIO Management Server （ XMS ）ホストの IP アドレス
- XtremIO の管理者のユーザ名とパスワード

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です。
インベントリのポーリング間隔（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。
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秒です。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Fujitsu Eternus データコレクタ

Fujitsu Eternus データコレクタは、管理者レベルのストレージシステムアクセスを使用してインベントリデータを取得します。

用語集

Data Infrastructure Insightsは、Fujitsu ETERNUSストレージから次のインベントリ情報を取得します。Data Infrastructure Insights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	**Data Infrastructure Insights**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、スナップデータボリューム（ SDV ）、スナップデータプールボリューム（ SDPV ）、シンプロビジョニングボリューム（ TPV ）、フレキシブル階層ボリューム（ FTV ）、ワイドストライピングボリューム（ WSV ）	ボリューム
チャネルアダプタ	コントローラ

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、このデータ照合のすべてのケースを表しているわけではありません。

要件

このデータコレクタを設定するには、次のものが必要です。

- 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（ clienv -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	Eternus ストレージのパスワード

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）	デフォルトは20分です。

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。

在庫

問題	次の操作を実行します
「 Error Retrieving data 」というエラーメッセージが表示され、「 Error Finding Prompt CLI 」または「 Error Finding prompt at the end of shell results 」が表示されます。	考えられる原因：ストレージシステムでページスクロールが有効になっています。 可能性のある解決策： *次のコマンドを実行して、ページのスクロールを無効にしてみてください。 clientv-show-more-scroll disableを設定します
「 Connecting error 」とエラーメッセージ「 Failed to instantiate an SSH connection to storage 」または「 Failed to instantiate a connection to VirtualCenter 」が表示されます。	考えられる原因： *認証情報が正しくありません。 * IP アドレスが正しくありません。 * ネットワークの問題。 * ストレージが停止しているか、応答しない可能性があります 考えられる解決策： * 入力された資格情報と IP アドレスを確認してください。 * SSH クライアントを使用してストレージと通信してみてください。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

NetApp Google Compute データコレクタ

このデータコレクタは、 Google Compute クラウドプラットフォーム構成からのインベントリとパフォーマンスの収集をサポートします。このコレクタは、 1 つの Google 組織内のすべてのプロジェクト内のすべてのコンピューティングリソースを検出しようとします。Data Infrastructure Insightsで検出したいGoogle組織が複数ある場合は、組織ごとにData Infrastructure Insightsコレクタを1つ導入します。

設定

フィールド	説明
組織 ID	このコレクタで検出する組織 ID 。サービスアカウントが複数の組織を表示できる場合は、このフィールドが必要です

フィールド	説明
GCP プロジェクトを ID でフィルタリングするには、[除外] または [含める] を選択します	Data Infrastructure Insightsに取り込むプロジェクトのリソースを制限する場合は、
プロジェクト ID	「除外する」値の値に応じて、フィルタするプロジェクト ID または検出から除外するプロジェクト ID のリスト。デフォルトリストは空です
クライアント ID	Google Cloud Platform 構成のクライアント ID
Google 資格情報ファイルの内容をここにコピーして貼り付けます	Cloud Platform アカウントの Google クレデンシャルをこのフィールドにコピーします

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
VM をラベルでフィルタリングするには、「除外」または「含める」を選択します	データの収集時に VM をラベルで含めるか除外するかを指定します。「含める」が選択されている場合は、「ラベルキー」フィールドを空白にすることはできません。
VM をフィルタリングするキーと値を指定します	VM のキーとラベルの値に一致するキーと値でフィルタリングして、対象に含める VM （および関連するディスク）を選択するには、「 * + フィルタラベル * 」をクリックします。ラベルキーは必須です。ラベル値はオプションです。ラベル値が空の場合、 VM はラベルキーと一致するかぎり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）	デフォルト値は 1800 秒です

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

HP エンタープライズ

HP Enterprise Alletra 9000/Primera Storage データコレクタ

Data Infrastructure Insightsは、HP Enterprise Alletra 9000/HP Enterprise Primera（以前の3PAR）データコレクタを使用してインベントリとパフォーマンスを検出します。

用語集

Data Infrastructure Insights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。Data Infrastructure Insights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。

フィールド	説明
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

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。

要件

このデータコレクタを設定するには、次のものが必要です。

- InServ クラスタの IP アドレスまたは FQDN
- インベントリの場合は、 StoreServ サーバへの読み取り専用のユーザ名とパスワード
- パフォーマンスを確保するために、 StoreServ サーバへの読み取り / 書き込み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 、 5989 （パフォーマンス収集） [注： StoreServ OS 3.x + ではパフォーマンスがサポートされます]
- パフォーマンス収集を行うには、 SSH を使用して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ます。

設定

フィールド	説明
ストレージ IP アドレス	StoreServ クラスタのストレージ IP アドレスまたは完全修飾ドメイン名
ユーザ名	StoreServ サーバのユーザ名
パスワード	StoreServ サーバのパスワード
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

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分です。
SMI-S 接続	SMI-S プロバイダへの接続に使用するプロトコル
SMI-S のデフォルトポートを上書きします	空白の場合は、 SMI-S Connectivity のデフォルトポートを使用します。それ以外の場合は、使用する接続ポートを入力します

フィールド	説明
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秒です。

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。

在庫

問題	次の操作を実行します
"showsys" コマンドを実行しても結果は返されません。	コマンドラインから「 showsys 」と「 showversion-a 」を実行し、バージョンがアレイでサポートされているかどうかを確認します。

パフォーマンス

問題	次の操作を実行します
接続またはログインに失敗しました。プロバイダの初期化に失敗しました	すべて数値のアレイ名は、 SMI-S サーバで原因の問題が発生する可能性があります。アレイ名を変更してください。
SMI-S ユーザが設定されていますが、ドメインがありません	構成した SMI-S ユーザに適切なドメイン権限を付与します
Data Infrastructure Insightsでは、SMI-Sサービスに接続/ログインできないと報告されています。	CI AU とアレイの間に、 CI AU と TCP 接続をブロックするファイアウォールがないことを確認します。これが完了し、ファイアウォールがないことを確認したら、アレイに SSH 接続し、「 showcim 」コマンドを使用して確認する必要があります。 以下を確認します。 *サービスは有効です * HTTPSが有効です * HTTPSポートは5989にする必要があります その場合は、「stopcim」を実行してから「startcim」を実行してCIM（SMI-Sサービスなど）を再起動します。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

HP Enterprise Command View データコレクタ

HP Enterprise Command View Advanced Edition データコレクタは、 Command View Advanced Edition (CVAE) サーバーを使用した XP アレイと P9500 アレイの検出をサポートしています。Data Infrastructure Insightsは、標準のCommand View APIを使用してCVAEと通信し、インベントリやパフォーマンスのデータを収集します。

用語集

Data Infrastructure Insightsは、HP Enterprise Command View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。Data Infrastructure Insights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	**Data Infrastructure Insights**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

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。

- CVAEサーバのIPアドレス
- CVAE ソフトウェアおよびピア特権の読み取り専用ユーザ名とパスワード
- ポート要件： 2001

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 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Data Infrastructure Insights AUにコピーし、特定の場所に展開する必要があります。CI Linux AUS で、「 ciscys 」に読み取りおよび実行権限があることを確認します。
  - 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。
- 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Data Infrastructure Insights AUにインストールされている。
- ネットワーク要件
  - エクスポートツールは Java ベースであり、 RMI を使用してアレイと通信します。これらのツール

は、呼び出しごとに送信元と宛先の TCP ポートを動的にネゴシエートするため、ファイアウォールとの親和性がない場合があります。また、異なるモデルアレイのエクスポートツールがネットワーク全体で異なる動作をする場合があります。ご使用のモデルの要件については、 HPE にお問い合わせください

設定

フィールド	説明
Command View Server の順にクリックします	Command View 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	Command View サーバのユーザ名。
パスワード	Command View サーバのパスワード
デバイス - VSP G1000 （ R800 ）、 VSP （ R700 ）、 HUS VM （ HM700 ）、および USP ストレージ	VSP G1000 （ R800 ）、 VSP （ R700 ）、 HUS VM （ HM700 ）、および USP ストレージのデバイスリスト。各ストレージには以下が必要です。 *アレイのIP：ストレージのIPアドレス *ユーザー名：ストレージのユーザー名 *パスワード：ストレージのパスワード *エクスポートユーティリティJARファイルを含むフォルダ
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。 *アレイのIP：ストレージのIPアドレス * Storage Navigator CLI Path：SNM2 CLIパス * Account Authentication Valid：有効なアカウント認証を選択する場合に選択します *ユーザー名：ストレージのユーザー名 *パスワード：ストレージのパスワード
「 Tuning Manager 」を「 Performance 」に選択します	他のパフォーマンスオプションよりも優先されます
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

注： 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
Command View Server のポート	Command View Server 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
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。

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。

在庫

問題	次の操作を実行します
エラー：ユーザに十分な権限がありません	別のユーザアカウントを使用して、権限を追加するか、データコレクタで設定されているユーザアカウントの権限を増やします
エラー：ストレージリストが空です。デバイスが設定されていないか、ユーザに十分な権限がありません	*デバイスが設定されているかどうかを確認するには、DeviceManagerを使用します。 *より多くの権限を持つ別のユーザーアカウントを使用するか、ユーザーアカウントの権限を増やしてください
エラー： HDS ストレージアレイが数日間更新されませんでした	HP CommandView AE でこのアレイが更新されない理由を確認してください。

パフォーマンス

問題	次の操作を実行します
エラー： *エクスポートユーティリティの実行中にエラーが発生しました *外部コマンド実行中にエラーが発生しました	* Data Infrastructure Insights Acquisition Unitにエクスポートユーティリティがインストールされていることを確認*データコレクタ設定でエクスポートユーティリティの場所が正しいことを確認*データコレクタ設定でUSP/R600アレイのIPが正しいことを確認*データコレクタ設定でユーザ名とパスワードが正しいことを確認* Data Insights Infrastructure Acquisition Unitのインストールディレクトリから次のディレクトリを開きますrunWin.bat。
エラー：ターゲット IP のエクスポートツールのログインに失敗しました	*ユーザー名/パスワードが正しいことを確認します *主にこのHDSデータコレクタのユーザIDを作成します *このアレイを取得するように他のデータコレクタが設定されていないことを確認します

問題	次の操作を実行します
エラー：「 Unable to get time range for monitoring 」というメッセージが表示されます。	* アレイでパフォーマンス監視が有効になっていることを確認します。* Data Infrastructure Insightsの外部でエクスポートツールを呼び出して、問題がData Infrastructure Insightsの外部にあることを確認してください。
エラー： *構成エラー：ストレージアレイはエクスポートユーティリティでサポートされていません *構成エラー：ストレージアレイはStorage Navigator Modular CLIでサポートされていません	* サポートされているストレージアレイのみを構成します。 * サポートされていないストレージ・アレイを除外するには ' フィルタ・デバイス・リストを使用します
エラー： *外部コマンド実行中にエラーが発生しました *構成エラー：ストレージアレイがインベントリで報告されていません *設定エラー：エクスポートフォルダにjarファイルが含まれていません	* エクスポートユーティリティの場所を確認します。 *対象のストレージアレイがCommand Viewサーバで設定されているかどうかを確認してください *パフォーマンスのポーリング間隔を60秒の倍数に設定します。
エラー： *ストレージナビゲータCLIでエラーが発生しました * auperformコマンドの実行中にエラーが発生しました *外部コマンド実行中にエラーが発生しました	* Data Infrastructure Insights Acquisition UnitにStorage Navigator Modular CLIがインストールされていることを確認*データコレクタ設定でStorage Navigator Modular CLIの場所が正しいことを確認*データコレクタ設定でWMS/SMS/SMSアレイのIPが正しいことを確認* Storage Navigator Modular CLIバージョンがデータコレクタに設定されているストレージアレイのマイクロコードバージョンと互換性があることを確認* Data Infrastructure Insights Acquisition Unitであることを実行していることを確認していることを確認していることを確認するコマンドを実行します。
エラー：設定エラー：ストレージアレイがインベントリから報告されません	Command View サーバで、該当するストレージアレイが設定されているかどうかを確認します
エラー： * Storage Navigator Modular 2 CLIに登録されているアレイがありません *アレイがStorage Navigator Modular 2 CLIに登録されていません *構成エラー：ストレージアレイがStorageNavigator Modular CLIに登録されていません	*コマンドプロンプトを開き、設定したパスにディレクトリを変更します *「SET=STONAVM_HOME=」コマンドを実行します。 *「auunitref」コマンドを実行します。 *コマンド出力にIPを持つアレイの詳細が含まれていることを確認します *出力にアレイの詳細が含まれていない場合は、ストレージナビゲータCLIにアレイを登録します。 -コマンドプロンプトを開き、設定したパスにディレクトリを変更します -「SET=STONAVM_HOME=」コマンドを実行します。 -コマンド「auunitaddauto-ip$ {ip} 」を実行します。$ ｛IP｝ を実際の IP に置き換えてください

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

HPE Alletra 6000 データコレクタ

HP Enterprise Alletra 6000 （以前の Nimble ）データコレクタは、 Alletra 6000 ストレージアレイのインベントリデータとパフォーマンスデータをサポートしています。

用語集

Data Infrastructure Insightsでは、このコレクタから次のインベントリ情報を取得します。Data Infrastructure Insights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	**Data Infrastructure Insights**の用語
配列	ストレージ
ディスク	ディスク
ボリューム	ボリューム
プール	ストレージプール
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

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。

要件

ストレージアレイからインベントリデータと構成データを収集するには、次の情報が必要です。

- 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「 Operator 」レベル以上のロールで設定されている必要があります。「ゲスト」ロールには、イニシエータの設定を理解するための十分なアクセス権がありません。
- アレイのポート 5392 が開いている必要があります。

ストレージアレイからパフォーマンスデータを収集するには、次の情報が必要です。

- アレイが NimbleOS 4.0.0 以降を実行している必要があります
- アレイにはボリュームが設定されている必要があります。NimbleOSのパフォーマンスAPIはボリュームのみで、Data Infrastructure Insightsの統計はボリュームの統計から取得されます。

設定

フィールド	説明
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	アレイのユーザ名
パスワード	アレイのパスワード

高度な設定

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

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。HPE Alletra 6000 でサポートされている唯一の間隔です。

Hitachi Data Systems の略

Hitachi Vantara Command Suite データコレクタ

Hitachi Vantara コマンドスイートのデータコレクタは、 HiCommand Device Manager サーバをサポートします。Data Infrastructure Insightsは、標準のHiCommand APIを使用してHiCommand Device Managerサーバと通信します。

用語集

Data Infrastructure Insightsは、Hitachi Vantara Command Suite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。Data Infrastructure Insights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	**Data Infrastructure Insights**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 'HDS プール	ストレージプール
論理ユニット、 LDEV	ボリューム

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。

ストレージ

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。

- 名前– HDS HiCommand Device Manager の「 name 」属性から GetStorageArray XML API 呼び出しを介して直接取得されます
- Model ： HDS HiCommand Device Manager の ［ arrayType ］ 属性から GetStorageArray XML API 呼び出しを使用して直接取得します
- ベンダー– HDS （ Hitachi ）
- Family - GetStorageArray XML API 呼び出しを使用して、 HDS HiCommand Device Manager の「 arrayFamily 」属性から直接取得します
- 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 アドレスの完全なリストではありません
- 物理容量–ディスクの役割に関係なく、このシステム内のすべてのディスクの合計容量を表す base2 値。

ストレージプール

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。
  - 予約済み：このプールがデータボリューム以外の目的専用の場合（ジャーナリング、スナップショット）
  - シンプロビジョニング– HDP プールの場合
  - RAID グループ–次のような理由が考えられません。

    Data Infrastructure Insightsでは、どのようなコストであっても容量が二重にカウントされることを避けるために、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。Data Infrastructure Insightsが基盤となるRAIDグループとプールの両方を現状のまま報告した場合、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。

  代わりに、Data Infrastructure InsightsのHDS Command Suite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、Data Infrastructure InsightsでRAIDグループがまったく報告されない可能性があります。また、作成されたRAIDグループには、Data Infrastructure Insights Web UIには表示されず、Data Infrastructure Insights Data Warehouse（DWH）には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を UI の混乱から回避することです。 HDS アレイに 50 MB の空きがある RAID グループがある場合は、その空きスペースを有効な結果に使用できない可能性があります。

- 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えている論理ボリ

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る」ことを示す派生値

- 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

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のフロントエンドディレクタ（ 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
- volumes –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 Volume テーブルに表示されます

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。

- 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 ）
- 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\http：//<HiCommand_Device_Manager_IP>：2001/service/StorageManager へのアクセスを確認します。

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 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Data Infrastructure Insights AU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。
- AMS のパフォーマンス：
  - NetAppでは、Data Infrastructure Insightsがパフォーマンスデータの取得に使用する専用のサービスアカウントをAMSアレイに作成することを強く推奨しています。Storage Navigator では、ユーザーアカウントでアレイへの同時ログインが 1 つだけ許可されています。Data Infrastructure Insightsで管理スクリプトまたはHiCommandと同じユーザアカウントを使用すると、1つのユーザアカウントの同時ログイン制限が原因でData Infrastructure Insights、管理スクリプト、またはHiCommandがアレイと通信できなくなることがあります。
  - 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Data Infrastructure Insights AUにインストールされている必要があります。

設定

フィールド	説明
HiCommand サーバ	HiCommand Device Manager サーバの IP アドレスまたは完全修飾ドメイン名
ユーザ名	HiCommand Device Manager サーバのユーザ名
パスワード	HiCommand Device Manager サーバのパスワード
デバイス - VSP G1000 （ R800 ）、 VSP （ R700 ）、 HUS VM （ HM700 ）、および USP ストレージ	VSP G1000 （ R800 ）、 VSP （ R700 ）、 HUS VM （ HM700 ）、および USP ストレージのデバイスリスト。各ストレージには以下が必要です。 *アレイのIP：ストレージのIPアドレス *ユーザー名：ストレージのユーザー名 *パスワード：ストレージのパスワード *エクスポートユーティリティJARファイルを含むフォルダ
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。 *アレイのIP：ストレージのIPアドレス * Storage Navigator CLI Path：SNM2 CLIパス * Account Authentication Valid：有効なアカウント認証を選択する場合に選択します *ユーザー名：ストレージのユーザー名 *パスワード：ストレージのパスワード
「 Tuning Manager 」を「 Performance 」に選択します	他のパフォーマンスオプションよりも優先されます
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 ポートを上書きします	空白の場合は、 Choose Tuning Manager for Performance フィールドのデフォルトポートを使用します。それ以外の場合は、使用するポートを入力します
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

注： 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
接続タイプ	HTTPS または HTTP では、デフォルトのポートも表示されます
HiCommand Server ポート	HiCommand Device Manager 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。
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がタイムアウトしました。デフォルトは300です。

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。

在庫

問題	次の操作を実行します
エラー：ユーザに十分な権限がありません	別のユーザアカウントを使用して、権限を追加するか、データコレクタで設定されているユーザアカウントの権限を増やします
エラー：ストレージリストが空です。デバイスが設定されていないか、ユーザに十分な権限がありません	*デバイスが設定されているかどうかを確認するには、DeviceManagerを使用します。 *より多くの権限を持つ別のユーザーアカウントを使用するか、ユーザーアカウントの権限を増やしてください
エラー： HDS ストレージアレイが数日間更新されませんでした	HDS HiCommand でこのアレイが更新されない理由を確認します。

パフォーマンス

問題	次の操作を実行します
エラー： *エクスポートユーティリティの実行中にエラーが発生しました *外部コマンド実行中にエラーが発生しました	* Data Infrastructure Insights Acquisition Unitにエクスポートユーティリティがインストールされていることを確認*データコレクタ設定でエクスポートユーティリティの場所が正しいことを確認*データコレクタ設定でUSP/R600アレイのIPが正しいことを確認*データコレクタ設定でユーザ名とパスワードが正しいことを確認* Data Insights Infrastructure Acquisition Unitのインストールディレクトリから次のディレクトリを開きますrunWin.bat。
エラー：ターゲット IP のエクスポートツールのログインに失敗しました	*ユーザー名/パスワードが正しいことを確認します *主にこのHDSデータコレクタのユーザIDを作成します *このアレイを取得するように他のデータコレクタが設定されていないことを確認します

問題	次の操作を実行します
エラー：「 Unable to get time range for monitoring 」というメッセージが表示されます。	* アレイでパフォーマンス監視が有効になっていることを確認します。* Data Infrastructure Insightsの外部でエクスポートツールを呼び出して、問題がData Infrastructure Insightsの外部にあることを確認してください。
エラー： *構成エラー：ストレージアレイはエクスポートユーティリティでサポートされていません *構成エラー：ストレージアレイはStorage Navigator Modular CLIでサポートされていません	* サポートされているストレージアレイのみを構成します。 * サポートされていないストレージ・アレイを除外するには ' フィルタ・デバイス・リストを使用します
エラー： *外部コマンド実行中にエラーが発生しました *構成エラー：ストレージアレイがインベントリで報告されていません *設定エラー：エクスポートフォルダにjarファイルが含まれていません	* エクスポートユーティリティの場所を確認します。 *問題のストレージアレイがHiCommandサーバで設定されているかどうかを確認してください *パフォーマンスのポーリング間隔を60秒の倍数に設定します。
エラー： *ストレージナビゲータCLIでエラーが発生しました * auperformコマンドの実行中にエラーが発生しました *外部コマンド実行中にエラーが発生しました	* Data Infrastructure Insights Acquisition UnitにStorage Navigator Modular CLIがインストールされていることを確認*データコレクタ設定でStorage Navigator Modular CLIの場所が正しいことを確認*データコレクタ設定でWMS/SMS/SMSアレイのIPが正しいことを確認* Storage Navigator Modular CLIバージョンがデータコレクタに設定されているストレージアレイのマイクロコードバージョンと互換性があることを確認* Data Infrastructure Insights Acquisition Unitであることを実行していることを確認していることを確認していることを確認するコマンドを実行します。
エラー：設定エラー：ストレージアレイがインベントリから報告されません	HiCommand サーバで該当するストレージアレイが設定されているかどうかを確認します
エラー： * Storage Navigator Modular 2 CLIに登録されているアレイがありません *アレイがStorage Navigator Modular 2 CLIに登録されていません *構成エラー：ストレージアレイがStorageNavigator Modular CLIに登録されていません	*コマンドプロンプトを開き、設定したパスにディレクトリを変更します *「SET=STONAVM_HOME=」コマンドを実行します。 *「auunitref」コマンドを実行します。 *コマンド出力にIPを持つアレイの詳細が含まれていることを確認します *出力にアレイの詳細が含まれていない場合は、ストレージナビゲータCLIにアレイを登録します。 -コマンドプロンプトを開き、設定したパスにディレクトリを変更します -「SET=STONAVM_HOME=」コマンドを実行します。 -コマンド「auunitaddauto-ip <ip>」を実行します。<ip>を正しいIPに置き換えます。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Hitachi Vantara NAS データコレクタの設定

Hitachi Vantara NAS データコレクタは、 HDS NAS クラスタの検出をサポートするインベントリおよび設定データコレクタです。Data Infrastructure Insightsは、NFS共有とCIFS共有、ファイルシステム（内部ボリューム）、スパン（ストレージプール）の検出をサポートします。

用語集

Data Infrastructure Insightsは、HNAS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。Data Infrastructure Insights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	**Data Infrastructure Insights**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
システムドライブ	バックエンド LUN
ファイルシステム	内部ボリューム

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。

要件

- 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。

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）	インベントリのポーリング間隔。デフォルトは30分です。

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。

在庫

問題	次の操作を実行します
「 Error connecting 」 with error messages 「 Error setting up shell channel ：」または「 Error opening shell channel 」というエラーメッセージが表示されます。	ネットワーク接続に問題があるか、 SSH の設定ミスが原因である可能性があります。代替 SSH クライアントとの接続を確認します
「 Command ： XXX has timed out 」というエラーメッセージが表示され、「 Timeout 」または「 Error Retrieving data 」というエラーが表示されます。	*別のSSHクライアントを使用してコマンドを実行してください *タイムアウトを増やします
" 接続エラー " または " 無効なログイン認証情報 " のエラーメッセージ " デバイスと通信できませんでした： "	* IPアドレスを確認します *ユーザー名とパスワードを確認してください *代替SSHクライアントとの接続を確認してください

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

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

Data Infrastructure Insights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。Data Infrastructure Insights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	**Data Infrastructure Insights**の用語
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）

ベンダー / モデルの用語	**Data Infrastructure Insights**の用語
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。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Infinidat InfiniBox データコレクタ

Infinidat InfiniBox（HTTP）データコレクタは、Infinidat InfiniBoxストレージシステムからインベントリ情報を収集するために使用します。

用語集

Data Infrastructure Insightsは、Infinidat InfiniBox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。Data Infrastructure Insights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	**Data Infrastructure Insights**の用語
ストレージプール	ストレージプール
ノード	コントローラ
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

要件

このデータコレクタを設定する際の要件は次のとおりです。

- InfiniBox 管理ノードの IP アドレスまたは FQDN
- 管理者のユーザ ID とパスワード
- ポート 443 - REST API を使用

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です。
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分です。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Huawei OceanStor データコレクタ

Data Infrastructure Insightsでは、Huawei OceanStor（REST / HTTPS）データコレクタを使用して、Huawei OceanStorおよびOceanStor Doradoストレージのインベントリとパフォーマンスを検出します。

用語集

Data Infrastructure Insightsは、Huawei OceanStorから次のインベントリ情報とパフォーマンス情報を取得します。Data Infrastructure Insights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	**Data Infrastructure Insights**の用語
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
iSCSI リンクターゲット	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するには、次の要件が必要です。

- デバイスの IP アドレス
- 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

詳細設定

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。
パフォーマンスのポーリング間隔（秒）。	デフォルトは300秒です。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

IBM 社

IBM Cleversafe データコレクタ

Data Infrastructure Insightsは、このデータコレクタを使用して、IBM Cleversafeストレージシステムのインベントリデータとパフォーマンスデータを検出します。

IBM Cleversafeは、管理ユニットに対して異なるRaw TBで測定されています。フォーマットされていないIBM Cleversafeの容量は40TBごとに1が充電されます "管理ユニット (MU)"。

用語集

Data Infrastructure Insightsは、IBM Cleversafe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。Data Infrastructure Insights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	**Data Infrastructure Insights**の用語
ストレージプール	ストレージプール
コンテナ	内部ボリューム

ベンダー / モデルの用語	**Data Infrastructure Insights**の用語
コンテナ	ファイル共有
NFS 共有	共有

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。

要件

- クラスタの外部データサービスの IP アドレス
- 管理者のユーザ名とパスワード
- ポート 9440

設定

フィールド	説明
Manager の IP 名またはホスト名	管理ノードの IP アドレスまたはホスト名
ユーザ名	スーパーユーザまたはシステム管理者のロールを持つユーザアカウントのユーザ名
パスワード	スーパーユーザまたはシステム管理者のロールを持つ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
インベントリのポーリング間隔（分）	インベントリのポーリング間隔。
HTTP 接続タイムアウト（秒）	HTTP タイムアウト（秒）。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

IBM CS データコレクタ

Data Infrastructure Insightsは、このデータコレクタを使用して、IBM CSストレージシステムのインベントリデータとパフォーマンスデータを検出します。

用語集

Data Infrastructure Insightsは、IBM CS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。Data Infrastructure Insights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	**Data Infrastructure Insights**の用語
ストレージプール	ストレージプール
コンテナ	内部ボリューム
コンテナ	ファイル共有
NFS 共有	共有

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。

要件

- クラスタの外部データサービスの IP アドレス
- 管理者のユーザ名とパスワード
- ポート 9440

設定

フィールド	説明
プリズム外部 IP アドレス	クラスタの外部データサービスの IP アドレス
ユーザ名	管理者アカウントのユーザ名
パスワード	管理者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	IBM CS アレイへの接続に使用する TCP ポート。デフォルトは 9440. です。
インベントリのポーリング間隔（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。
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秒です。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

IBM System Storage DS8000 シリーズデータコレクタ

IBM DS （ CLI ）データコレクタは、 DS6xxx および DS8xxx のデバイスのインベントリデータとパフォーマンスデータの収集をサポートします。

DS3xxx、DS4xxx、およびDS5xxxデバイスはでサポートされています"NetApp E シリーズのデータコレクタ"。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、Data Infrastructure Insightsサポートマトリックスを参照してください。

用語集

Data Infrastructure Insightsは、IBM DS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。Data Infrastructure Insights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	**Data Infrastructure Insights**の用語
ディスクドライブモジュール	ディスク
ストレージイメージ	ストレージ
エクステントプール	ストレージノード
固定ブロックボリューム	ボリューム
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

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、このデータ照合のすべてのケースを表しているわけではありません。

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。

- 各 DS アレイの IP アドレス
- 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Data Infrastructure Insights AUにインストール：ibm_dscli_
- アクセスの検証：ユーザ名とパスワードを使用して Run_dscli _ コマンドを実行します
- 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 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	DS CLI のユーザ名
パスワード	DS CLI のパスワード
_dscli 実行可能ファイルのパス	dscli_executable のフルパス

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（分）。デフォルトは40です。
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

フィールド	説明
パフォーマンスポーリング間隔（秒）	デフォルトは300です。
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

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。

在庫

問題	次の操作を実行します
CMUC00192E 、 CMUC00191E 、または CMUC00190E を含むエラーです	* 入力された資格情報と IP アドレスを確認してください。 * Web管理コンソール\https://<ip>:8452/DS8000/Consoleを使用して'アレイとの通信を試みます <ip>をデータコレクタが設定されたIPに置き換えます。
エラー： *プログラムを実行できません *コマンドの実行エラー	* Data Infrastructure Insights Acquisition UnitからCMD* CLIのホームディレクトリ/libでCLI.CFGファイルを開き、プロパティJAVA_INSTALLを確認し、環境に合わせて値を編集します。「**java-version**」と入力して、このマシンにインストールされている**Java**バージョンを表示します。 CLIコマンドで指定したIBMストレージデバイスのIPアドレスをpingします。* 上記のすべてが正常に動作した場合は、 CLI コマンドを手動で実行します

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

IBM PowerVM データコレクタの設定

IBM PowerVM （ SSH ）データコレクタは、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するために使用されます。

用語集

Data Infrastructure Insightsは、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から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	**Data Infrastructure Insights**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

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。

要件

このデータコレクタを設定して使用するには、次の要件を満たしている必要があります。

- ハードウェア管理コンソール（ HMC ）の IP アドレス
- SSH を使用してハードウェア管理コンソール（ HMC ）にアクセスするためのユーザ名とパスワード
- ポート要件は SSH-22 です
- すべての管理システムおよび論理パーティションセキュリティドメインに対する表示権限

  ユーザには、 HMC の設定に対する表示権限も必要であり、 HMC コンソールセキュリティグループの VPD 情報を収集できる必要があります。ユーザーは、論理パーティションセキュリティグループの Virtual IO Server コマンドへのアクセスも許可されている必要があります。オペレータのロールから開始し、すべてのロールを削除することを推奨します。HMC の読み取り専用ユーザには、 AIX ホストでプロキシされたコマンドを実行する権限はありません。

- IBM のベストプラクティスは、 2 台以上の HMI でデバイスを監視することです。これにより、原因 OnCommand Insight で重複したデバイスが報告される場合があるため、このデータコレクタの詳細設定の [デバイスを除外する] リストに冗長デバイスを追加することを強くお勧めします。

設定

フィールド	説明
ハードウェア管理コンソール（ HMC ）の IP 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	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20分です。
SSHポート	PowerVM への SSH に使用するポート
パスワード	ハードウェア管理コンソールのパスワード

フィールド	説明
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

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

IBM SAN Volume Controller データコレクタの設定

IBM SVC データコレクタは、 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、Data Infrastructure Insightsサポートマトリックスを参照してください。

用語集

Data Infrastructure Insightsは、IBM SVC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。Data Infrastructure Insights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	**Data Infrastructure Insights**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 とパス

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

- 各 SVC クラスタの IP アドレス
- ポート 22 を使用できます
- 読み取り専用のユーザ名とパスワード

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。
- クレデンシャルには、クラスタノードから構成ノードにパフォーマンスファイルをコピーするためだけに管理アクセスレベルが必要になります。
- 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_

  注：データ収集は SVC 管理ユーザインターフェイスを使用して有効にすることもできます。

設定

フィールド	説明
クラスタ IP アドレス	SVC ストレージの IP アドレスまたは完全修飾ドメイン名
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

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秒です。
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	ダンプされた統計情報ファイルをクリーンアップするには ' このチェックボックスをオンにします

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
エラー： " 構成ノードで実行されていないため、コマンドを開始できません。 "	このコマンドは構成ノードで実行する必要があります。

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
エラー： " 構成ノードで実行されていないため、コマンドを開始できません。 "	このコマンドは構成ノードで実行する必要があります。

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

IBM XIV / A9000 データコレクタの設定

IBM XIV および A9000 （ CLI ）データコレクタでは、 XIV コマンドラインインターフェイスを使用してインベントリデータを収集します。また、パフォーマンス収集は、ポート 7778 で SMI-S プロバイダを実行する XIV / A9000 アレイを SMI-S から呼び出して実行します。

用語集

ベンダー / モデルの用語	**Data Infrastructure Insights**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

要件

このデータコレクタを設定して使用するには、次の要件を満たしている必要があります。

- ポート要件： TCP ポート 7778
- 読み取り専用のユーザ名とパスワード
- XIV CLI が AU にインストールされている必要があります

パフォーマンス要件

パフォーマンス収集の要件は次のとおりです。

- SMI-S Agent 1.4 以降
- SMI-S 互換の CIMService がアレイ上で実行されています。 ほとんどの XIV アレイにはデフォルトで cimserver がインストールされています。
- cimserver にはユーザログインを指定する必要があります。 ログインには、アレイの構成とプロパティに対する完全な読み取りアクセス権が必要です。
- SMI-S ネームスペース。 デフォルトは root/IBM です。 これは cimserver で設定できます。
- ポート要件： HTTP の場合は 5988 、 HTTPS の場合は 5989 。
- SMI-S パフォーマンス収集用のアカウントの作成方法については、次のリンクを参照してください。 https://www.ibm.com/docs/en/products?topic=/com.ibm.tpc_V41.doc/fqz0_t_adding_cim_agent.html

設定

フィールド	説明
XIV 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

フィールド	説明
XIV CLI ディレクトリの完全パス	XIV CLI を含むフォルダの完全パス
SMI-S ホストの IP アドレス	SMI-S ホストの IP アドレス

