Data Infrastructure Insightsのドキュメント

Data Infrastructure Insights

NetApp
February 18, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/data-infrastructure-insights/index.html on February 18, 2026. Always check docs.netapp.com for the latest.

目次

Data Infrastructure Insightsのドキュメント 1
Data Infrastructure Insights は何ができるのでしょうか? 1
はじめに 1
Data Infrastructure Insightsの新機能 2
2025年12月 2
共有クエリによるクエリアクセスの制御 2
モニター管理時のフィルタリングの改善 3
よりクリーンなダッシュボードの視覚化 4
2025年11月 4
パーソナライズされたホームページを設定する 4
自動ダッシュボードグループ化で整理整頓 5
2025年10月 5
インフラストラクチャの健全性: ストレージとファブリックのリスクを即座に可視化 5
正確な警告のためのマルチコンディションモニター 6
クエリの改善: 一目でわかるオブジェクトの詳細 7
ワークロードセキュリティの改善 7
2025年8月 8
指先で操作できる集中ウィジェットデータ 8
ダッシュボードのエクスポートとインポート 8
強化されたクラウド統合: Google Cloud NetApp Volumes (GCNV) のサポート 9
強化されたStorageGRID監視 9
オペレーティングシステムのサポート 9
2025年6月 9
VM Analyzer: VMからストレージまでの包括的な可視性とトラブルシューティング 9
オペレーティングシステムのサポート 10
2025年5月 10
新しいランディングページで流れを維持 10
ワークロードセキュリティの改善 11
.CSV 非同期エクスポート 13
2025年4月 13
プロアクティブな問題解決のためのラインウィジェットにおける ML を活用した異常境界 13
VSAN ストレージ サポートによる VMware コストの最適化 14
アラートの詳細をすぐに確認 15
ワークロードセキュリティフォレンジック非同期エクスポート 15
ルールにグループ化されたデータコレクター通知 15
2025年3月 16
効率的なインフラストラクチャ管理のための強化されたコンテキストナビゲーション 16
削除された資産の履歴を保存する 16
Kubernetes オペレーターのプッシュボタンアップグレード 17

ストレージ ワークロード セキュリティ データ コレクターの接続テスト 18
オペレーティングシステムのサポート 18
2025年2月 19
DII API使用状況追跡：セキュリティと効率性の向上 19
ユーザーを制限するワークロードセキュリティAPI 20
2025年1月 20
フォレンジックグループでリスクを積極的に管理 20
ダッシュボードのアクセス制御 21
2024年12月 22
SAN Analyzer のご紹介: ブロック ワークロードの可視性強化 22
インテリジェントなホスト廃止と VM 再利用による VM コストの最適化 23
時間チャートとテーブルウィジェットのサポートによりログの洞察を明らかに 24
2024年11月 25
新しいワークロード セキュリティ アラート API 25
環境内の構成変更を分析する 25
KubeVirt サポート: Kubernetes
クラスター内で実行されている仮想マシンのワークロードを監視します 25
2024年10月 26
モニターのカスタム式で新たな洞察を獲得 26
メンテナンス期間中のアラートの中断を最小限に抑える 26
新しいアラート通知ルールでアラート管理を効率化 27
ダッシュボードのログ分析 28
VMware イベントによる VMware の可観測性の向上 28
データコレクターの更新: 29
2024年9月 29
Data Infrastructure Insights（旧Cloud Insights）のご紹介 29
2024年8月 29
時間範囲に固有のデータを表示する 29
変化と変化率（%）分析 29
ログクエリ結果を .CSV にエクスポートする 30
時間でアラートを解決する 30
2024年7月 31
AIOps: 異常検出 31
ワークロードセキュリティの改善 31
ダッシュボードのナビゲーションが簡単になりました 31
2024年6月 32
オペレーティングシステムのサポート 32
2024年5月 32
時間に基づいてアラートを自動的に解決する 32
2024年4月 33
Kubernetes の iSCSI サポート 33

オペレーティングシステムのサポート 34
2024年3月 34
ワークロードセキュリティエージェントの詳細 34
より多くのデータをより速くグラフ化 34
2024年2月 35
ユーザビリティの改善 35
名前空間内のすべての変更を表示する 36
アラートの関連ログ 37
ONTAPスイッチデータの収集 37
ワークロードセキュリティデータコレクターAPI 37
2024年1月 38
まだ使っていないCloud Insights の機能を試す 38
私のワークロードはどの程度健全でしょうか? 38
データコレクターの更新 38
強化されたランサムウェア検出MLアルゴリズム 38
非推奨の機能 39
2023年12月 39
変更分析の概要 39
Kubernetes ワークロード パフォーマンス ダッシュボード 40
クエリの詳細を1つの画面で表示 41
データコレクターの更新: 42
2023年11月 42
ワークロード セキュリティ: コレクターの一時停止/再開 42
ストレージノードのサポート情報 43
VMWare タグをCloud Insights のアノテーションにマッピングする 43
Brocade CLI コレクターの信頼性強化 (FOS 9.1.1c 以降のファームウェア) 43
2023年10月 43
強化されたワークロードセキュリティ 43
モジュールトライアル 44
指定されたドメインへのアクセスを制限する 44
データコレクターの更新 44
2023年9月 45
ログから必要なものを簡単に見つける 45
「フローティング」ログ詳細パネル 46
メニューを折りたたむ 47
データコレクターの改善 48
2023年8月 48
Isilon/PowerScale ログと高度な分析データの収集 49
改善されたワークロードマップ 49
Kubernetes 管理ユニットの使用量の調整 49
コレクター/取得の変更: 50

改善されたメニュー 50
2023年7月 52
最近の変更を表示 52
オペレーターの改善 52
洞察：冷蔵倉庫の再利用 53
オペレーター画像署名 53
クエリの集計、条件付き書式など 53
監査用API 54
データ収集者:Trident・エコノミー 55
2023年6月 55
使用状況を確認する 55
Kubernetesネットワーク監視とマップはすべての 55
コレクター/取得の変更: 55
新しいONTAP Essentials ダッシュボード 56
追加のシステムモニター 56
2023年5月 56
Kubernetes モニタリング オペレーターのインストールの改善 56
ストレージ仮想化 56
新しいWebhookパラメータ 57
Kubernetesデータのレポート 57
新規顧客向けにデフォルトのONTAPシステム モニターを有効化 57
2023年4月 57
Kubernetes パフォーマンス監視とマップ 57
ONTAP Essentials セキュリティダッシュボード 58
ONTAPコールド ストレージの再利用 59
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 60
レポートの見た目が新しくなりました 60
デフォルトで一時停止するモニター 60
API メータリング タブをお探しですか? 60
2023年3月 60
ONTAP 9.9以降のクラウド接続は廃止されました 61
2023年1月 61
新しいログモニター 61
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 61
2022年12月 61
Cloud Insightsトライアルでランサムウェア保護やその他のセキュリティ機能をご確認ください 61
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 61
チェックサムを確認する 62
ログアラートの改善 62
ビジネス継続性のためのSnapMirrorをカバーする11の新しいデフォルトのONTAPモニター 63
2022年11月 63

40 を超える新しいセキュリティ、データ収集、CVO モニター! 63
2022年10月 63
ONTAP Autonomous Ransomware Protection の統合により、より優れた正確なランサムウェア検出を実現 64
2022年9月 64
ベーシックエディションで利用可能なモニター 64
ONTAP PowerとStorageGRIDダッシュボード 64
表で一目でわかるしきい値の可視性 64
セキュリティモニター 64
どこからでもチャット 65
より目に見えるインサイト 65
新しいデータ収集者 65
その他のデータコレクターの更新 65
オペレーティングシステムのサポート 65
2022年8月 66
Cloud Insights の外観が新しくなりました。 66
処理を開始するには、ONTAP Essentials をチェックしてください! 66
ストレージデータファミリーが統合される 67
ストレージはどれくらいの電力を消費していますか? 68
プレビューから卒業した機能 69
データ収集の健全性はどうですか? 69
自動更新APIトークン 70
ベーシックエディションでは、これまで以上の機能が提供されます 70
さらに詳しく知りたいですか? 70
オペレーティングシステムのサポート 70
2022年6月 70
Kubernetes クラスターの飽和状態とその他の詳細 70
あなたの Kubernetes クラスターは何年経っていますか? 71
容量満杯までの時間予測 71
私の環境で何が変わったのでしょうか? 72
オペレーティングシステムのサポート 73
更新されたTelegrafエージェント 73
プレビュー機能 73
2022年5月 74
NetAppサポートとライブチャット 74
Kubernetesオペレーター 74
APIを使用してユーザーと招待を管理する 75
データ収集アラート 75
ONTAPストレージの変更に関するアラート 75
プレビュー機能 75
2022年4月 76

フィードバックを共有してください! 76
ダッシュボードエディターの更新 76
Kubernetes インフラストラクチャの強化された監視 77
プレビュー機能 77
新しいデータ収集者 77
その他のデータコレクターの更新 77
2022年3月 78
ONTAP 9.9以降のクラウド接続 78
NetApp ONTAPモニター用の新しい FSx 78
すべてのユーザーが利用できる新しいCloud Secure機能 78
更新されたTelegrafエージェント 79
データコレクターの更新 79
2022年2月 79
Cloud Insights がApache Log4j の脆弱性に対処 79
Kubernetes 名前空間の詳細ページ 79
2021年12月 80
ONTAPシステムとのより緊密な統合 80
ログのクエリ 80
データコレクターレベルの通知。 81
Cloud Secure の役割の柔軟性の向上 81
オペレーティングシステムのサポート 81
データコレクターの更新 81
2021年11月 82
適応型ダッシュボード 82
API経由でレポートデータベースにアクセスする 83
VM ランディング ページのポッド テーブル 83
データコレクターの更新 83
サポートされている追加のオペレーティングシステム 84
2021年10月 84
K8Sエクスプローラーページのフィルター 84
レポート用K8sデータ 84
ダークテーマが登場 85
データコレクターのサポート 85
2021年9月 85
パフォーマンスポリシーがモニターになりました 85
モニターの自動補完候補、ワイルドカード、および式 85
更新されたTelegrafエージェント 86
データコレクターのサポート 86
2021年8月 87
新しい監査ページのユーザーインターフェース 87
強化されたユーザーロール管理 87

2021年6月 87
フィルターのオートコンプリート候補、ワイルドカード、および式 87
エディション別に利用可能なAPI 88
Kubernetes PVとPodの可視性 88
Kubernetes ノードから VM へのリンク 88
パフォーマンス ポリシーに代わるアラート モニター 89
Cloud SecureはNFSをサポート 90
Cloud Secureスナップショットの消去 90
Cloud Secureデータ収集速度 90
2021年5月 90
更新されたTelegrafエージェント 91
アラートに是正措置を追加する 91
すべてのエディション向けのCloud Insights API 91
2021年4月 92
モニターの管理が簡単 92
Webhookを使用した強化されたアラートオプション 92
デバイス識別の改善 92
もっと求めてたよ！ 93
1 つのCloud Insights環境で複数のサブスクリプション 93
あなたの道を選びなさい 93
より簡単なCloud Secureオンボーディング 93
2021年2月 94
更新されたTelegrafエージェント 94
クラウドコストアナライザー 94
フィルターを使用して null 値を持つオブジェクトを照会する 95
マルチリージョンサポート 95
2021年1月 95
追加のONTAPメトリックの名前が変更されました 95
新しい Kubernetes エクスプローラー 97
2020年12月 98
よりシンプルなKubernetesのインストール 98
2020年11月 98
追加のダッシュボード 98
テーブルウィジェットの列名の変更 98
2020年10月 99
統合データのデフォルトの拡張 99
ベーシックエディションのテクニカルサポート 99
Cloud SecureパブリックAPI 99
2020年9月 99
統合データを含むクエリページ 99
テーブルウィジェットの単位表示書式 100

取得ユニット詳細ページ 100
Cloud SecureDocker依存関係の削除 100
ユーザーロールの報告 100
データ取り込み用の新しい API カテゴリ 101
2020年8月 101
監視と警告 101
2020年7月 102
Cloud Secure_スナップショット_アクション 102
メトリック/カウンターの更新 103
Cloud Secure潜在的攻撃検出 104
AWS 経由でプレミアムエディションをサブスクライブする 105
強化されたテーブルウィジェット 105
メトリクスフィルタリング 106
ONTAP高度なカウンタデータ 107
高度なカウンターダッシュボード 109
詳細情報 109
ポリシーと違反メニュー 109
更新されたTelegrafエージェント 109
2020年6月 110
簡素化されたデータコレクターエラーレポート 110
ウィジェットの改善 110
2020年5月 111
ユーザーロールの報告 111
Cloud Secureアップデート 112
ダッシュボードのグループ化 112
ダッシュボードのピン留め 113
TVモードと自動更新 113
2020年4月 114
新しいダッシュボードの時間範囲の選択肢 114
Cloud Secureアップデート 114
デフォルトのダッシュボード時間 114
最適化された集約時間 114
表示単位の自動フォーマット 114
APIを使用して注釈をインポートする 115
よりシンプルなウィジェットセレクター 115
2020年2月 116
プレミアムエディションのAPI 116
データコレクター追加後の初期ポーリング 116
ウィジェットの複製が簡単に 117
シングルサインオン（SSO） 117
2020年1月 118

REST API の Swagger ドキュメント 118
機能チュートリアルの進捗バー 118
取得ユニットの変更 118
ウィジェットにおける時間集計の最適化 118
簡素化された「 Cloud Insightsを使い始める」プロセス 118
Data Infrastructure Insightsインサイトオンボーディング 120
NetApp Console アカウントの作成 120
すでにNetApp Consoleログインをお持ちの場合はどうすればよいですか？ 120
Data Infrastructure Insights無料トライアルを開始する 120
ログアウト 121
非アクティブ時のタイムアウト 121
セキュリティ 122
Data Infrastructure Insightsセキュリティ 122
セキュリティの概要 122
情報と地域 124
Data Infrastructure Insights はどのような情報を保存しますか? 124
私の情報はどこに保存されますか? 125
詳細情報 126
セキュリティ管理ツール 126
アップグレードとインストールに関する考慮事項 127
買収部門のセキュリティ管理 127
開始する前に 127
SecurityAdminツールの使用 127
ツールを実行するユーザーを指定する 129
プロキシの更新または削除 130
外部キーの取得 131
APIで使用するパスワードの暗号化 132
はじめに 135
ビデオチュートリアルを始める 135
チェックリストとビデオチュートリアル 135
ビデオチュートリアル 136
データの収集 136
データ収集を始める 136
取得ユニットの要件 139
取得ユニットの設定 141
データ収集のためのエージェントの構成 (Windows/Linux) 148
データコレクターの構成 160
データコレクターの取得状況の判断 161
構成されたデータコレクターの管理 161
失敗したデータ収集装置の調査 163
ダッシュボードのインポート 164

ダッシュボードギャラリーからのインポート 164
エクスポートしたダッシュボードのインポート 164
ユーザーアカウントとロール 165
権限レベル 165
ユーザーを招待してアカウントを作成する 168
既存のユーザーの役割を変更する 169
ユーザーの削除 170
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 170
ドメインによるアクセス制限 173
Data Infrastructure Insightsデータコレクターリファレンスリスト 175
Data Infrastructure Insightsの購読 179
トライアル版 179
AWS Marketplace でのトライアル 180
試用期間が終了したらどうなりますか? 180
*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? 180
モジュール評価 180
見積もり 181
サブスクリプションオプション 182
可観測性メータリング 182
ワークロードセキュリティメータリング 183
どうやって登録すればいいですか? 183
NetApp Sales Directを通じて申し込む 183
AWS Marketplace を通じてセルフサブスクライブ 184
サブスクリプションのステータスを表示する 184
使用状況管理を表示する 185
登録した使用量を超えた場合はどうなりますか? 186
直接購読してトライアルをスキップ 186
資格IDの追加 186
可観測性 188
ダッシュボードの作成 188
ダッシュボードの概要 188
ダッシュボードの機能 192
ダッシュボードアクセス管理 225
ダッシュボードとウィジェットのベストプラクティス 227
サンプルダッシュボード 230
クエリの操作 235
アセットとメトリクスのクエリ 235
クエリの作成 236
クエリの表示 243
クエリ結果を .CSV ファイルにエクスポートする 243
クエリの変更または削除 245

資産に複数のアプリケーションを割り当てたり、資産から複数のアプリケーションを削除したりする 246
テーブルの値のコピー 247
ログエクスプローラー 247
非アクティブなデバイスの識別 252
洞察 253
洞察 253
洞察：ストレス下における共有リソース 253
洞察：Kubernetes 名前空間のスペース不足 256
洞察: ONTAPコールド ストレージの再利用 257
モニターとアラート 260
モニターによるアラート 260
モニターからのアラートの表示と管理 270
電子メール通知の設定 273
異常検出モニター 276
システムモニター 280
Webhook通知 355
注釈の操作 369
注釈の定義 369
注釈の使用 372
アノテーション ルールの作成 374
注釈のインポート 376
アプリケーションの操作 378
アプリケーション別の資産使用状況の追跡 378
アプリケーションの作成 379
自動デバイス解決 380
自動デバイス解決の概要 380
デバイス解像度ルール 383
ファイバーチャネルデバイスの解像度 385
IPデバイスの解像度 388
設定タブのオプションの設定 390
正規表現の例 391
資産ページ情報 397
資産ページの概要 397
コンテキスト内のオブジェクトのフィルタリング 402
ストレージ仮想化 404
資産とアラートを検索するためのヒントとコツ 406
データの分析 408
SANアナライザの概要 408
VMアナライザーの概要 411
インフラストラクチャの健全性を監視する 412
レポート 414

Data Infrastructure Insightsレポートの概要 414
Data Infrastructure Insightsレポートユーザーロール 416
定義済みレポートを簡単に作成 418
ストレージマネージャーダッシュボード 421
レポートの作成（例） 424
レポートの管理 427
カスタムレポートの作成 430
API経由でレポートデータベースにアクセスする 438
レポート用の注釈の公開と非公開 442
レポート用の履歴データの保存方法 443
Data Infrastructure Insightsレポートスキーマダイアグラム 444
Data Infrastructure Insightsサイト レポート用スキーマ 496
Kubernetes 498
Kubernetes クラスターの概要 498
フィルターの改良 498
NetApp Kubernetes Monitoring Operator をインストールまたはアップグレードする前に 499
始める前に注意すべき重要な事項 500
Kubernetes モニタリング オペレーターのインストールと構成 503
Kubernetesモニタリングオペレーターをインストールする前に 503
Kubernetes モニタリング オペレーターのインストール 504
Kubernetes 監視コンポーネント 506
最新のKubernetesモニタリングオペレーターへのアップグレード 507
Kubernetes モニタリング オペレーターの停止と起動 508
アンインストール 508
Kube-state-metricsについて 509
オペレーターの設定/カスタマイズ 509
秘密についてのメモ 513
Kubernetes モニタリング オペレーター イメージ署名の検証 514
トラブルシューティング 515
Kubernetes モニタリング オペレーターの設定オプション 523
サンプル AgentConfiguration ファイル 523
Kubernetes クラスターの詳細ページ 540
名前空間、ノード、ポッドの数 541
共有リソースと飽和 541
ネームスペース 541
ワークロード 542
クラスター「ホイール」 542
ゲージに関する注意 545
Kubernetes ネットワークパフォーマンス監視とマップ 545
前提条件 546
モニター 547

地図 547
ワークロードの詳細とアラート 549
検索とフィルタリング 549
ワークロードラベル 550
深く潜る 551
Kubernetes 変更分析 553
フィルタ 554
クイックステータス 555
詳細パネル 556
ONTAPエッセンシャル 558
概要 558
データ保護 559
セキュリティ 560
アラート 564
インフラ 565
ネットワーク 566
ワークロード 566
管理およびその他のタスク 568
Data Infrastructure InsightsAPI 568
APIアクセスの要件 568
APIドキュメント（Swagger） 568
APIアクセストークン 569
API タイプ 570
インベントリトラバーサル 571
拡大 571
パフォーマンス データ 573
オブジェクトパフォーマンスメトリック 575
パフォーマンス履歴データ 575
容量属性を持つオブジェクト 576
検索を使用してオブジェクトを検索する 577
APIトークンの無効化または取り消し 577
期限切れのAPIアクセストークンのローテーション 578
環境の監視 579
監査 579
Active IQ Digital Advisor 582
ワークロードセキュリティ 585
ストレージワークロードセキュリティについて 585
可視性 585
保護 585
コンプライアンス 585
はじめに 585

ワークロードセキュリティ入門 585
ワークロード セキュリティ エージェントの要件 586
ワークロードセキュリティエージェントの導入 590
ワークロードセキュリティエージェントの削除 597
Active Directory (AD) ユーザーディレクトリコレクターの構成 598
LDAPディレクトリサーバーコレクターの構成 603
ONTAP SVMデータコレクターの設定 608
ONTAP SVM データコレクタのトラブルシューティング 619
Cloud Volumes ONTAPとAmazon FSx for NetApp ONTAPコレクターの構成 626
ユーザー管理 627
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 628
アラートの理解と調査 632
アラート 633
フィルターオプション 634
アラートの詳細ページ 635
_スナップショットを撮る_アクション 636
アラート通知 637
保持ポリシー 637
トラブルシューティング 638
法医学 638
法医学 - すべての活動 638
フォレンジックユーザーの概要 649
自動応答ポリシー 650
許可されるファイルタイプのポリシー 652
ONTAP Autonomous Ransomware Protectionとの統合 653
前提条件 654
ユーザー権限が必要です 654
サンプルアラート 654
制限事項 656
トラブルシューティング 656
ONTAPとの統合アクセスが拒否されました 656
前提条件 656
ユーザー権限が必要です 657
アクセス拒否イベント 657
攻撃を阻止するためにユーザーアクセスをブロックする 658
ユーザーアクセスブロックの前提条件 658
この機能を有効にするにはどうすればいいですか? 659
自動ユーザーアクセスブロックを設定するにはどうすればいいですか? 659
システム内にブロックされたユーザーがいるかどうかを知るにはどうすればいいですか? 659
ユーザーアクセスを手動で制限および管理する 659
ユーザーアクセス制限履歴 659

機能を無効にするにはどうすればいいですか? 660
NFSのIPを手動で復元する 660
SMBのユーザーを手動で復元する 661
トラブルシューティング 662
ワークロードセキュリティ: ファイル改ざんのシミュレーション 663
始める前に注意すべきこと 663
ガイドライン: 664
手順： 664
プログラムでサンプル ファイルを生成します。 665
コレクターを再開する 666
プログラムでサンプル ファイルを生成します。 666
ワークロードセキュリティでアラートを生成する 667
アラートを複数回トリガーする 668
アラート、警告、エージェント/データソースコレクターの正常性に関する電子メール通知の構成 668
潜在的な攻撃の警告と警告 668
エージェントとデータコレクターのヘルスモニタリング 668
エージェントとデータコレクターのアップグレード通知の受信 669
トラブルシューティング 669
Webhook通知 669
Webhookを使用したワークロードセキュリティ通知 669
Discord 向けワークロード セキュリティ Webhook の例 675
PagerDuty のワークロード セキュリティ Webhook の例 678
Slack 向けワークロード セキュリティ Webhook の例 683
Microsoft Teams のワークロード セキュリティ Webhook の例 687
ワークロードセキュリティAPI 692
APIドキュメント（Swagger） 693
APIアクセストークン 693
API経由でデータを抽出するスクリプト 694
ONTAP SVM データコレクタのトラブルシューティング 694
トラブルシューティング 702
一般的なData Infrastructure Insightsの問題のトラブルシューティング 702
ログインに関する問題 702
その他の問題 703
リソース 703
Linux での取得ユニットの問題のトラブルシューティング 704
プロキシとファイアウォールに関する考慮事項 706
リソース 707
Windows での取得ユニットの問題のトラブルシューティング 707
プロキシとファイアウォールに関する考慮事項 709
リソース 710
失敗したデータ収集装置の調査 710

Data Infrastructure Insightsデータコレクターサポートマトリックス 712
HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ ストレージ 712
アマゾンAWSEC2 730
アマゾンAWSS3 735
Microsoft Azure NetApp Files 740
Brocadeファイバーチャネルスイッチ 747
Brocadeネットワークアドバイザー HTTP 759
BrocadeFOS REST 763
Cisco MDS および Nexus ファブリック スイッチ 774
結束力 784
EMC Celerra (SSH) 792
EMC CLARiX (NaviCLI) 800
EMC データドメイン (SSH) 813
EMC ECS 822
Dell EMC IsilonとPowerScale Rest 829
Dell EMC Isilon / PowerScale (CLI) 848
EMC PowerStore REST 861
EMC RecoverPoint (HTTP) 874
EMC ScaleIO および PowerFlex REST 878
EMC Symmetrix CLI 883
Dell ユニスフィア REST 904
EMC VNX (SSH) 920
EMC VNXe と Unity Unisphere (CLI) 939
EMC VPLEX 952
EMC XtremIO (HTTP) 954
NetApp Eシリーズ 966
ピュアストレージ フラッシュブレード REST 981
Google Cloud コンピューティング 991
HDS HCP (HTTPS) 996
HiCommand デバイス マネージャー 1000
日立オプスセンター 1016
HDS HNAS (CLI) 1031
HPE Nimble / Alletra 6000 ストレージ 1040
Huawei OceanStor（REST/HTTPS） 1051
IBM クレバーセーフ 1068
IBM DS 8K (DSCLI) 1073
IBM PowerVM (SSH) 1083
IBM SVC (CLI) 1086
IBM XIV & A9000 (XIVCLI) 1103
インフィニダット インフィニボックス (HTTP) 1108
Microsoft Azure コンピューティング 1116
Microsoft Hyper-V 1121
NetApp 7 モード 1131

NetApp Eシリーズ REST 1152
Amazon FSx for NetApp ONTAP 1160
NetAppクラスタ化Data ONTAP 8.1.1+ 1176
ASA 1210
NetApp ONTAP REST 1223
NetApp SolidFire 8.1 以上 1244
NetAppStorageGRID(HTTPS) 1261
Nutanix ストレージ (REST) 1274
Oracle ZFS (HTTPS) 1286
ピュアストレージ フラッシュアレイ (HTTP) 1299
レッドハット RHV (REST) 1314
ルーブリックストレージ 1318
VAST データストア 1327
NetApp HCI仮想センター 1338
VMware Cloud on AWS 1348
VMware vSphere (Web サービス) 1354
リファレンスとサポート 1368
サポートのリクエスト 1368
サポート資格の有効化 1368
サポート情報の入手 1371
Data Infrastructure Insightsデータコレクターサポートマトリックス 1372
データコレクターリファレンス - インフラストラクチャ 1372
ベンダー固有のリファレンス 1372
Amazon EC2 データコレクターの設定 1373
Amazon FSx for NetApp ONTAPデータコレクター 1376
Azure コンピューティング データ コレクターの構成 1379
Broadcom 1380
Cisco MDS ファブリック スイッチ データ コレクター 1388
Cohesity SmartFiles データコレクター 1390
Dell 1391
Dell EMC 1392
富士通 Eternus データコレクター 1417
NetApp Google Compute データコレクター 1419
Google Cloud NetApp Volumesデータコレクター 1420
HPエンタープライズ 1421
日立データシステムズ 1429
Infinidat InfiniBox データコレクター 1438
Huawei OceanStorデータコレクター 1439
IBM 1440
Lenovoデータコレクター 1447
Microsoft 1448
NetApp 1451

Nutanix NX データコレクター 1491
Oracle ZFS Storage Appliance データコレクター 1492
Pure Storage FlashArray データコレクター 1495
Red Hat Virtualization データコレクター 1496
Rubrik CDM データコレクター 1497
VMware VSphere データコレクターの構成 1499
データコレクターリファレンス - サービス 1502
ノードデータ収集 1502
ActiveMQ データコレクター 1505
Apache データコレクター 1507
領事データコレクター 1510
Couchbase データコレクター 1511
CouchDB データコレクター 1513
Docker データコレクター 1515
Elasticsearch データコレクター 1522
Flinkデータコレクター 1524
Hadoop データコレクター 1529
HAProxy データコレクター 1535
JVMデータコレクター 1542
Kafka データコレクター 1547
Kibana データコレクター 1550
Kubernetes モニタリング オペレーターのインストールと構成 1552
Memcached データコレクター 1571
MongoDB データコレクター 1573
MySQL データコレクター 1575
Netstat データコレクター 1580
Nginx データコレクター 1581
PostgreSQL データコレクター 1584
Puppet エージェント データコレクター 1586
Redis データコレクター 1588
オブジェクトアイコンリファレンス 1590
インフラストラクチャアイコン: 1590
Kubernetes アイコン: 1590
Kubernetes ネットワーク パフォーマンス監視とマップ アイコン: 1591
法律上の表示 1592
著作権 1592
商標 1592
特許 1592
プライバシー ポリシー 1592
オープンソース 1592

Data Infrastructure Insightsのドキュメント

NetApp Data Infrastructure Insights (旧称Cloud Insights) は、インフラストラクチャ全体の可視性を提供するクラウド インフラストラクチャ監視ツールです。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を監視、トラブルシューティング、最適化できます。

Data Infrastructure Insights は何ができるのでしょうか?

Data Infrastructure Insightsはハイブリッド マルチクラウド監視を提供し、インフラストラクチャとワークロードのフルスタックの観測可能性を実現します。

- Kubernetesを含む異機種インフラストラクチャとワークロード向けのデータコレクター
- オープンなTelegrafコレクターとオープンAPIで簡単に統合可能
- 包括的なアラートと通知
- インテリジェントな洞察のための機械学習
- リソース利用の最適化
- 表示ノイズを最小限に抑えて質問に答えるための高度なフィルター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
- ONTAPストレージ運用の健全性を確認する
- 最も貴重なビジネス資産であるデータを、ファイルの改ざんやデータ破壊攻撃から保護します

はじめに

- どうすれば"始めましょう"Data Infrastructure Insightsで?
- 登録しました。さて、どうすればいいでしょうか?"データの取得" "ユーザーの設定"
- 素晴らしい！次は何?"アセットの準備：注釈付け" "必要な資産を見つける: クエリ" "必要なデータを見る: ダッシュボード" "監視とアラート" "データの保護"
- これは素晴らしいですね！私は準備ができています"購読する"。

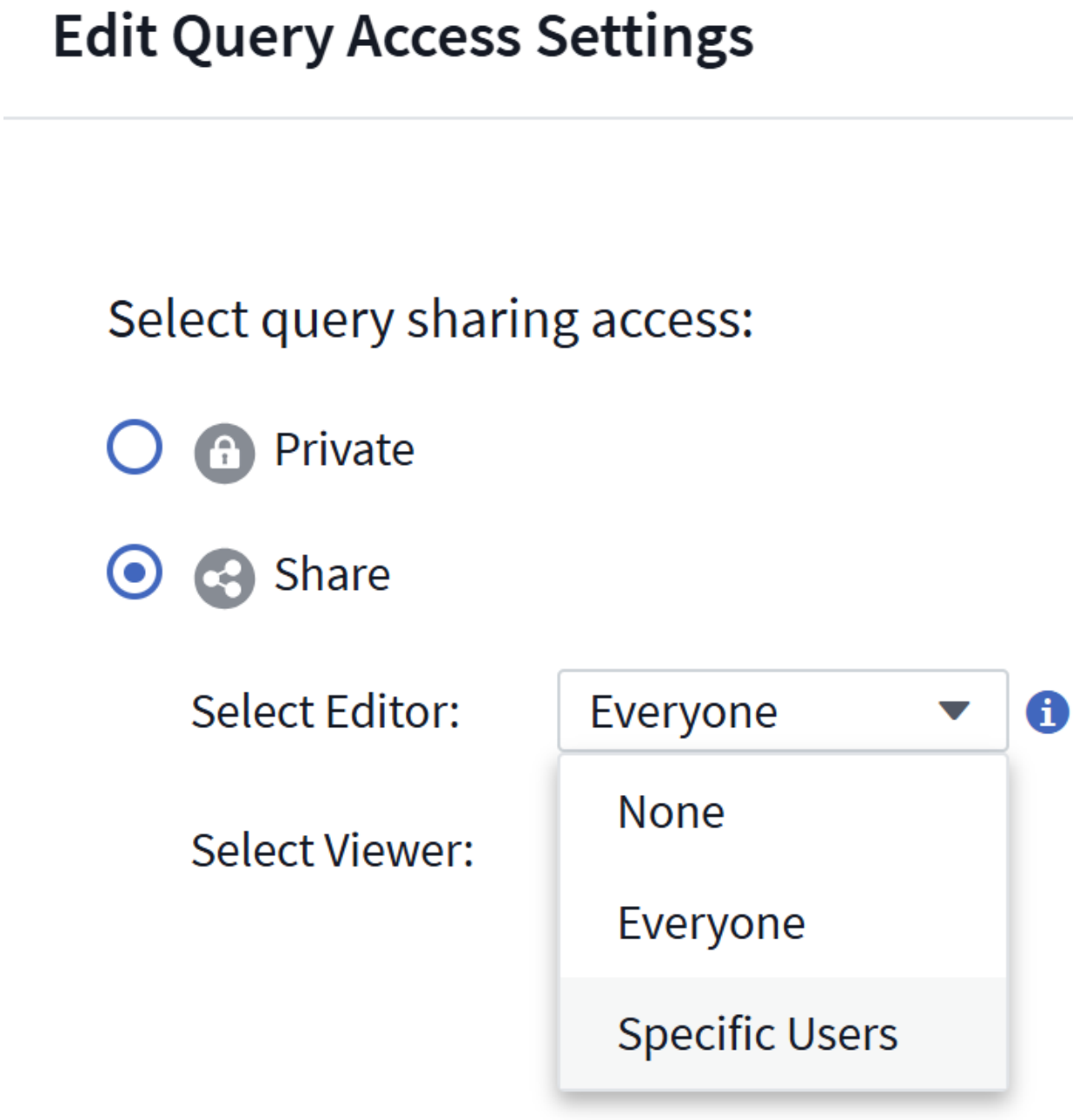
Data Infrastructure Insightsの新機能

NetAppは、製品とサービスを継続的に改善および強化しています。ここでは、Data Infrastructure Insights (旧称Cloud Insights) で利用できる最新の機能の一部を紹介します。

2025年12月

共有クエリによるクエリアクセスの制御

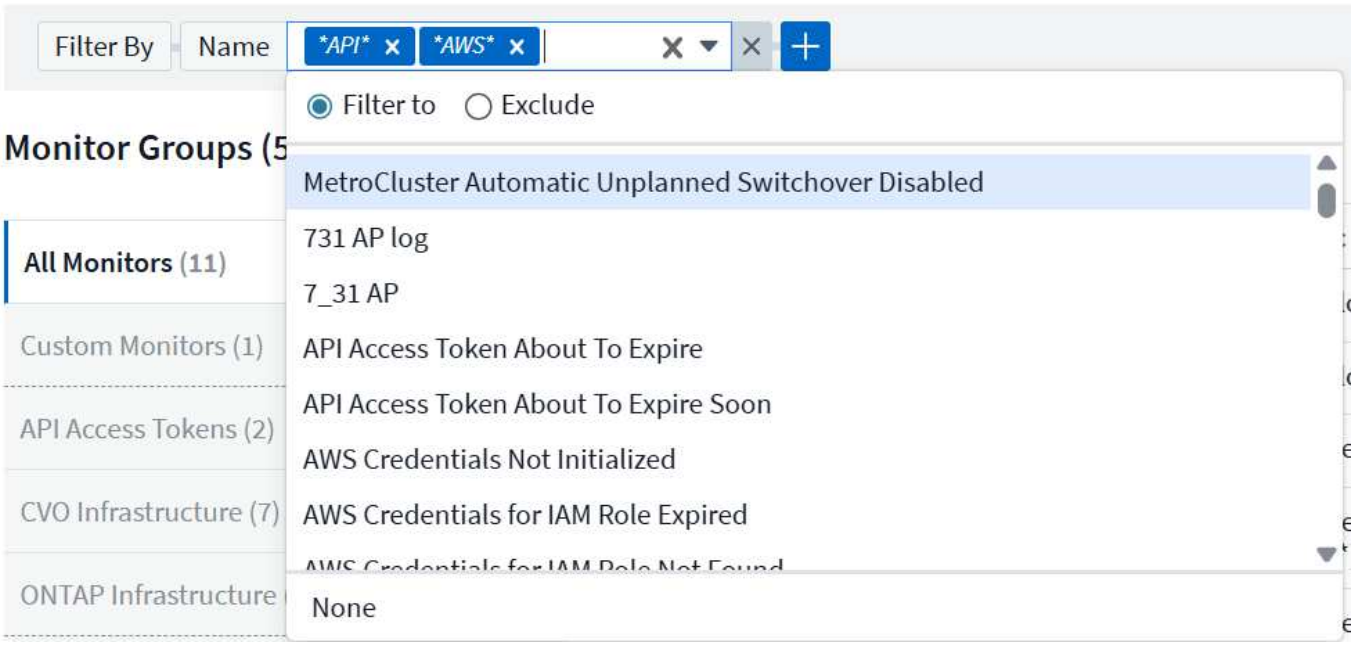
きめ細かな権限制御を使用して作成したクエリを共有します。変更を防止するには読み取り専用のビューアモードを選択し、変更を許可するには編集モードを選択します。プライベートクエリには作成者がアクセスできますが、共有クエリは注釈ルールで活用したり、特殊なユースケース用に複製したりできるため、組織全体でクエリの使用方法や変更方法を完全に制御できます。



さらに、*Guest* ロールを持つユーザーは、独自のプライベートクエリを作成および管理できるようになりました。

モニター管理時のフィルタリングの改善

モニター リストとグループのフィルタリングが改善され、ワイルドカード サポート、複数のフィルタ、含める/除外する機能などが追加されました。



よりクリーンなダッシュボードの視覚化

ダッシュボードのデザインが改善され、最も重要な情報を把握しやすくなりました。ウィジェットを区切るドロップ シャドウ ボーダーによって視覚的な明瞭性が向上し、区切り線が削除されたことで乱雑さが軽減され、データの分析に集中できるようになりました。これらの改良により、よりクリーンで直感的なダッシュボード エクスペリエンスが実現し、傾向や異常をより迅速かつ容易に発見できるようになります。

2025年11月

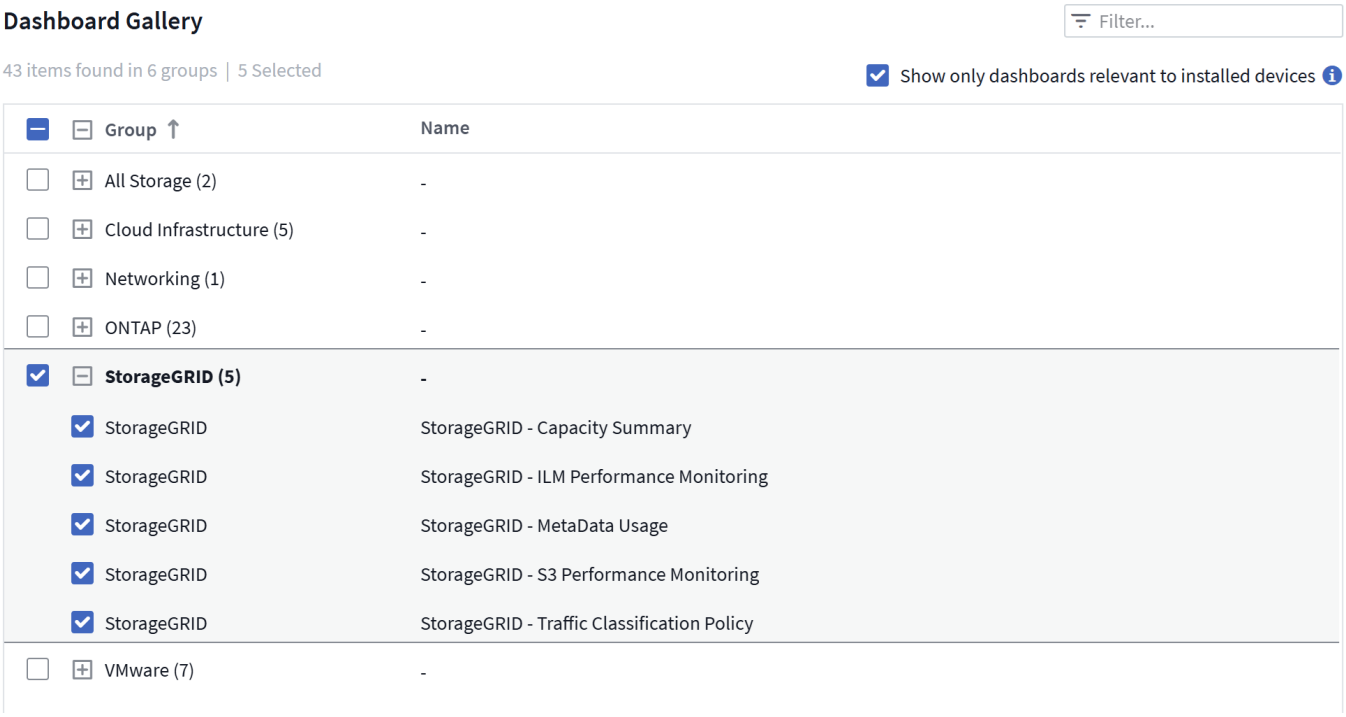
パーソナライズされたホームページを設定する

任意のData Infrastructure Insightsページをパーソナライズされたホームページとして設定することで、毎日の監視ワークフローを効率化します。各ユーザーは、重要なダッシュボード、アラート、インフラストラクチャの健全性、ワークロードのセキュリティなど、自分にとって重要なものに集中するために、異なるホームページを選択できます。



自動ダッシュボードグループ化で整理整頓

インポートされたギャラリー ダッシュボードを論理カテゴリに自動的に整理するインテリジェントなグループ化により、ダッシュボードのエクスペリエンスを変革します。新しいグループ化機能により、ダッシュボードのインポートが簡単になり、各ダッシュボードがその機能と環境との関連性に基づいて適切なグループに配置されます。

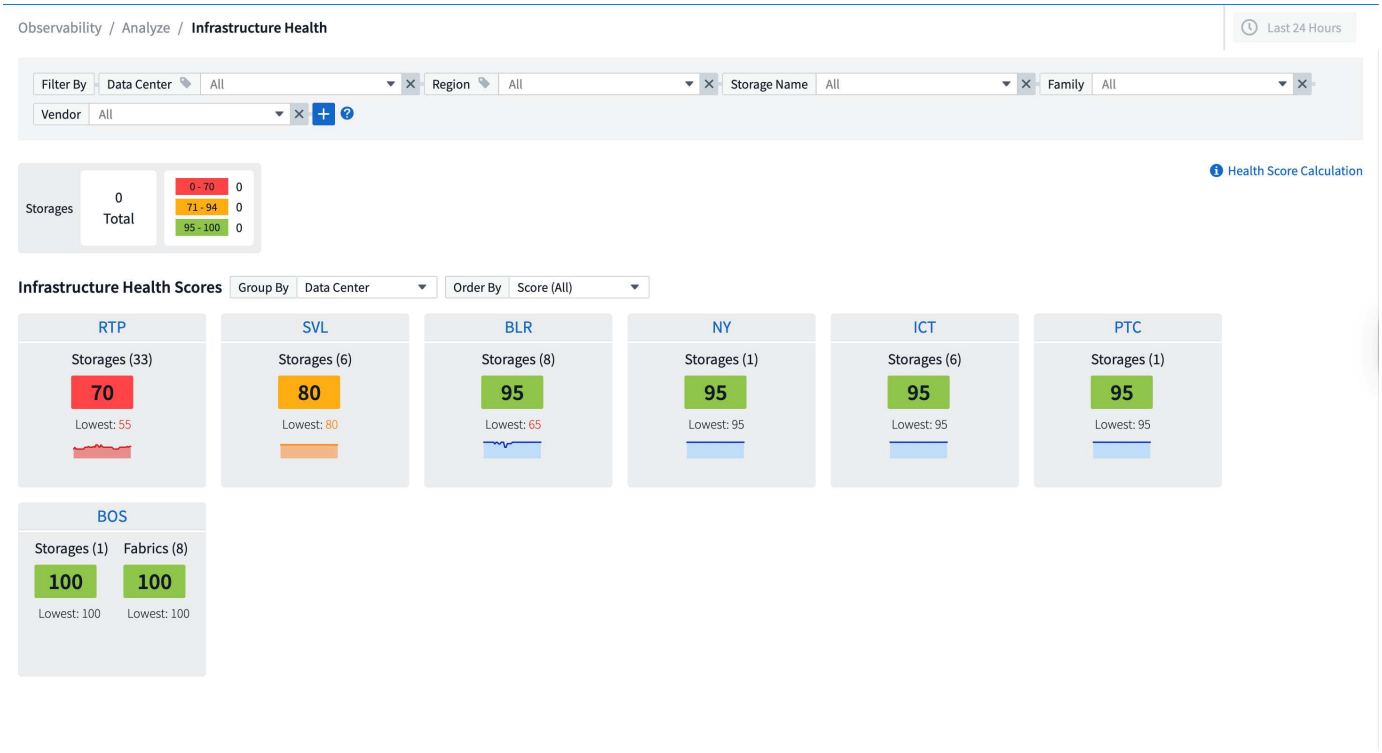


2025年10月

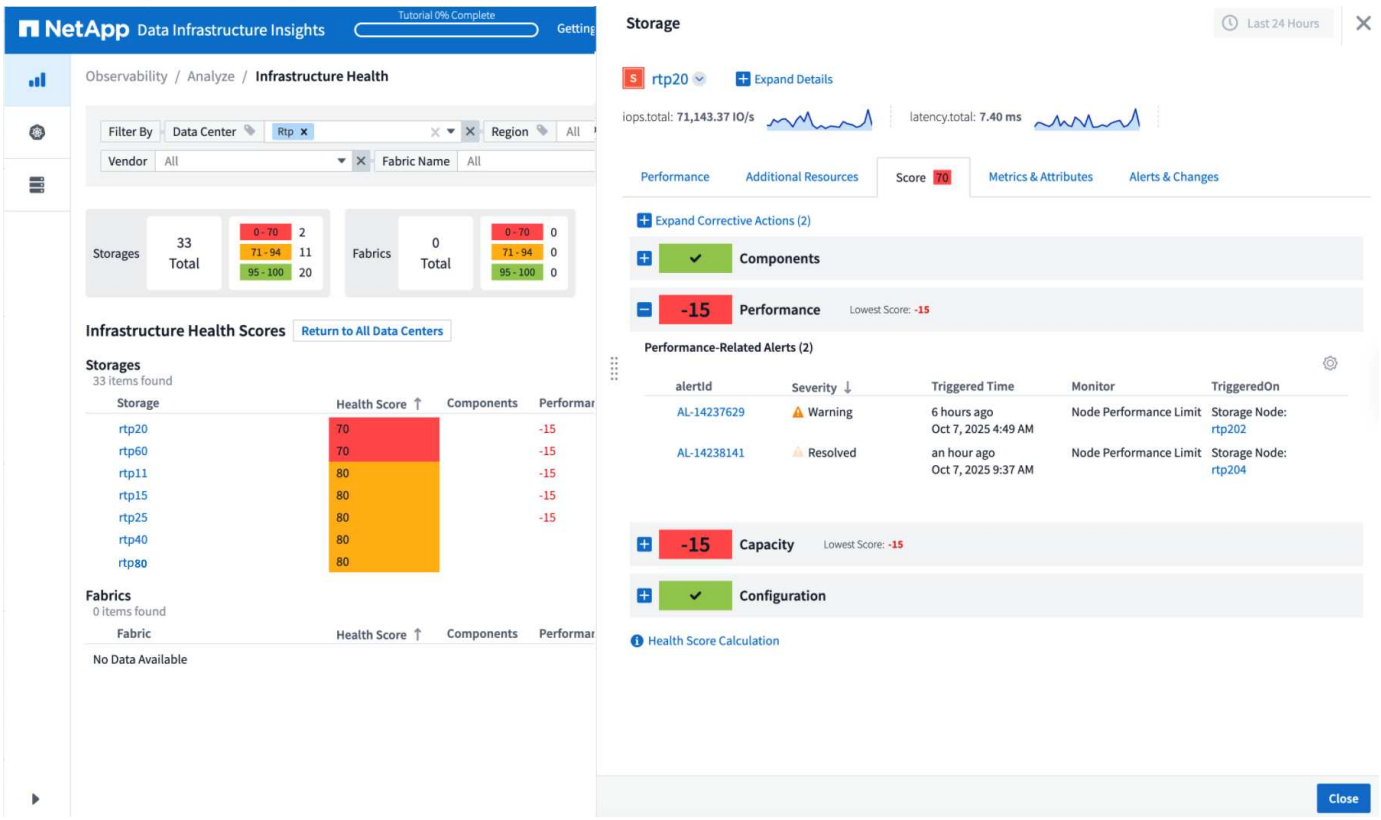
インフラストラクチャの健全性: ストレージとファブリックのリスクを即座に可視化

新しい インフラストラクチャの健全性 機能を使用すると、ストレージとファブリック全体の潜在的なリスクを即座に把握できます。単一の色分けされたダッシュボードにより、統合されたリスクの可視性が得られ、ダウンタイムを最小限に抑え、収益損失を迅速に軽減できます。

100 未満のスコアは潜在的な問題を示します。スコアが低いほど、リソースの健全性が低くなります。データセンターまたはリージョン別にリソースをグループ化して、直感的で統合されたヘルス スコアを得ることで、重要な領域の優先順位付けやトラブルシューティングを簡単に行うことができます。



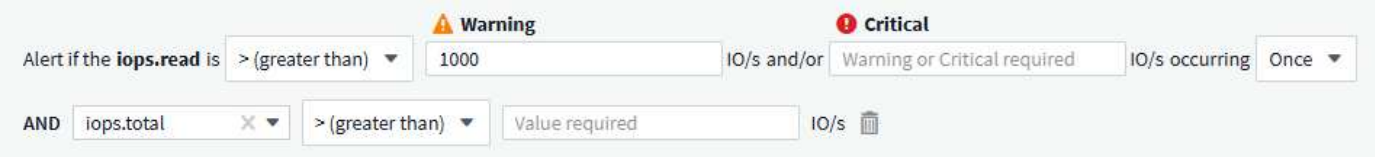
ボタンをクリックするだけで画面上のスライドアウト パネルに詳細情報が表示されるため、注意が必要な問題を迅速に特定し、システムの安全性と回復力を維持できます。



正確な警告のためのマルチコンディションモニター

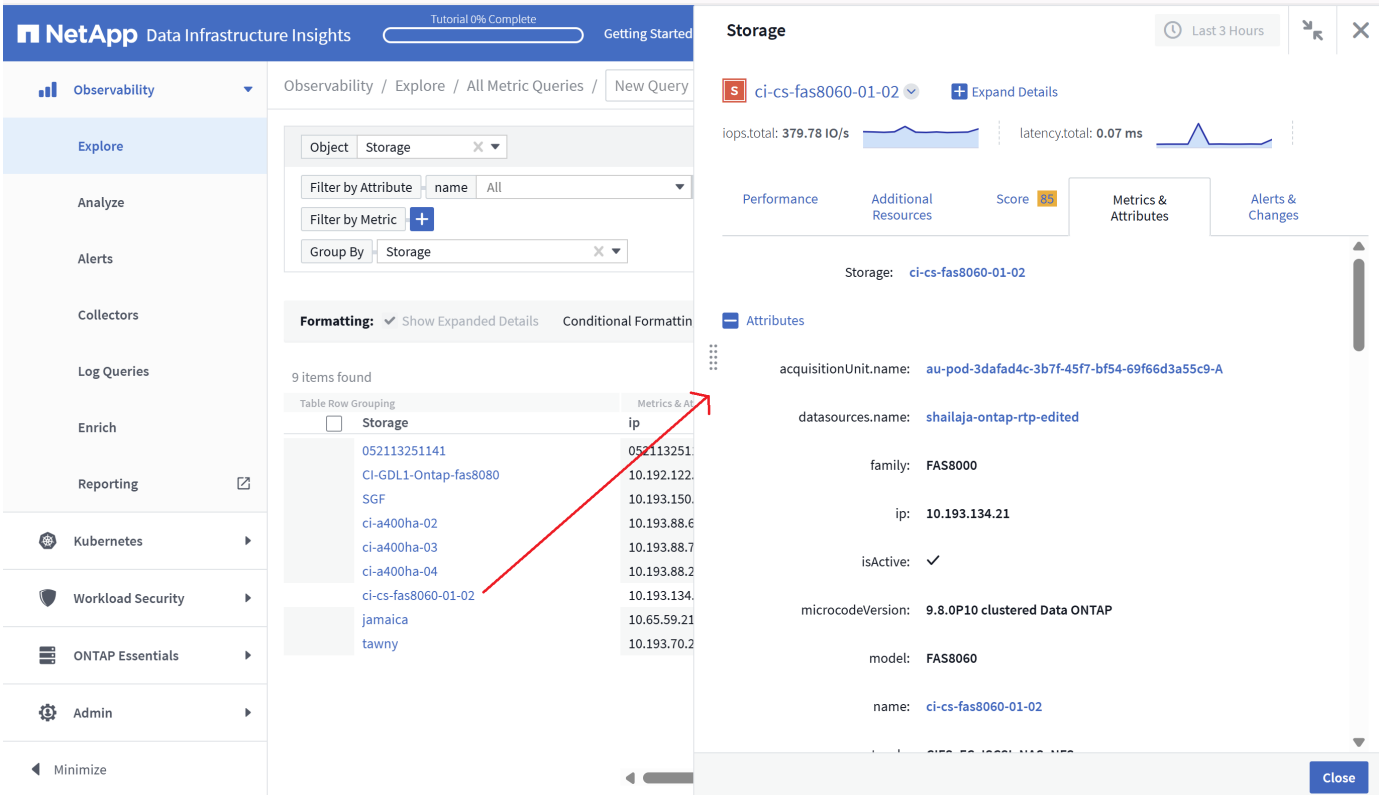
オプションの 2 番目の条件をメトリック モニターに追加することで、アラート ノイズを削減し、監視の精度

を向上します。アラートは両方の条件が満たされた場合にのみトリガーされるため、最も重要なシナリオに重点を置いた、よりターゲットを絞った通知が提供されます。



クエリの改善: 一目でわかるオブジェクトの詳細

オブジェクト クエリ結果リストの行を選択すると、選択したオブジェクトの詳細パネルが開きます。メトリックと属性 (オブジェクト クエリのデフォルト ビュー)、アラートと変更、パフォーマンス、ヘルス スコアをすばやく表示したり、関連リソースを調べたりできます。関連するオブジェクト情報はすべてすぐに入手できます。



ワークロードセキュリティの改善

2 つの新しい API により、Workload Security 環境をより詳細に制御できるようになります。

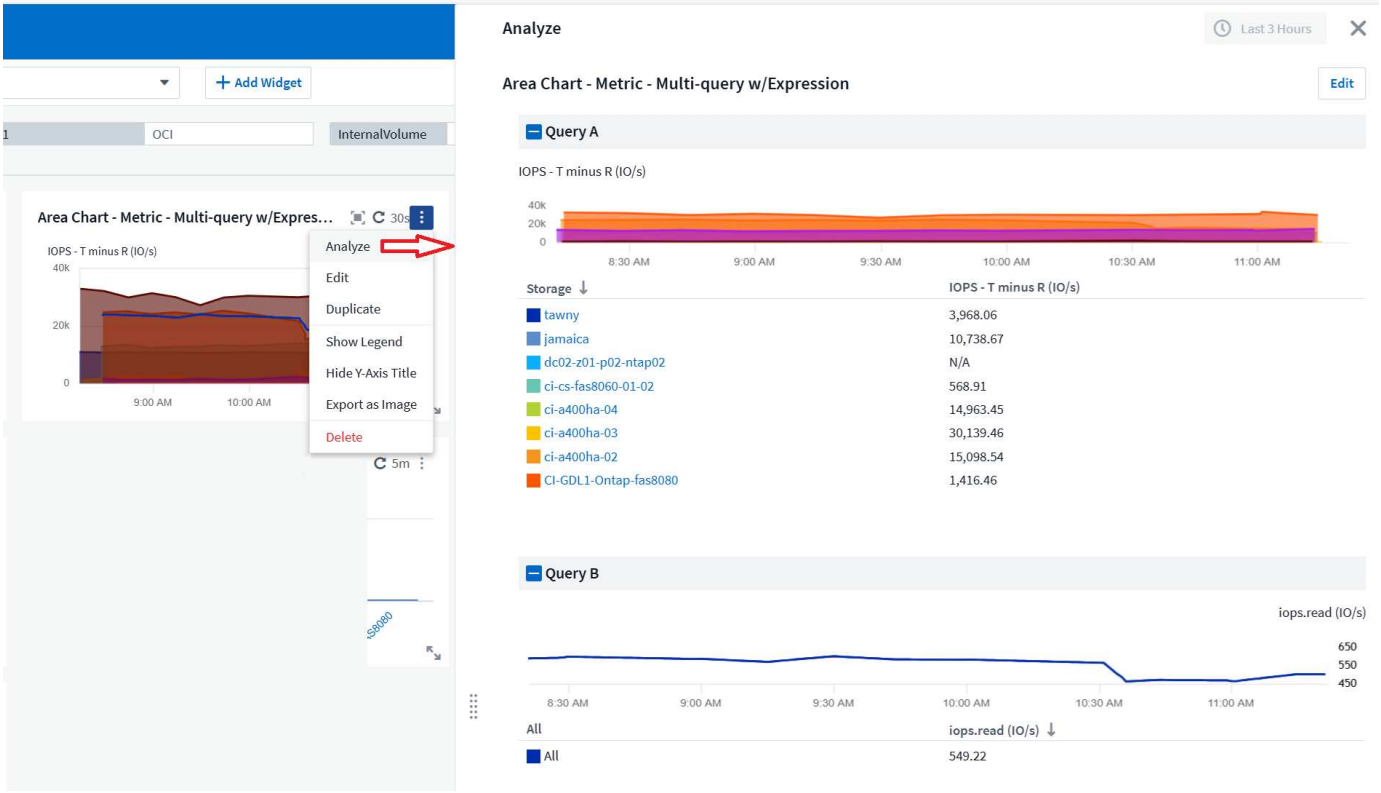
1. *GET /rest/v1/cloudsecure/activities/groups* を使用してグループを表示および管理します。
2. *POST /rest/v1/cloudsecure/collectors/{collector-uuid}/status* を使用してデータコレクターを一時停止および再開します。

さらに、Workload Security ロールの権限チェックがさらに安全になりました。セキュリティが強化された結果、既存のユーザーの一部はコレクターを追加するときに権限の問題が発生する可能性があります。指示に従ってユーザー権限を確認してください。"ドキュメント"。

2025年8月

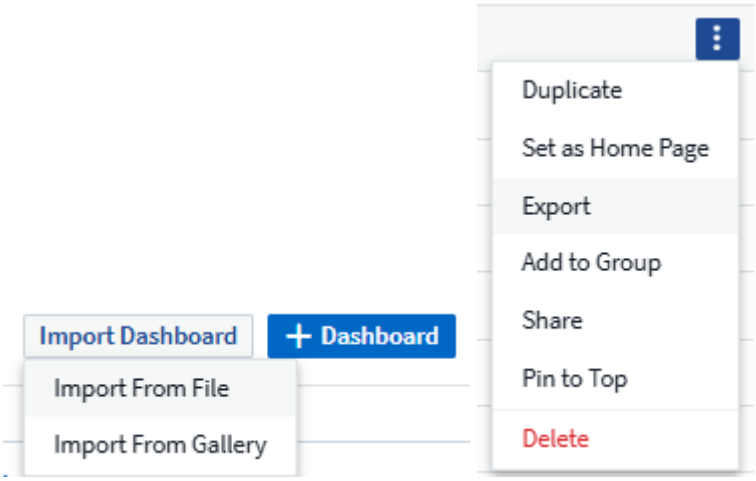
指先で操作できる集中ウィジェットデータ

ほとんどのウィジェットの新しい 分析 機能を使用すると、一度に 1 つのウィジェットのデータを詳しく調べることができます。ウィジェットの「分析」ボタンをクリックするだけで詳細ビューが開き、ダッシュボードのコンテキストを離れることなく、基礎となるデータをインタラクティブに探索し、ズームインしてより深い洞察を得ることができます。



ダッシュボードのエクスポートとインポート

複数のテナントを管理していて、便利なダッシュボードを開発している場合は、ダッシュボードをエクスポートして別のテナントにインポートできます。



強化されたクラウド統合: **Google Cloud NetApp Volumes (GCNV)** のサポート

- Google Cloud NetApp Volumes* (GCNV) が DII のデータ コレクターとして完全にサポートされるようになり、ハイブリッド クラウド監視のエコシステムが完成しました。インフラストラクチャ全体の組織、プール、ボリュームなどの重要なストレージ オブジェクトを可視化します。オンプレミスでもクラウドでも、すべてのストレージ環境を単一のプラットフォームから追跡できるようになりました。

強化された**StorageGRID**監視

StorageGRIDログ収集がデフォルトで有効になり、DII にイベント追跡データが提供されるようになりました。また、50 を超えるデフォルトのアラート、リアルタイム イベント追跡、および新しいダッシュボードによって StorageGrid 監視が拡張され、複雑なストレージ グリッド操作が簡素化されました。トラフィック ポリシーとバケットのパフォーマンスに関する詳細な情報を活用して、問題を事前に把握します。

オペレーティングシステムのサポート

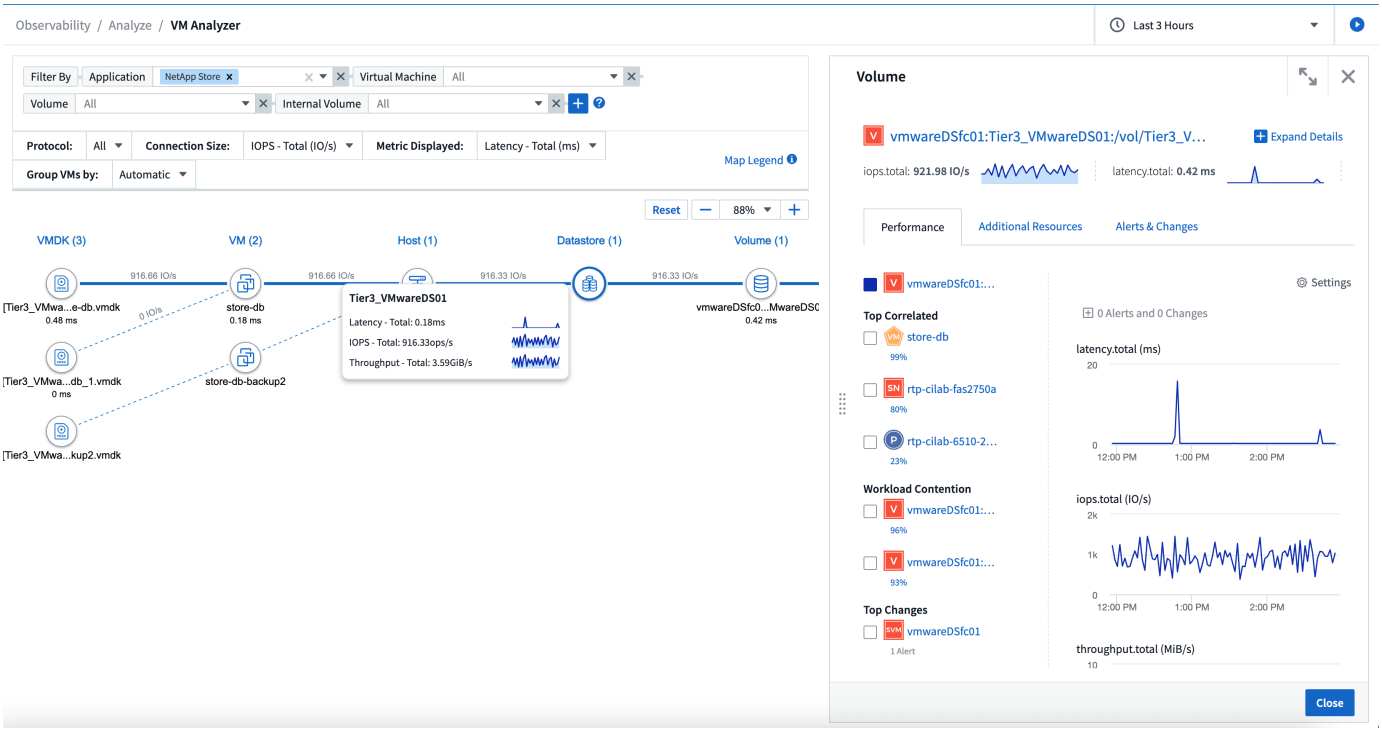
Data Infrastructure Insights Acquisition Unitsでは、以下のオペレーティングシステムがサポートされるようになりました。"すでにサポートされています" :

- AlmaLinux（64ビット）10
- Red Hat (64ビット) 10
- Rocky（64ビット）9.6

2025年6月

VM Analyzer: VMからストレージまでの包括的な可視性とトラブルシューティング

DII の **VM Analyzer** 機能は、仮想化環境の包括的なエンドツーエンドのビューを提供します。 VM Analyzer は、仮想マシンからストレージまでのパス全体をマッピングすることでトラブルシューティングを効率化し、仮想ディスク、VM、ホスト、データストア、ボリューム、ストレージ全体のパフォーマンスの問題をユーザーが迅速に特定できるようにします。直感的なトポロジ ビュー、フィルタリング、詳細なパフォーマンス メトリックにより、管理者はボトルネックを簡単に特定し、トラフィックの不均衡を分析し、全体的なストレージ パフォーマンスを最適化できます。



オペレーティングシステムのサポート

Data Infrastructure Insights Acquisition Unitsでは、以下のオペレーティングシステムがサポートされるようになりました。"すでにサポートされています"：

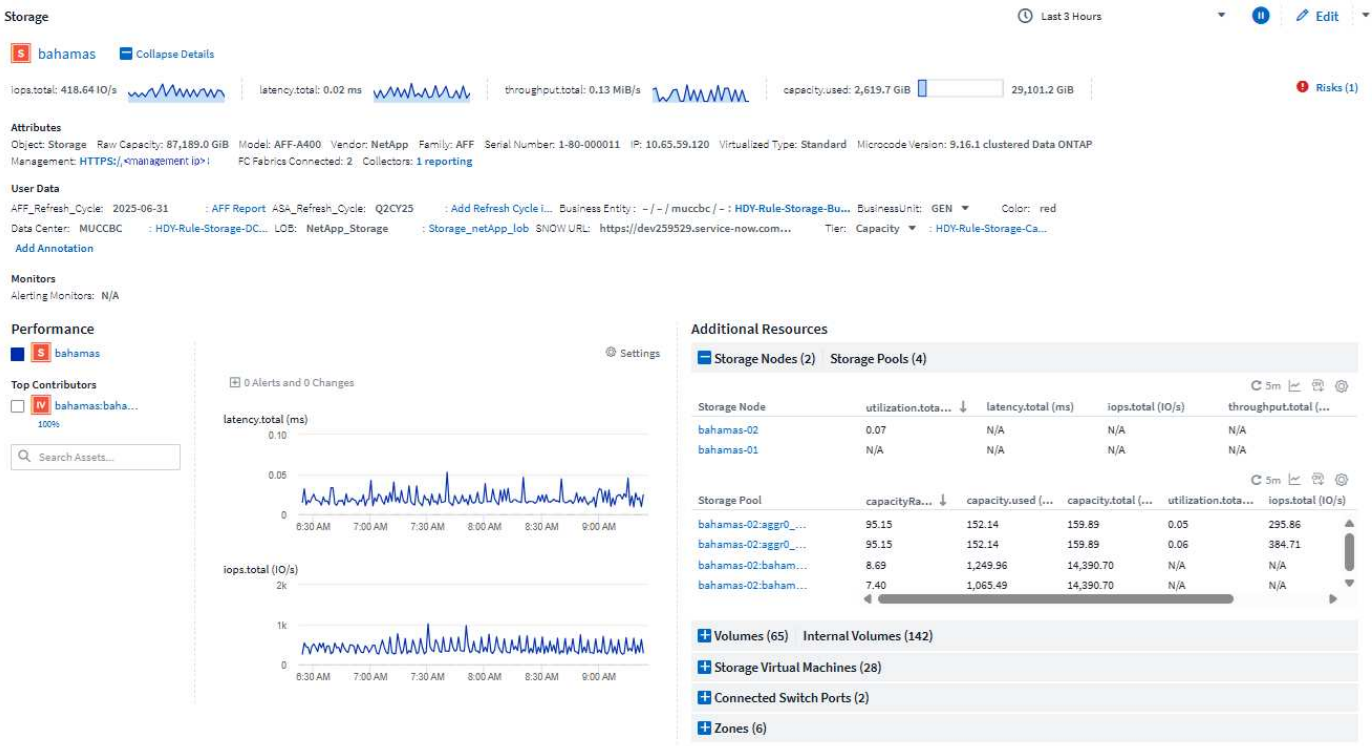
- Debian (64ビット) 12
- Oracle Enterprise Linux (64 ビット) 9.6
- Red Hat (64ビット) 9.6

2025年5月

新しいランディングページで流れを維持

再設計されたランディング ページには、概要データ、パフォーマンス チャート、相関関係、アラートと変更、主要なリソースなど、必要なものがすべて 1 つのビューに表示されます。

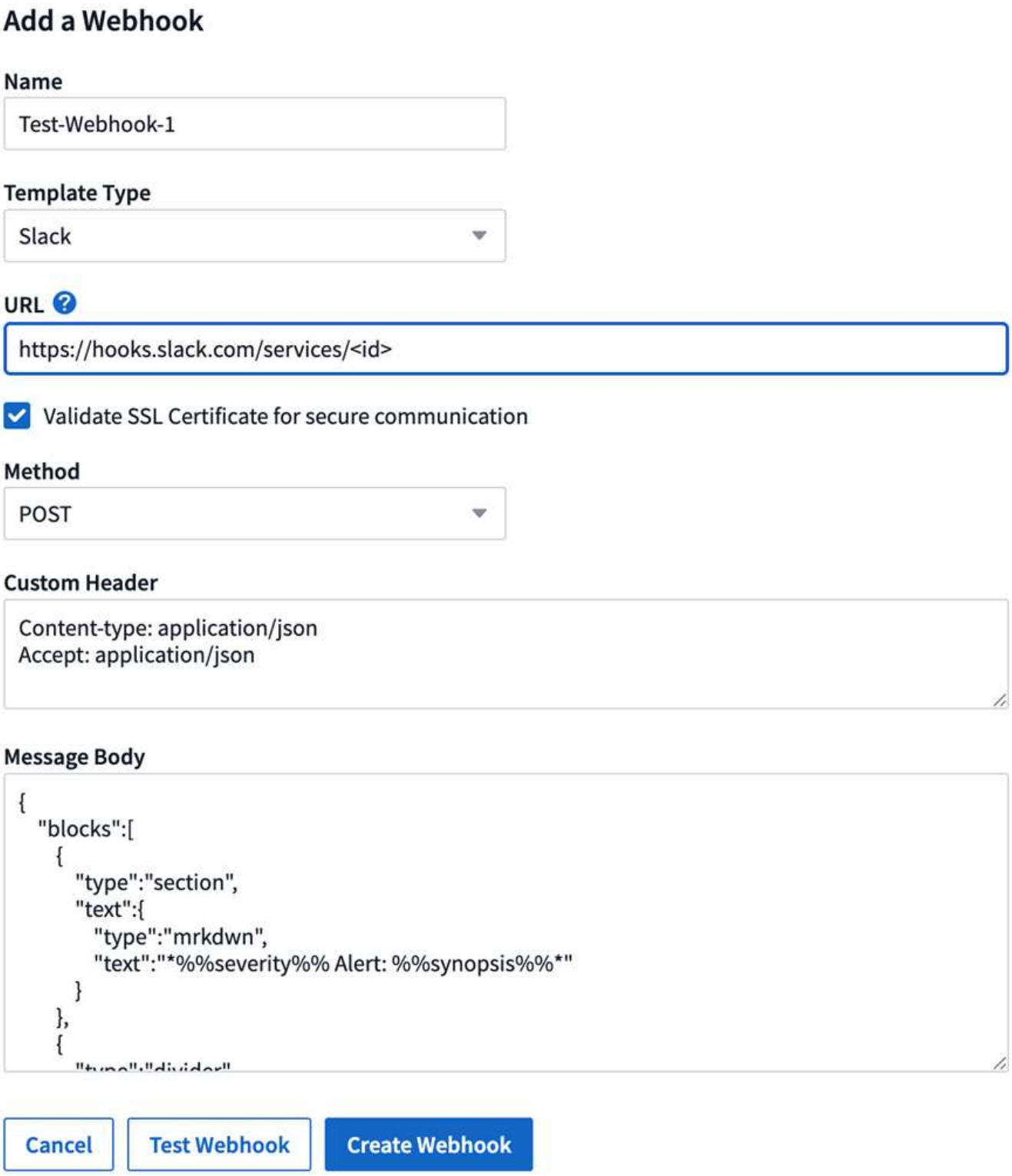
タブ間を移動したり、コンテキストを失ったりすることなく、トラブルシューティングを高速化し、作業の流れを維持できるようになりました。



ワークロードセキュリティの改善

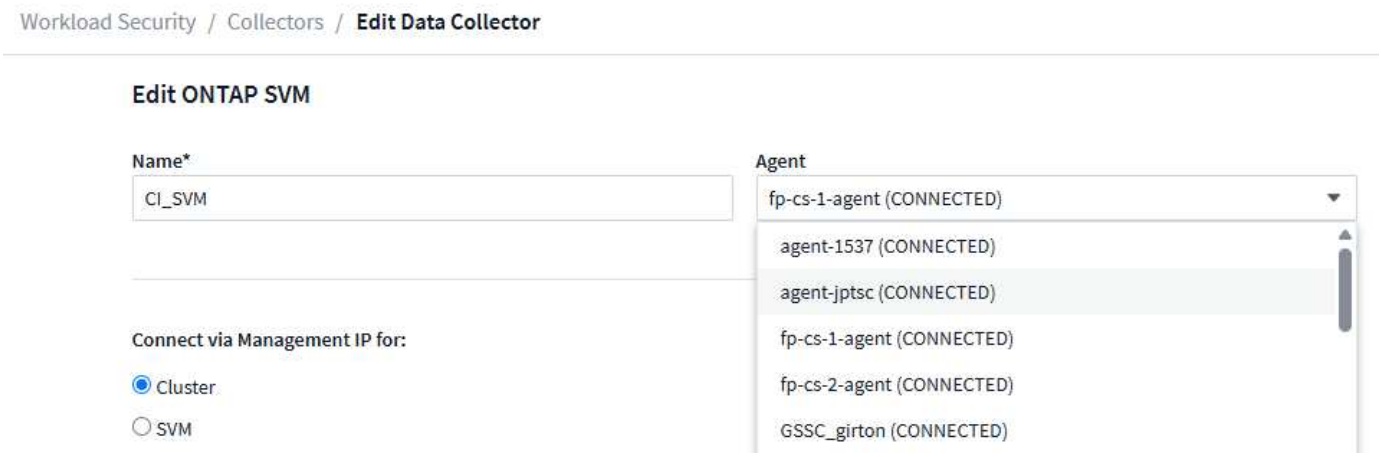
ワークロード セキュリティ アラートに **Webhook** が利用可能になりました

Workload Security では、Slack、PagerDuty、Teams などのツールへのすぐに使用できる Webhook 通知がサポートされるようになりました。さらに、メッセージをカスタマイズしたり、他の SIEM やサードパーティ アプリケーションと統合したりできるカスタマイズ可能なテンプレートも提供しています。重要なアラートを既存のセキュリティ ワークフローに直接ルーティングすることで、チームはより迅速に調査して対応できるようになります。



エージェント間でワークロード セキュリティ コレクターを移行する

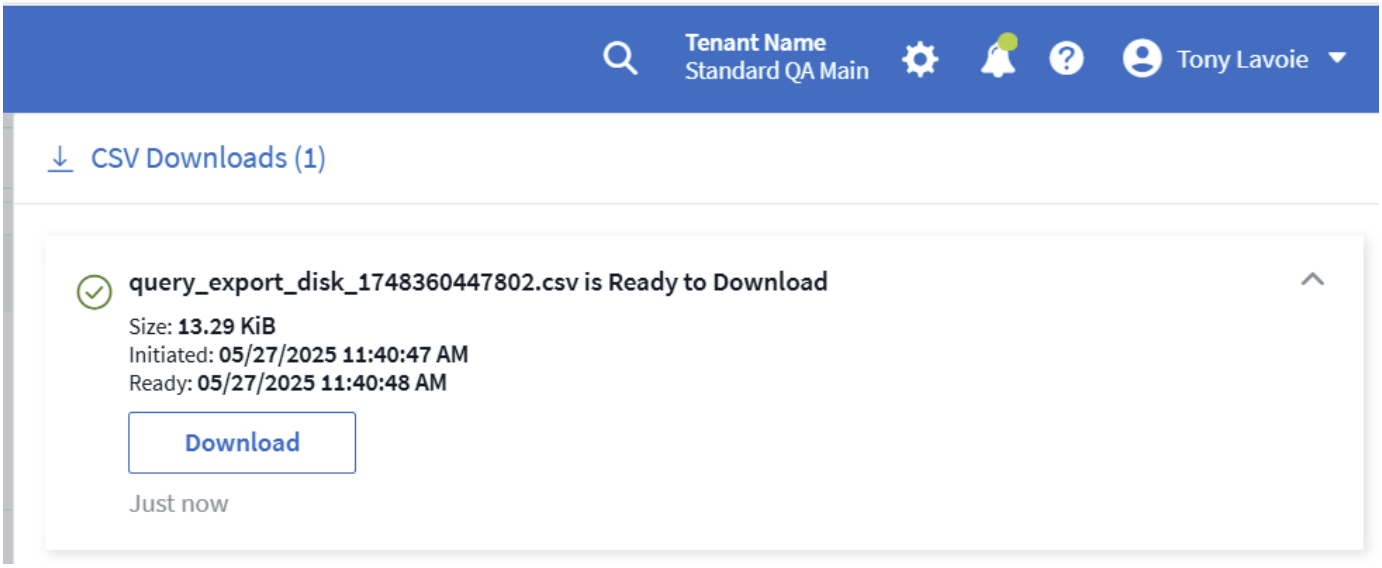
Workload Security コレクターをあるエージェントから別のエージェントに簡単に移行できるため、エージェント間でコレクターの負荷を効率的に分散できます。移行は、コレクターを編集し、リストから宛先エージェントを選択するだけで簡単です。



.CSV 非同期エクスポート

CSV へのデータのエクスポートには、エクスポートするデータの量に応じて、数秒から数時間かかる場合があります。 **Data Infrastructure Insights**では、そのデータが非同期的にエクスポートされるようになったため、**.CSV** がコンパイルされている間も作業を続行できます。

右上のツールバーの「ベル」アイコンを選択して、.CSV エクスポートを表示します。



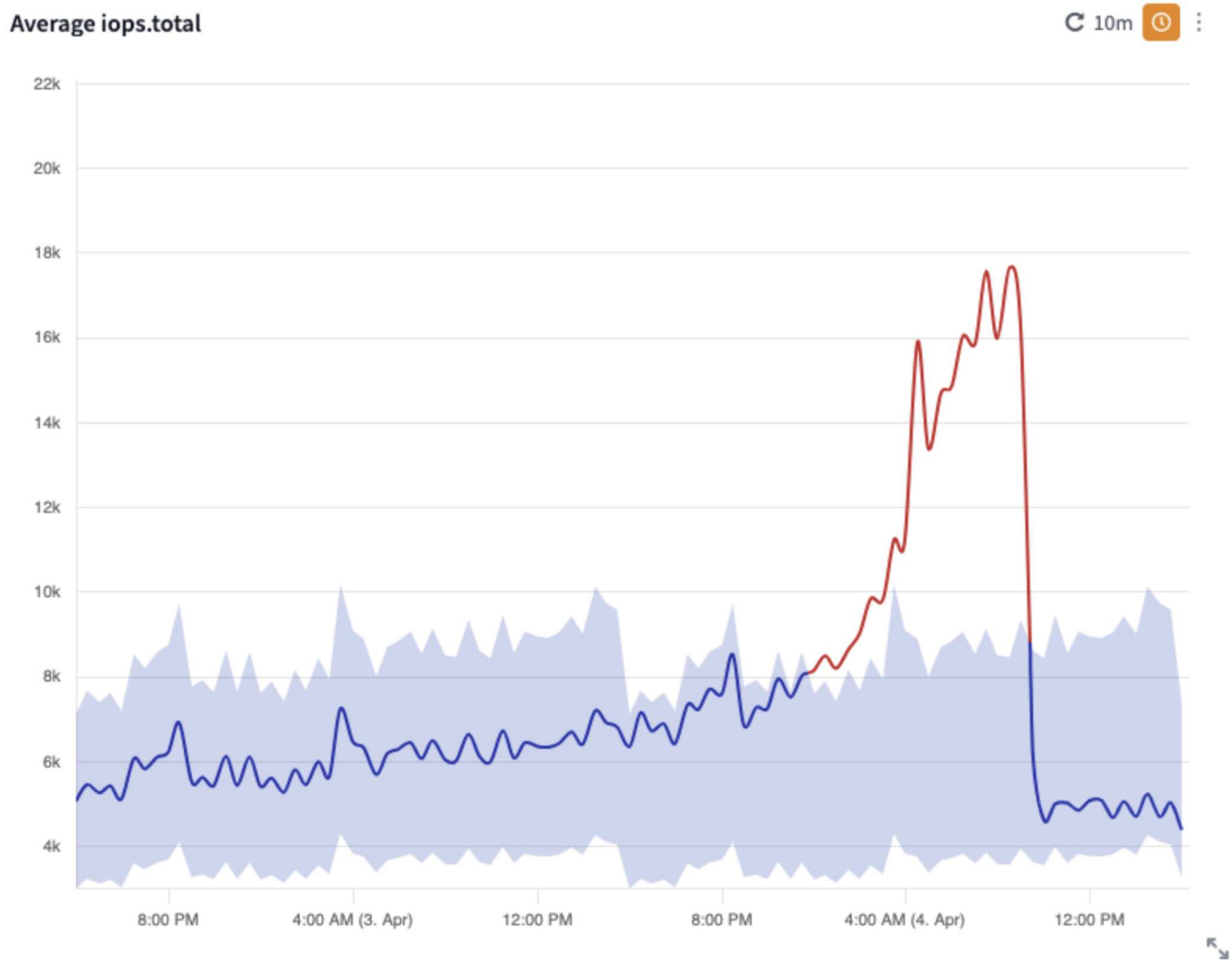
2025年4月

プロアクティブな問題解決のためのラインウィジェットにおける ML を活用した異常境界

折れ線グラフまたはスプライン グラフ ウィジェットのパフォーマンスの問題をトラブルシューティングするために、実際のメトリックとともに予想される動作の境界を表示できるようになりました。これにより、正常なメトリックの傾向と異常なメトリックの傾向を区別できます。

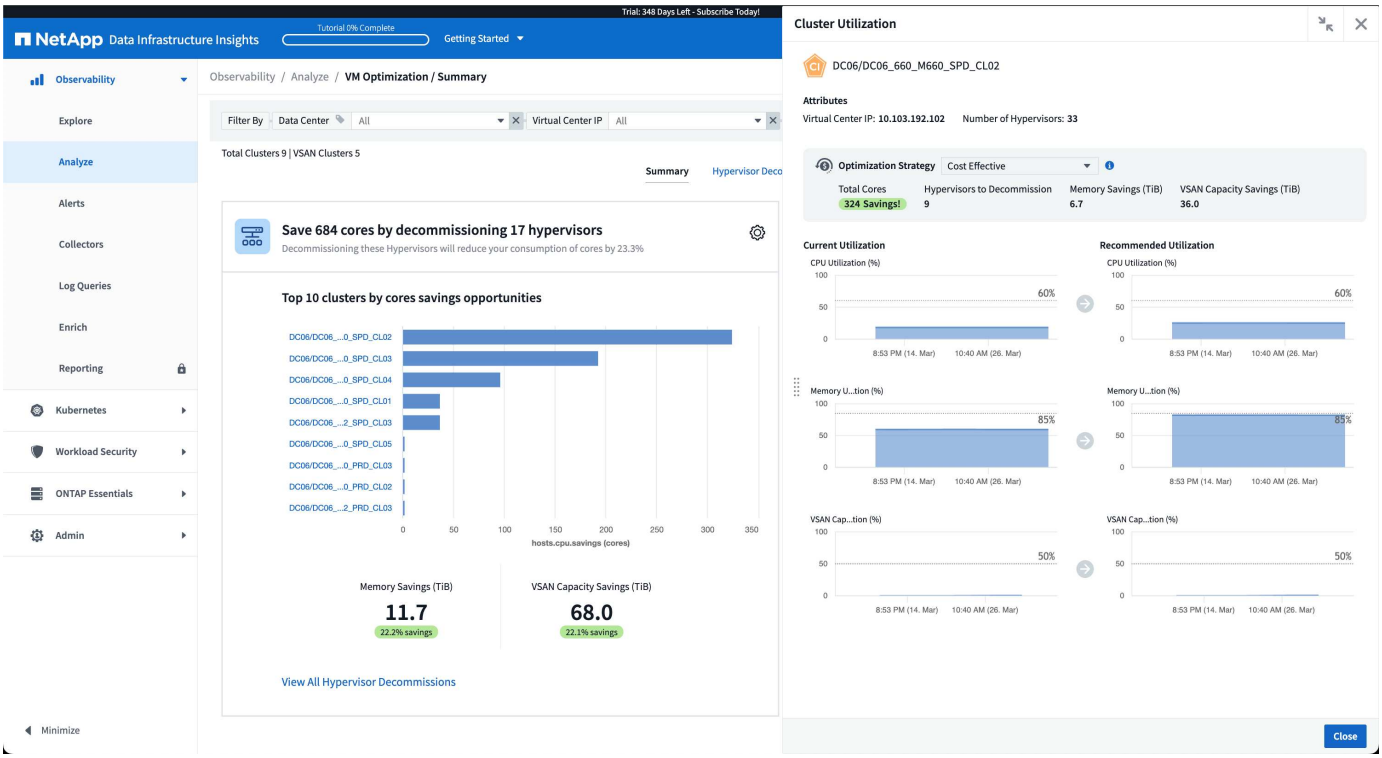
季節データ分析を備えた DII 機械学習は、履歴パターンに基づいてインテリジェントなしきい値を確立します。メトリクスが予想範囲から外れると、システムはそれを異常として強調表示し、問題を迅速に特定して平

均解決時間を短縮し、問題が運用に影響する前に対処できるようにします。



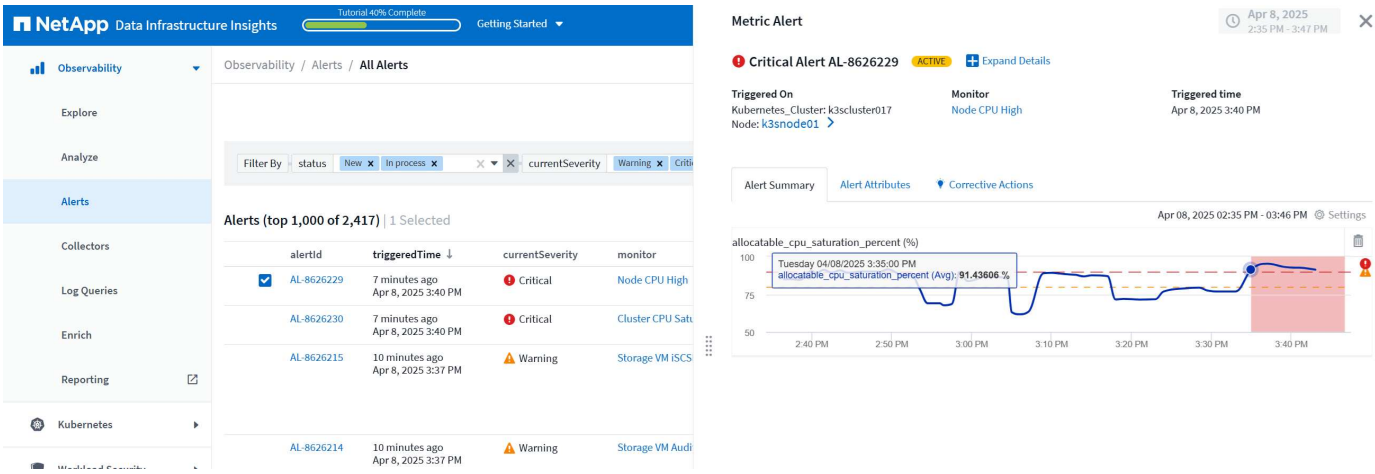
VSAN ストレージ サポートによる VMware コストの最適化

VM 最適化機能に、VSAN ストレージを備えた VMWare 環境のサポートが含まれるようになりました。 CPU とメモリの使用量に加えて、分析では再利用の推奨事項としてローカル VSAN ストレージが考慮されるようになったため、ライセンス コストをさらに削減できます。



アラートの詳細をすぐに確認

新しいスライドアウト パネルにより、アラートの調査がこれまで以上に簡単になりました。アラートを選択すると、そのアラートの詳細が表示され、問題を調査しているときに場所を失うことなくアラートを簡単に切り替えることができます。



ワークロードセキュリティフォレンジック非同期エクスポート

フォレンジック データのエクスポートには、エクスポートするデータの量に応じて、数秒から数時間かかる場合があります。 Workload Security はデータを非同期的にエクスポートするため、.CSV のコンパイル中でも作業を続行できます。

ルールにグループ化されたデータコレクター通知

データ コレクターで通知を構成している場合、4 月 15 日以降、それらの通知は通知ルールで処理され、受信

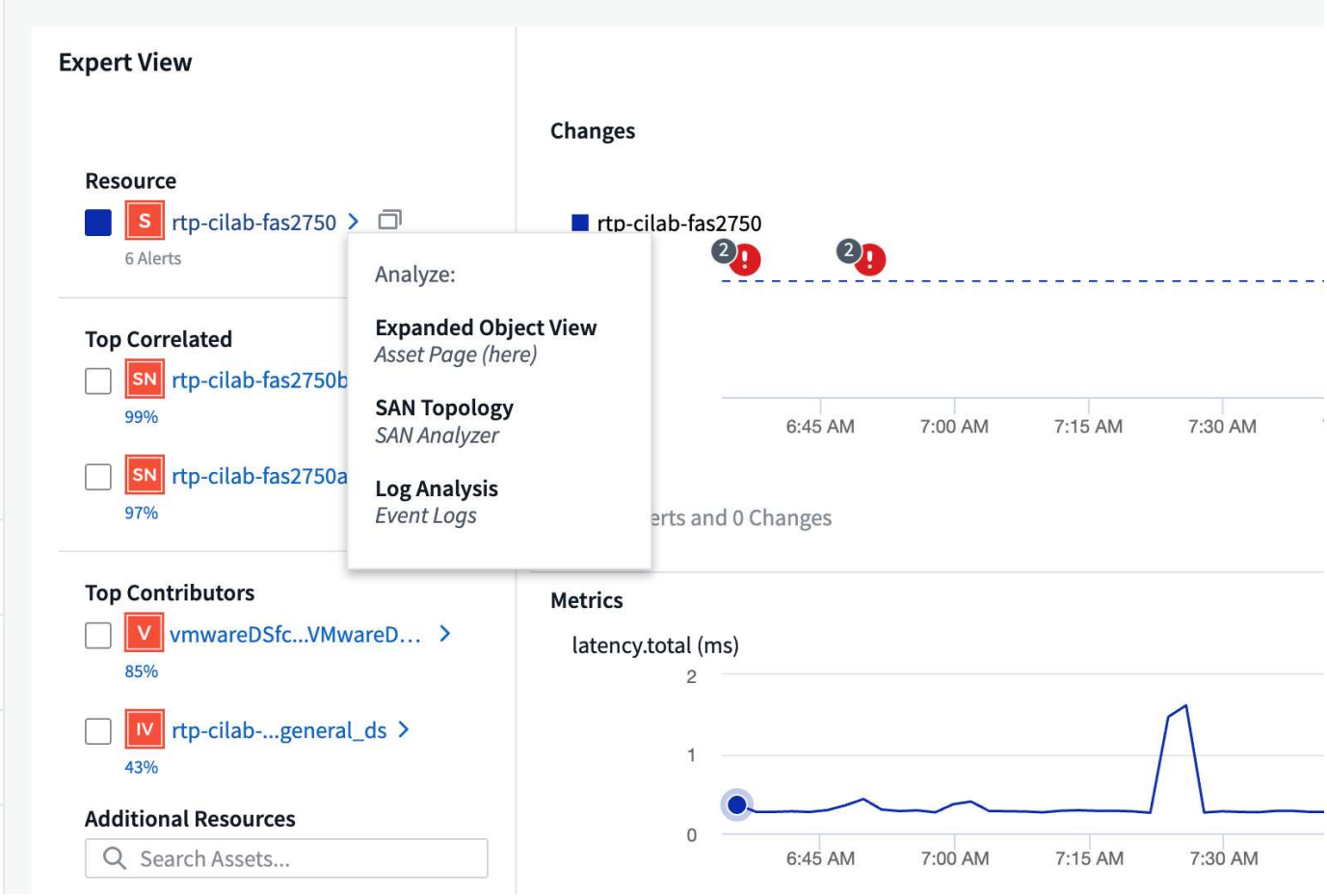
者が同一のコレクターに対しては単一のルールが適用されます。受取人が異なるコレクターには、別のルールが適用されます。既存のコレクター通知は通知ルールに移行されます。

2025年3月

効率的なインフラストラクチャ管理のための強化されたコンテキストナビゲーション

Data Infrastructure Insightsを活用して運用効率を高め、時間を節約します。現在、コンテキスト メニュー リンクが追加されており、任意のオブジェクトから、デバイス パフォーマンス分析情報の資産ランディング ページ、ネットワーク トポロジの視覚化のための SAN Analyzer、運用認識のログ、構成管理のための Change Analyzer に直接ジャンプできるようになりました。

複数のビューにわたる重要なデータに即座にアクセスできるため、オブジェクトの関係をより迅速かつ明確に把握できます。この合理化されたワークフローにより、意思決定と問題解決が加速され、最終的には時間が節約され、全体的な分析機能が向上します。



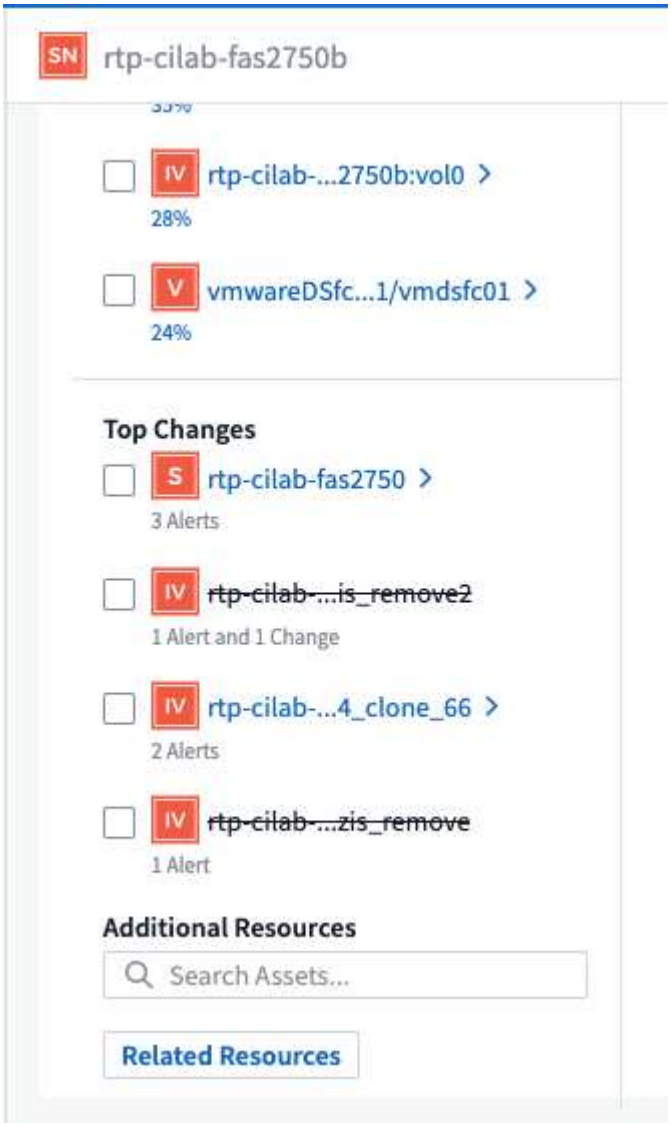
削除された資産の履歴を保存する

強化されたインフラ変更機能により、移動されて利用できなくなった qtree やボリュームなどの削除された資産の履歴が保存されるようになりました。

トラブルシューティングのパズルで何かが欠けていますか? もうない！取り消し線が引かれた削除済みオブジ

ェクトも含め、すべてが表示されるため、アセットが削除された後でも完全なコンテキストが得られ、エンドツーエンドのパス全体で過去の変更やアラートの重要な要素を見逃すことがなくなります。

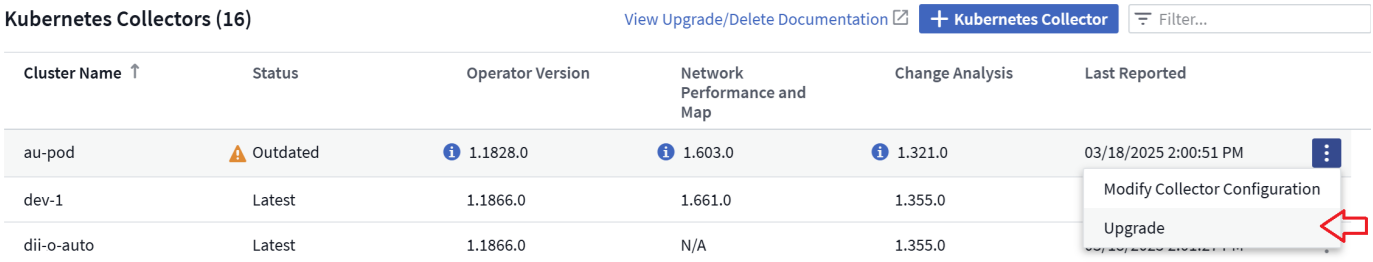
結果？問題の資産が存在しなくなった場合でも、解決時間が短縮され、インフラストラクチャの決定をより自信を持って行うことができます。



Kubernetes オペレーターのプッシュボタンアップグレード

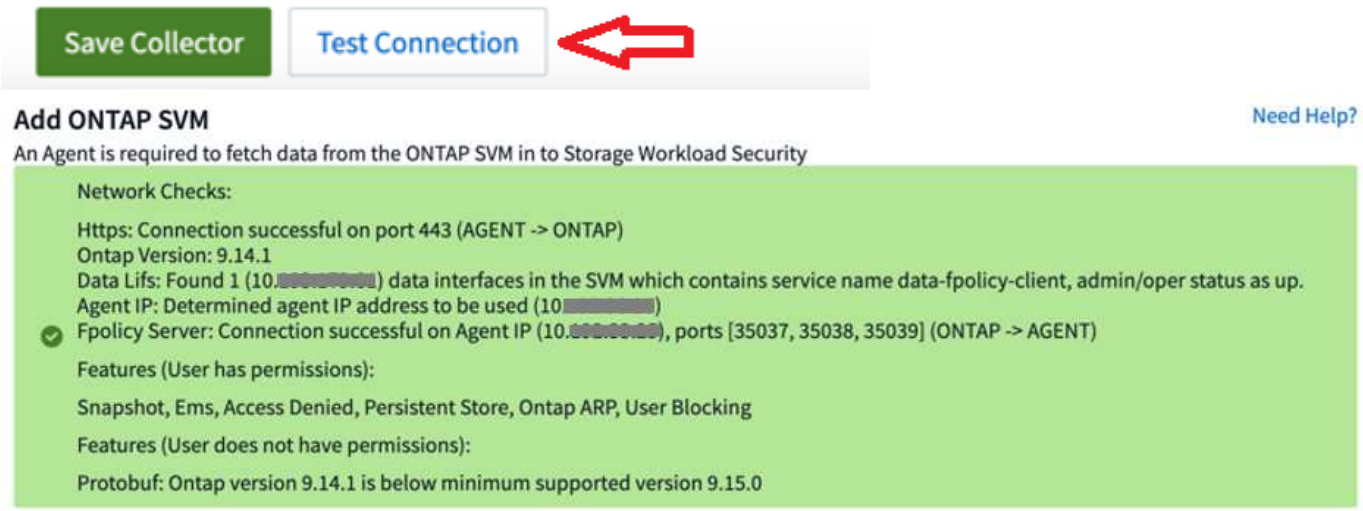
Kubernetes Operator が最新であることを確認したいですか? DII Kubernetes Collectors クラスター メニューからオンデマンドでオペレーターをアップグレードします。メニューから「アップグレード」を選択するだけで、オペレーターがイメージ署名を検証し、現在のインストールのスナップショットをキャプチャして、アップグレードを実行します。

プッシュボタン アップグレードはオプションの機能であり、そのアクティベーションはクラスターごとに管理できます。



ストレージ ワークロード セキュリティ データ コレクターの接続テスト

テスト接続機能は、Data Infrastructure Insights (DII) ワークロード セキュリティでデータ コレクターを設定するときに、エンド ユーザーが障害の具体的な原因を特定できるようにすることを目的としています。これにより、ユーザーはネットワーク通信や役割の不足に関連する問題を自己修正できるようになります。



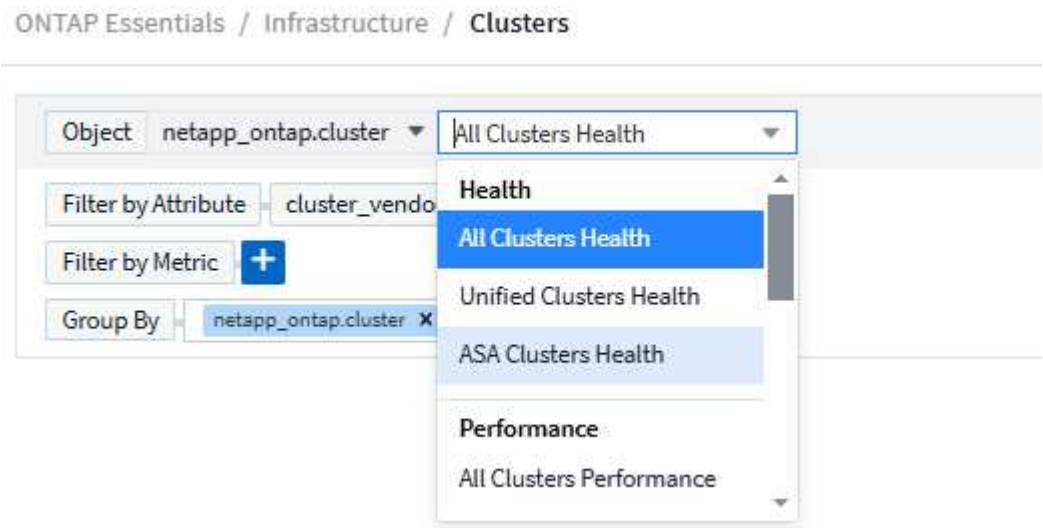
オペレーティングシステムのサポート

Data Infrastructure Insights Acquisition Unitsでは、以下のオペレーティングシステムがサポートされるようになりました。"すでにサポートされています" :

- アルマリナックス 9.5
- Debian (64ビット) 11
- OpenSUSE リープ 15.6
- Oracle Enterprise Linux (64 ビット) 8.9、8.10、9.5
- Red Hat (64 ビット) 8.9、8.10、9.5
- ロッキー 9.5
- SUSE Linux Enterprise Server 15 SP6
- Ubuntu サーバー 24.04 LTS

2025年2月

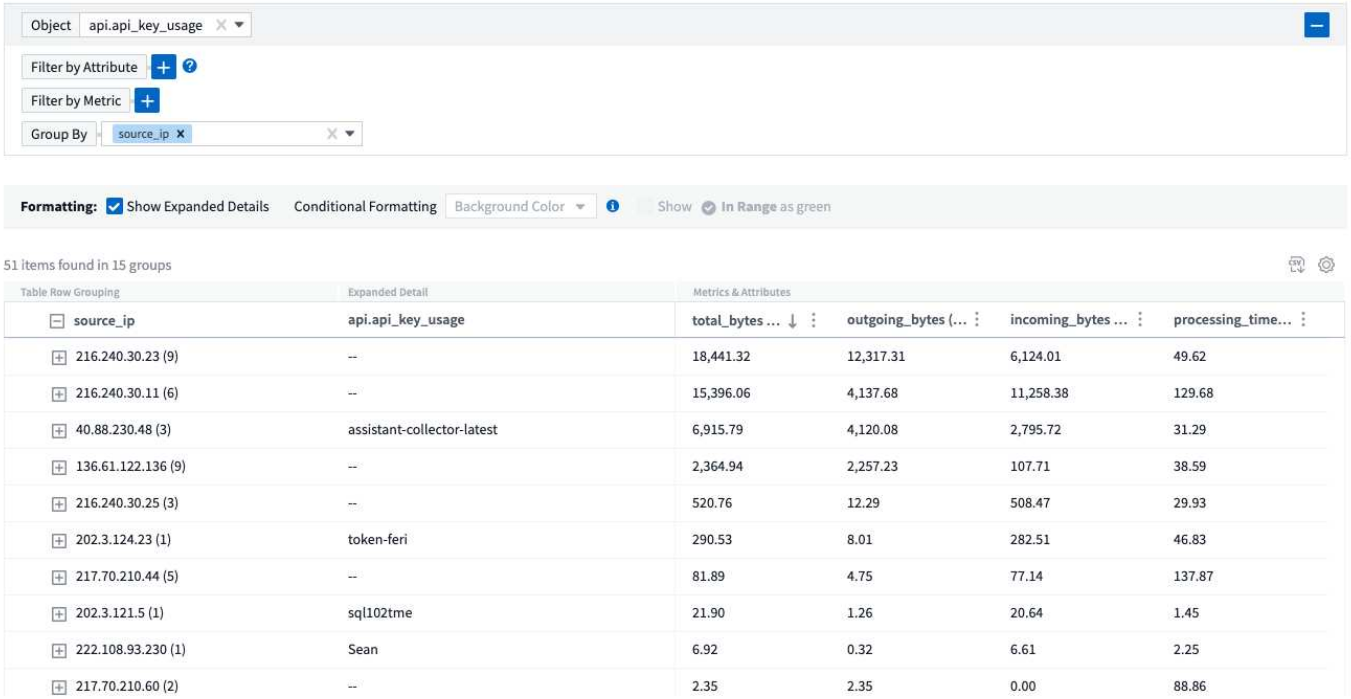
ONTAP Essentialsには、最新世代の"ASA"デバイス。これには、 ONTAP上で実行されているワークロードのVM-LUN トポロジ用の SAN Analyzer が含まれており、現在はData Infrastructure Insights Basic Edition の一部としてNetAppサポートでも利用できます。



DII API使用状況追跡：セキュリティと効率性の向上

管理者ユーザーが利用できる強化された REST API 使用状況追跡により、セキュリティ体制を強化し、リソース管理を合理化します。 API 使用状況の追跡を使用すると、どの API トークンが使用されているか、どの IP アドレスから使用されているか、およびそれらが生成するトラフィックの量を確認できます。トークンを特定の IP アドレスと使用レベルにリンクすることで、システム アクセスと使用傾向に関する強力な分析情報が得られ、安全で効率的な環境を維持し、運用を円滑に進めるために必要な制御が可能になります。

API 使用状況を表示するには、**Observability > Admin > API Access** に移動し、*View API Usage* を選択します。この API は DII Observability API でのみ使用可能であり、Workload Security には適用されないことに注意してください。



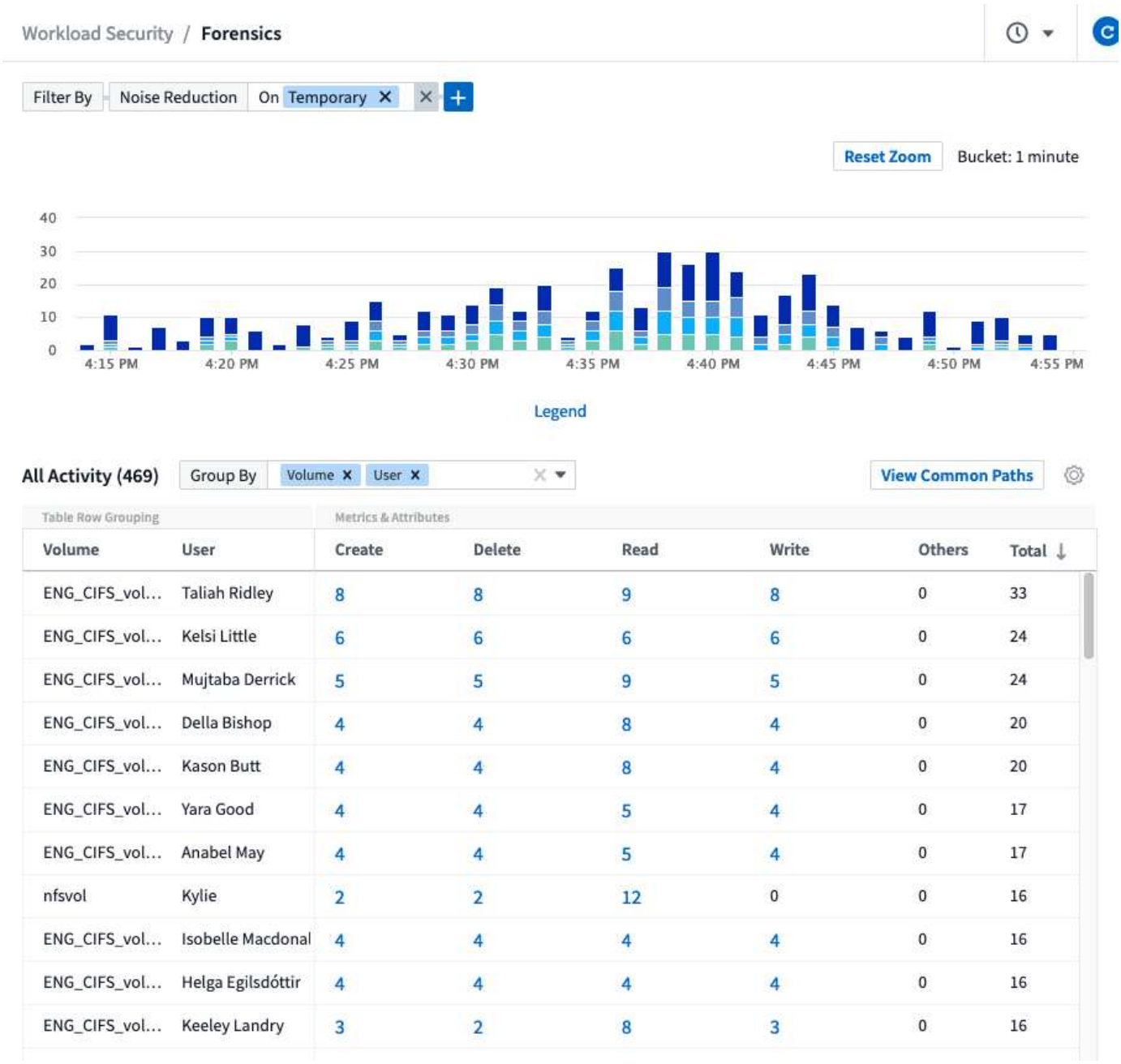
ユーザーを制限するワークロードセキュリティ**API**

Workload Security でユーザー制限を管理するための新しい API が追加されました。 API を使用すると、ユーザーをブロックまたはブロック解除したり、アクセス制限の期間を変更したりできます。 *cloudsecure_actions.block* API については、「管理 > API アクセス > API ドキュメント」ページを参照してください。

2025年1月

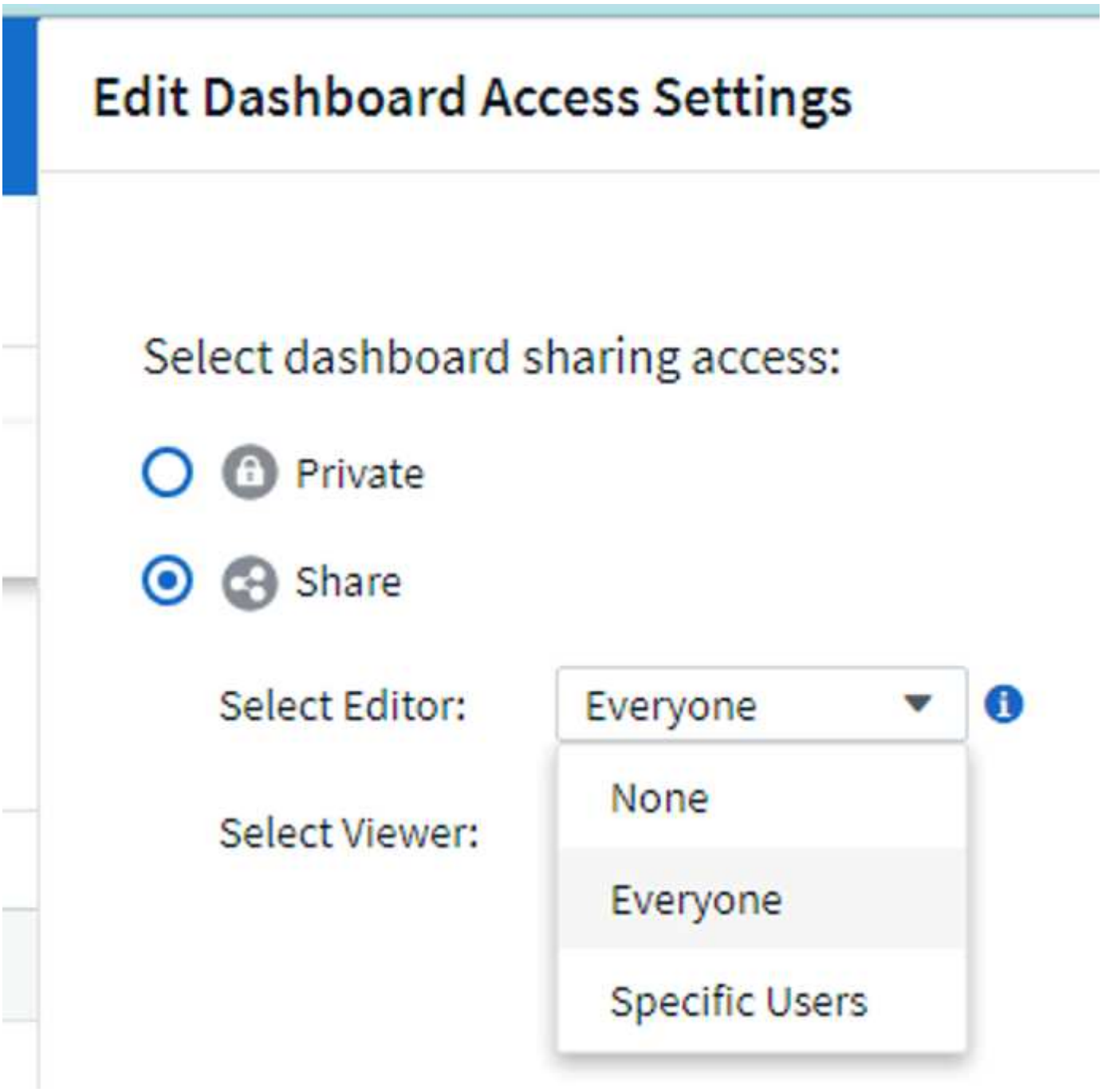
フォレンジックグループでリスクを積極的に管理

セキュリティとリソース管理機能を強化するために設計された最新機能をご紹介します。高度なグループ化機能と階層的な複数のグループ化のサポートにより、特定のフォルダーにアクセスしたユーザーを簡単に識別し、最もアクティブなユーザーと共有を判断し、アクティブなクライアント IP アドレスを追跡してリスクをプロアクティブに管理できるようになりました。最もアクセスの多いファイルとフォルダーを特定することでストレージと帯域幅の使用を最適化し、ユーザーを識別することでシステム アクセスの制御を強化します。



ダッシュボードのアクセス制御

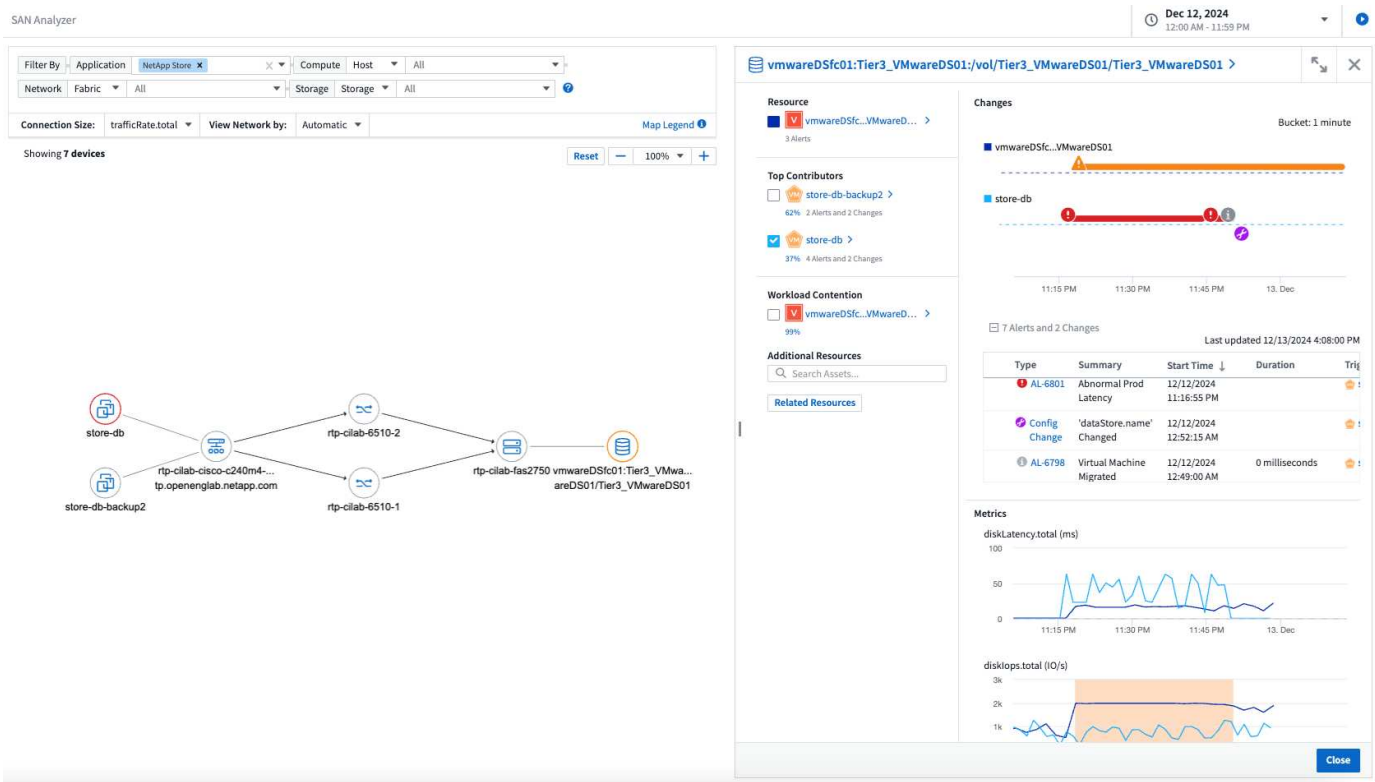
Data Infrastructure Insightsでは、作成したダッシュボードへのアクセスをより細かく制御できるようになりました。グラフを変更できるユーザーを選択します。潜在的に機密性の高い情報への公開を制御できます。一般公開の準備ができていないダッシュボードをまだ作成中ですか? 共有する準備ができるまで非公開にしておくこともできます。



2024年12月

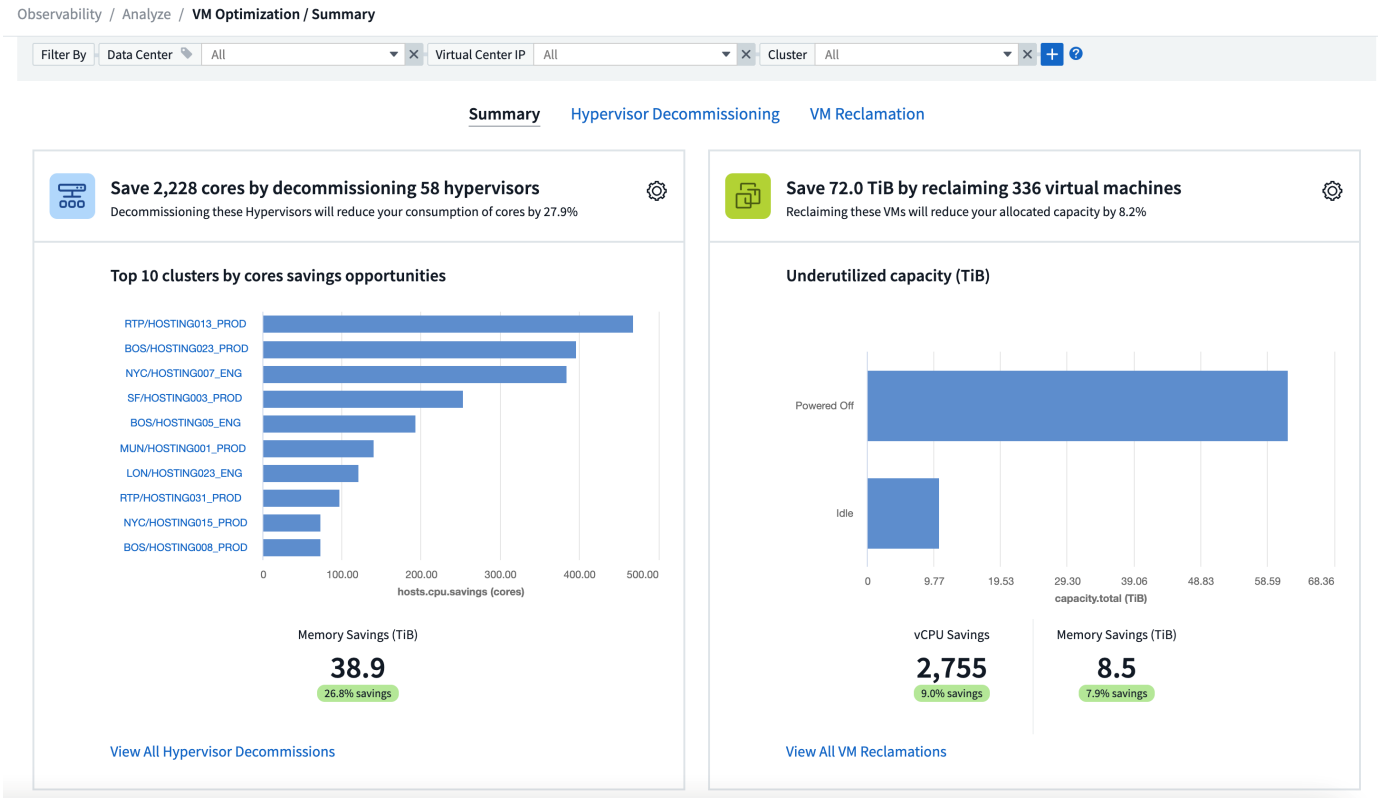
SAN Analyzer のご紹介: ブロック ワークロードの可視性強化

SAN は重要なワークロードの処理において重要な役割を果たしますが、その複雑さにより重大な停止や顧客の混乱が生じる可能性があります。 DII の **SAN Analyzer** を使用すると、SAN の管理がよりシンプルかつ効率的になります。この強力なツールは、エンドツーエンドの可視性を提供し、VM/ホストからネットワーク、LUN、ストレージへの依存関係をマッピングします。 SAN Analyzer は、インタラクティブなトポロジ マップを提供することで、問題を正確に特定し、変更を理解し、データ フローの理解を深めることを可能にします。 SAN Analyzer を使用して複雑な IT 環境での SAN 管理を合理化し、ブロック ワークロードの可視性を向上させます。



インテリジェントなホスト廃止と **VM** 再利用による **VM** コストの最適化

Data Infrastructure Insights は、環境の過去の動作を分析し、短期および長期の予測を確立し、ホストの廃止と、電源がオフになっているアイドル状態の VM の再利用に関する詳細な推奨事項を生成することで、インフラストラクチャとライセンスのコスト管理に役立ちます。これらの推奨事項は、パフォーマンスの安定性を確保し、未使用の容量を解放し、メモリと CPU の割り当てを削減するのに役立ちます。



時間チャートとテーブルウィジェットのサポートによりログの洞察を明らかに

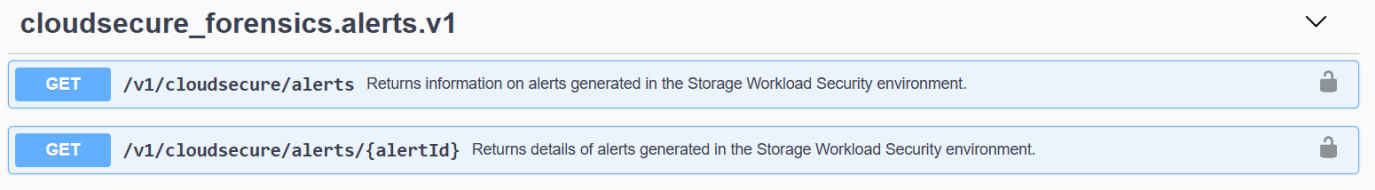
時間グラフ (棒グラフ、折れ線グラフ、面グラフ) を活用して、繰り返し発生するエラーやアクティビティの急増などのログ データの傾向やパターンを特定し、時間の経過に伴うシステムの動作に関する貴重な分析情報を得ることができます。さらに、テーブルを使用すると、ダッシュボードにログ メッセージを直接含めることができるため、ログの詳細をより包括的に表示できます。



2024年11月

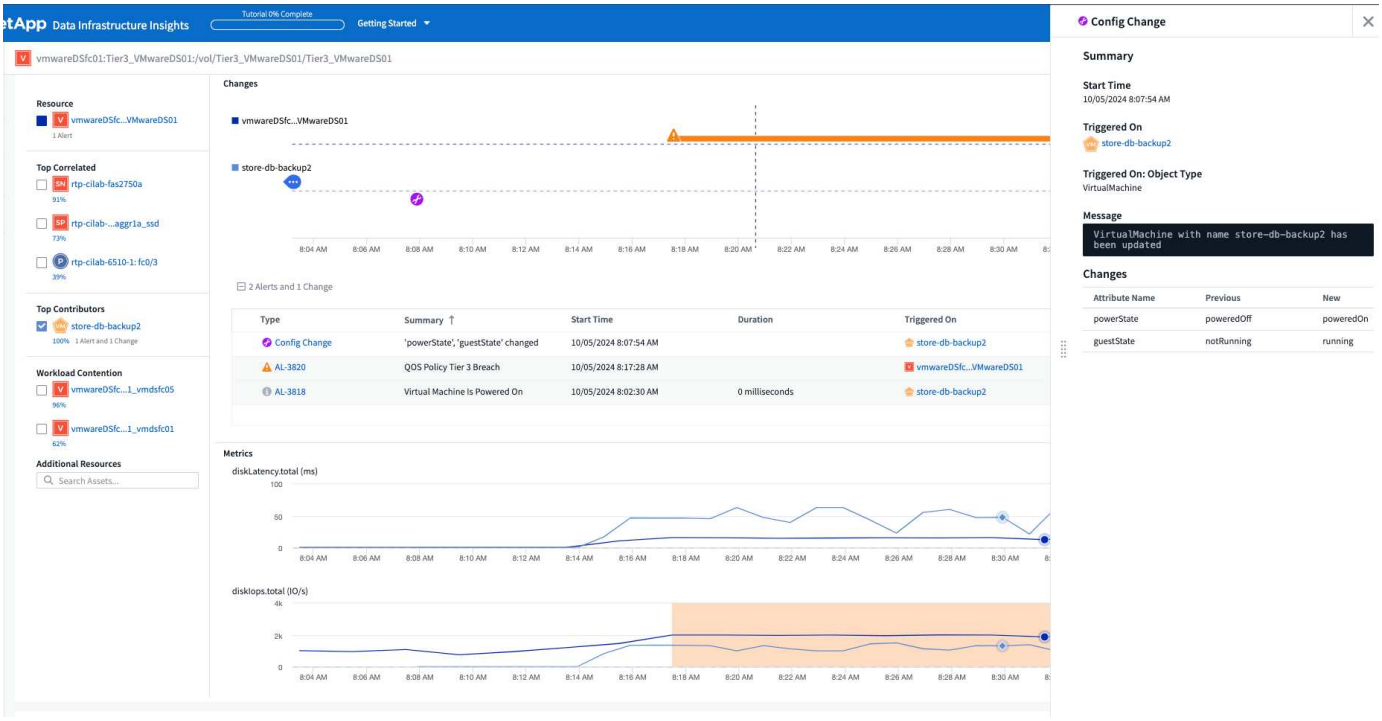
新しいワークロード セキュリティ アラート API

新しいワークロードセキュリティでフォレンジックアラートの詳細を取得"cloudsecure_forensics.alerts API"。



環境内の構成変更を分析する

構成の変更は、現代の IT における問題の最も一般的な原因の 1 つです。Data Infrastructure Insights（DII）の新しい"変更分析"機能により、環境で問題を引き起こす変更を明確に把握できます。問題の原因となった可能性のあるデバイスおよび関連インフラストラクチャ コンポーネントのすべての変更を表示することで、トラブルシューティングの時間を短縮します。さらに、あなたやあなたのチームが計画された変更を実行する場合、サービス レベルに影響が出る前にそれらの変更を迅速に検証し、予期しない影響がないことを確認できます。



KubeVirt サポート: Kubernetes クラスター内で実行されている仮想マシンのワークロードを監視します

DII は現在、OpenShift Virtualization や Harvester などのプラットフォームで使用される Kubernetes ネイティブ仮想化ソリューションである KubeVirt を完全にサポートしています。 Kubernetes クラスター内の仮想マシンとコンテナ ワークロードの両方のメトリック、イベント、構成の変更、ネットワーク トラフィックを完全に可視化します。

2024年10月

モニターのカスタム式で新たな洞察を獲得

式を使用すると、メトリックおよび異常検出モニターで算術演算を実行できます。以下に例をいくつか挙げます。

- 比率: クラウド ストレージ プロバイダーでサービス レベルの制限に達している場所を検出するための IOPS/TB。
- パーセンテージ: 使用率を計算するために使用済み/使用可能
- 集約: 複数の種類の物理ポートエラーを 1 つのモニターにまとめる
- 比較: 現在のリソース ヘッドルーム使用率を最適なヘッドルーム ポイントと比較して、フル稼働していないリソースを特定します。



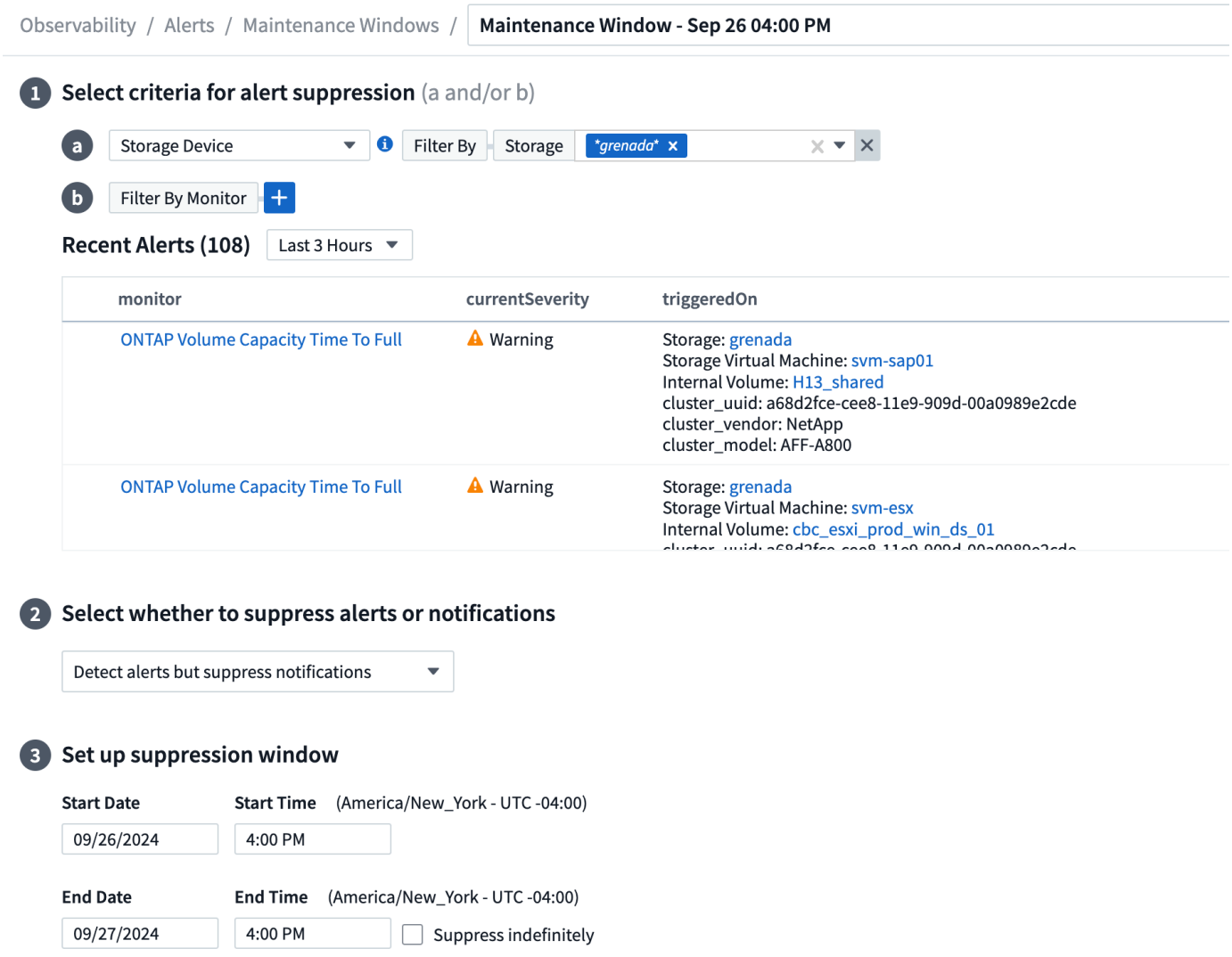


メンテナンス期間中のアラートの中断を最小限に抑える

メンテナンス ウィンドウを使用すると、スケジュールされたメンテナンス期間中にアラート通知を抑制できるため、不要な中断を回避できます。

メンテナンス ウィンドウを使用すると、選択したオブジェクトとメトリックに対して、アラート通知を抑制する特定のメンテナンス期間をスケジュールできます。たとえば、特定のストレージ システムが計画されたアップグレード期間内にある場合、それらのストレージ システムによってトリガーされるアラート通知を抑制できます。

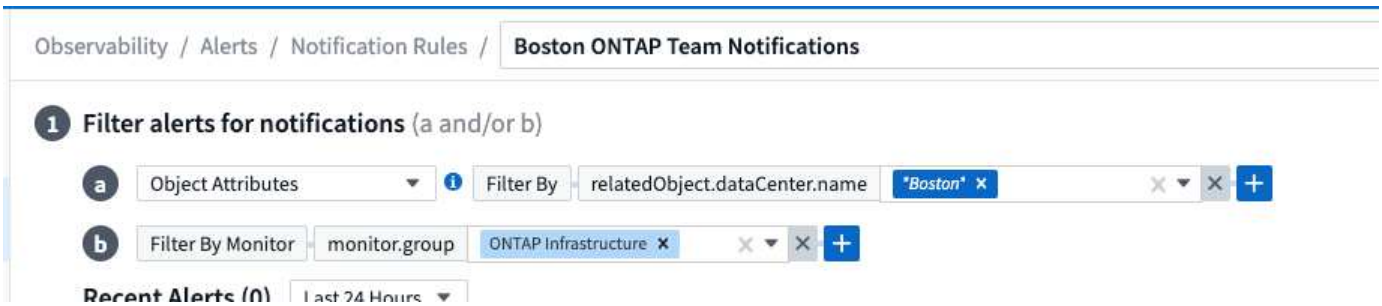
抑制されるのはアラート通知 (電子メール、Webhook) のみであることに注意してください。アラート自体は、Observability > Alerts > All Alerts ページに引き続き表示されます。



新しいアラート通知ルールでアラート管理を効率化

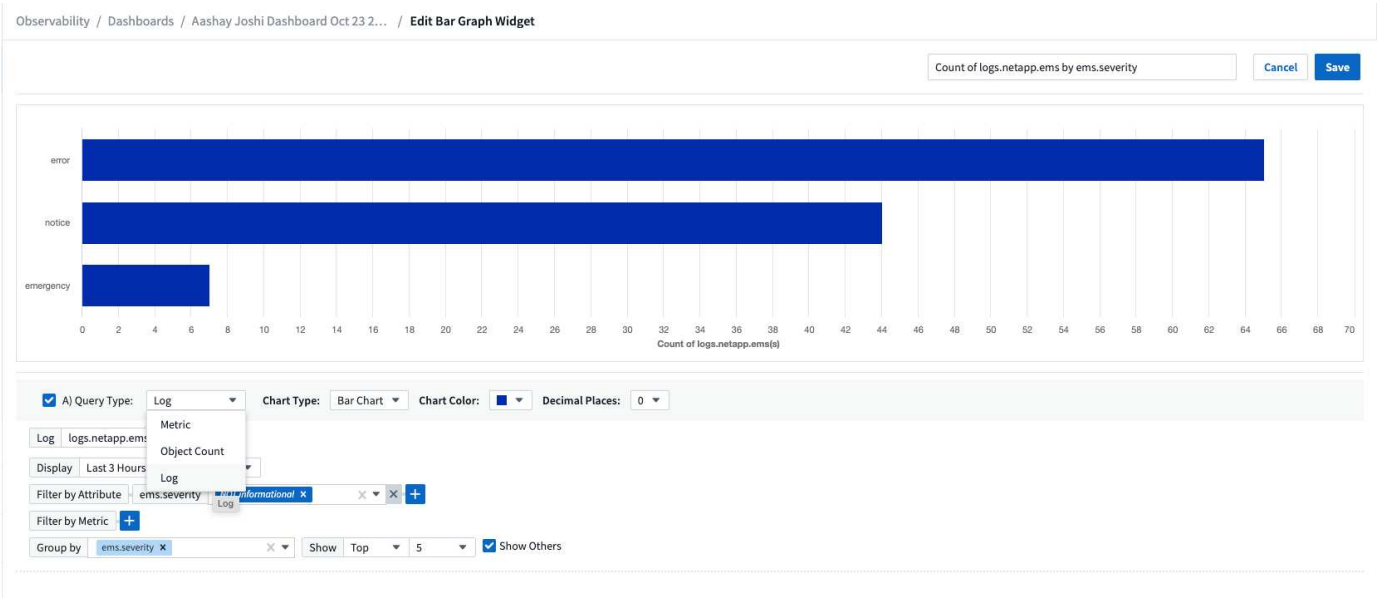
アラート通知ルールにより、モニターとチーム間の通知管理が簡素化されます。

組織のチャネル全体でアラートの配信を制御し、適切な情報が適切なチームに届くようにします。異なるチームごとに個別のモニターを管理する必要はありません。関連するオブジェクト属性 (ストレージ名、データセンター、アプリケーション名) またはモニター属性 (グループ、重大度) に基づいてアラートをルーティングします。



ダッシュボードのログ分析

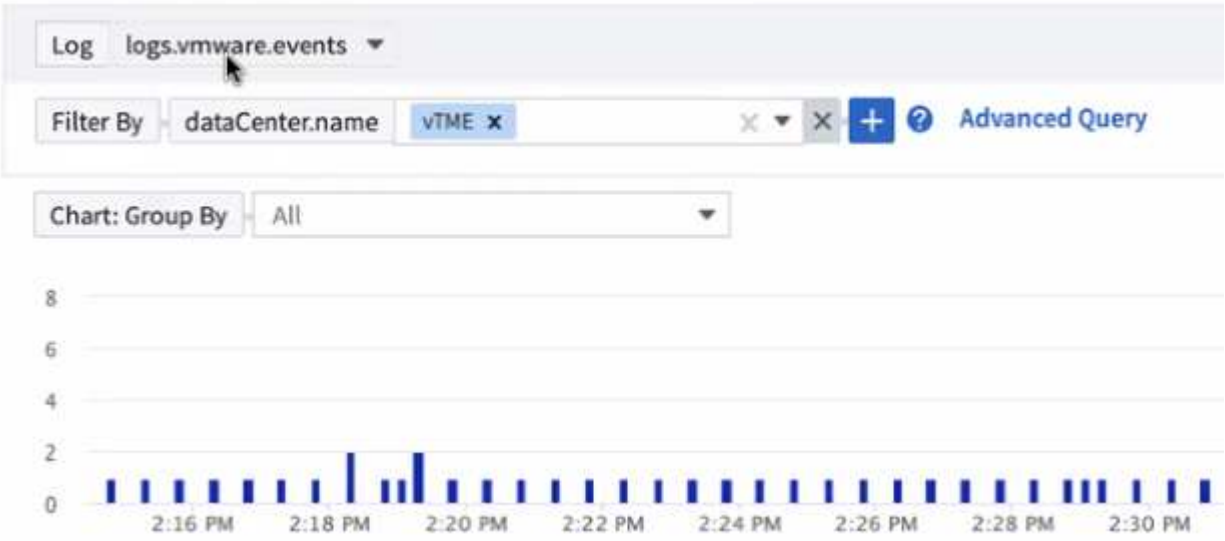
ダッシュボードにログ イベントを含めることができるようになり、イベント データを視覚化して、環境をより包括的かつ状況に応じて把握できるようになりました。ダッシュボードを離れずにログを調査し、関連するメトリックを表示します。



VMware イベントによる VMware の可観測性の向上

リアルタイム イベントを使用して VMware 環境をプロアクティブに管理およびトラブルシューティングします。 VMware イベントは、VM の移行、リソースの割り当て、ホストの健全性に関する分析情報を提供します。クエリ、ダッシュボード、モニターで使用できるようになりました。 VMware バージョン 8 以上が必要です。 *logs.vmware.events* ソースを選択するだけです。

VMware イベントは、前述の DII の新しい構成変更分析にも使用されます。



データコレクターの更新:

- **Pure FlashBlade**: このコレクターは、REST API バージョン 2 を公開する FlashBlade クラスターからインベントリとパフォーマンス データを収集します。

2024年9月

Data Infrastructure Insights（旧Cloud Insights）のご紹介

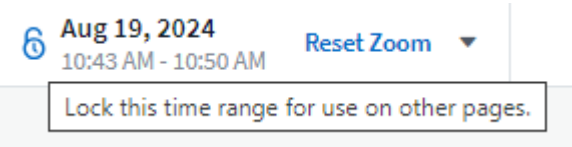
2024 年 9 月 24 日火曜日、 NetApp はCloud Insightsの名称を * Data Infrastructure Insights* (DII) に正式に変更しました。これは、Insight ユーザー カンファレンスのメイン ステージ基調講演および Insight カンファレンス製品プレス リリースにおいて、Haiyan Song 氏によって発表されました。

DII サービスは同じままです。機能の変更や修正はありません。これは、すべての IT インフラストラクチャに対するサービス名とその機能をより適切に一致させるための名前変更です。

2024年8月

時間範囲に固有のデータを表示する

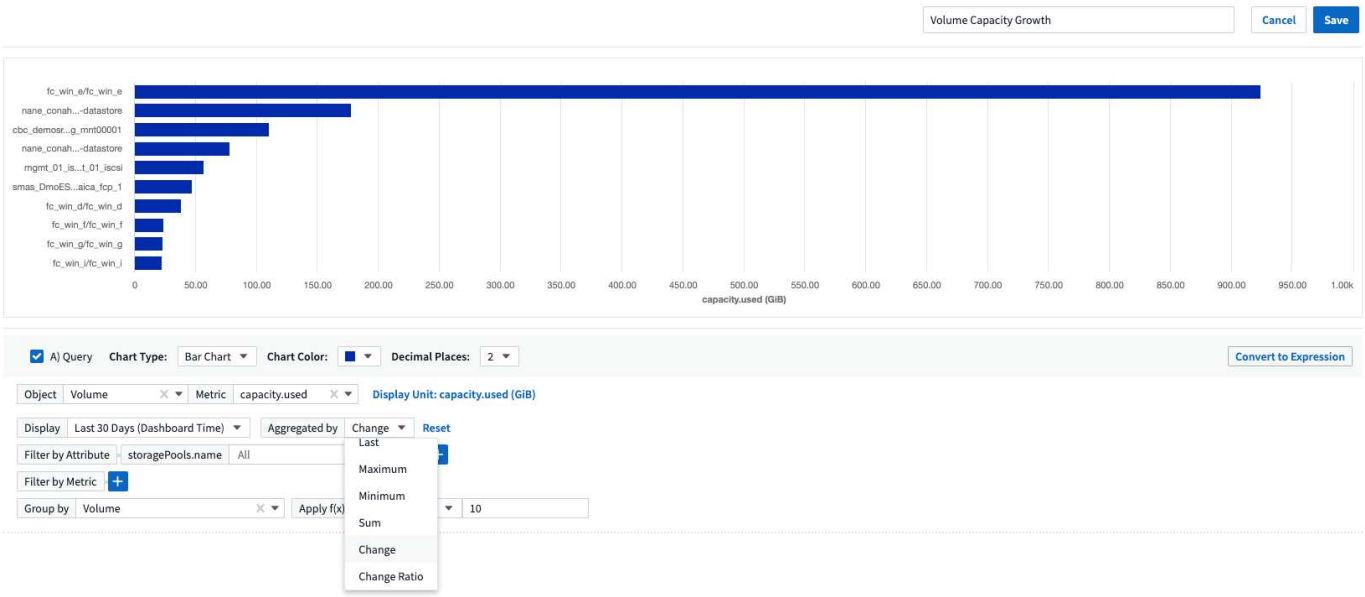
アラートを調査していますか? チャートを拡大しましたか? これらのアクションにより、それらのページの時間範囲が変更されます。これで、その時間範囲をロックし、他のCloud Insightsページに移動して、ロックされた時間範囲に固有のデータを表示できるようになります。調査とトラブルシューティングがずっと簡単になりました。



変化と変化率（%）分析

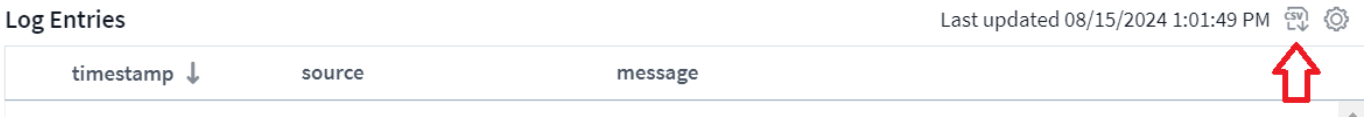
変化率の時間集計は、時間の経過に伴うメトリック値の重要な変化と傾向を識別するのに役立ちます。これらの洞察は、特定の時間における大幅な容量増加や単一ポートのパフォーマンスの変化など、何が変化したかを理解するための鍵となります。

- 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観察します。
- 変化率 - 選択した期間内の初期ポイントに対する 2 つのポイント間のメトリックの比例変化を観察します。



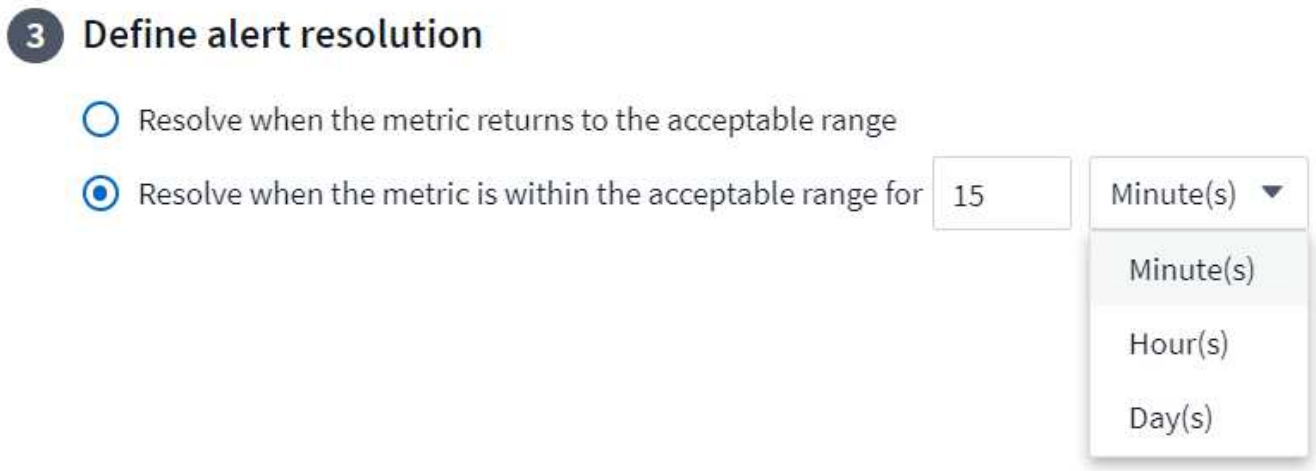
ログクエリ結果を .CSV にエクスポートする

ログ クエリの結果を表示するときに、新しい [エクスポート] ボタンをクリックすると、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、他のデータ処理ツールとのシームレスな統合が可能になります。



時間でアラートを解決する

Cloud Insightsでは、監視対象のメトリックが指定された期間にわたって許容範囲内に留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るメトリックに関連するノイズを削減し、真の問題に集中できるようになります。



2024年7月

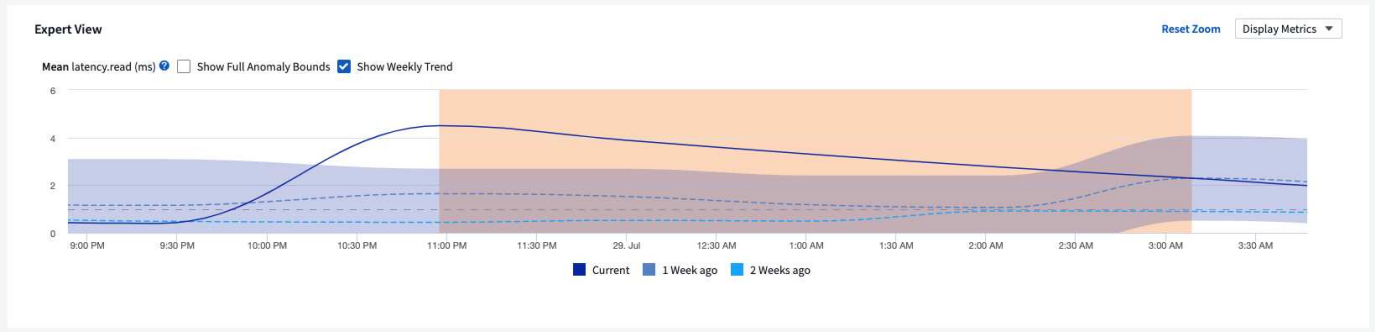
AIOps: 異常検出

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、問題を早期に特定できるようにプロアクティブなアラートを提供します。

データ センターは、時間帯や曜日によって動作が異なります。 Cloud Insights は、週ごとの季節性を使用して、各曜日と時間ごとの過去の行動を比較します。

異常検出モニタリングは、「正常」の定義が不明確な場合、時間の経過と共に動作が変化する、しきい値を手動で定義することが不可能な大量のデータを扱う場合などの状況に対してアラートを提供できます。

新しい"異常検出モニター"選択したオブジェクト メトリックでこのような異常が発生した場合に警告します。



ワークロードセキュリティの改善

NFS 4.1 サポート

SVM データ コレクターは、 ONTAP 9.15.1 以降で、**NFS 4.1** までの NFS バージョンをサポートす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**

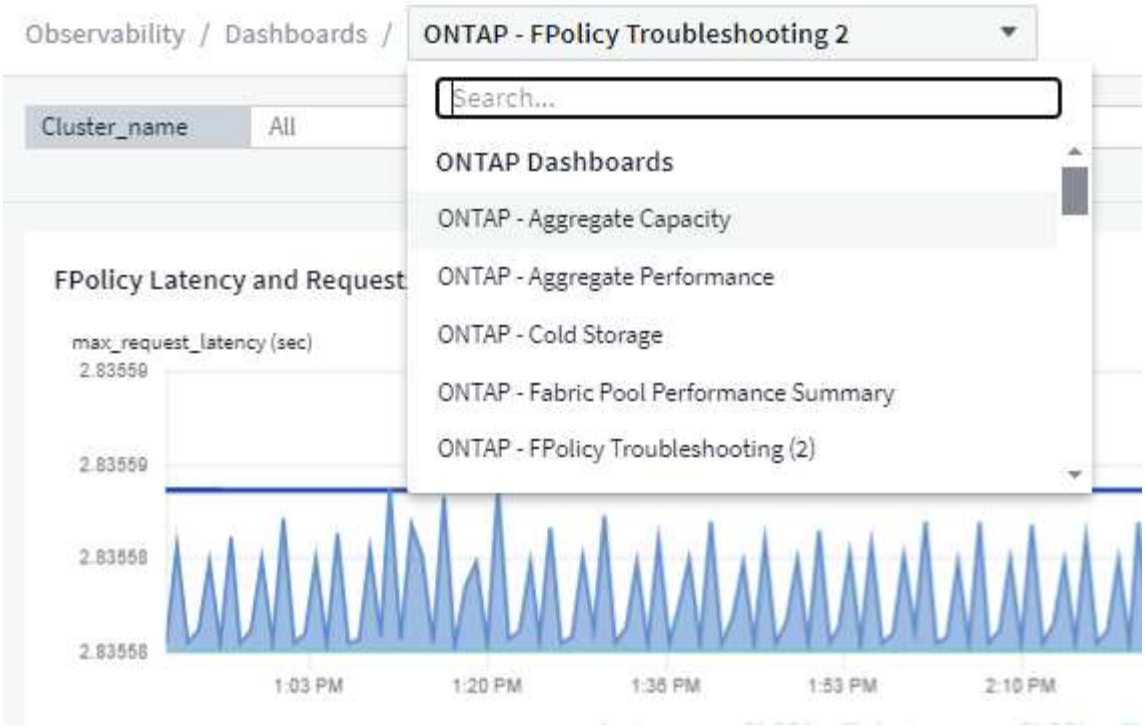
法医学活動"API"新しいバージョンがあります。フォレンジック アクティビティの API を呼び出す場合は、**cloudsecure_forensics.activities.*v2*** API を使用します。

この API を複数回呼び出す場合、最良の結果を得るには、呼び出しが並列ではなく順番に行われるようにしてください。複数の並列呼び出しにより、API がタイムアウトする可能性があります。

ダッシュボードのナビゲーションが簡単になりました

この機能は、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を目的としています。

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るようになります。また、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さまざまなダッシュボード間を移動できるため、インフラストラクチャの探索と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、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

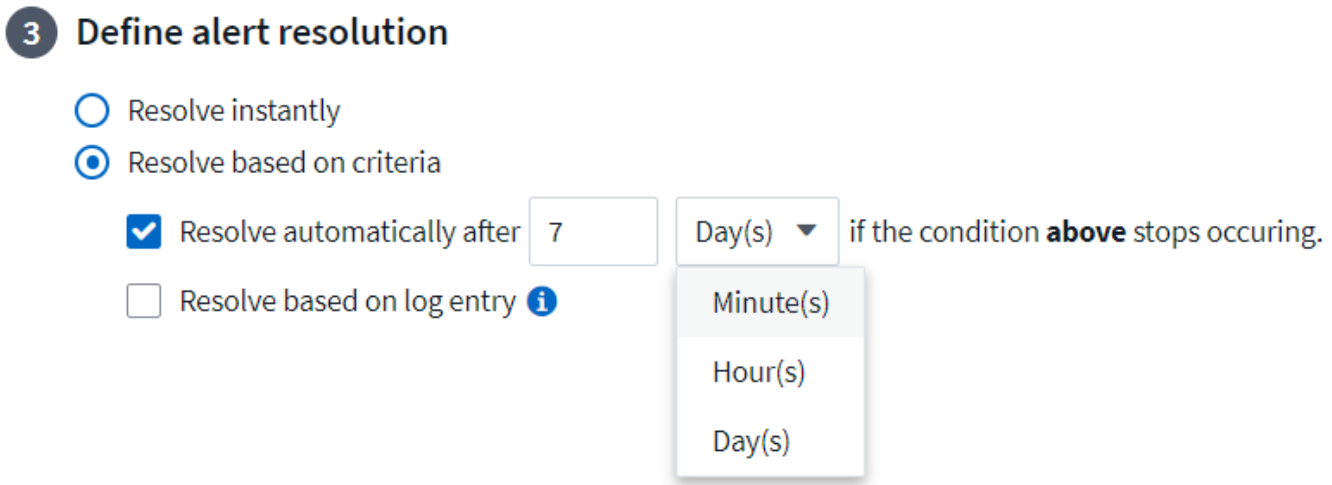
Cloud Insights Acquisition Unitsでは、以下のオペレーティングシステムがサポートされています。"すでにサポートされています" :

- 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する

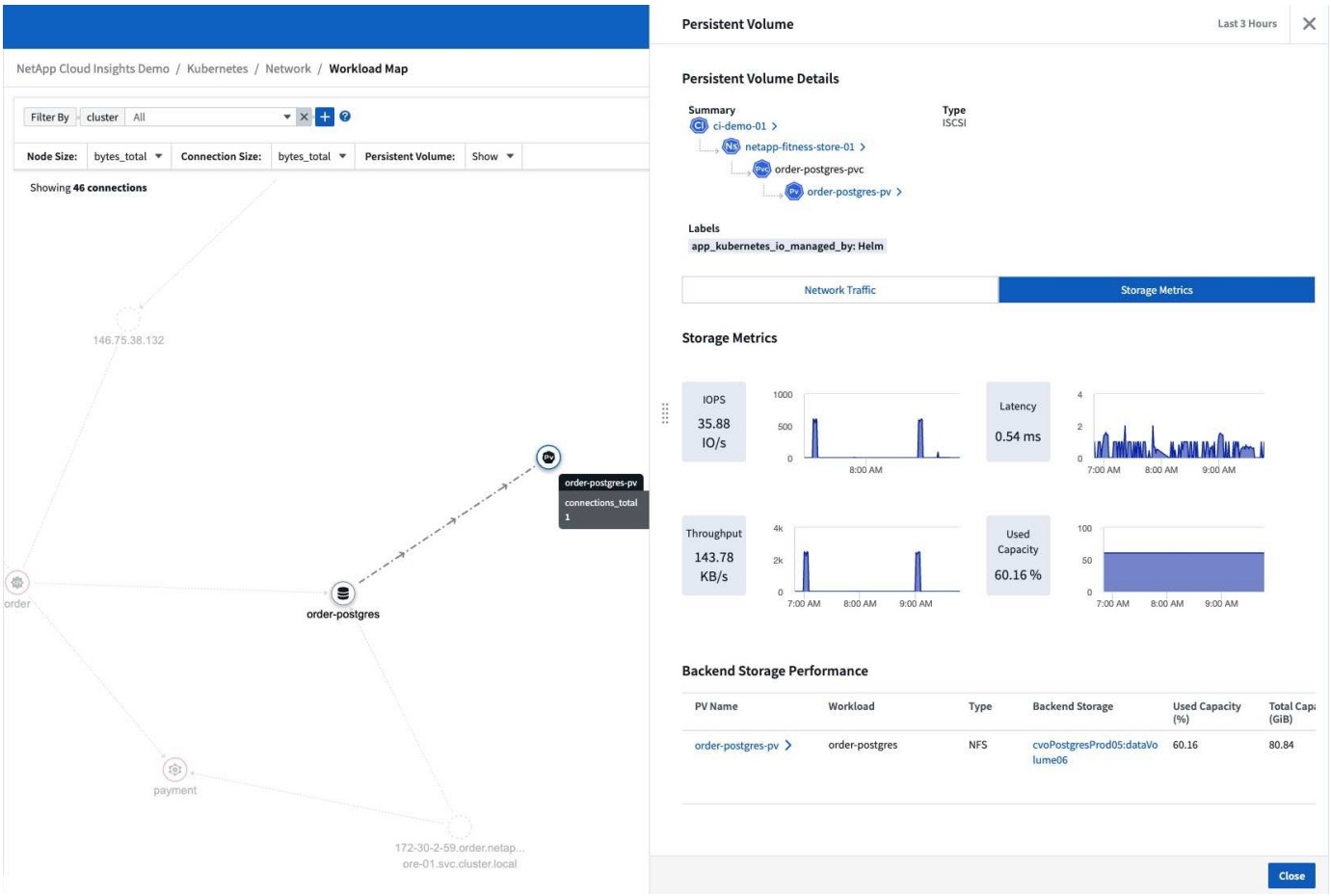
ログ アラートは時間に基づいて解決できるようになりました。アラート条件が発生しなくなった場合、指定された時間が経過すると、 Cloud Insights はアラートを自動的に解決できます。アラートを数分、数時間、または数日で解決することを選択できます。



2024年4月

Kubernetes 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、Kubernetes ネットワーク マップを使用してトラブルシューティングを高速化できるほか、レポート経由でチャージバック レポートやショーバック レポートを提供できるようになります。



オペレーティングシステムのサポート

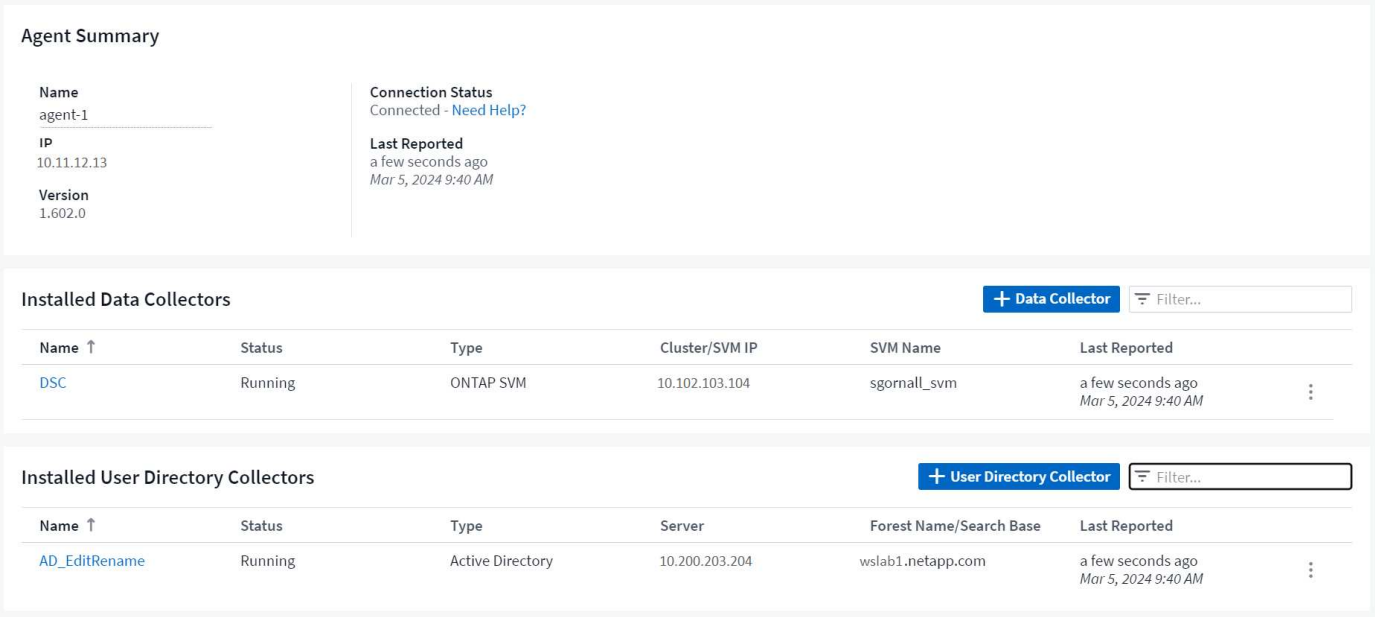
Cloud Insights Acquisition Unitsでは、以下のオペレーティングシステムがサポートされています。"すでにサポートされています" :

- Oracle エンタープライズ Linux 8.8
- Red Hat Enterprise Linux 8.8
- ロッキー 9.3
- OpenSUSE Leap 15.1 から 15.5
- SUSE Enterprise Linux Server 15、15 SP2 から 15 SP5

2024年3月

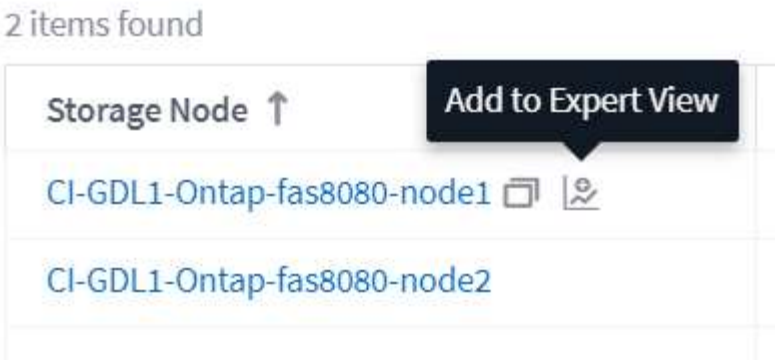
ワークロードセキュリティエージェントの詳細

各 Workload Security エージェントには独自のランディング ページがあり、そこではエージェントに関する概要情報や、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 コレクターとユーザー ディレクトリ コレクターを簡単に確認できます。

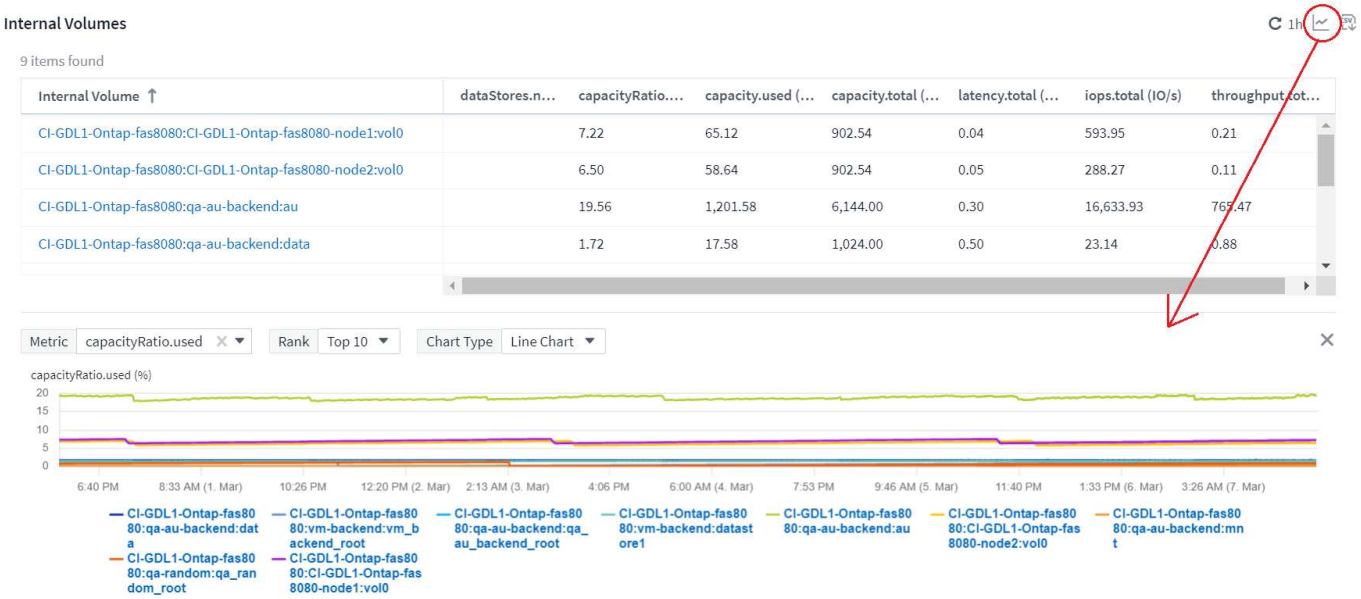


より多くのデータをより速くグラフ化

アセットのランディング ページでデータを分析する場合、エキスパート ビュー チャートに追加データを追加するのは簡単です。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、そのオブジェクトの上にマウス 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追加リソースに追加され、エキスパート ビュー チャートに表示されます。



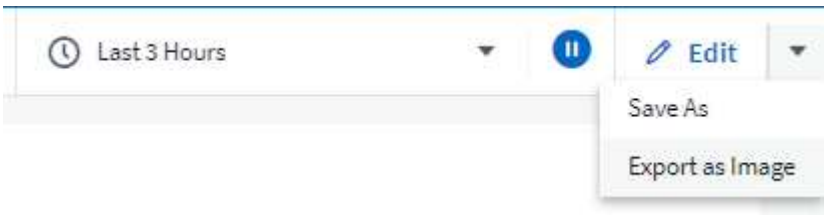
あるいは、ランディング ページ テーブルのデータを独自のグラフで表示したい場合もあります。 _チャートを表示_アイコンを選択するだけで、表の下のチャートが開きます。



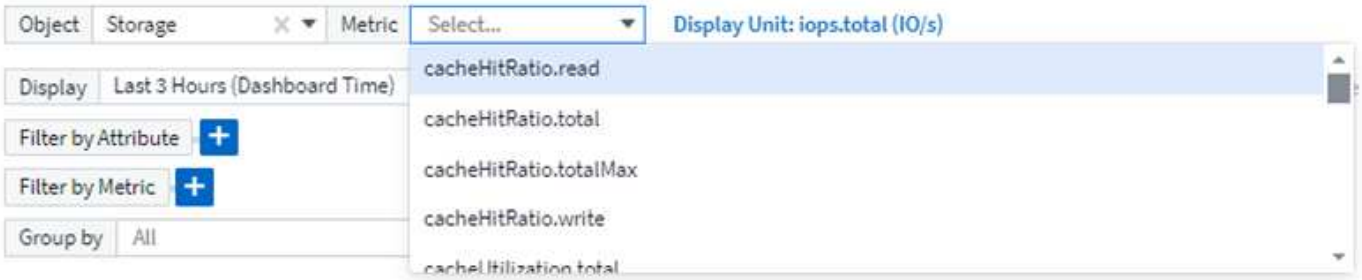
2024年2月

ユーザビリティの改善

右隅のドロップダウンから [画像としてエクスポート] 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。



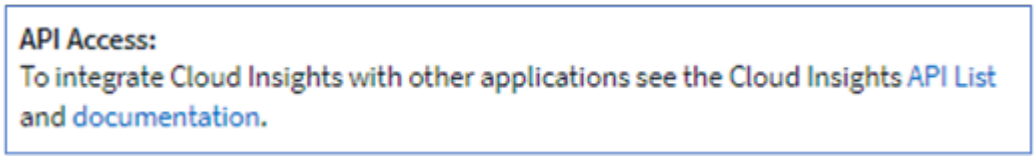
ウィジェットやモニターなどの*オブジェクトとメトリックの選択*がこれまで以上に簡単になりました。必要なオブジェクト タイプを選択し、別のドロップダウンでそのオブジェクトに関連するメトリックを選択します。



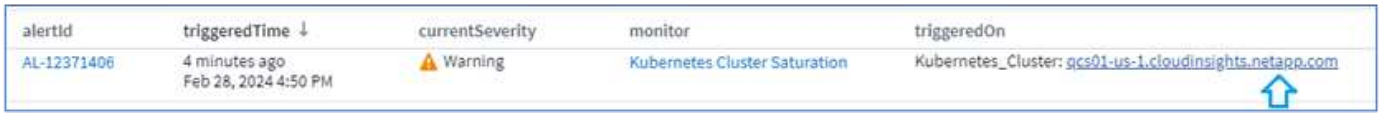
データ コレクターと取得ユニットのエクスポート リストを、ページ上部にあるアイコンを選択して .CSV にエクスポートします。



[ヘルプ **>** サポート**]** ページが再構成され、探している情報を見つけやすくなりました。また、ご要望にお応えして、このページに **API Swagger** とユーザー ドキュメントへの直接リンクを追加しました。

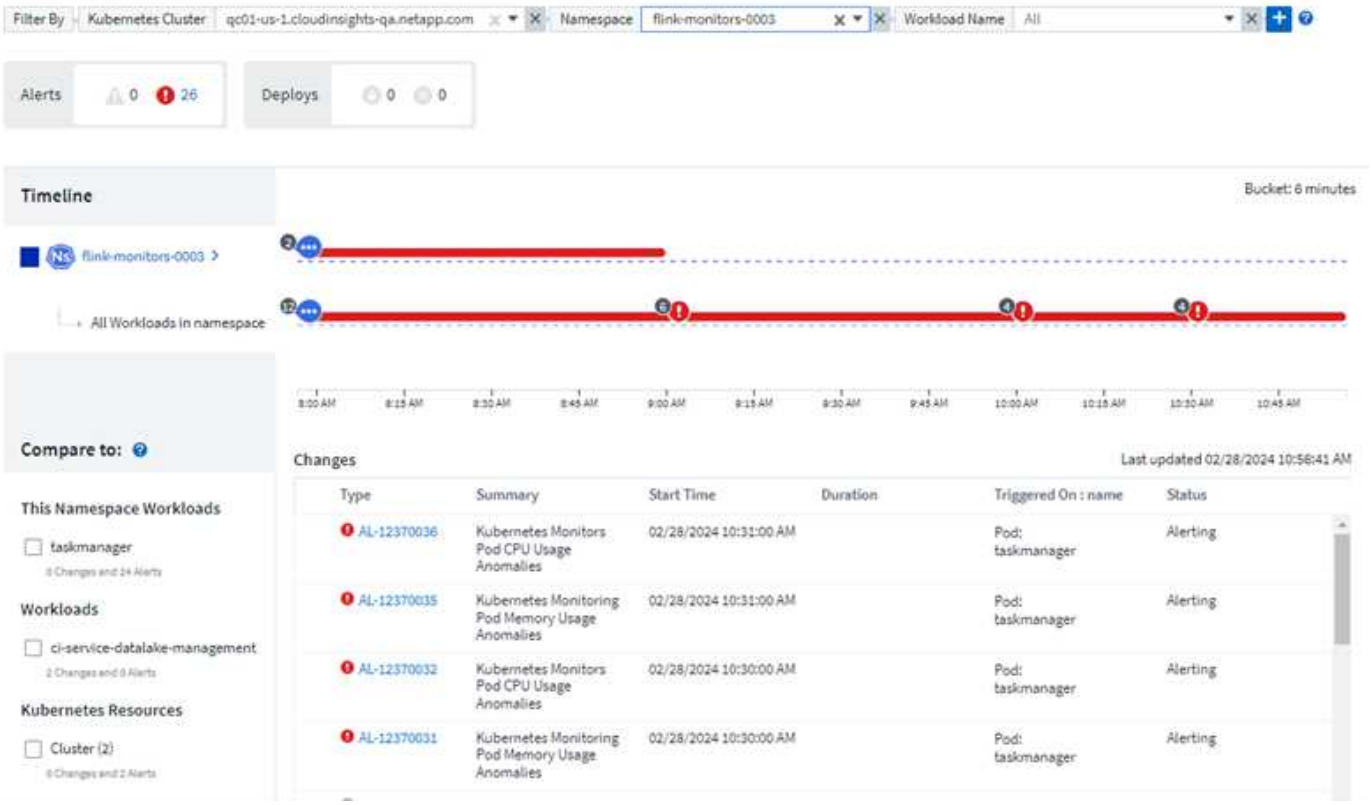


アラート リスト ページの「triggeredOn」列の リンク は、そのオブジェクトにランディング ページがある場合、適切なランディング ページに移動します。



名前空間内のすべての変更を表示する

Kubernetes 変更分析では、クラスターと名前空間を選択したときに変更のタイムラインを表示できるようになりました。事前にワークロードも選択しておく必要があります。クラスターと名前空間でフィルタリングすると、その名前空間内のすべてのワークロード変更のタイムラインが 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および期間内に発生し、同じ条件に該当する場合、関連しているとみなされます。さらに詳しく調べるには、「ログの分析」を選択します。



ONTAPスイッチデータの収集

Cloud Insights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、 ONTAPシステムが以下の情報を提供するように設定されていることを確認するだけです。"スイッチ情報"そして適切な"権限"セット。

ワークロードセキュリティデータコレクターAPI

大規模な環境では、新しいデータ コレクター API を使用して Workload Security コレクターの作成を自動化できます。詳細については、「管理 **>** API アクセス **>** API ドキュメント」に移動し、「*Workload Security*」API タイプを選択してください。

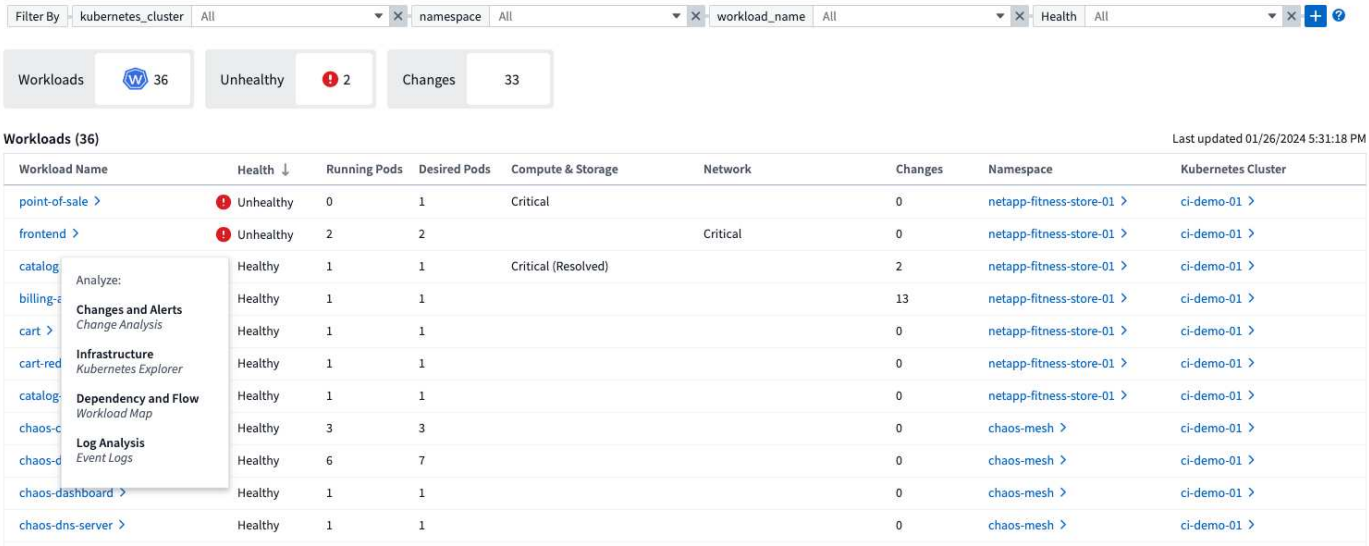
2024年1月

まだ使っていない**Cloud Insights** の機能を試す

Cloud Insightsの初期トライアルに加えて、以下の機能もご利用いただけます。"モジュール評価" 。たとえば、 Cloud Insightsに加入していて、ストレージと仮想マシンを監視している場合、Kubernetes を環境に追加すると、Kubernetes Observability の 30 日間の試用期間が自動的に開始されます。 Kubernetes Observability 管理対象ユニットの使用量は、試用期間が終了するまで、サブスクライブした権利にはカウントされません。

私のワークロードはどの程度健全でしょうか?

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、どのワークロードのパフォーマンスが良好で、どのワークロードに支援が必要かをすぐに確認できます。ヘルスの問題がインフラストラクチャ、ネットワーク、または構成の変更に関連しているかどうかを簡単に識別し、ドリルダウンして根本原因を分析します。



データコレクターの更新

データドメイン識別

Data Domain コレクターは、フェイルオーバー イベント全体にわたって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改善されました。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 再識別され、その後、それらの資産のすべての注釈が削除されます (これらのアレイが再識別されるため)。 Data Domain オブジェクトに注釈を再度添付する必要があります。

強化されたランサムウェア検出**ML**アルゴリズム

Workload Security 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は異なるパターンに従う場合があり、また朝の行動は午後とは異なる場合もあります。 Workload Security アルゴリズムでは、この季節性を考慮します。

非推奨の機能

機能が進化するにつれて、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以下に示します。

Workload Secure REST cloudsecure_forensics.activities.v1 API は非推奨になりました

cloudsecure_forensics.activities.v1 API は非推奨になりました。この API は、Storage Workload Security 環境内のエンティティに関連付けられた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 の GET は以前は次の結果を返していました。

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

この API は次を返します:

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

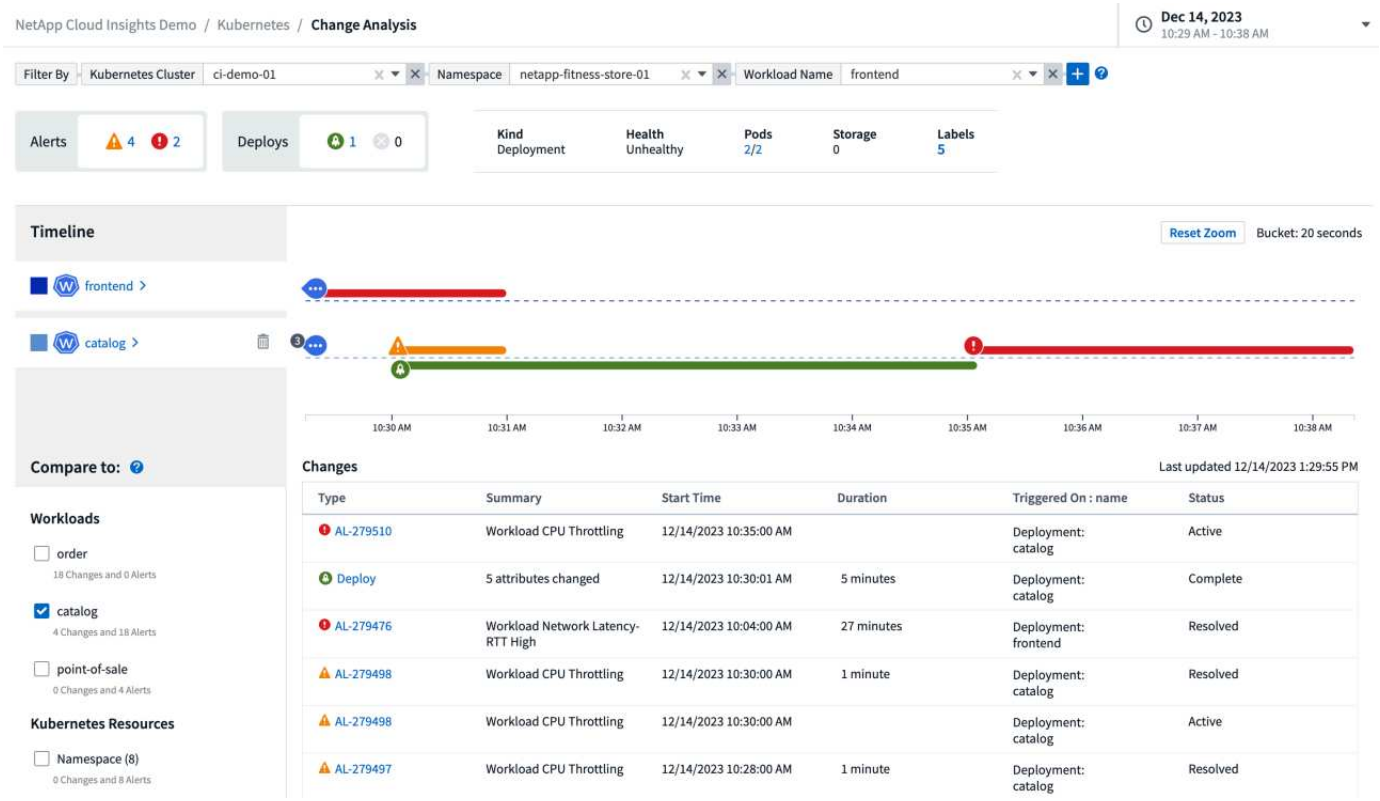
詳細については、「管理 > API アクセス > API ドキュメント > ワークロード セキュリティ」にある Swagger ドキュメントを参照してください。

2023年12月

変更分析の概要

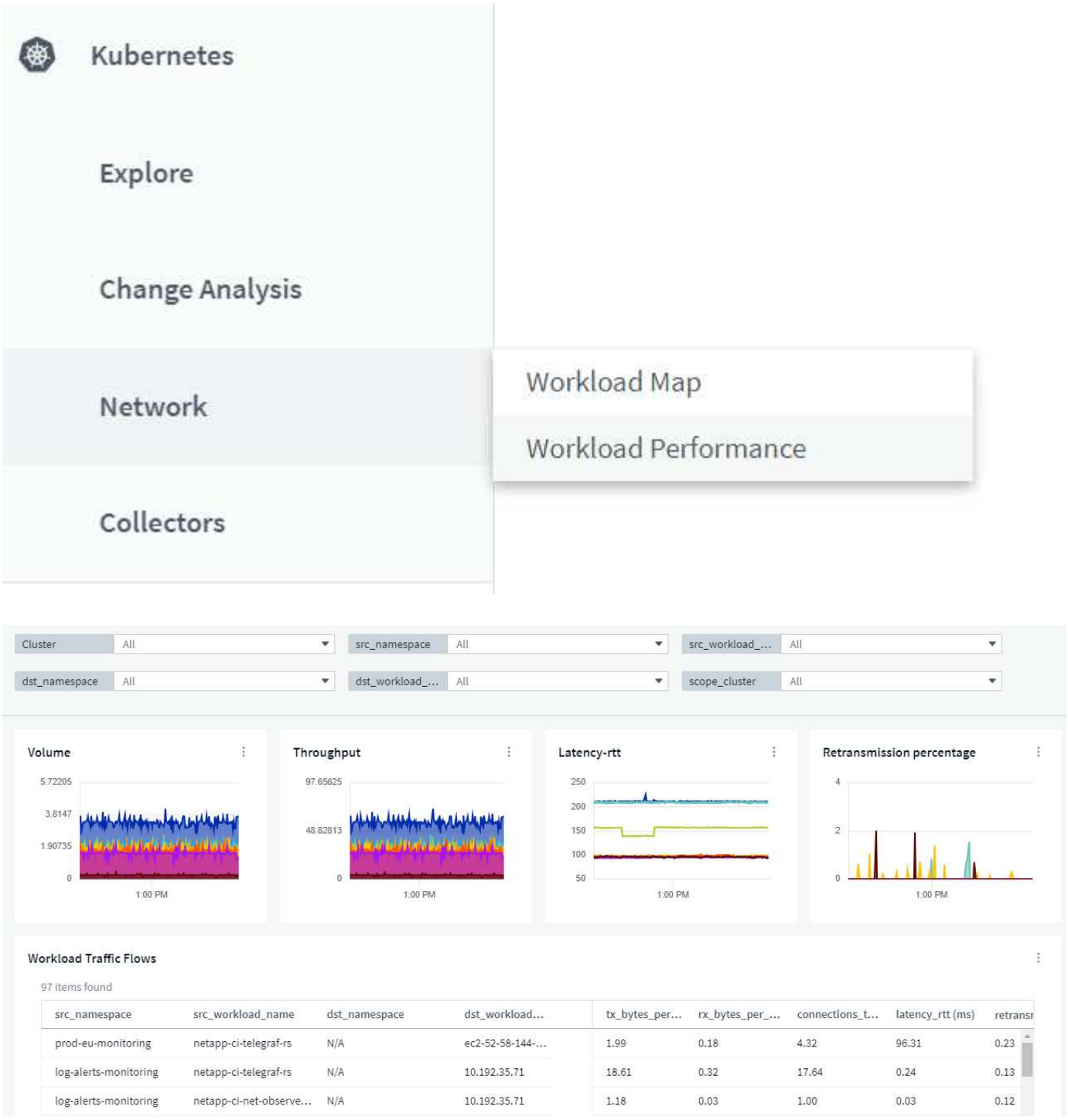
Kubernetes"変更分析" Kubernetes 環境の最近の変更を一括して表示します。アラートと展開ステータスを簡

単に確認できます。 Change Analytics を使用すると、すべてのデプロイメントと構成の変更を追跡し、それを K8s サービス、インフラストラクチャ、クラスターの健全性およびパフォーマンスと相関させることができます。



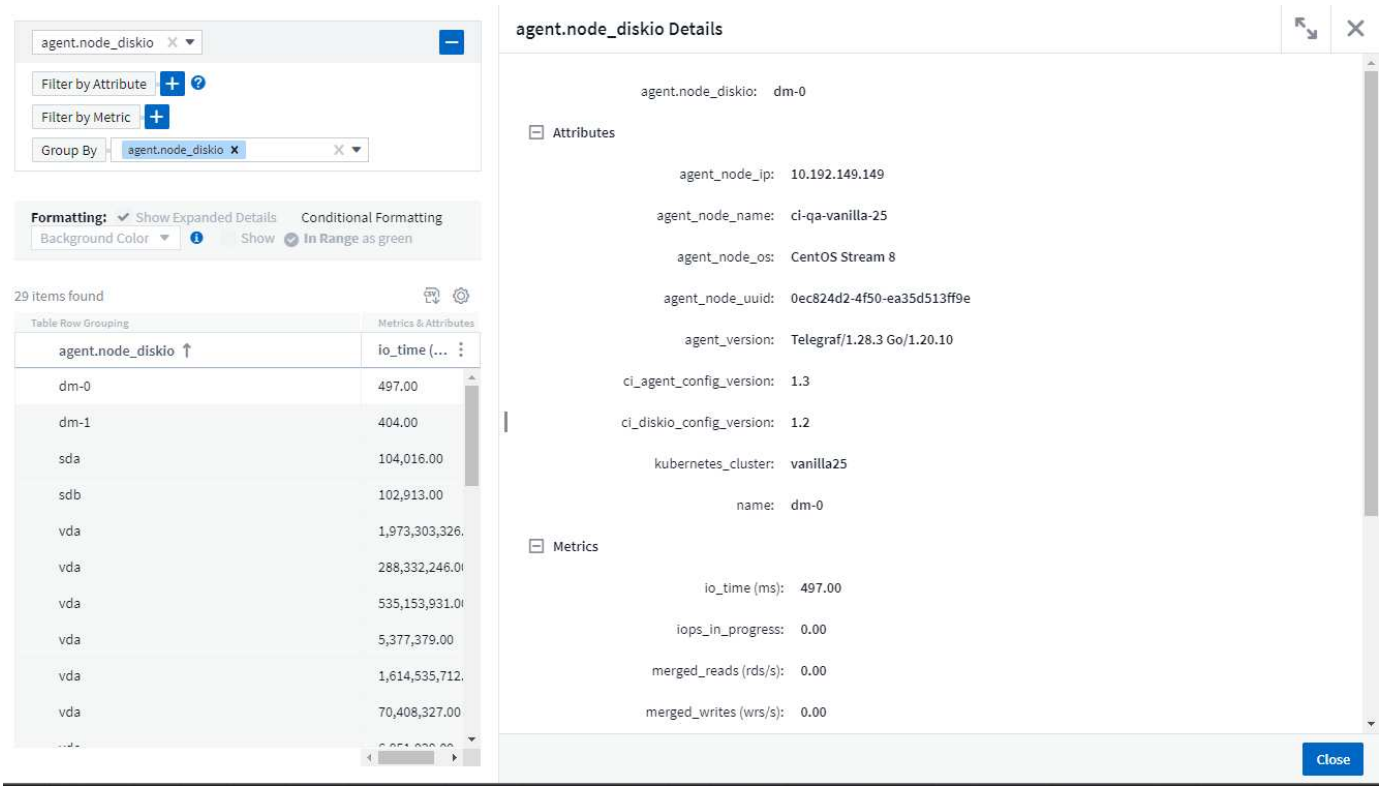
Kubernetes ワークロード パフォーマンス ダッシュボード

包括的な Kubernetes ワークロード パフォーマンス ダッシュボードでは、ワークロードのパフォーマンスを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と、環境内の各名前空間のワークロード トラフィックの表をすばやく表示します。フィルターを使用すると、関心のある領域に簡単に焦点を合わせることができます。



クエリの詳細を1つの画面で表示

クエリで行を選択すると、選択した行の属性、注釈、メトリックの詳細を示すサイド パネルが開き、オブジェクトのランディング ページにドリルダウンすることなく役立つ情報が提供されます。行またはサイド パネル内のリンクを使用すると、簡単にナビゲートできます。



データコレクターの更新:

- * Brocade FOS REST*: このコレクターは「プレビュー」から移行され、一般利用可能になりました。注意すべき点:
  - FOS は FOS 8.2 で REST API を導入しました。ただし、ルーティングなどの一部の機能は、9.0 でのみ REST API 機能を受け取ります。
  - 8.2 以降の FOS アセットと 8.2 未満の FOS アセットが混在するファブリックがある場合、 Cloud Insights FOS REST コレクターはそれらの古いアセットを検出できません。 FOS REST コレクターを編集し、そのコレクターから除外するデバイスの IPv4 アドレスのコンマ区切りリストを作成できます。
- **SELinux**: Cloud Insightsには、SELinux 強制が有効になっている Linux 環境内での操作の堅牢性を確保するための Linux Acquisition Unit の初期インストールの機能強化が含まれています。これらの機能強化は、新しい AU 展開にのみ影響します。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 構成を修正してください。

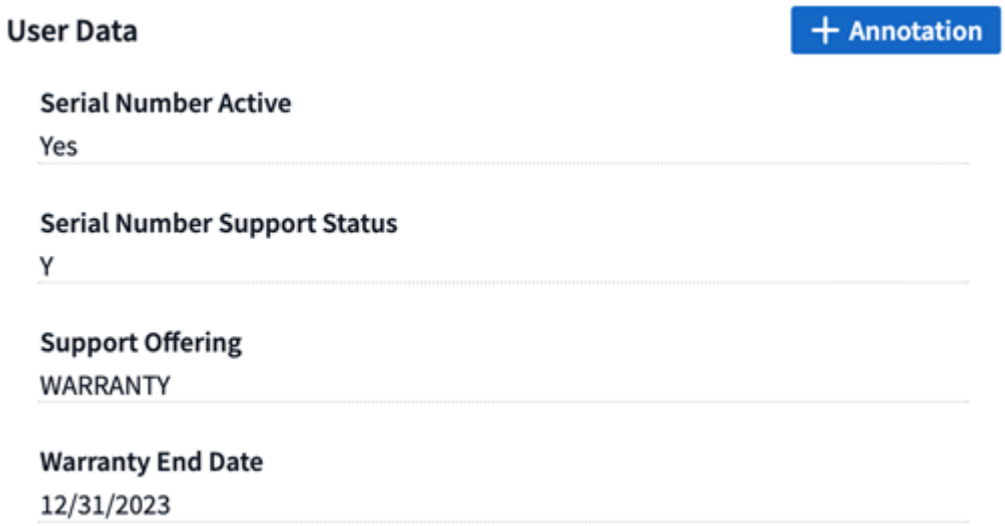
2023年11月

ワークロード セキュリティ: コレクターの一時停止/再開

Workload Security では、データ コレクターが 実行中 状態の場合、データ コレクター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。コレクターが一時停止している間は、 ONTAPからデータは収集されず、コレクターからONTAPにデータは送信されません。収集を再開するには、「再開」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 [ユーザー データ] セクションでは、サポート オファリング、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ります。 Cloud Insights は現在、 NetAppデバイスに関してのみこの情報を自動公開することに注意してください。また、これらのサポート フィールドは注釈であるため、クエリやダッシュボードで使用できることにも注意してください。



VMWare タグをCloud Insights のアノテーションにマッピングする

その"VMware"データ コレクターを使用すると、VMWare で構成されている同じ名前のタグを使用して、Cloud Insights のテキスト注釈を入力できます。

Brocade CLI コレクターの信頼性強化 (FOS 9.1.1c 以降のファームウェア)

9.1.1c ファームウェアを実行している一部のBrocade Fibre Channel 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、またはユーザーにデフォルトのパスワードを変更するように求める警告が追加される場合があります。 Brocade CLI コレクターは、これら 2 種類の不要なテキストを無視するように強化されました。

この機能強化の前は、仮想ファブリックが存在しない FOS 9.1.1c スイッチのみがこのコレクター タイプで検出可能でした。

2023年10月

強化されたワークロードセキュリティ

Workload Security は次のように改善されました。

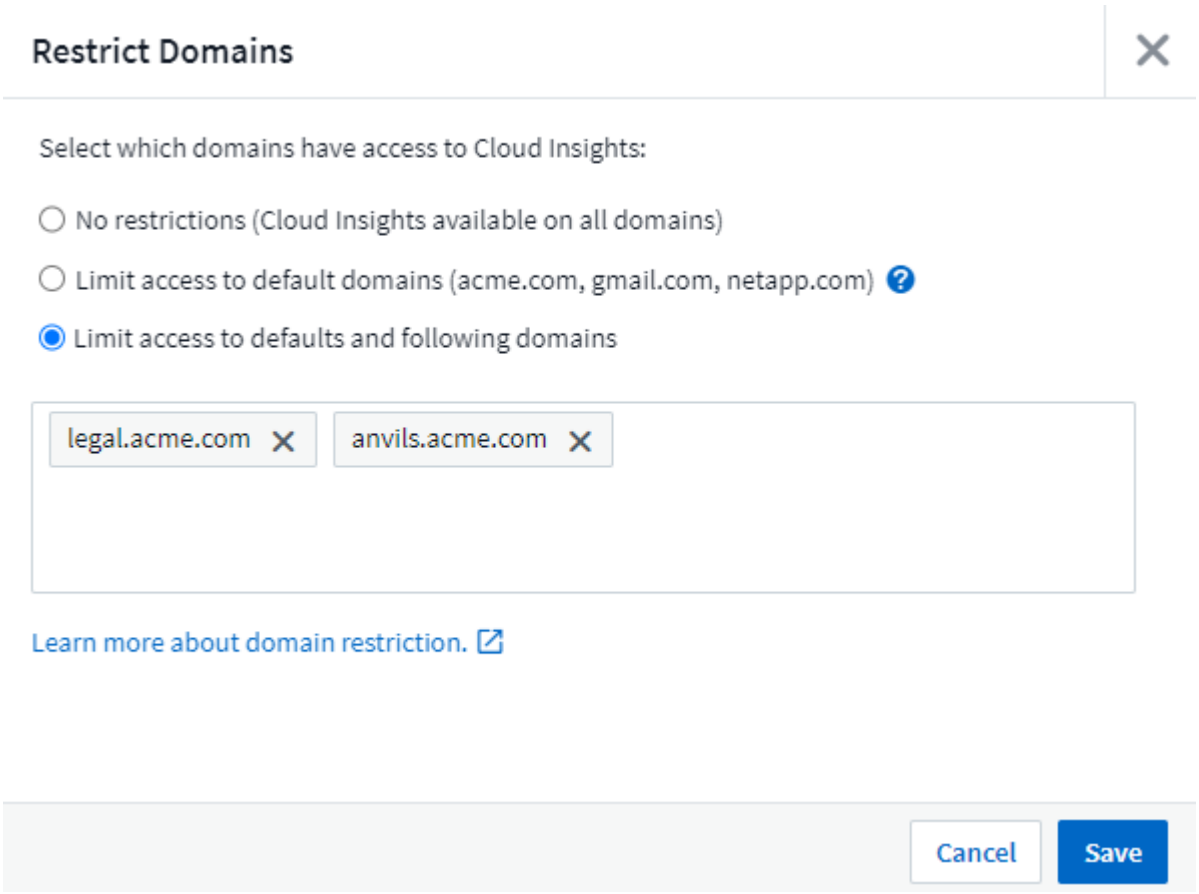
- アクセス拒否: ワークロードセキュリティはONTAPと統合して"「アクセス拒否」イベント"追加の分析および自動応答レイヤーを提供します。
- 許可されたファイルの種類: 既知のファイル拡張子でランサムウェア攻撃が検出された場合、そのファイル拡張子を"許可されるファイルの種類"不要なアラートを防ぐためのリスト。

モジュールトライアル

Cloud Insightsの初期トライアルに加えて、以下の機能もご利用いただけます。"モジュール評価" 。たとえば、すでに Infrastructure Observability に加入しているが、環境に Kubernetes を追加する場合は、Kubernetes Observability の 30 日間のトライアルが自動的に開始されます。評価期間の終了時に、Kubernetes Observability 管理対象ユニットの使用量に対してのみ課金されます。

指定され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、"Cloud Insightsへのアクセスを制限する"指定したドメインにメールを送信します。 管理 > ユーザー管理 に移動し、ドメインの制限 ボタンを選択します。



データコレクターの更新

次のデータ コレクター/取得ユニットの変更が行われます。

- **Isilon / PowerScale REST**: *emc_isilon.node_pool.** の名前で、 Cloud Insights の拡張分析機能にさまざまな新しい属性とメトリックが追加されました。これらのカウンターと属性により、ユーザーは *node_pool* 容量消費のダッシュボードとモニターを構築できるようになります。異なるハードウェア ノード モデルから構築された Isilon クラスターを持つユーザーには複数のノード プールがあり、ノード プール レベルで HDD/SSD/合計容量消費を把握することは、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 コレクターは、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。

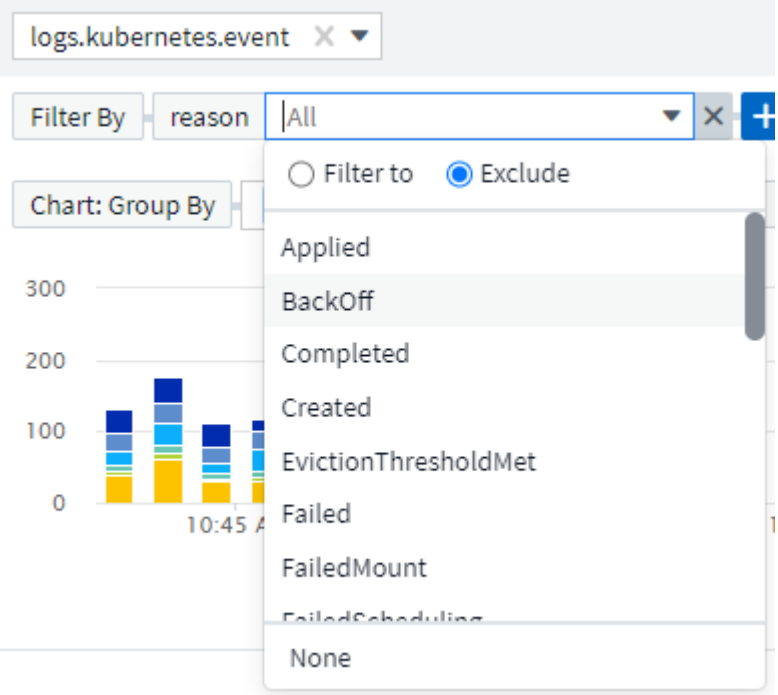
2023年9月

ログから必要なものを簡単に見つける

ログクエリ（オブザーバビリティ > ログクエリ > +新しいログクエリ）には、"機能強化"ログの探索をより簡単に、より有益なものにします。

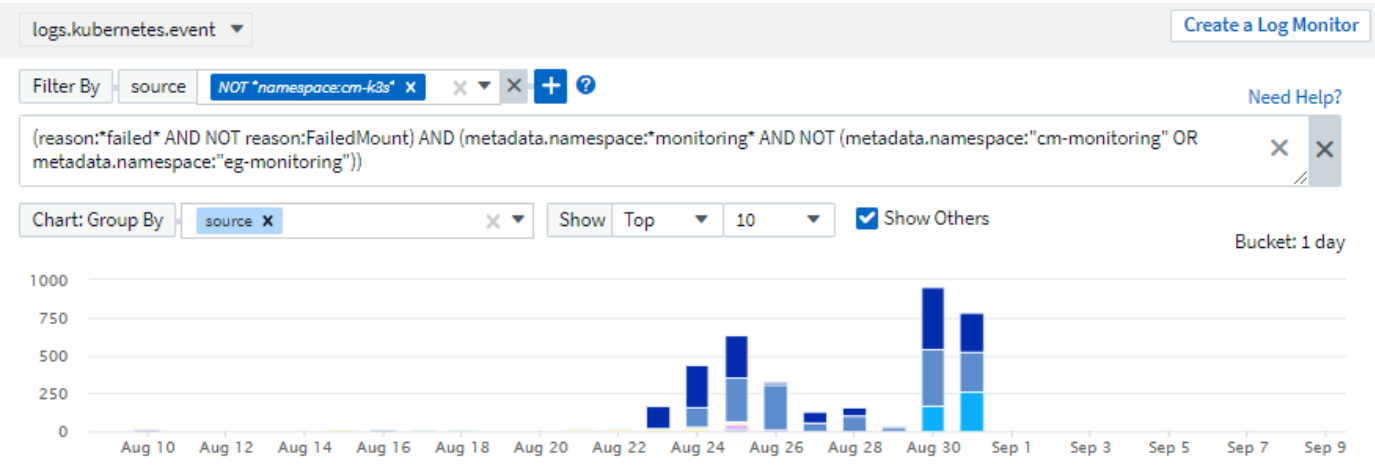
含める/除外する

値をフィルタリングする場合、フィルタに一致する結果を*含める*か*除外する*かを簡単に選択できます。「除外」を選択すると、「NOT <値>」フィルターが作成されます。含める値と除外値を 1 つのフィルターで組み合わせることができます。



高度なクエリ

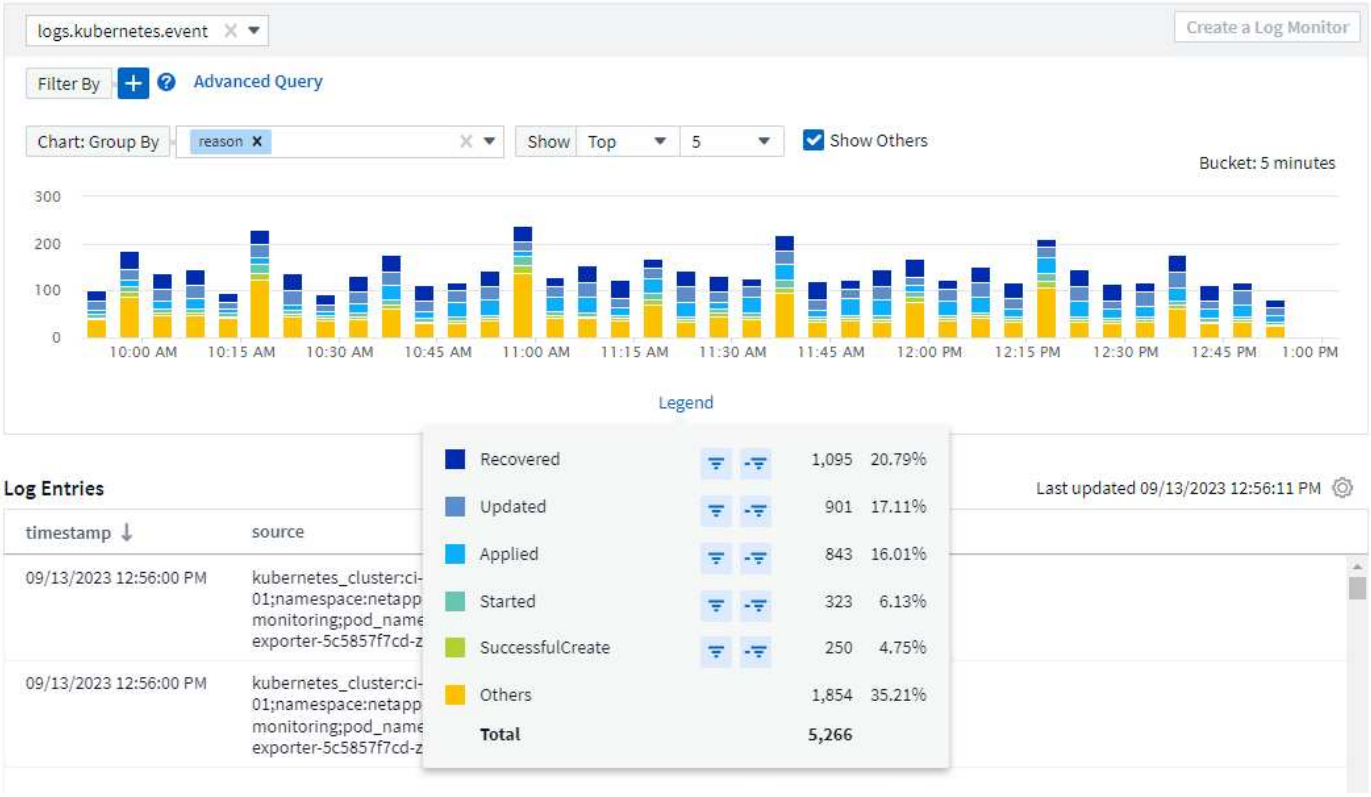
*高度なクエリ*を使用すると、AND、NOT、OR、ワイルドカードなどを使用して値を組み合わせたり除外したりする「自由形式」のフィルターを作成できます。



「フィルター条件」と高度なクエリは「AND」結合されて 1 つのクエリを形成します。結果は結果リストとグラフに表示されます。

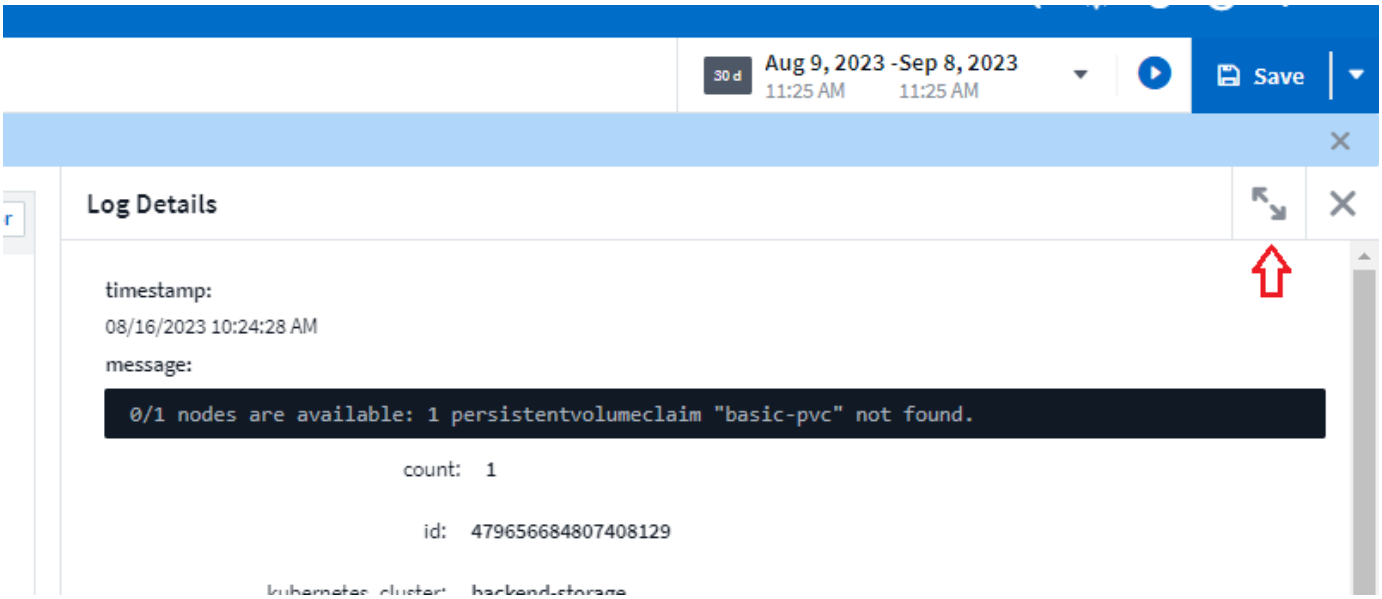
チャートのグループ化

ログ属性を選択して「グループ化」すると、リストとグラフに現在のフィルター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。グラフ内の列にマウスを移動すると、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、特定のグループに対して含めるフィルターまたは除外フィルターを設定することもできます。



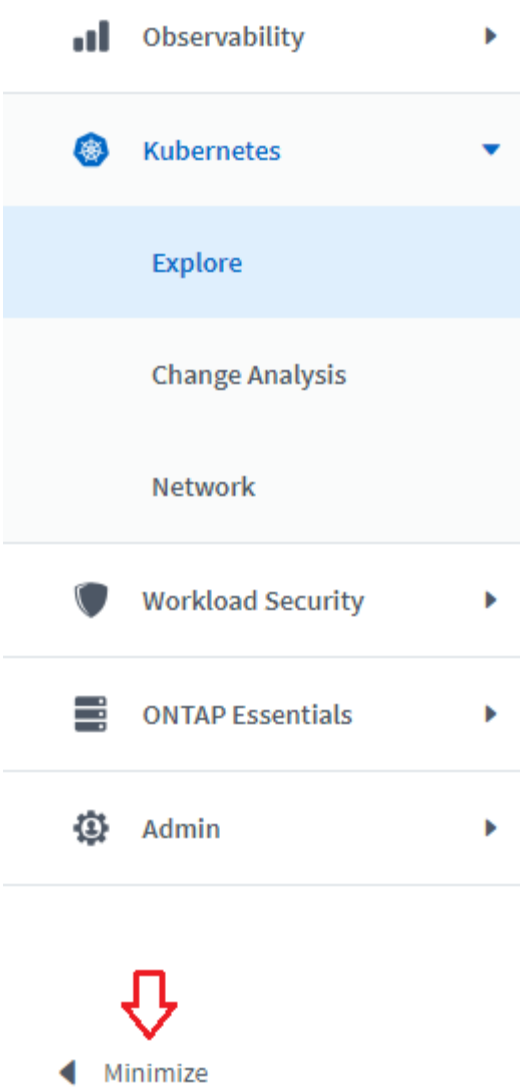
「フローティング」ログ詳細パネル

ログ クエリを使用してログを探索する場合、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」(画面の残りの部分の上に表示) するか、「ページ内」(ページ内の独自のフレームとして表示) で表示するか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

メニューの下にある「最小化」ボタンを選択すると、左側のCloud Insightsナビゲーション メニューを折りたたむことができます。メニューが最小化されているときにアイコンの上にマウスを置くと、どのセクションが開くかを確認できます。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。



データコレクターの改善

Cloud Insightsにより、データ コレクター情報の表示と検索が簡単になりました。

- データ コレクター リストの処理 がより効率的になり、リストの表示や移動にかかる時間が大幅に短縮されます。多数のデータ コレクターが存在する大規模な環境の場合は、データ コレクターの一覧を表示するときに大幅な改善が見られます。
- データ コレクター サポート マトリックス は .PDF ファイルから .HTML ベースのページに移動され、ナビゲートが高速化され、保守が容易になりました。新しいマトリックスをここでチェックしてください: 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 および PowerScale REST コレクターには、次の改善が含まれています。

- Isilon ログイベントはクエリやアラートで使用できます
- Isilon Advanced Analytic 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.ノード
  - emc_isilon.node_disk
  - emc_isilon.net_iface

これらは、Isilon REST および/または PowerScale REST コレクター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 は、Isilon CLI ベースのコレクターのユーザーに対し、上記のような機能強化を受けるために、新しい REST API ベースのコレクターに移行することを強く推奨しています。

改善されたワークロードマップ

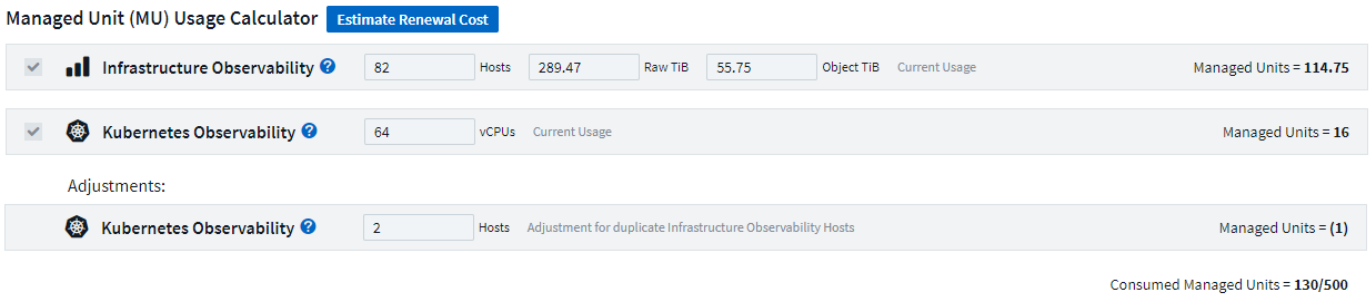
ワークロード マップは、より使いやすく、ノイズが少なくなっています。同じワークロードと通信するすべての類似した外部サービスを 1 つのノードにグループ化することで、グラフの複雑さが軽減され、サービスがどのように相互接続されているかを理解しやすくなります。

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テーブルが表示されます。

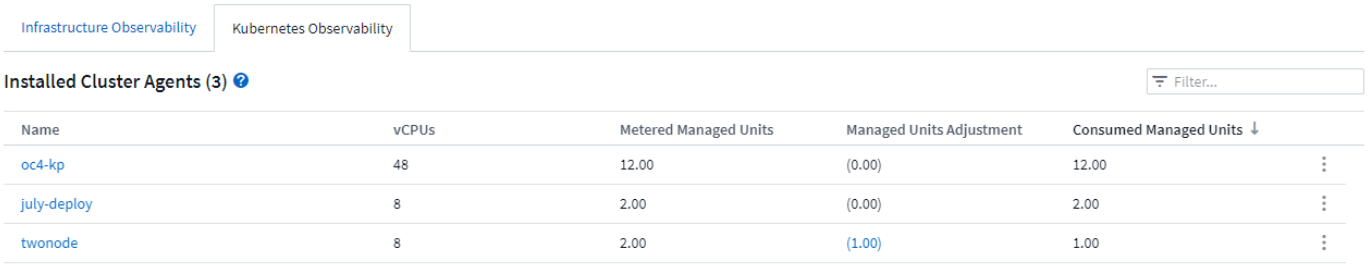
Kubernetes 管理ユニットの使用量の調整

Kubernetes クラスタ環境内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ストラクチャ データ コレクター (VMware など) の両方によってカウントされる場合、これらのリソースの使用量は、管理対象ユニットが最も効率的にカウントされるように調整されます。 Kubernetes MU の調整は、[管理] > [サブスクリプション] ページの [概要] タブと [使用状況] タブの両方で確認できます。

概要タブ
:



使用状況タブ
:



コレクター/取得の変更:

次のデータ コレクター/取得ユニットの変更が行われます。

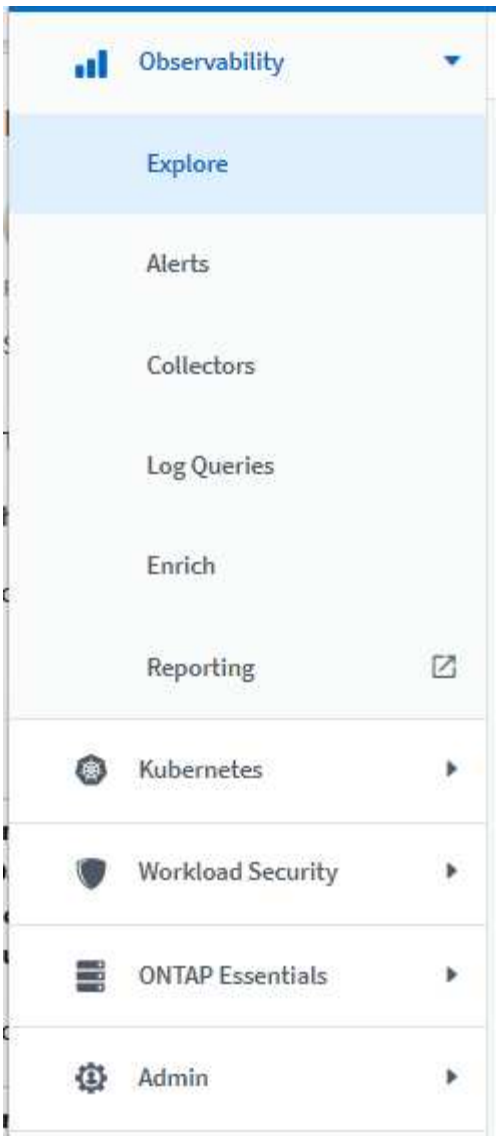
- 取得ユニットは RHEL 8.7 をサポートするようになりました。

改善されたメニュー

お客様のワークフローをより適切にサポートするために、左側のナビゲーション メニューを更新しました。*Kubernetes* などの新しいトップレベル項目により、顧客のニーズへの高速アクセスが提供され、統合された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。

変更点の追加例をいくつか示します。

- 最上位の_Observability_メニューには、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アクセス」機能が1つのメニューにまとめられました
- オブザーバビリティとワークロードセキュリティの「通知」機能も同様に、1つのメニューにまとめられました。



各メニューで見つけることができる機能の簡単なリストは次のとおりです。

可観測性:

- 探索（ダッシュボード、メトリッククエリ、インフラストラクチャインサイト）
- アラート（モニターとアラート）
- コレクター（データ収集装置および取得ユニット）
- ログクエリ
- エンリッチメント（注釈と注釈ルール、アプリケーション、デバイスの解像度）
- レポート

Kubernetes:

- クラスター探索とネットワークマップ

ワークロードセキュリティ:

- アラート
- 法医学
- コレクター
- ポリシー

ONTAP の基本:

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

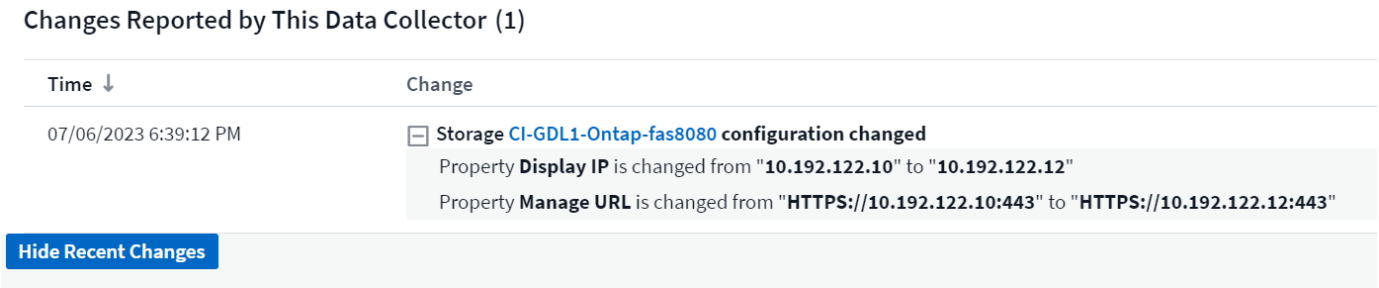
管理者:

- API アクセス
- 監査
- 通知
- 購読情報
- ユーザー管理

2023年7月

最近の変更を表示

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



オペレーターの改善

以下の改善が行われました"Kubernetesオペレーター"展開:

- Docker メトリック収集をバイパスするオプション

- Telegraf Daemonsets および Replicasets に許容範囲を追加およびカスタマイズする機能

洞察：冷蔵倉庫の再利用

その"ONTAP Cold Storage Insight の再利用"FlexGroups をサポートするようになり、すべてのお客様にご利用いただけるようになりました。

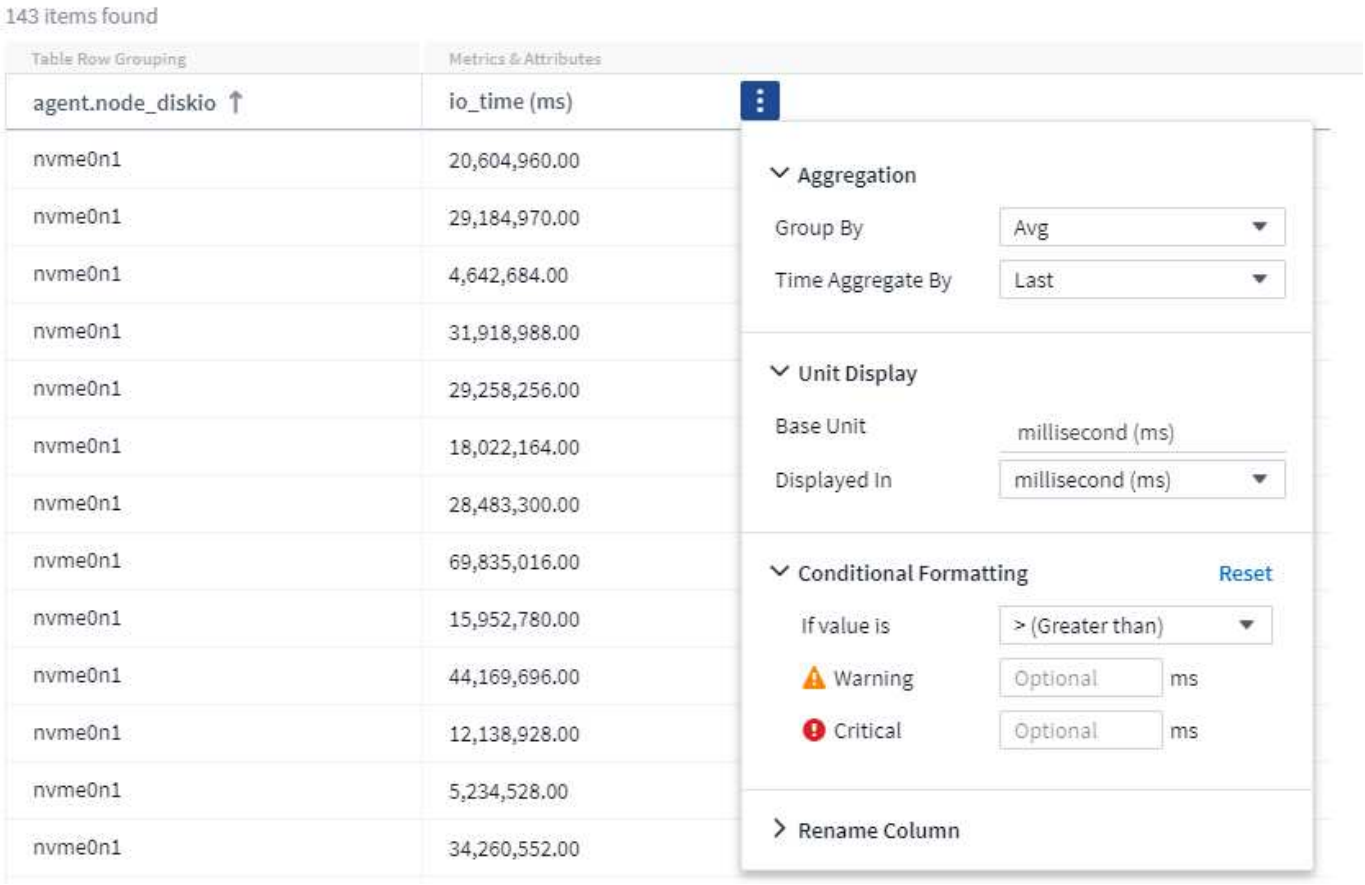
オペレーター画像署名

NetApp Kubernetes Monitoring Operator にプライベート リポジトリを使用するお客様は、Operator のインストール中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 [イメージ署名の公開キーをコピー] ボタンを選択し、オペレーター 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

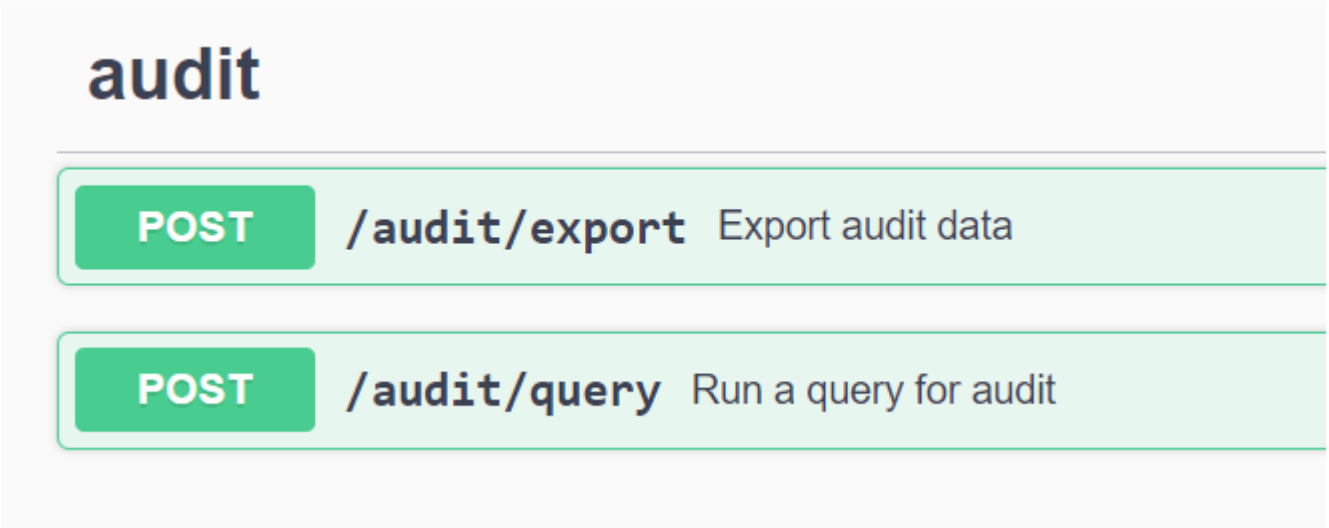
集計、単位選択、条件付き書式、列名の変更はダッシュボードテーブルウィジェットの最も便利な機能の一つであり、これらの同じ機能が"クエリ"。



これらの機能は現在、統合型データ（Kubernetes、 ONTAP Advanced Metrics など）で利用可能であり、インフラストラクチャ オブジェクト（ストレージ、ボリューム、スイッチなど）でもまもなく利用可能になる予定です。

監査用API

API を使用して監査イベントをクエリまたはエクスポートできるようになりました。詳細については、「管理」>「API アクセス」に移動し、「*API* ドキュメント」リンクを選択してください。



データ収集者:Trident・エコノミー

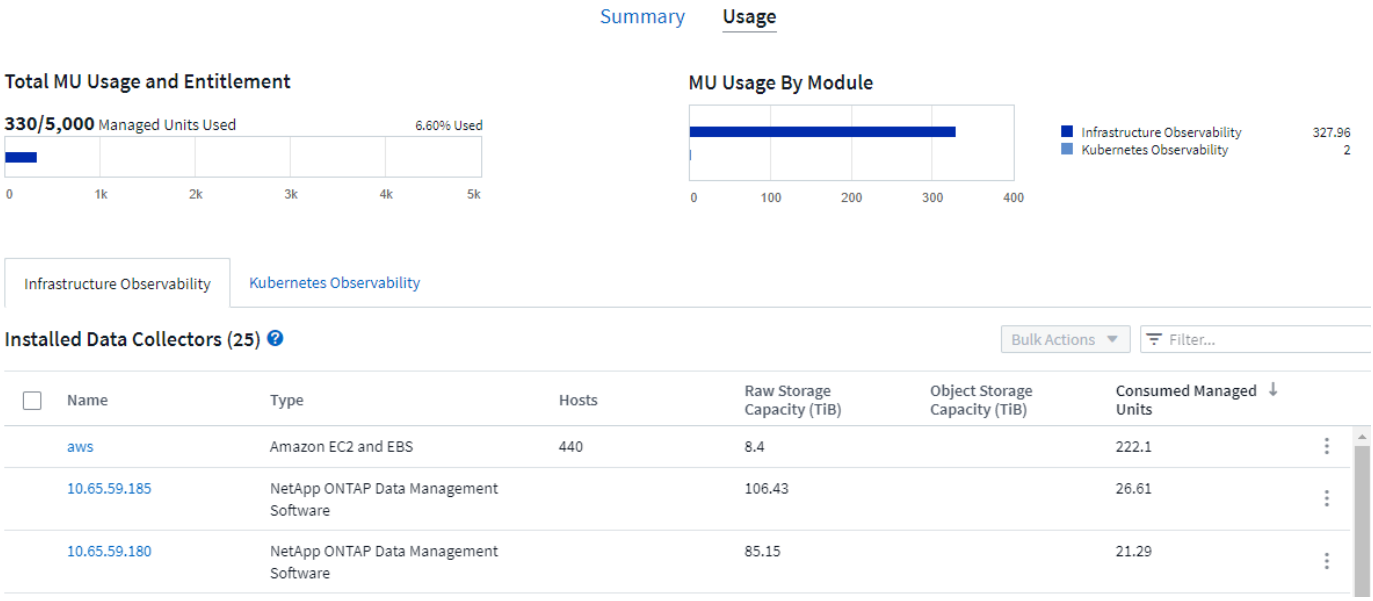
Cloud Insights はTrident Economy Driver をサポートするようになり、次のようなメリットが実現されています。

- ポッドとONTAP Qtree のマッピングとパフォーマンス メトリックを可視化します。
- Kubernetes ポッドからバックエンド ストレージまで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。
- モニターを使用して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する

2023年6月

使用状況を確認する

2023 年 6 月から、 Cloud Insights機能セットに基づいて管理対象ユニットの使用状況の内訳が提供されます。インフラストラクチャの管理対象ユニット (MU) の使用状況と、Kubernetes に関連付けられた MU の使用状況をすばやく表示および監視できるようになりました。



Kubernetesネットワーク監視とマップはすべての

その"*Kubernetes 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素化し、Kubernetes ネットワーク パフォーマンスの遅延と異常をリアルタイムで可視化して、ユーザーに影響が及ぶ前にパフォーマンスの問題を特定します。プレビュー期間中に多くのお客様に役立ったと評価いただき、現在では誰でもご利用いただけるようになりました。

コレクター/取得の変更:

次のデータ コレクター/取得ユニットの変更が行われます。

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

- 取得ユニットは、RHEL および Rocky 9.0 および 9.1 をサポートす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 ダッシュボードはプレビュー環境で利用可能でしたが、現在はすべてのユーザーが利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 (ローカルおよびリモート保護の概要を含む)

追加のシステムモニター

Cloud Insightsには次のシステム モニターが含まれています。

- ストレージ VM FCP サービスが利用できません
- ストレージ VM iSCSI サービスが利用できません

2023年5月

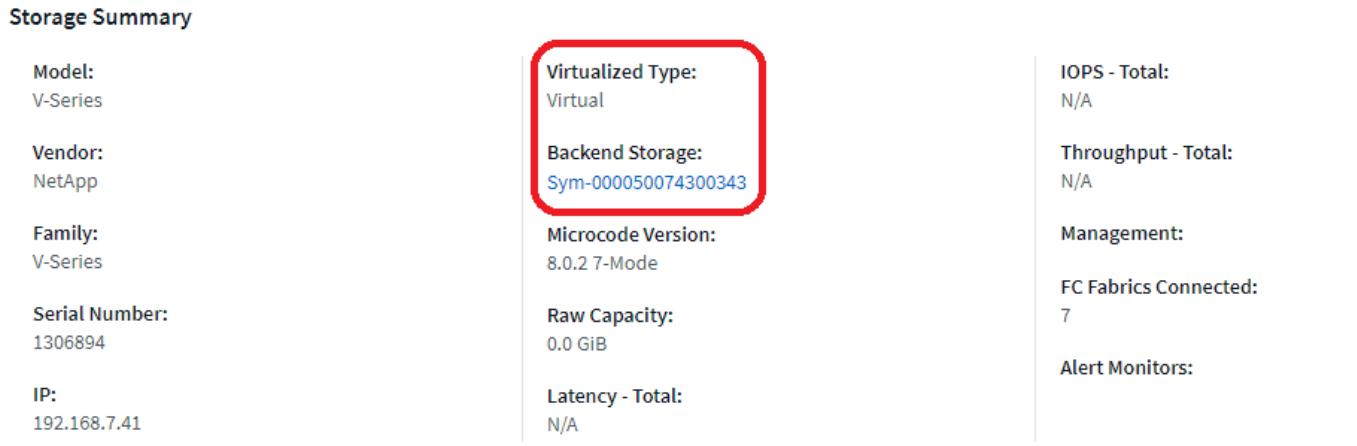
Kubernetes モニタリング オペレーターのインストールの改善

インストールと設定"NetApp Kubernetes 監視オペレーター"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"単一の自己文書化された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手順を説明します。
- カスタム構成を維持しながら Kubernetes モニタリングをアップグレードするには、1 つのコマンドで簡単にアップグレードできます。
- より安全: API キーは秘密を安全に管理します。
- CI/CD 自動化ツールとの統合と展開が簡単です。

ストレージ仮想化

Cloud Insights は、ローカル ストレージを持つストレージ アレイと他のストレージ アレイの仮想化を区別できます。これにより、インフラストラクチャのフロントエンドからバックエンドに至るまで、コストを関連付け、パフォーマンスを区別できるようになります。



新しいWebhookパラメータ

作成する際は"ウェブフック"通知では、Webhook 定義に次のパラメータを含めることができるようになりました。

- %%TriggeredOnKeys%%
- %%トリガーオン値%%

Kubernetesデータのレポート

Cloud Insightsによって収集された Kubernetes データ (永続ボリューム (PV)、PVC、ワークロード、クラスター、名前空間など) がレポートで使用できるようになり、Kubernetes のメトリックに関するチャージバック、傾向分析、予測、TTF 計算、その他のビジネス レポートが可能になります。

新規顧客向けにデフォルトのONTAPシステム モニターを有効化

新しいCloud Insights環境では、多くのONTAPシステム モニターがデフォルトで有効化（つまり、再開）されています。以前は、ほとんどのモニターはデフォルトで 一時停止 状態になっていました。ビジネスニーズは企業によって異なるため、"システムモニター"環境内でアラートを設定し、アラートのニーズ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

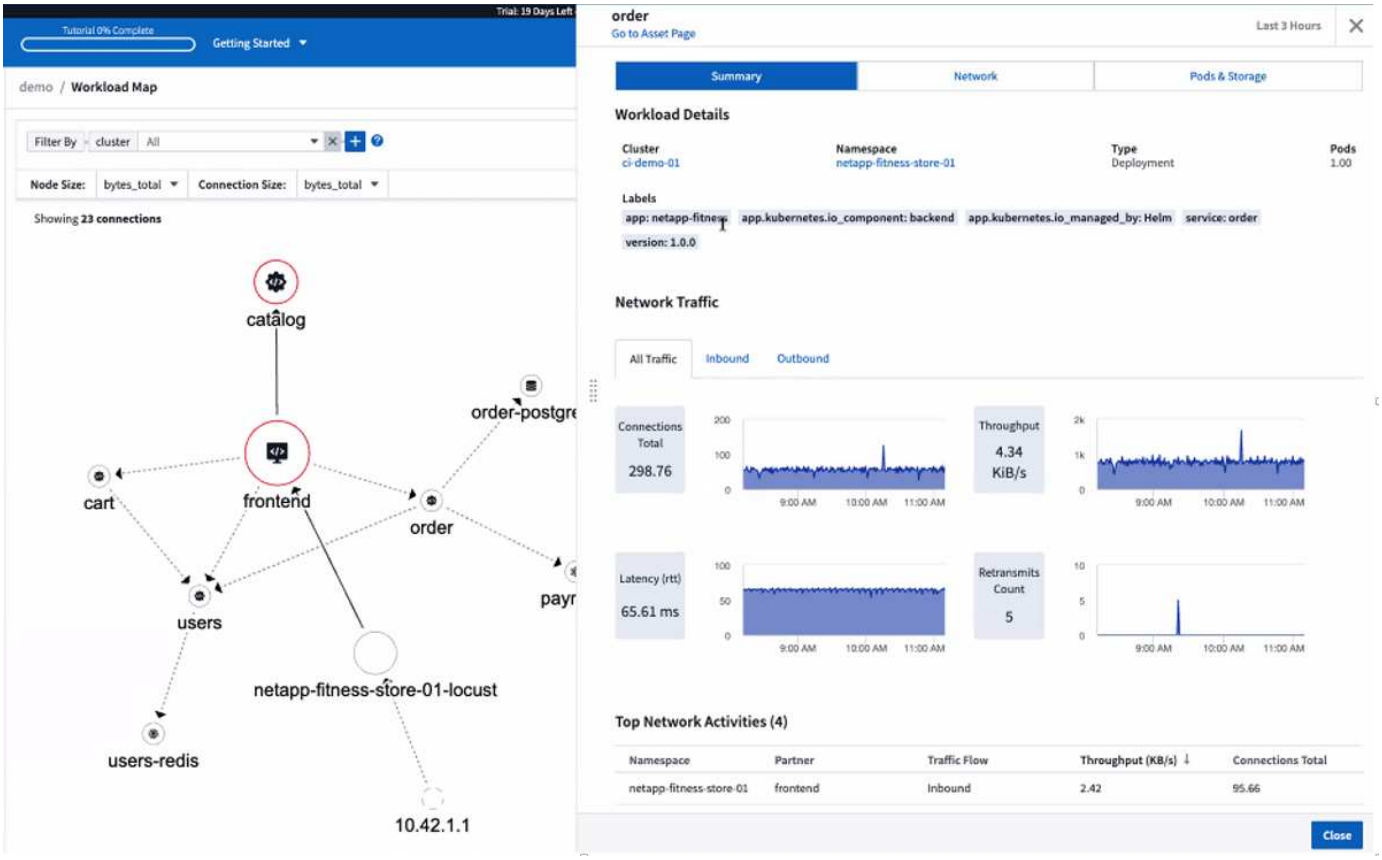
Kubernetes パフォーマンス監視とマップ

その"*Kubernetes ネットワークパフォーマンスとマップ*"この機能により、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が簡素化されます。 Kubernetes ネットワーク パフォーマンスの遅延と異常をリアルタイムで可視化し、パフォーマンスの問題がユーザーに影響を与える前に特定します。この機能により、組織は Kubernetes トラフィック フローを分析および監査して全体的なコストを削減できます。

主な機能: • 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強調表示します。 • 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。 • イングレス、エグレス、クロス

リージョン、クロスゾーンのネットワーク 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。

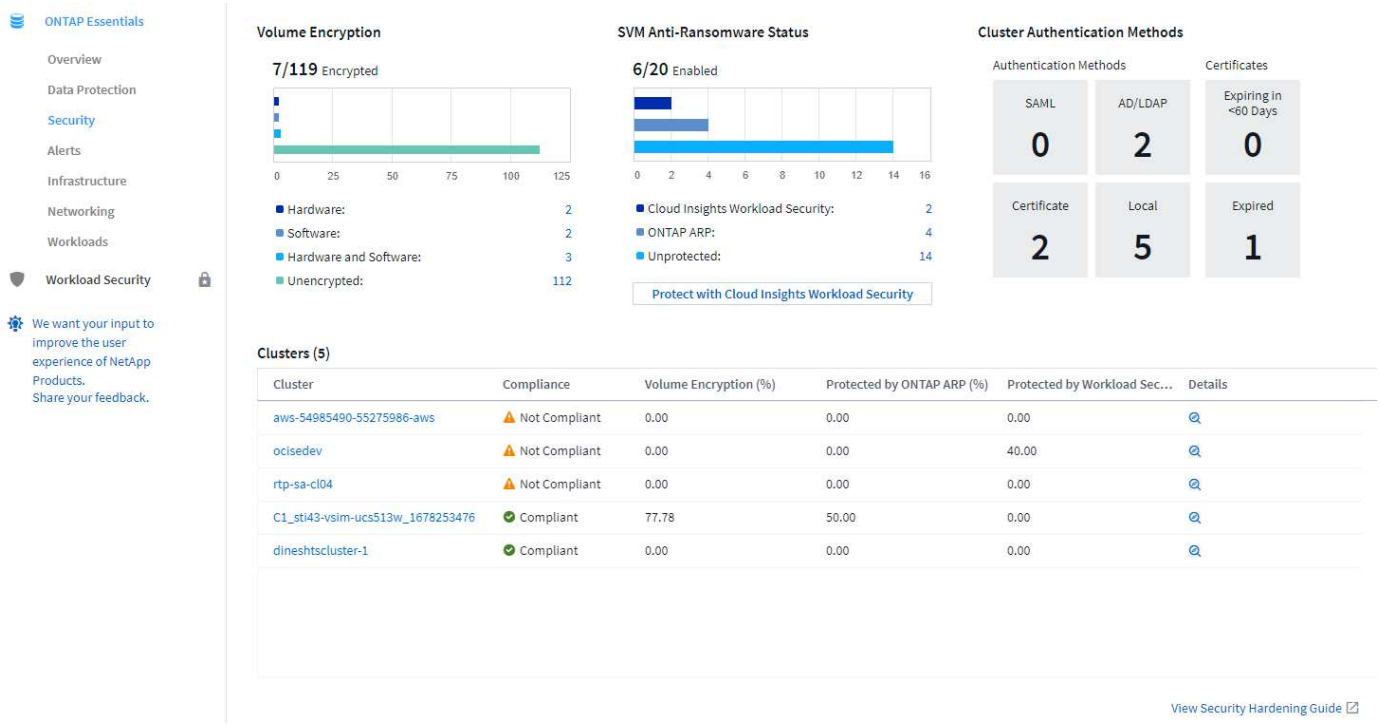
「スライドアウト」の詳細を表示するワークロード マップ:



Kubernetesパフォーマンスモニタリングとマップは、"プレビュー"特徴。

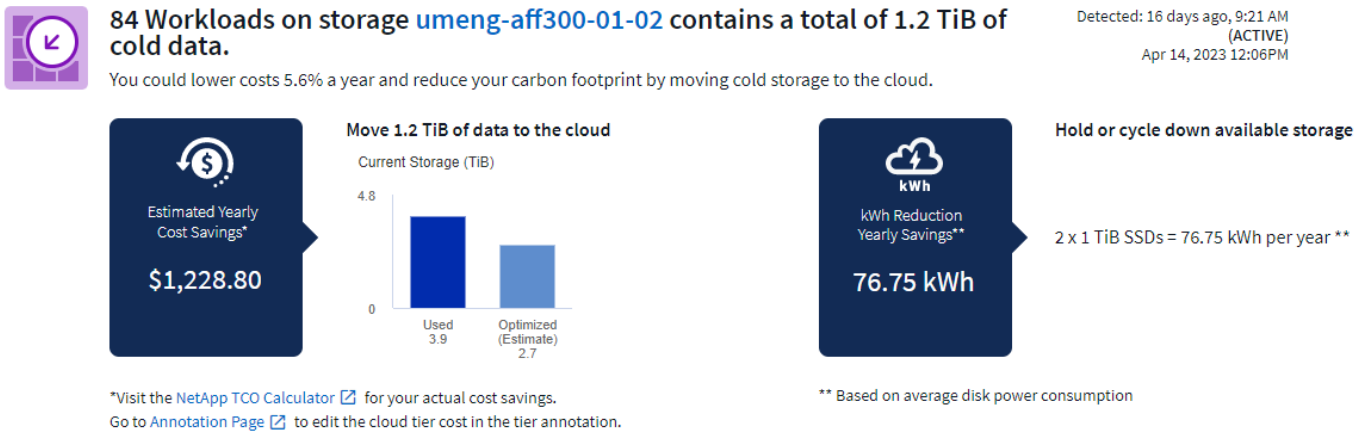
ONTAP Essentials セキュリティダッシュボード

その"セキュリティダッシュボード"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、クラスター認証方法のグラフを表示し、現在のセキュリティ状況を即座に確認できます。セキュリティダッシュボードは、"プレビュー"特徴。



ONTAPコールド ストレージの再利用

Reclaim ONTAP Cold Storage Insight は、 ONTAPシステム上のボリュームのコールド容量、潜在的なコスト/電力節約、および推奨されるアクション項目に関するデータを提供します。



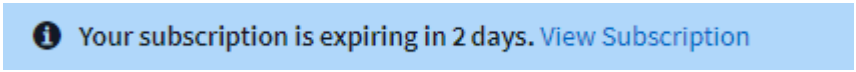
このインサイトを使用すると、次のような質問に答えることができます。

- ストレージ クラスター上のコールド データのうち、(a) 高価な SSD ディスク、(b) HDD ディスク、(c) 仮想ディスクに保存されているものは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、最も大きな影響を与え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状態であった期間 (日数) はどれくらいですか?

*Reclaim ONTAP Cold Storage_*は、"_プレビュー"機能であるため変更される可能性があります。

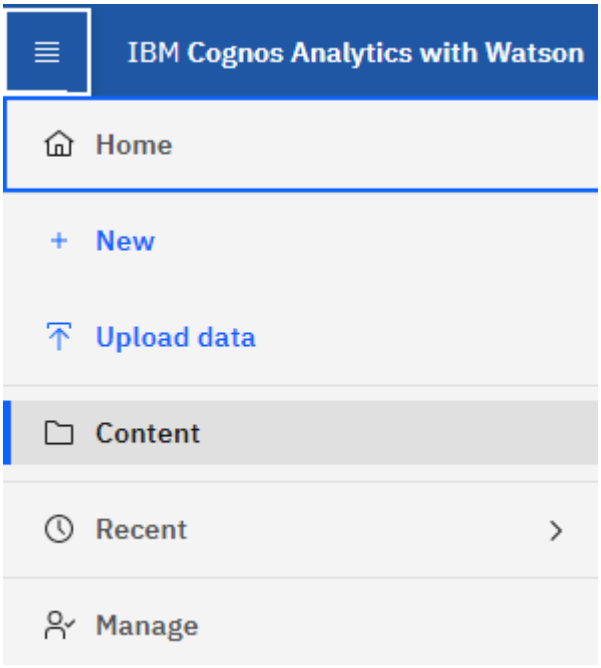
サブスクリプション通知はバナーメッセージも制御します

サブスクリプション通知の受信者の設定 (管理 > 通知) では、サブスクリプション関連の製品内バナー通知を誰が見るか制御できるようになりました。



レポートの見た目が新しくなりました

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に気付くでしょう。これらの画面とナビゲーションの変更は、現在更新されています。"報告文書" 。



デフォルトで一時停止するモニター

新しいCloud Insights環境では、次の点に注意してください。"システム定義モニター"デフォルトではアラート通知を送信しません。アラートを受け取りたいモニターに対して、通知を有効にするために、モニターに 1 つ以上の配信方法を追加する必要があります。既存のCloud Insights環境では、現在 一時停止 状態にあるシステム定義モニターのデフォルトの グローバル 通知受信者リストが削除されました。ユーザー定義の通知は変更されず、現在アクティブなシステム定義モニターの通知設定も変更されません。

API メータリング タブをお探しですか?

API メータリングは、サブスクリプション ページから 管理 > API アクセス ページに移動されました。

2023年3月

ONTAP 9.9以降のクラウド接続は廃止されました

ONTAP 9.9+ データ コレクターの Cloud Connection は廃止されます。 2023 年 4 月 4 日以降、環境内の Cloud Connection データ コレクターはデータを収集しなくなり、ポーリング時にエラーが表示されます。 Cloud Connection データ コレクターは、以降のアップデートでCloud Insightsから完全に削除されます。

2023 年 4 月 4 日より前に、現在 Cloud Connection によって収集されているすべてのONTAPシステムに対して、新しいNetApp ONTAP Data Management Software データ コレクターを構成することが必須です。

2023年1月

新しいログモニター

20個近く追加しました"追加のシステムモニター"相互接続リンクの破損、ハートビートの問題などを警告します。さらに、 SnapMirror自動再同期、 MetroClusterミラーリング、およびFabricPoolミラー再同期の変更について警告するための 3 つの新しいデータ保護ログ モニターが追加されました。

これらのモニターの一部はデフォルトで 有効 になっていることに注意してください。アラートを生成したくない場合は、それらを 一時停止 する必要があります。また、これらのモニターは通知を配信するように構成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 Webhook 経由でアラートを送信する場合は、これらのモニターで通知の受信者を構成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性を確保することは重要であるため、クエリするデータのタイプ (アセットまたは統合) に関係なく、すべてのメトリック クエリ、ダッシュボード テーブル ウィジェット、およびオブジェクト ランディング ページで .CSV エクスポートを利用できるようにしました。

列の選択、列名の変更、単位の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。

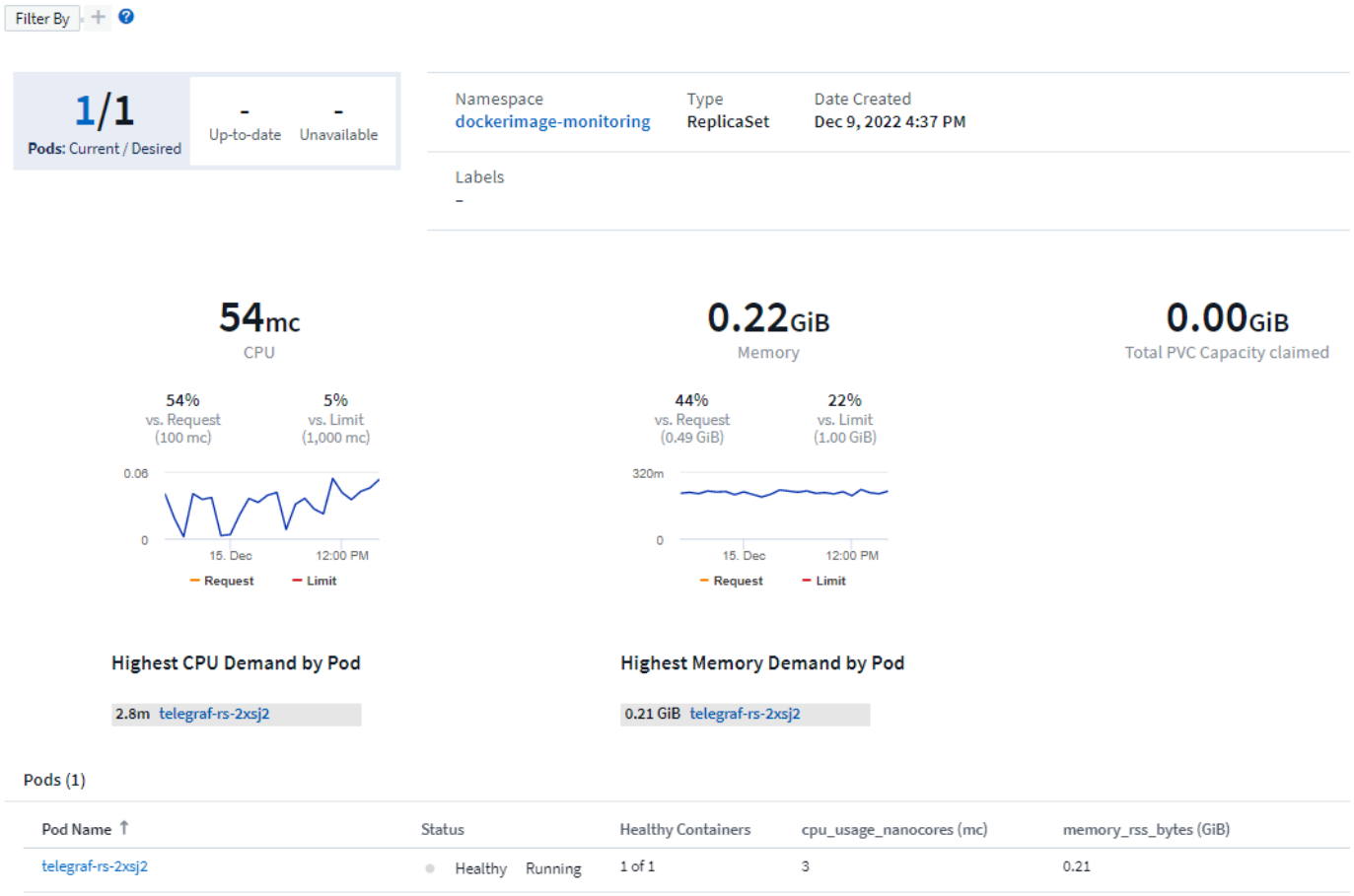
2022年12月

Cloud Insightsトライアルでランサムウェア保護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にサインアップすると、ランサムウェアの検出や自動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試すことができます。トライアルにまだ登録していない場合は、今すぐ登録してください。

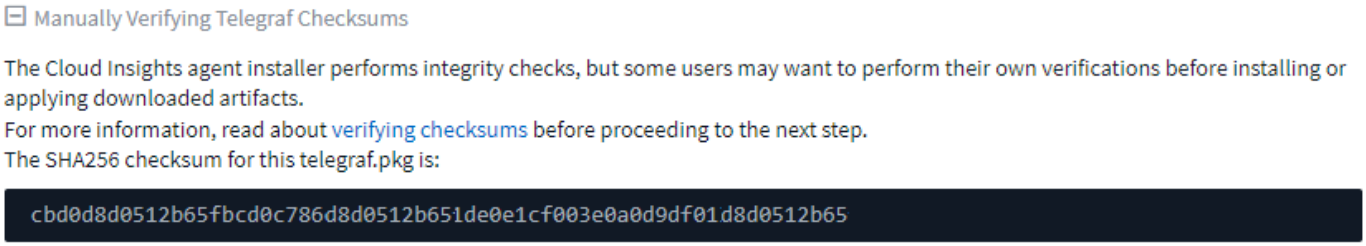
Kubernetesワークロードには独自のランディングページがあります

ワークロードは Kubernetes 環境の重要な部分であるため、 Cloud Insightsではそれらのワークロードのランディング ページが提供され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。



チェックサムを確認する

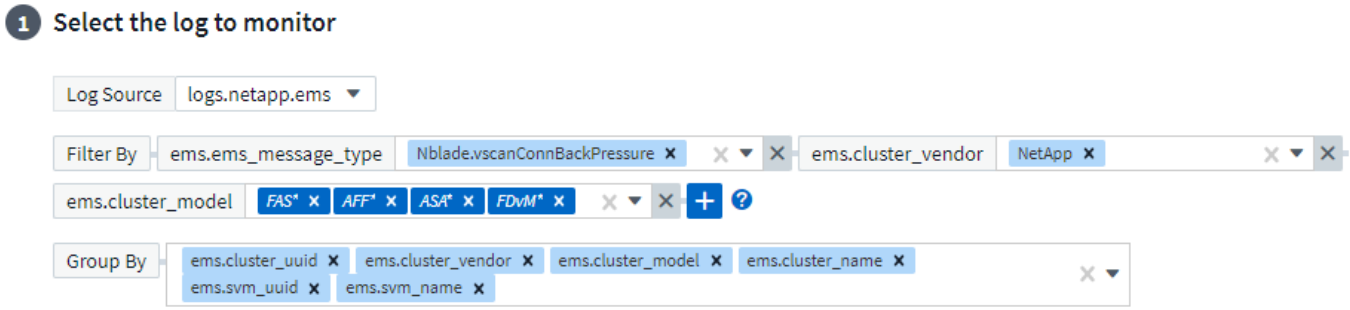
Windows および Linux 用エージェントのインストール中にチェックサム値を提供するようご要望がありましたが、これは素晴らしいアイデアだと思いました。それで、ここにあります:



ログアラートの改善

グループ化

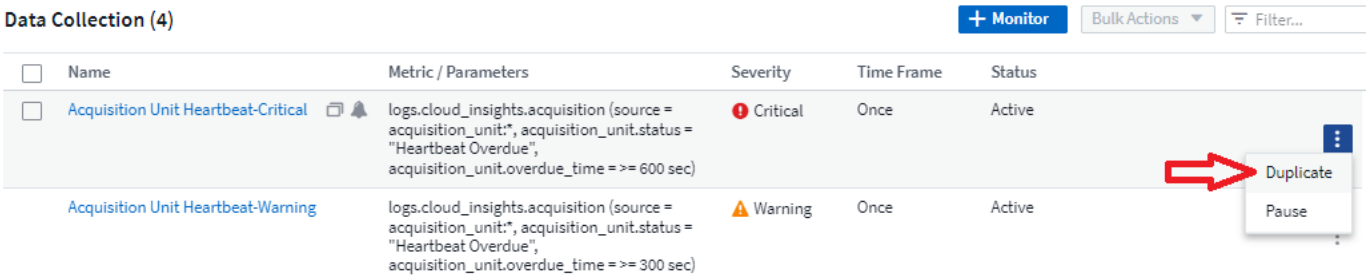
ログ モニターを作成または編集するときに、「グループ化」属性を設定して、より焦点を絞ったアラートを生成できるようになりました。モニター定義の「フィルター」設定の下にある「グループ化」属性を探します。



この変更により、モニター定義の「グループ化」の側面が正規化され、メトリック モニターとログ モニターの機能が同等になります。このパリティにより、顧客はシステム定義のデフォルト モニターをすべて複製/複製して、さらにカスタマイズできるようになります。

複製

変更ログ、Kubernetes ログ、およびデータ コレクター ログ モニターを複製 (クローン) できるようになりました。これにより、特定の定義に合わせて変更できる新しいカスタム ログ モニターが作成されます。



ビジネス継続性のための**SnapMirror**をカバーする**11**の新しいデフォルトの**ONTAP**モニター

12個近くの新しい"システムモニター"SnapMirror for Business Continuity (SMBC) の場合、SMBC 証明書とONTAP Mediator の変更について警告します。

2022年11月

40 を超える新しいセキュリティ、データ収集、CVO モニター!

Cloud Volumes、セキュリティ、データ保護に関する潜在的な問題を警告するために、数十の新しいシステム定義モニターを追加しました。これらのモニターについてもっと読む"ここをクリックしてください。"。

2022年10月

ONTAP Autonomous Ransomware Protection の統合により、より優れた正確なランサムウェア検出を実現

Cloud SecureはONTAPとの統合によりランサムウェア検出を向上"自律型ランサムウェア対策"（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に関するONTAP ARPイベントを受信し、

- ボリューム暗号化イベントとユーザーアクティビティを相関させて、誰が損害を引き起こしたかを特定します。
- 攻撃をブロックするための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、より迅速な復旧とデータ侵害調査の実施に役立ちます。

2022年9月

ベーシックエディションで利用可能なモニター

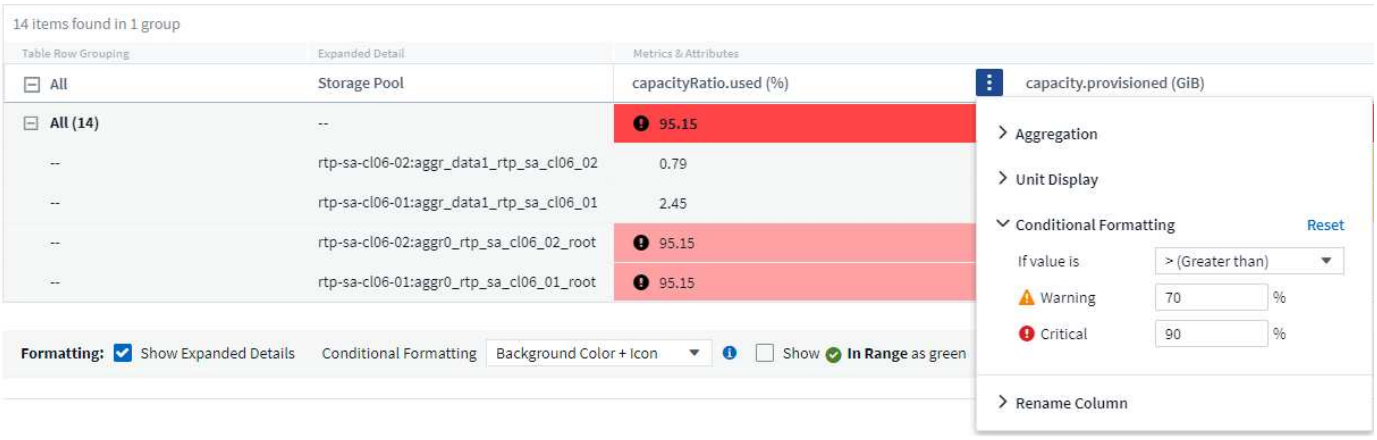
ONTAP"デフォルトのモニター"Cloud Insights Basic Edition で使用できるようになりました。これには、70 を超えるインフラストラクチャ モニターと 30 のワークロード例が含まれます。

ONTAP PowerとStorageGRIDダッシュボード

ダッシュボード ギャラリーには、 ONTAP電力と温度の新しいダッシュボードと、 StorageGRIDの 4 つのダッシュボードが含まれています。環境でONTAP電力メトリックやStorageGRIDデータを収集している場合は、+ギャラリーから 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。

表で一目でわかるしきい値の可視性

条件付き書式を使用すると、テーブル 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できるため、外れ値や例外的なデータ ポイントを即座に表示できます。



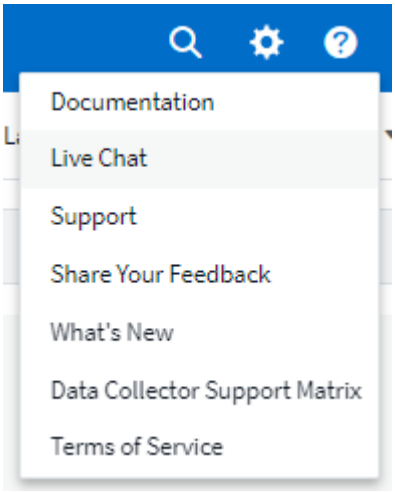
セキュリティモニター

Cloud Insights は、 ONTAPシステムで FIPS モードが無効になっていることを検出すると、警告を発すること

ができます。詳細はこちら"システムモニター"、また、近日中にさらに多くのセキュリティ モニターが登場する予定ですので、このページをご覧ください。

どこからでもチャット

新しい ヘルプ > ライブ チャット リンクを選択すると、任意のCloud Insights画面からNetAppサポート スペシャリストとチャットできます。ヘルプは画面右上の「？」アイコンからご利用いただけます。



より目に見えるインサイト

お使いの環境で"Insight"*Shared resources Under Stress* や *Kubernetes Namespaces Running Out of Space* など、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 Insight 自体へのリンクが含まれるようになり、より迅速な調査とトラブルシューティングが可能になります。

新しいデータ収集者

- Amazon S3 (プレビュー版で利用可能)
- BrocadeFOS 9.0.x
- Dell/EMC PowerStore 3.0.0.0

その他のデータコレクターの更新

すべてのデータ ソースは、取得ユニットの更新やパッチの適用後にパフォーマンス ポーリングを再開するように最適化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

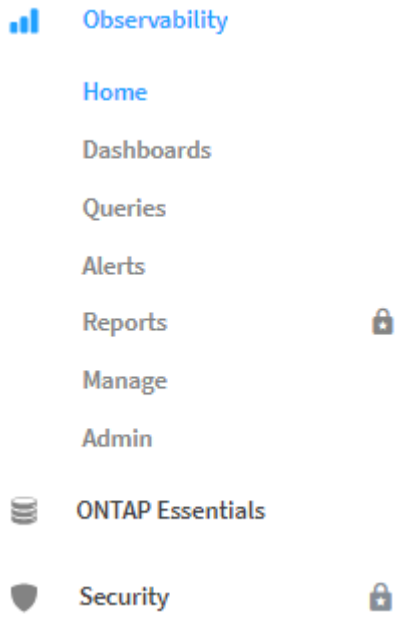
Cloud Insights Acquisition Unitsでは、以下のオペレーティングシステムがサポートされています。"すでにサポートされています" :

- Red Hat Enterprise Linux 8.5、8.6

2022年8月

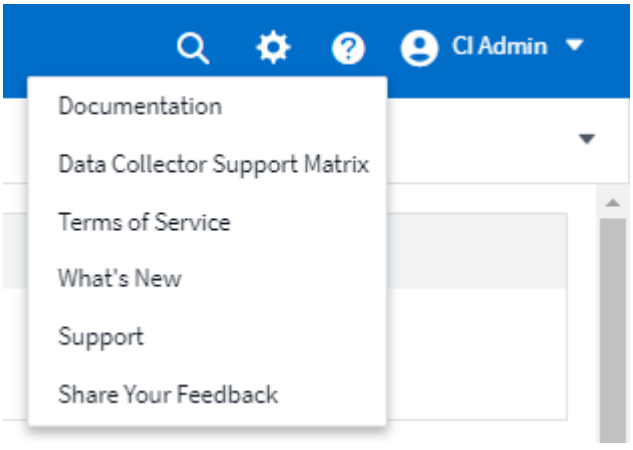
Cloud Insights の外観が新しくなりました。

今月より、「監視と最適化」は **Observability** に名前が変更されました。ダッシュボード、クエリ、アラート、レポートなどのお気に入りの機能はすべてここにあります。さらに、新しい セキュリティ メニューの下にあるCloud Secureを探してください。メニューのみが変更され、機能は同じままであることに注意してください。



ヘルプ メニューをお探しですか?

ヘルプは画面の右上に表示されるようになりました。

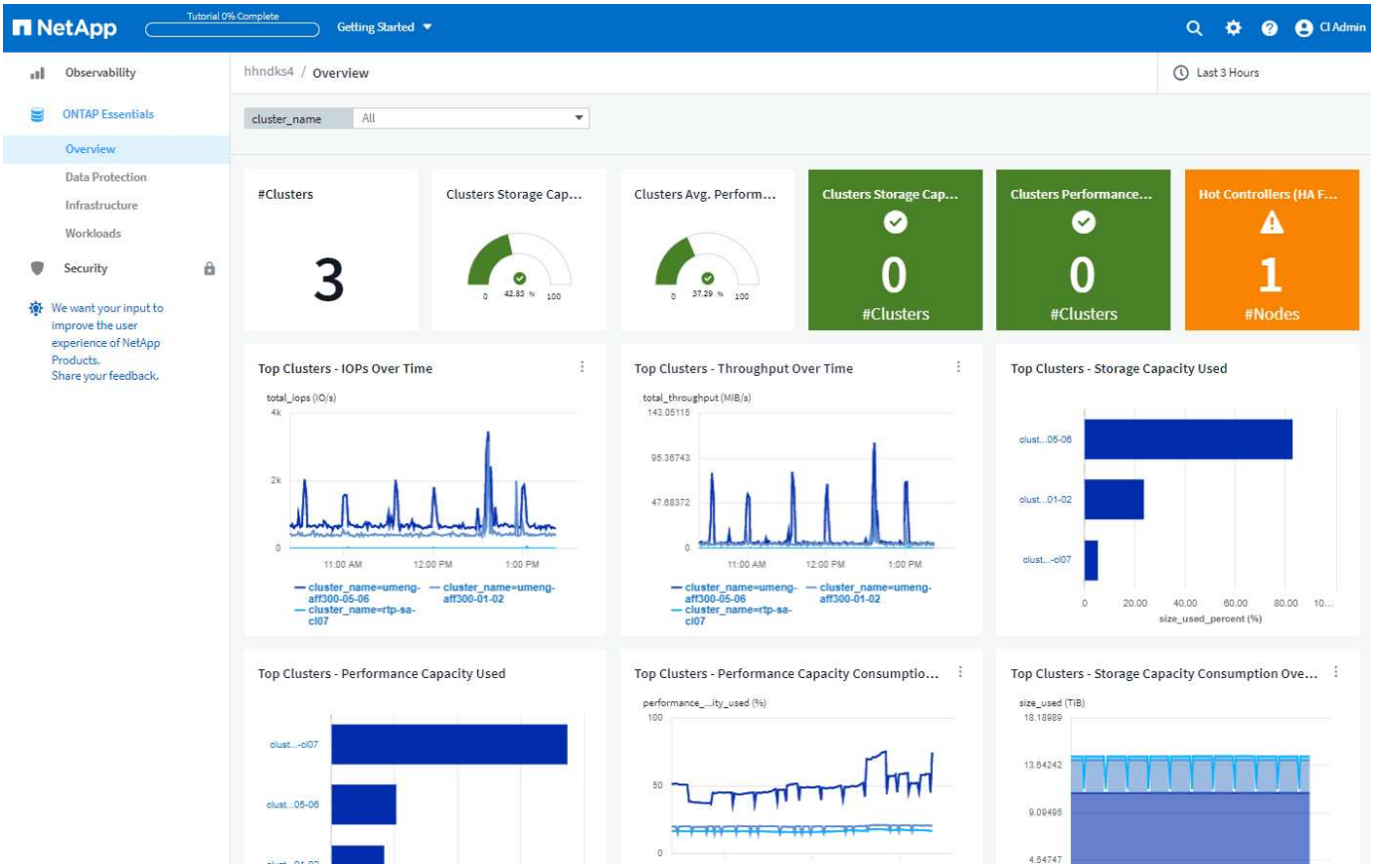


処理を開始するには、**ONTAP Essentials** をチェックしてください!

"* ONTAPエッセンシャル*"は、 NetApp ONTAPインベントリ、ワークロード、データ保護の詳細なビュー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。これには、ストレージ容量とパフォーマンスの完全使用までの日数予測も含まれます。高い使用率で実行されているコントローラーがあるかどうかを確認すること

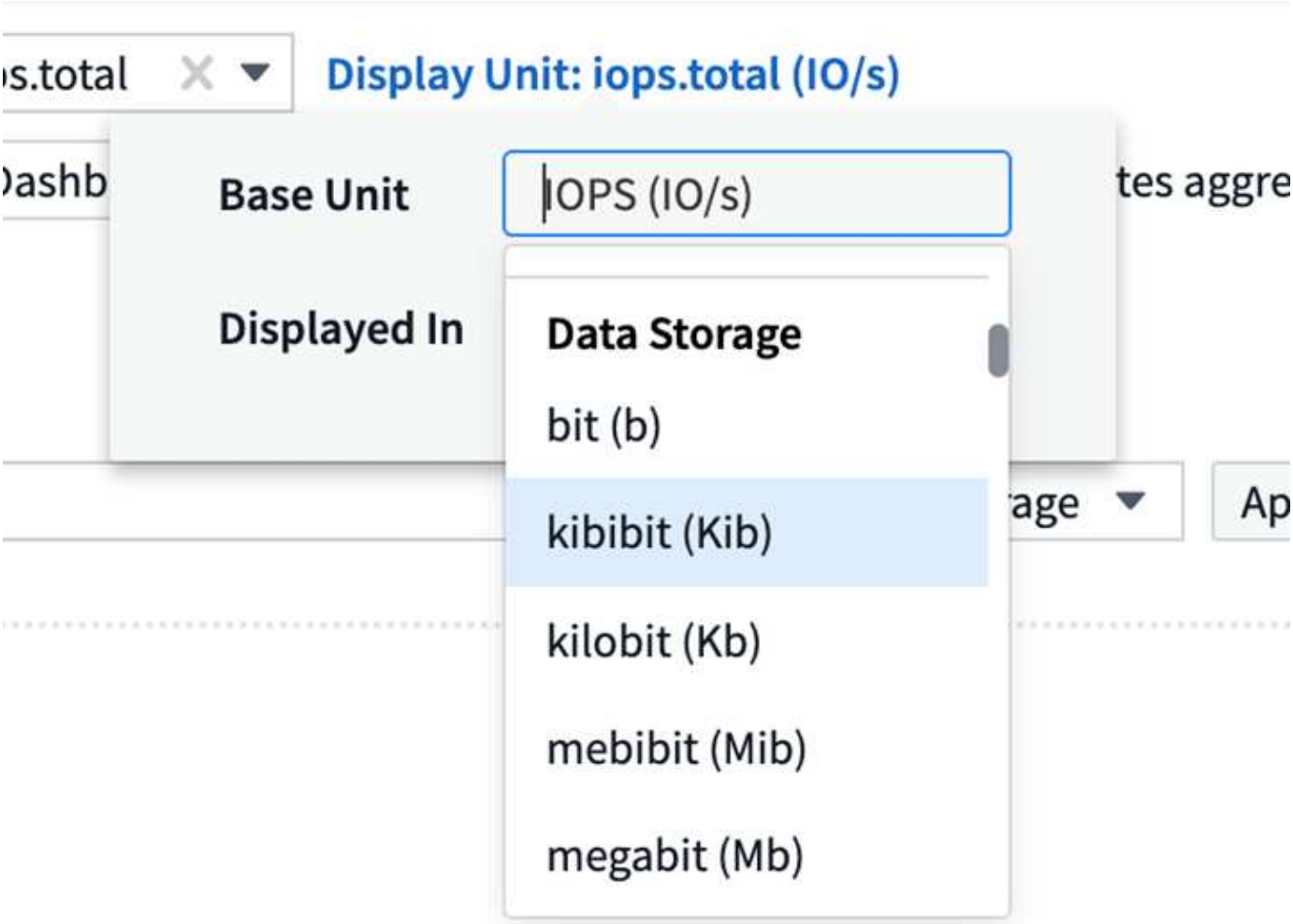
もできます。 ONTAP Essentials は、 NetApp ONTAP の監視のあらゆるニーズに最適な場所です。

すべてのエディションで利用可能なONTAP Essentials は、既存のONTAPオペレータと管理者にとって直感的に使用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。



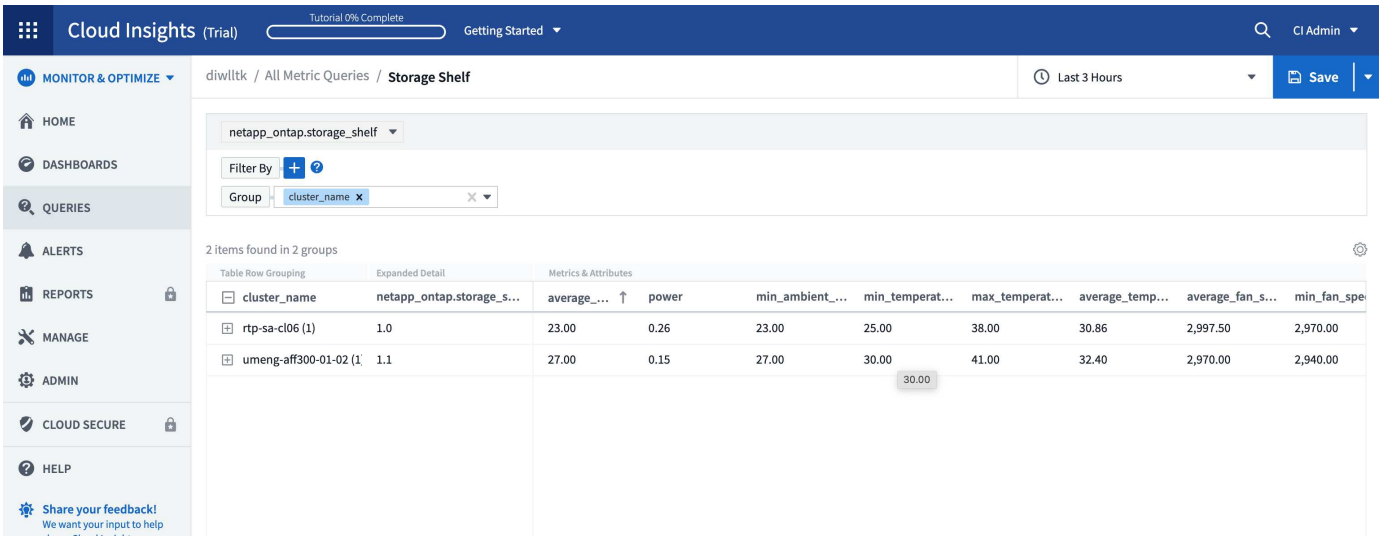
ストレージデータファミリーが統合される

あなたがそれを要求し、今それを手に入れました。ストレージの 2 進数と 10 進数のデータ単位が、ビットやバイトからテビビットやテラバイトまで 1 つのファミリに統合され、ダッシュボードにデータを好みの方法で表示しやすくなりました。データ レートも今では独自の 1 つの大きなファミリーになっています。



ストレージはどれくらいの電力を消費していますか?

netapp_ontap.storage_shelf、netapp_ontap.system_node、および netapp_ontap.cluster (電力消費のみ) メトリックを使用して、 ONTAPストレージ シェルフとノードの電力消費、温度、およびファン速度を表示および監視します。



プレビューから卒業した機能

以下の機能はプレビューから移行され、すべてのお客様が利用できるようになりました。

特徴	説明
Kubernetes 名前空間のスペース不足	*Kubernetes* 名前空間のスペース不足 インサイトでは、スペース不足になるリスクがある Kubernetes 名前空間のワークロードが表示され、各スペースがいっぱいになるまでの残り日数の見積もりも表示されます。"続きを読む"
ストレス下の共有リソース	*Shared Resource Under Stress* の分析情報は、AI/ML を使用して、環境内でリソースの競合がパフォーマンスの低下を引き起こしている場所を自動的に特定し、影響を受けるワークロードを強調表示して、修復するための推奨アクションを提供することで、パフォーマンスの問題をより迅速に解決できるようにします。"続きを読む"
Cloud Secure– 攻撃時にユーザーアクセスをブロック	攻撃が検出されるとユーザー アクセスをブロックする機能により、ビジネスに不可欠なデータをより強力に保護します。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ーの詳細ページから手動でブロックすることもできます。"続きを読む"

データ収集の健全性はどうですか?

Cloud Insightsには、Acquisition Unit 用の 2 つの新しいハートビート モニターと、データ コレクターの障害を警告する 2 つのモニターが用意されています。これらを使用すると、データ収集に関する問題を迅速に警告することができます。

Data Collection モニター グループでは、次のモニターが利用できるようになりました。

- 取得ユニットハートビートクリティカル
- 取得ユニットハートビート警告

- コレクターが失敗しました
- コレクターの警告

これらのモニターは、デフォルトでは 一時停止 状態になっていることに注意してください。これらを有効にすると、データ収集の問題について警告が表示されます。

自動更新APIトークン

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、期限切れのトークンに対して新しい/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。期限切れの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、シームレスに動作し続けることができます。トークンを作成するときに、「トークンを自動的に更新する」ボックスをチェックするだけです。この機能は現在、最新のNetApp Kubernetes Monitoring Operator を搭載した Kubernetes プラットフォーム上で実行されているCloud Insightsエージェントでサポートされています。

ベーシックエディションでは、これまで以上の機能が提供されます

試用期間が終了していますが、サブスクリプションが適切かどうかまだわかりませんか? Basic Edition では、現在のONTAPデータ コレクターでCloud Insightsを引き続き使用できるようになっていますが、VMWare バージョン、トポロジ、IOPS/スループット/レイテンシ データも引き続きキャプチャできるようになりました。ストレージ システムのプレミアム サポートを受けているNetApp のお客様は、 Cloud Insightsのサポートも受けられます。

さらに詳しく知りたいですか?

NetApp University Cloud Insightsコースへのリンクについては、[ヘルプ] > [サポート] ページの ラーニング センター セクションをご覧ください。

オペレーティングシステムのサポート

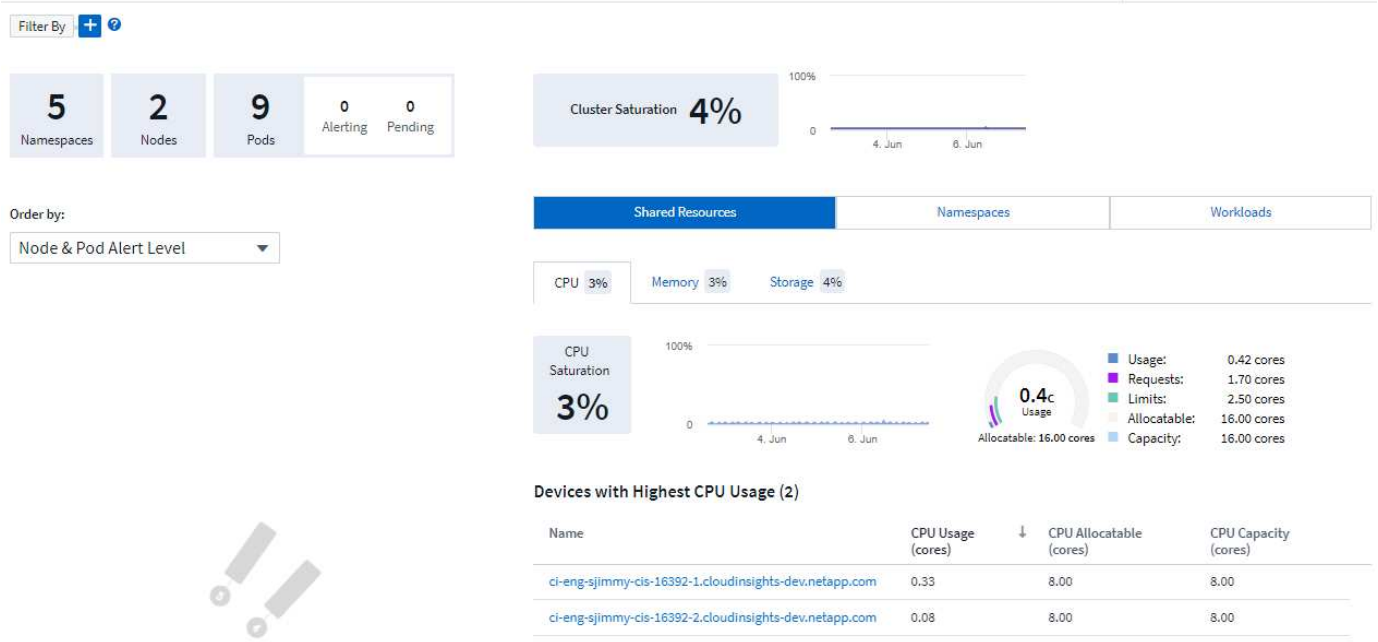
Cloud Insights Acquisition Unitsでは、以下のオペレーティングシステムがサポートされています。"すでにサポートされています" :

- Windows Server 11

2022年6月

Kubernetes クラスターの飽和状態とその他の詳細

Cloud Insights、飽和度の詳細と、名前空間とワークロードのより明確なビューを提供する改善されたクラスター詳細ページにより、Kubernetes 環境の探索がこれまで以上に簡単になります。

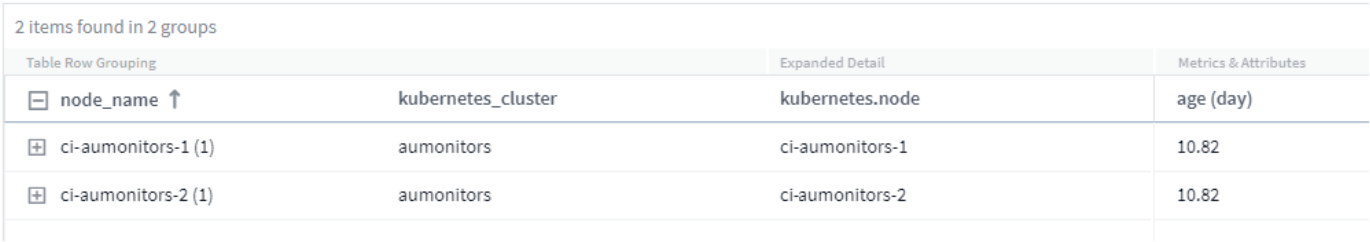


クラスター リスト ページでは、ノード、ポッド、名前空間、ワークロードの数に加えて、飽和状態も簡単に確認できます。



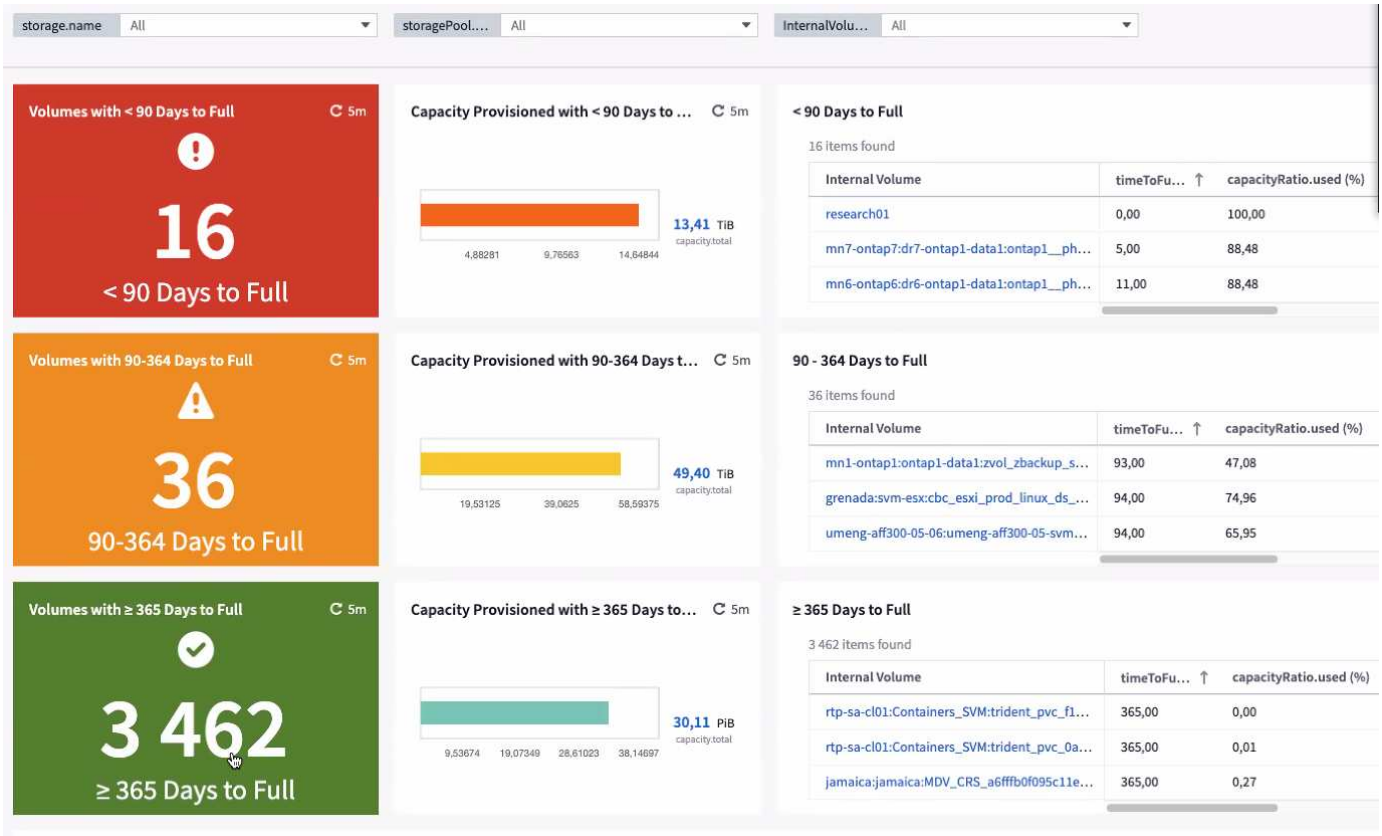
あなたの **Kubernetes** クラスターは何年経っていますか**?**

あなたのクラスターは世界に登場したばかりですか、それとも長いデジタルライフを経験してきましたか? Kubernetes ノードで収集される時間メトリックとして *Age* が追加されました。



容量満杯までの時間予測

Cloud Insights は、監視対象の内部ボリュームごとに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。これらの値は、停止のリスクを大幅に軽減するのに役立ちます。

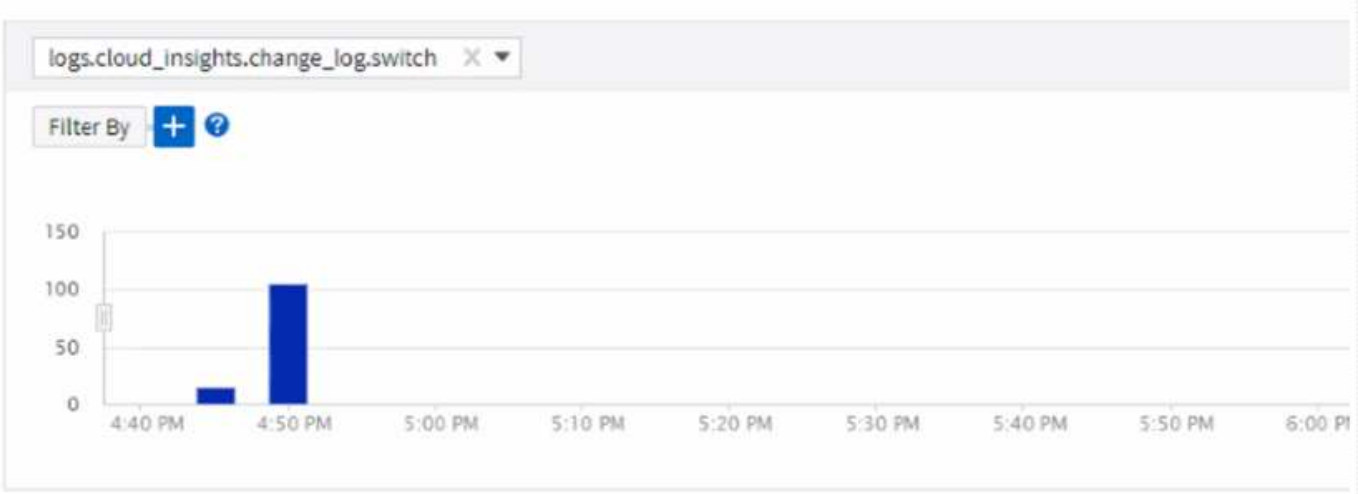


TTF カウンターは、ストレージ、ストレージ プール、ボリュームでも使用できます。これらのオブジェクトの追加ダッシュボードについては、このページを引き続きご覧ください。

なお、Time-to-Full 予測はプレビュー段階から移行し、すべての顧客に展開される予定です。

私の環境で何が変わったのでしょうか?

ONTAP変更ログ エントリは、ログ エクスプローラーで表示できます。



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 Unitsでは、以下のオペレーティングシステムがサポートされています。"すでにサポートされています" :

- CentOS ストリーム 9
- Windows Server 2022

更新された**Telegraf**エージェント

Telegraf 統合データを取り込むエージェントがバージョン **1.22.3** に更新され、パフォーマンスとセキュリティが向上しました。アップデートを希望するユーザーは、"エージェントのインストール"ドキュメント。エージェントの以前のバージョンは、ユーザーの操作を必要とせずに引き続き機能します。

プレビュー機能

Cloud Insights、数多くの新しい魅力的なプレビュー機能を定期的に紹介しています。これらの機能の1つ以上をプレビューすることにご興味がある場合は、"NetAppセールスチーム"詳細についてはこちらをご覧ください。

特徴	説明

Kubernetes 名前空間のスペース不足	*Kubernetes* 名前空間のスペース不足 インサイトでは、スペース不足になるリスクがある Kubernetes 名前空間のワークロードが表示され、各スペースがいっぱいになるまでの残り日数の見積もりも表示されます。"続きを読む"
Cloud Secure– 攻撃時にユーザーアクセスをブロック	攻撃が検出されるとユーザー アクセスをブロックする機能により、ビジネスに不可欠なデータをより強力に保護します。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ーの詳細ページから手動でブロックすることもできます。"続きを読む"
ストレス下の共有リソース	*Shared Resource Under Stress* の分析情報は、AI/ML を使用して、環境内でリソースの競合がパフォーマンスの低下を引き起こしている場所を自動的に特定し、影響を受けるワークロードを強調表示して、修復するための推奨アクションを提供することで、パフォーマンスの問題をより迅速に解決できるようにします。"続きを読む"

2022年5月

NetAppサポートとライブチャット

NetAppサポート担当者とライブチャットできるようになりました。 「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「チャット」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、Standard Edition および Premium Edition ユーザー向けに米国の平日にご利用いただけます。



Kubernetesオペレーター

Cloud Insightsの高度な Kubernetes モニタリングとクラスター エクスプローラーを使用すると、簡単に起動して実行できるようになります。

その"Kubernetes モニタリング オペレーター"(NKMO) は、 Cloud Insights Insights に Kubernetes をインストールするための推奨される方法です。これにより、より少ない手順でより柔軟に監視を構成できるようになり、K8s クラスターで実行されている他のソフトウェアを監視する機会も広がります。

詳細情報と前提条件については、上記のリンクをクリックしてください。

APIを使用してユーザーと招待を管理する

Cloud Insightsの強力な API を使用して、ユーザーと招待を管理できるようになりました。詳しくは"API Swaggerドキュメント"。

データ収集アラート

コレクターの失敗により重要なメトリックを見逃さないでください。

新しい機能により、データ収集者の追跡がこれまで以上に簡単になりました。"アラート"データコレクターおよび取得ユニットの障害の場合。これらのモニターはデフォルトでは一時停止されていることに注意してください。有効にするには、モニターページに移動し、「取得ユニットのシャットダウン」と「コレクターの失敗」を見つけて再開します。

ONTAPストレージの変更に関するアラート

予期しないストレージの変更によって停止が発生しないようにしてください。

ONTAPシステムで FlexVol、ノード、SVM の変更または削除が検出されたときにアラートを出すようにCloud Insightsを設定できるようになりました。

プレビュー機能

Cloud Insights、数多くの新しい魅力的なプレビュー機能を定期的に紹介しています。これらの機能の1つ以上をプレビューすることにご興味がある場合は、"NetAppセールスチーム"詳細についてはこちらをご覧ください。

特徴	説明
Kubernetes 名前空間のスペース不足	*Kubernetes* 名前空間のスペース不足 インサイトでは、スペース不足になるリスクがある Kubernetes 名前空間のワークロードが表示され、各スペースがいっぱいになるまでの残り日数の見積もりも表示されます。"続きを読む"
内部ボリュームとボリューム容量の満杯までの時間の予測	Cloud Insights は、監視対象の内部ボリュームとボリュームごとに、容量が不足するまでの日数を予測できます。この値は、停止のリスクを大幅に軽減するのに役立ちます。
Cloud Secure– 攻撃時にユーザーアクセスをブロック	攻撃が検出されるとユーザー アクセスをブロックする機能により、ビジネスに不可欠なデータをより強力に保護します。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ーの詳細ページから手動でブロックすることもできます。"続きを読む"
ストレス下の共有リソース	*Shared Resource Under Stress* の分析情報は、AI/ML を使用して、環境内でリソースの競合がパフォーマンスの低下を引き起こしている場所を自動的に特定し、影響を受けるワークロードを強調表示して、修復するための推奨アクションを提供することで、パフォーマンスの問題をより迅速に解決できるようにします。"続きを読む"

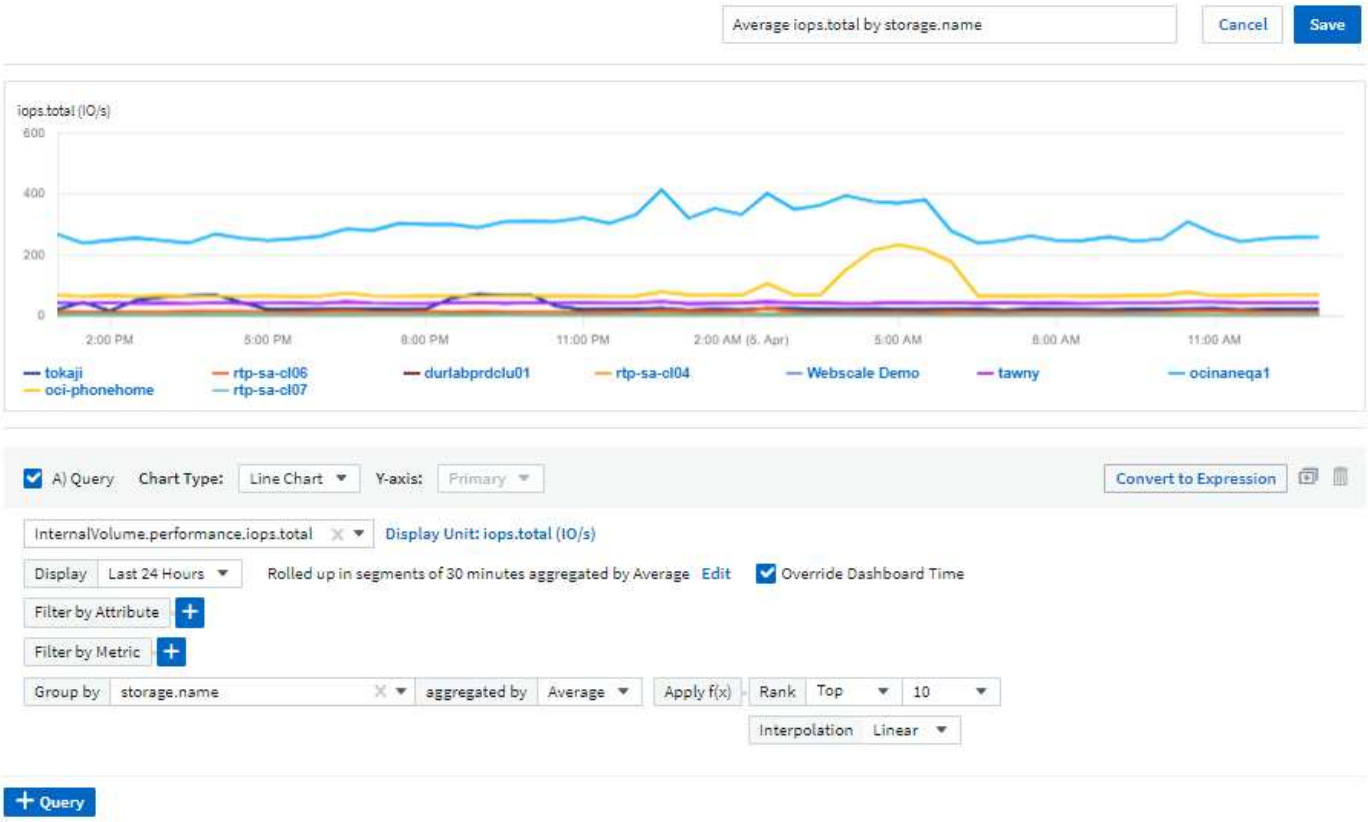
2022年4月

フィードバックを共有してください!

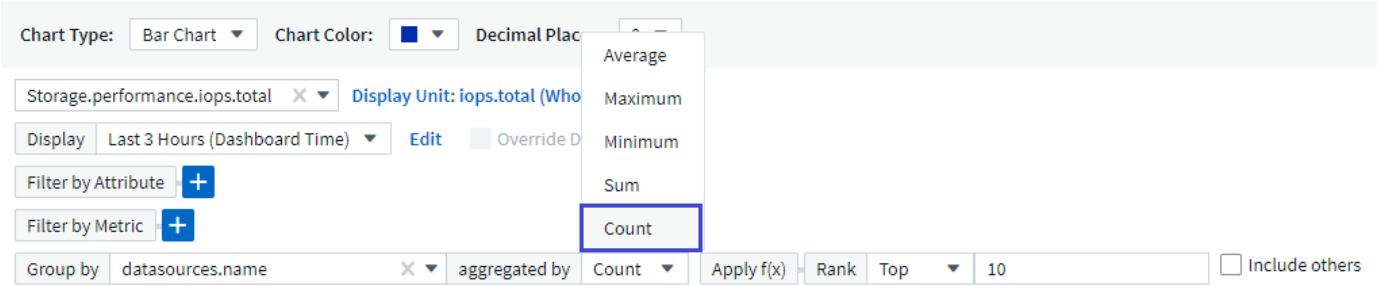
皆様のご意見をCloud Insightsの形成に役立てていただきたいと考えています。 NetApp の **Insights to Action** プログラムに参加してポイントと賞品を獲得しましょう。"今すぐ登録"！

ダッシュボードエディターの更新

ダッシュボード作成ツールを全面的に改良し、データをさらに素早く簡単に視覚化できるようになりました。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 ギャラリーからダッシュボードを追加したり、独自の新しいダッシュボードを作成して確認したりすることができます。



新しい Count 集計方法も導入されました。棒グラフ、縦棒グラフ、円グラフのウィジェットでデータをグループ化すると、選択したメトリックに関連するオブジェクトの数をすばやく簡単に表示できます。



さらに、折れ線グラフでは3つのタイプから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 - 既存のポイント間のデータポイントを補間します
- 階段 - 前のデータポイントを補間データポイントとして使用します

Kubernetes インフラストラクチャの強化された監視

Cloud Insights は、ポッド、デーモンセット、レプリカセットが作成または削除されたときや、新しいデプロイメントが作成されたときにアラートを通知することで、Kubernetes 環境の変更を常に把握できるようにします。 Kubernetes モニターはデフォルトで 一時停止 状態になっているため、必要なモニターのみを有効にする必要があります。

プレビュー機能

Cloud Insights、数多くの新しい魅力的なプレビュー機能を定期的に紹介しています。これらの機能の1つ以上をプレビューすることにご興味がある場合は、"NetAppセールスチーム"詳細についてはこちらをご覧ください。

特徴	説明
内部ボリュームとボリューム容量の満杯までの時間の予測	Cloud Insights は、監視対象の内部ボリュームとボリュームごとに、容量が不足するまでの日数を予測できます。この値は、停止のリスクを大幅に軽減するのに役立ちます。
Cloud Secure– 攻撃時にユーザーアクセスをブロック	攻撃が検出されるとユーザー アクセスをブロックする機能により、ビジネスに不可欠なデータをより強力に保護します。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ーの詳細ページから手動でブロックすることもできます。"続きを読む"
ストレス下の共有リソース	ストレス下にある共有リソースの分析情報は、AI/ML を使用して、環境内でリソースの競合がパフォーマンスの低下を引き起こしている場所を自動的に特定し、影響を受けるワークロードを強調表示し、修復するための推奨アクションを提供することで、パフォーマンスの問題をより迅速に解決できるようにします。"続きを読む"

新しいデータ収集者

- **Cohesity SmartFiles** - この REST API ベースのコレクターは、Cohesity クラスターを取得し、「ビュー」(CI 内部ボリュームとして) やさまざまなノードを検出し、パフォーマンス メトリックを収集します。

その他のデータコレクターの更新

次のデータ コレクターでパフォーマンス 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
- ピュアフラッシュアレイ

これらのパフォーマンス強化は、すべてのNetAppデータ コレクター、VMware、 Ciscoですでに利用可能であり、今後数か月以内に他のすべてのデータ コレクターにも展開される予定です。

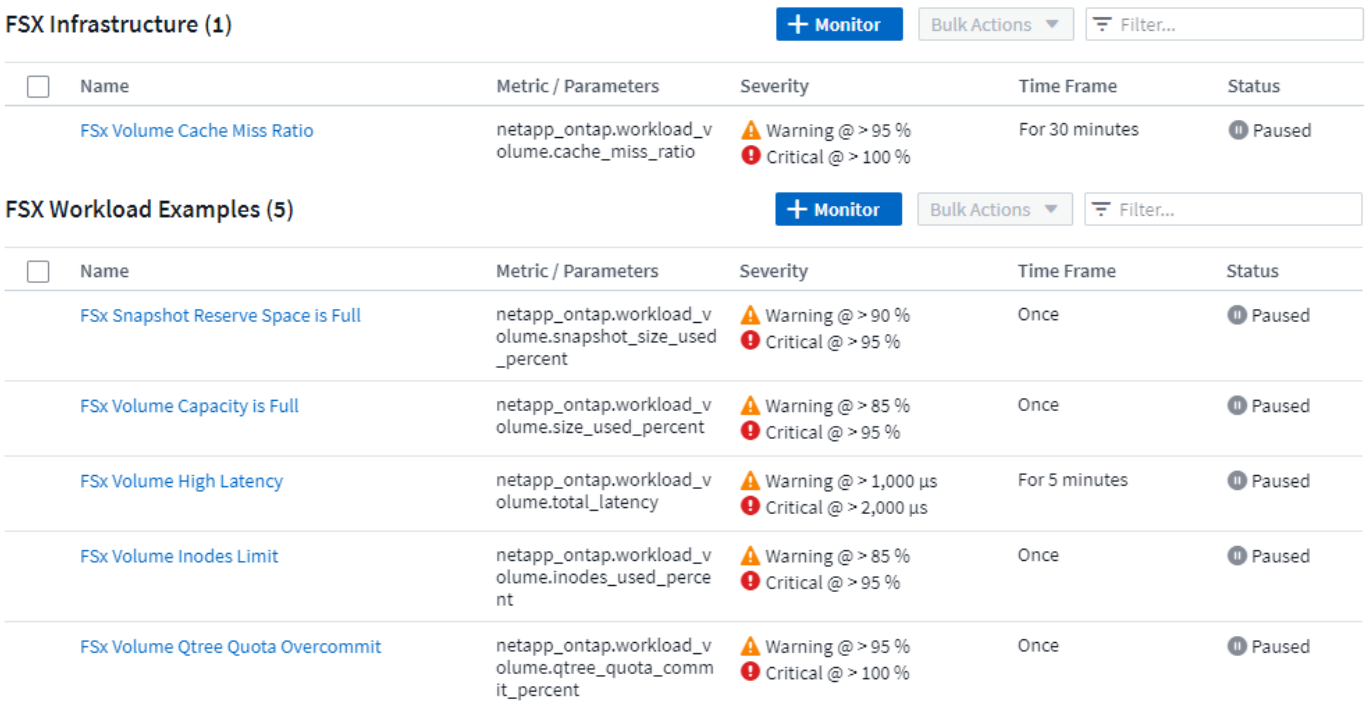
2022年3月

ONTAP 9.9以降のクラウド接続

その"ONTAP 9.9以降向けNetAppクラウド接続"データ コレクターを使用すると、外部の取得ユニットをインストールする必要がなくなり、トラブルシューティング、メンテナンス、初期導入が簡素化されます。

NetApp ONTAPモニター用の新しい FSx

FSx for NetApp ONTAP環境の監視は、新しい"システム定義モニター"インフラストラクチャ (メトリック) とワークロード (ログ) の両方に対して。



すべてのユーザーが利用できる新しいCloud Secure機能

現在一般提供されている以下のCloud Secure機能により、環境はこれまで以上に安全になります。

特徴	説明

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、悪意のあるユーザー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自動スナップショットを取得します。
警告とアラートの個別の通知	警告とアラートの通知を別々の受信者に送信できるため、適切なチームが常に情報を得ることができます。

更新されたTelegrafエージェント

Telegraf 統合データを取り込むエージェントがバージョン **1.21.2** に更新され、パフォーマンスとセキュリティが向上しました。アップデートを希望するユーザーは、"エージェントのインストール"ドキュメント。エージェントの以前のバージョンは、ユーザーの操作を必要とせずに引き続き機能します。

データコレクターの更新

- Broadcom ファイバー チャネル スイッチ データ コレクターは、各インベントリ ポーリングで発行される CLI コマンドの数を削減するように最適化されました。

2022年2月

Cloud Insights がApache Log4j の脆弱性に対処

顧客のセキュリティはNetAppにとって最優先事項です。 Cloud Insightsには、最近の Apache Log4j の脆弱性を解決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。

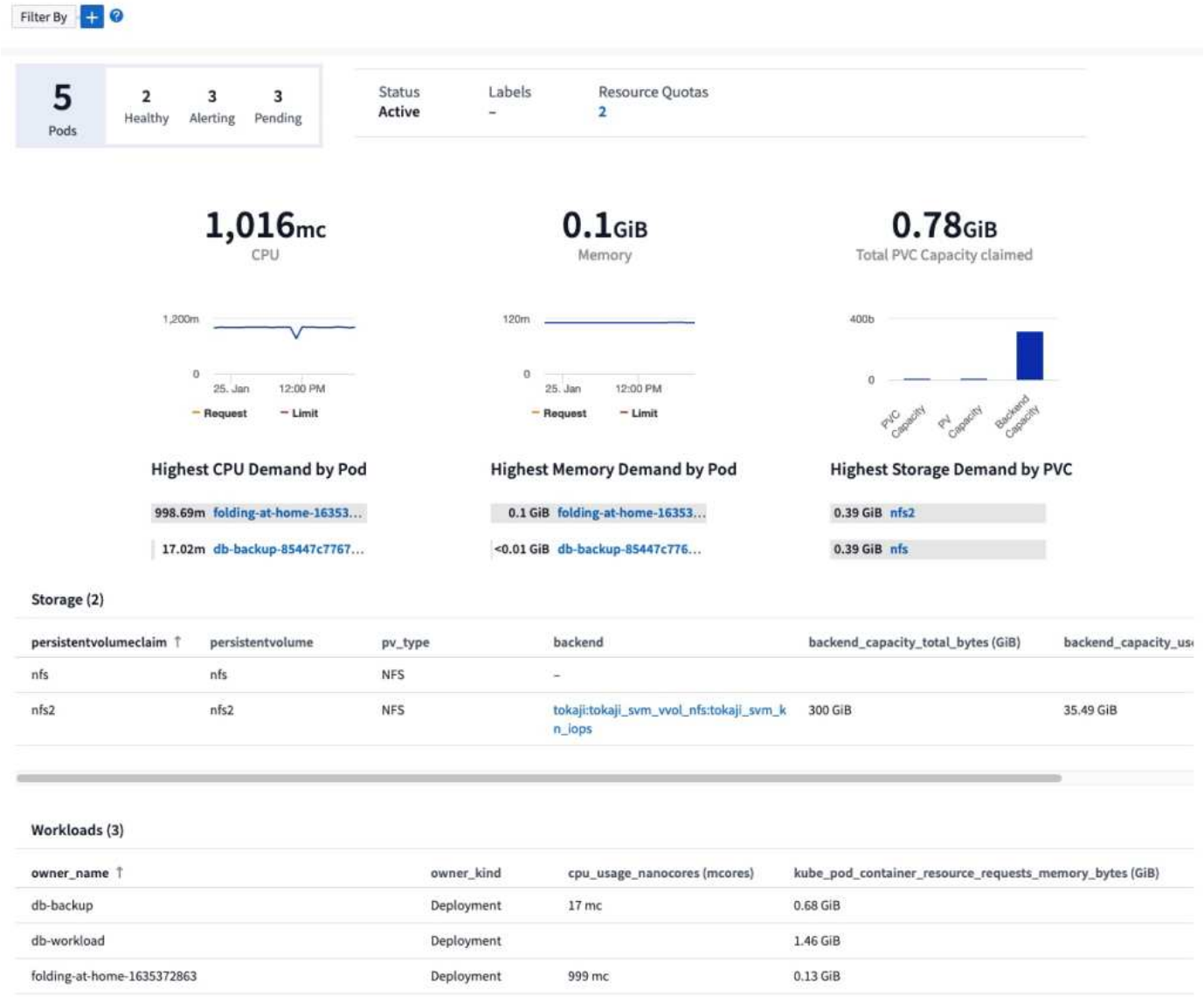
NetApp の製品セキュリティ アドバイザリ Web サイトで以下を参照してください。

"CVE-2021-44228" "CVE-2021-45046" "CVE-2021-45105"

これらの脆弱性とNetAppの対応の詳細については、"NetAppニュースルーム" 。

Kubernetes 名前空間の詳細ページ

クラスターの名前空間の詳細な情報ページが表示されるようになり、Kubernetes 環境の探索がこれまで以上に簡単になりました。名前空間の詳細ページには、すべてのバックエンド ストレージ リソースとその容量使用率など、名前空間で使用されるすべてのアセットの概要が表示されます。



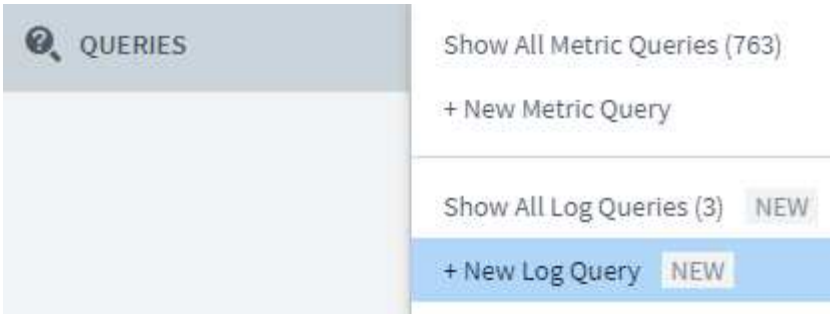
2021年12月

ONTAPシステムとのより緊密な統合

NetAppイベント管理システム (EMS) との新しい統合により、 ONTAPハードウェア障害などのアラートが簡素化されます。"探索と警告" Cloud Insightsの低レベルのONTAPメッセージに基づいて、トラブルシューティング 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。

ログのクエリ

ONTAPシステムの場合、 Cloud Insightsクエリには強力な"ログエクスプローラー"EMS ログ エントリを簡単に調査およびトラブルシューティングできます。



データコレクターレベルの通知。

アラート用のシステム定義およびカスタム作成されたモニターに加えて、 ONTAPデータ コレクターのアラート通知を設定することもできます。これにより、他のモニター アラートとは独立して、コレクター レベルのアラートの受信者を指定できます。

Cloud Secure の役割の柔軟性の向上

ユーザーは、以下の基準に基づいてCloud Secure機能へのアクセスを許可されます。"ロール"管理者によって設定:

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 コレクター、自動応答ポリシー、 Cloud Secureの 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 ロールでは、アラートのステータスを変更したり、メモを追加したり、スナップショットを手動で取得したり、ユーザー アクセスをブロックしたりできます。
ゲスト	アラートと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 ステータスを変更したり、メモを追加したり、スナップショットを手動で取得したり、ユーザー アクセスをブロックしたりすることはできません。

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、**CentOS 8 Stream** サポートに置き換えられます。 CentOS 8.x は 2021 年 12 月 31 日にサポートが終了します。

データコレクターの更新

ベンダーの変更を反映するために、いくつかのCloud Insightsデータ コレクター名が追加されました。

ベンダー/モデル	以前の名前
Dell EMC パワースケール	Isilon

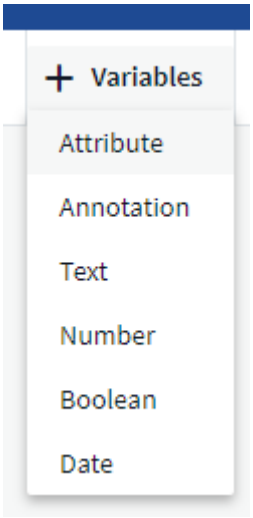
HPE アレトラ 9000 / プリメーラ	3PAR
HPE アレトラ 6000	機敏な

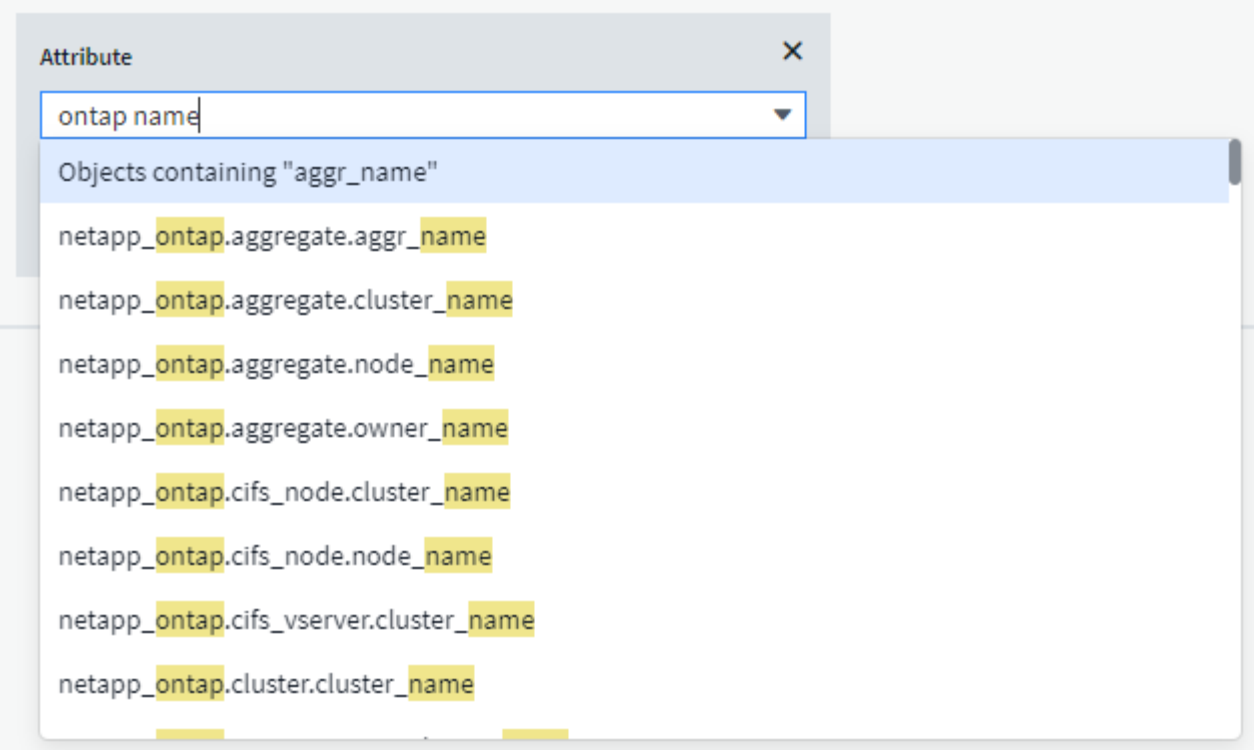
2021年11月

適応型ダッシュボード

属性用の新しい変数とウィジェットで変数を使用する機能。

ダッシュボードはこれまで以上に強力かつ柔軟になりました。属性変数を使用して適応型ダッシュボードを構築し、ダッシュボードを即座にフィルター処理します。これらと既存の"変数"環境全体のメトリックを表示し、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できる 1 つの高レベルダッシュボードを作成できるようになりました。ウィジェット内の数値変数を使用して、生のメトリックとコストを関連付けます (例: サービスとしてのストレージの 1 GB あたりのコスト)。



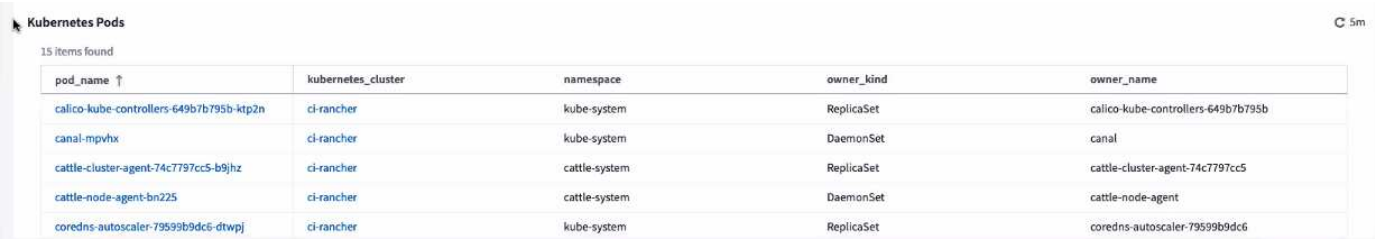


API経由でレポートデータベースにアクセスする

サードパーティのレポート、ITSM、自動化ツールとの統合のための強化された機能： Cloud Insightsの強力な"API"ユーザーは、Cognos レポート環境を経由せずに、 Cloud Insightsレポート データベースを直接クエリできます。

VM ランディング ページのポッド テーブル

VM とそれを使用する Kubernetes Pod 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のヘッドルーム管理を改善するために、関連付けられている Kubernetes Pod のテーブルが VM ランディング ページに表示されるようになりました。



データコレクターの更新

- ECSはストレージとノードのファームウェアを報告するようになりました
- Isilonは迅速な検出を改善しました
- 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 はシングル サインオン (SSO) をサポートす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追加のオペレーティングシステム

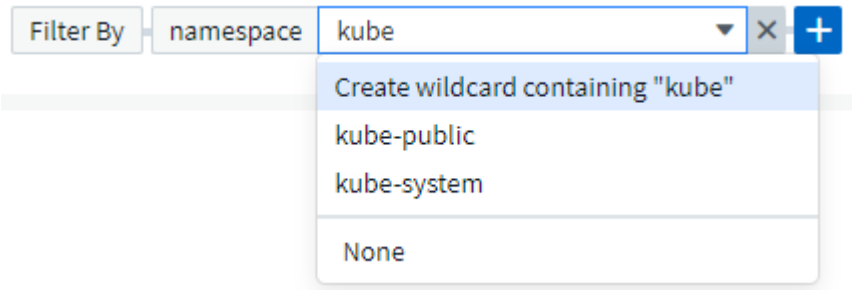
Cloud Insights Acquisition Unit は、既にサポートされているオペレーティング システムに加えて、次のオペレーティング システムもサポートしています。

- 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

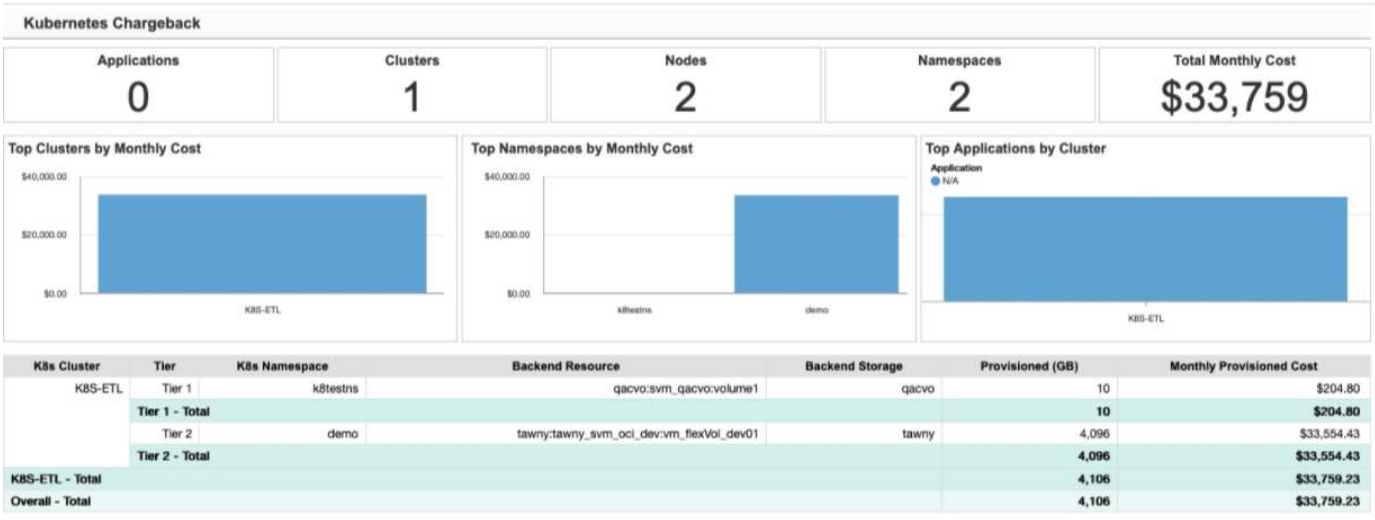
K8Sエクスプローラーページのフィルター

"Kubernetes エクスプローラー"ページ フィルターを使用すると、Kubernetes クラスター、ノード、ポッドの探索用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K8sデータ

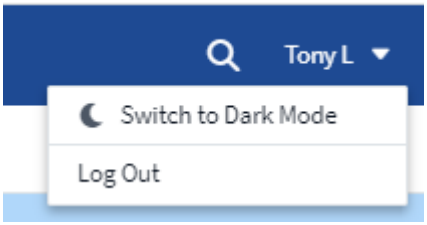
Kubernetes データがレポートで使用できるようになり、チャージバックやその他のレポートを作成できるようになりました。 Kubernetes チャージバック データをレポートに渡すには、Kubernetes クラスターとそのバックエンド ストレージへのアクティブな接続があり、 Cloud Insights がそこからデータを受信している必要があります。バックエンド ストレージからデータが受信されない場合、 Cloud Insights はKubernetes オブジェクト データを Reporting に送信できません。



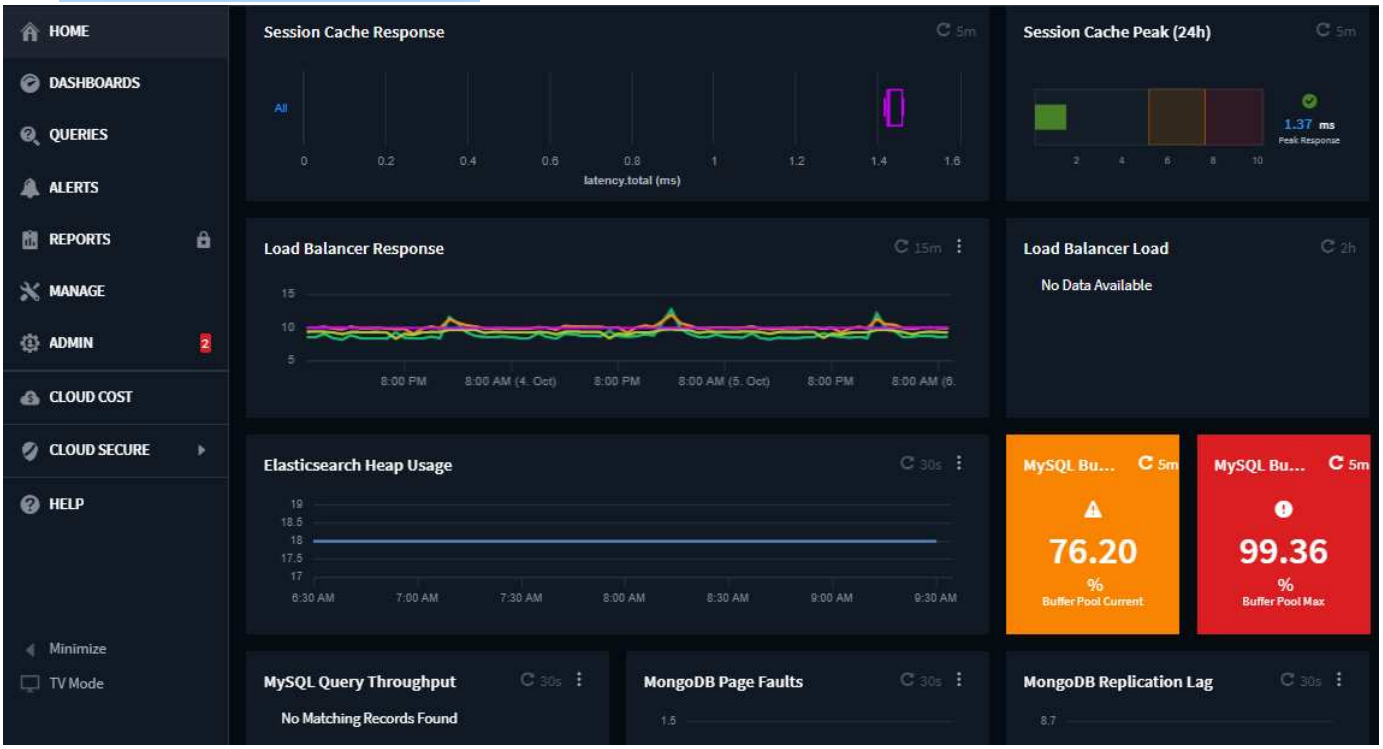
K8s Cluster	Tier	K8s Namespace	Backend Resource	Backend Storage	Provisioned (GB)	Monthly Provisioned Cost
K8S-ETL	Tier 1	k8testns	qacvo:svm_qacvo:volume1	qacvo	10	$204.80
	Tier 1 - Total				**10**	**$204.80**
	Tier 2	demo	tawny:tawny_svm_oci_dev:vm_flexVol_dev01	tawny	4,096	$33,554.43
	Tier 2 - Total				**4,096**	**$33,554.43**
K8S-ETL - Total					**4,106**	**$33,759.23**
Overall - Total					**4,106**	**$33,759.23**

ダークテーマが登場

多くの方からダーク テーマの要望がありましたが、 Cloud Insights がそれに応えました。明るいテーマと暗い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。



データコレクターのサポート

Cloud Insightsデータ コレクターにいくつかの改善を加えました。以下にハイライトをいくつか紹介します。

- Amazon FSx for ONTAPの新しいコレクター

2021年9月

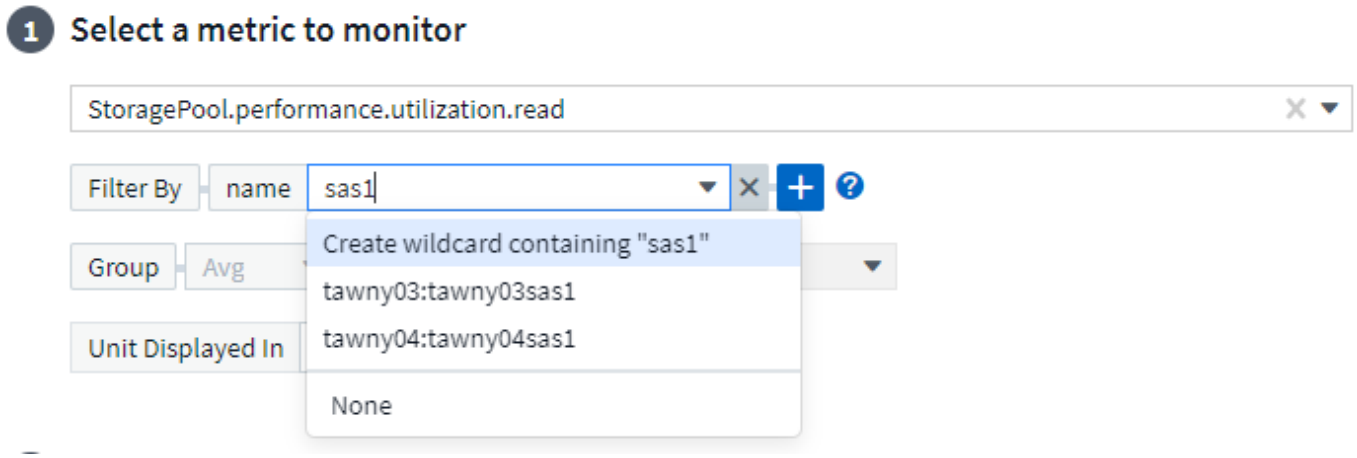
パフォーマンスポリシーがモニターになりました

Cloud Insights全体で、パフォーマンス ポリシーと違反がモニターとアラートに置き換えられました。"モニターによるアラート"環境内の潜在的な問題や傾向に対する柔軟性と洞察力が向上します。

モニターの自動補完候補、ワイルドカード、および式

アラート用のモニターを作成するときに、フィルターの入力が予測的になり、モニター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るようになりました。さらに、入力したテキストに基づいてワイルドカード フィルターを作成するオプションもあります。



更新されたTelegrafエージェント

Telegraf 統合データを取り込むエージェントがバージョン **1.19.3** に更新され、パフォーマンスとセキュリティが向上しました。アップデートを希望するユーザーは、"エージェントのインストール"ドキュメント。エージェントの以前のバージョンは、ユーザーの操作を必要とせずに引き続き機能します。

データコレクターのサポート

Cloud Insightsデータ コレクターにいくつかの改善を加えました。以下にハイライトをいくつか紹介します。

- Microsoft Hyper-V コレクターは WMI の代わりに PowerShell を使用するようになりました
- Azure VMおよびVHDコレクターは、並列呼び出しにより最大10倍高速化されました。
- HPE Nimbleはフェデレーション構成とiSCSI構成をサポートするようになりました

当社は常にデータ収集の改善に努めておりますので、注目すべき最近の変更点をいくつかご紹介します。

- EMC Powerstore の新しいコレクター
- 日立オプスセンターの新コレクター
- 日立コンテンツプラットフォームの新しいコレクター
- ファブリックプールを報告するためのONTAPコレクターの強化
- ストレージプールとボリュームのパフォーマンスを強化した ANF
- 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を備えた強化された EMC ECS
- ストレージノードとQtreeメトリックを備えたEMC Isilonの強化
- ボリューム QOS 制限メトリックを備えた拡張 EMC Symetrix
- 拡張IBM SVCおよびEMC PowerStore with Storage Nodes親シリアル番号

2021年8月

新しい監査ページのユーザーインターフェース

その"監査ページ"よりクリーンなインターフェースを提供し、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。

強化されたユーザーロール管理

Cloud Insightsでは、ユーザー ロールとアクセス制御の割り当てをさらに自由に行うことができるようになりました。ユーザーには、監視、レポート、 Cloud Secureの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、より多くのユーザーに監視、最適化、レポート機能への管理アクセスを許可しながら、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、必要なユーザーのみに制限することができます。

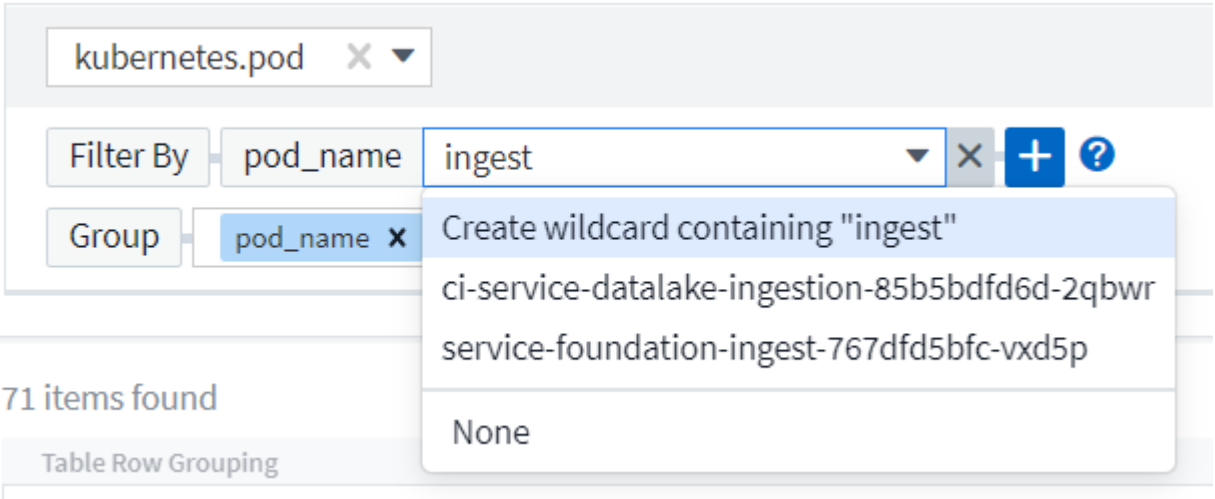
"詳細はこちら"Cloud Insightsドキュメントのさまざまなアクセス レベルについて説明します。

2021年6月

フィルターのオートコンプリート候補、ワイルドカード、および式

Cloud Insightsのこのリリースでは、クエリまたはウィジェットでフィルタリングできるすべての名前と値を知る必要がなくなりました。フィルタリングするときは、入力を開始するだけで、Cloud Insights がテキストに基づいて値を提案します。ウィジェットに表示するアプリケーション名や Kubernetes 属性を見つけるために、事前にアプリケーション名や Kubernetes 属性を調べる必要がなくなります。

フィルターを入力すると、フィルターによって選択可能な結果のスマート リストが表示されるほか、現在のテキストに基づいて ワイルドカード フィルター 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、フィルターに追加する複数の個別の値を選択することもできます。



さらに、NOT または OR を使用してフィルターに*式*を作成したり、「なし」オプションを選択してフィールド内の null 値をフィルターしたりすることもできます。

詳細はこちら"フィルタリングオプション"クエリとウィジェット内。

エディション別に利用可能なAPI

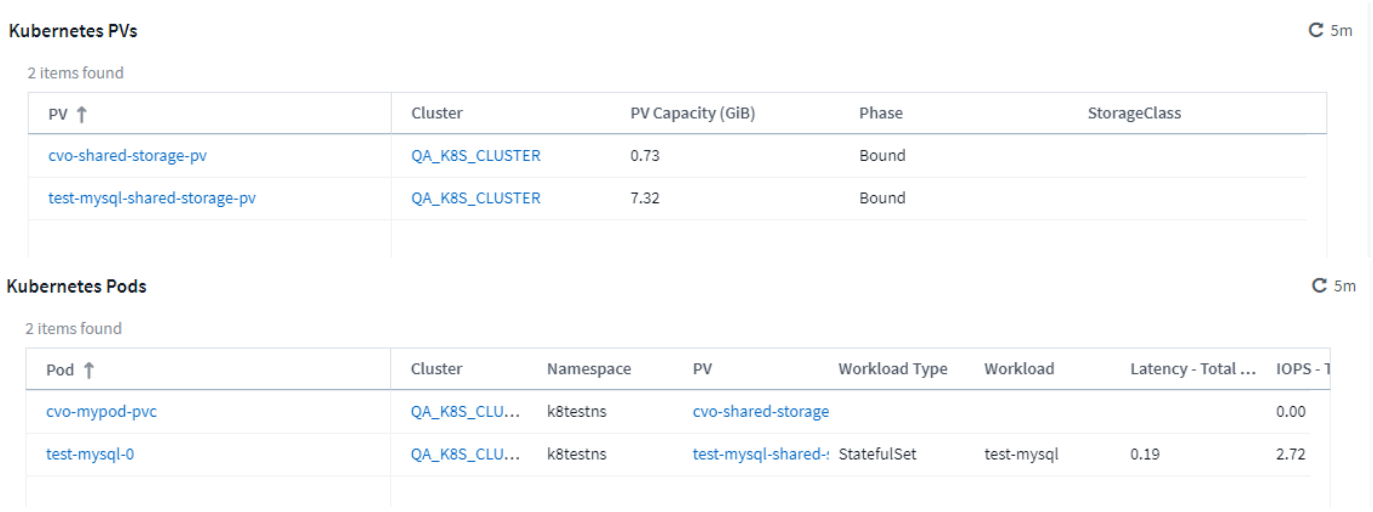
Cloud Insightsの強力な API はこれまで以上にアクセスしやすくなり、Alerts API が Standard エディションと Premium エディションで利用できるようになりました。各エディションでは次の API が利用可能です。

API カテゴリ	Basic	Standard	Premium
買収ユニット	✔	✔	✔
データの収集	✔	✔	✔
アラート		✔	✔
資産		✔	✔
データの取り込み		✔	✔

Kubernetes PVとPodの可視性

Cloud Insights は、Kubernetes 環境のバックエンド ストレージの可視性を提供し、Kubernetes Pod と永続ボリューム (PV) に関する分析情報を提供します。単一の Pod の使用状況から PV カウンター、PV、そしてバックエンド ストレージ デバイスに至るまで、IOPS、レイテンシー、スループットなどの PV カウンターを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 ページには、次の 2 つの新しいテーブルが表示されます。

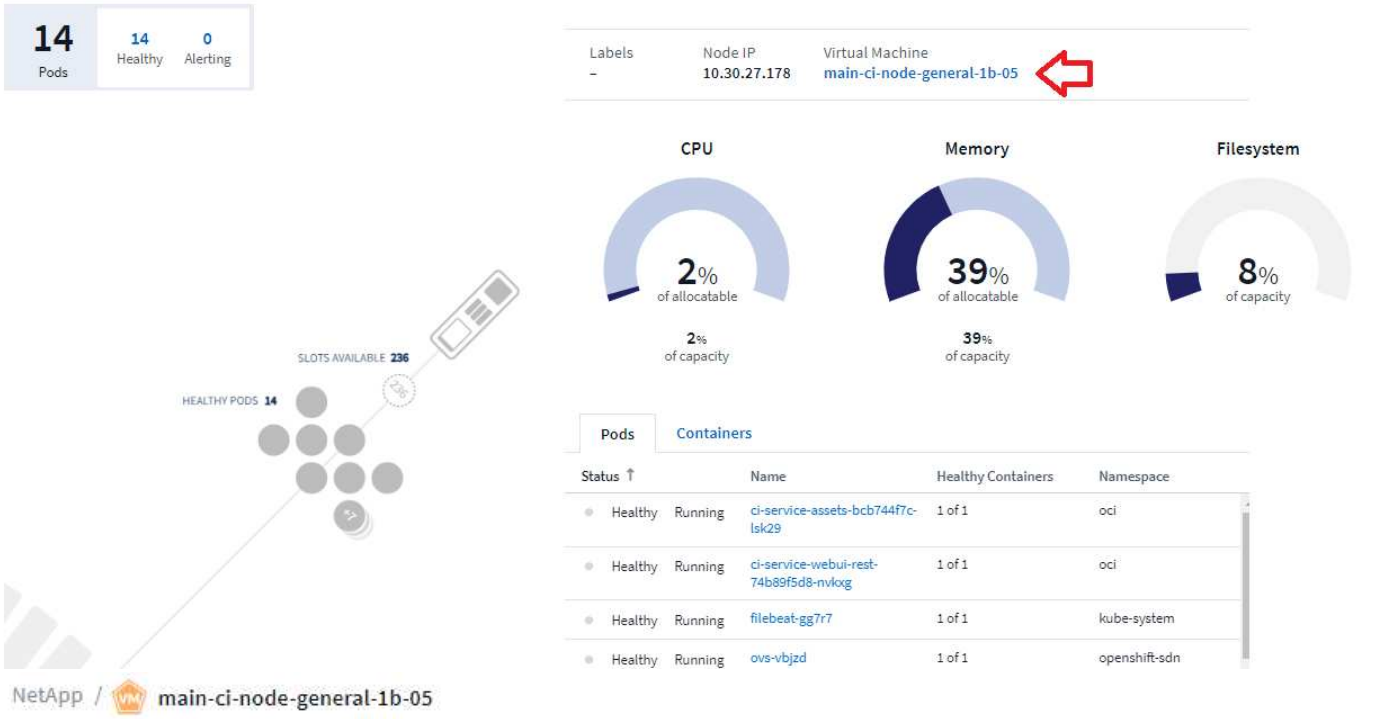


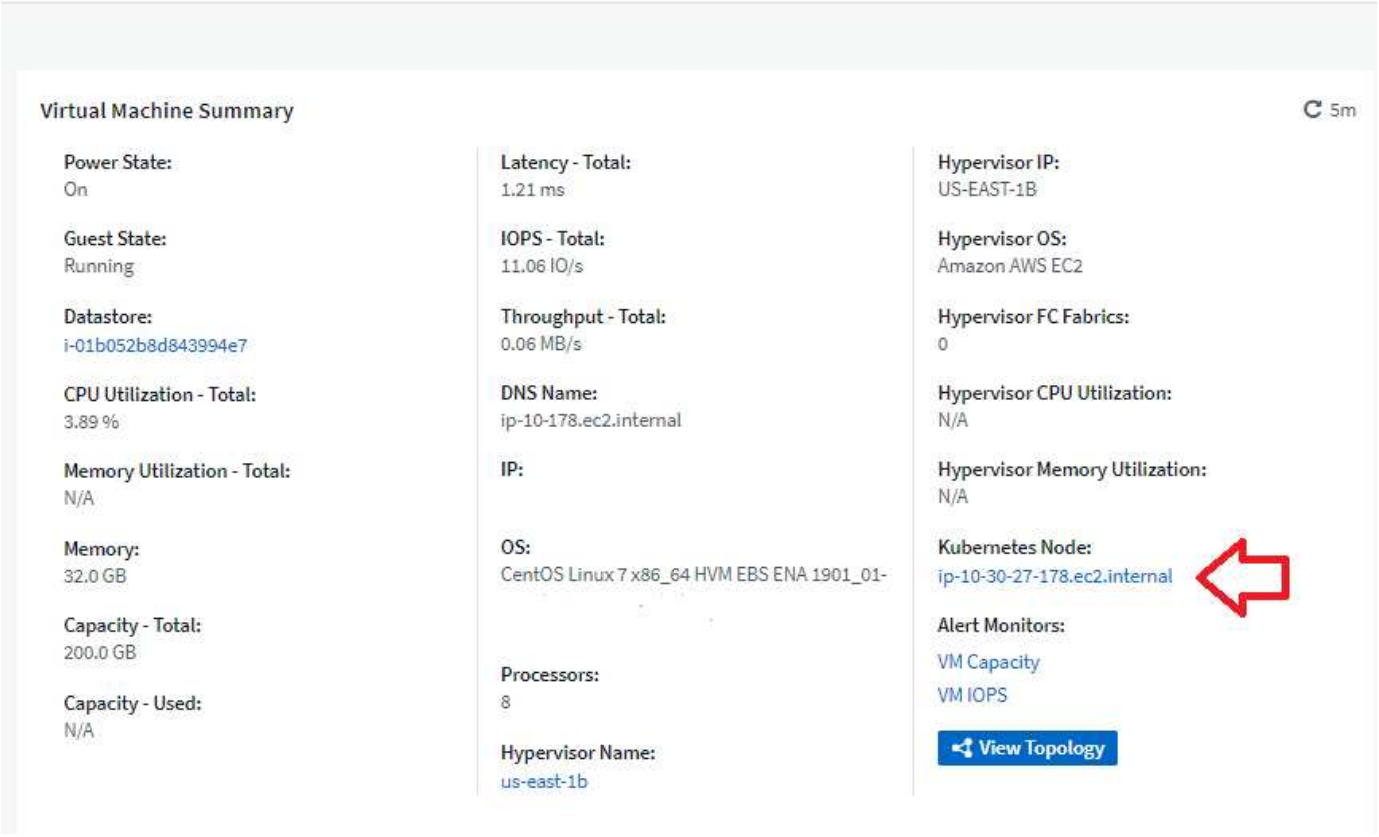
これらの新しいテーブルを活用するには、現在の Kubernetes エージェントをアンインストールして、新規にインストールすることをお勧めします。 Kube-State-Metrics バージョン 2.1.0 以降もインストールする必要があります。

Kubernetes ノードから VM へのリンク

Kubernetes ノード ページでクリックすると、ノードの VM ページが開くようになりました。 VM ページに

は、ノード自体へのリンクも含まれています。





パフォーマンス ポリシーに代わるアラート モニター

複数のしきい値、Webhook および電子メールアラートの配信、単一のインターフェースを使用したすべてのメトリックのアラートなどの追加のメリットを有効にするために、 Cloud Insights は2021 年 7 月から 8 月にかけて、Standard および Premium Edition のお客様を パフォーマンス ポリシー から モニター に変換しま

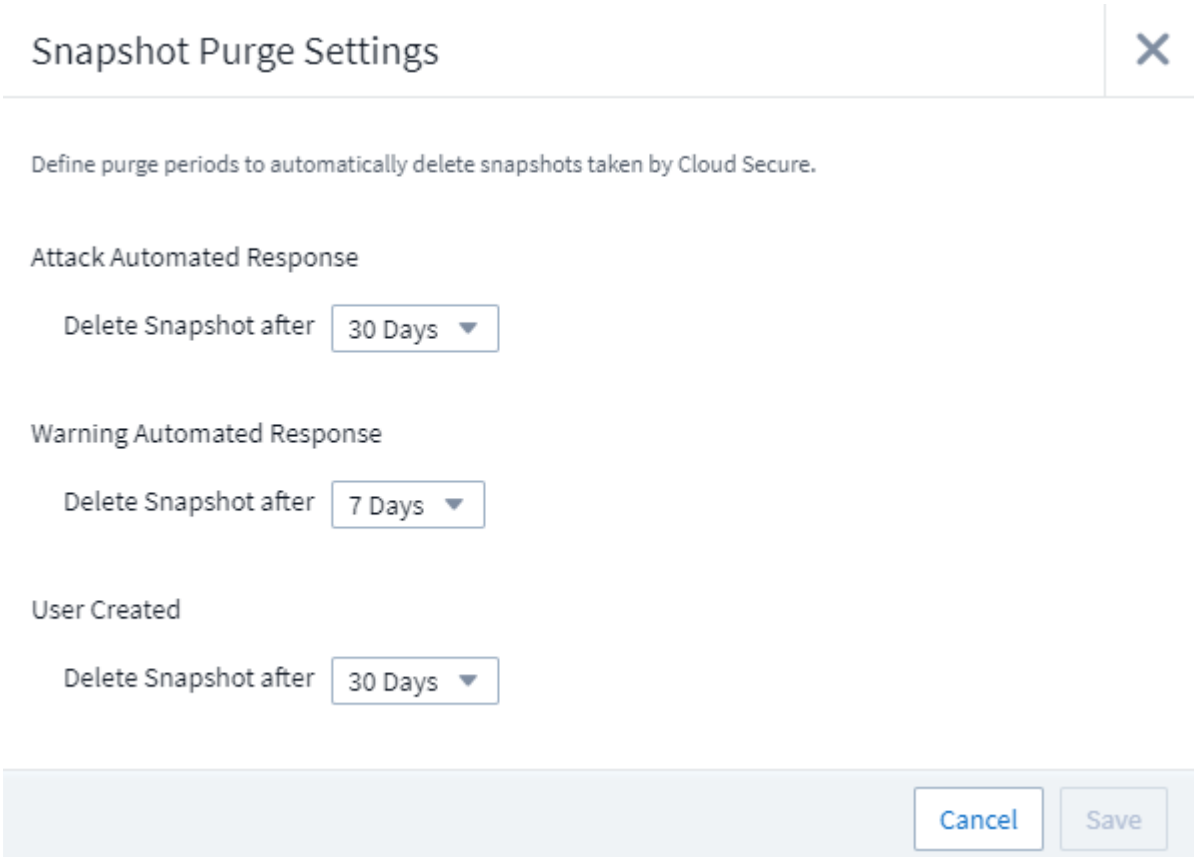
す。詳細はこちら"アラートとモニター"このエキサイティングな変化にご期待ください。

Cloud SecureはNFSをサポート

Cloud Secure は、 ONTAPデータ収集用の NFS をサポートするようになりました。 SMB および NFS ユーザー アクセスを監視して、ランサムウェア攻撃からデータを保護します。さらに、 Cloud Secure は、NFS ユーザー属性の収集のために Active-Directory および LDAP ユーザー ディレクトリをサポートしています。

Cloud Secureスナップショットの消去

Cloud Secure は、スナップショット消去設定に基づいてスナップショットを自動的に削除し、ストレージ スペースを節約し、手動でスナップショットを削除する必要性を減らします。



Cloud Secureデータ収集速度

単一のデータ コレクター エージェント システムは、1 秒あたり最大 20,000 件のイベントをCloud Secureに投稿できるようになりました。

2021年5月

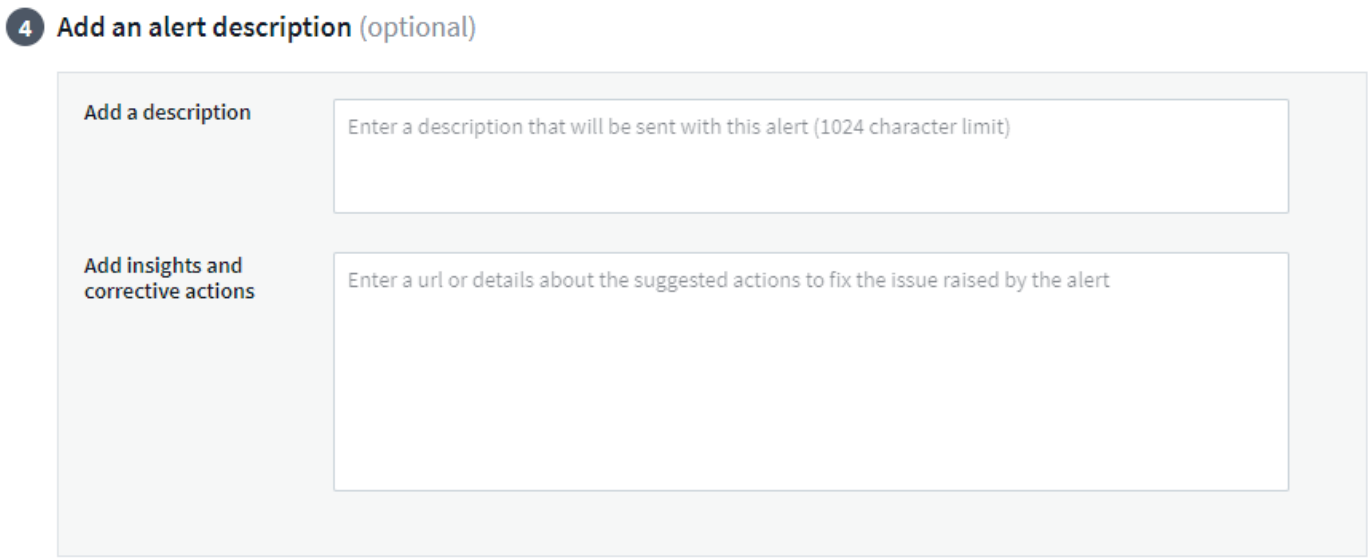
4 月に行った変更の一部をご紹介します。

更新されたTelegrafエージェント

Telegraf 統合データを取り込むエージェントがバージョン 1.17.3 に更新され、パフォーマンスとセキュリティが向上しました。アップデートを希望するユーザーは、"エージェントのインストール"ドキュメント。エージェントの以前のバージョンは、ユーザーの操作を必要とせずに引き続き機能します。

アラートに是正措置を追加する

*アラートの説明を追加*セクションに入力することで、モニターを作成または変更するときに、オプションの説明や追加の洞察や修正アクションを追加できるようになりました。説明はアラートとともに送信されます。洞察と是正措置 フィールドでは、アラートに対処するための詳細な手順とガイダンスが提供され、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。



すべてのエディション向けのCloud Insights API

API アクセスは、 Cloud Insightsのすべてのエディション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ーは、取得ユニットとデータ コレクターのアクションを自動化できるようになりました。また、Standard エディションのユーザーは、メトリックを照会したり、カスタム メトリックを取り込んだりすることができます。プレミアム エディションでは、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	Basic	Standard	Premium
買収ユニット	✔	✔	✔
データの収集	✔	✔	✔
資産		✔	✔
データの取り込み		✔	✔
Data Warehouse			✔

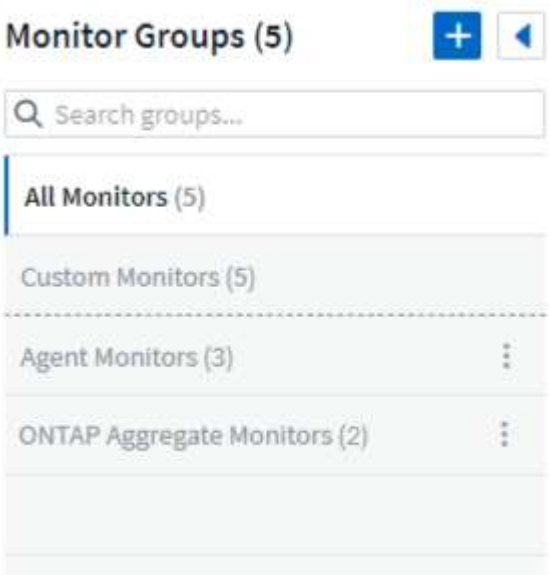
APIの使用に関する詳細は、"APIのドキュメント" 。

2021年4月

モニターの管理が簡単

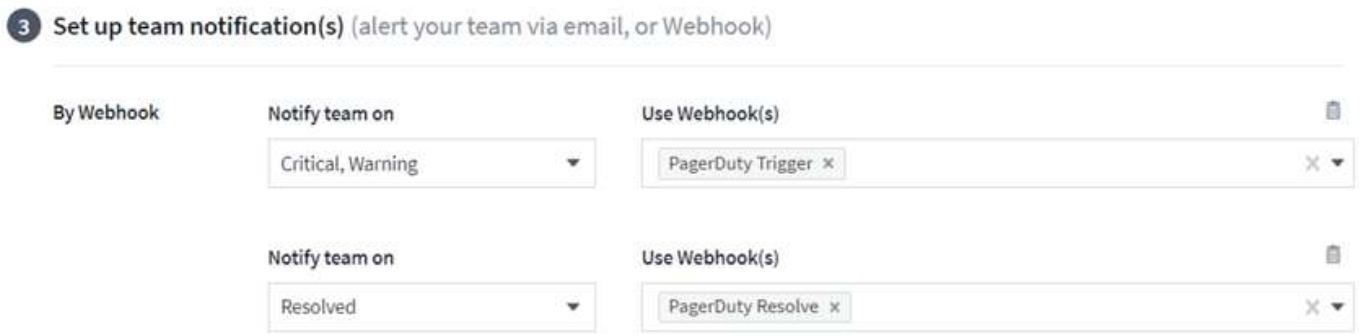
"モニターのグループ化"環境内のモニターの管理を簡素化します。複数のモニターをグループ化し、1 つとして一時停止できるようになりました。たとえば、インフラストラクチャのスタックで更新が行われている場合、ワンクリックですべてのデバイスからのアラートを一時停止できます。

モニター グループは、 Cloud InsightsにONTAPデバイスの管理機能の向上をもたらす魅力的な新機能の最初の部分です。



Webhookを使用した強化されたアラートオプション

多くの商用アプリケーションがサポート"ウェブフック"標準入力インターフェースとして。 Cloud Insights は現在、これらの配信チャネルの多くをサポートしており、Slack、PagerDuty、Teams、Discord のデフォルトテンプレートを提供しているほか、他の多くのアプリケーションをサポートするためにカスタマイズ可能な汎用 Webhook も提供しています。



デバイス識別の改善

監視とトラブルシューティングを改善し、正確なレポートを提供するには、デバイスの IP アドレスやその他の識別子ではなく、デバイスの名前を理解することが役立ちます。 Cloud Insightsには、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と物理ホストデバイスの名前を自動的に識別する方法が組み込まれま

した。"デバイスの解像度" *管理*メニューで利用できます。

もっと求めてたよ！

お客様から、データの範囲を視覚化するためのデフォルト オプションを増やしてほしいというご要望が多かったため、時間範囲ピッカーを通じてサービス全体で利用できる次の 5 つの新しい選択肢を追加しました。

- 最後の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

4 月 2 日より、 Cloud Insights は単一のCloud Insightsインスタンスで、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、顧客はCloud Insightsサブスクリプションの一部をインフラストラクチャの購入と同時に終了できるようになります。複数のサブスクリプションに関するサポートについては、 NetApp の営業部にお問い合わせください。

あなたの道を選びなさい

Cloud Insightsを設定する際に、監視とアラートから開始するか、ランサムウェアと内部脅威の検出から開始するか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構成します。他のパスは後からいつでも設定できます。

より簡単なCloud Secureオンボーディング

また、新しいステップバイステップのセットアップ チェックリストにより、 Cloud Secureの使用を開始するのがこれまで以上に簡単になりました。



いつものように、皆様からのご提案をお待ちしております。 ng-cloudinsights-customerfeedback@netapp.com までお送りください。

2021年2月

更新されたTelegrafエージェント

Telegraf 統合データを取り込むエージェントがバージョン 1.17.0 に更新され、脆弱性とバグの修正が含まれています。

クラウドコストアナライザー

過去、現在、および推定支出の詳細なコスト分析を提供し、環境内のクラウド使用状況を可視化する、NetAppの Spot と Cloud Cost のパワーを体験してください。クラウド コスト ダッシュボードでは、クラウド費用を明確に把握し、個々のワークロード、アカウント、サービスにドリルダウンすることができます。

Cloud Cost は、次のような大きな課題の解決に役立ちます。

- クラウド費用の追跡と監視
- 無駄と潜在的な最適化領域の特定
- 実行可能なアクションアイテムの提供

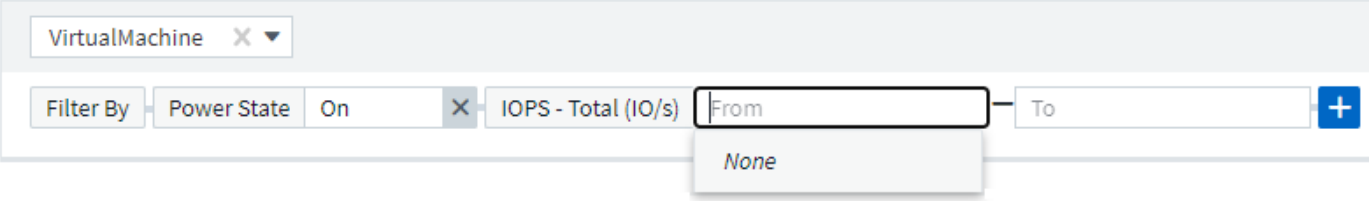
クラウドコストは監視に重点を置いています。完全な Spot by NetAppアカウントにアップグレードすると、自動的なコスト削減と環境の最適化が可能になります。

フィルターを使用して **null** 値を持つオブジェクトを照会する

Cloud Insightsでは、フィルターを使用して null/none 値を持つ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、次の場所の任意の属性/メトリックに対して実行できます。

- クエリページ
- ダッシュボードウィジェットとページ変数
- アラートリストページ
- 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、適切なフィルタ ドロップダウンに [なし] オプションが表示されたらそれを選択するだけです。



マルチリージョンサポート

本日より、世界中のさまざまな地域でCloud Insightsサービスの提供を開始し、米国外に拠点を置くお客様のパフォーマンス向上とセキュリティ強化を実現します。 Cloud Insights/ Cloud Secure は、環境が作成されたリージョンに応じて情報を保存します。

クリック"ここをクリックしてください。"詳細についてはこちらをご覧ください。

2021年1月

追加の**ONTAP**メトリックの名前が変更されました

ONTAPシステムからのデータ収集の効率を向上するための継続的な取り組みの一環として、次のONTAPメトリックの名前が変更されました。

これらのメトリックのいずれかを使用している既存のダッシュボード ウィジェットまたはクエリがある場合は、新しいメトリック名を使用するためにそれらを編集または再作成する必要があります。

以前のメトリック名	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.読み取りスループット

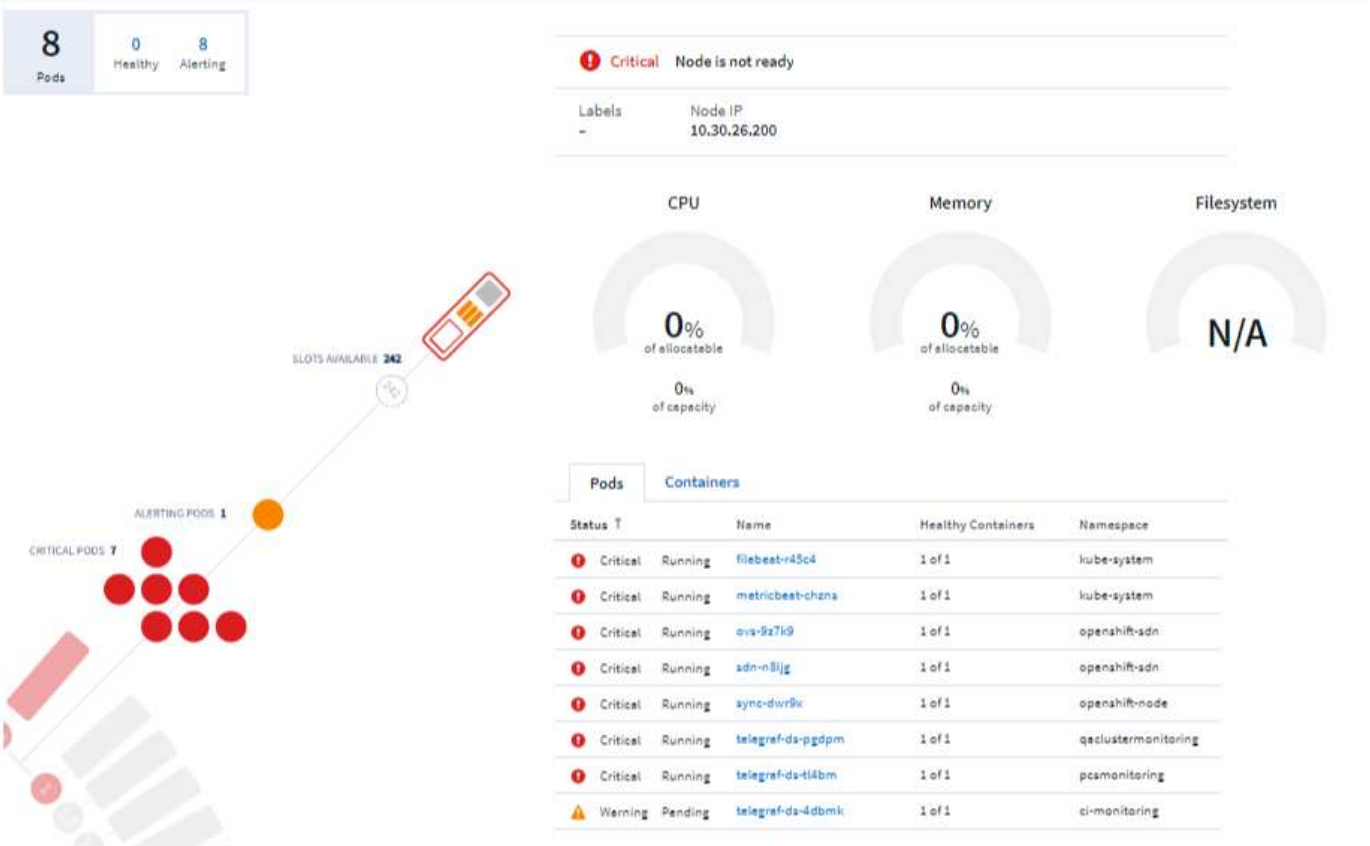
以前のメトリック名	新しいメトリック名
netapp_ontap.fcp_lif.write_data	netapp_ontap.fcp_lif.書き込みスループット
netapp_ontap.iscsi_lif.read_data	netapp_ontap.iscsi_lif.読み取りスループット
netapp_ontap.iscsi_lif.write_data	netapp_ontap.iscsi_lif.書き込みスループット
netapp_ontap.lif.recv_data	netapp_ontap.lif.recv_throughput
netapp_ontap.lif.送信データ	netapp_ontap.lif.送信スループット
netapp_ontap.lun.read_data	netapp_ontap.lun.読み取りスループット
netapp_ontap.lun.write_data	netapp_ontap.lun.書き込みスループット
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.読み取りスループット
netapp_ontap.path.write_data	netapp_ontap.path.write_throughput
netapp_ontap.path.total_data	netapp_ontap.path.合計スループット
netapp_ontap.ポリシーグループ.読み取りデータ	netapp_ontap.ポリシーグループ.読み取りスループット
netapp_ontap.ポリシーグループ.write_data	netapp_ontap.ポリシーグループ.書き込みスループット
netapp_ontap.ポリシーグループ.その他のデータ	netapp_ontap.ポリシーグループ.その他のスループット
netapp_ontap.ポリシーグループ.合計データ	netapp_ontap.ポリシーグループ.合計スループット
netapp_ontap.system_node.disk_data_read	netapp_ontap.system_node.disk_throughput_read
netapp_ontap.system_node.disk_data_written	netapp_ontap.system_node.disk_throughput_written
netapp_ontap.system_node.hdd_data_read	netapp_ontap.system_node.hdd_throughput_read
netapp_ontap.system_node.hdd_data_written	netapp_ontap.system_node.hdd_throughput_written
netapp_ontap.system_node.ssd_data_read	netapp_ontap.system_node.ssd_throughput_read
netapp_ontap.system_node.ssd_data_written	netapp_ontap.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_sent	netapp_ontap.system_node.fcp_throughput_sent
netapp_ontap.volume_node.cifs_read_data	netapp_ontap.volume_node.cifs_read_throughput
netapp_ontap.volume_node.cifs_write_data	netapp_ontap.volume_node.cifs_write_throughput
netapp_ontap.volume_node.nfs_read_data	netapp_ontap.volume_node.nfs_read_throughput
netapp_ontap.volume_node.nfs_write_data	netapp_ontap.volume_node.nfs_write_throughput
netapp_ontap.volume_node.iscsi_read_data	netapp_ontap.volume_node.iscsi_read_throughput

以前のメトリック名	新しいメトリック名
netapp_ontap.volume_node.iscsi_write_data	netapp_ontap.volume_node.iscsi_write_throughput
netapp_ontap.volume_node.fcp_read_data	netapp_ontap.volume_node.fcp_read_throughput
netapp_ontap.volume_node.fcp_write_data	netapp_ontap.volume_node.fcp_write_throughput
netapp_ontap.ボリューム.読み取りデータ	netapp_ontap.ボリューム.読み取りスループット
netapp_ontap.ボリューム.書き込みデータ	netapp_ontap.ボリューム.書き込みスループット
netapp_ontap.workload.read_data	netapp_ontap.workload.read_throughput
netapp_ontap.ワークロード.書き込みデータ	netapp_ontap.workload.write_throughput
netapp_ontap.ワークロードボリューム.読み取りデータ	netapp_ontap.ワークロードボリューム.読み取りスループット
netapp_ontap.ワークロードボリューム.書き込みデータ	netapp_ontap.ワークロードボリューム.書き込みスループット