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分です。
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。デフォルトのポートも表示されます。
SMI-S ポートを上書きします	空白の場合は、 [Connection Type] フィールドでデフォルトのポートを使用します。それ以外の場合は、使用する接続ポートを入力します
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秒です。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Lenovo データコレクタ

Data Infrastructure Insightsは、Lenovoデータコレクタを使用して、Lenovo HXストレージシステムのインベントリデータとパフォーマンスデータを検出します。

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。

要件

- プリズム外部 IP アドレス
- 管理者のユーザ名とパスワード
- TCP ポート要件： 9440

設定

フィールド	説明
プリズム外部 IP アドレス	クラスタの外部データサービスの IP アドレス
ユーザ名	管理者アカウントのユーザ名
パスワード	管理者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	アレイへの接続に使用する TCP ポート。デフォルトは 9440. です。
インベントリのポーリング間隔（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。
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秒です。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Microsoft 社

Azure NetApp Files データコレクタの設定

Data Infrastructure Insightsは、Azure NetApp Filesデータコレクタを使用して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の認証キー（ユーザパスワード）
- Data Infrastructure Insightsの検出用に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てAzureにアプリケーションを登録すると、Data Infrastructure 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取得されます。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

次の表に従って、データコレクタ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

フィールド	説明
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

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

トラブルシューティング

- ANF データコレクタで使用するクレデンシャルに、 ANF ボリュームを含む Azure サブスクリプションへのアクセス権がないことを確認してください。
- Reader へのアクセスによってパフォーマンス収集が失敗する場合は、リソースグループレベルで貢献者アクセスを許可してみてください。

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Microsoft Hyper-V データコレクタ

Microsoft Hyper-V データコレクタは、仮想サーバコンピューティング環境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。このデータコレクタは、スタンドアロンのHyper-Vホストを検出することも、クラスタ全体を検出して、スタンドアロンのホストまたはクラスタごとにコレクタを1つ作成することもできます。

用語集

Data Infrastructure Insightsは、Microsoft Hyper-V（WMI）から次のインベントリ情報を取得します。Data Infrastructure Insights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	**Data Infrastructure Insights**の用語
仮想ハードディスク	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

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。

要件

このデータコレクタを設定するには、次のものが必要です。

- 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。
- クラスタまたはスタンドアロンハイパーバイザーのIPアドレスまたはFQDN。フローティングクラスタのホスト名またはIPを使用する方法は、コレクタをクラスタ内の1つの特定のノードだけに指定する方法ではない可能性があります。
- クラスタ内のすべてのハイパーバイザーで機能する管理者レベルのユーザアカウント。
- WinRMを有効にし、すべてのハイパーバイザーでリスンする必要があります
- ポート要件： WMI 経由のポート 135 および Windows 2003 以前の場合は 1024~65535 、 Windows 2008 の場合は 49152~65535 の動的 TCP ポート。
- データコレクタが IP アドレスだけ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は、各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Data Infrastructure Insights用により多くのデータを使用できるようになります。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の次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"

Hyper-V データコレクタには Windows Acquisition Unit が必要です。

設定

フィールド	説明
クラスタIPアドレスまたはフローティングクラスタFQDN	クラスタのIPアドレスまたは完全修飾ドメイン名、またはスタンドアロンの非クラスタハイパーバイザー
ユーザ名	ハイパーバイザーの管理者のユーザ名です
パスワード	ハイパーバイザーのパスワードです
DNSドメインサフィックス	ハイパーバイザーのFQDNをレンダリングするために単純なホスト名と組み合わせたホスト名サフィックス

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）	デフォルトは20分です。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

NetApp Cloud Volumes ONTAP データコレクタ

このデータコレクタは、 Cloud Volumes ONTAP 構成からのインベントリ収集をサポートします。

設定

フィールド	説明
ネットアップ管理 IP アドレス	クラウドボリューム ONTAP の IP アドレス
ユーザ名	Cloud Volumes ONTAP のユーザ名
パスワード	上記のユーザのパスワード

高度な設定

フィールド	説明
接続タイプ	HTTPS を推奨。にはデフォルトのポートも表示されます。
通信ポートをオーバーライドします	デフォルト以外の場合に使用するポート。
インベントリポーリング間隔（分）	デフォルトは 60 分です。
インベントリの同時スレッド数	同時スレッド数。
HTTPS に TLS を強制します	HTTPS 経由で TLS を強制します
ネットグループを自動的に検索する	ネットグループを自動的に検索する
ネットグループの拡張	シェルまたはファイルを選択します
HTTP 読み取りタイムアウト秒数	デフォルトは 30 秒です
応答を UTF-8 として強制実行します	応答を UTF-8 として強制実行します
パフォーマンスポーリング間隔（分）	デフォルト値は 900 秒です。
パフォーマンス同時スレッド数	同時スレッド数。
高度なカウンタデータ収集	このチェックボックスをオンにすると、Data Infrastructure Insightsが以下のリストから高度な指標を収集します。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

NetApp Cloud Volume Services for AWS データコレクタ

このデータコレクタは、 NetApp Cloud Volume Services for AWS 構成からのインベントリ収集をサポートします。

設定

フィールド	説明
Cloud Volume リージョン	NetApp Cloud Volume Services for AWS のリージョン
API キー	Cloud Volume API キー
シークレットキー	Cloud Volume シークレットキー

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

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
次のようなエラーが表示されました。 'Failed to execute request：Connect to <AWS region endpoint >：8080 [<AWS region endpoint >/AWS region endpoint IP>] failed：connect timed out：GET https://<AWS Region Endpoint FQDN >：8080/v1/Storage/IPRanges HTTP/1.1'	"プロキシ"Data Infrastructure InsightsがAcquisition Unitとの通信に使用するは、Data Infrastructure InsightsとData Collector自体との間の通信は行いません。以下にいくつかの方法で試してみましょう。Acquisition UnitでFQDNを解決して、必要なポートに到達できることを確認してください。エラーメッセージに示されたエンドポイントにアクセスするためにプロキシが必要でないことを確認します。cURLを使用して、Acquisition Unitとエンドポイント間の通信をテストできます。このテストにプロキシを使用していない*ことを確認してください。例：root@acquisitionunit#curl -s -H accept: application/json -H "Content-type: application/json"-H api-key:<データコレクタの資格情報で使用されるAPIキー-H secret-key:<データコレクタの資格情報で使用されるシークレットキー>-X Get https://<AWS Regional Endpoint >: 808080/v1/Storage/IPRanges参照。"ネットアップの技術情報アーティクル"

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

NetApp ONTAP データ管理ソフトウェアのデータコレクタ

このデータコレクタは、 ONTAP アカウントからの読み取り専用の API 呼び出しを使用して、 ONTAP を実行しているストレージシステム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。このデータコレクタは、サポートを高速化するために、クラスタアプリケーションレジストリにレコードを作成します。

用語集

Data Infrastructure Insightsは、ONTAPデータコレクタ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。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	**Data Infrastructure Insights**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

ONTAP データ管理の用語

ONTAP データ管理ストレージ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。

ストレージ

- model –このクラスタ内で一意のディスクリートノードのモデル名をカンマで区切って指定します。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に表示されるベンダー名と同じです。
- Serial Number –アレイのシリアル番号。ONTAP データ管理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、このシリアル番号は個々の「ストレージノード」のシリアル番号よりも有用性が低い場合があります。
- IP –一般に、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 容量–システム内のすべての物理ディスクの合計 2 進数で、役割に関係なく加算されます。
- レイテンシ–読み取りと書き込みの両方について、ワークロードが直面しているホストの状況が表示されます。理想的なのは、Data Infrastructure Insightsがこの価値を直接提供していることですが、そうではないことがよくあります。Data Infrastructure Insights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約されたもの。管理–デバイスの管理インターフェイスのハイパーリンクが含まれている可能性があります。インベントリレポートの一部として、Data Infrastructure Insights 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。

ストレージプール

- storage –このプールのストレージアレイの場所。必須。
- Type –可能性のリストから説明的な値を入力します。最も一般的な構成は、「集約」または「 RAID グループ」です。

- ノード：プールが特定のストレージノードに属するようなストレージアレイのアーキテクチャの場合、その名前は、そのストレージアレイ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–値はあり / いいえ–この SATA / SAS ベースのプールでは、 SSD をキャッシュ高速化に使用していますか？
- 冗長性– RAID レベルまたは保護方式。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–使用済みの論理容量、使用可能な容量、および合計論理容量の値と、これらの要素で使用されている割合の値が表示されます。
- オーバーコミット容量–効率化テクノロジを使用して、ストレージプールの論理容量よりも大きいボリュームまたは内部ボリュームの容量の合計を割り当てている場合、この割合は 0% よりも大きくなります。
- スナップショット–スナップショット専用のセグメント領域にストレージプールアーキテクチャが容量の一部を割り当てている場合に使用されるスナップショット容量と合計容量。MetroCluster 構成の ONTAP はこのような構成を示しますが、それ以外の ONTAP 構成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追加しているディスクのビジー率の最大値を示した割合。ディスク利用率にアレイのパフォーマンスとの間に大きな相関関係があるとは限りません。ホストベースのワークロードがない場合は、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、内部ボリュームやボリュームのワークロードとしては表示されずにディスク使用率が向上する場合があります。
- IOPS –このストレージプールに容量の要因となっているすべてのディスクの合計 IOPS 。
  Throughput –このストレージプールの容量の要因となっているすべてのディスクの合計スループット。

ストレージノード

- Storage –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–通常、一方のノードだけにフェイルオーバーするプラットフォームでは、この画面が表示されます。
- State –ノードの健常性。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。
- メモリ–ベース 2 のメモリがあればそれ。
- 使用率– ONTAP では、これは独自のアルゴリズムのコントローラ応力インデックスです。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。継続的に測定される値が 50% を超えている場合は、サイジングが不十分であることを示します。コントローラや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足りない可能性があります。
- IOPS –ノードオブジェクトの ONTAP ZAPI コールから直接取得されます。
- レイテンシ–ノードオブジェクトの ONTAP ZAPI コールから直接取得されます。
- スループット–ノードオブジェクトの ONTAP ZAPI コールから直接取得されます。
- プロセッサ– CPU 数。

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。

- 読み取り専用の API 呼び出し用に設定された管理者アカウントへのアクセス権が必要です。
- アカウントの詳細には、ユーザ名とパスワードが含まれます。
- ポートの要件： 80 または 443
- アカウントの権限：
  - デフォルトの SVM の ONTAPI アプリケーションに対する読み取り専用のロール名
  - オプションの書き込み権限が追加で必要になる場合があります。以下の「アクセス権に関する注意」を参照してください。
- ONTAP ライセンスの要件：
  - ファイバチャネル検出に必要な FCP ライセンスおよびマッピング / マスクされたボリューム

ONTAPスイッチメトリックを収集するための権限要件

Data Infrastructure Insightsでは、コレクタ詳細設定設定のオプションとして、ONTAPクラスタスイッチのデータを収集できます。Data Infrastructure Insightsコレクタでこれを有効にするだけでなく、"スイッチ情報"権限スイッチデータをData Infrastructure Insightsに送信できるように、ONTAPシステム自体を構成して提供し、正しい設定を確認する必要があります。

設定

フィールド	説明
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	説明
接続タイプ	HTTP （デフォルトポート 80 ）または HTTPS （デフォルトポート 443 ）を選択します。デフォルトは HTTPS です
通信ポートをオーバーライドします	デフォルト以外のポートを使用する場合は、別のポートを指定します
インベントリポーリング間隔（分）	デフォルトは 60 分です。
TLS では HTTPS を使用します	HTTPS を使用する場合にのみ TLS をプロトコルとして許可します
ネットグループを自動的に検索する	エクスポートポリシールールのネットグループの自動検索を有効にします
ネットグループの拡張	ネットグループ拡張戦略： *FILE _* または *_SHELL _* を選択します。デフォルトは *_shell* です。

フィールド	説明
HTTP 読み取りタイムアウト秒数	デフォルトは30です
応答を UTF-8 として強制実行します	データコレクタコードに、 CLI からの応答を UTF-8 であると解釈させます
パフォーマンスポーリング間隔（秒）	デフォルト値は 900 秒です。
高度なカウンタデータ収集	ONTAP の統合を有効にします。ONTAP 詳細カウンタデータをポーリングに含める場合に選択します。リストから目的のカウンタを選択します。
クラスタスイッチ指標	Data Infrastructure Insightsでクラスタスイッチのデータを収集Data Infrastructure Insights側でこれを有効にするだけでなく、"スイッチ情報"権限スイッチのデータがData Infrastructure Insightsに送信されるように、ONTAPシステムで提供するように設定し、正しい設定が行われていることを確認する必要があります。下記の「権限に関する注意事項」を参照してください。

ONTAPの電力メトリック

いくつかのONTAPモデルは、監視やアラートに使用できるデータインフラインサイトの電力指標を提供します。以下のサポートされているモデルとサポートされていないモデルのリストは包括的ではありませんが、いくつかのガイダンスを提供する必要があります。一般的に、モデルがリストのものと同じファミリーに属している場合、サポートは同じである必要があります。

サポートされるモデル：

A200
A220
A250
A300 の比較
A320
A400
A700
A700s
A800
A900
C190
FAS2240-4
FAS2552
FAS2650
FAS2720
FAS2750
FAS8200
FAS8300
FAS8700
FAS9000

サポートされていないモデル：

FAS2620
FAS3250

FAS3270
FAS500f
FAS6280
FAS / AFF 8020
FAS / AFF 8040
FAS / AFF 8060
FAS / AFF 8080

アクセス権に関する注意事項

Data Infrastructure InsightsのONTAPダッシュボードの多くは、高度なONTAPカウンタに依存しているため、データコレクタの高度な設定セクションで*高度なカウンタデータ収集*を有効にする必要があります。

また、 ONTAP API への書き込み権限が有効になっていることも確認する必要があります。通常は、必要な権限を持つアカウントがクラスタレベルで必要になります。

クラスタレベルでData Infrastructure Insights用のローカルアカウントを作成するには、クラスタ管理者のユーザ名とパスワードを使用してONTAPにログインし、ONTAPサーバで次のコマンドを実行します。

1. 作業を開始する前に、 _Administrator_account および _diagnostic-level コマンド _ を使用して ONTAP にサインインする必要があります。
2. 次のコマンドを使用して、読み取り専用ロールを作成します。

```
security login role create -role ci_readonly -cmddirname DEFAULT -access
readonly
security login role create -role ci_readonly -cmddirname security
-access readonly
security login role create -role ci_readonly -access all -cmddirname
{cluster application-record create}
```

3. 次のコマンドを使用して、読み取り専用ユーザを作成します。create コマンドを実行すると、このユーザのパスワードを入力するように求められます。

```
security login create -username ci_user -application ontapi
-authentication-method password -role ci_readonly
```

AD / LDAP アカウントを使用する場合は、コマンドをに設定します

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application ontapi -authentication-method domain -role ci_readonly
```

クラスタスイッチのデータを収集する場合は、次の作業を行います。

```
 security login rest-role create -role ci_readonly -api
/api/network/ethernet -access readonly
```
作成されるロールとユーザログインは次のようになります。実際の出力は以下のように異なる場合があります

```
Role Command/ Access
Vserver Name Directory Query Level
---------- ------------ --------- ------------------ --------
cluster1 ci_readonly DEFAULT read only
cluster1 ci_readonly security readonly
```

```
cluster1::security login> show
Vserver: cluster1
Authentication Acct
UserName    Application   Method      Role Name      Locked
---------   -------      ----------- -------------- --------
ci_user     ontapi      password    ci_readonly   no
```

ONTAPアクセス制御が正しく設定されていないと、Data Infrastructure InsightsのREST呼び出しが失敗し、デバイスのデータにギャップが生じる可能性があります。たとえば、Data Infrastructure Insightsコレクタでこの機能を有効にしていて、ONTAPに対する権限が設定されていない場合、データの取得は失敗します。また、ロールが以前にONTAPで定義されていて、残りのAPI機能を追加する場合は、_http_がロールに追加されていることを確認してください。

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。

在庫

問題	次の操作を実行します
401 HTTP 応答または 13003 ZAPI エラーコードを受信し、 ZAPI から「 Insufficient privileges 」または「 Not authorized for this command 」が返される	ユーザ名とパスワード、およびユーザの権限と権限を確認してください。
クラスタバージョンが 8.1 より前である必要があります	クラスタでサポートされる最小バージョンは 8.1 です。サポートされる最小バージョンにアップグレードしてください。
ZAPI から「 cluster role is not cluster_mgmt LIF 」が返される	AU はクラスタ管理 IP と通信する必要があります。IP を確認し、必要に応じて別の IP に変更してください

問題	次の操作を実行します
エラー：「 7-Mode のストレージシステムはサポートされていません」	この問題は、このデータコレクタを使用して 7-Mode ファイラーを検出した場合に発生することがあります。IP を変更して、代わりに cdot クラスタを指すようにします。
ZAPI コマンドの再試行後に失敗する	AU でクラスタとの通信に問題があります。ネットワーク、ポート番号、および IP アドレスを確認してください。また、 AU マシンのコマンドラインからもコマンドを実行しようとします。
AU が HTTP 経由で ZAPI に接続できませんでした	ZAPI ポートでプレーンテキストが受け入れるかどうかを確認します。AU が SSL ソケットにプレーンテキストを送信しようとすると、通信に失敗します。
SSLException で通信が失敗します	AU が Filer 上のプレーンテキストポートに SSL を送信しようとしています。ZAPI ポートで SSL を受け入れるか、別のポートを使用するかを確認します。
追加の接続エラー： ZAPI応答のエラーコード13001：「database is not open」 ZAPIエラーコードが60で、応答に「API did not finish on time」が含まれている ZAPIの応答に「initialize_session () returned NULL environment」が含まれる ZAPIエラーコードが14007で、応答に「Node is not healthy」が含まれている	ネットワーク、ポート番号、および IP アドレスを確認してください。また、 AU マシンのコマンドラインからもコマンドを実行しようとします。

パフォーマンス

問題	次の操作を実行します
「 ZAPI からパフォーマンスを収集できませんでした」というエラーが表示される	これは通常、 perf stat が実行されていないことが原因です。各ノードで次のコマンドを実行します。 >_system node systemshell -node *-command“spmctl -h cmd–stop；spmctl -h cmd–exec”_

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

NetApp ONTAP RESTデータコレクタ

このデータコレクタは、REST API呼び出しを使用して、ONTAP 9.14.1以降を実行するストレージシステムからインベントリ、EMSログ、パフォーマンスデータを取得します。以前のリリースのONTAPシステムでは、ZAPIベースの「NetApp ONTAPデータ管理ソフトウェア」コレクタタイプを使用します。

ONTAP RESTコレクタは、以前のONTAPIベースのコレクタの代わりに使用できます。そのため、収集または報告される指標が異なる場合があります。ONTAPIとRESTの違いの詳細については、を参照してください。 "ONTAP 9.14.1 ONTAPI-REST間のマッピング" ドキュメント

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。

- 必要なレベルのアクセス権を持つユーザアカウントへのアクセス権が必要です。新しいRESTユーザ/ロールを作成する場合はAdmin権限が必要です。
  - 機能的には、Data Infrastructure Insightsは主に読み取り要求を行いますが、Data Infrastructure InsightsをONTAPアレイに登録するには書き込み権限が必要です。下記の「Permissions_immediately」を参照してください。
- ONTAPバージョン9.14.1以降。
- ポートの要件：443

アクセス権に関する注意事項

データインフラストラクチャインサイトのONTAPダッシュボードの多くは、高度なONTAPカウンタに依存しているため、データコレクタの[高度な設定]セクションで[高度なカウンタデータ収集を有効にする]*を有効にしておく必要があります。

クラスタレベルでData Infrastructure Insights用のローカルアカウントを作成するには、クラスタ管理者のユーザ名とパスワードを使用してONTAPにログインし、ONTAPサーバで次のコマンドを実行します。

1. 作業を開始する前に、 _Administrator_account および _diagnostic-level コマンド _ を使用して ONTAP にサインインする必要があります。
2. タイプが_admin_のSVMの名前を取得します。この名前は以降のコマンドで使用します。

```
 vserver show -type admin
```

. 次のコマンドを使用してロールを作成します。

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
```

3. 次のコマンドを使用して、読み取り専用ユーザを作成します。create コマンドを実行すると、このユーザのパスワードを入力するように求められます。

```
security login create -username ci_user -application http
-authentication-method password -role ci_readonly
```

AD / LDAP アカウントを使用する場合は、コマンドをに設定します

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
```

作成されるロールとユーザログインは次のようになります。実際の出力は以下のように異なる場合があります

```
security login rest-role show -vserver <vserver name> -role restRole

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   --------------------    ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                 Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

データ移行

以前のONTAP（ONTAPI）データコレクタから新しいONTAP RESTコレクタに移行するには、次の手順を実行します。

1. RESTコレクタを追加します。以前のコレクタ用に設定されたユーザとは別のユーザの情報を入力することを推奨します。たとえば、上記の「権限」セクションに記載されているユーザを使用します。
2. 前のコレクタを一時停止して、データの収集を継続しないようにします。
3. 新しいRESTコレクタで少なくとも30分間データを取得します。この期間中に「正常」に表示されないデータはすべて無視してください。
4. 残りの期間が経過すると、RESTコレクタがデータを取得し続けるため、データが安定します。

必要に応じて、この同じプロセスを使用して前のコレクタに戻ることができます。

設定

フィールド	説明
ONTAP管理IPアドレス	NetAppクラスタのIPアドレスまたは完全修飾ドメイン名。クラスタ管理IP / FQDNを指定する必要があります。
ONTAP RESTユーザ名	ネットアップクラスタのユーザ名
ONTAP REST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	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。
パフォーマンスポーリング間隔（秒）	デフォルトは60秒です。
高度なカウンタデータ収集	ONTAP 詳細カウンタデータをポーリングに含める場合に選択します。デフォルトは有効です。
EMSイベント収集を有効にする	ONTAP EMSログイベントデータを含める場合に選択します。デフォルトは有効です。
EMSポーリング間隔（秒）	デフォルトは60秒です。

用語集

Data Infrastructure Insightsは、ONTAPデータコレクタからインベントリ、ログ、パフォーマンスデータを取得します。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	**Data Infrastructure Insights**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
Storage Virtual Machine / SVM	Storage Virtual Machine の略

ONTAP データ管理の用語

ONTAP データ管理ストレージ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。

ストレージ

- model –このクラスタ内で一意のディスクリートノードのモデル名をカンマで区切って指定します。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に表示されるベンダー名と同じです。
- シリアル番号–アレイUUID
- IP –一般に、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 容量–システム内のすべての物理ディスクの合計 2 進数で、役割に関係なく加算されます。
- レイテンシ–読み取りと書き込みの両方について、ワークロードが直面しているホストの状況が表示されます。理想的なのは、Data Infrastructure Insightsがこの価値を直接提供していることですが、そうではないことがよくあります。Data Infrastructure Insights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約されたもの。管理–デバイスの管理インターフェイスのハイパーリンクが含まれている可能性があります。インベントリレポートの一部として、Data Infrastructure Insights 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。

ストレージプール

- storage –このプールのストレージアレイの場所。必須。
- Type –可能性のリストから説明的な値を入力します。最も一般的な構成は、「集約」または「 RAID グループ」です。
- ノード：プールが特定のストレージノードに属するようなストレージアレイのアーキテクチャの場合、その名前は、そのストレージアレイ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–値はあり / いいえ–この SATA / SAS ベースのプールでは、 SSD をキャッシュ高速化に使用していますか？
- 冗長性– RAID レベルまたは保護方式。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–使用済みの論理容量、使用可能な容量、および合計論理容量の値と、これらの要素で使用されている割合の値が表示されます。
- オーバーコミット容量–効率化テクノロジを使用して、ストレージプールの論理容量よりも大きいボリュームまたは内部ボリュームの容量の合計を割り当てている場合、この割合は 0% よりも大きくなります。
- スナップショット–スナップショット専用のセグメント領域にストレージプールアーキテクチャが容量の一部を割り当てている場合に使用されるスナップショット容量と合計容量。MetroCluster 構成の ONTAP はこのような構成を示しますが、それ以外の ONTAP 構成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追加しているディスクのビジー率の最大値を示した割合。ディスク利用率にアレイのパフォーマンスとの間に大きな相関関係があるとは限りません。ホストベースのワークロードがない場合は、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、内部ボリュームやボリュームのワークロードとしては表示されずにディスク使用率が向上する場合があります。
- IOPS –このストレージプールに容量の要因となっているすべてのディスクの合計 IOPS 。
  Throughput –このストレージプールの容量の要因となっているすべてのディスクの合計スループット。

ストレージノード

- Storage –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–通常、一方のノードだけにフェイルオーバーするプラットフォームでは、この画面が表示されます。
- State –ノードの健常性。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。
- メモリ–ベース 2 のメモリがあればそれ。
- 使用率– ONTAP では、これは独自のアルゴリズムのコントローラ応力インデックスです。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。継続的に測定される値が 50% を超えている場合は、サイジングが不十分であることを示します。コントローラや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足り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 REST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 REST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 REST呼び出しから直接導出されます。
- プロセッサ– CPU 数。

ONTAPの電力メトリック

いくつかのONTAPモデルは、監視やアラートに使用できるデータインフラインサイトの電力指標を提供します。以下のサポートされているモデルとサポートされていないモデルのリストは包括的ではありませんが、いくつかのガイダンスを提供する必要があります。一般的に、モデルがリストのものと同じファミリーに属している場合、サポートは同じである必要があります。

サポートされるモデル：

A200
A220
A250
A300 の比較
A320
A400
A700
A700s
A800
A900
C190
FAS2240-4
FAS2552
FAS2650
FAS2720
FAS2750
FAS8200
FAS8300

FAS8700
FAS9000

サポートされていないモデル：

FAS2620
FAS3250
FAS3270
FAS500f
FAS6280
FAS / AFF 8020
FAS / AFF 8040
FAS / AFF 8060
FAS / AFF 8080

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
ONTAP RESTデータコレクタを作成しようとすると、次のようなエラーが表示されます。 設定：10.193.70.14：10.193.70.14のONTAP REST APIを使用できません。10.193.70.14で/api/clusterを取得できませんでした：400 Bad Request	これは、古いONTAPアレイ（ONTAP 9.6など）にREST API機能がないことが原因である可能性があります。ONTAP 9.14.1は、ONTAP RESTコレクタでサポートされるONTAPの最小バージョンです。REST ONTAPより前のリリースでは、「400 Bad Request」応答が想定されます。 RESTをサポートしているが9.14.1以降ではないONTAPバージョンでは、次のようなsimillarメッセージが表示されることがあります。 Configuration：10.193.98.84：ONTAP REST API（10.193.98.84）は使用できません。10.193.98.84：ONTAP REST API（10.193.98.84）が使用可能です。cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7以上のバージョンではありません。

問題	次の操作を実行します
ONTAP ONTAPIコレクタにデータが表示される場合、空または「0」の指標が表示されます。	ONTAP RESTでは、ONTAPシステムの内部でのみ使用される指標はレポートされません。たとえば、システムアグリゲートはONTAP RESTでは収集されず、タイプが「data」のSVMのみが収集されます。 0または空のデータが報告される可能性のあるONTAP REST指標のその他の例： InternalVolumes：RESTでvol0が報告されなくなりました。 Aggregates：RESTでaggr0が報告されなくなりました。 ストレージ：ほとんどの指標は内部ボリュームの指標を集計したもので、上記の影響を受けます。 Storage Virtual Machine：RESTでは、「data」以外のタイプのSVM（「cluster」、「mgmt」、「node」など）は報告されなくなりました。 また、デフォルトのパフォーマンスポーリング期間が15分から5分に変更されたため、データを含むグラフの表示が変更されることもあります。 ポーリングの頻度が高いほど、プロットするデータポイントが増えます。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

NetApp Data ONTAP 7-Mode データコレクタ

Data ONTAP 7-Mode を使用するストレージシステムでは、 7-Mode のデータコレクタを使用します。このコレクタでは、 CLI を使用して容量とパフォーマンスのデータを取得します。

用語集

Data Infrastructure Insightsでは、NetApp 7-Mode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。

このデータコレクタはです "非推奨"。

ベンダー / モデルの用語	**Data Infrastructure Insights**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

ベンダー / モデルの用語	**Data Infrastructure Insights**の用語
LUN	ボリューム
ボリューム	内部ボリューム

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。

要件

このデータコレクタを設定して使用するには、次の情報が必要です。

- 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
- 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	説明
ストレージシステムのアドレス	ネットアップストレージシステムの IP アドレスまたは完全修飾ドメイン名
ユーザ名	ネットアップストレージシステムのユーザ名
パスワード	ネットアップストレージシステムのパスワード
クラスタの HA パートナーのアドレス	HA パートナーの IP アドレスまたは完全修飾ドメイン名
クラスタの HA パートナーのユーザ名	HA パートナーのユーザ名
クラスタ内の HA パートナーファイラーのパスワード	HAパートナーのパスワード

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20分です。
接続タイプ	HTTPS または HTTP では、デフォルトのポートも表示されます
接続ポートを上書きします	空白の場合は、 [Connection Type] フィールドでデフォルトのポートを使用します。それ以外の場合は、使用する接続ポートを入力します
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秒です。

ストレージシステム接続

このデータコレクタにデフォルトの管理ユーザを使用する代わりに、 NetApp 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、このデータコレクタ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ができます。

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NetAppストレージAPIコマンドをData Infrastructure Insightsで実行できるようにする場合に使用します。

    このコマンドは、 ZAPI を使用する場合は必須です。

  - 「login-http-admin」：Data Infrastructure InsightsがHTTP経由でNetAppストレージに接続できるようにする場合に使用します。このコマンドは、 ZAPI を使用する場合は必須です。
  - "security-api-vfiler"：Data Infrastructure InsightsがNetAppストレージAPIコマンドを実行してvFilerユニット情報を取得できるようにする場合に使用します。
  - 「 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 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 」：「 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 、 _
- login-http-admin 、 api- * 、 security-api-vFile 、 cli-

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。

在庫

問題	次の操作を実行します
401 HTTP 応答または 13003 ZAPI エラーコードを受信し、 ZAPI から「 Insufficient privileges 」または「 Not authorized for this command 」が返される	ユーザ名とパスワード、およびユーザの権限と権限を確認してください。
「コマンドの実行に失敗しました」エラー	ユーザがデバイスに対する次の権限を持っているかどうかを確認します。•api-*•cli-date•cli-df•cli-ifconfig•cli-lun•cli-operations•cli-rdfile•cli-snap•login-http-admin•security-api-vfiler ONTAPバージョンがData Infrastructure Insightsでサポートされているかどうかを確認し、使用されたクレデンシャルがデバイスのクレデンシャルと一致するかどうかを確認します。
クラスタバージョンが 8.1 より前である必要があります	クラスタでサポートされる最小バージョンは 8.1 です。サポートされる最小バージョンにアップグレードしてください。
ZAPI から「 cluster role is not cluster_mgmt LIF 」が返される	AU はクラスタ管理 IP と通信する必要があります。IP を確認し、必要に応じて別の IP に変更してください
エラー：「 7-Mode のストレージシステムはサポートされていません」	この問題は、このデータコレクタを使用して 7-Mode ファイラーを検出した場合に発生することがあります。代わりに、 IP を cdot ファイラーを指すように変更してください。
ZAPI コマンドの再試行後に失敗する	AU でクラスタとの通信に問題があります。ネットワーク、ポート番号、および IP アドレスを確認してください。また、 AU マシンのコマンドラインからもコマンドを実行しようとします。
AU が ZAPI に接続できませんでした	IP/ ポートの接続を確認し、 ZAPI の設定をアサートします。

問題	次の操作を実行します
AU が HTTP 経由で ZAPI に接続できませんでした	ZAPI ポートでプレーンテキストが受け入れるかどうかを確認します。AU が SSL ソケットにプレーンテキストを送信しようとすると、通信に失敗します。
SSLException で通信が失敗します	AU が Filer 上のプレーンテキストポートに SSL を送信しようとしています。ZAPI ポートで SSL を受け入れるか、別のポートを使用するかを確認します。
追加の接続エラー： ZAPI応答のエラーコード13001：「database is not open」 ZAPIエラーコードが60で、応答に「API did not finish on time」が含まれている ZAPIの応答に「initialize_session () returned NULL environment」が含まれる ZAPIエラーコードが14007で、応答に「Node is not healthy」が含まれている	ネットワーク、ポート番号、および IP アドレスを確認してください。また、 AU マシンのコマンドラインからもコマンドを実行しようとします。
ZAPI でソケットタイムアウトエラーが発生しました	ストレージシステムの接続を確認するか、タイムアウトを延長してください。
「 7-Mode データソースでは C モードクラスタはサポートされません」エラーが表示されます	IP をチェックし、 IP を 7-Mode クラスタに変更してください。
「 Failed to connect to vFiler 」というエラーが表示されます	取得するユーザ機能に少なくとも次のものが含まれていることを確認します。 API -* security-api-vfilerの略 login-http-adminをクリックします Filerで実行されているONTAPIバージョン1.7以上を確認します。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

NetApp Eシリーズの従来型**SANtricity API**データコレクタ

NetApp Eシリーズの従来型SANtricity APIデータコレクタは、インベントリとパフォーマンスのデータを収集します。コレクタは、同じ設定を使用して同じデータを報告するファームウェア 7.x 以上をサポートしています。

用語集

Cloud Insight では、 NetApp E シリーズ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	**Data Infrastructure Insights**の用語
ディスク	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

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。

E シリーズの用語（ランディングページ）

NetApp E シリーズ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。

ストレージ

- 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に表示されるベンダー名と同じです
- Serial Number –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、このシリアル番号は個々の「ストレージノード」のシリアル番号よりも便利でない場合があります
- IP –一般に、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 容量–システム内のすべての物理ディスクの合計 2 進数で、役割に関係なく加算されます
- レイテンシ–読み取りと書き込みの両方について、ワークロードが直面しているホストの状況が表示されます。理想的なのは、Data Infrastructure Insightsがこの価値を直接提供していることですが、そうではないことがよくあります。Data Infrastructure Insightsでは、この機能を提供するアレイの代わりに、通常、個 々 の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–アレイのホスト側のスループットの合計Data Infrastructure Insightsはアレイから直接調達するのが理想的で、利用できない場合はボリュームのスループットを合計してこの値を算出
- 管理–デバイスの管理インターフェイスのハイパーリンクが含まれている可能性があります。インベントリレポートの一部として、Data Infrastructure Insights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。