新しい **Kubernetes** エクスプローラー

その"Kubernetes エクスプローラー"Kubernetes クラスターのシンプルなトポロジ ビューを提供し、専門家でなくても、クラスター レベルからコンテナーやストレージに至るまで、問題と依存関係を迅速に特定できます。

Kubernetes Explorer のドリルダウン詳細を使用して、Kubernetes 環境内のクラスター、ノード、ポッド、コンテナー、ストレージのステータス、使用状況、正常性に関するさまざまな情報を調査できます。



2020年12月

よりシンプルな**Kubernetes**のインストール

Kubernetes エージェントのインストールが合理化され、ユーザーによる操作が少なくて済むようになりました。"Kubernetesエージェントのインストール" Kubernetes データ収集が含まれるようになりました。

2020年11月

追加のダッシュボード

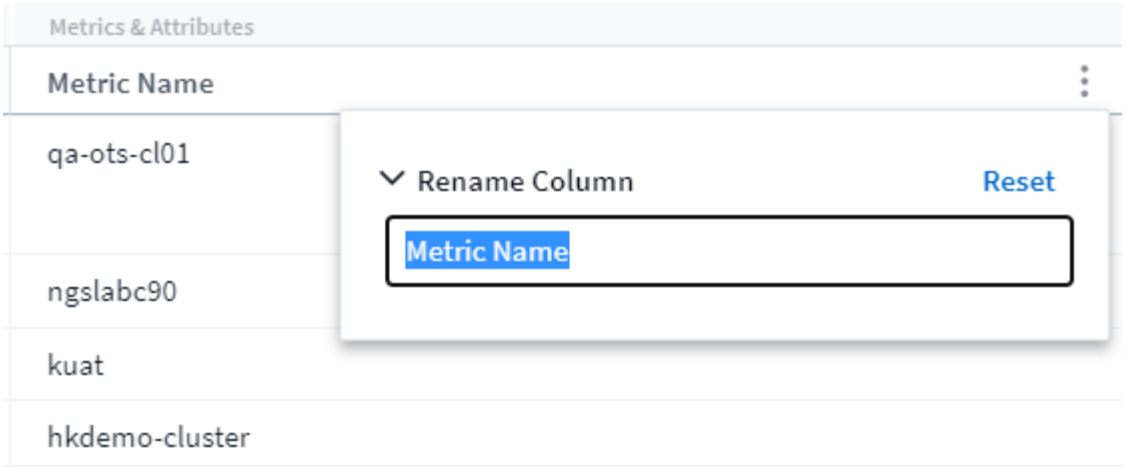
次の新しいONTAPに特化したダッシュボードがギャラリーに追加され、インポートできるようになりました。

- ONTAP: 総合的なパフォーマンスと容量
- ONTAP FAS/ AFF - 容量使用率
- ONTAP FAS/ AFF - クラスタ容量
- ONTAP FAS/ AFF - 効率
- ONTAP FAS/ AFF - FlexVol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 - 事前事後容量効率
- ONTAP: ネットワークポートアクティビティ
- 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 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 パフォーマンス (フロントエンド)

テーブルウィジェットの列名の変更

テーブル ウィジェットの [メトリックと属性] セクションの列の名前を変更するには、ウィジェットを編集モードで開き、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*] をクリックするか、[*Reset*] をクリックして列を元の名前に戻します。

これはテーブル ウィジェット内の列の表示名にのみ影響し、基になるデータ自体のメトリック/属性名は変更されないことに注意してください。



2020年10月

統合データのデフォルトの拡張

テーブル 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 ノードのメトリックのデフォルトの拡張が可能になりました。たとえば、Kubernetes *Nodes* を *Cluster* ごとにグループ化すると、テーブルに各クラスターの行が表示されます。次に、各クラスター行を展開して、ノードオブジェクトのリストを表示できます。

ベーシックエディションのテクニカルサポート

テクニカル サポートは、Standard Edition および Premium Edition に加えて、 Cloud Insights Basic Edition の加入者にも利用できるようになりました。さらに、 Cloud Insightsにより、 NetAppサポート チケットを作成するワークフローが簡素化されました。

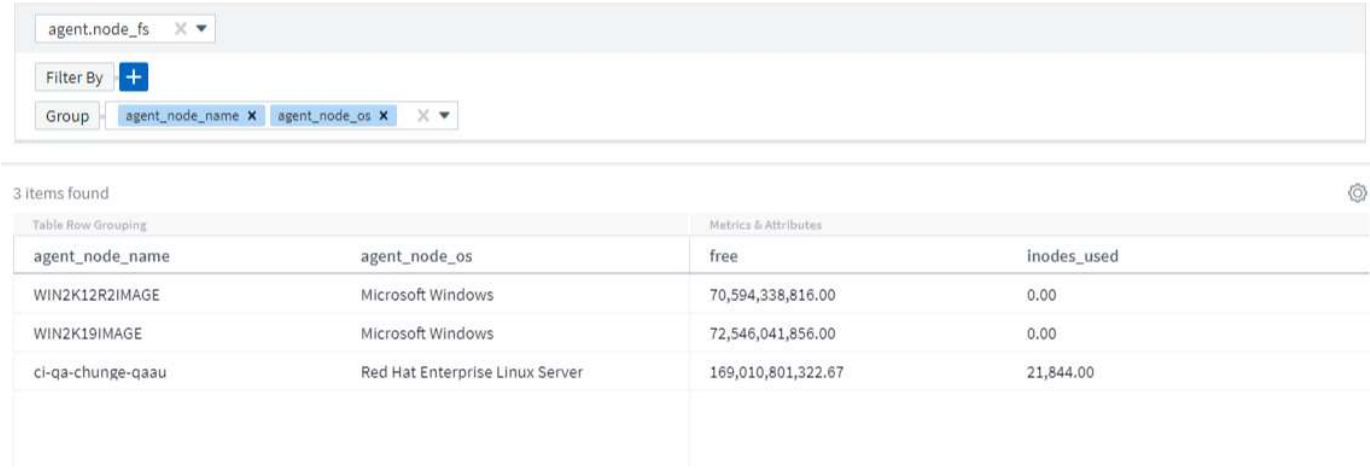
Cloud SecureパブリックAPI

Cloud Secureは"REST API"アクティビティとアラートの情報にアクセスします。これは、 Cloud Secure Admin UI を通じて作成された API アクセス トークンを使用することで実現され、その後 REST API へのアクセスに使用されます。これらの REST API の Swagger ドキュメントはCloud Secureと統合されています。

2020年9月

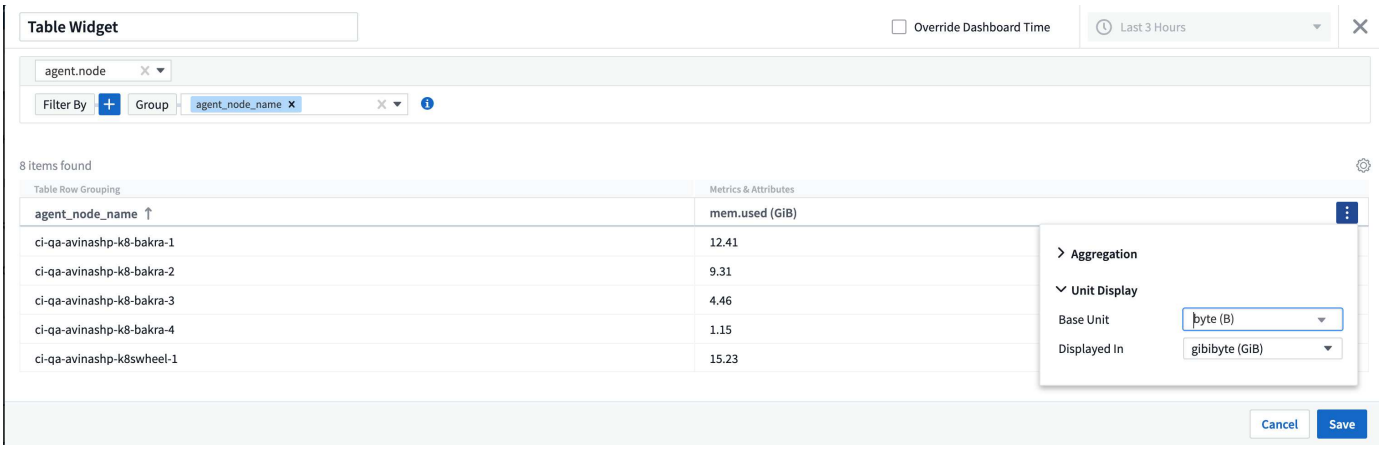
統合データを含むクエリページ

Cloud Insightsクエリ ページは、統合データ (Kubernetes、 ONTAP Advanced Metrics など) をサポートします。統合データを使用する場合、クエリ結果テーブルには「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、右側にオブジェクト データ (属性/メトリック) が表示されます。統合データをグループ化するために複数の属性を選択することもできます。



テーブルウィジェットの単位表示書式

メトリック/カウンター データ (ギガバイト、MB/秒など) を表示する列のテーブル ウィジェットで、単位表示フォーマットが利用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。利用可能なユニットから選択できます。使用可能な単位は、表示列のメトリック データの種類によって異なります。



取得ユニット詳細ページ

獲得ユニットには独自のランディング ページが用意され、各 AU に関する有用な詳細情報やトラブルシューティングに役立つ情報が提供されるようになりました。その"AU詳細ページ"AU のデータ収集者へのリンクと役立つステータス情報を提供します。

Cloud SecureDocker依存関係の削除

Cloud Secure の Docker への依存関係が削除されました。 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。

ユーザーロールの報告

Cloud Insights Premium Edition と Reporting をご利用の場合、環境内のすべてのCloud Insightsユーザーに Reporting アプリケーション (Cognos など) へのシングル サインオン (SSO) ログイン権限が付与されます。メニューの **Reports** リンクをクリックすると、Reporting に自動的にログインします。

Cloud Insightsにおけるユーザーの役割によって、"報告ユーザーの役割" :

Cloud Insightsの役割	報告役割	報告権限
ゲスト	消費者	レポートを表示、スケジュール、実行したり、言語やタイムゾーンなどの個人設定を行ったりできます。消費者はレポートを作成したり、管理タスクを実行したりすることはできません。
ユーザ	作成者	すべてのコンシューマー機能を実行できるほか、レポートとダッシュボードを作成および管理できます。
管理者	管理者	すべての作成者機能のほか、レポートの構成、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を実行できます。

Cloud Insights Reporting は、500 MU 以上の環境で利用できます。

現在プレミアムエディションをご利用で、レポートを保持したい場合は、こちらをお読みください。"既存のお客様への重要なお知らせ" 。

データ取り込み用の新しい **API** カテゴリ

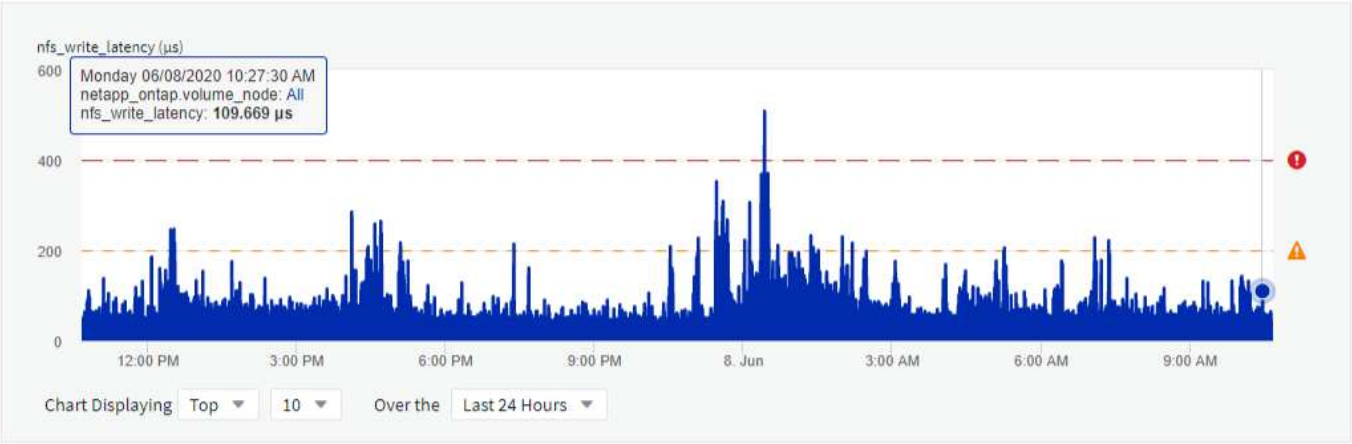
Cloud Insights に*データ取り込み* API カテゴリが追加され、カスタム データとエージェントをより細かく制御できるようになりました。この API カテゴリおよびその他の API カテゴリの詳細なドキュメントは、Cloud Insightsで **[管理] > [API** アクセス**]** に移動し、[API ドキュメント] リンクをクリックすると見つかります。 AU の詳細ページと AU リスト ページに表示される「メモ」フィールドで AU にコメントを添付することもできます。

2020年8月

監視と警告

ストレージオブジェクト、VM、EC2、ポートのパフォーマンスポリシーを設定する現在の機能に加えて、Cloud Insights Standard Editionには、"モニターを構成する" Kubernetes、 ONTAP の高度なメトリック、および Telegraf プラグインの統合データのしきい値。アラートをトリガーするオブジェクト メトリックごとにモニターを作成し、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、各レベルに必要な電子メール受信者を指定するだけです。その後、"アラートの表示と管理"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します。





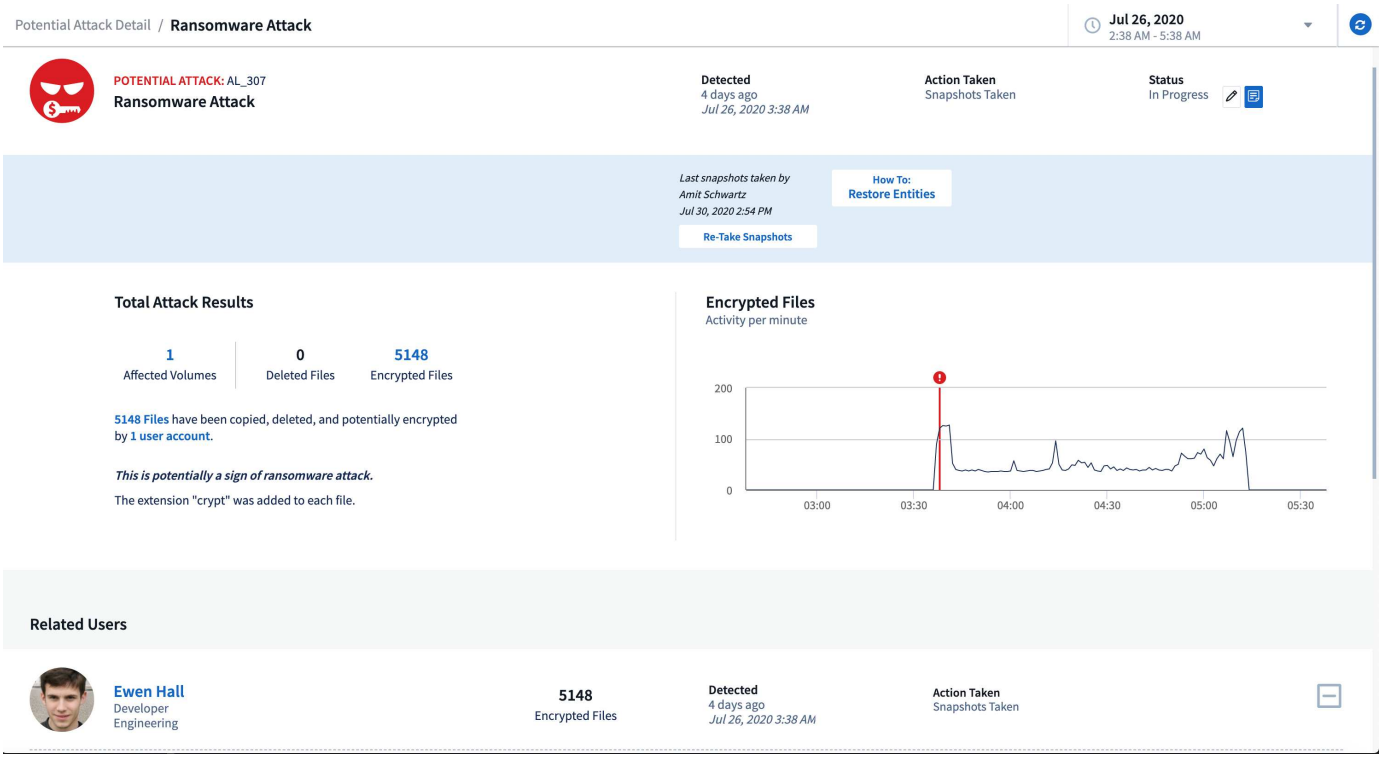
2020年7月

Cloud Secure_スナップショット_アクション

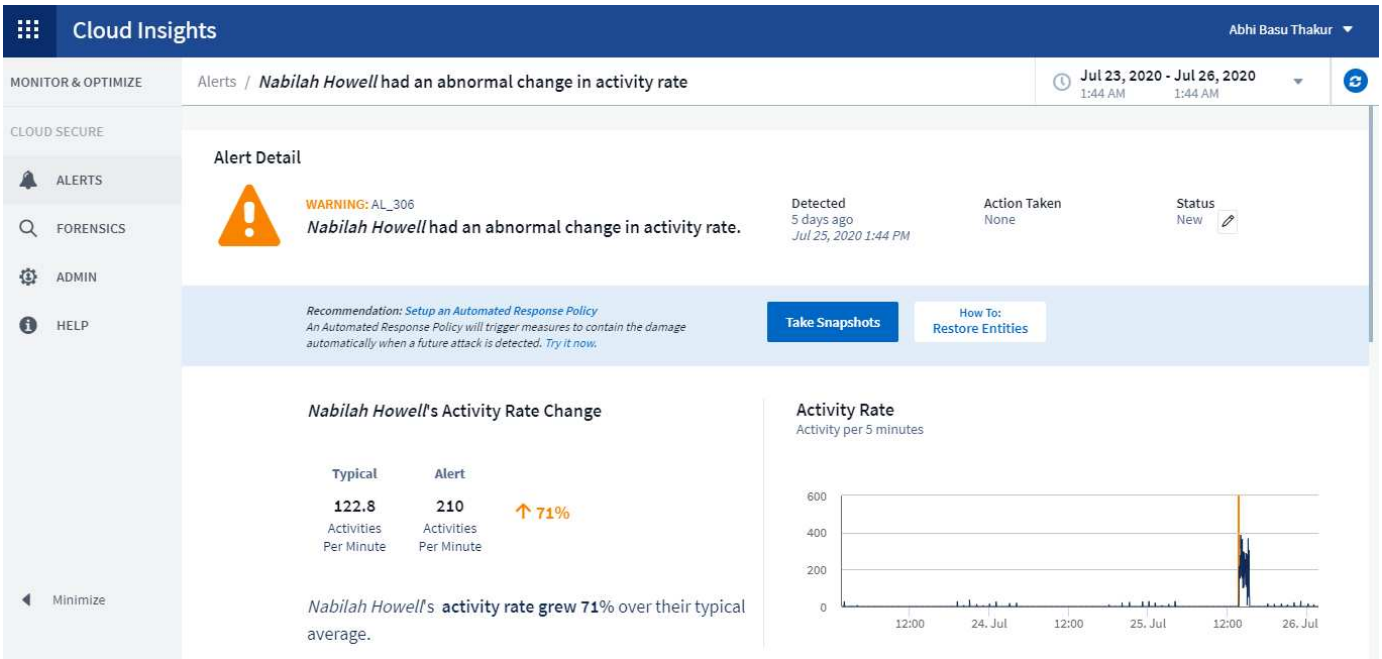
Cloud Secure は、悪意のあるアクティビティが検出されると自動的にスナップショットを取得してデータを保護し、データが安全にバックアップされることを保証します。

ランサムウェア攻撃やその他の異常なユーザー 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得する自動応答ポリシーを定義できます。アラート ページから手動でスナップショットを取得することもできます。

自動スナップショットが取得されました
:



手動スナップショット
:



メトリック/カウンターの更新

Cloud Insights UI および REST API では、次の容量カウンターを使用できます。以前は、これらのカウンターはデータ ウェアハウス/レポートでのみ使用可能でした。

オブジェクト タイプ	カウンタ
ストレージ	容量 - 予備のRAW容量 - 障害が発生したRAW

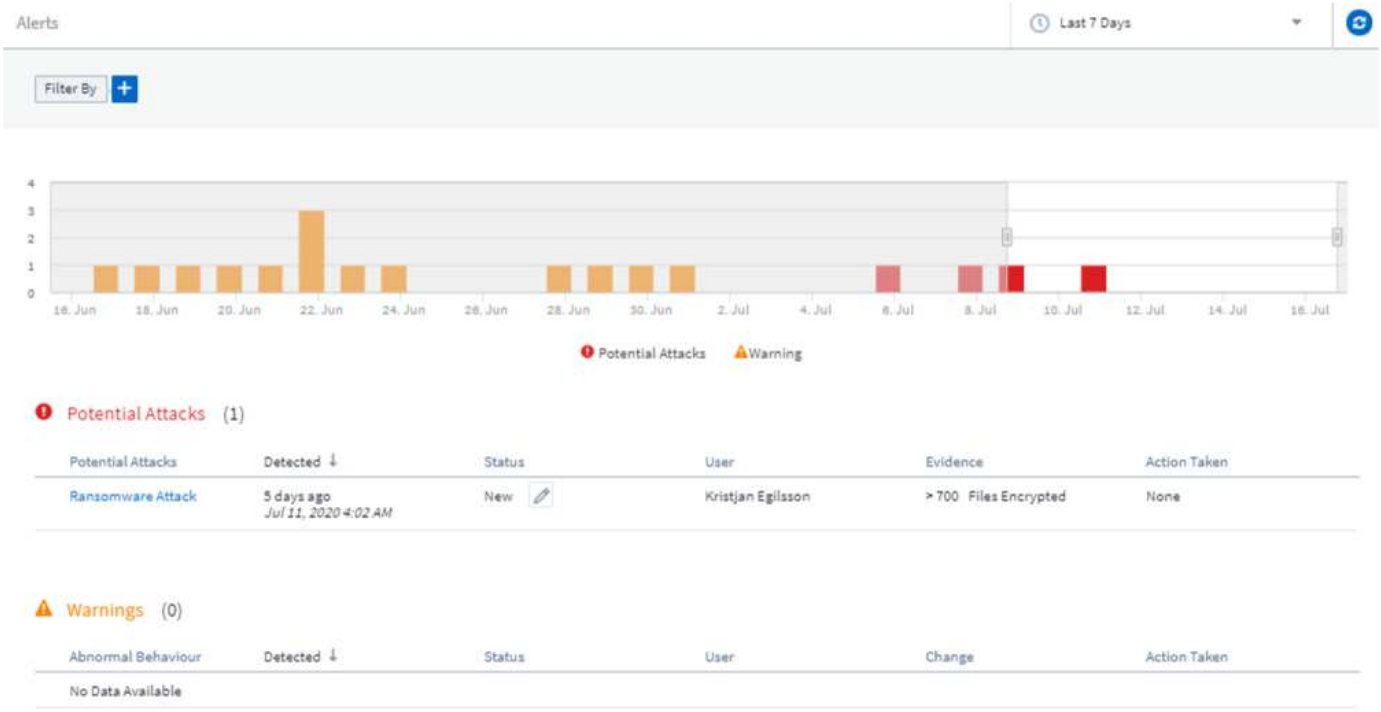
オブジェクト タイプ	カウンタ
ストレージ プール	データ容量 - 使用済みデータ容量 - 合計その他の容量 - 使用済みその他の容量 - 合計容量 - 生の容量 - ソフト制限
内部容積	データ容量 - 使用済み データ容量 - 合計 その他の容量 - 使用済み その他の容量 - 合計 クローン保存容量 - 合計

Cloud Secure潜在的攻撃検出

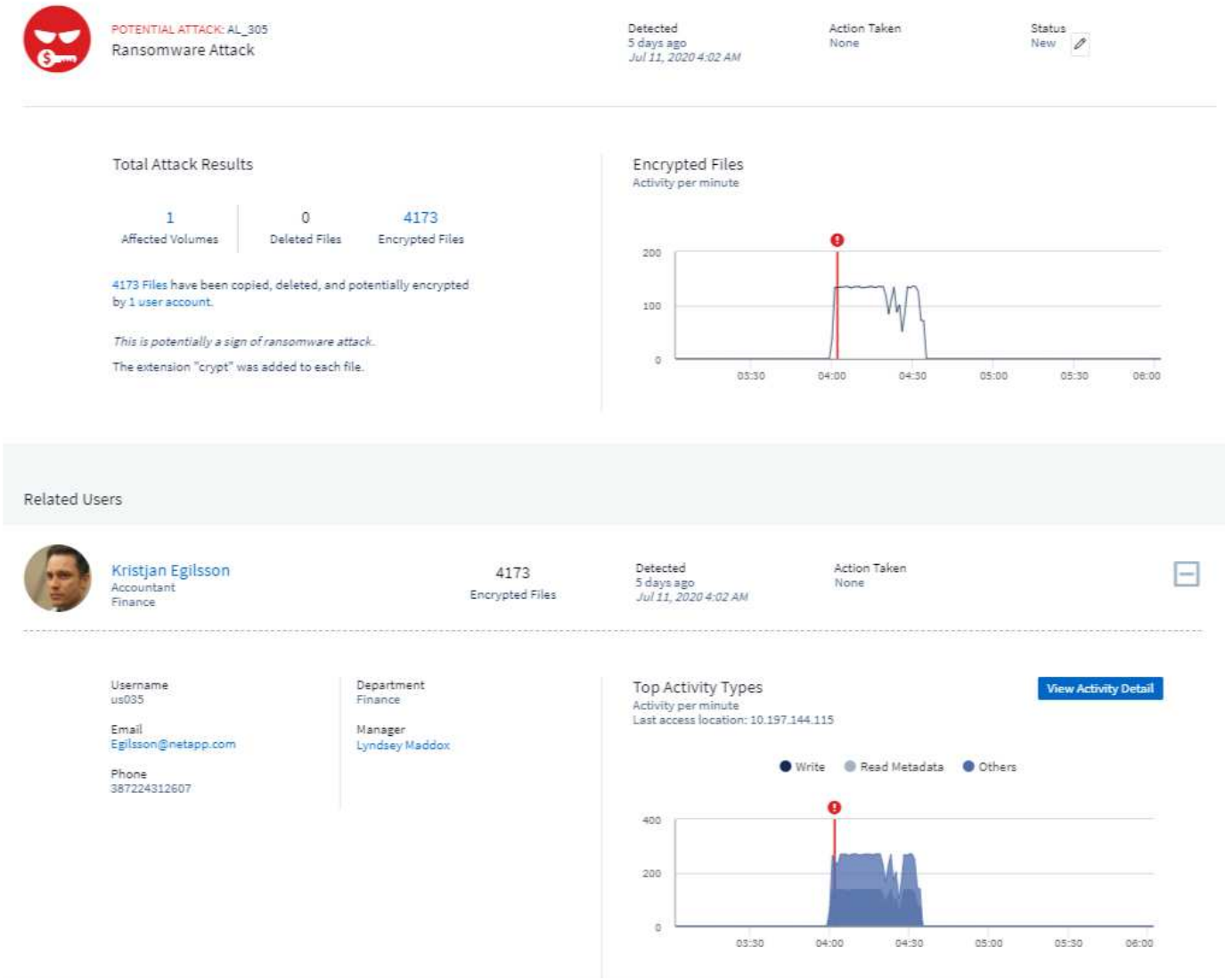
Cloud Secure は、ランサムウェアなどの潜在的な攻撃を検出できるようになりました。アラート リスト ページでアラートをクリックすると、次の内容を示す詳細ページが開きます。

- 攻撃時間
- 関連ユーザーとファイルアクティビティ
- 取られた措置
- セキュリティ侵害の可能性を追跡するのに役立つ追加情報

潜在的なランサムウェア攻撃を示すアラートページ
:



潜在的なランサムウェア攻撃の詳細ページ
:



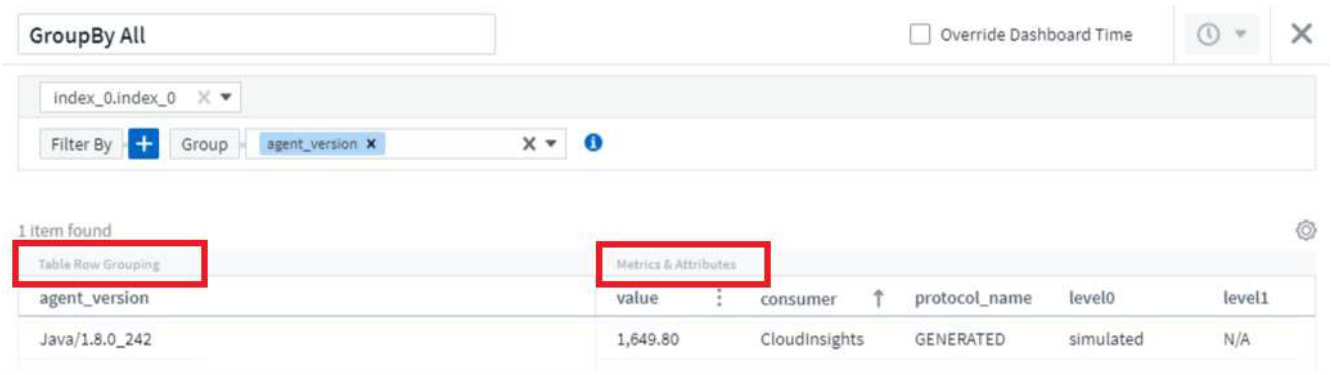
AWS 経由でプレミアムエディションをサブスクライブする

Cloud Insightsのトライアル期間中は、"セルフサブスクライブ" AWS Marketplace を通じてCloud Insights Standard Edition または Premium Edition にアップグレードできます。以前は、AWS Marketplace を通じて Standard Edition のみにセルフサブスクライブすることができました。

強化されたテーブルウィジェット

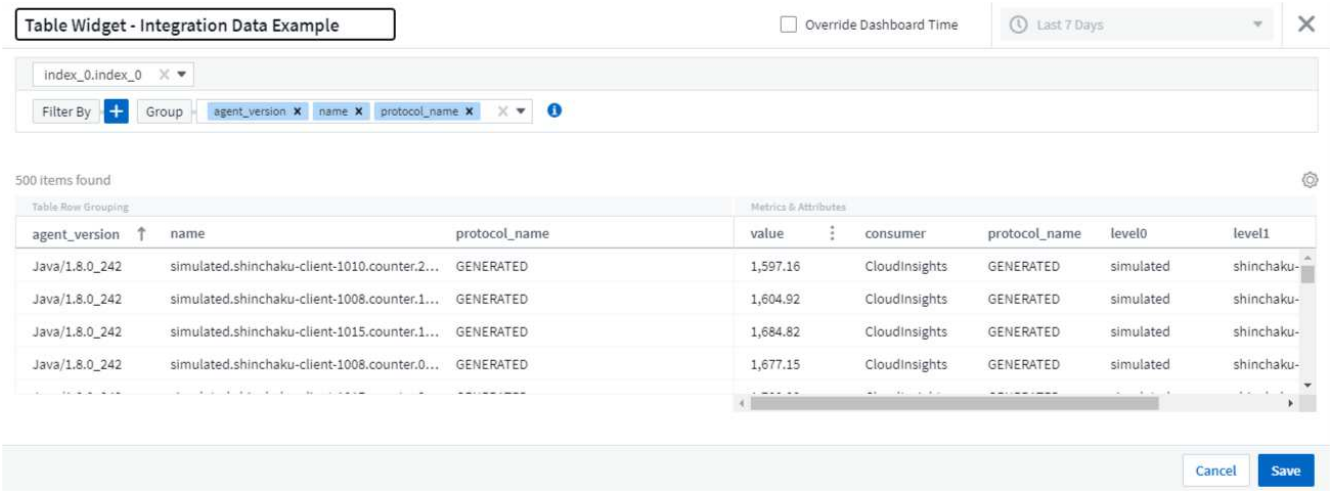
ダッシュボード/アセット ページのテーブル ウィジェットには、次の機能強化が含まれています。

- 「分割画面」ビュー: テーブル ウィジェットでは、左側にオブジェクト/グループが表示され、右側にオブジェクト データ (属性/メトリック) が表示されます。



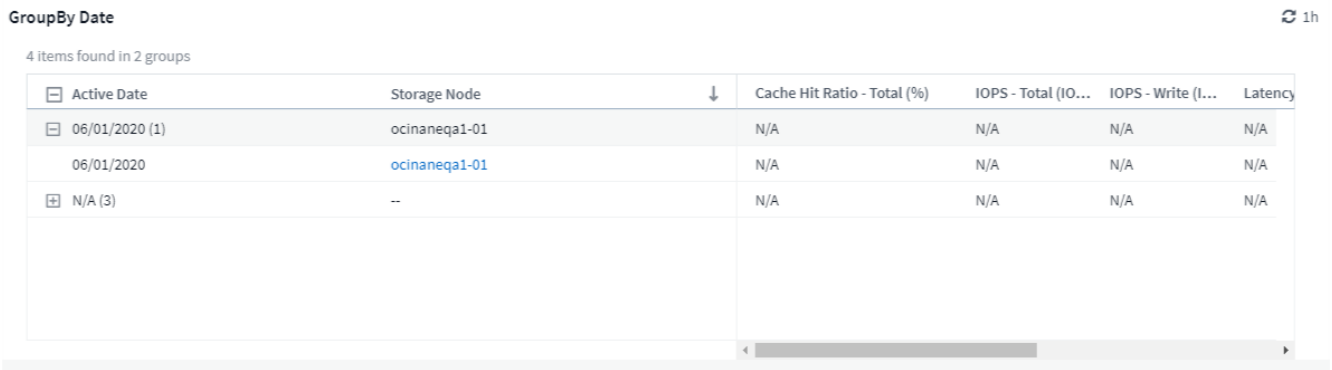
- 複数属性のグループ化: 統合データ (Kubernetes、 ONTAP高度なメトリック、Docker など) の場合、グループ化に複数の属性を選択できます。データは、選択したグループ化属性に従って表示されます。

  統合データによるグループ化（編集モードで表示）
  :



- インフラストラクチャ データ (ストレージ、EC2、VM、ポートなど) のグループ化は、以前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でグループ化する場合、テーブルではグループ行を展開してグループ内のすべてのオブジェクトを表示できます。

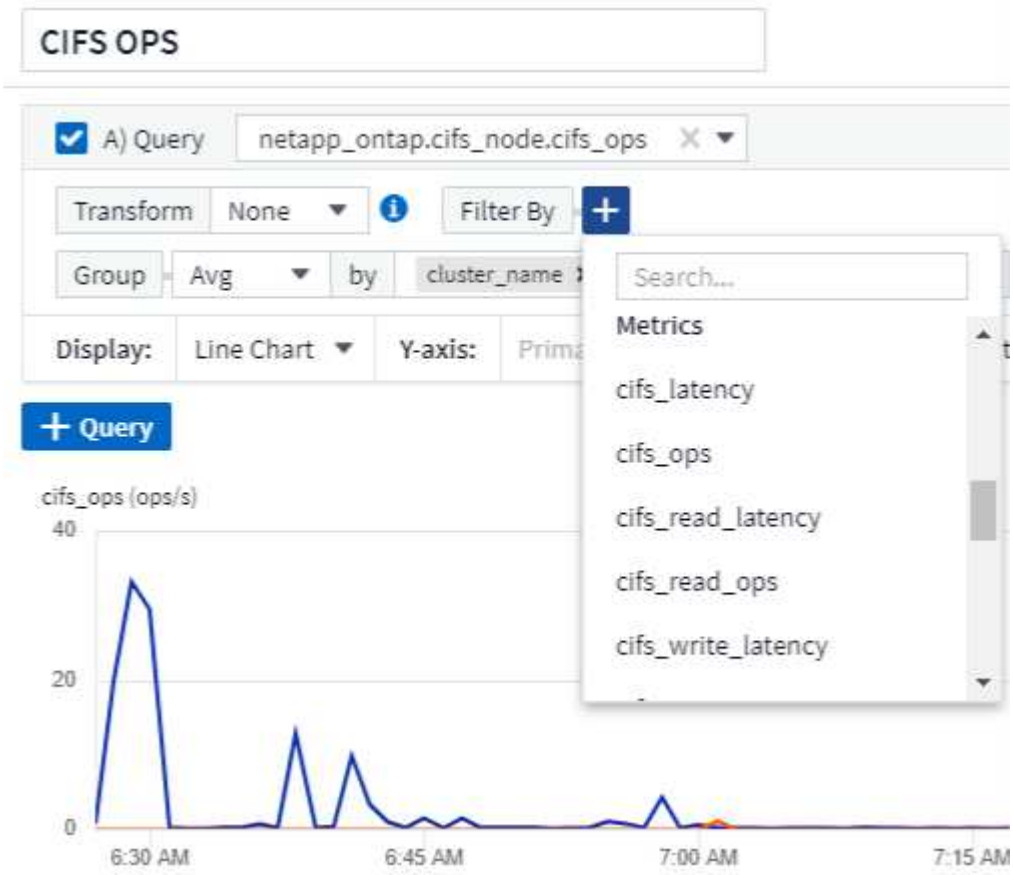
  インフラストラクチャ データによるグループ化 (表示モードで表示
  ):



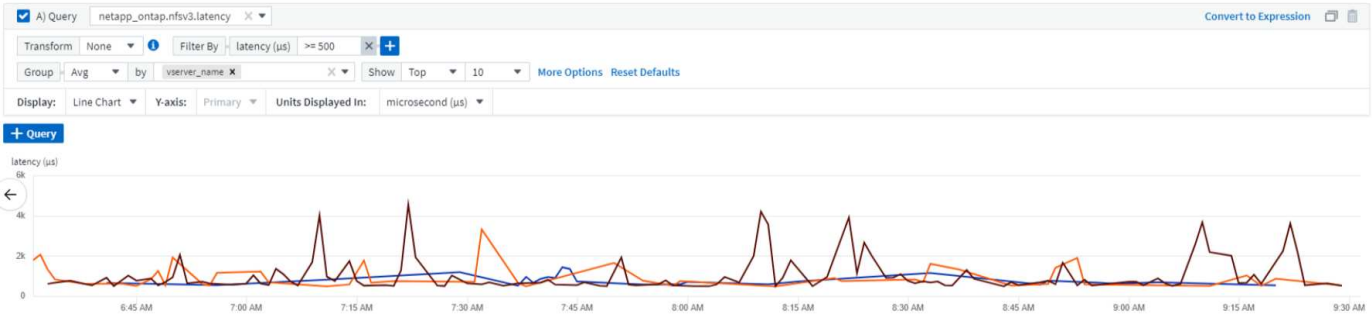
メトリクスフィルタリング

ウィジェット内のオブジェクトの属性に基づいてフィルタリングすることに加えて、メトリックに基づいてフ

ィルタリングすることもできるようになりました。



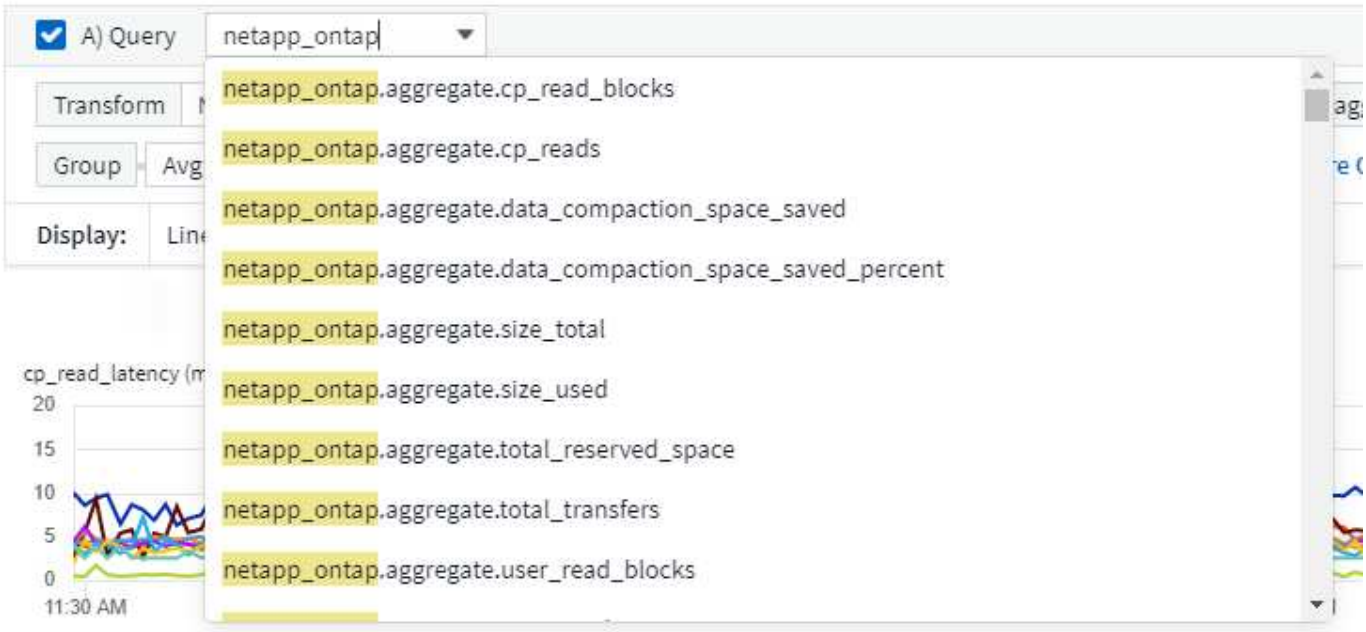
統合データ (Kubernetes、 ONTAP Advanced Data など) を操作する場合、メトリック フィルタリングによって、プロットされたデータ シリーズから個別のデータ ポイントや一致しないデータ ポイントが削除されます。これは、インフラストラクチャ データ (ストレージ、VM、ポートなど) の場合、フィルタがデータ シリーズの集計値に対して機能し、チャートからオブジェクト全体が削除される可能性があるのとは異なります。



ONTAP高度なカウンタデータ

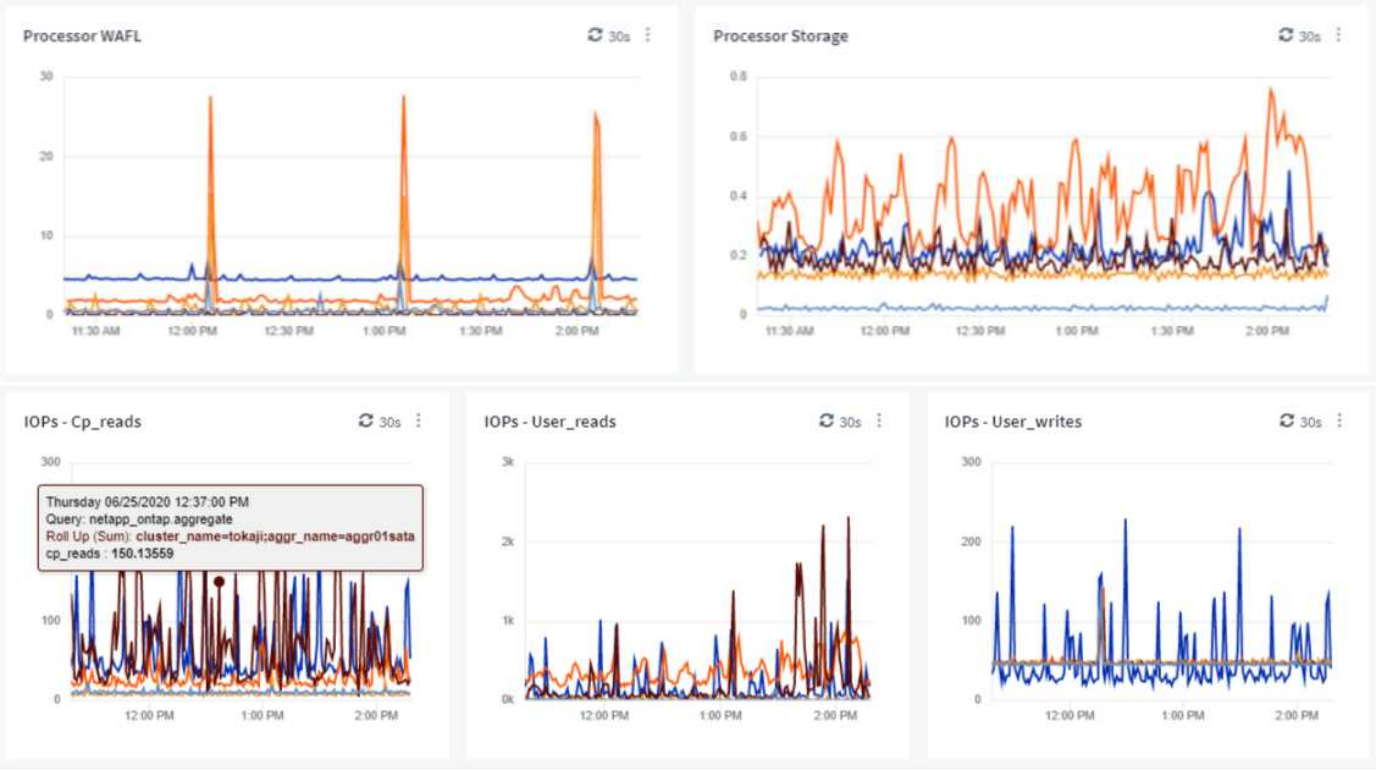
Cloud Insights は、 ONTAPデバイスから収集された多数のカウンターとメトリックを提供する、NetAppのONTAP固有の **Advanced Counter Data** を活用します。 ONTAP Advanced Counter Data は、すべてのNetApp ONTAP のお客様がご利用いただけます。これらのメトリックにより、Cloud Insightsウィジェットとダッシュボードでカスタマイズされた幅広い視覚化が可能になります。

ONTAPアドバンス カウンターは、ウィジェットのクエリで「netapp_ontap」を検索し、カウンターの中から選択することで見つかります。



カウンター名の追加部分を入力することで、検索を絞り込むことができます。例えば：

- *lif*
- 集計
- オフボックス_*vscan*_サーバー
- その他



以下の点にご注意ください。

- 新しいONTAPデータ コレクターでは、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 コレクターの高度なデータ収集を有効にするには、データ コレクターを編集し、[詳細構成] セクションを展開します。
- 高度なデータ収集は、7 モードONTAPでは使用できません。

高度なカウンターダッシュボード

Cloud Insights には、*Aggregate Performance*、*Volume Workload*、*Processor Activity* などのトピックに関するONTAP Advanced Counters の視覚化を開始できるように、さまざまな事前設計されたダッシュボードが付属しています。少なくとも 1 つのONTAPデータ コレクターが設定されている場合は、任意のダッシュボード リスト ページのダッシュボード ギャラリーからこれらをインポートできます。

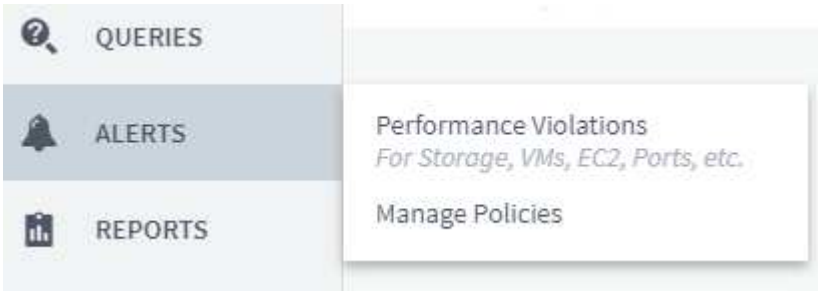
詳細情報

ONTAP Advanced Data 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: NetApp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 ポリシーと違反は、[アラート] メニューに表示されるようになりました。ポリシーと違反の機能は変更されていません。



更新された**Telegraf**エージェント

Telegraf統合データの取り込みエージェントが更新されました"version 1.14"これにはバグ修正、セキュリティ修正、新しいプラグインが含まれます。

注意: Kubernetes プラットフォームで Kubernetes データ コレクターを構成するときに、「clusterrole」属性の権限が不十分なため、ログに「HTTP ステータス 403 禁止」エラーが表示される場合があります。

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:* セクションに次の強調表示された行を追加し、Telegraf 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

簡素化されたデータコレクターエラーレポート

データ コレクターのエラーの報告は、データ コレクター ページの [エラー レポートの送信] ボタンを使用すると簡単になります。ボタンをクリックすると、エラーに関する基本情報がNetAppに送信され、問題の調査が促されます。押すと、 Cloud Insights はNetAppに通知されたことを認識し、エラー レポート ボタンが無効になり、そのデータ コレクターのエラー レポートが送信されたことが示されます。ブラウザ ページが更新されるまで、ボタンは無効のままになります。

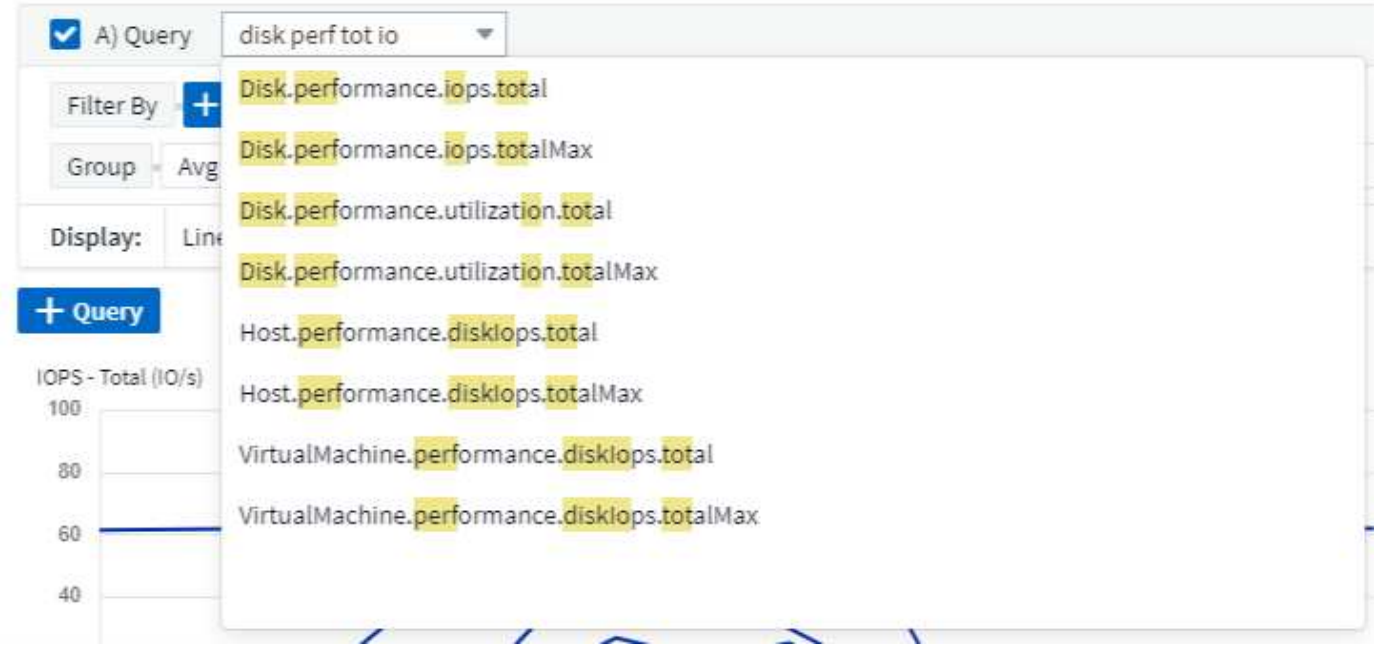


ウィジェットの改善

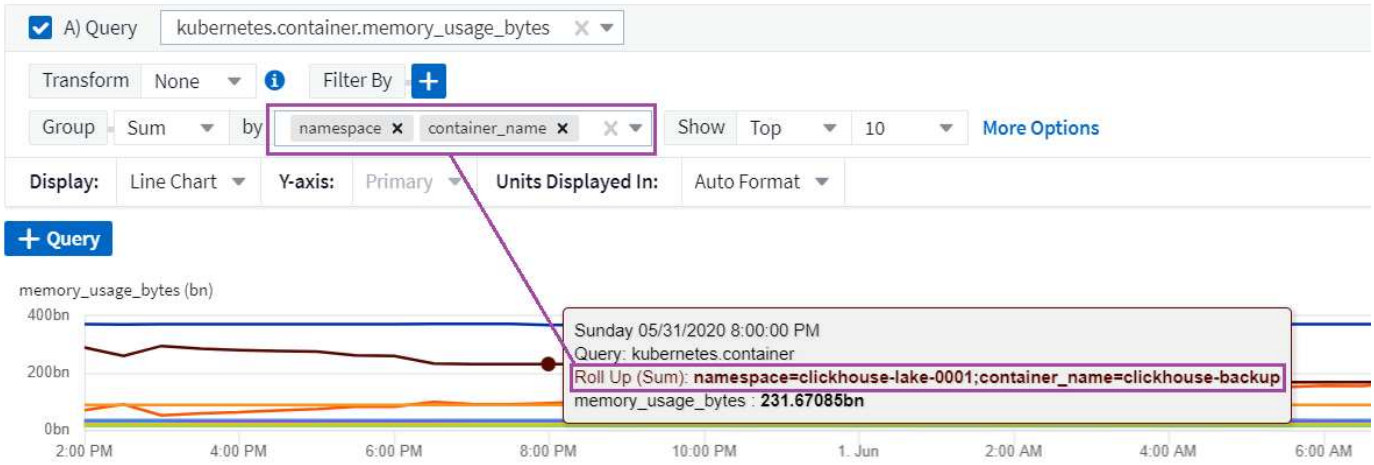
ダッシュボード ウィジェットに次の改善が加えられました。これらの改善はプレビュー機能とみなされており、すべてのCloud Insights環境で利用できるとは限りません。

- 新しいオブジェクト/メトリック選択: オブジェクト (ストレージ、ディスク、ポート、ノードなど) とそれに関連するメトリック (IOPS、レイテンシ、CPU 数など) が、強力な検索機能を備えた単一の包括的なドロップダウンのウィジェットで利用できるようになりました。ドロップダウンに複数の部分的な用語を入力すると、 Cloud Insights はそれらの用語に一致するすべてのオブジェクト メトリックを一覧表示しま

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 名前空間とコンテナ名によるメモリ使用量の合計などです。



2020年5月

ユーザーロールの報告

レポートに次のロールが追加されました:

- Cloud Insightsのコンシューマー: レポートの実行と表示が可能
- Cloud Insights Authors: 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および管理できます。

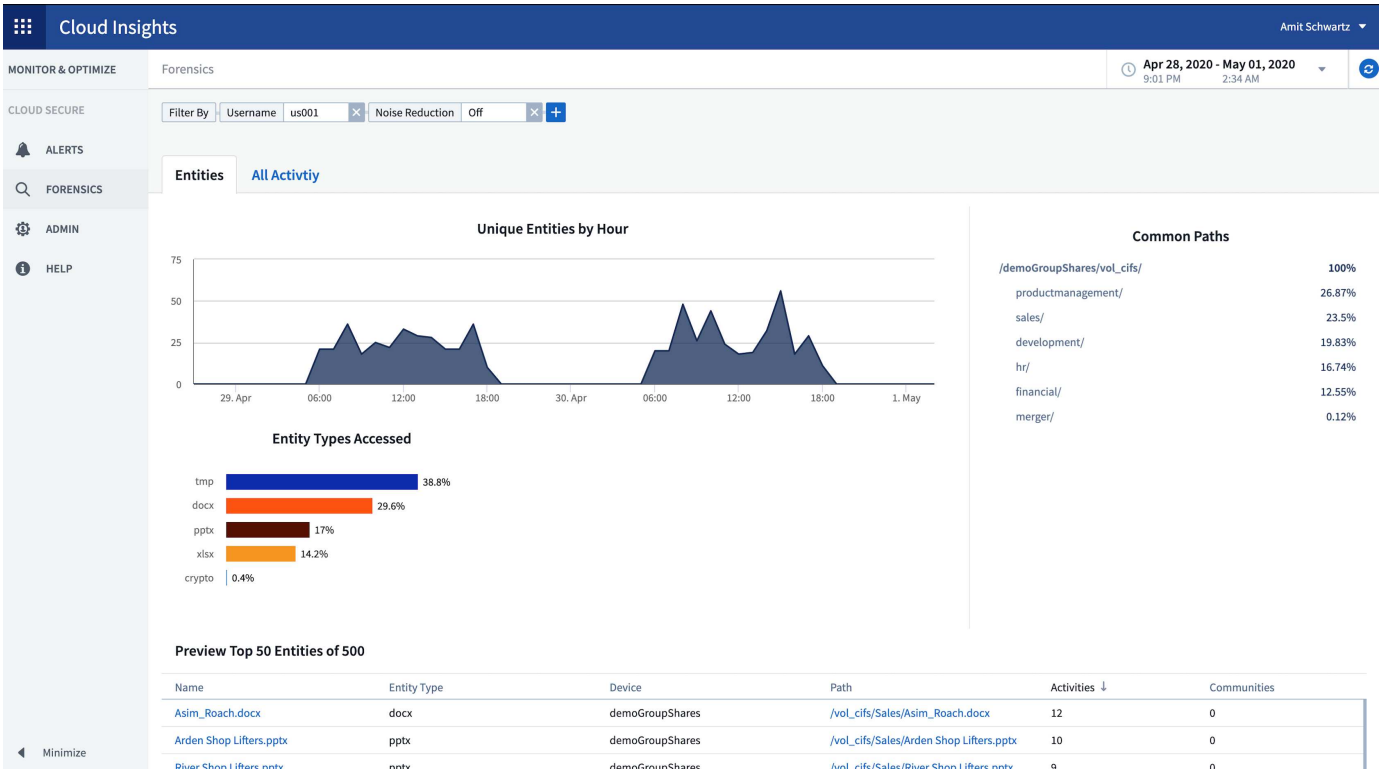
- Cloud Insights管理者: 作成者機能とすべての管理タスクを実行できます

Cloud Secureアップデート

Cloud Insightsには、次のような最近のCloud Secure の変更が含まれています。

「フォレンジック > アクティビティ フォレンジック」ページには、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 つのビューが用意されています。

- アクティビティ ビュー、ユーザー アクティビティに重点を置きます (どのような操作ですか?)どこで行われましたか?
- ユーザーがアクセスしたファイルに焦点を当てたエンティティ ビュー。

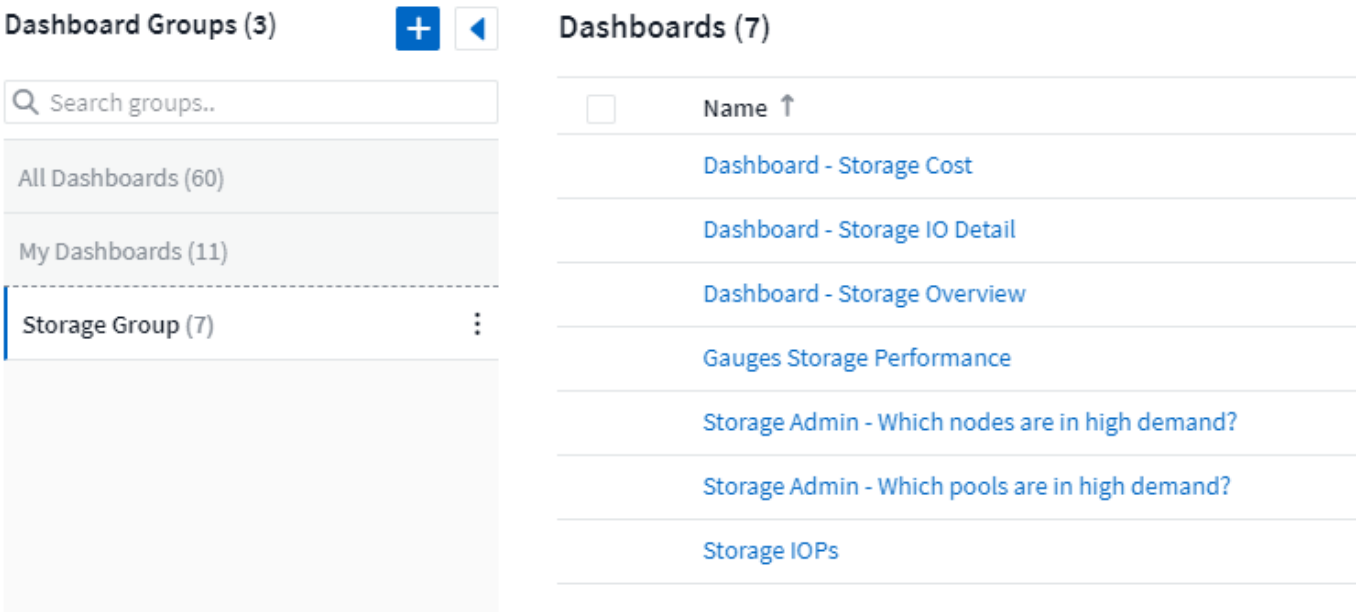


さらに、アラート電子メール通知にアラート ページへの直接リンクが含まれるようになりました。

ダッシュボードのグループ化

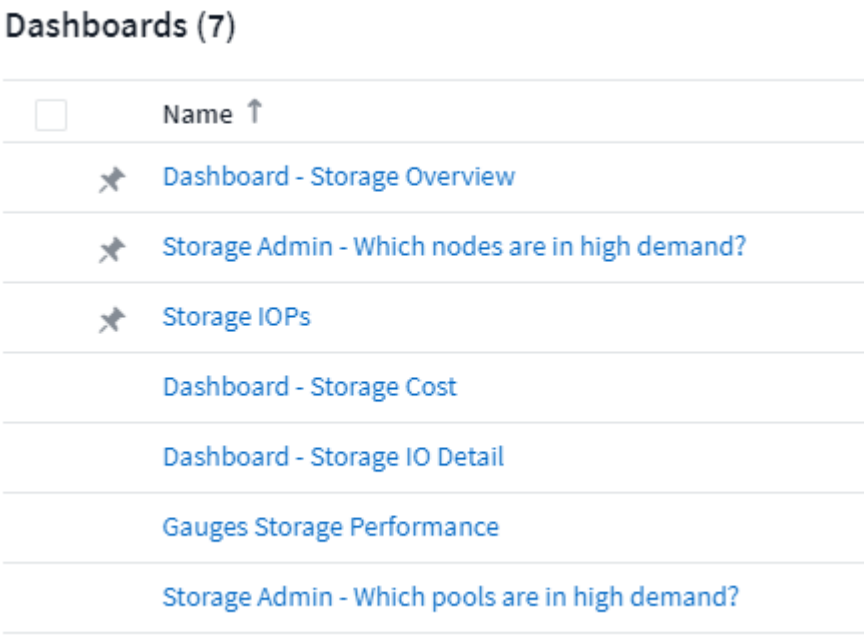
ダッシュボードのグループ化により、"ダッシュボードの管理"あなたにとって関連性のあるものです。関連するダッシュボードをグループに追加して、たとえばストレージや仮想マシンを「ワンストップ」で管理できます。

グループはユーザーごとにカスタマイズされるため、あるユーザーのグループは他のユーザーのグループと異なる場合があります。グループは必要なだけ作成でき、各グループ内のダッシュボードの数も必要なだけ増やすことができます。



ダッシュボードのピン留め

ダッシュボードをピン留めすると、お気に入りが常にリストの上部に表示されます。



TVモードと自動更新

"TVモードと自動更新"ダッシュボードまたはアセット ページでデータをほぼリアルタイムで表示できるようになります。

- **TV** モード では、すっきりとした表示が実現します。ナビゲーション メニューは非表示になり、データ表示用の画面領域が広がります。
- ダッシュボードとアセット ランディング ページ上のウィジェットのデータは、選択したダッシュボード

の時間範囲 (または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、ウィジェットの時間範囲) によって決まる更新間隔 (最短 10 秒ごと) に従って 自動更新 されます。

TV モードと自動更新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監視に最適です。

2020年4月

新しいダッシュボードの時間範囲の選択肢

ダッシュボードやその他の Cloud Insights ページの時間範囲の選択肢に、過去 *1* 時間 と 過去 *15* 分 が含まれるようになりました。

Cloud Secureアップデート

Cloud Insightsには、次のような最近のCloud Secure の変更が含まれています。

- ファイルとフォルダーのメタデータの変更認識が向上し、ユーザーが権限、所有者、またはグループの所有権を変更したかどうかを検出できるようになりました。
- ユーザー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、ファイルとフォルダーに対するすべてのユーザー アクセス操作を監視および監査します。アクティビティ監査により、社内のセキュリティ ポリシーに準拠し、PCI、GDPR、HIPAA などの外部コンプライアンス要件を満たし、データ侵害やセキュリティ インシデントの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時間範囲は、24 時間ではなく 3 時間になりました。

最適化された集約時間

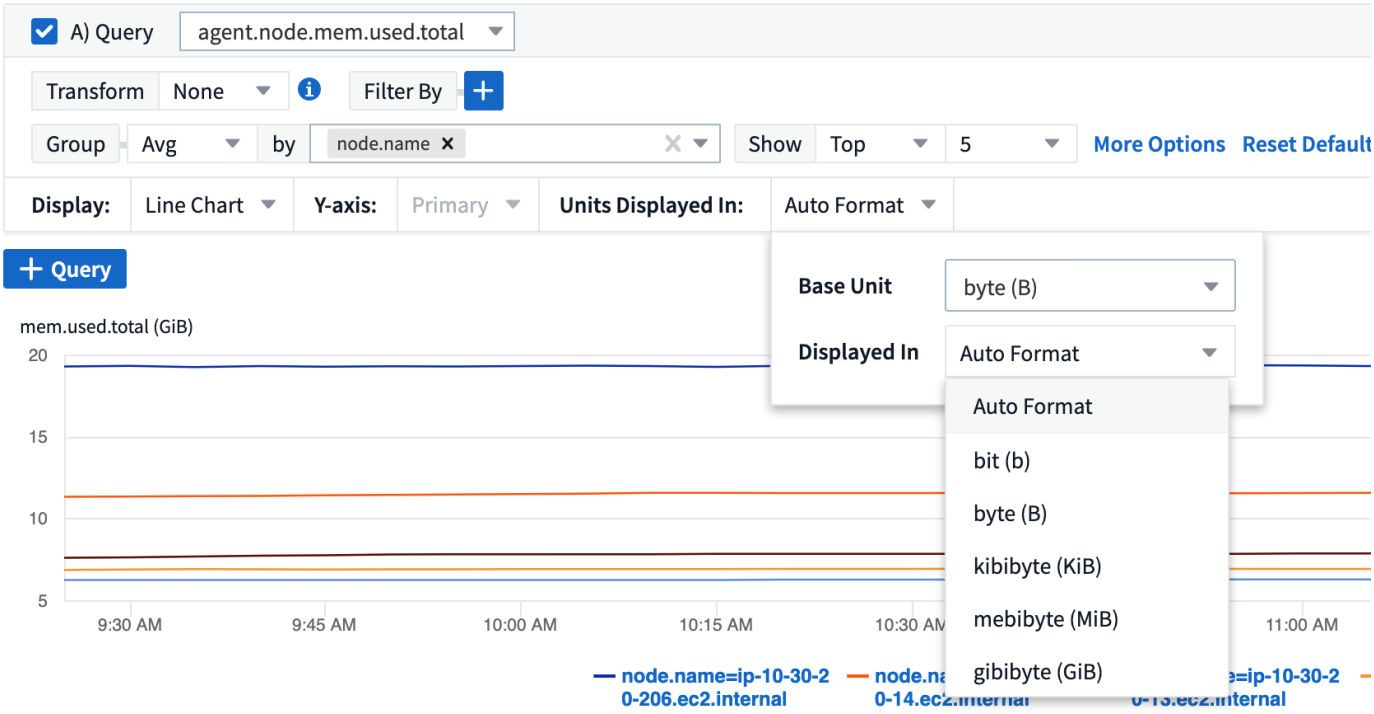
最適化"時間集約"時系列ウィジェット (折れ線グラフ、スプライン グラフ、面グラフ、積み上げ面グラフ) の間隔が 3 時間および 24 時間のダッシュボード/ウィジェットの時間範囲でより頻繁になり、データのグラフ化が高速化されます。

- 3 時間の時間範囲は 1 分の集約間隔に最適化されます。以前は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。

カスタム間隔を設定することで、最適化された集計をオーバーライドすることもできます。

表示単位の自動フォーマット

ほとんどのウィジェットでは、 Cloud Insightsは値を表示する基本単位（例えば、メガバイト、千、パーセント、_ミリ秒（ms）_など）を認識しており、"自動的にフォーマットする"ウィジェットを最も読みやすい単位にします。たとえば、1,234,567,890 バイトのデータ値は、1.23 ギビバイトに自動的にフォーマットされます。多くの場合、 Cloud Insights は取得されるデータに最適な形式を認識しています。最適な形式が不明な場合、または自動書式設定を上書きするウィジェットの場合は、必要な形式を選択できます。



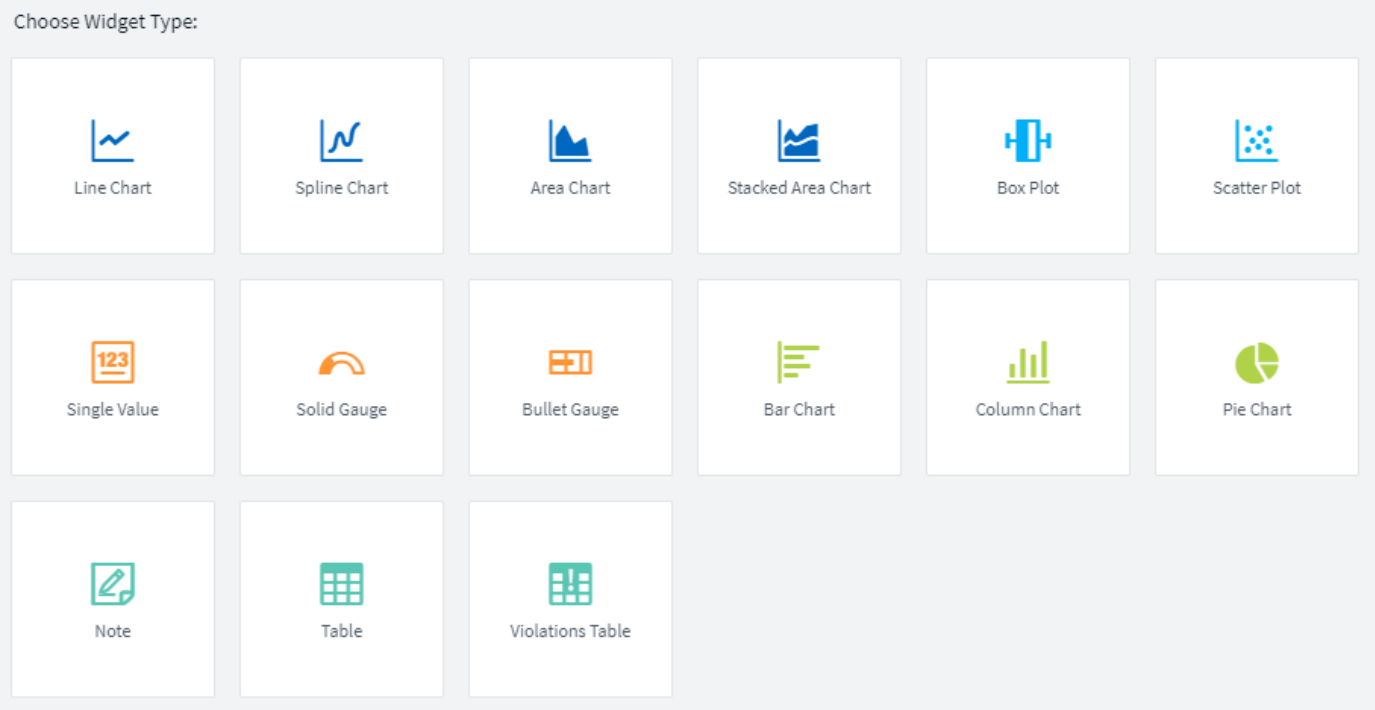
APIを使用して注釈をインポートする

Cloud Insights Premium Editionの強力なAPIを使用すると、"インポート注釈" .CSV ファイルを使用してオブジェクトに割り当てます。同様の方法でアプリケーションをインポートし、ビジネス エンティティを割り当てることもできます。



よりシンプルなウィジェットセレクター

ダッシュボードやアセットランディングページへのウィジェットの追加が、すべてのウィジェットタイプを一括表示できる新しいウィジェットセレクターによってさらに簡単になりました。ユーザーはウィジェットタイプのリストをスクロールして追加したいウィジェットを探す必要がなくなりました。新しいセレクターでは、関連ウィジェットが色分けされ、近接性に基づいてグループ化されています。



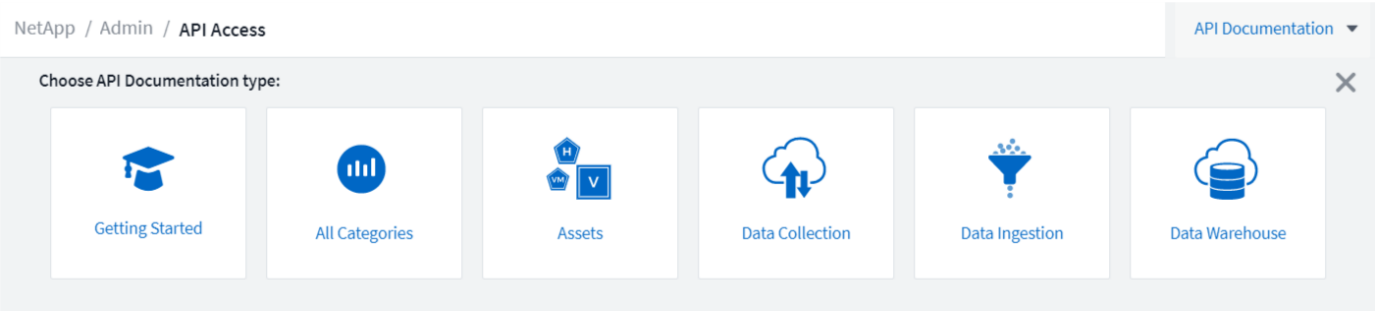
2020年2月

プレミアムエディションのAPI

Cloud Insights Premium Editionには、"強力なAPI" 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するために使用できます。

詳細な Swagger ベースの情報は、管理 **> API** アクセス の **API** ドキュメント リンクにあります。 Swagger は API の簡単な説明と使用方法の情報を提供するため、自分の環境で各 API を試すことができます。

Cloud Insights API は、アクセス トークンを使用して、ASSETS や COLLECTION などの API カテゴリへの権限ベースのアクセスを提供します。



データコレクター追加後の初期ポーリング

以前は、新しいデータ コレクターを構成すると、 Cloud Insights はデータ コレクターをすぐにポーリングして インベントリ データを収集していましたが、構成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、初期の パフォーマンス データを収集していました。その後、2 回目のパフォーマンス ポーリン

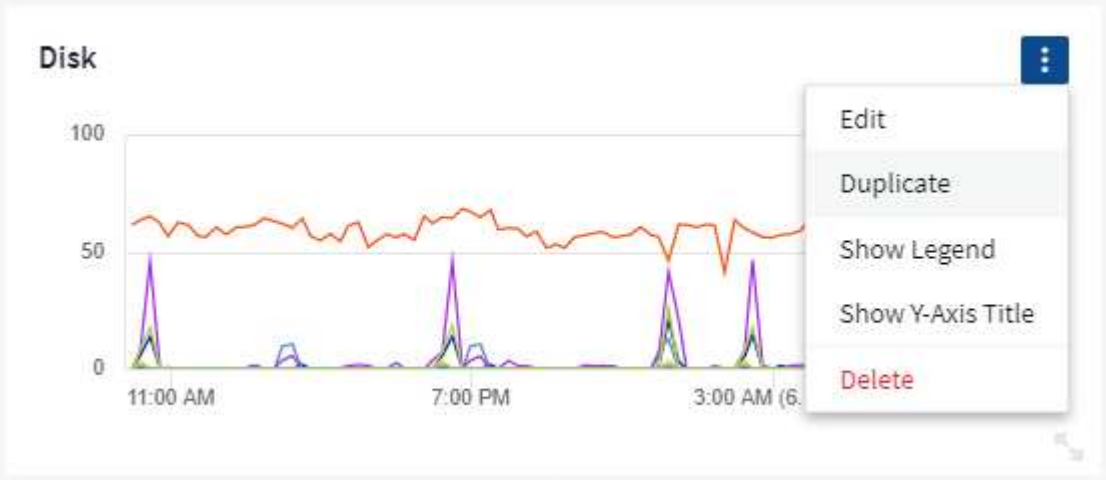
グを開始する前に別の間隔を待機するため、新しいデータ コレクターから意味のあるデータが取得されるまでに最大 30 分かかります。

データ収集者"投票"大幅に改善され、最初のパフォーマンス ポーリングはインベントリ ポーリングの直後に実行され、2 番目のパフォーマンス ポーリングは最初のパフォーマンス ポーリングの完了後数秒以内に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を表示できるようになります。

このポーリング動作は、既存のデータ コレクターの構成を編集した後にも発生します。

ウィジェットの複製が簡単に

ダッシュボードやランディング ページでウィジェットのコピーを作成するのがこれまで以上に簡単になりました。ダッシュボードの編集モードで、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 エディターが起動し、元のウィジェットの構成が事前に入力され、ウィジェット名に「コピー」サフィックスが付きます。必要な変更を簡単に行い、新しいウィジェットを保存できます。ウィジェットはダッシュボードの下部に配置され、必要に応じて配置できます。すべての変更が完了したら、ダッシュボードを必ず保存してください。



シングルサインオン（SSO）

Cloud Insights Premium Editionでは、管理者は*"シングルサインオン" * 企業ドメイン内のすべてのユーザーが、個別に招待することなくCloud Insightsに (SSO) アクセスできるようになります。 SSO を有効にすると、同じドメインのメール アドレスを持つすべてのユーザーが、企業の認証情報を使用してCloud Insightsにログインできるようになります。

SSO はCloud Insights Premium Edition でのみ使用可能であり、 Cloud Insightsで有効にする前に構成する必要があります。 SSO設定には以下が含まれます"アイデンティティ フェデレーション"NetApp Cloud Central を通じて。フェデレーションにより、シングル サインオン ユーザーは、企業ディレクトリの資格情報を使用してNetApp Cloud Central アカウントにアクセスできるようになります。

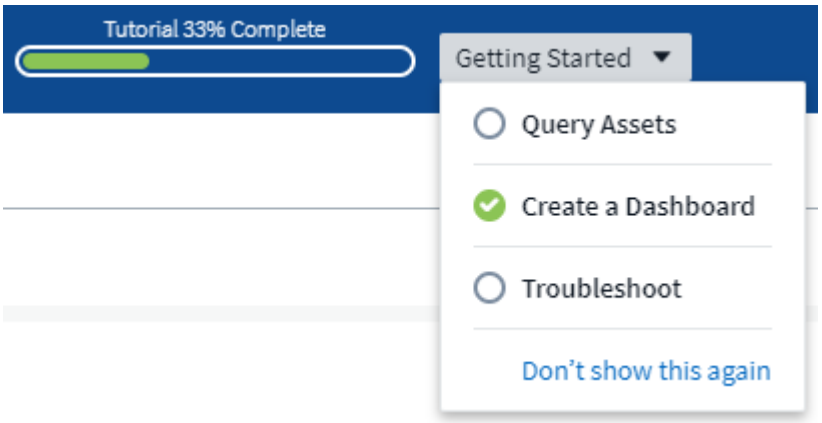
2020年1月

REST API の Swagger ドキュメント

Swagger では、 Cloud Insightsで利用可能な各 REST API と、その使用方法および構文について説明します。Cloud Insights APIに関する情報は、"ドキュメント"。

機能チュートリアルの進捗バー

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、進行状況インジケーターが追加されました。チュートリアルは、終了するまで各ユーザーが利用でき、 Cloud Insightsでいつでも利用できます。"ドキュメント"。



取得ユニットの変更

すでにインストールされている AU と同じ名前の Acquisition Unit (AU) をホストまたは VM にインストールする場合、 Cloud Insights はAU 名に「_1」、「_2」などを追加して一意の名前を保証します。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。まったく別の AU 名をご希望ですか? 問題ありません。AU はインストール後に名前を変更できます。

ウィジェットにおける時間集計の最適化

ウィジェットでは、_最適化された_時間集約間隔または設定した_カスタム_間隔を選択できます。最適化された集計では、選択したダッシュボードの時間範囲 (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。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、間隔は動的に変化します。

簡素化された「 Cloud Insightsを使い始める」プロセス

Cloud Insightsの使用を開始するためのプロセスが簡素化され、初回のセットアップがよりスムーズかつ簡単になりました。最初のデータコレクターを選択して、指示に従うだけです。 Cloud Insights、データ コレクターと、必要なエージェントまたは取得ユニットの構成手順を説明します。ほとんどの場合、1 つ以上の初期ダッシュボードがインポートされるため、環境の状況をすぐに把握できるようになります (ただし、 Cloud Insights が意味のあるデータを収集するまでに最大 30 分かかる場合があります)。

追加の改善点:

- 取得ユニットのインストールがより簡単になり、実行速度も速くなります。
- アルファベット順のデータ コレクターの選択肢により、探しているデータ コレクターを簡単に見つけることができます。
- 改善されたデータ コレクターのセットアップ手順がわかりやすくなりました。
- 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スキップできます。
- 新しい進行状況バーに、プロセスの進行状況が表示されます。



Data Infrastructure Insightsインサイトオンボーディング

Data Infrastructure Insightsでの作業を開始する前に、NetApp Consoleポータルでサインアップする必要があります。すでにNetApp Consoleのログインをお持ちの場合は、いくつかの簡単な手順でData Infrastructure Insightsの無料トライアルを開始できます。

NetApp Console アカウントの作成

NetAppのクラウドサービスを開始するには、"* NetApp Console*"にアクセスして*開始*をクリックします。

- まだサインアップしていない場合は、*Sign Up*を選択してください
- 有効なビジネス用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てください。
- 利用規約に同意して、**Continue** を選択します。
- Console では、開始ワークフローを案内します。

すでに**NetApp Console**ログインをお持ちの場合はどうすればよいですか？

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

画面上部のドロップダウンから組織を選択します。

DII サイトは、選択した Console Organization に関連付けられます。組織が複数ある場合は、DII テナントに関連付ける適切な組織を選択してください。

左上のメインメニューから、*ガバナンス > Data Infrastructure Insights*を選択します。

Data Infrastructure Insights無料トライアルを開始する

開始する準備ができたら、*30 日間の無料トライアルを開始*を選択します。サイトをホストする地域を選択し、その他の指示に従います。

DII サイトを作成するには、「Org Admin」ロールが必要であることに注意してください。

コンソールは、Data Infrastructure Insights（DII）サイトのオンボーディング準備が完了したことを通知します。*オンボーディングを開始*ボタンを選択してサイトをセットアップします。

オンボーディングプロセスが完了する前に中断した場合は、Consoleに再度ログインして*オンボーディングを完了*してください。

オンボーディングが完了すると、コンソールにテナントの使用準備が完了したことが通知されます。*Data Infrastructure Insightsの起動*を選択して開始します。一部のデータ（インベントリなど）はすぐに使用できますが、他のデータ（パフォーマンス監視など）は意味のあるものにするために取得に時間がかかる場合があります。

ログアウト

Data Infrastructure Insightsからログアウトするには、*ユーザー名*をクリックし、*ログアウト*を選択します。

Data Infrastructure Insightsからログアウトすると、コンソールからログアウトされます。コンソール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

デフォルトでは、Consoleは6時間（360分）にわたってアクティビティがない場合にユーザーをログアウトします。アクティビティに関係なく、ユーザーは7日後にログアウトされます。

セキュリティ

Data Infrastructure Insightsセキュリティ

NetAppでは、製品と顧客データのセキュリティが最も重要です。 Data Infrastructure Insights は、リリース ライフサイクル全体にわたってセキュリティのベスト プラクティスに従い、顧客情報とデータが可能な限り最善の方法で保護されるようにします。

セキュリティの概要

物理的なセキュリティ

Data Infrastructure Insights の運用インフラストラクチャは、Amazon Web Services (AWS) でホストされています。建物やドアに使用されるロックやキーを含む、 Data Infrastructure Insights実稼働サーバーの物理的および環境的なセキュリティ関連の制御は、AWS によって管理されます。 AWS によると、「物理的なアクセスは、ビデオ監視、侵入検知システム、その他の電子手段を利用する専門のセキュリティ スタッフによって、境界と建物の入口の両方で制御されます。」権限のあるスタッフは、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 によって説明されています。

製品セキュリティ

Data Infrastructure Insights は、アジャイル原則に沿った開発ライフサイクルに従うため、リリース サイクルが長い開発方法論と比較して、セキュリティ重視のソフトウェア欠陥に迅速に対処できます。継続的インテグレーション手法を使用することで、機能とセキュリティの両方の変更に迅速に対応できます。変更管理の手順とポリシーは、変更がいつどのように発生するかを定義し、運用環境の安定性を維持するのに役立ちます。影響のある変更は、実稼働環境にリリースされる前に正式に伝達、調整され、適切にレビューされ、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、そのリソースが機能を実行するために必要なポートのみに受信トラフィックを制限するホストベースのファイアウォールがあります。

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

リスクアセスメント

Data Infrastructure Insightsチームは、形式化されたリスク評価プロセスに従って、リスクを識別および評価するための体系的かつ反復可能な方法を提供し、リスク処理計画を通じてリスクを適切に管理できるようにします。

データ保護

Data Infrastructure Insights の運用環境は、すべてのサービスとコンポーネントに複数の可用性ゾーンを利用する、高度に冗長化されたインフラストラクチャ内にセットアップされています。可用性が高く冗長性のある

コンピューティング インフラストラクチャを活用するとともに、重要なデータは定期的にバックアップされ、復元は定期的にテストされます。正式なバックアップ ポリシーと手順により、ビジネス活動の中断の影響が最小限に抑えられ、情報システムの障害や災害の影響からビジネス プロセスが保護され、タイムリーかつ適切に再開されることが保証されます。

認証とアクセス管理

Data Infrastructure Insightsへのすべての顧客アクセスは、https 経由のブラウザ UI 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。 NetApp は、これをすべてのクラウド データ サービスの認証レイヤーとして一元化しています。

Data Infrastructure Insights は、 Data Infrastructure Insights の運用環境への論理アクセスに関する「最小権限」や「ロールベースのアクセス制御」などの業界のベスト プラクティスに従います。アクセスは厳密に必要に応じて制御され、多要素認証メカニズムを使用して、承認された特定の担当者にのみ許可されます。

顧客データの収集と保護

すべての顧客データは、パブリック ネットワーク経由での転送中および保存時に暗号化されます。 Data Infrastructure Insights は、システムのさまざまなポイントで暗号化を活用し、トランスポート層セキュリティ (TLS) や業界標準の AES-256 アルゴリズムなどのテクノロジーを使用して顧客データを保護します。

顧客のプロビジョニング解除

サブスクリプションの有効期限が近づいていることを顧客に通知するために、さまざまな間隔で電子メール通知が送信されます。サブスクリプションの有効期限が切れると、UI が制限され、データ収集の猶予期間が始まります。その後、顧客に電子メールで通知されます。試用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。猶予期間が過ぎると、2 日以内にアカウントが削除されることが電子メールで顧客に通知されます。有料のお客様は、サービスの利用停止を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および関連するすべての顧客データは、猶予期間の終了時、または顧客からのアカウント終了要求の確認時に、Data Infrastructure Insightsサイト オペレーション (SRE) チームによって削除されます。どちらの場合でも、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 呼び出しにより、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。顧客の削除は、同じ API を呼び出して、顧客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によって検証されます。

セキュリティインシデント管理

Data Infrastructure Insights は、既知の脆弱性を発見、評価、解決するために、NetApp の製品セキュリティ インシデント レスポンス チーム (PSIRT) プロセスと統合されています。 PSIRT は、顧客レポート、社内エンジニアリング、CVE データベースなどの広く認知されているソースを含む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 チームによって問題が検出された場合、チームは PSIRT プロセスを開始し、問題を評価し、場合によっては修復します。

また、 Data Infrastructure Insights の顧客または研究者が、 Data Infrastructure Insights製品のセキュリティ問題を特定し、その問題をテクニカル 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可能性もあります。このような場合、Data Infrastructure Insightsチームは PSIRT プロセスを開始し、問題を評価し、場合によっては修復します。

脆弱性と侵入テスト

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のテストを実行します。

セキュリティ意識向上トレーニング

すべてのData Infrastructure Insights従業員は、それぞれの役割に合わせて開発されたセキュリティ トレーニングを受け、各従業員が自分の役割に特有のセキュリティ重視の課題に対処できるようにしています。

コンプライアンス

Data Infrastructure Insights は、 SOC 2 監査の完了を含め、セキュリティ、プロセス、サービスについて、外部の認定 CPA 事務所による独立したサードパーティ監査と検証を実行します。

NetAppセキュリティアドバイザリ

NetAppのセキュリティアドバイザリは以下からご覧いただけます。"ここをクリックしてください。" 。

情報と地域

NetApp は顧客情報のセキュリティを非常に重視しています。 Data Infrastructure Insights が情報を保存する方法と場所は次のとおりです。

Data Infrastructure Insights はどのような情報を保存しますか?

Data Infrastructure Insightsには次の情報が保存されます。

- 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データです。これには、たとえば、ストレージ システムによって配信される IO の数、ファイバーチャネル ポートのスループット、Web サーバー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が含まれます。

- 在庫データ

  インベントリ データは、監視対象のデバイス/ソースとその構成方法を記述するメタデータで構成されます。これには、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、仮想マシンの RAM とディスク、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/ファイル名 (ストレージ ワークロード セキュリティが有効な場合) などが含まれます。

- 構成データ

  これは、監視対象デバイスのホスト名または IP アドレス、ポーリング間隔、タイムアウト値など、顧客のインベントリと操作を管理するために使用される顧客提供の構成データを要約したものです。

- 秘密

  シークレットは、Data Infrastructure Insights取得ユニットが顧客のデバイスやサービスにアクセスするた

めに使用する資格情報で構成されます。これらの資格情報は強力な非対称暗号化を使用して暗号化され、秘密鍵は取得ユニットにのみ保存され、顧客環境から外に出ることはありません。この設計により、特権を持つData Infrastructure Insights SRE であっても、プレーンテキストで顧客の秘密にアクセスすることはできません。

- 機能データ

  これは、 NetApp がクラウド データ サービスを提供した結果として生成されるデータであり、 NetApp にクラウド データ サービスの開発、導入、運用、保守、セキュリティ保護に関する情報を提供します。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 Consoleが地域の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 (ユーザー認証に関連するデータを含む)。

- ストレージワークロードセキュリティユーザーディレクトリデータ

  Workload Security 機能が有効になっていて、顧客がユーザー ディレクトリ コレクターを有効にすることを選択した場合、システムはユーザーの表示名、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を保存します。

> ユーザー ディレクトリ データとは、Workload Security ユーザー ディレクトリ データ コレクターによって収集されたユーザー ディレクトリ情報を指し、 Data Infrastructure Insights/Workload Security のユーザー自体に関するデータではありません。

*明示的な個人データは*インフラストラクチャおよびサービス リソースから収集されません。収集される情報は、 NetApp自動サポートや ActiveIQ などの多くのベンダーの電話サービスと同様に、パフォーマンス メトリック、構成情報、インフラストラクチャ メタデータのみで構成されます。ただし、顧客の命名規則によっては、共有、ボリューム、VM、qtree、アプリケーションなどのデータに個人を特定できる情報が含まれる場合があります。

Workload Security が有効になっている場合、システムは個人を特定できる情報が含まれている可能性のある 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も確認します。お客様が Workload Security User Directory Collector (基本的には Active Directory を通じて Windows SID をユーザー名にマッピングします) を有効にすると、表示名、会社の電子メール アドレス、および選択された追加属性が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 ログが保持され、サービスへのログインに使用されたユーザーの IP アドレスと電子メール アドレスが含まれます。

私の情報はどこに保存されますか?

Data Infrastructure Insights は、環境が作成されたリージョンに応じて情報を保存します。

ホスト領域には次の情報が保存されます。

- カウンターやパフォーマンス メトリックを含むテレメトリと資産/オブジェクト情報
- 取得ユニット情報
- 機能データ

- Data Infrastructure Insights内のユーザーアクティビティに関する監査情報
- ワークロードセキュリティ Active Directory 情報
- ワークロードセキュリティ監査情報

次の情報は、 Data Infrastructure Insights環境をホストしている地域に関係なく、米国にあります。

- サイト/アカウント所有者などの環境サイト (「テナント」と呼ばれることもあります) の情報。
- NetApp Consoleが地域のData Infrastructure Insightsサイトと通信できるようにする情報 (ユーザー認証に関連するものを含む)。
- Data Infrastructure Insightsユーザーとテナント間の関係に関する情報。

ホスト地域

ホスト地域は次のとおりです:

- 米国: us-east-1
- EMEA: eu-central-1
- APAC: ap-southeast-2

詳細情報

NetApp のプライバシーとセキュリティの詳細については、次のリンクをご覧ください。

- "信頼センター"
- "国境を越えたデータ転送"
- "拘束的企業準則"
- "サードパーティのデータ要求への対応"
- "NetAppプライバシー原則"

セキュリティ管理ツール

Data Infrastructure Insightsには、環境を強化されたセキュリティで運用できるようにするセキュリティ機能が含まれています。機能には、暗号化、パスワード ハッシュの改善、内部ユーザー パスワードの変更機能、およびパスワードを暗号化および復号化するキー ペアの変更機能が含まれます。

機密データを保護するために、 NetApp、インストールまたはアップグレード後にデフォルトのキーと *Acquisition* ユーザー パスワードを変更することをお勧めします。

データ ソースの暗号化されたパスワードはData Infrastructure Insightsに保存され、ユーザーがデータ コレクター構成ページでパスワードを入力すると、公開キー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 コレクターのパスワードを復号化するために必要な秘密キーがありません。データ コレクターのパスワードを復号化するために必要なデータ コレクターの秘密キーを持っているのは、Acquisition Unit (AU) 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構成が含まれている場合 (つまり、パスワードのキーを変更した場合)、セキュリティ構成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したり、場合によってはソフトウェアをアップグレードしたりすると、システムはデフォルトのセキュリティ構成に戻ります。システムをデフォルト構成に戻す場合、システムが正しく動作するために、デフォルト以外の構成を復元する必要があります。

買収部門のセキュリティ管理

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、取得ユニット システムで実行されます。セキュリティ管理には、キーとパスワードの管理、作成したセキュリティ構成の保存と復元、構成をデフォルト設定に復元することが含まれます。

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。
- 後で 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ーがいる場合は、そのユーザーを *cisys* グループに追加する必要があります。 *cisys* グループは AU インストール中に作成されます。

AU のインストール後、SecurityAdmin ツールは取得ユニット システムの次のいずれかの場所にあります。

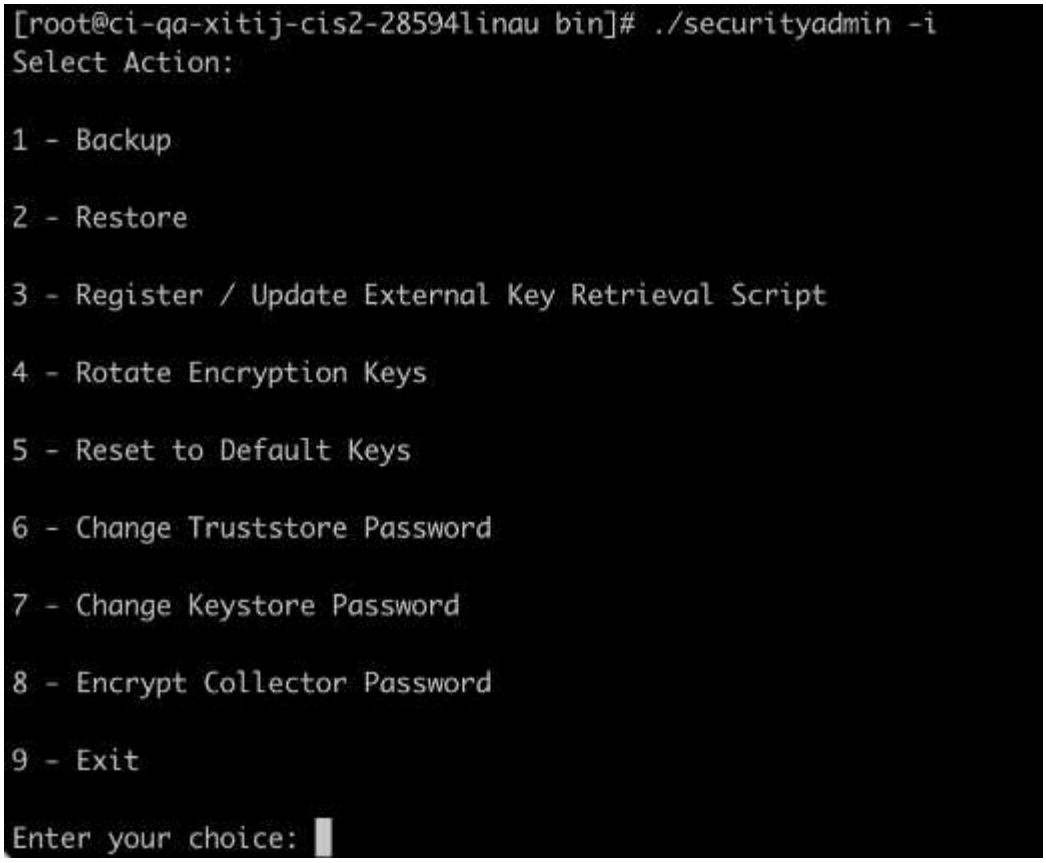
```
Windows - <install_path>\Cloud Insights\Acquisition
Unit\acq\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

SecurityAdminツールの使用

SecurityAdmin ツールを対話モード (-i) で起動します。

ログに記録される可能性のある秘密をコマンド ラインで渡すことを避けるため、SecurityAdmin ツールを対話型モードで使用することをお勧めします。

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を含む Vault のバックアップ zip ファイルを作成し、そのファイルをユーザーが指定した場所、または次のデフォルトの場所に配置します。

   ```
   Windows - <install_path>\Cloud Insights\Acquisition
   Unit\acq\securityadmin\backup\vault
   Linux - /var/log/netapp/oci/backup/vault
   ```

   ボ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お勧めします。

2. 復元する

   作成されたボールトの zip バックアップを復元します。復元されると、すべてのパスワードとキーはバックアップ作成時の値に戻ります。

   復元を使用すると、複数のサーバー上のパスワードとキーを同期できます。たとえば、次の手順に従います。1) AU の暗号化キーを変更します。 2) ボールトのバックアップを作成します。 3) 各 AU に Vault バックアップを復元します。

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、デバイスのパスワードを暗号化または復号化するために使用される AU 暗号化キーを登録または変更します。

   暗号化キーを変更する場合は、アップグレードまたはインストール後に復元できるように、新しいセキュ

リティ構成をバックアップする必要があります。

このオプションは Linux でのみ使用可能であることに注意してください。

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、最小 2048 ビットの 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してはなりません。
- スクリプトは、生のエンコードされたコンテンツ (PEM 形式のみ) を返す必要があります。
- 外部スクリプトには *execute* 権限が必要です。

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 (現在のキーを登録解除し、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、公開キー ID と秘密キー 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

   取得ユーザーのパスワードと取得ユーザー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提供される値です。

6. **Truststore**のパスワードを変更する

   トラストストアのパスワードを変更します。

7. キーストアのパスワードを変更する

   キーストアのパスワードを変更します。

8. コレクターパスワードの暗号化

   データ コレクターのパスワードを暗号化します。

9. 出口

   SecurityAdmin ツールを終了します。

設定するオプションを選択し、プロンプトに従います。

ツールを実行するユーザーを指定する

制御されたセキュリティ重視の環境の場合は、*cisys* グループがなくても、特定のユーザーに SecurityAdmin ツールを実行させたい場合があります。

これを実現するには、AU ソフトウェアを手動でインストールし、アクセスを許可するユーザー/グループを指定します。

- API を使用して、CI インストーラーを AU システムにダウンロードし、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 ドキュメント (*Admin* > *API Access* で *API Documentation* リンクを選択) を参照し、*GET /au/oneTimeToken* API セクションを見つけます。

◦ 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ー 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) とインストーラー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ー ファイルを AU システムにコピーし、解凍します。
- ファイルが含まれているフォルダに移動し、ユーザーとグループを指定して、インストーラをルートとして実行します。

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

指定されたユーザー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。

プロキシの更新または削除

SecurityAdmin ツールを *-pr* パラメータ付きで実行することで、取得ユニットのプロキシ情報を設定または削除できます。

```
[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
```

コマンドを実行した後、取得ユニットを再起動する必要があります。

プロキシを更新するには、コマンドは

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

外部キーの取得

UNIX シェル スクリプトを提供すると、取得ユニットによってそのスクリプトが実行され、キー管理システム

から 秘密キー と 公開キー 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。 キー タイプは「公開」または「秘密」のいずれかです。キー タイプが「public」の場合、スクリプトは公開キーを返す必要があります。キー タイプが「private」の場合、秘密キーを返す必要があります。

キーを取得ユニットに送り返すには、スクリプトでキーを標準出力に出力する必要があります。スクリプトはキーのみを標準出力に出力する必要があります。他のテキストを標準出力に出力してはなりません。要求されたキーが標準出力に印刷されると、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 ツールを使用して取得ユニットに登録する必要があります。これにより、取得ユニットとともにスクリプトが実行されます。スクリプトには、ルートおよび「cisys」ユーザーに対する *read* および *execute* 権限が必要です。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 スクリプトを取得ユニット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されるキー識別子。
入力パラメータ: キータイプ	公立か私立か。
出力	要求されたキーは標準出力に印刷する必要があります。現在、2048 ビットの RSA キーがサポートされています。キーは以下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	成功した場合の終了コードはゼロです。その他の終了値はすべて失敗とみなされます。
スクリプト権限	スクリプトには、ルートおよび「cisys」ユーザーの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ログに記録されます。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 を使用すると、パスワードを暗号化して、API 経由でデータ コレクターに渡すことができます。

SecurityAdmin ツールを対話モードで起動し、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を入力するよう求められます。入力した文字は画面に表示されないことに注意してください。プロンプトが表示されたらパスワードを再入力します。

あるいは、スクリプト内でコマンドを使用する場合は、コマンド ラインで *securityadmin.sh* を "-enc" パラメ

ータとともに使用し、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

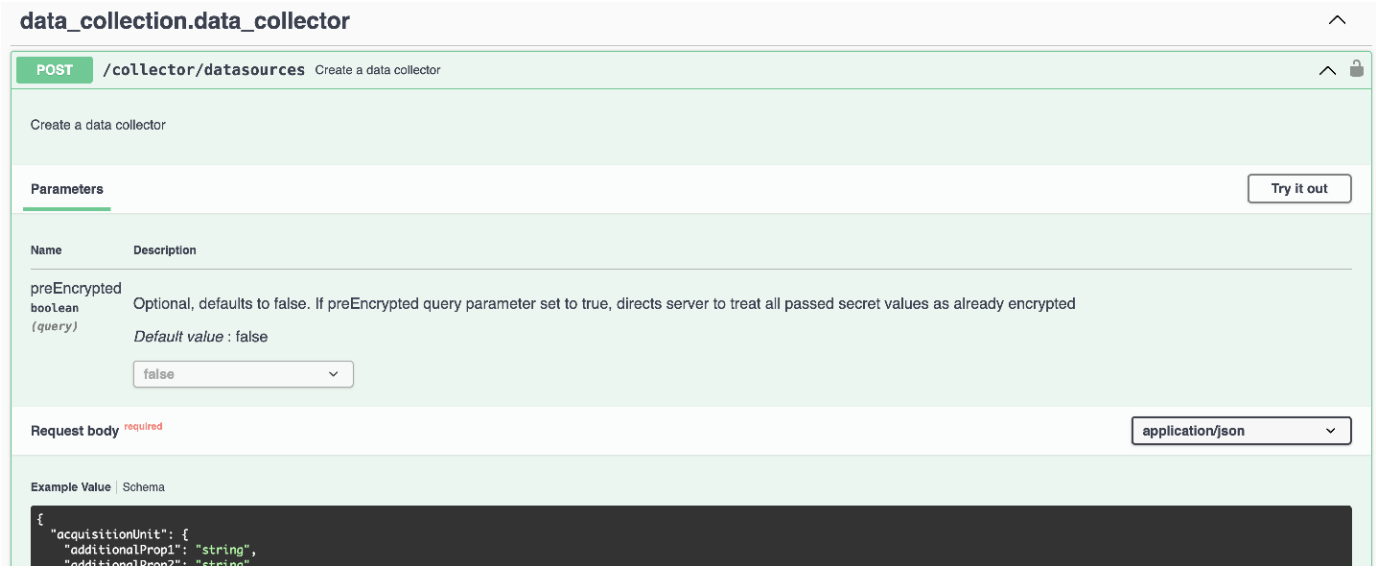
9 - Exit

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 コレクターに送信するには、Data Collection API を使用できます。この API の Swagger は、管理 **> API** アクセス で「API ドキュメント」リンクをクリックすると見つかります。 「データ収集」API タイプを選択します。この例では、*data_collection.data_collector* の見出しの下で、*/collector/datasources* POST API を選択します。



preEncrypted オプションを *True* に設定すると、API コマンドを通じて渡すパスワードは すでに暗号化されている ものとして扱われ、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、以前に暗号化し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"
  }
}
```

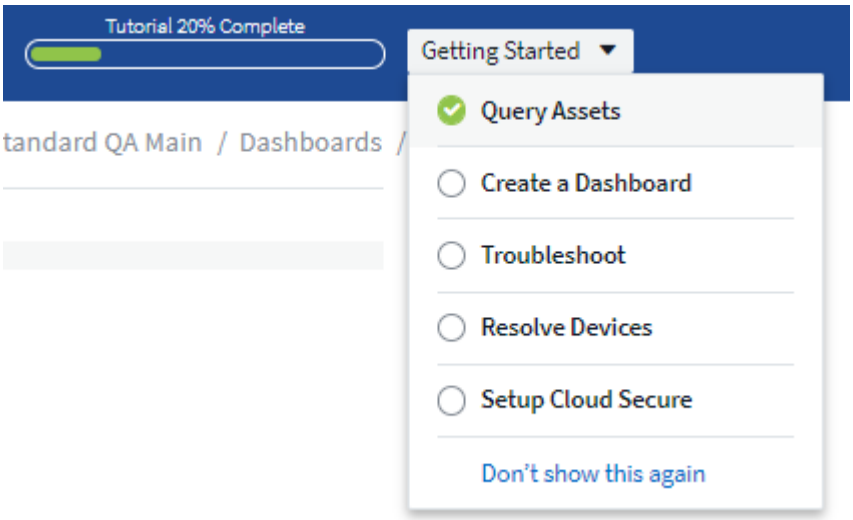
はじめに

ビデオチュートリアルを始める

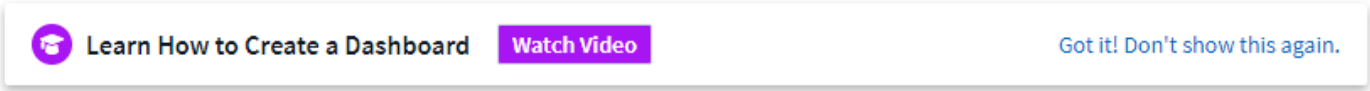
ステップバイステップのビデオ ガイドと進捗チェックリストを備えた機能チュートリアルを使用して、Data Infrastructure Insightsを効率的に学習します。すぐに生産性を高めるために設計された実践的なチュートリアルを通じて、ダッシュボードの作成、クエリの構築、監視の設定、問題のトラブルシューティングなどの重要なスキルを習得します。

チェックリストとビデオチュートリアル

Data Infrastructure Insightsテナントに表示される 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のリストが含まれています。チェックリスト内の項目を選択すると、その概念に適切なData Infrastructure Insightsサイト ページに移動します。たとえば、「ダッシュボードの作成」項目をクリックすると、 Data Infrastructure Insights の*ダッシュボード* 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。 「*Got it!*」をクリックするまで、ビデオを何度でも視聴できます。そのビデオの「*Don't Show This Again*」リンク。ビデオは、閉じるまで、ダッシュボード ページにアクセスするたびに利用できます。



ビデオを少なくとも 1 回視聴すると、チェックリストの [ダッシュボードの作成] 項目がチェックされ、チュートリアルが完了したことが示されます。その後、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、終了するまで好きな順序で何度でも表示できます。

チェックリストを無視する

スタートアップ チェックリストは、チェックリストの下部にある [次回表示しない] リンクをクリックするま

で表示されます。チェックリストを閉じた後でも、メッセージ ヘッダー バーから各チェックリストを閉じるまで、該当する各Data Infrastructure Insightsページでチュートリアルを引き続き利用できます。

ビデオチュートリアル

詳細については、次のビデオをご覧ください。

"生データを実用的な洞察に変える"

"NetAppで強力なダッシュボードを作成する"

"VM Analyzer によるトラブルシューティングの簡素化"

"Data Infrastructure Insightsのクエリを使用して探索および分析する"

"アラートとモニターによるプロアクティブなインフラストラクチャ監視"

データの収集

データ収集を始める

Data Infrastructure Insightsにサインアップし、環境に初めてログインすると、データの収集と管理を開始するために、次の手順が案内されます。

データ コレクターは、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 ソースから情報を検出します。収集された情報は、分析、検証、監視、トラブルシューティングに使用されます。

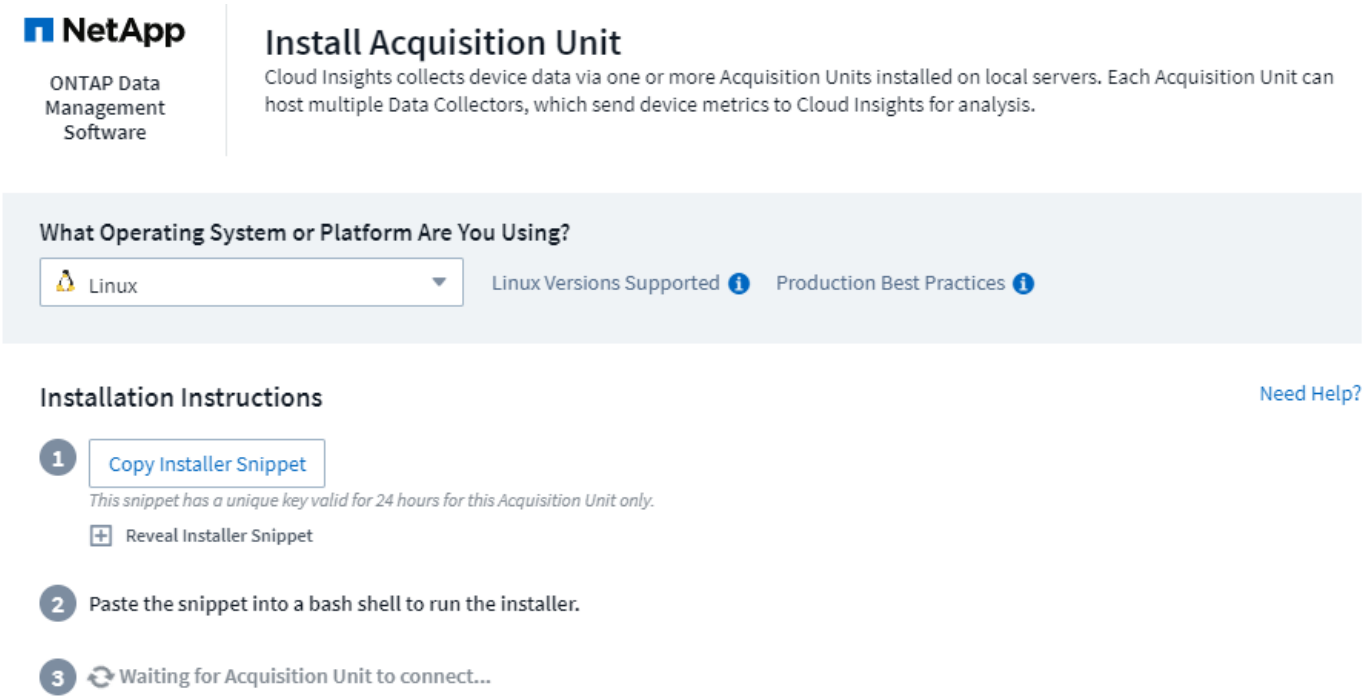
Data Infrastructure Insights、次の 3 種類のデータ コレクターが利用可能です。

- インフラストラクチャ（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ストラクチャ）
- オペレーティング システム (VMware や Windows など)
- サービス（Kafkaなど）

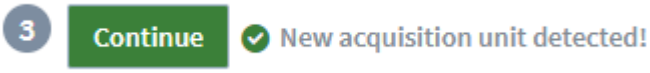
サポートされているベンダーと利用可能なモデルから最初のデータ コレクターを選択します。後でデータコレクターを簡単に追加できます。

取得ユニットをインストールする

インフラストラクチャ データ コレクターを選択した場合は、 Data Infrastructure Insightsにデータを挿入するために Acquisition Unit が必要です。収集元のデータ センターのサーバーまたは 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 つの取得ユニットを複数のデータ コレクターに使用できます。



- フォロー"確認方法"取得ユニットをインストールするには、次のメッセージが表示されます。取得ユニット ソフトウェアがインストールされると、[続行] ボタンが表示され、次の手順に進むことができます。



必要に応じて、後で追加の取得ユニットを設定できます。たとえば、異なる地域のデータ センターから情報を収集するために、異なる取得ユニットが必要になる場合があります。

データコレクターの構成 - インフラストラクチャ

インフラストラクチャ データ コレクターの場合は、表示されるデータ コレクター フィールドに入力するよう求められます。

- データ コレクターに一意で意味のある名前を付けます。
- 必要に応じて、デバイスに接続するための資格情報 (ユーザー名とパスワード) を入力します。
- *Configuration* セクションと *Advanced Configuration* セクションのその他の必須フィールドに入力します。
- データ コレクターを保存するには、[コレクターの追加] をクリックします。

後で追加のデータ コレクターを構成できるようになります。

データコレクターを構成する - 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：

オペレーティング システム データ コレクターの場合は、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 つのエージェントが必要です。エージェントは、 Data Infrastructure Insightsで使用するために、ホスト自体

からもデータを収集します。このデータはウィジェットなどでは「ノード」データとして分類されます。

- 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、「セットアップの完了」をクリックします。

サービス:

サービス データ コレクターの場合は、タイルをクリックすると、そのサービスの説明ページが開きます。

- 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、手順に従ってエージェントをインストールしてください。
- *続行*をクリックすると、データ コレクターの説明ページが開きます。
- 指示に従ってデータ コレクターを構成します。
- 設定が完了したら、[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する

構成するために選択した初期データ コレクターのタイプ (ストレージ、スイッチなど) に応じて、1 つ以上の関連するダッシュボードがインポートされます。たとえば、ストレージ データ コレクターを構成した場合、ストレージ関連のダッシュボードのセットがインポートされ、そのうちの 1 つがData Infrastructure Insights ホーム ページとして設定されます。 ダッシュボード **>** すべてのダッシュボードを表示 リストからホームページを変更できます。

後で追加のダッシュボードをインポートしたり、"自分で作成する" 。

以上です

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 (たとえば、ブラウザー ウィンドウを閉じた場合)、次の手順を手動で実行する必要があります。

- データコレクターを選択する
- プロンプトが表示されたらエージェントまたは取得ユニットをインストールします
- データコレクターを構成する

便利な定義

Data Infrastructure Insights のデータ コレクターまたは機能について説明するときは、次の定義が役立つ場合があります。

- コレクターのライフ サイクル: コレクターは、ライフ サイクルにおいて次のいずれかの状態に属します。
  - プレビュー: 限られた容量または限られた視聴者向けに提供されます。"プレビュー機能"データ コレクターは、プレビュー期間の後に 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、すべての顧客に一般公開されている機能またはデー

タ コレクター。

- 非推奨: 機能的に持続不可能になった、または持続不可能になると予想されるデータ コレクターに適用されます。廃止されたデータ コレクターは、多くの場合、機能が更新された新しいデータ コレクターに置き換えられます。
- 削除済み: 削除され、利用できなくなったデータ コレクター。

- 取得ユニット: データ コレクターをホストするための専用コンピューター (通常は仮想マシン)。このコンピューターは通常、監視対象項目と同じデータセンター/VPC 内に配置されます。
- 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。これは、デバイスと通信するために AU コンピュータ上で実行される構成とコードで構成されています。

取得ユニットの要件

インフラストラクチャ データ コレクター (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、テナントがオペレーティング システム、CPU、メモリ、およびディスク領域の要件を満たしていることを確認する必要があります。

要件

コンポーネント	Linux 要件	Windows の要件
オペレーティング システム	次のいずれかのライセンス版を実行しているコンピューター：* AlmaLinux 9.5、10 * Centos（64ビット）：Stream 9 * Debian（64ビット）：11から13 * OpenSUSE Leap 15.2から15.6、16 * Oracle Enterprise Linux（64ビット）：8.10、9.2、9.4、9.6、10 * Red Hat（64ビット）：8.10、9.2、9.4、9.6、10 * Rocky 9.2から9.6 * SUSE Linux Enterprise Server 15 SP4から15 SP7、16 * Ubuntu Server：20.04、22.04、24.04 LTS * 上記プラットフォーム上のSELinux 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。専用サーバーをお勧めします。SELinuxで実行している場合は、取得ユニットシステムで次のコマンドを実行することをお勧めします：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ー: * Microsoft Windows 11 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows Server 2025 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。専用サーバーをお勧めします。
CPU	2つのCPUコア	同じ

メモリ	8GBのRAM	同じ
使用可能なディスク容量	50 GB (100 GB を推奨) Linux の場合、ディスク領域は次のように割り当てる必要があります: /opt/netapp 10 GB (大規模環境の場合は 20 GB) /var/log/netapp 40 GB (大規模環境の場合は 80 GB) /tmp インストール時に少なくとも 1 GB 使用可能	50 GB
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.netapp.com またはData Infrastructure Insightsテナント (つまり https://<tenant_id>.c01.cloudinsights.netapp.com) へのポート 80 または 443 (送信) 接続が必要です。取得ユニットと各データ収集装置間の要件については、"データコレクター" 。組織でインターネット アクセスにプロキシの使用が必要な場合は、組織のプロキシの動作を理解し、 Data Infrastructure Insightsが機能するための特定の例外を探す必要がある場合があります。たとえば、組織ではデフォルトでアクセスをブロックし、例外的に特定の Web サイト/ドメインへのアクセスのみを許可していますか? もしそうなら、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 詳細については、プロキシについてお読みください。"ここ（Linux）" または"こちら（Windows）"。	同じ
権限	取得ユニット サーバーに対する Sudo 権限。 /tmp は exec 権限でマウントする必要があります。	取得ユニットサーバーの管理者権限
ウィルススキャン		インストール中は、すべてのウイルス スキャナーを完全に無効にする必要があります。インストール後、Acquisition Unit ソフトウェアで使用されるパスをウイルス スキャンから除外する必要があります。

追加の推奨事項

- 正確な監査とデータ レポートのために、ネットワーク タイム プロトコル **(NTP)** または 簡易ネットワーク タイム プロトコル **(SNTP)** を使用して取得ユニット マシンの時刻を同期することを強くお勧めします。

サイズについて

8 GB のメモリと 50 GB のディスク容量のみでData Infrastructure Insights Acquisition Unit を開始できますが、より大規模な環境では、次の質問を自問する必要があります。

以下のことを期待していますか:

- この取得ユニットで 2,500 台を超える仮想マシンまたは 10 個の大規模 (2 ノード超) ONTAPクラスター、Symmetrix、または HDS/HPE VSP/XP アレイを検出しますか?
- この取得ユニットに合計 75 台以上のデータ コレクターを展開しますか?

上記の各質問に「はい」と答えた場合は、AU に 8 GB のメモリと 50 GB のディスク容量を追加することをお勧めします。したがって、たとえば、両方の質問に「はい」と答えた場合は、150 GB 以上のディスク容量を備えた 24 GB のメモリ システムを展開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領域。

サイズに関する追加の質問については、 NetAppサポートにお問い合わせください。

取得ユニットの設定

Data Infrastructure Insights は、ローカル サーバーにインストールされた 1 つ以上の Acquisition Units を使用してデバイス データを収集します。各取得ユニットは複数のデータ コレクターをホストでき、データ コレクターは分析のためにデバイス メトリックをData Infrastructure Insightsに送信します。

このトピックでは、取得単位を追加する方法と、環境でプロキシを使用する場合に必要な追加手順について説明します。

正確な監査とデータ レポートのために、ネットワーク タイム プロトコル **(NTP)** または 簡易ネットワーク タイム プロトコル **(SNTP)** を使用して取得ユニット マシンの時刻を同期することを強くお勧めします。

Data Infrastructure Insightsのセキュリティについて読む"ここをクリックしてください。"。

Linux取得ユニットの追加

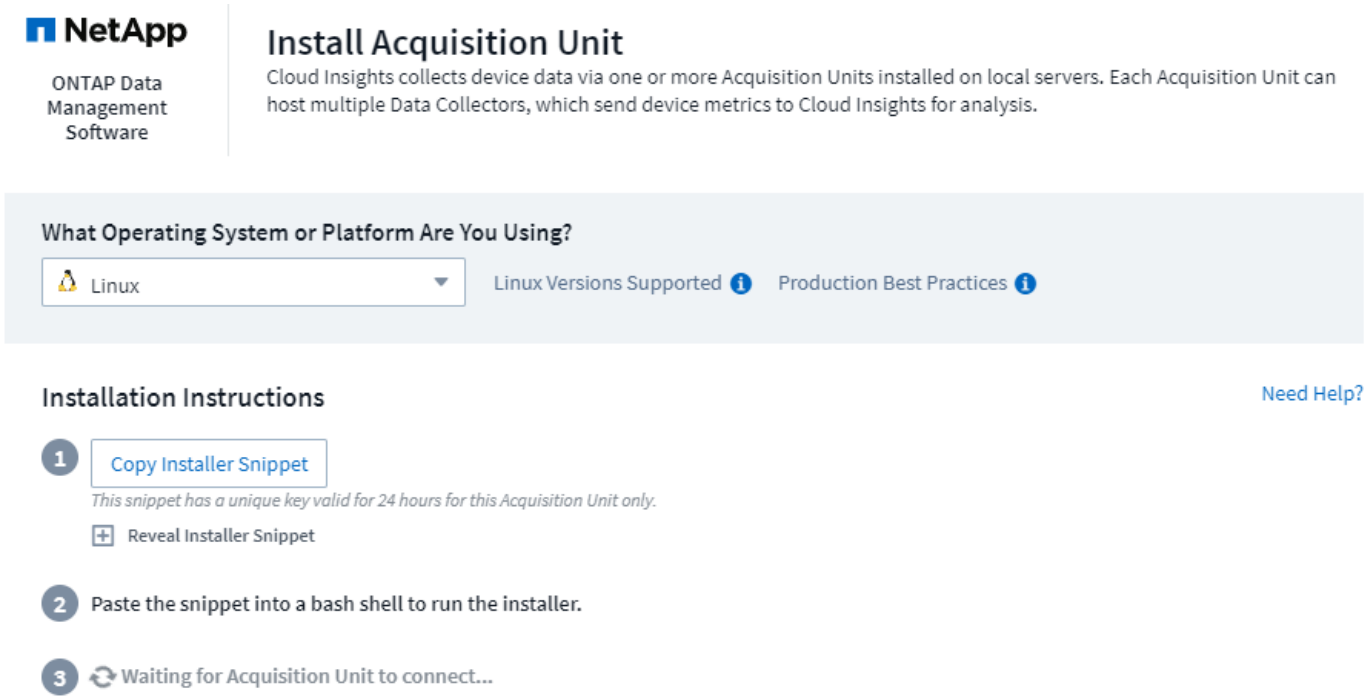
開始する前に

- システムでプロキシを使用している場合は、取得ユニット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、以下を参照してください。 [プロキシ環境変数の設定] 。

Linux 取得ユニット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. *観測性 > コレクター > 取得ユニット > +取得ユニット*をクリックします

   Install Acquisition Unit ダイアログが表示されます。 Linuxを選択します。



1. 取得ユニットをホストするサーバーまたは 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します。
2. サーバーがサポートされているバージョンの Linux を実行し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一覧については、[サポートされている *OS* バージョン *(i)*] をクリックします。
3. ダイアログ内のインストール コマンド スニペットを、取得ユニットをホストするサーバーまたは VM 上のターミナル 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。

終了後の操作

- **Observability > Collectors > Acquisition units** をクリックして、Acquisition Units のステータスを確認します。
- 取得ユニットのログには、/var/log/netapp/cloudinsights/acq/acq.log からアクセスできます。
- 取得ユニットを制御するには、次のスクリプトを使用します。
  - cloudinsights-service.sh (停止、開始、再起動、ステータスの確認)
- 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

プロキシ環境変数の設定

プロキシを使用する環境では、取得ユニット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。プロキシを構成する手順は、[取得ユニットの追加] ダイアログに記載されています。

1. プロキシサーバーはありますか? の + をクリックします。
2. コマンドをテキスト エディターにコピーし、必要に応じてプロキシ変数を設定します。

   注意: プロキシのユーザー名とパスワード フィールドの特殊文字に関する制限に注意してください。ユーザー名フィールドでは「%」と「!」が許可されます。パスワード フィールドでは、「:」、「%」、「!」

が使用できます。

3. Bash シェルを使用して、ターミナルで編集したコマンドを実行します。
4. 取得ユニット ソフトウェアをインストールします。

プロキシ設定

取得ユニットは、双方向/相互認証を使用して、 Data Infrastructure Insightsサーバーに接続します。クライアント証明書は、認証されるためにData Infrastructure Insightsサーバーに渡す必要があります。これを実現するには、データを復号化せずに https 要求をData Infrastructure Insightsサーバー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、プロキシ/ファイアウォールでワイルドカード構成を指定して、 Data Infrastructure Insightsと通信することです。次に例を示します。

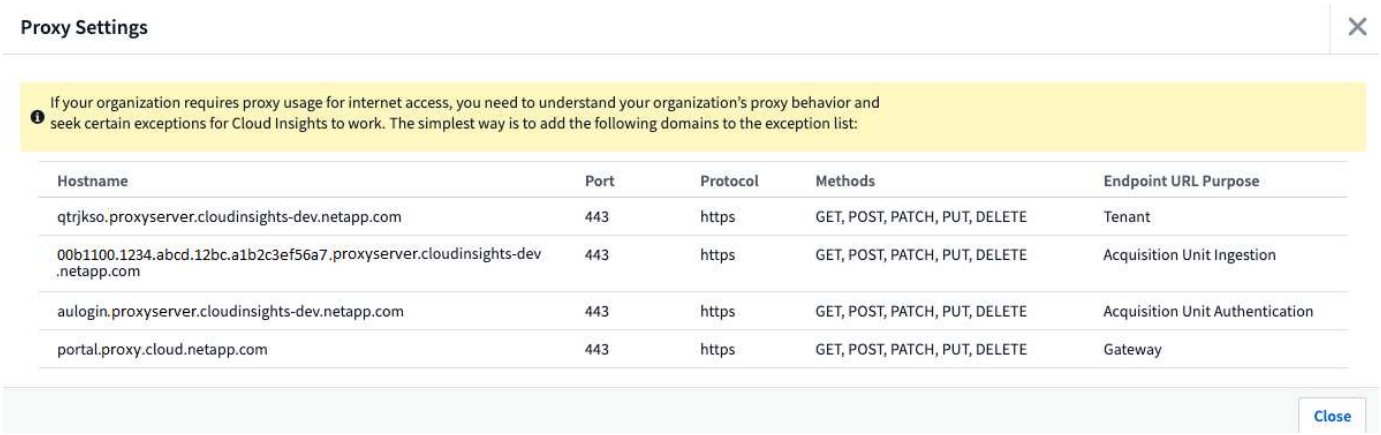
```
*.cloudinsights.netapp.com
```

ワイルドカードとしてアスタリスク (*) 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構成では異なる形式が使用される場合があります。プロキシのドキュメントを参照して、環境内でのワイルドカードの指定が正しい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、 NetApp"ナレッジベース" 。

プロキシ **URL** の表示

オンボーディング中にデータ コレクターを選択するときに [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 URL を表示できます。次のような表が表示されます。



テナントに Workload Security がある場合は、設定されたエンドポイント URL もこのリストに表示されます。

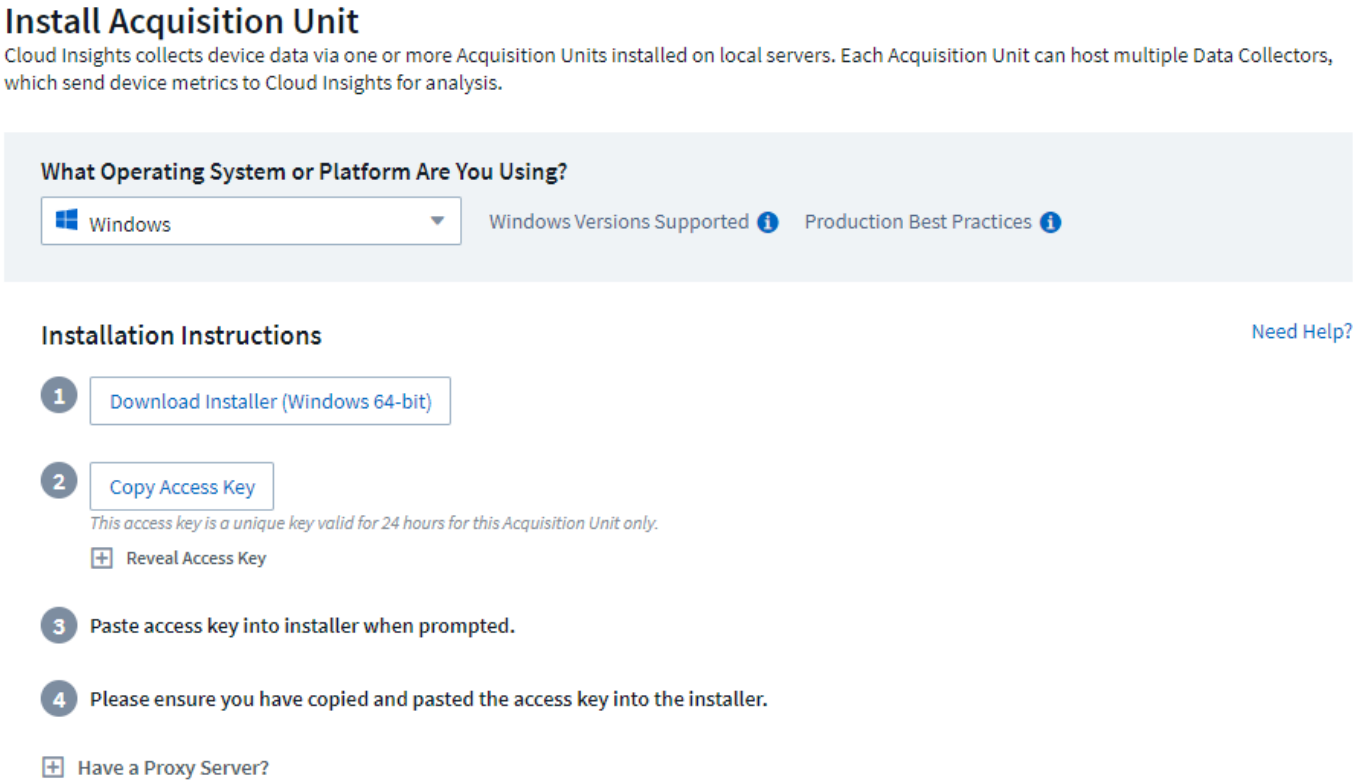
Windows 取得ユニットの追加

Windows Acquisition Unit のインストール手順

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

2. そのサーバーでブラウザ 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** をクリックします。

   Install Acquisition Unit ダイアログが表示されます。 Windowsを選択します。



1. 取得ユニットをホストするサーバーまたは 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します。
2. サーバーがサポートされているバージョンの Windows を実行し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一覧については、[サポートされている *OS* バージョン *(i)*] をクリックします。
3. インストーラーのダウンロード **(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れが必要になります。
5. 取得ユニット サーバー/VM で、ダウンロードしたインストーラーを実行します。
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 サーバーの設定を入力する機会が表示されます。

終了後の操作

- 取得ユニットのステータスを確認するには、* > 観測性 > コレクター > 取得ユニット* をクリックします。
- 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。
- 次のスクリプトを使用して、取得ユニットを停止、開始、再起動、またはステータスを確認します。

```
cloudinsights-service.sh
```

プロキシ設定

取得ユニットは、双方向/相互認証を使用して、 Data Infrastructure Insightsサーバーに接続します。クライアント証明書は、認証されるためにData Infrastructure Insightsサーバーに渡す必要があります。これを実現するには、データを復号化せずに https 要求をData Infrastructure Insightsサーバー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、プロキシ/ファイアウォールでワイルドカード構成を指定して、 Data Infrastructure Insightsと通信することです。次に例を示します。

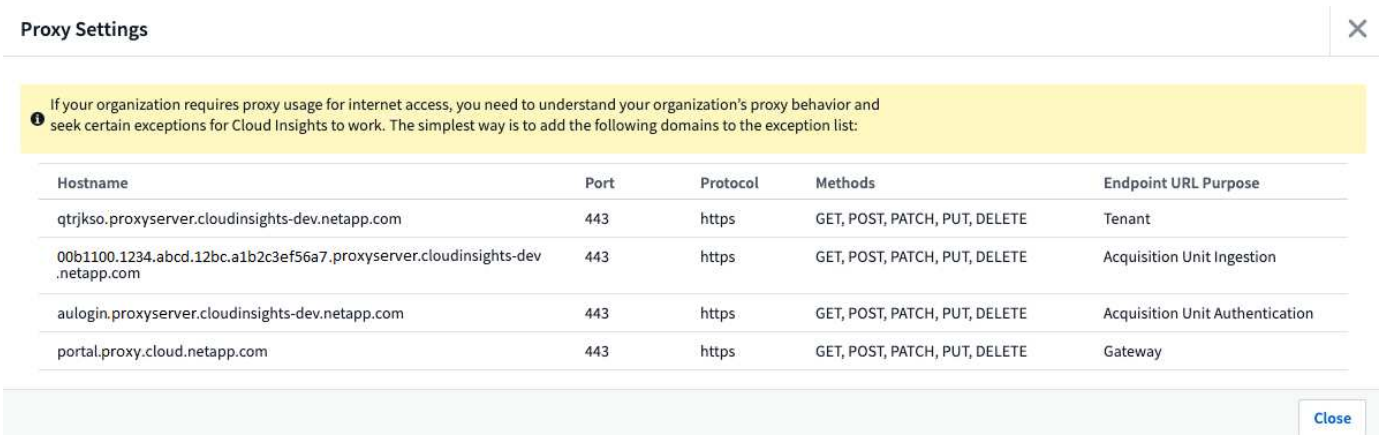
```
*.cloudinsights.netapp.com
```

ワイルドカードとしてアスタリスク (*) 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構成では異なる形式が使用される場合があります。プロキシのドキュメントを参照して、環境内でのワイルドカードの指定が正しい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、 NetApp"ナレッジベース" 。

プロキシ **URL** の表示

オンボーディング中にデータ コレクターを選択するときに [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 URL を表示できます。次のような表が表示されます。



テナントに Workload Security がある場合は、設定されたエンドポイント URL もこのリストに表示されます。

取得ユニット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。

ウィンドウズ:

Windows 取得ユニットをアンインストールする場合:

1. 取得ユニット サーバー/VM で、コントロール パネルを開き、[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、指示に従います。

リナックス:

Linux 取得ユニットをアンインストールする場合:

1. 取得ユニット サーバー/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、次を実行してください：

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

Windows と **Linux:**

AU をアンインストールした後:

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 [オプション] ボタンをクリックし、[削除] を選択します。取得ユニットを削除できるのは、その取得ユニットにデータ コレクターが割り当てられていない場合のみです。

> ⓘ データ コレクターが接続されている取得ユニット (AU) を削除することはできません。元の AU を削除する前に、AU のすべてのデータ コレクターを別の AU に移動します (コレクターを編集し、別の AU を選択します)。

横に星が付いている取得ユニットは、デバイスの解像度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 にマウスを移動し、「3 つのドット」メニューを開いて「デバイスの解像度に使用」を選択します。



取得ユニットの再インストール

同じサーバー/VM に Acquisition Unit を再インストールするには、次の手順に従う必要があります。

開始する前に

取得ユニットを再インストールする前に、別のサーバー/VM に一時的な取得ユニットを構成する必要があります。

手順

1. 取得ユニット サーバー/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、**Observability > Collectors** に移動します。
3. 各データ コレクターごとに、右側の [オプション] メニューをクリックし、[編集] を選択します。データ コレクターを一時的な取得ユニットに割り当て、[保存] をクリックします。

   同じタイプの複数のデータ コレクターを選択し、[一括アクション] ボタンをクリックすることもできます。 [編集] を選択し、データ コレクターを一時的な取得ユニットに割り当てます。

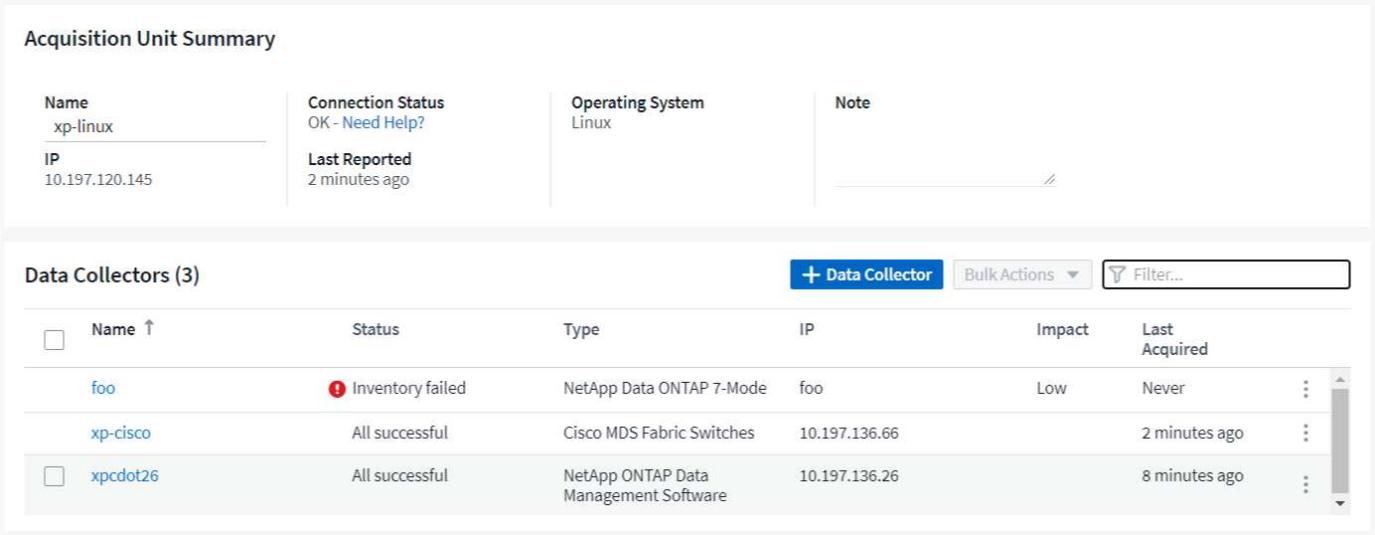
4. すべてのデータ コレクターが一時的な Acquisition Unit に移動されたら、**Observability > Collectors** に移動し、**Acquisition Units** タブを選択します。
5. 再インストールする取得ユニットの右側にある [オプション] ボタンをクリックし、[削除] を選択します。取得ユニットを削除できるのは、その取得ユニットにデータ コレクターが割り当てられていない場合のみです。
6. これで、Acquisition Unit ソフトウェアを元のサーバー/VM に再インストールできます。 **+Acquisition Unit** をクリックし、上記の手順に従って Acquisition Unit をインストールします。
7. 取得ユニットを再インストールしたら、データ コレクターを取得ユニットに再度割り当てます。

AUの詳細の表示

取得ユニット (AU) の詳細ページには、AU に関する有用な詳細情報と、トラブルシューティングに役立つ情報が提供されます。 AU 詳細ページには次のセクションが含まれています。

- 次の内容を示す 概要 セクション:
  - 取得ユニットの*名前*と*IP*
  - AUの現在の接続*ステータス*
  - 最終報告 成功したデータコレクターのポーリング時間
  - AUマシンの*オペレーティングシステム*
  - AU の現在の メモ。このフィールドを使用して、AU に関する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。
- AU の データ コレクター の表。各データ コレクターについて次の内容が表示されます。
  - 名前 - このリンクをクリックすると、追加情報を含むデータ収集者の詳細ページにドリルダウンします。
  - ステータス - 成功またはエラー情報
  - タイプ - ベンダー/モデル
  - データ収集者の*IP*アドレス

- 現在の*影響*レベル
- *最終取得*時間 - データコレクターが最後に正常にポーリングされた時間



各データ コレクターごとに、「3 つのドット」メニューをクリックして、データ コレクターの複製、編集、ポーリング、または削除を行うことができます。このリストで複数のデータ コレクターを選択し、一括アクションを実行することもできます。

取得ユニットを再起動するには、ページの上部にある [再起動] ボタンをクリックします。接続の問題が発生した場合に AU への 接続の復元 を試行するには、このボタンをドロップダウンします。

データ収集のためのエージェントの構成 (Windows/Linux)

Data Infrastructure Insightsサイトは"テレグラフ"統合データの収集エージェントとして。Telegraf は、メトリック、イベント、ログを収集およびレポートするために使用できるプラグイン駆動型のサーバー エージェントです。入力プラグインは、システム/OSに直接アクセスしたり、サードパーティの API を呼び出したり、構成されたストリーム (Kafka、statsD など) をリッスンしたりして、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。出力プラグインは、収集されたメトリック、イベント、および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。

Kubernetesへのインストールについては、"NetApp Kubernetes 監視オペレーター"ページ。

正確な監査とデータ レポートのために、ネットワーク タイム プロトコル **(NTP)** または 簡易ネットワーク タイム プロトコル **(SNTP)** を使用してエージェント 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検証したい場合は、以下のセクションを参照してください。Telegraf パッケージのチェックサムの検証 。

エージェントのインストール

サービス データ コレクターをインストールしていて、まだエージェントを構成していない場合は、まず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、次のオペレーティング システムに Telegraf エージェントをインストールする手順について説明します。

- Windows
- RHEL と 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、**Observability > Collectors** に移動します。
3. *+データコレクター*をクリックし、インストールするデータコレクターを選択します。
4. ホストに適したプラットフォームを選択します（Windows、Linux）
5. 各プラットフォームの残りの手順に従います。



一度ホストにエージェントをインストールすると、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。



サーバー/VM にエージェントをインストールすると、 Data Infrastructure Insights は、構成したデータ コレクターからの収集に加えて、そのシステムからメトリックを収集します。これらの指標は次のように収集されます"「ノード」メトリック"。



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

ログの場所

デフォルトでは、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。

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

Windows

前提条件

- PowerShellがインストールされている必要があります
- プロキシを使用している場合は、「**Windows** のプロキシ サポートの構成」セクションの指示に従う必要があります。

Windows のプロキシサポートの構成



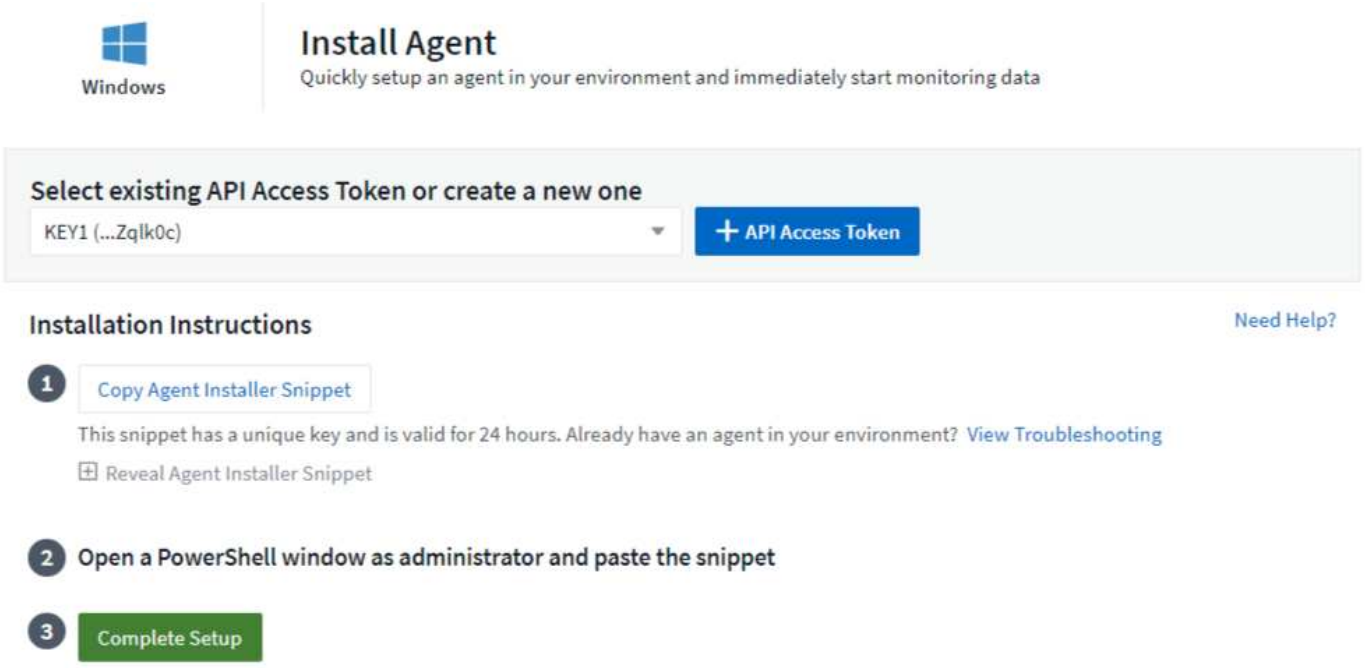
環境でプロキシを使用している場合は、インストールする前にこのセクションをお読みください。

以下の手順は、*http_proxy/https_proxy* 環境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、ユーザーは *no_proxy environment* 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、次の操作を実行して *https_proxy* および/または *http_proxy* 環境変数を設定します。

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

エージェントのインストール



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すばやくコピーできます。
3. PowerShellウィンドウを開く
4. コマンドを PowerShell ウィンドウに貼り付けて Enter キーを押します。
5. このコマンドは適切なエージェント インストーラーをダウンロードしてインストールし、デフォルト構成を設定します。完了すると、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

エージェントをインストールした後、次のコマンドを使用してサービスを開始/停止できます。

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

エージェントのアンインストール

Windows でエージェントをアンインストールするには、PowerShell ウィンドウで次の操作を行います。

1. Telegraf サービスを停止して削除します。

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

2. トラストストアから証明書を削除します。

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

3. *C:\Program Files\telegraf* フォルダを削除して、バイナリ、ログ、および構成ファイルを削除します。
4. レジストリから_SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf_キーを削除します。

エージェントのアップグレード

Telegraf エージェントをアップグレードするには、次の手順を実行します。

1. Telegraf サービスを停止して削除します。

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

2. レジストリから_SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf_キーを削除します。
3. *C:\Program Files\telegraf\telegraf.conf* を削除します。
4. *C:\Program Files\telegraf\telegraf.exe* を削除します。
5. "新しいエージェントをインストールする" 。

RHEL と CentOS

前提条件

- 次のコマンドが利用可能である必要があります: curl、sudo、ping、sha256sum、openssl、および dmidecode
- プロキシを使用している場合は、*RHEL/CentOS のプロキシ サポートの構成*セクションの指示に従う必

要があります。

RHEL/CentOS のプロキシサポートの設定

環境でプロキシを使用している場合は、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。

以下の手順は、*http_proxy/https_proxy* 環境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、ユーザーは *no_proxy environment* 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。

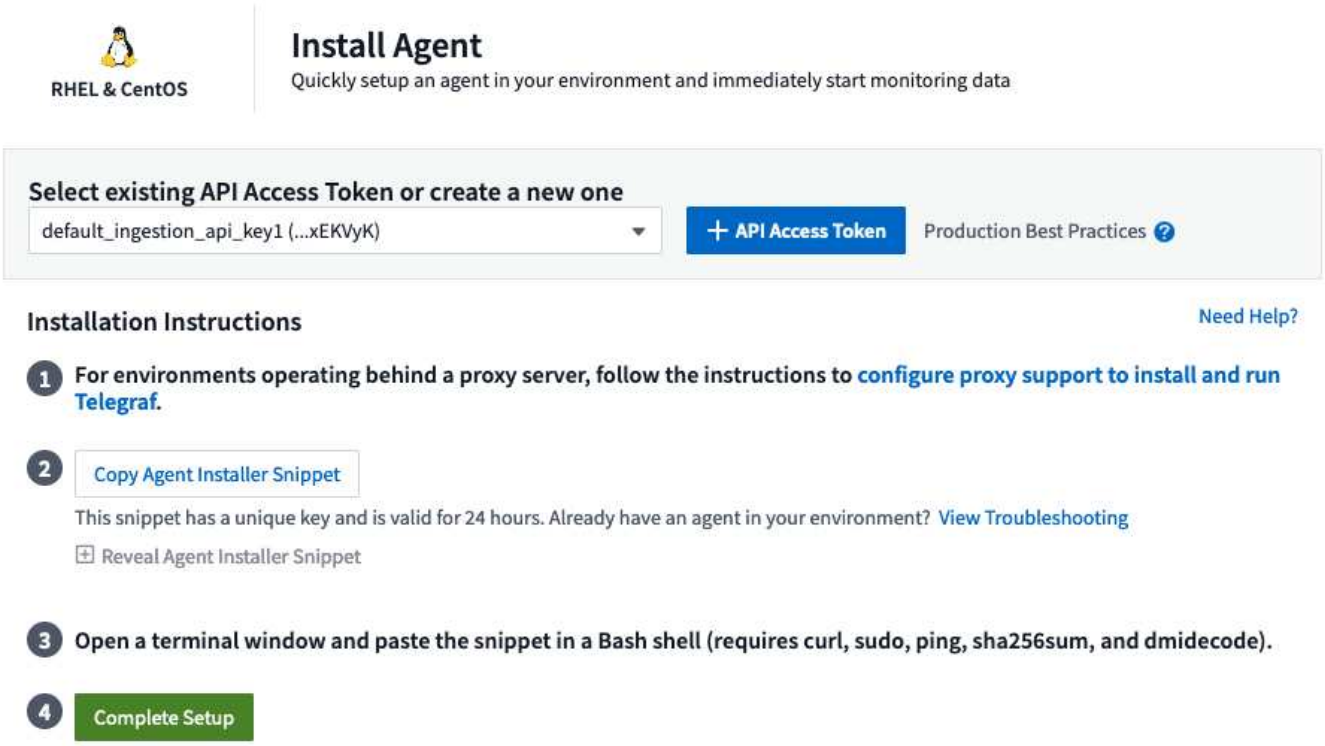
1. 現在のユーザーの *https_proxy* および/または *http_proxy* 環境変数を設定します。

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

. _/etc/default/telegraf_ を作成し、_https_proxy_ および/または _http_proxy_ 変数の定義を挿入します。

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

エージェントのインストール



RHEL/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すばやくコピーできます。
3. Bashウィンドウを開く
4. コマンドをBash ウィンドウに貼り付けて、Enter キーを押します。
5. このコマンドは適切なエージェント インストーラーをダウンロードしてインストールし、デフォルト構成を設定します。完了すると、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

エージェントをインストールした後、次のコマンドを使用してサービスを開始/停止できます。

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

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

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

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

エージェントのアンインストール

RHEL/CentOS 上の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. Telegraf エージェントを削除します。

```
 yum remove telegraf
```

. 残っている可能性のある構成ファイルやログ ファイルをすべて削除します。

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

エージェントのアップグレード

Telegraf エージェントをアップグレードするには、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. 以前の Telegraf 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する"]
。
```

UbuntuとDebian

前提条件

- 次のコマンドが利用可能である必要があります: curl、sudo、ping、sha256sum、openssl、および dmidecode
- プロキシを使用している場合は、**Ubuntu/Debian** のプロキシ サポートの構成 セクションの指示に従う必要があります。

Ubuntu/Debian のプロキシサポートの設定

環境でプロキシを使用している場合は、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。

以下の手順は、*http_proxy/https_proxy* 環境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、ユーザーは *no_proxy environment* 変数も設定する必要があります。

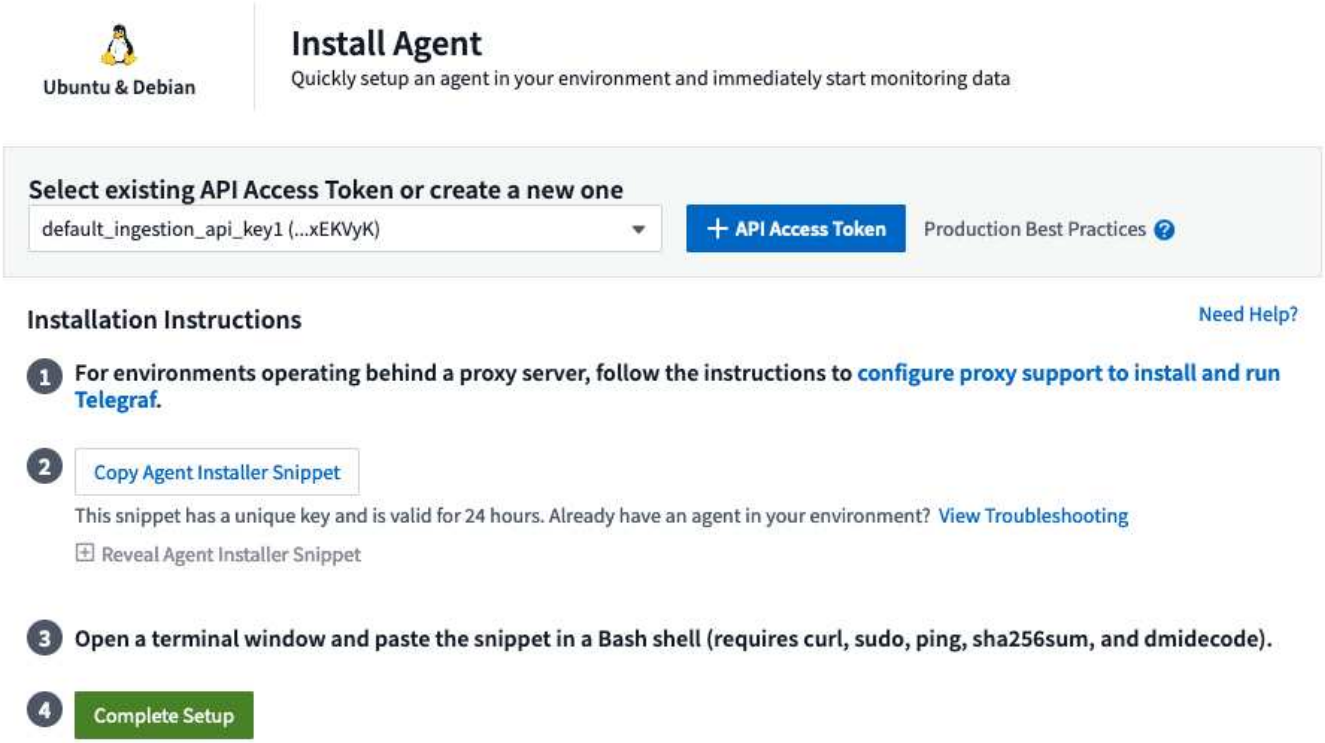
プロキシの背後にあるシステムの場合は、Telegraf エージェントをインストールする前に、次の手順を実行します。

1. 現在のユーザーの *https_proxy* および/または *http_proxy* 環境変数を設定します。

```
 export https_proxy=<proxy_server>:<proxy_port>
. /etc/default/telegraf を作成し、_https_proxy_ および/または _http_proxy_
変数の定義を挿入します。
```

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

エージェントのインストール



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すばやくコピーできます。
3. Bashウィンドウを開く
4. コマンドをBash ウィンドウに貼り付けて、Enter キーを押します。
5. このコマンドは適切なエージェント インストーラーをダウンロードしてインストールし、デフォルト構成を設定します。完了すると、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

エージェントをインストールした後、次のコマンドを使用してサービスを開始/停止できます。

オペレーティング システムで 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 システムで systemd を使用していない場合は、次の操作を行います。

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

エージェントのアンインストール

Ubuntu/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. Telegraf エージェントを削除します。

```
 dpkg -r telegraf
```

. 残っている可能性のある構成ファイルやログ ファイルをすべて削除します。

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

エージェントのアップグレード

Telegraf エージェントをアップグレードするには、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)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. 以前の Telegraf 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する"] 。

Telegraf パッケージのチェックサムの検証

Data Infrastructure Insightsエージェント インストーラーは整合性チェックを実行しますが、ダウンロードした Telegraf バイナリをインストールする前に独自の検証を実行することを望むユーザーもいます。これは、インストーラーをダウンロードし、ダウンロードしたパッケージのチェックサムを生成し、その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することで実行できます。

インストールせずにインストーラーパッケージをダウンロードする

ダウンロードのみの操作 (デフォルトのダウンロードとインストールではなく) を実行するには、ユーザーは 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、「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 インストーラー 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 エディターに貼り付けます。
3. コマンドの末尾の「--install」（Linux）または「-install」（Windows）を削除します。
4. テキスト エディターからコマンド全体をコピーします。
5. 次に、それをコマンド 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 (これらの例は Kubernetes 用です。実際のスクリプト名は異なる場合があります):

- ダウンロードしてインストールする（デフォルト）:

```
 installerName=cloudinsights-ubuntu_debian.sh … && ./$installerName
--download --verify && sudo -E -H ./$installerName --install
* ダウンロード専用:
```

```
installerName=cloudinsights-ubuntu_debian.sh … && ./$installerName
--download --verify
```

Windows：

- ダウンロードしてインストールする（デフォルト）:

```
 !$($installerName=".\cloudinsights-windows.ps1") … -and $(if(((Get-
FileHash $installerName).Hash).ToLower() -eq "INSTALLER_CHECKSUM ") {
&$installerName -download -verify -install } else { Write-Host "Install
script checksum does not match"})"
* ダウンロード専用:
```

```
!$($installerName=".\cloudinsights-windows.ps1") … -and $(if(((Get-
FileHash $installerName).Hash).ToLower() -eq "INSTALLER_CHECKSUM ") {
&$installerName -download -verify } else { Write-Host "Install script
checksum does not match"})"
```

ダウンロード専用コマンドは、必要なすべての成果物をData Infrastructure Insightsから作業ディレクトリにダウンロードします。アーティファクトには、以下のものが含まれますが、これらに限定されるわけではありません。

- インストールスクリプト
- 環境ファイル
- Telegrafバイナリ
- Telegrafバイナリの署名
- バイナリ署名を検証するための公開証明書

DII からダウンロードしてコピーされたインストール スニペットはインストール スクリプトのチェックサムを自動的に計算し、インストール スクリプトによって telegraf バイナリの署名が検証されます。

チェックサム値を検証する

チェックサム値を生成するには、適切な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：
```

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

ダウンロードしたパッケージをインストールする

すべてのアーティファクトが適切に検証されたら、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：
```

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

APIアクセストークンの作成と使用

Telegraf データ取り込み用の API アクセス トークンを作成するには、次のいずれかを実行してください。

データコレクターのインストールページから作成する

1. 使用するプラットフォーム (Windows、Linux) の Data Collector インストール ページに移動します。
2. + API アクセス トークン ボタンを使用してトークンを作成します。
3. 名前を入力して「保存」をクリックします。
4. ドロップダウンでトークン名が選択され、コレクターのインストール時に使用されます。

APIアクセストークンを手動で作成する

1. [管理] > [API アクセス] に移動します。
2. + API アクセス トークンをクリックします。
3. 名前と、オプションで説明を入力します。
4. 「このトークンはどのタイプの API を呼び出すために使用されますか?」の下で、「データ取り込み」のみを選択し、「取得ユニット」の選択を解除します。
5. 「権限」の下で「読み取り/書き込み」を選択します。
6. 「Kubernetes のトークンを自動的にローテーションする」の選択を解除します。

新しく作成した API アクセス トークンを使用するには、インストーラー ページの「既存の API アクセス トークンを選択するか、新しいトークンを作成する」ドロップダウンから選択します。次のプロパティを持つトークンのみが使用できることに注意してください。

- APIタイプ:「データ取り込み」のみ
- 権限: 読み取り/書き込み
- Kubernetes 自動ローテーション: オフ

トラブルシューティング

エージェントの設定中に問題が発生した場合に試すことができるいくつかのこと:

問題：	これを試してください:
新しいプラグインを設定して Telegraf を再起動した後、Telegraf が起動に失敗します。ログには、次のようなエラーが記録されています: "[telegraf] エージェント実行エラー: 設定ファイル /etc/telegraf/telegraf.d/cloudinsights-default.conf の読み込みエラー: プラグイン出力.http: 行 <行番号>: 設定でフィールド ["use_system_proxy"] が指定されましたが、使用されていません"	インストールされている Telegraf のバージョンが古くなっています。このページの手順に従って、適切なプラットフォームの*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ところ、エージェントがデータを送信しなくなりました	Telegraf エージェントをアンインストールしてから、インストール スクリプトを再実行します。適切なプラットフォームについては、このページの エージェントのアップグレード の手順に従ってください。

問題：	これを試してください:
Data Infrastructure Insightsを使用してエージェントをすでにインストールしました	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、エージェントのインストール画面で適切なプラットフォームとキーを選択し、「続行」または「完了」をクリックするだけです。
エージェントはすでにインストールされていますが、Data Infrastructure Insightsインストーラーを使用していません	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、適切なデフォルト構成ファイル設定を確認します。完了したら、[続行] または [完了] をクリックします。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

データコレクターの構成

データセンター内のデバイスからデータを収集するには、Data Infrastructure Insights環境でデータ コレクターを構成します。

開始する前に

- データの収集を開始する前に、取得ユニットを構成する必要があります。
- データを収集するデバイスの資格情報が必要です。
- データを収集する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メニューから、*オブザーバビリティ > コレクター*をクリックします。

   システムは、利用可能なデータ コレクターをベンダー別に表示します。

2. **+** コレクター をクリックし、構成するデータ コレクターを選択します。

   ダイアログ ボックスでは、データ コレクターを構成し、取得ユニットを追加できます。

3. データ コレクターの名前を入力します。
4. 追加の構成フィールドを追加するには、「詳細構成」をクリックします。 (すべてのデータ コレクターに高度な構成が必要なわけではありません。)
5. 構成のテスト をクリックして、データ コレクターが正しく構成されていることを確認します。
6. コレクターの追加 をクリックして構成を保存し、データ コレクターをData Infrastructure Insightsテナントに追加します。

サービスから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には、最大 2 回のポーリング期間かかる場合があります。

- 1回目の在庫調査: 即時
- ベースラインを確立するための最初のパフォーマンスデータポーリング：インベントリポーリングの直後

- 2回目のパフォーマンスアンケート: 1回目のパフォーマンスアンケートの完了後15秒以内

ポーリングは、構成されたインベントリおよびパフォーマンス ポーリング間隔に従って続行されます。

データコレクターの取得状況の判断

データ コレクターはData Infrastructure Insightsの主な情報源であるため、データ コレクターが実行状態にあることを確認することが不可欠です。

データ コレクターのステータスは、アセット ページの右上隅に「N 分前に取得」というメッセージとして表示されます。ここで、N はアセットのデータ コレクターの最新の取得時刻を示します。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 コレクターの名前、ステータス、および最後に成功した取得時刻を含む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、テーブル内のデータ コレクター名のリンクをクリックすると、そのデータ コレクターの詳細ページに移動します。

構成されたデータコレクターの管理

「インストールされたデータ コレクター」ページでは、Data Infrastructure Insights用に構成されたデータ コレクター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 コレクターを変更できます。

手順

1. Data Infrastructure Insightsサイトメニューで、*オブザーバビリティ>コレクター*をクリックします。

   利用可能なデータ コレクター画面が表示されます。

2. *インストールされたデータコレクター*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 コレクターのリストが表示されます。リストには、コレクターの名前、ステータス、コレクターがアクセスしている IP アドレス、デバイスから最後にデータが取得された日時が表示されます。この画面で実行できるアクションは次のとおりです。

   - ポーリングを制御する
   - データコレクターの資格情報を変更する
   - クローンデータコレクター

データコレクタのポーリングの制御

データ コレクターに変更を加えた後、変更内容を確認するためにすぐにポーリングを実行したい場合や、問題の解決に取り組んでいる間、データ コレクターでのデータ収集を 1 日、3 日、または 5 日間延期したい場合があります。

手順

1. Data Infrastructure Insightsサイトメニューで、*オブザーバビリティ>コレクター*をクリックします。
2. *インストールされたデータコレクター*をクリックします
3. 変更したいデータコレクターの左側のチェックボックスを選択します

4. *一括アクション*をクリックし、実行する投票アクションを選択します。

   複数のデータ コレクターに対して同時に一括アクションを実行できます。データ コレクターを選択し、[一括アクション] メニューから実行するアクションを選択します。

データ収集者の情報を編集する

既存のデータ コレクターのセットアップ情報を編集できます。

単一のデータコレクターを編集するには:

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

   コレクター編集ダイアログが開きます。

3. 変更を入力し、「構成のテスト」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 コレクターを編集することもできます。

1. 変更する各データ コレクターの左側にあるチェック ボックスをオンにします。
2. 一括操作 ボタンをクリックし、編集 を選択して、データ コレクターの編集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。

   選択したデータ コレクターは同じベンダーとモデルであり、同じ取得ユニット上に存在している必要があります。

   複数のデータ コレクターを編集する場合、データ コレクター名フィールドに「混合」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「混合」と表示され、編集できます。選択したデータ コレクター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 コレクターを編集する場合、[テスト構成] ボタンは使用できません。

データ収集装置のクローン作成

クローン機能を使用すると、別のデータ ソースと同じ資格情報と属性を持つデータ ソースをすばやく追加できます。クローン作成により、同じデバイス タイプの複数のインスタンスを簡単に構成できます。

手順

1. Data Infrastructure Insightsサイト メニューで、可観測性 **>** コレクター をクリックします。
2. *インストールされたデータコレクター*をクリックします。
3. コピーするデータ コレクターの左側にあるチェック ボックスをクリックします。
4. 選択したデータ コレクターの右側にあるオプション メニューで、[複製] をクリックします。

   クローン データ コレクター 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*をクリックします。

終了後の操作

クローン操作では、他のすべての属性と設定がコピーされ、新しいデータ コレクターが作成されます。

データコレクターに対する一括アクションの実行

複数のデータ コレクター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 コレクターでポーリングを開始したり、ポーリングを延期したり、ポーリングを再開したりできます。さらに、複数のデータ コレクターを削除することもできます。

手順

1. Data Infrastructure Insightsサイトメニューで、*オブザーバビリティ>コレクター*をクリックします。
2. *インストールされたデータコレクター*をクリックします
3. 変更するデータ コレクターの左側にあるチェック ボックスをクリックします。
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。

終了後の操作

選択した操作はデータ コレクターに対して実行されます。データ コレクターを削除することを選択した場合、アクションの確認を求めるダイアログが表示されます。

失敗したデータ収集装置の調査

データ コレクターに失敗メッセージがあり、影響度が高または中程度の場合、リンクされた情報を含むデータ コレクターの概要ページを使用してこの問題を調査する必要があります。

データ コレクターの障害の原因を特定するには、次の手順に従います。データ コレクターの障害メッセージは、管理者 メニューと インストールされたデータ コレクター ページに表示されます。

手順

1. 管理者 > データ コレクター > インストールされたデータ コレクター をクリックします。
2. 障害が発生したデータ コレクターのリンクされた名前をクリックして、[概要] ページを開きます。
3. [概要] ページで、[コメント] 領域をチェックして、この障害を調査している可能性のある別のエンジニアが残したメモを読んでください。
4. パフォーマンス メッセージがあればメモします。
5. イベント タイムライン グラフのセグメントの上にマウス ポインターを移動すると、追加情報が表示されます。
6. イベント タイムラインの下に表示されるデバイスのエラー メッセージを選択し、メッセージの右側に表示されるエラーの詳細アイコンをクリックします。

   エラーの詳細には、エラー メッセージのテキスト、最も可能性の高い原因、使用中の情報、問題を修正するために試すことができる内容の提案が含まれます。

7. 「このデータ コレクターによって報告されたデバイス」領域では、リストをフィルターして関心のあるデバイスのみを表示できます。また、デバイスのリンクされた 名前 をクリックして、そのデバイスの資産ページを表示できます。
8. データ コレクター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] 領域をチェックして、最近の変更が問題の原因になっているかどうかを確認します。

ダッシュボードのインポート

Data Infrastructure Insights は、データに関するビジネス分析情報を提供するための推奨ダッシュボードを多数提供します。各ダッシュボードには、テナントで現在収集されているデータに関連する特定の質問に答えたり、特定の問題を解決したりするために設計されたウィジェットが含まれています。DII を使用すると、便利なダッシュボードをエクスポートして別のテナントにインポートすることもできます。

ダッシュボードギャラリーからのインポート

ギャラリーからダッシュボードをインポートするには、次の手順を実行します。

1. *オブザーバビリティ > 探索 > すべてのダッシュボード*を選択します
2. *+ダッシュボードのインポート*をクリックし、_ギャラリーからのインポート_を選択します。

   環境内のデータ コレクターに基づいて、推奨ダッシュボード のリストが表示されます。ダッシュボードは、AWS、 NetApp、ストレージ、VMware など、さまざまな種類のオブジェクトに関する質問に答えるのに役立ちます。

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はダッシュボード リストに表示されます。

推奨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 コレクターがインストールされていないが、将来的に構成する予定がある場合でも、ストレージ関連のダッシュボードをインポートすることを選択できます。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 コレクターが構成されるまで、関連データは表示されない可能性があります。

ダッシュボード ギャラリーからのインポートは、管理者またはアカウント所有者の役割を持つユーザーが利用できます。

エクスポートしたダッシュボードのインポート

ダッシュボードを*エクスポート*するには、**[Observability] > [Explore] > [All Dashboards]** ページで、ダッシュボードの右側にあるメニューをクリックし、[*Export*] を選択します。複数のダッシュボードを選択し、「一括操作」ドロップダウンから「エクスポート」を選択することもできます。ダッシュボードは、ローカル システム上の .ZIP ファイルに保存されます。

ダッシュボードを*インポート*するには、目的のテナントに移動して次の操作を行います。

1. *オブザーバビリティ > 探索 > すべてのダッシュボード*を選択します
2. *+ダッシュボードのインポート*をクリックし、_ファイルからインポート_を選択します。以前にエクスポートしたファイルの .ZIP を選択します。ダッシュボードがインポートされ、ダッシュボード リストに

表示されます。既存のダッシュボードと同じ名前のダッシュボードをインポートする場合は、ダッシュボード名に「(2)」が追加されることに注意してください。

ユーザーアカウントとロール

Data Infrastructure Insights は、アカウント所有者、管理者、ユーザー、ゲストの最大 4 つのユーザー アカウント ロールを提供します。各アカウントには、以下の表に示すように特定の権限レベルが割り当てられます。ユーザーは"招待された"Data Infrastructure Insightsに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）認証"デフォルトの役割を持ちます。 SSO 認証は、Data Infrastructure Insights Premium Edition の機能として利用できます。

権限レベル

ユーザー 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。各ユーザー アカウントには、次の権限レベルから各Data Infrastructure Insights機能のロールが割り当てられます。

ロール	可観測性	ワークロードセキュリティ	レポート	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	管理者と同じ権限に加え、SSO 認証と ID フェデレーション構成も管理します。追加の所有者を割り当てたり、マネージド サービス プロバイダー (MSP) マスター テナントにクライアントを追加したりすることもできます。

ロール	可観測性	ワークロードセキュリティ	レポート	管理者
管理者	すべての監視機能とデータ コレクターの管理を実行できます。	アラート、フォレンジック、データ コレクター、自動応答ポリシー、セキュリティ用の 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セキュリティ ロールのみです。	レポート API トークンの管理を含むすべてのユーザー/作成者機能、およびレポートの構成、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レポート ロールのみです。	他のユーザーを招待できますが、割り当てることができるのは Observability ロールのみです。 SSO 構成を表示することはできますが、変更することはできません。 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と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、注釈、注釈ルール、アプリケーションを表示および変更し、デバイスの解像度を管理できます。	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取得、ユーザー アクセスの制限の管理を行うことができます。	すべてのゲスト/コンシューマー機能を実行できるほか、レポートとダッシュボードを作成および管理できます。	使用不可
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権を持ち、クエリを表示および実行できます。	アラートと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 ステータスを変更したり、メモを追加したり、スナップショットを手動で取得したり、ユーザー アクセスを制限したりすることはできません。	レポートを表示、スケジュール、実行したり、言語やタイムゾーンなどの個人設定を行ったりできます。ゲスト/コンシューマーはレポートを作成したり、管理タスクを実行したりすることはできません。	使用不可

ベストプラクティスとしては、管理者権限を持つユーザーの数を制限することです。最も多くのアカウントは、ユーザー アカウントまたはゲスト アカウントである必要があります。

ユーザーロール別の**Data Infrastructure Insights**の権限

次の表は、各ユーザー ロールに付与されるData Infrastructure Insights権限を示しています。

特徴	管理者/アカウント所有者	ユーザ	ゲスト
取得単位: 追加/変更/削除	Y	注	注
アラート*: 作成/変更/削除	Y	Y	注
アラート*: 表示	Y	Y	Y
注釈ルール: 作成/実行/変更/削除	Y	Y	注
注釈: 作成/変更/割り当て/表示/削除/削除	Y	Y	注
APIアクセス*: 作成/名前変更/無効化/取り消し	Y	注	注
アプリケーション: 作成/表示/変更/削除	Y	Y	注
アセットページ: 変更	Y	Y	注
アセットページ: 表示	Y	Y	Y
監査: 表示	Y	注	注
クラウドコスト	Y	注	注
セキュリティ	Y	注	注
ダッシュボード: 作成/変更/削除	Y	Y	注
ダッシュボード: 表示	Y	Y	Y
データコレクター: 追加/変更/ポーリング/削除	Y	注	注
通知: 表示	Y	Y	Y
通知: 変更	Y	注	注
クエリ: 作成/変更/削除	Y	Y	注
クエリ: 表示/実行	Y	Y	Y
デバイスの解像度	Y	Y	注
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	注
サブスクリプション: 表示/変更	Y	注	注
ユーザー管理: 招待/追加/変更/無効化	Y	注	注

*プレミアムエディションが必要です

ユーザーを招待してアカウントを作成する

新しいユーザー アカウントの作成は、NetApp Consoleを通じて行われます。ユーザーは電子メールで送信された招待に応答できますが、ユーザーがコンソールのアカウントを持っていない場合は、招待を承諾できるようにサインアップする必要があります。

開始する前に

- ユーザー名は招待状のメールアドレスです。
- 割り当てるユーザー ロールを理解します。
- パスワードはサインアッププロセス中にユーザーによって定義されます。

手順

1. Data Infrastructure Insightsサイトにログイン
2. メニューで*管理>ユーザー管理*をクリックします

   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

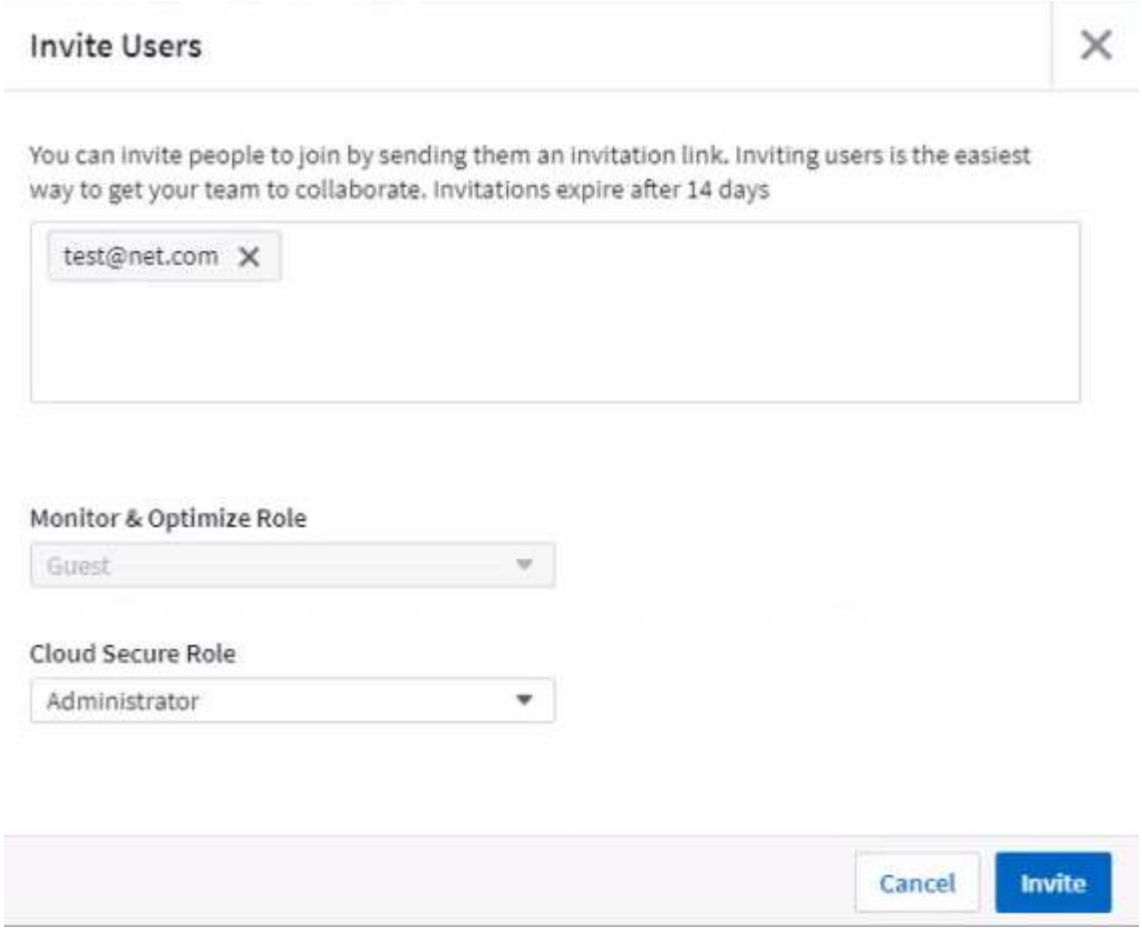
   *ユーザーを招待*画面が表示されます。

4. 招待用の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、それらはすべて同じ役割で作成されます。複数のユーザーを同じロールにのみ設定できます。

5. Data Infrastructure Insightsの各機能に対するユーザーの役割を選択します。

   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、レポート内の任意のロールにユーザーを割り当てることができますが、可観測性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

   招待状がユーザーに送信されます。ユーザーには招待を承諾するまで 14 日間の猶予があります。ユーザーが招待を承諾すると、 NetAppクラウド ポータルに移動し、招待状に記載されている電子メール アドレスを使用してサインアップします。そのメール アドレスの既存のアカウントがある場合は、サインインするだけで、 Data Infrastructure Insights環境にアクセスできるようになります。

既存のユーザーの役割を変更する

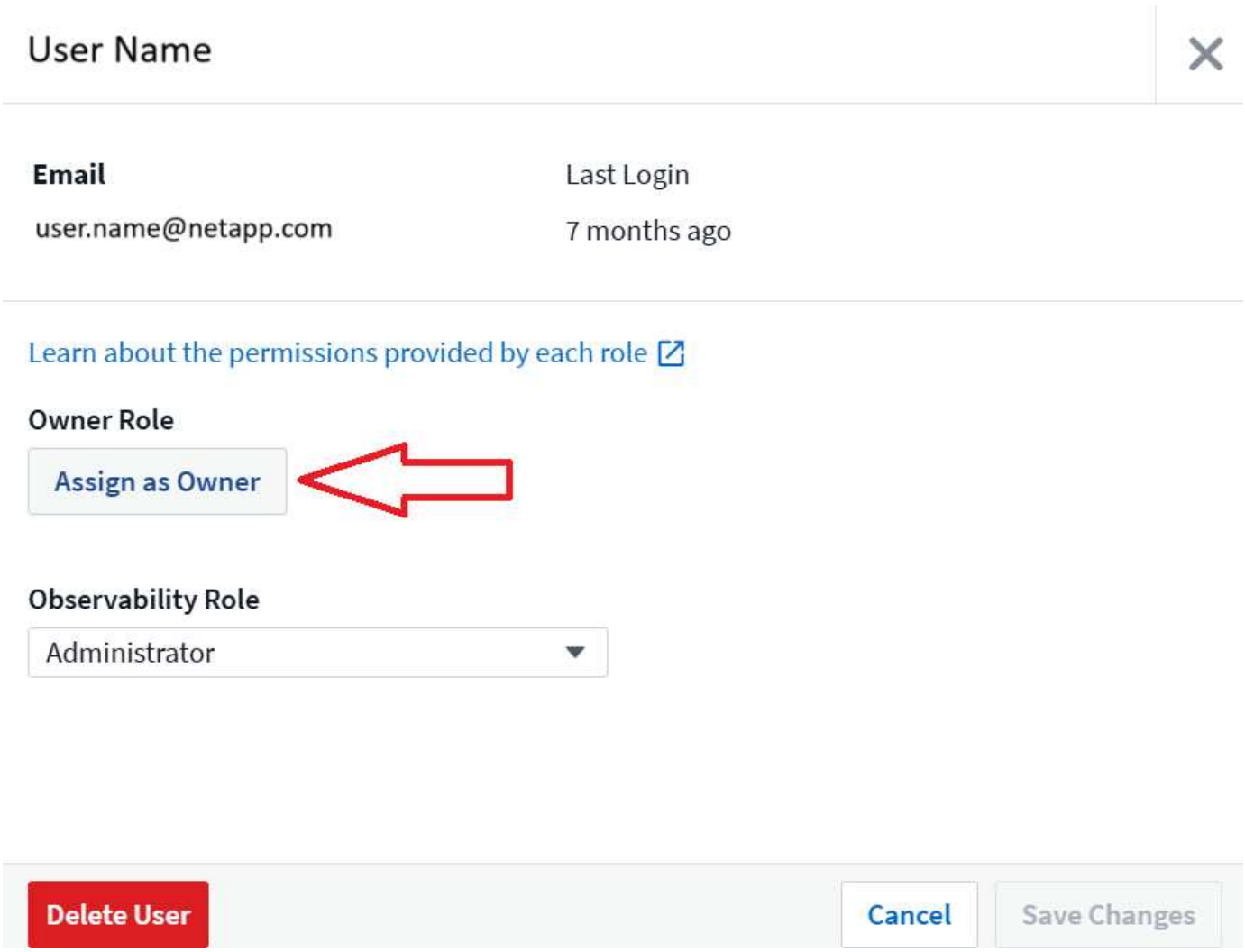
既存のユーザーの役割を変更するには（*セカンダリ アカウント所有者*として追加するなど）、次の手順に従います。

1. *管理 > ユーザー管理*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. 変更したいアカウントのユーザー名をクリックします。
3. 必要に応じて、各Data Infrastructure Insights機能セットにおけるユーザーの役割を変更します。
4. [変更を保存]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

アカウント所有者のロールを別のユーザーに割り当てるには、Observability 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. *管理 > ユーザー管理*をクリックします。
2. 変更したいアカウントのユーザー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必要な数だけ持つことができますが、ベストプラクティスとしては、所有者の役割を特定のユーザーのみに制限します。

ユーザーの削除

管理者ロールを持つユーザーは、ユーザー名をクリックし、ダイアログで [ユーザーの削除] をクリックすることで、ユーザー (たとえば、会社を退職したユーザー) を削除できます。ユーザーはData Infrastructure Insights環境から削除されます。

ユーザーが作成したダッシュボードやクエリなどは、ユーザーが削除された後もData Infrastructure Insights環境で引き続き利用できることに注意してください。

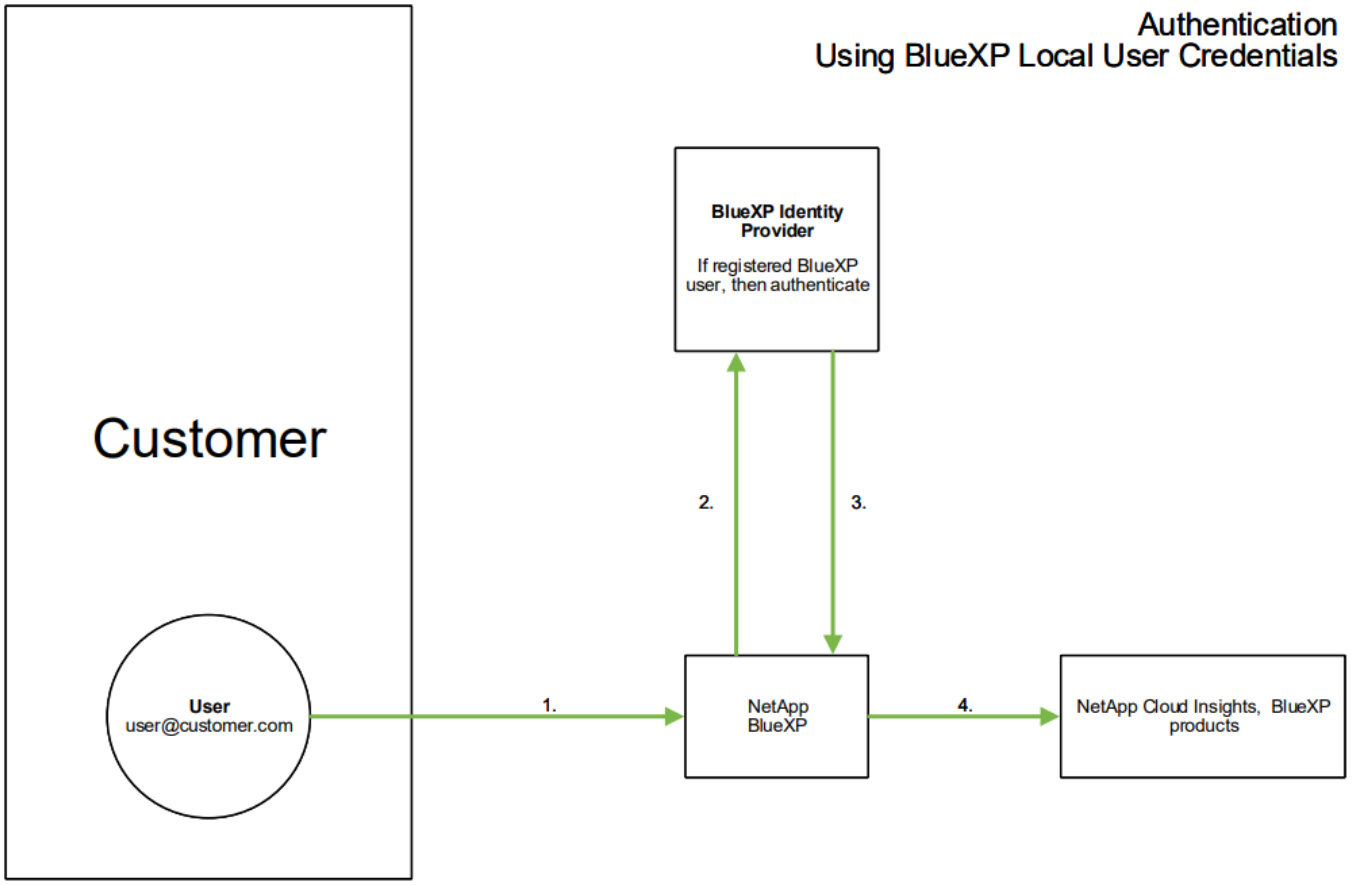
シングルサインオン（SSO）とアイデンティティフェデレーション

アイデンティティフェデレーションとは何ですか?

アイデンティティフェデレーションを使用する場合:

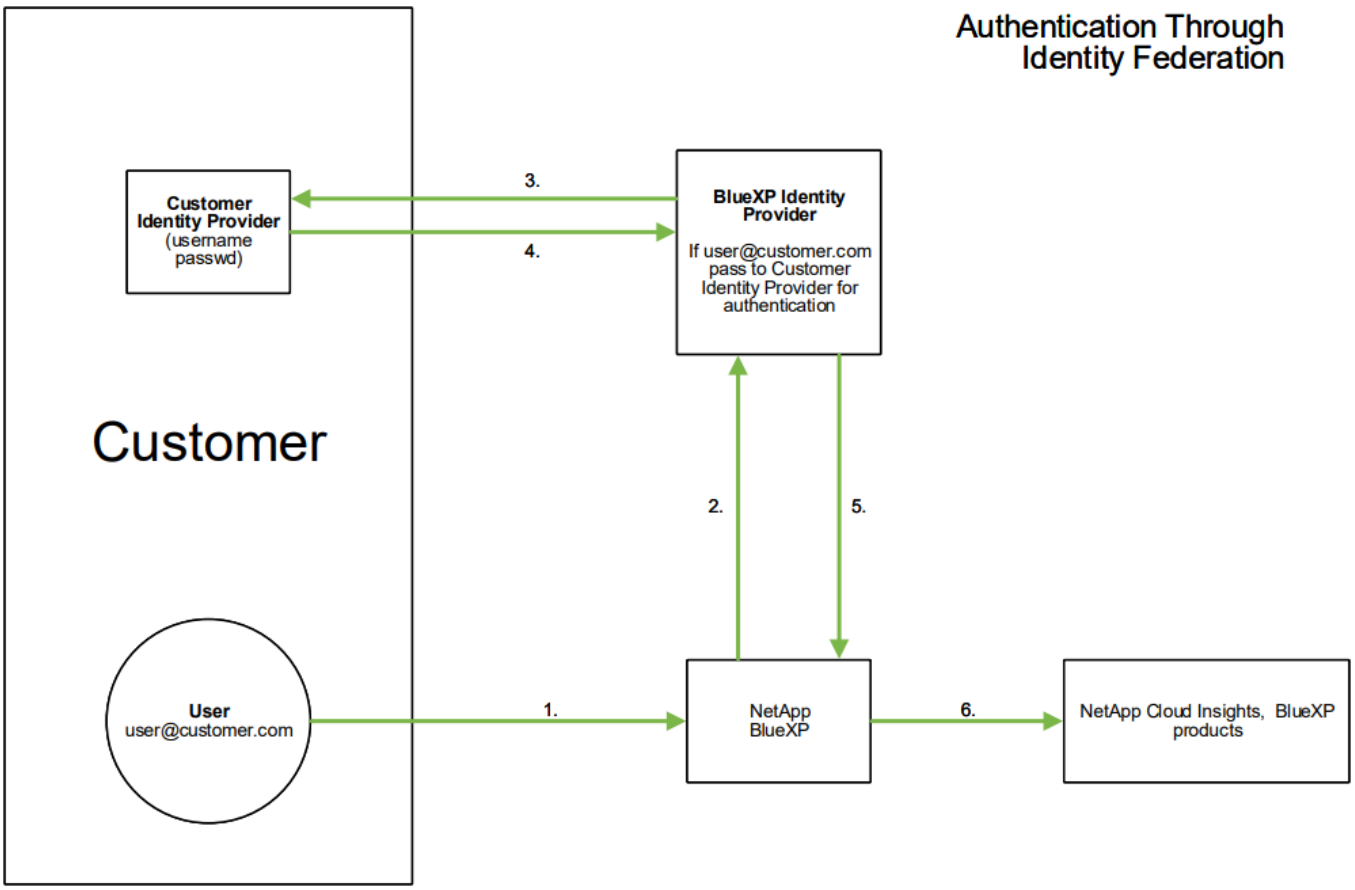
- 認証は、企業ディレクトリの顧客の資格情報と、多要素認証 (MFA) などの自動化ポリシーを使用して、顧客の ID 管理システムに委任されます。
- ユーザーはすべてのNetApp Consoleサービスに一度ログインします (シングル サインオン)。

すべてのクラウド サービスのユーザー アカウントは、NetApp Consoleで管理されます。デフォルトでは、認証はコンソールのローカル ユーザー プロファイルを使用して行われます。以下にそのプロセスの簡略化された概要を示します。



ただし、お客様によっては、 Data Infrastructure Insightsやその他のNetApp Consoleサービスのユーザーを認証するために独自の ID プロバイダーを使用したいと考えています。 Identity Federation を使用すると、NetApp Consoleアカウントは企業ディレクトリの資格情報を使用して認証されます。

以下はそのプロセスの簡略化された例です。



上の図では、ユーザーがData Infrastructure Insightsにアクセスすると、そのユーザーは認証のために顧客の ID 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、ユーザーはData Infrastructure Insightsテナント URL に誘導されます。

アイデンティティフェデレーションの有効化

コンソールは Auth0 を使用して ID フェデレーションを実装し、Active Directory Federation Services (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構成するには、"連盟の指示" 。

Data Infrastructure Insightsで SSO を使用する前に、Identity Federation を構成する必要があります。

アイデンティティ フェデレーションの変更は、Data Infrastructure Insightsだけでなく、すべてのNetApp Consoleサービスに適用されることを理解することが重要です。お客様は、所有する各製品のNetAppチームとこの変更について話し合い、使用している構成が Identity Federation で機能するか、アカウントに調整が必要かどうかを確認する必要があります。顧客は、アイデンティティ フェデレーションへの変更に社内の SSO チームも関与させる必要があります。

また、ID フェデレーションを有効にすると、会社の ID プロバイダーに変更を加える場合 (SAML から Microsoft AD への移行など)、ユーザーのプロファイルを更新するためにトラブルシューティングや変更、注意が必要になる可能性が高いことを認識しておくことも重要です。

この問題やその他のフェデレーションの問題については、次の場所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 。

シングルサインオン（SSO）ユーザー自動プロビジョニング

管理者は、ユーザーを招待するだけでなく、企業ドメイン内のすべてのユーザーに対して、個別に招待することなく、 Data Infrastructure Insightsへの シングル サインオン **(SSO)** ユーザー自動プロビジョニング アクセスを有効にできます。 SSO を有効にすると、同じドメインの電子メール アドレスを持つすべてのユーザーが、企業の資格情報を使用してData Infrastructure Insightsにログインできるようになります。

> *SSO* ユーザー自動プロビジョニング はData Infrastructure Insights Premium Edition で使用できますが、 Data Infrastructure Insightsで有効にする前に構成する必要があります。 SSOユーザー自動プロビジョニング構成には以下が含まれます"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 Console経由で実行します。フェデレーションにより、シングル サインオン ユーザーは、Security Assertion Markup Language 2.0 (SAML) や OpenID Connect (OIDC) などのオープン スタンダードを使用して、企業ディレクトリの資格情報を使用してNetApp Consoleアカウントにアクセスできるようになります。

SSO ユーザー自動プロビジョニング を構成するには、管理 **>** ユーザー管理 ページで、まず Identity Federation を設定する必要があります。バナーの*フェデレーションの設定*リンクを選択して、コンソール フェデレーションに進みます。設定が完了すると、 Data Infrastructure Insights管理者は SSO ユーザー ログインを有効にできるようになります。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 ユーザーのデフォルト ロール (ゲストやユーザーなど) を選択します。 SSO 経由でログインするユーザーには、そのデフォルトのロールが与えられます。



場合によっては、管理者が 1 人のユーザーをデフォルトの SSO ロールから昇格させたい場合があります (たとえば、管理者にするなど)。これは、管理者 **>** ユーザー管理 ページで、ユーザーの右側のメニューをクリックして [役割の割り当て] を選択することで実行できます。このように明示的にロールを割り当てられたユーザーは、その後 *SSO* ユーザー自動プロビジョニング が無効になっても、引き続きData Infrastructure Insightsにアクセスできます。

ユーザーが昇格されたロールを必要としなくなった場合は、メニューをクリックして [ユーザーの削除] できます。ユーザーはリストから削除されます。 *SSO* ユーザー自動プロビジョニング が有効になっている場合、ユーザーはデフォルトのロールを使用して、SSO を介してData Infrastructure Insightsに引き続きログインできます。

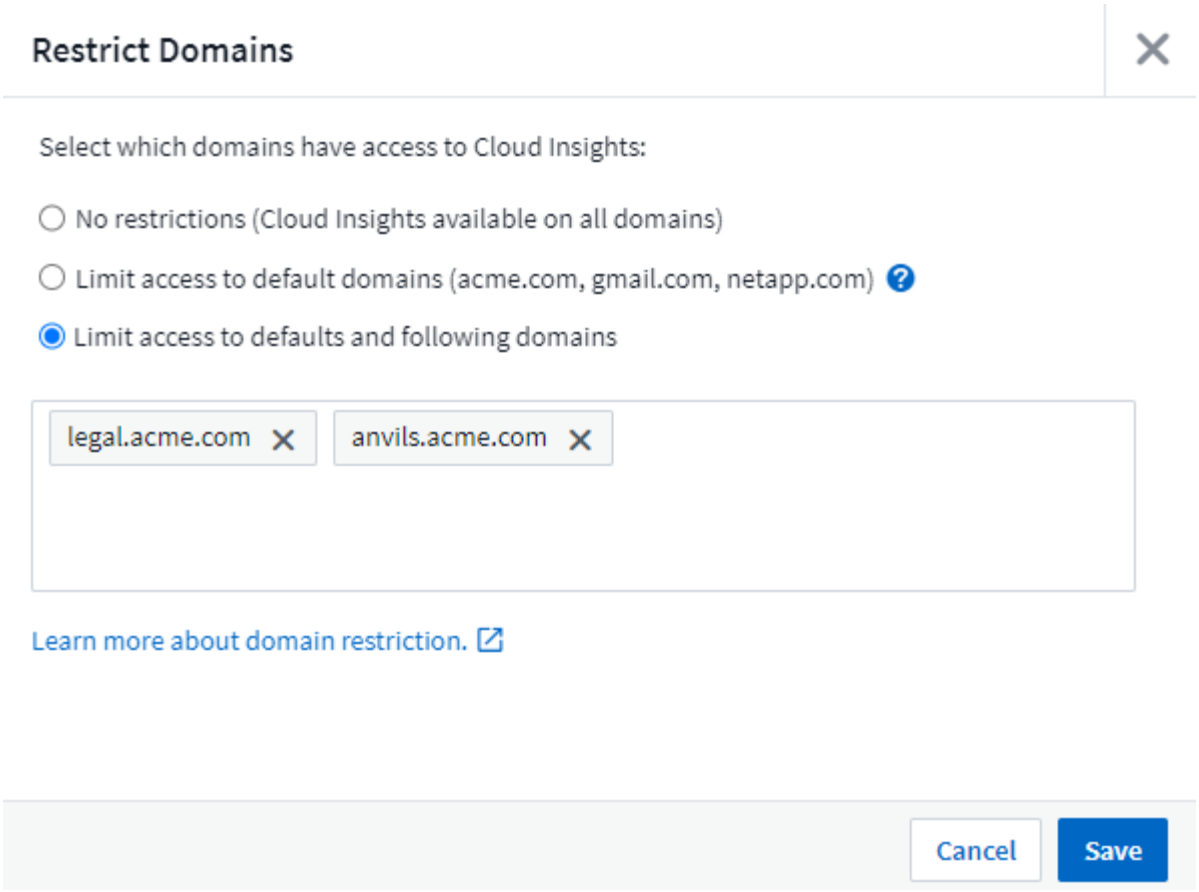
SSO ユーザーを表示 チェックボックスをオフにすると、SSO ユーザーを非表示にすることができます。

ただし、次のいずれかに該当する場合は、*SSO* ユーザー自動プロビジョニング を有効にしないでください。

- 組織には複数のData Infrastructure Insightsテナントがあります
- 組織では、フェデレーション ドメイン内のすべてのユーザーがData Infrastructure Insightsテナントに一定レベルの自動アクセス権を持つことを望んでいません。 現時点では、このオプションを使用してグループを使用してロール アクセスを制御する機能はありません。

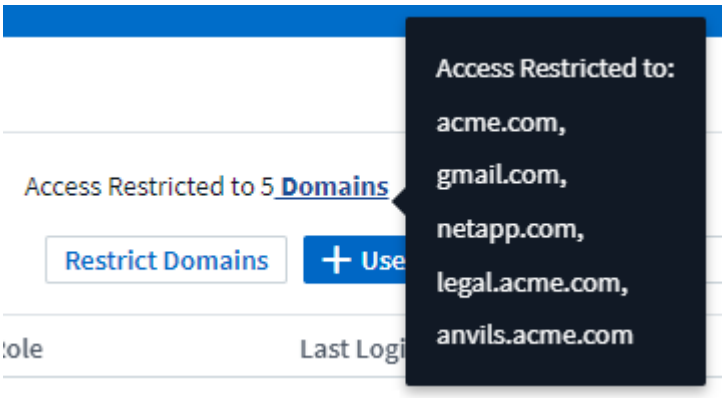
ドメインによるアクセス制限

Data Infrastructure Insights、指定したドメインのみにユーザー アクセスを制限できます。 管理 **>** ユーザー管理 ページで、「ドメインの制限」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、ユーザーは引き続き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します。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いつでもアクセス可能です。
- デフォルトと指定した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すべてリストします。



Data Infrastructure Insightsデータコレクターリファレンスリスト

Data Infrastructure Insights は、多くのベンダーやサービスからのさまざまなデータ コレクターをサポートしています。

データ コレクターは次のタイプに分類されます。

- インフラストラクチャ: 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 デバイスから取得されます。
- サービス: Kubernetes や Docker などのサービスから取得されます。 *Integration* とも呼ばれます。

Data Infrastructure Insightsでサポートされているデータ コレクターのアルファベット順リスト:

データコレクター	タイプ
"Amazon EC2 と EBS"	インフラ
"ストレージとしての AWS S3"	インフラ
"Amazon FSx for NetApp ONTAP"	インフラ
"アパッチ"	サービス
"Azure NetApp Files"	インフラ
"Azure VM と VHD"	インフラ
"Brocadeネットワーク アドバイザー (BNA)"	インフラ
"Brocadeファイバーチャネルスイッチ"	インフラ
"BrocadeFOS REST"	インフラ
"Cisco MDS ファブリック スイッチ"	インフラ
"領事"	サービス
"カウチベース"	サービス
"カウチDB"	サービス
"Cohesity スマートファイル"	インフラ
"Dell EMC データドメイン"	インフラ
"デル EMC ECS"	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 リカバリポイント"	インフラ
"Dell EMC スケールIO/PowerFlex"	インフラ
"Dell EMC ユニティ"	インフラ

データコレクター	タイプ
"Dell EMC ユニスフィア REST"	インフラ
"Dell EMC VMAX/PowerMaxデバイスファミリー"	インフラ
"Dell EMC VNX ブロック ストレージ"	インフラ
"Dell EMC VNX ファイル"	インフラ
"Dell EMC VNX 統合"	インフラ
"デル EMC VPLEX"	インフラ
"デル EMC XtremIO"	インフラ
"Dell XCシリーズ"	インフラ
"Docker"	サービス
"Elasticsearch"	サービス
"フリンク"	サービス
"富士通 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
"Google Cloud NetApp Volumes"	インフラ
"Hadoop"	サービス
"HAプロキシ"	サービス
"日立コンテンツプラットフォーム（HCP）"	インフラ
"日立ヴァンタラコマンドスイート"	インフラ
"日立ヴァンタラNASプラットフォーム"	インフラ
"日立オプスセンター"	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 エンタープライズ コマンド ビュー"	インフラ
"Huawei OceanStorおよびDoradoデバイス"	インフラ
"IBM クレバーセーフ"	インフラ
"IBM CSシリーズ"	インフラ
"IBM SAN ボリューム コントローラー (SVC)"	インフラ
"IBM システムストレージ DS8000 シリーズ"	インフラ
"IBM XIV および A9000 ストレージ"	インフラ
"インフィニダット インフィニボックス"	インフラ
"Java"	サービス
"カフカ"	サービス

データコレクター	タイプ
"カパシター"	サービス
"キバナ"	サービス
"Kubernetes"	サービス
"レノボ HXシリーズ"	インフラ
"メムキャッシュ"	サービス
"Microsoft Azure NetApp Files"	インフラ
"Microsoft Hyper-V"	インフラ
"MongoDB"	サービス
"MySQL"	サービス
"NetAppCloud Volumes ONTAP"	インフラ
"ONTAP 9.9以降向けNetAppクラウド接続"	インフラ
"NetApp Data ONTAP 7-Mode"	インフラ
"NetApp Eシリーズ"	インフラ
"NetApp Eシリーズ REST"	インフラ
"Amazon FSx for NetApp ONTAP"	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コレクター"	インフラ
"NetApp ONTAP AFX"	インフラ
"NetApp ONTAP ASA r2（オールSANアレイ）コレクター"	インフラ
"NetApp ONTAP Select"	インフラ
"NetApp SolidFireオールフラッシュアレイ"	インフラ
"NetAppStorageGRID"	インフラ
"ネットスタット"	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
"オープンZFS"	サービス
"Oracle ZFSストレージアプライアンス"	インフラ
"PostgreSQL"	サービス
"操り人形エージェント"	サービス
"ピュアストレージ フラッシュアレイ"	インフラ

データコレクター	タイプ
"レッドハット仮想化"	インフラ
"レディス"	サービス
"DBを再考する"	サービス
"RHEL と CentOS"	サービス
"ルーブリック CDM ストレージ"	インフラ
"UbuntuとDebian"	サービス
"VAST データストア"	インフラ
"VMware vSphere"	インフラ
"Windows"	サービス
"動物園飼育員"	サービス

Data Infrastructure Insightsの購読

Data Infrastructure Insightsの使用を開始するのは、次の 3 つの簡単な手順で完了します。

1. アカウント登録はこちら"* NetApp Console*"NetApp のすべてのクラウド サービスにアクセスできます。
2. 利用可能な機能を調べるには、 Data Infrastructure Insightsの無料トライアルに登録してください。無料トライアルに登録するには:
   - へ移動 https://netapp.com
   - ページ上部の*購入方法*を選択します。
   - *トライアルをリクエスト*を選択します。コンソールにまだ登録していない場合は、詳細を入力してサインアップしてください。それ以外の場合はサインインしてください。
   - 会議をスケジュールするか、担当者がトライアルに関して連絡するのをお待ちください。
3. さまざまな柔軟なサブスクリプション オプションを通じて、データへの継続的かつ中断のないアクセスを実現するには、 Data Infrastructure Insightsに*サブスクライブ*してください。
   - "NetAppセールスダイレクト"
   - AWS マーケットプレイス:
     - "固定期間サブスクリプション"
     - "従量課金制サブスクリプション"
     - "固定ベース + 従量課金超過サブスクリプション"
   - "Azureマーケットプレイス"（すべてのサブスクリプションオプション）

登録プロセス中に、 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をご覧ください。"情報と地域" 。

Data Infrastructure Insights機能と価格オプションの詳細については、"Data Infrastructure Insightsエディション"ページ。

Data Infrastructure Insightsの使用中に、南京錠アイコンが表示された場合  は、その機能が現在のサブスクリプションでは利用できないか、制限された形でしか利用できないことを意味します。フルアクセスするには、その機能に登録してください。一部の機能は、モジュール評価購読する前に。

トライアル版

Data Infrastructure Insightsにサインアップし、環境がアクティブになると、 Data Infrastructure Insightsの 30 日間無料トライアルが開始されます。このトライアル期間中、 Data Infrastructure Insightsが提供する機能を独自の環境で試すことができます。

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に加入すると、データへの中断のないアクセスと拡張された"製品サポート"オプション。

無料トライアルの終了が近づくと、 Data Infrastructure Insightsにバナーが表示されます。そのバナー内には [サブスクリプションの表示] リンクがあり、これをクリックすると 管理者 → サブスクリプション ページが開きます。管理者以外のユーザー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を評価するために追加の時間が必要で、試用期間が 4 日以内に終了する場合は、試用期間をさらに 30 日間延長できます。試用期間を延長できるのは 1 回のみです。試用期間が終了している場合は延長できません。

AWS Marketplace でのトライアル

AWS Marketplace を通じて無料トライアルにサインアップすることもできます。 AWS Marketplace の無料トライアルでは、33 日間の試用期間中、 Data Infrastructure Insightsにアクセスできます。

AWS Marketplace の無料トライアルは延長できません。

試用期間が終了したらどうなりますか?

無料トライアルの有効期限が切れており、まだData Infrastructure Insightsに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停止される場合があり、数週間後には、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の 5 日間の猶予期間が与えられます。この猶予期間中、すべてのData Infrastructure Insights機能はアクティブなままになります。

猶予期間が経過すると、更新するまでData Infrastructure Insights の機能は停止されます。更新するには、管理者 > サブスクリプション ページを参照するか、 NetApp の営業部門にお問い合わせください。

猶予期間後、 Data Infrastructure Insights のデータは 30 日間そのまま残ります。この期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できるようになります。

モジュール評価

*モジュール評価*を利用することもできます。たとえば、すでに Infrastructure Observability に加入していて、環境に Kubernetes を追加する場合、 NetApp Kubernetes Monitoring Operator をインストールした時点から 30 日間の Kubernetes Observability 評価が自動的に開始されます。評価期間の終了時に、Kubernetes Observability 管理対象ユニットの使用量に対してのみ課金されます。

評価後には新しい管理対象ユニット (MU) の使用料が発生することにご注意ください。それに応じて計画を立ててください。モジュールの評価が終了すると、サービスの中断を避けるために MU を追加する必要があるかどうかが通知されます。

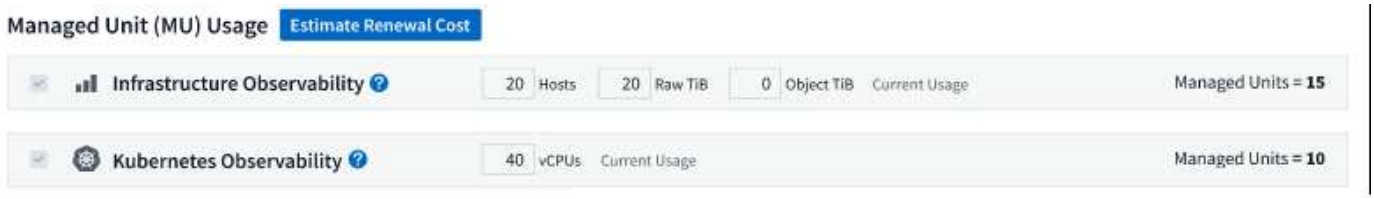
管理対象ユニットの使用状況は、管理 > サブスクリプション ページの 使用状況 タブで監視できます。



モジュール評価 は トライアル ではありません。トライアルという用語は、適合性を確認して購入を可能にするために、顧客にData Infrastructure Insightsサービスの無料トライアル期間を提供する場合に使用します。モジュール評価は異なります。これは、有料のお客様が、有料サブスクリプションの過去数か月間に使用していなかったData Infrastructure Insightsのモジュールを試用できるようにするものです。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みの料金が免除されます。顧客の作業環境はまだサブスクリプション中であり、無料トライアルに戻っていません。サブスクリプションは変更されていません。

見積もり

モジュールの評価中は、モジュールで消費されたリソースに対して MU 使用量は請求されませんが、見積もり (概要 タブ) を開いて、評価後に MU がどのように請求されるかを確認したり、将来必要になる可能性のある MU の数に関する「What if」シナリオを試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選択して、モジュール全体の MU を見積コストに追加または削除します。

また、Estimator を使用すると、現在のサブスクリプション期間を維持し、ライセンスされた管理対象ユニットの数を増やすアドオン、または現在のサブスクリプション期間が終了した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数値を確認することもできます。

お客様は、サブスクリプションごとに 1 回のみモジュール評価を受けることができることに注意してください。

サブスクリプションオプション

登録するには、管理者 → サブスクリプション に移動します。 サブスクライブ ボタンに加えて、インストールされているデータ コレクターを確認し、推定計測値を計算することもできます。一般的な環境では、セルフサービス AWS Marketplace ボタンをクリックできます。環境に 1,000 個以上の管理対象ユニットが含まれているか、含まれることが予想される場合は、ボリューム価格設定の対象となります。

可観測性メータリング

Data Infrastructure Insightsの可観測性は、次の 2 つの方法のいずれかで計測されます。

- 容量計測
- 管理対象ユニットメータリング（レガシー）

既存のサブスクリプションがあるか、新しいサブスクリプションを開始するかに応じて、サブスクリプションはこれらの方法のいずれかで計測されます。

容量計測

Data Infrastructure Insights Observability は、テナント上のストレージの層に応じて使用状況を測定します。以下の 1 つ以上のカテゴリに該当するストレージがある可能性があります。

- プライマリー生
- オブジェクト生
- クラウド消費量

各層は異なるレートで計測され、全体を合計して加重権利が与えられます。加重使用量を計算する式は次のとおりです。

```
 Weighted Capacity = Raw TiB + (0.1 x Object Tier Raw TiB) + (0.25 x Cloud Tier Provisioned TiB)
```

これを容易にするために、`DII` は、_サブスクライブされた_量に基づいて単一の*加重権利*数を計算します。次に、_検出された_ストレージに基づいて同じ数を計算し、検出された容量が加重権利よりも大きい場合にのみ違反を宣言します。これにより、各層のサブスクライブ量とは異なる数量を柔軟に監視できるようになります。これは、検出されたストレージの合計がサブスクライブされた加重資格の範囲内である限り、`DII` によって許可されます。

管理対象ユニットメータリング（レガシー）

管理対象ユニット*ごとの**Data Infrastructure Insights**インフラストラクチャ オブザーバビリティおよび **Kubernetes** オブザーバビリティ メーター使用量。管理対象ユニットの使用量は、インフラストラクチャ環境で管理されている *ホストまたは仮想マシン の数と 未フォーマット容量 の量に基づいて計算されます。

- 1 つの管理対象ユニット = 2 つのホスト (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未フォーマット容量 4 TiB
- 1 管理対象ユニット = 選択したセカンダリストレージの未フォーマット容量 40 TiB: AWS S3、Cohesity SmartFiles、Dell EMC Data Domain、Dell EMC ECS、Hitachi Content Platform、IBM Cleversafe、

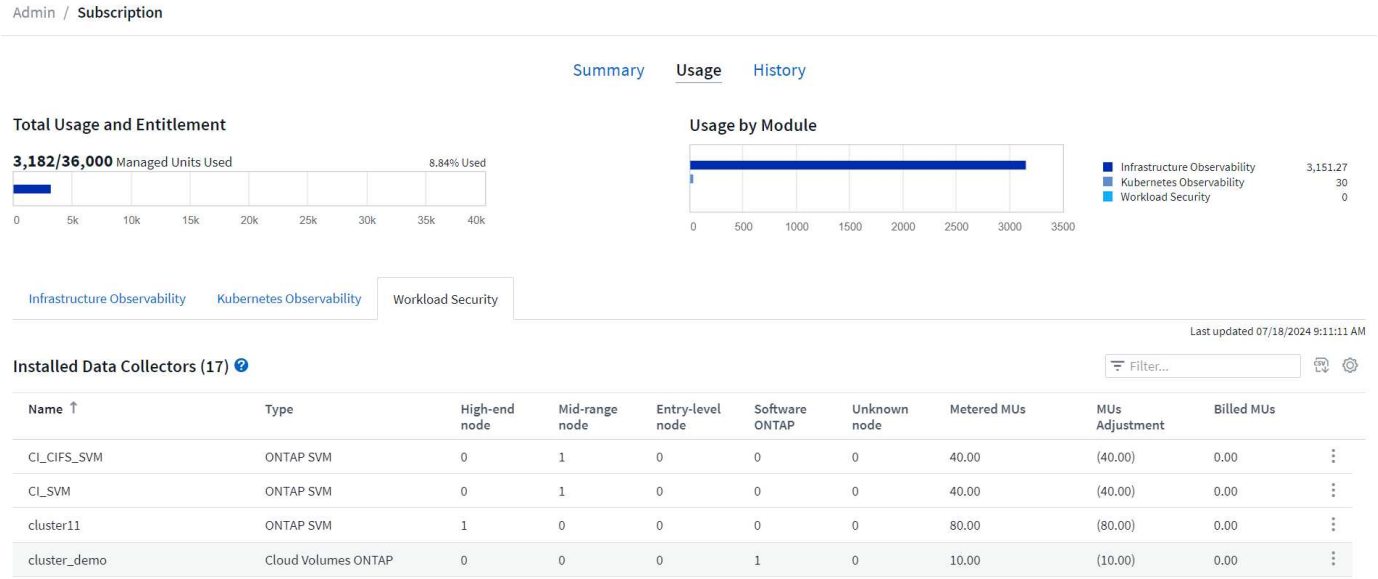
NetApp StorageGRID、Rubrik。

- 1 つの管理対象ユニット = 4 つの Kuberentes vCPU。
  - 1 つの管理対象ユニット K8s 調整 = インフラストラクチャによっても監視される 2 つのノードまたはホスト。

ワークロードセキュリティメータリング

Workload Security は、Observability 計測と同じアプローチを使用して Cluster によって計測されます。

Workload Security の使用状況は、管理 > サブスクリプション ページの **Workload Security** タブで確認できます。



既存の Workload Security サブスクリプションでは、ノードの使用によって管理対象ユニットが消費されないように MU の使用量が調整されます。 Data Infrastructure Insights は使用状況を計測し、ライセンスされた使用状況への準拠を確保します。

どうやって登録すればいいですか?

管理対象ユニット数が1,000未満の場合は、 NetApp Sales経由で申し込むか、セルフサブスクライブ AWS Marketplace 経由。

NetApp Sales Directを通じて申し込む

予想される管理対象ユニット数が1,000以上の場合は、"営業部へのお問い合わせ" NetAppセールス チームを通じてサブスクライブするためのボタン。

有料サブスクリプションをData Infrastructure Insights Data Infrastructure Insights Insights の シリアル番号をNetApp の営業担当者に提供する必要があります。シリアル番号は、Data Infrastructure Insights の試用環境を一意に識別するもので、管理 > サブスクリプション ページで確認できます。

AWS Marketplace を通じてセルフサブスクライブ

既存のData Infrastructure Insightsトライアルアカウントに AWS Marketplace サブスクリプションを適用するには、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マーケットプレイスのリンクをクリックするとと AWSが開きます "Data Infrastructure Insights"サブスクリプションページで、サブスクリプションを完了できます。計算ツールに入力した値は AWS サブスクリプション ページには入力されないことに注意してください。このページで管理対象ユニットの合計数を入力する必要があります。

管理対象ユニットの合計数を入力し、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 サブスクリプションプロセスが完了すると、 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)、NetAPp コンソールのサインイン ページに移動します。 Data Infrastructure Insightsに再度サインインすると、サブスクリプションがアクティブになります。

AWS Marketplace ページで アカウントの設定 をクリックした後、1 時間以内に AWS サブスクリプションプロセスを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、再度「アカウントの設定」をクリックしてプロセスを完了する必要があります。

問題が発生してサブスクリプション プロセスが正しく完了しなかった場合でも、環境にログインすると「試用版」バナーが表示されます。この場合は、管理 > サブスクリプション に移動して、サブスクリプション プロセスを繰り返すことができます。

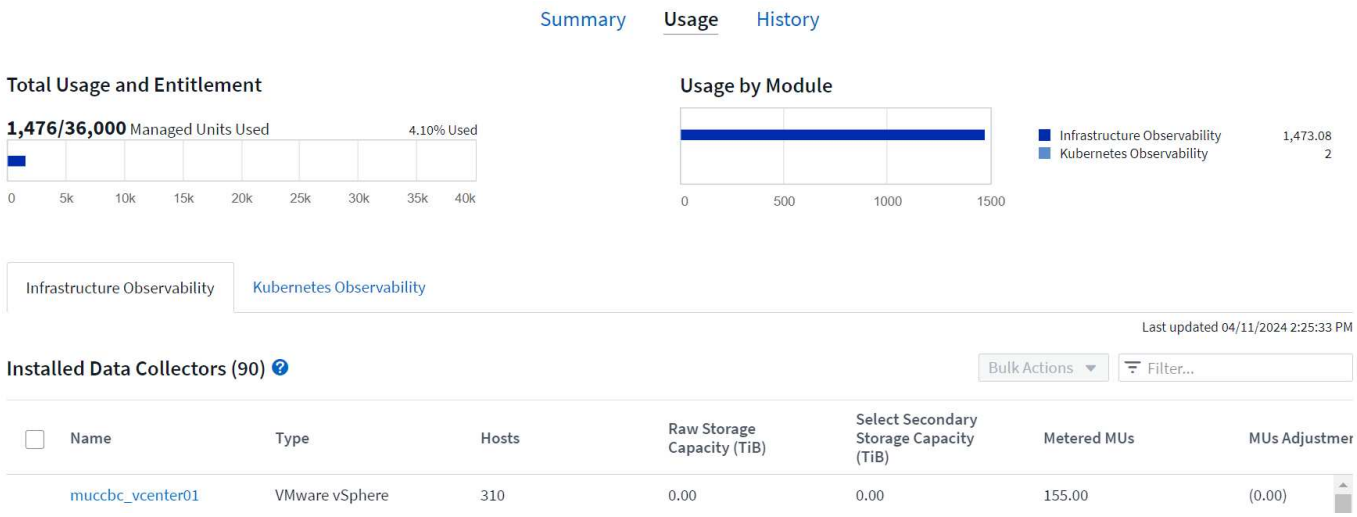
サブスクリプションのステータスを表示する

サブスクリプションがアクティブになると、管理 > サブスクリプション ページからサブスクリプションのステータスと管理対象ユニットの使用状況を確認できます。

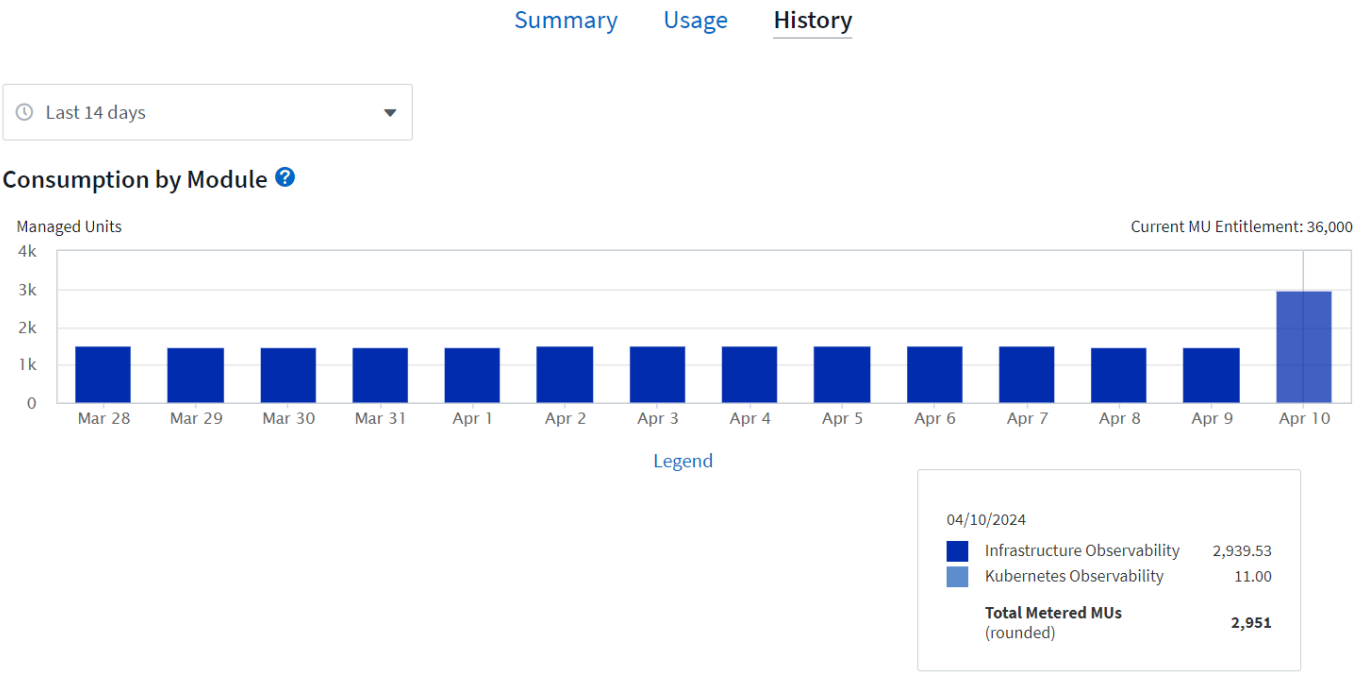
サブスクリプションの*概要*タブには次のような内容が表示されます。

- 最新版
- サブスクリプションのシリアル番号
- 現在のMU資格

*使用状況*タブには、現在の MU の使用状況と、その使用状況がデータ コレクターごとにどのように内訳されているかが表示されます。



*履歴*タブでは、過去 7 日から 90 日間の MU の使用状況を確認できます。グラフ内の列にマウスを移動すると、モジュール (Observability、Kubernetes など) ごとの内訳が表示されます。



使用状況管理を表示する

使用状況管理タブには、管理対象ユニットの使用状況の概要と、コレクターまたは Kubernetes クラスター別に管理対象ユニットの消費量を分類したタブが表示されます。

未フォーマット容量の管理対象ユニット数は、環境内の総生容量の合計を反映し、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、概要セクションのデータ コレクターの数と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 コレクター リスト内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わずかに高くなる場合があります。概要セクションには、サブスクリプションの実際の管理対象ユニット数が反映されます。

使用量がサブスクライブした量に近づいたり超えたりした場合は、データ コレクターを削除するか、Kubernetes クラスターの監視を停止することで使用量を削減できます。このリスト内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 [削除] を選択します。

登録した使用量を超えた場合はどうなりますか?

管理対象ユニットの使用量が合計サブスクリプション量の 80%、90%、100% を超えると、警告が表示されます。

使用量が超過した場合:	このようなことが起こる場合 / 推奨されるアクション:
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。サブスクライブしている管理対象ユニットの数を増やす必要がある場合があります。
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。 • 管理対象ユニットの使用量がサブスクリプションの量以下になるようにデータコレクターを削除します • サブスクリプションを変更して、サブスクライブされた管理対象ユニットの数を増やします

直接購読してトライアルをスキップ

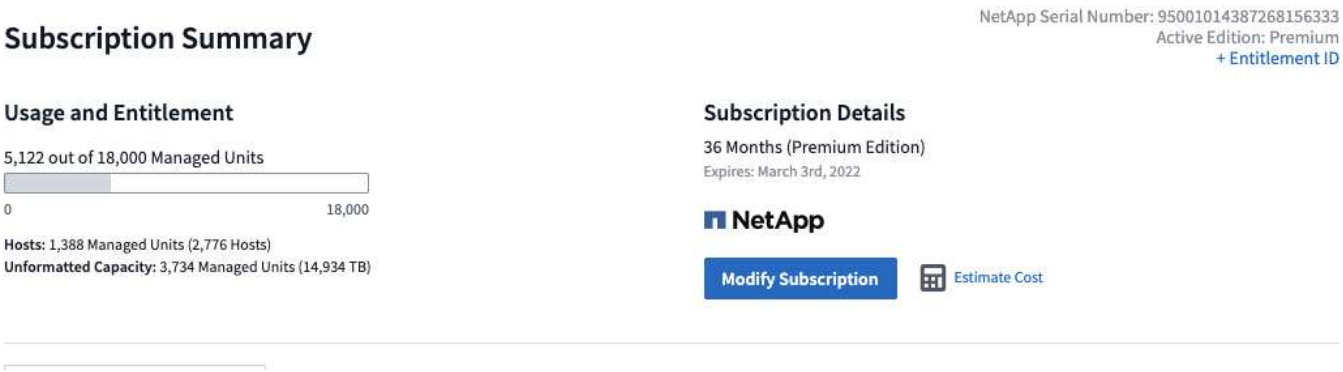
また、 Data Infrastructure Insightsを以下のサイトから直接購読することもできます。 "AWS マーケットプレイス"最初に試用環境を作成せずに。サブスクリプションが完了し、環境がセットアップされると、すぐにサブスクリプションが開始されます。

資格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、これを *Entitlement ID* と呼びます。

Data Infrastructure Insightsサブスクリプションに資格 ID を追加するには、管理者 > サブスクリプション ペー

ジで、+ 資格 *ID* をクリックします。



可観測性

ダッシュボードの作成

ダッシュボードの概要

Data Infrastructure Insights は、さまざまなウィジェットを使用してカスタム ダッシュボードを作成できるようにすることで、インフラストラクチャ データの運用ビューを柔軟に作成できるようにします。各ウィジェットは、データの表示とグラフ化に非常に柔軟に対応します。

これらのセクションの例は説明のみを目的としており、考えら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。ここで説明する概念と手順を使用すると、独自のダッシュボードを作成し、特定のニーズに固有のデータを強調表示することができます。

ダッシュボードの作成

新しいダッシュボードは、次の 2 つの場所のいずれかで作成します。

- 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

実際に動作を見てみましょう

"NetAppで強力なダッシュボードを作成する (ビデオ)"

ダッシュボードコントロール

ダッシュボード画面にはいくつかのコントロールがあります。

- 時間セレクター: 過去 15 分間から過去 30 日間までの時間範囲、または最大 31 日間のカスタム時間範囲のダッシュボード データを表示できます。個々のウィジェットでこのグローバル時間範囲を上書きすることもできます。
- 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] メニューから [名前の変更] をクリックすると、現在のダッシュボードの名前を変更できます。

- **+** ウィジェットを追加 ボタンを使用すると、任意の数のテーブル、グラフ、またはその他のウィジェットをダッシュボードに追加できます。

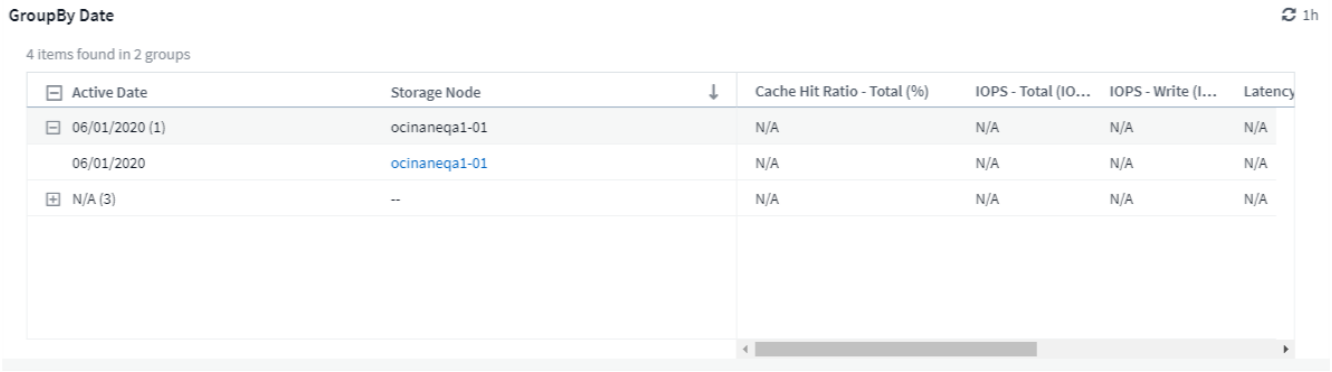
  ウィジェットはサイズを変更したり、ダッシュボード内のさまざまな位置に再配置したりできるため、現在のニーズに応じてデータを最適に表示できます。

- **+** 変数を追加 ボタン。変数を使用してダッシュボードのデータをアクティブにフィルターできます。

ウィジェットの種類

次のウィジェット タイプから選択できます。

- テーブル ウィジェット: 選択したフィルターと列に従ってデータを表示するテーブル。テーブル データは、折りたたんだり展開したりできるグループにまとめることができます。



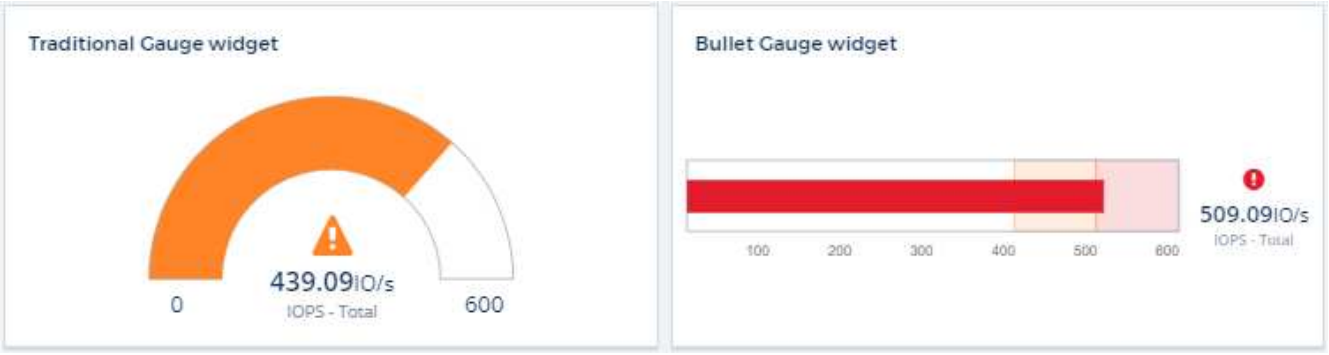
- 折れ線グラフ、スプライン グラフ、面グラフ、積み上げ面グラフ: これらは、時間の経過に伴うパフォーマンスやその他のデータを表示できる時系列グラフ ウィジェットです。



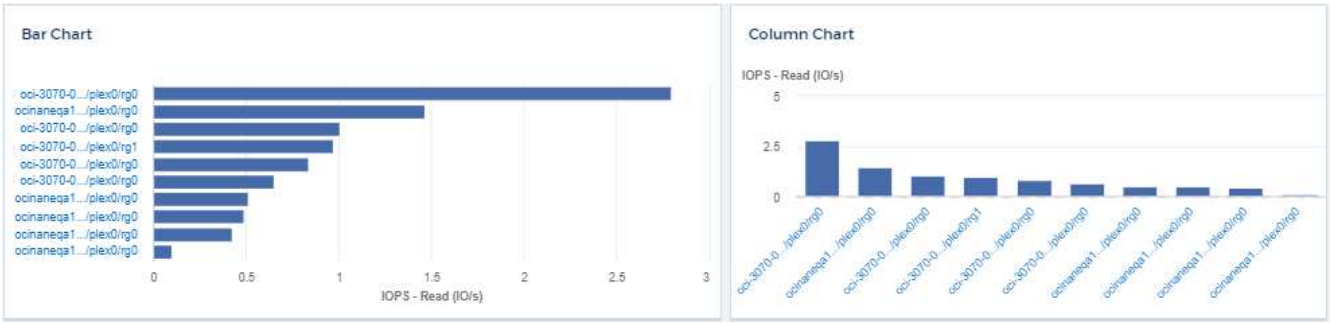
- 単一値ウィジェット: カウンターから直接取得するか、クエリまたは式を使用して計算できる単一の値を表示できるウィジェット。値が予想範囲内、警告範囲内、または重大な範囲内にあるかどうかを示すために、色の書式設定しきい値を定義できます。



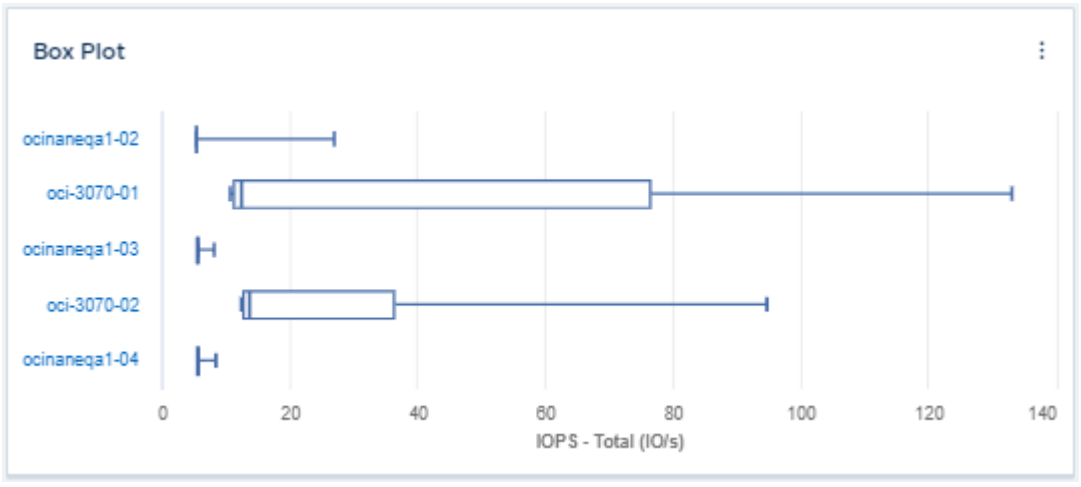
- ゲージウィジェット: 従来の（実線）ゲージまたは弾丸ゲージに単一値データを表示し、「警告」または「重大」な値に基づいて色分けします。"カスタマイズ" 。



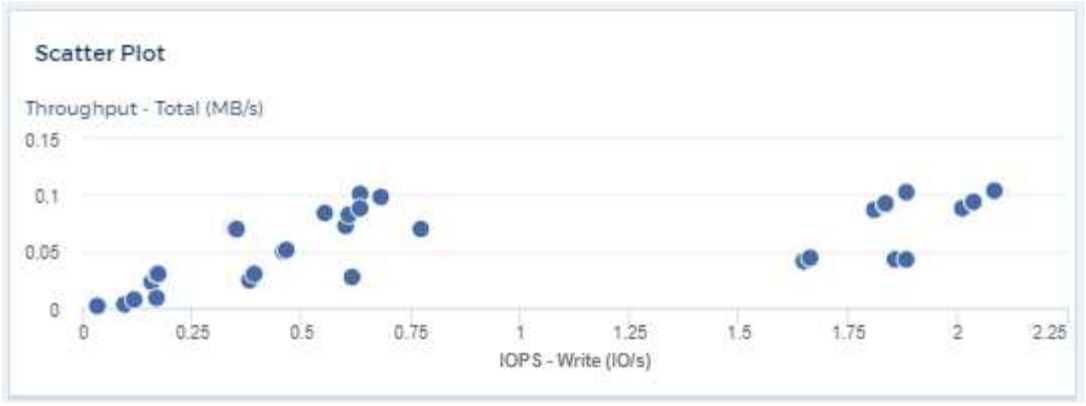
- 棒グラフ、縦棒グラフ: 容量による上位 10 件のストレージや IOPS による下位 5 件のボリュームなど、上位または下位 N 個の値を表示します。



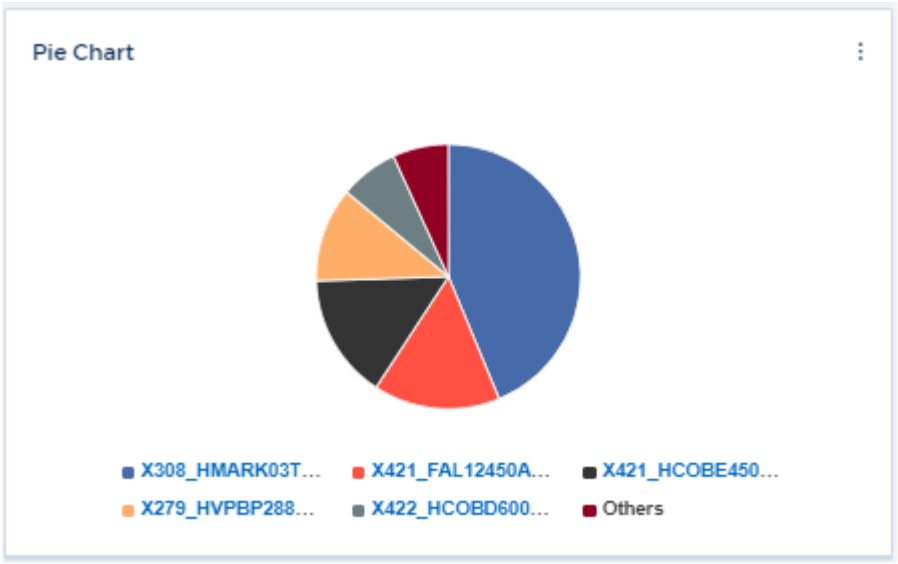
- ボックス プロット チャート: データの最小値、最大値、中央値、および下位四分位と上位四分位の範囲を 1 つのチャートにプロットします。



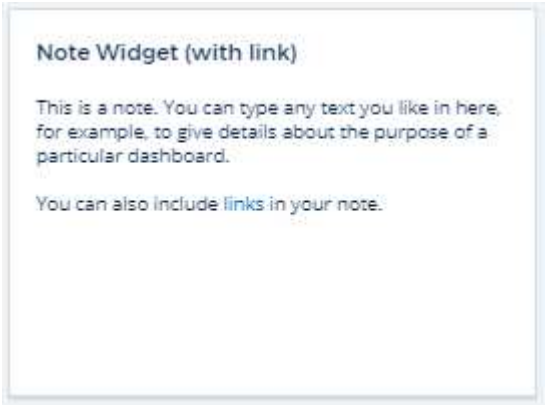
- 散布図チャート: IOPS やレイテンシなどの関連データをポイントとしてプロットします。この例では、スループットが高く IOPS が低い資産をすぐに見つけることができます。



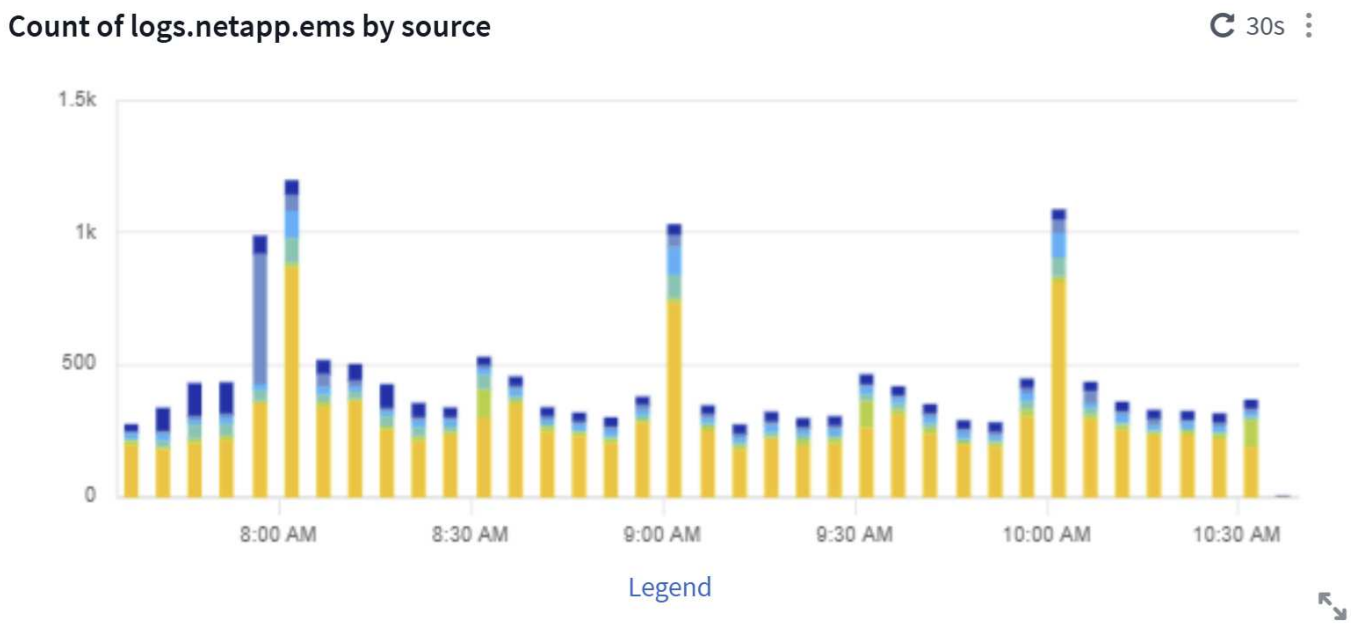
- 円グラフ: データを合計の一部として表示する従来の円グラフ。



- メモウィジェット: 最大 1000 文字の自由テキスト。



- 時間棒グラフ: 時間の経過に伴うログまたはメトリック データを表示します。



- アラート テーブル: 最新の 1,000 件までのアラートを表示します。

これらの機能やその他のダッシュボード機能の詳細な説明については、"ここをクリックしてくださいい" 。

ダッシュボードをホームページとして設定する

次のいずれかの方法を使用して、テナントの ホームページ として設定するダッシュボードを選択できます。

- ダッシュボード > すべてのダッシュボードを表示 に移動して、テナントのダッシュボードのリストを表示します。希望する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。上隅にあるドロップダウン 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。

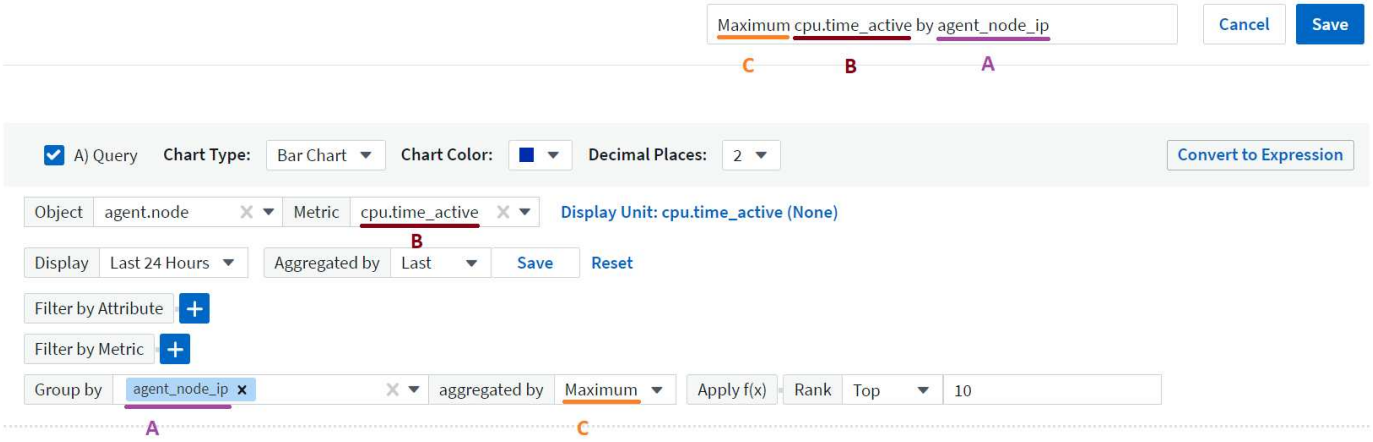
ダッシュボードの機能

ダッシュボードとウィジェットを使用すると、データの表示方法を柔軟に設定できます。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。

目次:[]

ウィジェットの命名

ウィジェットは、最初のウィジェット クエリで選択されたオブジェクト、メトリック、または属性に基づいて自動的に名前が付けられます。ウィジェットのグループ化も選択した場合、「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、自動名前が更新されます。

自動ウィジェット名を使用しない場合は、新しい名前を入力するだけです。

ウィジェットの配置とサイズ

すべてのダッシュボード ウィジェットは、特定のダッシュボードごとに、ニーズに応じて配置およびサイズを変更できます。

ウィジェットの複製

ダッシュボードの編集モードで、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 エディターが起動し、元のウィジェットの構成が事前に入力され、ウィジェット名に「コピー」サフィックスが付きます。必要な変更を簡単に行い、新しいウィジェットを保存できます。ウィジェットはダッシュボードの下部に配置され、必要に応じて配置できます。すべての変更が完了したら、ダッシュボードを必ず保存してください。

ウィジェットの凡例を表示する

ダッシュボード上のほとんどのウィジェットは、凡例の有無にかかわらず表示できます。ウィジェットの凡例は、次のいずれかの方法でダッシュボード上でオンまたはオフにすることができます。

- 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、メニューで 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更されると、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場合、凡例で示されるアセットのランディング ページに移動できる場合は、凡例はそのアセット 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、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。

指標の変革

Data Infrastructure Insights は、ウィジェット内の特定のメトリック (具体的には、Kubernetes、 ONTAP Advanced Data、Telegraf プラグインなどからの「カスタム」メトリックまたは統合メトリックと呼ばれるメトリック) に対してさまざまな 変換 オプションを提供し、さまざまな方法でデータを表示できるようにします。変換可能なメトリックをウィジェットに追加すると、次の変換の選択肢を示すドロップダウンが表示されます。

なし: データは操作されずにそのまま表示されます。

レート: 現在の値を前回の観測以降の時間範囲で割ったもの。

累積: 前の値の合計と現在の値の累積。

デルタ: 前回の観測値と現在の値の差。

デルタ レート: デルタ値を前回の観測以降の時間範囲で割った値。

累積率: 前回の観測以降の時間範囲で割った累積値。

メトリックを変換しても、基礎となるデータ自体は変更されず、データの表示方法のみが変更されることに注意してください。

ダッシュボードウィジェットのクエリとフィルター

クエリ

ダッシュボード ウィジェットのクエリは、データの表示を管理するための強力なツールです。ウィジェットクエリに関して注意すべき点がいくつかあります。

一部のウィジェットでは最大 5 つのクエリを持つことができます。各クエリはウィジェット内に独自の線またはグラフのセットをプロットします。 1 つのクエリでロールアップ、グループ化、上位/下位の結果などを設定しても、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、クエリを一時的に非表示にすることができます。クエリを非表示または表示すると、ウィジェットの表示が自動的に更新されます。これにより、ウィジェットを構築するときに、個々のクエリの表示データを確認できます。

次のウィジェット タイプでは複数のクエリを持つことができます。

- 面グラフ
- 積み上げ面グラフ
- 折れ線グラフ
- スプラインチャート
- 単一値ウィジェット

残りのウィジェット タイプには、単一のクエリのみを設定できます。

- テーブル
- 棒グラフ
- 箱ひげ図
- 散布図

ダッシュボードウィジェットクエリでのフィルタリング

フィルターを最大限に活用するために実行できることをいくつか紹介します。

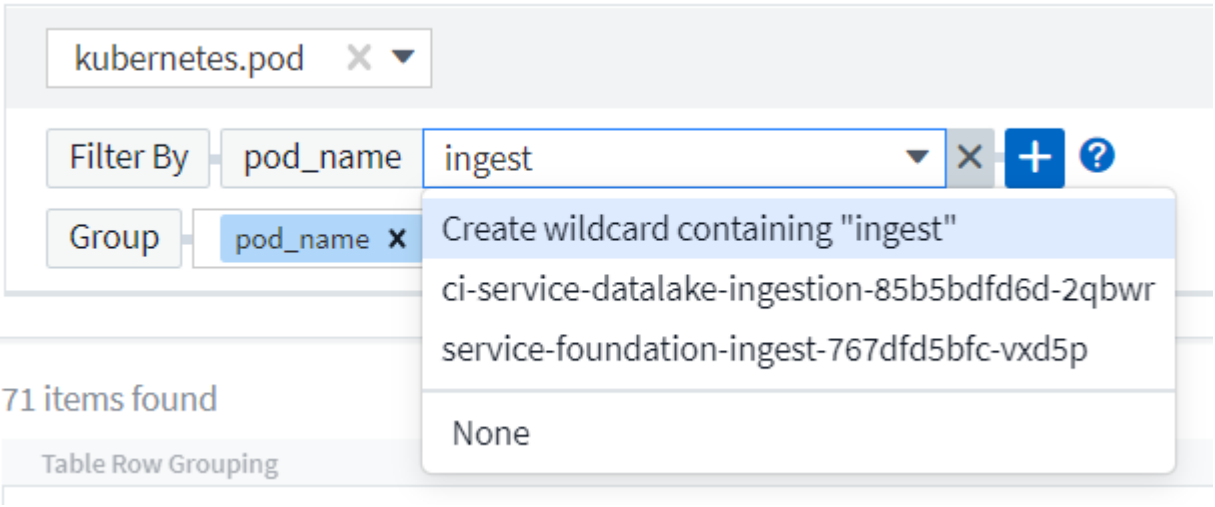
完全一致フィルタリング

フィルタ文字列を二重引用符で囲むと、Insight は最初の引用符と最後の引用符の間のすべてを完全一致として扱います。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、「*」でフィルタリングすると、文字通りのアスタリスクである結果が返されます。この場合、アスタリスクはワイルドカードとして扱われません。演算子 AND、OR、NOT も、二重引用符で囲むとリテラル文字列として扱われます。

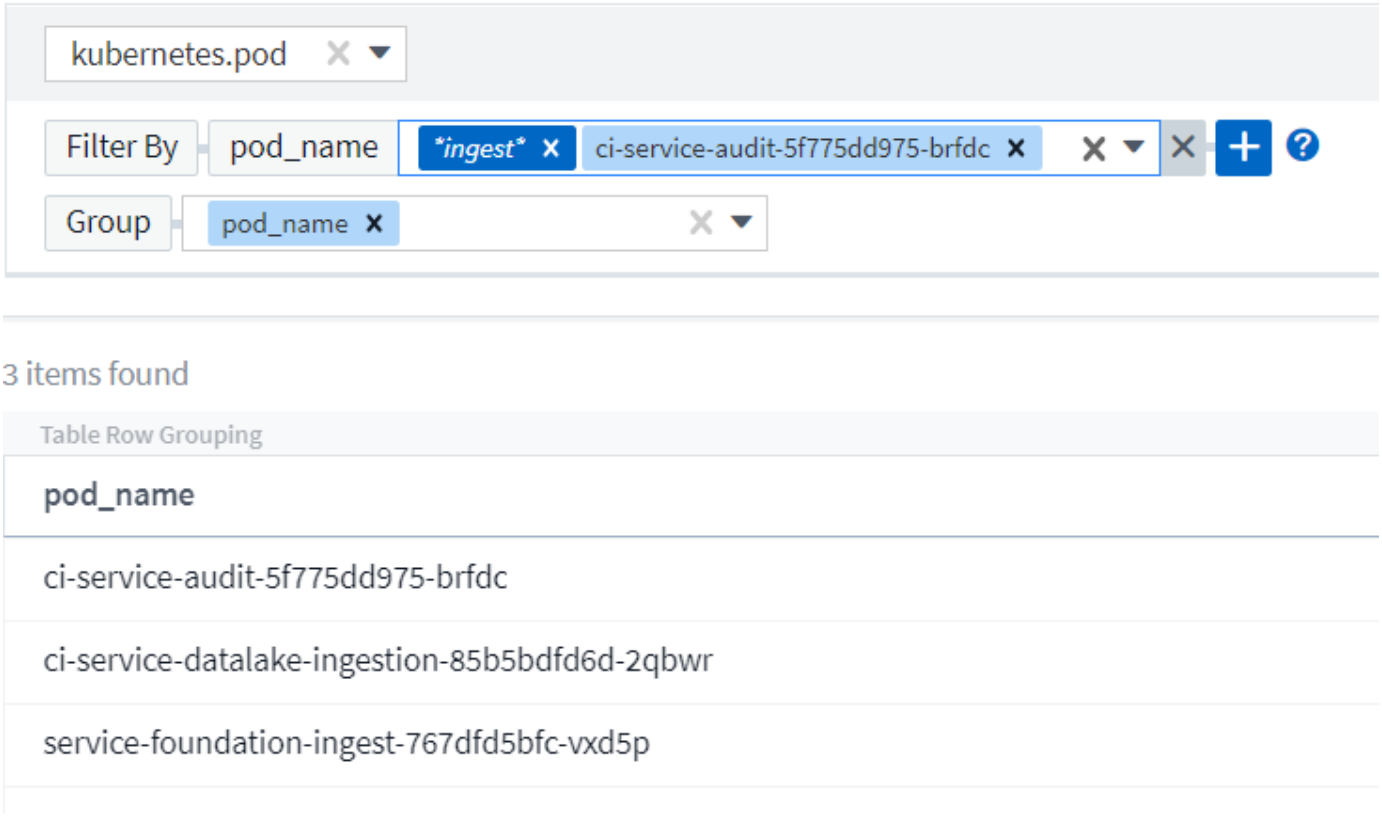
完全一致フィルターを使用して、ホスト名などの特定のリソースを見つけることができます。ホスト名「marketing」のみを検索し、「marketing01」、「marketing-boston」などを除外したい場合は、「marketing」という名前を二重引用符で囲むだけです。

ワイルドカードと式

クエリまたはダッシュボード ウィジェットでテキストまたはリストの値をフィルター処理する場合、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 フィルター 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 OR を使用して 式 を作成したり、「なし」オプションを選択してフィールド内の null 値をフィルター処理したりすることもできます。



ワイルドカードまたは式 (例: NOT、OR、「なし」など) に基づくフィルターは、フィルター フィールドに濃い青色で表示されます。リストから直接選択した項目は水色で表示されます。



ワイルドカードと式の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、ブール値では機能しないことに注意してください。

コンテキストに応じた入力候補による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リングはコンテキストに応じて行われます。つまり、フィールドのフィルタ値を選択すると、そのクエリの他のフィルタにそのフィルタに関連する値が表示されます。たとえば、特定のオブジェクト *Name* にフィルターを設定すると、*Model* をフィルター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。

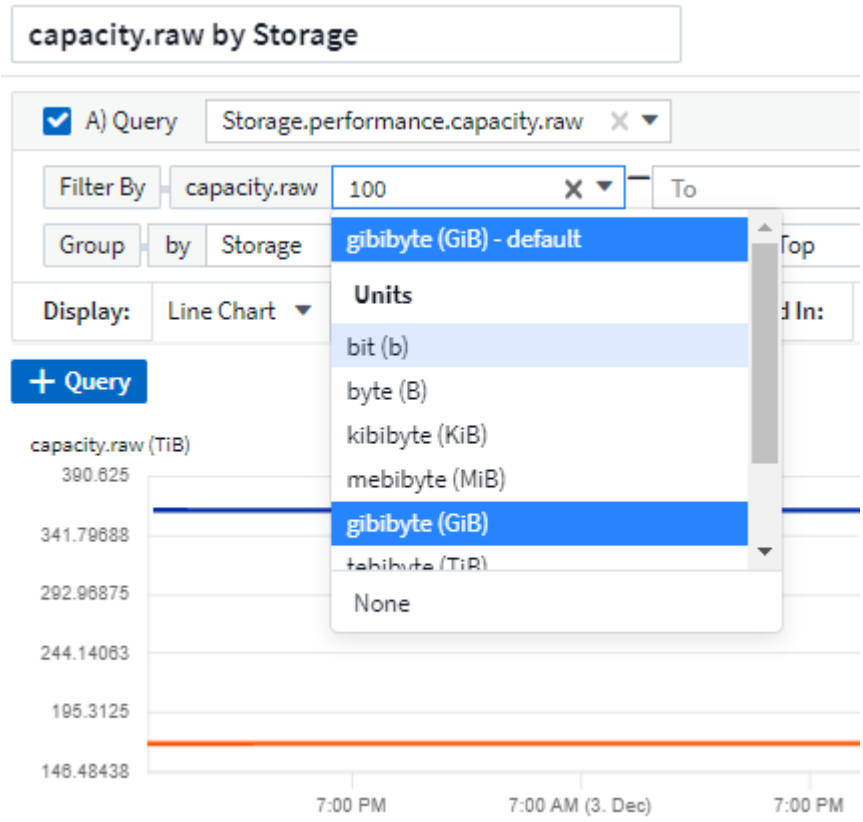
コンテキスト フィルタリングは、ダッシュボード ページ変数 (テキスト タイプの属性または注釈のみ) にも適用されます。 1 つの変数に対してフィルター値を選択すると、関連オブジェクトを使用する他の変数には、それらの関連変数のコンテキストに基づいて可能なフィルター値のみが表示されます。

テキスト フィルターのみがコンテキストに応じた先行入力候補を表示することに注意してください。日付、列挙型 (リスト) などでは、先行入力候補は表示されません。つまり、Enum (リスト) フィールドにフィルターを設定し、コンテキスト内で他のテキスト フィールドをフィルターすることは可能です。たとえば、データセンターなどの列挙フィールドの値を選択すると、他のフィルターにはそのデータ センター内のモデル/名前のみが表示されますが、その逆は当てはまりません。

選択した時間範囲は、フィルターに表示されるデータのコンテキストも提供します。

フィルターユニットの選択

フィルター 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、生の容量でフィルタリングして、デフォルトの GiB で表示するように選択したり、TiB などの別の形式を選択したりできます。これは、ダッシュボード上に TiB 単位の値を表示するグラフが多数あり、すべてのグラフで一貫した値を表示したい場合に便利です。



追加のフィルタリングの改良

以下を使用して、フィルターをさらに絞り込むことができます。

- アスタリスクを使用すると、すべてを検索できます。次に例を示します。

```
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、特定の文字数を検索できます。次に例を示します。

```
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。次に例を示します。

```
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。次に例を示します。

```
NOT EMC*
```

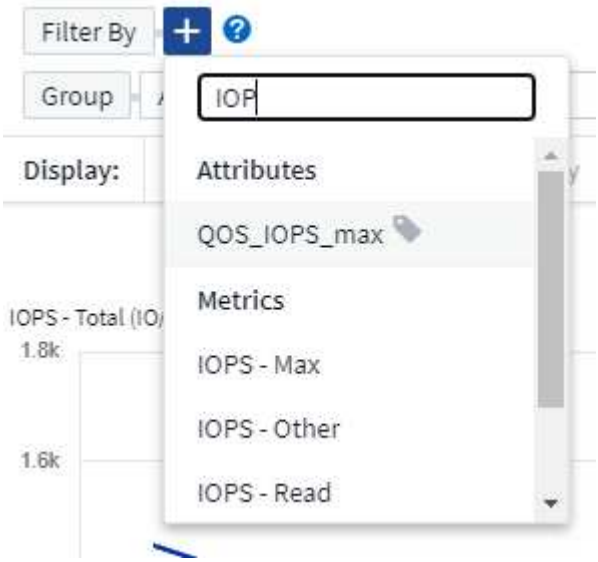
「EMC」で始まらないものをすべて検索します。使用できます

```
NOT *
```

値が含まれていないフィールドを表示します。

クエリとフィルターによって返されるオブジェクトの識別

クエリとフィルターによって返されるオブジェクトは、次の図に示すもののようになります。 「タグ」が割り当てられたオブジェクトは注釈であり、タグのないオブジェクトはパフォーマンス カウンターまたはオブジェクト属性です。



グループ化、識別、集約

グループ化（ロールアップ）

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基礎データ ポイントからグループ化されます (ロールアップと呼ばれることもあります)。たとえば、時間の経過に伴うストレージ IOPS を示す折れ線グラフ ウィジェットがある場合、簡単に比較できるように、データセンターごとに個別の線を表示したい場合があります。「グループ化」フィールドでオブジェクト タイプ自体を選択すると、ウィジェット タイプに応じて、各オブジェクトの個別の線、領域、棒、列などが表示されます。そのオブジェクトのリストで使用可能な任意の属性でグループ化することを選択できます。たとえば、内部ボリュームのデータを表示する場合、ストレージ名でデータをグループ化する必要がある場合があります。

統合されたデータを表示するには、グループ化属性をすべて削除します。これにより、デフォルトで「すべて」によるグループ化が設定されます。

このデータを集計するには、いくつかの方法があります。

- 平均: 各行を基礎データの 平均 として表示します。
- 最大値: 各行を基礎データの最大値として表示します。
- 最小値: 各行を基礎データの 最小値 として表示します。
- 合計: 各行を基礎データの 合計 として表示します。

ダッシュボードを表示するときに、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選択すると、ウィジェットで使用された最初のクエリの結果を示すクエリ ページが開きます。

クエリにフィルターを設定している場合は、フィルターされたデータに基づいてデータがグループ化されます。

カスタムデータの識別

独自のカスタム データに基づいて構築されたウィジェットを作成または変更する場合、識別属性がないとウィジェット内でデータが適切に表現されないことがあります。 DII がウィジェットに選択したオブジェクトを識別できない場合は、「グループ化」領域に [詳細構成] リンクが表示されます。これを展開して、データを識別する属性を選択します。



データの集約

データ ポイントを分、時間、または日のバケットに集計してから、そのデータを属性別にロールアップすることで (選択した場合)、チャートをさらに調整できます。データ ポイントを、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を選択できます。

短い間隔と長い時間範囲を組み合わせると、「集計間隔でデータ ポイントが多すぎます」という警告が表示される場合があります。間隔が短く、ダッシュボードの時間枠を 7 日間に増やすと、このメッセージが表示されることがあります。この場合、Insight は、より短い時間枠を選択するまで、集計間隔を一時的に増加します。

ほとんどの資産カウンターは、デフォルトで 平均 に集計されます。一部のカウンターは、デフォルトで *Max*、Min_、または *Sum* に集計されます。たとえば、ポート エラーはデフォルトで *Sum* に集計され、ストレージ IOPS は *Average* に集計されます。

上位/下位の結果を表示

チャート ウィジェットでは、ロールアップされたデータの 上位 または 下位 の結果を表示し、表示される結果の数をドロップダウン リストから選択できます。テーブル ウィジェットでは、任意の列で並べ替えることができます。

チャートウィジェット上部/下部

チャート ウィジェットでは、特定の属性でデータをロールアップすることを選択した場合、上位 N または下位 N の結果を表示するオプションがあります。 _すべての_属性によるロールアップを選択した場合は、上位または下位の結果を選択できないことに注意してください。

クエリの 表示 フィールドで 上位 または 下位 のいずれかを選択し、表示されるリストから値を選択することで、表示する結果を選択できます。

テーブルウィジェットにエントリを表示

テーブル ウィジェットでは、テーブル結果に表示される結果の数を選択できます。テーブルでは、必要に応じて任意の列で昇順または降順で並べ替えることができるため、上位または下位の結果を選択するオプションはありません。

クエリの「エントリを表示」フィールドから値を選択することで、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。

テーブルウィジェットのグループ化

テーブル ウィジェット内のデータは、利用可能な属性ごとにグループ化できるため、データの概要を表示したり、詳細をドリルダウンしたりできます。表内のメトリックは、折りたたまれた各行で簡単に確認できるようにまとめられています。

テーブル ウィジェットを使用すると、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、ストレージが存在するデータセンターごとにグループ化されたストレージ IOPS の合計をテーブルに表示したい場合があります。または、仮想マシンをホストするハイパーバイザーごとにグループ化された仮想マシンのテーブルを表示することもできます。リストから各グループを展開して、そのグループ内の資産を表示できます。

グループ化はテーブル 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（ロールアップの説明付き）

テーブル ウィジェットを使用すると、データをグループ化して表示しやすくなります。

この例では、データセンターごとにグループ化されたすべての VM を表示するテーブル ウィジェットを作成します。

手順

1. ダッシュボードを作成するか開き、*テーブル*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 [仮想マシン] を選択します。
3. 列セレクターをクリックし、_ハイパーバイザー名_と_IOPS - 合計_を選択します。

   これらの列がテーブルに表示されるようになりました。

4. IOPS のない VM は無視し、合計 IOPS が 1 を超える VM のみを含めます。 フィルター **[+]** ボタンをクリックし、*IOPS* - 合計 を選択します。 「*Any*」をクリックし、「**from**」フィールドに「**1**」と入力します。 *宛先*フィールドは空のままにしておきます。フィルターを適用するには、Enter キーを押すか、フィルター フィールドをクリックします。

   テーブルには、合計 IOPS が 1 以上のすべての VM が表示されます。表にはグループ化されていないこと

に注意してください。すべての VM が表示されます。

5. *グループ化[+]*ボタンをクリックします。

   表示されている属性または注釈ごとにグループ化できます。 すべて を選択すると、1 つのグループ内のすべての VM が表示されます。

   パフォーマンス メトリックの列ヘッダーには、「ロールアップ」オプションを含む「3 つのドット」メニューが表示されます。デフォルトのロールアップ方法は 平均 です。つまり、グループに表示される数値は、グループ内の各 VM について報告されたすべての合計 IOPS の平均です。この列を 平均、合計_、最小_、または 最大 でロールアップすることを選択できます。表示するパフォーマンス メトリックを含む列は、個別にロールアップできます。



6. [すべて] をクリックし、[ハイパーバイザー名] を選択します。

   VM リストがハイパーバイザーごとにグループ化されるようになりました。各ハイパーバイザーを展開して、そのハイパーバイザーでホストされている VM を表示できます。

7. 保存 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。必要に応じてウィジェットのサイズを変更したり移動したりできます。
8. ダッシュボードを保存するには、[保存] をクリックします。

パフォーマンスデータのロールアップ

テーブル ウィジェットにパフォーマンス データの列 (たとえば、*IOPS* - 合計) を含める場合、データをグループ化することを選択すると、その列のロールアップ方法を選択できます。デフォルトのロールアップ方法では、基になるデータの平均 (*avg*) がグループ行に表示されます。データの合計、最小値、最大値を表示するように選択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ー

ダッシュボード データの時間範囲を選択できます。選択した時間範囲に関連するデータのみがダッシュボードのウィジェットに表示されます。次の時間範囲から選択できます。

- 最後の15分
- 最後の30分
- 最後の60分
- 過去 2 時間
- 過去3時間（これがデフォルトです）
- 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
- カスタム時間範囲

  カスタム時間範囲では、最大 31 日間連続して選択できます。この範囲の開始時刻と終了時刻を設定することもできます。デフォルトの開始時刻は、選択した最初の日の午前 12:00 で、デフォルトの終了時刻は、選択した最後の日の午後 11:59 です。 *適用*をクリックすると、カスタム時間範囲がダッシュボードに適用されます。

時間範囲を拡大する

時系列ウィジェット (折れ線グラフ、スプライン グラフ、面グラフ、積み上げ面グラフ)、またはランディング ページのグラフを表示しているときに、グラフ上でマウスをドラッグして拡大することができます。その後、画面の右上でその時間範囲をロックして、他のページのグラフにロックした時間範囲のデータが反映されるようにすることができます。ロックを解除するには、リストから別の時間範囲を選択してください。

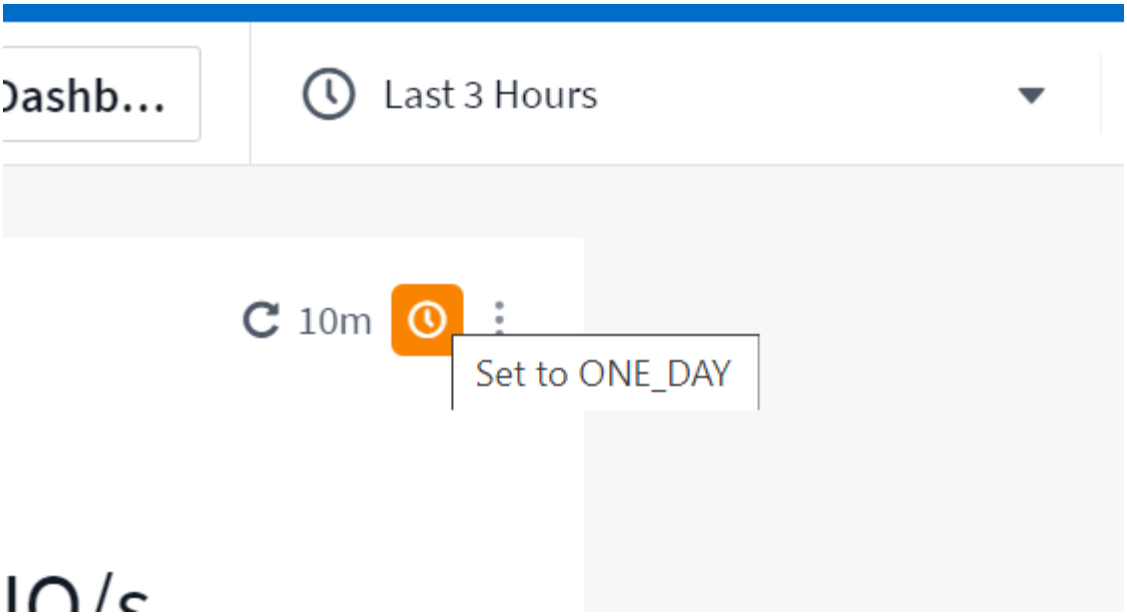
個々のウィジェットでダッシュボードの時間を上書きする

個々のウィジェットでメインダッシュボードの時間範囲設定を上書きできます。これらのウィジェットは、ダッシュボードの時間枠ではなく、設定された時間枠に基づいてデータを表示します。

ダッシュボードの時間を上書きし、ウィジェットが独自の時間枠を使用するように強制するには、ウィジェットの編集モードで希望の時間範囲を選択し、ウィジェットをダッシュボードに保存します。

ウィジェットは、ダッシュボード自体で選択した時間枠に関係なく、設定された時間枠に従ってデータを表示します。

1 つのウィジェットに設定した時間枠は、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。



主軸と副軸

メトリックごとに、グラフで報告するデータの測定単位が異なります。たとえば、IOPS の場合、測定単位は 1 秒あたりの I/O 操作数 (IO/s) ですが、レイテンシは純粋に時間の測定値 (ミリ秒、マイクロ秒、秒など) です。 Y 軸に単一の値セットを使用して両方のメトリックを 1 つの折れ線グラフにグラフ化すると、レイテンシの数値 (通常は数ミリ秒) が IOPS (通常は数千の数値) と同じスケールでグラフ化され、そのスケールではレイテンシの線が失われます。

ただし、1 つの測定単位を主 (左側) Y 軸に設定し、もう 1 つの測定単位を副 (右側) Y 軸に設定することで、両方のデータ セットを 1 つの意味のあるグラフにグラフ化することができます。各メトリックは独自のスケールでグラフ化されます。

手順

この例では、チャート ウィジェットのプライマリ軸とセカンダリ軸の概念を示します。

1. ダッシュボードを作成または開きます。ダッシュボードに折れ線グラフ、スプライン グラフ、面グラフ、または積み上げ面グラフ ウィジェットを追加します。
2. 資産タイプ (たとえば、ストレージ) を選択し、最初のメトリックとして [IOPS - 合計_] を選択します。好きなフィルターを設定し、必要に応じてロールアップ方法を選択します。

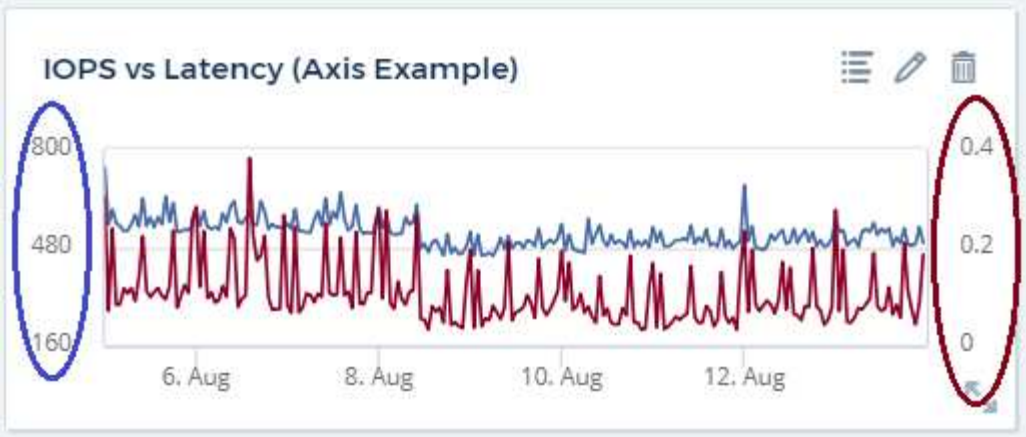
   IOPS ラインがグラフに表示され、そのスケールが左側に表示されます。

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、メトリックとして「*Latency - Total*」を選択します。

   グラフの下部に線が平らに表示されていることに注意してください。これは、IOPS ラインと同じスケールで描画されているためです。

4. レイテンシ クエリで、**Y 軸:** セカンダリ を選択します。

   レイテンシ ラインが独自のスケールで描画され、グラフの右側に表示されるようになりました。



ウィジェット内の式

ダッシュボードでは、任意の時系列ウィジェット（折れ線グラフ、スプライングラフ、面グラフ、積み上げ面グラフ）、棒グラフ、縦棒グラフ、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（またはテーブルウィジェット）。次の例では、式を使用して特定の問題を解決します。最初の例では、テナント上のすべてのストレージ資産の合計 IOPS に対する読み取り IOPS のパーセンテージを表示します。 2 番目の例では、テナント上で発生する「システム」または「オーバーヘッド」IOPS (データの読み取りや書き込みから直接発生するものではない IOPS) を可視化します。

式では変数を使用できます（例：*$Var1 * 100*）

式の例: 読み取り**IOPS**のパーセンテージ

この例では、読み取り IOPS を合計 IOPS のパーセンテージとして表示します。これは次の式として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、次の手順に従います。

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。 *面グラフ*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、*Storage* 資産の *IOPS - Total* を示すクエリが表示されます。必要に応じて、別の資産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。

   現在のクエリは式モードに変換されます。式モードではアセット タイプを変更できないことに注意してください。式モードの間は、リンクは「クエリに戻る」に変わります。いつでもクエリ モードに戻りたい場合は、これをクリックします。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ことに注意してください。

   今のところは、Expression モードのままにしておきます。

4. **IOPS -** 合計 メトリックは、アルファベット変数フィールド **"a"** に表示されます。 「**b**」変数フィールド

で、「選択」をクリックし、「**IOPS -** 読み取り」を選択します。

変数フィールドの後の + ボタンをクリックすると、式に最大 5 つのアルファベット変数を追加できます。読み取りパーセンテージの例では、合計 IOPS (「**a**」) と読み取り IOPS (「**b**」) のみが必要です。

5. 式 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。読み取りパーセンテージ = (読み取り IOPS / 合計 IOPS) x 100 であることがわかっているので、この式は次のように記述します。

```
 (b / a) * 100
```

. *ラベル*
フィールドは式を識別します。ラベルを「読み取り率」など、自分にとって意味のある名前に変更します。
. *単位*フィールドを「%」または「パーセント」に変更します。

グラフには、選択したストレージ デバイスの IOPS 読み取りパーセンテージが時間経過とともに表示されます。必要に応じて、フィルターを設定したり、別のロールアップ方法を選択したりできます。ロールアップ方法として合計を選択した場合は、すべてのパーセンテージ値が合計され、100% を超える可能性があることに注意してください。

6. 保存 をクリックして、チャートをダッシュボードに保存します。

式の例:「システム」**I/O**

例 2: データ ソースから収集されるメトリックには、読み取り、書き込み、合計 IOPS などがあります。ただし、データ ソースによって報告される IOPS の合計数には、データの読み取りや書き込みに直接関係のない IO 操作である「システム」IOPS が含まれることがあります。このシステム I/O は、適切なシステム操作に必要ですが、データ操作とは直接関係のない「オーバーヘッド」 I/O と考えることもできます。

これらのシステム I/O を表示するには、取得から報告された合計 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の折れ線グラフで表示できます。これを行うには、次の手順に従います。

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。 *折れ線グラフ*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、*Storage* 資産の *IOPS - Total* を示すクエリが表示されます。必要に応じて、別の資産タイプを選択します。

3. *ロールアップ*フィールドで、_すべて_による_合計_を選択します。

   チャートには、合計 IOPS の合計を示す線が表示されます。

4. クエリのコピーを作成するには、[このクエリを複製] アイコンをクリックします。

   クエリの複製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。

   現在のクエリは式モードに変換されます。いつでもクエリ モードに戻りたい場合は、[クエリに戻す] 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ことに注意してください。

   今のところは、Expression モードのままにしておきます。

6. *IOPS - Total* メトリックは、アルファベット変数フィールド「**a**」に表示されます。 「*IOPS - Total*」をクリックし、「*IOPS - Read*」に変更します。
7. 「**b**」変数フィールドで、「選択」をクリックし、「*IOPS* - 書き込み」を選択します。
8. 式 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。この式は単純に次のように記述します。

   ```
   a + b
   ```

   表示セクションで、この式に 面グラフ を選択します。

9. ラベル フィールドは式を識別します。ラベルを「System IOPS」または同様に意味のある名前に変更します。

   グラフには合計 IOPS が折れ線グラフで表示され、その下に読み取り IOPS と書き込み IOPS の組み合わせを示す面グラフが表示されます。 2 つの間のギャップは、データの読み取りまたは書き込み操作に直接関係しない IOPS を示しています。これらは「システム」IOPS です。

10. 保存 をクリックして、チャートをダッシュボードに保存します。

式で変数を使用するには、変数名を入力するだけです (例: *$var1 * 100*)。式では数値変数のみ使用できます。

テーブルウィジェット内の式

テーブル ウィジェットでは式の処理方法が少し異なります。 1 つのテーブル ウィジェットには最大 5 つの式を含めることができ、各式は新しい列としてテーブルに追加されます。各式には、計算を実行するための値を最大 5 つ含めることができます。列に意味のある名前を付けるのは簡単です。



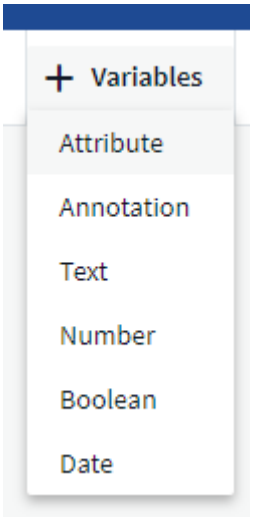
変数

変数を使用すると、ダッシュボード上の一部またはすべてのウィジェットに表示されるデータを一度に変更できます。 1 つ以上のウィジェットで共通変数を使用するように設定すると、1 か所で変更を加えると、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。

変数の型

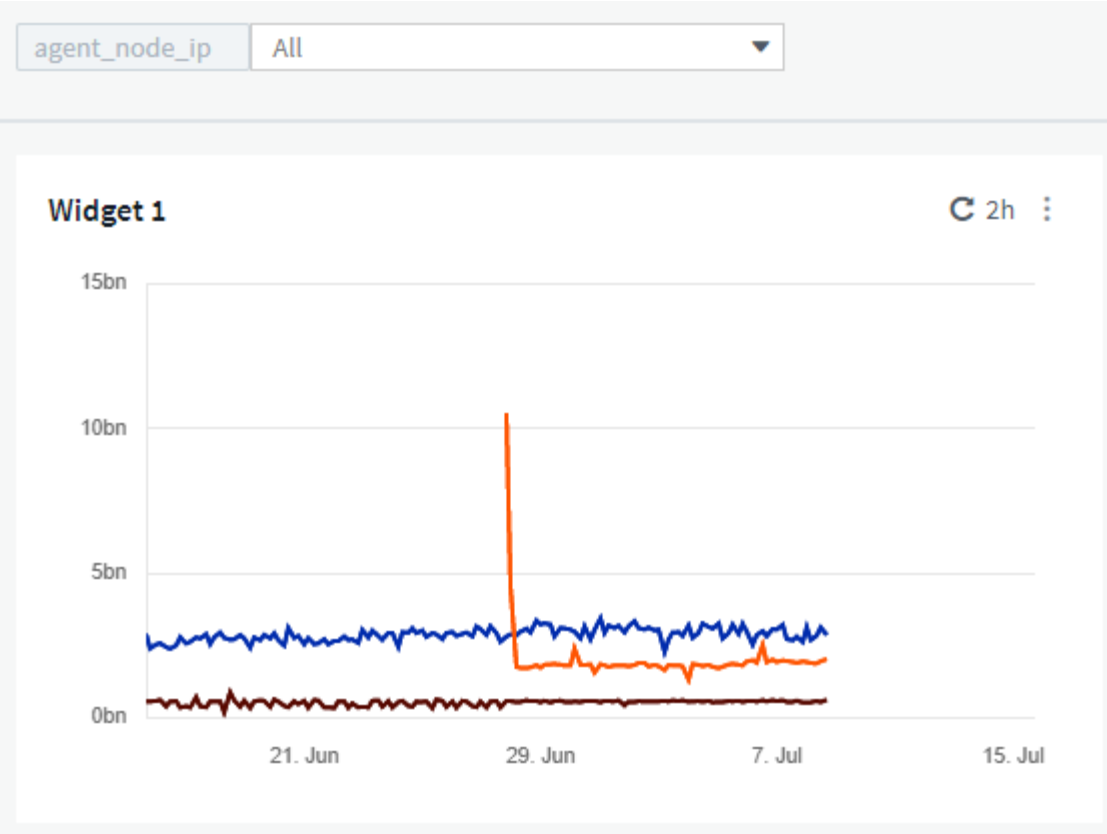
変数は次のいずれかの型になります。

- 属性: オブジェクトの属性または指標を使用してフィルタリングします
- 注釈: 定義済みの"注釈"ウィジェットデータをフィルタリングします。
- テキスト: 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、単独で使用するか、「開始」または「終了」の値として使用します。
- ブール値: 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: 日付の値。ウィジェットの設定に応じて、「開始」または「終了」の値として使用します。

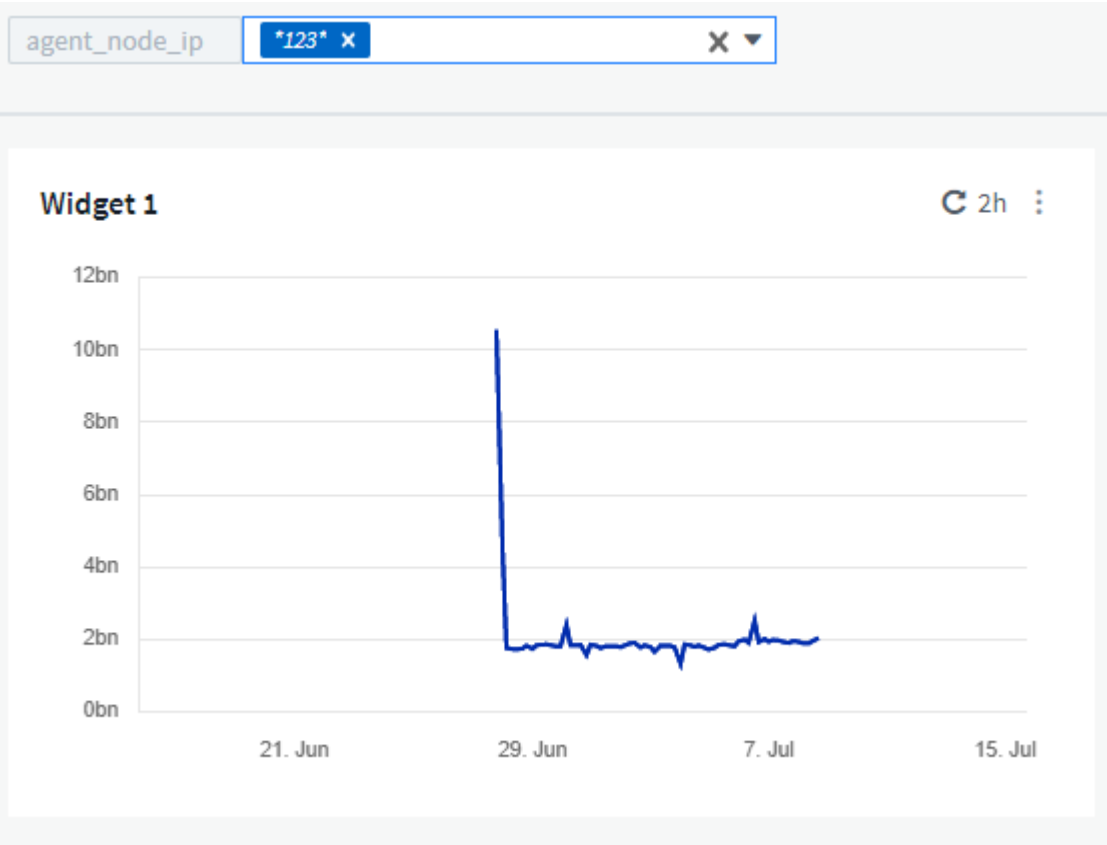


属性変数

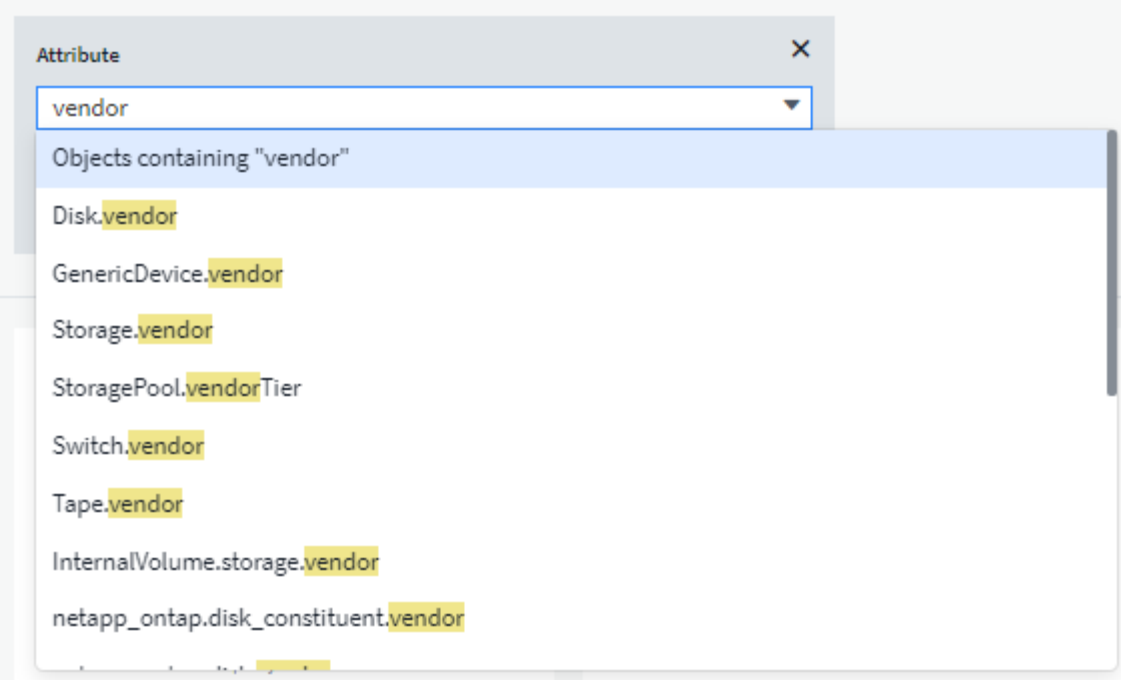
属性タイプの変数を選択すると、指定した属性値を含むウィジェット データをフィルターできます。以下の例は、エージェント ノードの空きメモリの傾向を表示する線ウィジェットを示しています。エージェント ノード IP の変数を作成しました。現在はすべての IP を表示するように設定されています。



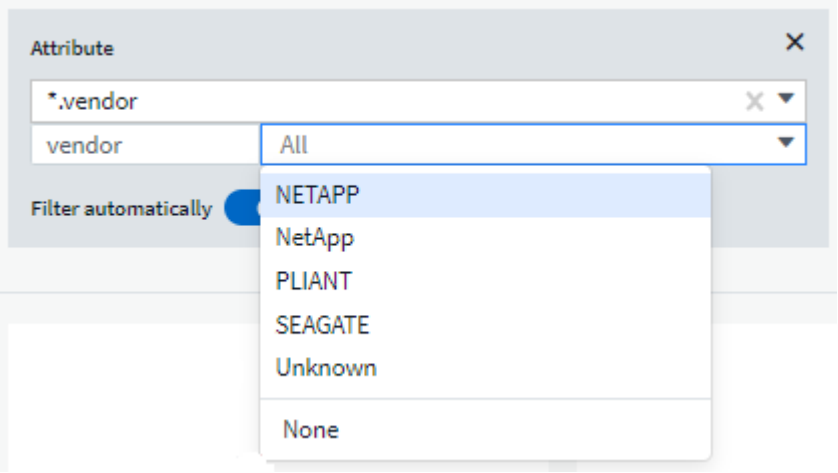
ただし、テナント上の個々のサブネット上のノードのみを一時的に表示したい場合は、変数を特定のエージェント ノード IP に設定または変更できます。ここでは、「123」サブネット上のノードのみを表示しています。



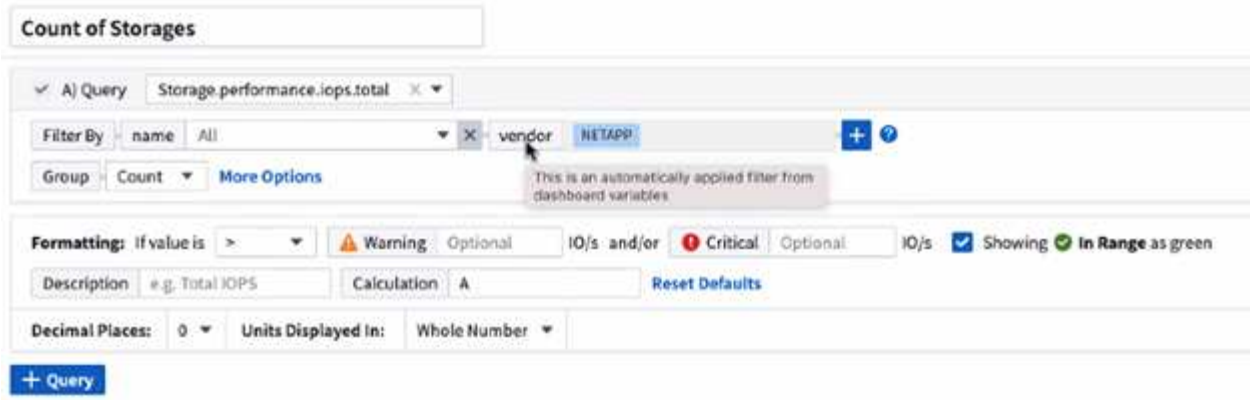
また、変数フィールドに *.vendor を指定して、オブジェクトの種類に関係なく、特定の属性を持つすべてのオブジェクト (たとえば、「ベンダー」属性を持つオブジェクト) をフィルターするように変数を設定することもできます。 「*.」を入力する必要はありません。ワイルドカード オプションを選択した場合、 Data Infrastructure Insightsによってこれが自動的に提供されます。



変数値の選択肢のリストをドロップダウンすると、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利用可能なベンダーのみが表示されます。



属性フィルターが関連するダッシュボード上のウィジェットを編集する場合 (つまり、ウィジェットのオブジェクトに *.vendor 属性 が含まれている場合)、属性フィルターが自動的に適用されていることが示されます。

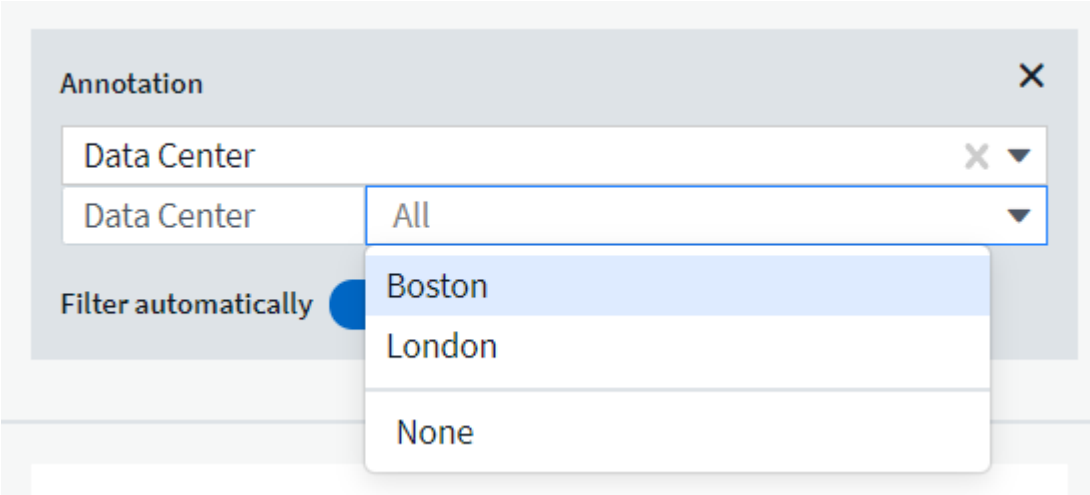


14

変数の適用は、選択した属性データを変更するのと同じくらい簡単です。

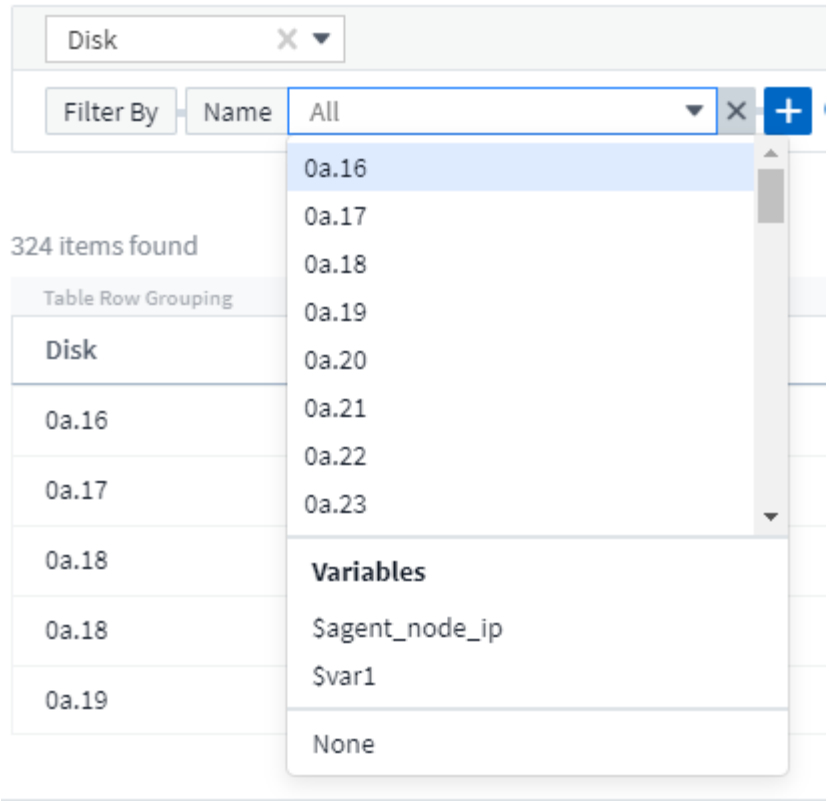
注釈変数

アノテーション変数を選択すると、同じデータ センターに属するオブジェクトなど、そのアノテーションに関連付けられたオブジェクトをフィルターできます。



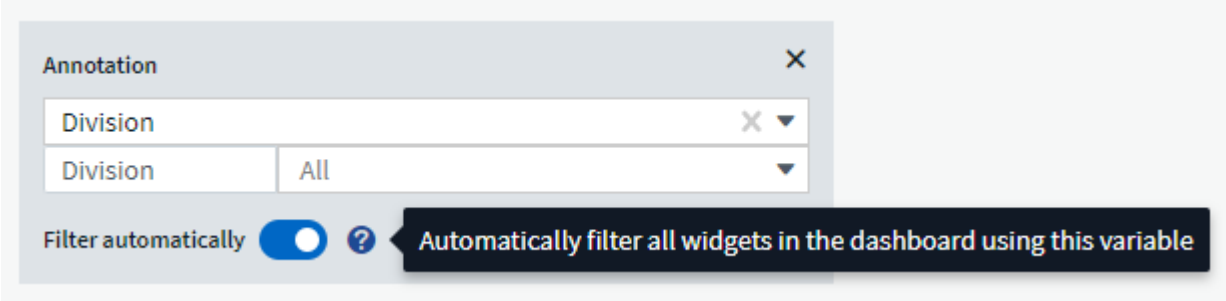
テキスト、数値、日付、またはブール変数

変数タイプとして「*Text*」、「*Number*」、「*Boolean*」、または「*Date*」を選択すると、特定の属性に関連付けられていない汎用変数を作成できます。変数が作成されると、ウィジェット フィルター フィールドで選択できるようになります。ウィジェットでフィルターを設定すると、フィルター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変数がリストに表示されます。これらの変数はドロップダウンの「変数」セクションにグループ化されており、名前は「$」で始まります。このフィルターで変数を選択すると、ダッシュボード自体の変数フィールドに入力した値を検索できるようになります。フィルター内でその変数を使用するウィジェットは動的に更新されます。



変数フィルターのスコープ

ダッシュボードに注釈または属性変数を追加すると、その変数はダッシュボード上のすべてのウィジェットに適用され、ダッシュボード上のすべてのウィジェットに、変数に設定した値に従ってフィルタリング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リングできるのは、属性変数と注釈変数のみであることに注意してください。非アノテーション変数または非属性変数は自動的にフィルタリングできません。個々のウィジェットはそれぞれ、これらのタイプの変数を使用するように構成する必要があります。

自動フィルタリングを無効にして、変数が明示的に設定したウィジェットにのみ適用されるようにするには、「自動的にフィルタリング」スライダー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、[フィルター条件] フィールドで特定の注釈または属性を選択します。注釈変数を使用すると、1 つ以上の特定の値を選択したり、変数名 (先頭の「$」で示される) を選択してダッシュボード レベルで変数を入力できるようにすることができます。属性変数にも同じことが当てはまります。変数を設定したウィジェットにのみ、フィルタリングされた結果が表示されます。

変数でのフィルタリングはコンテキストに依存します。変数のフィルタ値を選択すると、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、変数フィルターを特定のストレージ *Model* に設定すると、ストレージ *Name* のフィルター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するだけです (例: *$var1 * 100*)。式では数値変数のみ使用できます。式では数値の注釈変数または属性変数は使用できません。

変数でのフィルタリングはコンテキストに依存します。変数のフィルタ値を選択すると、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、変数フィルターを特定のストレージ *Model* に設定すると、ストレージ *Name* のフィルター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。

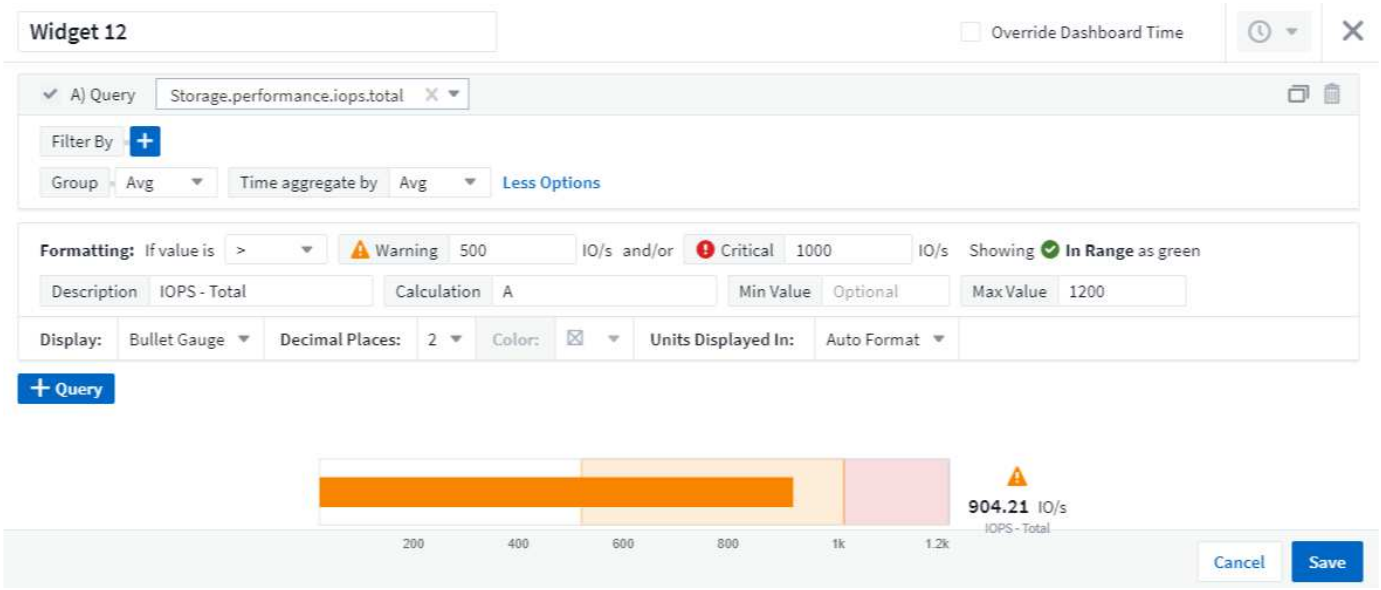
変数の命名

変数名:

- 使用できるのは、文字 a ～ z、数字 0 ～ 9、ピリオド (.)、アンダースコア (_)、スペース ( ) のみです。
- 20 文字を超えることはできません。
- 大文字と小文字が区別されます: $CityName と $cityname は異なる変数です。
- 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

ソリッド ゲージ ウィジェットとブレット ゲージ ウィジェットを使用すると、警告 レベルや クリティカル レベルのしきい値を設定して、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の書式を設定するには、次の手順に従います。

1. しきい値より大きい値 (>) を強調表示するか、しきい値より小さい値 (<) 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。ウィジェットがこのレベルより大きい値を表示する場合、ゲージはオレンジ色で表示されます。
3. 「重大」しきい値の値を選択します。このレベルを超える値の場合、ゲージは赤色で表示されます。

オプションで、ゲージの最小値と最大値を選択できます。最小値を下回る値の場合、ゲージは表示されません。最大値を超える値の場合は、ゲージがいっぱいに表示されます。最小値または最大値を選択しない場合、ウィジェットはウィジェットの値に基づいて最適な最小値と最大値を選択します。



単一値ウィジェットの書式設定

単一値ウィジェットでは、警告 (オレンジ) と重大 (赤) のしきい値を設定することに加えて、「範囲内」の値 (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。

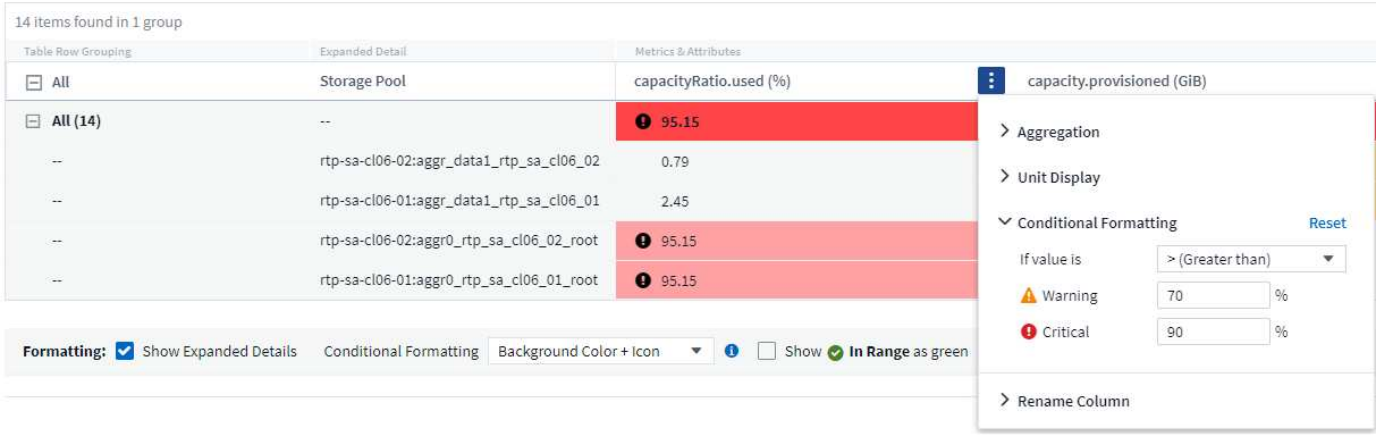


単一値ウィジェットまたはゲージ ウィジェット内のリンクをクリックすると、ウィジェットの最初のクエリに対応するクエリ ページが表示されます。

表ウィジェットの書式設定

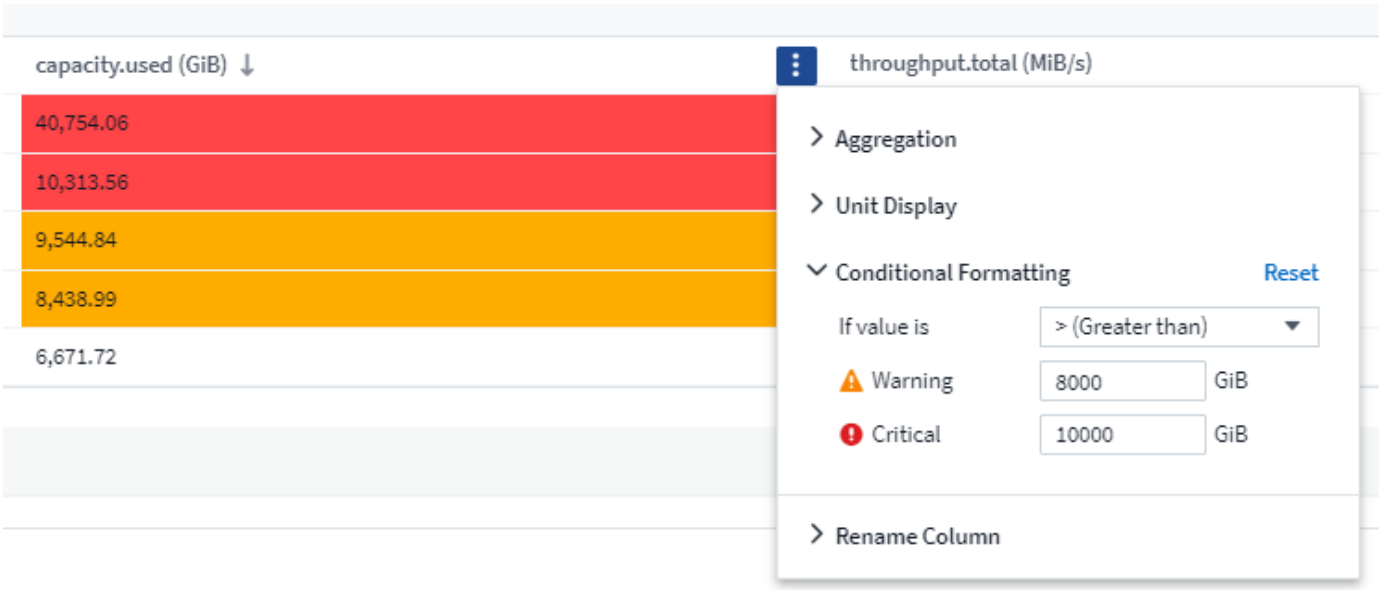
単一値ウィジェットやゲージ ウィジェットと同様に、テーブル ウィジェットでも条件付き書式を設定できるため、色や特殊なアイコンを使用してデータを強調表示できます。

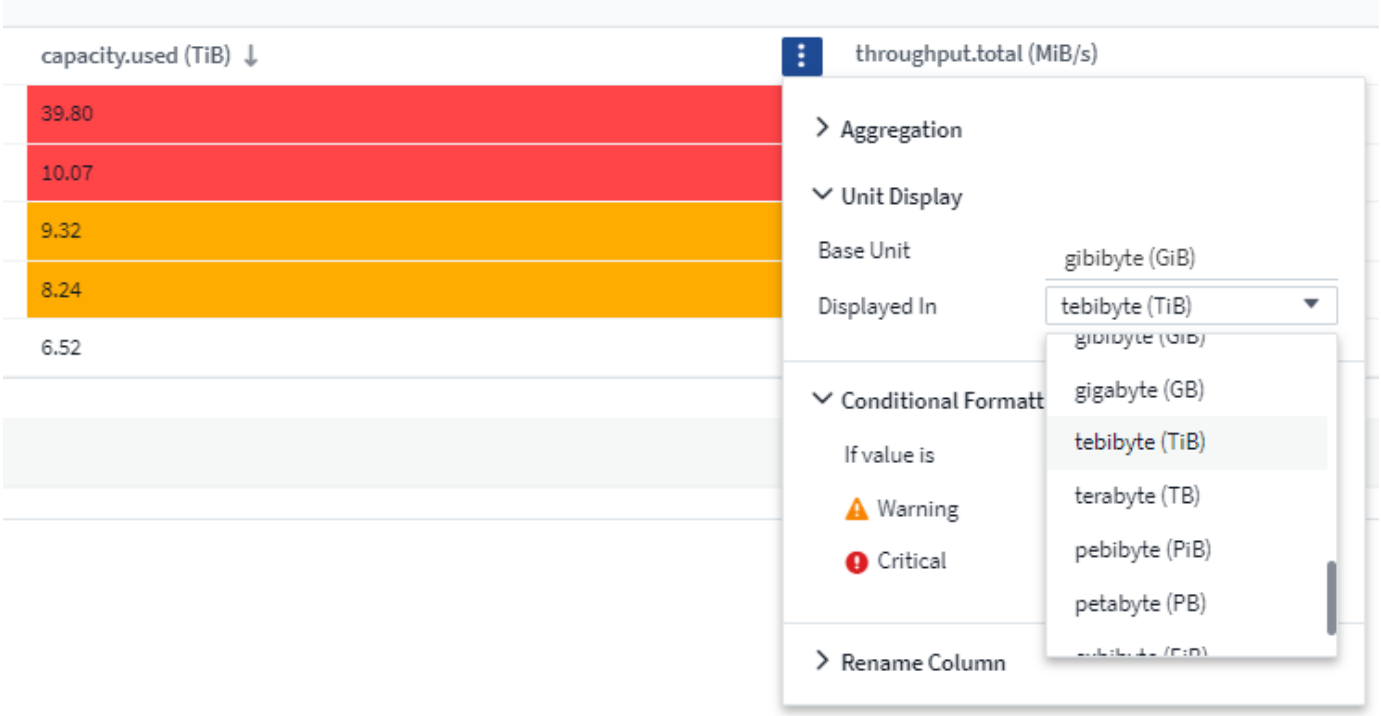
条件付き書式を使用すると、テーブル ウィジェットで警告レベルと重大レベルのしきい値を設定して強調表示できるため、外れ値や例外的なデータ ポイントを即座に表示できます。



条件付き書式は、テーブル内の各列ごとに個別に設定します。たとえば、容量列に 1 セットのしきい値を選択し、スループット列に別のセットのしきい値を選択できます。

列の単位表示を変更した場合、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、表示単位が異なっていても、同じ条件付き書式を示しています。



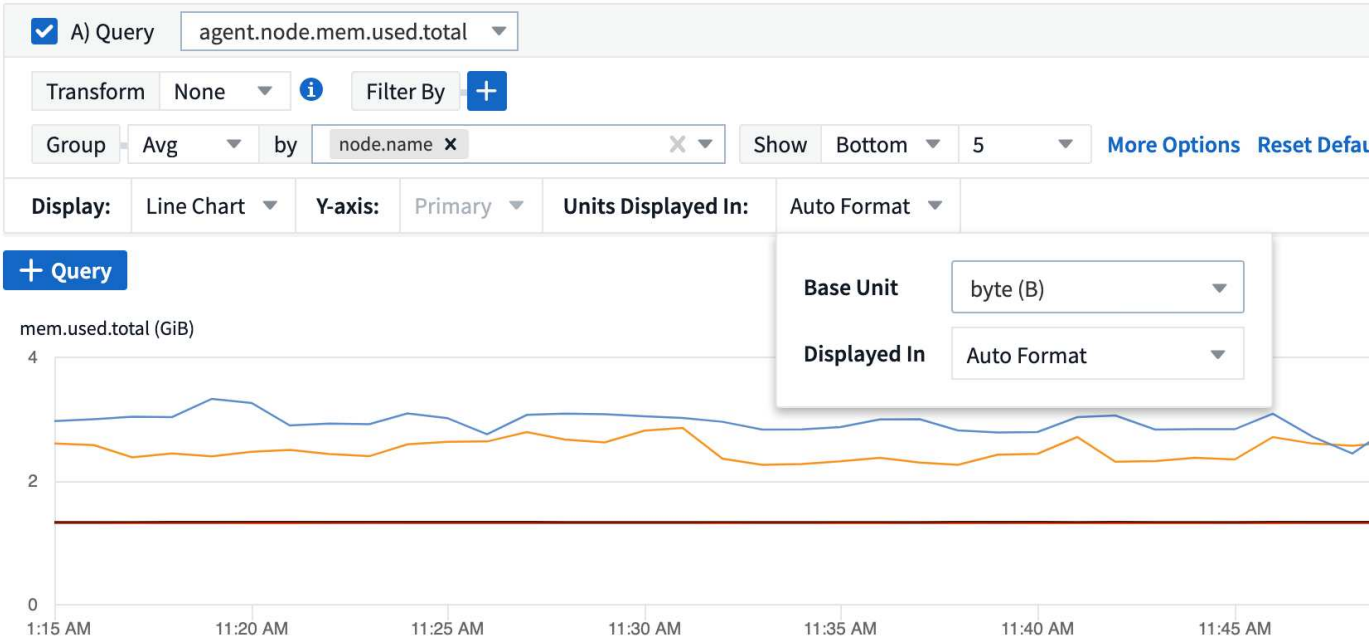


条件の書式設定を色、アイコン、またはその両方で表示するかを選択できます。

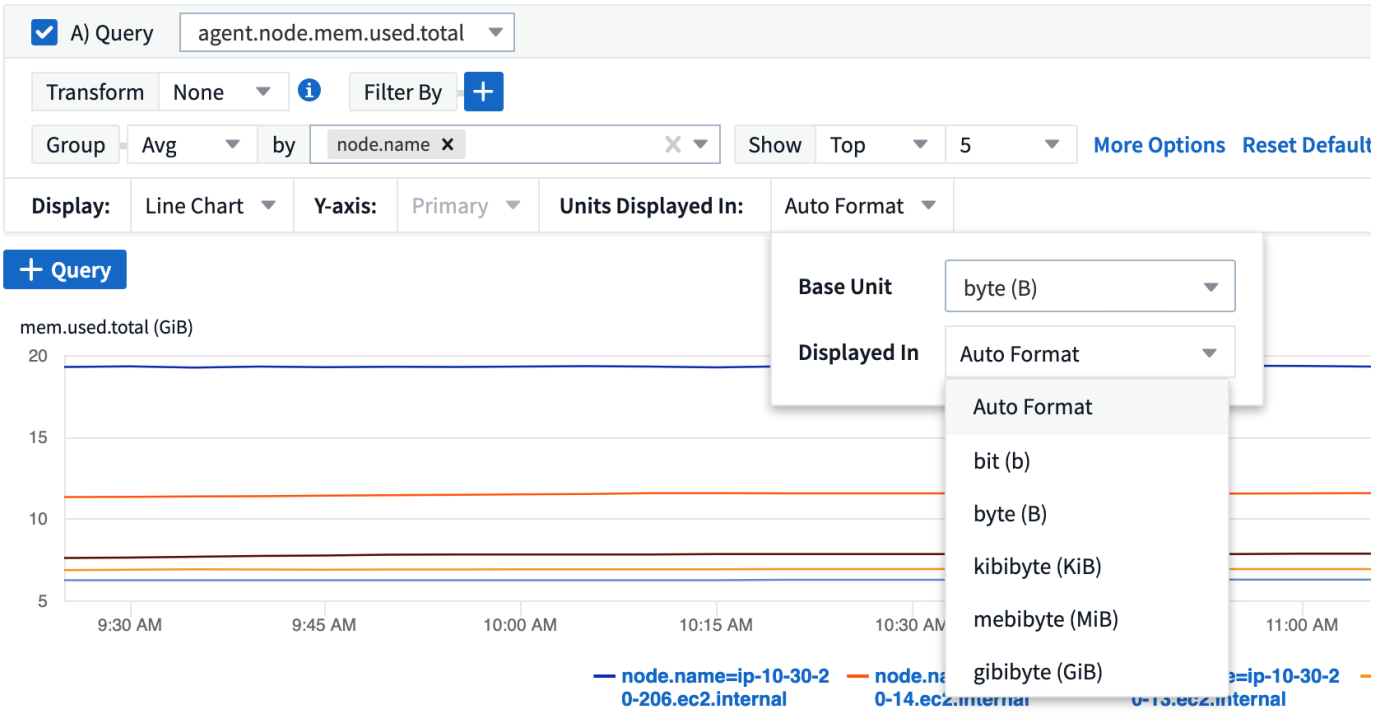
データを表示するための単位の選択

ダッシュボード上のほとんどのウィジェットでは、値を表示する単位（メガバイト、千、パーセンテージ、ミリ秒（ms）など）を指定できます。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、必要な形式を設定できます。

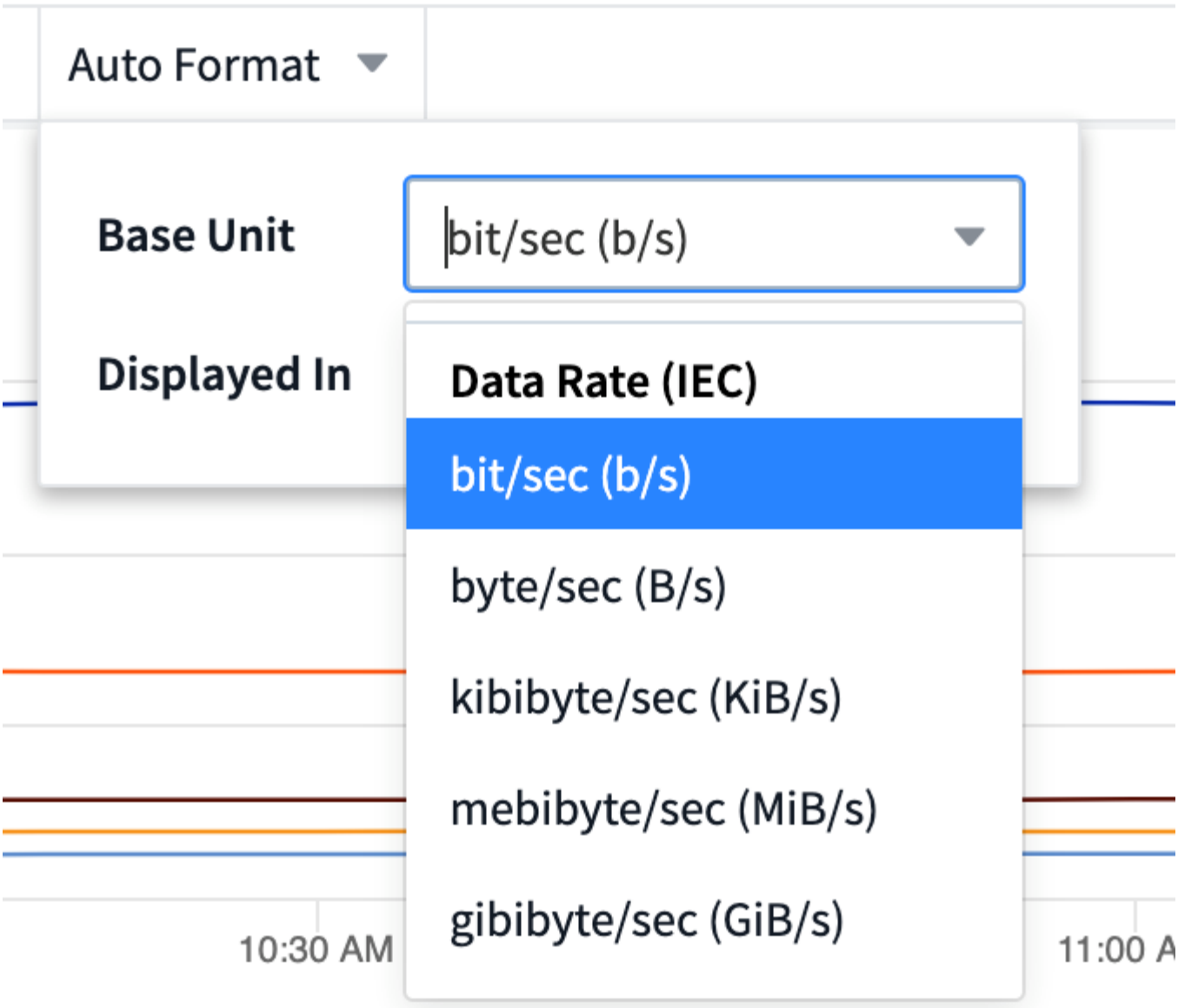
以下の折れ線グラフの例では、ウィジェットに選択されたデータは バイト (基本 IEC データ単位: 下の表を参照) であることがわかっているため、基本単位は自動的に「バイト (B)」として選択されます。ただし、データ値はギビバイト (GiB) で表示できるほど大きいため、 Data Infrastructure Insights はデフォルトで値を GiB として自動フォーマットします。グラフの Y 軸には表示単位として「GiB」が表示され、すべての値はその単位で表示されます。



グラフを別の単位で表示したい場合は、値を表示する別の形式を選択できます。この例では基本単位は バイト なので、サポートされている「バイトベース」の形式（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)）から選択できます。 Y 軸のラベルと値は、選択した形式に応じて変わります。



基本単位が不明な場合は、"利用可能なユニット" 、または独自のものを入力します。基本単位を割り当てたら、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するように選択できます。



設定をクリアして最初からやり直すには、「デフォルトにリセット」をクリックします。

自動フォーマットについて

ほとんどのメトリックは、データ コレクターによって、たとえば 1,234,567,890 バイトなどの整数などの最小単位で報告されます。デフォルトでは、 Data Infrastructure Insights は、最も読みやすい表示になるように値を自動的にフォーマットします。たとえば、1,234,567,890 バイトのデータ値は、1.23 ギビバイト に自動的にフォーマットされます。 *Mebibytes* などの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、アメリカ英語の数値命名標準を使用します。アメリカの「billion」は「thousand million」に相当します。

複数のクエリを持つウィジェット

2 つのクエリがあり、両方ともプライマリ Y 軸にプロットされる時系列ウィジェット (線、スプライン、面、積み上げ面) がある場合、基本単位は 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 軸のクエリとセカンダリ Y 軸のクエリがある場合は、それぞれの基本単位が表示されます。



ウィジェットに 3 つ以上のクエリがある場合、Y 軸に基本単位は表示されません。

利用可能なユニット

次の表には、利用可能なすべてのユニットがカテゴリ別に表示されています。

カテゴリ	単位
通貨	セントドル
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
データレート(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（メトリック）	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
データレート(メトリック)	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	kibi mebi gibi tebi pebi exbi
小数点	整数 千 百万 十億 兆
%	パーセンテージ
Time	ナノ秒、マイクロ秒、ミリ秒、秒、分、時間
温度	摂氏華氏
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 マイクロコア ミリコア コア キロコア メガコア ギガコア テラコア ペタコア エクサコア
スループット	I/O オペレーション/秒 オペレーション/秒 リクエスト/秒 読み取り/秒 書き込み/秒 オペレーション/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、選択したダッシュボードの時間範囲によって決ま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 (折れ線グラフ、スプライン グラフ、面グラフ、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) であるかによって決まります。

ダッシュボードの時間範囲	時系列更新間隔	非時系列更新間隔

最後の15分	10秒	1分
最後の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
過去 24 時間	5分	10分
過去 2 日間	10分	10分
過去 3 日間	15分	15分
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隅に自動更新間隔が表示されます。

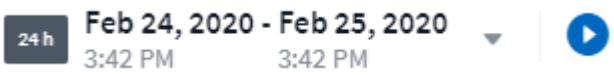
自動更新は、カスタム ダッシュボードの時間範囲では使用できません。

*TV モード*と組み合わせると、自動更新によりダッシュボードまたはアセット ページにデータをほぼリアルタイムで表示できます。 TV モードでは、すっきりとした表示が提供されます。ナビゲーション メニューは非表示になり、編集ボタンと同様に、データ表示用の画面領域が広くなります。 TV モードでは、一般的なData Infrastructure Insights のタイムアウトは無視され、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されるまで、ディスプレイはライブのままになります。

NetApp Consoleには 7 日間の独自のユーザー ログイン タイムアウトがあるため、 Data Infrastructure Insightsそのイベントで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が引き続き表示されます。

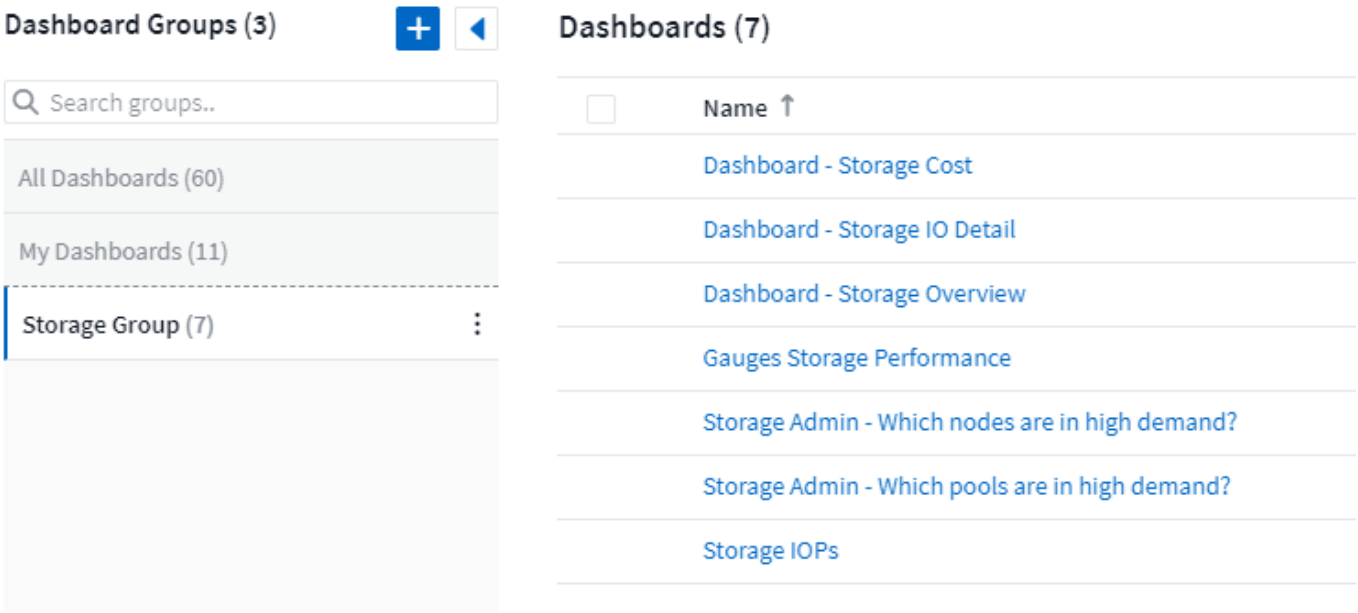
- TV モードを有効にするには、TV モード ボタンをクリックします。
- TV モードを無効にするには、画面の左上にある [終了] ボタンをクリックします。

右上隅の「一時停止」ボタンをクリックすると、自動更新を一時的に停止できます。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、データは引き続き取得および更新されます。データの自動更新を続行するには、[再開] ボタンをクリックします。



ダッシュボードグループ

グループ化すると、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、テナント上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 > すべてのダッシュボードを表示 ページで管理されます。



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一覧表示されます。
- *マイダッシュボード*には、現在のユーザーが作成したダッシュボードのみがリストされます。

各グループに含まれるダッシュボードの数は、グループ名の横に表示されます。

新しいグループを作成するには、「**"+"** 新しいダッシュボード 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。その名前で空のグループが作成されます。

グループにダッシュボードを追加するには、[すべてのダッシュボード] グループをクリックしてテナントのすべてのダッシュボードを表示するか、自分が所有するダッシュボードのみを表示する場合は [マイ ダッシュボード] をクリックして、次のいずれかを実行します。

- 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、「グループに追加」を選択します。
- 複数のダッシュボードをグループに追加するには、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選択し、[一括操作] ボタンをクリックして [グループに追加] を選択します。

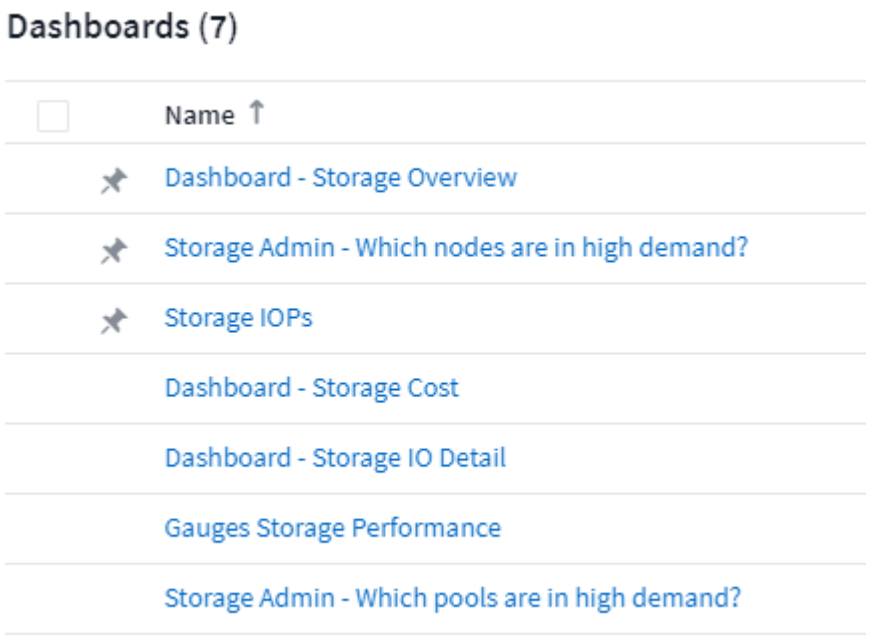
同じ方法で、[グループから削除] を選択して、現在のグループからダッシュボードを削除します。 すべてのダッシュボード または マイ ダッシュボード グループからダッシュボードを削除することはできません。

グループからダッシュボードを削除しても、Data Infrastructure Insightsからダッシュボードは削除されません。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、「削除」をクリックします。これにより、そのアイテムが属していたグループから削除され、どのユーザーも利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留めする

お気に入りのダッシュボードをダッシュボード リストの上部にピン留めすることで、ダッシュボードをさらに管理できます。ダッシュボードをピン留めするには、リスト内のダッシュボードにマウスを移動したときに表示される画鋲ボタンをクリックするだけです。

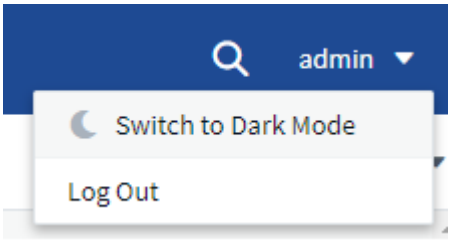
ダッシュボードのピン留め/ピン留め解除は個々のユーザー設定であり、ダッシュボードが属するグループ (複数可) とは無関係です。



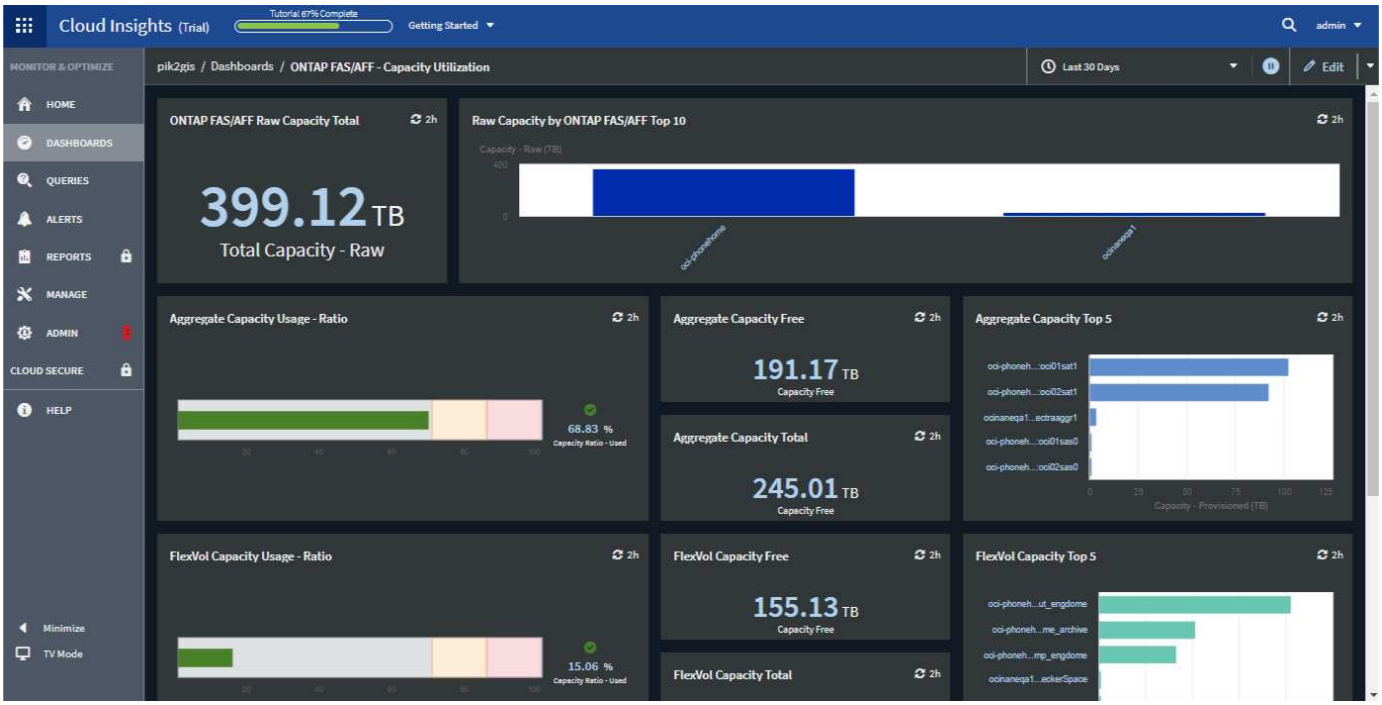
ダークテーマ

Data Infrastructure Insights は、明るいテーマ (デフォルト) (ほとんどの画面を明るい背景に暗いテキストで表示する)、または暗いテーマ (ほとんどの画面を暗い背景に明るいテキストで表示する) のいずれかを使用して表示することを選択できます。

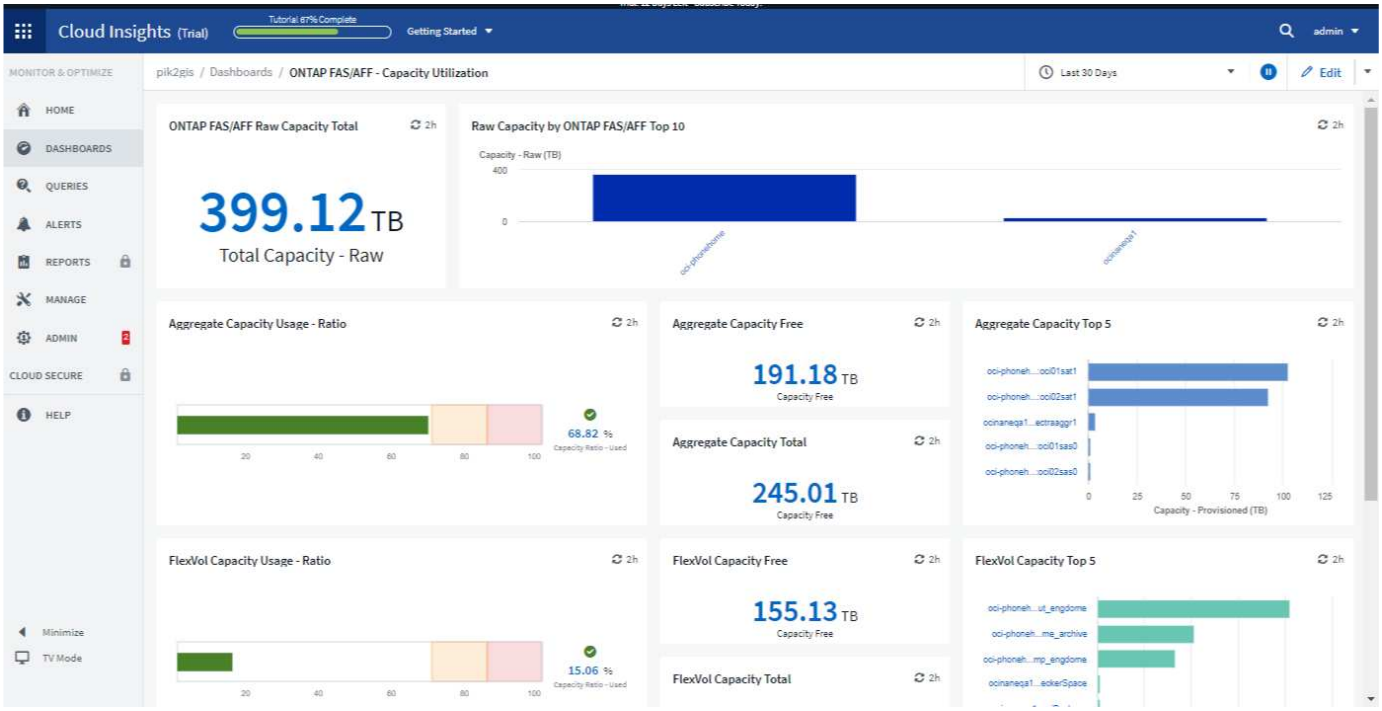
明るいテーマと暗いテーマを切り替えるには、画面の右上隅にあるユーザー名ボタンをクリックし、希望のテーマを選択します。



ダークテーマのダッシュボードビュー
:



ライトテーマのダッシュボードビュー
:



特定のウィジェット チャートなどの一部の画面領域では、ダーク テーマで表示されていても明るい背景が表示されます。

折れ線グラフの補間

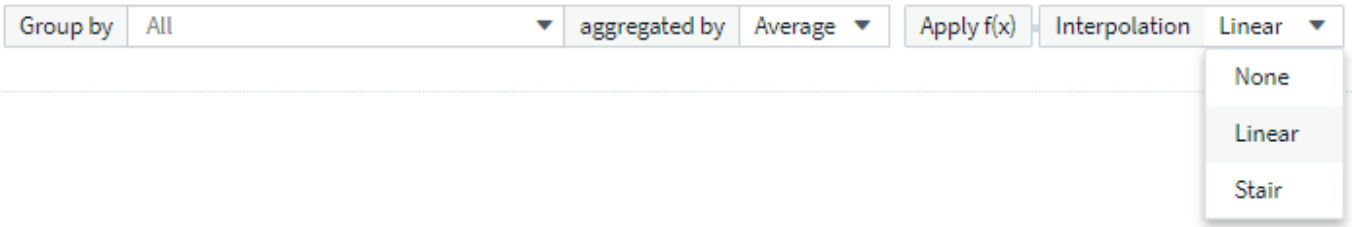
多くの場合、さまざまなデータ コレクターがさまざまな間隔でデータをポーリングします。たとえば、データ コレクター A は 15 分ごとにポーリングし、データ コレクター B は 5 分ごとにポーリングする場合があります。折れ線グラフ ウィジェット (スプライン グラフ、面グラフ、積み上げ面グラフも含む) が複数のデータ コレクターからのデータを 1 つの線に集計し (たとえば、ウィジェットが「すべて」でグループ化されている

場合)、その線を 5 分ごとに更新すると、コレクター B のデータは正確に表示されますが、コレクター A のデータにはギャップが生じる可能性があり、コレクター A が再度ポーリングするまで集計に影響します。

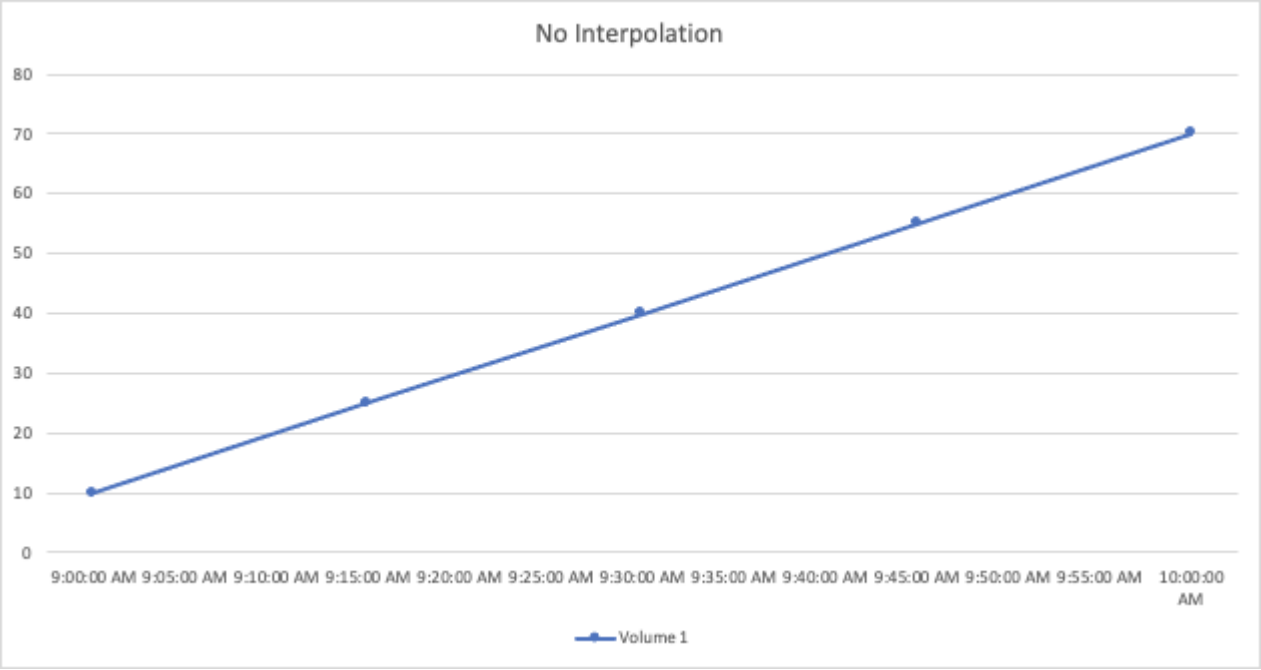
これを緩和するために、 Data Infrastructure Insights は、データ コレクターが再度ポーリングするまで、周囲のデータ ポイントを使用してデータの「最善の推測」を行い、集計時にデータを補間します。ウィジェットのグループ化を調整することで、各データ コレクターのオブジェクト データをいつでも個別に表示できます。

補間法

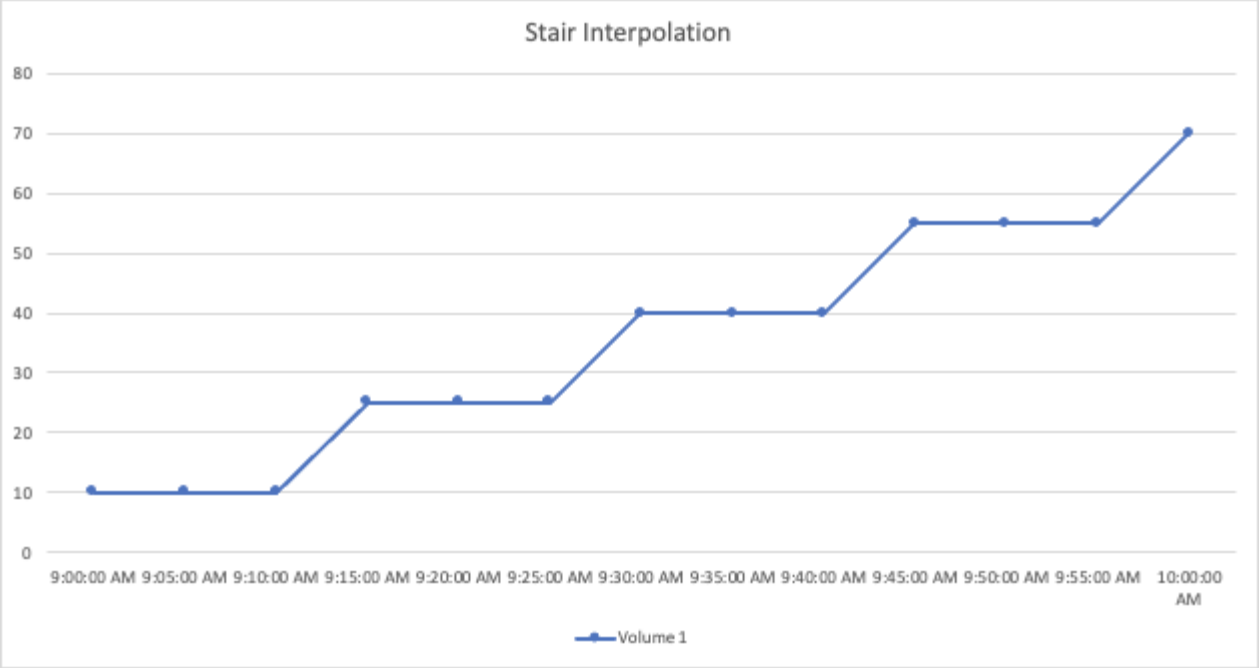
折れ線グラフ (またはスプライン グラフ、面グラフ、積み上げ面グラフ) を作成または変更するときに、補間方法を 3 つのタイプのいずれかに設定できます。 「グループ化」セクションで、必要な補間を選択します。



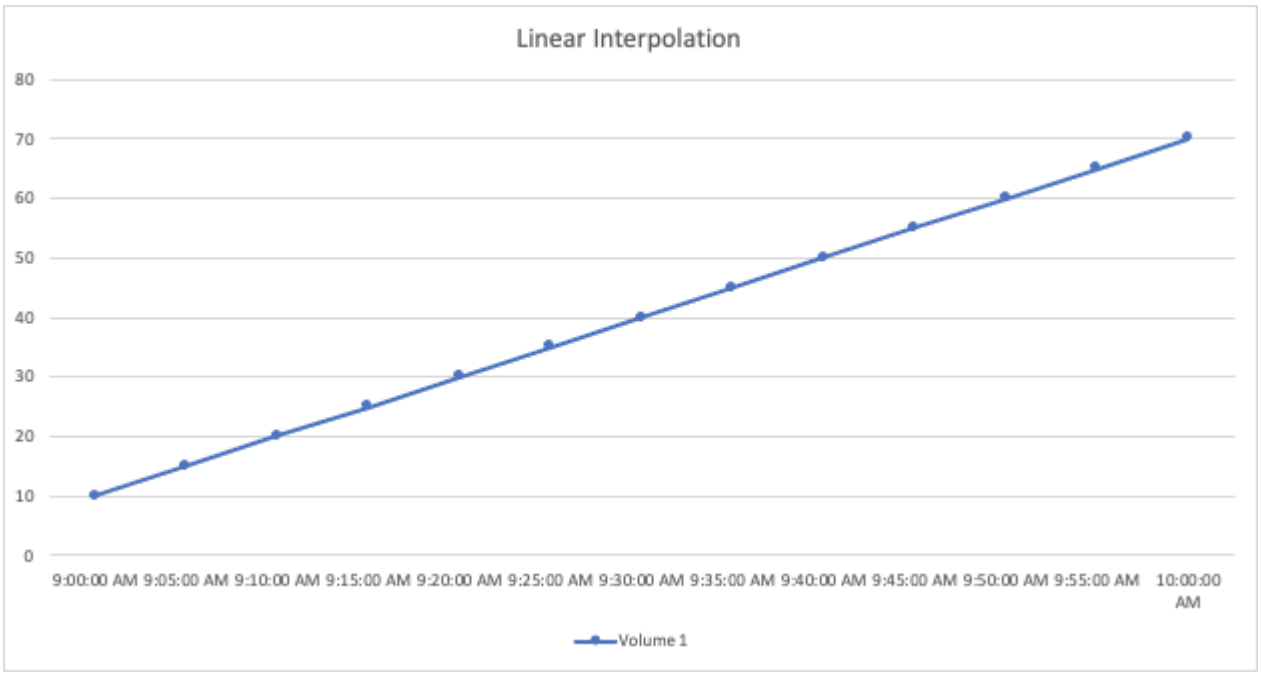
- なし: 何もしません。つまり、中間のポイントは生成されません。



- 階段: 前のポイントの値からポイントが生成されます。直線の場合、これは典型的な「階段」レイアウトとして表示されます。



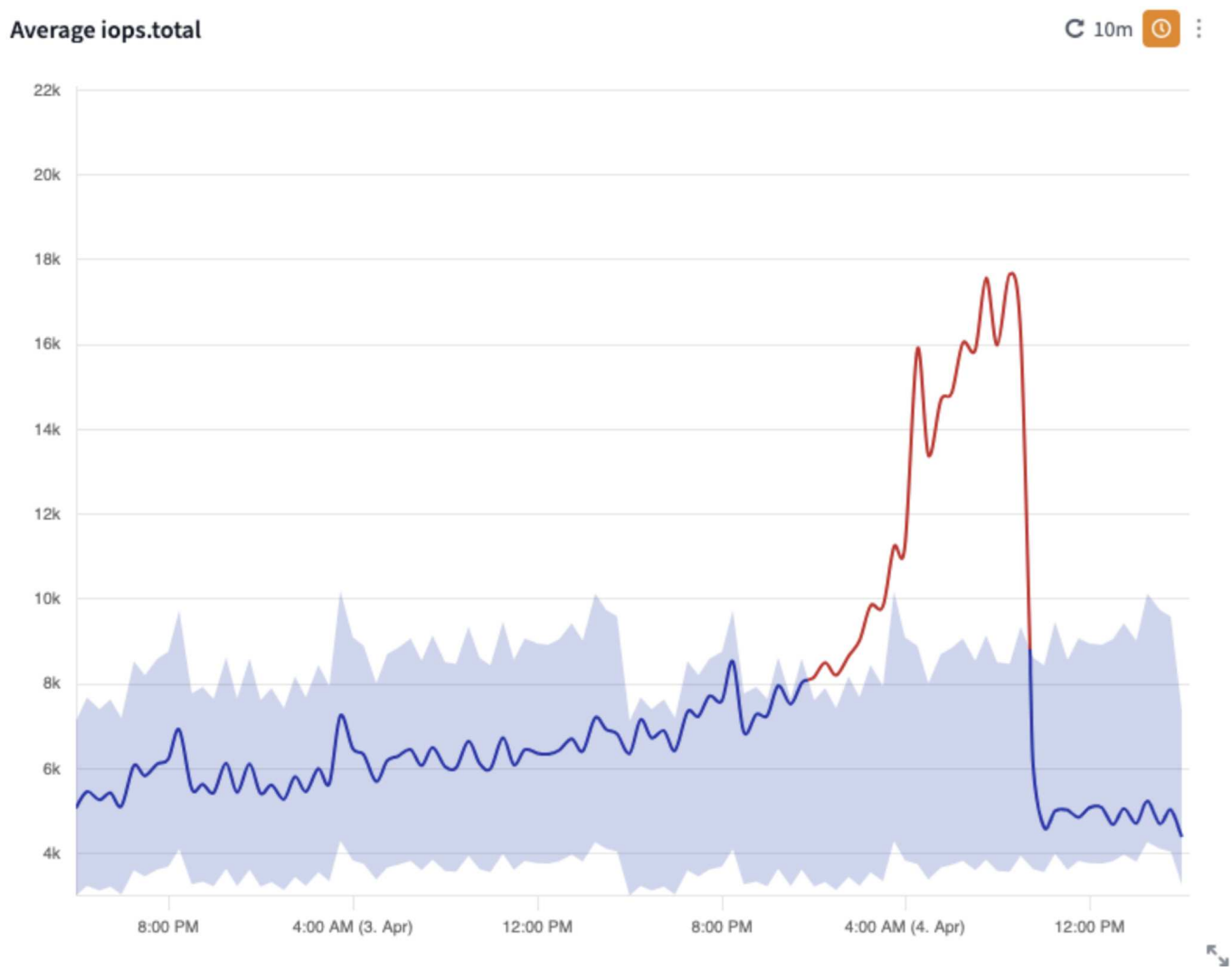
- 線形: 2 つのポイントを接続し、その間の値としてポイントが生成されます。 2 つのポイントを結ぶ線に似た線を生成しますが、追加の (補間された) データ ポイントが含まれます。



ラインウィジェットの異常境界

ダッシュボードまたはランディング ページに折れ線グラフまたはスプライン グラフ ウィジェットを含める場合、データの 予想される境界 のコンテキストでグラフを表示することを選択できます。これは、データのパターンにおける異常を探すことと考えることができます。

DII は季節データ (時間別または日別) を使用して、特定の時間にデータがどこに位置すると予想されるかの上限と下限を設定します。データが予想範囲を超えて急上昇したり、予想範囲を下回ったりした場合、グラフではそれが異常として強調表示されます。



異常境界を表示するには、ウィジェットを編集し、「異常境界を表示」を選択します。次の 2 つの検出アルゴリズムから選択できます。

- **Adaptive Detector** は変化に素早く適応するため、詳細な調査に役立ちます。
- スムーズ ディテクター は、ノイズと誤検知を最小限に抑え、短期的な変動を除去しながら、大きな変化を検出します。

さらに、季節性を 時間別 または 日別 で表示するように選択したり、検出の感度を設定したりすることもできます。 _高_感度ではより多くの境界越えが検出され、_低_感度ではより少ない境界越えが検出されます。

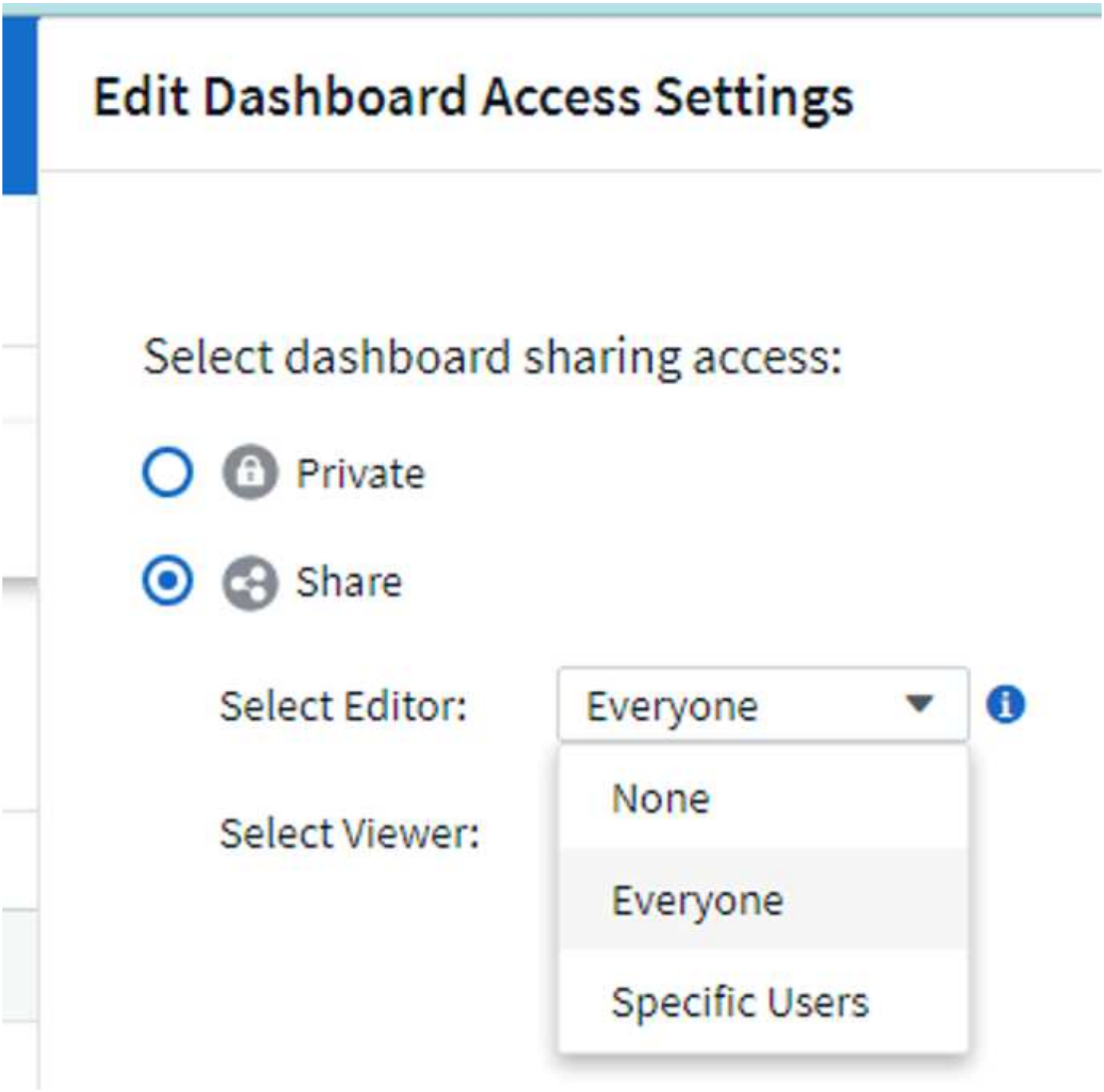


チャートが 1 本の線を表示するように設定されている場合にのみ、予想される境界が表示されることに注意してください。グループ化設定またはフィルターに複数の行が表示されている場合、またはウィジェットに複数のクエリを設定している場合、予想される境界を表示するオプションは無効になります。

ダッシュボードアクセス管理

Data Infrastructure Insightsでは、作成したダッシュボードへのアクセスをより細かく制

御できるようになりました。グラフを変更できるユーザーを選択します。潜在的に機密性の高い情報への公開を制御できます。ダッシュボードを非公開にしておくと、組織内の他のユーザーが使用できるようになるまで、視覚化を完成させることができます。

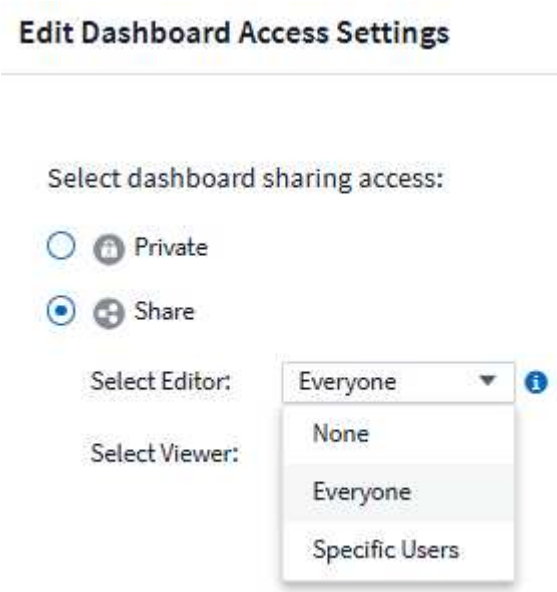


デフォルトでは、新しいダッシュボードを作成すると、そのダッシュボードは作成者であるあなただけに表示されます。他のユーザーはダッシュボードを表示したり変更したりすることはできません。

ダッシュボードが完成したら、組織内の他のユーザーがそれを閲覧できるようにすることができます。ダッシュボードを共有するには、ダッシュボード リストで、右側のメニューから [共有] を選択します。



ダッシュボードをすべてのユーザーと共有するか、編集権限または読み取り専用権限を持つ特定のユーザーと共有するかを選択できます。



ダッシュボードとウィジェットのベストプラクティス

ダッシュボードとウィジェットの強力な機能を最大限に活用するためのヒントとコツ。

適切な指標を見つける

Data Infrastructure Insights は、データ コレクターごとに異なる場合がある名前を使用してカウンターとメトリックを取得します。

ダッシュボード ウィジェットに適したメトリックまたはカウンターを検索するときは、必要なメトリックが、考えていたものとは異なる名前で表示されている可能性があることに注意してください。 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ですが、用語がリスト内の必要な場所に表示されない場合があります。たとえば、「生の容量」と「使用済み容量」などの用語は、ほとんどのリストでは一緒に表示されません。

ベスト プラクティス: [フィルター条件] などのフィールドや列セレクターなどの場所の検索機能を使用して、探しているものを見つけます。たとえば、「cap」を検索すると、リスト内のどこにあっても、名前に「capacity」が含まれるすべてのメトリックが表示されます。その後、その短いリストから必要なメトリックを簡単に選択できます。

メトリックを検索するときに試すことができるいくつかの代替フレーズを次に示します。

検索したい場合:	以下も検索してみてください:
CPU	プロセッサ
容量	使用済み容量 生容量 プロビジョニング済み容量 ストレージプールの容量 <その他の資産タイプ> の容量 書き込み済み容量
ディスク速度	最も低いディスク速度 最もパフォーマンスの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	ホストはハイパーバイザー
マイクロコード	ファームウェア
Name	エイリアス ハイパーバイザー名 ストレージ名 <その他の資産タイプ> 名 シンプル名 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は仮想です

これは包括的なリストではありません。これらは、可能な検索用語の例にすぎません。

適切な資産を見つける

ウィジェットのフィルターや検索で参照できるアセットは、アセットの種類によって異なります。

ダッシュボードとアセット ページでは、ウィジェットを構築するアセット タイプによって、フィルター処理や列の追加が可能な他のアセット タイプ カウンターが決まります。ウィジェットを構築するときは、次の点に留意してください。

この資産タイプ/カウンター:	以下のアセットでフィルタリングできます:
仮想マシン	VMDK
データストア	内部ボリューム VMDK 仮想マシンボリューム
ハイパーバイザー	仮想マシンはハイパーバイザーホストです
ホスト	内部ボリューム ボリューム クラスター 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資産タイプをフィルターする場合は、別の資産タイプを中心にクエリを構築してみてください。

散布図の例: 軸を知る

散布図ウィジェット内のカウンターの順序を変更すると、データが表示される軸が変更されます。

タスク概要

この例では、低い IOPS と比較してレイテンシが高いパフォーマンスの低い VM を確認できる散布図を作成します。

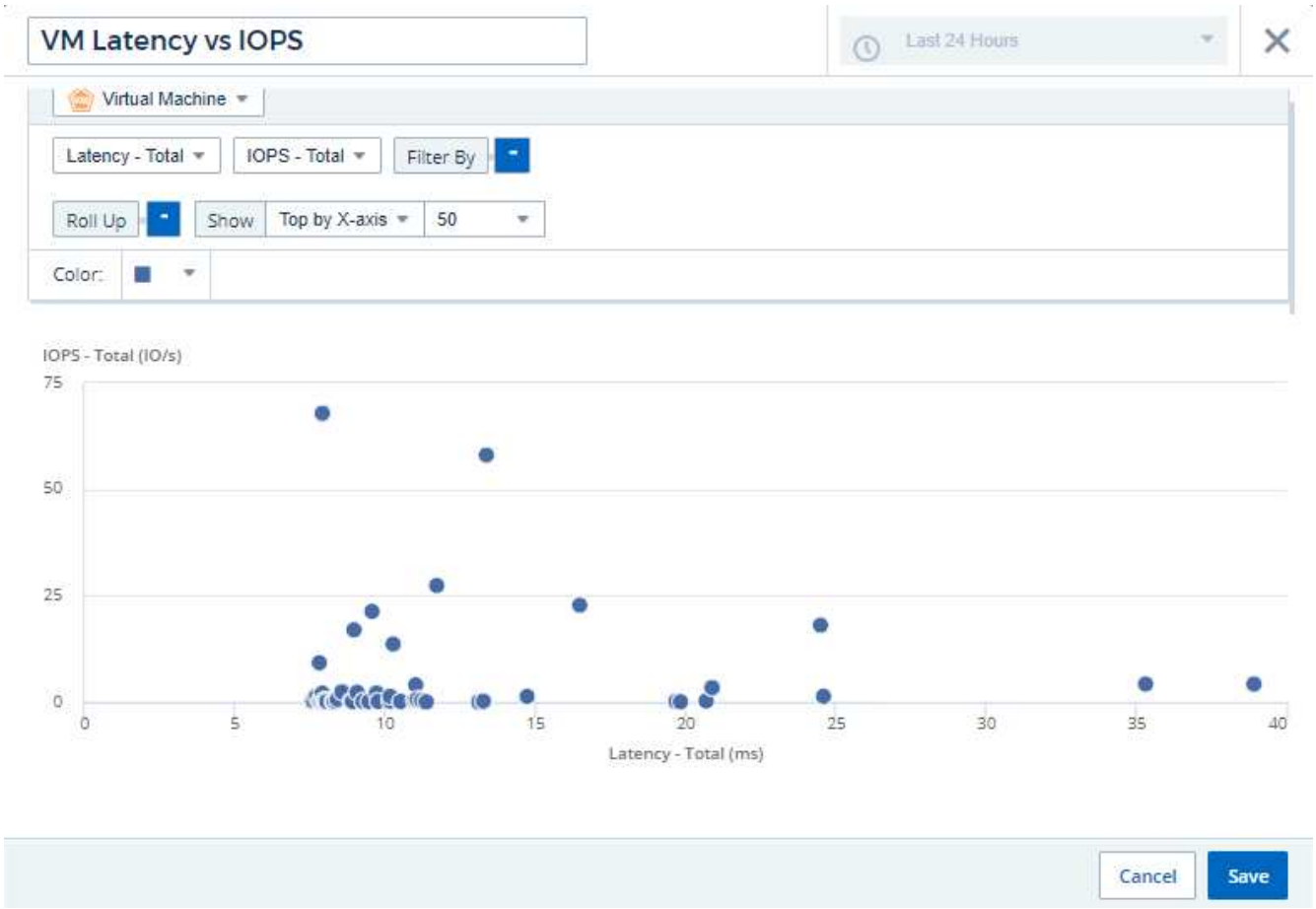
手順

1. 編集モードでダッシュボードを作成するか開き、*散布図チャート*ウィジェットを追加します。
2. 資産タイプ (例: 仮想マシン) を選択します。
3. プロットする最初のカウンターを選択します。この例では、「*Latency - Total*」を選択します。

   レイテンシ - 合計 は、グラフの X 軸に沿ってグラフ化されます。

4. プロットする 2 番目のカウンターを選択します。この例では、「*IOPS* - 合計」を選択します。

   IOPS - 合計 は、グラフの Y 軸に沿って表示されます。レイテンシの高い VM はグラフの右側に表示されます。 **X** 軸で上位 の設定が現在であるため、レイテンシが最も高い上位 100 個の VM のみが表示されます。

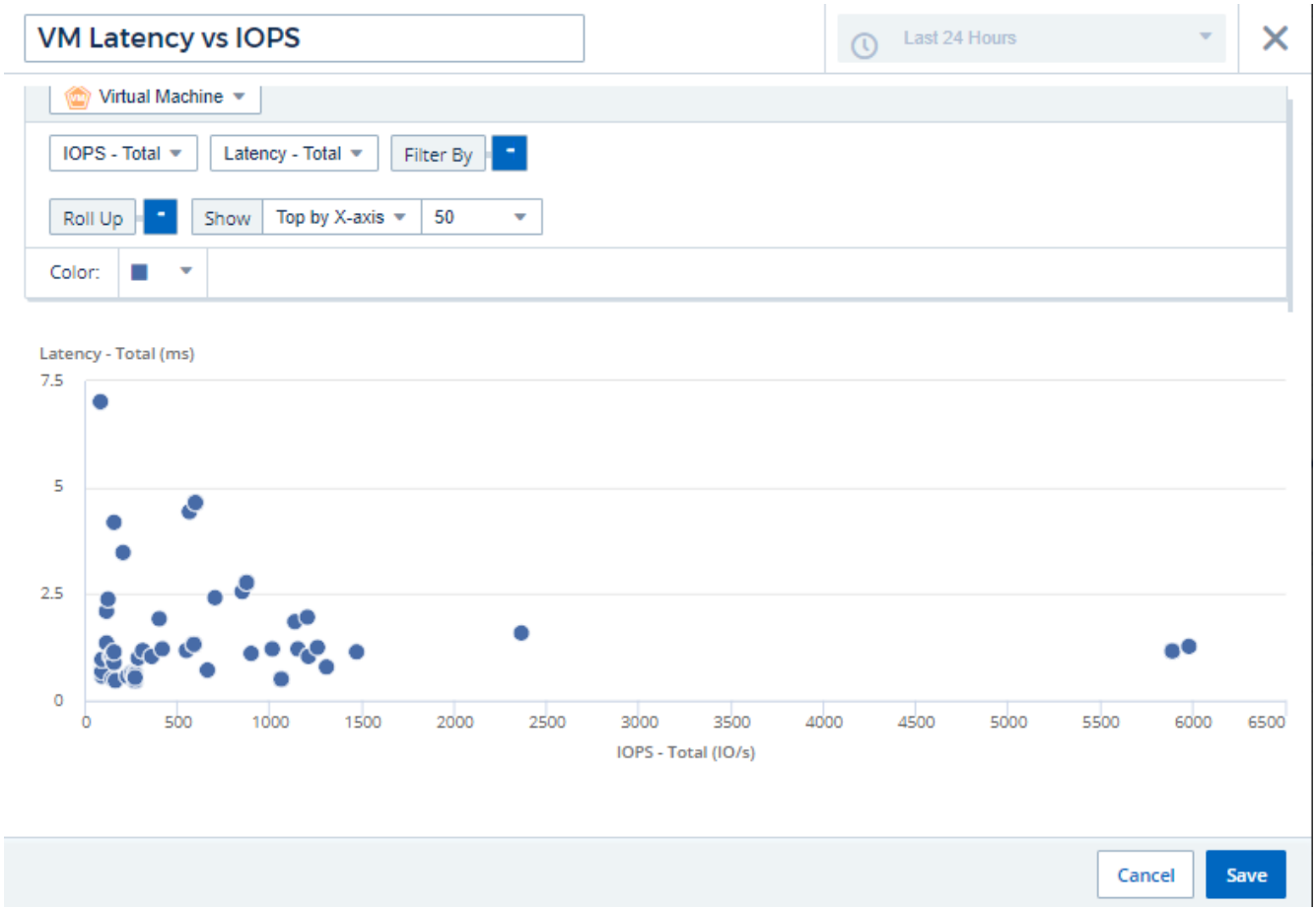


5. ここで、最初のカウンターを *IOPS - Total* に設定し、2 番目のカウンターを *Latency - Total* に設定して、カウンターの順序を逆にします。