ストレージプール

- storage –このプールのストレージアレイの場所。必須
- Type –可能性のリストから説明的な値を入力します。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：プールが特定のストレージノードに属するようなストレージアレイのアーキテクチャの場合、その名前は、そのストレージアレイ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 を使用します。値はありますか、いいえです
- 冗長性– RAID レベルまたは保護方式。E シリーズでは、 DDP プールの場合は「 RAID 7 」と報告されます
- 容量–使用済みの論理容量、使用可能な容量、および合計論理容量の値と、これらの要素で使用されている割合の値が表示されます。これらの値には、 E シリーズの「予約済み」容量が含まれ、 E シリーズのユーザインターフェイスで表示される値よりも数値と割合が高くなります
- オーバーコミット容量–効率化テクノロジを使用して、ストレージプールの論理容量を超える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ている場合、この割合の値は 0% を超えます。
- スナップショット–スナップショット専用のセグメント領域にストレージプールアーキテクチャが容量の一部を割り当てている場合に使用されるスナップショット容量と合計容量
- 利用率–このストレージプールに容量を追加しているディスクのビジー率の最大値を示した割合。ディスク利用率にアレイのパフォーマンスとの間に大きな相関関係があるとは限りません。ホストベースのワークロードがない場合は、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、ボリュームワークロードとして表示されずにディスク使用率が向上する場合があります。
- IOPS –このストレージプールに容量の要因となっているすべてのディスクの合計 IOPS 。特定のプラットフォームのディスク IOPS がない場合、この値は、このストレージプールにあるすべてのボリュームのボリューム IOPS の合計から取得されます
- Throughput –このストレージプールの容量の要因となっているすべてのディスクの合計スループット。特定のプラットフォームでディスクスループットを使用できない場合は、このストレージプールに配置されているすべてのボリュームの合計ボリューム数がこの値に基づいて算出されます

ストレージノード

- Storage –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–通常、一方のノードだけにフェイルオーバーするプラットフォームでは、この画面が表示されます
- State –ノードの健常性。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
- メモリ–ベース 2 のメモリがあればそれ
- 利用率–通常は CPU 利用率番号、または NetApp ONTAP の場合はコントローラに負荷がかかる指標。現在、 NetApp E シリーズでは利用率を利用できません
- IOPS –このコントローラのホスト主導の IOPS を表す数値。理想的なソースはアレイから直接取得され、使用できない場合は、このノードにのみ所属するボリュームのすべての IOPS を合計して算出されます。
- Latency –このコントローラのホストのレイテンシまたは応答時間を表す数値。使用できない場合はアレイから直接ソースを取得し、このノードにのみ所属するボリュームから IOPS の重み付き計算を実行することを推奨します。
- Throughput –このコントローラのホストで実行されるスループットを示す数値です。理想的なソースはアレイから直接取得され、使用できない場合は、このノードにのみ所属するボリュームのすべてのスループットを合計して算出されます。

- プロセッサ– CPU 数

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	説明
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	説明
インベントリポーリング間隔（分）	デフォルトは30分です
パフォーマンスポーリング間隔（最大 3600 秒）	デフォルトは300秒です

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

NetApp Eシリーズ**REST**データコレクタ

NetApp EシリーズRESTデータコレクタは、インベントリとパフォーマンスのデータを収集します。コレクタは、同じ設定を使用して同じデータを報告するファームウェア 7.x 以上をサポートしています。RESTコレクタは、ストレージプールの暗号化ステータスと関連するディスクおよびボリュームの暗号化ステータスを監視し、ストレージノードのCPU利用率をパフォーマンスカウンタとして提供します。これは、従来のSANtricity Eシリーズコレクタでは提供されていない機能です。

用語集

Insightでは、RESTを使用して、NetApp Eシリーズ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	**Data Infrastructure Insights**の用語
ディスク	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

ベンダー / モデルの用語	**Data Infrastructure Insights**の用語
ボリューム	ボリューム

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。

要件

- アレイの各コントローラの IP アドレス
- このコレクタは、*ネイティブのREST API機能*を備えたEシリーズモデルアレイのみをサポートします。Eシリーズ部門には、古いEシリーズアレイ向けにオフアレイでインストール可能なREST APIディストリビューションが付属しています。このコレクタではこのシナリオはサポートされません。古いアレイを使用している場合は、引き続きData Infrastructure Insightsの"EシリーズSANtricity API"コレクタを使用する必要があります。
- [E-Series Controller IP Addresses]フィールドでは、2つのIP /ホスト名をカンマで区切って指定できます。1つ目のIP /ホスト名にアクセスできない場合、コレクタは2つ目のIP /ホスト名をインテリジェントに試行します。
- HTTPSポート：デフォルトは8443です。

設定

フィールド	説明
EシリーズコントローラのIPアドレス	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をカンマで区切って指定

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30分です
パフォーマンスポーリング間隔（最大 3600 秒）	デフォルトは300秒です

E シリーズの用語（ランディングページ）

NetApp E シリーズ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。

ストレージ

- 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に表示されるベンダー名と同じです
- Serial Number –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、このシリアル番号は個々の「ストレージノード」のシリアル番号よりも便利でない場合があります
- IP –一般に、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 容量–システム内のすべての物理ディスクの合計 2 進数で、役割に関係なく加算されます
- レイテンシ–読み取りと書き込みの両方について、ワークロードが直面しているホストの状況が表示されます。理想的なのは、Data Infrastructure Insightsがこの価値を直接提供していることですが、そうではないことがよくあります。Data Infrastructure Insightsでは、この機能を提供するアレイの代わりに、通常、個 々 の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–アレイのホスト側のスループットの合計Data Infrastructure Insightsはアレイから直接調達するのが理想的で、利用できない場合はボリュームのスループットを合計してこの値を算出
- 管理–デバイスの管理インターフェイスのハイパーリンクが含まれている可能性があります。インベントリレポートの一部として、Data Infrastructure Insights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。

ストレージプール

- storage –このプールのストレージアレイの場所。必須
- Type –可能性のリストから説明的な値を入力します。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：プールが特定のストレージノードに属するようなストレージアレイのアーキテクチャの場合、その名前は、そのストレージアレイ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 を使用します。値はありますか、いいえです
- 冗長性– RAID レベルまたは保護方式。E シリーズでは、 DDP プールの場合は「 RAID 7 」と報告されます
- 容量–使用済みの論理容量、使用可能な容量、および合計論理容量の値と、これらの要素で使用されている割合の値が表示されます。これらの値には、 E シリーズの「予約済み」容量が含まれ、 E シリーズのユーザインターフェイスで表示される値よりも数値と割合が高くなります
- オーバーコミット容量–効率化テクノロジを使用して、ストレージプールの論理容量を超える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ている場合、この割合の値は 0% を超えます。
- スナップショット–スナップショット専用のセグメント領域にストレージプールアーキテクチャが容量の一部を割り当てている場合に使用されるスナップショット容量と合計容量
- 利用率–このストレージプールに容量を追加しているディスクのビジー率の最大値を示した割合。ディスク利用率にアレイのパフォーマンスとの間に大きな相関関係があるとは限りません。ホストベースのワークロードがない場合は、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、ボリュームワークロードとして表示されずにディスク使用率が向上する場合があります。
- IOPS –このストレージプールに容量の要因となっているすべてのディスクの合計 IOPS 。特定のプラットフォームのディスク IOPS がない場合、この値は、このストレージプールにあるすべてのボリュームのボリューム IOPS の合計から取得されます
- Throughput –このストレージプールの容量の要因となっているすべてのディスクの合計スループット。特定のプラットフォームでディスクスループットを使用できない場合は、このストレージプールに配置されているすべてのボリュームの合計ボリューム数がこの値に基づいて算出されます

ストレージノード

- Storage –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–通常、一方のノードだけにフェイルオーバーするプラットフォームでは、この画面が表示されます

- State –ノードの健常性。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
- メモリ–ベース 2 のメモリがあればそれ
- 利用率–通常は CPU 利用率番号、または NetApp ONTAP の場合はコントローラに負荷がかかる指標。現在、 NetApp E シリーズでは利用率を利用できません
- IOPS –このコントローラのホスト主導の IOPS を表す数値。理想的なソースはアレイから直接取得され、使用できない場合は、このノードにのみ所属するボリュームのすべての IOPS を合計して算出されます。
- Latency –このコントローラのホストのレイテンシまたは応答時間を表す数値。使用できない場合はアレイから直接ソースを取得し、このノードにのみ所属するボリュームから IOPS の重み付き計算を実行することを推奨します。
- Throughput –このコントローラのホストで実行されるスループットを示す数値です。理想的なソースはアレイから直接取得され、使用できない場合は、このノードにのみ所属するボリュームのすべてのスループットを合計して算出されます。
- プロセッサ– CPU 数

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

NetApp HCI 管理サーバのデータコレクタの設定

NetApp HCI 管理サーバデータコレクタは、 NetApp HCI ホスト情報を収集します。管理サーバ内のすべてのオブジェクトに対する読み取り専用の権限が必要です。

このデータコレクタは、 * NetApp HCI 管理サーバーのみ * から取得します。ストレージシステムからデータを収集するには、も設定する必要があります "NetApp SolidFire" データコレクタ：

用語集

Data Infrastructure Insights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	**Data Infrastructure Insights**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	ボリューム
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とは限りません

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。

- NetApp HCI 管理サーバの IP アドレス
- NetApp HCI 管理サーバの読み取り専用のユーザ名とパスワード
- NetApp HCI 管理サーバ内のすべてのオブジェクトに対する読み取り専用権限。
- NetApp HCI 管理サーバ上の SDK へのアクセス - 通常はセットアップ済みです。
- ポート要件： http - 80 https-443
- 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、 NetApp HCI 管理サーバにログインします
  - SDK が有効になっていることを確認します。 telnet <VC_IP> 443

セットアップと接続

フィールド	説明
名前	データコレクタの一意の名前
Acquisition Unit の場合	Acquisition Unit の名前

設定

フィールド	説明
NetApp HCI ストレージクラスタの MVIP	管理仮想 IP アドレス
SolidFire 管理ノード（ mNode ）	管理ノードの IP アドレス
ユーザ名	NetApp HCI 管理サーバへのアクセスに使用するユーザ名
パスワード	NetApp HCI 管理サーバへのアクセスに使用するパスワード
vCenter ユーザ名	vCenter のユーザ名
vCenter のパスワード	vCenter のパスワード

高度な設定

詳細設定画面で、 VM パフォーマンス * ボックスをオンにしてパフォーマンスデータを収集します。インベントリ収集は、デフォルトで有効になっています。
次のフィールドを設定できます。

フィールド	説明
インベントリのポーリング間隔（分）	デファントは 20 歳です

で VM をフィルタリングします	クラスタ、データセンター、または ESX ホストを選択します
「除外」または「含める」を選択してリストを指定します	VM を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	フィルタリングする 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で区切った）。ESX_host 、クラスタ、およびデータセンターでのみフィルタリングします
パフォーマンスのポーリング間隔（秒）	デフォルト値は 300 です

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。

在庫

問題	次の操作を実行します
エラー：フィルタリングする VM をリストに含めることはできません	[Include List] を選択した場合は、有効なデータセンター、クラスタ、またはホスト名をリストして、 VM をフィルタリングしてください
エラー： IP で VirtualCenter への接続をインスタンス化できませんでした	考えられる解決策： * 入力された資格情報と IP アドレスを確認してください。 * Infrastructure Client を使用して、 Virtual Center と通信してみてください。 * Managed Object Browser （ MOB など）を使用して Virtual Center と通信してみます。
エラー： IP の VirtualCenter には、 JVM で必要な非準拠の証明書があります	考えられる解決策： *推奨：より強力なRSAキー（1024ビットなど）を使用して、Virtual Center用の証明書を再生成します。 * 推奨されません。 JVM java.security 設定を変更して、 JDK.certPath.disableAlgorithms 制約を利用し、 512 ビット RSA キーを許可します。「 JDK 7 update 40 release notes 」を参照してください "http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

NetApp SolidFire オールフラッシュアレイデータコレクタ

NetApp SolidFire オールフラッシュアレイデータコレクタは、 iSCSI と Fibre Channel の両方の SolidFire 構成からのインベントリとパフォーマンスの収集をサポートします。

SolidFire データコレクタでは、 SolidFire REST API を使用します。データコレクタが配置されている Acquisition Unit から、 SolidFire クラスタ管理 IP アドレス上の TCP ポート 443 への HTTPS 接続を開始できる必要があります。データコレクタには、 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

Data Infrastructure Insightsでは、NetApp SolidFireオールフラッシュアレイ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。Data Infrastructure Insights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	**Data Infrastructure Insights**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
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

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。

要件

このデータコレクタを設定するための要件は次のとおりです。

- 管理仮想 IP アドレス
- 読み取り専用のユーザ名とクレデンシャル
- 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
接続タイプ	接続タイプを選択します

フィールド	説明
通信ポート	NetApp API に使用するポート
インベントリポーリング間隔（分）	デフォルトは 20 分です
パフォーマンスポーリング間隔（秒）	デフォルトは300秒です

トラブルシューティング

SolidFireからエラーが報告されると、Data Infrastructure Insightsに次のように表示されます。

データの取得中に SolidFire デバイスからエラーメッセージを受信しました。呼び出しは <method> （ <parameterString> ）でした。デバイスからのエラーメッセージは次のとおりです（デバイスマニュアルを確認してください）。 <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。

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

NetApp StorageGRID データコレクタ

NetApp StorageGRID データコレクタでは、 StorageGRID 構成からのインベントリやパフォーマンスの収集がサポートされます。

StorageGRID は、 raw TB から管理対象ユニットへのレートが異なる場合に測定されます。フォーマットされていない StorageGRID の容量が 40TB 個になると、 1 個のスペースが請求されます "管理ユニット (MU)"。

用語集

Data Infrastructure Insightsでは、NetApp StorageGRID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	**Data Infrastructure Insights**の用語
StorageGRID	ストレージ
ノード	ノード
テナント	ストレージプール
バケット	内部ボリューム

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 ホストの IP アドレス	StorageGRID アプライアンスの管理仮想 IP アドレス
ユーザ名	StorageGRID アプライアンスへのログインに使用する名前
パスワード	StorageGRID アプライアン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）	デフォルトは60分です
パフォーマンスポーリング間隔（秒）	デフォルトは900秒です

シングルサインオン（ **SSO** ）

。 "StorageGRID" ファームウェアバージョンには対応する API バージョンがあり、 3.0 API 以降のバージョンではシングルサインオン（ SSO ）ログインがサポートされています。

ファームウェアバージョン	API のバージョン	シングルサインオン（ SSO ）のサポート
11.1.	2.	いいえ
11.2.	3.0	はい。
11.5.	3.3	はい。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Nutanix NX データコレクタ

Data Infrastructure Insightsは、Nutanixデータコレクタを使用して、Nutanix NXストレージシステムのインベントリデータとパフォーマンスデータを検出します。

用語集

Data Infrastructure Insightsは、Nutanix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。Data Infrastructure Insights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	**Data Infrastructure Insights**の用語
ストレージプール	ストレージプール
Nutanix コンテナ	内部ボリューム
Nutanix コンテナ	ファイル共有
NFS 共有	共有

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。

要件

- クラスタの外部データサービスの IP アドレス
- volume_groups が使用されていないかぎり、読み取り専用のユーザ名とパスワード。この場合は、 Admin ユーザ名とパスワードが必要です
- ポート要件： HTTPS 443

設定

フィールド	説明
プリズム外部 IP アドレス	クラスタの外部データサービスの IP アドレス
ユーザ名	管理者アカウントのユーザ名
パスワード	管理者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	Nutanix アレイへの接続に使用する TCP ポート。デフォルトは 9440. です。
インベントリのポーリング間隔（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。
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秒です。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

OpenStack データコレクタ

OpenStack （ REST API / KVM ）データコレクタは、すべての OpenStack インスタンスのインベントリデータ、および必要に応じて VM のパフォーマンスデータを取得しま

す。

要件

- OpenStack コントローラの IP アドレス
- OpenStack admin 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。admin アカウントや admin 相当の権限を使用していない場合は、データコレクタユーザ ID に基づいて緩和するデフォルトポリシーを特定するために、トライアルとエラーを使用する必要があります。
- パフォーマンス収集用にOpenStack Gnocchi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。Gnocchiの設定は、各ハイパーバイザーのNova.confファイルを編集し、各ハイパーバイザーでNova Computeサービスを再起動することで行います。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 の統計情報の場合、コンピューティングノードの /etc/nova/nover.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
  - 8777（ニョッキ・パフォーマンス・サービス用）
  - Glance Image Serviceの場合は9292
    *注*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	説明
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 管理者のテナント名
KVM sudo ユーザー	KVM Sudo ユーザー名

フィールド	説明
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されるクレデンシャルのタイプ
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	説明
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
SSHポート	SSH に使用するポート
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）	インベントリのポーリング間隔。 デフォルトは20分です。

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。

在庫

問題	次の操作を実行します
「 Configuration error 」と表示され、「 Policy does not allow 」または「 You are not authorized 」というエラーメッセージが表示されます。	* IPアドレスを確認します *ユーザー名とパスワードを確認してください

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Oracle ZFS Storage Appliance データコレクタ

Data Infrastructure Insightsは、Oracle ZFS Storage Applianceデータコレクタ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ます。

用語集

Data Infrastructure Insightsは、Oracle ZFSデータコレクタを使用してインベントリ情報を取得します。Data Infrastructure Insights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	**Data Infrastructure Insights**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
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

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

- ZFS Controller-1 および ZFS Controller-2 のホスト名
- 管理者のユーザ名とパスワード
- ポート要件： 215 HTTP/HTTPS

必要なパフォーマンス指標

Oracle ZFSアプライアンスを使用すると、ストレージ管理者はパフォーマンス統計をキャプチャするための柔軟性を大幅に高めることができます。Data Infrastructure Insightsでは、次の指標を取得するようにハイアベイラビリティペアの_each_controllerを設定する必要があります。

- smb2。ops [共有]
- nfs3.ops [共有]
- nfs4.ops [共有]
- nfs4-1.ops [共有]

コントローラがこれらの一部またはすべてをキャプチャしていないと、「内部ボリューム」のワークロードがData Infrastructure Insightsに含まれていないか、アンダーレポートになる可能性があります。

設定

フィールド	説明
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 Hostname（ZFSコントローラ2ホスト名）の略	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
接続タイプ	HTTPS または HTTP では、デフォルトのポートも表示されます
接続ポートを上書きします	空白の場合は、 [Connection Type] フィールドでデフォルトのポートを使用します。それ以外の場合は、使用する接続ポートを入力します
インベントリのポーリング間隔	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）	デフォルトは300です。

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。

在庫

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 」というエラーメッセージが表示され、「 REST Service is disabled 」という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る。	このエラーは、特定のロール（「 advanced_analytics」など）が設定済みのユーザに含まれていないことが原因で発生する可能性があります。 読み取り専用ロールを持つユーザーにAnalyticsスコープを適用すると、エラーが削除される場合があります。次の手順を実行します。 1. ZFSシステムの[Configuration]→[Users]画面で'ロールの上にマウスを移動し'ダブルクリックして編集を許可します 2. [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。 3. 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。 4. 右側の[追加]ボタンをクリックします。 5. 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。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Pure Storage FlashArray データコレクタ

Data Infrastructure Insightsは、Pure Storage FlashArrayデータコレクタ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ます。

用語集

Data Infrastructure Insightsで取得したアセットタイプごとに、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	**Data Infrastructure Insights**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
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

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。

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	説明
FlashArray ホストの IP アドレス	ストレージシステムの IP アドレス
ユーザ名	admin 権限があるユーザ名
admin 権限があるアカウントのパスワード	パスワード

高度な設定

フィールド	説明
接続タイプ	HTTP または HTTPS を選択します。デフォルトのポートも表示されます。

フィールド	説明
TCP ポートを上書きします	空白の場合は、 [Connection Type] フィールドでデフォルトのポートを使用します。それ以外の場合は、使用する接続ポートを入力します
インベントリのポーリング間隔（分）	デフォルトは 60 分です
パフォーマンスポーリング間隔（秒）	デフォルトは300です

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。

在庫

問題	次の操作を実行します
「 Invalid login credentials 」というエラーメッセージが表示され、「 Policy does not allow 」または「 you are not authorized 」が表示されます。	Pure http インターフェイスで Pure のユーザアカウントとパスワードを検証します

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Red Hat Virtualization データコレクタ

Data Infrastructure Insightsは、Red Hat Virtualizationデータコレクタを使用して、仮想化されたLinuxおよびMicrosoft Windowsのワークロードからインベントリデータを収集します。

用語集

Data Infrastructure Insightsで取得したアセットタイプごとに、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	**Data Infrastructure Insights**の用語
ディスク	仮想ディスク
ホスト	ホスト
仮想マシン	仮想マシン
ストレージドメイン	データストア
Logical Unit の略	LUN

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。

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	ストレージシステムの IP アドレス
ユーザ名	admin 権限があるユーザ名
admin 権限があるアカウントのパスワード	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
インベントリのポーリング間隔（分）	デフォルトは20分です。

トラブルシューティング

この Data Collector の追加情報は、から入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Rubrik CDM Data Collectorの略

Data Infrastructure Insightsは、Rubrikのデータコレクタを使用して、Rubrikストレージアプライア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。

用語集

Data Infrastructure Insightsでは、Rubrik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。Data Infrastructure Insights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	**Data Infrastructure Insights**の用語
クラスタ	ストレージ、ストレージプール
ノード	ストレージノード
ディスク	ディスク

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

このデータコレクタを設定するには、次のものが必要です。

- Data Infrastructure Insights Acquisition Unitは、RubrikクラスタへのTCPポート443への接続を開始します。クラスタごとに1つのコレクタ。
- RubrikクラスタのIPアドレス。
- クラスタのユーザ名とパスワード。
- RubrikクラスタのIPアドレスまたはホスト名。
- Basic認証の場合は、クラスタのユーザ名とパスワード。サービスアカウントベースの認証を使用する場合は、サービスアカウント、シークレット、および組織IDが必要です。
- ポート要件： HTTPS 443

設定

フィールド	説明
IP	RubrikクラスタのIPアドレス
ユーザ名	クラスタのユーザ名
パスワード	クラスタのパスワード

高度な設定

インベントリのポーリング間隔（分）	デフォルトは**60**です
パフォーマンスポーリング間隔（秒）	デフォルトは300です

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。

在庫

問題	次の操作を実行します
複数のストレージが作成されているというメッセージを受け取りました。	クラスタが正しく設定されており、コレクタが単一のクラスタを参照していることを確認します。
ディスクAPIからより多くのデータが返されたという警告が表示されました	追加のデータを取得するには、サポートに確認してください。

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

VMware vSphere データコレクタの設定

VMware vSphereのデータコレクタは、VMゲストおよびESXiホストのパフォーマンスと構成に関する情報を収集します。vSphere内のすべてのオブジェクトに対して読み取り

専用のPrivilegesが必要です。2024年8月以降、vSphereコレクタは、vSphere環境からのログメッセージと一部のVMware固有の指標も取り込みます。Data Infrastructure Insightsは、vSphere 8.0.1以降の環境からのみVMwareログ情報を取得できます。同様に、ベンダー固有の指標はvSphere 7以降の環境でのみサポートされます。そのため、特定のコレクタが古いvSphereインスタンスを参照している場合は、そのコレクタのログやベンダー固有のメトリックのチェックボックスを無効にすることができます。

用語集

Data Infrastructure Insightsは、VMware vSphere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	**Data Infrastructure Insights**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	ボリューム
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とは限りません

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。

- 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が必要です。
- Virtual Center サーバの SDK へのアクセス - 通常はすでにセットアップされています。
- ポート要件： http - 80 https-443
- 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、 Virtual Center Client にログインします
  - SDK が有効になっていることを確認します。 telnet <VC_IP> 443

セットアップと接続

フィールド	説明
名前	データコレクタの一意の名前
Acquisition Unit の場合	Acquisition Unit の名前

設定

フィールド	説明
仮想センターの IP アドレス	Virtual Center の IP アドレス
ユーザ名	Virtual Center へのアクセスに使用するユーザ名
パスワード	Virtual Center へのアクセスに使用するパスワード

高度な設定

詳細設定画面で、 VM パフォーマンス * ボックスをオンにしてパフォーマンスデータを収集します。インベントリ収集は、デフォルトで有効になっています。
次のフィールドを設定できます。

フィールド	説明
インベントリのポーリング間隔（分）	デフォルトは20です
VM をフィルタリングします	クラスタ、データセンター、または ESX ホストを選択します
「除外」または「含める」を選択してリストを指定します	フィルタリストの作成（クラスタ、データセンター、ESX_host ）
再試行回数	デフォルトは3です
通信ポート	デフォルトは443です
デバイスリストのフィルタ …	このリストは、完全に一致する文字列で構成されている必要があります。esx_hostでフィルタリングする場合は、Data Infrastructure InsightsとvSphereの両方で報告されたESXホストの正確な「名前」をカンマで区切って作成する必要があります。「名前」には、 IP アドレス、単純なホスト名、または Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）を指定できます。この名前は、これらのホストが vSphere に最初に追加されたときの命名方法によって決まります。クラスタでフィルタリングする場合は、ハイパーバイザーのCIによって報告されるData Infrastructure Insights形式のクラスタ名を使用します。Data Infrastructure Insightsでは、vSphereクラスタ名の前にvSphereデータセンター名が付加され、スラッシュが付きます。「DC1/clusterA」は、Data Infrastructure InsightsがデータセンターDC1内のclusterAのハイパーバイザーについて報告するクラスタ名です。
パフォーマンスのポーリング間隔（秒）	デフォルト値は 300 です

VMwareのタグと**Data Infrastructure Insights**のアノテーションのマッピング

VMwareデータコレクタを使用すると、VMwareで設定されているタグを使用してData Infrastructure Insightsのアノテーションを入力できます。アノテーションにはVMwareタグとまったく同じ名前を付ける必要があります。Data Infrastructure Insights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「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コレクタ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で再作成する必要があります。

VMwareタグでは大文字と小文字が区別され、Data Infrastructure Insightsタグ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、Data Infrastructure Insightsで「owner」という名前のアノテーションを作成し、VMwareで「owner」、「Owner」、「owner」という名前のタグを作成すると、これらすべての「owner」の変化形がCloud Insightの「owner」アノテーションにマッピングされます。

次の事項に注意してください。

- 現在のところ、Data Infrastructure Insightsでは、NetAppデバイスのサポート情報を自動で公開するだけです。
- このサポート情報はアノテーション形式で保持されているため、クエリを実行したり、ダッシュボードで使用したりできます。
- ユーザがアノテーション値を上書きまたは空にした場合、Data Infrastructure Insightsでアノテーションが更新されると再び値が自動入力されます。更新は1日に1回行われます。

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。

在庫

問題	次の操作を実行します
エラー：フィルタリングする VM をリストに含めることはできません	[Include List] を選択した場合は、有効なデータセンター、クラスタ、またはホスト名をリストして、 VM をフィルタリングしてください
エラー： IP で VirtualCenter への接続をインスタンス化できませんでした	考えられる解決策： * 入力された資格情報と IP アドレスを確認してください。 * VMware Infrastructure Client を使用して、 Virtual Center との通信を試みます。 * Managed Object Browser （ MOB など）を使用して Virtual Center と通信してみます。
エラー： IP の VirtualCenter には、 JVM で必要な非準拠の証明書があります	考えられる解決策： *推奨：より強力なRSAキー（1024ビットなど）を使用して、Virtual Center用の証明書を再生成します。 * 推奨されません。 JVM java.security 設定を変更して、 JDK.certPath.disableAlgorithms 制約を利用し、 512 ビット RSA キーを許可します。「 JDK 7 update 40 release notes 」を参照してください "http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Data Collector Reference - サービス

ノードデータ収集

Data Infrastructure Insightsは、エージェントをインストールしたノードから指標を収集します。

インストール

1. [Observability]>[Collectors]*で、オペレーティングシステム/プラットフォームを選択します。統合データコレクタ（ Kubernetes 、 Docker 、 Apache など）をインストールすると、ノードのデータ収集も設定されることに注意してください。
2. 指示に従って、エージェントを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタがノードの指標として収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
ノードファイルシステム	ノード UUID デバイス パス を入力します	ノードIP ノード名 ノードOS モード	無料 空きinode inodeの合計 使用されているinode 合計 使用済み合計 使用済み
ノードディスク	ノード UUID ディスク	ノードIP ノード名 ノードOS	IO時間の合計 IOPSを実行中です 読み取りバイト数（1秒あたり） 読み取り時間合計 読み取り数（1秒あたり） Weighted IO Time Totalの略 書き込みバイト数（1秒あたり） 書き込み時間合計 1秒あたりの書き込み数 現在のディスクキューの長さ 書き込み時間 読み取り時間 IO時間

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
ノードCPU	ノード UUID CPU	ノードIP ノード名 ノードOS	システムCPU使用率 ユーザCPU使用率 アイドルCPU使用率 プロセッサCPU使用率 割り込みCPU使用率 DPC CPU使用率

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
ノード	ノード UUID	ノードIP ノード名 ノードOS	カーネル起動時間 カーネルコンテキストスイッチ（1秒あたり） カーネルエントロピーが利用可能です カーネル割り込み（1秒あたり） カーネルプロセスのフォーク（1秒あたり） メモリがアクティブです 使用可能なメモリの合計 使用可能なメモリ メモリがバッファされました メモリキャッシュ メモリコミット制限 メモリはとしてコミットされます メモリが汚れています メモリ空き メモリの空き容量が大きい Memory High Totalの略 メモリのページサイズが大きすぎます メモリ巨大なページ無料 Memory Huge Pages Totalの略 メモリが不足しています Memory Low Totalの略 メモリマップ済み Memory Page Tablesの略 メモリ共有 メモリスラブ メモリスワップキャッシュ メモリスワップフリー メモリスワップの合計 メモリ合計 使用メモリの合計 使用されているメモリ メモリvmallocチャンク メモリvmallocの合計 メモリvmallocが使用されています メモリが配線されています メモリライトバック合計 Memory Writeback tmp（ メモリライトバックtmp メモリキャッシュの障害 メモリ要求ゼロエラー メモリページ障害 メモリページ

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
ノードネットワーク	Network Interface の略 ノード UUID	ノード名 ノードIP ノードOS	受信したバイト数 送信されたバイト数 送信されたパケットが破棄されました Packets Outboud Errors （パケット送信エラー） 受信したパケットは破棄されました パケット受信エラー 受信したパケット 送信されたパケット

セットアップ（ **Setup** ）

セットアップおよびトラブルシューティングの情報は、にあります "エージェントの設定" ページ

ActiveMQ データコレクタ

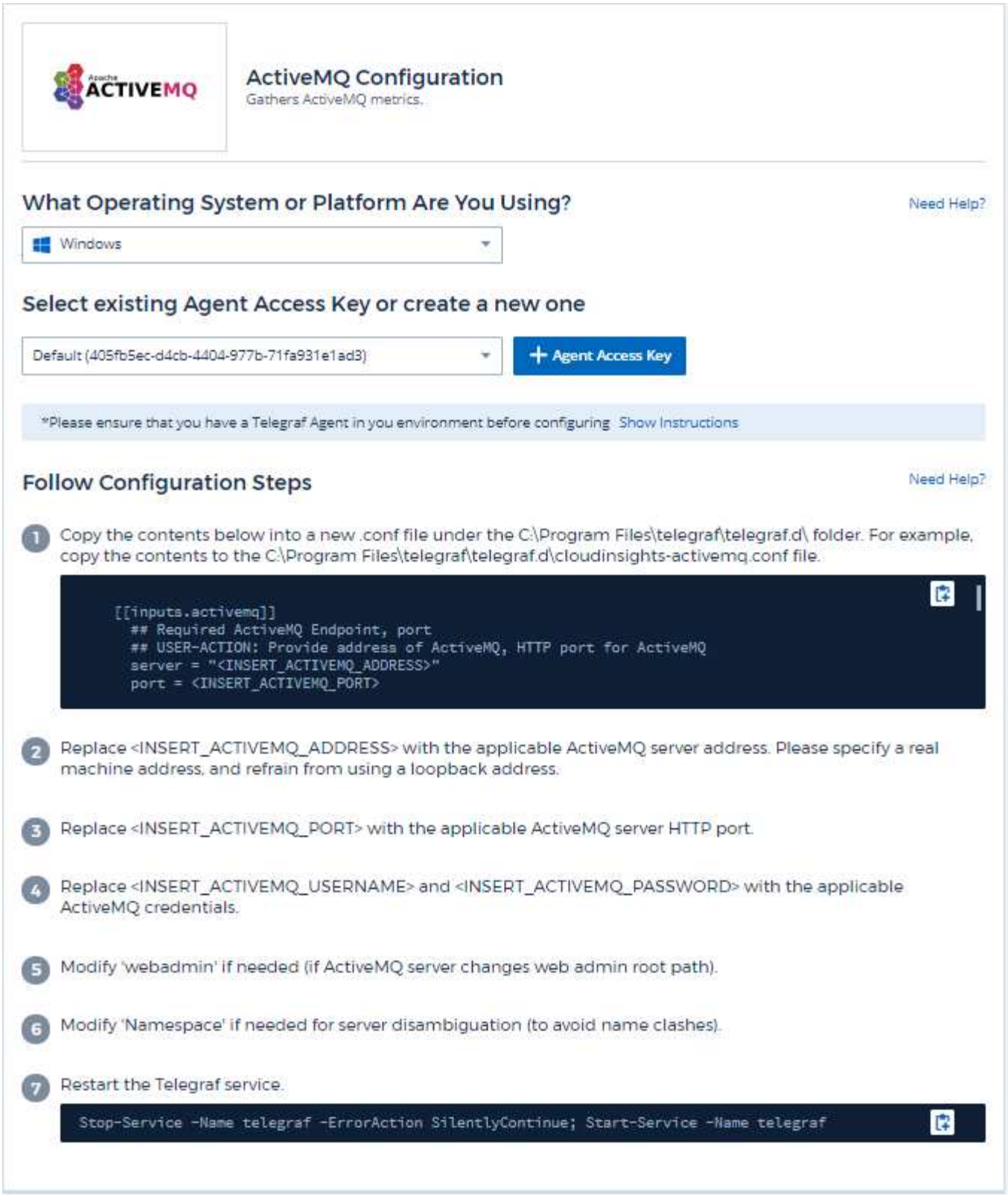
Data Infrastructure Insightsは、このデータコレクタを使用してActiveMQから指標を収集します。

インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。[ActiveMQ]を選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順
3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

情報は、に記載されています "ActiveMQ のドキュメント"

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
ActiveMQ キュー	ネームスペース キュー ポート サーバ	ノード名 ノードIP ノード UUID	消費者数 デキューカウント enqueueカウント キューサイズ
ActiveMQ サブスクライバ	クライアント ID 接続ID ポート サーバ ネームスペース	はアクティブです 宛先 ノード名 ノードIP ノード UUID ノードOS セレクタ サブスクリプション。	デキューカウント ディスパッチ数 ディスパッチキューサイズ enqueueカウント 保留中のキューサイズ
ActiveMQ トピック	トピック ポート サーバ ネームスペース	ノード名 ノードIP ノード UUID ノードOS	消費者数 デキューカウント enqueueカウント サイズ

トラブルシューティング

追加情報はから入手できます "サポート" ページ

Apache Data Collector

このデータコレクタを使用すると、環境内の Apache サーバからデータを収集できます。

前提条件

- Apache HTTP Server がセットアップされ、適切に実行されている必要があります
- エージェントのホスト / VM に対する sudo 権限または管理者権限が必要です
- 通常、 apache_mod_status_module は、 Apache サーバの「 /server-status?auto 」場所にページを公開するように設定されています。使用可能なすべてのフィールドを収集するには、 *ExtendedStatus* オプションを有効にする必要があります。サーバの設定方法については、 Apache モジュールのドキュメントを参照してください。 https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

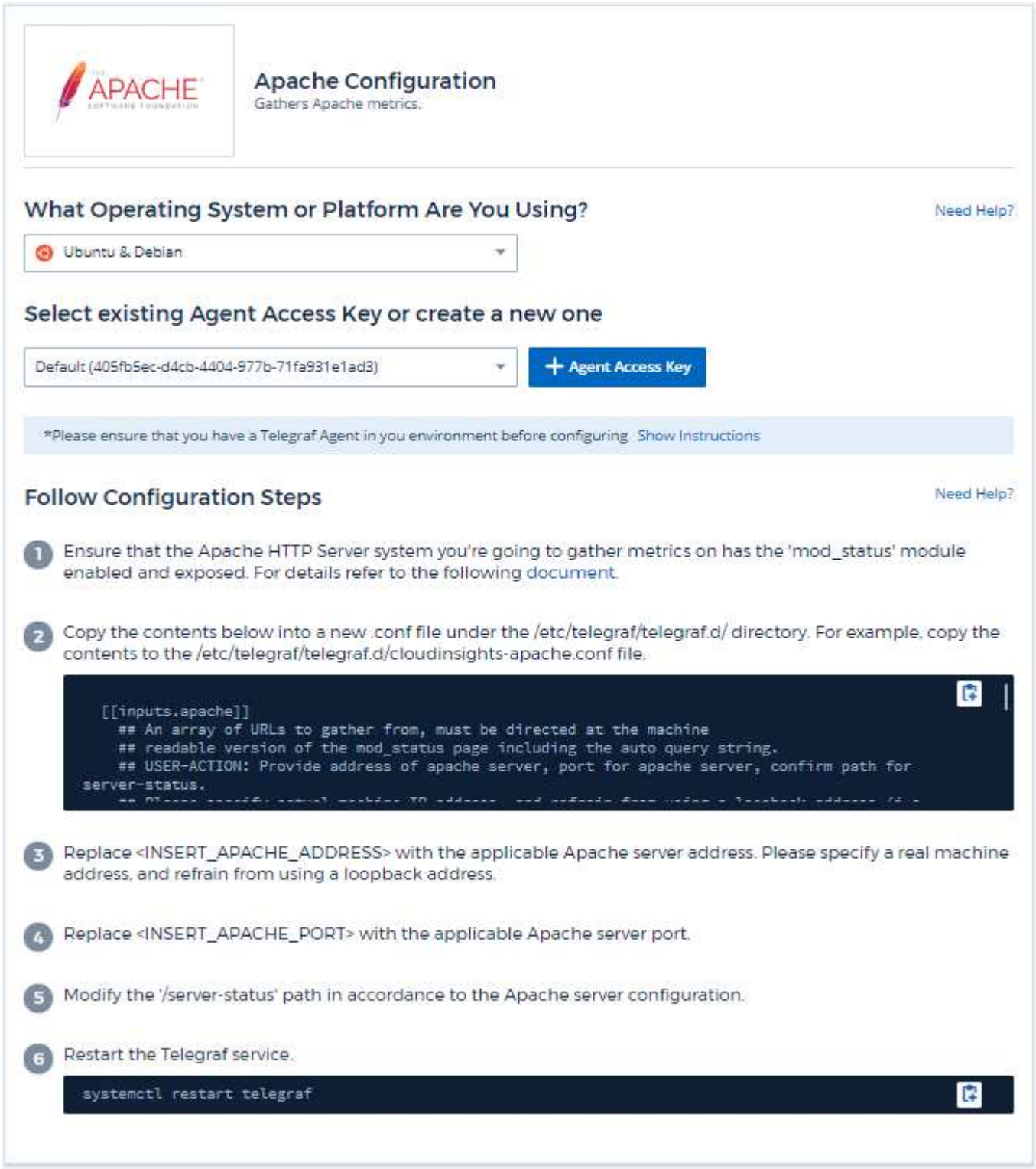
インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。Apacheを選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順

3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

Telegraf の Apache の HTTP Server 用プラグインは 'OD _status' モジュールを有効にする必要があります。これを有効にすると、 Apache の HTTP サーバは、ブラウザで表示したり、 Apache の HTTP サーバ設定の状態を抽出するためにスクレイピングされた HTML エンドポイントを公開します。

互換性：

構成は Apache の HTTP Server バージョン 2.4.38 に対して開発されました。

mod_status を有効にします。

'OD_status' モジュールを有効にして公開するには、次の 2 つの手順を実行します。

- イネーブルモジュール
- モジュールから統計情報を公開しています

イネーブルモジュール：

モジュールのロードは '/usr/local/apache/conf/httpd.conf ' の下の config ファイルによって制御されます。構成ファイルを編集し、次の行のコメントを解除します。

```
LoadModule status_module modules/mod_status.so
Include conf/extra/httpd-info.conf
```

モジュールからの統計情報の公開：

'OD_status' の公開は '/usr/local/apache2/conf/extra /httpd-info.conf' の下の config ファイルによって制御されます。設定ファイルに次のものがあることを確認してください (少なくとも、他のディレクティブが存在することを確認してください) 。

```
# Allow server status reports generated by mod_status,
# with the URL of http://servername/server-status
<Location /server-status>
    SetHandler server-status
</Location>

#
# ExtendedStatus controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information
(ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
ExtendedStatus On
```

'OD_status' モジュールの詳細な手順については、を参照してください "Apache のドキュメント"

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Apache	ネームスペース サーバ	ノードIP ノード名 ポート 親サーバー構成の生成 親サーバーのMPM生成 サーバの稼働時間 が停止しています	多忙な労働者 要求あたりのバイト数 1秒あたりのバイト数 CPU Children Systemの略 CPU Children Userの略 CPU負荷 CPUシステム CPUユーザ 非同期接続が終了しています 非同期接続のキープアライブ 非同期接続の書き込み 接続合計 リクエストごとの期間 アイドル状態の従業員 負荷平均（過去1m） 負荷平均（過去15m） 負荷平均（過去5m） プロセス 1秒あたりの要求数 合計アクセス数 合計期間 合計KB スコアボード終了 スコアボードのDNSルックアップ スコアボードの仕上げ スコアボードアイドルクリーンアップ スコアボードキープアライブ スコアボードログ スコアボードが開きます スコアボードの読み取り スコアボード送信 スコアボードが開始されました スコアボード待機中

トラブルシューティング

追加情報はから入手できます "サポート" ページ

総領事データ収集

Data Infrastructure Insightsは、このデータコレクタを使用してConsulから指標を収集し

ます。

インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。Consulを選択します。

   収集用にエージェントを設定していない場合は、にプロンプトが表示されます "エージェントをインストールします" お客様の環境で実現します。

   エージェントがすでに設定されている場合は、適切な OS またはプラットフォームを選択し、 [* Continue （続行）] をクリックします。

2. [Consul Configuration] 画面の指示に従って、データコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。

セットアップ（ **Setup** ）

情報は、に記載されています "総領事からのご説明"。

接続のためのオブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
総領事	ネームスペース IDを確認します サービスノード	ノードIP ノードOS ノード UUID ノード名 サービス名 [名前（ Name ）] を サービス ID ステータス	重要 パス 警告

トラブルシューティング

追加情報はから入手できます "サポート" ページ

Couchbase Data Collector

Data Infrastructure Insightsは、このデータコレクタを使用してCouchbaseから指標データを収集します。

インストール

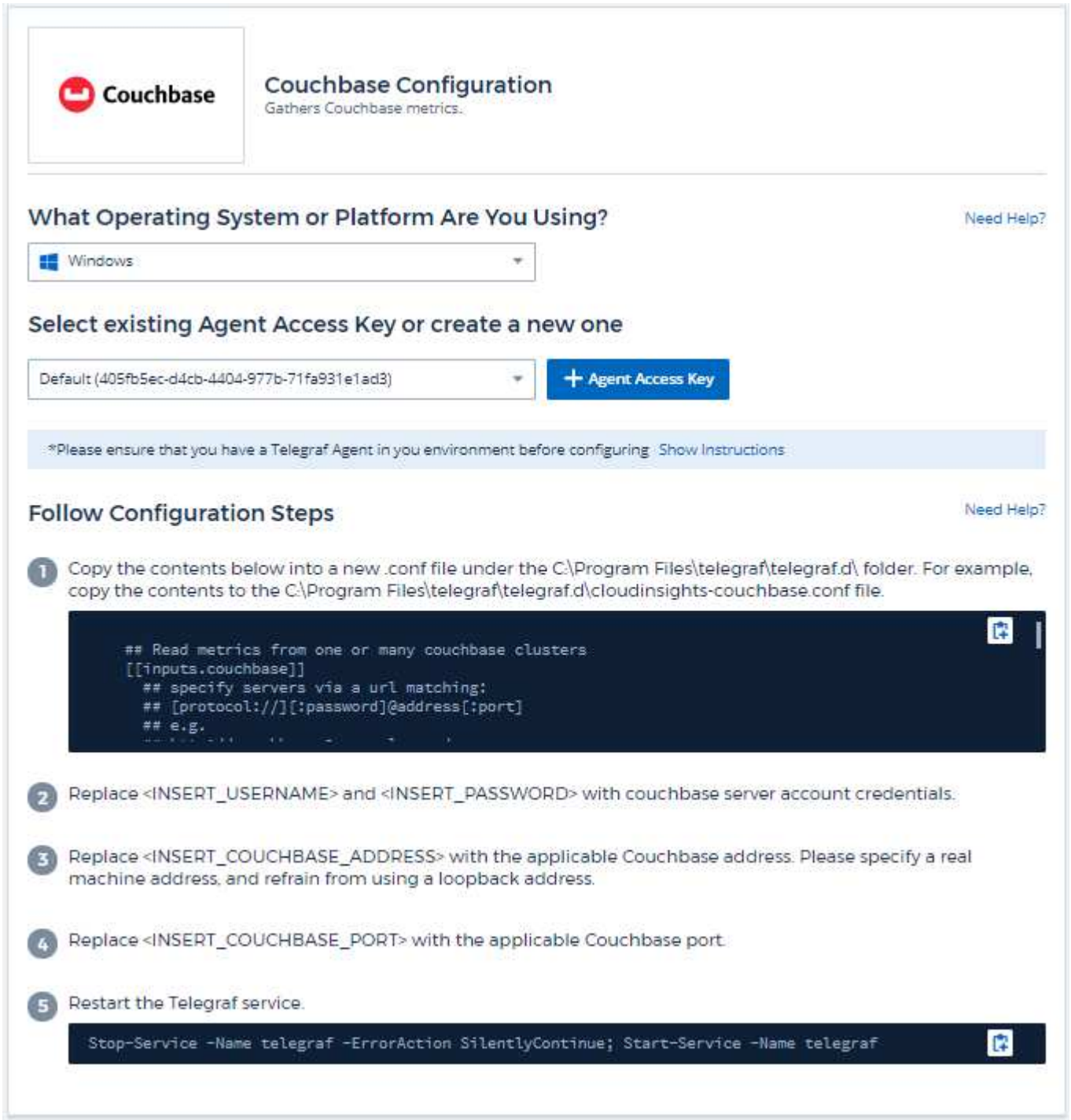
1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。[Couchbase]を選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エ

ージェントのインストール" 手順

3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

情報は、に記載されています "Couchbase ドキュメント"。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Couchbase Node	ネームスペース クラスタ Couchbaseノードのホスト名	ノード名 ノードIP	メモリ空き メモリ合計
Couchbase バケット	ネームスペース バケット クラスタ	ノード名 ノードIP	使用済みデータ データフェッチ 使用されているディスク アイテム数 使用されているメモリ 1秒あたりの処理数 使用済みクォータ

トラブルシューティング

追加情報はから入手できます "サポート" ページ

CouchDB データコレクタ

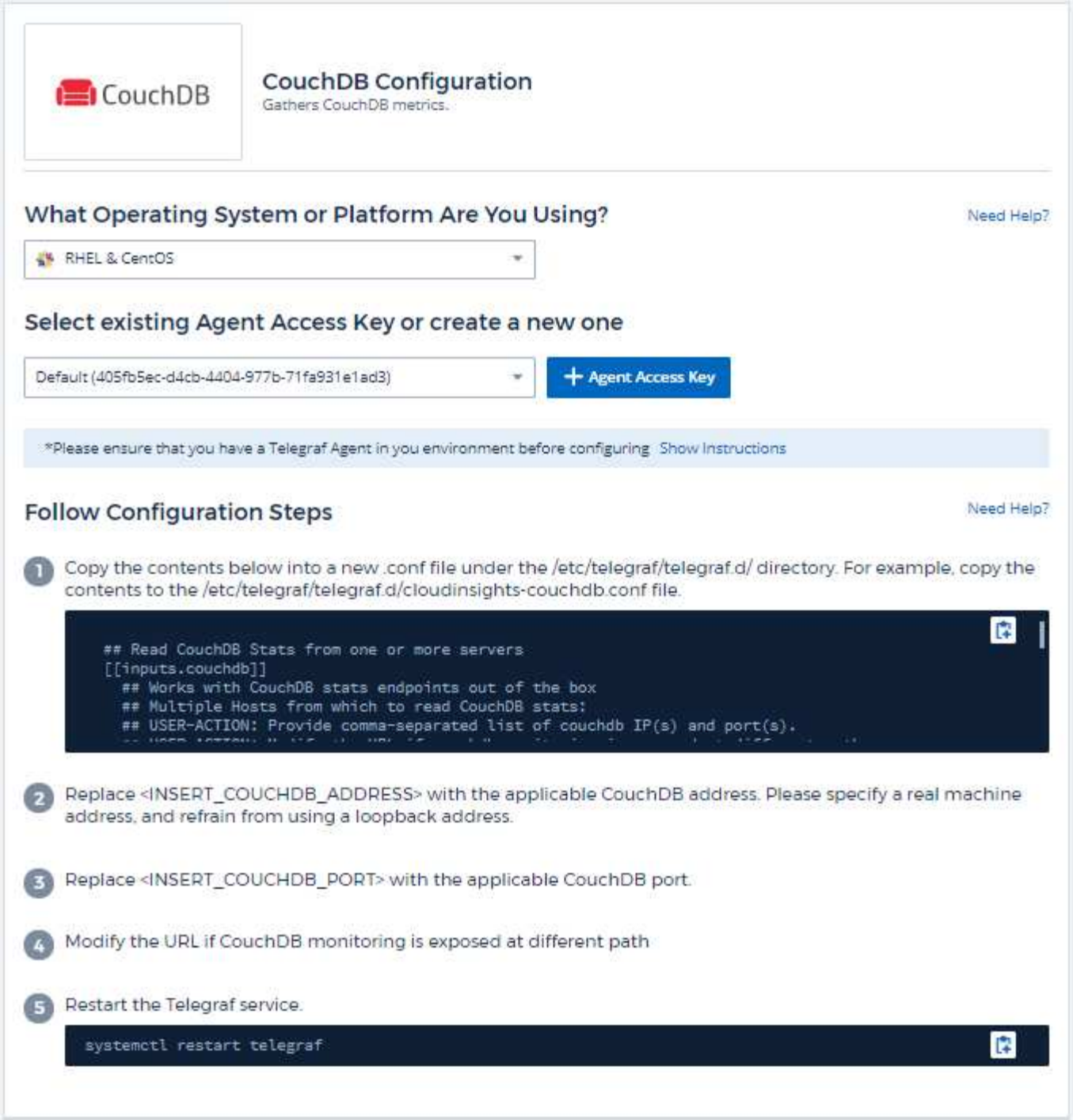
Data Infrastructure Insightsは、このデータコレクタを使用してCouchDBから指標データを収集します。

インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。[CouchDB]を選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順
3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

情報は、に記載されています "CouchDB のドキュメント"。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
CouchDB	ネームスペース サーバ	ノード名 ノードIP	認証キャッシュヒット 認証キャッシュミス データベースの読み取り データベースへの書き込み データベースが開きます OSファイルを開きます 最大要求時間 最小要求時間 httpdリクエストメソッドコピー httpdリクエストメソッド削除 httpdリクエストメソッドGET httpdリクエストメソッドヘッド httpdリクエストメソッドPost httpdリクエストメソッドPUT ステータスコード200 ステータスコード201 ステータスコード202 ステータスコード301 ステータスコード304. ステータスコード400 ステータスコード401 ステータスコード403 ステータスコード404 ステータスコード405 ステータスコード409 ステータスコード412 ステータスコード500

トラブルシューティング

追加情報はから入手できます "サポート" ページ

Docker Data Collector

Data Infrastructure Insightsは、このデータコレクタを使用してDockerから指標を収集します。

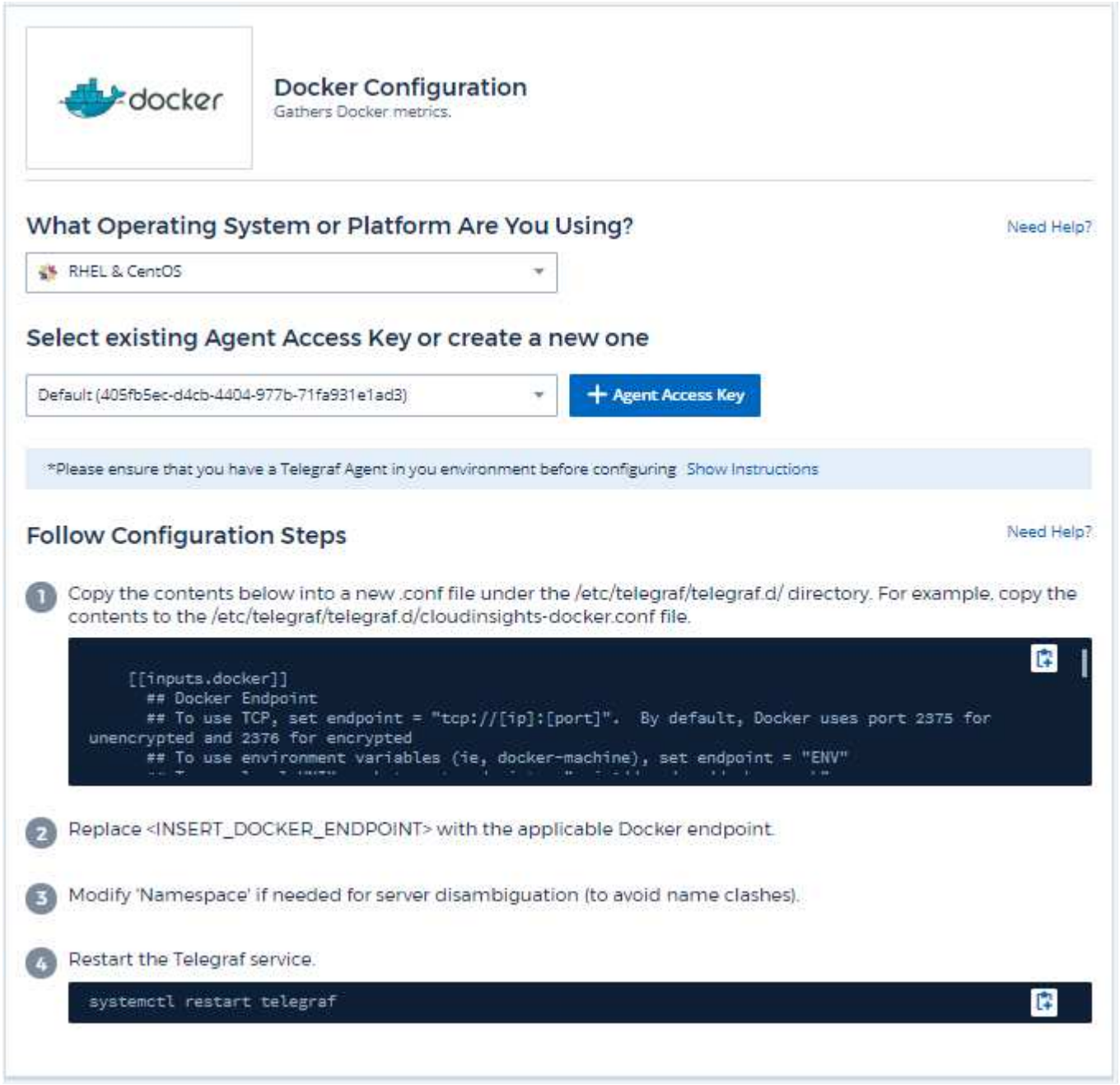
インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。[Docker]を選択します。

   収集用にエージェントを設定していない場合は、にプロンプトが表示されます "エージェントをインストールします" お客様の環境で実現します。

エージェントがすでに設定されている場合は、適切な OS またはプラットフォームを選択し、 [* Continue （続行）] をクリックします。

2. Docker Configuration 画面の指示に従って、データコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

Telegraf Docker 用入力プラグインは、指定された UNIX ソケットまたは TCP エンドポイントを介してメトリックを収集します。

互換性

Docker バージョン 1.12.6 に対して構成が開発されました。

UNIX ソケット経由で Docker にアクセスする

Tegraf エージェントが BareMetal 上で実行されている場合は、次のコマンドを実行して、テレグラフ UNIX ユーザを Docker UNIX グループに追加します。

```
 sudo usermod -aG docker telegraf
```

Telegraf エージェントが Kubernetes ポッド内で実行されている場合は、ソケットをポッドにボリュームとしてマッピングし、そのボリュームを /var/run/docker.sock にマウントすることで、 Docker Unix ソケットを公開します。　たとえば、 PodSpec に次の情報を追加します。

```
volumes:
...
- name: docker-sock
hostPath:
path: /var/run/docker.sock
type: File
```

次に、次の項目をコンテナに追加します。

```
volumeMounts:
...
- name: docker-sock
mountPath: /var/run/docker.sock
```

Kubernetesプラットフォーム用に提供されているData Infrastructure Insightsインストーラがこのマッピングを自動的に処理します。

TCP エンドポイントを介して Docker にアクセスする

デフォルトでは、 Docker は暗号化されていないアクセスにポート 2375 を使用し、暗号化されたアクセスにポート 2376 を使用します。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Docker Engine の略	ネームスペース Docker Engine の略	ノード名 ノードIP ノード UUID ノードOS Kubernetesクラスタ Dockerバージョン 単位	メモリ コンテナ コンテナが一時停止しました 実行中のコンテナ コンテナが停止しました CPU ルーチンを実行します イメージ リスナーイベント 使用されているファイル記述子 使用可能なデータ データ合計 使用済みデータ メタデータが使用可能です メタデータ合計 使用されているメタデータ プールのブロックサイズ

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Docker コンテナ	ネームスペース コンテナ名 Docker Engine の略	Kubernetesコンテナハッシュ Kubernetesコンテナポート Kubernetesコンテナの再起動数 Kubernetes Container Termination Message Pathの略 Kubernetes Container Termination Message Policyの略 Kubernetesポッド終了の猶予期間 コンテナイメージ コンテナのステータス コンテナバージョン ノード名 Kubernetesコンテナログパス Kubernetesコンテナ名 Kubernetes Dockerタイプ Kubernetesポッド名 Kubernetesポッドネームスペース KubernetesポッドUID KubernetesサンドボックスID ノードIP ノード UUID Dockerバージョン Kubernetes IO設定を確認しました Kubernetes IO構成ソース OpenShift IO SCC Kubernetes概要の略 Kubernetesの表示名 OpenShiftタグ Komposeサービス ポッドテンプレートハッシュ コントローラリビジョンハッシュ ポッドテンプレート生成使用許諾 スキーマビルド日 スキーマライセンス スキーマ名 スキーマURL スキーマVCS URL スキーマベンダー スキーマバージョン スキーマスキーマバージョン	Memory Active Anonymousの略 メモリアクティブファイル メモリキャッシュ メモリ階層の制限 メモリ非アクティブ匿名 メモリ非アクティブファイル メモリ制限 Memory Mapped Fileの略 Memory Max Usageの略 メモリページ障害 メモリページの重大な障害 メモリがページインされました メモリがページアウトされました メモリ常駐設定サイズ メモリ常駐セットサイズが大きすぎます Memory Total Active Anonymousの略 Memory Total Active Fileの略 メモリ合計キャッシュ Memory Total Inactive Anonymousの略 Memory Total Inactive Fileの略 Memory Total Mapped Fileの略 Memory Total Page Faultの略 Memory Total Page Major Faultの略 ページインされたメモリの合計 ページアウトされたメモリの合計 Memory Total Resident Set Sizeの略 メモリ合計常駐セットサイズが大きすぎます Memory Total Unevictableの略 Memory Unevictable（アクセス不能メモリ）の略 メモリ使用量 メモリ使用率 終了コード ウームは殺されたピッド

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Docker コンテナブロック IO	ネームスペース コンテナ名 デバイス Docker Engine の略	Kubernetesコンテナハッシュ Kubernetesコンテナポート Kubernetesコンテナの再起動数 Kubernetes Container Termination Message Pathの略 Kubernetes Container Termination Message Policyの略 Kubernetesポッド終了の猶予期間 コンテナイメージ コンテナのステータス コンテナバージョン ノード名 Kubernetesコンテナログパス Kubernetesコンテナ名 Kubernetes Dockerタイプ Kubernetesポッド名 Kubernetesポッドネームスペース KubernetesポッドUID Kubernetesサンドボックス ID ノードIP ノード UUID Dockerバージョン Kubernetes Configを確認 Kubernetes構成ソース OpenShift SCC Kubernetes概要の略 Kubernetesの表示名 OpenShiftタグ スキーマスキーマバージョン ポッドテンプレートハッシュ コントローラリビジョンハッシュ ポッドテンプレート生成 Komposeサービス スキーマビルド日 スキーマライセンス スキーマ名 スキーマベンダー 顧客ポッド Kubernetes StatefulSetポッド名 テナント WebConsoleの略	IO Service Bytes Recursive Asyncの略 IO Service Bytes Recursive Readの略 IO Service Bytes Recursive Syncの略 IOサービスバイト数の再帰的合計 IO Service Bytes Recursive Writeの略 IO Serviced Recursive Asyncの略 IO Serviced Recursive Readの略 IO Serviced Recursive Syncの略 IOサービス再帰合計 IO Serviced Recursive Writeの略

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Docker コンテナネットワーク	ネームスペース コンテナ名 ネットワーク Docker Engine の略	コンテナイメージ コンテナのステータス コンテナバージョン ノード名 ノードIP ノード UUID ノードOS Kubernetesクラスタ Dockerバージョン コンテナID	RXがドロップされました Rxバイト Rxエラー Rxパケット 送信がドロップされました 送信バイト数 TXエラー 送信パケット数

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Docker コンテナの CPU	ネームスペース コンテナ名 CPU Docker Engine の略	Kubernetesコンテナハッシュ Kubernetesコンテナポート Kubernetesコンテナの再起動数 Kubernetes Container Termination Message Pathの略 Kubernetes Container Termination Message Policyの略 Kubernetesポッド終了の猶予期間 Kubernetes Configを確認 Kubernetes構成ソース OpenShift SCC コンテナイメージ コンテナのステータス コンテナバージョン ノード名 Kubernetesコンテナログパス Kubernetesコンテナの名前 Kubernetes Dockerタイプ Kubernetesポッド名 Kubernetesポッドネームスペース KubernetesポッドUID Kubernetesサンドボックス ID ノードIP ノード UUID ノードOS Kubernetesクラスタ Dockerバージョン Kubernetes概要の略 Kubernetesの表示名 OpenShiftタグ スキーマバージョン ポッドテンプレートハッシュ コントローラリビジョンハッシュ ポッドテンプレート生成 Komposeサービス スキーマビルド日 スキーマライセンス スキーマ名 スキーマベンダー 顧客ポッド Kubernetes StatefulSetポッド名	スロットリング期間 調整された期間の調整 スロットル調整時間 カーネルモードでの使用 ユーザーモードでの使用方法 使用率 使用システム 使用量の合計

問題	次の操作を実行します
設定ページの手順に従っても、Data Infrastructure InsightsにDocker指標が表示されません。	Telegrafエージェントログで、次のエラーが報告されているかどうかを確認します。 来い! プラグイン[inputs.docker]のエラー：Dockerデーモンソケットに接続しようとしているときに権限が拒否されました もしそうなら、上記のようにTelegrafエージェントがDocker Unixソケットにアクセスできるようにするために必要な手順を実行します。

追加情報はから入手できます "サポート" ページ

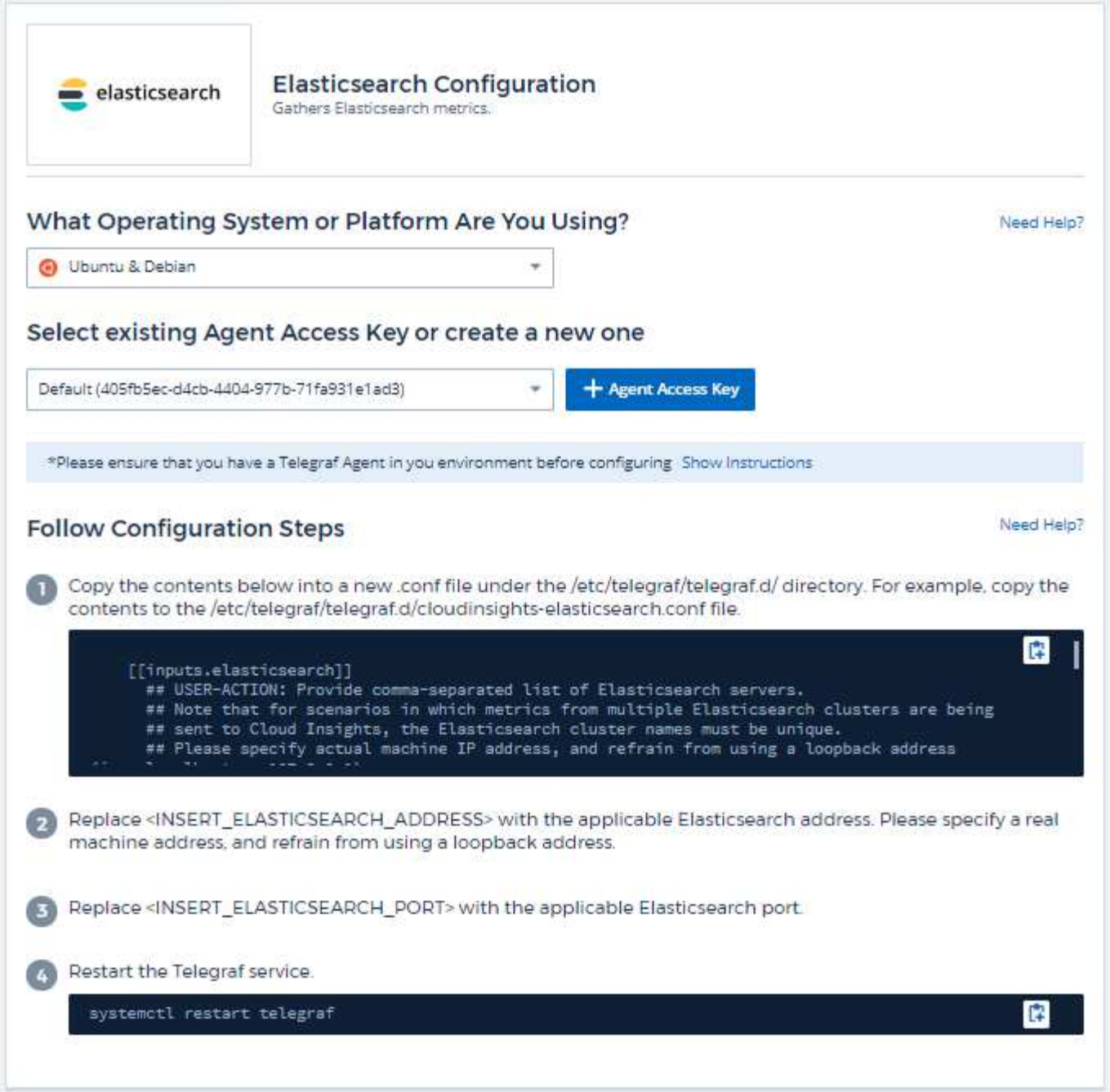
Elasticsearch Data Collector

Data Infrastructure Insightsは、このデータコレクタを使用してElasticsearchから指標を収集します。

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。[Elasticsearch]を選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順
3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

情報は、に記載されています "Elasticsearch のドキュメント"。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Elasticsearch クラスタ	ネームスペース クラスタ	ノードIP ノード名 クラスタのステータス	マスターノード数 合計ノード数 ファイルシステムの使用可能データ（バイト） ファイルシステムの空き容量（バイト） ファイルシステムデータ合計（バイト） JVMスレッド OS割り当て済みのプロセッサ OS利用可能なプロセッサ OSメモリ空き容量（バイト） OSメモリフリー OSメモリ合計（バイト） 使用済みOSメモリ（バイト） 使用されているOSメモリ プロセスCPU インデックス完了サイズ（バイト） インデックス数 インデックスドキュメント数 インデックスドキュメントが削除されました Indicesフィールドデータの削除 インデックスフィールドデータメモリサイズ（バイト） インデックスクエリキャッシュ数 インデックスキャッシュサイズ Indices Segments Countの略 インデックスセグメントドキュメント値メモリ（バイト） インデックスシャードインデックスプライマリー平均 インデックスシャードインデックスプライマリー最大 Indices shards Index Primaries Min インデックスシャードインデックスレプリケーション平均 インデックスシャードインデックスレプリケーシ

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Elasticsearch ノード	ネームスペース クラスタ ESノードID ESノードIP ESノード	ゾーン ID	機械学習が有効になりました 機械学習メモリ 機械学習の最大オープンジョブ数 X-Packがインストールされています ブレーカーアカウンティング推定サイズ（バイト） ブレーカーアカウンティング制限サイズ（バイト） ブレーカー会計オーバーヘッド ブレーカー会計が作動しました ブレーカーフィールドデータ推定サイズ（バイト） ブレーカーフィールドのデータ制限サイズ（バイト） ブレーカフィールドデータオーバーヘッド ブレーカーフィールドデータがトリップしました ブレーカの飛行中の推定サイズ（バイト） ブレーカインフライト制限サイズ（バイト） ブレーカインフライトオーバーヘッド ブレーカインフライトが停止しました ブレーカ親推定サイズ（バイト） ブレーカ親制限サイズ（バイト） Breakers親の頭上 ブレーカの親がトリップしました ブレーカー要求推定サイズ（バイト） ブレーカー要求制限サイズ（バイト） ブレーカー要求オーバーヘッド ブレーカー要求が作動しました ファイルシステムの使用可能データ（バイト） ファイルシステムの空き容量（バイト）

トラブルシューティング

追加情報はから入手できます "サポート" ページ

Flink Data Collector の使用

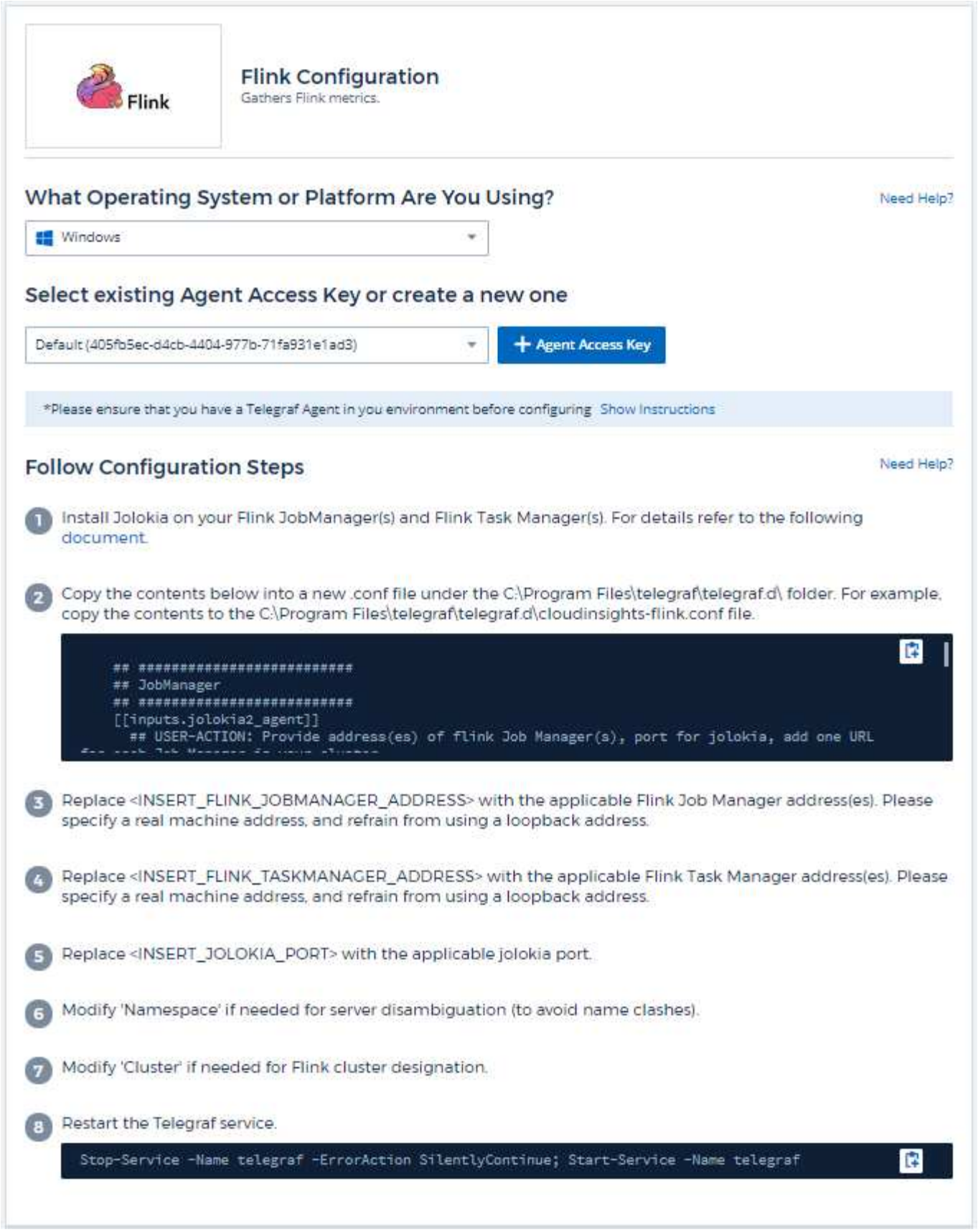
Data Infrastructure Insightsは、このデータコレクタを使用してFlinkから指標を収集します。

インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。[Flink]を選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順
3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

フルリンク展開では、次のコンポーネントが使用されます。

JobManager ： Flink プライマリシステム。一連の TaskManager を調整しますハイアベイラビリティ設定では、システムに複数の JobManager が存在します。
TaskManager ： Flink 演算子が実行される場所です。
Flink プラグインは、テレグラムの Jolokia プラグインに基づいています。すべての Flink コンポーネントから情報を収集するための要件など、 JMX はすべてのコンポーネントで Jolokia を介して設定および公開する必要があります。

互換性

Flink バージョン 1.7.0 に対して設定が開発されました。

セットアップ中です

Jolokia エージェント **JAR**

個々のコンポーネントについては、 Jolokia エージェント jar ファイルのバージョンをダウンロードする必要があります。テスト対象のバージョンは、でした "Jolokia 代理店 1.6.0"。

以下の手順では、ダウンロードした jar ファイル（ jolokia-jvm-1.6.0-agent.jar ）が「 /opt/Flink/lib/' 」の下に配置されると想定しています。

JobManager

JobManager で Jolokia API を公開するように設定するには、ノードで次の環境変数を設定して JobManager を再起動します。

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-agent.jar=port=8778,host=0.0.0.0"
```

Jolokia （ 8778 ）には別のポートを選択できます。Jolokia をロックする内部 IP を持っている場合は、「 catch all 」 0.0.0.0 を自分の IP で置き換えることができます。この IP には、テレグラムプラグインからアクセスできる必要があります。

TaskManager の略

Jolokia API を公開するように TaskManager を設定するには ' ノードに次の環境変数を設定し 'TaskManager を再起動します

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-agent.jar=port=8778,host=0.0.0.0"
```

Jolokia （ 8778 ）には別のポートを選択できます。Jolokia をロックする内部 IP を持っている場合は、「 catch all 」 0.0.0.0 を自分の IP で置き換えることができます。この IP には、テレグラムプラグインからアクセスできる必要があります。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Flink タスクマネージャ	クラスタ ネームスペース サーバ	ノード名 タスクマネージャID ノードIP	Network Available Memory Segmentsの略 Network Total Memory Segmentsの略 ガベージコレクションPS MarkSweep数 ガベージコレクションPS MarkSweep Timeの略 ガベージコレクションPS スカベンジ数 ガベージコレクションPS スカベンジ時間 ヒープメモリがコミットされました ヒープメモリの初期化 ヒープメモリ最大 ヒープメモリ使用済み スレッドカウントデーモン スレッド数のピーク スレッド数 スレッド数合計が開始されました
フリンクジョブ	クラスタ ネームスペース サーバ ジョブ ID	ノード名 ジョブ名 ノードIP Last Checkpoint External Pathの略 再起動時間	ダウンタイム 完全に再起動します 前回のチェックポイントアライメントがバッファリングされました 前回のチェックポイント期間 前回のチェックポイントサイズ 完了したチェックポイントの数 失敗したチェックポイントの数 進行中のチェックポイントの数 チェックポイントの数 アップタイム

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Flink ジョブマネージャー	クラスタ ネームスペース サーバ	ノード名 ノードIP	ガベージコレクションPS MarkSweep数 ガベージコレクションPS MarkSweep Timeの略 ガベージコレクションPS スカベンジ数 ガベージコレクションPS スカベンジ時間 ヒープメモリがコミットされました ヒープメモリの初期化 ヒープメモリ最大 ヒープメモリ使用済み 登録されているタスクマネージャの数 実行中のジョブの数 使用可能なタスクスロット タスクスロットの合計 スレッドカウントデーモン スレッド数のピーク スレッド数 スレッド数合計が開始されました

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Flink タスク	クラスタ ネームスペース ジョブ ID タスク ID	サーバ ノード名 ジョブ名 サブタスクインデックス タスク試行ID タスク試行番号 タスク名 タスクマネージャID ノードIP Current Input Watermarkの略	Pool Usageのバッファ Buffers in Queue Lengthの略 Buffers Out Pool Usageの略 バッファアウトキュー長 ローカルのバッファ数 Number Buffers in Local Per Secondカウント ローカル/秒レートのバッファ数 リモートのNumber Buffers（バッファ数） Number Buffers in Remote Per Second（リモート/秒）カウント Number Buffers in Remote Per Second Rate（リモート/秒レート） Number Buffers Outの略 Number Buffers Out Per Secondカウント Number Buffers Out Per Second Rateの略 ローカルのバイト数 1秒あたりのローカルバイト数 ローカル/秒レートのバイト数 リモートのバイト数 1秒あたりのリモートバイト数 Remote Per Second Rateのバイト数 送信されたバイト数 Number Bytes Out Per Second Count（1秒 1秒あたりの送信バイト数レート のレコード数 1秒あたりのレコード数 1秒あたりのレコード数 レコード数が出ている Number Records Out Per Second Countの略 Number Records Out Per Second Rateの略

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Flink タスクオペレータ	クラスタ ネームスペース ジョブ ID オペレータID タスク ID	サーバ ノード名 ジョブ名 演算子名 サブタスクインデックス タスク試行ID タスク試行番号 タスク名 タスクマネージャID ノードIP	Current Input Watermarkの略 Current Output Watermarkの略 のレコード数 1秒あたりのレコード数 1秒あたりのレコード数 レコード数が出ている Number Records Out Per Second Countの略 Number Records Out Per Second Rateの略 遅延レコード数がドロップされました 割り当て済みパーティション Bytes Consumed Rate コミットレイテンシの平均 コミットレイテンシ最大 コミット率 コミットに失敗しました コミットに成功しました 接続完了率 接続数 接続作成レート カウント フェッチレイテンシの平均 フェッチレイテンシの最大値 フェッチレート 取得サイズ平均 フェッチサイズ最大 フェッチスロットル時間平均 フェッチスロットル時間最大 ハートビートレート 受信バイトレート IO比率 IO時間の平均（ns） IO待機比率 IO待機時間の平均（ns） 参加率 ジョイン時間平均 前回のハートビート前 Network IO Rateの略 Outgoing Byte Rateの略 レコード消費率 最大遅延レコード リクエストあたりのレコード平均 リクエスト率

トラブルシューティング

追加情報はから入手できます "サポート" ページ

Hadoop Data Collector

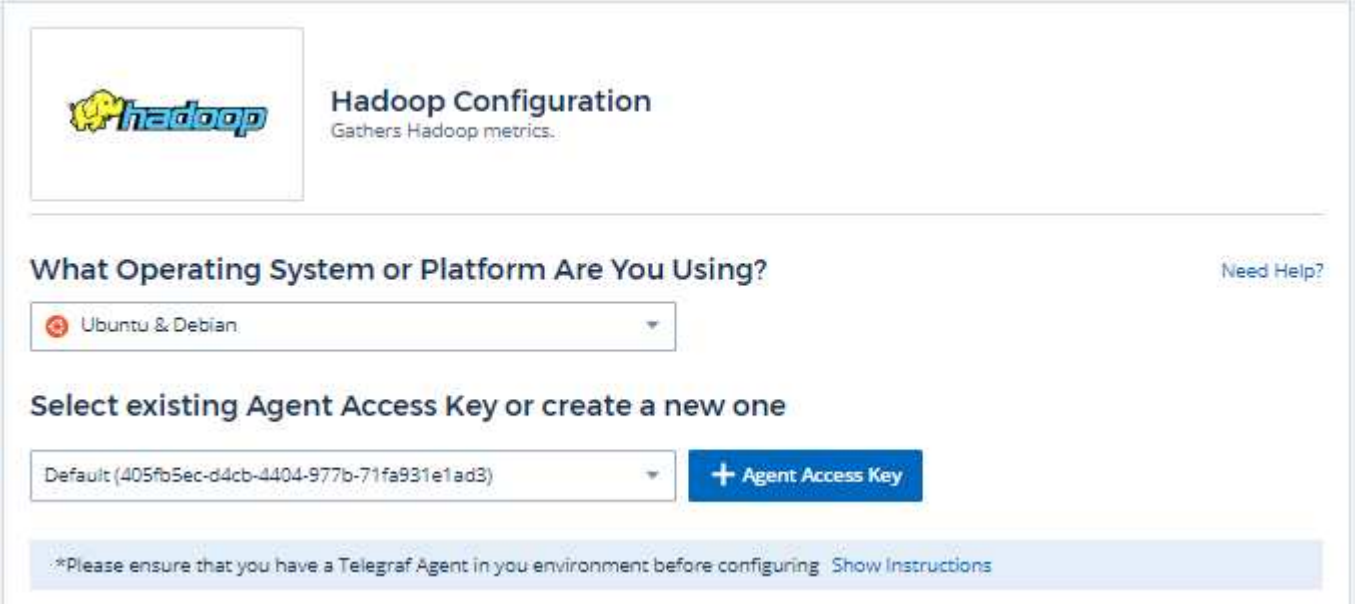
Data Infrastructure Insightsは、このデータコレクタを使用してHadoopから指標を収集します。

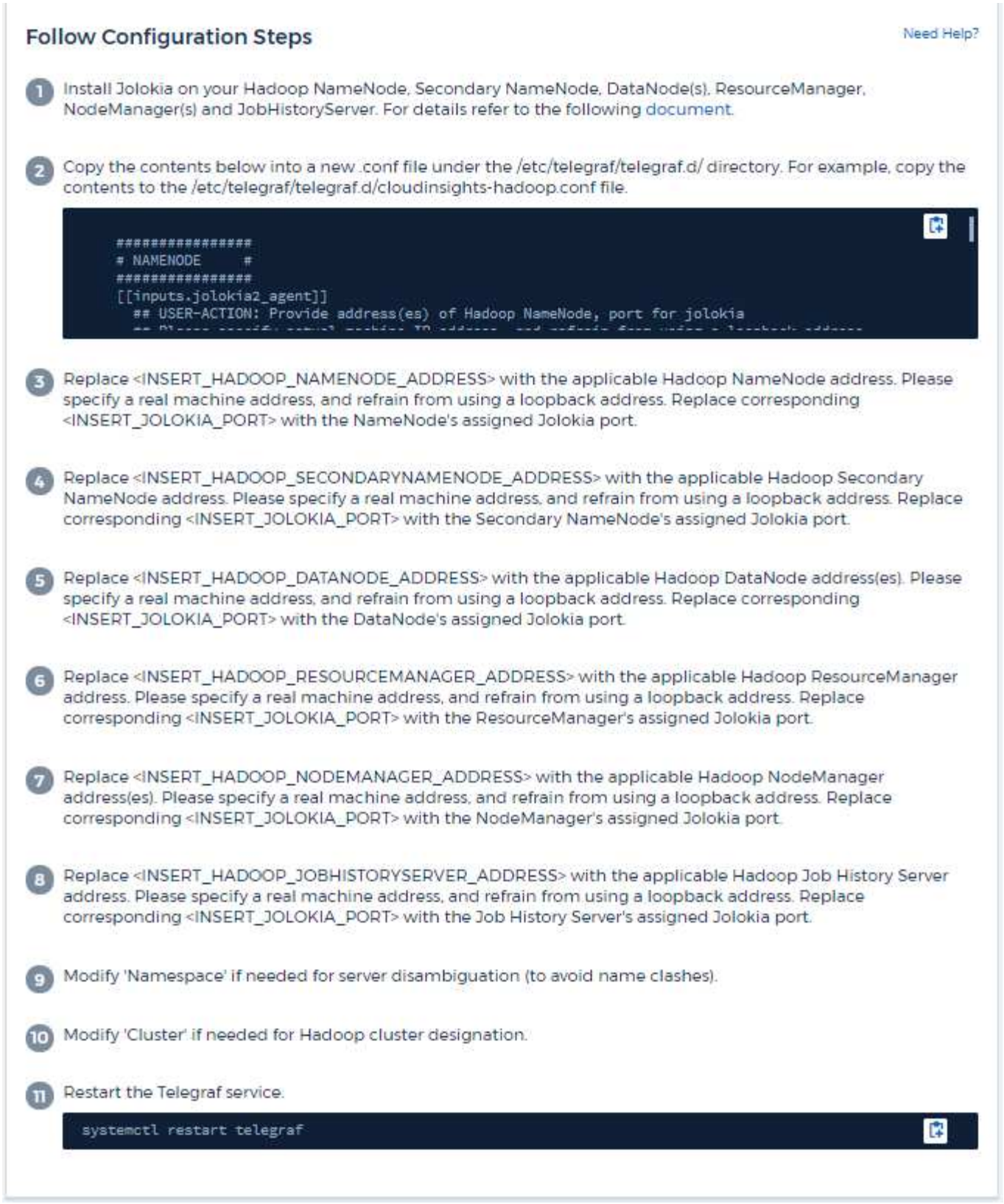
インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。Hadoopを選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順
3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。





セットアップ（ **Setup** ）

Hadoop を完全に導入するには、次のコンポーネントが必要です。

- NameNode ： Hadoop 分散型ファイルシステム（ HDFS ）プライマリシステム。一連の DataNode を調整します。

- セカンダリ NameNode ：メイン NameNode のウォームフェイルオーバー。Hadoop では、 NameNode への昇格は自動的には行われません。セカンダリ NameNode は、必要に応じてプロモート可能な状態にするために、 NameNode から情報を収集します。
- DataNode ：データの実際の所有者。
- ResourceManager ：コンピューティングのプライマリシステム（ yarn ）。一連の NodeManager を調整します。
- NodeManager ：コンピューティング用のリソース。アプリケーションを実行するための実際の場所。
- JobHistoryServer ：ジョブ履歴に関連するすべての要求の処理を担当します。

Hadoop プラグインは、テレグラムの Jolokia プラグインに基づいています。すべての Hadoop コンポーネントから情報を収集するための要件など、 JMX はすべてのコンポーネントで Jolokia 経由で設定および公開する必要があります。

互換性

構成は Hadoop バージョン 2.9.2 に対して開発されました。

セットアップ中です

Jolokia エージェント JAR

個々のコンポーネントについては、 Jolokia エージェント jar ファイルのバージョンをダウンロードする必要があります。テスト対象のバージョンは、でした "Jolokia 代理店 1.6.0"。

以下の手順では、ダウンロードした jar ファイル（ jolokia-jvm-1.6.0-agent.jar ）が「 /opt/hadoop /lib/' 」の下に配置されると想定しています。

NameNode

Jolokia API が公開されるように NameNode を設定するには、 <hadoop home>/etc/hadoop /hadoop -env.sh で次のセットアップを行います。

```
export HADOOP_NAMENODE_OPTS="$HADOOP_NAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7800,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8000
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8000 above) and Jolokia (7800).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

セカンダリ **NameNode**

セカンダリ NameNode で Jolokia API を公開するように設定するには、 <hadoop home>/etc/hadoop /hadoop -env.sh で次のように設定します。

```
export HADOOP_SECONDARYNAMENODE_OPTS="$HADOOP_SECONDARYNAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7802,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8002
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8002 above) and Jolokia (7802).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

DataNode

Jolokia API が公開されるように DataNode を設定するには、 <hopp_home>/etc/hadoop /hadoop -env.sh に以下のセットアップを行います。

```
export HADOOP_DATANODE_OPTS="$HADOOP_DATANODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7801,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8001
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8001 above) and Jolokia (7801).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

ResourceManager の略

ResourceManager で Jolokia API を公開するように設定するには、 <hadoop HOME>//etc/hadoop /hadoop -env.sh で次の設定を行うことができます。

```
export YARN_RESOURCEMANAGER_OPTS="$YARN_RESOURCEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7803,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8003
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8003 above) and Jolokia (7803).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

NodeManager

Jolokia API を公開するように NodeManager を設定するには、 <hadoop home>/etc/hadoop /hadoop -env.sh で次の設定を行うことができます。

```
export YARN_NODEMANAGER_OPTS="$YARN_NODEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7804,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8004
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8004 above) and Jolokia (7804).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

JobHistoryServer

JobHistoryServer で Jolokia API を公開するように設定するには、 <hadoop home>/etc/hadoop /hadoop -env.sh で次の設定を行うことができます。

```
export HADOOP_JOB_HISTORYSERVER_OPTS="$HADOOP_JOB_HISTORYSERVER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7805,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8005
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8005 above) and Jolokia (7805).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Hadoop セカンダリ NameNode	クラスタ ネームスペース サーバ	ノード名 ノードIP コンパイル情報 バージョン	GCカウント GCコピー数 GCマークスイープコンパクトカウント GC番号情報のしきい値を超えました GC番号警告しきい値を超えました GC時間 GCコピー時間 GCマークスイープコンパクト時間 GC合計エクストラスリープ時間 エラー数をログに記録します ログ致命的数 ログ情報数 警告数をログに記録します メモリヒープがコミットされました メモリヒープ最大 使用されているメモリヒープ メモリ最大 メモリのヒープがコミットされていません メモリ非ヒープ最大 メモリのヒープが使用されていません ブロックされたスレッド スレッド新規 スレッド実行可能 スレッドが終了しました スレッドの待機時間 待機中のスレッド

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Hadoop ノードマネージャ	クラスタ ネームスペース サーバ	ノード名 ノードIP	割り当て済みのコンテナ メモリ割り当て Memory Allocated Oportunisticの略 仮想コア割り当てオポチュニスティック 仮想コアが割り当てられました 使用可能なメモリ 使用可能な仮想コア ディレクトリがローカルではありません ディレクトリの不正なログ クリーニング前のキャッシュサイズ コンテナ起動時間平均時間 Container Launch Duration Number of Operations（コンテナ起動時間） コンテナが完了しました コンテナが失敗しました コンテナの初期化 コンテナを強制終了します コンテナをリリース コンテナの再構築 障害発生時にコンテナがロールバックされました 実行中のコンテナ ディスク使用率が良好なローカルディレクトリ Disk Utilization Good Log Directoriesの略 バイトがプライベート削除されました Bytes Deleted Public コンテナはOpportunityを実行しています 削除されたバイト数の合計 接続をシャッフルします 出力バイトをシャッフルします 出力のシャッフルに失敗しました シャッフル出力OK GCカウント GCコピー数 GCマークスイープコンパクトカウント GC番号情報のしきい値を

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Hadoop ResourceManager	クラスタ ネームスペース サーバ	ノード名 ノードIP	ApplicationMaster起動遅延平均 ApplicationMaster起動遅延番号 ApplicationMaster登録遅延平均 ApplicationMaster Register Delay Numberの略 NodeManagerアクティブ番号 NodeManagerの運用停止番号 NodeManagerの運用停止番号 NodeManagerの番号が失われました NodeManagerがリブートしました NodeManagerシャットダウン番号 NodeManagerの正常な番号 NodeManagerのメモリ制限 NodeManager仮想コア数の制限 使用済み容量 アクティブアプリケーション アクティブユーザー 割り当て済みアグリゲートコンテナ アグリゲートコンテナがプリエンプトされました アグリゲートコンテナが解放されました アグリゲートメモリの秒数がプリエンプトされました 割り当て済みアグリゲートノードのローカルコンテナ アグリゲートオフスイッチコンテナの割り当て済み アグリゲートのAckローカルコンテナの割り当て済み容量 アグリゲート仮想コア（秒）がプリエンプトされました 割り当て済みのコンテナ 割り当てられたメモリ

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Hadoop DataNode	クラスタ ネームスペース サーバ	ノード名 ノードIP クラスタID バージョン	トランシーバ数 送信が進行中です キャッシュ容量 使用されているキャッシュ 容量 使用されるDFS 推定損失合計容量 前回のボリューム障害率 キャッシュされた番号をブロックする ブロック番号のキャッシュに失敗しました ブロック番号のキャッシュ解除に失敗しました ボリューム番号に失敗しました 残り容量 GCカウント GCコピー数 GCマークスイープコンパクトカウント GC番号情報のしきい値を超えました GC番号警告しきい値を超えました GC時間 GCコピー時間 GCマークスイープコンパクト時間 GC合計エクストラスリープ時間 エラー数をログに記録します ログ致命的数 ログ情報数 警告数をログに記録します メモリヒープがコミットされました メモリヒープ最大 使用されているメモリヒープ メモリ最大 メモリのヒープがコミットされていません メモリ非ヒープ最大 メモリのヒープが使用されていません ブロックされたスレッド スレッド新規 スレッド実行可能 スレッドが終了しました スレッドの待機時間

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Hadoop NameNode	クラスタ ネームスペース サーバ	ノード名 ノードIP 最後に書き込まれたトランザクションID 最後にロードされた編集からの時間 HAの状態 File System Stateの略 ブロックプールID クラスタID コンパイル情報 個別のバージョン数 バージョン	ブロック容量 合計ブロック数 合計容量 使用済み容量 Capacity Used Non DFSの略 ブロックが壊れています 推定損失合計容量 超過をブロックします ハートビートの期限が切れました ファイル合計 File System Lock Queue Lengthの略 ブロックが見つかりません 第1因子のレプリケーションが欠落しているブロック クライアントがアクティブです データノードが故障しています 稼働を停止しているデータノードが故障しています ライブを運用停止するデータノード データノードの運用停止 暗号化ゾーン番号 データノードがメンテナンスに移行しています 作成中のファイル メンテナンス中のデータノードが停止しました データノードはメンテナンス中です Data Nodes Liveの略 ストレージが古い レプリケーション保留タイムアウト データノードメッセージが保留中です 削除を保留中のブロック レプリケーションを保留中のブロック ミスレプリケートされたブロックが延期されました スケジュールされたレプリケーションをブロックします Snapshot スナップショット可能な

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Hadoop ジョブ履歴サーバ	クラスタ ネームスペース サーバ	ノード名 ノードIP	GCカウント GCコピー数 GCマークスイープコンパクトカウント GC番号情報のしきい値を超えました GC番号警告しきい値を超えました GC時間 GCコピー時間 GCマークスイープコンパクト時間 GC合計エクストラスリープ時間 エラー数をログに記録します ログ致命的数 ログ情報数 警告数をログに記録します メモリヒープがコミットされました メモリヒープ最大 使用されているメモリヒープ メモリ最大 メモリのヒープがコミットされていません メモリ非ヒープ最大 メモリのヒープが使用されていません ブロックされたスレッド スレッド新規 スレッド実行可能 スレッドが終了しました スレッドの待機時間 待機中のスレッド

トラブルシューティング

追加情報はから入手できます "サポート" ページ

HAProxy Data Collector

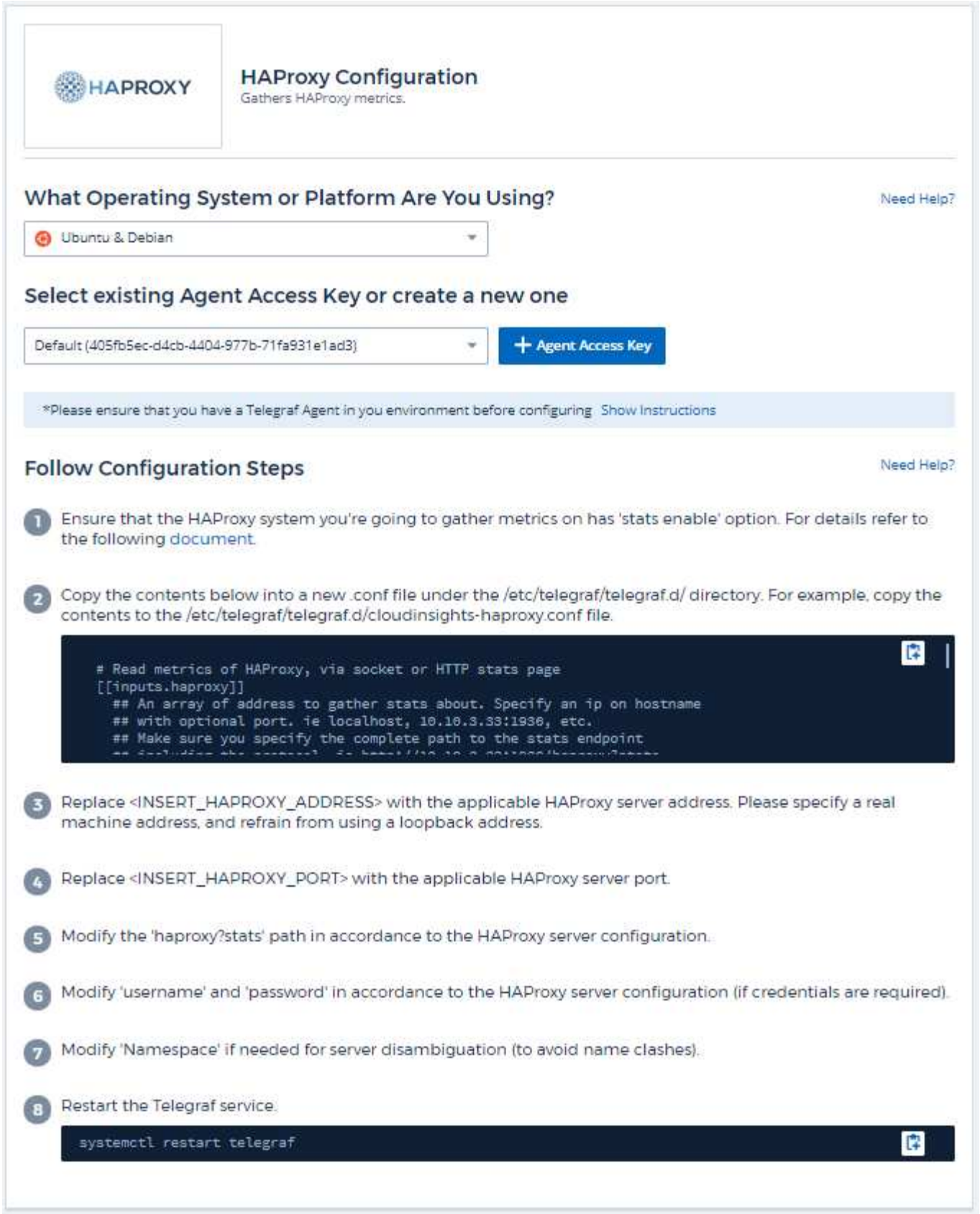
Data Infrastructure Insightsは、このデータコレクタを使用してHAProxyから指標を収集します。

インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。[HAProxy]を選択します。

Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順
3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

Telegraf の HAProxy 用プラグインは、 HAProxy Stats の有効化に依存しています。これは HAProxy に組み込まれている構成ですが、すぐに有効にすることはできません。有効にすると 'HAProxy はブラウザで表示でき

る HTML エンドポイントを公開したり ' すべての HAProxy 構成のステータスを抽出するためにスクレイピングしたりできます

互換性：

構成は HAProxy バージョン 1.9.4 に対して開発されました。

設定：

統計情報を有効にするには、 haproxy 設定ファイルを編集し、「金庫」セクションの後に次の行を追加します。この行には、ユーザー自身のユーザー名とパスワード、および / または haproxy URL を使用します。

```
stats enable
stats auth myuser:mypassword
stats uri  /haproxy?stats
```

次に、 stats を有効にした単純な構成ファイルの例を示します。

```
global
  daemon
  maxconn 256

defaults
  mode http
  stats enable
  stats uri /haproxy?stats
  stats auth myuser:mypassword
  timeout connect 5000ms
  timeout client 50000ms
  timeout server 50000ms

frontend http-in
  bind *:80
  default_backend servers

frontend http-in9080
  bind *:9080
  default_backend servers_2

backend servers
  server server1 10.128.0.55:8080 check ssl verify none
  server server2 10.128.0.56:8080 check ssl verify none

backend servers_2
  server server3 10.128.0.57:8080 check ssl verify none
  server server4 10.128.0.58:8080 check ssl verify none
```

最新の手順の詳細については、を参照してください "HAProxy のドキュメント"。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
HAProxy フロントエンド	ネームスペース 住所 プロキシ	ノードIP ノード名 プロキシID モード プロセスID セッションレート制限 サーバID セッション制限 ステータス	受信バイト数 バイトアウト キャッシュヒット キャッシュルックアップ 圧縮バイトがバイパスされました 圧縮バイト数 圧縮バイトが送信されました 圧縮応答 接続レート 接続レート最大 接続合計 接続ルールによって拒否された要求 セキュリティ上の懸念により拒否されたリクエスト セキュリティ上の懸念により拒否された応答 セッションルールによって拒否された要求 エラーを要求します 応答1xx 応答は2xx 応答は3xx 応答は4xx 応答は5xx 応答その他 要求が傍受されました セッションレート セッションレート最大 リクエスト率 要求レート最大 リクエストの合計 セッション セッションの最大数 セッションの合計 書き換えを要求します

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
HAProxy サーバ	ネームスペース 住所 プロキシ サーバ	ノードIP ノード名 完了までの時間を確認します フォール設定を確認します 健全性の値を確認します 立ち上がり設定を確認します ステータスを確認します プロキシID 最終変更時刻 前回のセッション時間 モード プロセスID サーバID ステータス 重量	アクティブサーバ バックアップサーバ 受信バイト数 バイトアウト チェックダウン チェックに失敗しました クライアントが中止されました 接続 接続平均時間 ダウンタイムの合計 拒否された応答 接続エラー 応答エラー 応答1xx 応答は2xx 応答は3xx 応答は4xx 応答は5xx 応答その他 サーバ選択合計 キューの現在 キューの最大数 キュー平均時間 1秒あたりのセッション数 1秒あたりのセッションの最大数 接続の再利用 応答時間平均 セッション セッションの最大数 サーバ転送が中止されます セッションの合計 セッション合計時間平均 再ディスパッチを要求します 再試行を要求します 書き換えを要求します