   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。より高い IOPS を持つ VM がグラフの右側に表示されるようになりました。

   *X 軸上位*設定を変更していないため、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 が表示されることに注意してください。



グラフに X 軸の上位 N、Y 軸の上位 N、X 軸の下位 N、または Y 軸の下位 N を表示するように選択できます。最後の例では、合計 IOPS が最も高い上位 100 個の VM がグラフに表示されます。これを **Y** 軸による上位 に変更すると、チャートには、合計レイテンシが最も高い上位 100 個の VM が再び表示されます。

散布図では、ポイントをクリックすると、そのリソースの資産ページにドリルダウンできることに注意してください。

サンプルダッシュボード

ダッシュボードの例: 仮想マシンのパフォーマンス

今日の IT 運用には多くの課題が存在します。管理者は少ないリソースでより多くの成果を出すことが求められており、動的なデータセンターを完全に可視化することが必須となっています。この例では、テナント上の仮想マシン (VM) のパフォーマンスに関する運用上の洞察を提供す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説明します。この例に従い、独自の特定のニーズをターゲットにしたウィジェットを作成することで、バックエンドのストレージ パフォーマンスをフロントエンドの仮想マシンのパフォーマンスと比較して視覚化したり、VM のレイテンシと I/O 需要を比較表示したりといったことが可能になります。

タスク概要

ここでは、次の内容を含む仮想マシン パフォーマンス 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したテーブル
- VMレイテンシとストレージレイテンシを比較したグラフ
- VMの読み取り、書き込み、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

これは単なる基本的な例です。ダッシュボードをカスタマイズして、選択したパフォーマンス データを強調表示して比較し、独自の運用のベスト プラクティスをターゲットにすることができます。

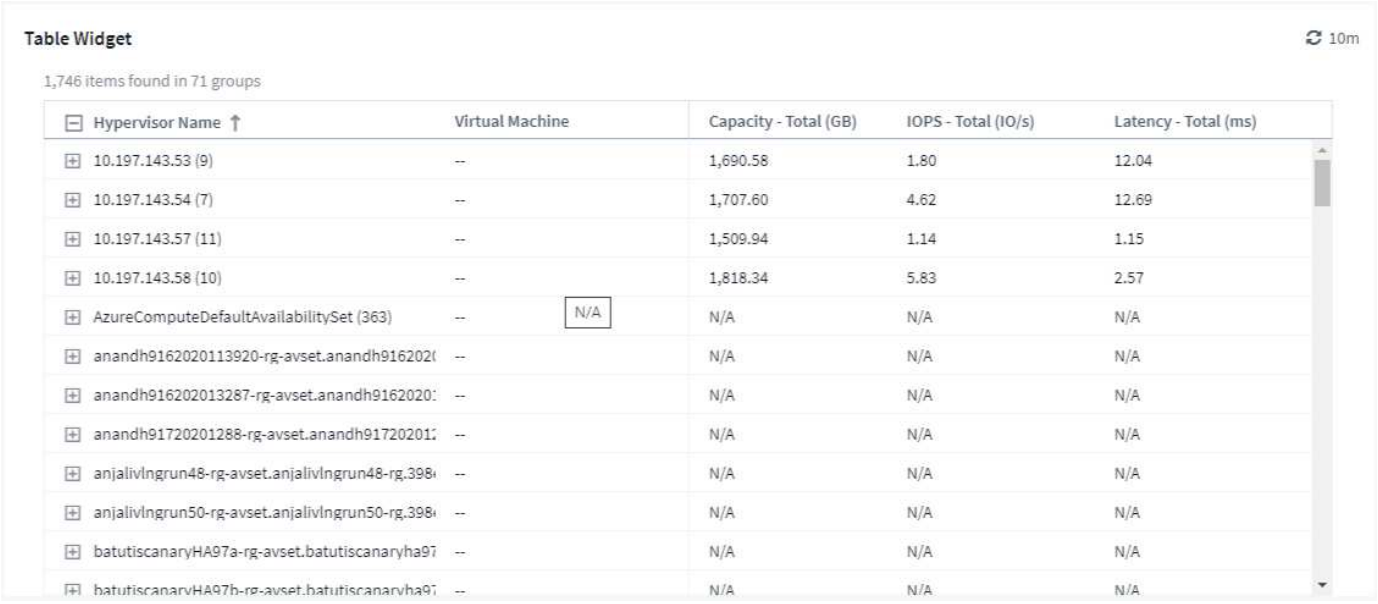
手順

1. 管理者権限を持つユーザーとして 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、ダッシュボードの一意の名前を入力します (例: 「アプリケーション別の VM パフォーマンス」)。
4. **[**保存**]** をクリックして、ダッシュボードを新しい名前で保存します。
5. ウィジェットの追加を始めましょう。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*アイコンをクリックし、*テーブル*を選択して、ダッシュボードに新しいテーブル ウィジェットを追加します。

   ウィジェット編集ダイアログが開きます。表示されるデフォルトのデータは、テナント上のすべてのストレージに関するものです。



1. このウィジェットはカスタマイズできます。上部の名前フィールドで、「Widget 1」を削除し、「Virtual Machine Performance table」と入力します。
2. 資産タイプのドロップダウンをクリックし、*Storage* を *Virtual Machine* に変更します。

テーブル データが変更され、テナント上のすべての仮想マシンが表示されます。

3. テーブルにいくつかの列を追加してみましょう。右側の歯車アイコンをクリックし、ハイパーバイザー名、*IOPS* - 合計、_レイテンシ - 合計_を選択します。検索に名前を入力して、目的のフィールドをすばやく表示することもできます。

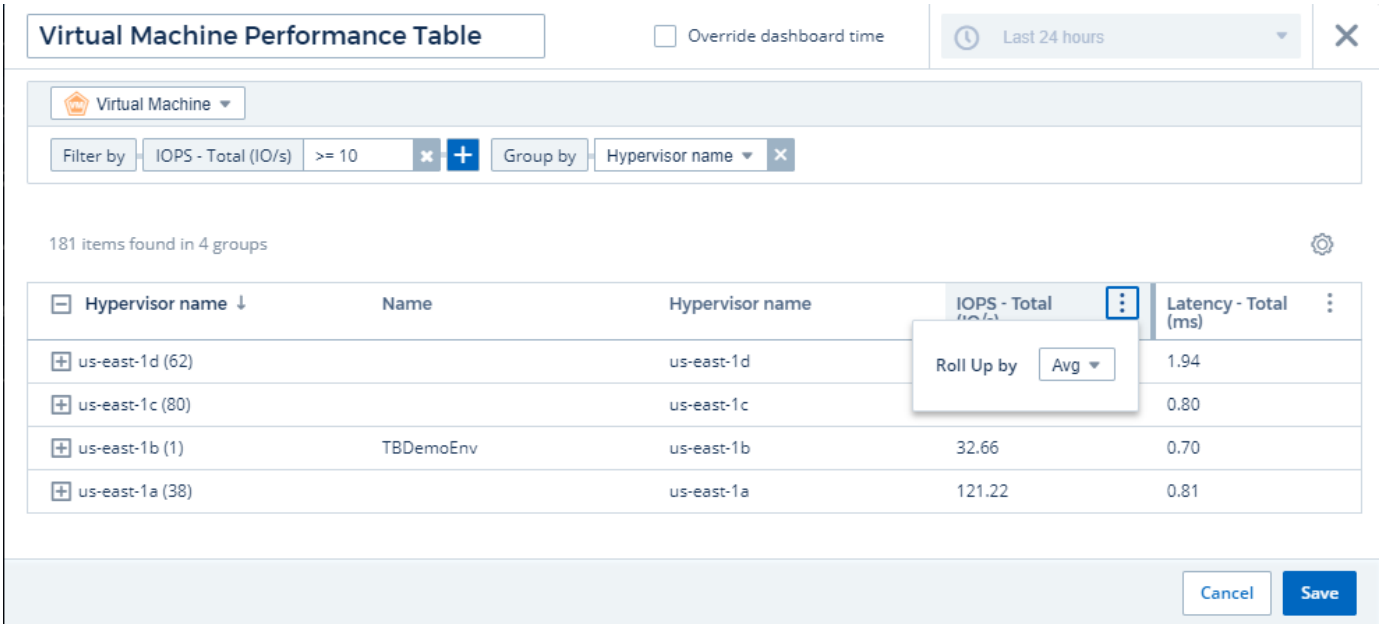
   これらの列がテーブルに表示されるようになりました。これらの列のいずれかでテーブルを並べ替えることができます。列はウィジェットに追加された順序で表示されることに注意してください。

4. この演習では、アクティブに使用されていない VM を除外するため、合計 IOPS が 10 未満のものをフィルター処理しましょう。 フィルター条件*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*をクリックし、*開始*フィールドに「10」と入力します。 *宛先*フィールドは空のままにしておきます。フィルターを設定するには、フィルター フィールドの外側をクリックするか、Enter キーを押してください。

   テーブルには、合計 IOPS が 10 以上の VM のみが表示されるようになりました。

5. 結果をグループ化することで、テーブルをさらに折りたたむことができます。 グループ化*の横にある[+]*ボタンをクリックし、_アプリケーション_や_ハイパーバイザー名_などのグループ化するフィールドを選択します。グループ化は自動的に適用されます。

   これで、テーブル行が設定に従ってグループ化されました。必要に応じてグループを展開したり折りたたんだりできます。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、その列のロールアップ方法を選択できます。



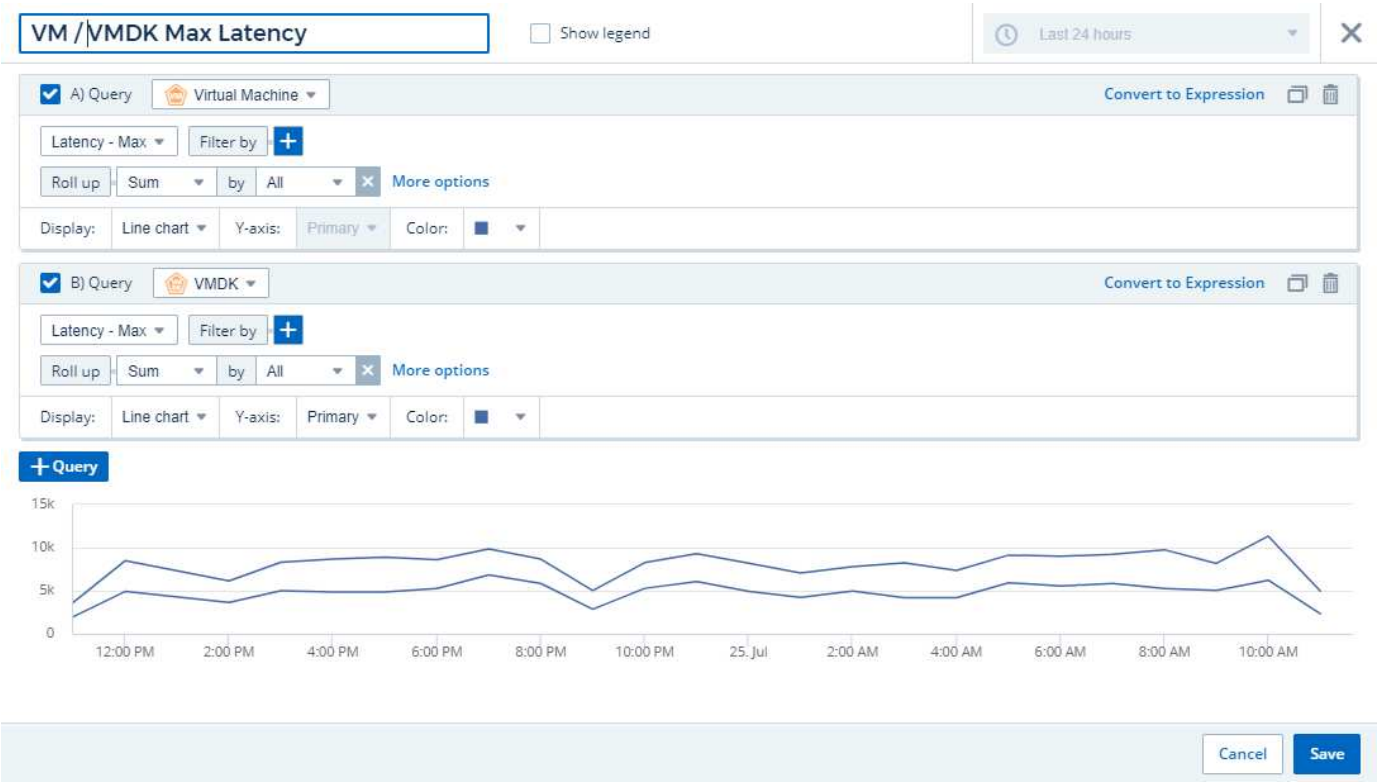
1. テーブル ウィジェットを満足のいくようにカスタマイズしたら、**[[保存]]** ボタンをクリックします。

   テーブル ウィジェットは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隅をドラッグしてサイズを変更できます。すべての列を明確に表示するには、ウィジェットの幅を広げます。現在のダッシュボードを保存するには、[保存] をクリックします。

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。 VM レイテンシと VMDK レイテンシを比較する折れ線グラフを作成しましょう。

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. **[**ウィジェットを追加**]** アイコンをクリックし、折れ線グラフ を選択して、ダッシュボードに新しい折れ線グラフ ウィジェットを追加します。
3. *ウィジェットの編集*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」という名前を付けます
4. *仮想マシン*を選択し、*Latency - Max*_を選択します。必要なフィルターを設定するか、*[*フィルター条件*]* を空のままにしておきます。 *ロールアップ*の場合は、*[*すべて合計*]* を選択します。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。
5. 2 番目のデータ ラインを追加するには、**[+** クエリ**]** ボタンをクリックします。この行では、*VMDK* と *Latency - Max* を選択します。必要なフィルターを設定するか、[フィルター条件] を空のままにしておきます。 *ロールアップ*の場合は、[すべて合計] を選択します。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。
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。

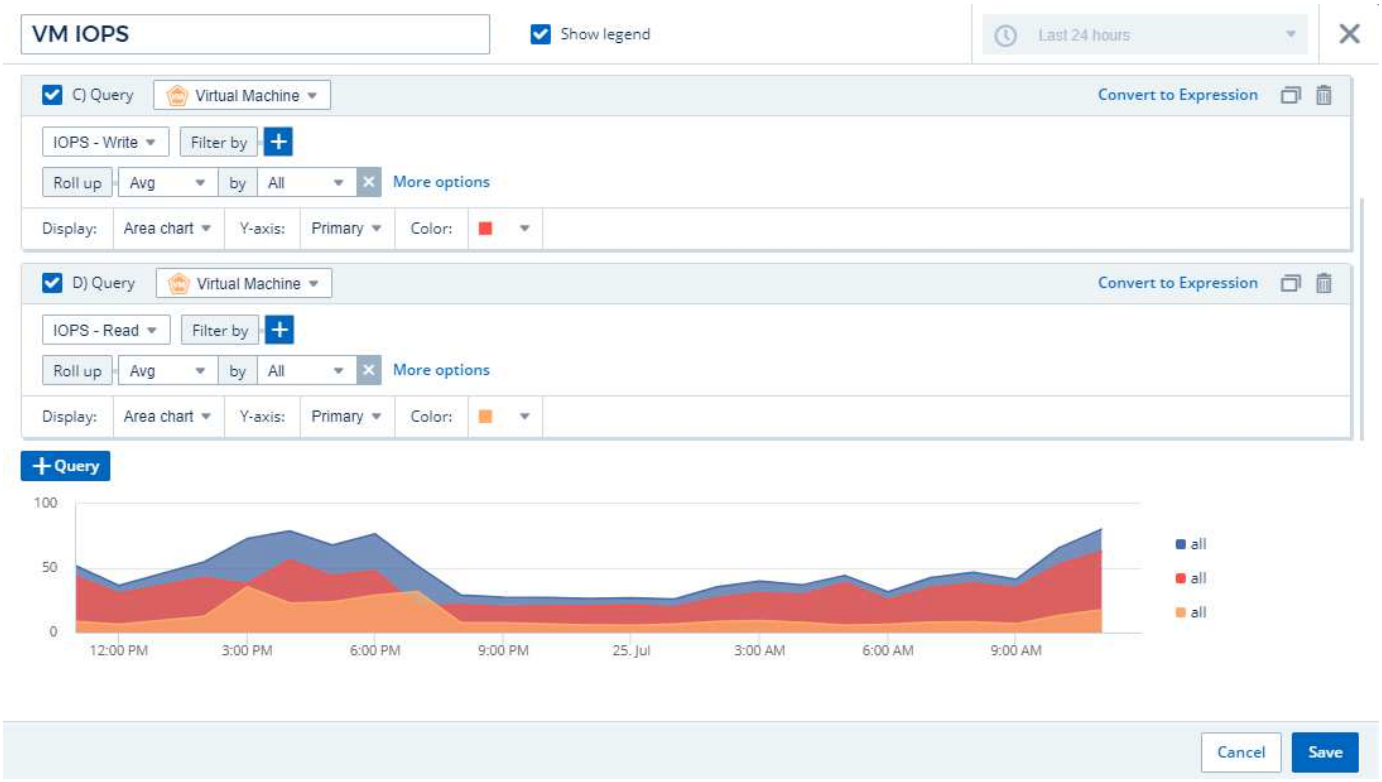


次に、VM の読み取り、書き込み、および合計 IOPS を 1 つのグラフで表示するグラフを追加します。

1. **[**ウィジェットを追加**]** アイコンをクリックし、エリア チャート を選択して、ダッシュボードに新しいエリア チャート ウィジェットを追加します。
2. ウィジェット編集ダイアログが開きます。このウィジェットに「VM IOPS」という名前を付けます
3. *仮想マシン*を選択し、_IOPS - 合計_を選択します。必要なフィルターを設定するか、[フィルター条件] を空のままにします。[ロールアップ] の場合は、[すべて] で [合計] を選択します。このデータを_面グラフ_として表示し、_Y 軸_を_プライマリ_のままにします。
4. 2 番目のデータ ラインを追加するには、**[+** クエリ**]** ボタンをクリックします。この行では、*仮想マシン*を選択し、_IOPS - 読み取り_を選択します。
5. 3 番目のデータ行を追加するには、[+クエリ]* ボタンをクリックします。この行では、*仮想マシン*を選

択し、_IOPS - 書き込み_を選択します。

6. ダッシュボードにこのウィジェットの凡例を表示するには、[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各アプリケーションの VM スループットを示す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。

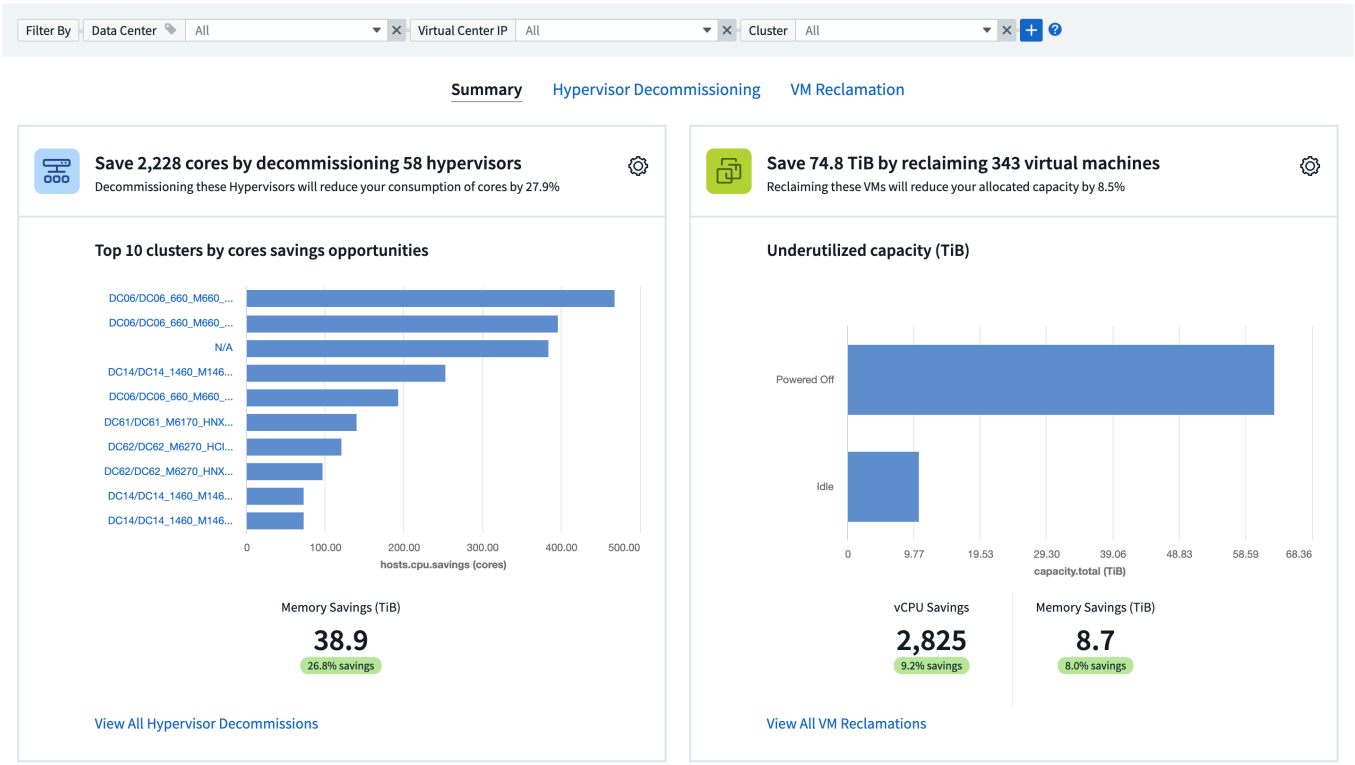
1. **[**ウィジェットを追加**]** アイコンをクリックし、折れ線グラフ を選択して、ダッシュボードに新しい折れ線グラフ ウィジェットを追加します。
2. ウィジェット編集ダイアログが開きます。このウィジェットに「アプリケーション別のVMスループット」という名前を付けます。
3. 仮想マシンを選択し、スループット - 合計を選択します。必要なフィルターを設定するか、「フィルター条件」を空のままにします。ロールアップの場合は、「最大」を選択し、「アプリケーション」または「名前」で選択します。上位 10 件のアプリケーションを表示します。このデータを折れ線グラフとして表示し、Y 軸をプライ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。

ダッシュボード上のウィジェットを移動するには、ウィジェットの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。

右下隅をドラッグしてウィジェットのサイズを変更できます。

変更を加えた後は、必ずダッシュボードを*[保存]*してください。

最終的な VM パフォーマンス ダッシュボードは次のようになります。



クエリの操作

アセットとメトリクスのクエリ

インフラストラクチャの物理資産と仮想資産をクエリすることで、パフォーマンスの監視、問題のトラブルシューティング、注釈などのカスタム基準に基づいたきめ細かな検索を実行できます。Data Infrastructure Insightsは、ストレージアレイやホストからアプリケーションや仮想マシンまで、多様な資産タイプを対象としたクエリに加え、Kubernetes、Docker、ONTAP Advanced Dataの統合メトリクスも提供し、包括的な可視性を実現します。

アセットに自動的にアノテーションを割り当てるアノテーション ルールを使用するには、クエリを全員に共有する必要があります。クエリの共有の詳細については、以下をご覧ください。

テナント上の物理または仮想インベントリ資産（および関連するメトリック）や、Kubernetes やONTAP Advanced Data などの統合によって提供されるメトリックをクエリできます。

在庫資産

すべてのインベントリ（インフラストラクチャとも呼ばれる）アセット タイプ（ストレージ、スイッチ、VM、アプリケーションなど）は、クエリ、ダッシュボード ウィジェット、カスタマイズされたアセット ランディング ページで使用できます。フィルター、式、表示に使用できるフィールドとカウンターは、アセット タイプによって異なります。

統合メトリクス

インベントリ資産とそれに関連するパフォーマンス メトリックのクエリに加えて、Kubernetes または Docker によって生成されたメトリックや、 ONTAP Advanced Metrics で提供されるメトリックなどの 統合データ メトリックもクエリできます。



クエリの共有

クエリへのアクセスを制御するには、クエリを表示および編集できるユーザーを選択します。デフォルトでは、新しいクエリは非公開で、自分だけが閲覧できます。また、柔軟な権限レベル（Read-Only または Edit）を設定して、特定のユーザーまたは組織全体と共有することもできます。

クエリをすべてのユーザーと共有するか、編集権限または読み取り専用権限を持つ特定のユーザーと共有するかを選択できます。

アカウント所有者権限を持つユーザーは、プライバシー設定に関係なく、すべてのクエリを表示できます。

クエリの作成

クエリを使用すると、テナント上のアセットを詳細なレベルで検索できるため、必要なデータをフィルタリングし、結果を好みに合わせて並べ替えることができます。

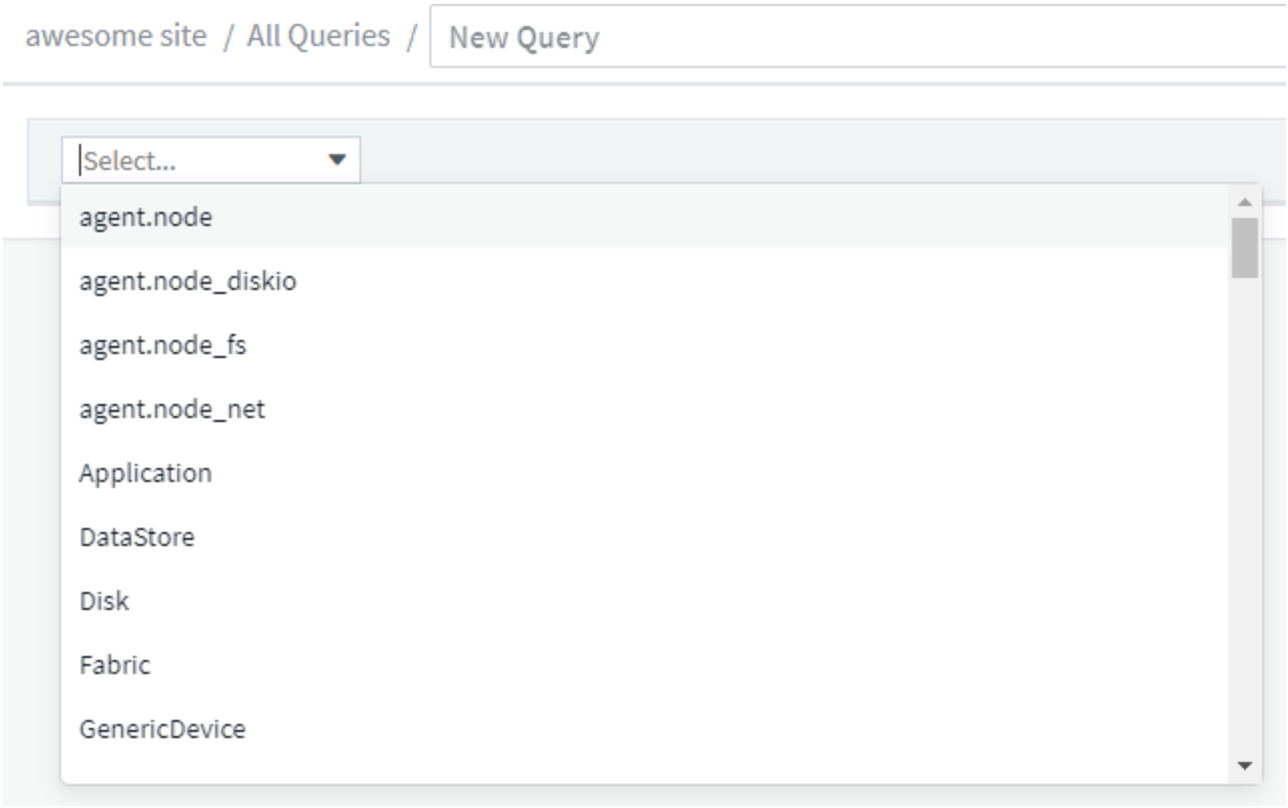
たとえば、ボリュームのクエリを作成し、選択したボリュームに関連付けられた特定のストレージを検索するフィルターを追加し、選択したストレージの「Tier 1」などの特定の注釈を検索する別のフィルターを追加し、最後に IOPS - 読み取り (IO/s) が 25 を超えるすべてのストレージを検索する別のフィルターを追加できます。結果が表示されたら、クエリに関連付けられた情報の列を昇順または降順で並べ替えることができます。

注: アセットを取得する新しいデータ コレクターが追加されたり、注釈やアプリケーションの割り当てが行われたりした場合は、クエリがインデックス化された後でのみ、それらの新しいアセット、注釈、またはアプリケーションをクエリできます。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、または注釈ルールの実行などの特定のイベント中に実行されます。

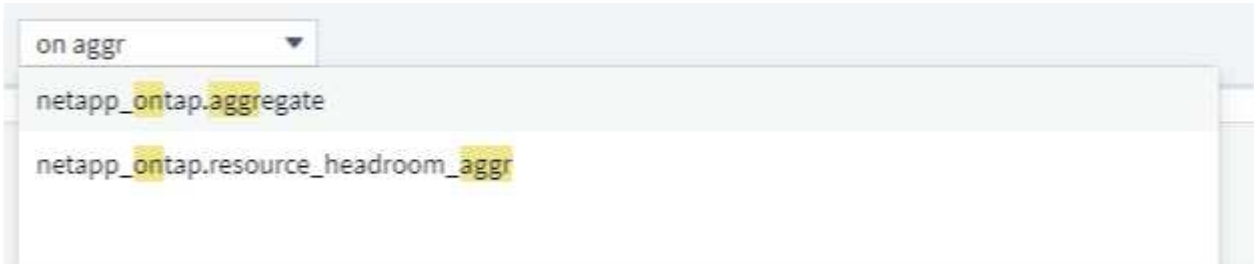
クエリの作成は非常に簡単です。

1. クエリ **> *+**新しいクエリ に移動します。
2. 「選択…」リストから、クエリを実行するオブジェクト タイプを選択します。リストをスクロールするか、入力を開始して検索対象をより速く見つけることができます。

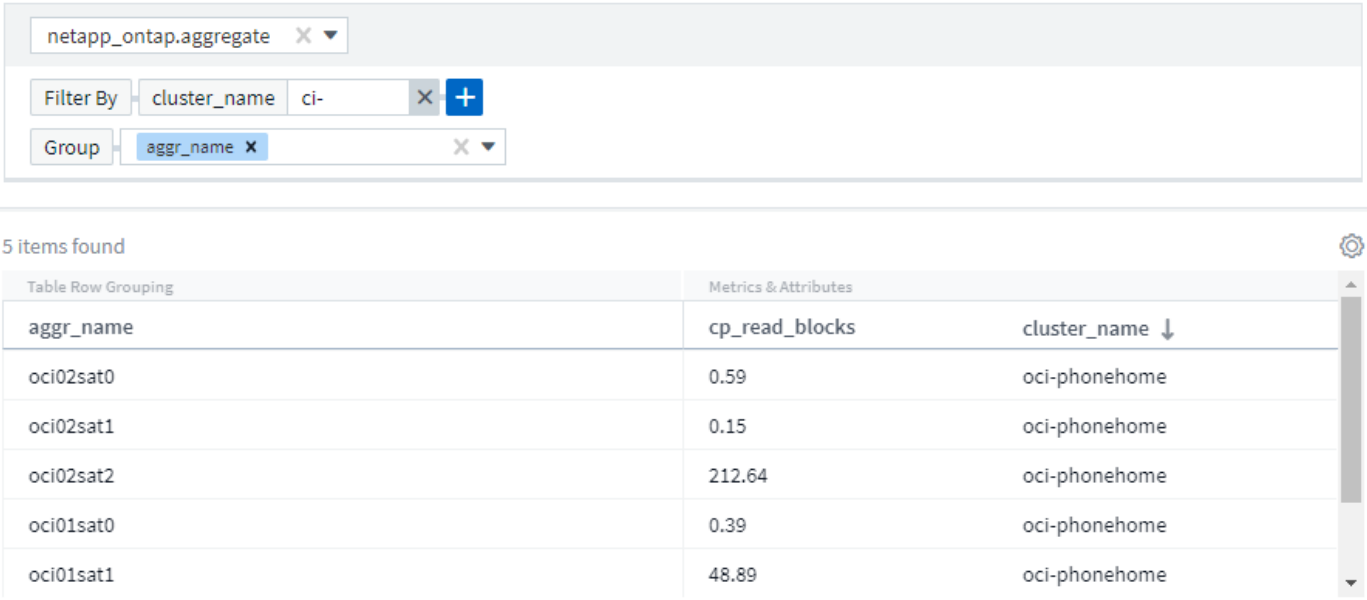
スクロールリスト:



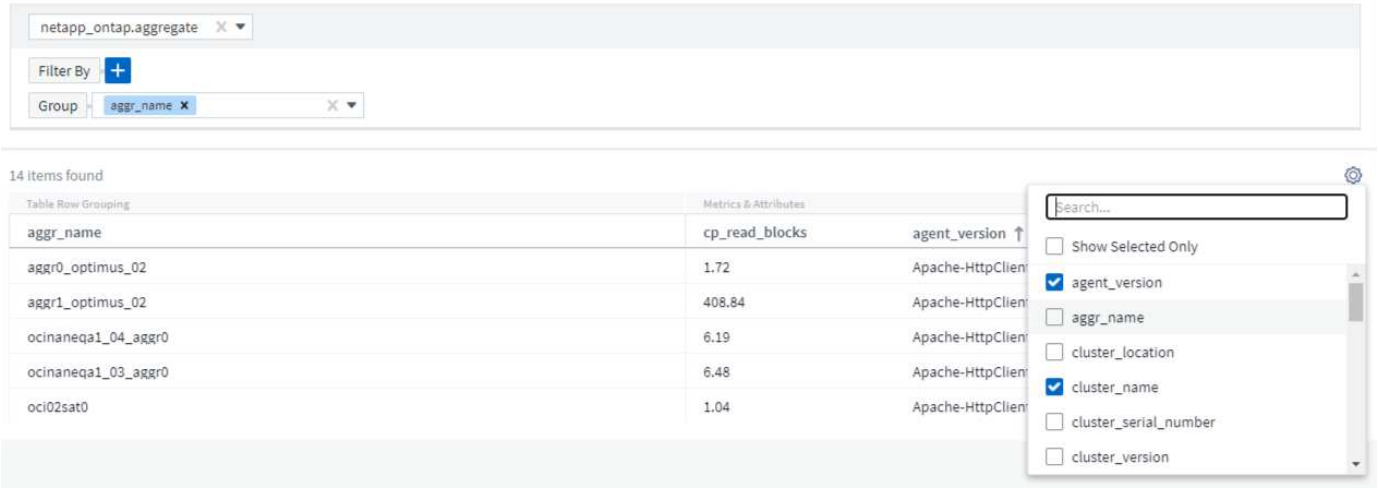
入力して検索:



[フィルター条件] フィールドの + ボタンをクリックすると、フィルターを追加してクエリをさらに絞り込むことができます。オブジェクトまたは属性ごとに行をグループ化します。統合データ (Kubernetes、 ONTAP高度なメトリックなど) を操作する場合、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、検索したオブジェクトの種類に応じて、いくつかのデフォルトの列が表示されます。列を追加、削除、または変更するには、表の右側にある歯車アイコンをクリックします。利用可能な列は、アセット/メトリックの種類によって異なります。



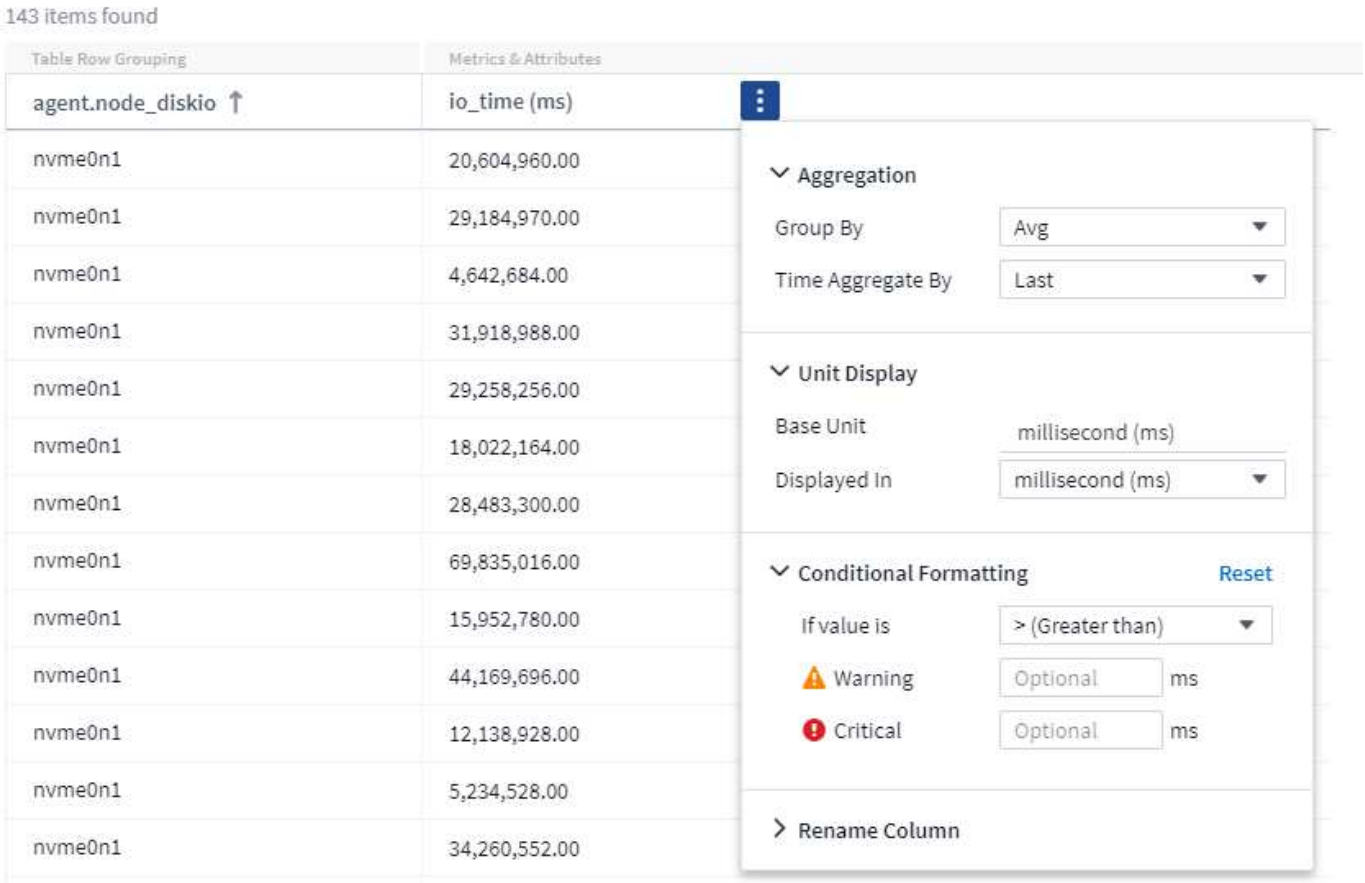
実際に動作を見てみましょう

"Data Infrastructure Insightsのクエリを使用して探索および分析する (ビデオ)"

集計、単位、条件付き書式の選択

集計と単位

「値」列の場合、表示される値の集計方法と値の表示単位を選択することにより、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、列の上隅にある「3 つのドット」メニューを選択すると見つかります。



単位

値を表示する単位を選択できます。たとえば、選択した列に生の容量が表示され、値が GiB で表示されているが、TiB で表示したい場合は、[単位表示] ドロップダウンから TiB を選択するだけです。

集約

同様に、表示される値が基になるデータから「平均」として集計されているが、すべての値の合計を表示する場合は、[グループ化基準] ドロップダウン (グループ化された値の合計を表示する場合) または [時間集計基準] ドロップダウン (行の値に基になるデータの合計を表示する場合) から「合計」を選択します。

グループ化されたデータ ポイントを 平均、最大、最小、または合計 で集計することを選択できます。

個々の行データは、平均、最後に取得したデータ ポイント、最大値、最小値、または合計 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大レベルのしきい値を強調表示できるため、外れ値や例外的なデータ ポイントを即座に確認できます。



条件付き書式は列ごとに個別に設定します。たとえば、容量列に 1 セットのしきい値を選択し、スループット列に別のセットのしきい値を選択できます。

列の名前を変更

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、結果のファイルに新しい列名も表示されます。

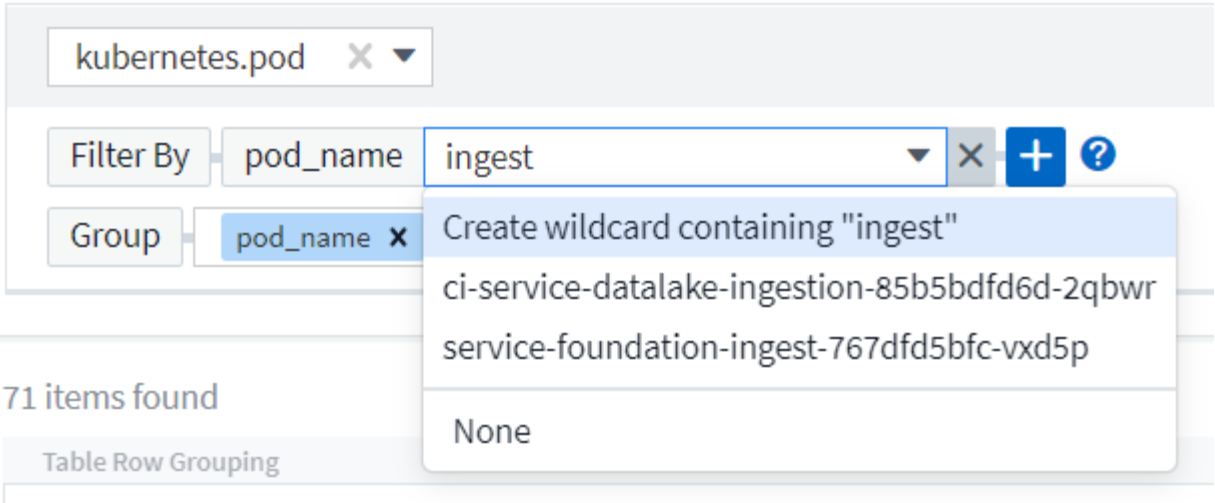
保存

必要な結果を表示す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、将来使用するためにクエリを保存できます。意味のある一意の名前を付けます。

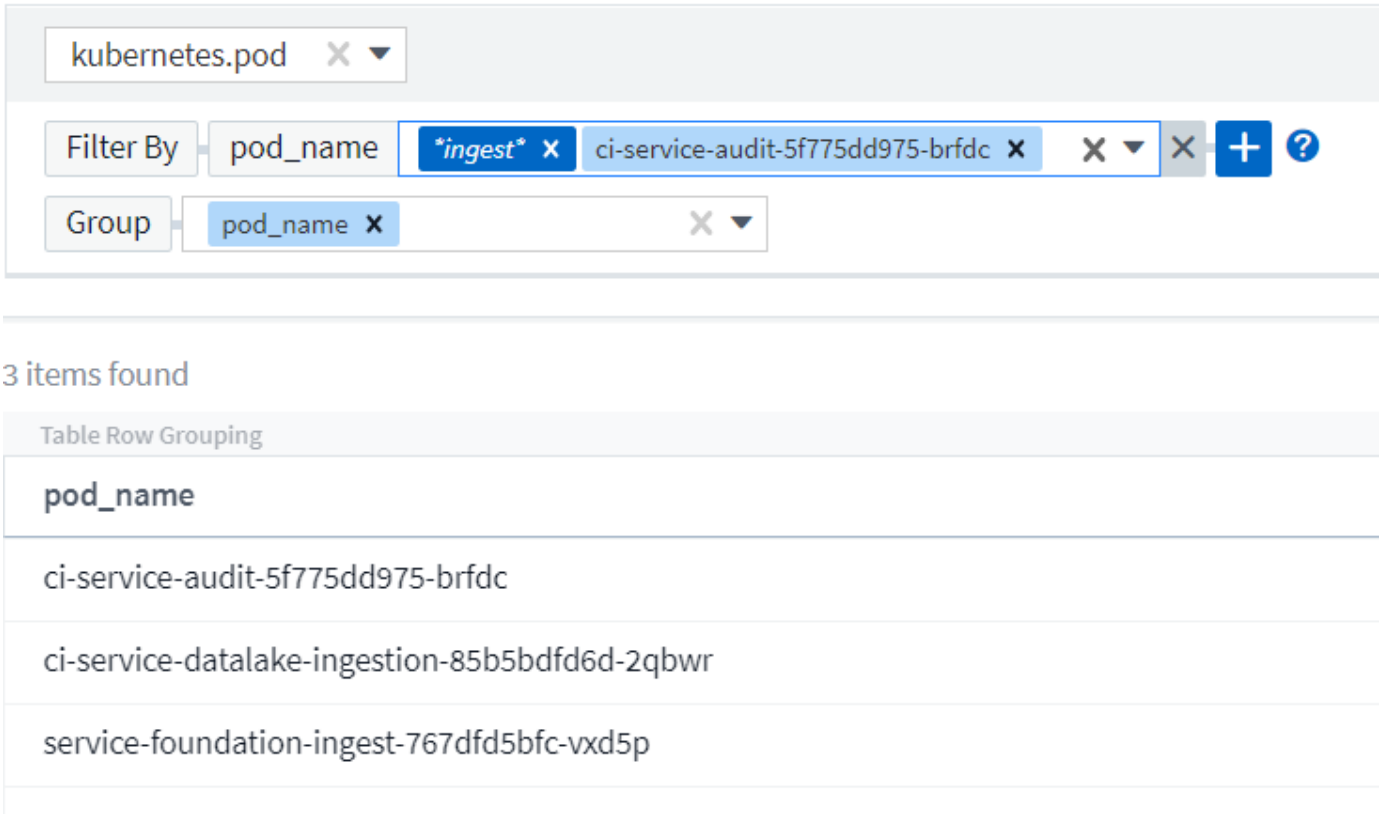
フィルタリングの詳細

ワイルドカードと式

クエリまたはダッシュボード ウィジェットでテキストまたはリストの値をフィルター処理する場合、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 フィルター 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 OR を使用して 式 を作成したり、「なし」オプションを選択してフィールド内の null 値をフィルター処理したりすることもできます。



ワイルドカードまたは式 (例: NOT、OR、「なし」など) に基づくフィルターは、フィルター フィールドに濃い青色で表示されます。リストから直接選択した項目は水色で表示されます。



ワイルドカードと式の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、ブール値では機能しないことに注意してください。

フィルターの調整

フィルターを絞り込むには、次のものを使用できます。

フィルタ	何をするのか	例	結果

*（アスタリスク）	あらゆるものを検索できます	ヴォル*レル	「vol」で始まり「rhel」で終わるすべてのリソースを返します。
？（疑問符）	特定の文字数を検索できます	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る	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
ない	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」で始まらない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	対象フィールドが空の場合の結果を返します
ない *	テキストのみのフィールドでNULL値を検索します	ない *	対象フィールドが空の場合の結果を返します

フィルタ文字列を二重引用符で囲むと、Insight は最初の引用符と最後の引用符の間のすべてを完全一致として扱います。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、「*」でフィルタリングすると、文字通りのアスタリスクである結果が返されます。この場合、アスタリスクはワイルドカードとして扱われません。演算子 OR と NOT も、二重引用符で囲むとリテラル文字列として扱われます。

ブール値のフィルタリング

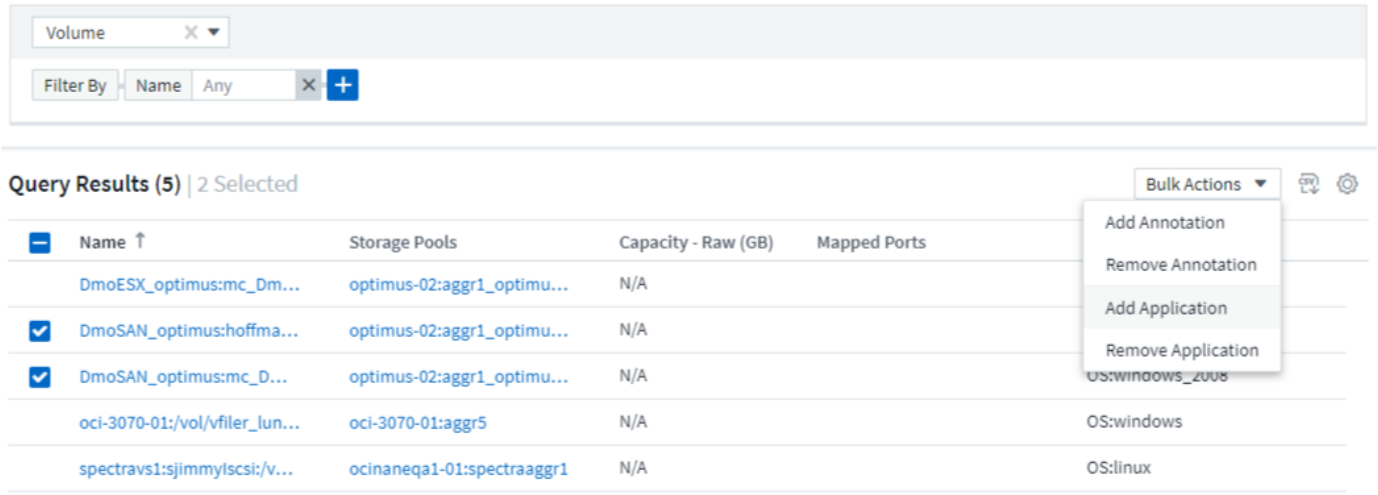
ブール値をフィルタリングする場合、フィルタリングする次の選択肢が表示されることがあります。

- 任意: 「はい」、「いいえ」に設定された結果、またはまったく設定されていない結果を含む、すべての結果が返されます。
- はい: 「はい」の結果のみを返します。DII では、ほとんどの表で「はい」にチェックマークが表示されることに注意してください。値は「True」、「On」などに設定できます。DII はこれらすべてを「Yes」として扱います。
- いいえ: 「いいえ」の結果のみを返します。DII では、ほとんどの表で「いいえ」が「X」として表示されることに注意してください。値は「False」、「Off」などに設定できますが、DII はこれらすべてを「No」として扱います。
- なし: 値がまったく設定されていない結果のみを返します。「Null」値とも呼ばれます。

クエリ結果が得られたので、次に何をすればよいですか**?**

クエリを実行すると、簡単に注釈を追加したり、アセットにアプリケーションを割り当てたりできるようになります。アプリケーションまたは注釈は、インベントリ資産 (ディスク、ストレージなど) にのみ割り当てることができることに注意してください。統合メトリックは、注釈やアプリケーションの割り当てを行うことはできません。

クエリの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*ボタンをクリックするだけです。選択したアセットに適用する目的のアクションを選択します。



注釈ルールにはクエリが必要

設定する場合"アノテーション ルール"各ルールには、操作対象となる基礎クエリが必要です。しかし、上で見たように、クエリは必要に応じて広くしたり狭くしたりすることができます。

クエリの表示

クエリを表示して資産を監視したり、クエリで資産に関連するデータを表示する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。次のいずれかの方法で、クエリの表示方法を変更できます。
3. フィルター ボックスにテキストを入力して検索し、特定のクエリを表示できます。
4. 列ヘッダーの矢印をクリックすると、クエリ テーブル内の列の並べ替え順序を昇順 (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、青いバーが表示されるまで列ヘッダーの上にマウスを置きます。マウスをバーの上に置き、右または左にドラッグします。
6. 列を移動するには、列ヘッダーをクリックして右または左にドラッグします。

クエリ結果をスクロールする場合、 Data Infrastructure Insights がデータ コレクターを自動的にポーリングするため、結果が変わる可能性があることに注意してください。その結果、一部の項目が欠落したり、並べ替え方法によっては一部の項目が順序どおりに表示されなくなったりする可能性があります。

クエリ結果を .CSV ファイルにエクスポートする

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することができます。

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。

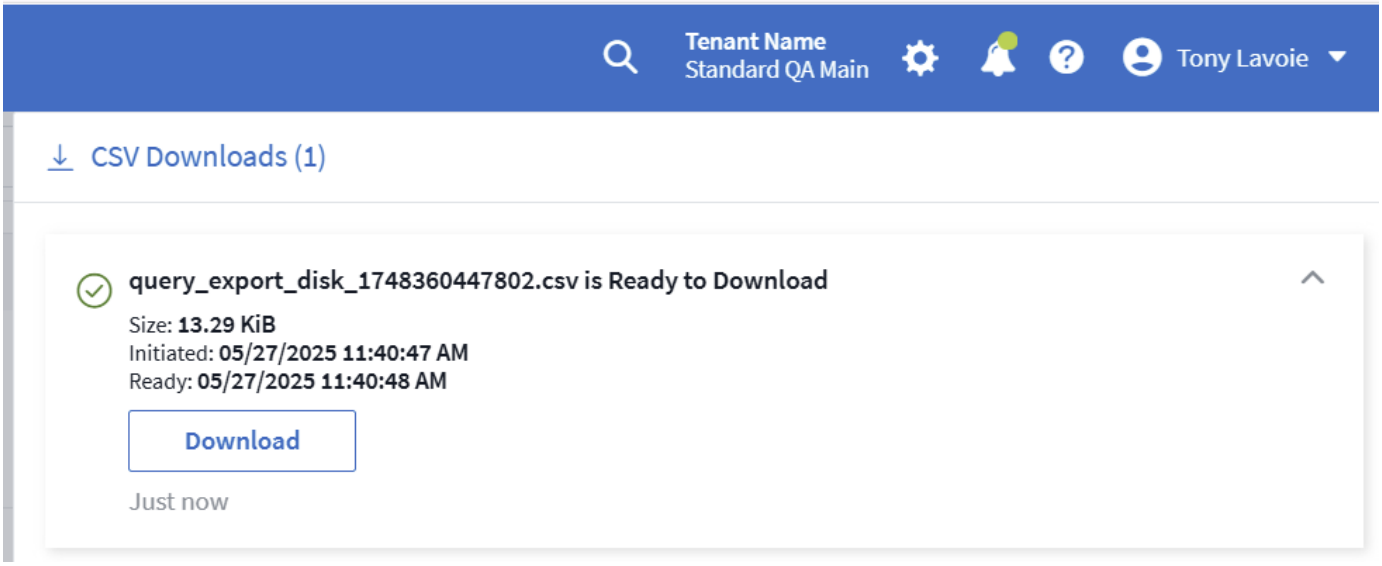
3. クエリをクリックします。
4. クリック クエリ結果を .CSV ファイルにエクスポートします。

> .CSV へのエクスポートは、ダッシュボード テーブル ウィジェットおよびほとんどのランディング ページ テーブルの「3 つのドット」メニューでも利用できます。

非同期エクスポート

CSV へのデータのエクスポートには、エクスポートするデータの量に応じて、数秒から数時間かかる場合があります。 **Data Infrastructure Insights** はデータを非同期的にエクスポートするため、**.CSV** がコンパイルされている間も作業を続行できます。

右上のツールバーの「ベル」アイコンを選択して、.CSV エクスポートを表示およびダウンロードします。



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リング、列、列名が反映されます。

資産名内のカンマ

注: アセット名にコンマが含まれている場合、エクスポートでは名前が引用符で囲まれ、アセット名と適切な .csv 形式が保持されます。

時刻形式か、時刻形式ではないか**?**

エクスポートされた .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 (2 桁の数字の後にコロン、さらに 2 桁の数字が続く) 形式である場合、Excel ではその名前がテキスト形式ではなく時刻形式として解釈されることがあります。その結果、Excel でそれらの列に誤った値が表示される可能性があります。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。

この問題を回避するには、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. 必要な .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」を選択し、「次へ」をクリックします。
5. 区切り文字として「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、列のデータ形式として「テキスト」を選択します。
7. [Finish]をクリックします。

   オブジェクトは適切な形式で Excel に表示されるはずです。

クエリの変更または削除

クエリするアセットの検索条件を変更する場合は、クエリに関連付けられている条件を変更できます。

クエリの変更

手順

1. *探索*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
3. クエリに条件を追加するには、列アイコンをクリックし、リストからメトリック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。

- **[**保存**]** ボタンをクリックして、最初に使用した名前でクエリを保存します。
- *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。これによって元のクエリが上書きされることはありません。
- *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、クエリを最後に保存した変更に戻します。

クエリの削除

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、次のいずれかを実行します。

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。

資産に複数のアプリケーションを割り当てたり、資産から複数のアプリケーションを削除したりする

複数割り当て可能"アプリケーション"手動で複数のアプリケーションを割り当てたり削除したりする代わりに、クエリを使用して複数のアプリケーションを資産に追加したり削除したりできます。

以下の手順で追加または削除できます"アノテーション"同じように。

開始する前に

編集するすべてのアセットを検索するクエリをすでに作成しておく必要があります。

手順

1. *探索*をクリックし、*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. アセットを検索するクエリの名前をクリックします。

   クエリに関連付けられたアセットのリストが表示されます。

3. リストで必要なアセットを選択するか、上部のチェックボックスをクリックして「すべて」を選択します。

   一括アクションのドロップダウンが表示されます。

4. 選択したアセットにアプリケーションを追加するには、「一括操作」をクリックし、「アプリケーションの追加」を選択します。
5. 1 つ以上のアプリケーションを選択します。

   ホスト、内部ボリューム、qtree、仮想マシンに対しては複数のアプリケーションを選択できますが、ボリュームまたは共有に対しては 1 つのアプリケーションしか選択できません。

6. *保存*をクリックします。
7. 資産に割り当てられたアプリケーションを削除するには、「一括操作」をクリックし、「アプリケーションの削除」を選択します。
8. 削除するアプリケーションを選択します。
9. *削除*をクリックします。

割り当てた新しいアプリケーションは、別のアセットから派生したアセット上のアプリケーションを上書きします。たとえば、ボリュームはホストからアプリケーションを継承し、新しいアプリケーションがボリュームに割り当てられると、新しいアプリケーションは派生アプリケーションよりも優先されます。

一括追加アクションで [保存] をクリックするか、一括削除アクションで [削除] をクリックすると、 Data Infrastructure Insights、アクションに時間がかかることが通知されます。このメッセージは閉じても構いません。アクションはバックグラウンドで続行されます。

関連する資産が大量にある環境では、それらの資産へのアプリケーション割り当ての継承に数分かかることがあります。関連する資産が多数ある場合は、継承が発生するまでにさらに時間がかかります。

テーブルの値のコピー

検索ボックスや他のアプリケーションで使用するために、テーブル内の値をクリップボードにコピーできます。

タスク概要

テーブルまたはクエリ結果の値をクリップボードにコピーするには、2 つの方法があります。

手順

1. 方法 1: マウスで目的のテキストを強調表示し、コピーして、検索フィールドまたは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、フィールドにマウスを移動し、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。

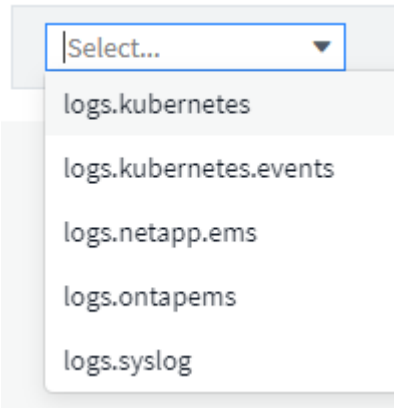
   このメソッドを使用してコピーできるのは、アセットへのリンクである値のみであることに注意してください。単一の値 (リスト以外) を含むフィールドにのみコピー アイコンが表示されます。

ログエクスプローラー

Data Infrastructure Insightsログ エクスプローラーは、システム ログを照会するための強力なツールです。調査に役立つだけでなく、モニターにログ クエリを保存して、特定のログ トリガーがアクティブ化されたときにアラートを提供することもできます。

ログの調査を開始するには、[ログ クエリ] **>** **[+**新しいログ クエリ**]** をクリックします。

リストから利用可能なログを選択します。

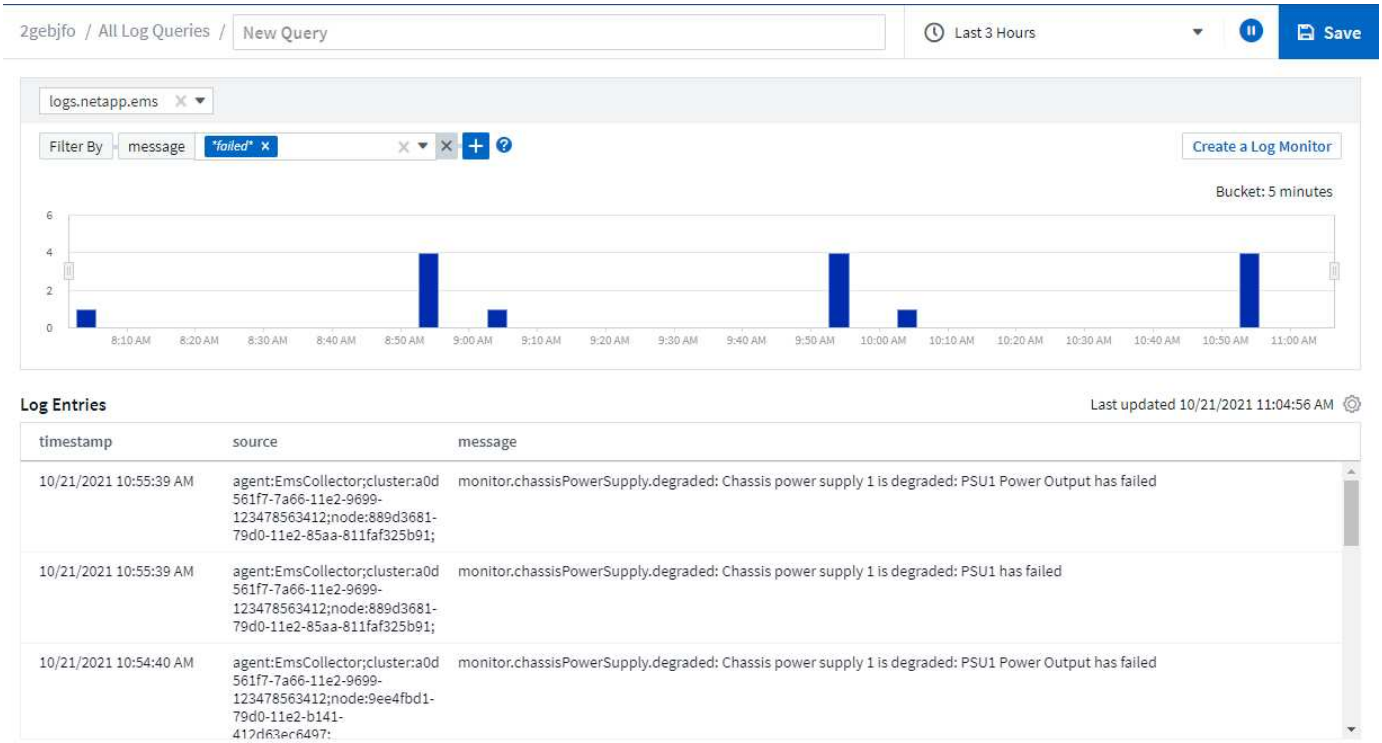


クエリに使用できるログの種類は、環境によって異なる場合があります。今後、ログ タイプが追加される可能性もあります。

フィルターを設定して、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、失敗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* のフィルターを設定します。

フィルター フィールドに目的のテキストを入力し始めると、入力した文字列を含むワイルドカード検索を作成するようにData Infrastructure Insightsから要求されます。

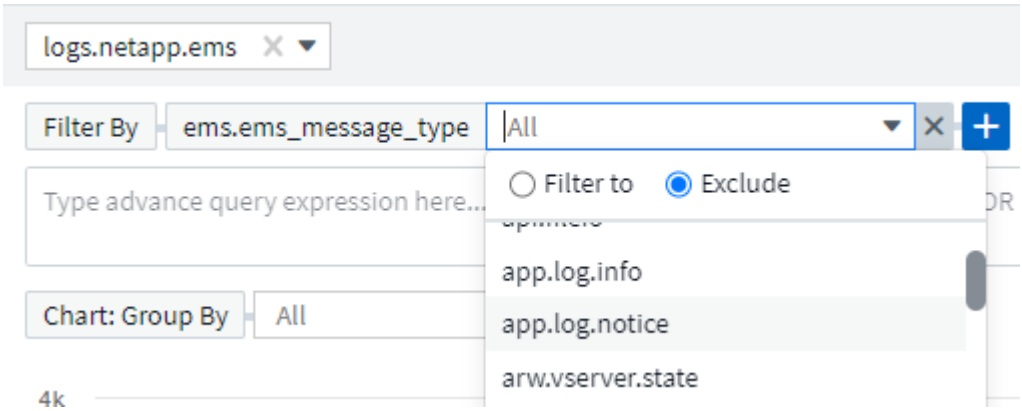
結果はグラフで表示され、表示される各期間のログのインスタンスの数が表示されます。グラフの下にはログエントリ自体が表示されます。グラフとエントリは、選択した時間範囲に基づいて自動的に更新されます。



フィルタ

含める/除外する

ログをフィルタリングするときに、入力した文字列を 含める (つまり、「フィルタリング対象」) か 除外するかを選択できます。除外された文字列は、完了したフィルターに「NOT <文字列>」と表示されます。



ワイルドカードまたは式 (例: NOT、OR、「なし」など) に基づくフィルターは、フィルター フィールドに濃い青色で表示されます。リストから直接選択した項目は水色で表示されます。

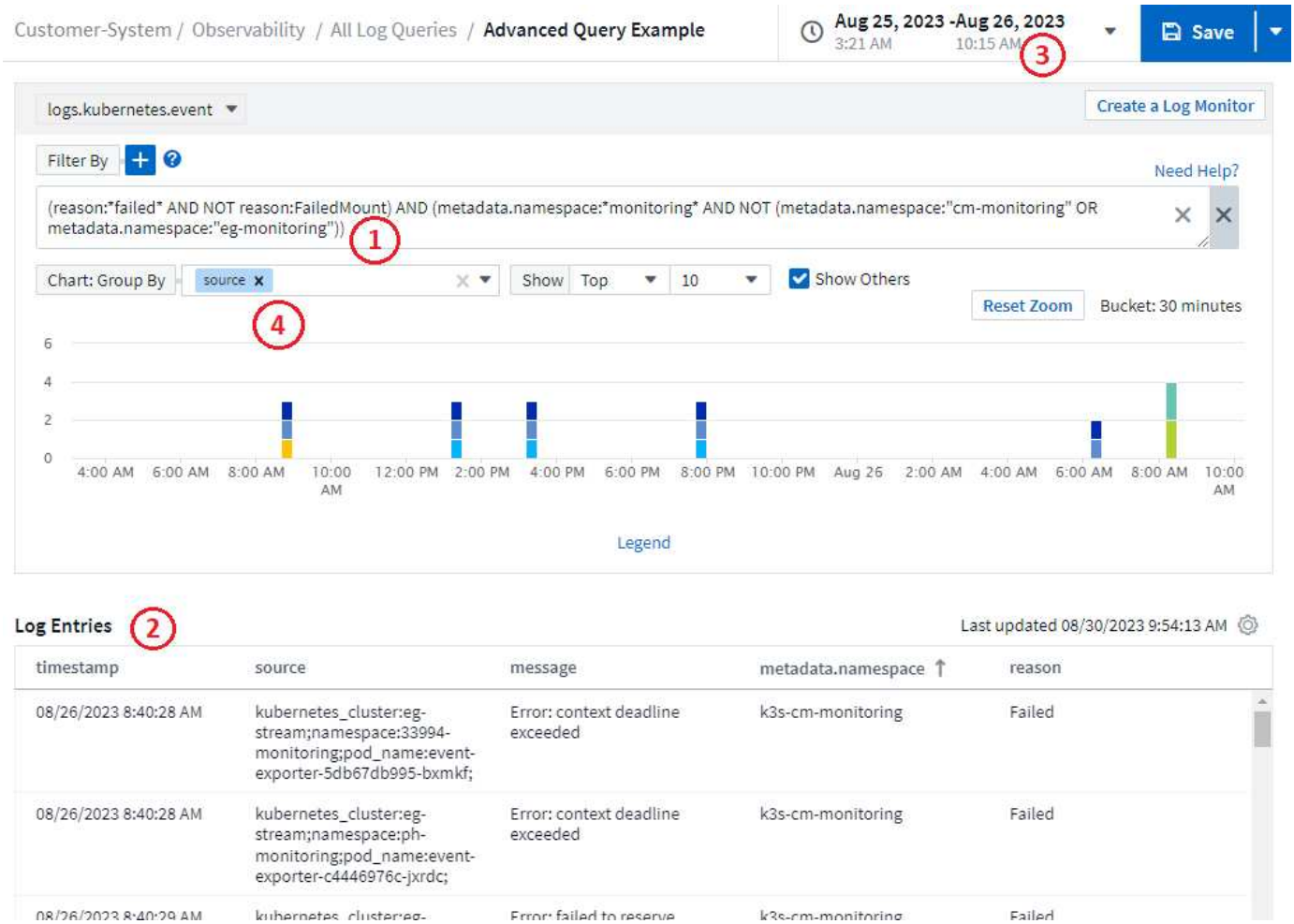
いつでも、[ログ モニターの作成] をクリックして、現在のフィルターに基づいて新しいモニターを作成できます。

高度なフィルタリング

クエリまたはダッシュボード ウィジェットでテキストまたはリストの値をフィルター処理する場合、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 フィルター 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したり、「なし」オプションを選択して null 値をフィルターしたりすることもできます。

フィルタリングを構築するときは、必ず早めに頻繁にクエリを保存してください。高度なクエリは「自由形式」の文字列入力であり、ビルド時に解析エラーが発生する可能性があります。

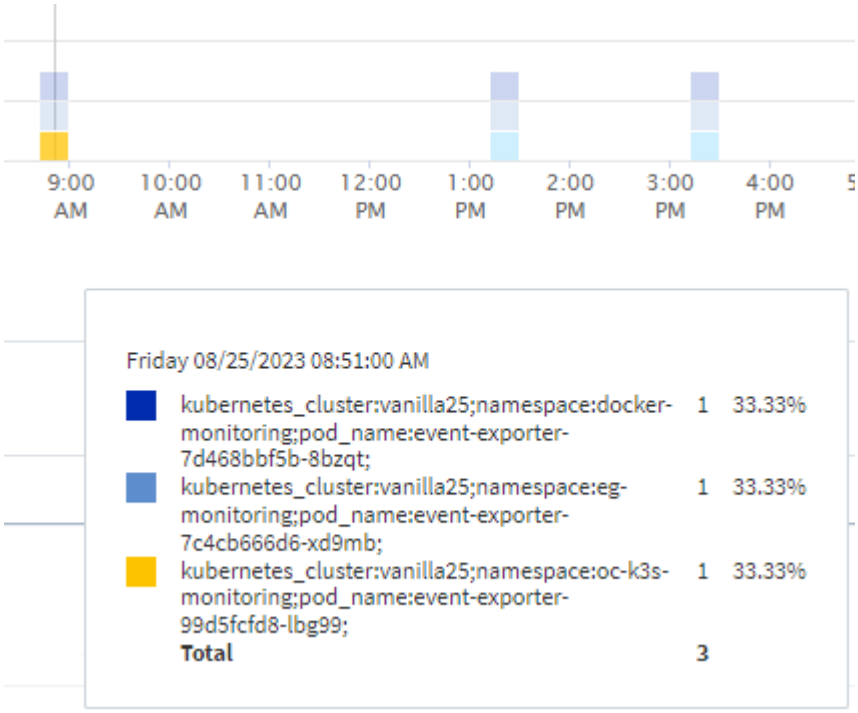
logs.kubernetes.event ログの高度なクエリのフィルタリングされた結果を示すこの画面イメージをご覧ください。このページでは多くのことが行われており、画像の下に説明があります。



1. この高度なクエリ文字列は、次のものをフィルターします。
   - 「failed」という単語を含む *reason* を持つログ エントリをフィルターしますが、「FailedMount」という具体的な理由を持つものはフィルターしません。
   - 「monitoring」という単語を含む *metadata.namespace* も含むエントリをすべて含めますが、「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。ダッシュや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。疑問がある場合は、文字列を引用符で囲んでみてください。

2. 現在のフィルターの結果（「フィルター条件」値と高度なクエリ フィルターを含む）が結果リストに表示されます。リストは表示されている列ごとに並べ替えることができます。追加の列を表示するには、「歯車」アイコンを選択します。
3. グラフは拡大され、特定の期間内に発生したログ結果のみが表示されます。ここで表示される時間範囲は、現在のズーム レベルを反映しています。 ズームのリセット ボタンを選択すると、ズーム レベルが現在のData Infrastructure Insights の時間範囲に戻ります。
4. グラフの結果は、*source* フィールドごとに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。グラフ内の列にマウスを移動すると、特定のエントリに関する詳細が表示されます。



フィルターの調整

フィルターを絞り込むには、次のものを使用できます。

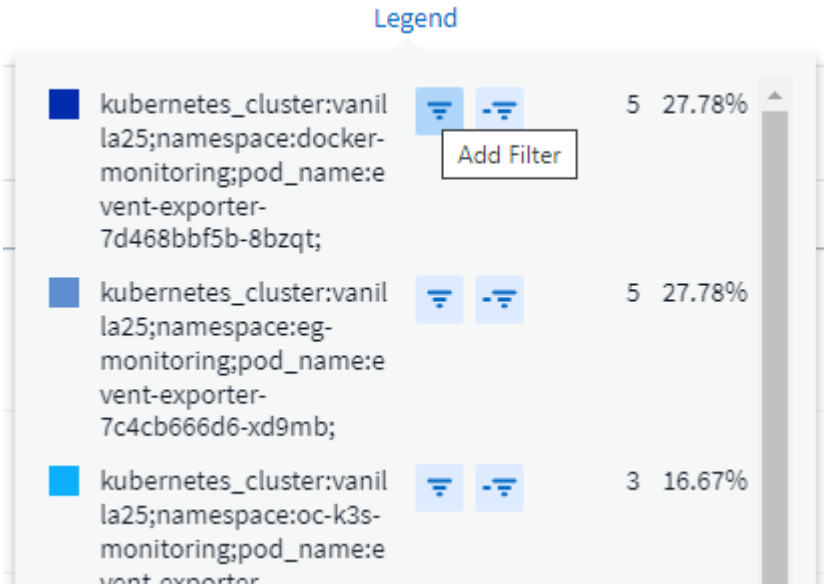
フィルタ	何をするのか
*（アスタリスク）	あらゆるものを検索できます
? （疑問符）	特定の文字数を検索できます
または	複数のエンティティを指定できる
ない	検索結果からテキストを除外できます
なし	すべてのフィールドでNULL値を検索します
ない *	テキストのみのフィールドでNULL値を検索します

フィルタ文字列を二重引用符で囲むと、Insight は最初の引用符と最後の引用符の間のすべてを完全一致として扱います。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、「*」でフィルタリングすると、文字通りのアスタリスクである結果が返されます。この場合、アスタリスクはワイルドカードとして扱われません。演算子 OR と NOT も、二重引用符で囲むとリテラル文字列として扱われます。

シンプルなフィルターと高度なクエリ フィルターを組み合わせることができます。結果のフィルターは 2 つのフィルターの「AND」になります。

チャートの凡例

グラフの下の「凡例」にもいくつか驚くべき点があります。凡例に表示される各結果 (現在のフィルターに基づく) に対して、その行の結果のみを表示する (フィルターの追加) か、その行に該当しない結果を表示する (除外フィルターの追加) かを選択できます。グラフとログ エントリ リストが更新され、選択内容に基づいて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、凡例を再度開き、[X] を選択して凡例ベースのフィルタをクリアします。

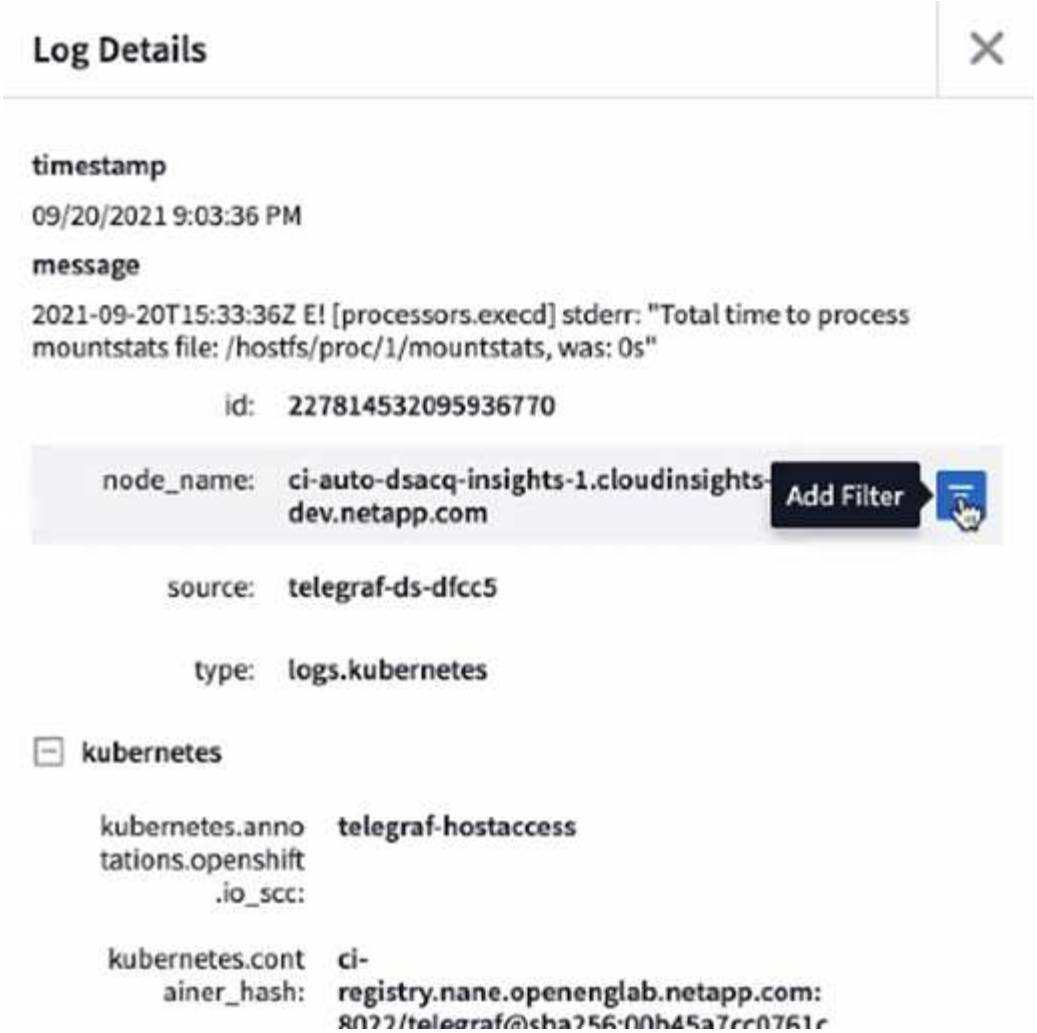


ログの詳細

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情報を調べることができます。

「フィルターを追加」をクリックすると、選択したフィールドが現在のフィルターに追加されます。ログ エントリ リストは新しいフィルターに基づいて更新されます。

一部のフィールドはフィルターとして追加できないことに注意してください。その場合、[フィルターの追加] アイコンは使用できません。



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に関する提案を紹介します。

問題：	これを試してみてください:
ログクエリに「デバッグ」メッセージが表示されない	デバッグ ログ メッセージは収集されません。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*、または *_notice* レベルに変更します。

非アクティブなデバイスの識別

保有している資産とそれを使用しているユーザーを特定することは、「適正規模化」と未使用のインフラストラクチャの解放に不可欠です。十分に活用されていないリソースを簡単に再割り当てまたは廃止し、不要な購入を避けることができます。

非アクティブな資産を識別するには、次の手順に従います。

手順

- **Observability > Explore → +New Metric Query** に移動します。

- ドロップダウンから_Storage_を選択します。
- 歯車をクリックして、*isActive* を列として追加します。

  チェックが表示されている行はアクティブです。 「X」は非アクティブなデバイスを示します。

非アクティブなデバイスを削除するには、削除するデバイスを選択し、[一括操作] ドロップダウンで [非アクティブなデバイスの削除] を選択します。

洞察

洞察

Insights を使用すると、リソースの使用状況やそれが他のリソースに与える影響、またはフル稼働までの時間の分析などを調べることができます。

多数の Insights が利用可能です。詳細を確認するには、ダッシュボード > インサイト に移動します。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 タブに表示され、非アクティブなインサイトは [非アクティブなインサイト] タブに表示されます。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が、現在は発生していないインサイトです。

インサイトの種類

ストレス下における共有リソース

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、共有リソースにストレスがかかります。 Data Infrastructure Insights は、リソースの飽和状態とテナントへの影響を調査するのに役立つツールを提供します。"詳細情報"

Kubernetes 名前空間のスペース不足

Kubernetes 名前空間のスペース不足インサイトでは、スペース不足になるリスクがある Kubernetes 名前空間のワークロードが表示され、各スペースがいっぱいになるまでの残り日数の見積もりも表示されます。"詳細情報"

ONTAPコールド ストレージの再利用

Reclaim ONTAP Cold Storage Insight は、 ONTAPシステム上のボリュームのコールド容量、潜在的なコスト/電力節約、推奨されるアクション項目に関するデータを提供します。"詳細情報"

これはプレビュー機能であり、改善が進むにつれて変更される可能性があります。"詳細情報" Data Infrastructure Insightsプレビュー機能について。

洞察：ストレス下における共有リソース

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、共有リソースにストレスがかかります。 Data Infrastructure Insights は、リソースの飽和状態とテナント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

ワークロードまたはリソース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現在影響を与えていると特定されているワークロードです。これらのワークロードは、たとえば IOPS を高め、影響を受けるワークロードの IOPS を低下させます。要求の厳しいワークロードは、_高消費ワークロード_と呼ばれることもあります。

影響を受けるワークロード とは、共有ストレージ プール内の消費量の多いワークロードの影響を受けるワークロードです。これらのワークロードでは、要求の厳しいワークロードが原因で、IOPS が低下したり、レイテンシが長くなったりしています。

Data Infrastructure Insights が主要なコンピューティング ワークロードを検出しなかった場合、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。これは、要求の厳しいワークロードと影響を受けるワークロードの両方に適用されます。

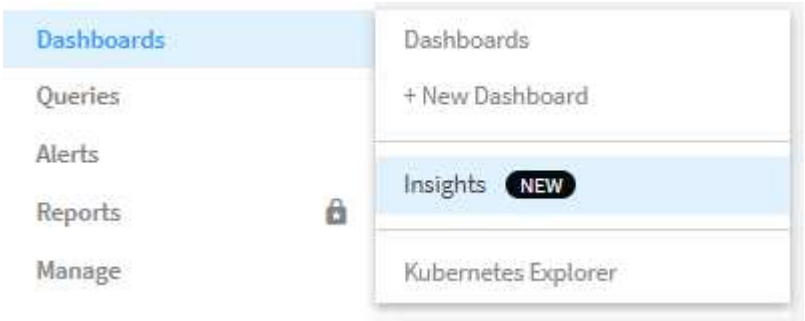
共有リソースの飽和度 は、影響を与える IOPS と ベースライン の比率です。

ベースライン は、検出された飽和の直前の 1 時間における各ワークロードの最大報告データ ポイントとして定義されます。

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を与えていると判断された場合、競合 または 飽和 が発生します。

要求の厳しいワークロード

共有リソース内の要求が厳しく、影響を受けているワークロードを調べるには、ダッシュボード > インサイト をクリックし、ストレスがかかっている共有リソース インサイトを選択します。

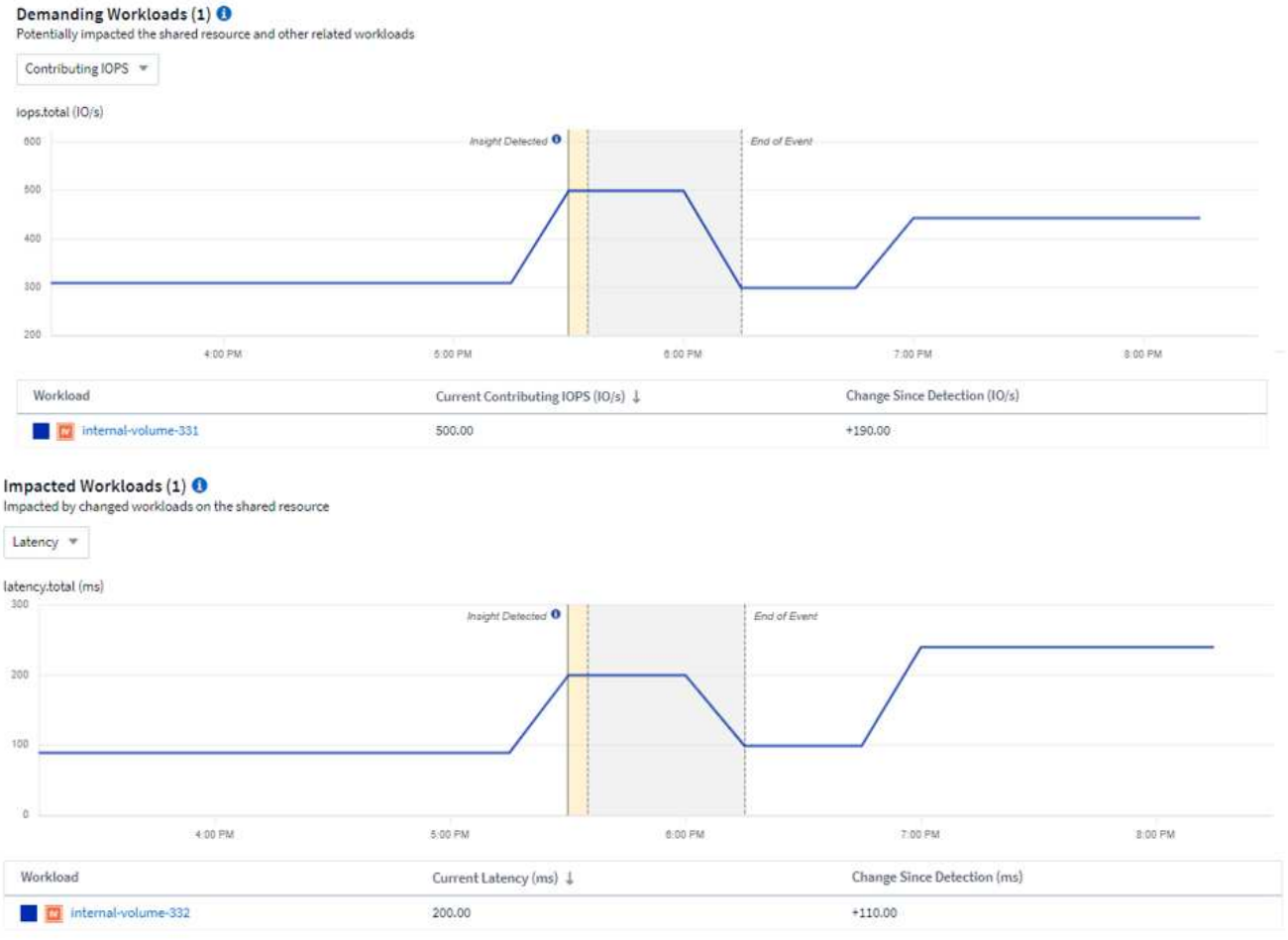


Data Infrastructure Insights には、飽和が検出されたワークロードのリストが表示されます。 Data Infrastructure Insightsでは、少なくとも 1 つの 要求の厳しいリソース または 影響を受けたリソース が検出されたワークロードが表示されることに注意してください。

ワークロードをクリックすると、その詳細ページが表示されます。上のグラフには、競合/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。



その下には、要求の厳しいワークロードと、それらの要求の厳しいワークロードによって影響を受けるワークロードを示す 2 つのグラフがあります。



各テーブルの下には、競合に影響を与えている、または競合の影響を受けるワークロードやリソースのリストがあります。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、関連するポッドを表示するクエリ ページが開きます。リンクによって空のクエリが開かれる場合は、影響を受けるポッドがアクティブな競合の一部ではなくなったことが原因である可能性があることに注意してください。クエリの時間範囲を変更して、より広い範囲またはより限定された範囲でポッド リストを表示できます。

飽和を解決するにはどうすればいいですか**?**

テナントの飽和の可能性を減らす、または排除するために実行できる手順はいくつかあります。これらは、ペ

ージ上の + 推奨事項を表示 リンクを展開すると表示されます。試すことができるいくつかの方法を以下に示します。

- 高IOPSの消費者を移動

  「貪欲な」ワークロードを、飽和度の低いストレージ プールに移動します。不要なコストや追加の競合を避けるために、ワークロードを移動する前にこれらのプールの層と容量を評価することをお勧めします。

- サービス品質（QoS）ポリシーを実装する

  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 プールの飽和状態が緩和されます。これは長期的な解決策です。

- 追加のリソースを追加する

  共有リソース (たとえば、ストレージ プール) が IOPS 飽和点に達した場合は、プールにディスクを追加したり、より高速なディスクを追加することで、飽和を緩和するのに十分な空きリソースを確保できます。

最後に、「インサイト リンクをコピー」をクリックしてページの URL をクリップボードにコピーし、同僚と簡単に共有できるようになります。

洞察：**Kubernetes** 名前空間のスペース不足

テナントのスペースが不足することは決して良い状況ではありません。 Data Infrastructure Insights は、 Kubernetes の永続ボリュームがいっぱいになるまでの時間を予測するのに役立ちます。

Kubernetes 名前空間のスペース不足 インサイトでは、スペース不足になるリスクがある Kubernetes 名前空間のワークロードを把握でき、各永続ボリュームがいっぱいになるまでの残り日数を推定できます。

このインサイトは、ダッシュボード > インサイト に移動すると表示できます。

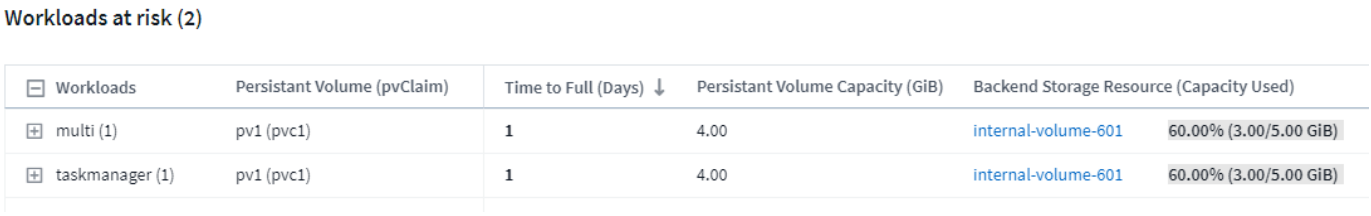
Kubernetes Namespaces Running Out of Space (3)

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。このページには、ワークロード容量の傾向を示すグラフと、次の内容を示す表が表示されます。

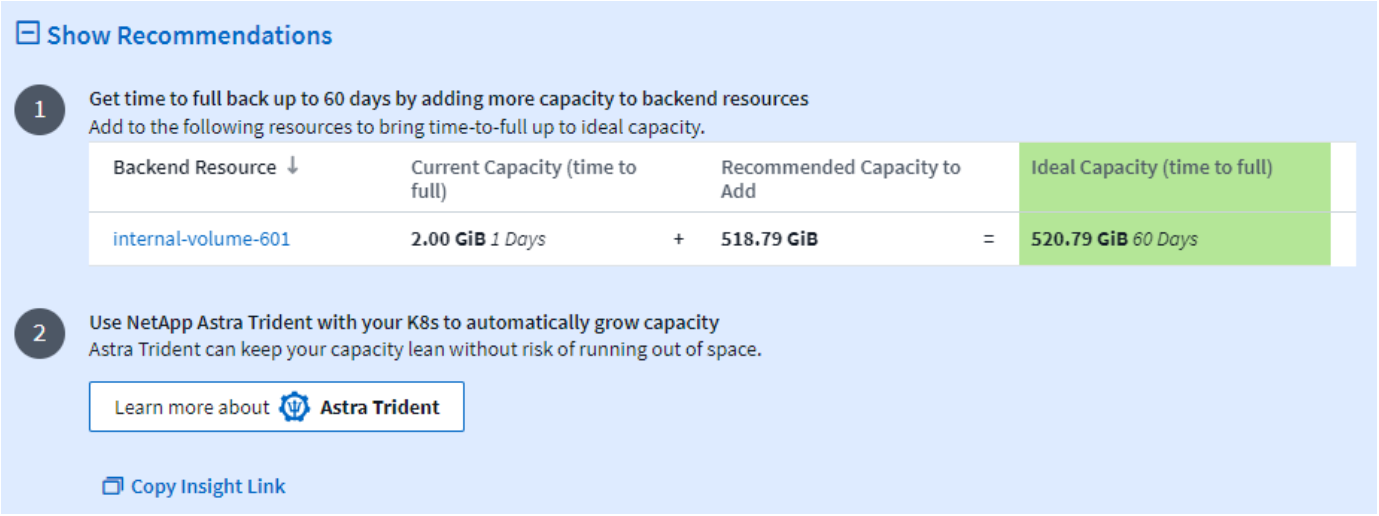
- ワークロード名
- 影響を受ける永続ボリューム
- 満杯になるまでの予測時間（日数）

- 永続ボリュームの容量
- バックエンド ストレージ リソースが影響を受けており、合計容量のうち現在の容量が使用されています。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 ページが開きます。



スペースが不足している場合はどうすればいいですか?

インサイト ページで、+ 推奨事項を表示 をクリックして、考えられる解決策を表示します。スペースが不足した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 Data Infrastructure Insights は、目標の 60 日間の予測まで容量がいっぱいになるまでの時間を延長するために追加する最適な容量を示します。その他の推奨事項も表示されます。



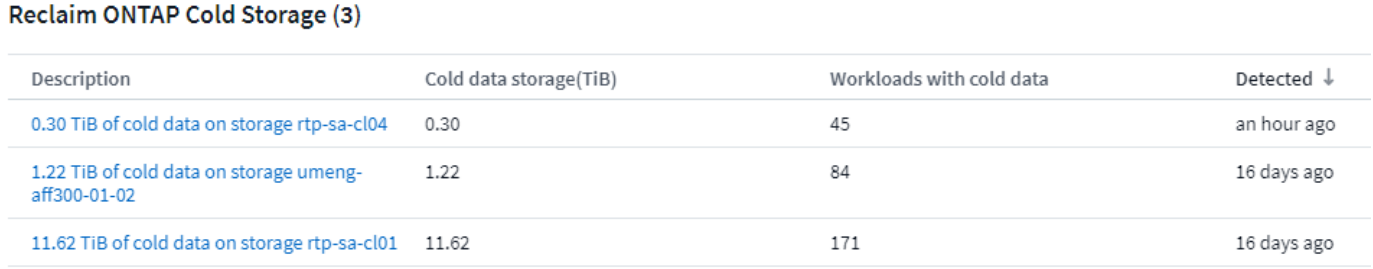
ここでは、このインサイトへの便利なリンクをコピーして、ページをブックマークしたり、チームと簡単に共有したりすることもできます。

洞察: ONTAPコールド ストレージの再利用

Reclaim ONTAP Cold Storage Insight は、 ONTAPシステム上のボリュームのコールド容量、潜在的なコスト/電力節約、推奨されるアクション項目に関するデータを提供します。

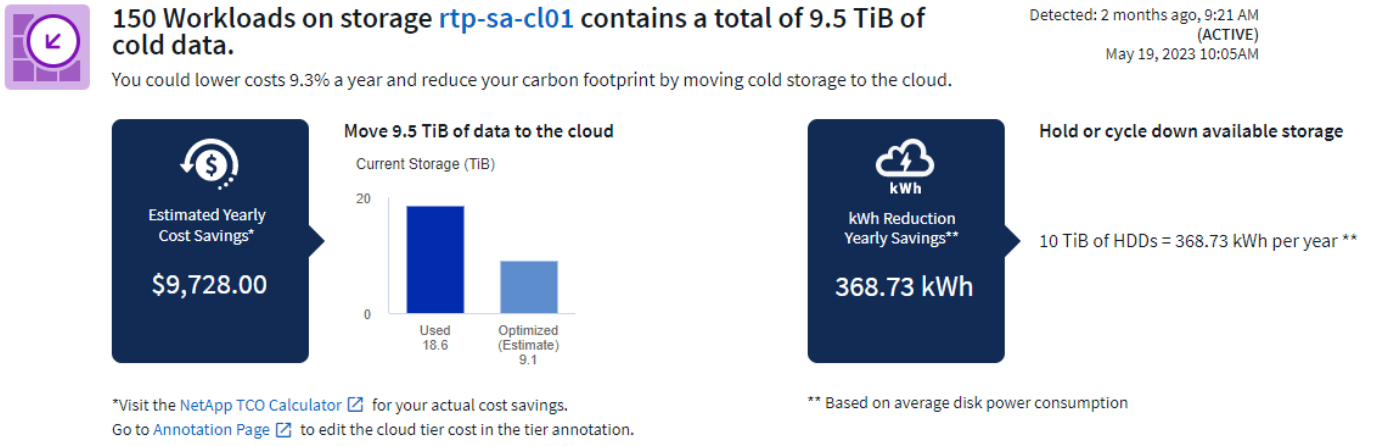
これらの Insights を表示するには、**Dashboards > Insights** に移動し、*Reclaim ONTAP Cold Storage* Insight を確認します。この Insight では、Data Infrastructure Insightsがコールド ストレージを検出した場合にのみ影響を受けるストレージがリストされ、それ以外の場合は「すべてクリア」メッセージが表示されます。

30 日未満のコールド データは表示されないことに注意してください。



Insight の説明には、「コールド」として検出されたデータの量と、そのデータが保存されているストレージが簡単に示されます。この表には、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。

リストからインサイトを選択すると、データをクラウドに移動する、または統合ディスクを停止する推奨事項や、それらの推奨事項を実装することで実現できる推定コストと電力節約などの詳細を示すページが開きます。このページには、"NetAppのTCO計算ツール"数字を試してみましょう。



推奨

[インサイト] 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層（HDD）に移動する

  ゾンビ フラグ、コールド ストレージ、日数を利用して、最もコールドで大量のデータを見つけ、ワークロードをより低コストのストレージ層 (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) に移動します。ワークロードは、30 日以上重要な IO 要求を受信していない場合、「ゾンビ」と見なされます。

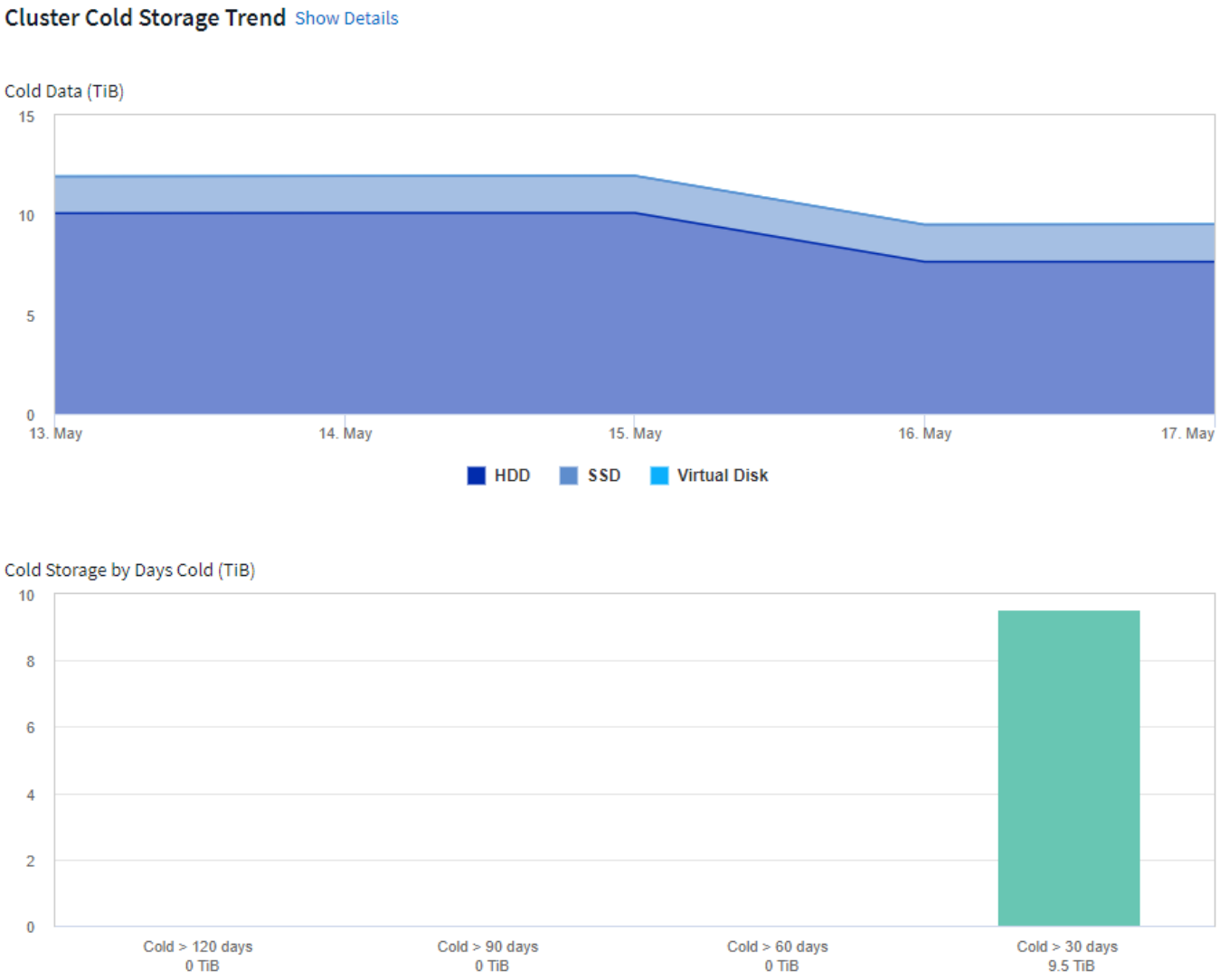
- 未使用のワークロードを削除する

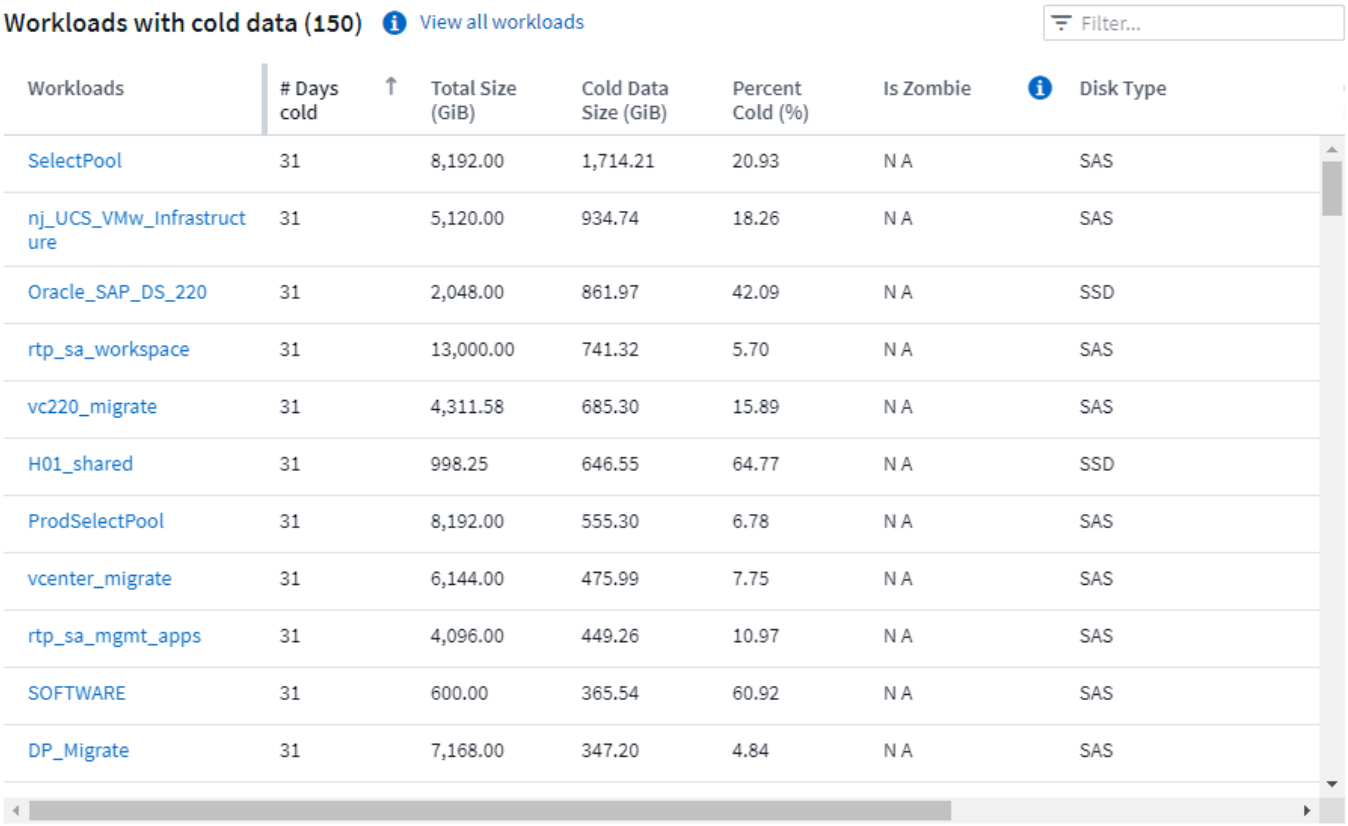
  使用されていないワークロードを確認し、それらをアーカイブするか、ストレージ システムから削除することを検討します。

- NetAppのファブリックプールソリューションを検討してください

  NetAppの"ファブリックプールソリューション"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、パフォーマンス層の効率性を高め、リモート データ保護を実現します。

グラフと表では追加の傾向情報が提供され、個々のワークロードを詳細に調べることもできます。





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

モニターとアラート

モニターによるアラート

インフラストラクチャ リソース全体のパフォーマンスしきい値、ログ イベント、および異常を追跡するようにモニターを構成します。ノードの書き込み遅延、ストレージ容量、アプリケーション パフォーマンスなどのメトリックのカスタム アラートを作成し、これらの条件が満たされたときに通知を受け取ります。

モニターを使用すると、ストレージ、VM、EC2、ポートなどの「インフラストラクチャ」オブジェクトによって生成されたメトリックや、Kubernetes、 ONTAP の高度なメトリック、Telegraf プラグインなどで収集された「統合」データのしきい値を設定できます。これらのメトリック モニターは、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警告を発します。

指定されたログ イベントが検出されたときに、警告、重大、または情報レベルのアラートをトリガーするモニターを作成することもできます。

Data Infrastructure Insightsは、"システム定義モニター"環境に応じても同様です。

セキュリティのベストプラクティス

Data Infrastructure Insightsアラートは、テナント上のデータ ポイントと傾向を強調するように設計されており、 Data Infrastructure Insightsでは、アラートの受信者として有効な電子メール アドレスを入力できます。安全な環境で作業している場合は、通知を受信するユーザーやアラートにアクセスできるユーザーについて特に注意してください。

メトリックまたはログモニター?

1. Data Infrastructure Insightsメニューから、*アラート>モニターの管理*をクリックします。

   現在構成されているモニターを示すモニター リスト ページが表示されます。

2. 既存のモニターを変更するには、リスト内のモニター名をクリックします。
3. モニターを追加するには、[+ モニター] をクリックします。



   新しいモニターを追加すると、メトリック モニターまたはログ モニターを作成するように求められます。

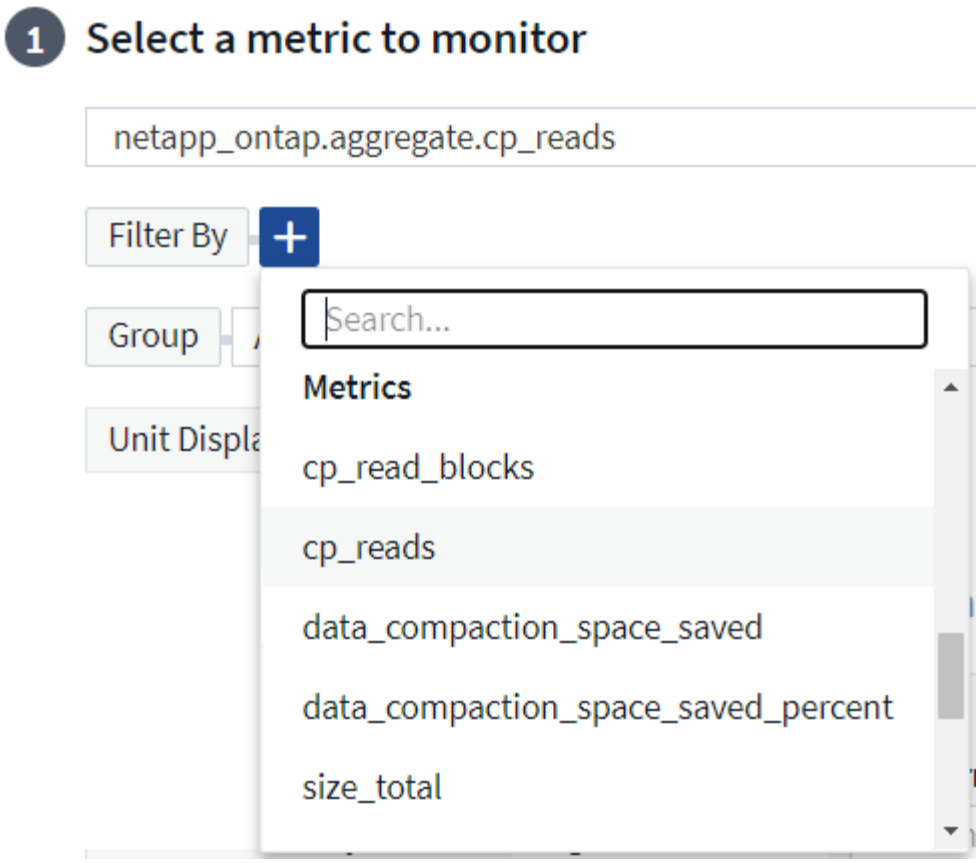
   - *Metric* はインフラストラクチャまたはパフォーマンス関連のトリガーに関するアラートを監視します
   - *Log* はログ関連のアクティビティに関するアラートを監視します

   モニターの種類を選択すると、モニター構成ダイアログが表示されます。作成するモニターの種類に応じて構成が異なります。

メトリックモニター

1. ドロップダウンで、監視するオブジェクト タイプとメトリックを検索して選択します。

フィルターを設定して、監視するオブジェクト属性またはメトリックを絞り込むことができます。

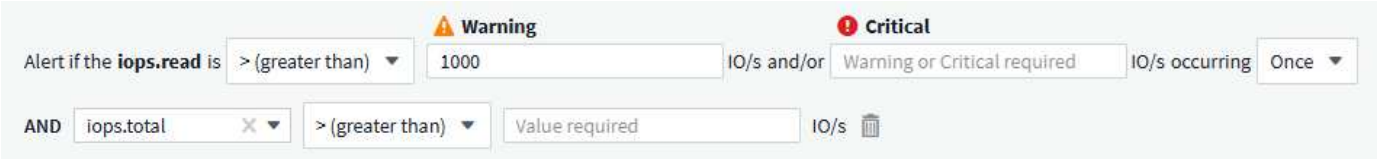


統合データ (Kubernetes、 ONTAP Advanced Data など) を操作する場合、メトリック フィルタリングによって、プロットされたデータ シリーズから個別のデータ ポイントや一致しないデータ ポイントが削除されます。これは、インフラストラクチャ データ (ストレージ、VM、ポートなど) の場合、フィルタがデータ シリーズの集計値に対して機能し、チャートからオブジェクト全体が削除される可能性があるのとは異なります。

メトリック モニターは、ストレージ、スイッチ、ホスト、VM などのインベントリ オブジェクト、およびONTAP Advanced や Kubernetes データなどの統合メトリックに適用されます。インベントリ オブジェクトを監視する場合、「グループ化」方法を選択できないことに注意してください。ただし、統合データを監視する場合はグループ化が許可されます。

マルチコンディションモニター

2 番目の条件を追加して、メトリック モニターをさらに絞り込むこともできます。「+ セカンダリメトリック条件の追加」プロンプトを展開し、追加の条件を構成するだけです。



両方の条件が満たされた場合、モニターは警告を発します。

2 番目の条件は「AND」のみで実行できることに注意してください。1 つの条件または他の条件に基づいてアラートを生成することはできません。

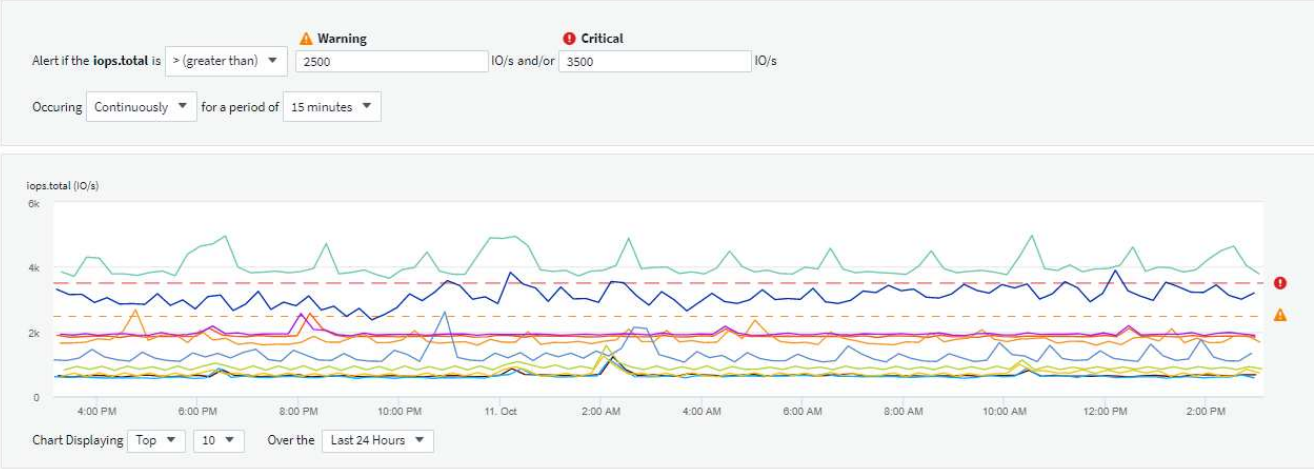
モニターの条件を定義します。

1. 監視するオブジェクトとメトリックを選択した後、警告レベルおよび/または重大レベルのしきい値を設定します。
2. 警告 レベルには、この例では 200 と入力します。この警告レベルを示す破線がサンプルグラフに表示されます。
3. *Critical* レベルには 400 と入力します。この重大レベルを示す破線がサンプルグラフに表示されます。

   グラフには履歴データが表示されます。グラフ上の警告レベルと重大レベルの線はモニターの視覚的な表現であるため、それぞれのケースでモニターがいつアラートをトリガーするかを簡単に確認できます。

4. 発生間隔には、[*15* 分] の期間で [連続] を選択します。

   しきい値を超えた瞬間に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超過するまで待つかを選択できます。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警告を受け取るのではなく、監視対象オブジェクトが少なくとも 15 分間、これらのレベルのいずれかを継続して超えた場合にのみ警告を受け取ります。



アラート解決動作を定義する

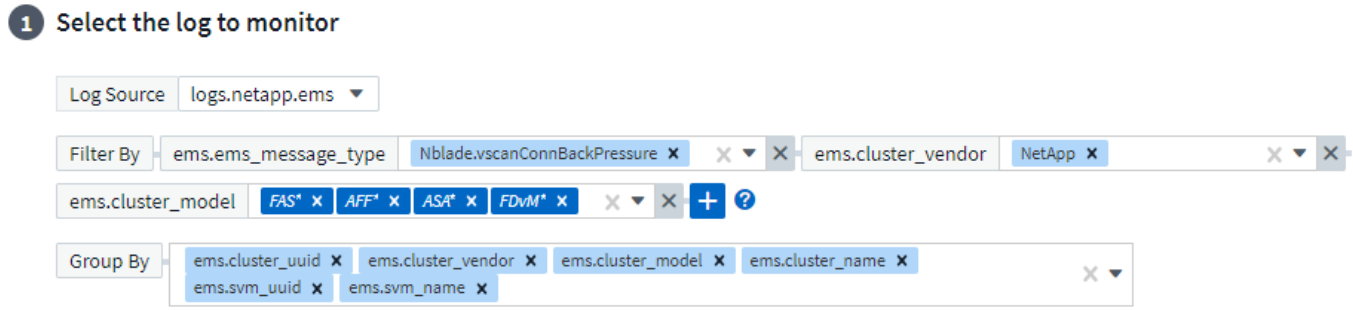
メトリック モニターのアラートを解決する方法を選択できます。次の 2 つの選択肢が表示されます。

- メトリックが許容範囲に戻ったら解決します。
- 指定された時間 (1 分から 7 日間) にわたってメトリックが許容範囲内にある場合に解決します。

ログモニター

*ログ モニター*を作成するときは、まず利用可能なログ リストから監視するログを選択します。上記のように、利用可能な属性に基づいてフィルタリングできます。 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 モニター フィルターは空にできません。



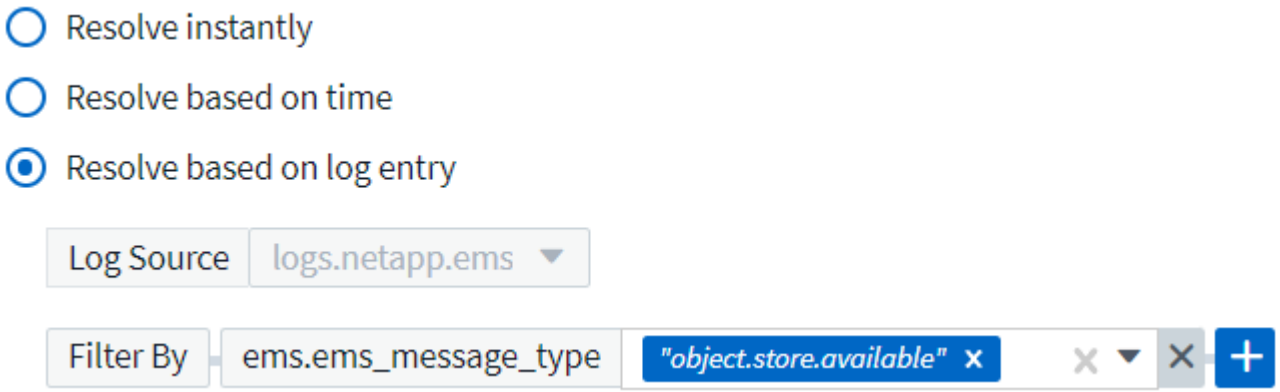
アラートの動作を定義する

上記で定義した条件が 1 回 (つまり即時) 発生したときに、重大度レベルが *Critical*、*Warning*、または *Informational* であるアラートを送信するモニターを作成するか、条件が 2 回以上発生するまでアラートを待機することができます。

アラート解決動作を定義する

ログ モニターのアラートを解決する方法を選択できます。次の 3 つの選択肢が表示されます。

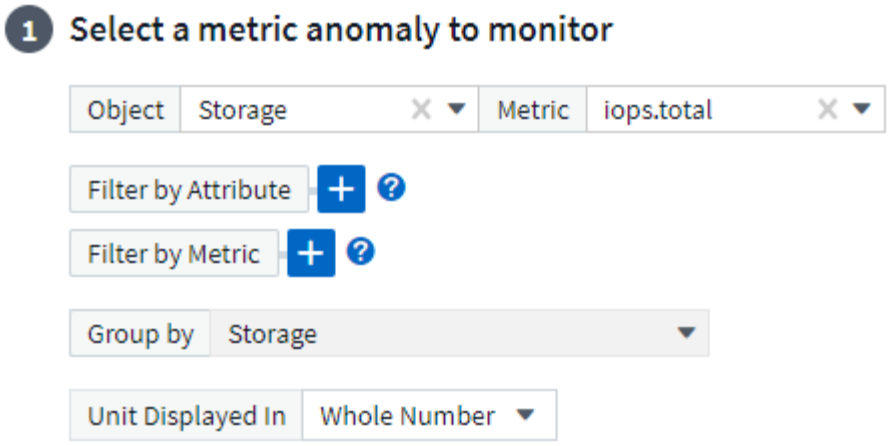
- すぐに解決: アラートはすぐに解決され、それ以上のアクションは必要ありません
- 時間に基づいて解決: 指定された時間が経過するとアラートが解決されます
- ログ エントリに基づいて解決: 後続のログ アクティビティが発生すると、アラートが解決されます。たとえば、オブジェクトが「使用可能」としてログに記録される場合などです。



異常検出モニター

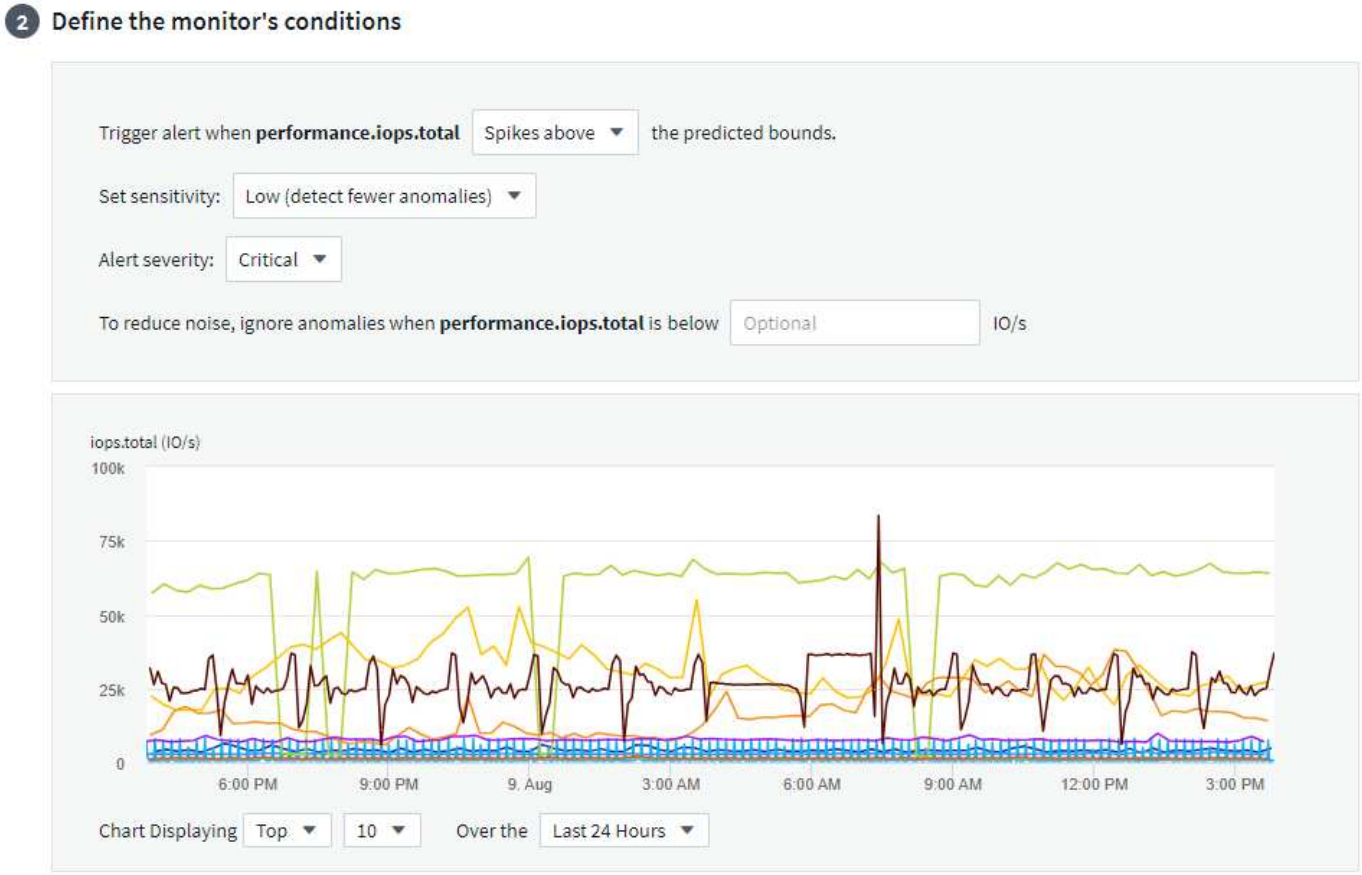
1. ドロップダウンで、監視するオブジェクト タイプとメトリックを検索して選択します。

フィルターを設定して、監視するオブジェクト属性またはメトリックを絞り込むことができます。

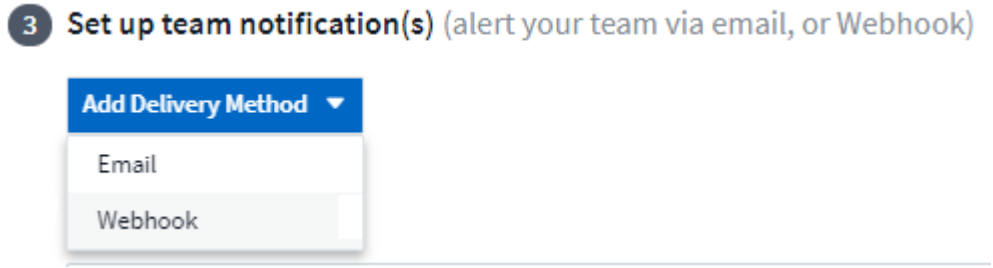


モニターの条件を定義します。

1. 監視するオブジェクトとメトリックを選択したら、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が予測された境界を*上回った*場合、*その境界を下回った*場合、または境界を*上回ったか下回った*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)。
   - アラートを*警告*または*重大*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ている場合に異常を無視して、ノイズを減らすこともできます。

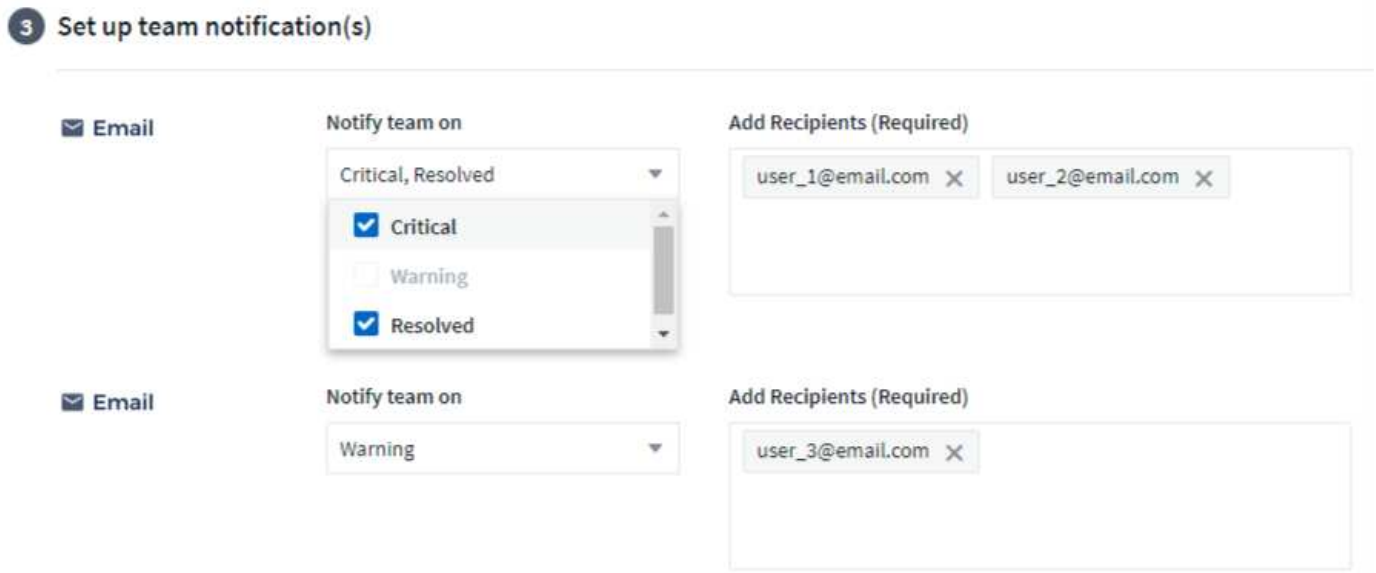


[チーム通知の設定] セクションでは、電子メールまたは Webhook のどちらでチームに通知するかを選択できます。



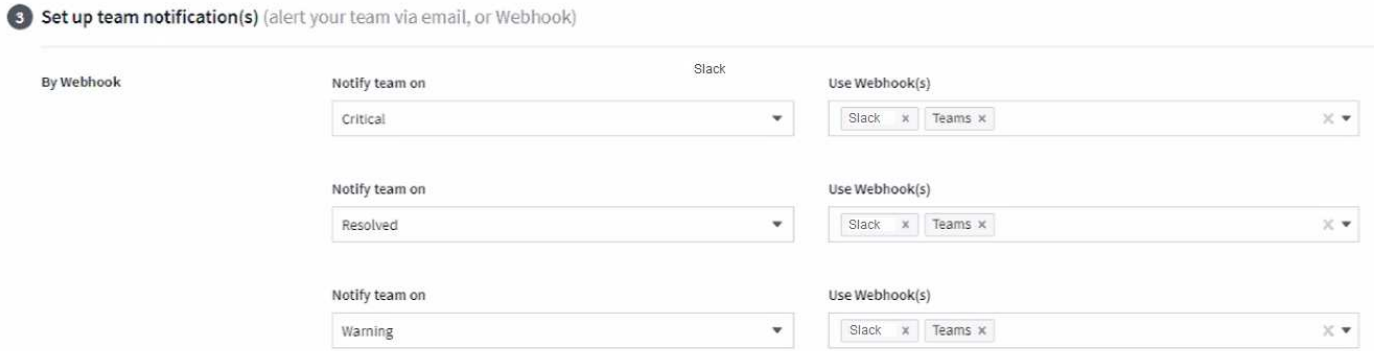
電子メールによるアラート:

アラート通知の電子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に異なる受信者を選択できます。



Webhook経由のアラート:

アラート通知用の Webhook 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異なる Webhook を選択できます。



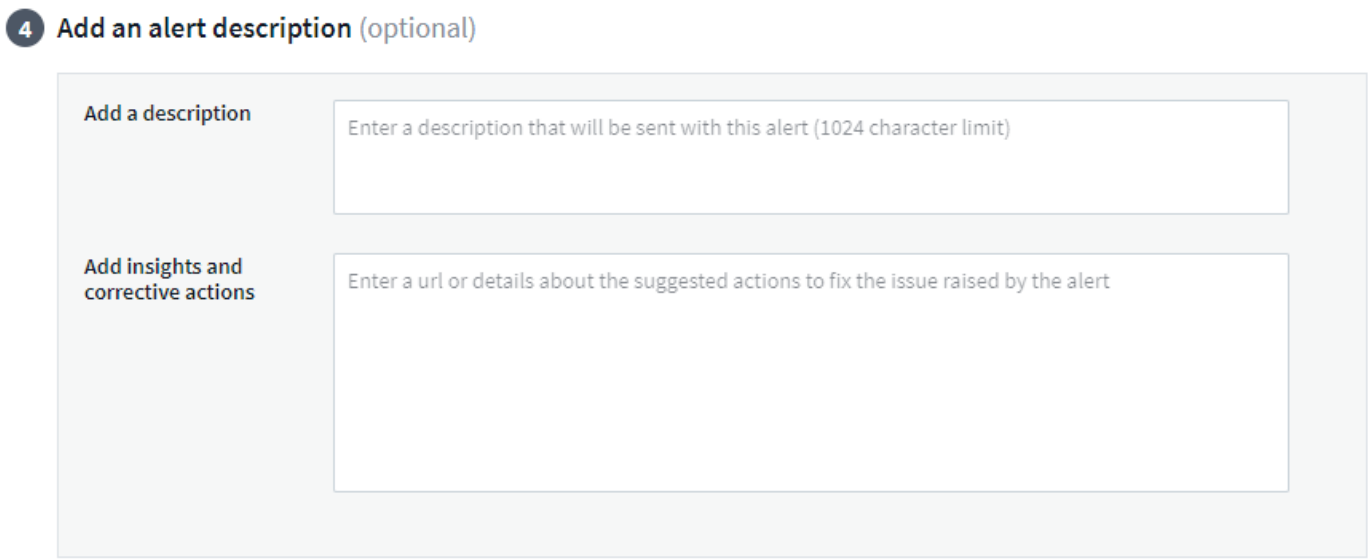
ONTAPデータ コレクターの通知は、クラスタ/データ コレクターに関連する特定のモニター通知よりも優先されます。データ コレクター自体に設定した受信者リストには、データ コレクターのアラートが送信されます。アクティブなデータ コレクター アラートがない場合、モニターによって生成されたアラートが特定のモニター受信者に送信されます。

是正措置または追加情報の設定

*アラートの説明を追加*セクションに入力することで、オプションの説明や追加の洞察や是正アクションを追加できます。説明は最大 1024 文字まで入力でき、アラートとともに送信されます。洞察/是正措置フィールドは最大 67,000 文字まで入力でき、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では、アラートを修正または対処するためのメモ、リンク、または手順を入力できます。

任意のオブジェクト属性 (たとえば、ストレージ名) をアラートの説明にパラメータとして追加できます。たとえば、「ボリューム: *%%relatedObject.volume.name%%*、ストレージ: *%%relatedObject.storage.name%%* の待機時間が長い」のような説明で、ボリューム名とストレージ名のパラメータを設定できます。



モニターを保存する

1. 必要に応じて、モニターの説明を追加できます。
2. モニターにわかりやすい名前を付けて、[保存] をクリックします。

   新しいモニターがアクティブなモニターのリストに追加されます。

モニターリスト

モニター ページには、現在構成されているモニターが一覧表示され、次の情報が表示されます。

- モニター名
- ステータス
- 監視対象のオブジェクト/メトリック
- モニターの条件

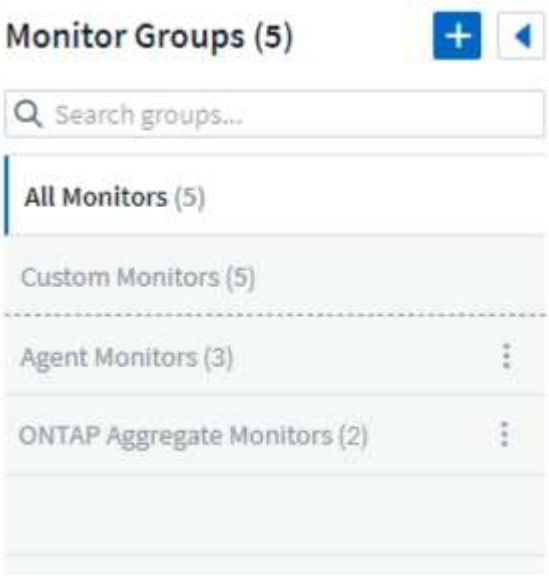
モニターの右側にあるメニューをクリックし、「一時停止」を選択すると、オブジェクト タイプの監視を一時的に一時停止できます。監視を再開する準備ができたら、[再開] をクリックします。

メニューから*複製*を選択すると、モニターをコピーできます。その後、新しいモニターを変更し、オブジェクト/メトリック、フィルター、条件、電子メールの受信者などを変更できます。

モニターが不要になった場合は、メニューから*削除*を選択して削除できます。

モニターグループ

グループ化すると、関連するモニターを表示および管理できます。たとえば、テナント上のストレージ専用のモニター グループを作成したり、特定の受信者リストに関連するモニターを作成したりできます。



次のモニター グループが表示されます。グループに含まれるモニターの数は、グループ名の横に表示されます。

- すべてのモニター にはすべてのモニター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ているシステム モニターが一覧表示されます。
- Data Infrastructure Insightsには、システム監視グループもいくつか表示されます。これには、"システム定義モニター" ONTAPインフラストラクチャおよびワークロード モニターなど。

カスタム モニターは、一時停止、再開、削除、または別のグループに移動できます。システム定義のモニター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。

サスペンドモニター

このグループは、Data Infrastructure Insights が1 つ以上のモニターを一時停止している場合にのみ表示されます。過剰なアラートや継続的なアラートが生成されている場合、モニターは一時停止されることがあります。モニターがカスタム モニターの場合は、継続的なアラートを防止するために条件を変更してから、モニターを再開します。一時停止の原因となった問題が解決されると、モニターは一時停止中のモニター グループから削除されます。

システム定義モニター

モニター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、これらのグループには、 Data Infrastructure Insightsによって提供されるモニターが表示されます。

システム定義のモニターは、変更したり、別のグループに移動したり、削除したりすることはできません。ただし、システム モニターを複製し、その複製を変更または移動することはできます。

システム モニターには、 ONTAPインフラストラクチャ (ストレージ、ボリュームなど) やワークロード (ログモニターなど)、その他のグループのモニターが含まれる場合があります。 NetAppは顧客のニーズと製品の機能を継続的に評価しており、必要に応じてシステム モニターとグループを更新または追加します。

カスタムモニターグループ

ニーズに応じて、モニターを含む独自のグループを作成できます。たとえば、ストレージ関連のすべてのモニターのグループが必要な場合があります。

新しいカスタム モニター グループを作成するには、[**"+"** 新しいモニター 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。その名前で空のグループが作成されます。

グループにモニターを追加するには、[すべてのモニター] グループ (推奨) に移動し、次のいずれかを実行します。

- 単一のモニターを追加するには、モニター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。モニターを追加するグループを選択します。
- モニター名をクリックしてモニターの編集ビューを開き、[モニター グループに関連付ける] セクションでグループを選択します。



グループをクリックし、メニューから [グループから削除] を選択して、モニターを削除します。 すべてのモニター または カスタム モニター グループからモニターを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ーを削除するには、モニター自体を削除する必要があります。

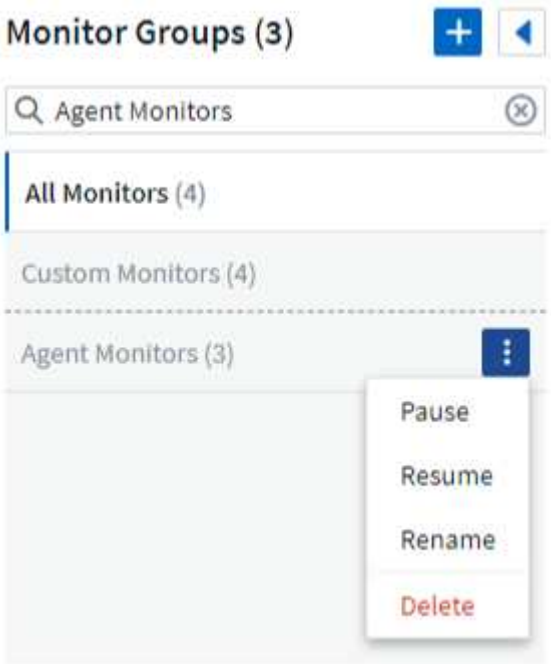
> グループからモニターを削除しても、Data Infrastructure Insightsからモニターは削除されません。モニターを完全に削除するには、モニターを選択し、[削除] をクリックします。これにより、そのアイテムは所属していたグループからも削除され、どのユーザーも利用できなくなります。

同様に、[グループに移動] を選択して、モニターを別のグループに移動することもできます。

グループ内のすべてのモニター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、[一時停止] または [再開] をクリックします。

グループの名前を変更したり、グループを削除したりする場合にも、同じメニューを使用します。グループを

削除しても、 Data Infrastructure Insightsからモニターは削除されません。モニターは引き続き [すべてのモニター] で利用できます。



システム定義モニター

Data Infrastructure Insights には、メトリックとログの両方に対するシステム定義のモニターが多数含まれています。利用可能なシステム モニターは、テナントに存在するデータ コレクターによって異なります。そのため、データ コレクターが追加されたり、その構成が変更されたりすると、 Data Infrastructure Insightsで使用できるモニターが変わる可能性があります。

表示"システム定義モニター"Data Infrastructure Insightsに含まれるモニターの説明ページ。

詳細情報

- "アラートの表示と消去"

モニターからのアラートの表示と管理

Data Infrastructure Insightsは、次のような場合にアラートを表示します。"監視対象の閾値"超過しています。

モニターとアラートは、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. アラート > すべてのアラート ページに移動します。
2. 最新の 1,000 件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、このリストを任意のフィールドで並べ替えることができます。リストには次の情報が表示されます。これらの列のすべてがデフォルトで表示されるわけではないことに注意してください。 「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
- トリガー時刻: 関連するモニターがアラートをトリガーした時刻
- 現在の重大度 (アクティブアラートタブ): アクティブアラートの現在の重大度
- 最高重大度 (解決済みアラートタブ); 解決前のアラートの最大の重大度
- モニター: アラートをトリガーするように設定されたモニター
- トリガーオン: 監視対象のしきい値を超えたオブジェクト
- ステータス: 現在のアラートのステータス、新規 または 処理中
- アクティブ ステータス: アクティブ または 解決済み
- 条件: アラートをトリガーしたしきい値条件
- メトリック: 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
- モニターステータス: アラートをトリガーしたモニターの現在のステータス
- 修正アクションあり: アラートには修正アクションが提案されています。これらを表示するにはアラート ページを開いてください。

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することで、アラートを管理できます。

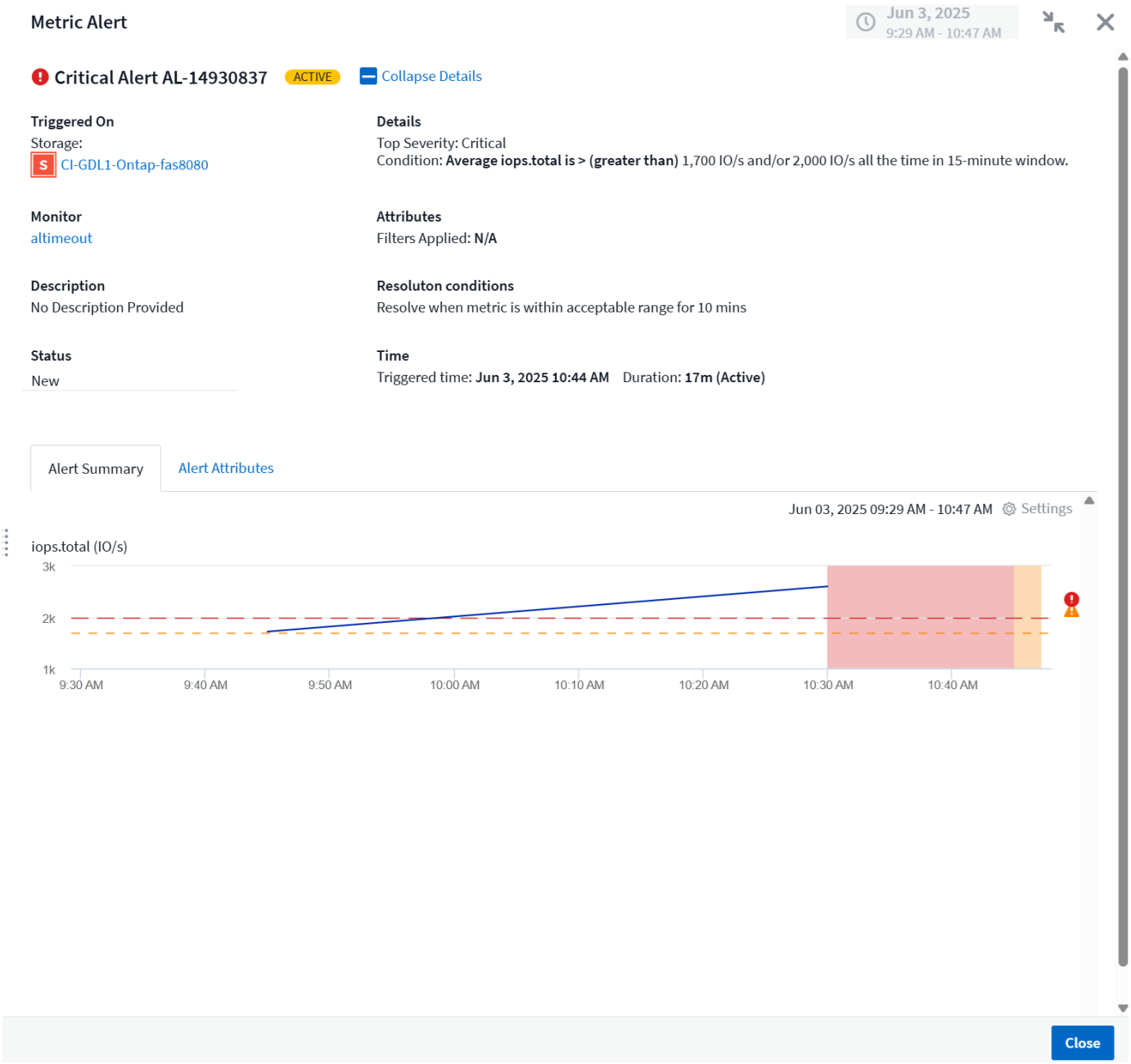
- 処理中 アラートが調査中であるか、またはオープンのままにしておく必要があることを示します。
- *[閉じる]*をクリックすると、アクティブなアラートのリストからアラートが削除されます。

各アラートの左側にあるチェックボックスを選択し、「選択したアラートのステータスを変更」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、アラートの詳細ページが開きます。

アラート詳細パネル

任意のアラート行を選択すると、アラートの詳細パネルが開きます。アラートの詳細パネルには、アラートに関する追加の詳細が表示されます。これには、概要、オブジェクトのデータに関連するグラフを表示する_パフォーマンス_セクション、関連資産、アラート調査員が入力した_コメント_が含まれます。



データが欠落している場合のアラート

Data Infrastructure Insightsなどのリアルタイム システムでは、モニターの分析をトリガーしてアラートを生成するかどうかを決定するために、次の 2 つのいずれかに依存します。

- 次に到着するデータポイント
- データポイントがなく、十分に待った場合に起動するタイマー

データの到着が遅い場合、またはデータが到着しない場合は、データ到着率が「リアルタイム」でアラートをトリガーするには不十分であるため、タイマー メカニズムが引き継ぐ必要があります。したがって、一般的な質問は、「分析ウィンドウを閉じて、結果を確認するまでにどれくらい待てばよいですか?」となります。待つ時間が長すぎると、役に立つほど速くアラートが生成されなくなります。

長期的なデータ損失が発生する前の最後のデータ ポイントで条件に違反していることを通知する 30 分のウィンドウを持つモニターがある場合、モニターはメトリックの回復を確認するために使用する他の情報や条件が

持続していることを通知する情報を受け取っていないため、アラートが生成されます。

「常時アクティブ」アラート

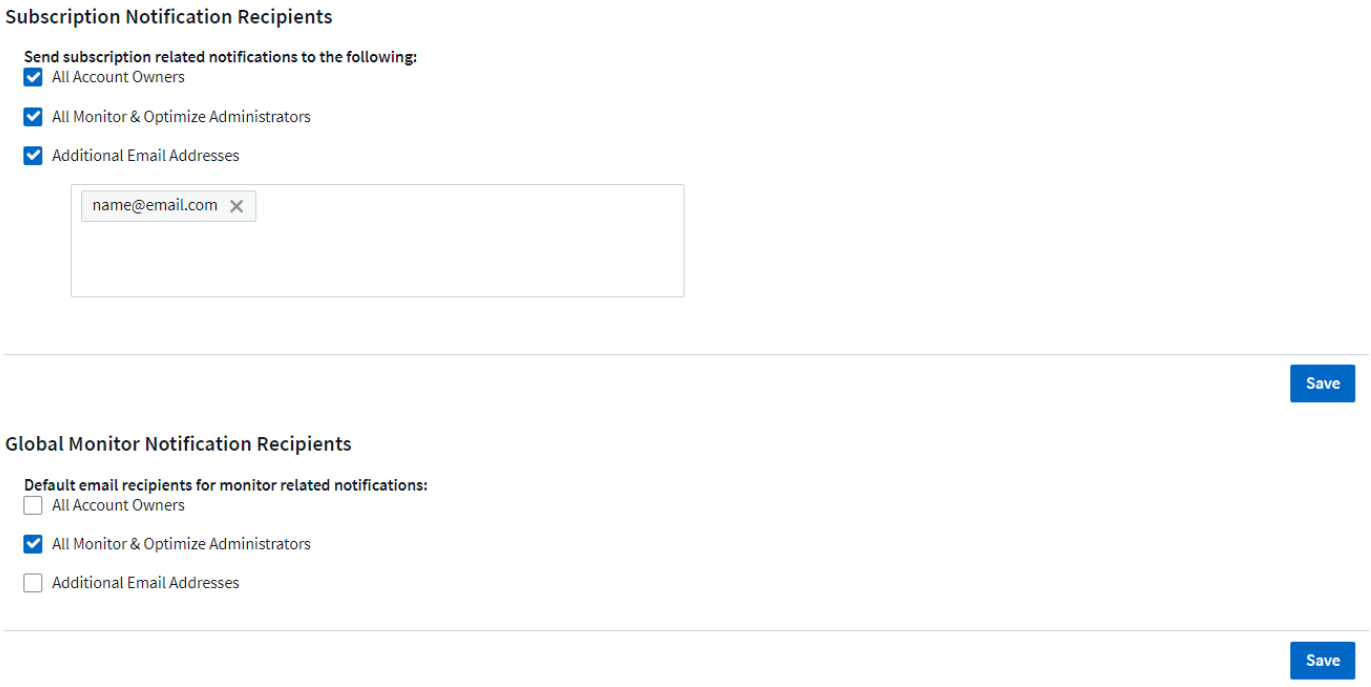
監視対象オブジェクトに条件が 常に 存在するようにモニターを構成することもできます (例: IOPS > 1 またはレイテンシ > 0)。これらは多くの場合、「テスト」モニターとして作成され、その後忘れ去られます。このようなモニターは、構成オブジェクトに対して永続的に開いたままのアラートを作成するため、時間の経過とともにシステムのストレスや安定性の問題が発生する可能性があります。

これを防ぐために、 Data Infrastructure Insights は、 7 日後に「永続的にアクティブな」アラートを自動的に閉じます。基礎となるモニター条件は (おそらく) 引き続き存在し、新しいアラートがほぼ即座に発行される可能性があることに注意してください。ただし、この「常にアクティブな」アラートを閉じると、発生する可能性のあるシステム ストレスの一部が軽減されます。

電子メール通知の設定

サブスクリプション関連の通知用の電子メール リストと、パフォーマンス ポリシーしきい値違反の通知の受信者のグローバル電子メール リストを構成できます。

通知メールの受信者設定を構成するには、管理 > 通知 ページに移動し、メール 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構成するには、「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。サブスクリプション関連のイベントに関する電子メール通知を、次の受信者のいずれかまたは全員に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_Monitor & Optimize_管理者
- 指定する追加のメールアドレス

以下は、送信される可能性のある通知の種類と、実行できるユーザーアクションの例です。

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	サブスクリプションの詳細を確認する"Subscription"ページ
サブスクリプションは90日後に期限切れになります サブスクリプションは30日後に期限切れになります	「自動更新」が有効になっている場合は、何もする必要はありません。サブスクリプションを更新するには、 NetAppの営業担当者にお問い合わせください。
トライアルは2日後に終了します	トライアルの更新"Subscription"ページ。試用版は 1 回更新できます。サブスクリプションを購入するには、 NetApp の営業担当者にお問い合わせください。
試用版またはサブスクリプションの有効期限が切れました。アカウントは48時間以内にデータ収集を停止します。アカウントは48時間後に削除されます。	サブスクリプションを購入するには、 NetApp の営業担当者にお問い合わせください。

受信者がData Infrastructure Insightsから通知を確実に受信できるようにするには、次のメールアドレスを「許可」リストに追加します。

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

アラートのグローバル受信者リスト

アラートに関するアクションごとに、アラートの電子メール通知が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を選択できます。

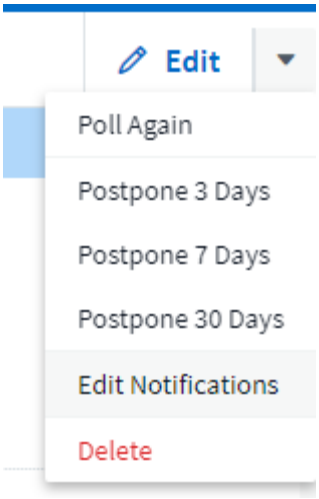
グローバルアラートの受信者を設定するには、「グローバルモニター通知の受信者」セクションで目的の受信者を選択します。

モニターを作成または変更するときに、いつでも個々のモニターのグローバル受信者リストを上書きできます。

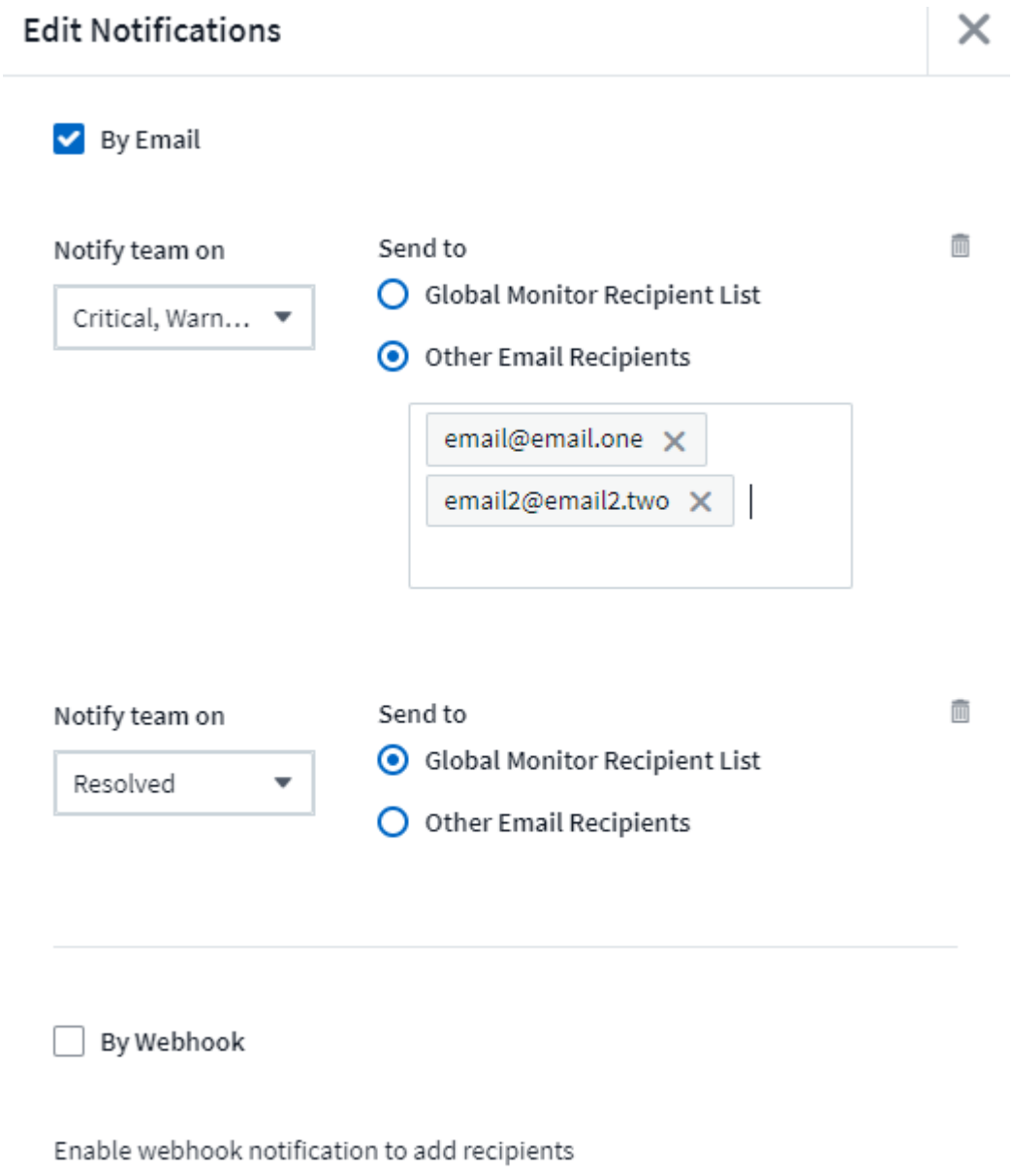
ONTAPデータ コレクターの通知は、クラスタ/データ コレクターに関連する特定のモニター通知よりも優先されます。データ コレクター自体に設定した受信者リストには、データ コレクターのアラートが送信されます。アクティブなデータ コレクター アラートがない場合、モニターによって生成されたアラートが特定のモニター受信者に送信されます。

ONTAPの通知の編集

ストレージ ランディング ページの右上にあるドロップダウンから [通知の編集] を選択すると、 ONTAPクラスターの通知を変更できます。



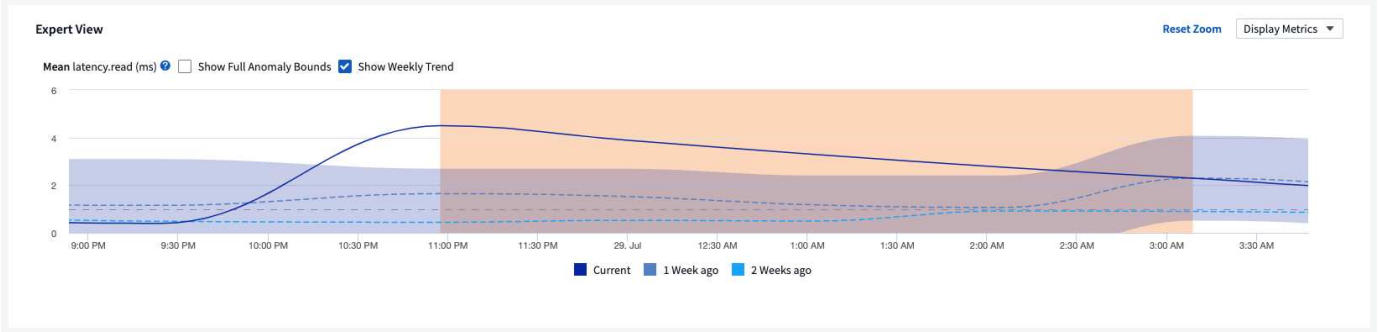
ここから、重大、警告、情報、解決済みのアラートの通知を設定できます。各シナリオでは、グローバル受信者リストまたは選択した他の受信者に通知できます。



異常検出モニター

異常検出は、テナント上のデータ パターンの予期しない変化に関する洞察を提供します。異常は、オブジェクトの動作パターンが変化すると発生します。たとえば、オブジェクトが水曜日の特定の時間に特定のレベルのレイテンシを経験し、次の水曜日の同じ時間にレイテンシがそのレベルを超えて急上昇した場合、その急上昇は異常と見なされます。 Data Infrastructure Insights を使用すると、このような異常が発生したときに警告を発するモニターを作成できます。

異常検出は、繰り返し発生する予測可能なパターンを示すオブジェクト メトリックに適しています。これらのオブジェクト メトリックが予想レベルを上回ったり下回ったりすると、 Data Infrastructure Insights はアラートを生成して調査を促します。



異常検出とは何ですか?