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
HAProxy バックエンド	ネームスペース 住所 プロキシ	ノードIP ノード名 プロキシID 最終変更時刻 前回のセッション時間 モード プロセスID サーバID セッション制限 ステータス 重量	アクティブサーバ バックアップサーバ 受信バイト数 バイトアウト キャッシュヒット キャッシュルックアップ チェックダウン クライアントが中止されました 圧縮バイトがバイパスされました 圧縮バイト数 圧縮バイトが送信されました 圧縮応答 接続 接続平均時間 ダウンタイムの合計 セキュリティ上の懸念により拒否されたリクエスト セキュリティ上の懸念により拒否された応答 接続エラー 応答エラー 応答1xx 応答は2xx 応答は3xx 応答は4xx 応答は5xx 応答その他 サーバ選択合計 キューの現在 キューの最大数 キュー平均時間 1秒あたりのセッション数 1秒あたりのセッションの最大数 リクエストの合計 接続の再利用 応答時間平均 セッション セッションの最大数 サーバ転送が中止されます セッションの合計 セッション合計時間平均 再ディスパッチを要求します 再試行を要求します 書き換えを要求します

トラブルシューティング

追加情報はから入手できます "サポート" ページ

JVM Data Collector （ JVM データ収集）

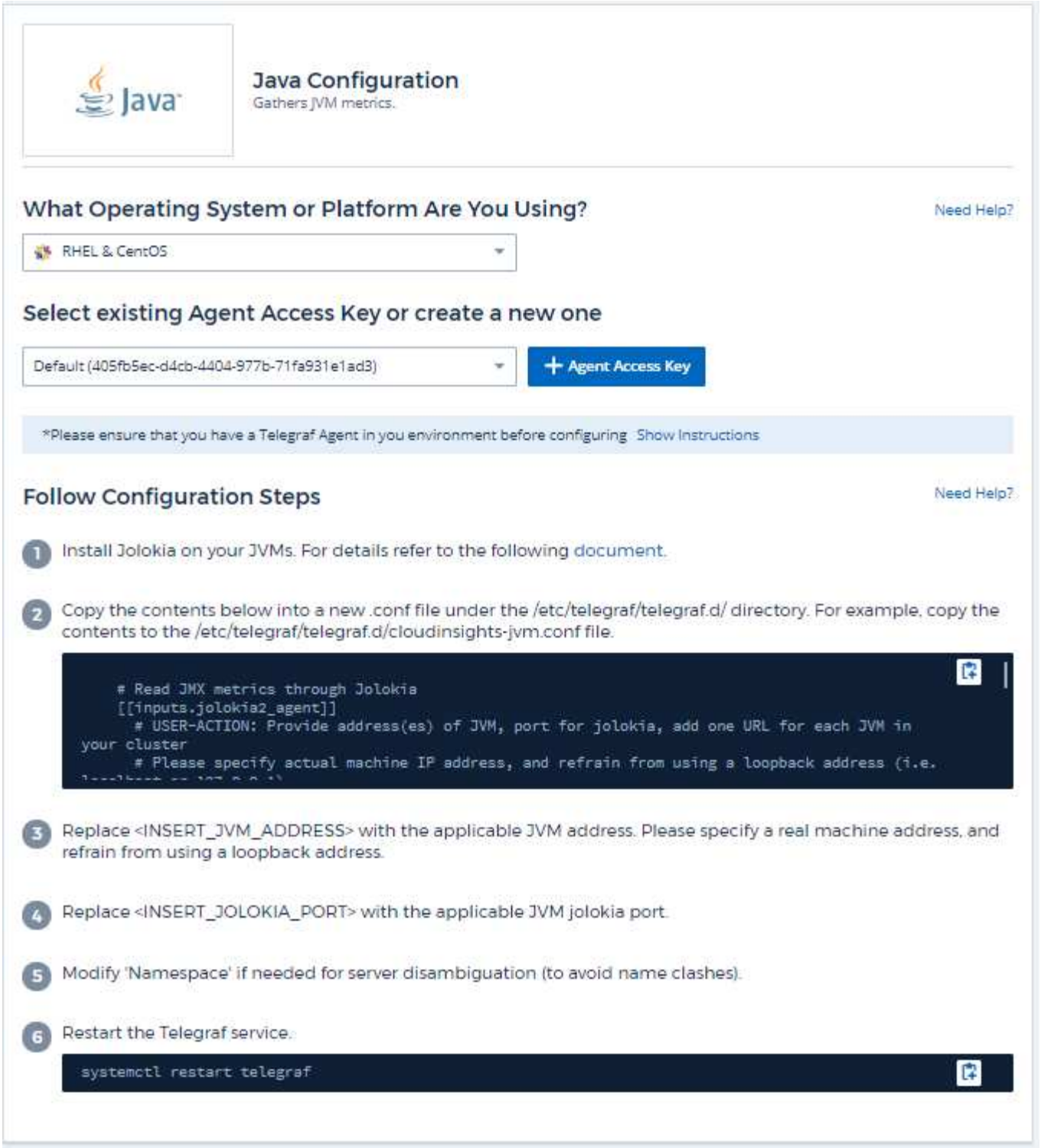
Data Infrastructure Insightsは、このデータコレクタを使用してJVMから指標を収集します。

インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。JVMを選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順
3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

情報については、を参照してください "JVMのドキュメント"。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
JVM	ネームスペース JVM	OSアーキテクチャ OS名 OSバージョン ランタイム仕様 ランタイム仕様ベンダー ランタイム仕様バージョン アップタイム ランタイムVM名 ランタイムVMベンダー ランタイムVMバージョン ノード名 ノードIP	クラスが読み込まれました クラスロード合計 クラスがアンロードされました メモリヒープがコミットされました メモリヒープ初期化 使用メモリヒープの最大値 使用されているメモリヒープ メモリのヒープがコミットされていません メモリ非ヒープ初期化 メモリ非ヒープ最大 メモリのヒープが使用されていません Memory Objects Pending Finalizationの略 OSプロセッサが使用可能です OS Committed Virtual Memory Sizeの略 OS Free Physical Memory Sizeの略 OS Free Swap Space Size（OS空きスワップスペースサイズ） OS最大ファイル記述子数 OS Open File Descriptors Count（OSオープンファイル記述子数） OSプロセッサCPU負荷 OSプロセッサCPU時間 OSシステムCPU負荷 OSシステム負荷平均 OS合計物理メモリサイズ [OS Total Swap Space Size]をクリックします スレッドデーモン数 スレッドのピーク数 スレッド数 スレッド合計開始数 ガベージコレクタコピーコレクション数 ガベージコレクタのコピー収集時間 ガベージコレクタマーク-スイープ収集数 ガベージコレクタマークスイープ収集時間 ガベージコレクタG1旧世代コレクション数

トラブルシューティング

追加情報はから入手できます "サポート" ページ

Kafka Data Collector の利用

Data Infrastructure Insightsは、このデータコレクタを使用してKafkaから指標データを収集します。

インストール

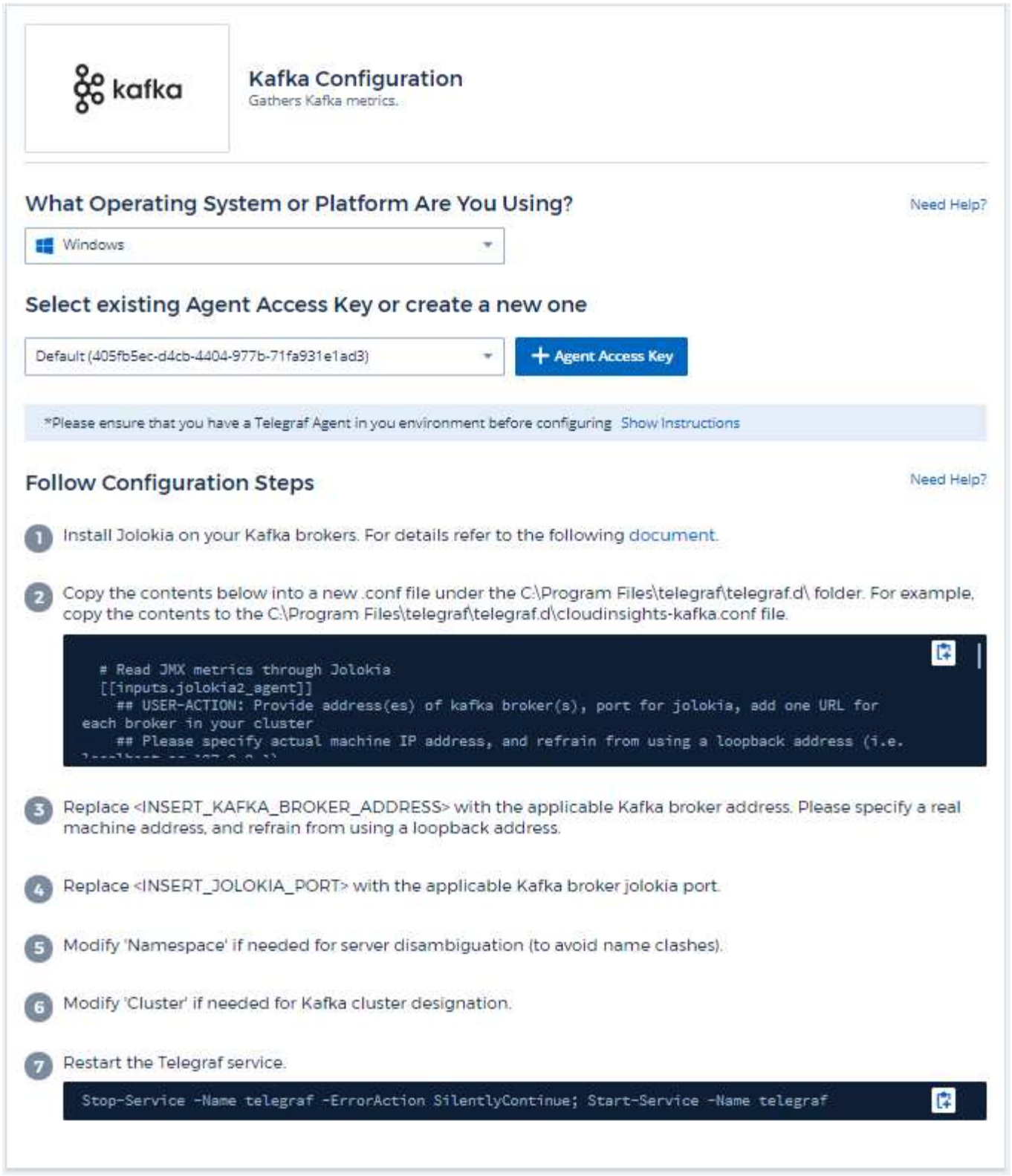
1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。Kafkaを選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順

3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。

4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

Kafka プラグインは、テレグラムの Jolokia プラグインに基づいています。すべての Kafka ブローカーから情報を収集する必要があるため、 JMX はすべてのコンポーネントで Jolokia 経由で設定および公開する必要があります。

互換性

Kafka バージョン 0.11.0.2 の構成向けに開発されました。

セットアップ中です

以下の手順はすべて、 Kafka のインストール場所が「 /opt/Kafka 」であることを前提としています。以下の手順を使用して、設置場所を変更できます。

Jolokia エージェント JAR

Jolokia エージェント jar ファイルのバージョン "ダウンロードしました"。テスト対象のバージョンは Jolokia エージェント 1.6.0 でした。

以下の手順では、ダウンロードした jar ファイル（ jolokia-jvm-1.6.0-agent.jar ）が「 /opt/Kafka/libs/' 」の下に配置されると想定しています。

Kafka Brokers のようになります

Kafka Brokers で Jolokia API を公開するように設定するには、「 Kafka -run-class.sh 」コールの直前に、<Kafka_home>/bin/Kafka-server-start.sh に次の項目を追加します。

```
export JMX_PORT=9999
export RMI_HOSTNAME=`hostname -I`
export KAFKA_JMX_OPTS="-javaagent:/opt/kafka/libs/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0
-Dcom.sun.management.jmxremote.password.file=/opt/kafka/config/jmxremote.p
assword -Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname=$RMI_HOSTNAME
-Dcom.sun.management.jmxremote.rmi.port=$JMX_PORT"
```

上記の例では 'hostname-i' を使用して 'RMI_HOSTNAME' 環境変数を設定しています。複数の IP マシンでは、 RMI 接続に使用する IP を収集するために、これを調整する必要があります。

JMX (9999 以上) とジョロキア (8778) には別のポートを選択できますJolokia をロックする内部 IP を持っている場合は、「 catch all 」 0.0.0.0 を自分の IP で置き換えることができます。この IP には、テレグラムプラグインからアクセスできる必要があります。認証を行わない場合は、オプション「 -Dcom.sun.management.jmxremote.authenticate=false' 」を使用できます。自己責任で使用してください。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Kafka Broker	クラスタ ネームスペース ブローカー	ノード名 ノードIP	レプリカマネージャフェッチャー最大遅延 Zookeeperクライアント接続 ZooKeeperクライアント接続（15mレート） ZooKeeperクライアント接続（5mレート） ZooKeeperクライアント接続（平均速度） ZooKeeperクライアント接続（1mレート） レプリカマネージャのパーティション数 スレッドカウントデーモン スレッド数のピーク 現在のスレッド数 スレッド数合計が開始されました オフラインパーティション Produce Requests Total Time（50パーセンタイル値） Produce Requests Total Time（75パーセンタイル値） Produce Requests Total Time（95パーセンタイル値） Produce Requests Total Time（98パーセンタイル値） Produce Requests Total Time（999パーセンタイル値） Produce Requests Total Time（99パーセンタイル値） Produce Requests Total Timeの略 Produce Requests Total Time Max Produce Requests Total Time Meanの略 Produce Requests Total Time Min Produce Requests Total Time stddev レプリカマネージャISRが縮小されます レプリカ・マネージャのISRが縮小（15mレート

トラブルシューティング

追加情報はから入手できます "サポート" ページ

Kibana データコレクタ

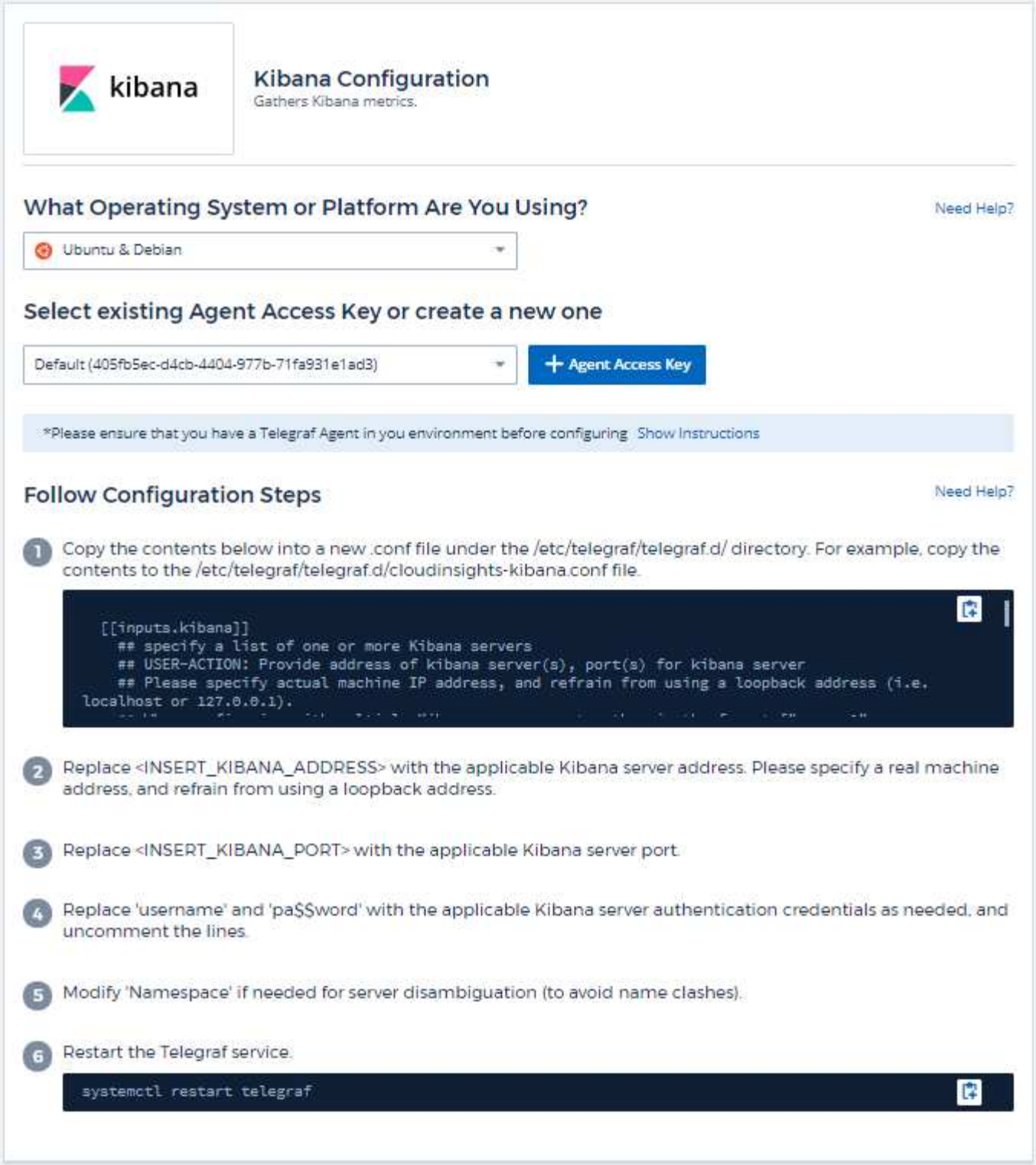
Data Infrastructure Insightsでは、このデータコレクタを使用してKibanaから指標データを収集します。

インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。「きばな」を選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順
3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

情報は、に記載されています "Kibana のドキュメンテーション"。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
キバナ	ネームスペース 住所	ノードIP ノード名 バージョン ステータス	同時接続 ヒープ最大 ヒープが使用されました 1秒あたりの要求数 応答時間平均 最大応答時間 アップタイム

トラブルシューティング

追加情報はから入手できます "サポート" ページ

Kubernetes Monitoring Operatorのインストールと設定

Data Infrastructure Insightsは、Kubernetesコレクション向けの「Kubernetes Monitoring Operator」を提供しています。新しいオペレータを導入するには、* Kubernetes > Collectors >+ Kubernetes Collector *に移動します。

Kubernetes Monitoring Operatorをインストールする前に

を参照してください "前提条件" Kubernetes Monitoring Operatorをインストールまたはアップグレードする前のドキュメント。

Kubernetes Monitoring Operatorのインストール

kubernetes
Kubernetes

Deploy NetApp Monitoring Operator

Quickly install and configure a Kubernetes Operator to send cluster information to Cloud Insights.

Select existing API Access Token or create a new one

KEY2024 (...vw6NdM) | + API Access Token | Production Best Practices

Installation Instructions

Need Help?

Please review the pre-requisites for installing the NetApp Kubernetes Monitoring Operator.
To update an existing operator installation please follow these steps.

1 Define Kubernetes cluster name and namespace

Provide the Kubernetes cluster name and specify a namespace for deploying the monitoring components.

Cluster	Namespace
clustername	netapp-monitoring

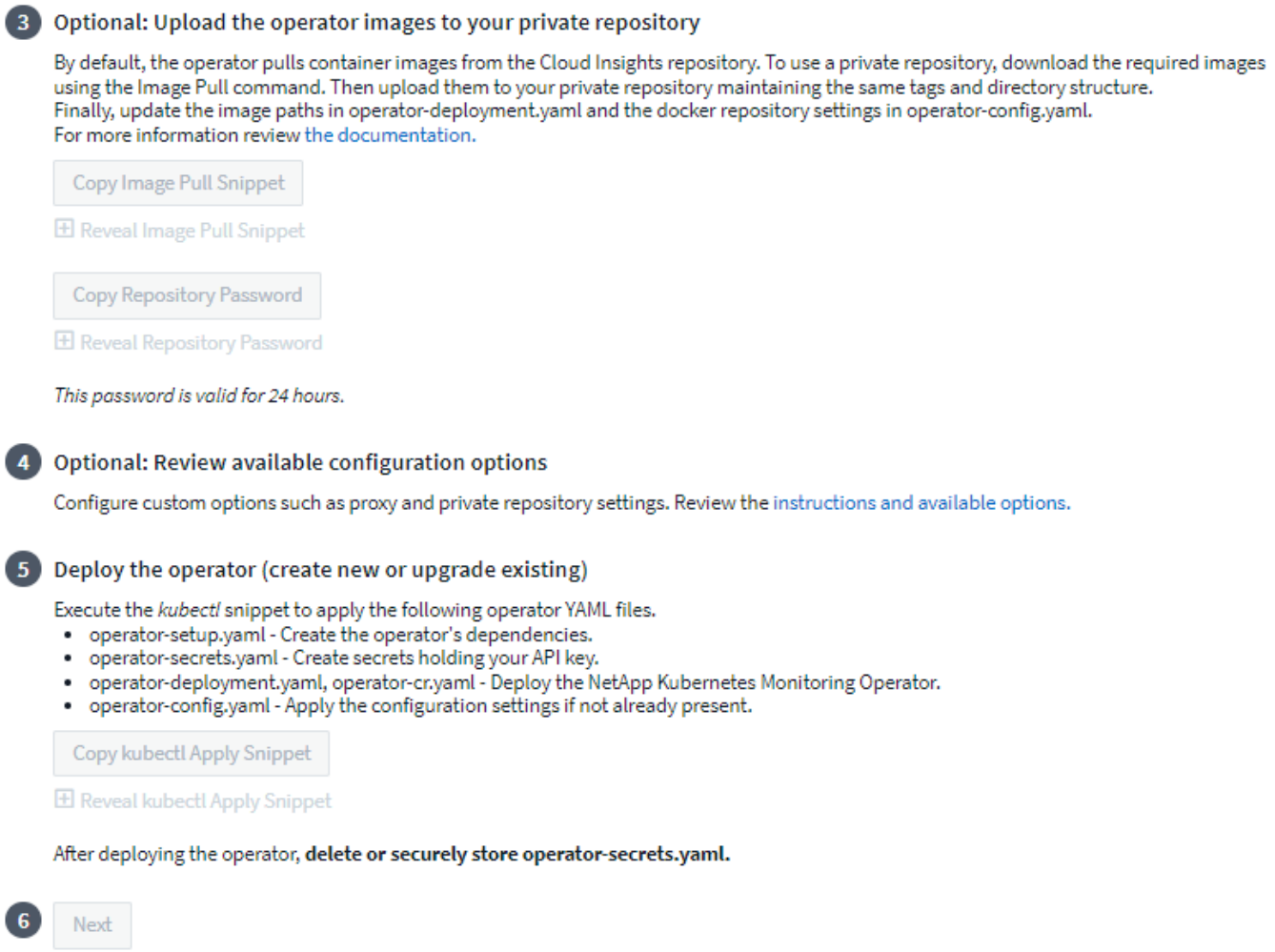
2 Download the operator YAML files

Execute the following download command in a *bash* prompt.

Copy Download Command Snippet

Reveal Download Command Snippet

This snippet includes a unique access key that is valid for 24 hours.



Kubernetesに**Kubernetes Monitoring Operator**エージェントをインストールする手順は次のとおりです。

1. 一意のクラスタ名およびネームスペースを入力してください。実行中の場合 をアップグレードして 以前のKubernetes Operatorで、同じクラスタ名とネームスペースを使用します。
2. これらを入力すると、ダウンロードコマンドスニペットをクリップボードにコピーできます。
3. スニペットを a_bash_window に貼り付け、実行します。Operatorインストールファイルがダウンロードされます。スニペットには固有のキーがあり、24時間有効です。
4. カスタムリポジトリまたはプライベートリポジトリがある場合は、オプションのImage Pullスニペットをコピーし、a_bash_shellに貼り付けて実行します。画像がプルされたら、プライベートリポジトリにコピーします。必ず同じタグとフォルダ構造を維持してください。_operator-deployment.yaml_のパスと_operator-config.yaml_のDockerリポジトリ設定を更新します。
5. 必要に応じて、プロキシやプライベートリポジトリの設定など、使用可能な設定オプションを確認します。あなたはについてもっと読むことができます "設定オプション"。
6. 準備ができたら、kubectl Applyスニペットをコピーしてダウンロードし、実行してOperatorをデプロイします。
7. インストールが自動的に開始されます。完了したら、[*Next*]ボタンをクリックします。
8. インストールが完了したら、[*Next*]ボタンをクリックします。また、_operator-secrets.yaml_fileを削除するか、安全に保存してください。

プロキシを使用している場合は、 プロキシを設定します。

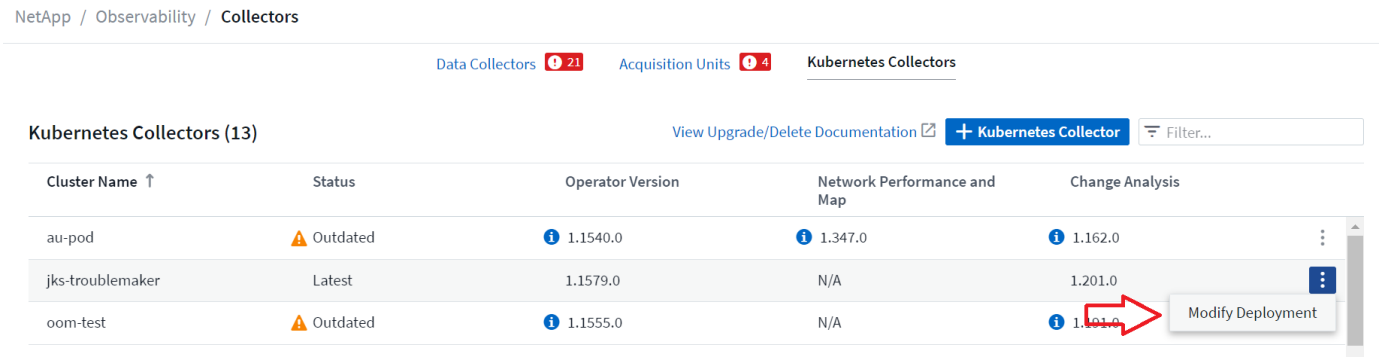
カスタムリポジトリをお持ちの場合は、 カスタム/プライベートDockerリポジトリを使用する。

Kubernetes監視コンポーネント

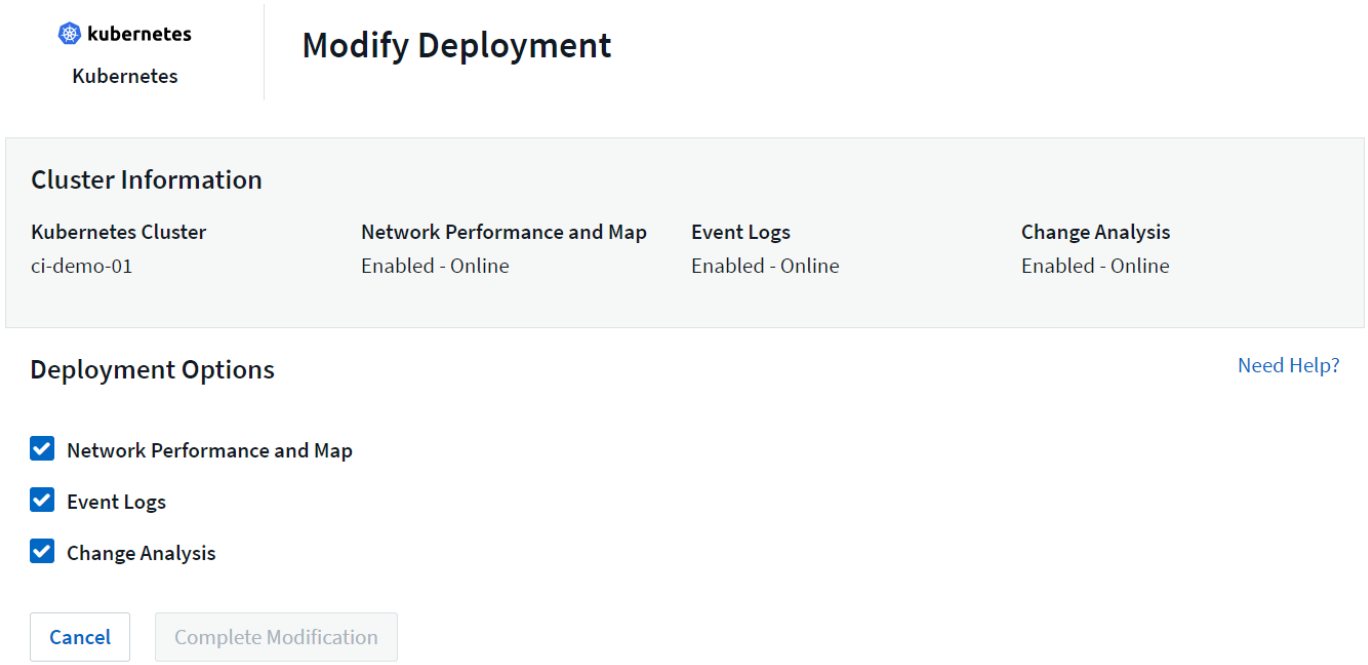
Data Infrastructure Insights Kubernetes Monitoringは、次の4つの監視コンポーネントで構成されます。

- クラスタ指標
- ネットワークパフォーマンスとマップ（オプション）
- イベントログ（オプション）
- 変更分析（オプション）

上記のオプションコンポーネントは、各Kubernetesコレクタに対してデフォルトで有効になっています。特定のコレクタ用のコンポーネントが必要ないと判断した場合は、* Kubernetes > Collectors *に移動し、画面右側のコレクタの「three dots」メニューから_Modify Deployment_を選択して無効にできます。



画面には各コンポーネントの現在の状態が表示され、必要に応じてそのコレクタのコンポーネントを無効または有効にすることができます。



をアップグレードして

最新の**Kubernetes Monitoring Operator**へのアップグレード

既存のOperatorにAgentConfigurationが存在するかどうかを確認します（ネームスペースがdefault_netapp-monitoring_でない場合は、適切なネームスペースに置き換えてください）。

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-monitoring-
configuration
AgentConfigurationが存在する場合：
```

- をインストールします 既存の演算子の上にある最新の演算子。
  - 確認してください 最新のコンテナイメージを取得します カスタムリポジトリを使用している場合。

AgentConfigurationが存在しない場合は、次の手順を実行します。

- クラスタ名がData Infrastructure Insightsで認識される名前であることをメモします（ネームスペースがデフォルトのNetApp監視機能でない場合は、適切なネームスペースで置き換えてください）。

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* 既存の
Operatorのバックアップを作成します（ネームスペースがデフォルトのネットアップ監視機能になっていない場合は、適切なネームスペースで置き換えてください）。
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-operator,をアンインストールします>>
既存の演算子。
* <<installing-the-kubernetes-monitoring-operator,をインストールします>>
最新の演算子。
```

  - 同じクラスタ名を使用してください。
  - 最新のOperator YAMLファイルをダウンロードしたら、展開する前に、agent_backup.yamlにあるカスタマイズをダウンロードしたoperator-config.yamlに移植します。
  - 確認してください 最新のコンテナイメージを取得します カスタムリポジトリを使用している場合。

Kubernetes Monitoring Operatorの停止と起動

Kubernetes Monitoring Operatorを停止するには：

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Kubernetes Monitoring Operatorを起動するには：
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

アンインストール中です

Kubernetes Monitoring Operatorを削除するには

Kubernetes Monitoring Operatorのデフォルトのネームスペースは「netapp-monitoring」です。 独自のネームスペースを設定した場合は、それらのネームスペースと、以降のすべてのコマンドおよびファイルを置き換えます。

新しいバージョンの監視オペレータは、次のコマンドを使用してアンインストールできます。

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

監視オペレータが専用のネームスペースに配置されている場合は、ネームスペースを削除します。

```
 kubectl delete ns <NAMESPACE>
```
最初のコマンドが「リソースが見つかりません」を返した場合は、次の手順に従って古いバージョンの監視オペレータをアンインストールします。

次の各コマンドを順番に実行します。現在のインストール状況によっては、これらのコマンドの一部で「オブジェクトが見つかりません」というメッセージが返される場合があります。これらのメッセージは無視してかまいません。

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

セキュリティコンテキスト制約が事前に作成されている場合は、次の手順を実行します。

```
kubectl delete scc telegraf-hostaccess
```

Kubeステートメトリックについて

NetApp Kubernetes Monitoring Operatorは、他のインスタンスとの競合を回避するために独自のkube-state-metricsをインストールします。

Kube-State-Metricsの詳細については、を参照してください。 "このページです"。

オペレータの設定/カスタマイズ

これらのセクションでは、オペレータ設定のカスタマイズ、プロキシの操作、カスタムまたはプライベートDockerリポジトリの使用、OpenShiftの操作について説明します。

設定オプション

最も一般的に変更される設定は、_AgentConfiguration_customリソースで構成できます。オペレータを配備する前に、_operator-config.yaml_fileを編集して、このリソースを編集できます。このファイルには、コメントアウトされた設定例が含まれています。のリストを参照してください "使用可能な設定" 演算子の最新バージョン。

オペレータが配備された後で、次のコマンドを使用してこのリソースを編集することもできます。

```
kubectl -n netapp-monitoring edit AgentConfiguration
```
展開したオペレータのバージョンが`AgentConfiguration`をサポートしているかどうかを確認するには、次のコマンドを実行します。

```
kubectl get crd agentconfigurations.monitoring.netapp.com
```
「`Error from server (NotFound)`」というメッセージが表示された場合は、`AgentConfiguration`を使用する前にオペレータをアップグレードする必要があります。

プロキシサポートを設定しています

Kubernetes Monitoring Operatorをインストールするために、環境内でプロキシを使用できる場所は2つあります。同じプロキシシステムでも、別のプロキシシステムでもかまいません。

- インストールコードスニペット（「curl」を使用）の実行中に、スニペットが実行されるシステムをData Infrastructure Insights環境に接続するために必要なプロキシ
- ターゲットのKubernetesクラスタがData Infrastructure Insights環境と通信するために必要なプロキシ