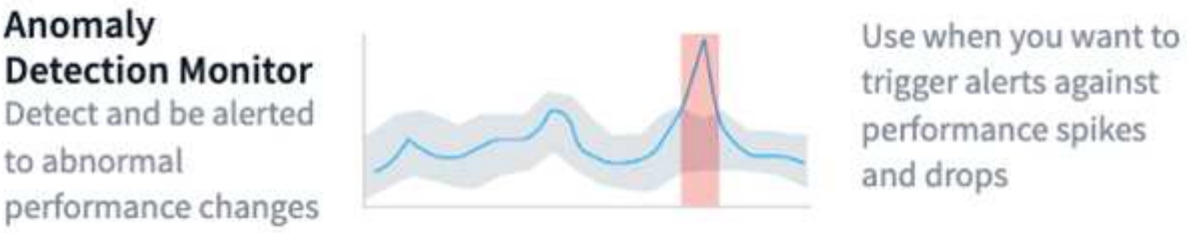
異常は、メトリックの平均値が、過去数週間のそのメトリックの加重平均から標準偏差の数だけ離れており、最近の週が以前の週よりも重み付けが大きい場合に発生します。 Data Infrastructure Insights は、データを監視し、異常が検出された場合に警告する機能を提供します。検出の「感度」レベルを設定することができます。たとえば、平均値と平均値からの標準偏差が少ないほど感度が高くなり、生成されるアラートが多くなります。逆に、感度が低い = 平均からの標準偏差が大きい = アラートが少ない。

異常検出監視はしきい値監視とは異なります。

- *しきい値ベースの監視*は、特定のメトリックに対して事前に定義されたしきい値がある場合に機能します。言い換えれば、何が期待されているか（つまり、正常範囲内）を明確に理解している場合です。



- *異常検出モニタリング*は、機械学習アルゴリズムを使用して、「正常」の定義が明確でない場合に、標準から逸脱する外れ値を識別します。



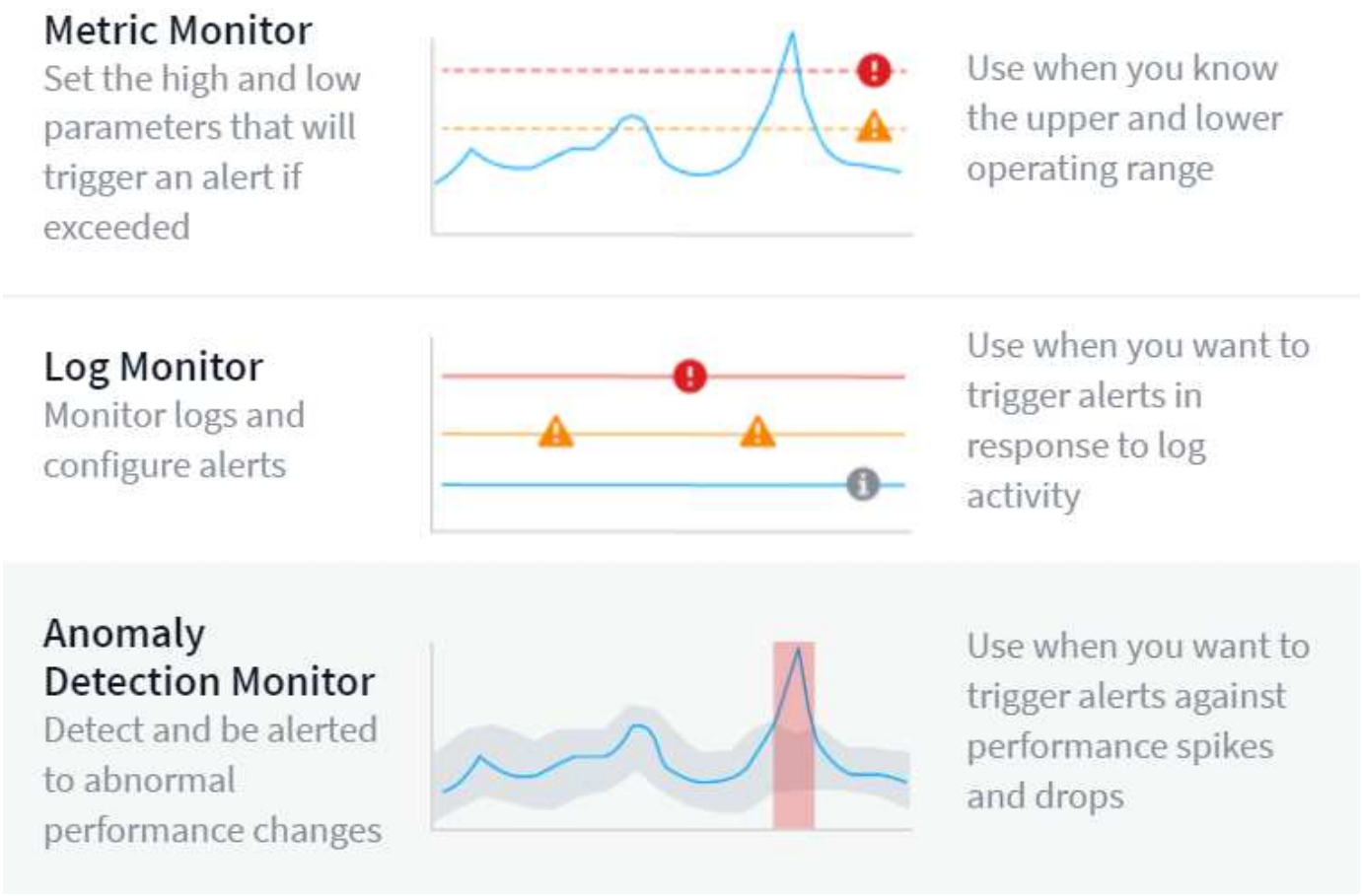
異常検出はいつ必要になるのでしょうか**?**

異常検出モニタリングは、次のような多くの状況で役立つアラートを提供できます。

- _正常_の定義が不明瞭な場合。たとえば、SAN エラー率はポートに応じて異なる量が予想される場合があります。 1 つのエラーについて警告するのはノイズが多く不必要ですが、突然のまたは大幅な増加は広範囲にわたる問題を示している可能性があります。
- 時間の経過とともに変化がある場所。季節性があるワークロード (つまり、特定の時間に忙しいか静かである)。これには、バッチの停止を示す可能性のある予期しない静かな期間が含まれる場合があります。
- しきい値を手動で定義および調整することが非現実的な大量のデータを扱う場合。たとえば、ワークロードが異なる多数のホストやボリュームを持つテナントなどです。それぞれ SLA が異なる場合があるため、標準を超える SLA を理解することが重要です。

異常検出モニターの作成

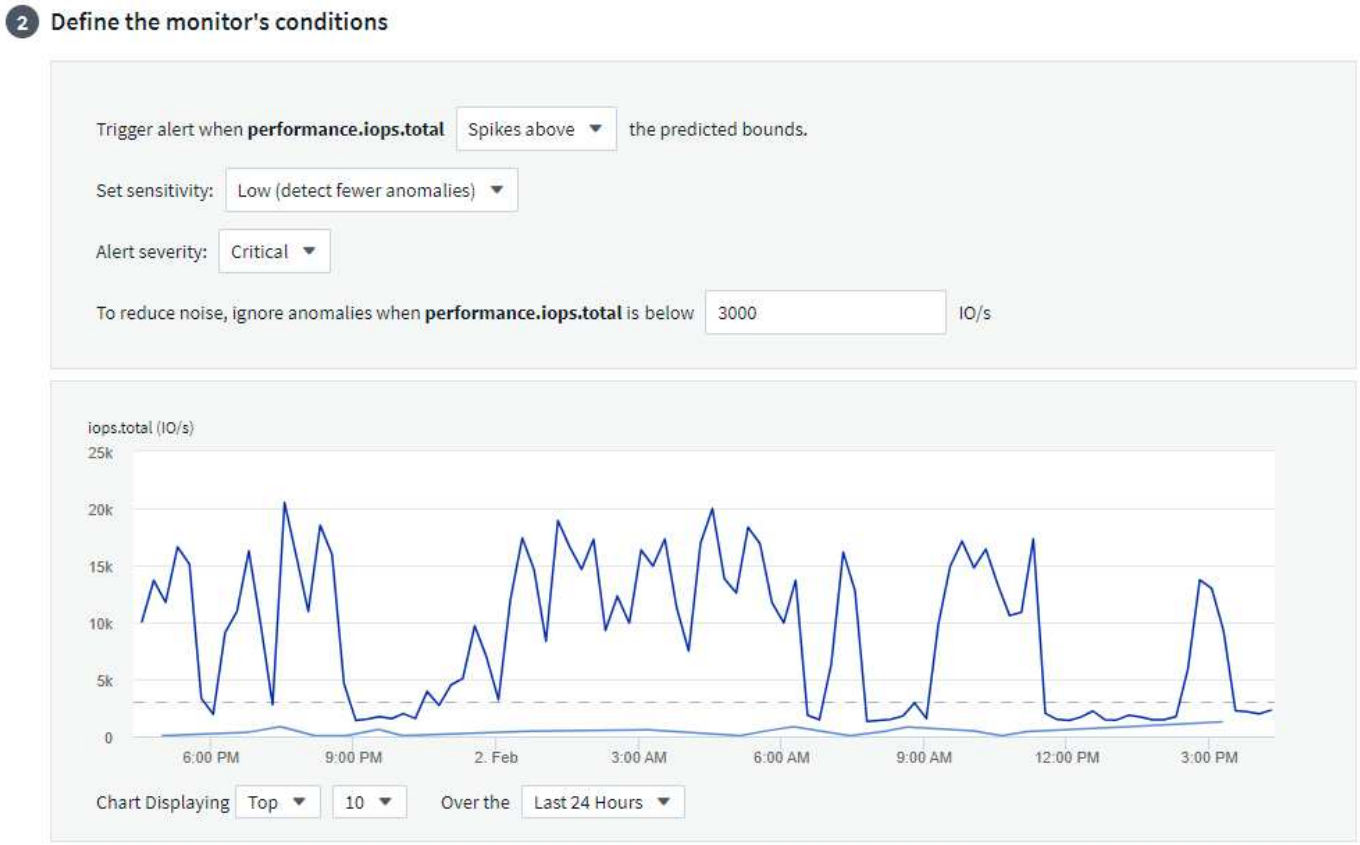
異常を警告するには、**Observability > Alerts > +Monitor** に移動してモニターを作成します。モニタータイプとして「異常検出モニター」を選択します。



監視するオブジェクトとメトリックを選択します。他の種類のモニターと同様に、フィルターやグループ化を設定できます。

次にモニターの条件を設定します。

- 選択したメトリックが予測された境界を 上回る 場合、その境界を下回る場合、またはその両方の場合にアラートをトリガーします。
- 感度を「中」、「低」（より少ない異常が検出される）、または「高」（より多くの異常が検出される）に設定します。
- 警告レベルが *Critical* か *Warning* かを判断します。
- オプションで、その値を下回る異常は無視される値を設定します。これによりノイズを軽減できます。この値はサンプル グラフでは破線で表示されます。



最後に、アラートの配信方法 (電子メール、Webhook、またはその両方) を構成し、モニターにオプションの説明や修正アクションを指定し、必要に応じてモニターをカスタム グループに追加できます。

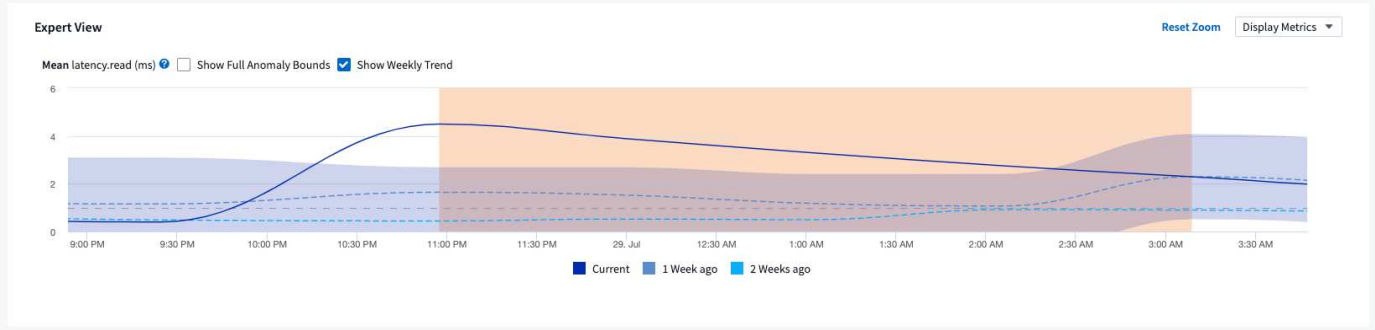
モニターを意味のある名前で保存すれば完了です。

作成時に、モニターは前週のデータを分析して初期ベースラインを確立します。異常検出は、時間が経過し、履歴が増えるにつれて、より正確になります。

> モニターが作成されると、DII は前の週の既存のデータを調べて、大幅なデータの急増や減少がないか調べます。これらは異常とみなされます。モニター作成後の最初の 1 週間 (「学習」フェーズ) は、アラートの「ノイズ」が増加する可能性があります。このノイズを軽減するために、30 分以上続く急上昇または急降下のみが異常とみなされ、アラートが生成されます。次の週には、より多くのデータが分析されるにつれて、通常、ノイズは減少し、一定期間続く大幅な急上昇または急降下は異常とみなされます。

異常の観察

アラート ランディング ページでは、異常が検出されたときにトリガーされるアラートにより、メトリックが予測された境界の外側に急上昇した時点から、その境界内に戻った時点までの、チャートに強調表示されたバンドが表示されます。



アラート ランディング ページで異常チャートを表示しているときに、次のオプションを選択できます。

- 週次傾向: 最大 5 週間前の同じ時刻、同じ日の値と比較します。
- 完全な異常境界: デフォルトでは、グラフはメトリック値に焦点を当てているため、メトリックの動作をより適切に分析できます。完全な異常境界（最大値など）を表示する場合に選択します

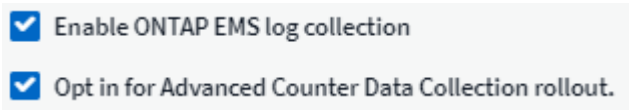
ランディング ページのパフォーマンス セクションでオブジェクトを選択して、異常の原因となったオブジェクトを表示することもできます。チャートには選択したオブジェクトの動作が表示されます。



システムモニター

Data Infrastructure Insights には、メトリックとログの両方に対するシステム定義のモニターが多数含まれています。利用可能なシステム モニターは、テナントに存在するデータ コレクターによって異なります。そのため、データ コレクターが追加されたり、その構成が変更されたりすると、 Data Infrastructure Insightsで使用できるモニターが変わる可能性があります。

多くのシステム モニターは、デフォルトでは 一時停止 状態になっています。モニターの [再開] オプションを選択すると、システム モニターを有効にすることができます。データ コレクターで [Advanced Counter Data Collection] と [Enable ONTAP EMS log 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 コレクターの [*Advanced Configuration*] にあります。



目次:[]

モニターの説明

システム定義のモニターは、事前定義されたメトリックと条件、および変更できないデフォルトの説明と修正アクションで構成されます。システム定義モニターの通知受信者リストを変更することができます。メトリック、条件、説明、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ー グループを開き、リスト内のモニター名をクリックします。

システム定義のモニター 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ーは、記載されているグループで使用できます。

- * ONTAPインフラストラクチャ* には、 ONTAPクラスタのインフラストラクチャ関連の問題を監視するモニターが含まれています。
- * 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ーはデフォルトで 一時停止 状態になります。

以下は、現在Data Infrastructure Insightsに含まれているシステム モニターです。

メトリックモニター

モニター名	重大度	モニターの説明	対処方法

ファイバーチャネルポート使用率が高い	重大	ファイバー チャネル プロトコル ポートは、顧客のホスト システムとONTAP LUN 間の SAN トラフィックを受信および転送するために使用されます。ポートの使用率が高い場合、それがボトルネックとなり、最終的にはファイバー チャネル プロトコルのワークロードの重要なパフォーマンスに影響を及ぼします。…警告アラートは、ネットワーク トラフィックを分散させ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。…重大なアラートは、サービスの中断が差し迫っており、サービスの継続性を確保するためにネットワーク トラフィックを分散するための緊急措置を実行する必要があることを示します。	重要な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、直ちに次のアクションを検討してください。1.ワークロードを、使用率の低い別の FCP ポートに移動します。2. ONTAP のQoS ポリシーまたはホスト側の構成を使用して、特定の LUN のトラフィックを必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た場合は、次のアクションを実行するように計画します。1.ポート使用率がより多くのポートに分散されるように、データ トラフィックを処理するためにさらに多くの FCP ポートを構成します。2.ワークロードを、使用率の低い別の FCP ポートに移動します。3. ONTAP のQoS ポリシーまたはホスト側の構成を使用して、特定の LUN のトラフィックを必要な作業のみに制限し、FCP ポートの使用率を軽減します。

Lunレイテンシ高	重大	LUN は、データベースなどのパフォーマンスが重視されるアプリケーションによって実行されることが多い I/O トラフィックを処理するオブジェクトです。 LUN のレイテンシが高い場合、アプリケーション自体に問題が発生し、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。…重大なアラートは、サービスの中断が差し迫っており、サービスの継続性を確保するために緊急措置を講じる必要があることを示します。メディアの種類に応じて予想されるレイテンシは次のとおりです - SSD 最大 1～2 ミリ秒、SAS 最大 8～10 ミリ秒、SATA HDD 17～20 ミリ秒	重大な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アクション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、それが LUN ワークロードの調整を引き起こしているかどうかを検証します。…警告しきい値を超えた場合は、次のアクションを実行するように計画します。1.アグリゲートの使用率も高い場合は、LUN を別のアグリゲートに移動します。2.ノードの使用率も高い場合は、ボリュームを別のノードに移動する、またはノードの合計ワークロードを削減します。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、そのしきい値制限を評価し、それが LUN ワークロードの調整を引き起こしているかどうかを検証します。

ネットワークポート使用率が高い	重大	ネットワーク ポートは、顧客のホスト システムとONTAPボリューム間のNFS、CIFS、およびiSCSI プロトコル トラフィックを受信および転送するために使用されます。ポートの使用率が高い場合、それがボトルネックとなり、最終的にはNFS、CIFS、iSCSI ワークロードのパフォーマンスに影響します。…警告アラートは、ネットワーク トラフィックを分散させ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。…重大なアラートは、サービスの中断が差し迫っており、サービスの継続性を確保するためにネットワーク トラフィックを分散するための緊急措置を実行する必要があることを示します。	重大な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、次の即時アクション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必要な作業のみに制限し、ネットワーク ポートの使用率を下げます。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 つ以上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、次の即時アクションを検討してください。1.ポート使用率がより多くのポートに分散されるように、データ トラフィックを処理するためにさらに多くのネットワーク ポートを構成します。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 つ以上のボリュームを構成します。

NVMe名前空間レイテンシ高	重大	NVMe 名前空間は、データベースなどのパフォーマンスが重視されるアプリケーションによって実行される I/O トラフィックを処理するオブジェクトです。 NVMe 名前空間のレイテンシが高いと、アプリケーション自体に問題が発生し、タスクを完了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。…重大なアラートは、サービスの中断が差し迫っており、サービスの継続性を確保するために緊急措置を講じる必要があることを示します。	重要な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即時のアクションを検討してください。NVMe 名前空間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、その制限しきい値が NVMe 名前空間のワークロードの調整を引き起こしていないかどうか確認してください。…警告しきい値を超えた場合は、次のアクションを実行することを検討してください。1.アグリゲートの使用率も高い場合は、LUN を別のアグリゲートに移動します。2.ノードの使用率も高い場合は、ボリュームを別のノードに移動する、またはノードの合計ワークロードを削減します。3. NVMe 名前空間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、そのポリシーによって NVMe 名前空間のワークロードが調整される可能性がないか、その制限しきい値を評価します。

QTree 容量がいっぱい	重大	qtree は、ボリューム内のルート ディレクトリの特別なサブディレクトリとして存在できる、論理的に定義されたファイル システムです。各 qtree には、デフォルトのスペース クォータまたはクォータ ポリシーによって定義されたクォータがあり、ボリューム容量内でツリーに保存されるデータの量を制限します。…警告アラートは、スペースを増やす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。…重大なアラートは、サービスの中断が差し迫っており、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緊急措置を実行する必要があることを示します。	重要な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、直ちに次のアクションを検討してください。1.成長に対応するために 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た場合は、次の即時措置を講じる計画を立ててください。1.成長に対応するために 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 容量のハード制限	重大	qtree は、ボリューム内のルート ディレクトリの特別なサブディレクトリとして存在できる、論理的に定義されたファイル システムです。各 qtree には、KB 単位で測定されるスペース クォータがあり、これを使用してデータを保存します。これにより、ボリューム内のユーザー データの増加を制御し、合計容量を超えないようにします。…qtree は、qtree の合計容量クォータ制限に達してデータを保存できなくなる前に、ユーザーに事前に警告するソフト ストレージ容量クォータを維持します。 qtree 内に保存されているデータの量を監視することで、ユーザーは中断のないデータ サービスを受けることができます。	重大な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、次の即時アクションを検討してください。1.成長に対応するために、ツリーのスペース割り当てを増やします 2。スペースを解放するためにツリー内の不要なデータを削除するようにユーザーに指示します

QTree 容量ソフト制限	警告	qtree は、ボリューム内のルート ディレクトリの特別なサブディレクトリとして存在できる、論理的に定義されたファイル システムです。各 qtree には、KB 単位で測定されるスペース クォータがあり、これを使用してデータを保存することで、ユーザー データの増加を制御し、合計容量を超えないようにします。…qtree は、qtree の合計容量クォータ制限に達してデータを保存できなくなる前に、ユーザーに事前に警告するソフト ストレージ容量クォータを維持します。 qtree 内に保存されているデータの量を監視することで、ユーザーは中断のないデータ サービスを受けることができます。	警告しきい値を超えた場合は、次の即時アクションを検討してください。1.成長に対応するためにツリーのスペース割り当てを増やします。2.スペースを解放するために、ツリー内の不要なデータを削除するようにユーザーに指示します。
QTree ファイルのハード制限	重大	qtree は、ボリューム内のルート ディレクトリの特別なサブディレクトリとして存在できる、論理的に定義されたファイル システムです。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 ファイル数クォータを維持します。 qtree 内のファイル数を監視することで、ユーザーは中断のないデータ サービスを受けることができます。	重要な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、直ちに次のアクション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 ファイルのソフト制限	警告	qtree は、ボリューム内のルート ディレクトリの特別なサブディレクトリとして存在できる、論理的に定義されたファイル システムです。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、格納できるファイル数のクォータがあります。…qtree は、qtree 内のファイル制限に達して追加のファイルを保存できなくなる前に、ユーザーに事前に警告するためにソフト ファイル数クォータを維持します。 qtree 内のファイル数を監視することで、ユーザーは中断のないデータ サービスを受けることができます。	警告しきい値を超えた場合は、次の即時措置を講じる計画を立ててください。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。

スナップショット予約領域がいっぱいです	重大	アプリケーションと顧客データを保存するには、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その領域の一部は、データをローカルで保護できるようにするスナップショットを保存するために使用されます。ONTAPボリュームに保存される新規データや更新データが増えるほど、使用されるスナップショット容量が増え、将来の新規データや更新データに使用できるスナップショット ストレージ容量は少なくなります。ボリューム内のスナップショットデータ容量が合計スナップショット予約領域に達すると、新しいスナップショット データを保存できなくなり、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スナップショット容量を監視することで、データ サービスの継続性が確保されます。	重要な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、直ちに次のアクション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内のデータ領域を使用するようにスナップショットを構成します。2.古くて不要なスナップショットをいくつか削除して、スペースを解放します。…警告しきい値を超えた場合は、次の即時措置を講じる計画を立ててください。1.成長に対応するために、ボリューム内のスナップショット予約領域を増やします。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構成します。

ストレージ容量制限	重大	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 操作が遅くなり、最終的には停止して、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、最小限の空き領域を回復するために計画されたアクションをすぐに実行する必要があることを示します。重大なアラートは、サービスの中断が差し迫っており、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の緊急措置を講じる必要があることを示します。	重大な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、直ちに次のアクションを検討してください。1.重要でないボリューム上のスナップショットを削除します。2.重要でないワークロードであり、オフストレージ コピーから復元でき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た場合は、次の即時アクションを計画してください。1. 1 つ以上のボリュームを別の保存場所に移動します。2.ストレージ容量を追加します。3.ストレージ効率設定を変更するか、非アクティブなデータをクラウド 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	重大	ストレージ システムのパフォーマンス限界に達すると、操作が遅くなり、待ち時間が増加し、ワークロードとアプリケーションに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、消費されたパフォーマンスの割合を推定します。…警告アラートは、ワークロードのピークに対応するために十分なストレージ プール パフォーマンスを確保するために、ストレージ プールの負荷を軽減するための計画的なアクションを実行する必要があることを示します。…重大なアラートは、パフォーマンスの低下が差し迫っており、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の緊急措置を実行する必要があることを示します。	重大な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、次の即時アクションを検討してください。1. スナップショットやSnapMirrorレプリケーションなどのスケジュールされたタスクを一時停止します。2.重要でないワークロードをアイドル状態にします。…警告しきい値を超えた場合は、直ちに次の措置を講じてください。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.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、ワークロードを再分配します 3.ワークロード特性 (ブロック サイズ、アプリケーション キャッシュ) を変更します。

ユーザークォータ容量のハード制限	重大	ONTAP は、ボリューム、ボリューム内のファイル、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 システムのユーザーを認識します。その結果、ONTAP を使用すると、顧客は Linux または Windows システムのユーザーまたはユーザー グループのストレージ容量を構成できるようになります。ユーザーまたはグループ ポリシー クォータは、ユーザーが自身のデータに利用できるスペースの量を制限します。…このクォータのハード制限により、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する直前にユーザーに通知することができます。ユーザーまたはグループのクォータ内に保存されるデータの量を監視することで、ユーザーが中断のないデータ サービスを受けられるようになります。	重大な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、次の即時アクションを検討してください。1.成長に対応するために、ユーザーまたはグループの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ーまたはグループに指示します。

ユーザークォータ容量ソフト制限	警告	ONTAP は、ボリューム、ボリューム内のファイル、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 システムのユーザーを認識します。その結果、ONTAP を使用すると、顧客は Linux または Windows システムのユーザーまたはユーザー グループのストレージ容量を構成できるようになります。ユーザーまたはグループ ポリシー クォータは、ユーザーが自身のデータに利用できるスペースの量を制限します。…このクォータのソフト制限により、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、ユーザーにプロアクティブに通知することができます。ユーザーまたはグループのクォータ内に保存されるデータの量を監視することで、ユーザーが中断のないデータ サービスを受けられるようになります。	警告しきい値を超えた場合は、次の即時措置を講じる計画を立ててください。1.成長に対応するために、ユーザーまたはグループの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。

ボリューム容量がいっぱいです	重大	アプリケーションと顧客データを保存するには、ボリュームのストレージ容量が必要です。 ONTAP ボリュームに保存されるデータが増えるほど、将来のデータのストレージ可用性は低下します。ボリューム内のデータ保存容量が合計保存容量に達した場合、保存容量不足によりお客様がデータを保存できなくなる可能性があります。使用されたボリュームのストレージ容量を監視することで、データ サービスの継続性が確保されます。	重大な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、次の即時アクションを検討してください。1.成長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.不要なデータを削除してスペースを解放します。3.スナップショットのコピーがスナップショット リザーブよりも多くのスペースを占有している場合は、古いスナップショットを削除するか、ボリューム スナップショットの自動削除を有効にします。…警告しきい値を超えた場合は、次の即時アクションを実行するように計画してください。1.成長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。スナップショットのコピーがスナップショット リザーブよりも多くのスペースを占有する場合は、古いスナップショットを削除するか、ボリューム スナップショットの自動削除を有効にします。……

ボリュームのiノード制限	重大	ファイルを保存するボリュームは、インデックスノード (inode) を使用してファイルのメタデータを保存します。ボリュームの inode 割り当てを使い果たすと、それ以上ファイルを追加できなくなります。…警告アラートは、使用可能な inode の数を増やす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。…重大なアラートは、ファイル制限の使い果たしが差し迫っており、サービスの継続性を確保するために inode を解放する緊急措置を講じる必要があることを示します。	重大な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、次の即時アクションを検討してください。1. ボリュームの inode 値を増やします。 inode 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 システムに対応しやすくなります。警告しきい値を超えた場合は、次の即時措置を講じる計画を立ててください。1.ボリュームの inode 値を増やします。 inode 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。

ボリュームレイテンシー高	重大	ボリュームは、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が重視されるアプリケーションによって実行されることが多い I/O トラフィックを処理するオブジェクトです。大量の待ち時間が発生すると、アプリケーション自体に問題が発生し、タスクを完了できなくなる可能性があります。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ためには、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 タイプに基づいて予想されるレイテンシは次のとおりです - SSD 最大 1 ～ 2 ミリ秒、SAS 最大 8 ～ 10 ミリ秒、SATA HDD 17 ～ 20 ミリ秒。	重要な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、次の即時アクション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となっていないか、その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、次の即時アクションを検討してください。1.アグリゲートの使用率も高い場合は、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は、ボリュームのワークロードが調整される原因にならないように、その制限しきい値を評価します。3.ノードの使用率も高い場合は、ボリュームを別のノードに移動する、またはノードの合計ワークロードを削減します。
モニター名	重大度	モニターの説明	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を及ぼす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一貫したパフォーマンスが保証されます。メディア タイプに基づいて予想されるレイテンシは、SSD で最大 1 ～ 2 ミリ秒、SAS で最大 8 ～ 10 ミリ秒、SATA HDD で 17 ～ 20 ミリ秒です。	重要な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、直ちに措置を講じる必要があります。1.スケジュールされたタスク、スナップショット、またはSnapMirrorレプリケーションを一時停止します 2。 QoS 制限 3 を介して、優先度の低いワークロードの需要を下げます。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、直ちに次のアクション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 3 を介して、優先度の低いワークロードの需要を下げます。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、ワークロードを再分配します 4。ワークロード特性の変更（ブロックサイズ、アプリケーションキャッシュなど）

ノード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、ノードでサポートされている IO およびアプリケーションのパフォーマンスに影響を及ぼす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使用率が低いため、アプリケーションのパフォーマンスが一貫して確保されます。	重要な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、直ちに措置を講じる必要があります。1.スケジュールされたタスク、スナップショット、またはSnapMirrorレプリケーションを一時停止します 2。 QoS 制限 3 を介して、優先度の低いワークロードの需要を下げます。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、次のアクション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 3 を介して、優先度の低いワークロードの需要を下げます。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、ワークロードを再分配します 4. ワークロード特性の変更（ブロックサイズ、アプリケーションキャッシュなど）

ストレージVMの高レイテンシ	警告/重大	ストレージ VM (SVM) のレイテンシが、ストレージ VM 上のアプリケーションのパフォーマンスに影響を及ぼす可能性があるレベルに達しました。ストレージ VM のレイテンシが低いため、アプリケーションの一貫したパフォーマンスが保証されます。メディア タイプに基づいて予想されるレイテンシは、SSD で最大 1 ～ 2 ミリ秒、SAS で最大 8 ～ 10 ミリ秒、SATA HDD で 17 ～ 20 ミリ秒です。	重大なしきい値を超えた場合は、QoS ポリシーが割り当てられたストレージ VM のボリュームのしきい値制限を直ちに評価し、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、次の即時アクションを検討してください。1.アグリゲートの使用率も高い場合は、ストレージ 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たストレージ VM のボリュームについては、しきい値制限によってボリューム ワークロードが調整されるかどうかを評価します 3。ノードの使用率が高い場合は、ストレージVMの一部のボリュームを別のノードに移動する、またはノードの全体的なワークロードを削減します。
ユーザークォータファイルハード制限	重大	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、追加のファイルを作成できません。保存されているファイルの数を監視することで、ユーザーは中断のないデータ サービスを受けることができます。	重要な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即時の措置が必要です。…次の措置を検討してください。1.特定のユーザー 2 のファイル数クォータを増やします。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の負担を軽減します。

ユーザークォータファイルソフト制限	警告	ボリューム内に作成されたファイルの数がクォータのしきい値制限に達しており、重大な制限に近づいています。クォータが重大な制限に達した場合、追加のファイルを作成することはできません。ユーザーが保存するファイルの数を監視することで、ユーザーが中断のないデータ サービスを受けられるようになります。	警告しきい値を超えた場合は、直ちにアクションを検討してください。1. 特定のユーザー クォータ 2 のファイル数クォータを増やします。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の負担を軽減します。
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のうち、キャッシュから返されるのではなくディスクから返される要求の割合です。これは、音量が設定されたしきい値に達したことを意味します。	重要な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、直ちに措置を講じる必要があります。1. IO 負荷 2 を軽減するために、一部のワークロードをボリュームのノードから移動します。ボリュームのノードにまだない場合は、Flash Cache 3 を購入して追加し、 WAFLキャッシュを増やします。QoS 制限を使用して、同じノード上の優先度の低いワークロードの需要を下げます。警告しきい値を超えた場合は、直ちに次のアクションを検討してください。1. IO 負荷 2 を軽減するために、一部のワークロードをボリュームのノードから移動します。ボリュームのノードにまだない場合は、Flash Cache 3 を購入して追加し、 WAFLキャッシュを増やします。QoS 制限 4 を使用して、同じノード上の優先度の低いワークロードの需要を下げます。ワークロード特性の変更（ブロックサイズ、アプリケーションキャッシュなど）

ボリューム Qtree クォータ オーバーコミット	警告/重大	ボリューム 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見なされるパーセンテージを指定します。ボリュームの qtree クォータに設定されたしきい値に達しました。ボリューム qtree クォータのオーバーコミットを監視することで、ユーザーは中断のないデータ サービスを受けることができます。	重要な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、直ちに措置を講じる必要があります。1.ボリューム2のスペースを増やします。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

ログモニター

モニター名	重大度	説明	対処方法
AWS 認証情報が初期化されていません	情報	このイベントは、モジュールがクラウド資格情報スレッドから Amazon Web Services (AWS) Identity and Access Management (IAM) ロールベースの資格情報にアクセスしようとしたときに、資格情報が初期化される前に発生します。	クラウド資格情報スレッドとシステムの初期化が完了するまで待ちます。

クラウド層にアクセスできません	重大	ストレージ ノードは Cloud Tier オブジェクト ストア API に接続できません。一部のデータにアクセスできなくなります。	オンプレミス製品を使用している場合は、次の修正アクションを実行してください。…「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。…宛先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。…次の点を確認してください。…オブジェクト ストアの構成が変更されていないこと。…ログインおよび接続情報がまだ有効であること。…問題が解決しない場合は、 NetApp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、次の修正アクションを実行します。…オブジェクト ストアの構成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情報がまだ有効であることを確認してください。問題が解決しない場合は、 NetAppテクニカル サポートにお問い合わせください。
ディスクが使用不可	情報	このイベントは、ディスクが障害としてマークされた、サニタイズされている、またはメンテナンス センターに入ったためにサービスから削除されたときに発生します。	なし。

FlexGroup構成員全員	重大	FlexGroupボリューム内の構成要素がいっぱいなので、サービスが中断される可能性があります。FlexGroupボリューム上でファイルを作成または拡張することは可能です。ただし、構成要素に保存されているファイルは変更できません。その結果、 FlexGroupボリュームで書き込み操作を実行しようとすると、ランダムに領域不足エラーが発生す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お勧めします。または、 FlexGroupボリュームからファイルを削除します。ただし、どのファイルが構成要素に到達したかを判断するのは困難です。
Flexgroupの構成員がほぼ満員	警告	FlexGroupボリューム内の構成要素のスペースがほとんど不足しており、サービスが中断される可能性があります。ファイルの作成と展開が可能です。ただし、構成要素のスペースが不足すると、構成要素上のファイルに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お勧めします。または、 FlexGroupボリュームからファイルを削除します。ただし、どのファイルが構成要素に到達したかを判断するのは困難です。
FlexGroup構成要素の inode がほぼ不足しています	警告	FlexGroupボリューム内の構成要素の inode がほとんど不足しているため、サービスが中断される可能性があります。構成要素は平均よりも少ない作成要求を受け取ります。要求はより多くの inode を持つ構成要素にルーティングされるため、FlexGroupボリュームの全体的なパフォーマンスに影響す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お勧めします。または、 FlexGroupボリュームからファイルを削除します。ただし、どのファイルが構成要素に到達したかを判断するのは困難です。

FlexGroup構成要素の inode 不足	重大	FlexGroupボリュームの構成要素の inode が不足しており、サービスが中断される可能性があります。この構成要素に新しいファイルを作成することはできません。これにより、 FlexGroupボリューム全体でコンテンツの配分が全体的に不均衡に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お勧めします。または、 FlexGroupボリュームからファイルを削除します。ただし、どのファイルが構成要素に到達したかを判断するのは困難です。
LUN はオフライン	情報	このイベントは、LUN が手動でオフラインになったときに発生します。	LUN をオンラインに戻します。
本体ファンの故障	警告	メインユニットの 1 つ以上のファンが故障しました。システムは引き続き動作します。…ただし、この状態が長時間続くと、過熱により自動シャットダウンがトリガーされる可能性があります。	故障したファンを取り付け直してください。エラーが解決しない場合は交換してください。
本体ファンが警告状態	情報	このイベントは、メインユニットの 1 つ以上のファンが警告状態にある場合に発生します。	過熱を防ぐため、指定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バッテリー容量が極めて低くなっています。バッテリが切れると、データが失われる可能性があります。…システムは、 AutoSupportまたは「コール ホーム」メッセージを生成し、NetAppテクニカル サポートおよび設定された送信先（そのように設定されている場合は）に送信します。 AutoSupportメッセージが正常に配信されると、問題の特定と解決が大幅に改善されます。	次の修正アクションを実行してください。…「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、充電状態を表示します。…バッテリを最近交換した場合、またはシステムが長期間動作していなかった場合は、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ます。…バッテリのランタイムが引き続き危険なレベルを下回り、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、 NetAppテクニカル サポートに問い合わせてください。

サービス プロセッサが未設定	警告	このイベントは毎週発生し、サービス プロセッサ (SP) を構成するよう通知します。 SP は、リモート アクセスおよびリモート管理機能を提供するためにシステムに組み込まれる物理デバイスです。 SP のすべての機能を使用するには、 SPを構成する必要があります。	次の修正アクションを実行します。…「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がAutoSupport電子メールを送信できることを確認します。注: このコマンドを発行する前に、 ONTAPでAutoSupport電子メールホストと受信者を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	重大	すべてのSPリカバリアクションが実行されたにもかかわらず、 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なしではハードウェアの状態を監視できません。…ハードウェアの損傷とデータ損失を防ぐためにシステムはシャットダウンします。 SPがオフラインになった場合に直ちに通知されるパニックアラートを設定します。	次の操作を実行して、システムの電源を入れ直します。…コントローラをシャーシから引き出します。…コントローラを押し込みます。…コントローラの電源を入れ直します。…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。

棚ファンが故障しました	重大	シェルフの指定された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冷却気流が供給されず、ディスク障害が発生する可能性があります。	次の修正アクションを実行します。…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。注: 一部のディスク シェルフでは、ファンは電源モジュールに統合されています。…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、 NetAppテクニカル サポートにお問い合わせください。
本体ファンの故障によりシステムが動作不能	重大	1 つ以上のメインユニットファンが故障し、システムの動作が中断されました。これにより、データが失われる可能性があります。	故障したファンを交換してください。
未割り当てのディスク	情報	システムには未割り当てのディスクがあり、容量が無駄になっており、システムに誤った構成や部分的な構成変更が適用されている可能性があります。	次の修正アクションを実行します。…「disk show -n」コマンドを使用して、割り当てられていないディスクを特定します。…「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。
ウイルス対策サーバーがビジー状態です	警告	ウイルス対策サーバーがビジー状態のため、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発生する場合は、SVM によって生成されるウイルス スキャン負荷を処理できる十分なウイルス対策サーバーがあることを確認してください。

IAM ロールの AWS 認証情報が期限切れです	重大	Cloud Volume ONTAPにアクセスできなくなりました。 Identity and Access Management (IAM) のロールベースの認証情報の有効期限が切れました。認証情報は、IAM ロールを使用して Amazon Web Services (AWS) メタデータ サーバーから取得され、Amazon Simple Storage Service (Amazon S3) への API リクエストに署名するために使用されます。	以下の手順を実行します。…AWS EC2 マネジメント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デプロイメントのインスタンスを見つけて、そのヘルスを確認します。…インスタンスに関連付けられた AWS IAM ロールが有効であり、インスタンスに対する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 認証情報が見つかりません	重大	クラウド資格情報スレッドは、AWS メタデータ サーバーから Amazon Web Services (AWS) Identity and Access Management (IAM) ロールベースの資格情報を取得できません。認証情報は、Amazon Simple Storage Service (Amazon S3) への API リクエスト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。…	以下の手順を実行します。…AWS EC2 マネジメント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デプロイメントのインスタンスを見つけて、そのヘルスを確認します。…インスタンスに関連付けられた AWS IAM ロールが有効であり、インスタンスに対する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 認証情報が無効です	重大	Identity and Access Management (IAM) のロールベースの認証情報が無効です。認証情報は、IAM ロールを使用して Amazon Web Services (AWS) メタデータ サーバーから取得され、Amazon Simple Storage Service (Amazon S3) への API リクエスト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。	以下の手順を実行します。…AWS EC2 マネジメント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デプロイメントのインスタンスを見つけて、そのヘルスを確認します。…インスタンスに関連付けられた AWS IAM ロールが有効であり、インスタンスに対する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	重大	Identity and Access Management (IAM) ロール スレッドは、AWS メタデータ サーバーで Amazon Web Services (AWS) IAM ロールを見つけることができません。 Amazon Simple Storage Service (Amazon S3) への API リクエストに署名するために使用されるロールベースの認証情報を取得するには、IAM ロールが必要です。 Cloud Volume ONTAPにアクセスできなくなりました。…	次の操作を実行します。…AWS EC2 マネジメント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デプロイメントのインスタンスを見つけて、その正常性を確認します。…インスタンスに関連付けられた 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	重大	AWS メタデータ サーバーの 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。	以下の手順を実行します。…AWS EC2 マネジメント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デプロイメントのインスタンスを見つけて、そのヘルスを確認します。…インスタンスに関連付けられた AWS IAM ロールが有効であり、インスタンスに対する適切な権限が付与されていることを確認します。
AWS メタデータサーバーの接続失敗	重大	Identity and Access Management (IAM) ロール スレッドは、Amazon Web Services (AWS) メタデータ サーバーとの通信リンクを確立できません。 Amazon Simple Storage Service (Amazon S3) への API リクエストに署名するために使用される必要な AWS IAM ロールベースの認証情報を取得するための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。…	以下の手順を実行します。…AWS EC2 マネジメント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デプロイメントのインスタンスを見つけて、そのヘルスを確認します。…

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 プロバイダーからのオブジェクトストアのクラスター全体のFabricPoolスペース使用量の合計が、ライセンス制限にほぼ達しています。	次の修正アクションを実行します。…「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、階層化ポリシーが「snapshot」または「backup」であるボリュームから Snapshot コピーを削除し、スペースを解放します。…クラスターに新しいライセンスをインストールして、ライセンス容量を増やします。
FabricPool のスペース使用制限に達しました	重大	容量ライセンス プロバイダーからのオブジェクトストアのクラスタ全体のFabricPoolスペース使用量の合計がライセンス制限に達しました。	次の修正アクションを実行します。…「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、階層化ポリシーが「snapshot」または「backup」であるボリュームから Snapshot コピーを削除し、スペースを解放します。…クラスターに新しいライセンスをインストールして、ライセンス容量を増やします。

集計のギブバックに失敗しました	重大	このイベントは、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ているときに、宛先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。	次の修正アクションを実行します。…「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。…宛先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 ストアの構成が変更されておらず、ログインおよび接続情報が正確であることを確認してください。…または、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、 NetAppテクニカル サポートにお問い合わせください。

HA相互接続ダウン	警告	高可用性 (HA) 相互接続がダウンしています。フェイルオーバーが利用できない場合、サービス停止のリスクがあります。	修正アクションは、プラットフォームでサポートされている HA 相互接続リンクの数とタイプ、および相互接続がダウン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、および該当する場合は Small Form-Factor Pluggable (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、リンクを順番に無効にしてから再度有効にします。…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、リンクを順番に無効にしてから再度有効にします。…問題が解決しない場合は、 NetAppテクニカル サポートにお問い合わせください。

ユーザーあたりの最大セッション数を超えました	警告	TCP 接続でユーザーごとに許可されるセッションの最大数を超えました。いくつかのセッションが解放されるまで、セッションを確立する要求はすべて拒否されます。…	次の修正アクションを実行します。…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。…問題の原因が新しいアプリケーションか既存のアプリケーションかを確認します。…アプリケーションが新しい場合は、「cifs option modify -max-opens-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。場合によっては、クライアントは期待どおりに動作しますが、より高いしきい値が必要になります。クライアントに対してより高いしきい値を設定するには、高度な権限が必要です。 …問題が既存のアプリケーションによって発生している場合は、クライアントに問題がある可能性があります。詳細情報やサポートについては、 NetApp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 接続経由でファイルを開くことができる最大回数を超えました。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、このファイルを開く要求はすべて拒否されます。これは通常、異常なアプリケーションの動作を示します。…	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るアプリケーションを検査します。クライアント上で実行されているアプリケーションが原因で、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てください。…問題の原因が新しいアプリケーションか既存のアプリケーションかを確認してください。…アプリケーションが新しい場合は、「cifs option modify -max-opens-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てください。場合によっては、クライアントは期待どおりに動作しますが、より高いしきい値が必要になります。クライアントに対してより高いしきい値を設定するには、高度な権限が必要です。 …問題が既存のアプリケーションによって発生している場合は、クライアントに問題がある可能性があります。詳細情報やサポートについては、 NetAppテクニカルサポートにお問い合わせください。

NetBIOS名の競合	重大	NetBIOS ネーム サービスは、リモート マシンからの名前登録要求に対する否定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によって発生します。その結果、クライアントはデータにアクセスできないか、クラスター内の適切なデータ提供ノードに接続できない可能性があります。	次のいずれかの修正処置を実行してください。…NetBIOS 名またはエイリアスに競合がある場合は、次のいずれかを実行してください。…「vserver cifs delete -aliases alias -vserver vserver」コマンドを使用して、重複した 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、重複した名前を削除し、新しい名前のエイリアスを追加することで、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 名が競合している場合は、「vserver cifs delete -vserver vserver」および「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。注意: CIFS サーバーを削除すると、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 マシン上の NetBIOS の名前を変更します。
NFSv4 ストア プールが枯渇しました	重大	NFSv4 ストア プールが使い果たされました。	このイベント後、NFS サーバーが 10 分以上応答しない場合は、 NetApp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	重大	ウイルス対策コネクタは、登録済みのスキャンエンジンがないことをONTAP に通知しました。「スキャン必須」オプションが有効になっている場合、データが利用できなくなる可能性があります。	次の修正アクションを実行します。…ウイルス対策サーバ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されており、ローカル ループバックを介してウイルス対策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	重大	ONTAP には、ウイルススキャン要求を処理するための Vscan 接続がありません。「スキャン必須」オプションが有効になっている場合、データが利用できなくなる可能性があります。	スキャナ プールが適切に設定されており、ウイ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。
ノードルートボリュームの空き容量が少ない	重大	システムはルート ボリュームの空き容量が危険なほど少ないことを検出しました。ノードは完全には動作していません。データ LIF がクラスター内でフェイルオーバーした可能性があります。そのため、ノード上の NFS および CIFS アクセスが制限されています。管理機能は、ルート ボリューム上のスペースをクリアするためのノードのローカル回復手順に制限されます。	次の修正アクションを実行してください。…古いスナップショット コピーを削除するか、/mroot ディレクトリから不要になったファイルを削除するか、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解放します。…コントローラを再起動します。…詳細またはサポートについては、 NetAppテクニカル サポートにお問い合わせください。
管理者共有が存在しません	重大	Vscan の問題: 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。	指定された SVM ID に対して Vscan が有効になっていることを確認します。 SVM で Vscan を有効にすると、SVM に対して ONTAP_ADMIN$ 共有が自動的に作成されます。
NVMe名前空間のスペース不足	重大	スペース不足による書き込み失敗のため、NVMe 名前空間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 名前空間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) プロトコルが使用されており、ライセンスの猶予期間がアクティブな場合に毎日発生します。ライセンスの猶予期間が終了した後、NVMe-oF 機能にはライセンスが必要になります。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、それをクラスターに追加するか、クラスターから NVMe-oF 構成のすべてのインスタンスを削除してください。
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 機能が無効になっています。	営業担当者に連絡して NVMe-oF ライセンスを取得し、クラスターに追加してください。
NVMe-oF 猶予期間の開始	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) 構成が検出されました。ライセンスの猶予期間が終了した後、NVMe-oF 機能にはライセンスが必要になります。	営業担当者に連絡して NVMe-oF ライセンスを取得し、クラスターに追加してください。
オブジェクトストアホストが解決できません	重大	オブジェクト ストア サーバーのホスト名を IP アドレスに解決できません。オブジェクト ストア クライアントは、IP アドレスを解決しないとオブジェクト ストア サーバーと通信できません。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 構成をチェックして、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がダウンしています	重大	オブジェクト ストア クライアントは、オブジェクト ストア サーバーと通信するための動作可能な LIF を見つけることができません。インタークラスタ LIF が動作可能になるまで、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。	次の修正アクションを実行します。…「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の署名の不一致	重大	オブジェクト ストア サーバーに送信された要求署名が、クライアントによって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、 NetApp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	重大	READDIR ファイル操作が、 WAFLで実行でき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いか、またはディレクトリがまばらであるために発生する可能性があります。是正措置をお勧めします。	次の修正アクションを実行します。…次の「diag」権限ノードシェル CLI コマンドを使用して、READDIR ファイル操作の有効期限が切れ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 ファイルのスパース性を削除するために、ディレクトリの内容を新しいディレクトリにコピー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して、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。

集計の再配置に失敗しました	重大	このイベントは、集約の再配置中に、宛先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。	次の修正アクションを実行します。…「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。…宛先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 ストアの構成が変更されておらず、ログインおよび接続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。…詳細またはサポートについては、 NetApp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	重大	Microsoft Server のバックアップおよび復元サービス操作であるボリューム シャドウ コピー サービス (VSS) が失敗しました。	イベント メッセージに提供される情報を使用して、次の点を確認してください。…シャドウ コピー構成は有効になっていますか?…適切なライセンスがインストールされていますか? …シャドウ コピー操作はどの共有で実行されますか?…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ですか?

ストレージスイッチの電源が故障しました	警告	クラスタ スイッチに電源がありません。冗長性が低下し、さらなる停電で停電の危険が生じます。	次の修正アクションを実行してください。…クラスタ スイッチに電力を供給する電源装置のメイン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、 NetAppテクニカル サポートに問い合わせてください。
CIFS認証が多すぎる	警告	多くの認証ネゴシエーションが同時に発生しました。このクライアントからの不完全な新規セッション要求が 256 件あります。	クライアントが 256 個以上の新しい接続要求を作成した理由を調査します。エラーが発生した原因を特定するには、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る必要がある場合があります。
管理者共有への不正ユーザーアクセス	警告	ログインしているユーザーが許可されたユーザーではないにもかかわらず、クライアントは特権のある ONTAP_ADMIN$ 共有に接続しようとしました。	次の修正アクションを実行します。…指定されたユーザー名と 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。
ウイルスが検出されました	警告	Vscan サーバーがストレージ システムにエラーを報告しました。これは通常、ウイルスが見つかったことを示します。ただし、Vscan サーバー上の他のエラーがこのイベントの原因となる場合があります。…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 サーバーは、設定と構成に応じて、ファイルを消去したり、隔離したり、削除したりする場合があります。	「syslog」イベントで報告された Vscan サーバーのログをチェックして、感染したファイルを正常にクリーンアップ、隔離、または削除できたかどうかを確認します。それができなかった場合、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可能性があります。

ボリュームはオフライン	情報	このメッセージは、ボリュームがオフラインになっていることを示します。	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	情報	このイベントは、フレキシブル ボリュームが制限されたことを示します。	ボリュームをオンラインに戻します。
ストレージ VM の停止に成功しました	情報	このメッセージは、「vserver stop」操作が成功したときに表示されます。	'vserver start' コマンドを使用して、ストレージ VM 上のデータ アクセスを開始します。
ノードパニック	警告	このイベントはパニックが発生したときに発行されます	NetApp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ー

モニター名	重大度	説明	対処方法
ストレージ VM のランサムウェア対策監視が無効	警告	ストレージ VM のランサムウェア対策監視が無効になっています。ランサムウェア対策を有効にして、ストレージ VM を保護します。	なし
ストレージ VM のランサムウェア対策監視が有効 (学習モード)	情報	ストレージ VM のランサムウェア対策監視が学習モードで有効になっています。	なし
ボリュームランサムウェア対策監視が有効	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ます。	なし
ボリュームランサムウェア対策監視が無効	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。ボリュームを保護するためにランサムウェア対策を有効にします。	なし
ボリュームランサムウェア対策監視が有効（学習モード）	情報	ボリュームのランサムウェア対策監視が学習モードで有効になっています。	なし
ボリュームランサムウェア対策監視の一時停止（学習モード）	警告	ボリュームのランサムウェア対策監視は学習モードで一時停止されています。	なし

ボリュームランサムウェア対策監視の一時停止	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
ボリュームランサムウェア対策監視の無効化	警告	ボリュームのランサムウェア対策監視が無効になっています。	なし
ランサムウェア活動が検出されました	重大	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、元のデータを復元するために使用できるスナップショット コピーが作成されました。システムはAutoSupportまたは「コール ホーム」メッセージを生成し、 NetAppテクニカル サポートおよび設定された送信先に送信します。 AutoSupportメッセージにより、問題の特定と解決が向上します。	ランサムウェア活動に対する是正措置を講じるには、「FINAL-DOCUMENT-NAME」を参照してください。

トップに戻る

NetApp ONTAPモニターの **FSx**

モニター名	しきい値	モニターの説明	対処方法
FSxボリュームの容量がいっぱいです	警告 @ > 85 %…重大 @ > 95 %	アプリケーションと顧客データを保存するには、ボリュームのストレージ容量が必要です。 ONTAPボリュームに保存されるデータが増えるほど、将来のデータのストレージ可用性は低下します。ボリューム内のデータ保存容量が合計保存容量に達した場合、保存容量不足によりお客様がデータを保存できなくなる可能性があります。使用されたボリュームのストレージ容量を監視することで、データ サービスの継続性が確保されます。	重要な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、直ちにアクションを実行する必要があります。…1.スペースを空けるために、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ボリュームの高レイテンシー	警告 @ > 1000 µs…重大 @ > 2000 µs	ボリュームは、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が重視されるアプリケーションによって発生することが多い IO トラフィックを処理するオブジェクトです。大量の待ち時間が発生すると、アプリケーション自体に問題が発生し、タスクを完了できなくなる可能性があります。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ためには、ボリュームのレイテンシを監視することが重要です。	重要な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、直ちにアクションを実行する必要があります。…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調整される原因にならないように、その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、すぐに次のアクションを実行するように計画します:…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調整される原因にならないように、その制限しきい値を評価します。…2.ノードの使用率も高い場合は、ボリュームを別のノードに移動する、またはノードの合計ワークロードを削減します。

FSxボリュームのiノード制限	警告 @ > 85 %…重大 @ > 95 %	ファイルを保存するボリュームは、インデックスノード (inode) を使用してファイルのメタデータを保存します。ボリュームの inode 割り当てを使い果たすと、それ以上のファイルを追加できなくなります。警告アラートは、利用可能な inode の数を増やす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。重大なアラートは、ファイル制限の枯渇が差し迫っており、サービスの継続性を確保するために、iノードを解放するための緊急措置を講じる必要があることを示します。	重要な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、直ちにアクションを実行する必要があります。…1.ボリュームの inode 値を増やすことを検討してください。 inode 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……警告しきい値を超えた場合は、すぐに次のアクションを実行するように計画してください:…1.ボリュームの inode 値を増やすことを検討してください。 inode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。
FSx ボリューム Qtree クォータ オーバーコミット	警告 @ > 95 %…重大 @ > 100 %	ボリューム 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見なされるパーセンテージを指定します。ボリュームの qtree クォータに設定されたしきい値に達しました。ボリューム qtree クォータのオーバーコミットを監視することで、ユーザーは中断のないデータ サービスを受けることができます。	重要な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、直ちに措置を講じる必要があります。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、ボリュームのスペースを増やすことを検討してください。

FSxスナップショットの予約スペースがいっぱいです	警告 @ > 90 %…重大 @ > 95 %	アプリケーションと顧客データを保存するには、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その領域の一部は、データをローカルで保護できるようにするスナップショットを保存するために使用されます。ONTAPボリュームに保存される新規データや更新データが増えるほど、使用されるスナップショット容量が増え、将来の新規データや更新データに使用できるスナップショット ストレージ容量は少なくなります。ボリューム内のスナップショットデータ容量が合計スナップショット予約領域に達すると、顧客が新しいスナップショット データを保存できなくなり、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スナップショット容量を監視することで、データ サービスの継続性が確保されます。	重要な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、直ちにアクションを実行する必要があります。…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構成することを検討してください…2.スペースを解放するために、不要になった可能性のある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は、すぐに次のアクションを実行するように計画してください:…1.成長に対応するためにボリューム内のスナップショット予約領域を増やすことを検討してください…2.スナップショットの予約領域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構成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 %…重大 @ > 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のうち、キャッシュから返されるのではなくディスクから返される要求の割合です。これは、音量が設定されたしきい値に達したことを意味します。	重要な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、直ちに措置を講じる必要があります。1. IO 負荷 2 を軽減するために、一部のワークロードをボリュームのノードから移動します。 QoS 制限を使用して、同じノード上の優先度の低いワークロードの需要を下げます…警告しきい値を超えた場合は、直ちにアクションを検討してください。1. IO 負荷 2 を軽減するために、一部のワークロードをボリュームのノードから移動します。 QoS 制限 3 を使用して、同じノード上の優先度の低いワークロードの需要を下げます。ワークロード特性の変更（ブロックサイズ、アプリケーションキャッシュなど）

トップに戻る

K8sモニター

モニター名	説明	対処方法	重大度/閾値

永続ボリュームのレイテンシが高い	永続ボリュームのレイテンシが高いということは、アプリケーション自体に問題が発生し、タスクを完了できなくなる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ためには、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 タイプに基づいて予想されるレイテンシは次のとおりです - SSD 最大 1 ～ 2 ミリ秒、SAS 最大 8 ～ 10 ミリ秒、SATA HDD 17 ～ 20 ミリ秒。	即時アクション 重要な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即時アクション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となっていないか、その制限しきい値を評価します。 すぐに行うべきアクション 警告しきい値を超えた場合は、次の即時アクションを計画してください。1.ストレージ プールの使用率も高い場合は、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は、ボリュームのワークロードが調整される原因にならないように、その制限しきい値を評価します。3.コントローラの使用率も高い場合は、ボリュームを別のコントローラに移動する、またはコントローラの全体的なワークロードを減らします。	警告 @ > 6,000 µs 重大 @ > 12,000 µs
クラスタメモリ飽和度が高い	クラスターの割り当て可能なメモリの飽和度が高くなっています。クラスターの CPU 飽和度は、メモリ使用量の合計をすべての K8s ノード全体の割り当て可能なメモリの合計で割って計算されます。	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。ポッドのサイズを適正化してノード上のメモリを解放します。	警告 @ > 80 % 重大 @ > 90 %
POD接続に失敗しました	このアラートは、POD を使用したボリューム接続が失敗したときに発生します。		警告

高い再送信率	高いTCP再送信率	ネットワークの輻輳をチェックする - 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 使用率が高くないか確認します。ハードウェアのネットワーク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高	ノードファイルシステム容量高	- アプリケーション ファイルに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増やします。 - アプリケーション ファイルの使用量を減らします。	警告 @ > 80 % 重大 @ > 90 %
ワークロードネットワークジッター高	高い TCP ジッタ (高いレイテンシ/応答時間の変動)	ネットワークの混雑を確認します。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 使用率が高くないか確認します。ハードウェアネットワークのパフォーマンスを確認する	警告 @ > 30 ms 重大 @ > 50 ms

永続ボリュームのスループット	永続ボリュームの MBPS しきい値を使用すると、永続ボリュームが事前定義されたパフォーマンスの期待値を超え、他の永続ボリュームに影響を及ぼす可能性がある場合に管理者に警告することができます。このモニターを有効にすると、SSD 上の永続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。このモニターは、テナント上のすべての永続ボリュームをカバーします。このモニターを複製し、ストレージ クラスに適したしきい値を設定することで、監視目標に基づいて警告および重大なしきい値を調整できます。複製されたモニターは、テナント上の永続ボリュームのサブセットをさらにターゲットにすることができます。	即時のアクション 重要な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即時のアクションを計画します。1.ボリュームに QoS MBPS 制限を導入します。2.ボリューム上のワークロードを実行しているアプリケーションに異常がないか確認します。すぐに行うべきアクション 警告しきい値を超えた場合は、次の即時アクションを実行するように計画してください。1.ボリュームに QoS MBPS 制限を導入します。2.ボリューム上のワークロードを実行しているアプリケーションに異常がないか確認します。	警告 @ > 10,000 MB/s 重大 @ > 15,000 MB/s
OOM になる危険性のあるコンテナが強制終了される	コンテナのメモリ制限が低すぎます。コンテナは、排除される危険があります (メモリ不足による強制終了)。	コンテナのメモリ制限を増やします。	警告 @ > 95 %
作業負荷の減少	ワークロードには正常なポッドがありません。		クリティカル @ < 1
永続ボリュームの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ときに発生します。		警告
リソースクォータのメモリ制限を超過します	名前空間のメモリ制限が ResourceQuota を超えようとしています		警告 @ > 80 % 重大 @ > 90 %
リソースクォータメモリ要求が超過しそうです	名前空間のメモリ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 %
ノードの作成に失敗しました	構成エラーのため、ノードをスケジュールできませんでした。	構成失敗の原因については、Kubernetes イベントログを確認してください。	致命的
永続ボリュームの再利用に失敗しました	ボリュームの自動再利用が失敗しました。		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。コンテナのプロセスが遅くなります。	コンテナの CPU 制限を増やします。	警告 @ > 95 % 重大 @ > 98 %
サービス ロードバランサの削除に失敗しました			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定義されたパフォーマンス期待値を超えたときに管理者に警告することができます。このモニターを有効にすると、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。このモニターは、テナント上のすべての永続ボリュームをカバーします。このモニターを複製し、ワークロードに適したしきい値を設定することで、監視目標に基づいて警告および重大しきい値を調整できます。	即時のアクション 重要な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即時のアクションを計画します。1.ボリュームに QoS IOPS 制限を導入します。2.ボリューム上のワークロードを実行しているアプリケーションに異常がないか確認します。すぐに行うべきアクション 警告しきい値を超えた場合は、次の即時アクションを計画してください。1.ボリュームに QoS IOPS 制限を導入します。2.ボリューム上のワークロードを実行しているアプリケーションに異常がないか確認します。	警告 @ > 20,000 IO/s 重大 @ > 25,000 IO/s
サービス ロードバランサの更新に失敗しました			警告
PODマウント失敗	このアラートは、POD でのマウントが失敗したときに発生します。		警告
ノードPID圧力	(Linux) ノード上の使用可能なプロセス ID が、削除しきい値を下回りました。	多く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見つけて修正します。過剰なプロセスを生成するポッドまたはコンテナからノードを保護するには、PodPidsLimit を設定します。	クリティカル @ > 0

ポッドイメージのプル失敗	Kubernetes はポッド コンテナ イメージのプルに失敗しました。	- ポッド構成でポッドのイメージが正しく入力されていることを確認します。 - レジストリにイメージタグが存在することを確認します。 - イメージ レジストリの資格情報を確認します。 - レジストリ接続の問題がないか確認します。 - パブリック レジストリ プロバイダーによって課せら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る	ジョブの実行時間が長すぎます		1時間以上で警告、5時間以上で重大
ノードメモリ高	ノードのメモリ使用量が高い	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。ポッドのサイズを適正化してノード上のメモリを解放します。	警告 @ > 85 % 重大 @ > 90 %
リソースクォータCPU制限を超過しそうです	名前空間の CPU 制限が ResourceQuota 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、複数回再起動を試行しました。		クリティカル @ > 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。ポッドのサイズを適正化して、ノード上の CPU を解放します。	警告 @ > 80 % 重大 @ > 90 %
ワークロードネットワーク遅延RTT高	TCP RTT（ラウンドトリップタイム）の遅延が高い	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 使用率が高くないか確認します。ハードウェアのネットワークパフォーマンスを確認します。	警告 @ > 150 ms 重大 @ > 300 ms
ジョブが失敗しました	ノードのクラッシュまたは再起動、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失敗のため、ジョブは正常に完了しませんでした。	Kubernetes イベント ログで失敗の原因を確認します。	警告 @ > 1

数日で永続ボリュームがいっぱいになる	永続ボリュームの容量は数日で不足します	- アプリケーション ファイルに十分なスペースを確保するためにボリューム サイズを増やします。 - アプリケーションに保存されるデータの量を削減します。	警告 @ < 8日 重大 @ < 3日
ノードメモリの圧力	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。ポッドのサイズを適正化してノード上のメモリを解放します。	クリティカル @ > 0
ノードが準備完了ではありません	ノードは5分間準備されていません	ノードに十分な CPU、メモリ、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ます。Kubernetes イベント ログで失敗の原因を確認します。	クリティカル @ < 1
永続ボリューム容量大	永続ボリュームのバックエンドの使用容量が高くなっています。	- アプリケーション ファイルに十分なスペースを確保するためにボリューム サイズを増やします。 - アプリケーションに保存されるデータの量を減らします。	警告 @ > 80 % 重大 @ > 90 %
サービス ロードバランサの作成に失敗しました	サービス ロードバランサの作成に失敗しました		致命的
ワークロードレプリカの不一致	一部のポッドは現在、デプロイメントまたは DaemonSet で使用できません。		警告 @ > 1
リソースクォータCPU要求が超過しそうです	名前空間の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 %
高い再送信率	高いTCP再送信率	ネットワークの輻輳をチェックする - 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 使用率が高くないか確認します。ハードウェアのネットワーク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 システムのいずれかで使用可能なディスク領域と inode が、削除しきい値を満たしました。	- アプリケーション ファイルに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増やします。 - アプリケーション ファイルの使用量を減らします。	クリティカル @ > 0
クラスターCPU飽和度が高い	クラスターの割り当て可能な CPU 飽和度が高くなっています。クラスターの CPU 飽和度は、CPU 使用量の合計をすべての K8s ノード全体の割り当て可能な CPU の合計で割って計算されます。	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。ポッドのサイズを適正化して、ノード上の CPU を解放します。	警告 @ > 80 % 重大 @ > 90 %

トップに戻る

変更ログモニター

モニター名	重大度	モニターの説明
内部ボリュームを発見	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発生します。
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ときに発生します。
ストレージノードが検出されました	情報	このメッセージは、ストレージ ノードが検出されたときに表示されます。
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ときに表示されます。
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ときに表示されます。
ストレージ仮想マシンが検出されました	情報	このメッセージは、ストレージ仮想マシンが検出されたときに表示されます。
ストレージ仮想マシンが変更されました	情報	このメッセージは、ストレージ仮想マシンが変更されたときに発生します。

トップに戻る

データ収集モニター

モニター名	説明	対処方法

買収ユニットのシャットダウン	Data Infrastructure Insights取得ユニットは、新しい機能を導入するために、アップグレードの一環として定期的に再起動されます。通常の環境では、これは月に 1 回以下発生します。取得ユニットがシャットダウンしたという警告アラートの直後には、新しく再起動された取得ユニットがData Infrastructure Insightsへの登録を完了したことを通知する解決策が続く必要があります。通常、このシャットダウンから登録までのサイクルには 5 〜 15 分かかります。	アラートが頻繁に発生する場合、または 15 分以上続く場合は、Acquisition Unit をホストするシステム、ネットワーク、および AU をインターネットに接続しているプロキシの動作を確認してください。
コレクターが失敗しました	データ コレクターのポーリングで予期しない障害状況が発生しました。	状況の詳細については、 Data Infrastructure Insightsのデータ コレクター ページをご覧ください。
コレクターの警告	このアラートは通常、データ コレクターまたはターゲット システムの構成が誤っているために発生する可能性があります。今後のアラートを防ぐために構成を見直してください。また、データ収集者が収集可能なすべてのデータを収集したにもかかわらず、不完全なデータを取得したことが原因である可能性もあります。これは、データ収集中に状況が変化した場合に発生する可能性があります (たとえば、データ収集の開始時に存在していた仮想マシンが、データ収集中、データがキャプチャされる前に削除された場合など)。	データ コレクターまたはターゲット システムの構成を確認します。コレクター警告のモニターは他のモニター タイプよりも多くのアラートを送信する可能性があるので、トラブルシューティングを行わない限り、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ー

モニター名	しきい値	モニターの説明	対処方法

AutoSupport HTTPS 転送が無効	警告 @ < 1	AutoSupportは、転送プロトコルとしてHTTPS、HTTP、およびSMTPをサポートします。AutoSupportメッセージは機密性が高いため、NetAppでは、NetAppサポートにAutoSupportメッセージを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メッセージのトランスポートプロトコルとして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 のクラスタ安全でない暗号	警告 @ < 1	SSH が安全でない暗号 (例: *cbc で始まる暗号) を使用し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
クラスターログインバナーが無効です	警告 @ < 1	ONTAPシステムにアクセスするユーザーに対してログイン 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、システムへのアクセスと使用に関する期待を確立するのに役立ちます。	クラスタの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 "Access limited to authorized users"
クラスタ ピア通信が暗号化されていない	警告 @ < 1	ディザスタ リカバリ、キャッシュ、またはバックアップの目的でデータをレプリケートする場合は、あるONTAPクラスタから別のONTAPクラスタへの転送時にそのデータを保護する必要があります。暗号化は、ソース クラスターと宛先クラスターの両方で構成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。次に、「cluster peer modify」コマンドを使用して、ソース クラスタ ピアと宛先クラスタ ピアの両方がクラスタ ピアリング暗号化を使用するように変更します。詳細については、『 NetAppセキュリティ強化ガイド for ONTAP 9』を参照してください。

デフォルトのローカル管理ユーザが有効	警告 @ > 0	NetApp、lock コマンドを使用して、不要なデフォルトの管理者ユーザー (組み込み) アカウントをロック (無効化) することを推奨しています。これらは主に、パスワードが更新または変更されたことのないデフォルトのアカウントです。	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	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への準拠が有効な場合、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準拠を有効にするには、次のONTAPコマンドを詳細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	情報の流出を単一のシステムまたはソリューションに限定するためには、syslog情報をオフロードする必要があります。そのため、syslog情報を安全な保管場所にオフロードすることを推奨します。	ログ転送先を作成したら、その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ハッシュパスワード	警告 @ > 0	NetApp、 ONTAPユーザー アカウント 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強くお勧めします。安全性の低い MD5 ハッシュ関数を使用しているアカウントは、SHA-512 ハッシュ関数に移行する必要があります。	NetAppは、ユーザーにパスワードを変更させることで、ユーザーアカウントをより安全なSHA-512ソリューションに移行することを強く推奨しています。…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サーバーが設定されていません	警告 @ < 1	クラスターに NTP サーバーが構成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確保するために、 NetApp少なくとも 3 台の NTP サーバーをクラスタに関連付けることを推奨しています。	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>
NTP サーバ数が不足しています	警告 @ < 3	クラスターに構成されている NTP サーバーが 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確保するために、NetApp少なくとも 3 台の NTP サーバーをクラスタに関連付けることを推奨しています。	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サーバのホスト名またはIPアドレス>
リモートシェルが有効	警告 @ > 0	リモート シェルは、ONTAPソリューションへのコマンド ライン アクセスを確立するための安全な方法ではありません。安全なリモート アクセスを実現するには、リモート シェルを無効にする必要があります。	NetAppは、安全なリモートアクセスのためにセキュアシェル（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、次のONTAPコマンドを高度な権限モードで実行します。…security protocol modify -application rsh-enabled false
ストレージ VM 監査ログが無効	警告 @ < 1	SVM の監査ログが無効になっていることを示します。	Vserver 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>
ストレージ VM SSH の安全でない暗号	警告 @ < 1	SSH が安全でない暗号 (例: *cbc で始まる暗号) を使用し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
ストレージ VM ログインバナーが無効になっています	警告 @ < 1	システム上の SVM にアクセスするユーザーに対してログイン 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、システムへのアクセスと使用に関する期待を確立するのに役立ちます。	クラスタの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 "Access limited to authorized users"

Telnet プロトコルが有効	警告 @ > 0	Telnet は、 ONTAPソリューションへのコマンドライン アクセスを確立するための安全な方法ではありません。安全なリモート アクセスのために、Telnet を無効にする必要があります。	セキュアなリモート アクセスを確立するために、Secure Shell（SSH）を推奨します。クラスタ上でTelnetを無効にするには、次のONTAPコマンドを詳細権限モードで実行します。…security protocol modify -application telnet -enabled false

トップに戻る

データ保護モニター

モニター名	しきい値	モニターの説明	対処方法
LUNスナップショットコピー用のスペースが不足しています	(フィルター contains_luns = Yes) 警告 @ > 95 %… 重大 @ > 100 %	アプリケーションと顧客データを保存するには、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その領域の一部は、データをローカルで保護できるようにするスナップショットを保存するために使用されます。ONTAPボリュームに保存される新規データや更新データが増えるほど、使用されるスナップショット容量が増え、将来の新規データや更新データに使用できるスナップショット ストレージ容量は少なくなります。ボリューム内のスナップショット データ容量が合計スナップショット予約領域に達すると、顧客が新しいスナップショット データを保存できなくなり、ボリューム内の LUN 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スナップショット容量を監視することで、データ サービスの継続性が確保されます。	即時のアクション 重要な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、即時のアクション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内のデータ領域を使用するようにスナップショットを構成します。2.古くて不要なスナップショットをいくつか削除して、スペースを解放します。 すぐに行うべきアクション 警告しきい値を超えた場合は、次の即時アクションを実行するように計画してください。1.成長に対応するために、ボリューム内のスナップショット予約領域を増やします。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構成します。

SnapMirror関係の遅延	警告 @ > 150%…重大 @ > 300%	SnapMirror関係の遅延は、スナップショットのタイムスタンプと宛先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_percent は 100% になります。SnapMirrorポリシーにスケジュールがない場合、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の転送履歴を確認します。

トップに戻る

クラウドボリューム（**CVO**）モニター

モニター名	CIの重症度	モニターの説明	対処方法
CVO ディスクがサービス停止中	情報	このイベントは、ディスクが障害としてマークされた、サニタイズされている、またはメンテナンス センターに入ったためにサービスから削除されたときに発生します。	なし

ストレージプールの CVO ギブバックに失敗しました	重大	このイベントは、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ているときに、宛先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。	次の修正アクションを実行します。「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。宛先ノードのクラスタ間 LIF 経由で「ping」コマンドを使用して、オブジェクト ストア サーバー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 ストアの構成が変更されておらず、ログインおよび接続情報がまだ正確であることを確認します。あるいは、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。詳細情報やサポートについては、 NetAppテクニカル サポートにお問い合わせください。

CVO HA相互接続ダウン	警告	高可用性 (HA) 相互接続がダウンしています。フェイルオーバーが利用できない場合、サービス停止のリスクがあります。	修正アクションは、プラットフォームでサポートされている HA 相互接続リンクの数とタイプ、および相互接続がダウン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、および該当する場合は Small Form-Factor Pluggable (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。内部的に接続されたリンクの場合は、「ic link off」コマンドと「ic link on」コマンドを使用して、リンクを順番に無効にしてから再度有効にします。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、リンクを順番に無効にしてから再度有効にします。問題が解決しない場合は、 NetAppテクニカル サポートにお問い合わせください。

ユーザーあたりの CVO 最大セッション数を超えました	警告	TCP 接続でユーザーごとに許可されるセッションの最大数を超えました。いくつかのセッションが解放されるまで、セッションを確立する要求はすべて拒否されます。	次の修正アクションを実行します。クライアントで実行され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。クライアントをリブートします。問題の原因が新しいアプリケーションか既存のアプリケーションかを確認します。アプリケーションが新しい場合は、「cifs option modify -max-opens-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。場合によっては、クライアントは期待どおりに動作しますが、より高いしきい値が必要になります。クライアントに対してより高いしきい値を設定するには、高度な権限が必要です。問題が既存のアプリケーションによって発生している場合は、クライアントに問題がある可能性があります。詳細情報やサポートについては、NetApp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	重大	NetBIOS ネーム サービスは、リモート マシンからの名前登録要求に対する否定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によって発生します。その結果、クライアントはデータにアクセスできないか、クラスター内の適切なデータ提供ノードに接続できない可能性があります。	次のいずれかの修正アクションを実行します。NetBIOS 名またはエイリアスに競合がある場合は、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、重複した NetBIOS エイリアスを削除します。重複した名前を削除し、「vserver cifs create -aliases alias -vserver vserver」コマンドを使用して新しい名前のエイリアスを追加することで、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 名が競合している場合は、「vserver cifs delete -vserver vserver」および「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。注意: CIFS サーバーを削除すると、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 マシン上の NetBIOS の名前を変更します。
CVO NFSv4 ストア プールが枯渇しました	重大	NFSv4 ストア プールが使い果たされました。	このイベント後、NFS サーバーが 10 分以上応答しない場合は、 NetAppテクニカル サポートにお問い合わせください。
CVOノードパニック	警告	このイベントはパニックが発生したときに発行されます	NetAppカスタマー サポートにお問い合わせください。

CVOノードルートボリュームスペース不足	重大	システムはルート ボリュームの空き容量が危険なほど少ないことを検出しました。ノードは完全には動作していません。データ LIF がクラスター内でフェイルオーバーした可能性があります。そのため、ノード上の NFS および CIFS アクセスが制限されています。管理機能は、ルート ボリューム上のスペースをクリアするためのノードのローカル回復手順に制限されます。	次の修正アクションを実行します。古いスナップショット コピーを削除するか、/mroot ディレクトリから不要になったファイルを削除するか、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解放します。コントローラーを再起動します。詳細情報やサポートについては、NetAppテクニカル サポートにお問い合わせください。
CVO 存在しない管理者共有	重大	Vscan の問題: 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。	指定された SVM ID に対して Vscan が有効になっていることを確認します。 SVM で Vscan を有効にすると、SVM に対して 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 ホストが解決できません	重大	オブジェクト ストア サーバーのホスト名を IP アドレスに解決できません。オブジェクト ストア クライアントは、IP アドレスを解決しないとオブジェクト ストア サーバーと通信できません。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 構成をチェックして、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 インタークラスタ LIF ダウン	重大	オブジェクト ストア クライアントは、オブジェクト ストア サーバーと通信するための動作可能な LIF を見つけることができません。インタークラスタ LIF が動作可能になるまで、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。	次の修正アクションを実行します。「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。

CVO オブジェクト ストア署名の不一致	重大	オブジェクト ストア サーバーに送信された要求署名が、クライアントによって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、 NetAppテクニカル サポートにお問い合わせください。
CVO QoS モニターのメモリが上限に達しました	重大	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 ハードウェアの限界に達しました。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。	アクティブなワークロードまたはストリームをいくつか削除して、メモリを解放します。「statistics show -object workload -counter ops」コマンドを使用して、どのワークロードがアクティブであるかを確認します。アクティブなワークロードにはゼロ以外の操作が表示されます。次に、「workload delete <workload_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付けられているストリームを削除します。

CVO READDIR タイムアウト	重大	READDIR ファイル操作が、 WAFLで実行でき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いか、またはディレクトリがまばらであるために発生する可能性があります。是正措置をお勧めします。	次の修正アクションを実行します。次の「diag」権限ノードシェル CLI コマンドを使用して、READDIR ファイル操作の有効期限が切れた最近のディレクトリに固有の情報を検索します: wafl readdir notification show。ディレクトリがスパースとして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 ファイルのスパース性を解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して、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。

CVO ストレージ プールの再配置に失敗しました	重大	このイベントは、集約の再配置中に、宛先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。	次の修正アクションを実行します。「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。宛先ノードのクラスタ間 LIF 経由で「ping」コマンドを使用して、オブジェクト ストア サーバー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 ストアの構成が変更されておらず、ログインおよび接続情報がまだ正確であることを確認します。あるいは、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。詳細情報やサポートについては、 NetAppテクニカル サポートにお問い合わせください。
CVO シャドウコピーに失敗しました	重大	Microsoft Server のバックアップおよび復元サービス操作であるボリューム シャドウ コピー サービス (VSS) が失敗しました。	イベント メッセージに提供される情報を使用して、次の点を確認します。シャドウ コピー構成は有効になっていますか? 適切なライセンスがインストールされていますか? シャドウ コピー操作はどの共有で実行されますか? 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?
CVO ストレージ VM の停止に成功しました	情報	このメッセージは、「vserver stop」操作が成功したときに表示されます。	'vserver start' コマンドを使用して、ストレージ VM 上のデータ アクセスを開始します。

CVO CIFS 認証が多すぎる	警告	多くの認証ネゴシエーションが同時に発生しました。このクライアントからの不完全な新規セッション要求が 256 件あります。	クライアントが 256 個以上の新しい接続要求を作成した理由を調査します。エラーが発生した原因を特定するには、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る必要がある場合があります。
CVO 未割り当てディスク	情報	システムには未割り当てのディスクがあり、容量が無駄になっており、システムに誤った構成や部分的な構成変更が適用されている可能性があります。	次の修正アクションを実行します。「disk show -n」コマンドを使用して、割り当てられていないディスクを特定します。「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ユーザーアクセス	警告	ログインしているユーザーが許可されたユーザーではないにもかかわらず、クライアントは特権のある ONTAP_ADMIN$ 共有に接続しようとしました。	次の修正アクションを実行します。指定されたユーザー名と IP アドレスがアクティブな Vscan スキャナー 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 プールの構成を確認します。
CVOウイルスが検出されました	警告	Vscan サーバーがストレージ システムにエラーを報告しました。これは通常、ウイルスが見つかったことを示します。ただし、Vscan サーバー上の他のエラーによってこのイベントが発生する場合があります。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 サーバーは、設定と構成に応じて、ファイルを消去したり、隔離したり、削除したりする場合があります。	「syslog」イベントで報告された Vscan サーバーのログをチェックして、感染したファイルを正常にクリーンアップ、隔離、または削除できたかどうかを確認します。それができなかった場合、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可能性があります。
CVOボリュームオフライン	情報	このメッセージは、ボリュームがオフラインになっていることを示します。	ボリュームをオンラインに戻します。

CVO ボリューム制限	情報	このイベントは、フレキシブル ボリュームが制限されたことを示します。	ボリュームをオンラインに戻します。

トップに戻る

SnapMirror for Business Continuity (SMBC) メディエーター ログ モニター

モニター名	重大度	モニターの説明	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 Mediator がクラスタに正常に追加されたときに表示されます。	なし
ONTAPメディエーターにアクセスできません	重大	このメッセージは、ONTAP Mediator が再利用されたか、Mediator パッケージが Mediator サーバーにインストールされなくなった場合に表示されます。その結果、SnapMirrorフェイルオーバーは不可能になります。	「snapmirror mediator remove」コマンドを使用して、現在のONTAP Mediator の設定を削除します。 「snapmirror mediator add」コマンドを使用して、 ONTAP Mediator 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 Mediator がクラスタから正常に削除されたときに表示されます。	なし
ONTAPメディエーターにアクセスできません	警告	このメッセージは、クラスタ上でONTAP Mediatorにアクセスできない場合に表示されます。その結果、 SnapMirrorフェイルオーバーは不可能になります。	「network ping」および「network traceroute」コマンドを使用して、ONTAP Mediator へのネットワーク接続を確認します。問題が解決しない場合は、「snapmirror mediator remove」コマンドを使用して、現在のONTAP Mediator の設定を削除します。 「snapmirror mediator add」コマンドを使用して、 ONTAP Mediator 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ました	重大	このメッセージは、ONTAP Mediator 証明機関 (CA) 証明書の有効期限が切れたときに表示されます。その結果、 ONTAP Mediator への以降の通信はすべてできなくなります。	「snapmirror mediator remove」コマンドを使用して、現在のONTAP Mediator の設定を削除します。 ONTAP Mediator サーバー上の新しい CA 証明書を更新します。「snapmirror mediator add」コマンドを使用して、 ONTAP Mediator へのアクセスを再設定します。
SMBC CA証明書の有効期限切れ	警告	このメッセージは、ONTAP Mediator の証明機関 (CA) 証明書の有効期限が 30 日以内に切れる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 Mediator の設定を削除します。 ONTAP Mediator サーバー上の新しい CA 証明書を更新します。 「snapmirror mediator add」コマンドを使用して、 ONTAP Mediator 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ました	重大	このメッセージは、ONTAP Mediator クライアント証明書の有効期限が切れたときに表示されます。その結果、 ONTAP Mediator への以降の通信はすべてできなくなります。	「snapmirror mediator remove」コマンドを使用して、現在のONTAP Mediator の設定を削除します。 「snapmirror mediator add」コマンドを使用して、 ONTAP Mediator 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切れ	警告	このメッセージは、ONTAP Mediator クライアント証明書の有効期限が 30 日以内に切れる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 Mediator の設定を削除します。「snapmirror mediator add」コマンドを使用して、 ONTAP Mediator へのアクセスを再設定します。

SMBC関係の同期が取れていない注:UMにはこれがありません	重大	このメッセージは、SnapMirror for Business Continuity (SMBC) 関係のステータスが「同期中」から「非同期」に変更されたときに表示されます。このため、RPO=0 のデータ保護は中断されます。	ソースボリュームと宛先ボリューム間のネットワーク接続を確認します。宛先では「snapmirror show」コマンドを使用し、ソースでは「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。自動再同期は、関係を「同期中」の状態に戻そうとします。再同期が失敗した場合は、クラスター内のすべてのノードがクォーラム状態にあり、正常であることを確認します。
SMBC サーバー証明書の有効期限が切れました	重大	このメッセージは、ONTAP Mediator サーバ証明書の有効期限が切れたときに表示されます。その結果、 ONTAP Mediator への以降の通信はすべてできなくなります。	「snapmirror mediator remove」コマンドを使用して、現在のONTAP Mediator の設定を削除します。 ONTAP Mediator サーバー上の新しいサーバー証明書を更新します。 「snapmirror mediator add」コマンドを使用して、 ONTAP Mediator へのアクセスを再設定します。
SMBCサーバー証明書の有効期限切れ	警告	このメッセージは、ONTAP Mediator サーバ証明書の有効期限が 30 日以内に切れる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 Mediator の設定を削除します。 ONTAP Mediator サーバー上の新しいサーバー証明書を更新します。 「snapmirror mediator add」コマンドを使用して、 ONTAP Mediator へのアクセスを再設定します。

トップに戻る

追加の電源、ハートビート、およびその他のシステムモニター

モニター名	重大度	モニターの説明	対処方法
ディスクシェルフ電源装置を検出しました	情報	このメッセージは、ディスク シェルフに電源ユニットが追加されたときに発生します。	NONE
ディスクシェルフ電源を取り外しました	情報	このメッセージは、電源ユニットがディスク シェルフから取り外されたときに表示されます。	NONE
MetroCluster の自動計画外スイッチオーバーが無効	重大	このメッセージは、計画外の自動切り替え機能が無効になっている場合に表示されます。	自動スイッチオーバーを有効にするには、クラスター内の各ノードに対して「metrocluster modify -node-name <nodename> -automatic-switchover -onfailure true」コマンドを実行します。
MetroClusterストレージブリッジに到達できません	重大	ストレージブリッジは管理ネットワーク経由でアクセスできません	1) ブリッジが SNMP によって監視されている場合は、「network interface show」コマンドを使用して、ノード管理 LIF が起動していることを確認します。 「network ping」コマンドを使用して、ブリッジが動作してい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 ケーブルを確認し、ブリッジの電源がオンになっていることを確認します。
MetroClusterブリッジ温度異常 - 危険未満	重大	ファイバー チャネル ブリッジのセンサーは、重大なしきい値を下回る温度を報告しています。	1) ストレージブリッジ上のファンの動作状態を確認します。 2) ブリッジが推奨温度条件下で動作していることを確認します。
MetroClusterブリッジ温度異常 - 危険域以上	重大	ファイバー チャネル ブリッジのセンサーが、重大なしきい値を超える温度を報告しています。	1) コマンド「storage bridge show -cooling」を使用して、ストレージ ブリッジ上のシャーシ温度センサーの動作状態を確認します。 2) ストレージブリッジが推奨温度条件下で動作していることを確認します。

モニター名	重大度	モニターの説明	対処方法
MetroCluster で残ったアグリゲートあり	警告	骨材はスイッチバック中に取り残されました。	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は、「metrocluster switchback」コマンドを使用して、アグリゲートを元の所有者に戻します。
メトロクラスターパートナー間のすべてのリンクがダウン	重大	RDMA 相互接続アダプタおよびクラスタ間 LIF とピア クラスタとの接続が切断されているか、ピアクラスタがダウンしています。	1) クラスタ間 LIF が稼働していることを確認します。クラスタ間 LIF がダウン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 クラスターが起動して実行されていることを確認します。ピア クラスタがダウンしている場合は、『 MetroCluster ディザスタ リカバリ ガイド』を参照してください。 3) ファブリックMetroClusterの場合、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 がダウンしている場合は修復します。 4) 非ファブリックMetroCluster構成の場合、RDMA 相互接続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、ケーブルを再構成してください。

モニター名	重大度	モニターの説明	対処方法
MetroClusterパートナーがピアリング ネットワーク経由でアクセスできない	重大	ピア クラスターへの接続が切断されました。	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します。 3) コマンド「cluster peer ping」を使用して、ピア クラスターが起動して実行されていることを確認します。ピア クラスタがダウンしている場合は、『 MetroClusterディザスタ リカバリ ガイド』を参照してください。
MetroClusterスイッチ間全リンクダウン	重大	ストレージ スイッチ上のすべてのスイッチ間リンク (ISL) がダウンしています。	1) ストレージ スイッチ上のバックエンド ファブリック ISL を修復します。 2) パートナー スイッチが起動しており、その 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リンクがダウンしています	警告	SAS アダプタまたはそれに接続されたケーブルに障害がある可能性があります。	1.SAS アダプターがオンラインで実行されていることを確認します。2.物理的なケーブル接続が安全で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 とディスクが正しく取り付けられていることを確認します。
MetroClusterFCイニシエータリンクダウン	重大	FC イニシエーター アダプターに障害があります。	1.FC イニシエーター リンクが改ざんされていないことを確認します。2.「system node run -node local -command storage show adapter」コマンドを使用して、FC イニシエーター アダプターの動作ステータスを確認します。

モニター名	重大度	モニターの説明	対処方法
FC-VIインターコネクトリンクダウン	重大	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. 「metrocluster interconnect adapter show」コマンドを使用して、FC-VI アダプタの物理ステータスが「Up」であることを確認します。3.構成にファブリック スイッチが含まれている場合は、それらが正しくケーブル接続され、構成されていることを確認します。
MetroCluster で残ったスペア ディスクあり	警告	スイッチバック中にスペア ディスクが残されました。	ディスクに障害が発生していない場合は、「metrocluster switchback」コマンドを使用して、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 ポートがダウンしています	重大	ストレージ ブリッジのポートがオフラインです。	1) コマンド「storage bridge show -ports」を使用して、ストレージ ブリッジ上のポートの動作状態を確認します。 2) ポートへの論理的および物理的な接続を確認します。
MetroClusterストレージ スイッチ ファンの故障	重大	ストレージ スイッチのファンが故障しました。	1) コマンド「storage switch show -cooling」を使用して、スイッチ内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 スイッチにアクセスできません	重大	ストレージ スイッチは管理ネットワーク経由ではアクセスできません。	1) コマンド「network interface show」を使用して、ノード管理 LIF が起動していることを確認します。 2) 「network ping」コマンドを使用して、スイッチが動作していることを確認します。 3) スイッチにログインした後、SNMP 設定をチェックして、スイッチが SNMP 経由で到達可能であることを確認します。

モニター名	重大度	モニターの説明	対処方法
MetroClusterスイッチの電源装置に障害が発生しました	重大	ストレージ スイッチの電源ユニットが動作していません。	1) コマンド「storage switch show -error -switch -name <スイッチ名>」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、障害のある電源ユニットを特定します。 3) 電源ユニットがストレージ 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が故障しました	重大	ファイバー チャネル 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状態を確認します。 2) スイッチが推奨温度条件下で動作していることを確認します。
MetroClusterスイッチの温度異常	重大	ファイバー チャネル 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状態を確認します。 2) スイッチが推奨温度条件下で動作していることを確認します。
サービス プロセッサのハートビートが失われました	情報	このメッセージは、ONTAP がサービス プロセッサ (SP) から予期される「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。このメッセージとともに、 SPからのログ ファイルがデバッグ用に送信されます。 ONTAP はSPをリセットして通信を復元しようとします。 SPは再起動中、最大 2 分間使用できなくなります。	NetAppテクニカル サポートにお問い合わせください。

モニター名	重大度	モニターの説明	対処方法
サービス プロセッサのハートビートが停止しました	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ときに表示されます。ハードウェアの設計に応じて、システムはデータの提供を継続するか、データの損失やハードウェアの損傷を防ぐためにシャットダウンすることを決定する場合があります。システムは引き続きデータを提供しますが、 SPが動作していない可能性があるため、ダウンしたアプライアンス、ブート エラー、または Open Firmware (OFW) 電源投入時セルフテスト (POST) エラーに関する通知を送信できません。システムがそのように構成されている場合、 AutoSupport (または「コール ホーム」) メッセージが生成され、NetAppテクニカル サポートと構成された送信先に送信されます。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、ハードパワーサイクルを試してください。コントローラをシャーシから引き出し、押し戻して、システムの電源を入れます。電源を入れ直しても問題が解決しない場合、または他に注意が必要な状況がある場合は、 NetApp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

- "アラートの表示と消去"

Webhook通知

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は、標準入力インターフェースとして Webhook をサポートしています。たとえば、Slack、PagerDuty、Teams、Discord はすべて Webhook をサポートしています。汎用的でカスタマイズ可能な Webhook チャネルをサポートすることで、 Data Infrastructure Insights はこれらの配信チャネルの多くをサポートできます。 Webhook に関する情報は、これらのアプリケーション Web サイトで参照できま

す。例えば、Slackは"この便利なガイド"。

複数の Webhook チャネルを作成し、各チャネルを異なる目的 (個別のアプリケーション、異なる受信者など) に向けることができます。

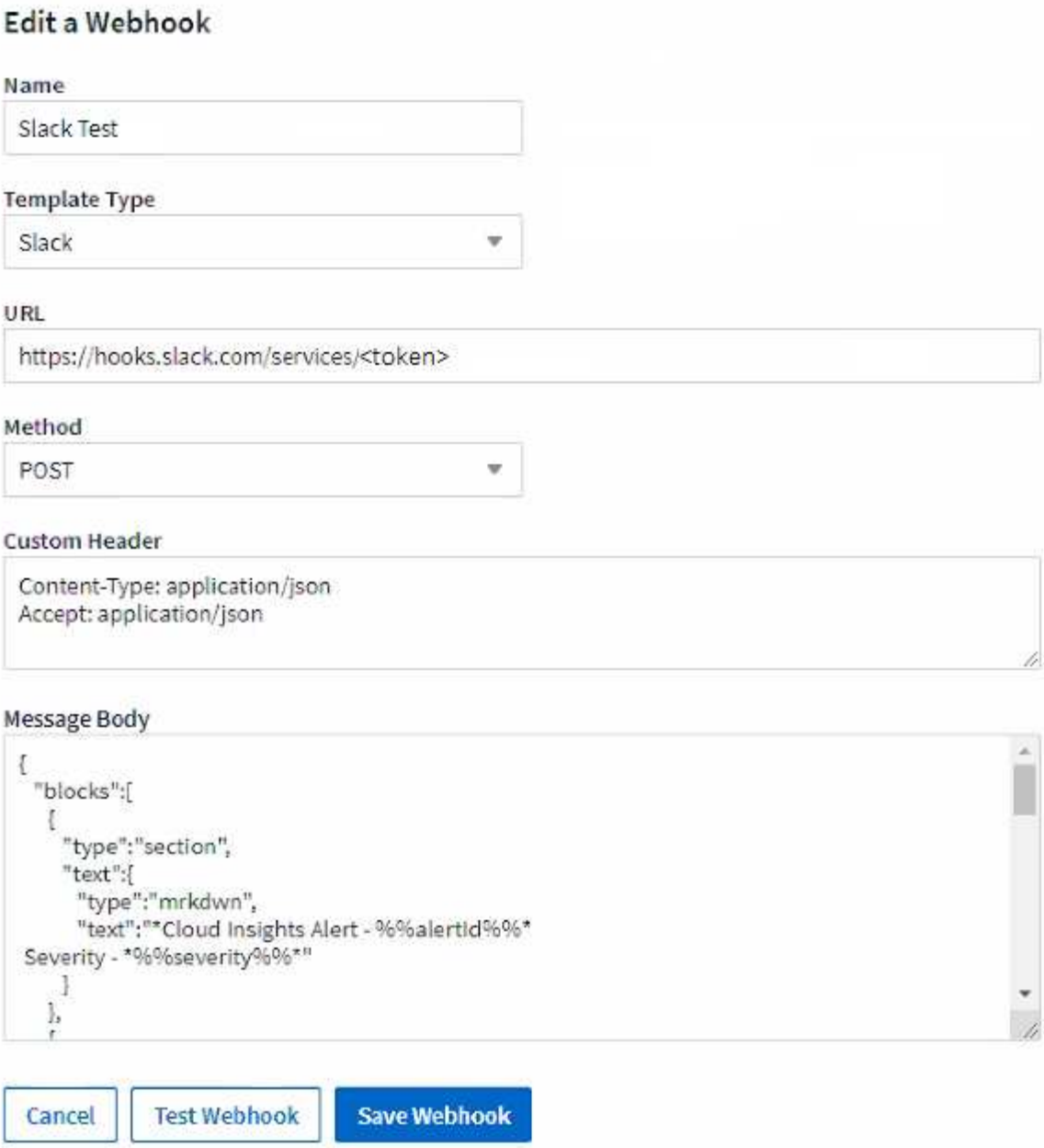
Webhook チャネル インスタンスは、次の要素で構成されます。

Name	一意の名前
URL	Webhook ターゲット 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）
方法	GET、POST - デフォルトはPOST
カスタムヘッダー	ここで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てください
デフォルトのアラートパラメータ	Webhookのデフォルトパラメータを一覧表示します
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、固有のパラメータやパスワードなどの安全な要素を追加できます。

Webhookの作成

Data Infrastructure Insights Webhook を作成するには、管理 **>** 通知 に移動し、**Webhooks** タブを選択します。

次の画像は、Slack 用に構成された 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。

「Webhook 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、選択したメソッドに従って、定義された URL に「メッセージ本文」（置換なし）が送信されることに注意してください。

Data Infrastructure Insights Webhook は、いくつかのデフォルト パラメータで構成されています。さらに、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

パラメーター: パラメーターとは何ですか? また、どのように使用しますか?

アラート パラメータは、アラートごとに設定される動的な値です。たとえば、*%%TriggeredOn%%* パラメータは、アラートがトリガーされたオブジェクトに置き換えられます。

任意のオブジェクト属性 (ストレージ名など) をパラメータとして Webhook に追加できます。たとえば、Webhook の説明に、次のようにボリューム名とストレージ名のパラメータを設定できます: 「ボリューム: *%%relatedObject.volume.name%%*、ストレージ: *%%relatedObject.storage.name%%* の待機時間が長い」。

このセクションでは、「Webhook をテスト」ボタンをクリックしたときに置換は実行されないことに注意してください。ボタンは、%% 置換を示すペイロードを送信しますが、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

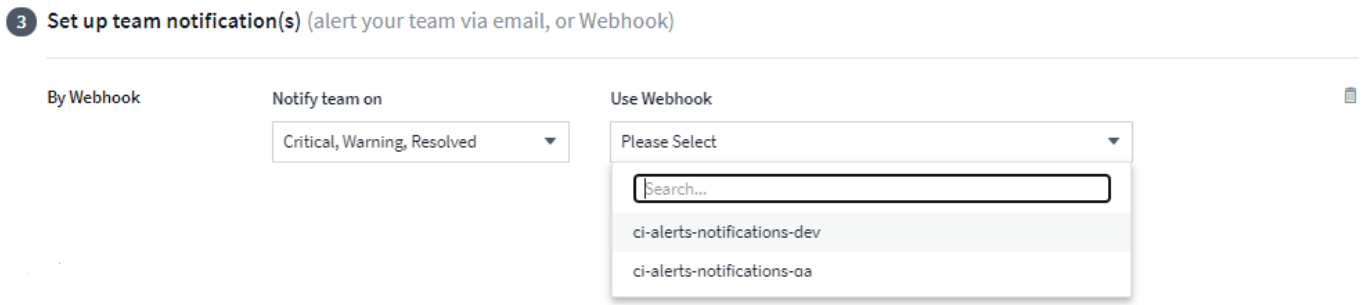
このセクションでは、必要なカスタム パラメータやシークレットを追加できます。セキュリティ上の理由から、シークレットが定義されている場合、この Webhook チャネルを変更できるのは Webhook 作成者のみです。他のユーザーにとっては読み取り専用となります。 URL/ヘッダーでは、*%%<secret_name>%%* のようにシークレットを使用できます。

Webhooksリストページ

Webhook リスト ページには、名前、作成者、作成日、ステータス、セキュリティ、最終報告のフィールドが表示されます。

モニターで**Webhook**通知を選択する

ウェブフック通知を選択するには"monitor"、アラート > モニターの管理 に移動して目的のモニターを選択するか、新しいモニターを追加します。 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。アラート レベル (重大、警告、解決済み) を選択し、目的の Webhook を選択します。



Webhook の例:

Webhooksの"スラック"Webhooksの"ページャーデューティ"Webhooksの"チーム"Webhooksの"不和"

Discord の **Webhook** の例

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。このページでは、Discord 用の Webhook を設定する例を示します。

このページはサードパーティの指示を参照しており、変更される可能性があります。参照"Discordドキュメント"最新情報についてはこちらをご覧ください。

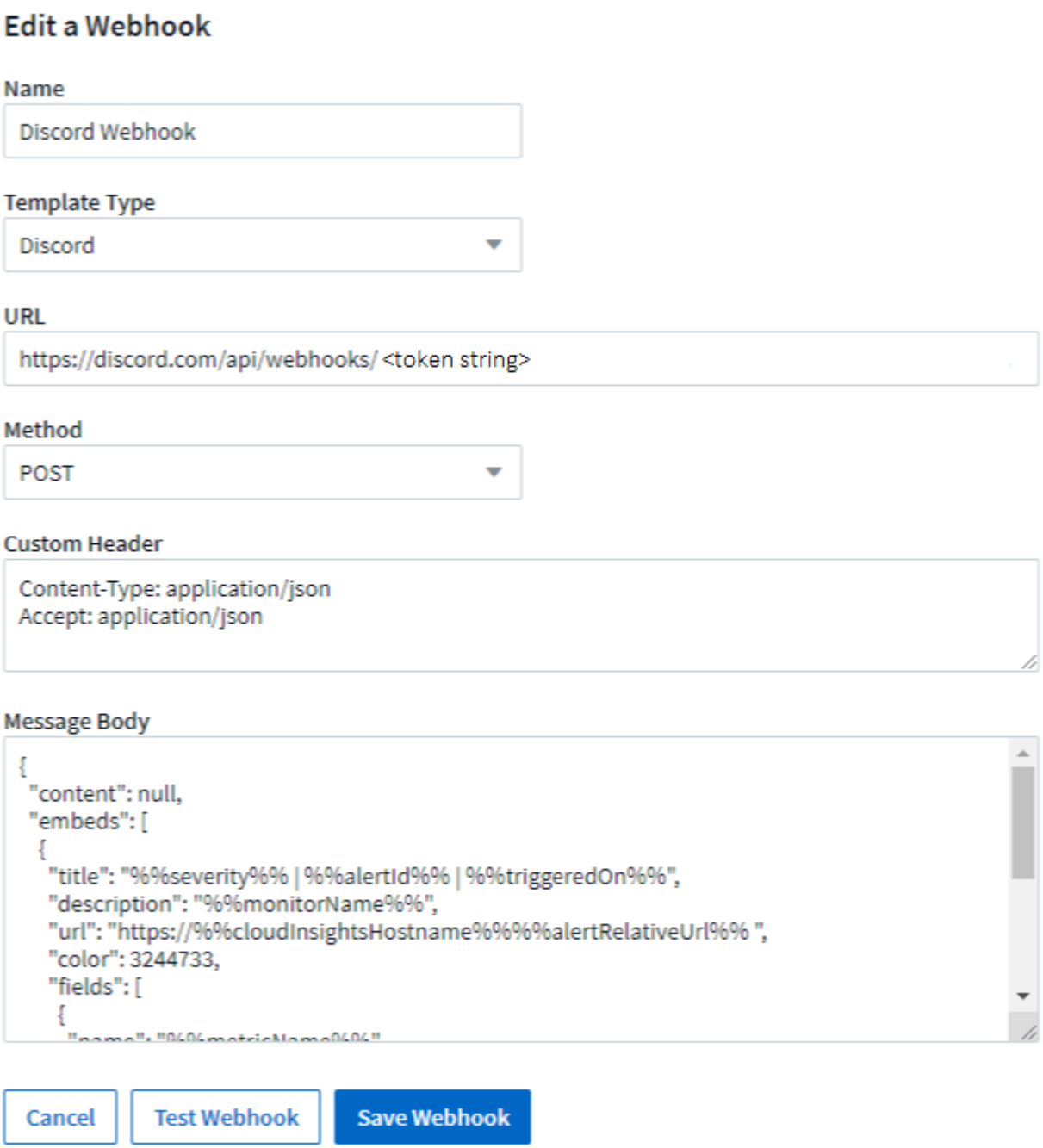
Discordの設定:

- Discordでサーバーを選択し、テキストチャンネルの下にあるチャンネル編集（歯車アイコン）を選択します。
- *統合 > Webhookの表示*を選択し、*新しいWebhook*をクリックします。

- Webhook URL をコピーします。これをData Infrastructure Insights のWebhook 構成に貼り付ける必要があります。

Data Infrastructure Insights Webhook を作成します。

1. Data Infrastructure Insightsで、管理 **>** 通知 に移動し、**Webhooks** タブを選択します。新しい Webhook を作成するには、[+Webhook] をクリックします。
2. Webhook に「Discord」などの意味のある名前を付けます。
3. テンプレート タイプ ドロップダウンで、**Discord** を選択します。
4. 上記の URL を *URL* フィールドに貼り付けます。

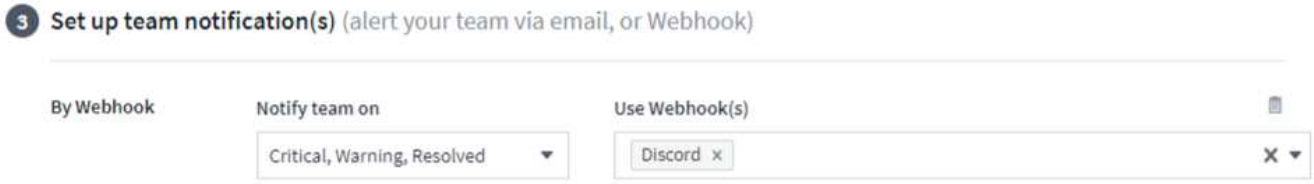


Webhook をテストするには、メッセージ本文の URL 値を有効な URL (*https://netapp.com* など) に一時的に置き換えて、[*Test Webhook*] ボタンをクリックします。テストが完了したら、必ずメッセージ本文を元に戻してください。

Webhook経由の通知

Webhook経由でイベントを通知するには、Data Infrastructure Insightsで*アラート>モニター*に移動し、*+モニター*をクリックして新しいモニターを作成します。"monitor" 。

- メトリックを選択し、モニターの条件を定義します。
- [チーム通知の設定] の下で、**Webhook** 配信方法を選択します。
- 必要なイベント（重大、警告、解決済み）の「Discord」Webhookを選択します。



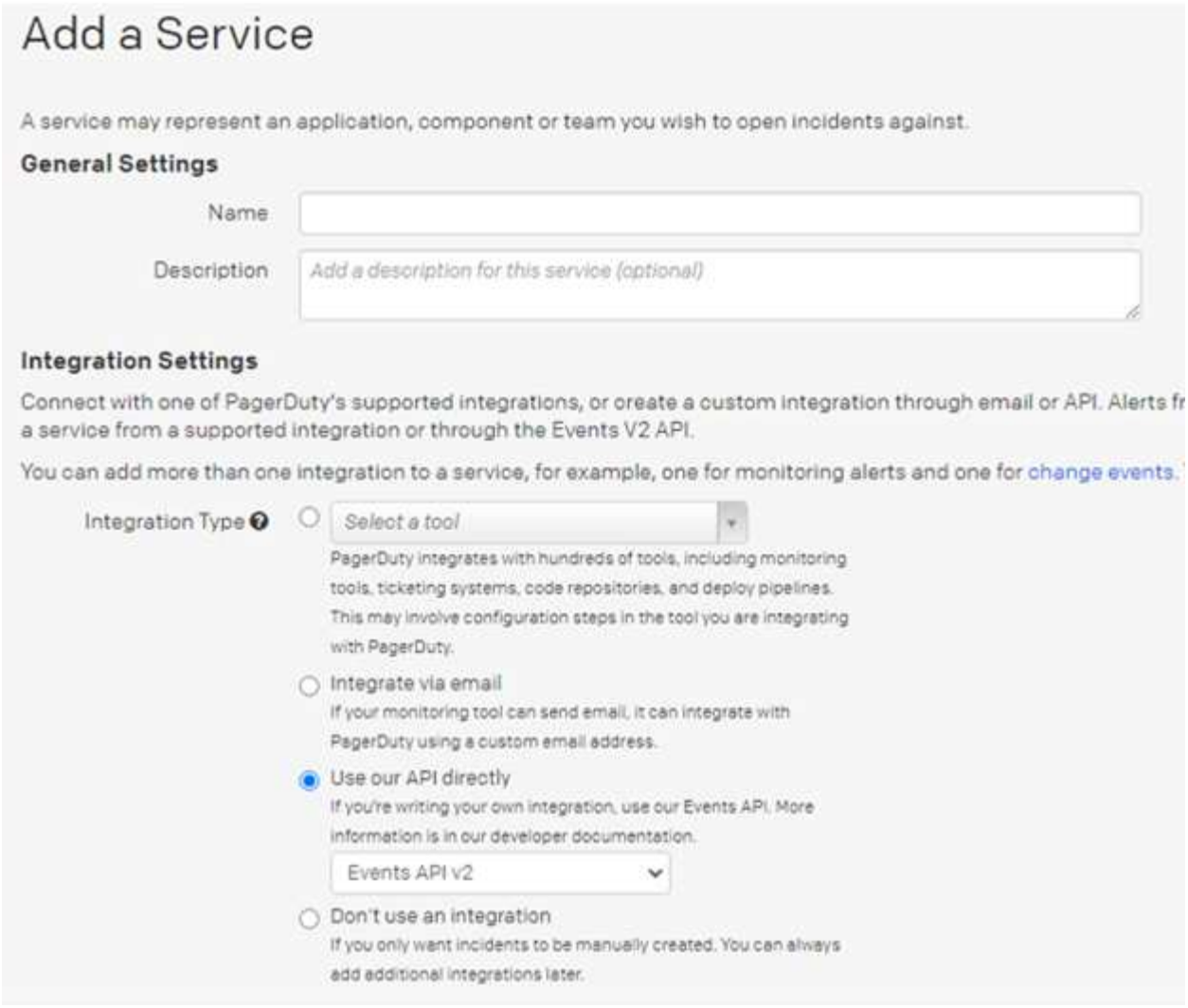
PagerDuty の **Webhook** の例

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。このページでは、PagerDuty の Webhook を設定する例を示します。

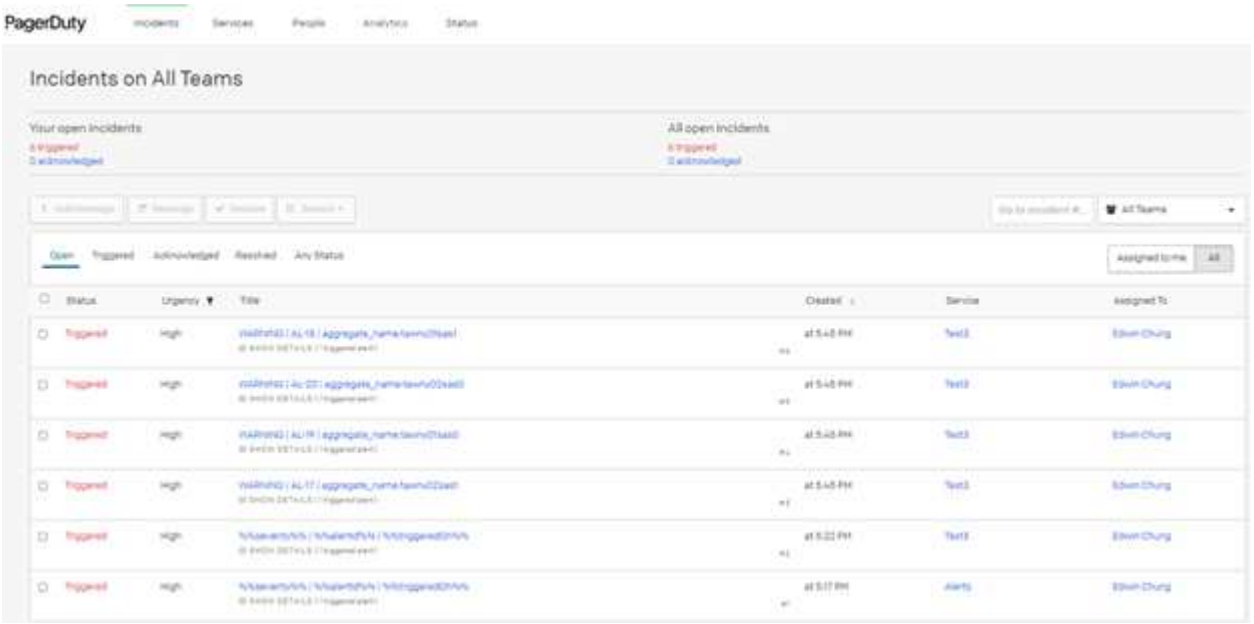
このページはサードパーティの指示を参照しており、変更される可能性があります。参照"PagerDutyのドキュメント"最新情報についてはこちらをご覧ください。

PagerDutyのセットアップ:

1. PagerDutyで*サービス>サービスディレクトリ*に移動し、*+新しいサービス*ボタンをクリックします。
2. 名前_を入力し、*[_API* を直接使用] を選択します。 _サービスの追加_をクリックします。

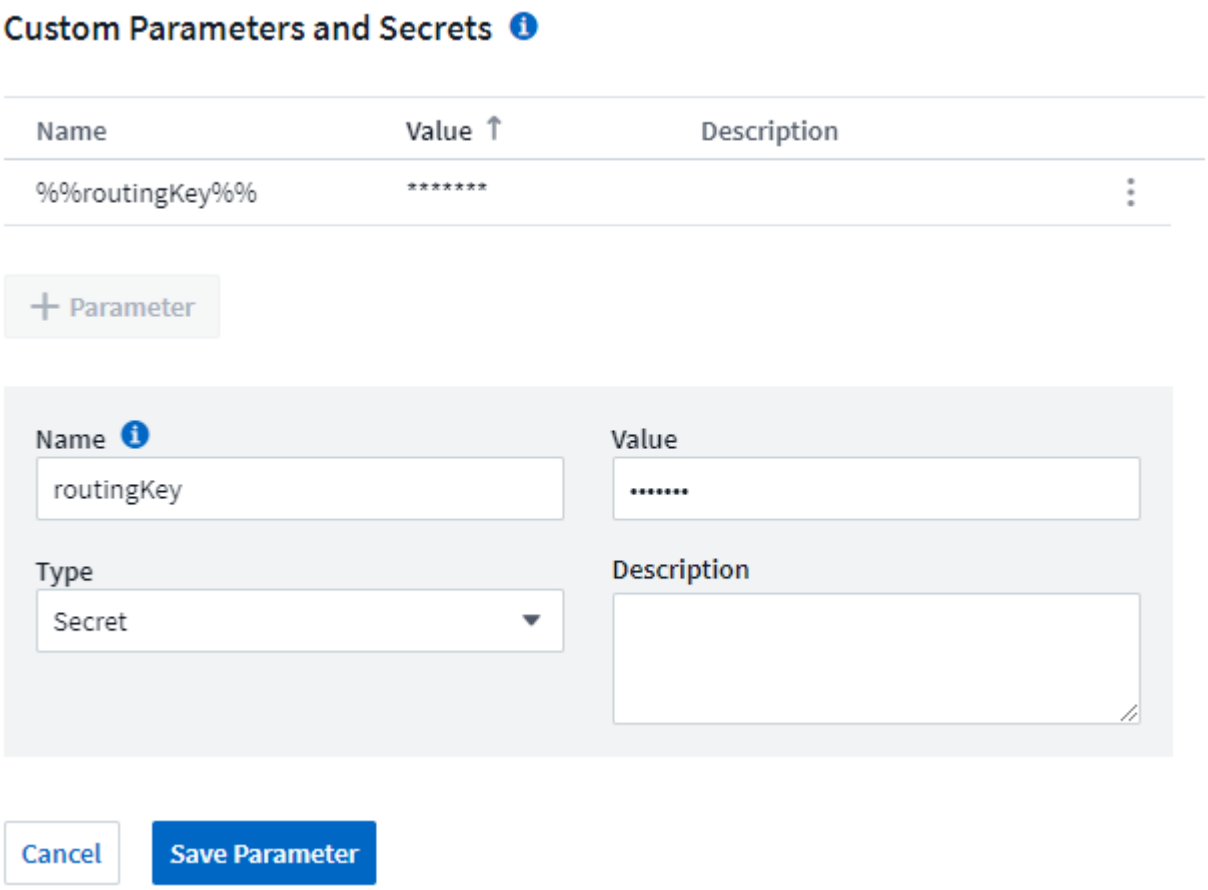


3. *統合キー*を表示するには、[統合] タブをクリックします。以下のData Infrastructure Insights Webhook を作成するときに、このキーが必要になります。
4. アラートを表示するには、「インシデント」または「サービス」に移動します。



Data Infrastructure Insights Webhook を作成します。

1. Data Infrastructure Insightsで、管理 **>** 通知 に移動し、**Webhooks** タブを選択します。新しい Webhook を作成するには、[+Webhook] をクリックします。
2. Webhook に「PagerDuty Trigger」などの意味のある名前を付けます。この Webhook は、重大レベルおよび警告レベルのイベントに使用します。
3. テンプレート タイプ ドロップダウンで、**PagerDuty** を選択します。
4. *routingKey* という名前のカスタム パラメータ シークレットを作成し、その値を上記の PagerDuty *Integration Key* 値に設定します。



これらの手順を繰り返して、解決されたイベントの「PagerDuty Resolve」Webhook を作成します。

PagerDuty から**Data Infrastructure Insights**へのフィールド マッピング

次の表と画像は、PagerDuty とData Infrastructure Insights間のフィールドのマッピングを示しています。

ページャーデューティ	**Data Infrastructure Insights**
アラートキー	Alert ID
ソース	トリガーオン
コンポーネント	メトリック名
グループ	オブジェクト タイプ

ページャーデューティ	**Data Infrastructure Insights**
クラス	モニター名

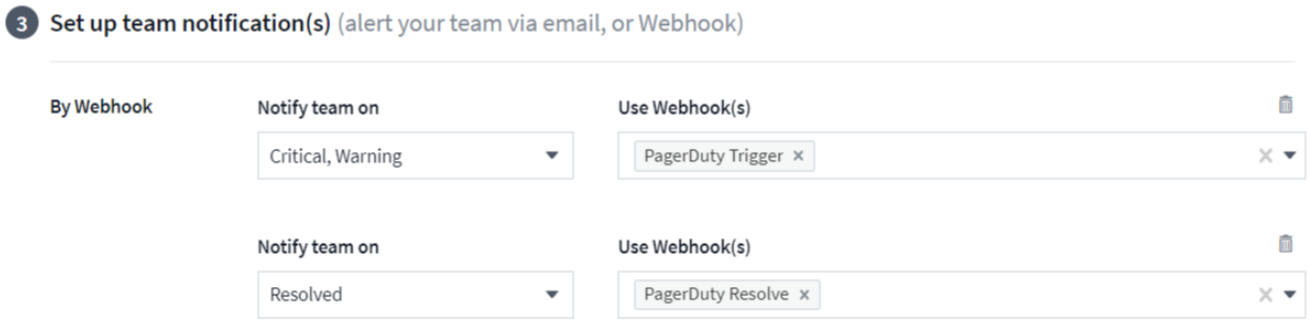
Message Body

```
{
 "dedup_key": "%%alertId%%",
 "event_action": "trigger",
 "links": [
  {
   "href": "https://%%cloudInsightsHostname%%%%alertRelativeUrl%%",
   "text": "'%%metricName%%' value of %%value%% (%%alertCondition%%) for
%%triggeredOn%%"
  }
 ],
 "payload": {
  "class": "%%monitorName%%",
  "component": "%%metricName%%",
  "group": "%%objectType%%",
  "severity": "critical",
  "source": "%%triggeredOn%%",
  "summary": "%%severity%% | %%alertId%% | %%triggeredOn%%"
 },
 "routing_key": "%%routingKey%%"
}
```

Webhook経由の通知

Webhook経由でイベントを通知するには、Data Infrastructure Insightsで*アラート>モニター*に移動し、*+モニター*をクリックして新しいモニターを作成します。"monitor" 。

- メトリックを選択し、モニターの条件を定義します。
- [チーム通知の設定] の下で、**Webhook** 配信方法を選択します。
- 重大レベルおよび警告レベルのイベントには、「PagerDuty トリガー」Webhook を選択します。
- 解決されたイベントには「PagerDuty Resolve」を選択します。



PagerDuty はトリガー イベントを解決済みイベントとは異なる方法で処理するため、トリガー イベントと解決済みイベントに別々の通知を設定することがベスト プラクティスです。

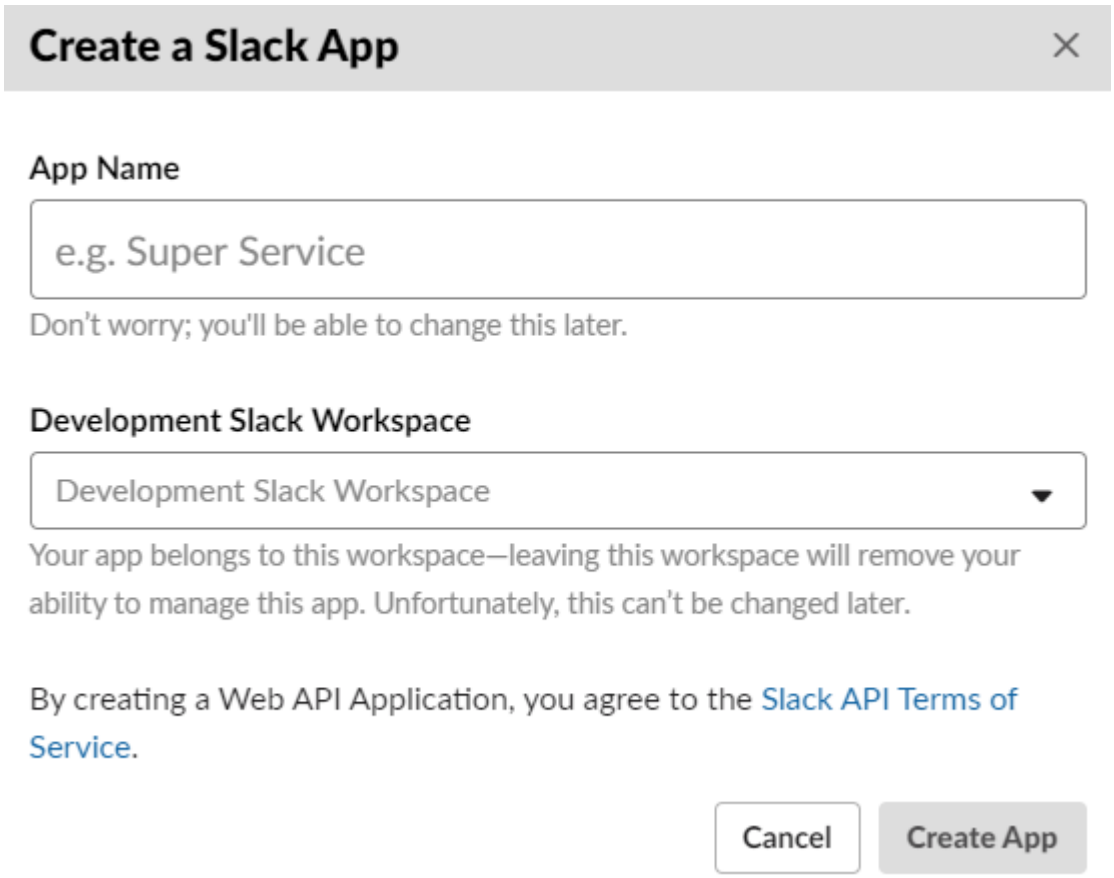
Slack の Webhook の例

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。このページでは、Slack 用の Webhook を設定する例を示します。

このページはサードパーティの指示を参照しており、変更される可能性があります。参照"Slackドキュメント"最新情報についてはこちらをご覧ください。

Slackの例:

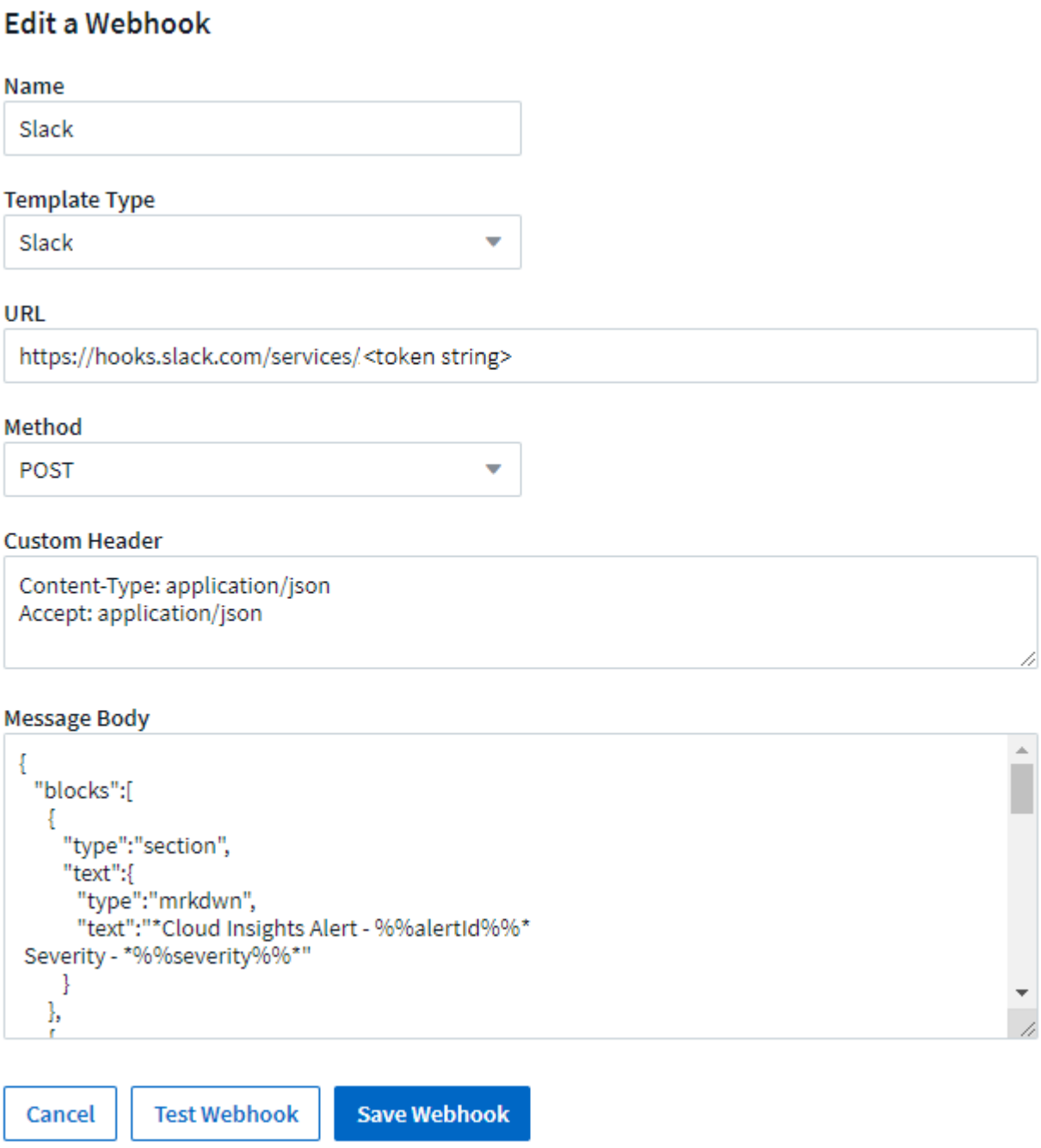
- へ移動 https://api.slack.com/apps新しいアプリを作成します。意味のある名前を付けて、Slack ワークスペースを選択します。



- 「受信 Webhooks」に移動し、「受信 *Webhook* のアクティブ化」をクリックし、「新しい *Webhook* の追加」をリクエストして、投稿するチャネルを選択します。
- Webhook URL をコピーします。これをData Infrastructure Insights のWebhook 構成に貼り付ける必要があります。

Data Infrastructure Insights Webhook を作成します。

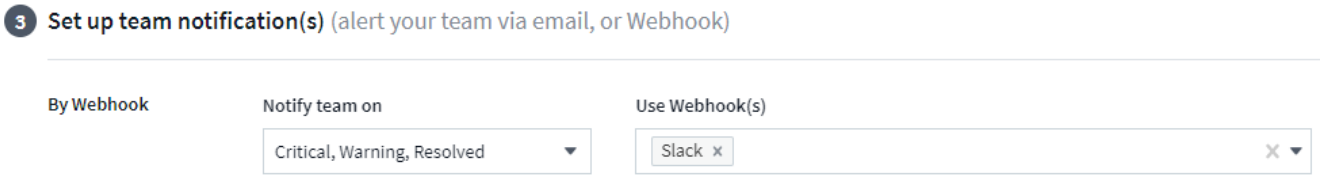
1. Data Infrastructure Insightsで、管理 **>** 通知 に移動し、**Webhooks** タブを選択します。新しい Webhook を作成するには、[+Webhook] をクリックします。
2. Webhook に「Slack Webhook」などの意味のある名前を付けます。
3. テンプレート タイプ ドロップダウンで、**Slack** を選択します。
4. 上記の URL を *URL* フィールドに貼り付けます。



Webhook経由の通知

Webhook経由でイベントを通知するには、Data Infrastructure Insightsで*アラート>モニター*に移動し、*+モニター*をクリックして新しいモニターを作成します。"monitor" 。

- メトリックを選択し、モニターの条件を定義します。
- [チーム通知の設定] の下で、**Webhook** 配信方法を選択します。
- 必要なイベント（重大、警告、解決済み）の「Slack」Webhookを選択します。



詳細情報：

- メッセージの形式とレイアウトを変更するには、 https://api.slack.com/messaging/composing
- エラー処理: https://api.slack.com/messaging/webhooks#handling_errors

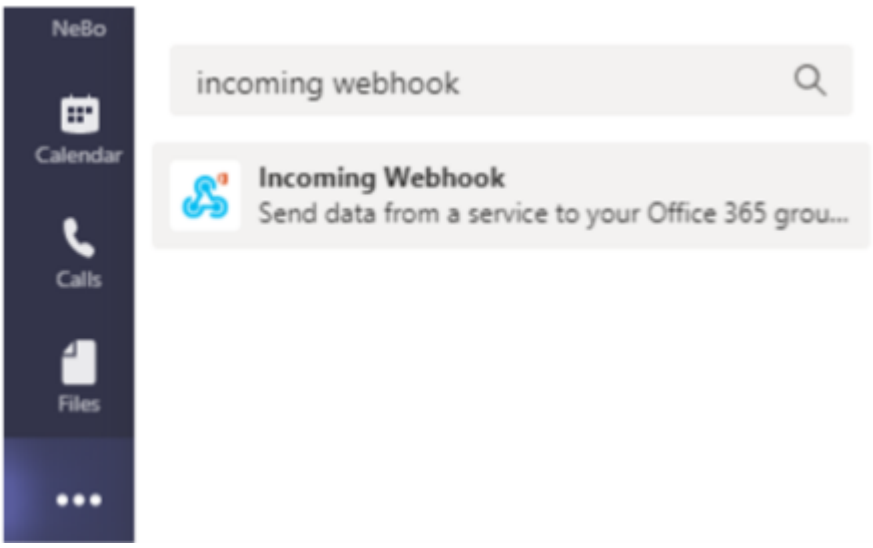
Microsoft Teams の **Webhook** の例

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。このページでは、Teams の Webhook を設定する例を示します。

このページはサードパーティの指示を参照しており、変更される可能性があります。参照"Teamsドキュメント"最新情報についてはこちらをご覧ください。

Teams のセットアップ**:**

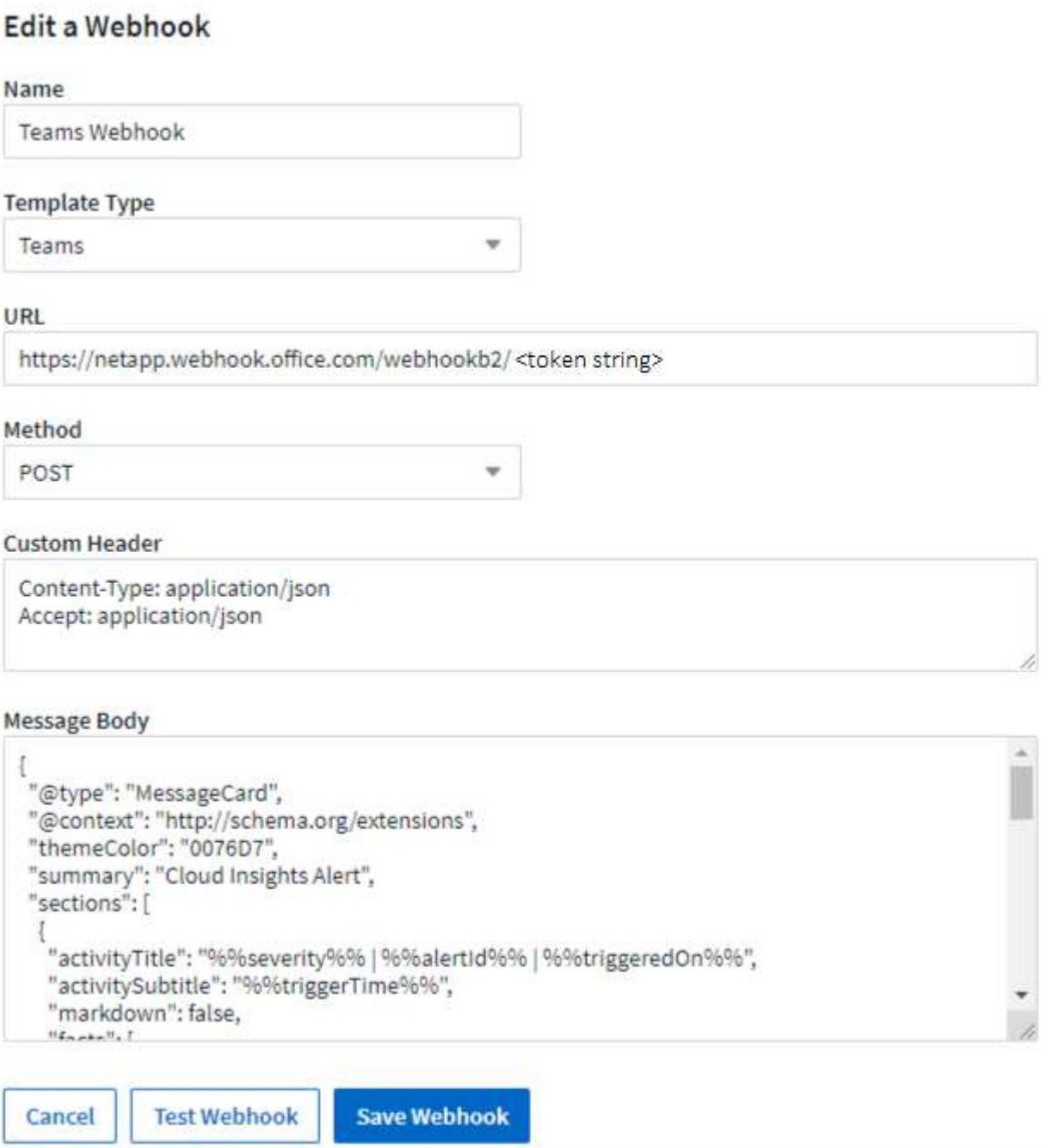
1. Teams でケバブを選択し、Incoming Webhook を検索します。



2. *チームに追加 > チームを選択 > コネクタの設定*を選択します。
3. Webhook URL をコピーします。これをData Infrastructure Insights のWebhook 構成に貼り付ける必要があります。

Data Infrastructure Insights Webhook を作成します。

1. Data Infrastructure Insightsで、管理 **>** 通知 に移動し、**Webhooks** タブを選択します。新しい Webhook を作成するには、[+Webhook] をクリックします。
2. Webhook に「Teams Webhook」などのわかりやすい名前を付けます。
3. [テンプレート タイプ] ドロップダウンで、[**Teams**] を選択します。

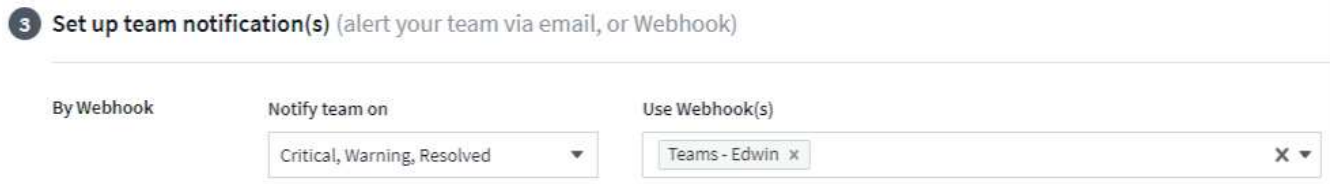


1. 上記の URL を *URL* フィールドに貼り付けます。

Webhook経由の通知

Webhook経由でイベントを通知するには、Data Infrastructure Insightsで*アラート>モニター*に移動し、*+モニター*をクリックして新しいモニターを作成します。"monitor" 。

- メトリックを選択し、モニターの条件を定義します。
- [チーム通知の設定] の下で、**Webhook** 配信方法を選択します。
- 必要なイベント（重大、警告、解決済み）の「Teams」Webhookを選択します。



注釈の操作

注釈の定義

企業の要件に合わせてデータを追跡するためにData Infrastructure Insightsをカスタマイズする場合、注釈と呼ばれる特殊なメモを定義し、それを資産に割り当てることができます。

資産の耐用年数、データセンター、建物の場所、ストレージ層、ボリューム サービス レベルなどの情報を資産に注釈として割り当てることができます。

注釈を使用して環境を監視するには、次の高レベルのタスクが含まれます。

- すべての注釈タイプの定義を作成または編集します。
- アセット ページを表示し、各アセットを 1 つ以上の注釈に関連付けます。

  たとえば、資産がリースされており、そのリースが 2 か月以内に期限切れになる場合は、資産に耐用年数終了の注釈を適用することが考えられます。これにより、他の人がその資産を長期間使用することを防ぐことができます。

- 同じタイプの複数のアセットに注釈を自動的に適用するためのルールを作成します。
- 注釈によってアセットをフィルタリングします。

デフォルトの注釈タイプ

Data Infrastructure Insightsには、いくつかのデフォルトの注釈タイプが用意されています。これらの注釈は、データをフィルタリングまたはグループ化するために使用できます。

次のようなデフォルトの注釈タイプにアセットを関連付けることができます。

- 資産のライフサイクル（誕生日、終了、使用終了など）
- データセンター、建物、フロアなどのデバイスの位置情報
- 資産の分類（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）
- ステータス（ホット（高使用率）など）

次の表は、Data Infrastructure Insightsが提供する注釈タイプを示しています。

注釈の種類	説明	タイプ
エイリアス	リソースのユーザーフレンドリーな名前	文章
コンピューティング リソース グループ	ホストおよび VM ファイルシステム データ コレクターによって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	定期的に頻繁に使用されるデバイス、または容量の限界に達しているデバイス	ブーリアン
メモ	リソースに関連付けられたコメント	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、サポートされているサービス レベルのセット。内部ボリューム、qtree、ボリュームの順序付けられたオプション リストを提供します。サービス レベルを編集して、さまざまなレベルのパフォーマンス ポリシーを設定します。	リスト
日没	このしきい値を超えると、そのデバイスに新しい割り当てを行うことができなくなります。計画された移行やその他の保留中のネットワーク変更に役立ちます。	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定義済みオプション。通常、これらの指定はデバイスの寿命の間は保持されますが、編集することもできます。スイッチのみ使用可能です。	リスト
階層	環境内でさまざまなレベルのサービスを定義するために使用できます。ティアでは、必要な速度などのレベルのタイプを定義できます (たとえば、ゴールドまたはシルバー)。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、およびボリュームでのみ使用できます。	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落など) の重要度の最高から最低の階層でのランク (たとえば、メジャー)。	リスト

エイリアス、データ センター、ホット、サービス レベル、サンセット、スイッチ レベル、層、違反の重大度はシステム レベルの注釈であり、削除または名前変更はできません。変更できるのは割り当てられた値のみです。

カスタム注釈の作成

注釈を使用すると、ビジネスニーズに合ったカスタムのビジネス固有のデータをアセットに追加できます。Data Infrastructure Insightsでは一連のデフォルトの注釈が提供されますが、他の方法でデータを表示したい場合もあります。カスタム注釈のデータは、ストレージの製造元、ボリューム数、パフォーマンス統計など、すでに収集されているデバイス データを補足します。注釈を使用して追加したデータは、Data Infrastructure Insightsによって検出されません。

手順

1. Data Infrastructure Insightsサイト メニューで、管理 > 注釈 をクリックします。

   「注釈」ページには注釈のリストが表示されます。

2. *+追加*をクリック
3. 注釈の*名前*と*説明*を入力します。

   これらのフィールドには最大 255 文字を入力できます。

4. *タイプ*をクリックし、この注釈で許可され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。

注釈の種類

- ブール値: はい/いいえの選択肢を持つドロップダウンリストを作成します。例えば、「直接接続」という注釈はブール値です。
- 日付: 日付を保持するフィールドを作成します。たとえば、注釈を日付にする場合は、これを選択します。
- リスト: 次のいずれかを作成します。
  - ドロップダウン固定リスト

    他のユーザーがデバイス上でこの注釈タイプを割り当てている場合、リストにさらに値を追加することはできません。

  - ドロップダウンの柔軟なリスト

    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する] オプションを選択すると、他のユーザーがデバイスでこの注釈タイプを割り当てるときに、リストにさらに値を追加できます。

- 数値: 注釈を割り当てるユーザーが数値を入力できるフィールドを作成します。たとえば、注釈タイプが「階」の場合、ユーザーは「数値」の値タイプを選択し、階数を入力できます。
- テキスト: 自由形式のテキストを入力できるフィールドを作成します。たとえば、注釈タイプとして「言語」を入力し、値タイプとして「テキスト」を選択し、値として言語を入力します。



タイプを設定して変更を保存した後は、注釈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、注釈を削除して新しい注釈を作成する必要があります。

1. 注釈タイプとしてリストを選択した場合は、次の操作を行います。
   a. アセット ページ上で注釈に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、[新しい値を即座に追加] を選択します。

      たとえば、アセット ページにいて、そのアセットに Detroit、Tampa、Boston という値を持つ City 注釈が付いているとします。 *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、注釈ページに移動して値を追加するのではなく、アセット ページで直接、サンフランシスコやシカゴなどの都市に値を追加できます。このオプションを選択しないと、注釈を適用するときに新しい注釈値を追加できず、固定リストが作成されます。

   b. *値*フィールドと*説明*フィールドに値と説明を入力します。
   c. 追加の値を追加するには、[追加] をクリックします。
   d. 値を削除するには、ゴミ箱アイコンをクリックします。
2. *保存*をクリックします

注釈は「注釈」ページのリストに表示されます。

ブール注釈に関する注意

ブール型注釈でフィルタリングする場合、フィルタリング対象となる次の値が表示されることがあります。

- 任意: 「はい」、「いいえ」に設定された結果、またはまったく設定されていない結果を含む、すべての結果が返されます。
- はい: 「はい」の結果のみを返します。DII では、ほとんどの表で「はい」にチェックマークが表示されることに注意してください。値は「True」、「On」などに設定できます。DII はこれらすべてを「Yes」として扱います。
- いいえ: 「いいえ」の結果のみを返します。DII では、ほとんどの表で「いいえ」が「X」として表示されることに注意してください。値は「False」、「Off」などに設定できますが、DII はこれらすべてを「No」として扱います。
- なし: アノテーションがまったく設定されていない結果のみを返します。「Null」値とも呼ばれます。

終了後の操作

UI では、注釈はすぐに使用できるようになります。

注釈の使用

注釈を作成し、監視する資産に割り当てます。注釈は、物理的な場所、耐用年数、ストレージ層、ボリューム サービス レベルなど、資産に関する情報を提供するメモです。

注釈の定義

注釈を使用すると、ビジネスニーズに合ったカスタムのビジネス固有のデータをアセットに追加できます。Data Infrastructure Insightsでは、資産のライフ サイクル (誕生日または寿命)、建物またはデータ センターの場所、階層などの一連のデフォルトの注釈が提供されますが、他の方法でデータを表示することが必要になる場合があります。

カスタム注釈のデータは、スイッチの製造元、ポート数、パフォーマンス統計など、すでに収集されているデバイス データを補足します。注釈を使用して追加したデータは、Data Infrastructure Insightsによって検出されません。

開始する前に

- 環境データを関連付ける必要がある業界用語をリストします。
- 環境データを関連付ける必要がある企業用語をリストします。
- 使用できる可能性のあるデフォルトの注釈タイプを特定します。
- 作成する必要があるカスタム注釈を特定します。注釈をアセットに割り当てる前に、注釈を作成する必要があります。

注釈を作成するには、次の手順に従います。

手順

1. Data Infrastructure Insightsサイト メニューで、オブザーバビリティ **>** エンリッチ **>** アノテーション をクリックします。
2. 新しい注釈を作成するには、[**+** 注釈] をクリックします。

3. 新しい注釈の名前、説明、およびタイプを入力します。

   たとえば、データセンター 4 内の資産の物理的な場所を定義するテキスト注釈を作成するには、次のように入力します。

   - 「場所」などの注釈の名前を入力します
   - 「物理的な場所はデータセンター4です」など、注釈が説明している内容の説明を入力します。
   - 「テキスト」など、注釈の「タイプ」を入力します。

アセットに手動で注釈を割り当てる

アセットに注釈を割り当てると、ビジネスに関連した方法でアセットを並べ替え、グループ化し、レポートすることができます。注釈ルールを使用して特定のタイプのアセットに注釈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注釈を割り当てることもできます。

開始する前に

- 割り当てる注釈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. 注釈を適用するアセットを見つけます。
   - クエリを実行したり、ダッシュボード ウィジェットから選択したり、検索したりして、アセットを見つけることができます。必要な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、[+ 注釈] 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. リストから注釈を選択します。
6. [値] をクリックし、選択した注釈の種類に応じて次のいずれかを実行します。
   - 注釈タイプがリスト、日付、またはブール値の場合は、リストから値を選択します。
   - 注釈タイプがテキストの場合は、値を入力します。
7. *保存*をクリックします。

注釈を割り当てた後にその値を変更する場合は、注釈フィールドをクリックして別の値を選択します。注釈がリスト タイプで、[新しい値をオンザフライで追加] オプションが選択されている場合は、既存の値を選択するだけでなく、新しい値を入力することもできます。

注釈ルールを使用して注釈を割り当てる

定義した基準に基づいてアセットに注釈を自動的に割り当てるには、注釈ルールを構成します。 Data Infrastructure Insights は、これらのルールに基づいてアセットに注釈を割り当てます。 Data Infrastructure Insightsには 2 つのデフォルトの注釈ルールも用意されており、ニーズに合わせて変更したり、使用しない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

個々のアセットに手動で注釈を適用する代わりに、注釈ルールを使用して複数のアセットに注釈を自動的に適

用できます。 Insight が注釈ルールを評価する際、個々のアセット ページに手動で設定された注釈は、ルールベースの注釈よりも優先されます。

開始する前に

注釈ルールのクエリを作成しておく必要があります。

タスク概要

ルールの作成中に注釈タイプを編集できますが、事前にタイプを定義しておく必要があります。

手順

1. *管理 > 注釈ルール*をクリックします

   「注釈ルール」ページには、既存の注釈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「注釈ルール」ページに表示されます。

   b. *クエリ*をクリックし、アセットに注釈を適用するために使用するクエリを選択します。
   c. *注釈*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、注釈の値を選択します。

      たとえば、注釈として「誕生日」を選択した場合は、値に日付を指定します。

   e. *保存*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。それ以外の場合は、ルールは定期的にスケジュールされた間隔で実行されます。

アノテーション ルールの作成

注釈ルールを使用すると、定義した基準に基づいて複数のアセットに注釈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注釈を割り当てます。 Cloud Insight が注釈ルールを評価する際、個々のアセット ページに手動で設定された注釈は、ルールベースの注釈よりも優先されます。

開始する前に

注釈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サイト メニューで、管理 **>** 注釈ルール をクリックします。
2. 新しい注釈ルールを追加するには、[**+** ルール] をクリックします。

   「ルールの追加」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。

   名前は「注釈ルール」ページに表示されます。

b. *クエリ*をクリックし、注釈が適用される資産を識別するためにData Infrastructure Insightsが使用するクエリを選択します。

c. *注釈*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、注釈の値を選択します。

   たとえば、注釈として「誕生日」を選択した場合は、値に日付を指定します。

e. *保存*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。それ以外の場合は、ルールは定期的にスケジュールされた間隔で実行されます。

> ⓘ 大規模なData Infrastructure Insights環境では、注釈ルールの実行が完了するまでに時間がかかることがあります。これは、インデクサーが最初に実行され、ルールを実行する前に完了する必要があるためです。インデクサーにより、 Data Infrastructure Insights 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ーを検索したりフィルター処理したりできるようになります。ルール エンジンは、インデクサー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。

注釈ルールの変更

注釈ルールを変更して、ルールの名前、注釈、注釈の値、またはルールに関連付けられたクエリを変更できます。

手順

1. Data Infrastructure Insightsメニューで、管理 > 注釈ルール をクリックします。

   「注釈ルール」ページには、既存の注釈ルールのリストが表示されます。

2. 変更する注釈ルールを見つけます。

   フィルター ボックスに値を入力して注釈ルールをフィルターしたり、ページ番号をクリックしてページごとに注釈ルールを参照したりできます。

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*をクリック

   ルールの編集ダイアログが表示されます。

5. 注釈ルールの名前、注釈、値、またはクエリを変更します。

ルールの順序の変更

注釈ルールは、ルール リストの上から下に向かって処理されます。ルールが処理される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. ルールが目的の場所に表示されるまで、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。

アセット上の同じ注釈を更新する複数のルールを実行する場合、最初のルール (上から下に実行) が注釈を適用してアセットを更新し、次に 2 番目のルールが適用されますが、前のルールによって既に設定されている注釈は変更されないことに注意してください。

アノテーション ルールの削除

使用されなくなった注釈ルールを削除する必要がある場合があります。

手順

1. Data Infrastructure Insightsメニューで、管理 **>** 注釈ルール をクリックします。

   「注釈ルール」ページには、既存の注釈ルールのリストが表示されます。

2. 削除する注釈ルールを見つけます。

   フィルター ボックスに値を入力して注釈ルールをフィルターしたり、ページ番号をクリックしてページごとに注釈ルールを参照したりできます。

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*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確認メッセージが表示されます。

5. [OK]をクリックします

注釈のインポート

Data Infrastructure Insights には、CSV ファイルから注釈または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

管理 **> API**アクセス*リンクには"ドキュメント"***Assets/Import** API 用。このドキュメントには、.CSV ファイル形式に関する情報が含まれています。



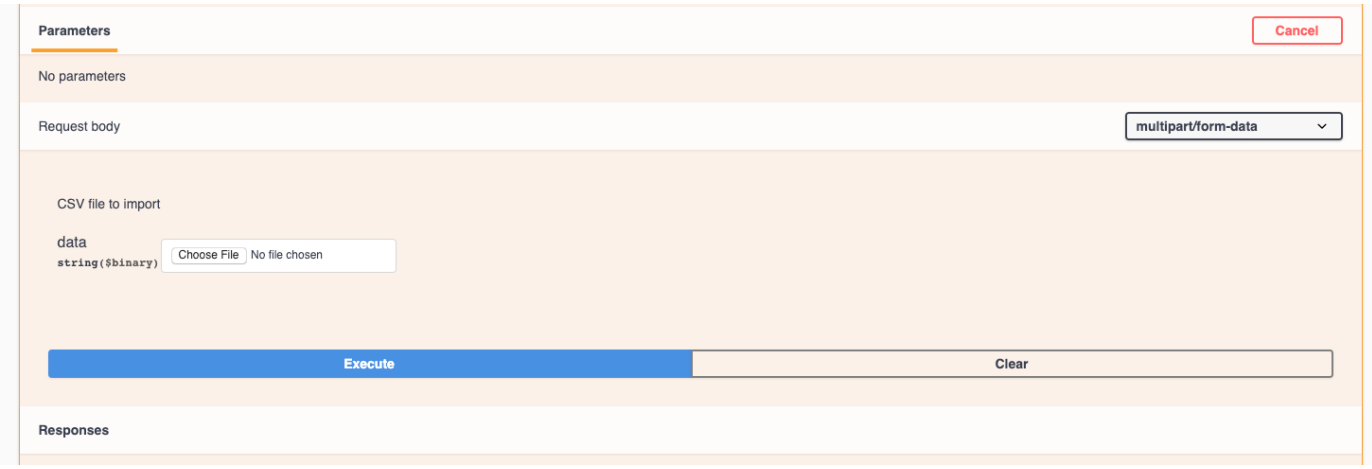
.CSVファイル形式

CSV ファイルの一般的な形式は次のとおりです。ファイルの最初の行はインポート フィールドを定義し、フィールドの順序を指定します。その後に、注釈またはアプリケーションごとに個別の行が続きます。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 ドキュメントを参照してください。

API Swagger 自体から .CSV ファイルから注釈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て、[実行] ボタンをクリックするだけです。



インポート動作

インポート操作中、インポートされるオブジェクトとオブジェクト タイプに応じて、データが追加、結合、または置換されます。インポート中は、次の動作に注意してください。

- ターゲット システムに同じ名前の注釈またはアプリケーションが存在しない場合は、注釈またはアプリケーションを追加します。
- 注釈タイプがリストであり、ターゲット システムに同じ名前の注釈が存在する場合は、注釈をマージします。
- 注釈タイプがリスト以外で、ターゲット システムに同じ名前の注釈が存在する場合は、注釈を置き換えます。

注意: ターゲット システムに同じ名前だがタイプが異なる注釈が存在する場合、インポートは失敗します。オブジェクトが失敗した注釈に依存している場合、それらのオブジェクトには不正確な情報や不要な情報が表示される可能性があります。インポート操作が完了したら、すべての注釈の依存関係を確認する必要があります。

- 注釈の値が空の場合、その注釈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。
- 日付型の注釈値は、ミリ秒単位の Unix 時間として渡す必要があります。
- ボリュームまたは内部ボリュームに注釈を付ける場合、オブジェクト名は「->」区切り文字を使用したストレージ名とボリューム名の組み合わせになります。例: <ストレージ名>-><ボリューム名>
- オブジェクト名にコ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。例: *"NetApp1,NetApp2"->023F*
- ストレージ、スイッチ、ポートに注釈を添付する場合、「アプリケーション」列は無視されます。
- テナント、Line_Of_Business、Business_Unit、および/またはプロジェクトによってビジネス エンティティが構成されます。すべてのビジネス エンティティと同様に、いずれかの値が空になる場合があります。

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 <名前> または <IP>
VM	id-><id> または <名前>
ストレージプール	id-><id> または <ストレージ名>-><ストレージプール名>
内部ボリューム	id-><id> または <ストレージ名>-><内部ボリューム名>
Volume	id-><id> または <ストレージ名>-><ボリューム名>
ストレージ	id-><id> または <名前> または <IP>
スイッチ	id-><id> または <名前> または <IP>
ポート	id-><id> または <WWN>
qtree	id-><id> または <ストレージ名>-><内部ボリューム名>-><Qtree 名>
共有	id-><id> または <ストレージ名>-><内部ボリューム名>-><共有名>-><プロトコル>[-><Qtree 名 (デフォルトの Qtree の場合はオプション)>]

アプリケーションの操作

アプリケーション別の資産使用状況の追跡

会社の環境で使用されているアプリケーションを理解することは、資産の使用状況とコストを追跡するのに役立ちます。

テナントで実行されているアプリケーションに関連付けられたデータを追跡する前に、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、ハイパーバイザーなどの資産に関連付けることができます。

このトピックでは、マーケティング チームが Exchange 電子メールに使用する仮想マシンの使用状況を追跡する例を示します。

次のような表を作成して、テナントで使用されるアプリケーションを識別し、各アプリケーションを使用しているグループまたはビジネス ユニットを記録することをお勧めします。

テナント	事業分野	Business Unit（ビジネス ユニット）	プロジェクト	アプリケーション
NetApp	データストレージ	法律上の	特許	Oracle Identity Manager、Oracle On Demand 、PatentWiz
NetApp	データストレージ	マーケティング	販売イベント	Exchange、Oracle 共有データベース、BlastOff イベント プランナー

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。 Exchange の仮想マシンの使用率を追跡して、いつストレージを追加する必要があるかを予測できるように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 **>** **+** 新しいクエリ に移動して、仮想マシンの新しいクエリを作成します (または、該当する場合は既存の VM クエリを選択します)。

   マーケティング チームの VM の名前にはすべて「**mkt**」という文字列が含まれていると仮定して、VM 名を「mkt」でフィルターするクエリを作成します。

3. VMを選択します。
4. 一括操作 **>** アプリケーションの追加 を使用して、VM を *Exchange* アプリケーションに関連付けます。
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

テナント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たデータを追跡するには、 Data Infrastructure Insightsでアプリケーションを定義できます。

タスク概要

Data Infrastructure Insights を使用すると、使用状況やコストのレポートなど、アプリケーションに関連付けられた資産からのデータを追跡できます。

手順

1. Data Infrastructure Insightsサイト メニューで、可観測性 **>** エンリッチ **>** アプリケーション 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*をクリックします。

アプリケーションを定義したら、それを資産に割り当てることができます。

資産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資産を見つけます。
2. クエリ **>** **+**新しいクエリ をクリックし、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クリックします。
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. 資産を割り当てるアプリケーションを選択します。

割り当てた新しいアプリケーションは、別のアセットから派生したアセット上のアプリケーションを上書きします。たとえば、ボリュームはホストからアプリケーションを継承し、新しいアプリケーションがボリュームに割り当てられると、新しいアプリケーションは派生アプリケーションよりも優先されます。

関連する資産が大量にある環境では、それらの資産へのアプリケーション割り当ての継承に数分かかることがあります。関連する資産が多数ある場合は、継承が発生するまでにさらに時間がかかります。

終了後の操作

ホストをアプリケーションに割り当てた後、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、[管理] > [アプリケーション] をクリックし、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を使用して監視するすべてのデバイスを特定する必要があります。テナントのパフォーマンスと在庫を正確に追跡するには、識別が必要です。通常、テナント上で検出されたデバイスの大部分は、自動デバイス解決 によって識別されます。

データ コレクターを構成すると、スイッチ、ストレージ アレイ、ハイパーバイザーと VM の仮想インフラストラクチャなど、テナント上のデバイスが識別されます。ただし、通常、これによってテナント上のデバイス

が 100% 識別されるわけではありません。

データ コレクター タイプのデバイスを構成した後は、デバイス解決ルールを活用してテナントに残っている不明なデバイスを識別するのがベスト プラクティスです。デバイスの解決は、次のデバイス タイプとして不明なデバイスを解決するのに役立ちます。

- 物理ホスト
- ストレージ アレイ
- テープ

デバイスの解決後も不明のままになっているデバイスは汎用デバイスとみなされ、クエリやダッシュボードにも表示できます。

作成されたルールは、環境に追加された新しいデバイスと同様の属性を持つ新しいデバイスを自動的に識別します。場合によっては、デバイス解決により、Data Infrastructure Insights内で検出されていないデバイスのデバイス解決ルールをバイパスして手動で識別することも可能になります。

デバイスの識別が不完全な場合、次のような問題が発生する可能性があります。

- 不完全なパス
- 未確認のマルチパス接続
- アプリケーションをグループ化できない
- 不正確なトポロジビュー
- データウェアハウスとレポート内の不正確なデータ

デバイス解決機能 ([管理] > [デバイス解決]) には次のタブが含まれており、各タブはデバイス解決の計画と結果の表示に役立ちます。

- ファイバー チャネル識別 には、自動デバイス解決では解決されなかったファイバー チャネル デバイスの WWN とポート情報のリストが含まれています。このタブには、識別されたデバイスの割合も表示されます。
- **IP** アドレス識別 には、自動デバイス解決では識別されなかった CIFS 共有および NFS 共有にアクセスするデバイスのリストが含まれています。このタブには、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、ファイバー チャネル デバイスの解決を実行するときに実行されるルールのリストが含まれています。これらは、識別されていないファイバー チャネル デバイスを解決するために作成するルールです。
- 環境設定 では、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に使用する構成オプションが提供されます。

開始前の準備

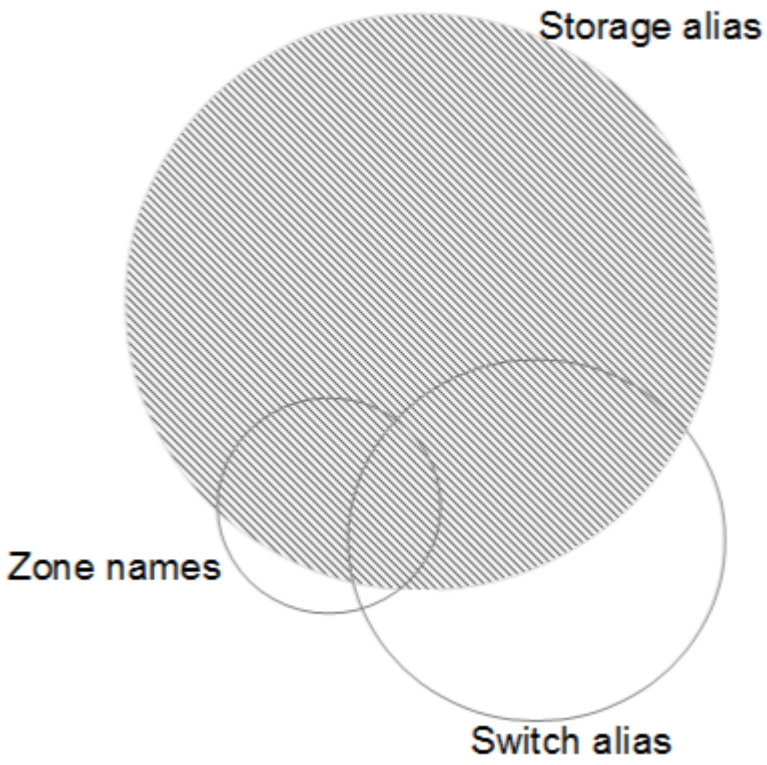
デバイスを識別するためのルールを定義する前に、環境がどのように構成されているかを知っておく必要があります。環境について詳しく知れば知るほど、デバイスを識別しやすくなります。

正確なルールを作成するには、次のような質問に答える必要があります。

- あなたの環境にはゾーンまたはホストの命名標準がありますか? また、それらの正確さはどのくらいの割合ですか?

- ご使用の環境ではスイッチ エイリアスまたはストレージ エイリアスが使用されており、それらはホスト名と一致していますか?
- テナントの命名スキームはどのくらいの頻度で変更されますか?
- 異なる命名スキームを導入した買収や合併はありましたか?

環境を分析した後、信頼性に関係する可能性のある命名標準を特定できるはずです。収集した情報は、次のような図でグラフ化されることがあります。



この例では、最大数のデバイスがストレージ エイリアスによって確実に表されます。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、スイッチ エイリアスを使用するルールを次に記述し、最後に作成されるルールではゾーン エイリアスを使用する必要があります。ゾーン エイリアスとスイッチ エイリアスの使用が重複するため、一部のストレージ エイリアス ルールで追加のデバイスが識別され、ゾーン エイリアスとスイッチ エイリアスに必要なルールが少なくなる場合があります。

デバイスを識別する手順

通常、テナント上のデバイスを識別するには、次のようなワークフローを使用します。識別は反復的なプロセスであり、ルールの計画と調整に複数のステップが必要になる場合があります。

- 研究環境
- 計画ルール
- ルールの作成/修正
- レビュー結果
- 追加のルールを作成するか、デバイスを手動で識別する
- 完了

テナントに識別されていないデバイス (不明デバイスまたは汎用デバイスとも呼ばれる) があり、その後ポーリング時にそれらのデバイスを識別するデータ ソースを構成すると、それらのデバイスは汎用デバイスとして表示またはカウントされなくなります。

関連している："デバイス解決ルールの作成" "ファイバーチャネルデバイスの解像度" "IPデバイスの解像度" "デバイスの解像度の設定"

デバイス解像度ルール

現在Data Infrastructure Insightsによって自動的に識別されないホスト、ストレージ、およびテープを識別するためのデバイス解決ルールを作成します。作成するルールは、現在環境内にあるデバイスを識別し、環境に追加された類似のデバイスも識別します。

デバイス解決ルールの作成

ルールを作成するときは、まず、ルールが実行される情報のソース、情報の抽出に使用する方法、およびルールの結果に DNS ルックアップが適用されるかどうかを特定します。

デバイスを識別するために使用されるソース	* ホストの SRM エイリアス * 埋め込まれたホスト名またはテープ名を含むストレージ エイリアス * 埋め込まれたホスト名またはテープ名を含むスイッチ エイリアス * 埋め込まれたホスト名を含むゾーン名
ソースからデバイス名を抽出するために使用される方法	* そのまま（SRMから名前を抽出） * 区切り文字 * 正規表現
DNSルックアップ	DNSを使用してホスト名を検証するかどうかを指定します

自動解決ルール タブでルールを作成します。次の手順では、ルール作成プロセスについて説明します。

手順

1. *管理 > デバイスの解像度*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*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、[一致条件の表示] 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、ホストを識別するため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 は次の応答を表示します。

   a. ゾーン には、Data Infrastructure Insightsによって識別される必要があるゾーンと WWN がリストされます。

b. **SRM** は、Data Infrastructure Insightsによって識別される必要がある未識別のエイリアスをリストします。

c. *ストレージエイリアス*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をリストします。

d. *スイッチエイリアス*は、Data Infrastructure Insightsで識別する必要があるスイッチエイリアスをリストします。

5. 方法 リストで、ホストを識別するために使用する方法を選択します。

ソース	方法
SRM	そのまま、区切り文字、正規表現
ストレージエイリアス	区切り文字、正規表現
エイリアスを切り替える	区切り文字、正規表現
ゾーン	区切り文字、正規表現

◦ 区切り文字を使用するルールでは、区切り文字とホスト名の最小長が必要です。ホスト名の最小長は、 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 は、この長さ以上であるホスト名に対してのみ DNS ルックアップを実行します。

区切り文字を使用するルールの場合、入力文字列は区切り文字によってトークン化され、隣接するトークンのいくつかの組み合わせを作成することによってホスト名候補のリストが作成されます。リストは最大から最小の順に並べ替えられます。たとえば、入力ストリングが *vipsnq03_hba3_emc3_12ep0* の場合、リストは次のようになります。

- vipsnq03_hba3_emc3_12ep0
- vipsnq03_hba3_emc3
- hba3 emc3_12ep0
- vipsnq03_hba3
- emc3_12ep0
- hba3_emc3
- vipsnq03
- 12話0話
- emc3
- hba3

◦ 正規表現を使用するルールでは、正規表現、形式、大文字と小文字の区別の選択が必要です。

6. すべてのルールを実行するには、[**AR** を実行] をクリックします。作成したルール (および AR の最後の完全実行以降に作成されたその他のルール) を実行するには、ボタンの下矢印をクリックします。

ルール実行の結果は **FC** 識別 タブに表示されます。

デバイスの解像度の自動更新を開始します

デバイス解像度の更新では、前回の完全自動デバイス解像度実行以降に追加された手動変更がコミットされます。更新を実行すると、デバイスの解像度構成に対して行われた新しい手動エントリのみをコミットして実行

できます。完全なデバイス解像度の実行は実行されません。

手順

1. Data Infrastructure Insights Web UI にログインします。
2. *管理 > デバイスの解像度*をクリックします
3. *デバイス解像度*画面で、*AR 実行*ボタンの下向き矢印をクリックします。
4. 更新を開始するには、[更新] をクリックします。

ルール支援による手動識別

この機能は、特定のルールまたはルールのリスト（1 回限りの並べ替えの有無にかかわらず）を実行して、不明なホスト、ストレージ、およびテープ デバイスを解決する特殊な場合に使用されます。

開始する前に

識別されていないデバイスがいくつかあり、他のデバイスを正常に識別したルールも複数あります。

ソースにホスト名またはデバイス名の一部のみが含まれている場合は、正規表現ルールを使用してフォーマットし、不足しているテキストを追加します。

手順

1. Data Infrastructure Insights Web UI にログインします。
2. *管理 > デバイスの解像度*をクリックします
3. *ファイバーチャネル識別*タブをクリックします。

   システムは、デバイスとその解決ステータスを表示します。

4. 識別されていないデバイスを複数選択します。
5. *一括アクション*をクリックし、*ホスト解像度の設定*または*テープ解像度の設定*を選択します。

   システムは、デバイスを正常に識別したすべてのルールのリストを含む「識別」画面を表示します。

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てください。

Data Infrastructure Insights は、メソッドが表示されている順序で、上位のメソッドから順にホスト解決プロセスを実行します。

適用されるルールに遭遇すると、ルール名がルール列に表示され、手動として識別されます。

関連している："ファイバーチャネルデバイスの解像度" "IPデバイスの解像度" "デバイスの解像度の設定"

ファイバーチャネルデバイスの解像度

ファイバー チャネル識別画面には、自動デバイス解決によってホストが識別されなかっ

たファイバー チャネル デバイスの WWN と WWPN が表示されます。画面には、手動デバイス解決によって解決されたデバイスも表示されます。

手動解決によって解決されたデバイスには、*OK* のステータスが含まれ、デバイスを識別するために使用されたルールが識別されます。見つからないデバイスのステータスは「未識別」になります。識別から明示的に除外されているデバイスのステータスは「除外」になります。デバイスの識別の全範囲はこのページに記載されています。

ファイバー チャネル識別画面の左側で複数のデバイスを選択して、一括操作を実行します。デバイスの上にマウスを移動し、リストの右端にある [識別] または [未識別] ボタンを選択すると、単一のデバイスに対してアクションを実行できます。

合計カバレッジ リンクには、識別されたデバイスの数/構成で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
- エイリアスを切り替える
- ゾーン
- ユーザー定義

ファイバーチャネルデバイスを手動で追加する

デバイス解決のファイバー チャネル識別タブで使用可能な 手動追加 機能を使用して、ファイバー チャネル デバイスをData Infrastructure Insightsに手動で追加できます。このプロセスは、将来発見されると予想されるデバイスの事前識別に使用される可能性があります。

開始する前に

デバイス ID をシステムに正常に追加するには、WWN または IP アドレスとデバイス名を知っておく必要があります。

タスク概要

ホスト、ストレージ、テープ、または不明なファイバー 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にログインする
2. *管理 > デバイスの解像度*をクリックします
3. *ファイバーチャネル識別*タブをクリックします。
4. *追加*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、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、ファイバー チャネル識別タブのデバイス リストに追加されます。ルールは_手動_として識別されます。

.CSV ファイルからファイバー チャネル デバイス ID をインポートする

CSV ファイル内のデバイスのリストを使用して、ファイバー チャネル デバイス ID をData Infrastructure Insights のデバイス解決に手動でインポートできます。

1. 開始する前に

デバイス ID をデバイス解決に直接インポートするには、正しくフォーマットされた .CSV ファイルが必要です。ファイバー 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	Name	タイプ

以下の例に示すように、データ フィールドは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、最初にファイバー チャネル識別情報を .CSV ファイルにエクスポートし、そのファイルで必要な変更を加えてから、そのファイルをファイバー チャネル識別に再度インポートすることをお勧めします。これにより、必要な列が存在し、適切な順序になっていることが保証されます。

ファイバーチャネル識別情報をインポートするには:

1. Data Infrastructure Insights Web UI にログインします。
2. *管理 > デバイスの解像度*をクリックします
3. *ファイバーチャネル識別*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 ファイルが含まれているフォルダーに移動し、目的のファイルを選択します。

   入力したデバイスは、ファイバー チャネル識別タブのデバイス リストに追加されます。 「ルール」は手動として識別されます。

ファイバーチャネルデバイス**ID**を**.CSV**ファイルにエクスポートする

Data Infrastructure Insights のデバイス解決機能から、既存のファイバー チャネル デバイス ID を .CSV ファイルにエクスポートできます。デバイス ID をエクスポートして変更し、 Data Infrastructure Insightsに再度インポートして、エクスポートした ID に元々一致していたデバイスに類似したデバイスを識別するために使用することができます。

タスク概要

このシナリオは、デバイスに類似した属性があり、それらを .CSV ファイルで簡単に編集してシステムに再度インポートできる場合に使用される可能性があります。

ファイバー チャネル デバイス ID を .CSV ファイルにエクスポートすると、ファイルには次の情報が表示されている順序で含まれます。

WWN	IP	Name	タイプ

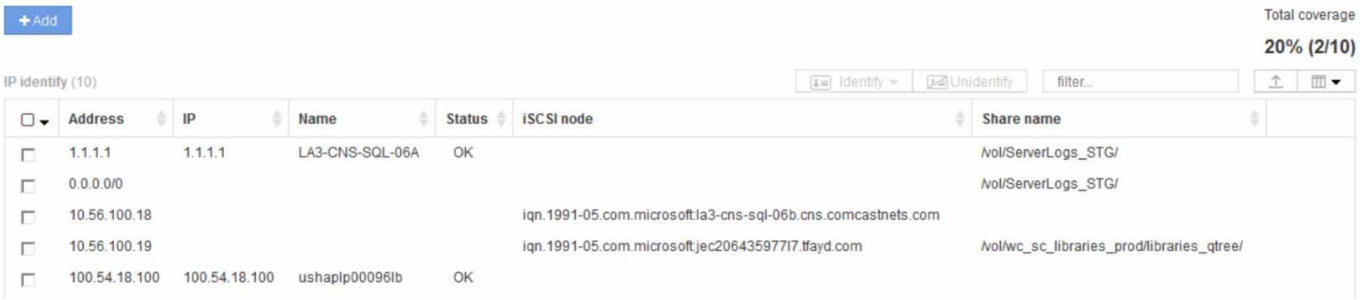
手順

1. Data Infrastructure Insights Web UI にログインします。
2. *管理 > デバイスの解像度*をクリックします
3. *ファイバーチャネル識別*タブを選択します。
4. 識別子をエクスポートするファイバー チャネル デバイスを選択します。
5. *エクスポート*をクリックします ボタン。

関連している："IPデバイスの解像度" "デバイス解決ルールの作成" "デバイスの解像度の設定"

IPデバイスの解像度

IP 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 および CIFS または NFS 共有が表示されます。識別されていない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、共有名が表示されます。正常に識別され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 識別画面で利用可能な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. *管理 > デバイスの解像度*をクリックします
3. **IP** アドレス識別 タブをクリックします。
4. *追加*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. アドレス、IP アドレス、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 アドレス識別] タブのデバイス リストに追加されます。

.CSV ファイルから IP デバイス ID をインポートする

CSV ファイル内のデバイス ID のリストを使用して、IP デバイス ID をデバイス解決機能に手動でインポートできます。

1. 開始する前に

デバイス ID をデバイス解決機能に直接インポートするには、正しくフォーマットされた .CSV ファイルが必要です。 IP デバイスの .CSV ファイルには次の情報が必要です。

アドレス	IP	Name

以下の例に示すように、データ フィールドは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、最初に IP アドレス識別情報を .CSV ファイルにエクスポートし、そのファイルで必要な変更を加えてから、そのファイルを IP アドレス識別に再度インポートすることをお勧めします。これにより、必要な列が存在し、適切な順序になっていることが保証されます。

IPデバイス識別情報を.CSVファイルにエクスポートする

Data Infrastructure Insights のデバイス解決機能から、既存の IP デバイス ID を .CSV ファイルにエクスポートできます。デバイス ID をエクスポートして変更し、 Data Infrastructure Insightsに再度インポートして、エクスポートした ID に元々一致していたデバイスに類似したデバイスを識別するために使用することができます。

タスク概要

。このシナリオは、デバイスに類似した属性があり、それらを .CSV ファイルで簡単に編集してシステムに再度インポートできる場合に使用される可能性があります。

IP デバイス ID を .CSV ファイルにエクスポートすると、ファイルには次の情報が表示されている順序で含まれます。

アドレス	IP	Name

手順

1. Data Infrastructure Insights Web UI にログインします。
2. *管理 > デバイスの解像度*をクリックします
3. **IP** アドレス識別 タブを選択します。
4. 識別子をエクスポートする IP デバイスを選択します。
5. *エクスポート*をクリックします ボタン"]ボタン。

関連している："ファイバーチャネルデバイスの解像度" "デバイス解決ルールの作成" "デバイスの解像度の設

定"

設定タブのオプションの設定

デバイス解決の設定タブでは、自動解決スケジュールを作成したり、識別に含めるか除外するストレージおよびテープ ベンダーを指定したり、DNS ルックアップ オプションを設定したりできます。

自動解決スケジュール

自動解決スケジュールでは、自動デバイス解決がいつ実行されるかを指定できます。

オプション	説明
間隔	このオプションを使用して、日、時間、または分間隔で自動デバイス解決を実行します。
毎日	このオプションを使用すると、毎日特定の時間に自動デバイス解決を実行できます。
手動	自動デバイス解決を手動でのみ実行するには、このオプションを使用します。
あらゆる環境の変化において	このオプションを使用すると、環境に変化があるたびに自動デバイス解決が実行されます。

Manually を指定すると、夜間の自動デバイス解決は無効になります。

DNS処理オプション

DNS 処理オプションでは、次の機能を選択できます。

- DNS ルックアップ結果処理が有効になっている場合は、解決されたデバイスに追加する DNS 名のリストを追加できます。
- IP の自動解決を選択すると、DNS ルックアップを使用して iSCSI イニシエーターおよび NFS 共有にアクセスするホストの自動ホスト解決が有効になります。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許可し、結果に標準のポートエイリアスの代わりに「接続先」エイリアスを使用するように選択できます。

特定のストレージおよびテープベンダーを含めるか除外するか

自動解決のために特定のストレージおよびテープ ベンダーを含めたり除外したりできます。たとえば、特定のホストがレガシー ホストになり、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場合は、特定のベンダーを除外する必要があるかもしれません。以前除外したが、今後は除外したくないベンダーを再度追加することもできます。

テープ デバイス解決ルールは、ベンダー設定でその WWN のベンダーが [テープとしてのみ含める] に設定されている WWN に対してのみ機能します。

参照:"正規表現の例"

正規表現の例

ソース命名戦略として正規表現アプローチを選択した場合は、正規表現の例を、Data Infrastructure Insights の自動解決方法で使用する独自の式のガイドとして使用できます。

正規表現のフォーマット

Data Infrastructure Insightsの自動解決用の正規表現を作成するときに、*FORMAT* というフィールドに値を入力して出力形式を構成できます。

デフォルト設定は \1 です。これは、正規表現に一致するゾーン名が、正規表現によって作成された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、変数値は括弧内のステートメントによって作成されます。括弧内のステートメントが複数ある場合、変数は左から右へ数値的に参照されます。変数は出力形式で任意の順序で使用できます。定数テキストを FORMAT フィールドに追加することで、出力に挿入することもできます。

たとえば、このゾーン命名規則では次のゾーン名が考えられます。

```
 [Zone number]_[data center]_[hostname]_[device type]_[interface number]
* S123_マイアミ_ホスト名1_filer_FC1
* S14_タンパ_ホスト名2_スイッチ_FC4
* S3991_ボストン_ホスト名3_windows2K_FC0
* S44_Raleigh_ホスト名4_solaris_FC1
```

出力を次の形式にしたい場合があります。

```
 [hostname]-[data center]-[device type]
```

これを行うには、ホスト名、データセンター、デバイス タイプ
フィールドを変数にキャプチャし、出力で使用する必要があります。次の正規表現はこれを実行します。

```
 .*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
```

括弧が `3` セットあるため、変数 `\1`、`\2`、`\3` に値が設定されます。

次に、次の形式を使用して、希望する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、フォーマットされた出力に挿入される定数テキストの例を示します。

例

ゾーン名を示す例**1**

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

ホスト名を取得するために使用できる正規表現は次のようになります。

```
 S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
```

結果は、`S` で始まり、その後に任意の数字の組み合わせ、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`、および `1` つの数字 `(0 ～ 9)` が続くすべてのゾーンに一致します。ホスト名のみが `*\1*` 変数に保存されます。

正規表現は、次の構成要素に分解できます。

- 「S」はゾーン名を表し、式の始まりとなります。これは、ゾーン名の先頭の「S」のみに一致します。
- 括弧内の文字 [0-9] は、「S」に続く文字が 0 から 9 までの数字でなければならないことを示します。
- + 記号は、前の括弧内の情報が 1 回以上出現する必要があることを示します。
- _ (アンダースコア) は、ゾーン名では S の後の数字の直後にアンダースコア文字のみが続く必要があることを意味します。この例では、ゾーンの命名規則により、アンダースコアを使用してゾーン名とホスト名を区別しています。
- 必須のアンダースコアの後の括弧は、その中に含まれるパターンが \1 変数に格納されることを示します。
- 括弧で囲まれた文字 [a-zA-Z0-9] は、一致する文字がすべて文字（大文字と小文字を区別しない）と数字であることを示します。
- 括弧の後の * (アスタリスク) は、括弧内の文字が 0 回以上出現することを示します。
- 括弧で囲まれた文字 [_-] (アンダースコアとダッシュ) は、英数字パターンの後にアンダースコアまたはダッシュが続く必要があることを示します。
- 正規表現内の文字 HBA は、この文字シーケンスがゾーン名に正確に出現する必要があることを示します。
- 最後の括弧で囲まれた文字セット [0-9] は、0 から 9 までの 1 つ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「」までスキップし、*E* とその後の *2* 番目の「」までのすべてを一致させてから、それ以降のすべてをスキップします。

ゾーン: Z_E2FHDBS01_E1NETAPP

ホスト名: E2FHDBS01

正規表現: .*?(E.?).*?

例3

正規表現 (下記) の最後のセクションを囲む括弧「()」は、どの部分がホスト名であるかを識別します。VSAN3 をホスト名にする場合は、_([a-zA-Z0-9]).* になります。

ゾーン: A_VSAN3_SR48KENT_A_CX2578_SPA0

ホスト名: SR48KENT

正規表現: _[a-zA-Z0-9]+_([a-zA-Z0-9]).*

より複雑な命名パターンを示す例4

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

これらをキャプチャするために使用できる正規表現は次のようになります。

```
([a-zA-Z0-9]*)_.*
```

この式で評価された後、`\1` 変数には `_myComputerName123_` のみが含まれます。

正規表現は、次の構成要素に分解できます。

- 括弧は、その中に含まれるパターンが \1 変数に格納されることを示します。
- 括弧で囲まれた文字 [a-zA-Z0-9] は、任意の文字 (大文字と小文字を区別しない) または数字が一致することを意味します。
- 括弧の後の * (アスタリスク) は、括弧内の文字が 0 回以上出現することを示します。
- 正規表現内の _ (アンダースコア) 文字は、ゾーン名には、先行する括弧に一致する英数字文字列の直後にアンダースコアが必要であることを意味します。
- その。 (ピリオド) は任意の文字と一致します (ワイルドカード)。
- * (アスタリスク) は、先行するピリオド ワイルドカードが 0 回以上出現する可能性があることを示します。

  つまり、.* の組み合わせは、任意の文字を任意の回数示します。

例**5**：パターンなしのゾーン名を示す

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。

- 私のコンピュータ名_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

これらをキャプチャするために使用できる正規表現は次のようになります。

```
(.*?)_.*
```

`\1` 変数には、`_myComputerName_`（最初のゾーン名の例） または `_myComputerName123_`（2番目のゾーン名の例）
が含まれます。したがって、この正規表現は最初のアンダースコアより前のすべてに一致します。

正規表現は、次の構成要素に分解できます。

- 括弧は、その中に含まれるパターンが \1 変数に格納されることを示します。
- 。* (ピリオド アスタリスク) は任意の文字に任意の回数一致します。
- 括弧の後の * (アスタリスク) は、括弧内の文字が 0 回以上出現することを示します。
- ? 文字により、一致は非貪欲になります。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一致が停止されるようになります。
- 文字 _.* は、最初に見つかったアンダースコアとそれに続くすべての文字と一致します。

例**6**：パターン付きコンピュータ名の表示

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。

- ストレージ1_スイッチ1_myComputerName123A_A1_FC1
- ストレージ2_スイッチ2_myComputerName123B_A2_FC2
- ストレージ3_スイッチ3_myComputerName123T_A3_FC3

これらをキャプチャするために使用できる正規表現は次のようになります。

```
.*?_.*?_([a-zA-Z0-9]*[ABT])_.*
```

ゾーンの命名規則にはより多く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` で終わるホスト名（例では `myComputerName`）
のすべてのインスタンスと一致し、そのホスト名を `\1` 変数に配置します。

正規表現は、次の構成要素に分解できます。

- 。* (ピリオド アスタリスク) は任意の文字に任意の回数一致します。
- ? 文字により、一致は非貪欲になります。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一致が停止されるようになります。
- 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と一致します。

- したがって、最初の .*?_ の組み合わせは、最初のゾーン名の例の文字 Storage1_ と一致します。
- 2 番目の .*?_ の組み合わせは最初のものと同じように動作しますが、最初のゾーン名の例の Switch1_ と一致します。
- 括弧は、その中に含まれるパターンが \1 変数に格納されることを示します。
- 括弧で囲まれた文字 [a-zA-Z0-9] は、任意の文字 (大文字と小文字を区別しない) または数字が一致することを意味します。
- 括弧の後の * (アスタリスク) は、括弧内の文字が 0 回以上出現することを示します。
- 正規表現 [ABT] 内の括弧で囲まれた文字は、ゾーン名内の A、B、または T のいずれかの 1 文字と一致します。
- 括弧の後の _ (アンダースコア) は、[ABT] 文字一致の後にアンダースコアが続く必要があることを示します。
- 。* (ピリオド アスタリスク) は任意の文字に任意の回数一致します。

したがって、この結果、\1 変数には次のような英数字文字列が含まれることになります。

- いくつかの英数字と2つのアンダースコアが先行する
- アンダースコア（その後に任意の数の英数字）が続く
- 3 番目のアンダースコアの前に、最後の文字が A、B、または T でした。

例**7**

ゾーン**:** myComputerName123_HBA1_Symm1_FA1

ホスト名**:** myComputerName123

正規表現**:** ([a-zA-Z0-9]+)_.*

例**8**

この例では、最初の _ の前にあるすべてのものを検索します。

ゾーン：MyComputerName_HBA1_Symm1_FA1

マイコンピュータ名123_HBA1_Symm1_FA1

ホスト名: MyComputerName

正規表現: (.**?)_.**

例**9**

この例では、最初の _ の後から 2 番目の _ までのすべてを検索します。

ゾーン**:** Z_MyComputerName_StorageName

ホスト名**:** 私のコンピュータ名

正規表現**:** .***?(.?)***.*?

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

ストレージ2_スイッチ2_マイコンピュータ名123B_A2_FC2

ストレージ3_スイッチ3_マイコンピュータ名123T_A3_FC3

ホスト名**:** MyComputerName123

正規表現**:** .**?.?**([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**

角括弧内の ^ (サーカムフレックスまたはキャレット) は式を否定します。たとえば、[^Ff] は大文字または小文字の F 以外のすべてを意味し、[^az] は小文字の a から z 以外のすべてを意味し、上記の例では _ 以外のすべてを意味します。フォーマット 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

正規表現**:** ()_([AB]).* Data Infrastructure Insightsでの形式: \1-\2 ([^_])_ ()_([^_]).* Data Infrastructure Insightsでの形式: \1-\2-\3

例**13**

この例では、ストレージ エイリアスは "\" で区切られており、式では "\\" を使用して、文字列で実際に "\" が使用されていること、およびそれらが式自体の一部ではないことを定義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

正規表現**:** \\.**?\\.**?\\(.*?)