これらのいずれかまたは両方にプロキシを使用する場合、Kubernetes Operating Monitorをインストールするには、まず、Data Infrastructure Insights環境との通信が良好になるようにプロキシが設定されていることを確認する必要があります。プロキシがあり、Operatorをインストールするサーバ/ VMからData Infrastructure Insightsにアクセスできる場合は、プロキシが適切に設定されている可能性があります。

Kubernetes Operating Monitorのインストールに使用するプロキシについては、Operatorをインストールする

前に、_http_proxy/https_proxy_environment変数を設定します。一部のプロキシ環境では'_no_proxy環境変数も設定する必要があります

変数を設定するには、Kubernetes Monitoring Operatorをインストールする前に、システム*で次の手順を実行します。

1. 現在のユーザの *https_proxy* 変数と _http_proxy_environment 変数を設定します。
   a. セットアップするプロキシに認証（ユーザ名/パスワード）がない場合は、次のコマンドを実行します。

```
 export https_proxy=<proxy_server>:<proxy_port>
```

. . セットアップするプロキシに認証（ユーザ名/パスワード）が設定されている場合は、次のコマンドを実行します。

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_port>
```

KubernetesクラスタがData Infrastructure Insights環境と通信するために使用するプロキシの場合は、以下の手順をすべて読んでからKubernetes Monitoring Operatorをインストールします。

Kubernetes Monitoring Operatorをデプロイする前に、operator-config.yamlのAgentConfigurationのプロキシセクションを設定します。

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Kubernetes監視オペレータは、デフォルトで、Data Infrastructure Insightsリポジトリからコンテナイメージを取得します。監視のターゲットとして使用されているKubernetesクラスタがあり、そのクラスタがカスタムまたはプライベートのDockerリポジトリまたはコンテナレジストリからコンテナイメージのみをプルするように構成されている場合は、Kubernetes Monitoring Operatorが必要とするコンテナへのアクセスを設定する必要があります。

NetApp Monitoring Operatorのインストールタイルから[Image Pull Snippet]を実行します。このコマンドを実行すると、Data Infrastructure Insightsリポジトリにログインし、オペレータが必要とするすべてのイメージを取得して、Data Infrastructure Insightsリポジトリからログアウトします。プロンプトが表示されたら、指定したリポジトリの一時パスワードを入力します。このコマンドは、オプション機能を含む、オペレータが使用するすべてのイメージをダウンロードします。これらの画像がどの機能に使用されるかについては、以下を参照してください。

Core Operator Functionality and Kubernetes Monitoringの略

- ネットアップによる監視
- ci-kube-rbac-proxy
- CI-KSM
- CI-テレグラフ
- distroless-root-user

イベントログ

- CI-fluent-bit
- ci-kubernetes-event-exporter

ネットワークのパフォーマンスとマップ

- ci-net-observerの略

社内のポリシーに従って、オペレータ用の Docker イメージをプライベート / ローカル / エンタープライズ Docker リポジトリにプッシュします。リポジトリ内のこれらのイメージへのイメージタグとディレクトリパスが、Data Infrastructure Insightsリポジトリ内のイメージタグとディレクトリパスと一致していることを確認します。

operator-deployment.yamlでmonitoring-operatorデプロイメントを編集し、プライベートDockerリポジトリを使用するようにすべてのイメージ参照を変更します。

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

operator-config.yamlのAgentConfigurationを編集して、新しいDockerリポジトリの場所を反映します。プライベートリポジトリ用に新しいimagePullSecretを作成します。詳細については、_ https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/_を参照してください

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here:
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

OpenShift の手順

OpenShift 4.6以降で実行している場合は、_runPrivileged_settingを有効にするには、_operator-config.yaml_でAgentConfigurationを編集する必要があります。

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

OpenShiftは、一部のKubernetesコンポーネントへのアクセスをブロックする可能性のある追加のセキュリティレベルを実装する場合があります。

秘密に関する注意事項

Kubernetes Monitoring Operatorのシークレットをクラスタ全体で表示する権限を削除するには、インストール前に_operator-setup.yaml_fileから次のリソースを削除します。

```
 ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-clusterrolebinding
```

アップグレードの場合は、クラスタからリソースも削除します。

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

変更分析が有効になっている場合は、_AgentConfiguration_or_operator -config.yaml_を変更して、変更管理セクションのコメントを解除し、変更管理セクションの下に_kindsToIgnoreFromWatch：'"secrets"'_を含めます。この行の一重引用符と二重引用符の存在と位置に注意してください。

```
# change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Kubernetes のチェックサムの検証

Data Infrastructure Insightsエージェントインストーラは整合性チェックを実行しますが、ダウンロードしたアーティファクトをインストールまたは適用する前に独自の検証を実行することもできます。デフォルトのダウンロードおよびインストールではなく、ダウンロードのみの操作を実行するには、 UI から取得したエージェントインストールコマンドを編集し、末尾の「インストール」オプションを削除します。

次の手順を実行します。

1. 指示に従ってエージェントインストーラスニペットをコピーします。
2. スニペットをコマンドウィンドウに貼り付ける代わりに、テキストエディタに貼り付けます。
3. コマンドから末尾の「--install」を削除します。
4. コマンド全体をテキストエディタからコピーします。
5. 次に、コマンドウィンドウ（作業ディレクトリ内）に貼り付けて実行します。
   - Download and install （デフォルト）：

```
 installerName=cloudinsights-rhel_centos.sh … && sudo -E -H
./$installerName --download --install
** ダウンロードのみ：
```

```
installerName=cloudinsights-rhel_centos.sh … && sudo -E -H
./$installerName --download
```

download-onlyコマンドを実行すると、必要なすべてのアーティファクトがData Infrastructure Insightsから作業ディレクトリにダウンロードされます。アーティファクトには次のものがありますが、これらに限定することはできません。

- インストールスクリプト
- 環境ファイル
- YAMLファイル
- 署名済みチェックサムファイル（ SHA256 署名）

- 署名の検証に使用する PEM ファイル（ NetApp_cert.pem ）

インストールスクリプト、環境ファイル、 YAML ファイルは、目視検査を使用して検証できます。

PEM ファイルは、フィンガープリントが次のようになっていることを確認することで検証できます。

```
 1A918038E8E127BB5C87A202DF173B97A05B4996
```
具体的には、

```
 openssl x509 -fingerprint -sha1 -noout -inform pem -in netapp_cert.pem
```
署名済みチェックサムファイルは、 `PEM` ファイルを使用して確認できます。

```
 openssl smime -verify -in sha256.signed -CAfile netapp_cert.pem -purpose
any
```
すべてのアーティファクトが正常に検証されたら、次のコマンドを実行してエージェントのインストールを開始できます。

```
sudo -E -H ./<installation_script_name> --install
```

公差と接線（**Tolerations and Taints**）

NetApp-ci-telegraf-ds_、*NetApp-CI-fluent-bit-ds*、および_NetApp-CI-net-observer-l4-DS_DaemonSetsは、すべてのノードのデータを正しく収集するために、クラスタ内のすべてのノードでポッドをスケジュールする必要があります。オペレータは、いくつかの既知の*テイント*に耐えられるように設定されています。ノードにカスタムのtaintsを設定して、すべてのノードでポッドが実行されないようにしている場合は、それらのtaintsに* toleration *を作成できます "（*AgentConfiguration*）をクリックします"。クラスタ内のすべてのノードにカスタムテイントを適用した場合は、オペレータの導入に必要な許容範囲を追加して、オペレータポッドをスケジュールおよび実行できるようにする必要があります。

Kubernetesの詳細はこちらをご覧ください "塗料および耐性"。

に戻ります "* NetApp Kubernetes監視オペレータのインストール*ページ"

トラブルシューティング

Kubernetes Monitoring Operatorの設定で問題が発生した場合に試すべきこと：

問題	次の操作を実行します
Kubernetes 永続ボリュームと対応するバックエンドストレージデバイスの間にハイパーリンク / 接続がありません。My Kubernetes Persistent Volume がストレージサーバのホスト名を使用して設定されます。	手順に従って既存の Tegraf エージェントをアンインストールし、最新の Tegraf エージェントを再インストールします。Telegrafバージョン2.0以降を使用しており、KubernetesクラスタストレージがData Infrastructure Insightsによってアクティブに監視されている必要があります。

問題	次の操作を実行します
ログに次のようなメッセージが表示されます。 E0901 15:21:39.962145 1 reflector.go:178]k8s.io/kube-state-metrics/internal/store/builder.go:352:リストに失敗しました*v1.MutatingWebhookConfiguration:サーバーは要求されたリソースを見つけることができませんでした E0901 15:21:43.168161 1 reflector.go:178]k8s.io/kube-state-metrics/internal/store/builder.go:352:リストに失敗しました*v1 Lease:サーバーは要求されたリソースを見つけることができませんでした(GET leases.coordination.k8s.io) など	これらのメッセージは、1.20より前のバージョンのKubernetesでkube-state-metricsバージョン2.0.0以上を実行している場合に発生する可能性があります。 Kubernetesのバージョンを取得するには： *kubectl*バージョン kube-state-metricsバージョンを取得するには、次の手順を実行します。 *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* これらのメッセージが発生しないように、ユーザはkube-state-metrics展開を変更して、次のリースを無効にすることができます。 *mutatingwebhookconfigurations* 検証webhookconfigurations_ *volumeattachments*リソース 具体的には、次のCLI引数を使用できます。 resources=certificatesigningrequests, configmaps, cronjobs, daemonsets, deployments, endpoints, horizontalpodautoscalers, ingresses, jobs, limitranges, namespaces, networkpolicies, poddisruptionbudgets, pods, ReplicaSets, replicationcontrollasses, resourcequotases, secrets, resourcequotases, secrets, services, storage, storefuls. デフォルトのリソースリストは次のとおりです。 certificatesigningrequests, configmaps, cronjobs, daemonsets, deployments, endpoints, horizontalpododautoscalers, ingresses, jobs, leases, limitranges, mutatingwebhookconfiguration, namespaces, networkpersistentvolumes, poddisruptionbudgets, pers, persistentresets, pondsets, podsets, postresets, replicassess, replicastess, replicatess, replicastorets, replicast 検証Webhook構成’ボリューム添付ファイル"\y"ケンショウ:Webhookコウセイ’ボリュームアタッチメント

問題	次の操作を実行します
Telegrafから次のようなエラーメッセージが表示されますが、Telegrafは起動して実行されます。 10月11日14:23:41 IP-172-31-39-47 systemd[1]: InfluxDBにメトリックを報告するプラグイン駆動のサーバーエージェントを起動しました。 10 月 11 日 14 ： 23 ： 41 IP-172-41-39-47 テレグラム [1827] ： time="2021 - 10-11T14 ： 23 ： 41Z" level= error msg=" キャッシュディレクトリの作成に失敗しました。/etc/telegraf/.cache/snowflake 、err:mkdir /etc/telegraf/.ca CHE：権限が拒否されました。無視\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 10月11日14：23：41 IP-172-31-39-47 telegraf [1827] ：time="2021-10-11T14：23：41Z" level=error msg="failed to open.無視されます。/etc/telegraf/.cache/snowflake/ocsp_response_cache.jsonを開きます。no such ファイルまたはディレクトリ\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 10月11日14:23:41 IP-172-31-39-47 telegraf [1827]: 2021-10-11T14:23:41Z I! Telegraf 1.19.3 を起動しています	これは問題と呼ばれています。 を参照してください "この GitHub の記事" 詳細：Tegraf が起動して動作している限り、ユーザはこのエラーメッセージを無視できます。
Kubernetesで、Telegrafポッドが次のエラーを報告しています。 "mountstats情報の処理中にエラーが発生しました：mountstatsファイルを開けませんでした：/hostfs/proc/1/mountstats、エラー：open/hostfs/proc/1/mountstats：権限が拒否されました"	SELinuxを有効にして強制すると、TelegrafポッドがKubernetesノードの/proc/1/mountstatsファイルにアクセスできなくなる可能性があります。この制限を克服するには、agentconfigurationを編集し、runPrivileged設定を有効にします。詳細については、 "OpenShift の手順"。
Kubernetesで、Telegraf ReplicaSetポッドが次のエラーを報告しています。 [プラグインのinputs.prometheus]エラー：keypair /etc/kubernetes/pki/etcd/server.crtをロードできませんでした：/etc/kubernetes/pki/etcd/server.key：open /etc/kubernetes/pki/etcd/server.crt：該当するファイルまたはディレクトリはありません	Telegraf ReplicaSet ポッドは、マスターまたは etcd 用に指定されたノード上で実行することを目的としています。これらのノードのいずれかで ReplicaSet ポッドが実行されていない場合は、これらのエラーが発生します。マスター / etcd ノードに汚染があるかどうかを確認します。その場合は、 Telegraf ReplicaSet 、テレグラム af-RS に必要な忍容を追加します。 たとえば、ReplicaSet… kubectl edit rs telegraf-rs 仕様に適切な公差を追加します。次に、 ReplicaSet ポッドを再起動します。

問題	次の操作を実行します
PSP/PSA環境があります。これはモニタリングオペレータに影響しますか？	KubernetesクラスタがPod Security Policy（PSP）またはPod Security Admission（PSA）を使用して実行されている場合は、最新のKubernetes Monitoring Operatorにアップグレードする必要があります。PSP/PSAをサポートしている現在のオペレータにアップグレードするには、次の手順に従います。 1. をアンインストールします 以前の監視オペレータ： kubectl delete agent agent-monitoring-netapp-n netapp-monitoring kubectlによってネットアップによる監視が削除されます kubectlはCRD agents.monitoring.netapp.comを削除します kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 2. をインストールします モニタリングオペレータの最新バージョン。
Operatorを展開しようとして問題が発生しましたが、PSP/PSAを使用しています。	1.次のコマンドを使用してエージェントを編集します。 kubectl -n <name-space>編集エージェント 2.「security-policy-enabled」を「false」に設定します。これにより、PodセキュリティポリシーとPodセキュリティアドミッションが無効になり、オペレータが展開できるようになります。次のコマンドを使用して確認します。 kubectl get psp（Pod Security Policy removedを表示する必要があります） kubectl get all -n <namespace>
grep -i psp (should show that nothing is found)	「ImagePullBackoff」エラーが発生しました
これらのエラーは、カスタムまたはプライベートのDockerリポジトリがあり、Kubernetes Monitoring Operatorを適切に認識するように設定していない場合に表示されることがあります。 詳細はこちら カスタム/プライベートリポジトリの設定について	監視オペレータの配置に問題 を使用していますが、現在のドキュメントでは解決できません。

問題	次の操作を実行します
次のコマンドの出力をキャプチャまたはメモし、テクニカルサポートチームに連絡します。 `kubectl -n netapp-monitoring get all` `kubectl -n netapp-monitoring describe all` `kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true` `kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true`	Operator名前空間のNet-Observer（ワークロードマップ）ポッドがCrashLoopBackOffにある
これらのポッドは、Network ObservabilityのWorkload Mapデータコレクタに対応しています。以下をお試しください。 •いずれかのポッドのログをチェックして、カーネルの最小バージョンを確認します。例： --- {"ci-tenant-id"："your-tenant-id"、"collector-cluster"："your-k8s-cluster-name"、"environment"："prod"、"level"："error"、"msg"："検証に失敗しました。理由：カーネルバージョン3.10.0が最小カーネルバージョン4.18.0よりも小さい、"time"："2022-11-09T08:23:08Z"} --- •Net-Observerポッドを使用するには、Linuxカーネルのバージョンが4.18.0以上である必要があります。「uname -r」コマンドを使用してカーネルのバージョンを確認し、4.18.0以上であることを確認します	PodはOperatorネームスペース（デフォルト：netapp-monitoring）で実行されているが、Queriesのワークロードマップまたはkubernetes指標のデータがUIに表示されない
K8Sクラスタのノードの時間設定を確認します。監査およびデータレポートを正確に作成するには、Network Time Protocol（NTP；ネットワークタイムプロトコル）またはSimple Network Time Protocol（SNTP；簡易ネットワークタイムプロトコル）を使用してAgentマシンの時刻を同期することを強く推奨します。	Operator名前空間の一部のnet-observerポッドがPending状態です

問題	次の操作を実行します
net-observerはデーモンセットであり、Kubernetesクラスタの各ノードでポッドを実行します。 •保留状態のポッドをメモし、CPUまたはメモリのリソース問題が発生しているかどうかを確認します。必要なメモリとCPUがノードにあることを確認します。	Kubernetes Monitoring Operatorをインストールした直後にログに次のようなメッセージが表示されます。 [プラグインのinputs.prometheus]エラー：\http://kube-state-metricsへの要求エラー。<namespace>.svc.cluster.local：8080/metrics：get\ http://kube-state-metrics <namespace>.svc.cluster.local：8080/metrics：dial tcp：lookup kube-state-metrics 。<namespace>.svc.cluster.local：該当するホストはありません。
このメッセージが表示されるのは、通常、_KSM_PODが起動する前に、新しいオペレータがインストールされ、_テレ グラム-RS_PODが稼働している場合のみです。これらのメッセージは、すべてのポッドが実行されると停止します。	クラスタに存在するKubernetes CronJobsについて収集された指標が表示されません。
Kubernetesのバージョンを確認します（ `kubectl version`）。 v1.20.x以下の場合、これは想定される制限です。 Kubernetes Monitoring Operatorで導入されたkube-state-metricsリリースでは、v1.cronjobのみがサポートされます。 Kubernetes 1.20.x以前では、cronjobリソースはv1beta.cronjobにあります。その結果、kube-state-metricsはcronjobリソースを見つけることができません。	オペレータのインストール後、telegraf-DSポッドがCrashLoopBackOffに入り、PODログに「su：Authentication failure」と表示されます。
_AgentConfiguration_のtelegrafセクションを編集し、set_dockerMetricCollectionEnabled_をfalseに設定します。詳細については、オペレータのを参照して"設定オプション"ください。注: Data Infrastructure Insights Federal Editionを使用している場合、_su_の使用が制限されているユーザーはDockerメトリクスを収集できません。Dockerソケットにアクセスするには、telegrafコンテナをrootとして実行するか、_su_を使用してtelegrafユーザーをDockerグループに追加する必要があるためです。Dockerメトリック収集と_su_の使用はデフォルトで有効になっています。両方を無効にするには、_AgentConfiguration_fileの_telegraf.docker_entryを削除します。…spec:…telegraf:… -name：docker run-mode： -DaemonSet 置換： -key：docker_unix_sock_placeholder 値：unix：//run/docker.sock……	Telegrafログに次のようなエラーメッセージが繰り返し表示されます。 来い! [agent]出力への書き込み中にエラーが発生しました。http：Post "\https：//<tenant_url>/rest/v1/lake/ingest/influxdb"：context deadline exceeded (Client. ヘッダー待機中にタイムアウトを超過しました）
_AgentConfiguration_およびincrease_outputTimeout_のtelegrafセクションを10秒に編集します。詳細については、オペレータのを参照してください "設定オプション"。	一部のイベントログの_involvedobject_dataが見つかりません。
次の手順を実行していることを確認してください： "権限" 上記のセクション。	2つの監視オペレータポッド（netapp-ci-monitoring-operator-pod <pod>とmonitoring-operator-pod）が実行されているのはなぜ<pod>ですか？

問題	次の操作を実行します
2023年10月12日付けで、Data Infrastructure Insightsは、ユーザへのサービス向上のためにオペレータをリファクタリングしました。これらの変更を完全に採用するには古いオペレータを削除します。、とが必要です。新しいものを取り付ける	Kubernetesイベントが予期せずData Infrastructure Insightsに報告されなくなりました。
event-exporterポッドの名前を取得します。 `kubectl -n netapp-monitoring get pods`	grep event-exporter
awk '{print $1}'	sed 's/event-exporter./event-exporter/` 「netapp-ci-event-exporter」または「event-exporter」のいずれかにする必要があります。 次に、監視エージェントを編集します。 `kubectl -n netapp-monitoring edit agent`をクリックし、log_fileの値を設定して、前の手順で見つけた適切なイベントエクスポータポッド名を反映します。 具体的には、log_fileは「/var/log/containers/netapp-ci-event-exporter.log」または「/var/log/containers/event-exporter 。**log**」のいずれかに設定する必要があります。 …. **fluent-bit:** … **- name: event-exporter-ci** **substitutions:** **- key: LOG_FILE** **values:** **- /var/log/containers/netapp-ci-event-exporter**.log … …. 別の方法として、 をアンインストールします および再インストール エージェント。
リソースが不足しているため、Kubernetes Monitoring Operatorによってデプロイされたポッドがクラッシュしています。	Kubernetes Monitoring Operatorを参照 "設定オプション" 必要に応じてCPUやメモリの制限を増やします。
イメージがないか無効な設定が原因で、netapp-ci-kube-state-metricsポッドが起動しないか準備完了状態になりました。これでStatefulSetが停止し、設定の変更がnetapp-ci-kube-state-metricsポッドに適用されなくなりました。	StatefulSetは "切断" 状態。設定の問題を修正したら、netapp-ci-kube-state-metricsポッドをバウンスします。
NetApp-ci-kube-state-metricsポッドがKubernetes Operatorのアップグレード実行後に起動せず、ErrImagePullがスローされる（イメージをプルできない）。	ポッドを手動でリセットしてみてください。

問題	次の操作を実行します
Kubernetesクラスタの[Log Analysis]で、「Event discarded as being older then maxEventAgeSeconds」というメッセージが確認されています。	Operator_agentconfiguration_を変更し、*event-exporter-maxEventAgeSeconds*（60秒）、*event-exporter-kubeQPS*（100）、および_event-exporter-kubeBurst_（500）を増やします。これらの設定オプションの詳細については、を参照してください。 "設定オプション" ページ
Telegrafが警告するか、ロック可能なメモリが不足しているためにクラッシュします。	基盤となるオペレーティングシステム/ノードでTelegrafのロック可能メモリの制限を増やしてみてください。制限値を増やすことができない場合は'NKMOエージェントの構成を変更して'_unprotected_to_true_に設定します これにより、Telegrafはロックされたメモリページを予約しないように指示します。復号化されたシークレットがディスクにスワップアウトされる可能性があるため、セキュリティリスクが発生する可能性がありますが、ロックされたメモリを予約できない環境では実行できます。_unprotected_configurationオプションの詳細については、 "設定オプション" ページ

追加情報はから入手できます "サポート" ページまたはを参照してください "Data Collector サポートマトリックス"。

Memcached Data Collector

Data Infrastructure Insightsは、このデータコレクタを使用してMemcachedから指標を収集します。

インストール

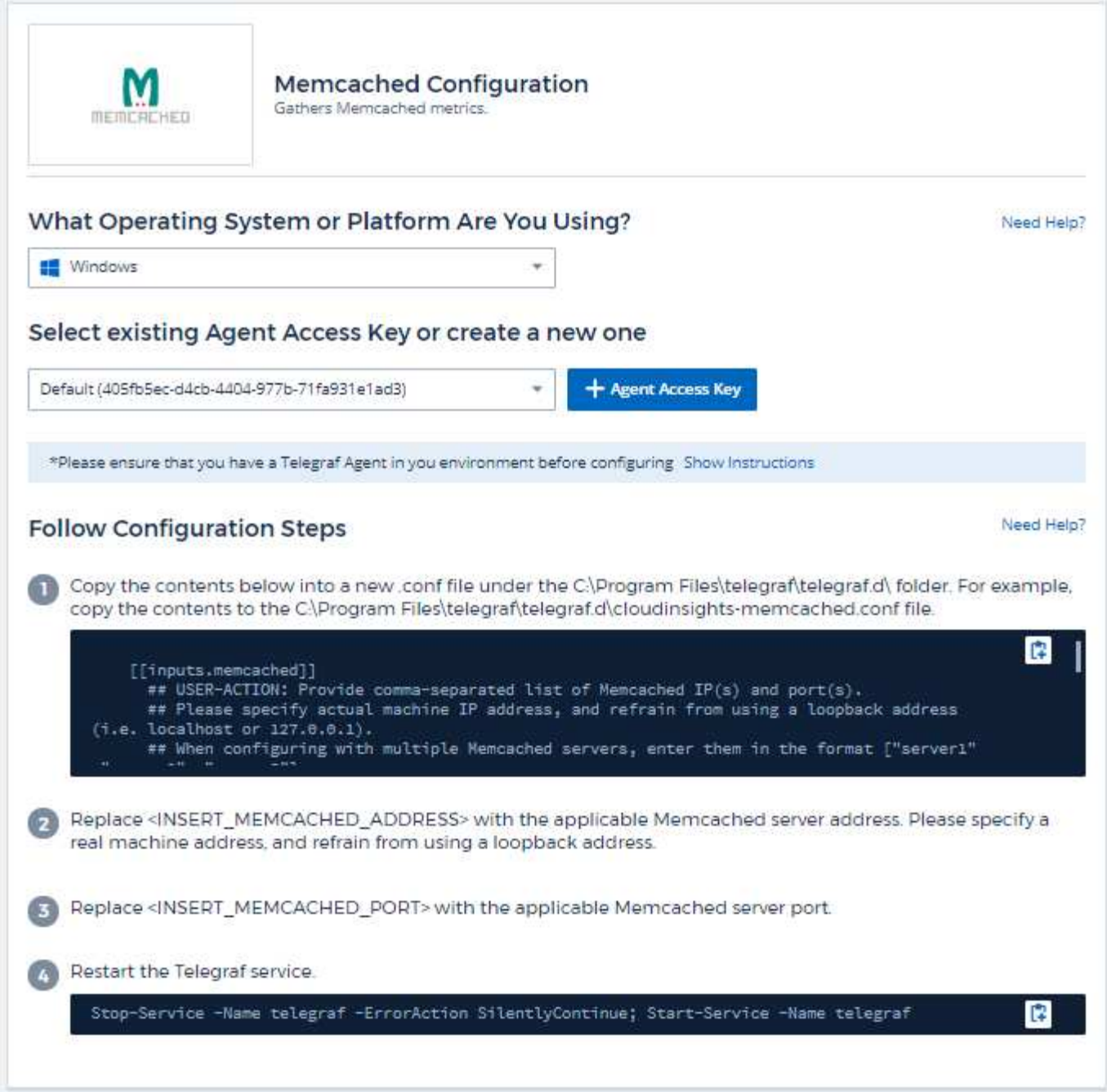
1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。Memcachedを選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順

3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。

4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

情報は、に記載されています "Memcached Wiki"。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Memcached	ネームスペース サーバ	ノードIP ノード名	接続を受け入れています 認証要求を処理しました 認証に失敗しました 使用済みバイト数 読み取りバイト数（1秒あたり） 書き込みバイト数（1秒あたり） キャス・バヴァル CASヒット CASミス フラッシュ要求（1秒あたり） 要求の取得（1秒あたり） 要求の設定（1秒あたり） タッチ要求（1秒あたり） 接続歩留まり（1秒あたり） 接続構造 接続を開きます 現在保存されているアイテム Decr Requests Hits（1秒あたり） Decr Requests Misses（1秒あたり） Delete Requests Hits（1秒あたり） Delete Requests Misses（1秒あたり） 削除されたアイテム 有効な削除 期限切れのアイテム GETヒット数（1秒あたり） Get Misses（1秒あたり） 使用されているハッシュバイト数 ハッシュが拡張されています ハッシュパワーレベル Incr Requests Hits（1秒あたり） Incr Requests Misses（1秒あたり） サーバ最大バイト数 リッスン無効番号 再生されました ワーカースレッド数 オープンされている接続の総数 保存されている合計アイテム数 [ヒット]に触れます

トラブルシューティング

追加情報はから入手できます "サポート" ページ

MongoDB データコレクタ

Data Infrastructure Insightsは、このデータコレクタを使用してMongoDBから指標を収集します。

インストール

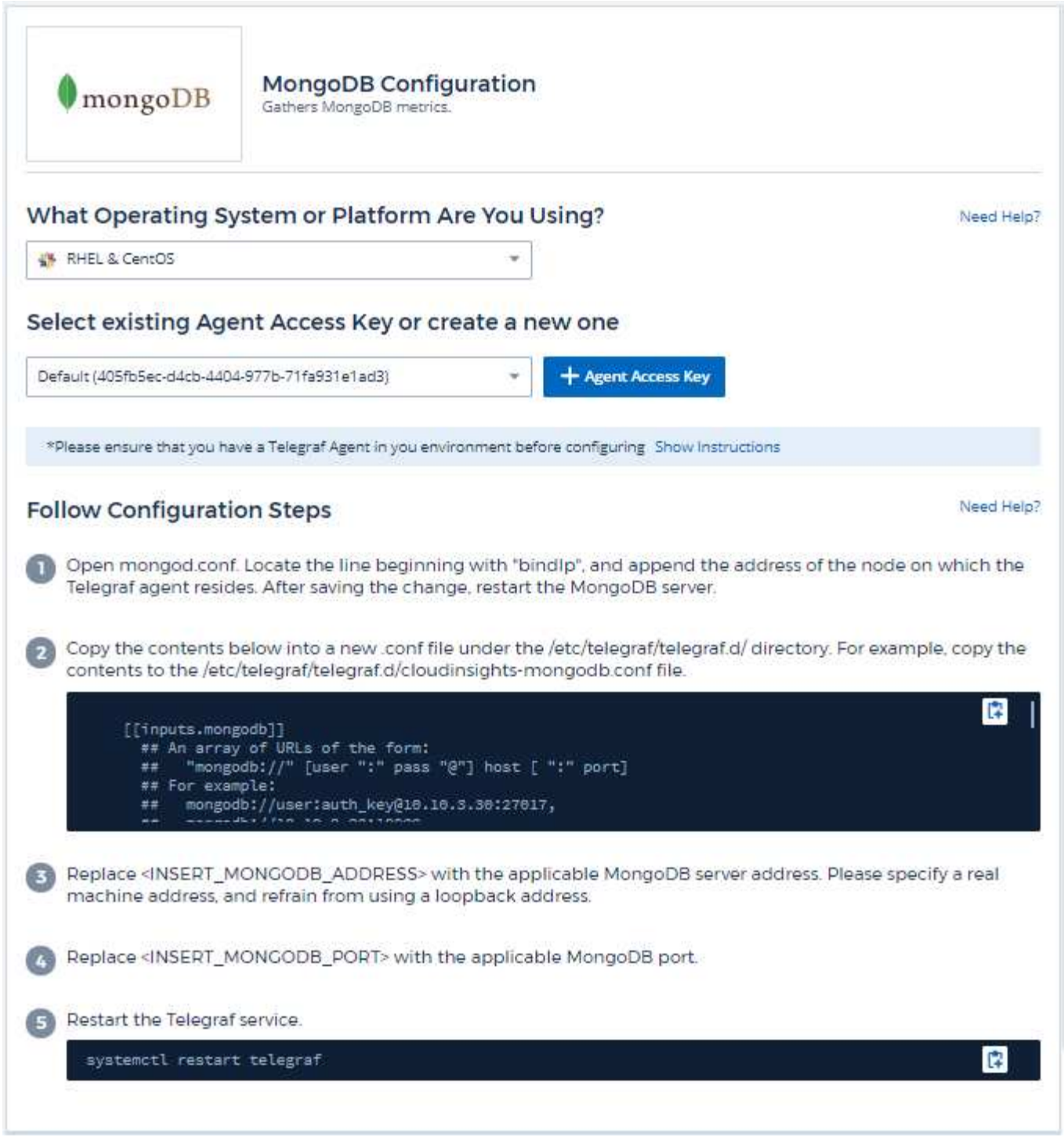
1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。[MongoDB]を選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順

3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。

4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

情報は、に記載されています "MongoDB のドキュメント"。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
MongoDB	ネームスペース ホスト名		
MongoDB データベース	ネームスペース ホスト名 データベース名		

トラブルシューティング

情報はから入手できます "サポート" ページ

MySQL データコレクタ

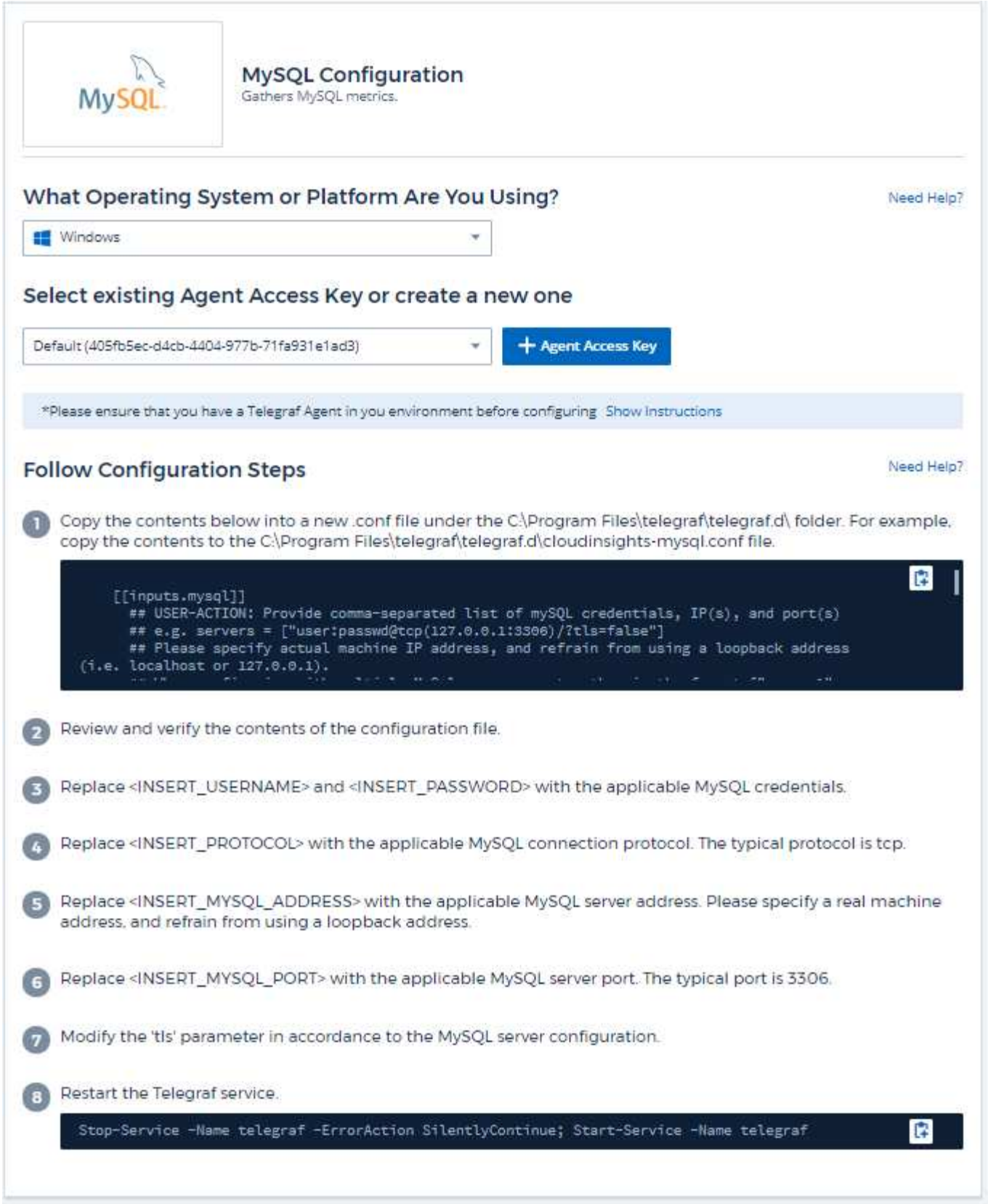
Data Infrastructure Insightsは、このデータコレクタを使用してMySQLから指標を収集します。

インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。MySQLを選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順
3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

情報は、に記載されています "MySQL のドキュメント"。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
MySQL	ネームスペース MySQLサーバ	ノードIP ノード名	中止されたクライアント数（1秒あたり） 中断された接続数（1秒あたり） 受信バイト数（1秒あたり） 転送バイト数（1秒あたり） 管理コマンド数（1秒あたり） コマンドはイベントを変更します コマンドは機能を変更します コマンドはインスタンスを変更します コマンドは手順を変更します コマンドはサーバーを変更します コマンドはテーブルを変更します コマンドはテーブルスペースを変更します コマンドはユーザーを変更します コマンド解析（Commands Analyze コマンドはキーキャッシュに割り当てます コマンドが開始されます コマンドBinlog コマンド手順を呼び出します コマンド変更DB コマンドマスターを変更します [コマンド][リプレゼンテーションフィルタを変更] コマンドチェック コマンドチェックサム コマンドCommit コマンドCreate DB コマンドイベントを作成します コマンド機能を作成します コマンドインデックスを作成します コマンドCreate手順 コマンドサーバーを作成します コマンドテーブルを作成します

トラブルシューティング

追加情報はから入手できます "サポート" ページ

netstat Data Collector の場合

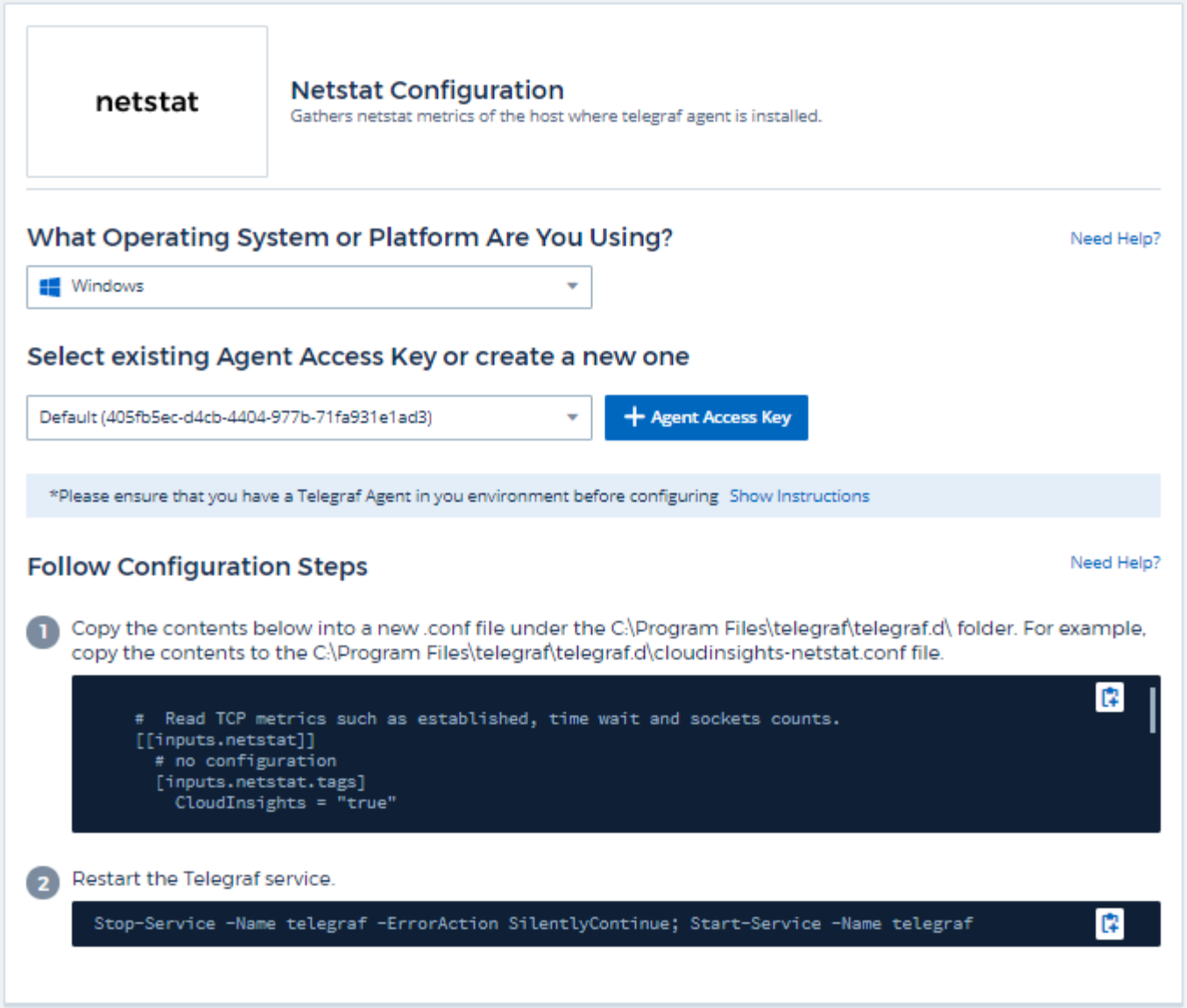
Data Infrastructure Insightsは、このデータコレクタを使用してnetstat指標を収集します。

インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。netstatを選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順
3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 dataPoints 」：
netstat	ノード UUID	ノードIP ノード名	

トラブルシューティング

追加情報はから入手できます "サポート" ページ

nginx データコレクタ

Data Infrastructure Insightsは、このデータコレクタを使用してNginxから指標を収集しま

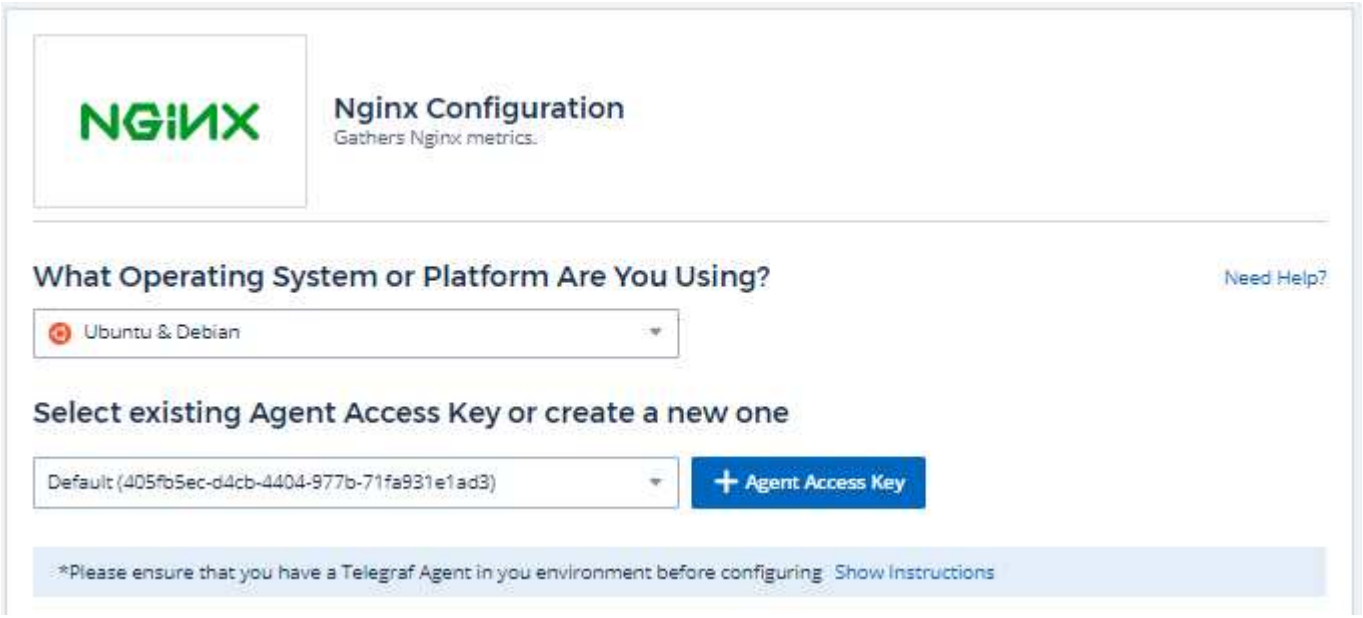
す。

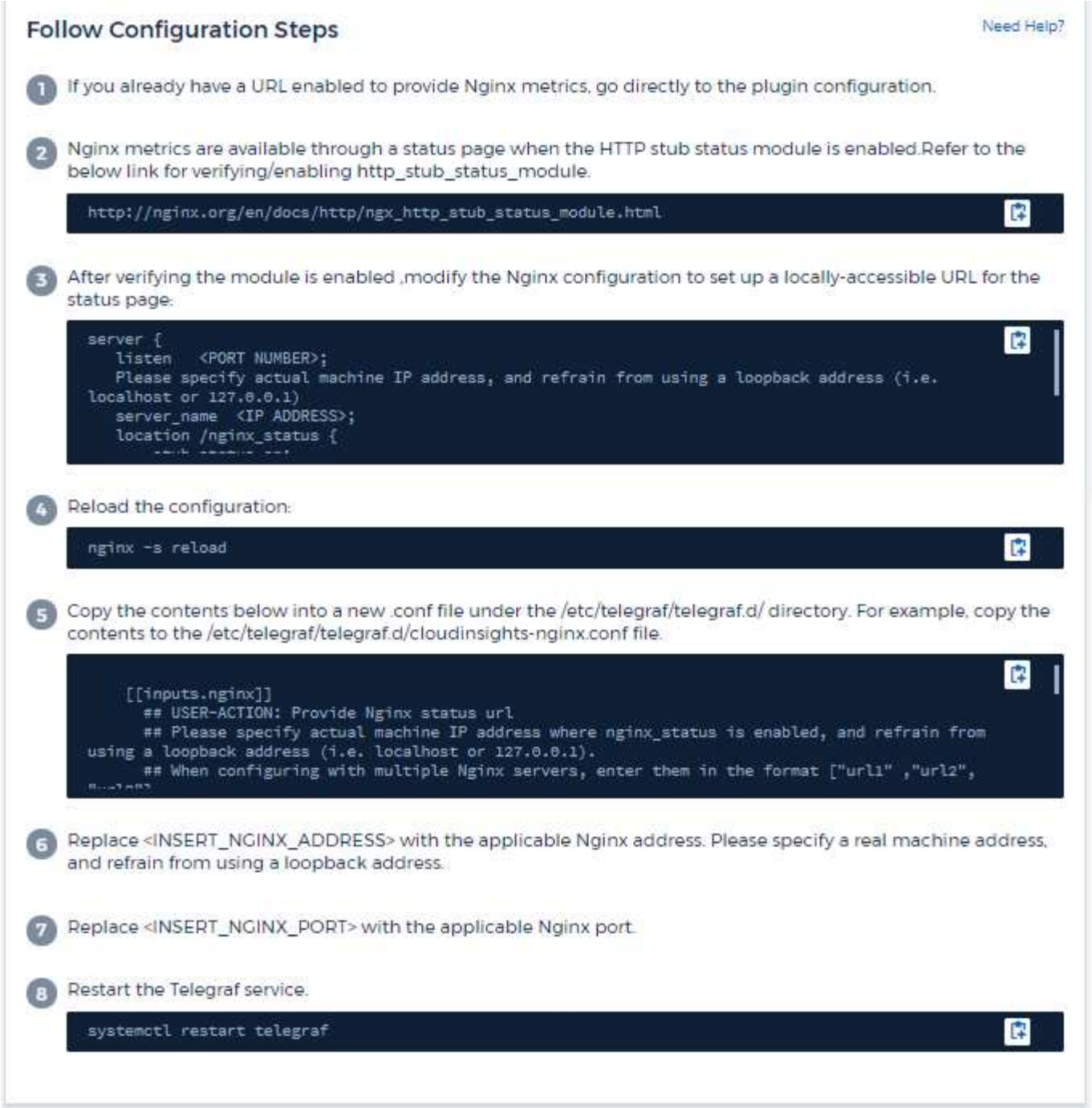
インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。[Nginx]を選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順
3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。





セットアップ（ **Setup** ）

nginx メトリックの収集では、 Nginx が必要です "HTTP_STUB_STATE_MODULE" を有効にします。

追加情報は、にあります "nginx のドキュメント"。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
nginx	ネームスペース サーバ	ノードIP ノード名 ポート	受け入れます アクティブ 処理されます 読書 リクエスト 待機中です 書くこと

トラブルシューティング

追加情報はから入手できます "サポート" ページ

PostgreSQL データコレクタ

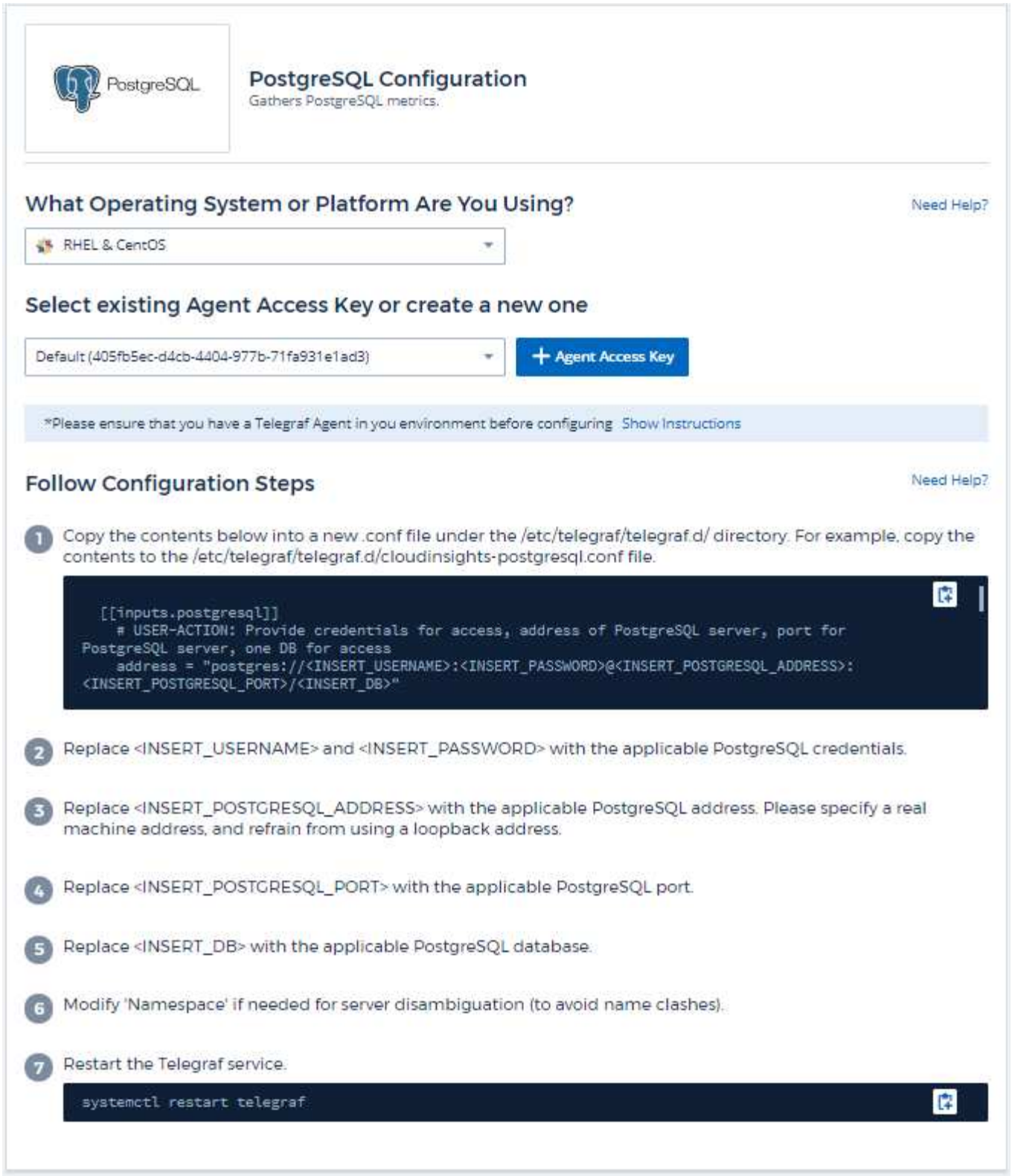
Data Infrastructure Insightsは、このデータコレクタを使用してPostgreSQLから指標を収集します。

インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。PostgreSQLを選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順
3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

情報は、に記載されています "PostgreSQL のドキュメント"。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
PostgreSQL サーバ	ネームスペース データベース サーバ	ノード名 ノードIP	割り当てられたバッファ バッファバックエンド バッファーバックエンド ファイル同期 バッファチェックポイント バッファクリーニング Checkpoints Sync Timeの略 Checkpoints Write Timeの略 チェックポイントリクエスト チェックポイントに時間が設定されました MAX Written Clean
PostgreSQL データベース	ネームスペース データベース サーバ	データベースOID ノード名 ノードIP	Blocks Read Timeの略 Blocks Write Timeの略 ブロックヒット 読み取りをブロックします コンフリクト デッドロック クライアント番号 一時ファイルのバイト数 一時ファイル番号 行を削除しました 行がフェッチされました 挿入された行 返される行数 行を更新しました コミットされたトランザクション ロールバックされたトランザクション

トラブルシューティング

追加情報はから入手できます "サポート" ページ

Puppet Agent データコレクタ

Data Infrastructure Insightsは、このデータコレクタを使用してPuppet Agentから指標を収集します。

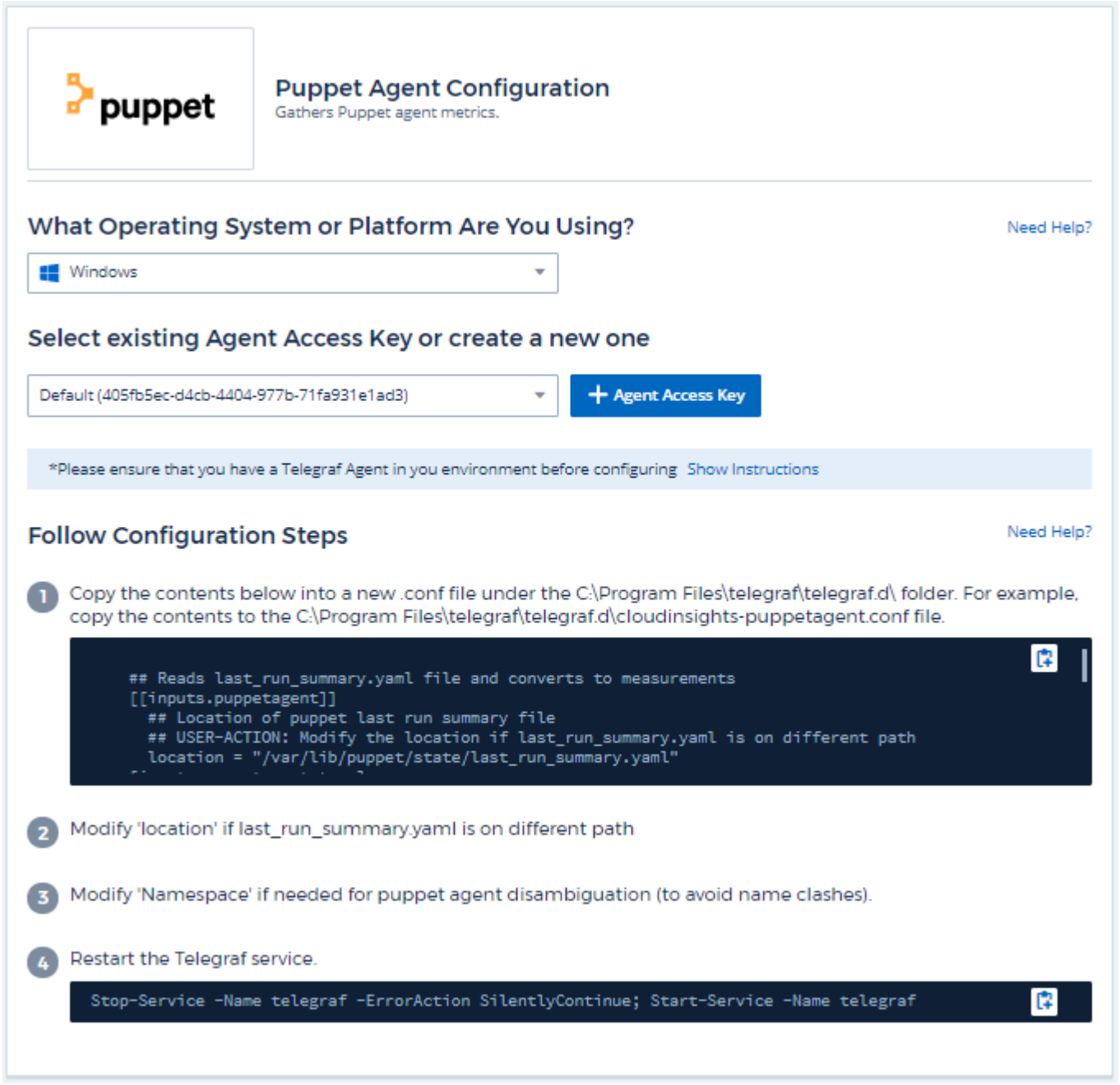
インストール

1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。[Puppet]を選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択

します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順
3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。
4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

情報は、に記載されています "Puppet のドキュメント"

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 dataPoints 」：
Puppet Agent	ネームスペース ノード UUID	ノード名 場所 ノードIP バージョン設定文字列 バージョンPuppet	合計を変更します イベント失敗 イベント成功 イベント合計 リソースが変更されました リソースに失敗しました リソースを再起動できませんでした リソースOutofsync リソースが再起動しました リソースがスケジュールされました リソースがスキップされました リソース合計 タイムアンカー Time Configretrievalの略 タイムcron タイム・エグゼクティブ 時間ファイル（Time File） Time Filebucketの略 タイムラストラン タイムパッケージ タイムスケジュール タイムサービス 時間Sshauthorizedキー 合計時間 タイムユーザー

トラブルシューティング

追加情報はから入手できます "サポート" ページ

Redis Data Collector の場合

Data Infrastructure Insightsは、このデータコレクタを使用してRedisから指標を収集します。Redis は、データベース、キャッシュ、メッセージブローカーとして使用されるオープンソースのインメモリデータ構造ストアで、文字列、ハッシュ、リスト、セットなどのデータ構造をサポートしています。

インストール

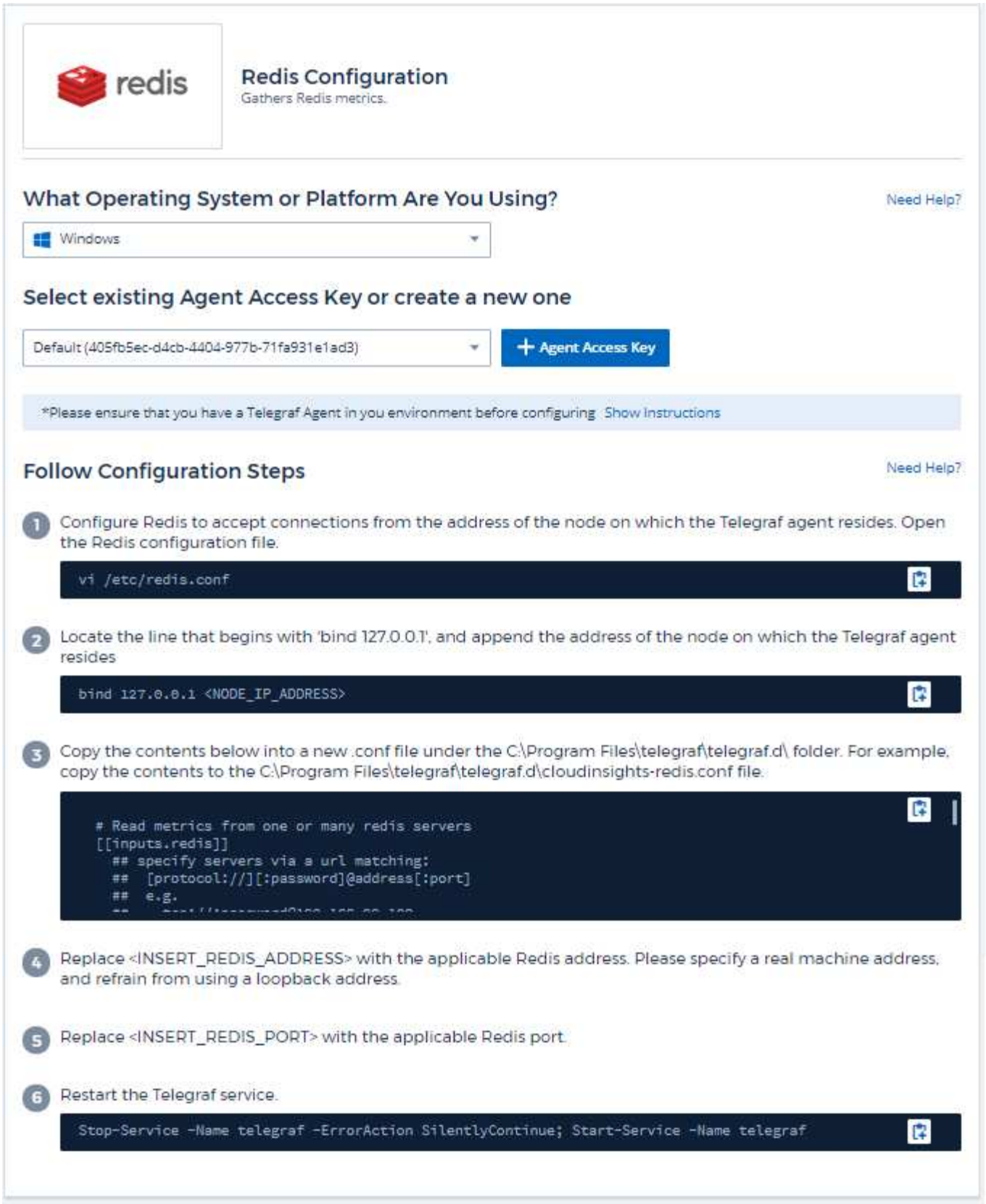
1. [Observability]>[Collectors]で、+ Data Collector *をクリックします。Redisを選択します。

   Tegraf エージェントがインストールされているオペレーティングシステムまたはプラットフォームを選択します。

2. Agent for Collection をまだインストールしていない場合、または別のオペレーティングシステムまたはプラットフォームに Agent をインストールする場合は、 *Show Instructions* をクリックしてを展開します "エージェントのインストール" 手順

3. このデータコレクタで使用するエージェントアクセスキーを選択します。[**+Agent Access Key**] ボタンをクリックすると、新しいエージェントアクセスキーを追加できます。ベストプラクティス：別のエージェントアクセスキーを使用するのは、たとえば OS/ プラットフォーム別にデータコレクタをグループ化する場合だけです。

4. 設定手順に従ってデータコレクタを設定します。手順は、データの収集に使用するオペレーティングシステムまたはプラットフォームのタイプによって異なります。



セットアップ（ **Setup** ）

情報は、に記載されています "Redis 文書"。

オブジェクトとカウンタ

次のオブジェクトとそのカウンタが収集されます。

オブジェクト：	識別子：	属性：	「 **dataPoints** 」：
Redis	ネームスペース サーバ		

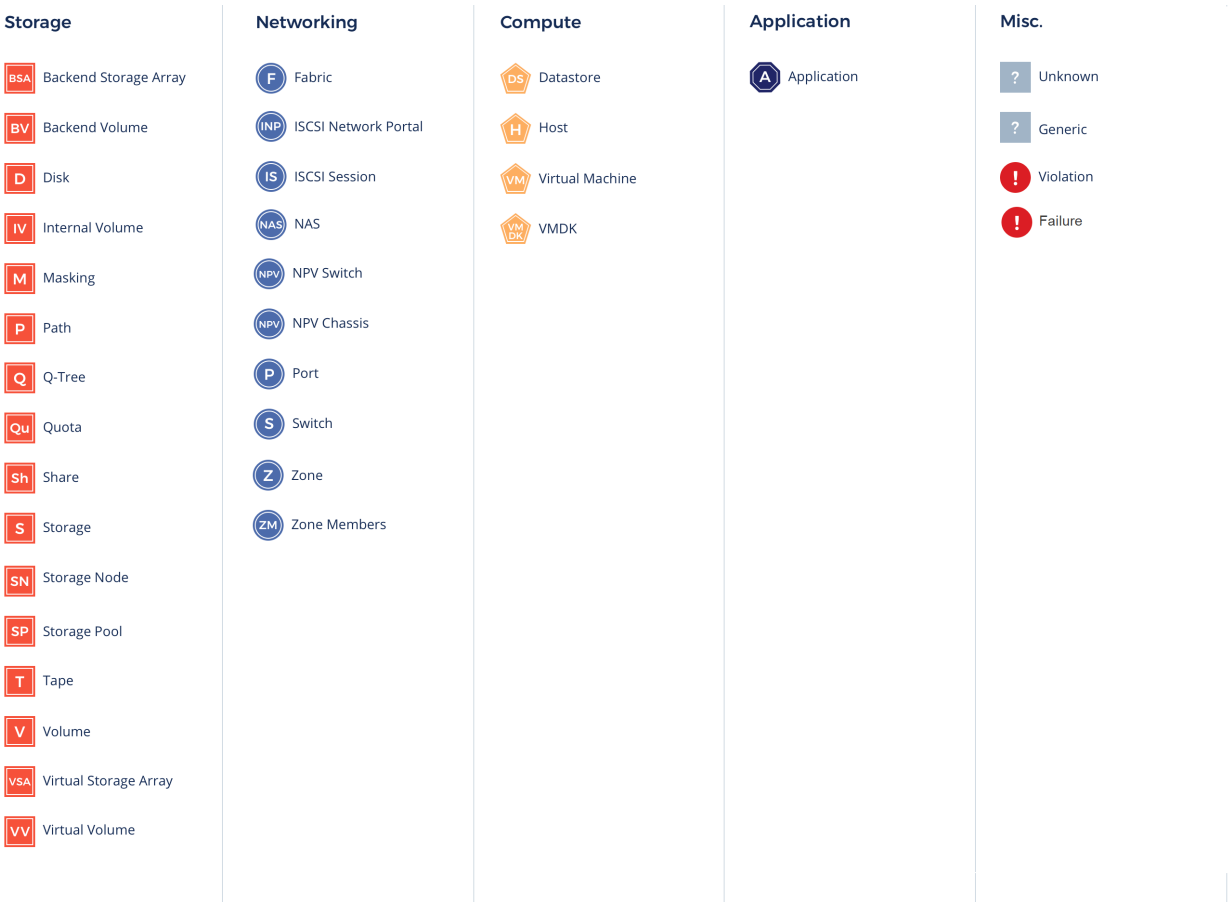
トラブルシューティング

追加情報はから入手できます "サポート" ページ

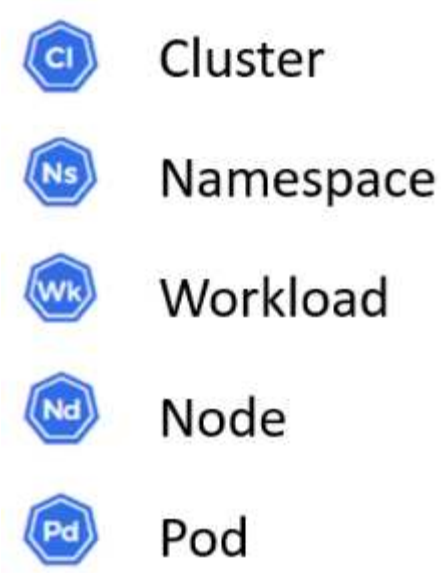
オブジェクトアイコンリファレンス

Data Infrastructure Insightsで使用されるオブジェクトアイコン。

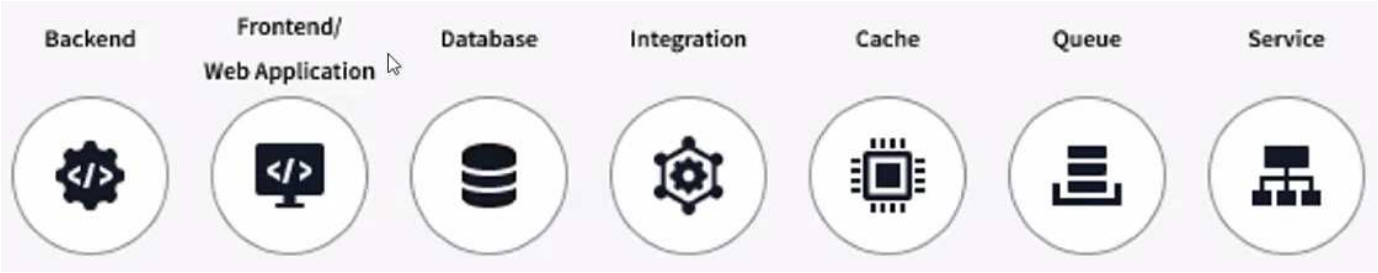
インフラストラクチャアイコン：



Kubernetesのアイコン：



Kubernetesのネットワークパフォーマンスの監視とマップアイコン：



法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp 、 NetApp のロゴ、および NetApp の商標ページに記載されているマークは、 NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

"データインフラに関する分析情報（旧称Cloud Insights）に関するお知らせ"

"ワークロードのセキュリティに関する通知（旧称Cloud Secure ）"