例**14**

この例では、ゾーンの例から「PD-RV-W-AD-2」を抽出します。

ゾーン**:** PD_D-PD-RV-W-AD-2_01

ホスト名**:** PD-RV-W-AD-2

正規表現: -(.*-\d).*

例**15**

この場合のフォーマット設定では、ホスト名に「US-BV-」が追加されます。

ゾーン: SRV_USBVM11_F1

ホスト名: US-BV-M11

正規表現: SRV_USBV([A-Za-z0-9]+)_F[12]

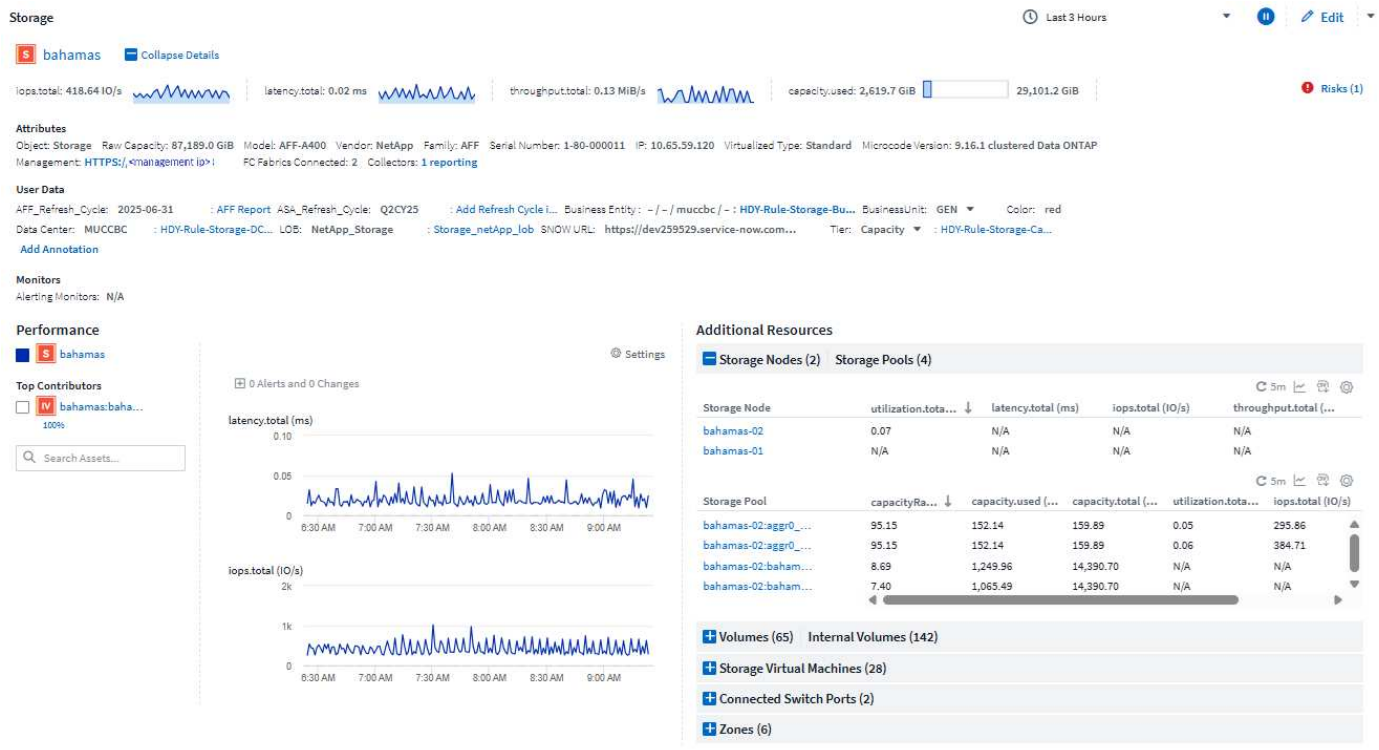
フォーマット: US-BV-\1

資産ページ情報

資産ページの概要

アセット ランディング ページには、アセットの現在のステータスの概要が示され、アセットと関連アセットに関する追加情報へのリンクが含まれています。

ランディング ページでは、概要、パフォーマンス、関連リソース情報を含むオブジェクトの 1 ページ ビューが提供されます。



概要セクション

ランディング ページの上部には、展開可能な概要セクションがあります。このセクションには、スループットやレイテンシなどの最近のデータ傾向、オブジェクトの情報と属性、オブジェクトに対してアラートを発し

ている可能性のあるモニターなどを表示するスパークライン グラフがいくつか含まれています。

概要セクションには、アセットに割り当てられた注釈も表示され、変更することもできます。

パフォーマンスセクション

パフォーマンス セクションには、オブジェクトのパフォーマンス データが表示されます。 設定 を選択して、スループットや容量などの追加のグラフを表示に追加したり、相関または寄与するリソースを選択して、オブジェクトのデータと一緒にグラフ化したりします。競合の原因となる可能性のあるデバイスも、パフォーマンス セクションにリストされます。データ コレクターがポーリングし、更新されたデータが取得されると、グラフ内のデータは自動的に更新されます。

選択できるのは指標選択した期間のパフォーマンス チャートに表示する内容です。 [設定] ドロップダウンをクリックし、リストされている指標から選択します。

パフォーマンス データに加えて、選択したページの時間範囲内でアクティブである、またはアクティブであったアラートも表示されます。



パフォーマンス セクションにリストされる次のデバイスから選択できます。

- 最も相関が高い

  ベース資産に対して 1 つ以上のパフォーマンス メトリックとの相関 (パーセンテージ) が高い資産を表示します。

- トップ貢献者

  基本資産に貢献する資産（パーセンテージ）を表示します。

- 主な変更点

  最近の変更に関連する資産。

- 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与える、または他の共有リソースから影響を受ける資産を表示します。これらは、*greedy* リソースや *degraded* リソースと呼ばれることもあります。

追加リソースセクション

追加リソース セクションには、現在のオブジェクト タイプに関連するリソースのデータ テーブルが表示されます。特定のリソースに焦点を当てるために、これらのテーブルを展開したり折りたたんだりすることができます。歯車アイコンを選択すると、追加のメトリックまたは属性が一時的にテーブルに表示されます。

カスタムウィジェットを追加する

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、カスタム ウィジェットをストレージ アセット ページに追加すると、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。

カスタム ウィジェットは、ランディング ページの下部、パフォーマンス セクションとリソース セクションの下に配置されます。

アセットページの種類

Data Infrastructure Insightsでは、次のアセットのアセット ページが提供されます。

- 仮想マシン
- Storage Virtual Machine（SVM）
- Volume
- 内部容積
- 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
- Application
- ストレージ ノード
- qtree
- ディスク
- VMDK
- ポート
- スイッチ
- ファブリック
- ホスト

- ゾーン

表示データの時間範囲の変更

デフォルトでは、アセット ページには過去 3 時間のデータが表示されますが、アセットの種類に関係なく、すべてのアセット ページにあるオプションを使用して、表示されるデータの時間セグメントを変更できます。時間範囲を変更するには、上部の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
- 最後の30分
- 最後の60分
- 過去 2 時間
- 過去3時間（これがデフォルトです）
- 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 14 日間
- 過去 30 日間
- カスタム時間範囲

カスタム時間範囲では、最大 31 日間連続して選択できます。この範囲の開始時刻と終了時刻を設定することもできます。デフォルトの開始時刻は、選択した最初の日の午前 12:00 で、デフォルトの終了時刻は、選択した最後の日の午後 11:59 です。 「適用」をクリックすると、カスタム時間範囲がアセット ページに適用されます。

ページの情報は、選択した時間範囲に基づいて自動的に更新されます。現在の更新レートは、概要セクションの右上隅と、ページ上の関連するテーブルやウィジェットに表示されます。

パフォーマンスメトリックの定義

パフォーマンス セクションでは、アセットに対して選択した期間に基づいていくつかのメトリックを表示できます。各メトリックは、独自のパフォーマンス チャートに表示されます。表示するデータに応じて、グラフにメトリックや関連アセットを追加したり削除したりできます。選択できるメトリックは、アセットの種類によって異なります。

メトリック	説明
BBクレジットゼロRx、Tx	サンプリング期間中に受信/送信バッファ間クレジット カウントがゼロに移行した回数。このメトリックは、このポートが提供できるクレジットが不足したために、接続されたポートが送信を停止しなければならなかった回数を表します。

BBクレジットゼロ期間取引	サンプリング間隔中に送信 BB クレジットがゼロであった時間 (ミリ秒)。
キャッシュヒット率（合計、読み取り、書き込み）%	キャッシュヒットとなるリクエストの割合。ボリュームへのアクセス数に対するヒット数が多いほど、パフォーマンスは向上します。キャッシュ ヒット情報を収集しないストレージ アレイの場合、この列は空になります。
キャッシュ使用率（合計）%	キャッシュヒットにつながるキャッシュリクエストの合計割合
クラス3の廃棄	ファイバー チャネル クラス 3 データ転送の破棄の数。
CPU使用率（合計）%	アクティブに使用されている CPU リソースの量 (使用可能な合計の割合、すべての仮想 CPU 全体)。
CRC エラー	サンプリング期間中にポートによって検出された無効な巡回冗長検査 (CRC) を持つフレームの数
フレームレート	送信フレームレート（フレーム/秒（FPS））
フレームサイズの平均（Rx、Tx）	トラフィックとフレーム サイズの比率。このメトリックを使用すると、ファブリック内にオーバーヘッド フレームがあるかどうかを識別できます。
フレームサイズが長すぎます	長すぎるファイバー チャネル データ転送フレームの数。
フレームサイズが短すぎます	短すぎるファイバー チャネル 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）で割った IOPS の数。 1 秒あたり TB あたりの I/O 操作数で測定されます。
IOPS（合計、読み取り、書き込み）	単位時間あたりに 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 サービス要求の数 (I/O/秒で測定)
IPスループット（合計、読み取り、書き込み）	合計: IP データが送受信された合計速度 (メガバイト/秒)。
読み取り: IPスループット(受信):	IP データが受信された平均速度（メガバイト/秒）。
書き込み: IPスループット（送信）:	IP データが送信された平均速度（メガバイト/秒）。
レイテンシ（合計、読み取り、書き込み）	レイテンシ (R&W): 一定の時間内に仮想マシンにデータが読み取られたり書き込まれたりする際の速度。値はメガバイト/秒単位で測定されます。
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。
最高レイテンシー:	データ ストア内の仮想マシンからの最長応答時間。
リンク障害	サンプリング期間中にポートによって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の受信または送信リンクのリセットの数。このメトリックは、このポートに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）%	ホストが使用するメモリのしきい値。
部分R/W（合計）%	RAID 5、RAID 1/0、または RAID 0 LUN 内のディスク モジュール上で読み取り/書き込み操作がストライプ境界を越える合計回数。通常、ストライプの越えは、そのたびに追加の I/O が必要になるため、有益ではありません。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（NetApp のLUN）のアライメントは不適切であることを示します。 CLARiiON の場合、この値はストライプ交差の数を IOPS の合計数で割った値です。
ポートエラー	サンプリング期間/指定された期間にわたるポート エラーのレポート。
信号損失数	信号損失エラーの数。信号損失エラーが発生した場合、電気的な接続が存在せず、物理的な問題が発生します。
スワップレート（トータルレート、インレート、アウトレート）	サンプリング期間中にメモリがディスクからアクティブ メモリにスワップイン、スワップアウト、またはその両方されるレート。このカウンターは仮想マシンに適用されます。
同期損失回数	同期損失エラーの数。同期損失エラーが発生すると、ハードウェアはトラフィックを理解したり、ロックしたりすることができません。すべての機器が同じデータ レートを使用していないか、光学接続または物理接続の品質が低い可能性があります。このようなエラーが発生するたびにポートを再同期する必要があり、システムのパフォーマンスに影響を及ぼします。 KB/秒単位で測定されます。
スループット（合計、読み取り、書き込み）	I/O サービス要求に応答して、一定の時間内にデータが送信、受信、またはその両方される速度 (MB/秒で測定)。
タイムアウト破棄フレーム - 送信	タイムアウトによって破棄された送信フレームの数。
トラフィックレート（合計、読み取り、書き込み）	サンプリング期間中に送信、受信、または受信の両方されたトラフィック（メビバイト/秒）。
トラフィック使用率（合計、読み取り、書き込み）	サンプリング期間中の受信/送信/合計トラフィックと受信/送信/合計容量の比率。
使用率（合計、読み取り、書き込み）%	送信 (Tx) および受信 (Rx) に使用される利用可能な帯域幅の割合。
書き込み保留中（合計）	保留中の書き込み I/O サービス要求の数。

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構成するときに、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するように *in-context* フィルターを設定できます。デフォルトでは、ウィジェットを追加すると、テナント上の選択したタイプのすべてのオブジェクトが表示されます。コンテキスト内フィルターを使用すると、現在のアセットに関連するデータのみを表示できます。

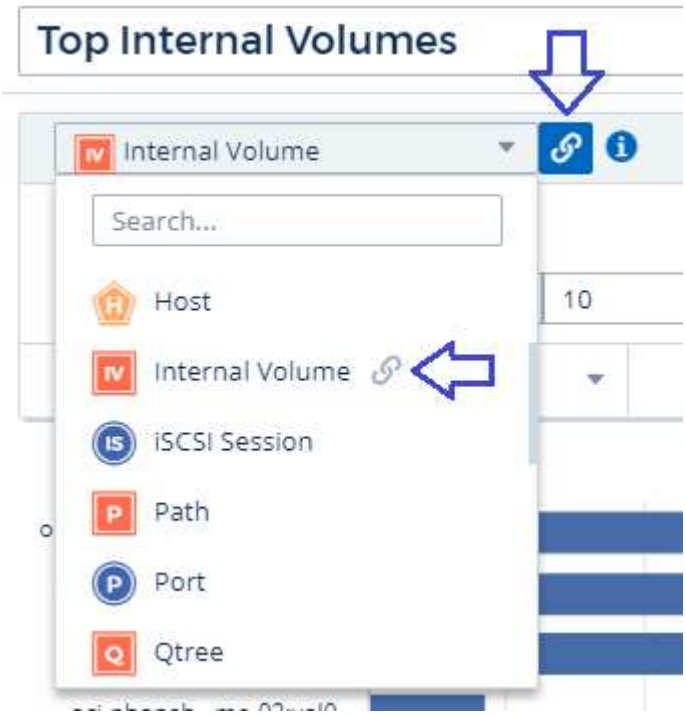
ほとんどのアセット ランディング ページでは、ウィジェットを使用して、現在のアセットに関連するオブジェクトをフィルターできます。フィルター ドロップダウンでは、リンク アイコンが表示されるオブジェクト タイプを、現在のアセットのコンテキスト内でフィルターできます。

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して、そのストレージの内部ボリュームの上位 IOPS 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、テナント上のすべての内部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 **Storage** アセットのアセット ページを開きます。
2. *編集*をクリックすると、アセット ページが編集モードで開きます。
3. *ウィジェットを追加*をクリックし、_棒グラフ_を選択します。
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 オブジェクト タイプの横にリンク アイコンがあることに注意してください。 「リンク」アイコンはデフォルトで有効になっています。



5. _IOPS - 合計_を選択し、必要に応じて追加のフィルターを設定します。
6. *ロールアップ*フィールドの横にある[X]をクリックして折りたたみます。 *表示*フィールドが表示されます。
7. トップ 10 を表示するように選択します。

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 アセットに存在する内部ボリュームのみが表示されます。

ウィジェットは、すべてのストレージ オブジェクトのアセット ページに表示されます。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、棒グラフに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のみが表示されます。

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、チャートにはテナント上のすべてのオブジェクトのデータが表示されます。

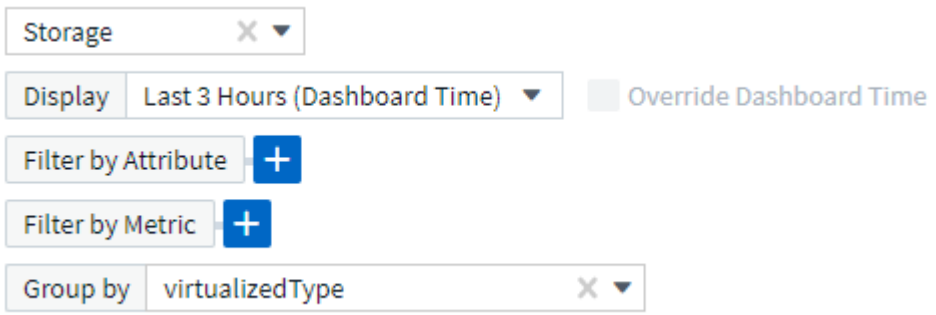
使用することもできます"ウィジェット内の特殊変数"ランディングページに資産関連の情報を表示します。

ストレージ仮想化

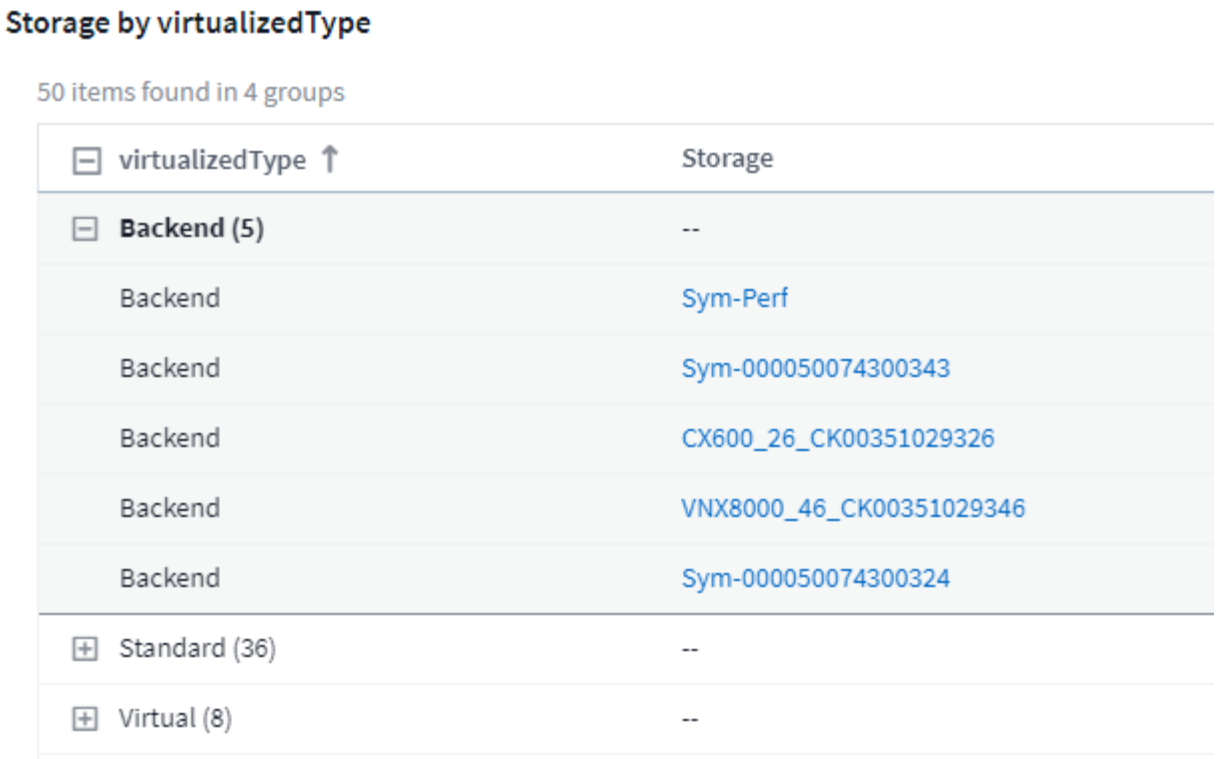
Data Infrastructure Insights は、ローカル ストレージを持つストレージ アレイと他のストレージ アレイの仮想化を区別できます。これにより、インフラストラクチャのフロントエンドからバックエンドに至るまで、コストを関連付け、パフォーマンスを区別できるようになります。

テーブルウィジェットの仮想化

ストレージ仮想化の確認を始める最も簡単な方法の 1 つは、仮想化タイプを表示するダッシュボード テーブル 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構築するときは、グループ化またはフィルターに「virtualizedType」を追加するだけです。

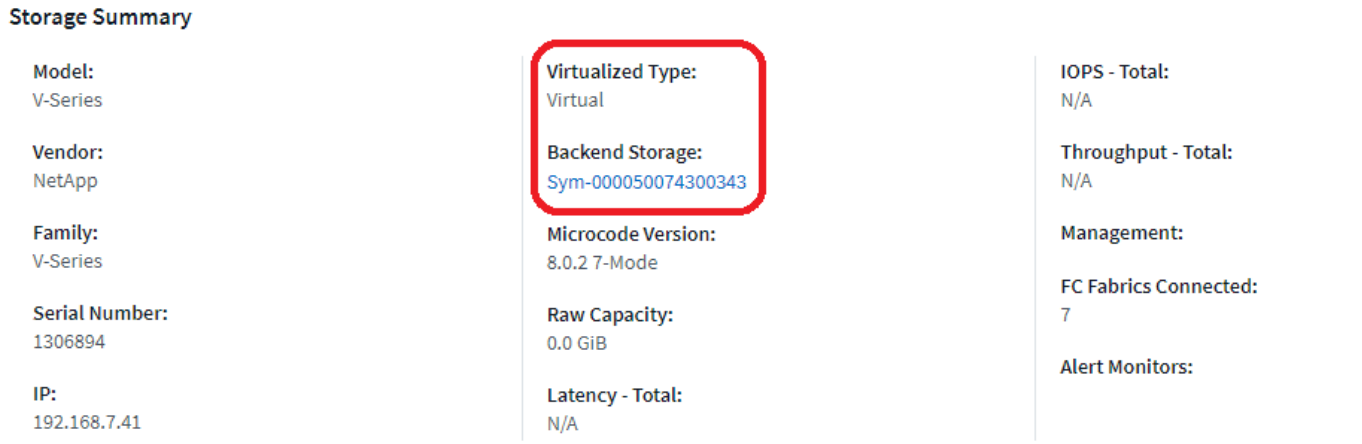


結果のテーブル ウィジェットには、テナント上の *Standard*、*Backend*、および *Virtual* ストレージが表示されます。



ランディングページには仮想化された情報が表示されます

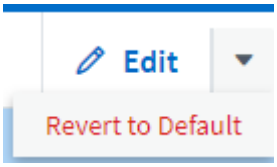
ストレージ、ボリューム、内部ボリューム、またはディスクのランディング ページでは、関連する仮想化情報を確認できます。たとえば、以下のストレージ ランディング ページを見ると、これが仮想ストレージであり、どのバックエンド ストレージ システムが適用されるかがわかります。ランディング ページ上の関連するテーブルにも、該当する場合は仮想化情報が表示されます。



既存のランディングページとダッシュボード

現在、テナントにカスタマイズされたランディング ページまたはダッシュボードがある場合、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ないことに注意してください。ただし、カスタマイズされたダッシュボードやランディング ページを デフォルトに戻す ことはできます (カスタマイズを再実装する必要があります)。また、関連するウィジェットを変更して、必要な仮想化属性やメトリックを含めることもできます。

デフォルトに戻す は、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ります。



資産とアラートを検索するためのヒントとコツ

監視対象環境内のデータやオブジェクトを検索するには、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。
- 検索に使用したフレーズ

  フレーズとは、二重引用符で囲まれた単語のグループです。たとえば、「VNX LUN 5」などです。名前または属性にスペースが含まれるドキュメントを検索するには、二重引用符を使用できます。

- ブール演算子

  ブール演算子 OR、AND、NOT を使用すると、複数の用語を組み合わせてより複雑なクエリを作成できます。

  または

  OR 演算子はデフォルトの結合演算子です。

  2 つの用語の間にブール演算子がない場合、OR 演算子が使用されます。

  OR 演算子は 2 つの用語をリンクし、いずれかの用語がドキュメント内に存在する場合に一致するドキュメントを検索します。

  たとえば、*storage OR netapp* は、*storage* または *netapp* のいずれかを含むドキュメントを検索します。

  ほとんどの用語に一致するドキュメントには高いスコアが与えられます。

  および

  AND 演算子を使用すると、1 つのドキュメント内に両方の検索用語が存在するドキュメントを見つけることができます。たとえば、*storage AND netapp* は、*storage* と *netapp* の両方を含むドキュメントを検索します。

  AND という単語の代わりに、記号 **&&** を使用できます。

  ない

  NOT 演算子を使用すると、NOT の後の用語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* は、*storage* のみが含まれ、*netapp* が含まれないドキュメントを検索します。

  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。

インデックスされた用語を使用して検索する

インデックスされた用語に一致する検索が多いほど、スコアが高くなります。

検索文字列はスペースによって個別の検索用語に分割されます。たとえば、検索文字列「storage aurora netapp」は、「storage」、「aurora」、「netapp」の 3 つのキーワードに分割されます。検索は 3 つの用語すべてを使用して実行されます。これらの用語のほとんどに一致するドキュメントのスコアが最高になります。提供する情報が多ければ多いほど、検索結果は良くなります。たとえば、ストレージを名前とモデルで検索できます。

UI には、カテゴリ全体の検索結果が表示され、カテゴリごとに上位 3 つの結果が表示されます。期待したオブジェクトが見つからなかった場合は、検索文字列にさらに多くの用語を含めることで、検索結果を向上させることができます。

次の表は、検索文字列に追加できるインデックス用語の一覧を示しています。

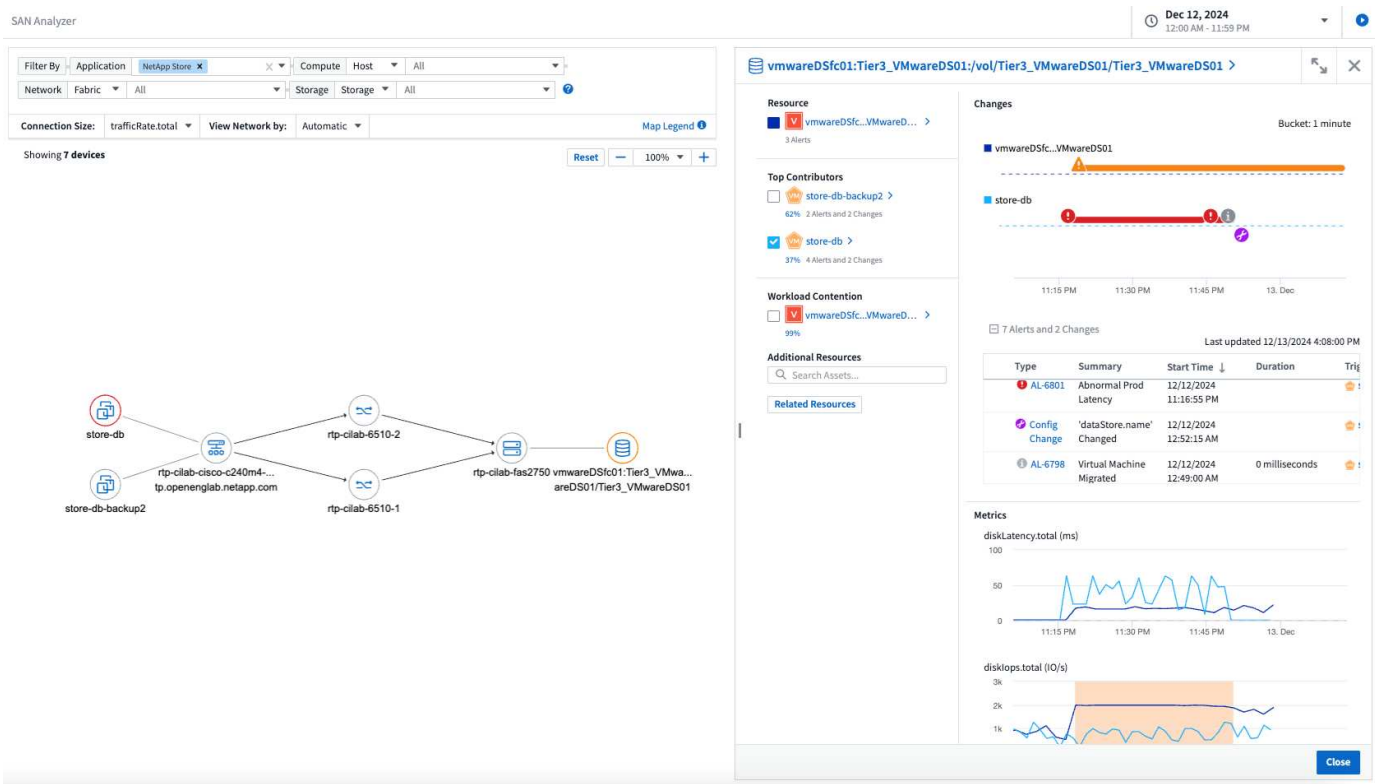
カテゴリ	索引用語
ストレージ	「ストレージ」名ベンダーモデル
ストレージプール	「ストレージプール」名、ストレージの名前、ストレージのIPアドレス、ストレージのシリアル番号、ストレージベンダー、ストレージモデル、関連付けられているすべての内部ボリュームの名前、関連付けられているすべてのディスクの名前
内部容積	「internalvolume」名、ストレージ名、ストレージのIPアドレス、ストレージのシリアル番号、ストレージベンダー、ストレージモデル、ストレージプール名、関連付けられているすべての共有名、関連付けられているすべてのアプリケーション名
Volume	「ボリューム」名ラベル、すべての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	「storagenode」名 ストレージ名 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 IPアドレス 関連す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 仮想センターIP すべてのボリュームの名前 すべての内部ボリュームの名前
仮想マシン	「仮想マシン」名 DNS名 IPアドレス ホストの名前 ホスト名のIPアドレス すべてのデータストアの名前 関連付けられたすべてのアプリケーションの名前
スイッチ（通常およびNPV）	「スイッチ」IPアドレス WWN名 シリアル番号 モデル ドメインID ファブリック名 ファブリックのWWN

カテゴリ	索引用語
Application	「アプリケーション」名 テナント 事業部門 プロジェクト
Tape	「テープ」IPアドレス名シリアル番号ベンダー
ポート	「ポート」WWN名
ファブリック	「ファブリック」WWN名
Storage Virtual Machine（SVM）	「storagevirtualmachine」の名前UUID

データの分析

SANアナライザの概要

SAN は重要なワークロードの処理において重要な役割を果たしますが、その複雑さにより重大な停止や顧客の混乱が生じる可能性があります。 DII の **SAN Analyzer** を使用すると、SAN の管理がよりシンプルかつ効率的になります。この強力なツールは、エンドツーエンドの可視性を提供し、VM/ホストからネットワーク、LUN、ストレージへの依存関係をマッピングします。 SAN Analyzer は、インタラクティブなトポロジ マップを提供することで、問題を正確に特定し、変更を理解し、データ フローの理解を深めることを可能にします。 SAN Analyzer を使用して複雑な IT 環境での SAN 管理を合理化し、ブロック ワークロードの可視性を向上させます。



資産間のつながりを探索する

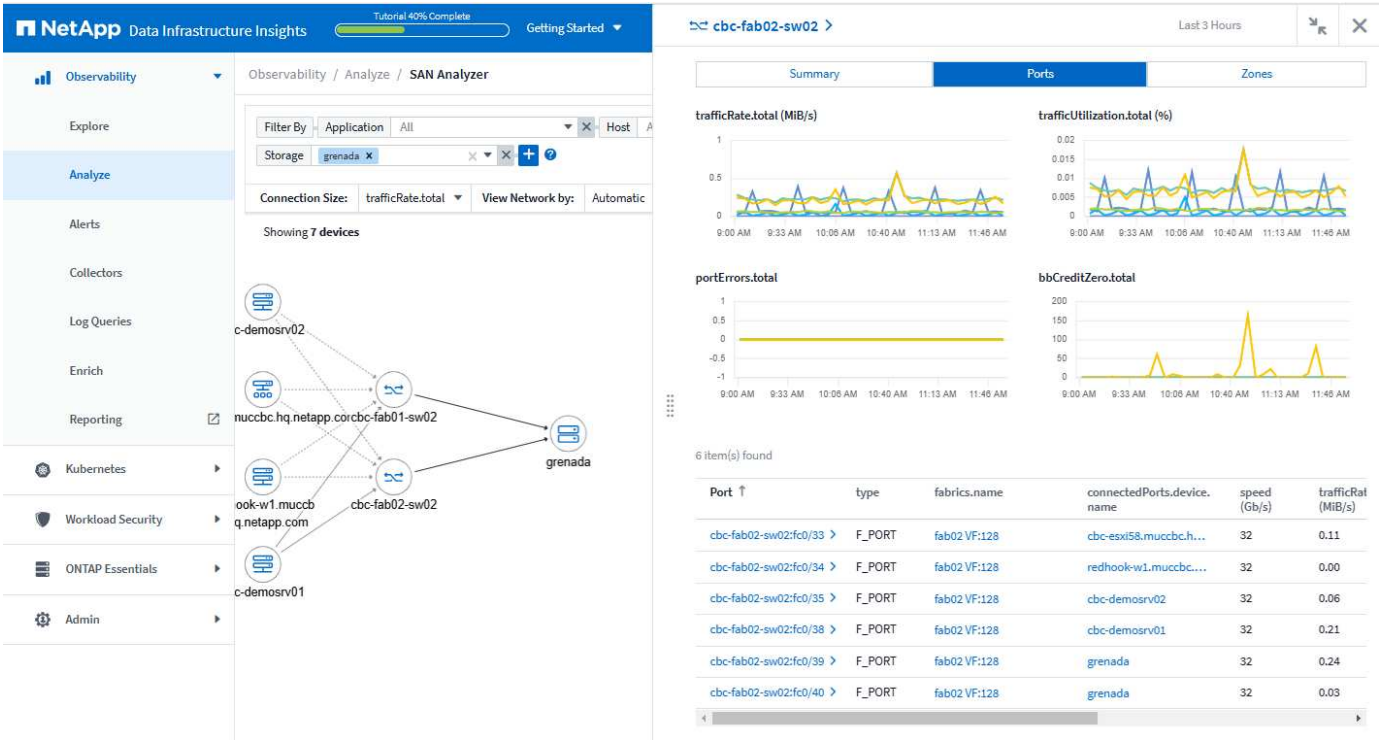
SAN アナライザーを表示するには、**Observability > Analyze > SAN Analyzer** を選択します。アプリケーション、ホスト、ファブリック、ストレージのフィルターを設定します。オブジェクトのマップが表示され、接続されたオブジェクトが示されます。オブジェクトの上にマウスを置くと、その接続のトラフィック メトリックが表示されます。



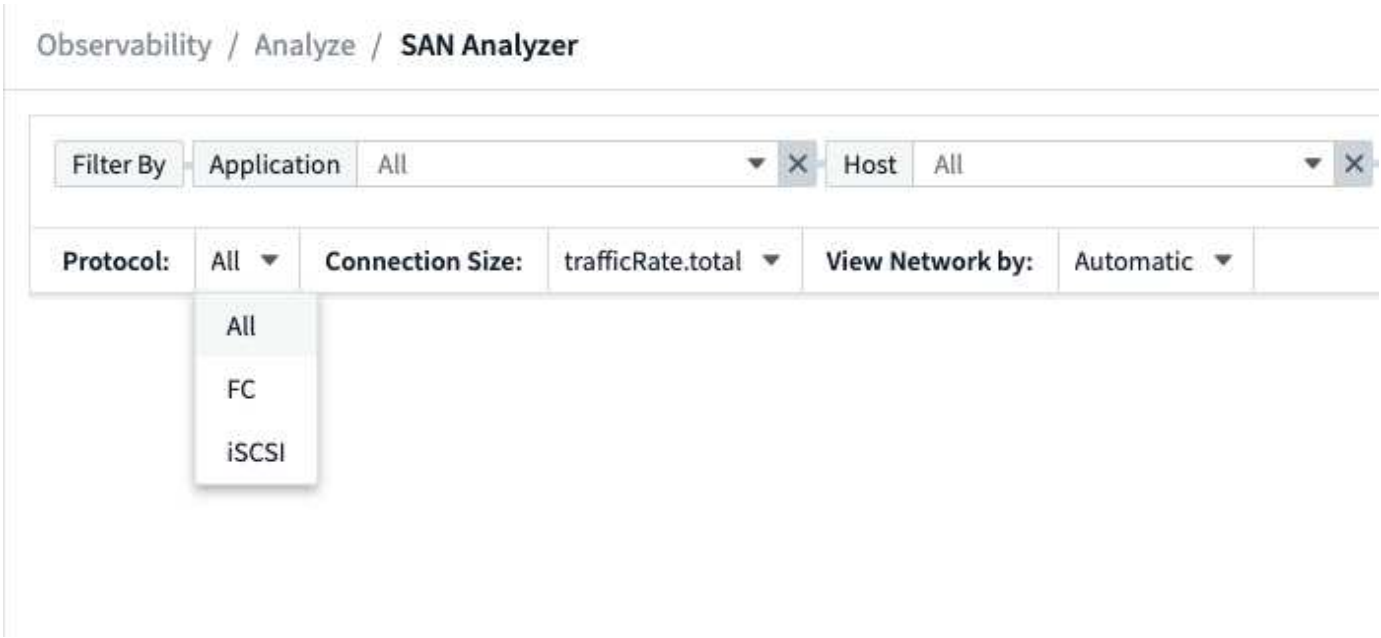
SAN Analyzer のフィルタのほとんどは (追加できるものも含め) コンテキスト依存です。これらのフィルタのいずれかでオブジェクトを選択すると、選択したオブジェクトに応じて、他のフィルタ ドロップダウンに表示される選択肢が更新されます。唯一の例外は、アプリケーション、ポート、スイッチです。これらのフィルターはコンテキストに依存しません。

オブジェクトまたはグループをクリックすると、スライドアウト パネルが開き、オブジェクトとその接続に関する追加の詳細が表示されます。スライドアウト パネルには、選択したオブジェクトの詳細 (オブジェクトのタイプに応じて、IP、ハイパーバイザー、接続されたファブリックなど) を示す概要と、オブジェクトのメトリック (レイテンシや IOPS など) を示すグラフ、および関連する場合は変更とアラートが表示されます。必要に応じて、相関性の高い上位オブジェクトのメトリックもグラフに表示するように選択できます。

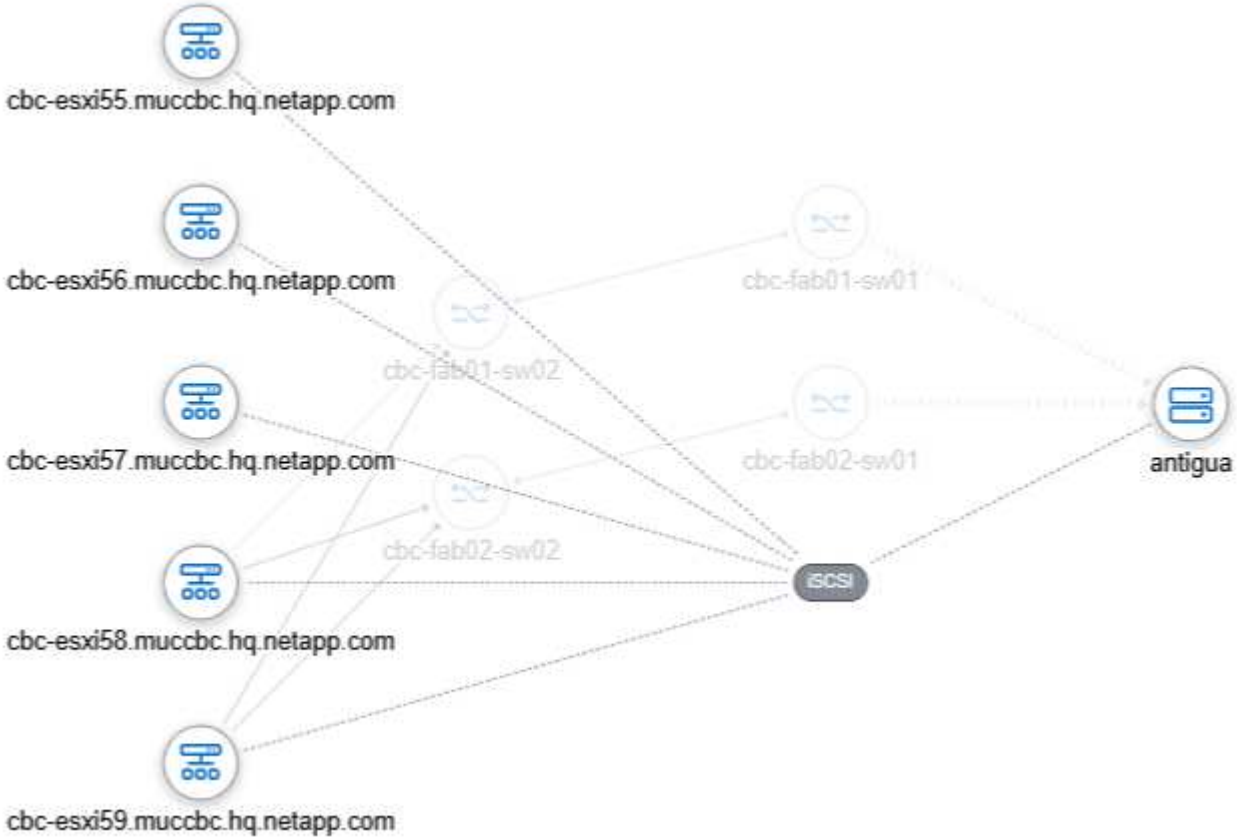
スライドアウト パネルには、[概要] タブに加えて、選択したオブジェクトに応じて、ポートの詳細やゾーン情報などのタブが表示されます。



環境に異なるプロトコルがある場合は、iSCSI または FC でフィルタリングできます。



環境に iSCSI デバイスが含まれている場合、*iSCSI* オブジェクトにマウスを移動すると、関連する iSCSI デバイスに関連する接続が強調表示されます。



トラブルシューティングのヒント

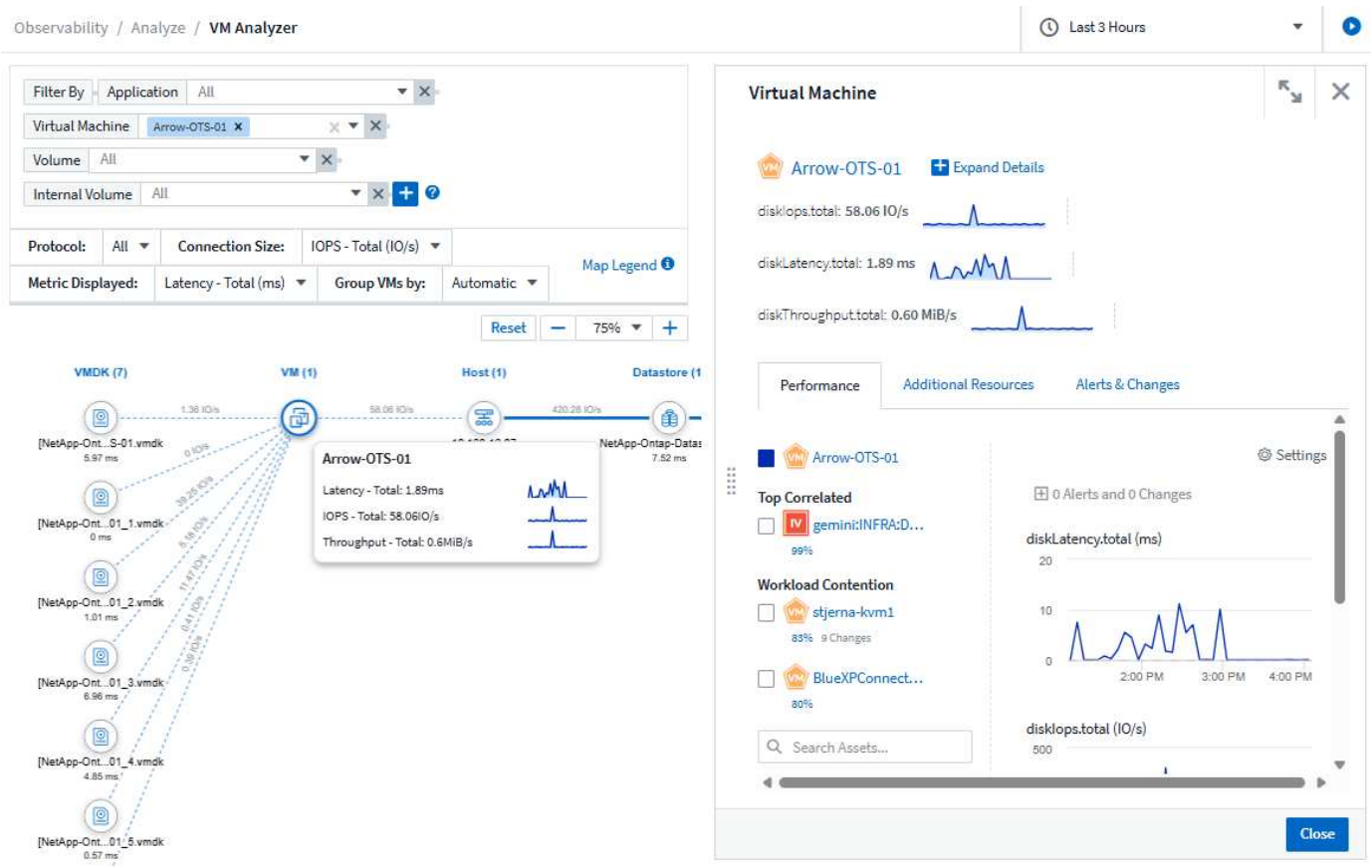
問題が発生した場合に試すことができるいくつかのこと:

問題：	これを試してみてください:
trafficUtilization や *trafficRate* などのメトリックの凡例に、<0、=0、または >0 が表示されます。	これは、メトリック値が 0.000123 のように小数点以下 2 桁未満の非常にまれなケースで発生する可能性があります。時間ウィンドウを拡張すると、メトリックをより効果的に分析できるようになります。

VMアナライザーの概要

DII の **VM Analyzer** を使用すると、仮想資産の管理がよりシンプルかつ効率的になります。この強力なツールは、VMDK/VM からホスト、データストア、内部ボリューム/ボリューム、ストレージへの依存関係をマッピングし、エンドツーエンドの可視性を提供します。

VM Analyzer は、インタラクティブなトポロジ マップを提供することで、問題を正確に特定し、変更を理解し、データ フローの理解を深めることを可能にします。 VM 管理を合理化し、仮想ワークロードの可視性を向上させます。



資産間のつながりを探索する

VM アナライザーを表示するには、**Observability > Analyze > VM Analyzer** を選択します。アプリケーション、仮想マシン、ボリューム、内部ボリュームのフィルターを設定するか、独自のフィルターを追加します。

オブジェクトのマップが表示され、接続されたオブジェクトが示されます。オブジェクトの上にマウスを置くと、その接続のトラフィック メトリックが表示されます。



VM Analyzer のフィルターのほとんどは (追加するフィルターも含め) コンテキスト依存です。これらのフィルターのいずれかでオブジェクトを選択すると、選択したオブジェクトのコンテキストで他のフィルター ドロップダウンに表示される選択肢が更新されます。

オブジェクトまたはグループをクリックすると、スライドアウト パネルが開き、オブジェクトとその接続に関する追加の詳細が表示されます。スライドアウト パネルには、選択したオブジェクトの詳細 (オブジェクトのタイプに応じてスループットや使用率など) を示す概要と、待機時間や IOPS などのオブジェクトのメトリックを示すグラフが表示されます。追加のタブを使用すると、関連する追加のリソースや変更、アラートを調べることができます。必要に応じて、相関性の高い上位オブジェクトや競合オブジェクトのメトリックもチャートに表示するように選択できます。

実際に動作を見てみましょう

VM Analyzer によるトラブルシューティングの簡素化 (ビデオ)、window=後で読む

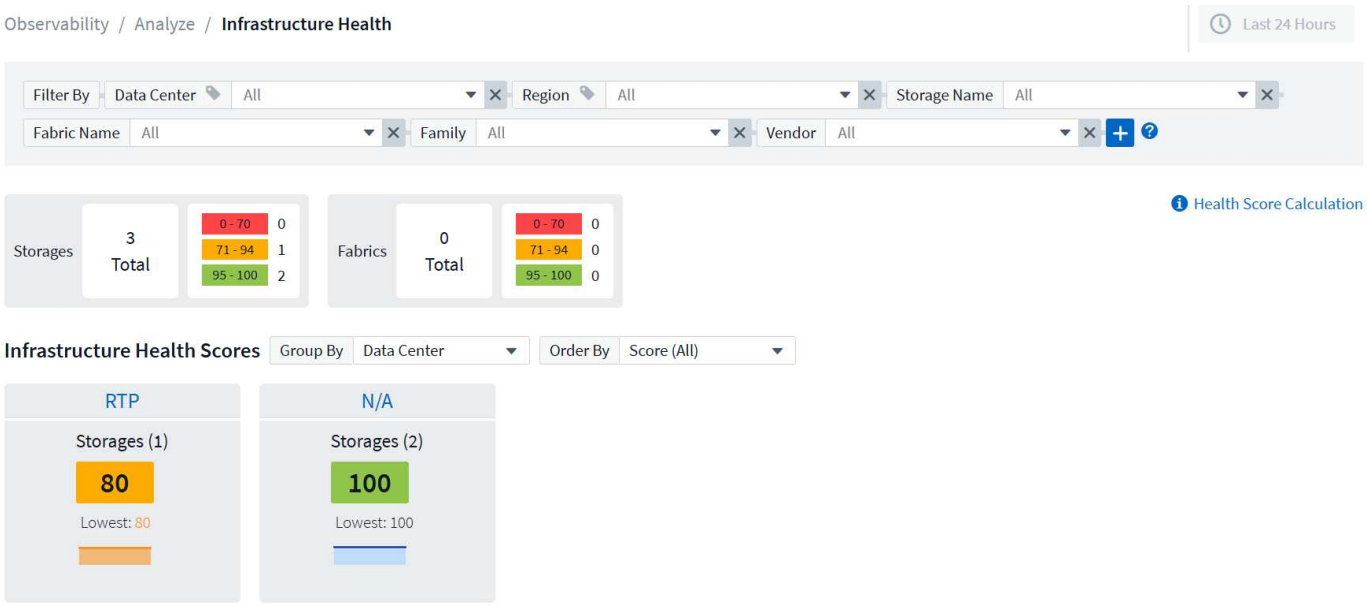
インフラストラクチャの健全性を監視する

Data Infrastructure Insights は、ストレージ環境のパフォーマンス、容量、構成、コンポーネントの状態を追跡する包括的なインフラストラクチャのヘルス監視を提供します。ヘルススコアは、これらのカテゴリ全体のモニターアラートに基づいて計算され、システムのヘルスを統合的に表示して、問題をプロアクティブに解決できるようになります。

インフラストラクチャヘルスダッシュボード

インフラストラクチャの健全性の監視は"プレビュー"機能は変更される可能性があります。

可観測性 > 分析 に移動し、インフラストラクチャの健全性 を選択します。ダッシュボードには、以下に説明するモニターのアラート カテゴリとスコアに基づいて、システムの健全性の概要が表示されます。上部でフィルターを設定して、調査の焦点を絞り込みます。



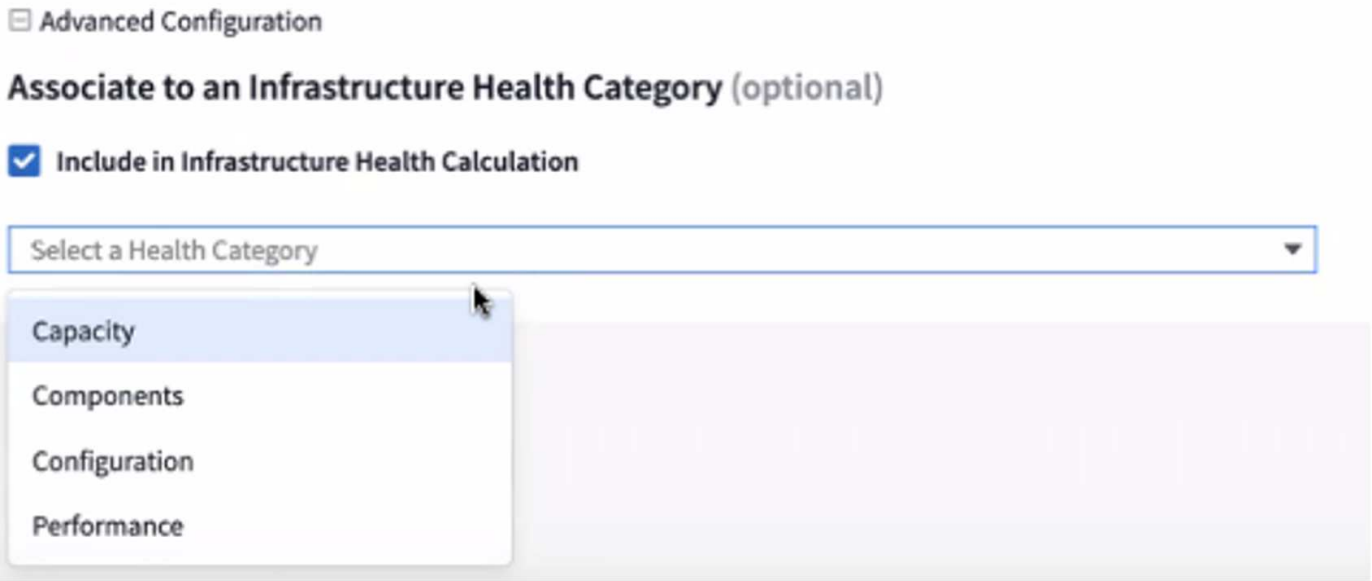
デフォルトでは、ヘルススコアはデータセンターごとにグループ化されています。セッションに最適なグループ化を選択できます。

インフラストラクチャの健全性に使用するモニターを構成する

ヘルススコアは、システム ヘルス計算に含めるように構成されたアラートによって決まります。

インフラストラクチャ オブジェクトのモニターを作成するときに、モニターからのアラートを計算に含めるかどうかを選択できます。画面の下部で、[詳細構成] を展開し、[インフラストラクチャの健全性計算に含める] を選択します。モニターの計算を適用するカテゴリを選択します。

- コンポーネントの健全性 - ファンの障害、サービス プロセッサのオフラインなど。
- パフォーマンスの健全性 - ストレージ ノードの使用率が高い、ノードのレイテンシが異常に上昇しているなど。
- 容量の健全性 - ストレージ プールの容量がいっぱいに近づいている、LUN スナップショット用のスペースが不足しているなど。
- 構成の健全性 - クラウド層に到達できない、 SnapMirror関係が同期していないなど。



健康スコアの説明

スコアは 0 から 100 までのスケールで表示され、100 が完全な健康状態を表します。現在または最近問題が発生している監視対象インフラストラクチャ オブジェクトでは、次の加重平均に従ってこのスコアが下がります。

- コンポーネント、パフォーマンス、または容量: それぞれ 30%
- 構成: 10%

ヘルススコアは、インフラストラクチャのヘルス計算に含めるように構成されたモニターによって生成されるアラートによって次のように影響を受けます。

- 重大なアラートは、カテゴリ全体の重みによってヘルススコアを下げます。
- 警告アラートにより、カテゴリの重みのスコアが半分に下がります。

いずれかのカテゴリが報告されていない場合は、加重平均がそれに応じて調整されます。

たとえば、コンポーネントに関する重大なアラートが 1 件 (-30)、パフォーマンスに関する警告アラートが 1 件 (30 の 50% = -15) の場合、正常性スコアは 55 (100 から 45 を引いた値) になります。

アラートが解決されると、これらのヘルススコアの低下は徐々に解消され、スコアは 2 時間以内に完全に回復します。

レポート

Data Infrastructure Insightsレポートの概要

Data Infrastructure Insightsレポートは、定義済み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で利用できます。"プレミアムエディション" 。レポート機能の利用には、最小フットプリント要件が適用されます。"NetAppの営業担当者にお問い合わせください"詳細についてはこちらをご覧ください。

Data Infrastructure Insightsレポートを使用すると、次のタスクを実行できます。

- 定義済みレポートを実行する
- 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
- レポートを自動的に実行するようにスケジュールする
- メールレポート
- データのしきい値を色で表す

Data Infrastructure Insights Reporting 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 レポートを生成し、次のような質問に答えるのに役立ちます。

- どのような在庫がありますか?
- 私の在庫はどこにありますか?
- 私たちの資産を使っているのは誰ですか?
- ビジネス ユニットに割り当てられたストレージのチャージバックとは何ですか?
- 追加のストレージ容量を取得する必要があるまでどのくらいかかりますか?
- ビジネス ユニットは適切なストレージ層に沿って配置されていますか?
- ストレージの割り当ては、1 か月、四半期、または 1 年にわたってどのように変化していますか?

Data Infrastructure Insightsサイトレポートへのアクセス

メニューの*レポート*リンクをクリックすると、 Data Infrastructure Insightsレポートにアクセスできます。

レポート インターフェースに移動します。 Data Infrastructure Insights は、レポート エンジンとして IBM Cognos Analytics を使用します。

ETL とは何ですか**?**

レポートを扱うときには、「データ ウェアハウス」と「ETL」という用語を耳にするでしょう。 ETL は「抽出、変換、ロード」の略です。 ETL プロセスは、 Data Infrastructure Insightsで収集されたデータを取得し、そのデータをレポートで使用できる形式に変換します。 「データ ウェアハウス」とは、レポートに使用できる収集されたデータを指します。

ETL プロセスには、次の個別のプロセスが含まれます。

- 抽出: Data Infrastructure Insightsからデータを取得します。
- 変換: Data Infrastructure Insightsから抽出されたデータにビジネス ロジック ルールまたは関数を適用します。
- ロード: レポートで使用するために、変換されたデータをデータ ウェアハウスに保存します。

Data Infrastructure Insightsレポートユーザーロール

Data Infrastructure Insights Premium Edition と Reporting をご利用の場合、テナント上のすべてのData Infrastructure Insightsユーザーに Reporting アプリケーション (Cognos など) へのシングル サインオン (SSO) ログイン権限も付与されます。メニューの*レポート*リンクをクリックするだけで、レポートに自動的にログインします。

Data Infrastructure Insightsでのユーザー ロールによって、レポート ユーザー ロールが決まります。

Data Infrastructure Insightsの役割	報告役割	報告権限
ゲスト	消費者	レポートを表示、スケジュール、実行したり、言語やタイムゾーンなどの個人設定を行ったりできます。消費者はレポートを作成したり、管理タスクを実行したりすることはできません。
ユーザ	作成者	すべてのコンシューマー機能を実行できるほか、レポートとダッシュボードを作成および管理できます。
管理者	管理者	すべての作成者機能のほか、レポートの構成、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を実行できます。

次の表は、各レポート ロールで使用できる機能を示しています。

特徴	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する	はい	はい	はい
レポートを実行する	はい	はい	はい
スケジュールレポート	はい	はい	はい
外部ファイルをアップロードする	いいえ	はい	はい
雇用を創出する	いいえ	はい	はい
ストーリーを作成する	いいえ	はい	はい
レポートを作成する	いいえ	はい	はい
パッケージとデータモジュールを作成する	いいえ	はい	はい
管理タスクを実行する	いいえ	いいえ	はい
HTMLアイテムの追加/編集	いいえ	いいえ	はい
HTMLアイテムでレポートを実行する	はい	はい	はい

カスタムSQLの追加/編集	いいえ	いいえ	はい
カスタムSQLでレポートを実行する	はい	はい	はい

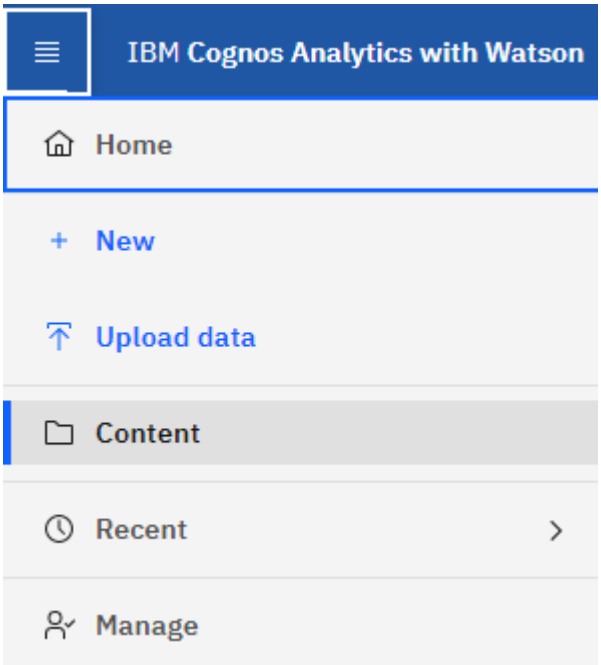
レポート（**Cognos**）の電子メール設定

Data Infrastructure Insights Reporting (Cognos アプリケーション) 内でユーザーの電子メール設定を変更した場合、その設定は 現在のセッションのみ アクティブになります。 Cognos からログアウトして再度ログインすると、電子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**?**

レポートが保持されるようにするには、次の手順に従って、すべてのレポートを *My Content* から *Team Content* に移行します。テナントで SSO を有効にする前に、これを実行する必要があります。

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. 複数のユーザーを作成した場合は、重複した名前でレポートが上書きされないように、ユーザーごとに別のフォルダを作成してください。
2. _マイコンテンツ_へ移動
3. 保持したいレポートをすべて選択します。
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* に新しく作成され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電子メール アドレスを使用してData Infrastructure Insightsにログインします。

8. Cognos 内の *Team Content* フォルダーに移動し、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。

定義済みレポートを簡単に作成

Data Infrastructure Insightsレポートには、いくつかの一般的なレポート要件に対応する定義済みレポートが含まれており、関係者がストレージ インフラストラクチャについて十分な情報に基づいた意思決定を行うために必要な重要な洞察を提供します。

レポート機能は、Data Infrastructure Insightsで利用できます。"プレミアムエディション" 。

Data Infrastructure Insightsレポート ポータルから事前定義されたレポートを生成し、他のユーザーに電子メールで送信したり、変更したりすることもできます。いくつかのレポートでは、デバイス、ビジネス エンティティ、または層別にフィルタリングできます。レポート ツールは IBM Cognos を基盤として使用し、さまざまなデータ表示オプションを提供します。

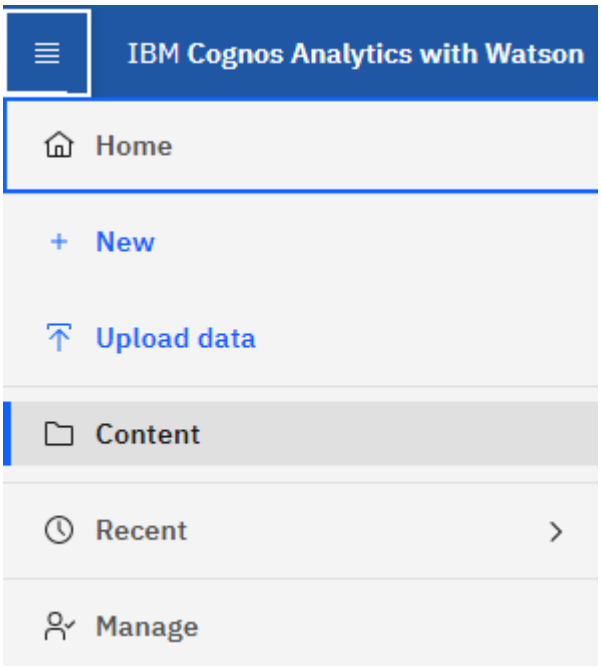
事前定義されたレポートには、インベントリ、ストレージ容量、チャージバック、パフォーマンス、ストレージ効率、クラウド コスト データが表示されます。これらの定義済みレポートを変更し、変更内容を保存できます。

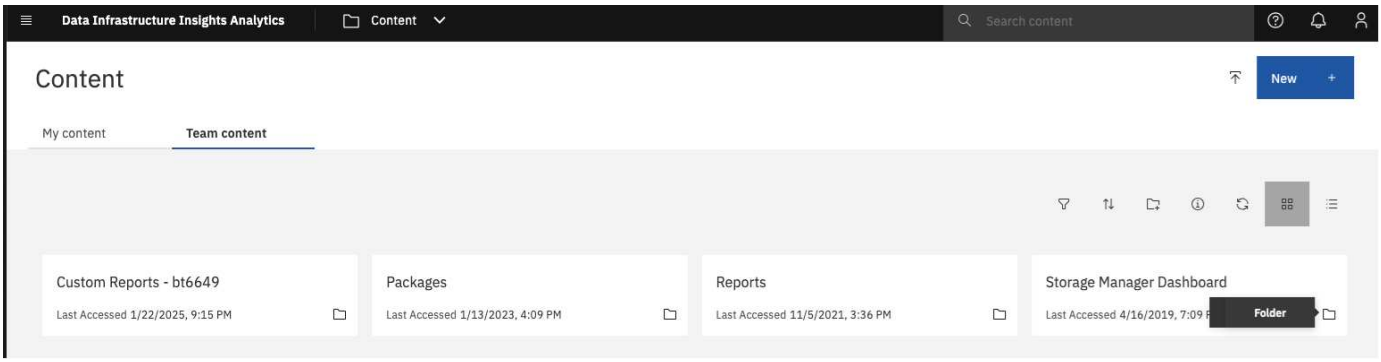
HTML、PDF、CSV、XML、Excel など、さまざまな形式でレポートを生成できます。

定義済みレポートへの移動

レポート ポータルを開くと、チーム コンテンツ フォルダーが、Data Infrastructure Insightsサイト レポートで必要な情報の種類を選択するための開始点になります。

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. 事前定義されたレポートにアクセスするには、「レポート」を選択します。





定義済みのレポートを使用してよくある質問に回答する

次の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

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 レポートは、アプリケーションの概要を提供します。この情報は、容量計画や移行計画に使用できます。

チャージバック

チャージバック レポートには、ホスト、アプリケーション、ビジネス エンティティ別の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情報が提供され、現在のデータと履歴データの両方が含まれます。

二重カウントを防ぐには、ESX サーバーを含めず、VM のみを監視します。

データソース

データ ソース 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 (成功/失敗)、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 ソースのトラブルシューティングをどこから開始するかに関する情報が提供されます。失敗したデータ ソースは、レポートの精度と製品の全体的な使いやすさに影響します。

ESXと**VM**のパフォーマンス

ESX と VM のパフォーマンス レポートでは、ESX サーバーと VM の比較が提供され、ESX サーバーと VM の平均およびピーク IOPS、スループット、待ち時間、および使用率が表示されます。二重カウントを防ぐには、ESX サーバーを除外し、VM のみを含めます。このレポートの更新バージョンは、 NetApp Storage Automation Store で入手できます。

生地概要

ファブリック サマリー 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 ステータスなどのスイッチとスイッチ情報が示されます。レポートには NPV スイッチ ポートは含まれません。

ホスト**HBA**

ホスト HBA レポートには、環境内のホストの概要が表示され、HBA のベンダー、モデル、ファームウェア バージョン、およびそれらが接続されているスイッチのファームウェア レベルが示されます。このレポートは、スイッチまたは HBA のファームウェア アップグレードを計画するときに、ファームウェアの互換性を分析するために使用できます。

ホストのサービスレベル容量とパフォーマンス

ホスト サービス レベル容量およびパフォーマンス レポートには、ブロックのみのアプリケーションのホスト別のストレージ使用率の概要が表示されます。

ホストの概要

ホスト サマリー レポートには、ファイバー チャネル ホストと iSCSI ホストの情報とともに、選択された各ホストのストレージ使用率の概要が表示されます。このレポートを使用すると、ポートとパス、ファイバー チャネルと iSCSI の容量、違反数を比較できます。

ライセンスの詳細

ライセンスの詳細レポートには、アクティブなライセンスを持つすべてのサイトにわたって、ライセンスが付与されているリソースの数量が表示されます。レポートには、アクティブなライセンスを持つすべてのサイト全体の実際の数量の合計も表示されます。合計には、複数のサーバーによって管理されるストレージ アレイの重複が含まれる場合があります。

マップされているがマスクされていないボリューム

マップされているがマスクされていないボリューム レポートには、論理ユニット番号 (LUN) が特定のホストで使用するためにマップされているが、そのホストに対してマスクされていないボリュームがリストされます。場合によっては、これらはマスク解除された廃止された 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はどのホストからもアクセスできるため、データ破損の危険にさらされます。

NetAppの容量とパフォーマンス

NetApp の容量とパフォーマンス レポートには、割り当て済み、使用済み、コミット済みの容量のグローバルデータと、 NetApp の容量の傾向およびパフォーマンス 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によって取得されたすべての資産の概要と全体的なステータスが示されます。ステータスは緑、黄、赤のフラグで示されます。

- 緑は正常な状態を示します
- 黄色は環境における潜在的な問題を示します
- 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は、レポートに付属するデータ ディクショナリに説明されています。

ストレージの概要

ストレージ サマリー レポートには、未加工、割り当て済み、ストレージ プール、およびボリュームの使用済みおよび未使用の容量データのグローバル サマリーが提供されます。このレポートには、検出されたすべてのストレージの概要が示されます。

VMの容量とパフォーマンス

仮想マシン (VM) 環境とその容量使用状況について説明します。 VM の電源がオフになったときなどの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 パス レポートには、どのホストでどの仮想マシンが実行されているか、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 パスは何か、容量の割り当てと使用状況を構成するものは何であるかなど、データ ストアの容量データとパフォーマンス メトリックが提供されます。

シンプール別のHDS容量

HDS シン プール別容量レポートには、シン プロビジョニングされたストレージ プール上の使用可能な容量が表示されます。

NetAppの総容量

NetAppのアグリゲート別容量レポートには、アグリゲートの生の合計、合計、使用済み、使用可能、コミット済みのスペースが表示されます。

シックアレイによるSymmetrix容量

Symmetrix のシック アレイ別容量レポートには、生の容量、使用可能な容量、空き容量、マップされた容量、マスクされた容量、および合計空き容量が表示されます。

シンプール別のSymmetrix容量

Symmetrix のシン プール別容量レポートには、生の容量、使用可能な容量、使用済み容量、空き容量、使用率、サブスクライブされた容量、サブスクリプション レートが表示されます。

XIV アレイ別容量

XIV アレイ別容量レポートには、アレイの使用済み容量と未使用容量が表示されます。

XIV プール別収容人数

XIV プール別容量レポートには、ストレージ プールの使用済み容量と未使用容量が表示されます。

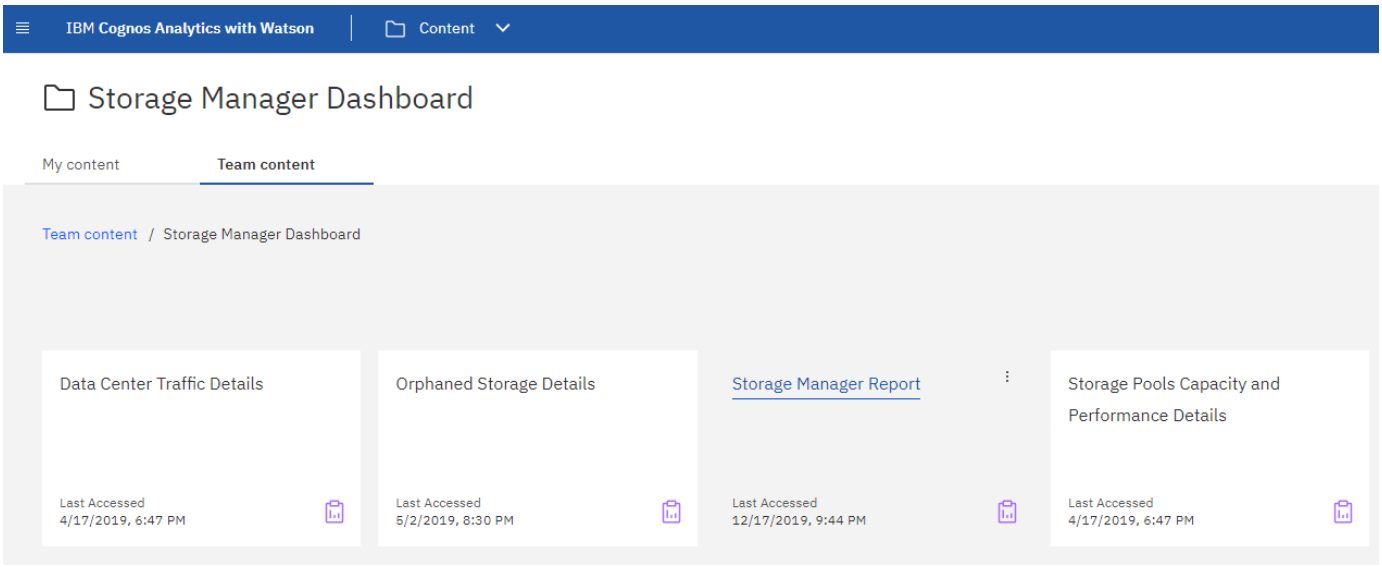
ストレージマネージャーダッシュボード

ストレージ マネージャー ダッシュボードでは、集中化された視覚化が提供され、時間の経過に伴うリソースの使用状況を許容範囲や過去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 メトリックのみを表示することで、データ センターの保守方法を決定できます。

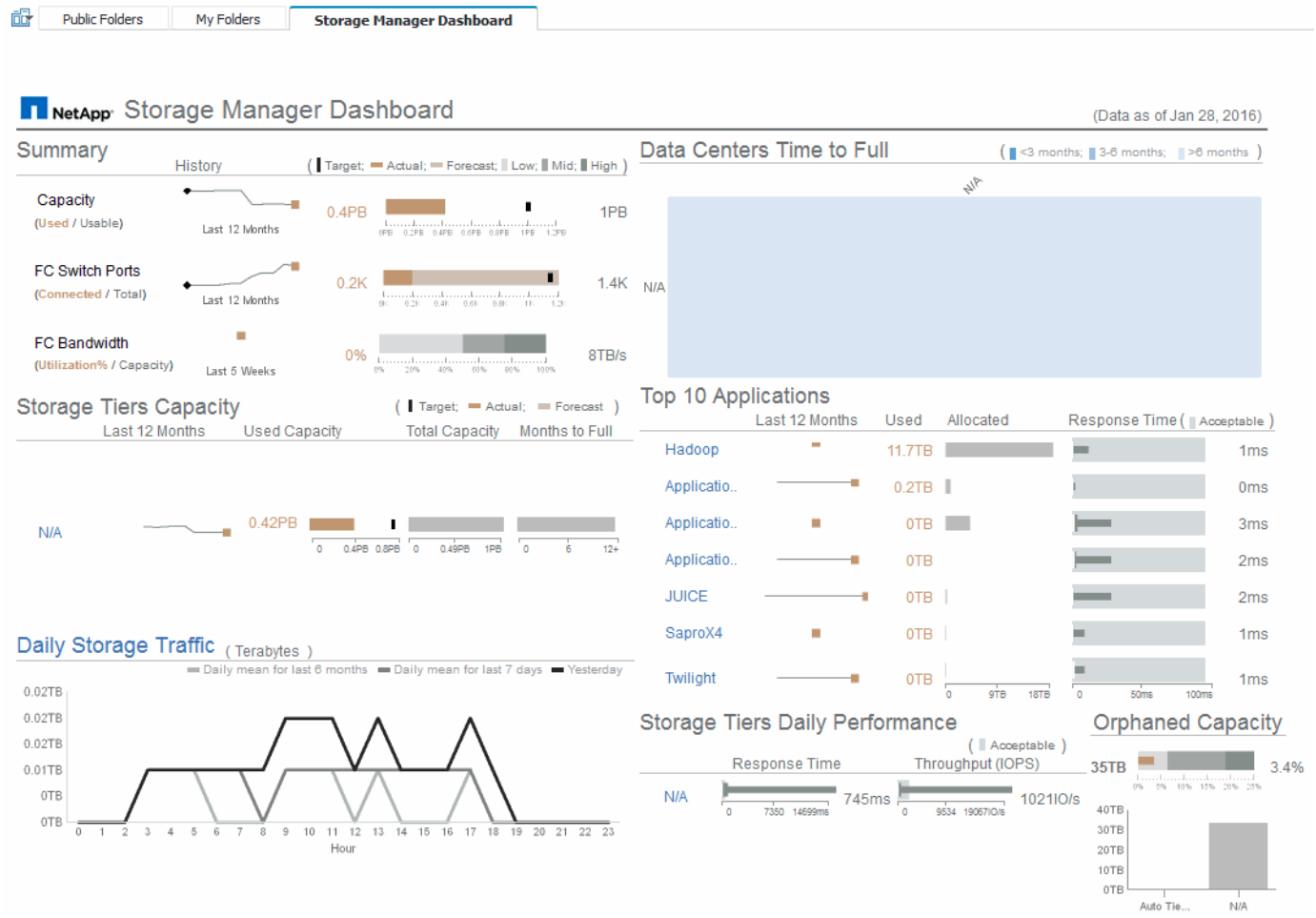
レポート機能は、Data Infrastructure Insightsで利用できます。"プレミアムエディション" 。

まとめ

チーム コンテンツから ストレージ マネージャー ダッシュボード 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いくつかのレポートが表示されます。



一目でわかるように、ストレージ マネージャー レポート 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 サービスの側面をドリルダウンして、最も関心のあるセクションの詳細な分析を実行できます。



このコンポーネントには、使用済みストレージ容量と使用可能なストレージ容量、スイッチ ポートの合計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 ポートの使用率の合計と合計帯域幅、およびこれらの各値の時間の経過に伴う傾向が表示されます。実際の使用率を低、中、高の範囲と比較して表示できるため、ターゲットに基づいて予測と希望する実際の使用率を比較対照できます。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。予測は現在の成長率と設定した日付に基づいて推定されます。将来の使用量予測日に基づいて予測される使用容量が目標を超えると、「容量」の横にアラート (赤い実線の円) 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は、使用されている層容量と層に割り当てられた容量を比較して表示します。これにより、12 か月間で使用済み容量がどのように増加または減少するか、および全容量に達するまであと何ヶ月残っているかがわかります。容量の使用状況は、実際の使用量、使用量の予測、および構成可能な容量のターゲットに対して提供された値とともに表示されます。将来の使用量予測日に基づいて予測される使用容量が目標容量を超えると、層の横にアラート (赤い実線の円) が表示されます。

任意の層をクリックすると、ストレージ プールの容量とパフォーマンスの詳細レポートが表示されます。このレポートには、選択した層内のすべてのプールの空き容量と使用済み容量、いっぱいになるまでの日数、パフォーマンス (IOPS と応答時間) の詳細が表示されます。このレポート内の任意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、そのリソースの現在の状態をまとめた資産ページを表示することもできます。

毎日のストレージトラフィック

このコンポーネントは、環境のパフォーマンス、過去 6 か月間と比較して大きな増加、変更、または潜在的な問題があるかどうかを示します。また、過去 7 日間および前日のトラフィックとの比較による平均トラフィックも表示されます。周期的な変動 (過去 7 日間) と季節的な変動 (過去 6 か月間) の両方を強調表示する情報を提供するため、インフラストラクチャのパフォーマンスの異常を視覚化できます。

タイトル (日次ストレージ トラフィック) をクリックすると、ストレージ トラフィック詳細レポートが表示されます。このレポートには、各ストレージ システムの前日の 1 時間ごとのストレージ トラフィックのヒートマップが表示されます。このレポート内の任意のストレージ名をクリックすると、そのリソースの現在の状態をまとめた資産ページが表示されます。

データセンターの満杯までの時間

このコンポーネントは、すべてのデータ センターとすべての層を比較し、予測される成長率に基づいて、各データ センターの各層ストレージに残っている容量を表示します。ティアの容量レベルは青で表示されます。色が濃いほど、その場所のティアがいっぱいになるまでの残り時間が少なくなります。

層のセクションをクリックすると、ストレージ プールのフル使用までの日数の詳細レポートが表示されます。このレポートには、選択した層とデータ センター内のすべてのプールの合計容量、空き容量、フル使用までの日数が表示されます。このレポート内の任意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、そのリソースの現在の状態をまとめた資産ページが表示されます。

トップ**10**アプリケーション

このコンポーネントは、使用容量に基づいて上位 10 件のアプリケーションを表示します。層がデータをどのように編成しているかに関係なく、この領域にはインフラストラクチャの現在の使用容量とシェアが表示されます。過去 7 日間のユーザー エクスペリエンスの範囲を視覚化して、消費者が許容できる (または、さらに重要なことに、許容できない) 応答時間を経験しているかどうかを確認できます。

この領域には傾向も表示され、アプリケーションがパフォーマンス サービス レベル目標 (SLO) を満たしているかどうかを示します。前週の最小応答時間、第 1 四分位、第 3 四分位、最大応答時間を表示でき、設定可能な許容可能な SLO に対する中央値も表示されます。いずれかのアプリケーションの平均応答時間が許容可能な SLO 範囲外になると、アプリケーションの横にアラート (赤い実線の円) が表示されます。アプリケーションをクリックすると、その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。

ストレージ階層の日々のパフォーマンス

このコンポーネントには、過去 7 日間の応答時間と IOPS に関する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、構成可能な SLO と比較され、層を統合する機会があるかどうか、それらの層から配信されるワークロードを再調整する機会があるかどうか、または特定の層の問題を特定することができます。平均応答時間または平均 IOPS が許容可能な SLO 範囲外の場合、層の横にアラート (赤い実線の円) が表示されます。

層名をクリックすると、ストレージ プールの容量とパフォーマンスの詳細レポートが表示されます。このレポートには、選択した層内のすべてのプールの空き容量と使用済み容量、いっぱいになるまでの日数、パフォーマンス (IOPS と応答時間) の詳細が表示されます。このレポート内の任意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、そのリソースの現在の状態をまとめた資産ページが表示されます。

孤立した容量

このコンポーネントは、合計孤立容量と層別の孤立容量を表示し、合計使用可能容量の許容範囲と比較して、実際に孤立している容量を表示します。孤立した容量は、構成とパフォーマンスによって定義されます。構成によって孤立したストレージとは、ホストにストレージが割り当てられている状況を指します。ただし、構成が適切に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。パフォーマンスによって孤立化されるのは、ストレージがホストからアクセスできるように正しく構成されている場合です。ただし、ストレージ トラフィックは発生していません。

水平に積み上げられたバーには、許容範囲が表示されます。灰色が濃ければ濃いほど、状況は受け入れがたいものになります。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 バーで示されます。

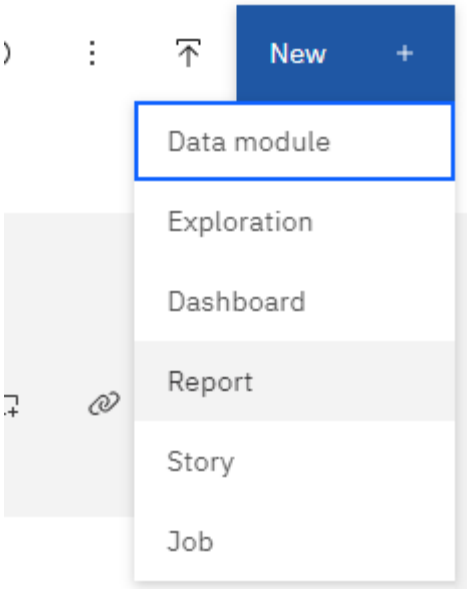
層をクリックすると、孤立ストレージの詳細レポートが表示されます。このレポートには、選択した層の構成とパフォーマンスによって孤立していると識別されたすべてのボリュームが表示されます。このレポート内の任意のストレージ、ストレージ プール、またはボリュームをクリックすると、そのリソースの現在の状態をまとめた資産ページが表示されます。

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のストレージおよびストレージ プールの物理容量に関する簡単なレポートを生成します。

手順

1. *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



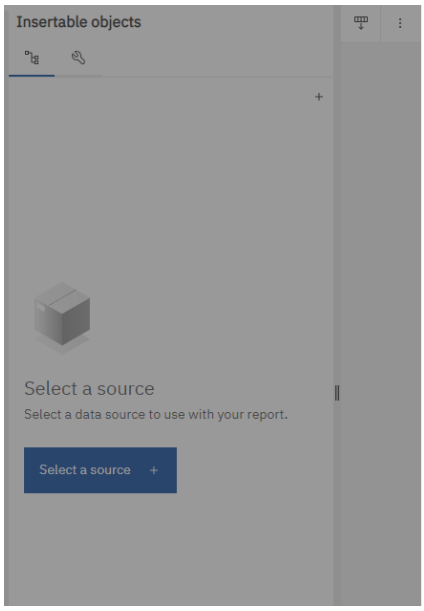
4. *テンプレート*タブで_空白_を選択します

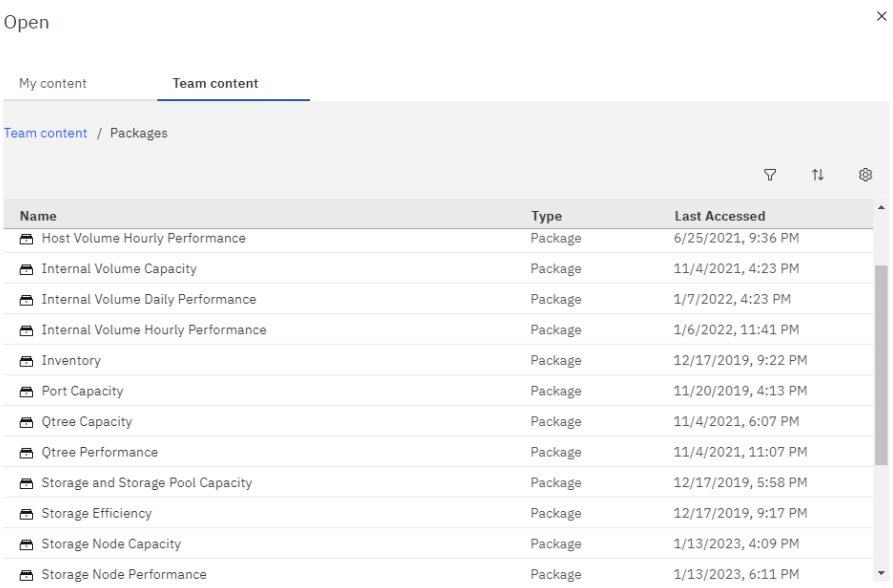
   ソースとデータタブが表示されます

5. 開く ソースを選択 **+**
6. *チームコンテンツ*の下で*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





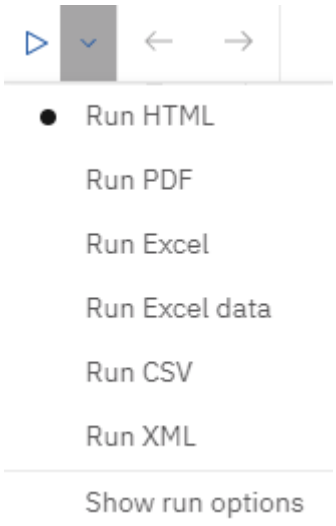
8. *開く*を選択

   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

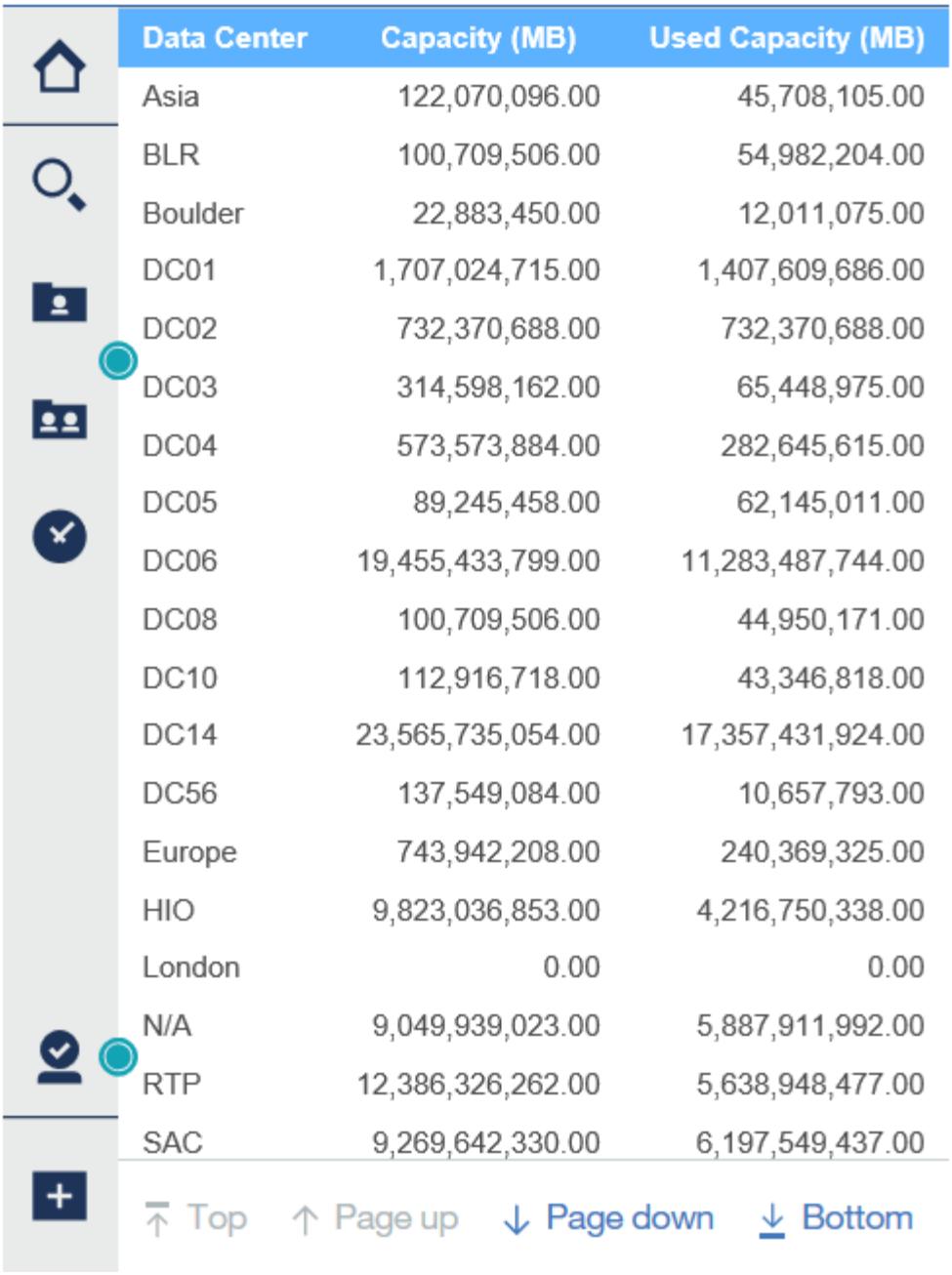
リストとクエリに適切な名前を追加します

10. [OK]を選択します
11. _物理容量_の拡張
12. _データセンター_の最下層まで拡張
13. *Data Center* をレポートパレットにドラッグします。
14. _容量(MB)_を拡張
15. 容量 *(MB)* をレポートパレットにドラッグします。
16. 使用容量 *(MB)* をレポートパレットにドラッグします。
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をカスタマイズしたり、レポートのプロパティやスケジュールを設定したり、レポートを電子メールで送信したりできます。

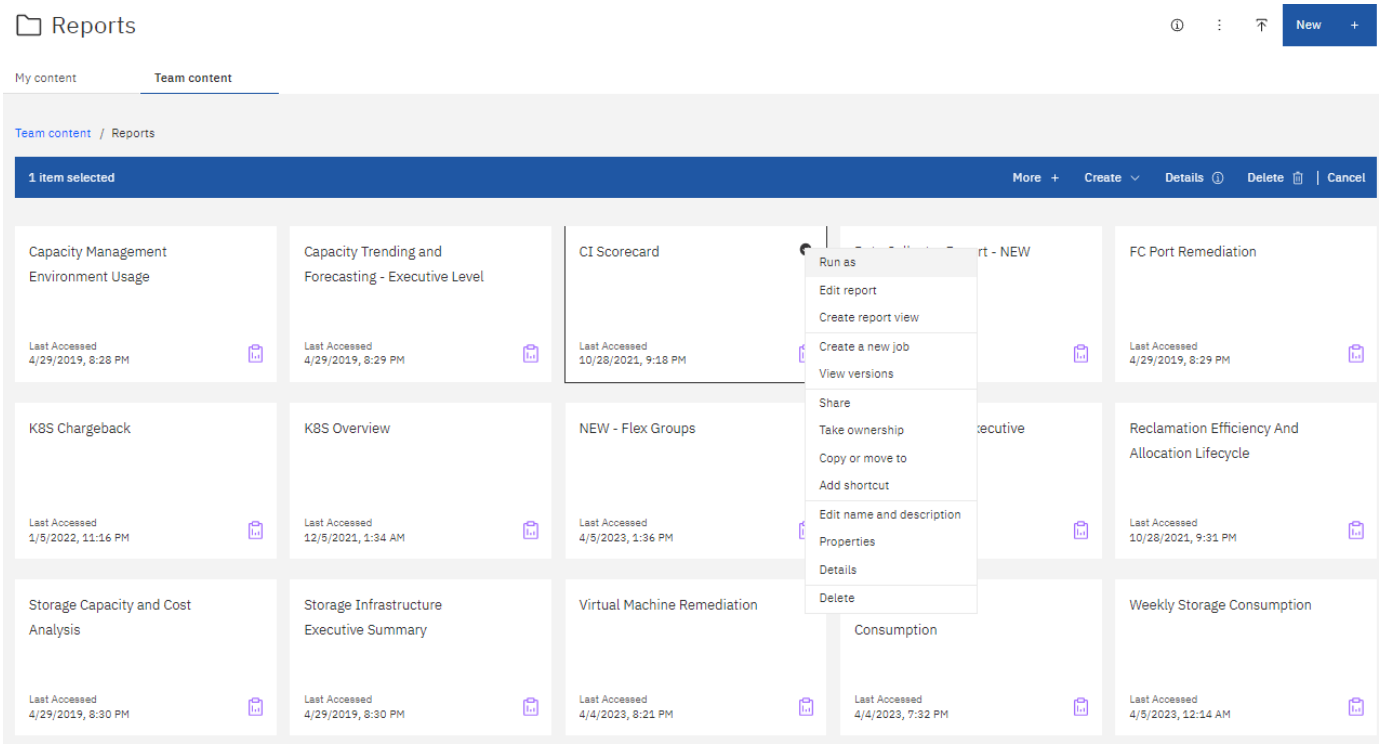
レポート機能は、Data Infrastructure Insightsで利用できます。"プレミアムエディション"。

レポート権限またはセキュリティを変更する前に、「マイ コンテンツ」レポートを「チーム コンテンツ」フォルダーにコピーして、レポートが確実に保存されるようにする必要があります。

レポートの出力形式と配信のカスタマイズ

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インサイト レポート 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。カスタマイズしたいレポートの上にマウスを移動し、「3 つのドット」メニューを開きます。

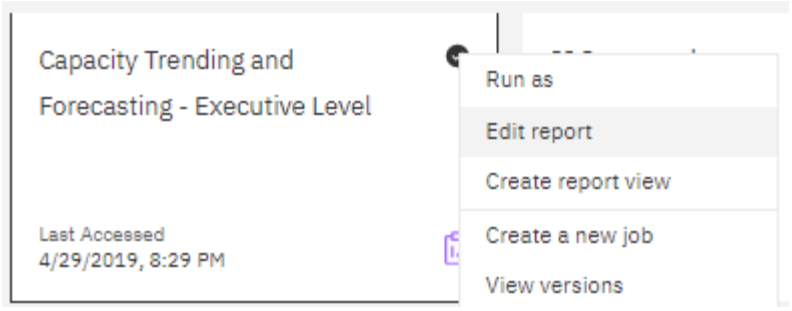


1. *プロパティ>スケジュール*をクリックします
2. 次のオプションを設定できます。
   - レポートを実行するタイミングを*スケジュール*します。
   - レポートの形式と配信 (保存、印刷、電子メール) および言語の オプション を選択します。
3. *保存*をクリックすると、選択内容を使用してレポートが作成されます。

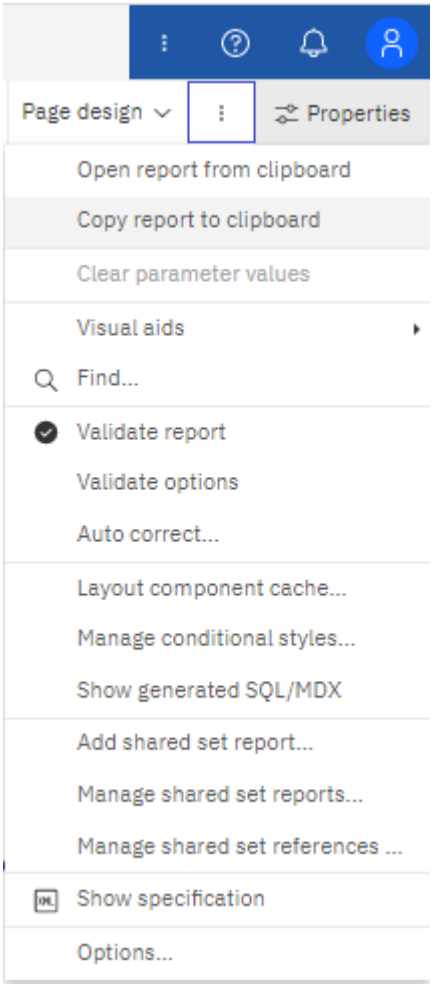
レポートをクリップボードにコピーする

このプロセスを使用して、レポートをクリップボードにコピーします。

1. コピーする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「レポートの編集」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。



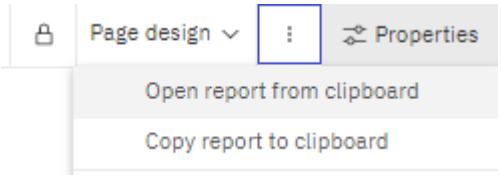
クリップボードからレポートを開く

以前に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 まず、新しいレポートを作成するか、コピーしたレポートに置き換える既存のレポートを開きます。以下の手順は新しいレポート用です。

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て、「**OK**」を選択します。
2. レポートを保存するには、フロッピー ディスク アイコンを選択します。
3. レポートを保存する場所を選択します (*My Content*、*Team Content*、または新しいフォルダーを作成します)。
4. 新しいレポートにわかりやすい名前を付けて、[保存] を選択します。

既存のレポートの編集

デフォルトの場所で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危険性があることに注意してください。編集したレポートを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のヒントを紹介します。

問題：	これを試してみてください:
レポートを電子メールで送信するようにスケジュールすると、ログインしているユーザーの名前が電子メールの「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）の形式になります。これは有効な電子メール アドレスではないため、スケジュールされたレポートを実行しても電子メールは送信されません。	レポートを電子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、「宛先」フィールドに有効で適切な形式の電子メール アドレスを入力します。
スケジュールされたレポートは電子メールで送信されますが、レポートの発信元が「マイ コンテンツ」フォルダーである場合はレポートにアクセスできません。	これを回避するには、レポートまたはレポート ビューを「チーム コンテンツ > カスタム レポート - xxxxxx」フォルダーに保存し、その保存バージョンからスケジュールを作成する必要があります。 「カスタム レポート - xxxxxx」フォルダは、テナントのすべてのユーザーに表示されます。
ジョブを保存すると、フォルダーに「カスタム レポート - xxxxxx」のコンテンツのリストを含む「チーム コンテンツ」が表示されることがあります が、Cognos はこれが書き込み権限のない「チーム コンテンツ」フォルダーであると認識するため、ここにジョブを保存することはできません。	回避策としては、一意の名前 (つまり「NewFolder」) を持つ新しいフォルダーを作成してそこに保存するか、「マイ コンテンツ」に保存してから「カスタム レポート - xxxxxx」にコピー/移動します。

カスタムレポートの作成

レポート作成ツールを使用してカスタム レポートを作成できます。レポートを作成したら、それを保存し、定期的に実行することができます。レポートの結果は、自分自身や

他の人に電子メールで自動的に送信できます。

レポート機能は、Data Infrastructure Insightsで利用できます。"プレミアムエディション" 。

このセクションの例では、 Data Infrastructure Insights Reporting のデータ モデルのいずれかに使用できる次のプロセスを示します。

- レポートで回答すべき質問を特定する
- 結果を裏付けるために必要なデータの決定
- レポートのデータ要素の選択

カスタム レポートを設計する前に、いくつかの前提条件となるタスクを完了する必要があります。これらを完了しないと、レポートが不正確または不完全になる可能性があります。

たとえば、デバイス識別プロセスを完了しないと、容量レポートは正確ではなくなります。または、注釈 (層、ビジネス ユニット、データ センターなど) の設定を完了しないと、カスタム レポートでドメイン全体のデータが正確にレポートされなかったり、一部のデータ ポイントに「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、次のタスクを完了します。

- すべて設定"データ収集者"きちんと。
- テナント上のデバイスとリソースに注釈 (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 は履歴情報を収集するため、レポートを生成する前に注釈を安定させておくことは有益です。

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。
- 結果を裏付けるデータを特定します。
- データが含まれているデータ モデル (たとえば、チャージバック データ モデル、インベントリ 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、レポートの結果をフォーマット、並べ替え、フィルタリングします。

カスタムレポートの結果を計画する

レポート作成ツールを開く前に、レポートから得たい結果を計画しておくとよいでしょう。レポート作成ツールを使用すると、レポートを簡単に作成でき、多くの計画を立てる必要がない場合もありますが、レポートの要求者からレポートの要件について把握しておくことをお勧めします。

- 回答したい質問を正確に特定します。例えば：
  - どれくらいの容量が残っていますか?
  - 事業単位あたりのチャージバックコストはいくらですか?

- ビジネス ユニットが適切なストレージ層に揃えられるようにするための層別の容量はどのくらいですか。
- 電力と冷却の要件を予測するにはどうすればよいでしょうか? (リソースに注釈を追加して、カスタマイズされたメタデータを追加します。)

- 回答を裏付けるために必要なデータ要素を特定します。
- 回答で確認したいデータ間の関係を特定します。質問には非論理的な関係を含めないでください。たとえば、「容量に関連するポートを確認したい」などです。
- データに必要な計算を特定します。
- 結果を制限するために必要なフィルタリングの種類を決定します。
- 現在のデータまたは履歴データを使用する必要があるかどうかを決定します。
- データを特定の対象者に制限するためにレポートにアクセス権限を設定する必要があるかどうかを決定します。
- 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に従って電子メールで送信するか、チームのコンテンツ フォルダー領域に含める必要がありますか?
- レポートを保守する担当者を決定します。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。

レポート設計のヒント

レポートを設計するときに役立つヒントがいくつかあります。

- 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。

  ほとんどのレポートでは、Data Infrastructure Insightsで利用可能な最新のデータについてのみレポートする必要があります。

- Data Infrastructure Insightsサイト レポートでは、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。
- すべてのユーザーはすべてのデータを見ることができますが、特定の対象ユーザーにデータを制限する必要がある場合があります。

  異なるユーザーの情報をセグメント化するには、レポートを作成し、それらにアクセス権限を設定できます。

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、そこから定義済みレポートを選択したり、独自のカスタム レポートを作成したりできます。

各データ モデルには、単純なデータ 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 データ マートは、最も一般的に使用されるデータ要素への迅速なアクセスを提供し、データ ウェアハウス データの最新のスナップショットのみを含み、履歴データは含みません。
- 高度なデータ マートは、単純なデータ マートから入手でき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も含まれます。

ストレージ容量、ファイル システムの使用率、内部ボリューム容量、ポート容量、qtree 容量、仮想マシン (VM) 容量に関する質問に答えることができます。容量データ モデルは、複数の容量データ モデルのコンテナーです。このデータ モデルを使用して、さまざまな種類の質問に答えるレポートを作成できます。

ストレージとストレージプール容量データモデル

ストレージおよびストレージ プールを含むストレージ容量リソース計画に関する質問に答えることができ、物理ストレージ プール データと仮想ストレージ プール データの両方が含まれます。このシンプルなデータ モデルは、フロア容量や、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 プールの容量使用状況に関する質問に答えるのに役立ちます。容量レポートを初めて使用する場合は、よりシンプルでターゲットを絞ったこのデータ モデルから始めることをお勧めします。このデータ モデルを使用すると、次のような質問に答えることができます。

- 物理ストレージの容量しきい値 80% に達する予定日はいつですか?
- 特定の層のアレイ上の物理的なストレージ容量はどれくらいですか?
- メーカー別、ファミリ別、データ センター別のストレージ容量はどれくらいですか?
- すべての層のアレイ上のストレージ使用率の傾向はどうですか?
- 使用率が最も高い上位 10 のストレージ システムは何ですか?
- ストレージ プールのストレージ使用率の傾向はどうですか?
- すでにどのくらいの容量が割り当てられていますか?
- 割り当て可能な容量はどれくらいですか?

ファイルシステム使用率データモデル

このデータ モデルは、ファイル システム レベルでのホストの容量使用率に関する可視性を提供します。管理者は、ファイル システムごとに割り当てられた容量と使用済み容量を決定し、ファイル システムのタイプを判別し、ファイル システム タイプ別の傾向統計を特定できます。このデータ モデルを使用すると、次の質問に答えることができます。

- ファイルシステムのサイズはどれくらいですか?
- データはどこに保存され、どのようにアクセスされますか (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? それでは、これに基づいて、将来のニーズについて何を予測できるでしょうか?

内部ボリューム容量データモデル

内部ボリュームの使用済み容量、割り当て済み容量、および時間の経過に伴う容量使用状況に関する質問に答えることができます。

- 事前定義されたしきい値よりも使用率が高い内部ボリュームはどれですか?
- 傾向に基づいて、どの内部ボリュームが容量不足になる危険がありますか? 8 内部ボリュームの使用容量と割り当て容量はどれくらいですか?

ポート容量データモデル

スイッチ ポートの接続性、ポートの状態、およびポート速度に関する質問に時間の経過とともに回答できるようになります。新しいスイッチの購入計画を立てる際に役立つ、次のような質問に答えることができます。リソース (ポート) の可用性 (データ センター、スイッチ ベンダー、ポート速度に応じて) 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?

- データ速度、データセンター、ベンダー、ホストおよびストレージ ポートの数を考慮すると、どのポートの容量が不足する可能性が高いですか。
- スイッチ ポート容量の傾向は時間とともにどう変化しますか?
- ポート速度はどれくらいですか?
- どのようなタイプのポート容量が必要であり、どの組織で特定のポート タイプまたはベンダーが不足しつつありますか。
- その容量を購入して利用可能にする最適な時期はいつでしょうか?

Qtree 容量データモデル

時間の経過に伴う qtree 使用率の傾向 (使用済み容量と割り当て済み容量などのデータ) を把握できます。ビジネス エンティティ、アプリケーション、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、次の質問に答えることができます。

- 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た制限に対する qtree の使用容量はどれくらいですか?
- 容量計画を立てるために、使用済み容量と空き容量の傾向を把握してください。
- 最も多くの容量を使用している事業体はどれですか?
- 最も多くの容量を消費するアプリケーションはどれですか?

VM容量データモデル

仮想環境とその容量使用状況をレポートできます。このデータ モデルを使用すると、VM およびデータ ストアの容量使用量の経時的な変化をレポートできます。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 およびデータ ストアにプロビジョニングされた容量に基づいて容量チャージバックを決定するにはどうすればよいですか?
- VM によって使用されていない容量はどれですか。また、未使用の容量のうち、空き容量、孤立容量、その他の容量はどれですか。
- 消費動向を踏まえて何を購入すべきでしょうか？
- ストレージ シン プロビジョニングと重複排除テクノロジを使用することで、どの程度のストレージ効率の節約が達成されますか?

VM 容量データ 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 容量データ モデルを使用してプロビジョニングされた VM のサイズは、その仮想ディスクのサイズになります。これは、VM 自体のプロビジョニングされたサイズを表示する、 Data Infrastructure Insightsの仮想マシン ビューのプロビジョニングされた容量とは異なります。

ボリューム容量データモデル

テナント上のボリュームのあらゆる側面を分析し、ベンダー、モデル、層、サービス レベル、データ センターごと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、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) を確認し、アレイ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、次のような質問に答えることができます。

- 事前定義されたしきい値よりも使用率が高いボリュームはどれですか?
- データセンターにおける孤立ボリュームの容量の傾向はどうなっていますか?
- データセンターの容量のうち、どれくらいが仮想化またはシンプロビジョニングされていますか?
- データセンターの容量のどれくらいをレプリケーション用に予約する必要がありますか?

チャージバックデータモデル

ストレージ リソース (ボリューム、内部ボリューム、qtree) の使用済み容量と割り当て済み容量に関する質問に答えることができます。このデータ モデルは、ホスト、アプリケーション、ビジネス エンティティ別の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情報を提供し、現在のデータと履歴データの両方を含みます。レポート データは、サービス レベルとストレージ層別に分類できます。

このデータ モデルを使用すると、ビジネス エンティティによって使用されている容量の量を調べて、チャージバック レポートを生成できます。このデータ モデルを使用すると、複数のプロトコル (NAS、SAN、FC、iSCSI など) の統合レポートを作成できます。

- 内部ボリュームの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ごとのチャージバックが表示されます。
- 内部ボリュームを持つストレージの場合:
  - 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に割り当てられておらず、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 ごと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割り当てられておらず、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。
  - チャージバックをボリューム、qtree、または内部ボリューム別に表示するかどうかの決定は各内部ボリュームごとに行われるため、同じストレージ プール内の異なる内部ボリュームに異なるレベルで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、デフォルトの時間間隔が経過すると消去されます。詳細については、データ ウェアハウス プロセスを参照してください。

チャージバック データ モデルを使用するレポートでは、ストレージ容量 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。

- NetAppストレージ システム以外のストレージ 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 ストレージ システムの場合、チャージバック データ モデルは単一レイヤー (ボリューム、内部ボリューム、または qtree) を使用して料金を算出しますが、ストレージ容量データ モデル

は複数レイヤー (ボリュームおよび内部ボリューム) を使用して料金を算出します。

在庫データモデル

ホスト、ストレージ システム、スイッチ、ディスク、テープ、qtree、クォータ、仮想マシンとサーバー、汎用デバイスなどのインベントリ リソースに関する質問に答えることができます。インベントリ 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、違反に関する情報を表示できるサブマートがいくつか含まれています。在庫データ モデルには履歴データは含まれません。このデータで答えられる質問

- どのような資産を所有しており、それらはどこにあるのでしょうか?
- 資産を使用しているのは誰ですか?
- 所有しているデバイスの種類と、それらのデバイスのコンポーネントは何ですか?
- OS ごとにホストがいくつあり、それらのホストにはポートがいくつありますか?
- 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 アレイが存在しますか?
- 各データセンターにはベンダーごとにいくつのスイッチがありますか?
- ライセンスされていないポートはいくつありますか?
- どのベンダーのテープを使用していますか? また、各テープにはいくつのポートがありますか? レポートの作業を開始する前に、すべての汎用デバイスが識別されていますか?
- ホストとストレージ ボリュームまたはテープ間のパスは何ですか?
- 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は何ですか?
- データセンターごとに各タイプの違反がいくつありますか?
- 複製されたボリュームごとに、ソース ボリュームとターゲット ボリュームは何ですか?
- ファイバー チャネル ホスト HBA とスイッチ間でファームウェアの非互換性やポート速度の不一致はありますか?

パフォーマンスデータモデル

ボリューム、アプリケーション ボリューム、内部ボリューム、スイッチ、アプリケーション、VM、VMDK、ESX と VM、ホスト、およびアプリケーション ノードのパフォーマンスに関する質問に答えることができます。これらの多くは、_時間別_データ、_日別_データ、またはその両方を報告します。このデータ モデルを使用すると、パフォーマンス管理に関するさまざまな質問に答える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はどれですか?
- アプリケーションのストレージ (未使用) の潜在的な構成ミスを特定できますか?
- アプリケーションの全体的なアクセス動作パターンは何でしたか?
- 階層化されたボリュームは特定のアプリケーションに適切に割り当てられていますか?
- アプリケーションのパフォーマンスに影響を与えずに、現在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?
- 現在構成されているストレージへのアクセスを多く生成しているアプリケーションは何ですか?

スイッチ パフォーマンス テーブルを使用すると、次の情報を取得できます。

- 接続されたポートを経由するホスト トラフィックはバランスが取れていますか?

- どのスイッチまたはポートでエラー数が多くなっていますか?
- ポートの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何ですか?
- ポートのパフォーマンスに基づいて、十分に活用されていないスイッチは何ですか?
- ポートのパフォーマンスに基づくホストのスループットの傾向は何ですか?
- 指定されたホスト、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使用率はどれくらいですか?
- 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はどれですか (たとえば、使用率の高いスイッチの使用に関与しているデバイスはどれですか)。
- 私たちの環境における特定のビジネス ユニットのスループットはどのくらいですか?

ディスク パフォーマンス 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 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はどれくらいですか?
- 最も使用されているストレージ プールは何ですか?
- 特定のストレージの平均ディスク使用率はどれくらいですか?
- 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 プールの使用傾向はどのようなものですか?
- 特定のストレージ プールのディスク使用率の傾向はどうですか?

VM および VMDK パフォーマンス テーブルを使用すると、次の情報を取得できます。

- 仮想環境は最適に動作していますか?
- 最も高いワークロードを報告している VMDK はどれですか?
- 異なるデータストアにマップされた VMD から報告されたパフォーマンスを使用して、再階層化に関する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、層の適切性、アプリケーションのストレージの誤った構成、ボリュームと内部ボリュームの最終アクセス時刻を判断するのに役立つ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、アクセス状態などのデータを提供します。

ストレージ効率データモデル

ストレージ効率スコアと潜在能力を時間の経過とともに追跡できます。このデータ モデルには、プロビジョニングされた容量だけでなく、使用または消費された量 (物理測定) の測定値も保存されます。たとえば、シン プロビジョニングが有効になっている場合、 Data Infrastructure Insights はデバイスから取得される容量を示します。このモデルを使用して、重複排除が有効になっている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、さまざまな質問に答えることができます。

- シン プロビジョニングと重複排除テクノロジを実装した結果、ストレージ効率はどの程度節約できるでしょうか。
- データセンター全体のストレージ節約量はどのくらいですか?
- 過去の容量傾向に基づくと、いつ追加のストレージを購入する必要がありますか?
- シン プロビジョニングや重複排除などのテクノロジーを有効にした場合、容量はどの程度増加しますか?

- ストレージ容量に関しては、現在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ます。

- ファクト テーブル: 数量、生容量、使用可能容量など、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 ユニットなどのファクトに関する説明情報が含まれます。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、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を記述するのに役立ちます。

異なるまたは複数のディメンション属性 (レポートでは列として表示) を使用して、データ モデルに記述されている各ディメンションのデータに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さまざまな表示があります。

- 黄色のアセット: 測定値を表します。
- 黄色以外の資産: 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、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 モデルのデータを組み合わせたレポートを作成することはできます。

複数のデータ モデルのデータを組み合わせ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 モデルの 1 つを選択し、追加のデータ マートのデータにアクセスするための SQL クエリを記述します。 SQL 結合機能を使用すると、さまざまなクエリからのデータを 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が必要で、アレイのカスタム注釈をキャプチャするとします。ストレージ容量データ モデルを使用してレポートを作成できます。現在の容量とディメンション テーブルの要素を使用し、別の SQL クエリを追加して、在庫データ モデル内の注釈情報にアクセスできます。最後に、ストレージ名と結合条件を使用して、在庫ストレージ データをストレージ ディメンション テーブルにリンクすることで、データを結合できます。

API経由でレポートデータベースにアクセスする

Data Infrastructure Insightsの強力な API を使用すると、ユーザーは Cognos Reporting 環境を経由せずに、 Data Infrastructure Insights Reporting データベースを直接クエリできます。

このドキュメントは、 Data Infrastructure Insights Premium Edition で利用できるData Infrastructure Insightsレポート機能について説明しています。

小田田

Data Infrastructure InsightsサイトレポートAPIは、"OData v4"レポート データベースのクエリを実行するため

の Open Data Protocol (Open Data Protocol) 標準。さらに詳しい情報や詳細については、"このチュートリアル" OData で。

すべてのリクエストは、URL *https://< Data Infrastructure Insights URL>/rest/v1/dwh-management/odata* で始まります。

APIキーの生成

詳細はこちら"Data Infrastructure InsightsAPI"。

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、管理者 **> API** アクセス を選択します。
- 「+ API アクセス トークン」をクリックします。
- 名前と説明を入力します。
- タイプには、「データ ウェアハウス」を選択します。
- 権限を読み取り/書き込みに設定します。
- 希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。後で完全なキーにアクセスすることはできません。

APIキーは次の用途に使えます同期 または 非同期。

テーブルの直接クエリ

API キーを設定すると、レポート データベースへの直接クエリが可能になります。長い URL は、表示上の都合上、完全な https://< Data Infrastructure Insights URL>/rest/v1/dwh-management/odata/ ではなく、\https://…/odata/ のように簡略化される場合があります。

次のような簡単なクエリを試してみましょう

- https://<Data Infrastructure InsightsのURL>/rest/v1/dwh-management/odata/dwh_custom
- https://<Data Infrastructure Insightsサイト URL>/rest/v1/dwh-management/odata/dwh_inventory
- https://<Data Infrastructure InsightsURL>/rest/v1/dwh-management/odata/dwh_inventory/storage
- https://<Data Infrastructure Insights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 URL>/rest/v1/dwh-management/odata/<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"
        }
    ]
}
```


役立つヒント

Reporting API クエリを使用するときは、次の点に留意してください。

- クエリペイロードは有効なJSON文字列である必要があります
- 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。例: \"
- タブは\tとしてサポートされています
- コメントを避ける
- 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:
  - 名前を「X-CloudInsights-ApiKey」にする
  - 属性値 "<apikey>"

API キーは、Data Infrastructure Insights環境に固有のものになります。

同期か非同期か**?**

デフォルトでは、API コマンドは同期モードで動作します。つまり、リクエストを送信すると、すぐに応答が返されます。ただし、クエリの実行に長い時間がかかり、リクエストがタイムアウトになる場合があります。これを回避するには、リクエストを非同期的に実行します。非同期モードでは、リクエストは実行を監視できる URL を返します。準備ができたら、URL から結果が返されます。

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**`リクエストに応じて。実行が成功すると、応答には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>
```

場所の URL を照会すると、応答がまだ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。応答コンテンツはテキスト タイプになり、元のクエリの http ステータスといくつかの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、そのうちのどれが準備完了しているかを確認するには、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
       }
   ]
}
```

レポート用の注釈の公開と非公開

レポート用の注釈の公開と非公開

レポートやデータ ウェアハウスで使用するために注釈を公開する方法と、不要になった注釈を適切に非公開にする方法について説明します。

レポート用の注釈の公開

Data Infrastructure Insightsで注釈を作成したら、それをレポートで使用するために公開できます。

注釈を公開する手順

1. *「観察可能性」>「強化」>「注釈」ページに移動し、「レポートの注釈」タブを選択します。
2. 公開する注釈を見つけます。
3. 注釈を選択し、[レポートに公開] を選択します。また、「履歴データに適用」を選択して、履歴レポートの実行時に注釈を使用できるようにすることもできます。
4. 公開されると、注釈はレポートで使用できるようになります。
5. 注釈は、次の ETL 実行後のレポートで使用するために公開されます。

> ⓘ 注釈を参照するレポートでは、公開された値が使用されます。公開後に注釈を変更した場合、その変更をレポートに反映させるには、再度公開する必要がある場合があります。

レポート用の注釈を非公開にする

レポートで注釈が使用されないように、注釈を削除または非公開にする必要がある場合があります。たとえば、注釈が不要になったり、レポートに表示すべきでない古い情報が含まれている場合があります。

注釈を非公開にする手順

注釈を非公開にする前に、この操作によって注釈を使用している既存のレポートに影響が及ぶことに注意してください。レポートでは、注釈参照を削除するために編集や専門サービスの支援が必要になる場合があります。

1. Data Infrastructure Insightsユーザー インターフェースで、[レポートの注釈] タブに移動します。
2. 非公開にする注釈を見つけます。
3. 注釈が公開されているオブジェクトごとに、注釈の選択を解除し、[保存] を選択します。
4. まだ注釈を参照しているクエリやルールを削除して、注釈が「使用中」としてマークされていないことを確認します。
5. 次回の ETL 実行後、注釈は非公開になります。
6. ETL が完了したら、テナント側で不要になった注釈は注釈のリストから削除できます。

> ⓘ 注釈は、適切に非公開にされるまで、データ ウェアハウスに引き続き表示されます。最初に非公開にせずに「注釈」ページから注釈を削除するだけでは、古いデータが残り、既存のレポートに表示される可能性があります。完全に削除するには、上記の非公開手順に従ってください。

既存のレポートへの影響

注釈を削除または非公開にするには、それらの注釈を参照する既存のレポートを変更する必要がある場合があります。次の点を考慮してください。

- 注釈をフィルターまたはディメンションとして使用するレポートは更新する必要があります。
- 依存レポートを更新せずに注釈を削除すると、それらのレポートでエラーや予期しない結果が返される可能性があります。
- 複雑なシナリオでは、レポートの修復を支援するために専門サービスが必要になる場合があります。

注釈を非公開にする前に、注釈に依存するすべてのレポートを確認することをお勧めします。

レポート用の履歴データの保存方法

Data Infrastructure Insights は、次の表に示すように、データ マートとデータの粒度に基づいて、レポートで使用するための履歴データを保持します。

データマート	測定対象物	粒度	保持期間
パフォーマンスマート	ボリュームと内部ボリューム	時間単位	14日間
パフォーマンスマート	ボリュームと内部ボリューム	日次	13カ月
パフォーマンスマート	Application	時間単位	13カ月
パフォーマンスマート	ホスト	時間単位	13カ月
パフォーマンスマート	ポートのスイッチパフォーマンス	時間単位	35日間
パフォーマンスマート	ホスト、ストレージ、テープのスイッチパフォーマンス	時間単位	13カ月
パフォーマンスマート	ストレージ ノード	時間単位	14日間

パフォーマンスマート	ストレージ ノード	日次	13カ月
パフォーマンスマート	VMパフォーマンス	時間単位	14日間
パフォーマンスマート	VMパフォーマンス	日次	13カ月
パフォーマンスマート	ハイパーバイザーのパフォーマンス	時間単位	35日間
パフォーマンスマート	ハイパーバイザーのパフォーマンス	日次	13カ月
パフォーマンスマート	VMDKパフォーマンス	時間単位	35日間
パフォーマンスマート	VMDKパフォーマンス	日次	13カ月
パフォーマンスマート	ディスクパフォーマンス	時間単位	14日間
パフォーマンスマート	ディスクパフォーマンス	日次	13カ月
キャパシティマート	すべて（個別巻を除く）	日次	13カ月
キャパシティマート	すべて（個別巻を除く）	月間代表	14ヶ月以上
在庫マート	個々の巻	現在の状態	1日（または次のETLまで）

Data Infrastructure Insightsレポートスキーマダイアグラム

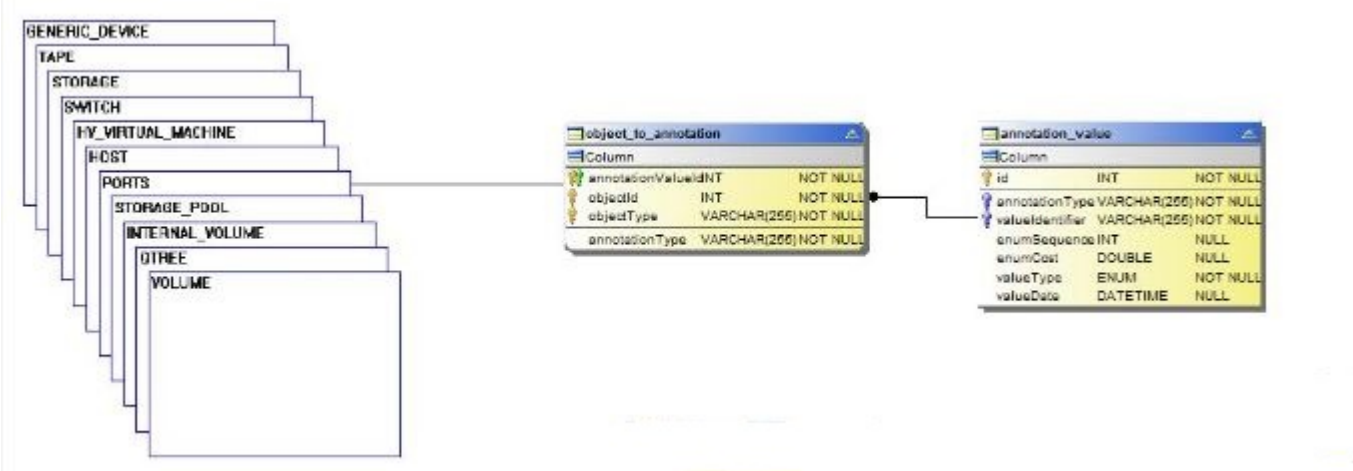
このドキュメントでは、レポート データベースのスキーマ ダイアグラムを示します。

レポート機能は、Data Infrastructure Insightsで利用できます。"プレミアムエディション" 。

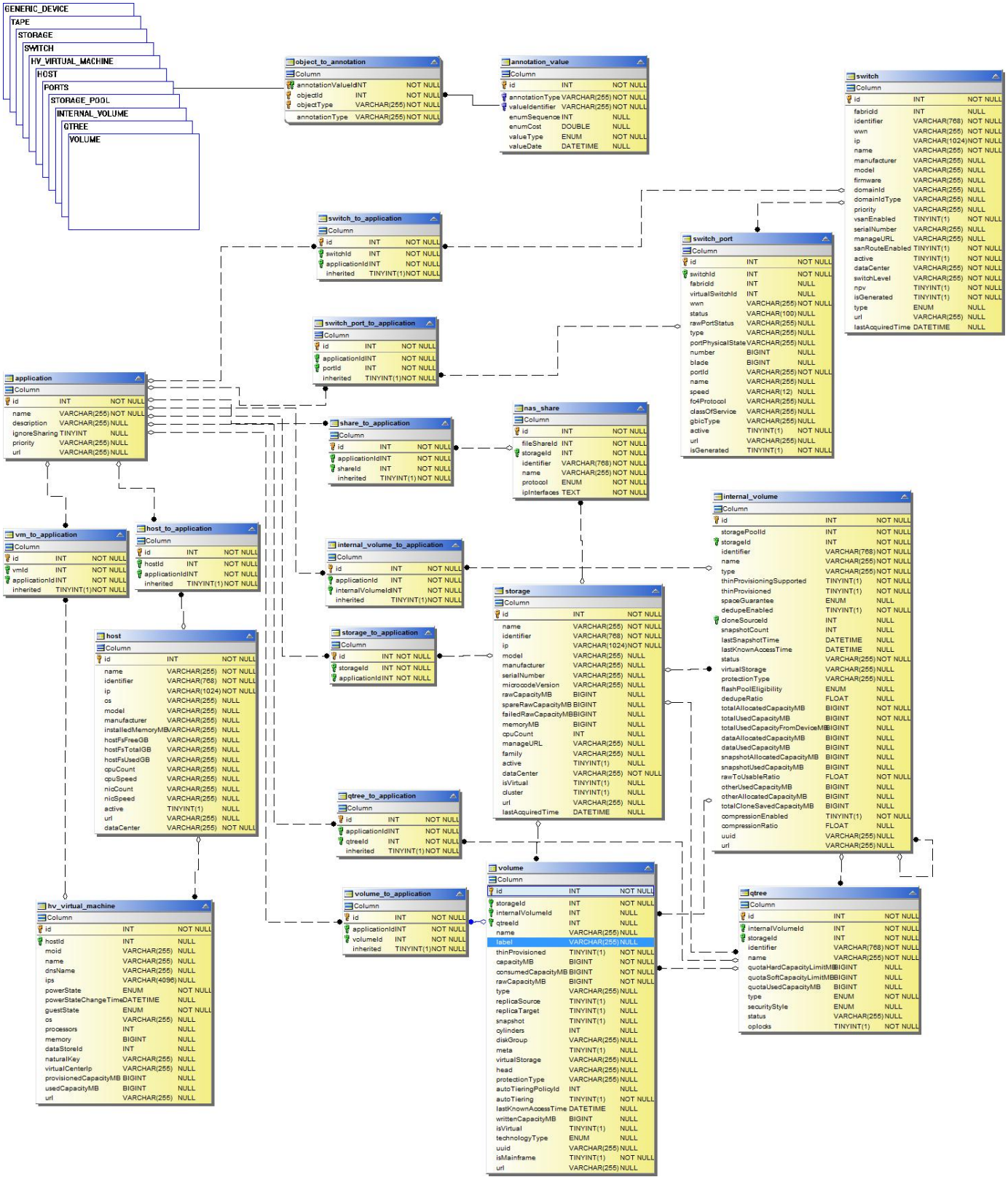
在庫データマート

次の画像は在庫データマートを説明しています。

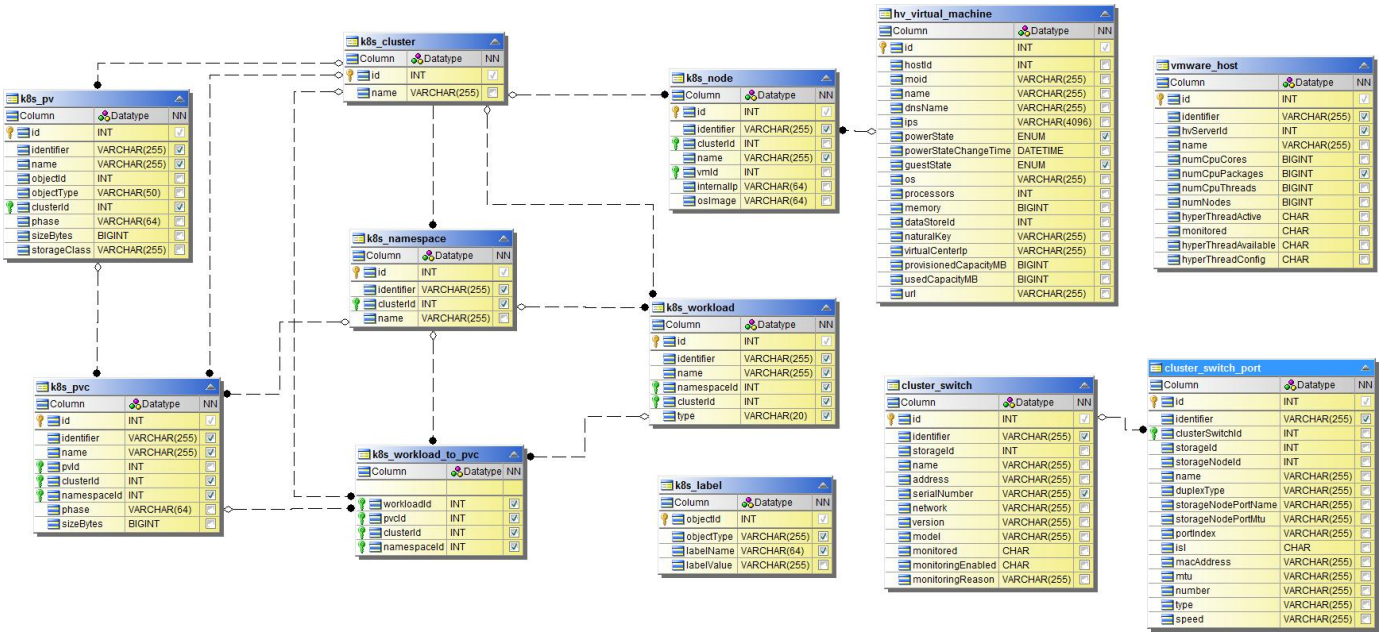
アノテーション



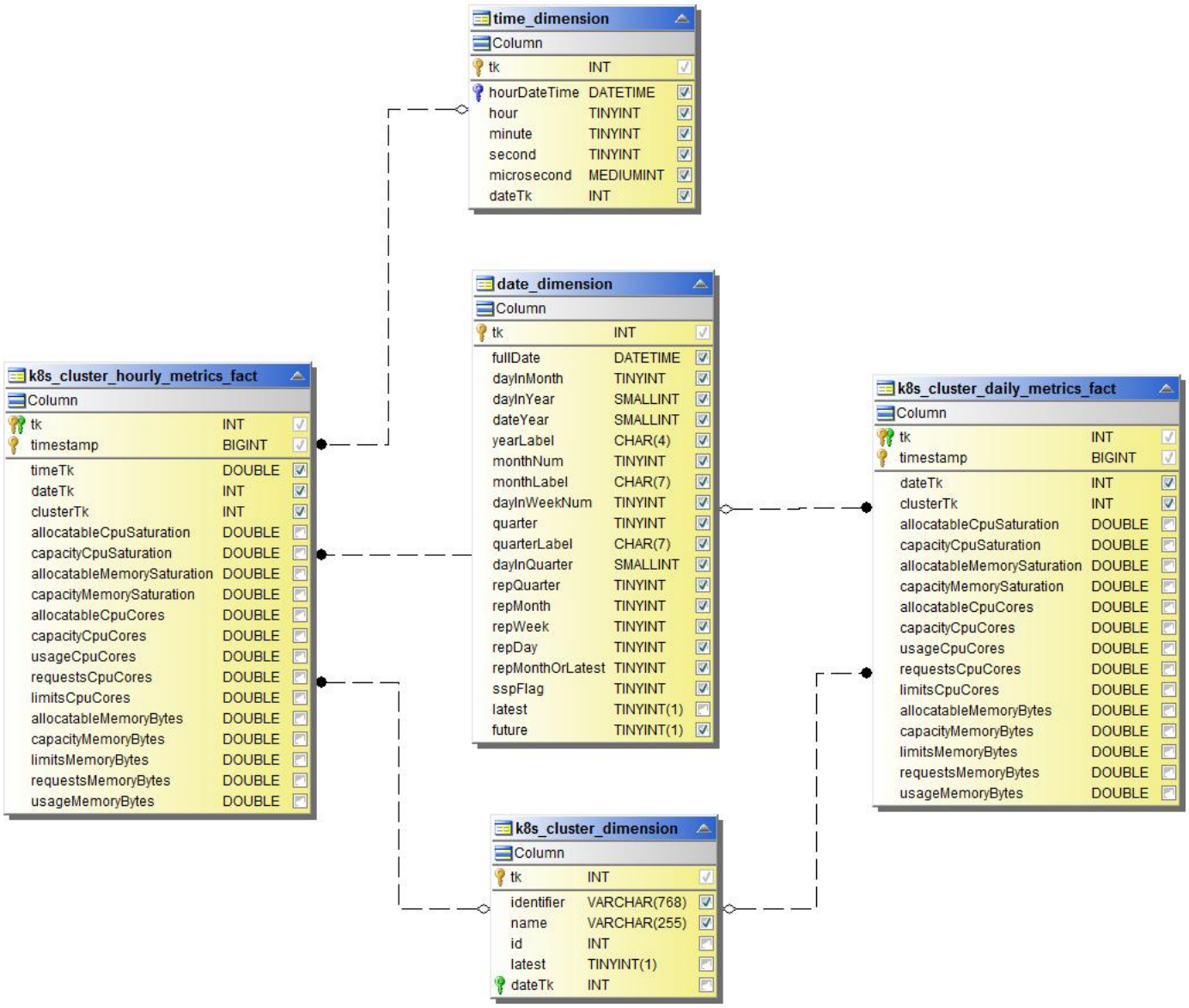
アプリケーション



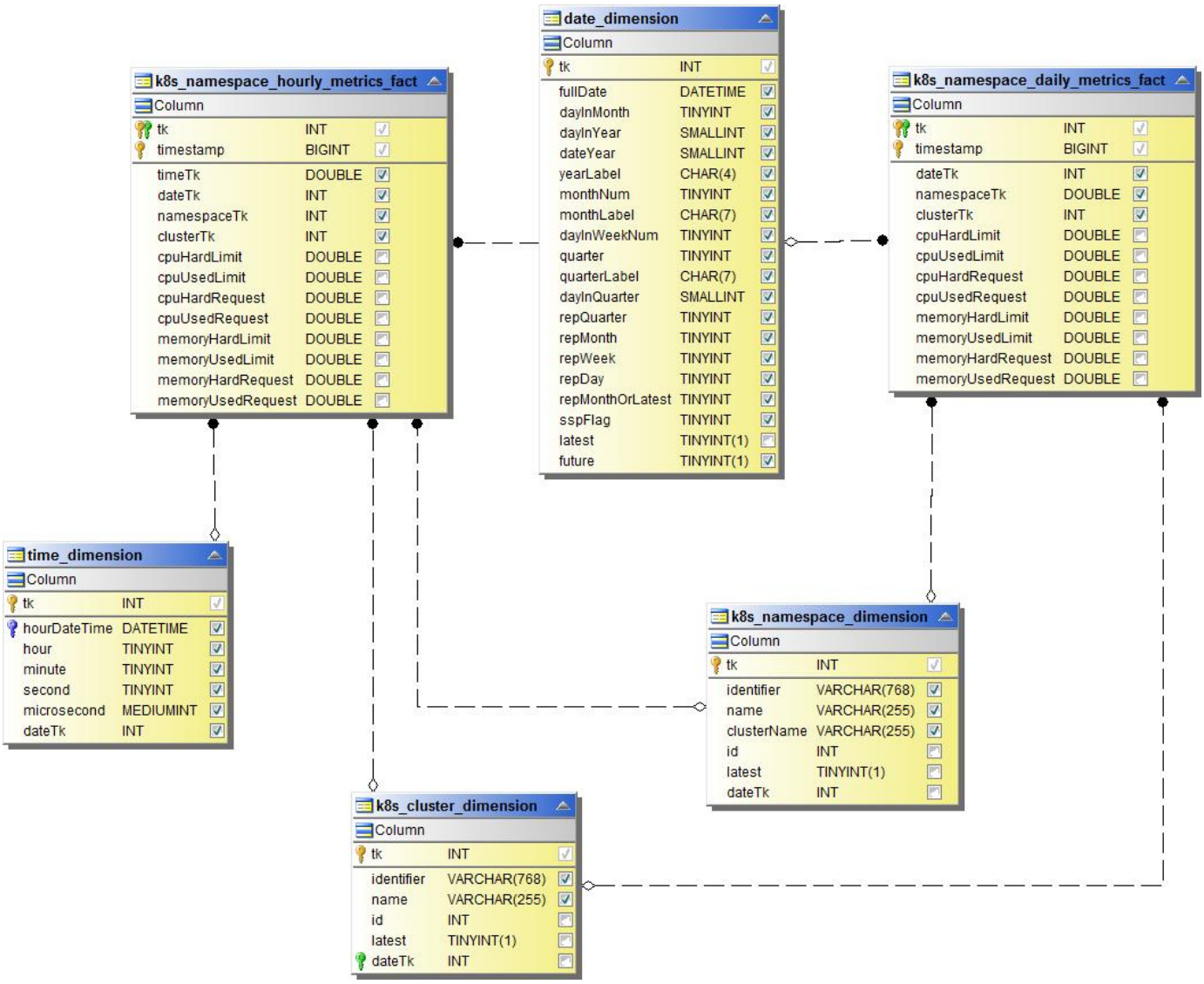
Kubernetes メトリクス



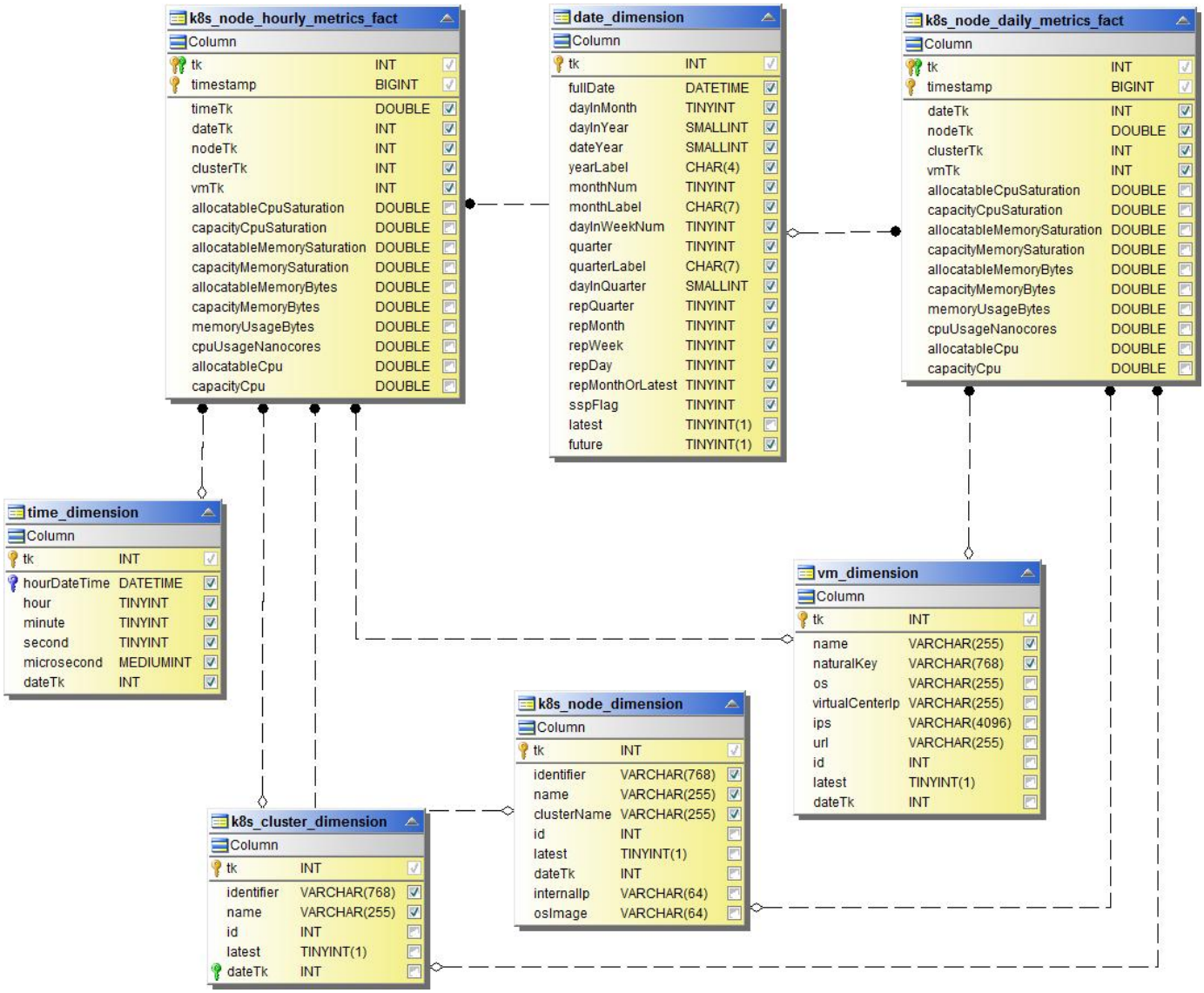
Kubernetes クラスターメトリクスの事実



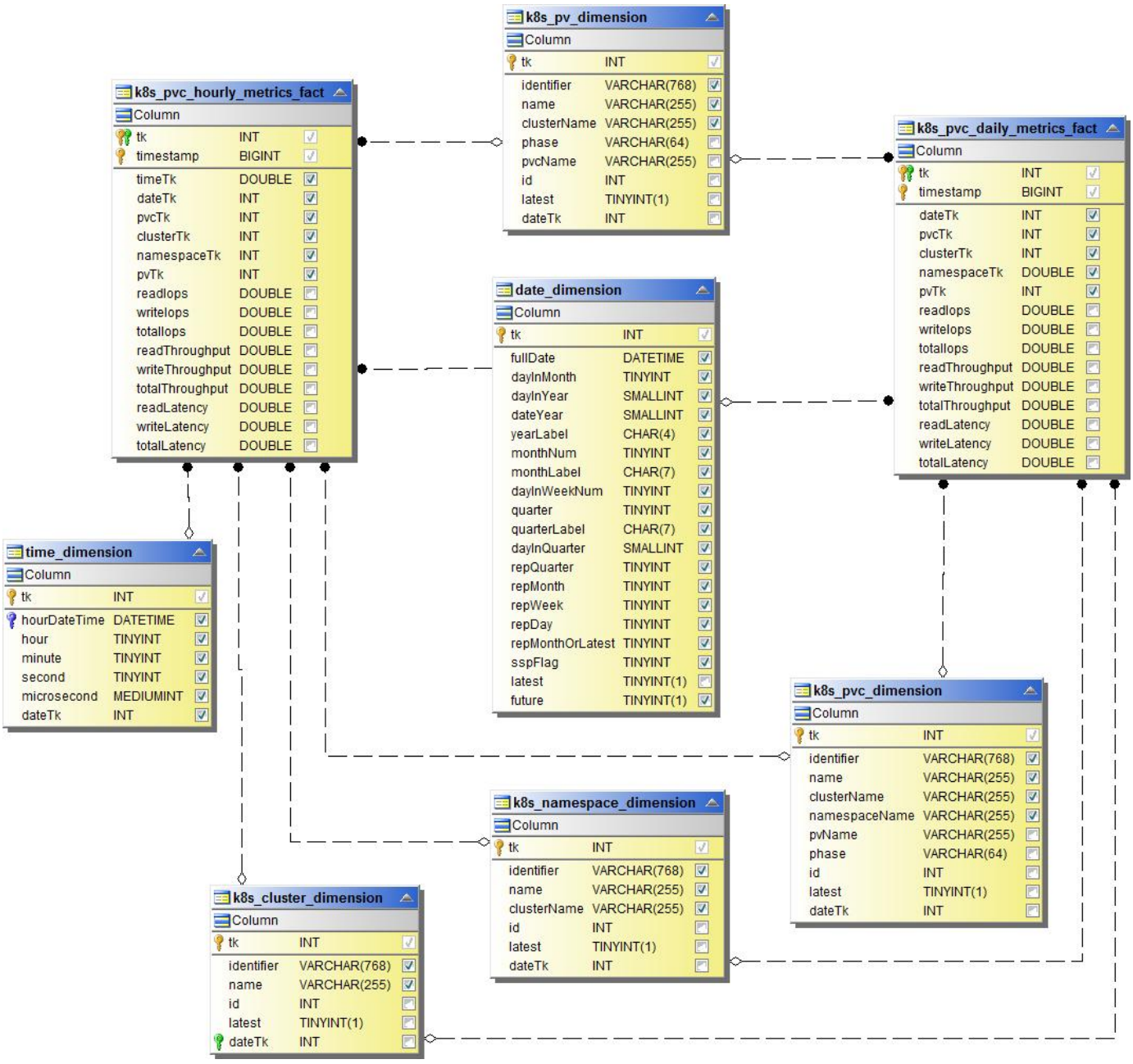
Kubernetes 名前空間メトリクスの事実



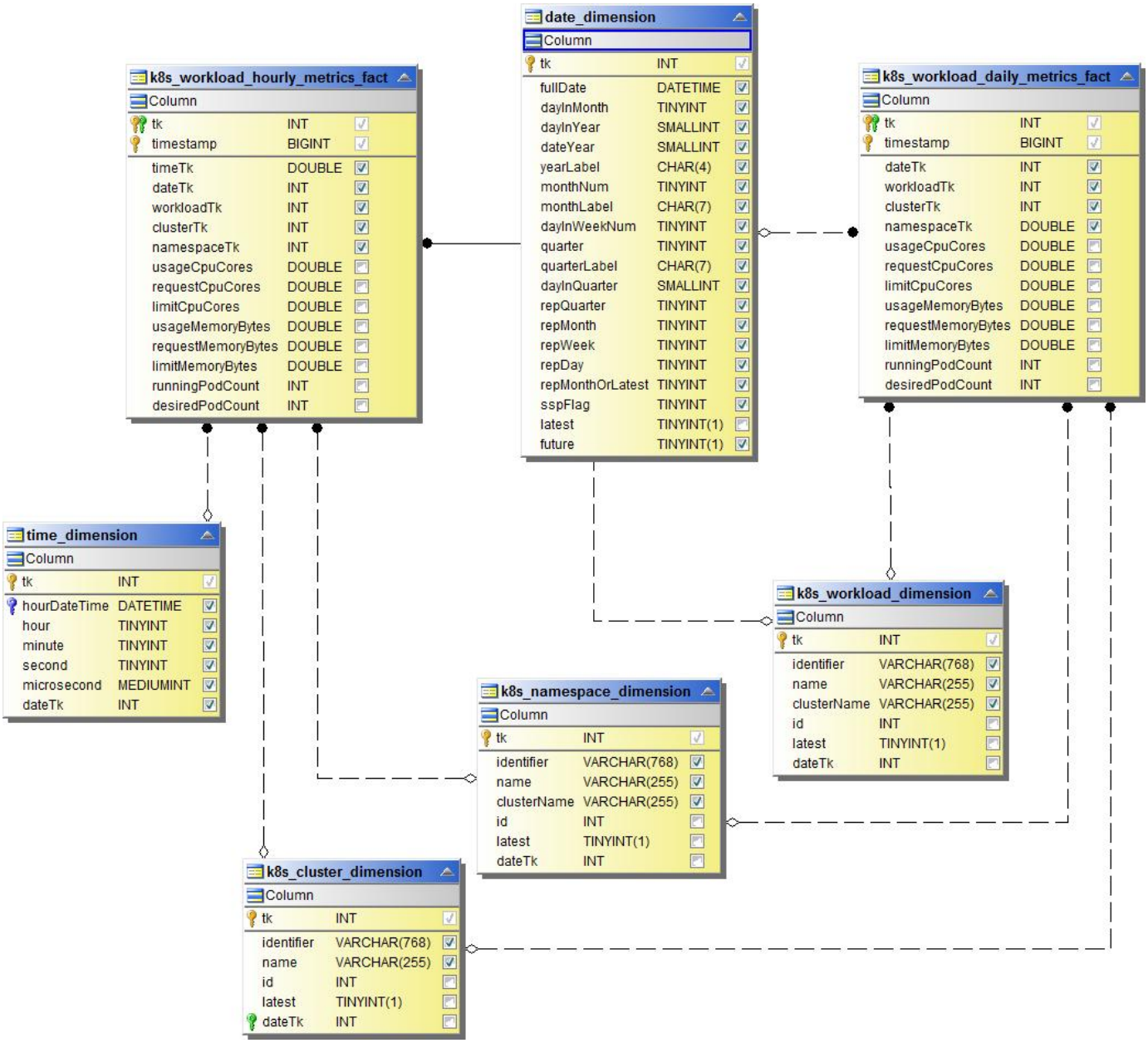
Kubernetes ノードメトリクスの事実



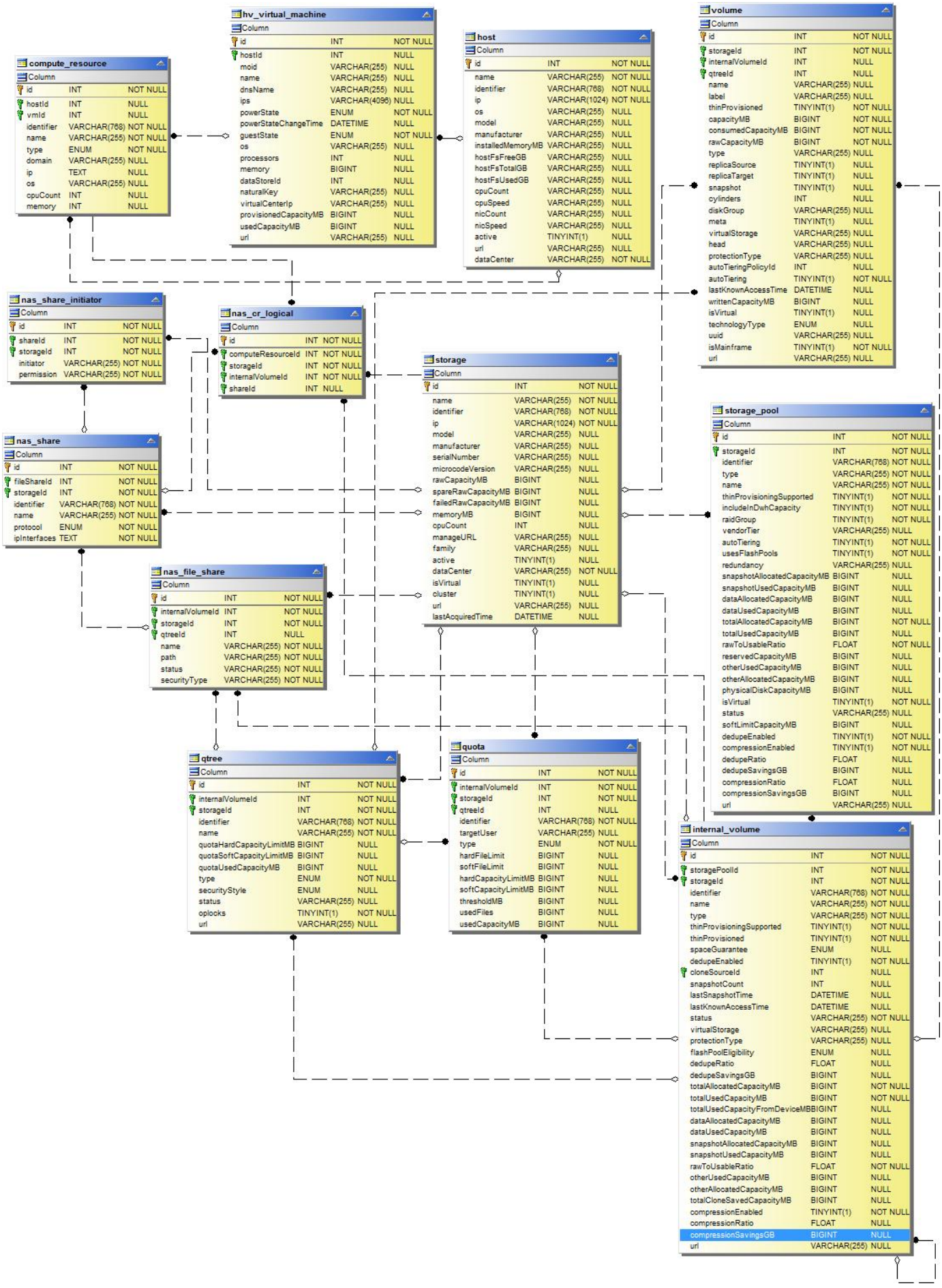
Kubernetes PVC メトリクスの事実



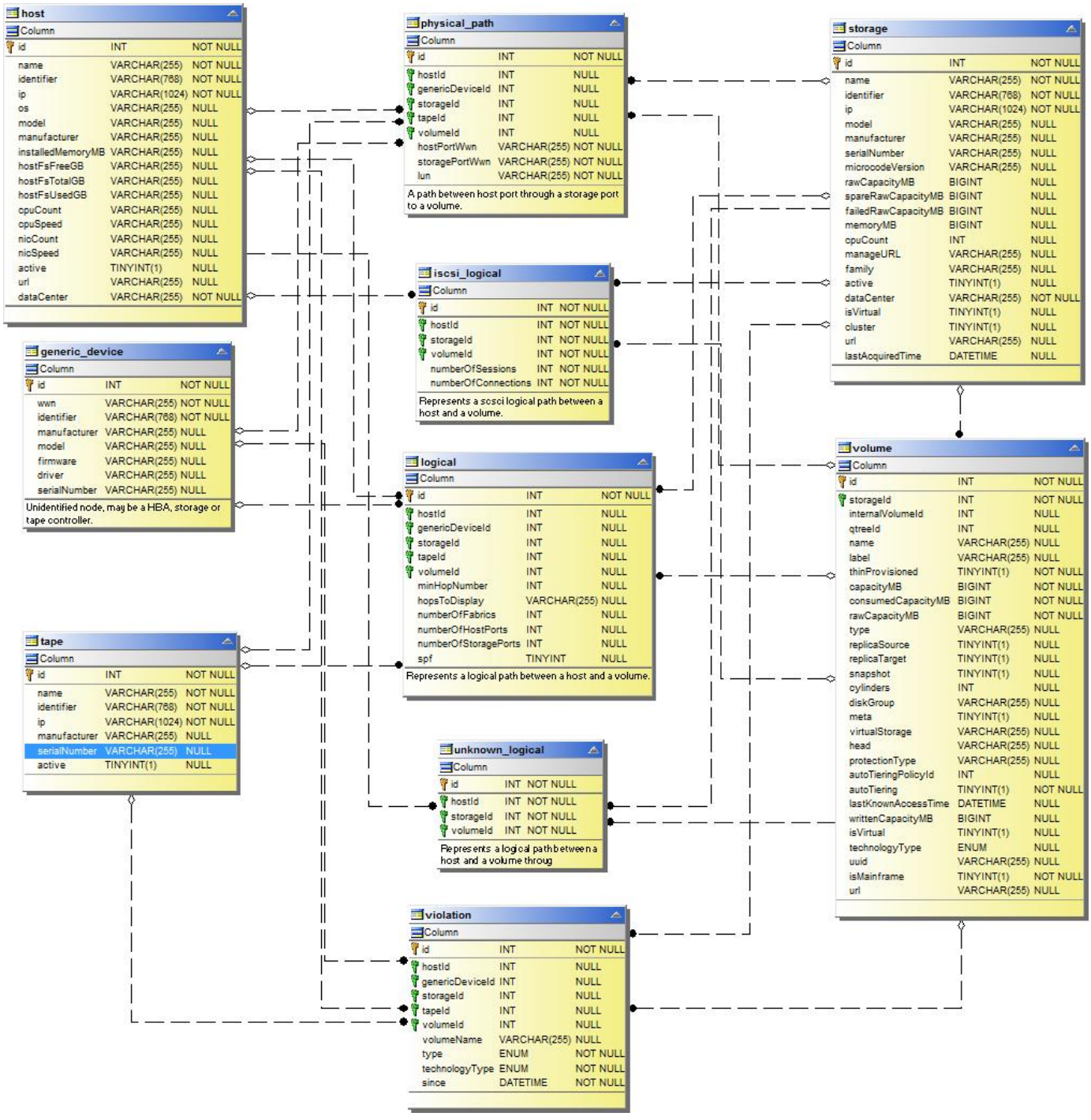
Kubernetes ワークロード メトリクスの事実


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

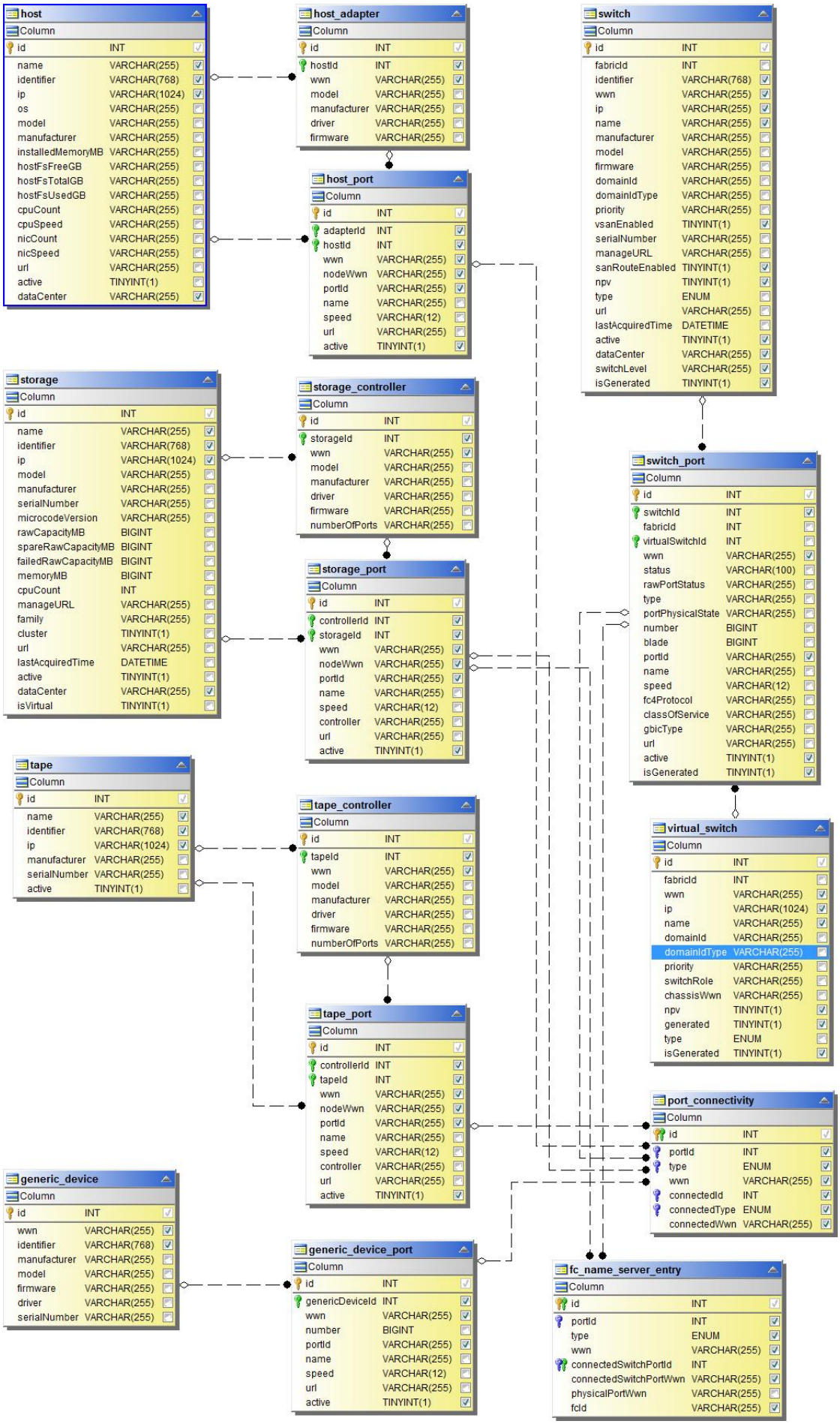
NAS


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(1024) 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(1024) 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
includeInDwhCapacity 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
dedupeSavingsGB BIGINT NULL
compressionRatio FLOAT NULL
compressionSavingsGB BIGINT 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
dedupeSavingsGB BIGINT 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
compressionSavingsGB BIGINT NULL
url VARCHAR(255) NULL

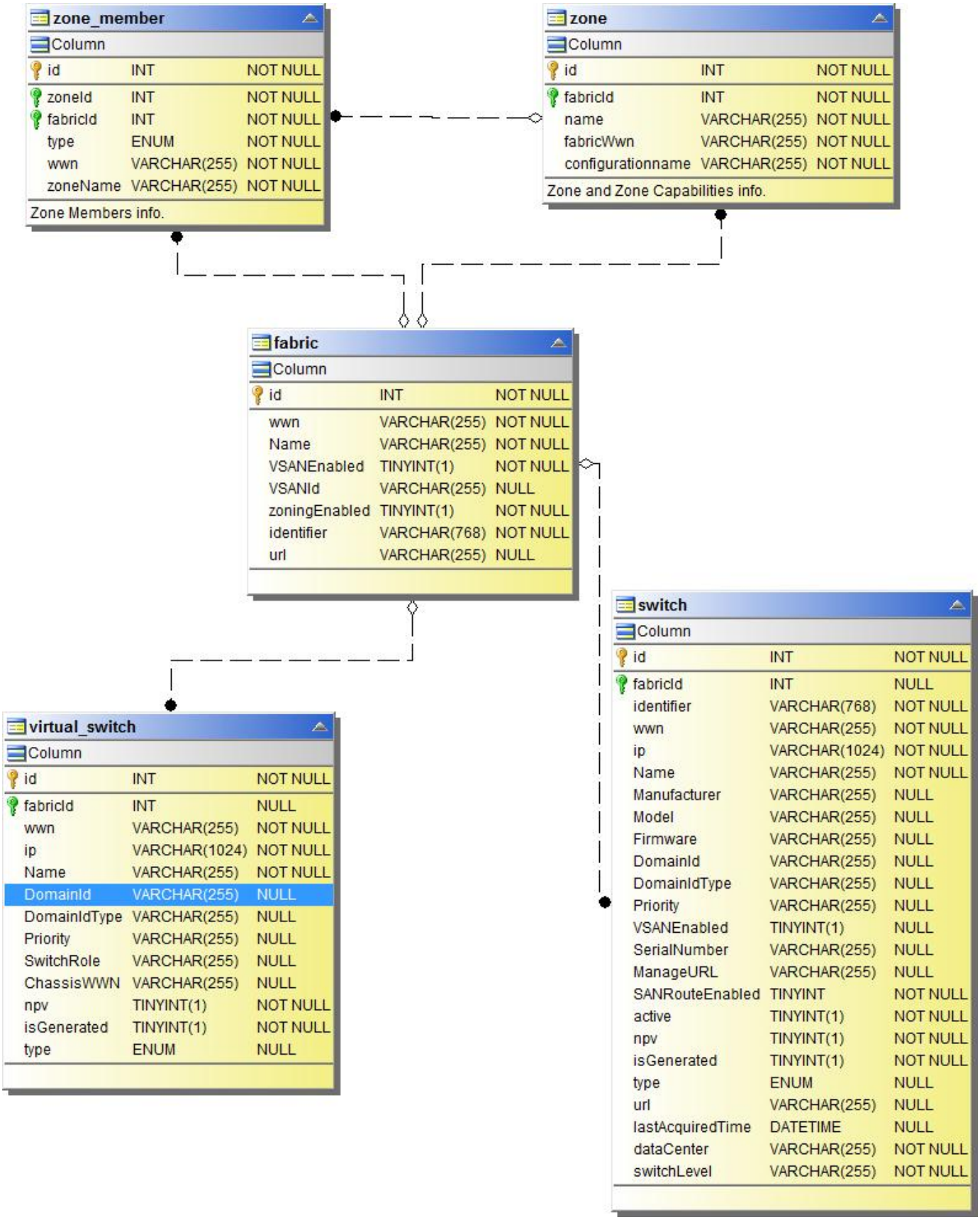
パスと違反

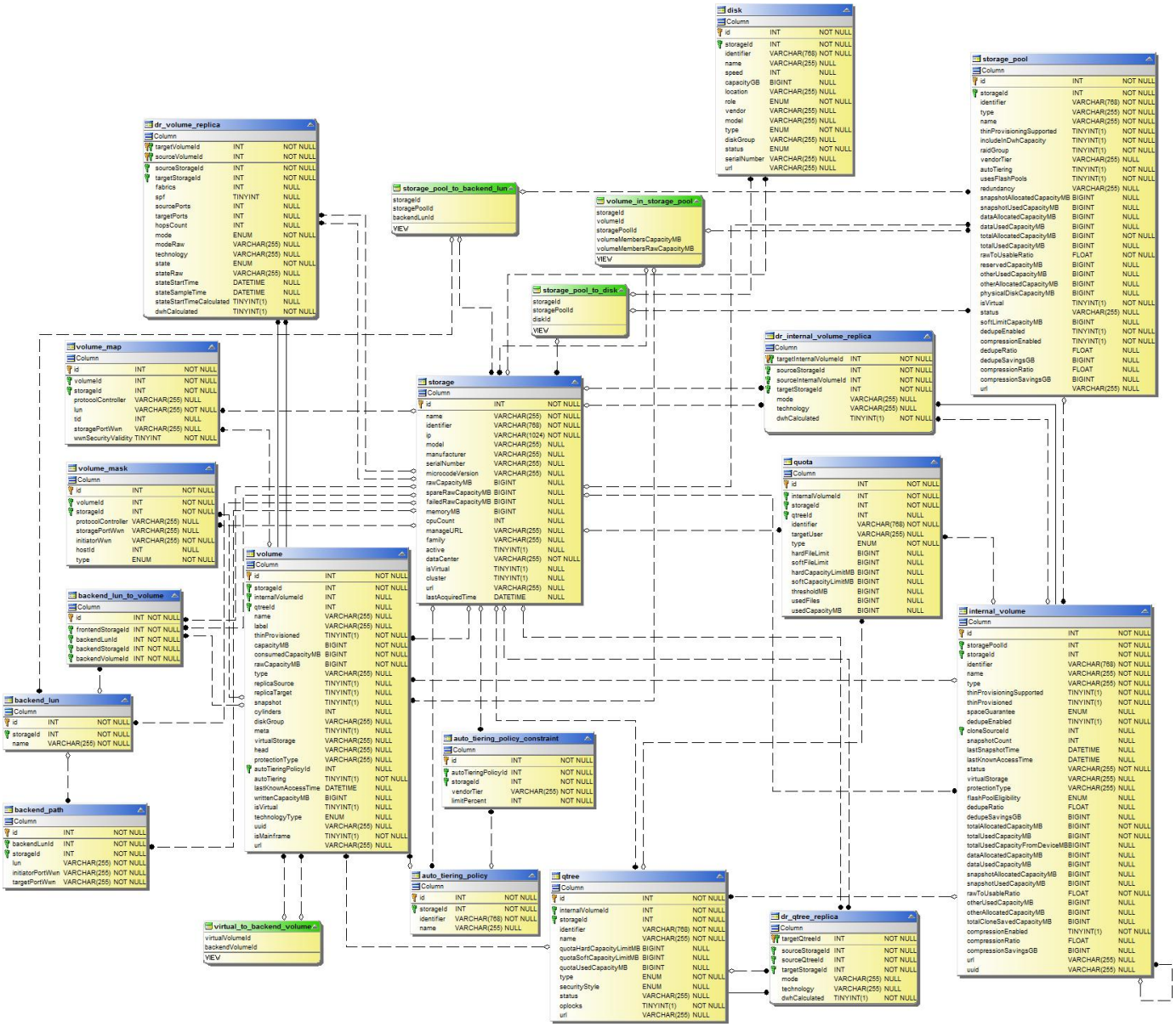

host
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(1024) NOT NULL
os VARCHAR(255) NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
installedMemoryMB VARCHAR(255) NULL
hostFsFreeGB VARCHAR(255) NULL
hostFsTotalGB VARCHAR(255) NULL
hostFsUsedGB 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(1024) 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(1024) 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

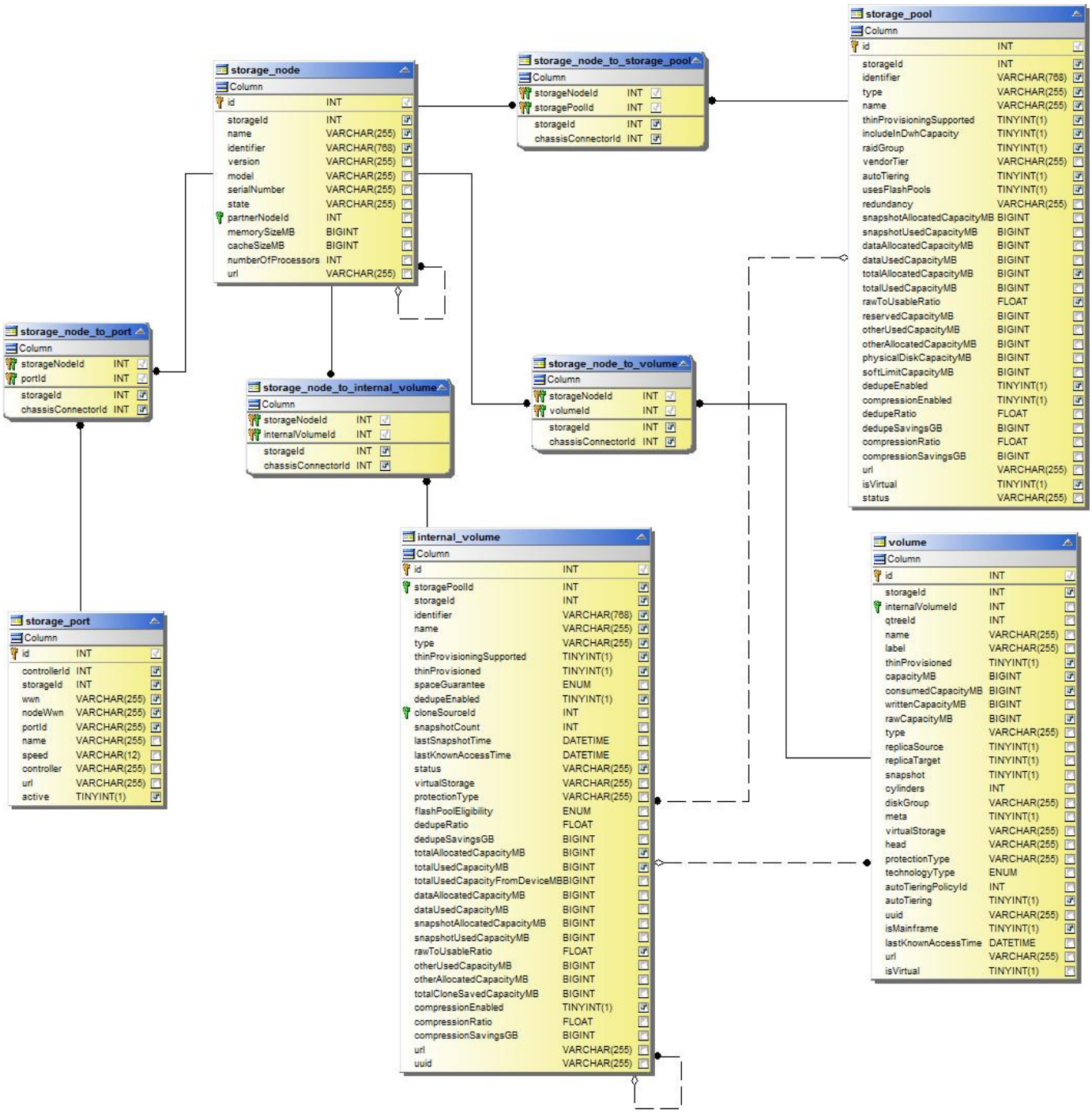

host
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
os VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
installedMemoryMB VARCHAR(255)
hostFsFreeGB VARCHAR(255)
hostFsTotalGB VARCHAR(255)
hostFsUsedGB VARCHAR(255)
cpuCount VARCHAR(255)
cpuSpeed VARCHAR(255)
nicCount 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(1024)
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(1024)
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)
virtual_switch
Column
id INT
fabricId INT
wwn VARCHAR(255)
ip VARCHAR(1024)
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)
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)
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

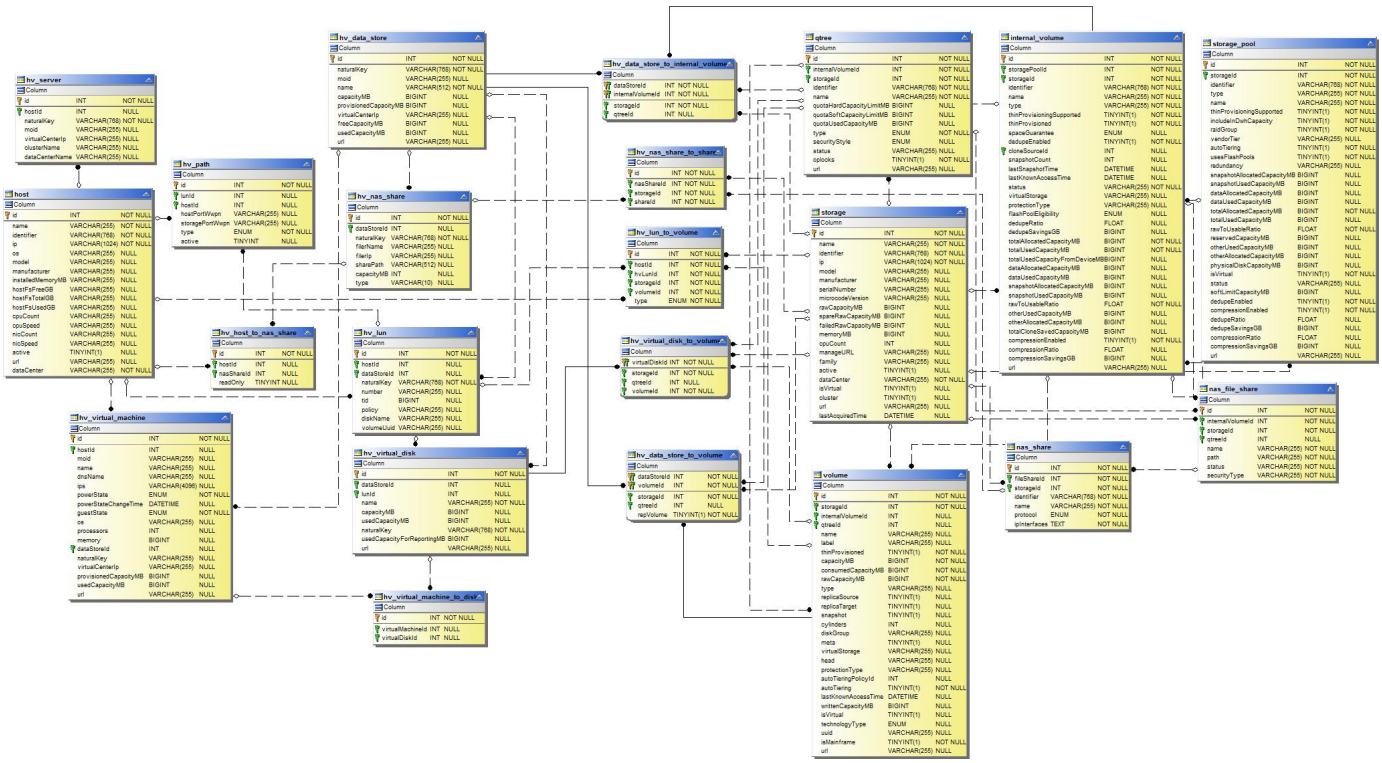

zone_member
Column
id INT NOT NULL
zoneId INT NOT NULL
fabricId INT NOT NULL
type ENUM NOT NULL
wwn VARCHAR(255) NOT NULL
zoneName VARCHAR(255) NOT NULL
Zone Members info.
zone
Column
id INT NOT NULL
fabricId INT NOT NULL
name VARCHAR(255) NOT NULL
fabricWwn VARCHAR(255) NOT NULL
configurationname VARCHAR(255) 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(1024) 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(1024) 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
dr_internal_volume_replica
volume_map
storage
volume_mask
quota
volume
backend_lun_to_volume
internal_volume
backend_lun
auto_tiering_policy_constraint
backend_path
auto_tiering_policy
qtree
virtual_to_backend_volume
dr_qtree_replica

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
dedupeSavingsGB BIGINT
compressionRatio FLOAT
compressionSavingsGB BIGINT
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
dedupeSavingsGB BIGINT
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
compressionSavingsGB BIGINT
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)

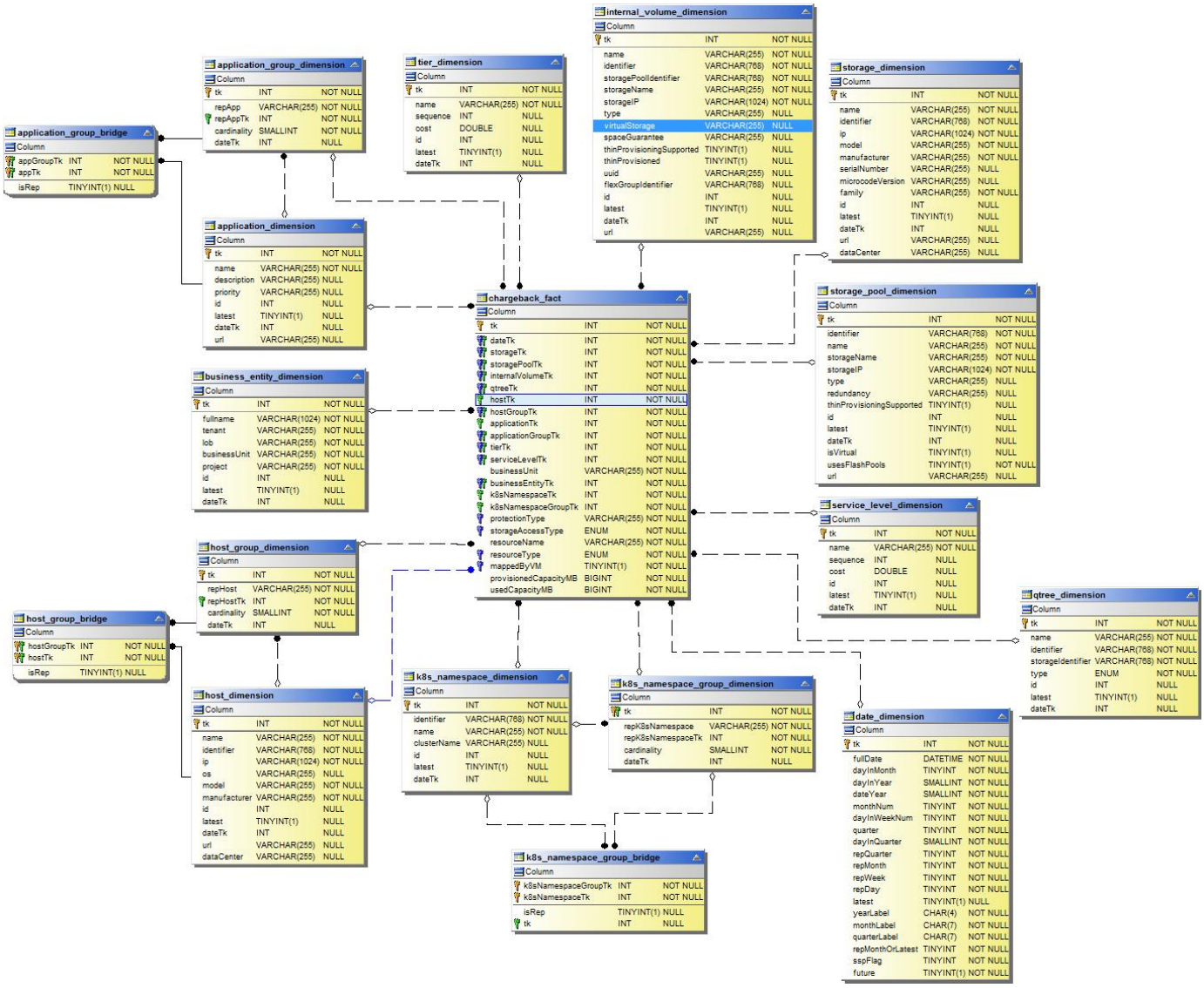
VM



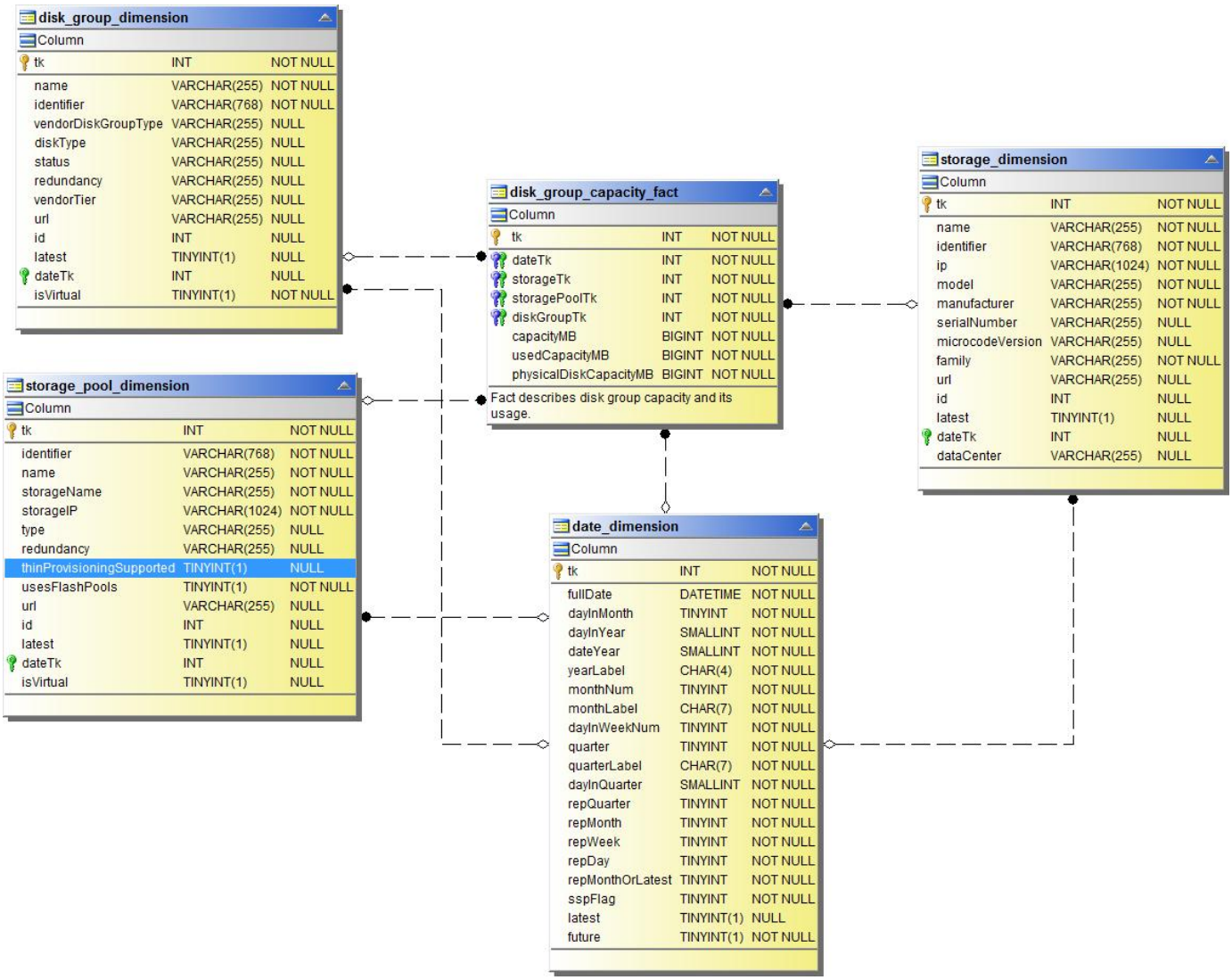
容量データマート

次の画像は容量データマートを説明しています。

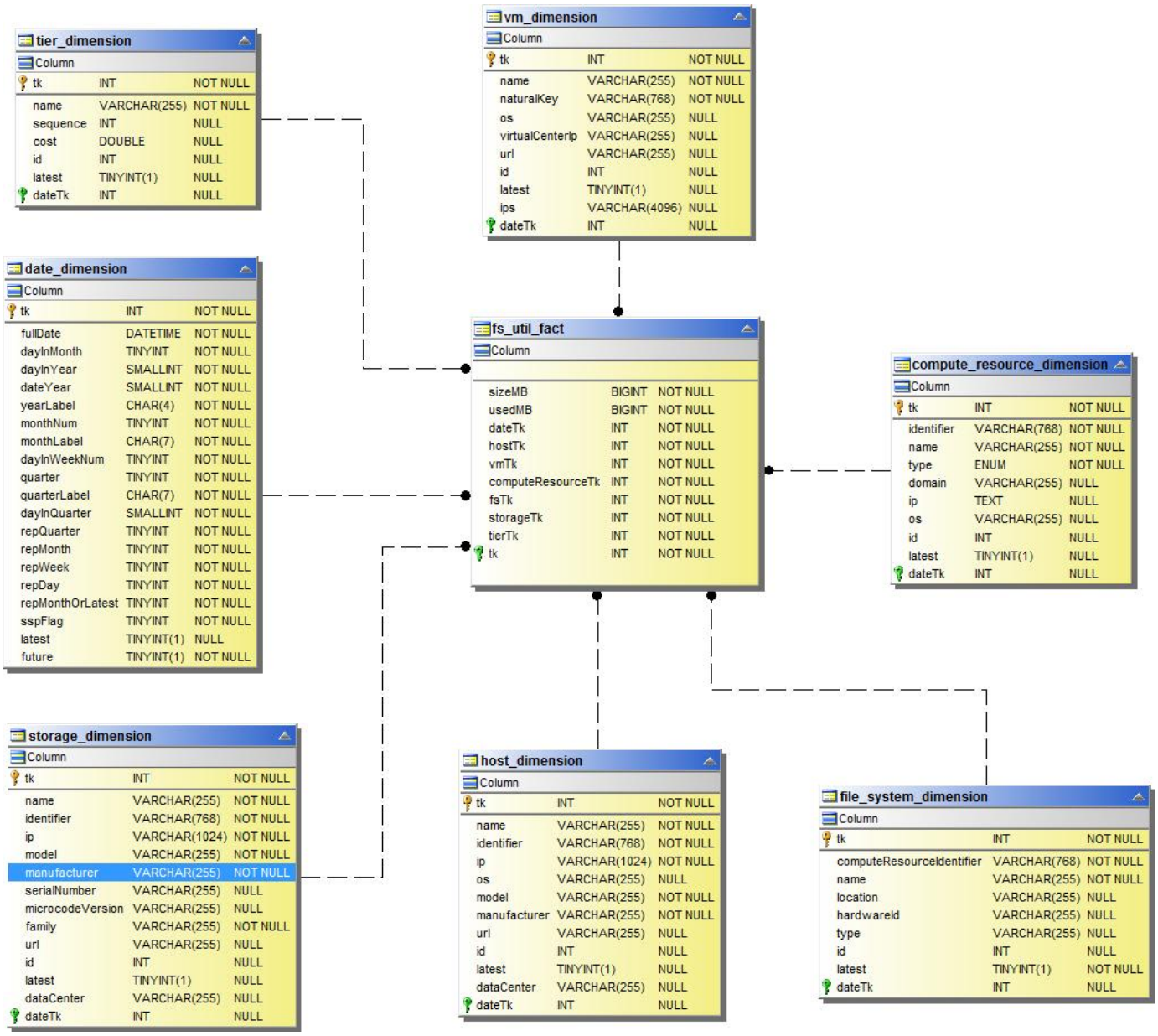
チャージバック


application_group_bridge
Column
appGroupTk INT NOT NULL
appTk INT NOT NULL
isRep TINYINT(1) 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
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
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(1024) NOT NULL
type VARCHAR(255) NULL
virtualStorage VARCHAR(255) NULL
spaceGuarantee VARCHAR(255) NULL
thinProvisioningSupported TINYINT(1) NULL
thinProvisioned TINYINT(1) NULL
uuid VARCHAR(255) NULL
flexGroupIdentifier VARCHAR(768) NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
url VARCHAR(255) NULL
storage_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(1024) 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
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
chargeback_fact
Column
tk INT NOT NULL
dateTk INT NOT NULL
storageTk INT NOT NULL
storagePoolTk INT NOT NULL
internalVolumeTk INT NOT NULL
qtreeTk INT NOT NULL
hostTk INT NOT NULL
hostGroupTk INT NOT NULL
applicationTk INT NOT NULL
applicationGroupTk INT NOT NULL
tierTk INT NOT NULL
serviceLevelTk INT NOT NULL
businessUnit VARCHAR(255) NOT NULL
businessEntityTk INT NOT NULL
k8sNamespaceTk INT NOT NULL
k8sNamespaceGroupTk INT NOT NULL
protectionType VARCHAR(255) NOT NULL
storageAccessType ENUM NOT NULL
resourceName VARCHAR(255) NOT NULL
resourceType ENUM NOT NULL
mappedByVM TINYINT(1) NOT NULL
provisionedCapacityMB BIGINT NOT NULL
usedCapacityMB BIGINT NOT NULL
storage_pool_dimension
Column
tk INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
storageName VARCHAR(255) NOT NULL
storageIP VARCHAR(1024) NOT NULL
type VARCHAR(255) NULL
redundancy VARCHAR(255) NULL
thinProvisioningSupported TINYINT(1) NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
isVirtual TINYINT(1) NULL
usesFlashPools TINYINT(1) NOT 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
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
host_group_dimension
Column
tk INT NOT NULL
repHost VARCHAR(255) NOT NULL
repHostTk INT NOT NULL
cardinality SMALLINT NOT NULL
dateTk INT 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
host_group_bridge
Column
hostGroupTk INT NOT NULL
hostTk INT NOT NULL
isRep TINYINT(1) NULL
host_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(1024) 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
k8s_namespace_dimension
Column
tk INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
clusterName VARCHAR(255) NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
k8s_namespace_group_dimension
Column
tk INT NOT NULL
repK8sNamespace VARCHAR(255) NOT NULL
repK8sNamespaceTk INT NOT NULL
cardinality SMALLINT NOT 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
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
k8s_namespace_group_bridge
Column
k8sNamespaceGroupTk INT NOT NULL
k8sNamespaceTk INT NOT NULL
isRep TINYINT(1) NULL
tk INT NULL

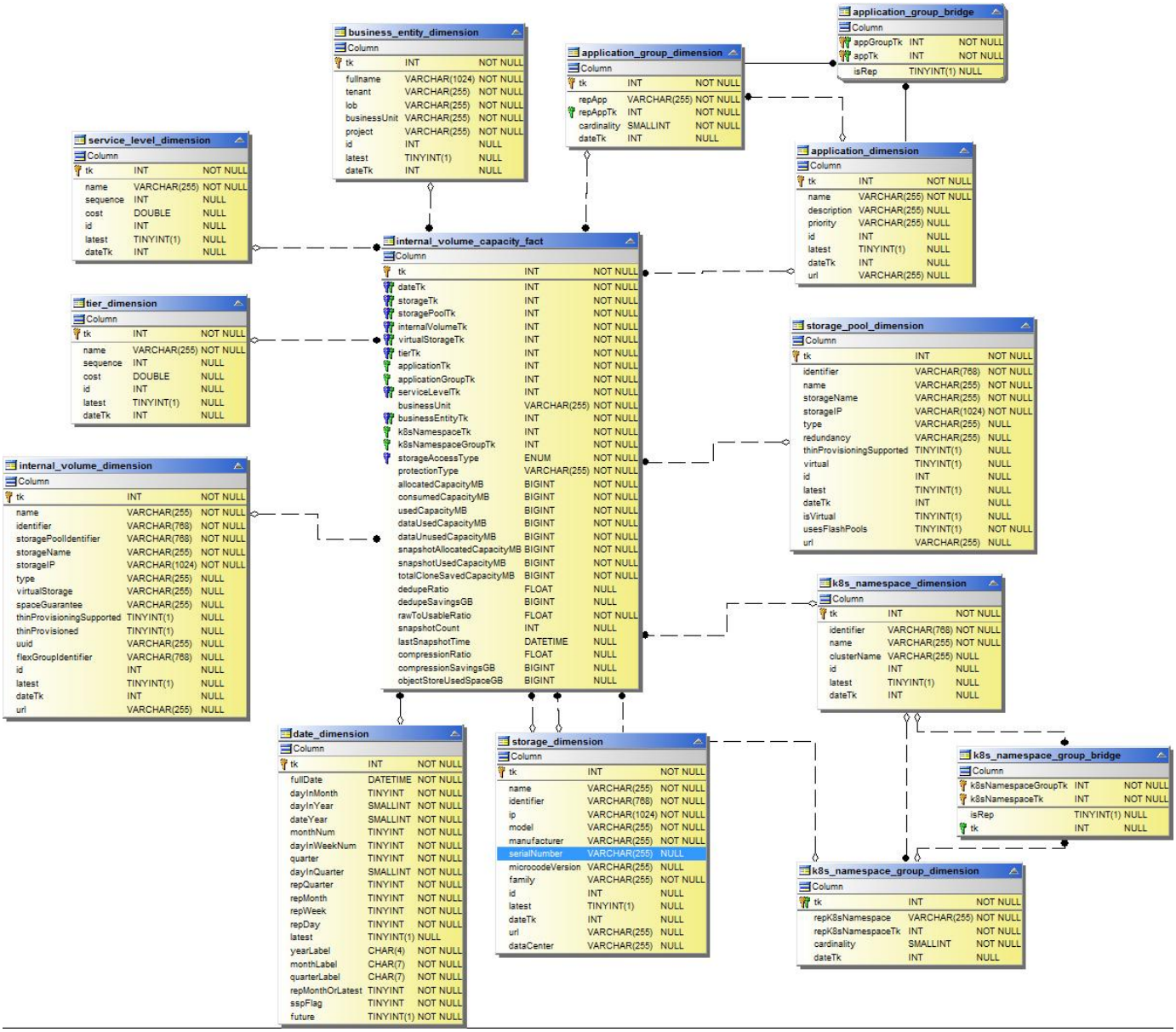
ディスクグループ容量



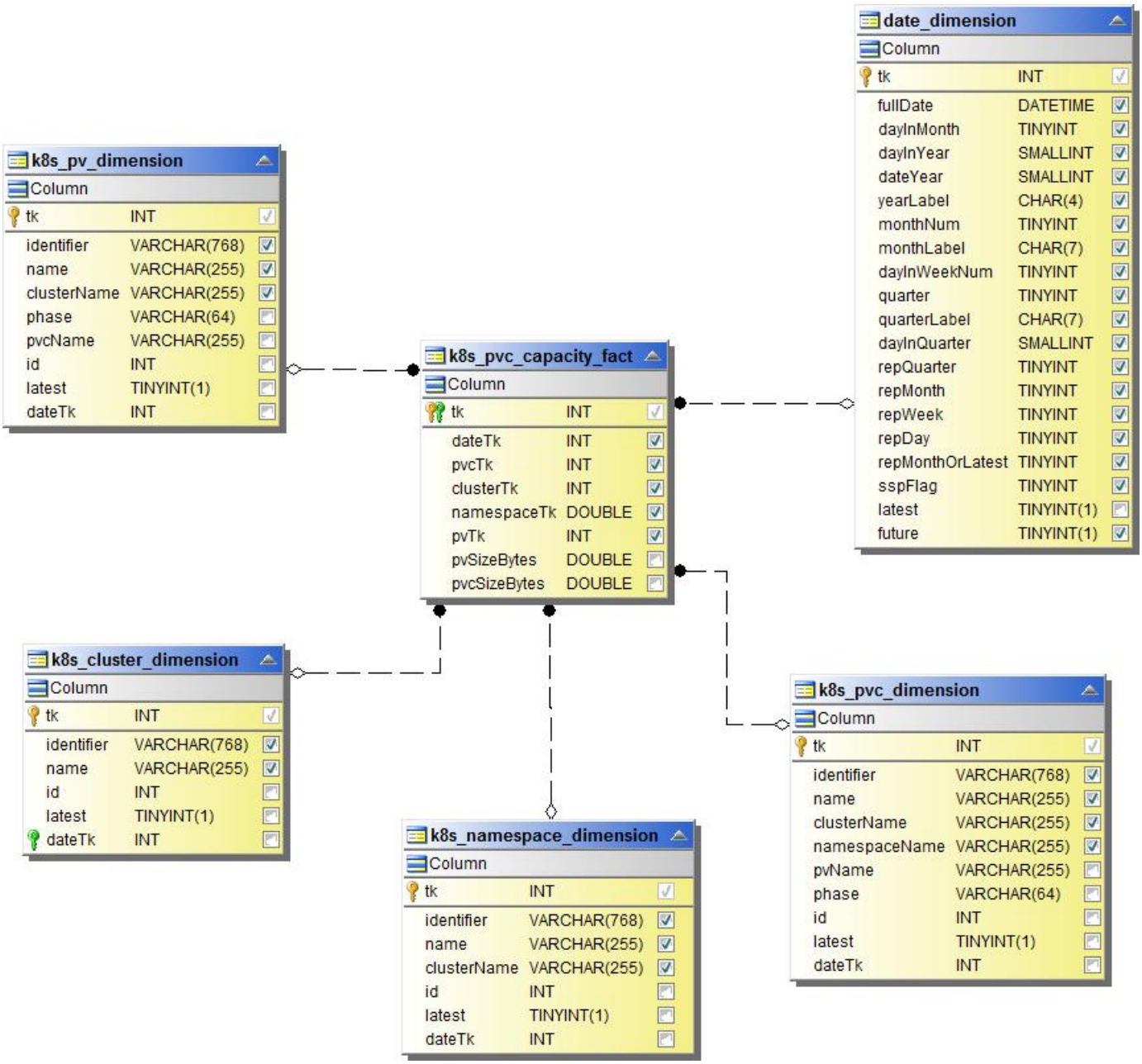
ファイルシステムの使用率


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(1024) 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(1024) 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

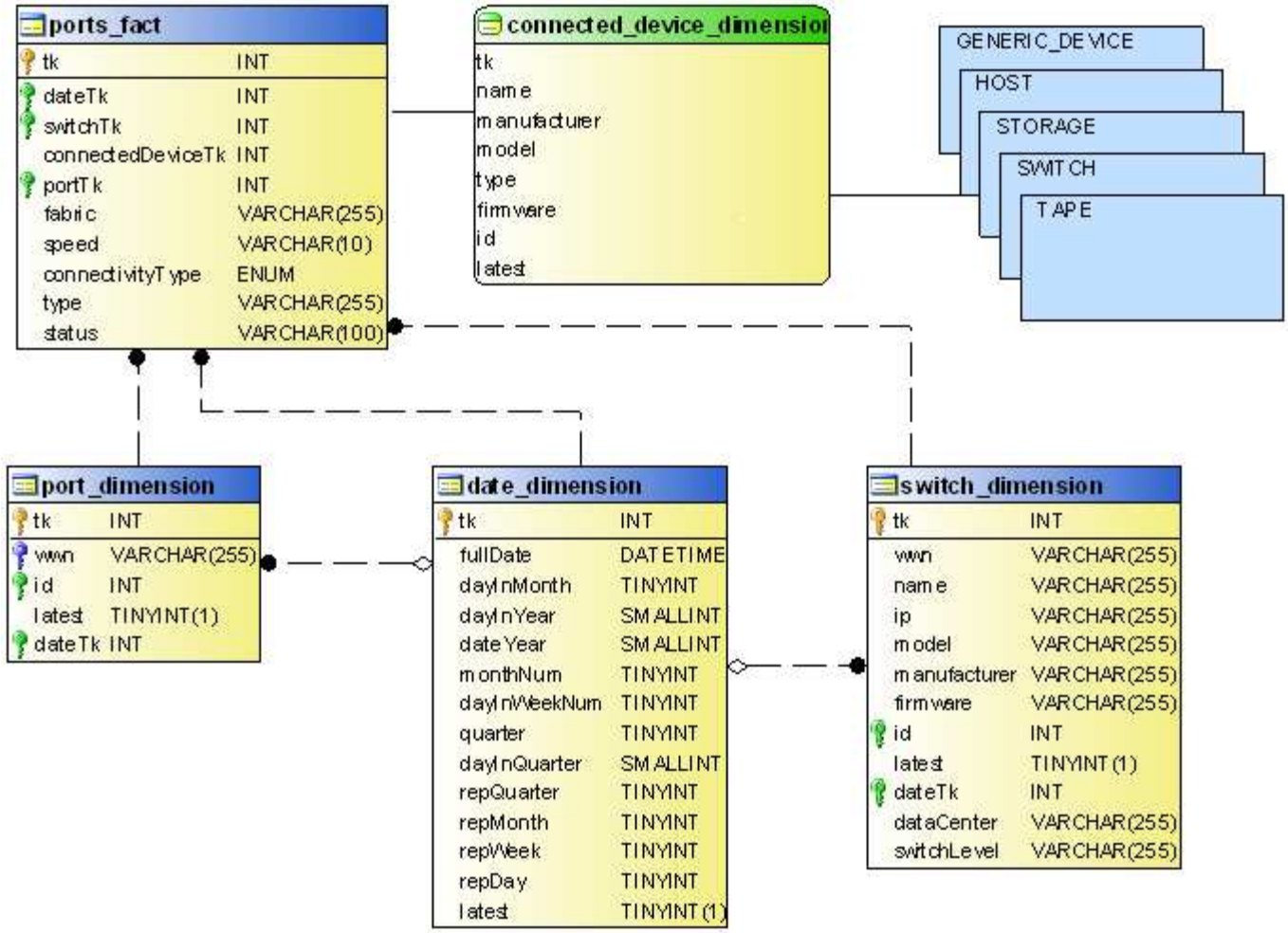
内部容積容量



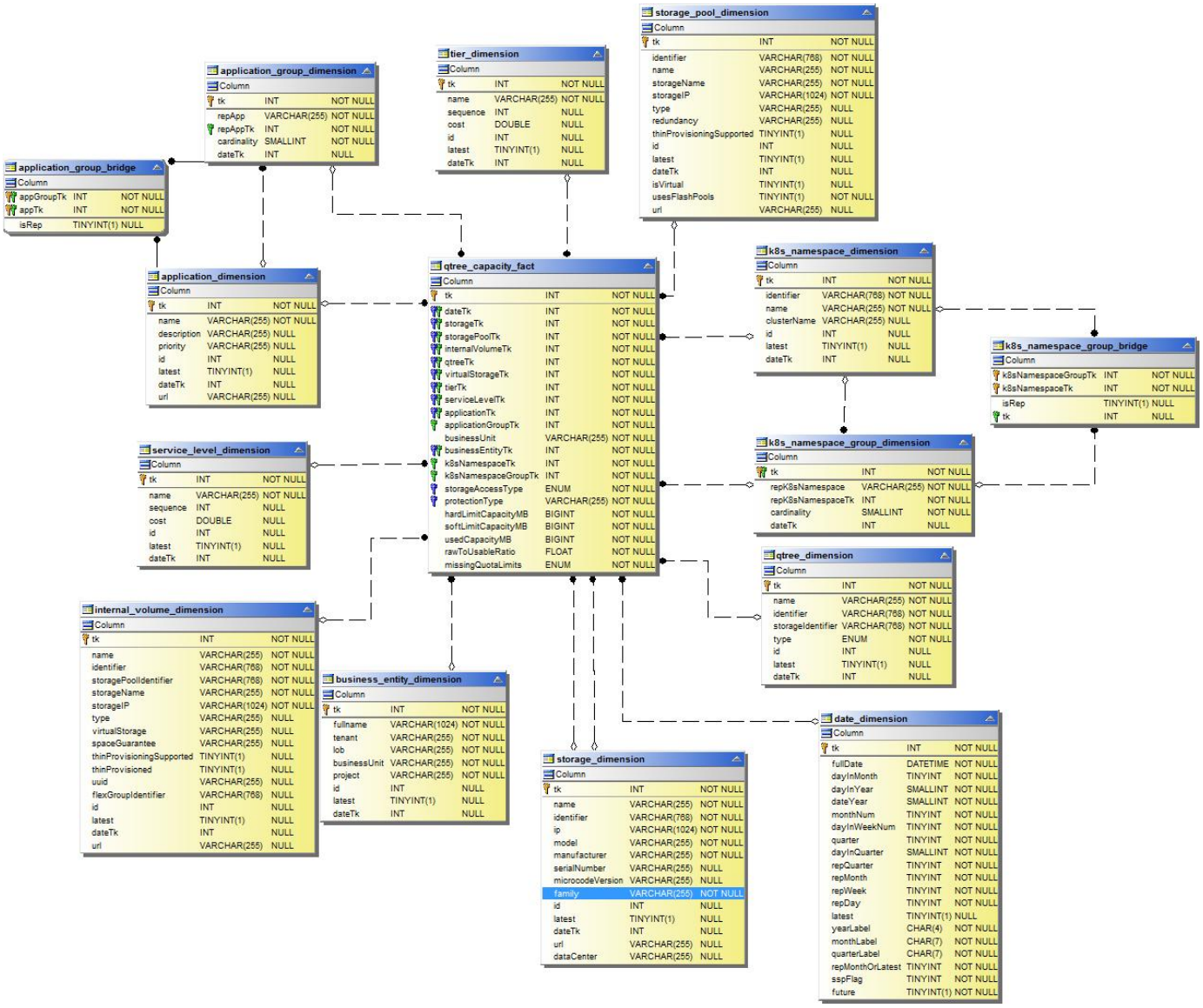
Kubernetes PV 容量


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

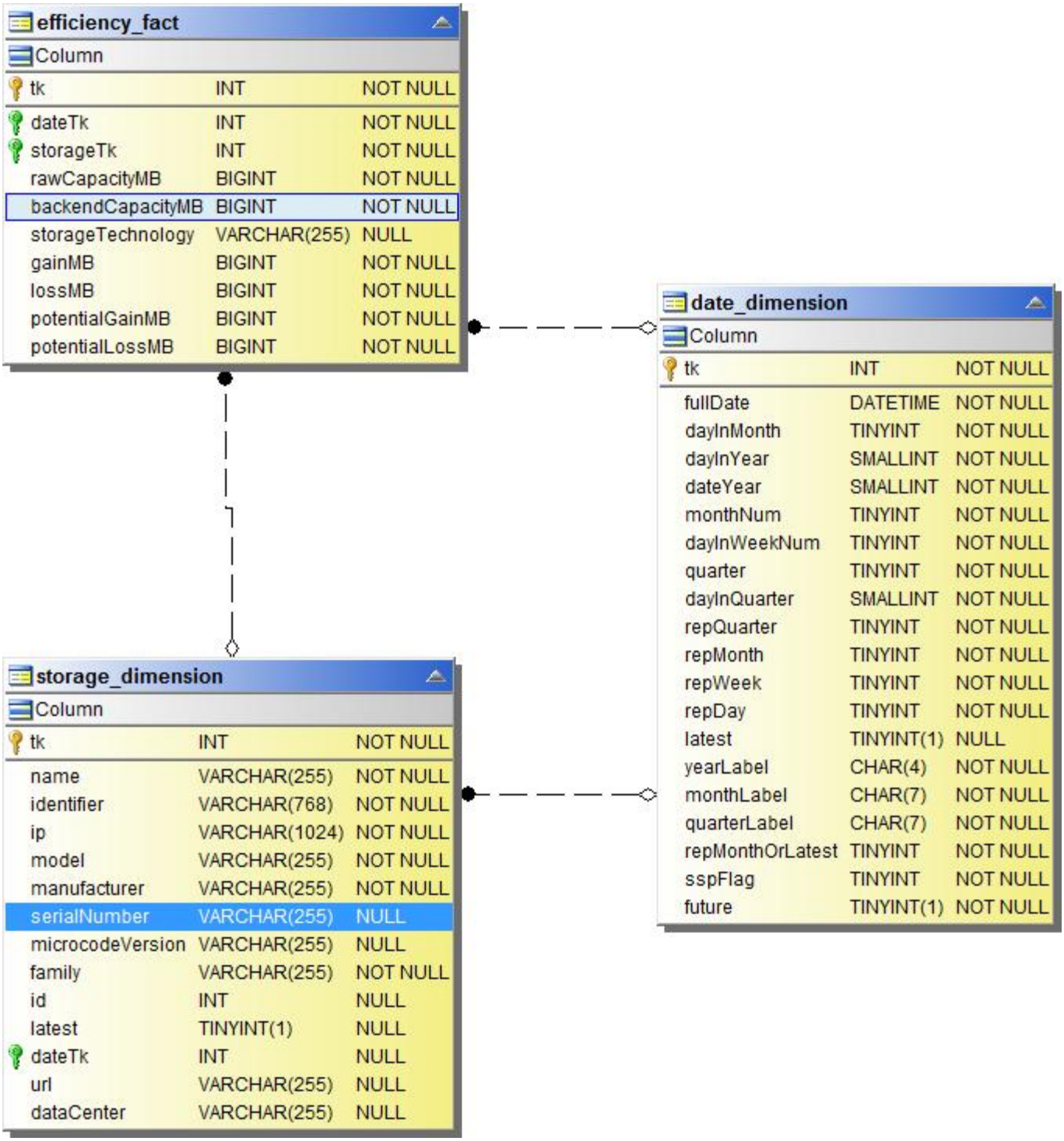
ポート容量


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)

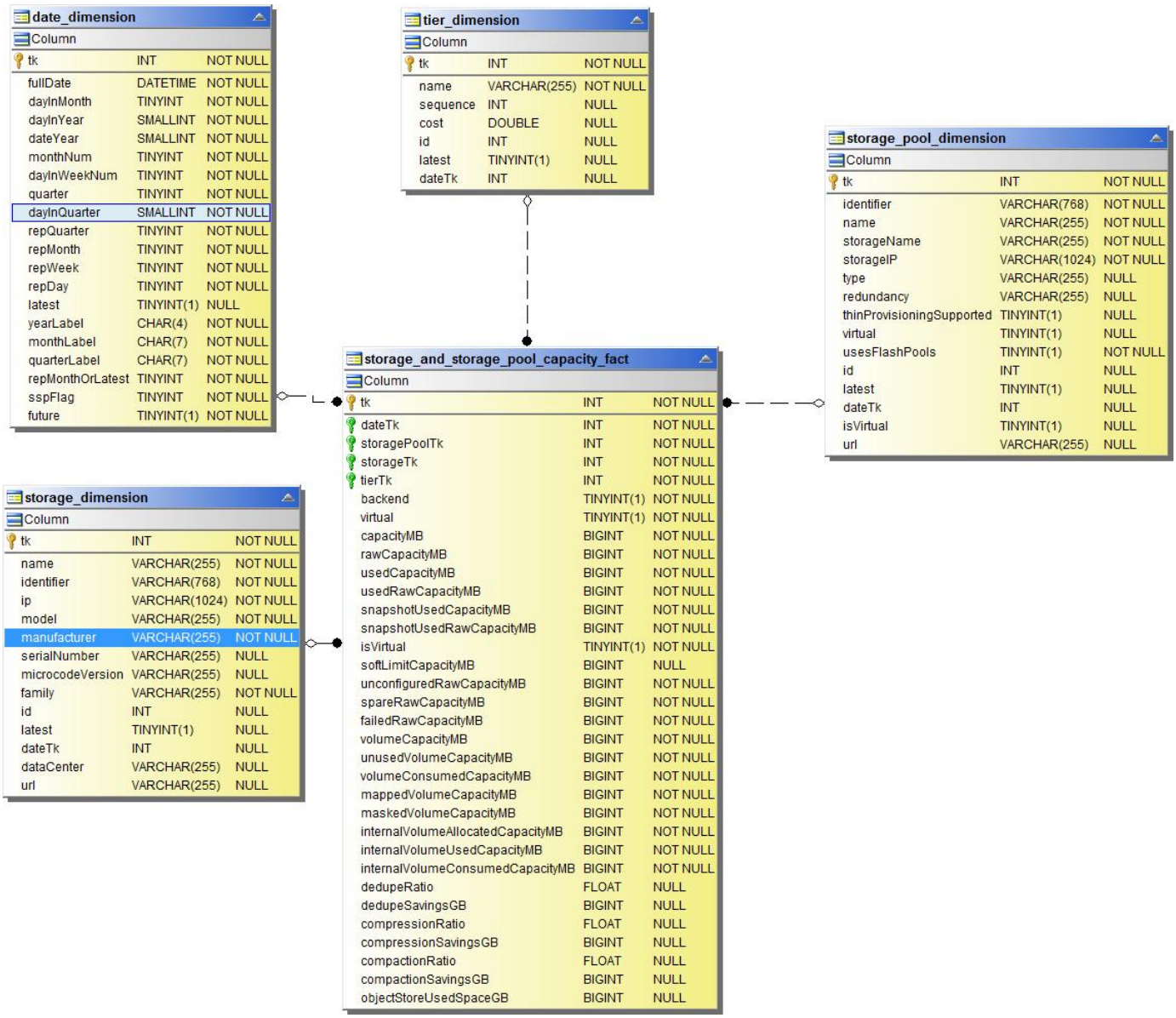
Qtree容量


storage_pool_dimension
Column
tk INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
storageName VARCHAR(255) NOT NULL
storageIP VARCHAR(1024) NOT NULL
type VARCHAR(255) NULL
redundancy VARCHAR(255) NULL
thinProvisioningSupported TINYINT(1) NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
isVirtual TINYINT(1) NULL
usesFlashPools TINYINT(1) NOT 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
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
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
qtree_capacity_fact
Column
tk INT NOT NULL
dateTk INT NOT NULL
storageTk INT NOT NULL
storagePoolTk INT NOT NULL
internalVolumeTk INT NOT NULL
qtreeTk INT NOT NULL
virtualStorageTk INT NOT NULL
tierTk INT NOT NULL
serviceLevelTk INT NOT NULL
applicationTk INT NOT NULL
applicationGroupTk INT NOT NULL
businessUnit VARCHAR(255) NOT NULL
businessEntityTk INT NOT NULL
k8sNamespaceTk INT NOT NULL
k8sNamespaceGroupTk INT NOT NULL
storageAccessType ENUM NOT NULL
protectionType VARCHAR(255) NOT NULL
hardLimitCapacityMB BIGINT NOT NULL
softLimitCapacityMB BIGINT NOT NULL
usedCapacityMB BIGINT NOT NULL
rawToUsableRatio FLOAT NOT NULL
missingQuotaLimits ENUM NOT NULL
k8s_namespace_dimension
Column
tk INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
clusterName VARCHAR(255) NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
k8s_namespace_group_bridge
Column
k8sNamespaceGroupTk INT NOT NULL
k8sNamespaceTk INT NOT NULL
isRep TINYINT(1) NULL
tk INT NULL
k8s_namespace_group_dimension
Column
tk INT NOT NULL
repK8sNamespace VARCHAR(255) NOT NULL
repK8sNamespaceTk INT NOT NULL
cardinality SMALLINT NOT NULL
dateTk INT 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
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
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(1024) NOT NULL
type VARCHAR(255) NULL
virtualStorage VARCHAR(255) NULL
spaceGuarantee VARCHAR(255) NULL
thinProvisioningSupported TINYINT(1) NULL
thinProvisioned TINYINT(1) NULL
uuid VARCHAR(255) NULL
flexGroupIdentifier VARCHAR(768) 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
storage_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(1024) 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
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

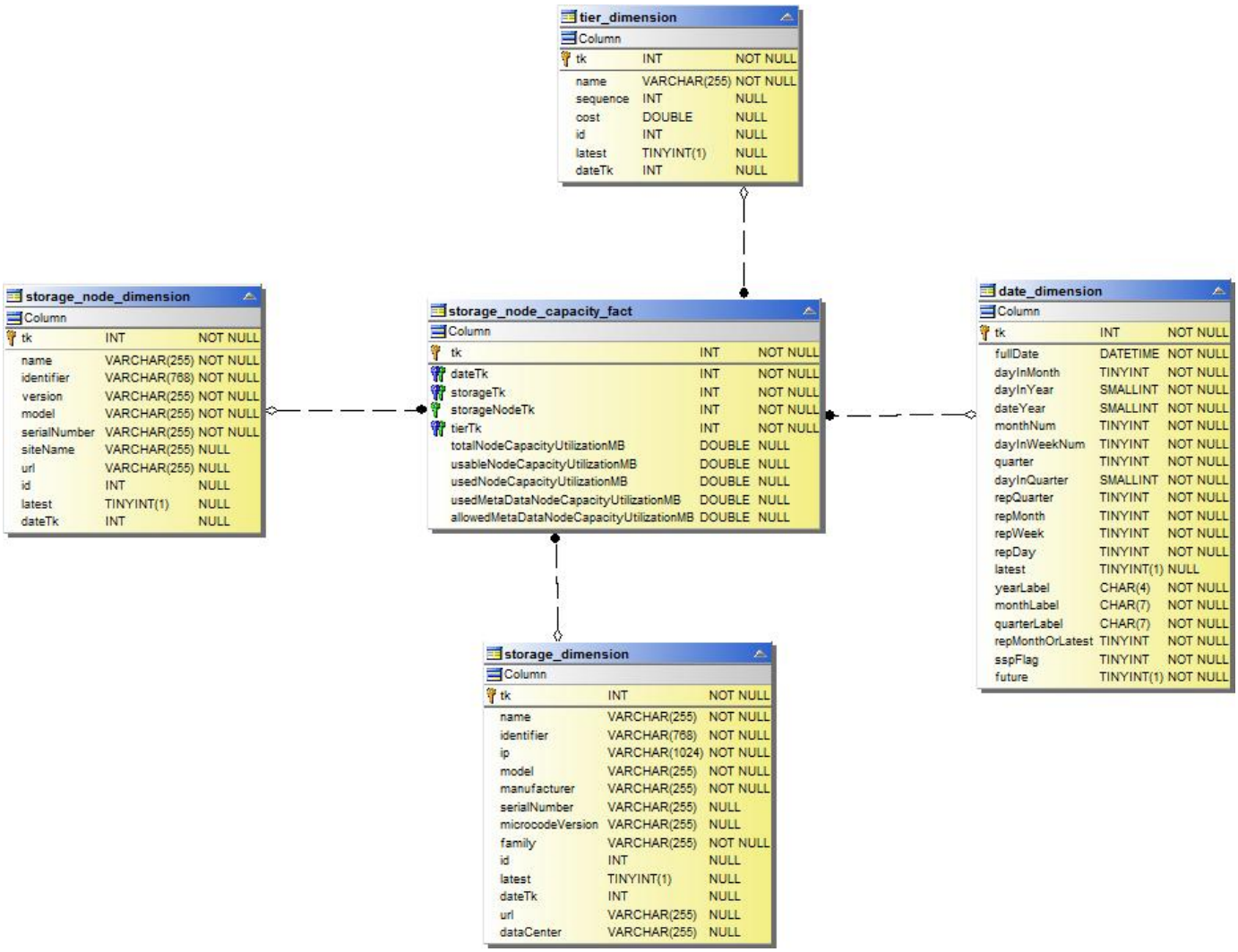
ストレージ容量効率



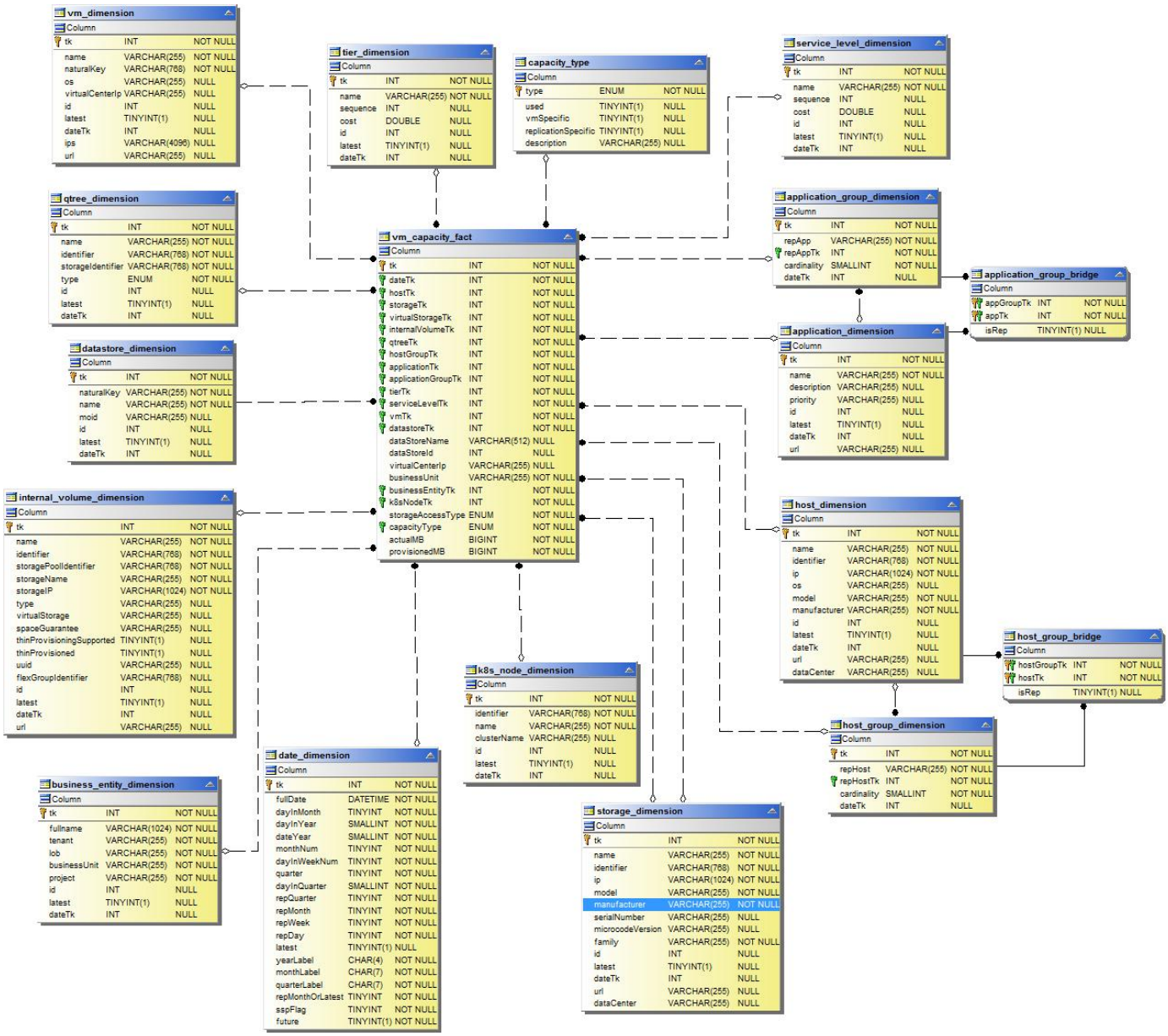
Storage and Storage Pool Capacity


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
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_pool_dimension
Column
tk INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
storageName VARCHAR(255) NOT NULL
storageIP VARCHAR(1024) NOT NULL
type VARCHAR(255) NULL
redundancy VARCHAR(255) NULL
thinProvisioningSupported TINYINT(1) NULL
virtual TINYINT(1) NULL
usesFlashPools TINYINT(1) NOT NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
isVirtual TINYINT(1) NULL
url VARCHAR(255) NULL
storage_and_storage_pool_capacity_fact
Column
tk INT NOT NULL
dateTk INT NOT NULL
storagePoolTk INT NOT NULL
storageTk INT NOT NULL
tierTk INT NOT NULL
backend TINYINT(1) NOT NULL
virtual TINYINT(1) NOT NULL
capacityMB BIGINT NOT NULL
rawCapacityMB BIGINT NOT NULL
usedCapacityMB BIGINT NOT NULL
usedRawCapacityMB BIGINT NOT NULL
snapshotUsedCapacityMB BIGINT NOT NULL
snapshotUsedRawCapacityMB BIGINT NOT NULL
isVirtual TINYINT(1) NOT NULL
softLimitCapacityMB BIGINT NULL
unconfiguredRawCapacityMB BIGINT NOT NULL
spareRawCapacityMB BIGINT NOT NULL
failedRawCapacityMB BIGINT NOT NULL
volumeCapacityMB BIGINT NOT NULL
unusedVolumeCapacityMB BIGINT NOT NULL
volumeConsumedCapacityMB BIGINT NOT NULL
mappedVolumeCapacityMB BIGINT NOT NULL
maskedVolumeCapacityMB BIGINT NOT NULL
internalVolumeAllocatedCapacityMB BIGINT NOT NULL
internalVolumeUsedCapacityMB BIGINT NOT NULL
internalVolumeConsumedCapacityMB BIGINT NOT NULL
dedupeRatio FLOAT NULL
dedupeSavingsGB BIGINT NULL
compressionRatio FLOAT NULL
compressionSavingsGB BIGINT NULL
compactionRatio FLOAT NULL
compactionSavingsGB BIGINT NULL
objectStoreUsedSpaceGB BIGINT NULL
storage_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(1024) 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
dataCenter VARCHAR(255) NULL
url VARCHAR(255) NULL

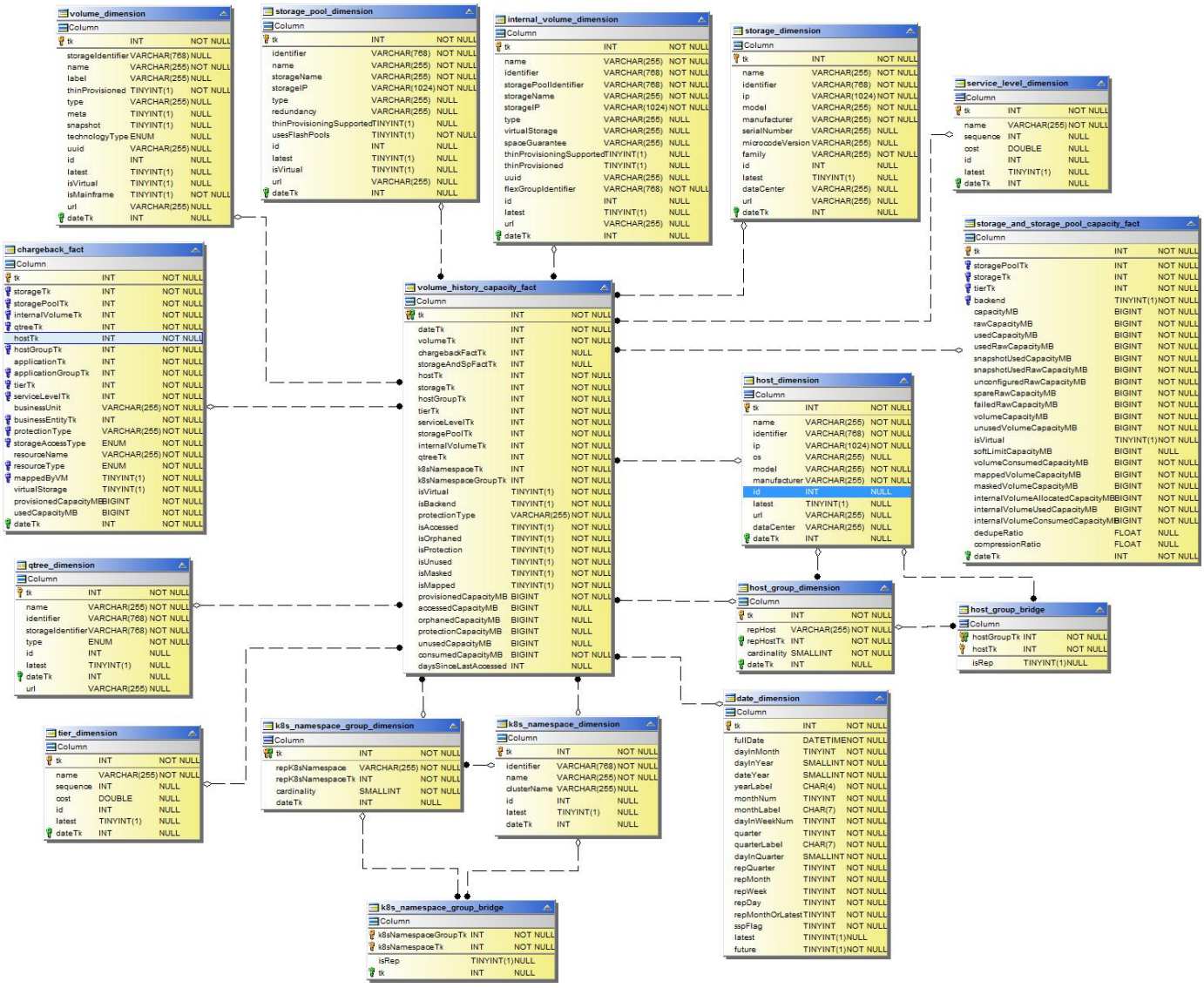
ストレージノード容量


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(1024) 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
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
k8sNodeTk INT NOT NULL
storageAccessType ENUM NOT NULL
capacityType ENUM NOT NULL
actualMB BIGINT NOT NULL
provisionedMB BIGINT NOT 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
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
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
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(1024) NOT NULL
type VARCHAR(255) NULL
virtualStorage VARCHAR(255) NULL
spaceGuarantee VARCHAR(255) NULL
thinProvisioningSupported TINYINT(1) NULL
thinProvisioned TINYINT(1) NULL
uuid VARCHAR(255) NULL
flexGroupIdentifier VARCHAR(768) NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT NULL
url VARCHAR(255) NULL
host_dimension
Column
tk INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(1024) 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
host_group_bridge
Column
hostGroupTk INT NOT NULL
hostTk INT NOT NULL
isRep TINYINT(1) NULL
k8s_node_dimension
Column
tk INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
clusterName VARCHAR(255) NULL
id INT NULL
latest TINYINT(1) NULL
dateTk INT 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
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
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(1024) 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

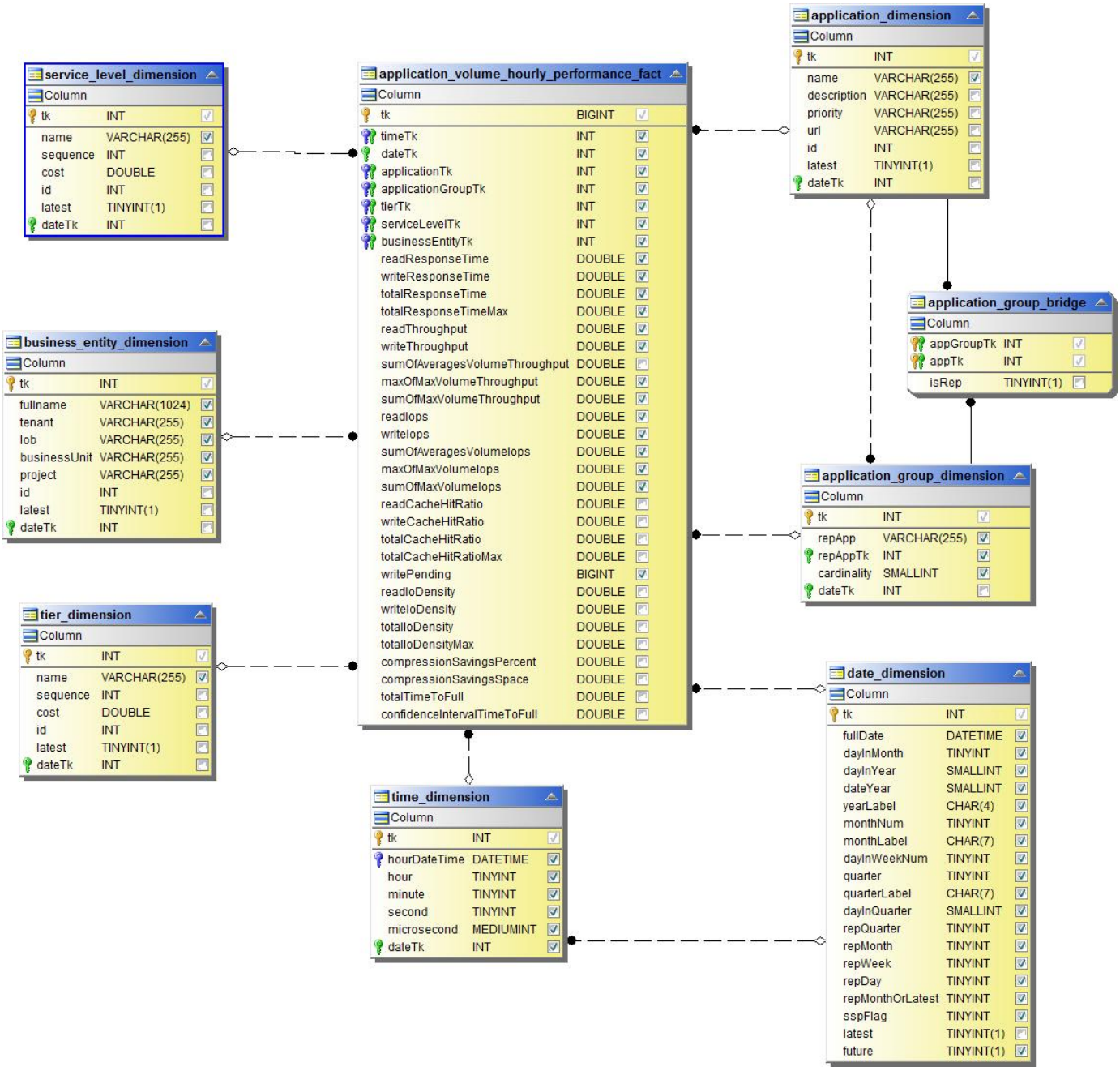
ボリューム容量



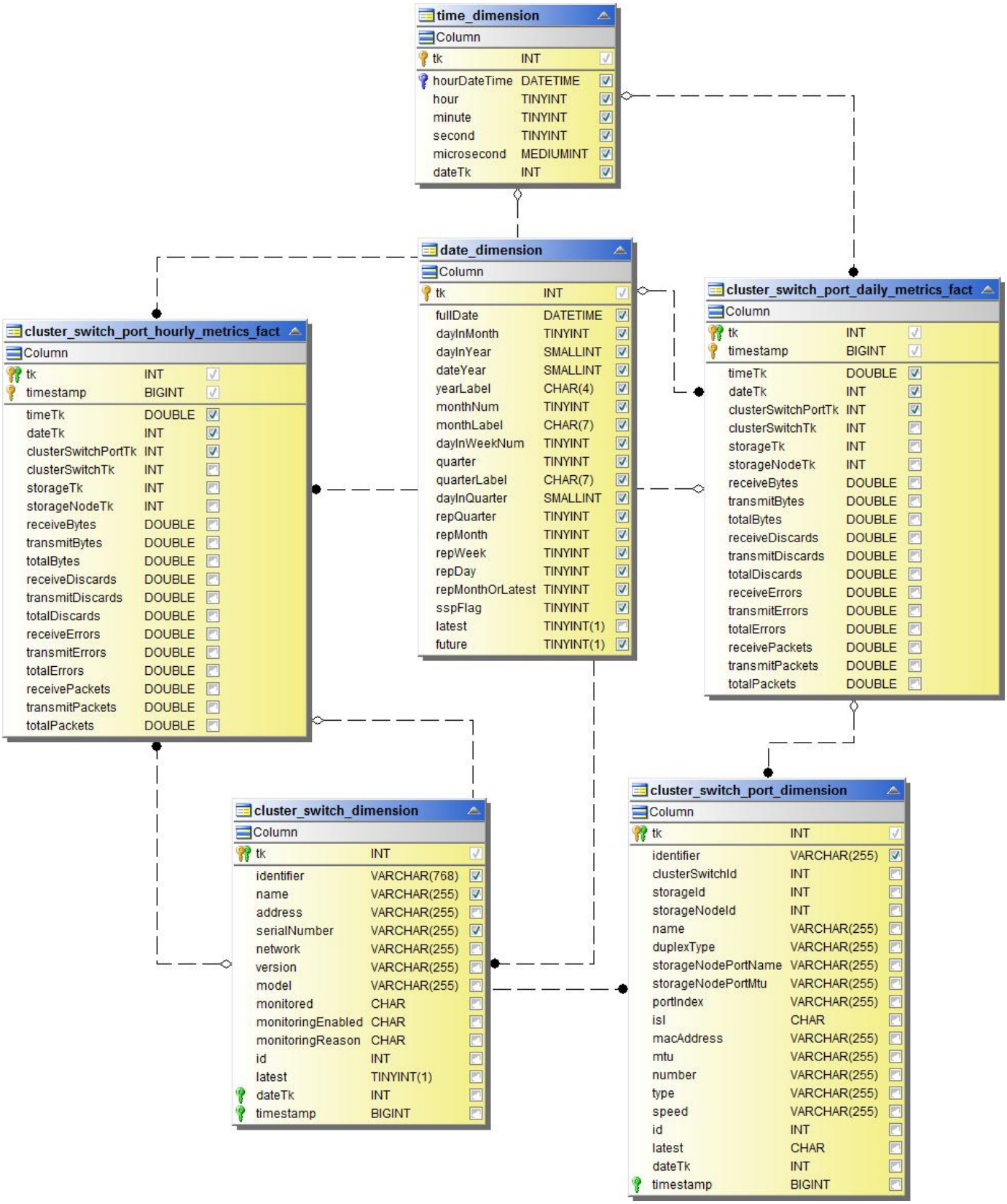
パフォーマンスデータマート

次の画像はパフォーマンス データマートを説明しています。

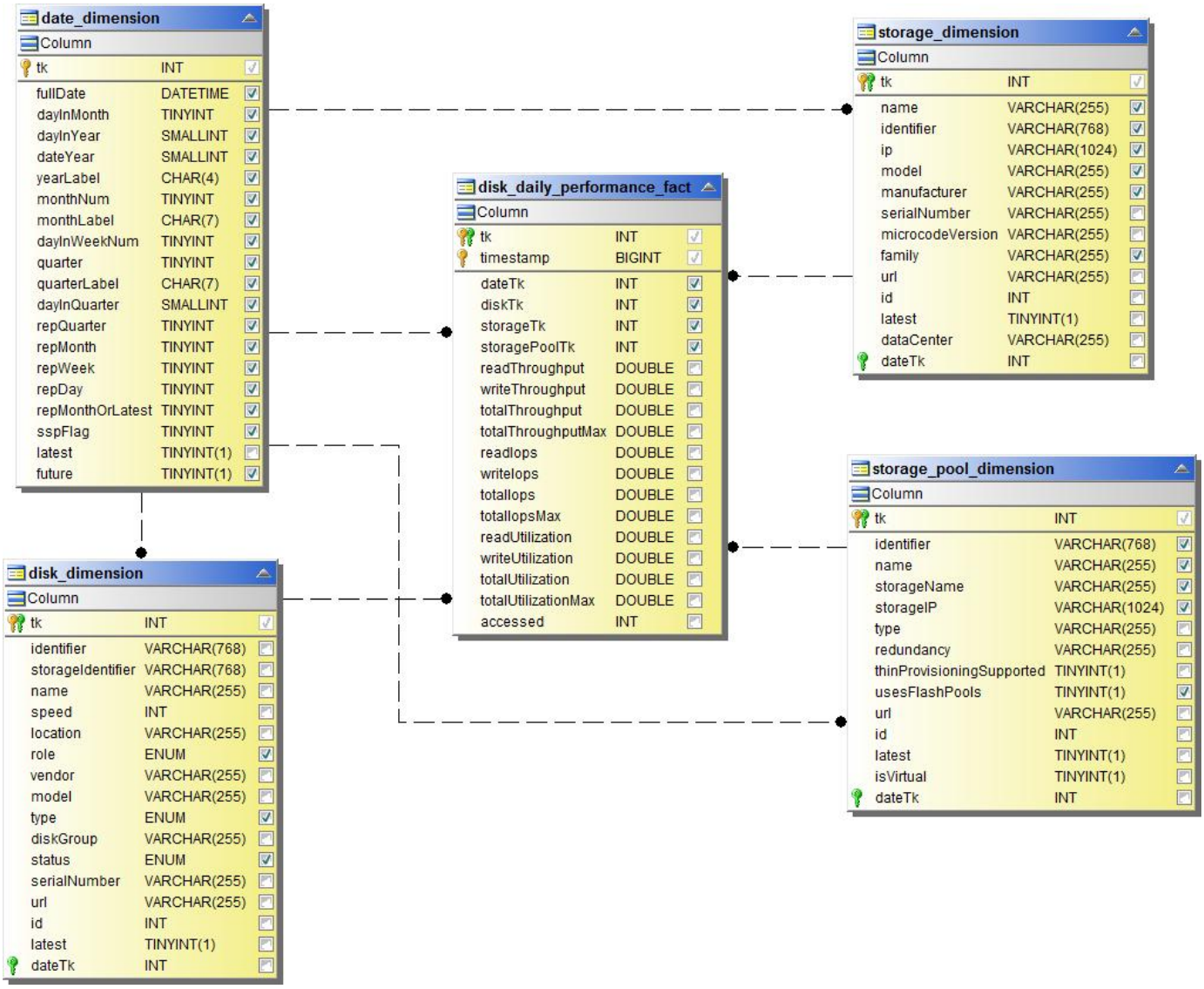
アプリケーションボリュームの時間別パフォーマンス



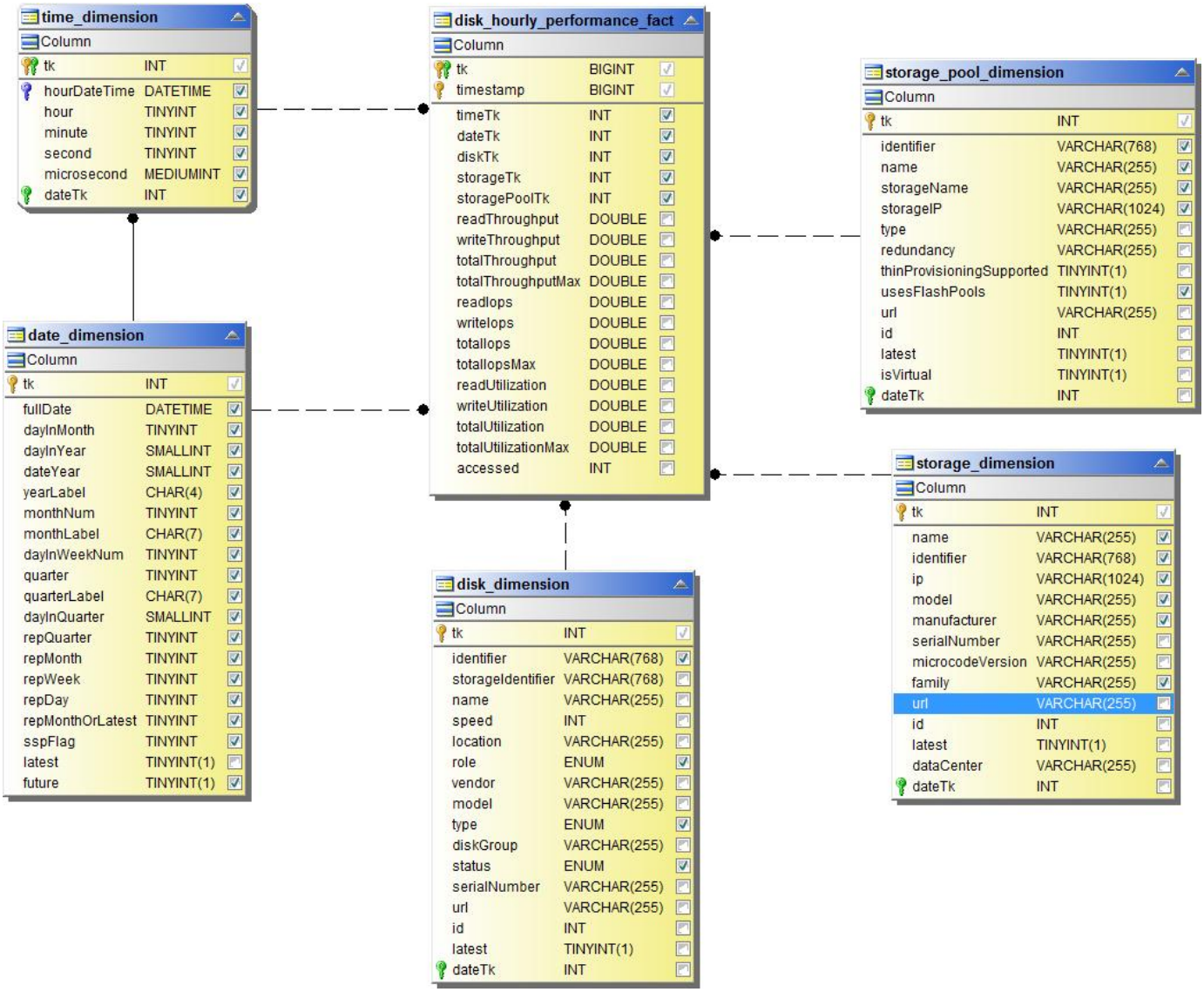
クラスタスイッチのパフォーマンス



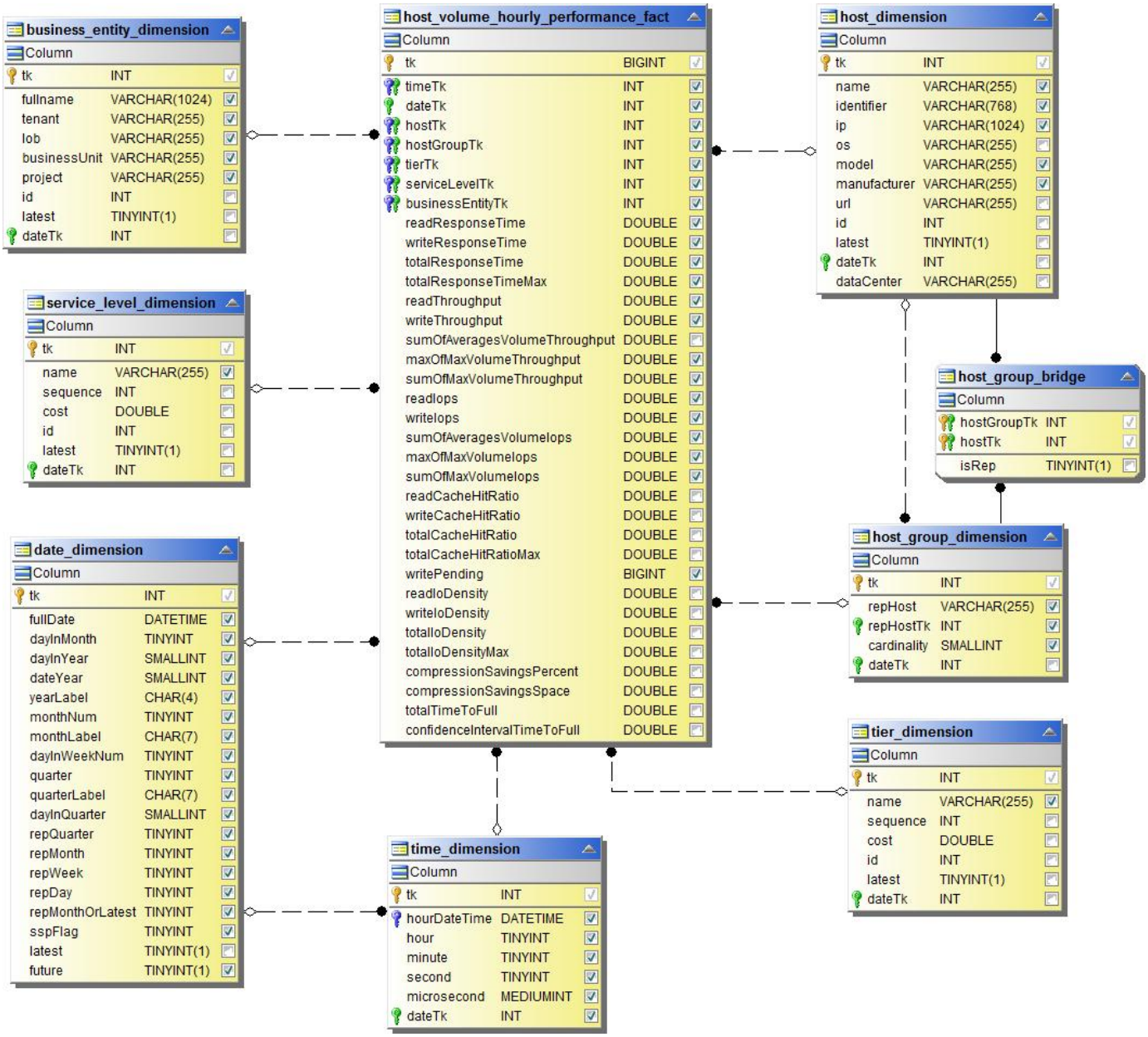
ディスクの**1**日あたりパフォーマンス



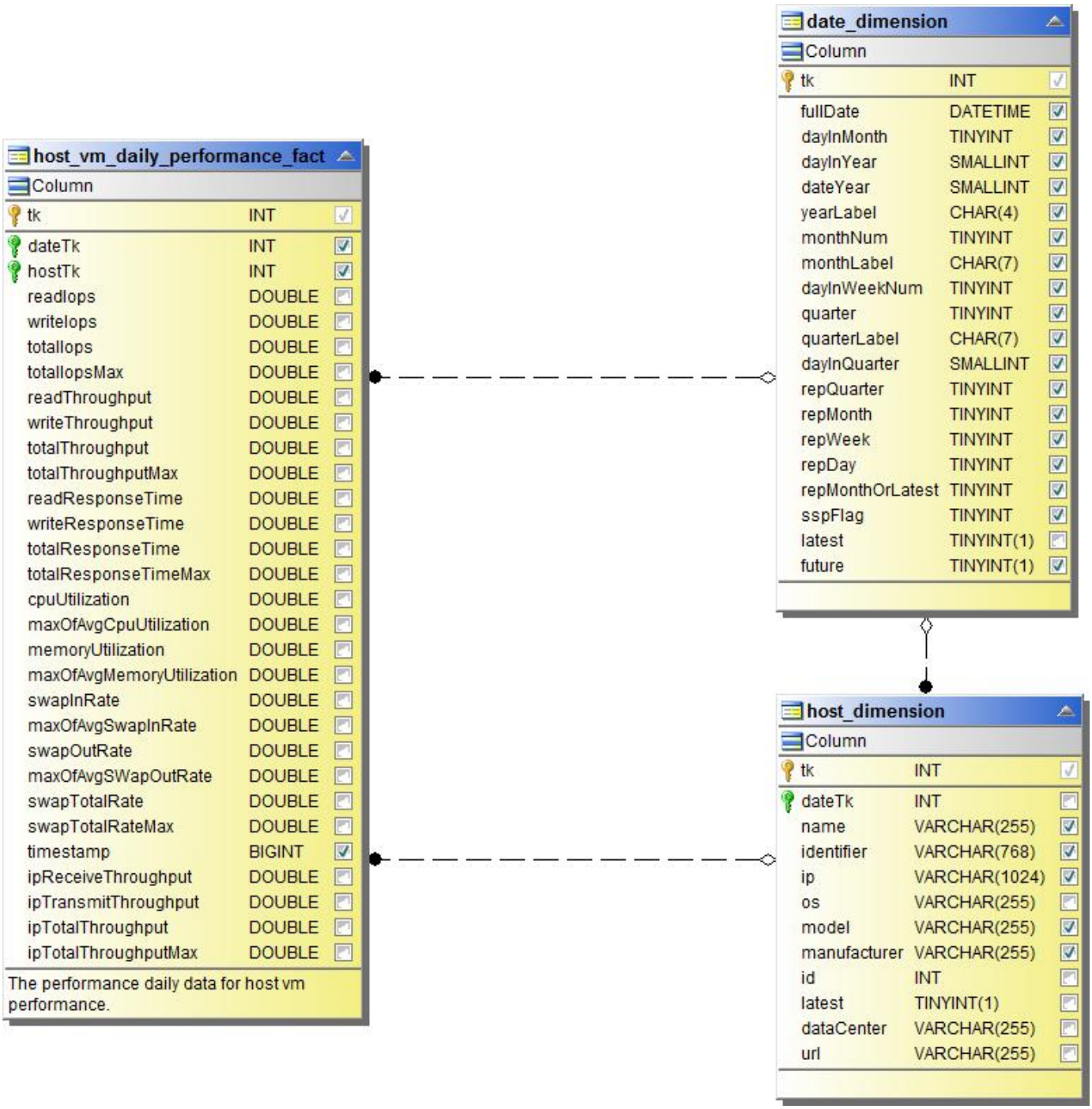
ディスクの時間別パフォーマンス



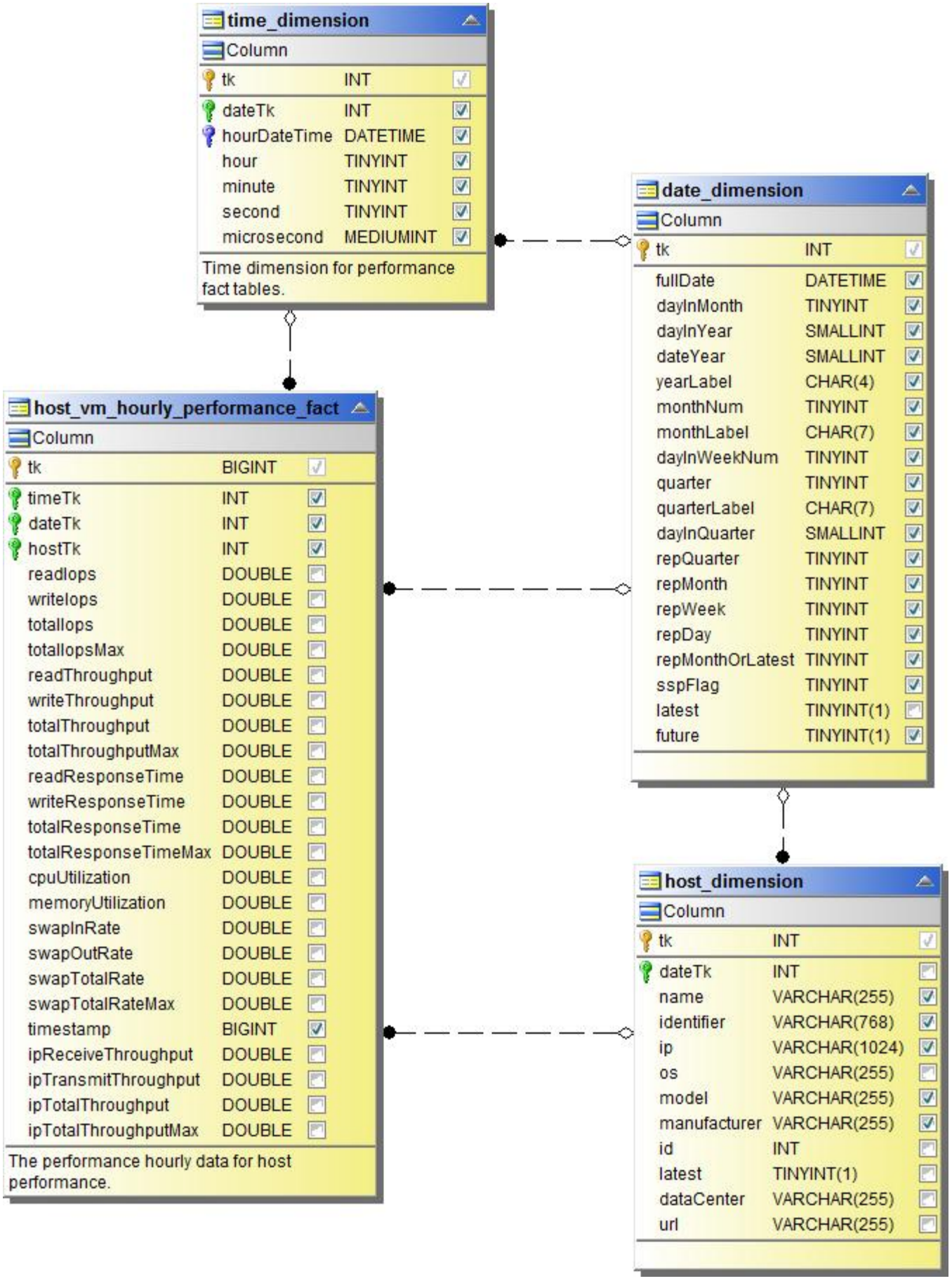
ホストの時間別パフォーマンス



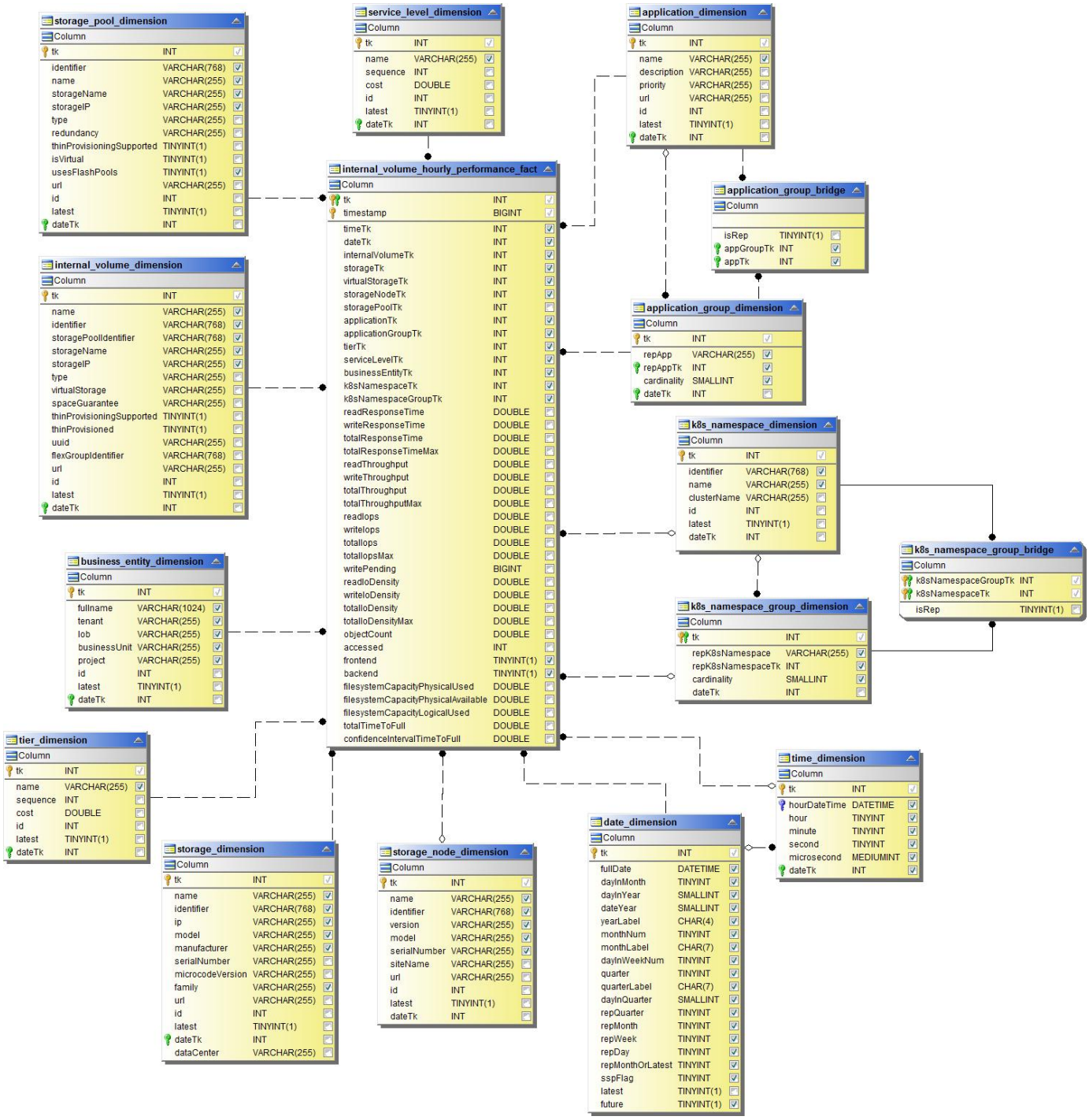
ホスト**VM**の毎日のパフォーマンス



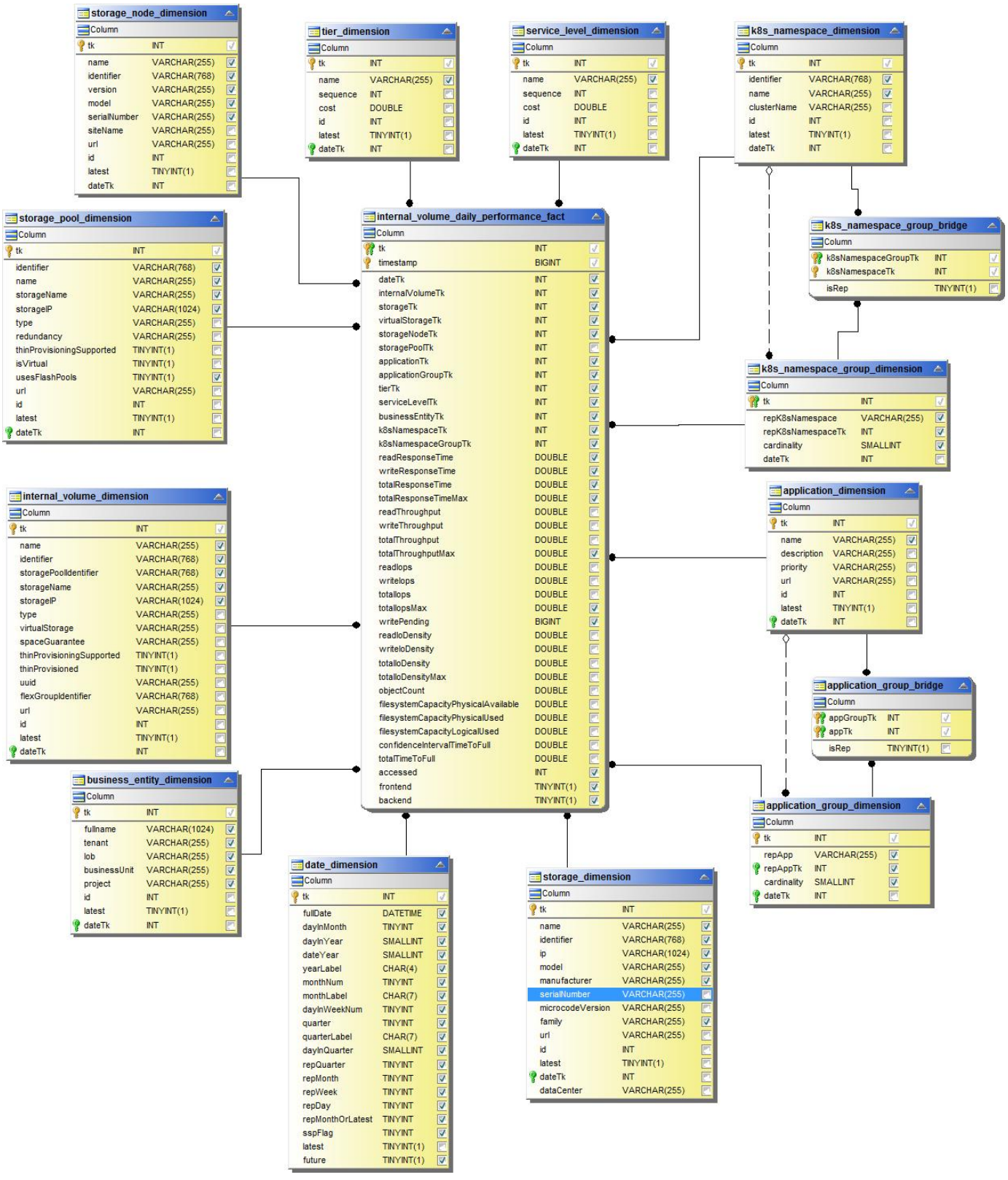
ホスト**VM**の時間別パフォーマンス


time_dimension
Column
tk INT
dateTk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
Time dimension for performance fact tables.
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)
host_vm_hourly_performance_fact
Column
tk BIGINT
timeTk INT
dateTk INT
hostTk INT
readIops DOUBLE
writeIops DOUBLE
totalIops DOUBLE
totalIopsMax DOUBLE
readThroughput DOUBLE
writeThroughput DOUBLE
totalThroughput DOUBLE
totalThroughputMax DOUBLE
readResponseTime DOUBLE
writeResponseTime DOUBLE
totalResponseTime DOUBLE
totalResponseTimeMax DOUBLE
cpuUtilization DOUBLE
memoryUtilization DOUBLE
swapInRate DOUBLE
swapOutRate DOUBLE
swapTotalRate DOUBLE
swapTotalRateMax DOUBLE
timestamp BIGINT
ipReceiveThroughput DOUBLE
ipTransmitThroughput DOUBLE
ipTotalThroughput DOUBLE
ipTotalThroughputMax DOUBLE
The performance hourly data for host performance.
host_dimension
Column
tk INT
dateTk INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
os VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
id INT
latest TINYINT(1)
dataCenter VARCHAR(255)
url VARCHAR(255)

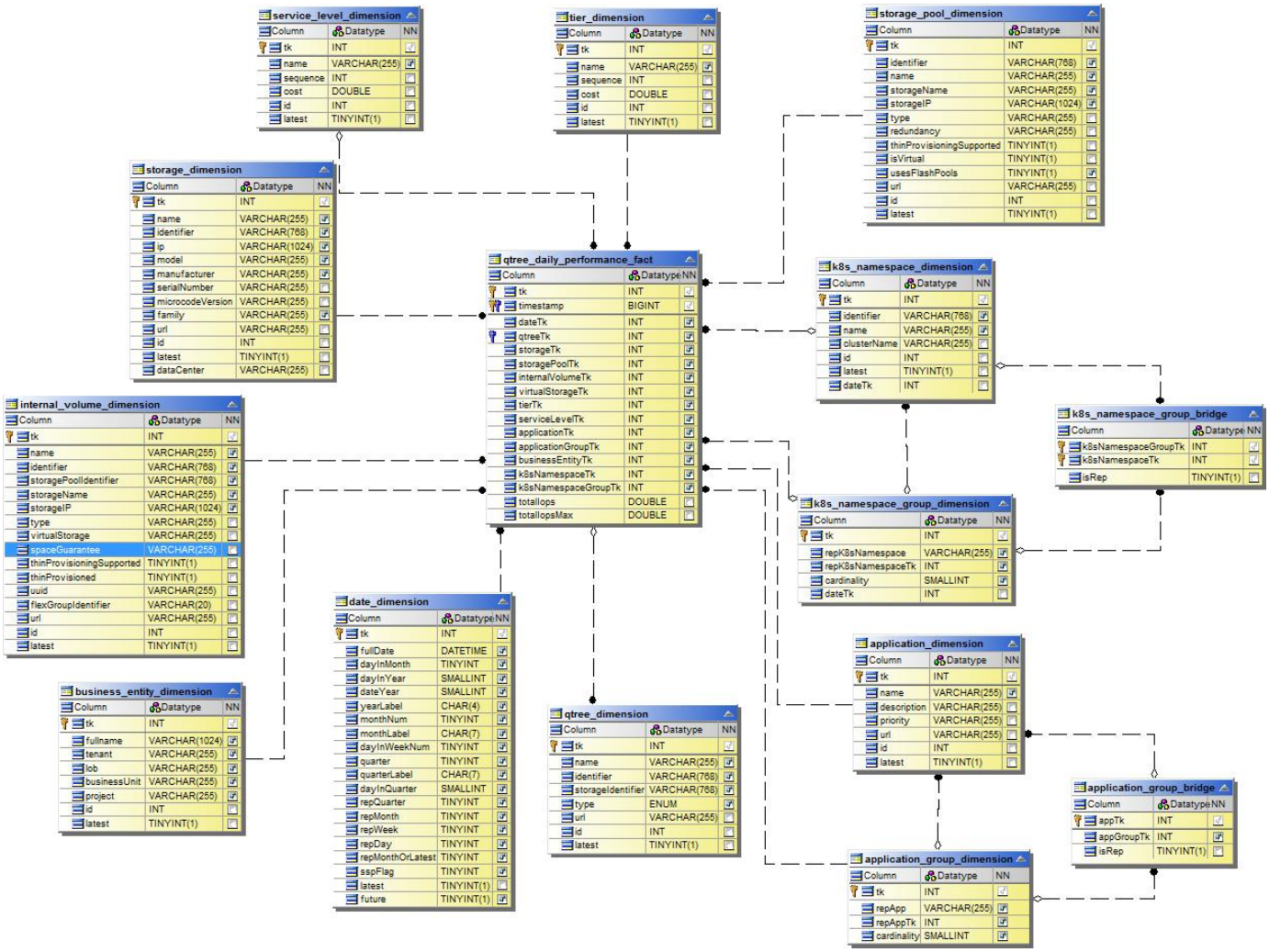
内部容積の**1**時間当たりのパフォーマンス



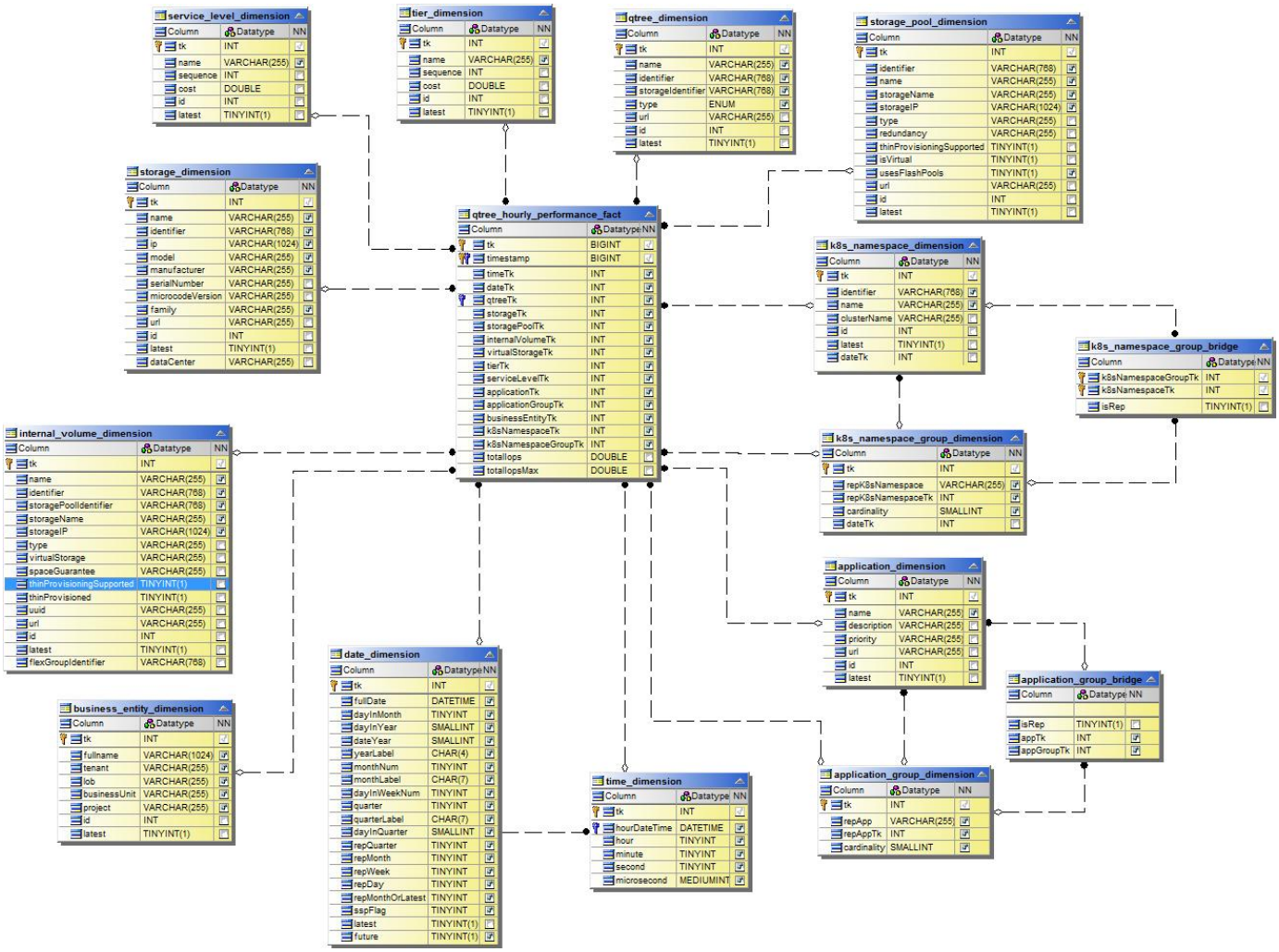
内部ボリュームの日々のパフォーマンス



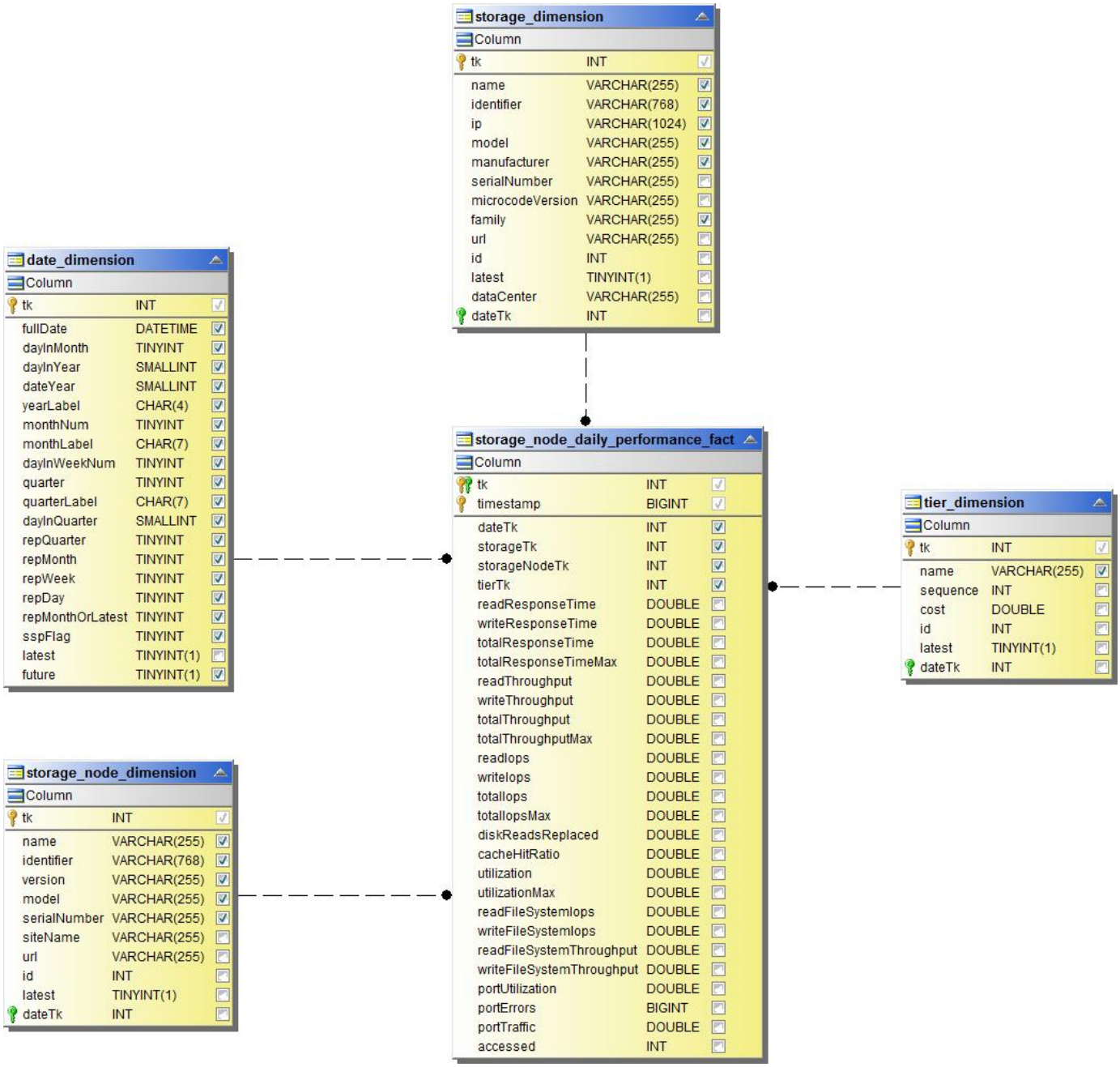
Qtree デイリーパフォーマンス



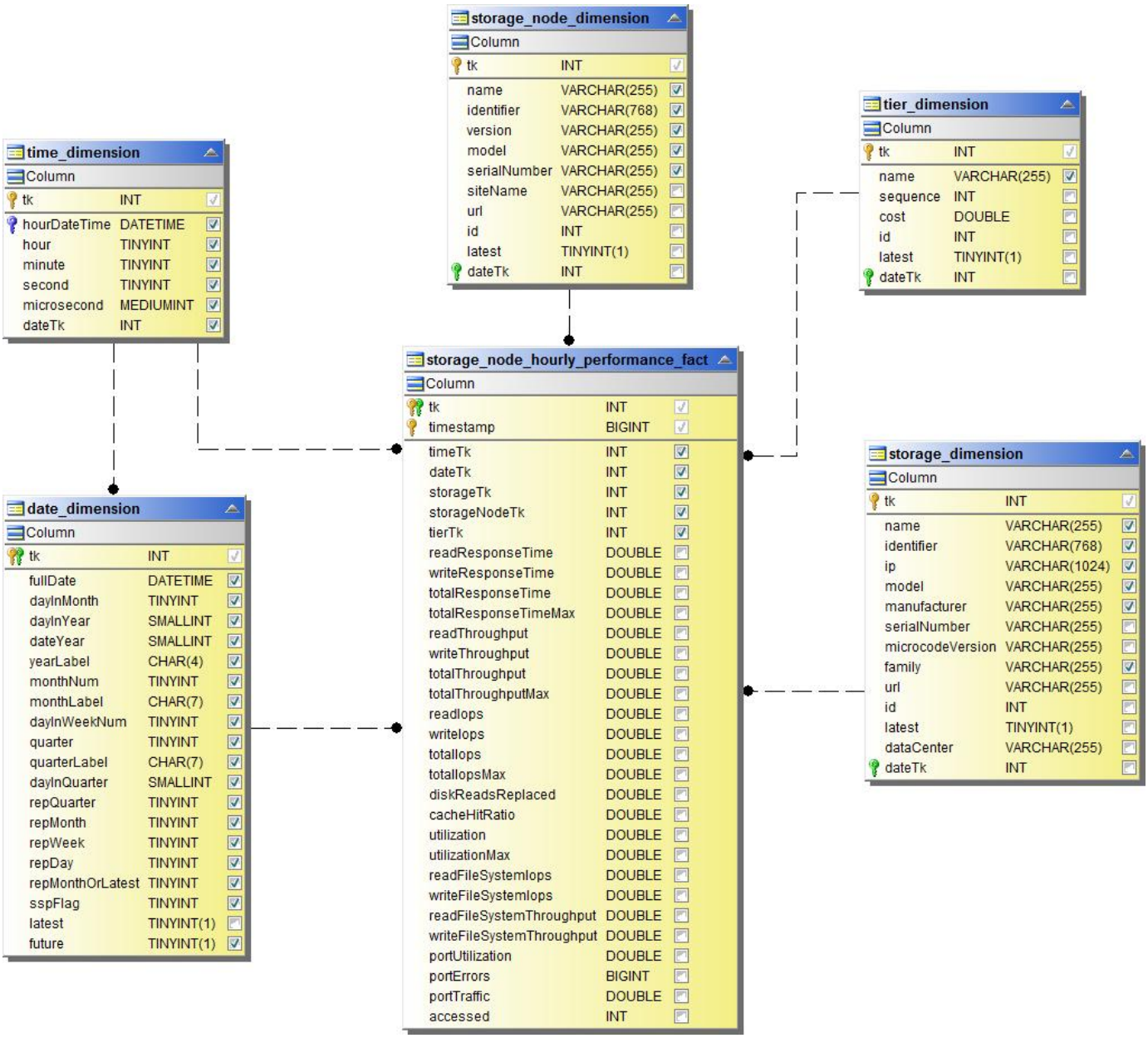
Qtree 時間別パフォーマンス



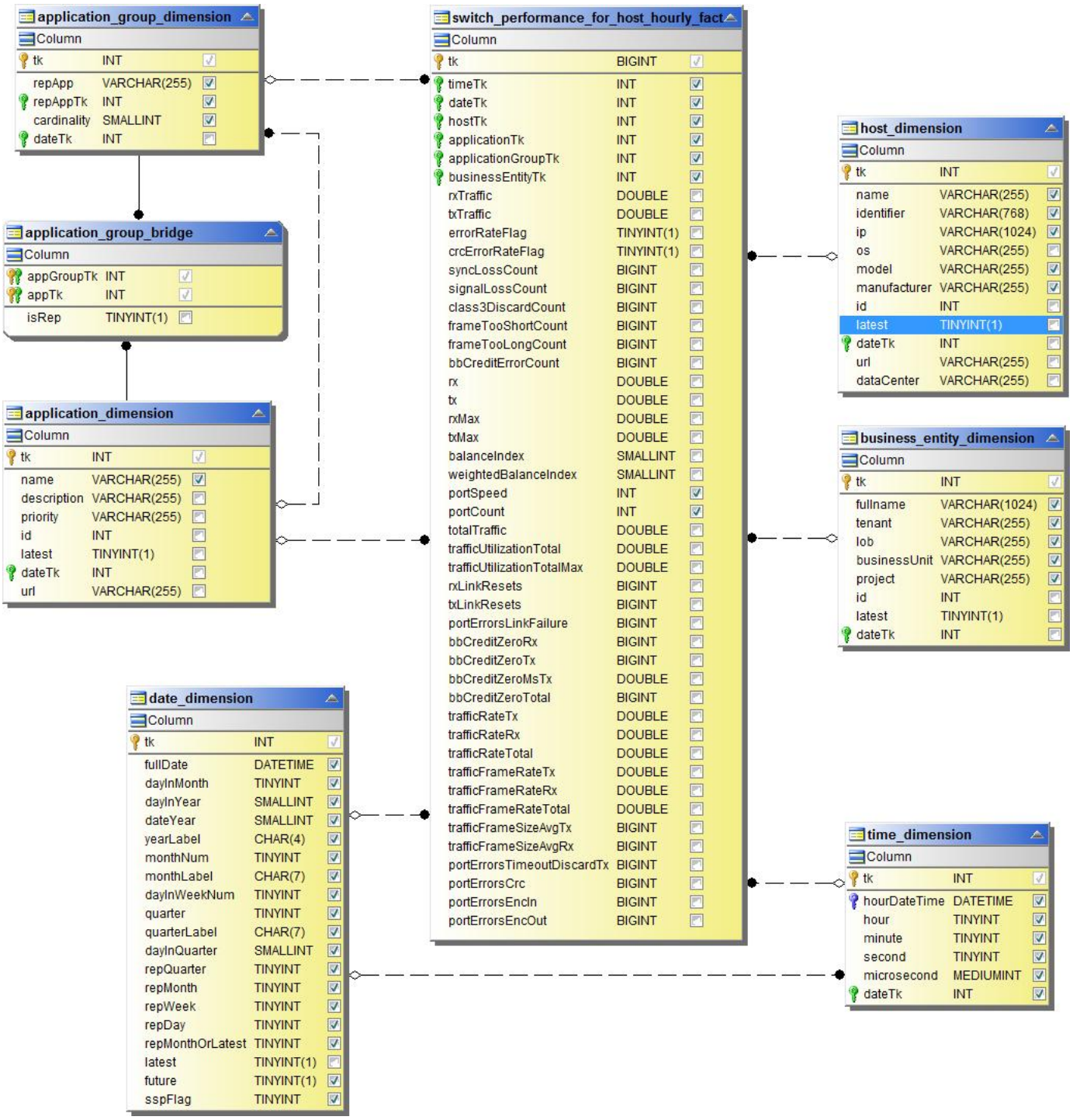
ストレージノードの日々のパフォーマンス



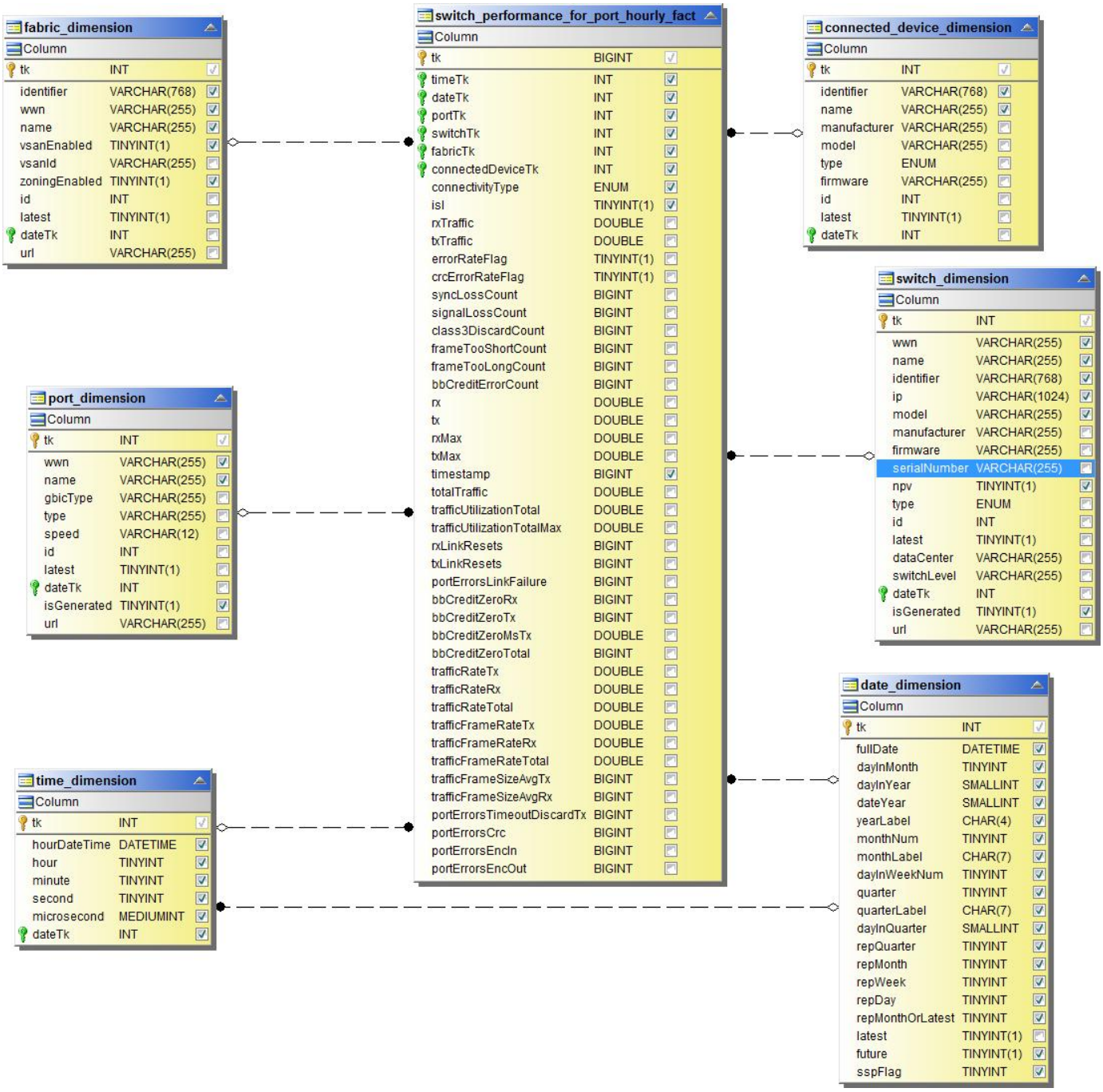
ストレージノードの時間別パフォーマンス



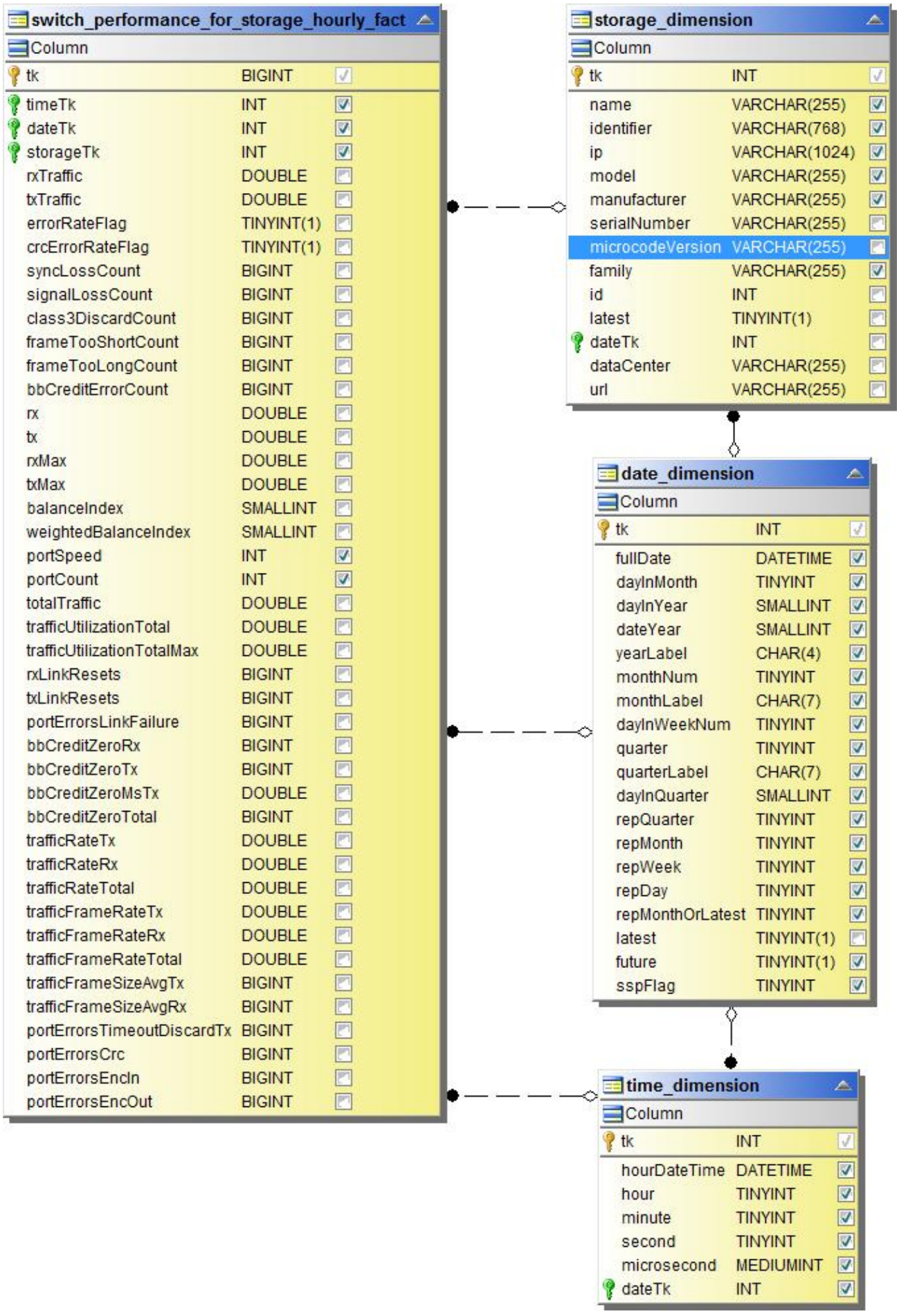
ホストのスイッチ時間別パフォーマンス



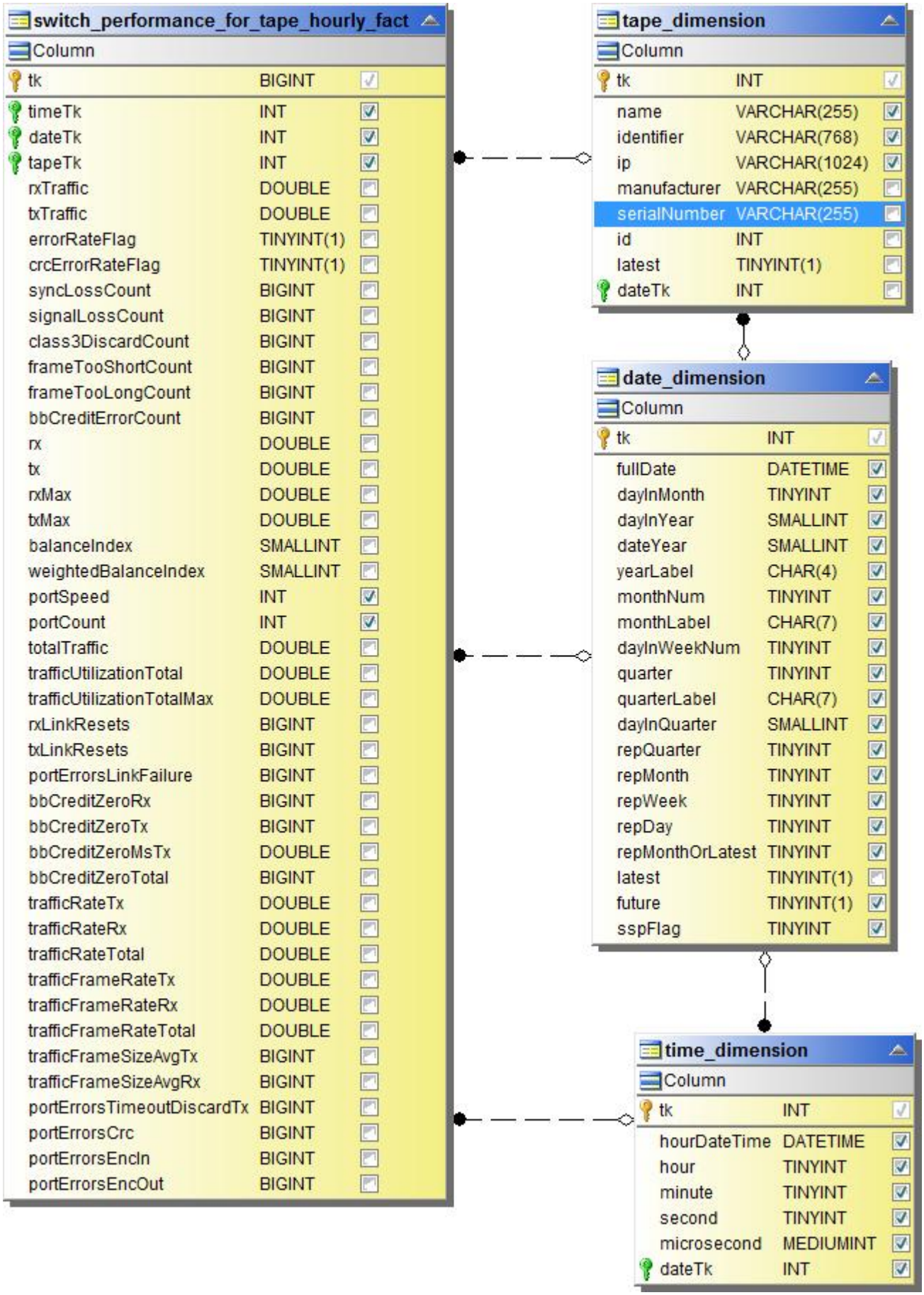
ポートのスイッチ時間別パフォーマンス



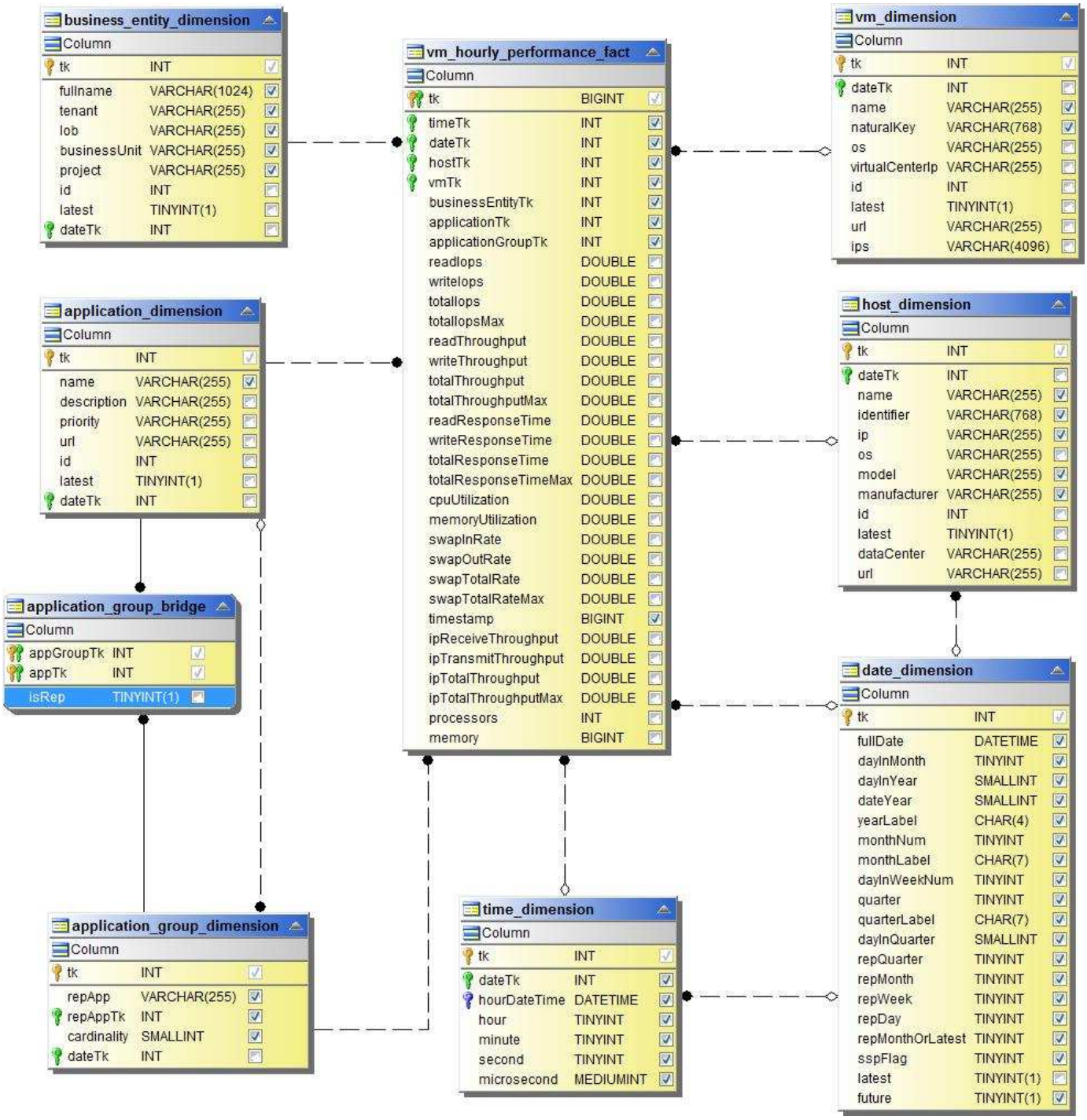
ストレージのスイッチ時間別パフォーマンス


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(1024)
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

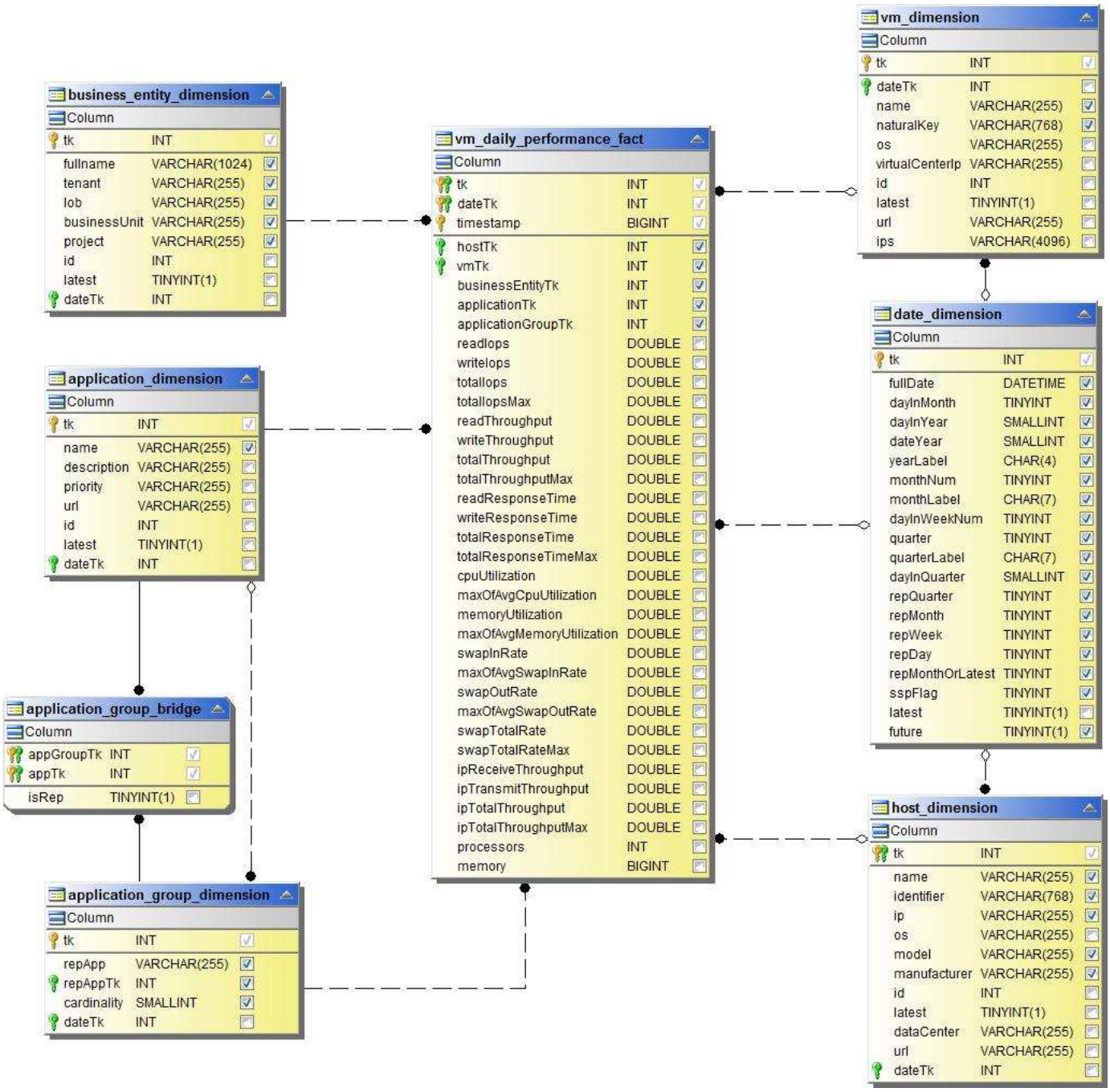
テープのスイッチ時間別パフォーマンス



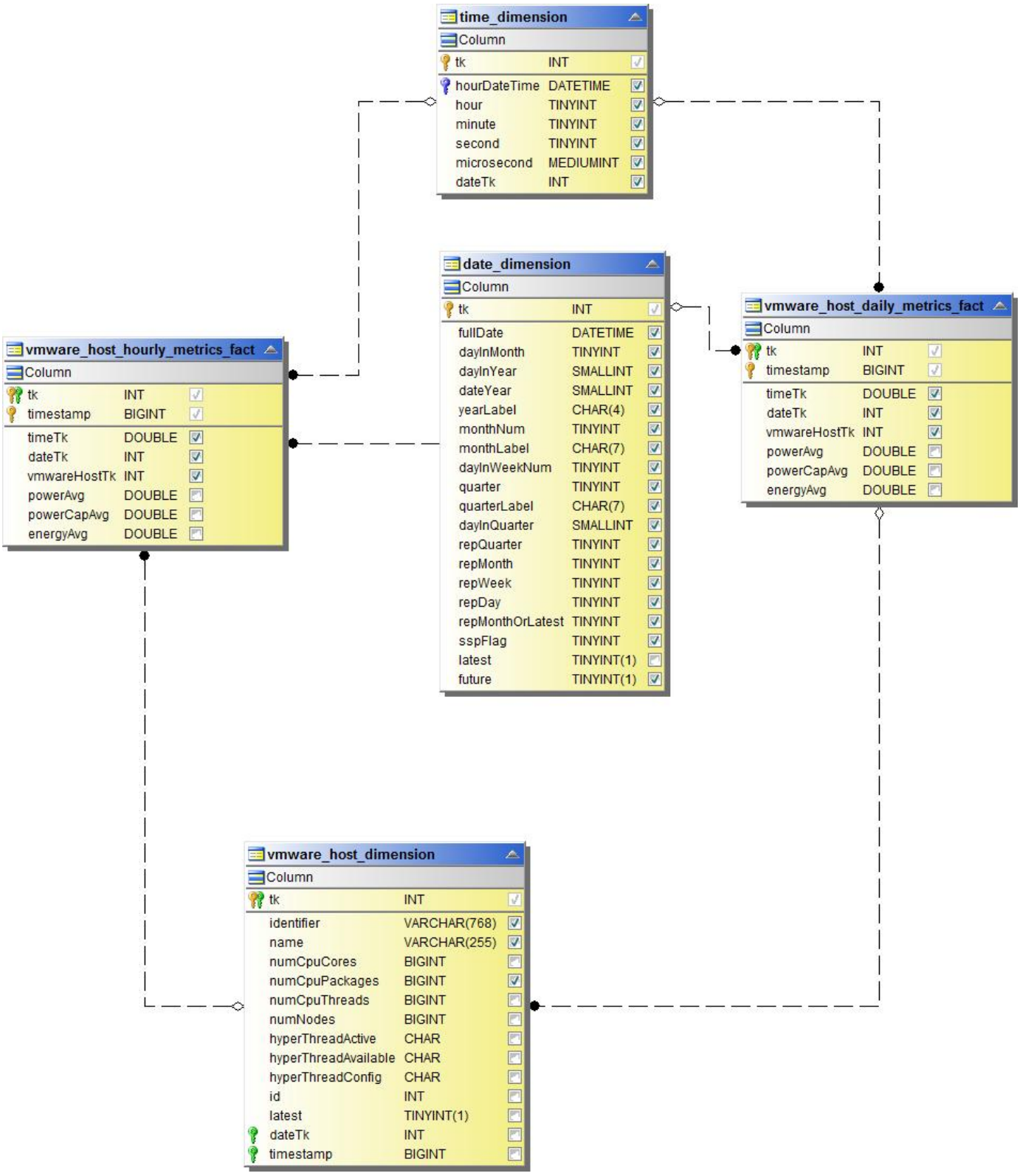
VMパフォーマンス



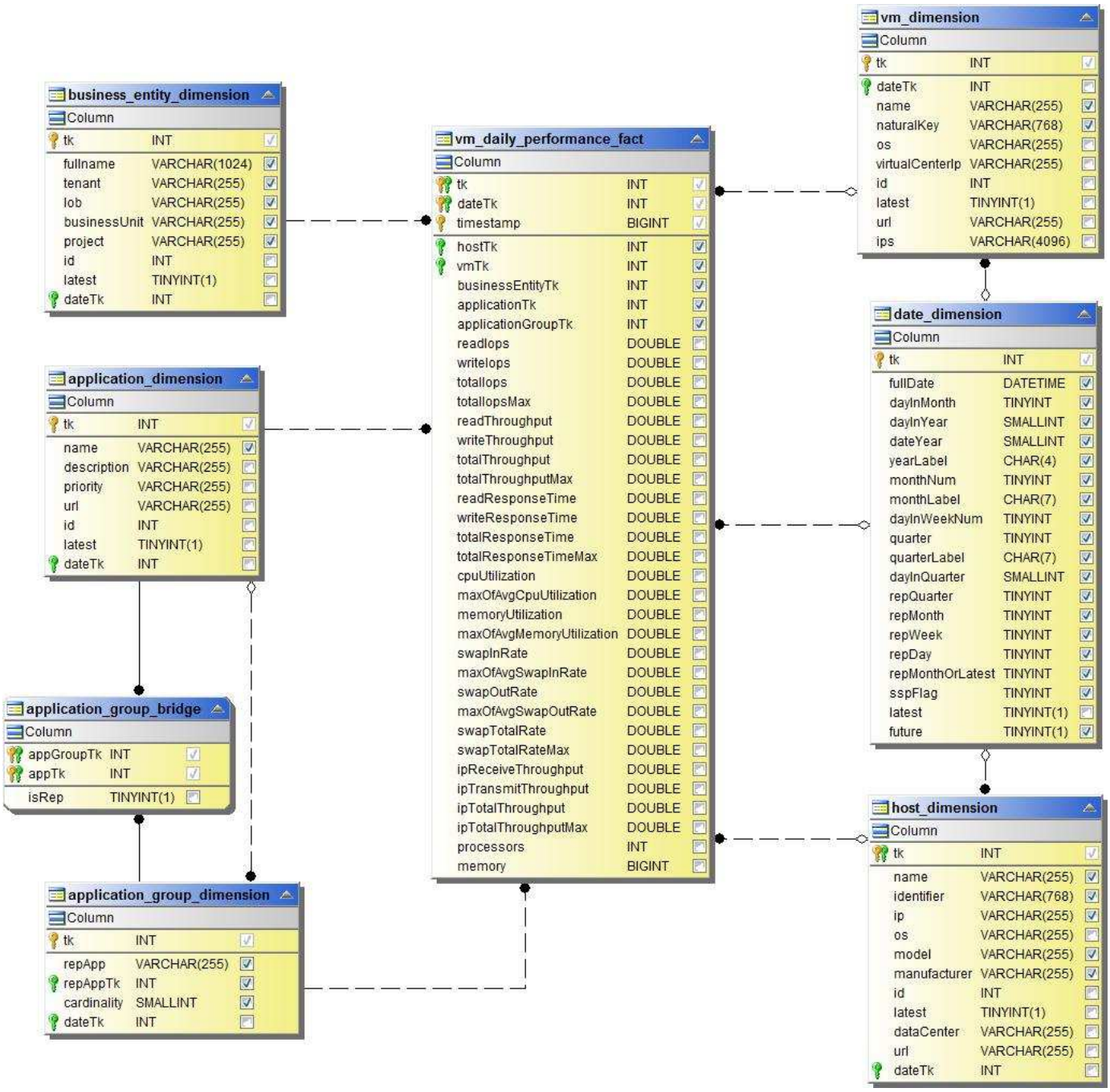
ホストの**VM**日次パフォーマンス



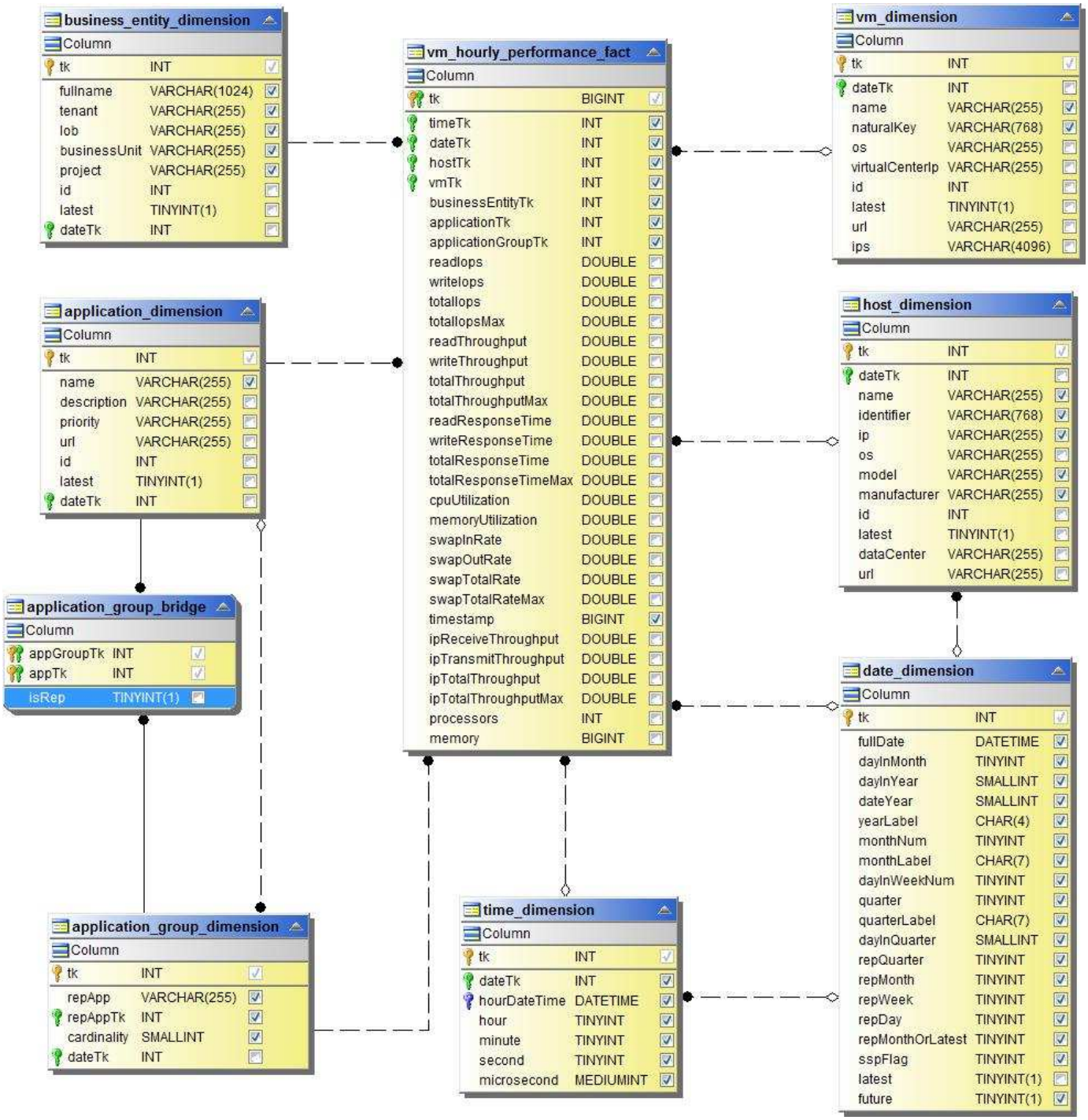
ホストの**VM**時間別パフォーマンス



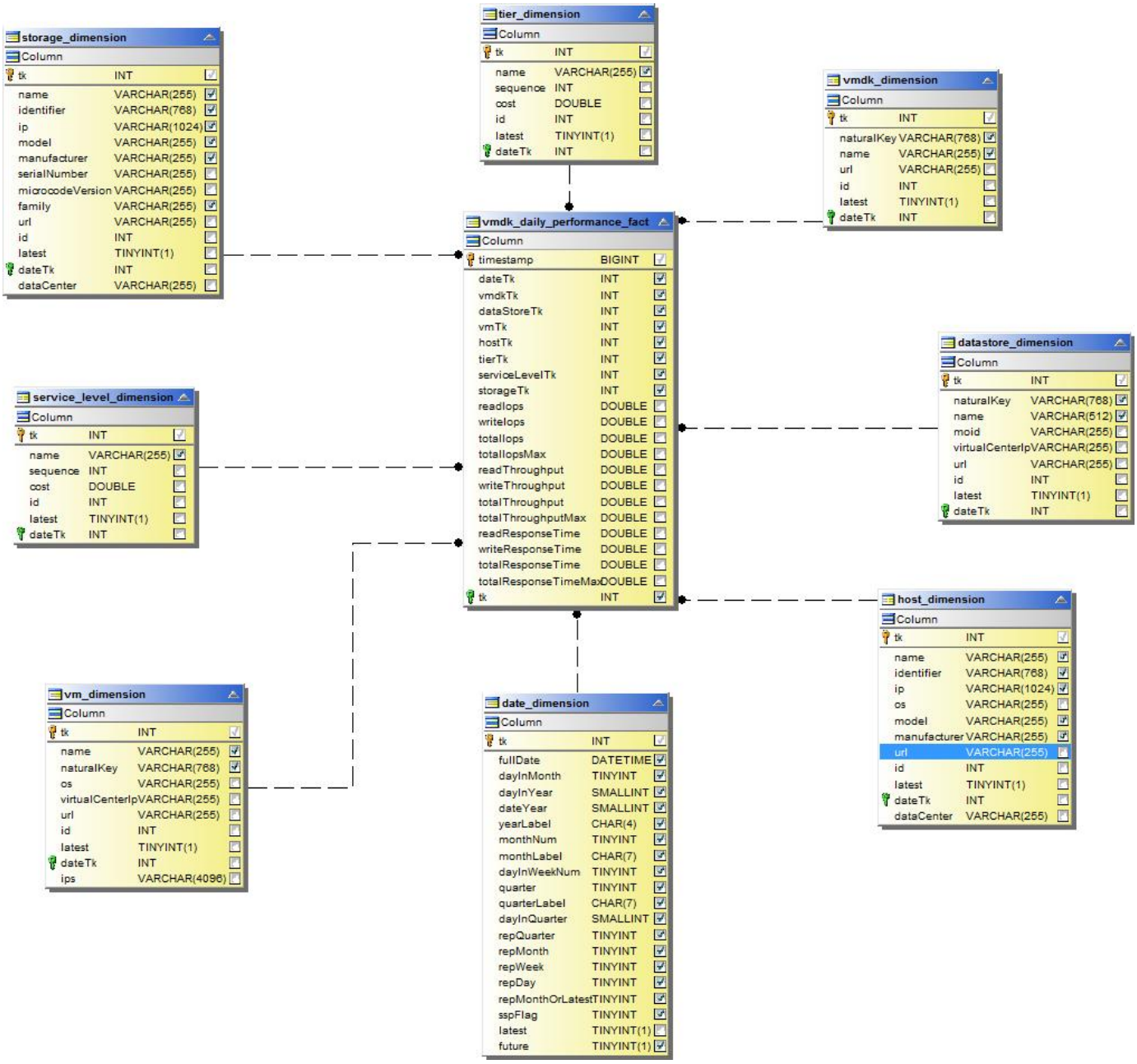
ホストの**VM**日次パフォーマンス



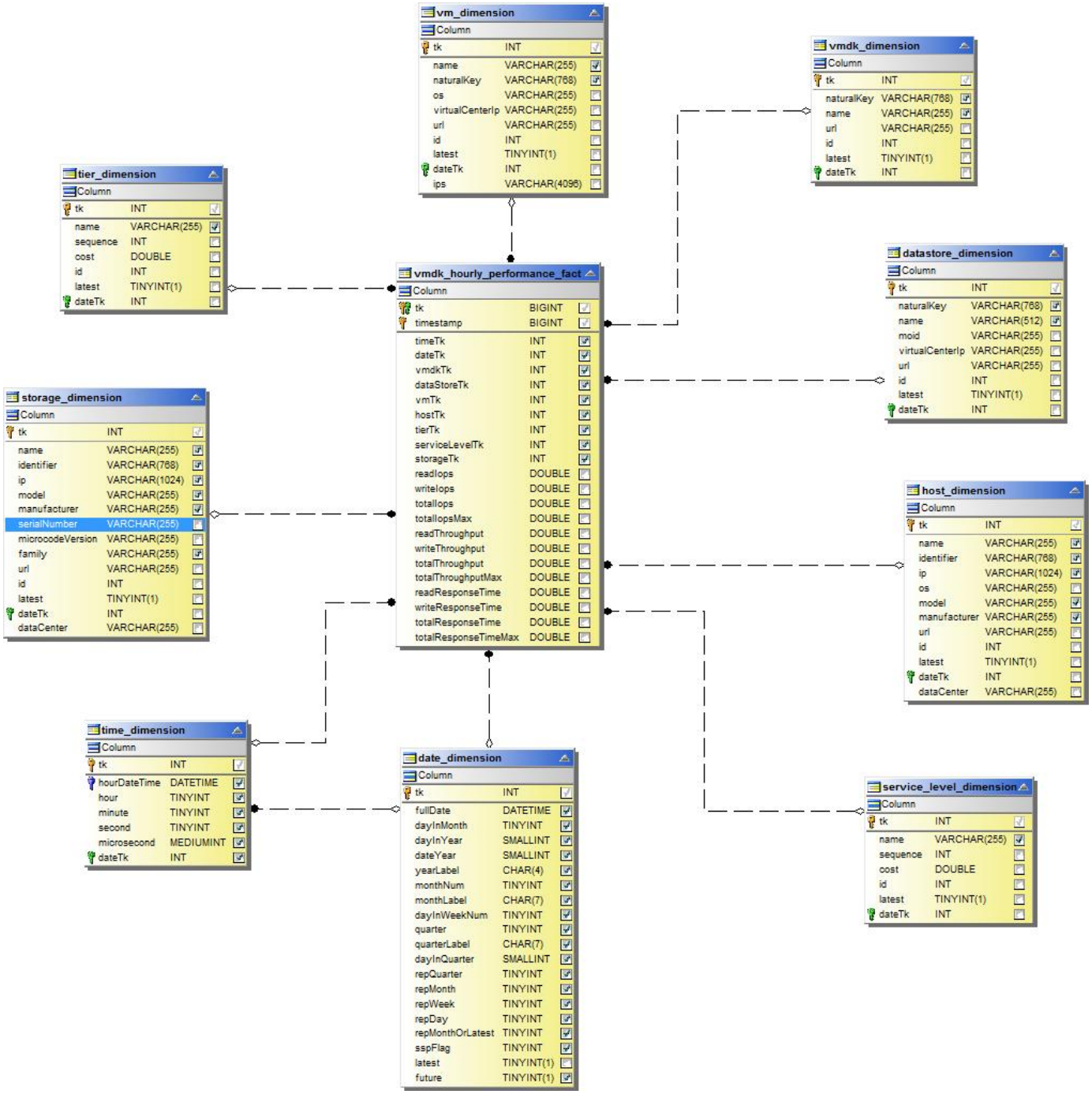
ホストの**VM**時間別パフォーマンス



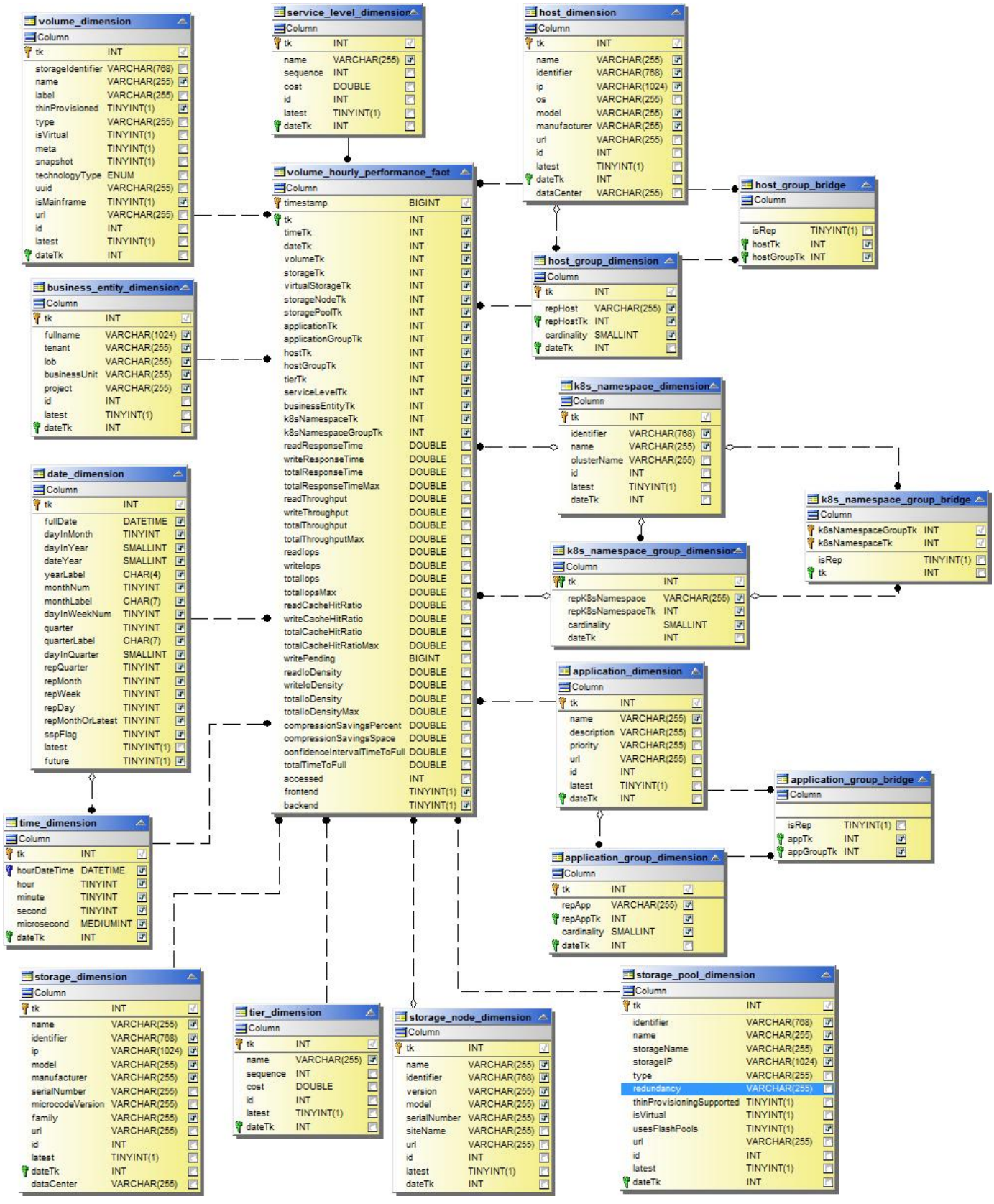
VMDK の日々のパフォーマンス



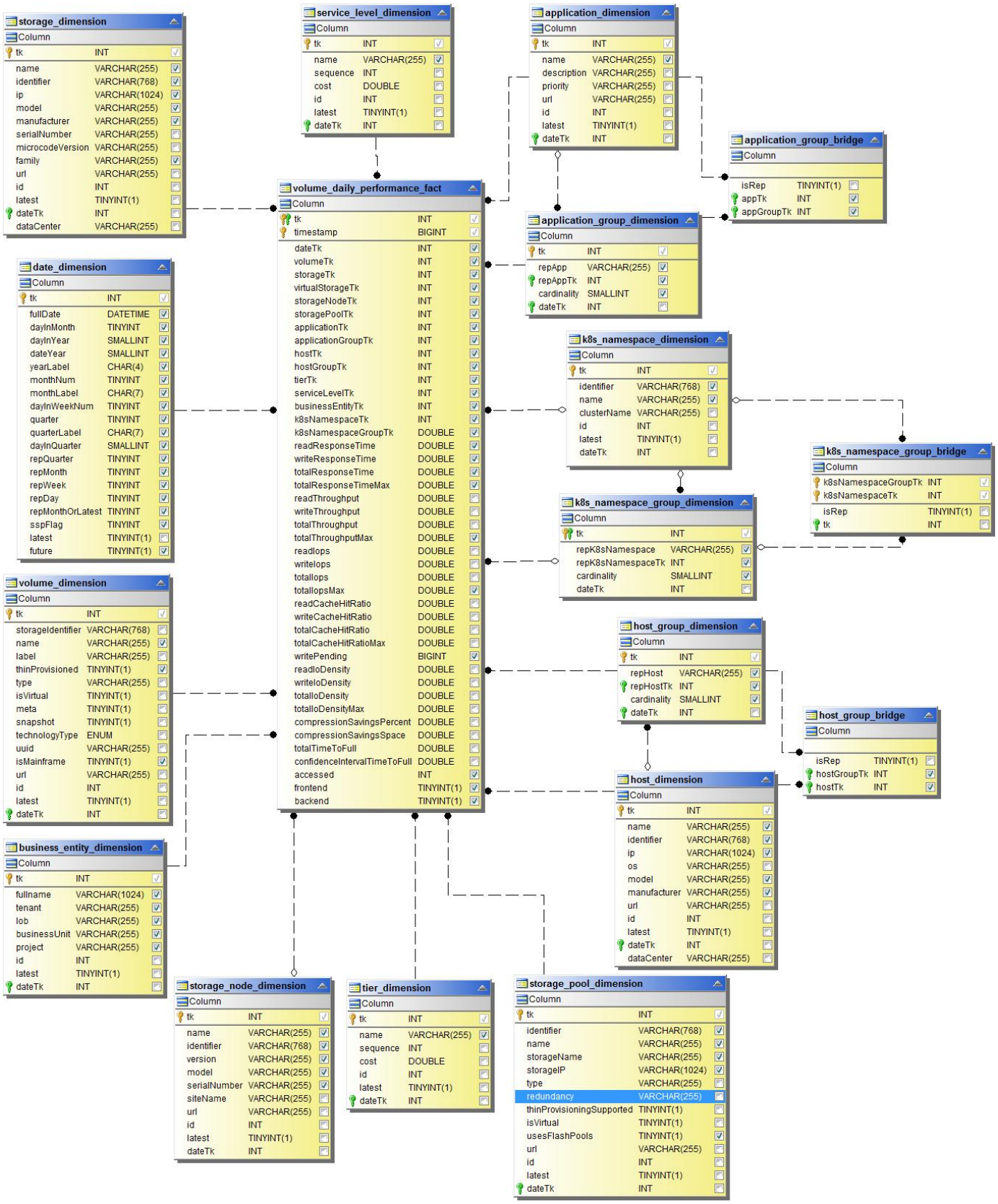
VMDK の時間別パフォーマンス



ボリューム時間別パフォーマンス



取引量日次パフォーマンス



Data Infrastructure Insightsサイト レポート用スキーマ

これらのスキーマ テーブルと図は、Data Infrastructure Insightsサイト レポートの参照としてここに提供されています。

"スキーマテーブル".PDF 形式です。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"

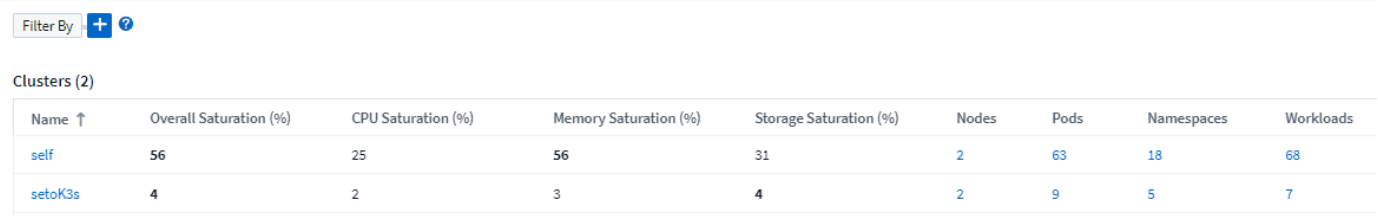
レポート機能は、Data Infrastructure Insightsで利用できます。"プレミアムエディション" 。

Kubernetes

Kubernetes クラスターの概要

Data Infrastructure Insights Kubernetes Explorer は、Kubernetes クラスターの全体的な健全性と使用状況を表示し、調査領域を簡単にドリルダウンできる強力なツールです。

ダッシュボード **> Kubernetes Explorer** をクリックすると、Kubernetes クラスターのリスト ページが開きます。この概要ページには、テナント上の Kubernetes クラスターの表が含まれています。



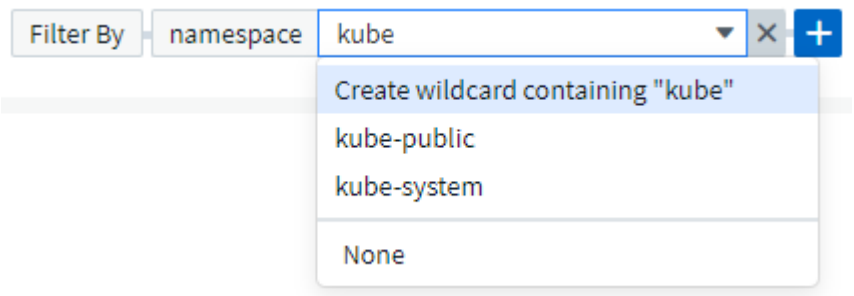
クラスターリスト

クラスター リストには、テナント上の各クラスターの次の情報が表示されます。

- クラスター 名前。クラスター名をクリックすると、"詳細ページ"そのクラスターに対して。
- *彩度*のパーセンテージ。全体的な飽和度は、CPU、メモリ、またはストレージの飽和度のうち最も高い値です。
- クラスター内の ノード の数。この番号をクリックすると、ノード リスト ページが開きます。
- クラスター内の **Pod** の数。この番号をクリックすると、Pod リスト ページが開きます。
- クラスター内の*名前空間*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。
- クラスター内の ワークロード の数。この番号をクリックすると、ワークロード リスト ページが開きます。

フィルターの改良

フィルタリングを行う場合、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 または AND を使用して 式 を作成したり、「なし」オプションを選択してフィールド内の null 値をフィルター処理したりすることもできます。



ワイルドカードまたは式 (例: NOT、AND、「なし」など) に基づくフィルターは、フィルター フィールドに

濃い青色で表示されます。リストから直接選択した項目は水色で表示されます。



Kubernetes フィルターはコンテキストに依存します。つまり、たとえば特定のノード ページにいる場合、pod_name フィルターによってそのノードに関連するポッドのみがリストされます。さらに、特定の名前空間にフィルターを適用すると、pod_name フィルターによって、そのノード上およびその名前空間内のポッドのみがリストされます。

ワイルドカードと式の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、ブール値では機能しないことに注意してください。

NetApp Kubernetes Monitoring Operator をインストールまたはアップグレードする前に

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 モニタリング オペレーター"。

コンポーネント	要件
Kubernetes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 Rancher Kubernetes Engine (RKE) VMware Tanzu
Linux OS	Data Infrastructure Insights は、 Arm64 アーキテクチャで実行されているノードをサポートしていません。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、これらのプラットフォームで次の Kubernetes ラベルを検索する Kubernetes ノード セレクターを指定することにより、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 以上: Kubernetes.io/os = linux Rancher + cattle.io (オーケストレーション/Kubernetes プラットフォームとして): 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 PATH に追加します。

コンポーネント	要件
接続	kubectl cli は、ターゲットの K8s クラスターと通信するように構成されており、 Data Infrastructure Insights環境にインターネット接続できます。インストール中にプロキシを使用している場合は、"プロキシサポートの設定"オペレータインストールのセクション。正確な監査とデータ レポートを行うには、ネットワーク タイム プロトコル (NTP) または簡易ネットワーク タイム プロトコル (SNTP) を使用してエージェント 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"これらの前提条件が満たされていることを確認することに加えて。
APIトークン	Operator を再デプロイする場合 (つまり、更新または置換する場合)、新しい API トークンを作成する必要はなく、以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な事項

もしあなたがプロキシ、持っているカスタムリポジトリ、または使用中オープンシフト、以下のセクションを注意深くお読みください。

こちらもご覧ください権限。

プロキシサポートの設定

NetApp Kubernetes Monitoring Operator をインストールするために、テナント上でプロキシを使用できる場所は 2 つあります。これらは同じプロキシ システムである場合もあれば、別のプロキシ システムである場合もあります。

- インストール コード スニペットの実行中（「curl」を使用）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 Kubernetes クラスターが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 Operating Monitor をインストールするには、まずプロキシがData Infrastructure Insights環境との良好な通信を許可するように構成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ー/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については、Operator をインストールする前に、*http_proxy/https_proxy* 環境変数を設定します。一部のプロキシ環境では、*no_proxy environment* 変数も設定する必要がある場合があります。

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. 現在のユーザーの *https_proxy* および/または *http_proxy* 環境変数を設定します。
    a. セットアップするプロキシに認証 (ユーザー名/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（ユーザー名/パスワード）
がある場合は、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 クラスターがData Infrastructure Insights環境と通信するために使用するプロキシについては、これらの手順をすべて読んだ後、 NetApp Kubernetes Monitoring Operator をインストールしてください。

NetApp Kubernetes Monitoring Operator をデプロイする前に、operator-config.yaml の AgentConfiguration の proxy セクションを構成します。

```
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**Docker**リポジトリの使用

デフォルトでは、 NetApp Kubernetes Monitoring Operator は、 Data Infrastructure Insightsリポジトリからコンテナ イメージをプルします。監視のターゲットとして Kubernetes クラスタが使用されており、そのクラスタがカスタムまたはプライベート 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 イメージをプルするように構成されている場合は、 NetApp Kubernetes Monitoring Operator に必要なコンテナへのアクセスを構成する必要があります。

NetApp Monitoring Operator インストール タイルから「イメージ プル スニペット」を実行します。このコマ

ンドは、 Data Infrastructure Insightsリポジトリにログインし、オペレーターのすべてのイメージ依存関係をプルし、 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、提供され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ているかについては、以下を参照してください。

コアオペレーター機能とKubernetesモニタリング

- netapp 監視
- kube-rbac-プロキシ
- kube-state-metrics
- テレグラフ
- ディストロレスルートユーザー

イベントログ

- 流暢なビット
- kubernetes イベント エクスポーター

ネットワークパフォーマンスとマップ

- ci-net-オブザーバー

企業ポリシーに従って、オペレーターの 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リポジトリのものと一致していることを確認します。

operator-deployment.yaml の monitoring-operator デプロイメントを編集し、すべてのイメージ参照を変更してプライベート Docker リポジトリを使用します。

```
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>
```

新しい docker リポジトリの場所を反映するように、operator-config.yaml の AgentConfiguration を編集します。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、*operator-config.yaml* の AgentConfiguration を編集して、*runPrivileged* 設定を有効に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

監視対象のクラスタに、ClusterRoleを持たないカスタムリソースが含まれている場合、"表示する集計"イベント ログでこれらのリソースを監視するには、オペレーター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. インストール前に *operator-additional-permissions.yaml* を編集するか、インストール後にリソース *ClusterRole/<namespace>-additional-permissions* を編集します。
2. 動詞 ["get", "watch", "list"] を使用して、目的の apiGroup とリソースの新しいルールを作成します。参照\https://kubernetes.io/docs/reference/access-authn-authz/rbac/
3. 変更をクラスターに適用する

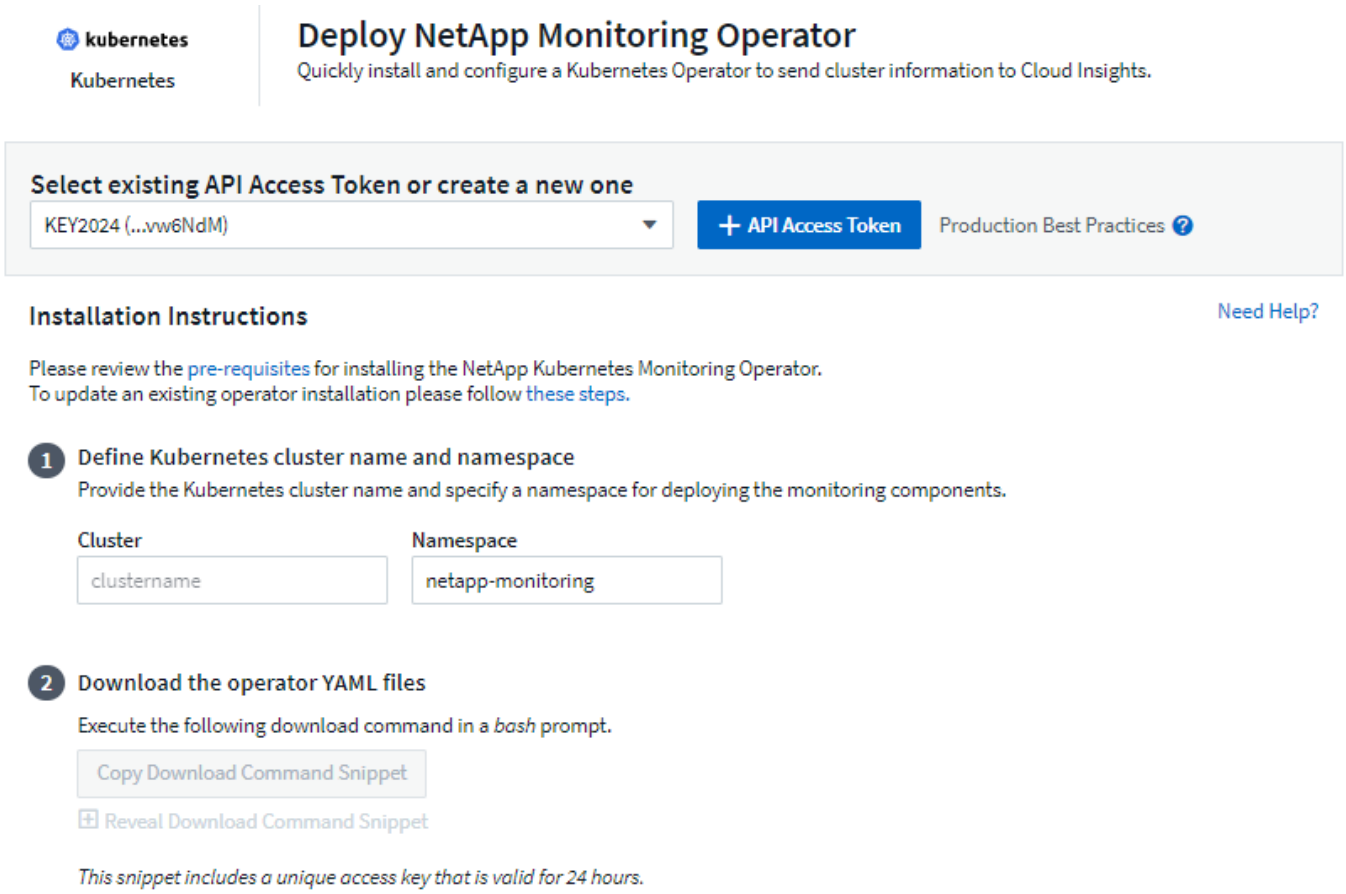
Kubernetes モニタリング オペレーターのインストールと構成

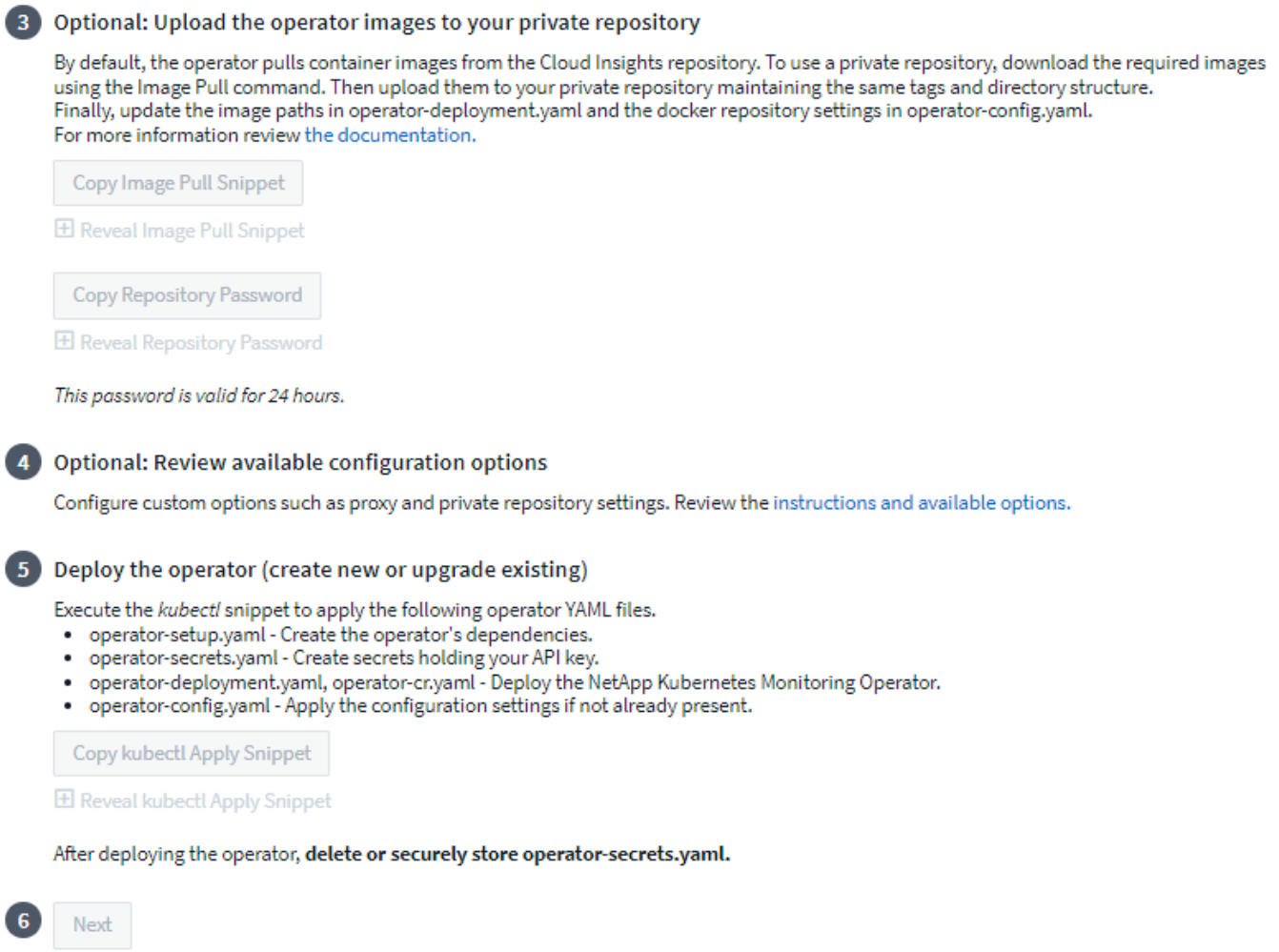
Data Infrastructure Insights は、 Kubernetes コレクション用の **Kubernetes Monitoring Operator** を提供します。新しいオペレーターをデプロイするには、**Kubernetes > Collectors > +Kubernetes Collector** に移動します。

Kubernetesモニタリングオペレーターをインストールする前に

参照"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に、ドキュメントを参照してください。

Kubernetes モニタリング オペレーターのインストール





Kubernetes に **Kubernetes Monitoring Operator** エージェントをインストールする手順:

1. 一意のクラスター名と名前空間を入力します。もしあなたがアップグレード以前の Kubernetes Operator からの場合は、同じクラスター名と名前空間を使用します。
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 *bash* ウィンドウに貼り付けて実行します。 Operator インストール ファイルがダウンロードされます。スニペットには一意のキーがあり、24 時間有効であることに注意してください。
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、*bash* シェルに貼り付けて実行します。イメージをプルしたら、それをプライベート リポジトリにコピーします。必ず同じタグとフォルダー構造を維持してください。 *operator-deployment.yaml* 内のパスと、*operator-config.yaml* 内の 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 リポジトリ設定などの利用可能な構成オプションを確認します。詳細については、"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、ダウンロードして実行して、Operator をデプロイします。
7. インストールは自動的に進行します。完了したら、[次へ] ボタンをクリックします。
8. インストールが完了したら、[次へ] ボタンをクリックします。 *operator-secrets.yaml* ファイルも必ず削除するか、安全に保存してください。

カスタムリポジトリをお持ちの場合は、以下をお読みください。カスタム/プライベートDockerリポジトリを

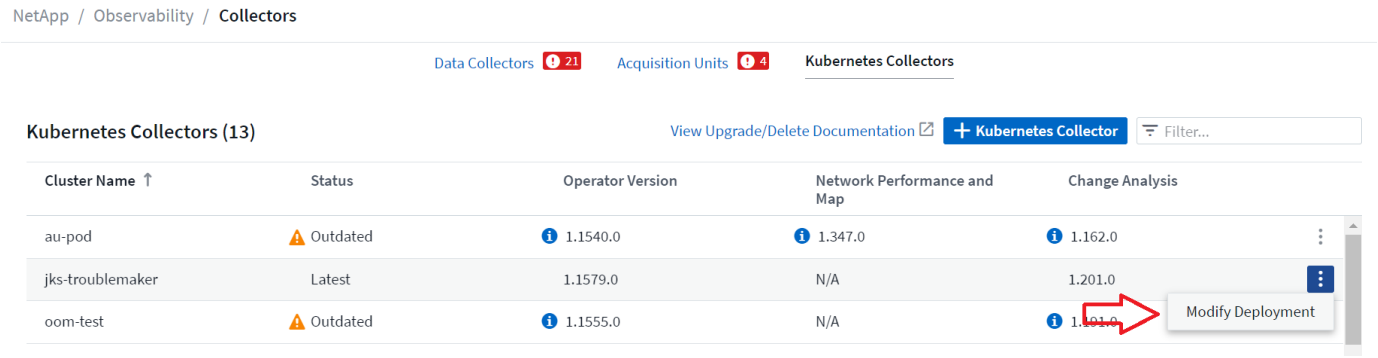
使用する 。

Kubernetes 監視コンポーネント

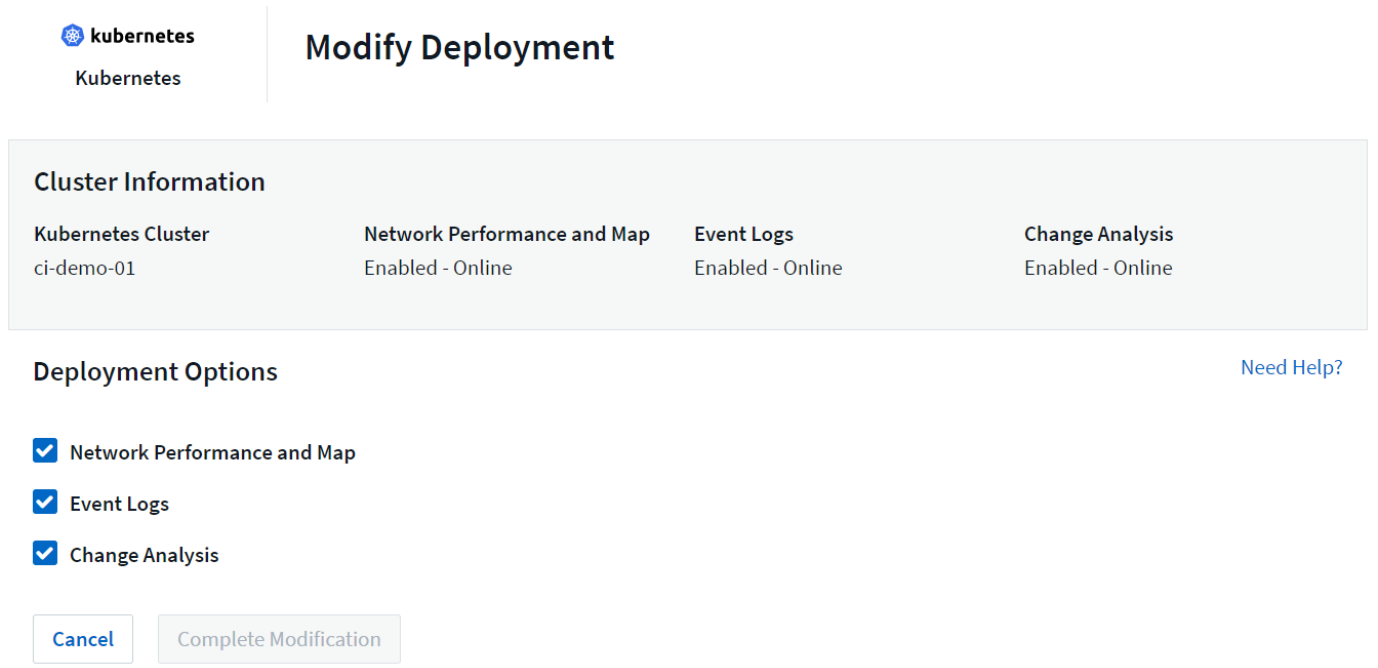
Data Infrastructure Insights Kubernetes モニタリングは、次の 4 つのモニタリング コンポーネントで構成されています。

- クラスターメトリック
- 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 コレクターに対してデフォルトで有効になっています。特定のコレクターに対して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、画面の右側にあるコレクターの「3 つのドット」メニューから *Modify Deployment* を選択して無効にすることができます。



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ー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。



最新のKubernetesモニタリングオペレーターへのアップグレード

DII プッシュボタンアップグレード

DII Kubernetes Collectors ページから Kubernetes Monitoring Operator をアップグレードできます。アップグレードするクラスターの横にあるメニューをクリックし、「アップグレード」を選択します。オペレーターはイメージ署名を検証し、現在のインストールのスナップショットを実行して、アップグレードを実行します。数分以内に、オペレーターのステータスが「アップグレード進行中」から「最新」へと進行していくのが確認できます。エラーが発生した場合は、詳細を表示するにはエラー ステータスを選択し、以下のプッシュ ボタン アップグレードのトラブルシューティング表を参照してください。

プライベートリポジトリによるプッシュボタンアップグレード

オペレーターがプライベート リポジトリを使用するように構成されている場合は、オペレーターの実行に必要なすべてのイメージとその署名がリポジトリで使用可能であることを確認してください。アップグレード プロセス中にイメージが不足しているためにエラーが発生した場合は、イメージをリポジトリに追加して、アップグレードを再試行してください。リポジトリにイメージ署名をアップロードするには、次のようにcosign ツールを使用してください。3 オプション: 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 > イメージプルスニペットで指定されたすべてのイメージの署名をアップロードしてください。

```
cosign copy example.com/src:v1 example.com/dest:v1
#Example
cosign copy <DII container registry>/netapp-monitoring:<image version>
<private repository>/netapp-monitoring:<image version>
```

以前実行していたバージョンにロールバックする

プッシュボタン アップグレード機能を使用してアップグレードし、アップグレード後 7 日以内に現在のバージョンのオペレーターに問題が発生した場合は、アップグレード プロセス中に作成されたスナップショットを使用して、以前実行していたバージョンにダウングレードできます。ロールバックするクラスターの横にあるメニューをクリックし、[ロールバック] を選択します。

手動アップグレード

既存の Operator に *AgentConfiguration* が存在するかどうかを判断します（名前空間がデフォルトの *netapp-monitoring* でない場合は、適切な名前空間に置き換えます）：

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
```

AgentConfiguration が存在する場合：

- インストール既存のオペレータよりも最新のオペレータを優先します。
  - 必ず最新のコンテナイメージを取得するカスタム リポジトリを使用している場合。

AgentConfiguration が存在しない場合：

- Data Infrastructure Insightsによって認識されるクラスター名をメモします (名前空間がデフォルトの netapp-monitoring でない場合は、適切な名前空間に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（名前空間がデフォルトの netapp-
monitoring でない場合は、適切な名前空間に置き換えます）。
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-operator,アンインストール
>>既存のオペレータ。
* <<installing-the-kubernetes-monitoring-operator,インストール
>>最新のオペレーター。
```

- 同じクラスター名を使用します。
- 最新の Operator YAML ファイルをダウンロードした後、デプロイする前に、*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。
- 必ず最新のコンテナイメージを取得するカスタム リポジトリを使用している場合。

Kubernetes モニタリング オペレーターの停止と起動

Kubernetes モニタリング オペレーターを停止するには:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Kubernetes モニタリング オペレーターを起動するには:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

アンインストール

Kubernetesモニタリングオペレーターを削除するには

Kubernetes モニタリング オペレーターのデフォルトの名前空間は「netapp-monitoring」であることに注意してください。独自の名前空間を設定している場合は、これらのコマンドと後続のすべてのコマンドおよびファイルでその名前空間を置き換えます。

監視オペレーターの新しいバージョンは、次のコマンドで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>
```

監視オペレーターが専用のネームスペースにデプロイされている場合は、ネームスペースを削除します。

```
 kubectl delete ns <NAMESPACE>
```

注：
最初のコマンドで「リソースが見つかりません」と返された場合は、次の手順に従って、監視オペレーターの古いバージョンをアンインストールしてください。

以下の各コマンドを順番に実行します。現在のインストールによっては、これらのコマンドの一部が「オブジェクトが見つかりません」というメッセージを返す場合があります。これらのメッセージは無視しても問題ありません。

```
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以前に作成されている場合:

```
kubectl delete scc telegraf-hostaccess
```

Kube-state-metricsについて

NetApp Kubernetes Monitoring Operator は、他のインスタンスとの競合を避けるために独自の kube-state-metrics をインストールします。

Kube-State-Metricsの詳細については、以下を参照してください。"このページ" 。

オペレーターの設定/カスタマイズ

これらのセクションには、オペレーター構成のカスタマイズ、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 の操作に関する情報が含まれています。

設定オプション

最も頻繁に変更される設定は、*AgentConfiguration* カスタム リソースで構成できます。オペレーターをデプロイする前に、*operator-config.yaml* ファイル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の例が含まれています。リストを見る"利用可能な設定"オペレーターの最新バージ

ョン。

オペレーターをデプロイした後、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
```

デプロイされたオペレーターのバージョンが _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
```

「サーバーからのエラー (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ーをアップグレードする必要があります。

プロキシサポートの設定

Kubernetes モニタリング オペレーターをインストールするために、テナント上でプロキシを使用できる場所は 2 つあります。これらは同じプロキシ システムである場合もあれば、別のプロキシ システムである場合もあります。

- インストール コード スニペットの実行中（「curl」を使用）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 Kubernetes クラスターが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、まずプロキシがData Infrastructure Insights環境との良好な通信を許可するように構成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ー/VM からData Infrastructure Insightsにアクセスできる場合は、プロキシは適切に構成されている可能性があります。

Kubernetes オペレーティング モニター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* 環境変数を設定します。一部のプロキシ環境では、*no_proxy environment* 変数も設定する必要がある場合があります。

変数を設定するには、Kubernetes モニタリング オペレーター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. 現在のユーザーの *https_proxy* および/または *http_proxy* 環境変数を設定します。
   a. セットアップするプロキシに認証 (ユーザー名/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 （ユーザー名/パスワード）がある場合は、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 クラスターがData Infrastructure Insights環境と通信するために使用するプロキシについては、これらの手順をすべて読んだ後、Kubernetes Monitoring Operator をインストールしてください。

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**Docker**リポジトリの使用

デフォルトでは、Kubernetes Monitoring Operator はData Infrastructure Insightsリポジトリからコンテナ イメージをプルします。監視のターゲットとして Kubernetes クラスターが使用されており、そのクラスターがカスタムまたはプライベート Docker リポジトリまたはコンテナー レジストリからのみコンテナー イメージをプルするように構成されている場合は、Kubernetes 監視オペレーターに必要なコンテナーへのアクセスを構成する必要があります。

NetApp Monitoring Operator インストール タイルから「イメージ プル スニペット」を実行します。このコマンドは、 Data Infrastructure Insightsリポジトリにログインし、オペレーターのすべてのイメージ依存関係をプルし、 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、提供され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ているかについては、以下を参照してください。

コアオペレーター機能とKubernetesモニタリング

- netapp 監視
- ci-kube-rbac-プロキシ
- ci-ksm
- ci-telegraf
- ディストロレスルートユーザー

イベントログ

- ci-fluent-bit
- ci-kubernetes-イベントエクスポーター

ネットワークパフォーマンスとマップ

- ci-net-オブザーバー

企業ポリシーに従って、オペレーターの 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リポジトリのものと一致していることを確認します。

operator-deployment.yaml の monitoring-operator デプロイメントを編集し、すべてのイメージ参照を変更してプライベート Docker リポジトリを使用します。

```
image: <docker repo of the enterprise/corp docker repo>/ci-kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

新しい docker リポジトリの場所を反映するように、*operator-config.yaml* の *AgentConfiguration* を編集します。プライベートリポジトリ用の新しい 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
```

長期パスワード用の **API** アクセストークン

一部の環境（プロキシリポジトリなど）では、Data Infrastructure Insights docker リポジトリの長期パスワードが必要です。インストール時に UI で提供されるパスワードは 24 時間のみ有効です。それを使用する代わりに、API アクセストークンを docker リポジトリパスワードとして使用できます。このパスワードは、API アクセストークンが有効である限り有効です。この特定の目的のために新しい API アクセストークンを生成することも、既存のものを使用することもできます。

"こちらをお読みください"新しいAPIアクセストークンを作成する手順については、こちらをご覧ください。

ダウンロードした *operator-secrets.yaml* ファイルから既存の API アクセス トークンを抽出するには、ユーザーは以下を実行できます：

```
grep '\.dockerconfigjson' operator-secrets.yaml |sed 's/.*\.dockerconfigjson:
//g' |base64 -d |jq
```

実行中のオペレーターインストールから既存のAPIアクセストークンを抽出するには、ユーザーは以下を実行できます：

```
kubectl -n netapp-monitoring get secret netapp-ci-docker -o
jsonpath='{.data.\.dockerconfigjson}' |base64 -d |jq
```

OpenShift の手順

OpenShift 4.6 以降で実行している場合は、*operator-config.yaml* の *AgentConfiguration* を編集して *runPrivileged* 設定を有効に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。

寛容と汚点

netapp-ci-telegraf-ds、*netapp-ci-fluent-bit-ds*、および *netapp-ci-net-observer-l4-ds* DaemonSets は、すべてのノードでデータを正しく収集するために、クラスター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。オペレーターは、いくつかのよく知られた 汚染 を許容するように設定されています。ノードにカスタムテイントを設定して、ポッドがすべてのノードで実行されないようにしている場合は、それらのテイントに対して*許容*を作成できます。"_AgentConfiguration_内" 。クラスター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、オペレーター ポッドをスケジュールして実行できるように、オペレーター デプロイメントに必要な許容値も追加する必要があります。

Kubernetesについて詳しく知る"汚名と寛容"。

戻る"* NetApp Kubernetes Monitoring Operator のインストール* ページ"

秘密についてのメモ

Kubernetes モニタリング オペレーターがクラスター全体でシークレットを表示する権限を削除するには、インストール前に *operator-setup.yaml* ファイルから次のリソースを削除します。

```
 ClusterRole/netapp-ci<namespace>-agent-secret
 ClusterRoleBinding/netapp-ci<namespace>-agent-secret
```

アップグレードの場合は、クラスター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* または *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。この行における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 モニタリング オペレーター イメージ署名の検証

オペレータのイメージとそれが展開するすべての関連イメージは、 NetAppによって署名されています。インストール前に cosign ツールを使用してイメージを手動で検証したり、Kubernetes アドミッション コントローラーを構成したりすることができます。詳細については、"Kubernetesドキュメント" 。

イメージ署名の検証に使用される公開鍵は、モニタリング オペレーターのインストール タイルの「オプション: オペレーター イメージをプライベート リポジトリにアップロード > イメージ署名公開鍵」で入手できます。

イメージ署名を手動で検証するには、次の手順を実行します。

1. 画像プルスニペットをコピーして実行する
2. リポジトリパスワードをコピーしてプロンプトが表示されたら入力します
3. イメージ署名公開鍵（例では dii-image-signing.pub）を保存します。
4. cosign を使用してイメージを検証します。共同署名の使用例を参照してください

```
$ cosign verify --key dii-image-signing.pub --insecure-ignore-sct
--insecure-ignore-tlog <repository>/<image>:<tag>
Verification for <repository>/<image>:<tag> --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - The signatures were verified against the specified public key
[{"critical":{"identity":{"docker-
reference":"<repository>/<image>"},"image":{"docker-manifest-
digest":"sha256:<hash>"},"type":"cosign container image
signature"},"optional":null}]
```

トラブルシューティング

Kubernetes モニタリング オペレーターの設定中に問題が発生した場合に試すことは次のとおりです。

問題：	これを試してください:
Kubernetes 永続ボリュームと対応するバックエンド ストレージ デバイス間のハイパーリンク/接続が表示されません。私の Kubernetes 永続ボリュームは、ストレージ サーバーのホスト名を使用して構成されています。	手順に従って既存の Telegraf エージェントをアンインストールし、最新の Telegraf 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 以降を使用している必要があり、Kubernetes クラスター 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：	これを試してください:
ログには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: *v1.MutatingWebhookConfiguration の一覧を取得できませんでした: 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: *v1.Lease の一覧を取得できませんでした: 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、Kubernetes バージョン 1.20 未満で kube-state-metrics バージョン 2.0.0 以上を実行している場合に表示されることがあります。 Kubernetes のバージョンを取得するには: *kubectl version* kube-state-metrics のバージョンを取得するには: *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* これらのメッセージが表示されないようにするには、ユーザーは kube-state-metrics デプロイメントを変更して、次のリースを無効にすることができます: *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* 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,nodes,persistentvolumeclaims,persistentvolumes, poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas, secrets、services 、statefulsets、storageclasses 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、horizontalpodautoscalers、ingresses、jobs、leases、limitranges 、mutatingwebhookconfigurations、namespaces、networkpolicies、nodes、persistentvolumeclaims、persistentvolumes、poddisruptionbudgets、pods、replicasets、replicationcontrollers、resourcequotas、secrets 、services、statefulsets、storageclasses、validatingwebhookconfigurations、volumeattachments"
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: Oct 11 14:23:41 ip-172-31-39-47 systemd[1]: Started The plugin-driven server agent for reporting metrics into InfluxDB. 10月11日 14:23:41 ip-172-31-39-47 telegraf[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。無視されました\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="開けませんでした。無視されました。open /etc/telegraf/.cache/snowflake/ocsp_response_cache.json: そのようなファイルまたはディレクトリはありません\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021-10-11T14:23:41Z I! Telegraf 1.19.3 の起動	これは既知の問題です。参照"このGitHubの記事"詳細についてはこちらをご覧ください。 Telegraf が稼働している限り、ユーザーはこれらのエラー メッセージを無視できます。

問題：	これを試してください:
Kubernetes では、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 が有効になっていて強制されている場合、Telegraf ポッドが Kubernetes ノード上の /proc/1/mountstats ファイルにアクセスできない可能性があります。この制限を克服するには、エージェント構成を編集し、runPrivileged 設定を有効にします。詳細については、OpenShift の手順を参照してください。
Kubernetes では、Telegraf ReplicaSet ポッドが次のエラーを報告しています: [inputs.prometheus] プラグインのエラー: キーペア /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: そのような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 として指定されたノード上で実行されることを目的としています。 ReplicaSet ポッドがこれらのノードのいずれかで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 taint があるかどうかを確認します。そうなる場合は、Telegraf ReplicaSet (telegraf-rs) に必要な許容範囲を追加します。たとえば、ReplicaSet を編集します… kubectl edit rs telegraf-rs …そして、適切な許容値を仕様に追加します。次に、ReplicaSet ポッドを再起動します。
PSP/PSA環境があります。これは監視オペレーターに影響しますか?	Kubernetes クラスターが Pod Security Policy (PSP) または Pod Security Admission (PSA) を適用した状態で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 をサポートする現在の Operator にアップグレードするには、次の手順に従います。1. アンインストール以前の監視オペレーター: kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com 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. インストール監視オペレータの最新バージョン。
PSP/PSA を使用しているのですが、Operator を展開しようとして問題が発生しました。	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> edit agent 2. 「security-policy-enabled」を「false」としてマークします。これにより、ポッド セキュリティ ポリシーとポッド セキュリティ アドミッションが無効になり、オペレーターがデプロイ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 が削除されたことが表示されます) kubectl get all -n <namespace>
grep -i psp (何も見つからないことが表示されます)	「ImagePullBackoff」エラーが発生
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 モニタリング オペレーターがそれを適切に認識するようにまだ構成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 リポジトリの構成について。	モニタリング オペレーターのデプロイメントで問題が発生していますが、現在のドキュメントでは解決できません。

問題：	これを試してください:
次のコマンドの出力をキャプチャまたはメモして、テクニカル サポート チームに連絡してください。 ``` 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) ポッドは CrashLoopBackOff にあります
これらのポッドは、ネットワーク可観測性のワークロード マップ データ コレクターに対応します。以下を試してください: • いずれかのポッドのログをチェックして、最小カーネル 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 は、最小カーネル バージョン 4.18.0 より小さいです","time":"2022-11-09T08:23:08Z"} ---- • Net-observer ポッドでは、Linux カーネル バージョンが少なくとも 4.18.0 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。	ポッドはオペレーター名前空間（デフォルト：netapp-monitoring）で実行されていますが、ワークロードマップのUIやクエリのKubernetesメトリックにデータが表示されません。
K8S クラスターのノード上の時刻設定を確認します。正確な監査とデータ レポートを実現するために、ネットワーク タイム プロトコル (NTP) または簡易ネットワーク タイム プロトコル (SNTP) を使用してエージェント マシンの時刻を同期することを強くお勧めします。	オペレーター名前空間内の一部のネットオブザーバーポッドが保留状態になっています
Net-observer は DaemonSet であり、k8s クラスターの各ノードでポッドを実行します。 • 保留中の状態のポッドに注意し、CPU またはメモリのリソースの問題が発生しているかどうかを確認します。ノードで必要なメモリと CPU が使用可能であることを確認します。	Kubernetes モニタリング オペレーターをインストールした直後、ログに次の内容が表示されます: [inputs.prometheus] プラグインでエラーが発生しました: http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics への HTTP リクエストの作成エラー: http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics を取得: tcp をダイヤル: kube-state-metrics.<namespace>.svc.cluster.local を検索: そのようなホストはありません

問題：	これを試してください:
このメッセージは通常、新しいオペレータがインストールされ、*ksm* ポッドが起動する前に *telegraf-rs* ポッドが起動している場合にのみ表示されます。すべてのポッドが実行されると同時に、これらのメッセージは停止します。	クラスター内に存在する Kubernetes CronJobs に対して収集されているメトリックが表示されません。
Kubernetesのバージョンを確認してください（つまり `kubectl version`）。 v1.20.x 以下の場合、これは予想される制限です。 Kubernetes Monitoring Operator とともにデプロイされた kube-state-metrics リリースは、v1.CronJob のみをサポートします。 Kubernetes 1.20.x 以下では、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。	オペレーターをインストールすると、telegraf-ds ポッドは CrashLoopBackOff 状態になり、ポッド ログに「su: 認証失敗」と表示されます。
AgentConfiguration の telegraf セクションを編集し、*dockerMetricCollectionEnabled* を false に設定します。詳細については、オペレーターの"設定オプション"を参照してください。… spec：… telegraf：…-name：docker run-mode：- DaemonSet substitutions：- key：DOCKER_UNIX_SOCK_PLACEHOLDER value：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: E! [エージェント] 出力への書き込みエラー: http: Post "https://<tenant_url>/rest/v1/lake/ingest/influxdb": コンテキストの期限が切れました (ヘッダーの待機中に Client.Timeout を超えました)
AgentConfiguration の telegraf セクションを編集し、*outputTimeout* を 10 秒に増やします。詳細については、オペレーターの"設定オプション"。	一部のイベント ログの *involvedobject* データが見つかりません。
必ず、"権限"上記のセクション。	netapp-ci-monitoring-operator-<pod> と monitoring-operator-<pod> という名前の 2 つの監視オペレータ ポッドが実行されているのはなぜですか?
2023年10月12日現在、 Data Infrastructure Insights は、ユーザーへのサービス向上のため、オペレーターをリファクタリングしました。これらの変更を完全に適用するには、古い演算子を削除するそして新しいものをインストールする。	Kubernetes イベントが予期せずData Infrastructure Insightsへのレポートを停止しました。
イベント エクスポーター ポッドの名前を取得します。 `kubectl -n netapp-monitoring get pods`	grep event-exporter

問題：	これを試してください:
awk '{print $1}'	sed 's/event-exporter./event-exporter/'` 「netapp-ci-event-exporter」または「event-exporter」のいずれかである必要があります。次に、監視エージェントを編集します `kubectl -n netapp-monitoring edit agent`、LOG_FILE の値を、前の手順で見つかった適切なイベント エクスポーター ポッド名を反映するように設定します。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 … …. あるいは、uninstallそして再インストールエージェント。
Kubernetes モニタリング オペレーターによってデプロイされたポッドが、リソース不足のためにクラッシュしているのがわかります。	Kubernetesモニタリングオペレーターを参照してください"設定オプション"必要に応じて CPU および/またはメモリの制限を増やします。
イメージが欠落しているか、構成が無効であるため、netapp-ci-kube-state-metrics ポッドの起動または準備ができませんでした。現在、StatefulSet はスタックしており、構成の変更が netapp-ci-kube-state-metrics ポッドに適用されていません。	StatefulSetは"壊れた"州。構成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 ポッドは、Kubernetes Operator のアップグレードを実行した後に起動に失敗し、ErrImagePull (イメージのプルに失敗します) をスローします。	ポッドを手動でリセットしてみてください。
ログ分析の Kubernetes クラスターで、「イベントは maxEventAgeSeconds より古いため破棄されました」というメッセージが表示されています。	Operator の *agentconfiguration* を変更し、*event-exporter-maxEventAgeSeconds* (つまり 60 秒)、*event-exporter-kubeQPS* (つまり 100)、および *event-exporter-kubeBurst* (つまり 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、"設定オプション"ページ。

問題：	これを試してください:
Telegraf は、ロック可能なメモリが不足しているために警告を発したりクラッシュしたりします。	基盤となるオペレーティング システム/ノードで Telegraf のロック可能なメモリの制限を増やしてみてください。制限を増やすことができない場合は、NKMO エージェント構成を変更し、*unprotected* を *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されます。復号化された秘密がディスクにスワップアウトされる可能性があるため、セキュリティ上のリスクが生じ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の実行が可能になります。*unprotected* 設定オプションの詳細については、"設定オプション"ページ。
Telegraf から次のような警告メッセージが表示されます: *W! [inputs.diskio] "vdc"* のディスク名を収集できません*: /dev/vdc* の読み取りエラー*:* そのようなファイルまたはディレクトリはありません	Kubernetes Monitoring Operator の場合、これらの警告メッセージは無害であり、無視しても問題ありません。または、AgentConfiguration の telegraf セクションを編集し、*runDsPrivileged* を true に設定します。詳細については、"オペレータの設定オプション"を参照してください。

問題：	これを試してください:

Fluent-bit ポッドが次のエラーで失敗しています: [2024/10/16 14:16:23] [error] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] 開いているファイルが多すぎます [2024/10/16 14:16:23] [error] 入力 tail.0 の初期化に失敗しました [2024/10/16 14:16:23] [error] [engine] 入力の初期化に失敗しました	クラスター内の *fsnotify* 設定を変更してみます。
	
	`sudo sysctl fs.inotify.max_user_instances (take note of setting)`
	
	`sudo sysctl fs.inotify.max_user_instances=<something larger than current setting>`
	
	`sudo sysctl fs.inotify.max_user_watches (take note of setting)`
	
	`sudo sysctl fs.inotify.max_user_watches=<something larger than current setting>`
	
	Fluent-bit を再起動します。
	
	注意: これらの設定をノードの再起動後も維持するには、*/etc/sysctl.conf* に次の行を追加する必要があります。
	
	`fs.inotify.max_user_instances=<something larger than current setting>`
	`fs.inotify.max_user_watches=<something larger than current setting>`

Telegraf DS ポッドは、TLS 証明書を検証できないために kubernetes 入力プラグインが HTTP リクエストを実行できないことに関連するエラーを報告しています。例: E! [inputs.kubernetes] プラグインのエラー: HTTPリクエストの送信中にエラーが発生しました"<a href="https://<kubelet_IP>:10250/stats/summary":" class="bare">https://<kubelet_IP>:10250/stats/summary":得る"<a href="https://<kubelet_IP>:10250/stats/summary":" class="bare">https://<kubelet_IP>:10250/stats/summary":tls: 証明書の検証に失敗しました: x509: IP SANが含まれていないため、<kubelet_IP>の証明書を検証できません	これは、kubelet が自己署名証明書を使用している場合、および/または指定された証明書の証明書の *Subject Alternative Name* リストに <kubelet_IP> が含まれていない場合に発生します。これを解決するには、ユーザーは"エージェント構成"、*telegraf:insecureK8sSkipVerify* を *true* に設定します。これにより、Telegraf 入力プラグインが検証をスキップするように設定されます。あるいは、ユーザーはkubeletを次のように設定することができます。"サーバーTLSブートストラップ"これにより、「certificates.k8s.io」API からの証明書要求がトリガーされます。

問題：	これを試してください:
Fluent-bit ポッドで次のエラーが発生し、ポッドを起動できません：026/01/12 20:20:32] [error] [sqldb] error=unable to open database file [2026/01/12 20:20:32] [error] [input:tail:tail.0] db: could not create 'in_tail_files' table [2026/01/12 20:20:32] [error] [input:tail:tail.0] could not open/create database [2026/01/12 20:20:32] [error] failed initialize input tail.0 [2026/01/12 20:20:32] [error] [engine] input initialization failed	DBファイルが存在するホストディレクトリに適切な読み取り / 書き込み権限があることを確認してください。具体的には、ホストディレクトリは非ルートユーザーに読み取り / 書き込み権限を付与する必要があります。デフォルトのDBファイルの場所は、fluent-bit-dbFile *agentconfiguration* オプションで上書きされない限り、/var/log/ です。SELinuxが有効になっている場合は、fluent-bit-seLinuxOptionsType agentconfigurationオプションを 'spc_t' に設定してみてください。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Kubernetes モニタリング オペレーターの設定オプション

その"Kubernetes モニタリング オペレーター" AgentConfiguration ファイルを通じて、幅広いカスタマイズオプションが提供されます。リソース制限、収集間隔、プロキシ設定、許容値、コンポーネント固有の設定を構成して、Kubernetes 環境の監視を最適化できます。これらのオプションを使用して、Telegraf、kube-state-metrics、ログ収集、ワークロードマッピング、変更管理、その他の監視コンポーネントをカスタマイズできます。

サンプル **AgentConfiguration** ファイル

以下に、各オプションの説明を含むサンプルの *AgentConfiguration* ファイルを示します。

```
apiVersion: monitoring.netapp.com/v1alpha1
kind: AgentConfiguration
metadata:
  name: netapp-ci-monitoring-configuration
  namespace: "netapp-monitoring"
  labels:
    installed-by: nkmo-netapp-monitoring

spec:
  ##
  ## One can modify the following settings to configure and customize the
operator.
  ## Optional settings are commented out with their 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 cluster name
    ## The cluster name must be unique across all clusters in your Data
Infrastructure Insights (DII) environment.
    ##
    clusterName: "my_cluster"

    ##
    ## Proxy settings
    ## If applicable, specify the proxy through which the operator should
communicate with DII.
    ## Refer to additional 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]
    ## Repository from which the operator pulls the required images
    ## By default, the operator pulls from the DII repository. To use a
private repository, set this field to the
    ## applicable repository name. Refer to additional 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]
    ## Name of the imagePullSecret required for dockerRepo
    ## When using a private repository, set this field to the applicable
secret name.
    ##
    dockerImagePullSecret: 'netapp-ci-docker'

    ##
```

```
    ## Automatic expiring API key rotation settings
    ## Allow the operator to automatically rotate its expiring API key,
generating a new API key and
    ## using it to replace the expiring one. The expiring API key itself
must support auto rotation.
    ##
    # tokenRotationEnabled: 'true'
    ##
    ## Threshold (number of days before expiration) at which the operator
should trigger rotation.
    ## The threshold must be less than the total duration of the API key.
    ##
    # tokenRotationThresholdDays: '30'

  push-button-upgrades:
    ##
    ## Allow the operator to be upgraded using the Data Infrastructure
Insights (DII) UI
    ##
    # enabled: 'true'

    ##
    ## Frequency at which the operator polls and checks for upgrade
requests from DII
    ##
    # polltimeSeconds: '60'

    ##
    ## Allow operator upgrade to proceed even if new images are not
present
    ##
    # ignoreImageNotPresent: 'false'

    ##
    ## Allow operator upgrade to proceed even if image signature
verification fails
    ## Warning: Enabling this setting is dangerous!
    ##
    # ignoreImageSignatureFailure: 'false'

    ##
    ## Allow operator upgrade to proceed even if image signature
verification fails
    ## Warning: Enabling this setting is dangerous!
    ##
    # ignoreYAMLSignatureFailure: 'false'
```

```
    ##
    ## Use dockerImagePullSecret to access the image repository and verify
the existence of the new images
    ##
    # imageValidationUseSecret: 'true'

    ##
    ## Time allowed for the old operator pod to shutdown before reporting
an upgrade failure to DII
    ##
    # upgradesShutdownTime: '240'

    ##
    ## Time allowed for the new operator pod to startup before reporting
an upgrade failure to DII
    ##
    # upgradesStartupTime: '600'

  telegraf:
    ##
    ## Frequency at which telegraf collects data
    ## The frequency should not exceed 60s.
    ##
    # collectionInterval: '60s'

    ##
    ## Maximum number of metrics per batch
    ## Telegraf sends metrics to outputs in batches. This controls the
size of those writes.
    ##
    # batchSize: '10000'

    ##
    ## Maximum number of unwritten metrics per output
    ## Telegraf caches metrics until they are successfully written by the
output. This controls how many metrics
    ## can be cached. Once the buffer is filled, the oldest metrics will
get dropped.
    ##
    # bufferLimit: '150000'

    ##
    ## Rounds collection interval to collectionInterval
    ## If collectionInterval is 60s, collection will occur on-the-minute
    ##
    # roundInterval: 'true'
```

```
    ##
    ## Jitter between plugins on collection
    ## Each input plugin sleeps a random amount of time within jitter
before collecting. This can be used to prevent
    ## multiple input plugins from querying the same resources at the same
time. The maximum collection interval would
    ## be collectionInterval + collectionJitter.
    ##
    # collectionJitter: '0s'

    ##
    ## Precision to which collected metrics are rounded
    ## When set to "0s", precision will be set by the units specified by
collectionInterval.
    ##
    # precision: '0s'

    ##
    ## Frequency at which telegraf flushes and writes data
    ## Frequency should not exceed collectionInterval.
    ##
    # flushInterval: '60s'

    ##
    ## Jitter between plugins on writes
    ## Each output plugin sleeps a random amount of time within jitter
before flushing. This can be used to prevent
    ## multiple output plugins from writing the same resources at the same
time, and causing large spikes. The maximum
    ## flush interval would be flushInterval + flushJitter.
    ##
    # flushJitter: '0s'

    ##
    ## Timeout for HTTP output plugins
    ## Time allowed for http output plugins to successfully writing before
failing.
    ##
    # outputTimeout: '5s'

    ##
    ## CPU/Mem limits and requests for netapp-ci-telegraf-ds DaemonSet
    ##
    # dsCpuLimit: '750m'
    # dsMemLimit: '800Mi'
    # dsCpuRequest: '100m'
```

```
    # dsMemRequest: '500Mi'

    ##
    ## CPU/Mem limits and requests for netapp-ci-telegraf-rs ReplicaSet
    ##
    # rsCpuLimit: '3'
    # rsMemLimit: '4Gi'
    # rsCpuRequest: '100m'
    # rsMemRequest: '500Mi'

    ##
    ## telegraf runs through the processor plugins a second time after the
aggregators plugins, by default. Use this
    ## option to skip the second run.
    ##
    # skipProcessorsAfterAggregators: 'false'

    ##
    ## Additional tolerations for netapp-ci-telegraf-ds DaemonSet and
netapp-ci-telegraf-rs ReplicaSet
    ## Inspect the netapp-ci-telegraf-rs ReplicaSet and netapp-ci-
telegraf-ds DaemonSet to view the default tolerations.
    ## If additional tolerations are needed, specify them here using the
following abbreviated single line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # dsTolerations: ''
    # rsTolerations: ''

    ##
    ## Additional node selector terms for netapp-ci-telegraf-rs ReplicaSet
    ## Inspect the netapp-ci-telegraf-rs ReplicaSet to view the default
node selectors terms. If additional node
    ## selector terms are needed, specify them here using the following
abbreviated single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
    # rsNodeSelectorTerms: ''
```

```
    ##
    ## telegraf uses lockable memory to protect secrets in memory. If
telegraf issues warnings about insufficient
    ## lockable memory, try increasing the limit of lockable memory on the
applicable nodes. If increasing this limit
    ## is not an option for the given environment, set unprotected to true
so telegraf does not attempt to use
    ## lockable memory.
    ##
    # unprotected: 'false'

    ##
    ## Run the netapp-ci-telegraf-ds DaemonSet's telegraf-mountstats-
poller container in privileged mode
    ## The telegraf-mountstats-poller container needs read-only access to
system files such as those in /proc/ (i.e. to
    ## monitor NFS IO metrics, etc.). Some environments impose restricts
that prevent the container from reading these
    ## system files. Unless those restrictions are lifted, users may need
to run this container in privileged mode.
    ##
    # runPrivileged: 'false'

    ##
    ## Run the netapp-ci-telegraf-ds DaemonSet's telegraf container in
privileged mode
    ## The telegraf container needs read-only access to system files such
as those in /dev/ (i.e. for the telegraf
    ## diskio input plugin to retrieve disk metrics). Some environments
impose restricts that prevent the container from
    ## accessing these system files. Unless those restrictions are lifted,
users may need to run this container in
    ## privileged mode.
    ##
    # runDsPrivileged: 'false'

    ##
    ## Allow the netapp-ci-telegraf-ds DaemonSet's telegraf-ds, telegraf-
init, and telegraf-mountstats-poller containers
    ## to run with escalation privilege. This is needed to access/read
root-protected files (node UUID,
    ## /proc/1/mountstats, etc.). Allowing escalation privilege should
negate the need to run these containers in
    ## privileged mode.
    ##
    # allowDsPrivilegeEscalation: 'true'
```

```
    ##
    ## Allow the netapp-ci-telegraf-rs DaemonSet's telegraf-rs and
telegraf-rs-init containers
    ## to run with escalation privilege. This is needed to access/read
root-protected files (node UUID,
    ## etcd credentials when applicable, etc.). Allowing escalation
privilege should negate the need to run these
    ## containers in privileged mode.
    ##
    # allowRsPrivilegeEscalation: 'true'

    ##
    ## Enable collection of block IO metrics (kubernetes.pod_to_storage)
    ##
    # dsBlockIOEnabled: 'true'

    ##
    ## Enable collection of NFS IO metrics (kubernetes.pod_to_storage)
    ##
    # dsNfsIOEnabled: 'true'

    ##
    ## Enable collection of system-specific objects/metrics for managed
k8s clusters
    ## This consists of k8s objects within the kube-system and cattle-
system namespaces for managed k8s clusters
    ## (i.e. EKS, AKS, GKE, managed Rancher, etc.).
    ##
    # managedK8sSystemMetricCollectionEnabled: 'false'

    ##
    ## Enable collection of pod ephemeral storage metrics
(kubernetes.pod_volume)
    ##
    # podVolumeMetricCollectionEnabled: 'false'

    ##
    ## Declare Rancher cluster is managed
    ## Rancher can be deployed in managed or on-premise environments. The
operator contains logic to try to determine
    ## which type of environment Rancher is running in (i.e. to factor
into managedK8sSystemMetricCollectionEnabled).
    ## If the operator logic misidentifies whether Rancher is running in a
managed environment or not, use this option
    ## to declare Rancher is managed.
```

```
    ##
    # isManagedRancher: 'false'

    ##
    ## Locations for the etcd certificate and key files
    ## The operator looks at well-known locations for the etcd certificate
and key files. If this cannot find these
    ## files, the applicable telegraf input plugin will fail. Use this
option to specify the complete filepath to these
    ## files on the nodes.
    ## Note that the well-known locations for these files are typically
root-protected. This is one of the reasons why
    ## the netapp-ci-telegraf-rs ReplicaSet's telegraf-rs-init container
needs to run with escalation privileges.
    ##
    # rsHostEtcdCrt: ''
    # rsHostEtcdKey: ''

    ##
    ## Allow operator/telegraf communications with k8s without TLS
verification
    ## In some environments, TLS verification will not succeed (i.e.
certificates lack IP SANs). To skip the
    ## verification, use this option.
    ##
    # insecureK8sSkipVerify: 'false'

  kube-state-metrics:
    ##
    ## CPU/Mem limits and requests for netapp-ci-kube-state-metrics
StatefulSet
    ##
    # cpuLimit: '500m'
    # memLimit: '1Gi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    ##
    ## Comma-separated list of k8s resources for which to collect metrics
    ## Refer to the kube-state-metrics --resources CLI option
    ##
    # resources:
'cronjobs,daemonsets,deployments,horizontalpodautoscalers,ingresses,jobs,n
amespaces,nodes,persistentvolumeclaims,persistentvolumes,pods,replicasets,
resourcequotas,services,statefulsets'
```

```
    ##
    ## Comma-separated list of k8s metrics to collect
    ## Refer to the kube-state-metrics --metric-allowlist CLI option
    ##
    # 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,kube_horizontal
podautoscaler_spec_max_replicas,kube_horizontalpodautoscaler_spec_min_repl
icas,kube_horizontalpodautoscaler_status_condition,kube_horizontalpodautos
caler_status_current_replicas,kube_horizontalpodautoscaler_status_desired_
replicas'

    ##
    ## Comma-separated list of k8s label keys that will be used to
determine which labels to export/collect
    ## Refer to the kube-state-metrics --metric-labels-allowlist CLI
option
    ##
    # labels:
'cronjobs=[*],daemonsets=[*],deployments=[*],horizontalpodautoscalers=[*],
ingresses=[*],jobs=[*],namespaces=[*],nodes=[*],persistentvolumeclaims=[*]
,persistentvolumes=[*],pods=[*],replicasets=[*],resourcequotas=[*],service
s=[*],statefulsets=[*]'

    ##
    ## Additional tolerations for netapp-ci-kube-state-metrics StatefulSet
    ## Inspect the netapp-ci-kube-state-metrics StatefulSet to view the
default tolerations. If additional
    ## tolerations are needed, specify them here using the following
abbreviated single line format:
    ##
```

```
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # tolerations: ''

    ##
    ## Additional node selector terms for netapp-ci-kube-state-metrics
StatefulSet
    ## Inspect the kube-state-metrics StatefulSet to view the default node
selectors terms. If additional node selector
    ## terms are needed, specify them here using the following abbreviated
single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
    # nodeSelectorTerms: ''

    ##
    ## Number of kube-state-metrics shards
    ## For large clusters, kube-state-metrics may be overwhelmed with
collecting and exporting the amount of metrics
    ## generated. This can lead to collection timeouts for the netapp-ci-
telegraf-rs pod. If this is observed, use this
    ## option to increase the number of kube-state-metrics shards to
redistribute the workload.
    ##
    # shards: '2'

  logs:
    ##
    ## Allow the netapp-ci-fluent-bit-ds DaemonSet's fluent-bit container
to run with escalation privilege.
    ## This is needed to access/read root-protected files (event-exporter
pod log, fluent-bit DB file, etc.).
    ##
    # fluent-bit-allowPrivilegeEscalation: 'true'

    ##
    ## Read content from the head of the file, not the tail
    ##
    # readFromHead: "true"
```

```
    ##
    ## Network protocol for DNS (i.e. UDP, TCP, etc.)
    ##
    # dnsMode: "UDP"

    ##
    ## DNS resolver (i.e. LEGACY, ASYNC, etc.)
    ##
    # fluentBitDNSResolver: "LEGACY"

    ##
    ## Additional tolerations for netapp-ci-fluent-bit-ds DaemonSet
    ## Inspect the netapp-ci-fluent-bit-ds DaemonSet to view the default
tolerations. If additional tolerations are
    ## needed, specify them here using the following abbreviated single
line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # fluent-bit-tolerations: ''

    ##
    ## CPU/Mem limits and requests for netapp-ci-fluent-bit-ds DaemonSet
    ##
    # fluent-bit-cpuLimit: '500m'
    # fluent-bit-memLimit: '1Gi'
    # fluent-bit-cpuRequest: '50m'
    # fluent-bit-memRequest: '100Mi'

    ##
    ## Top-level host path in which the kubernetes container logs reside,
including any symlinks from var/log/containers
    ## For example, if /var/log/containers/*.log is a symlink to
/kubernetes/log to
    ## /kubernetes/var/lib/docker/containers/*/*.log, fluent-bit-
containerLogPath should be set to '/kubernetes'.
    ##
    # fluent-bit-containerLogPath: '/var/lib/docker/containers'

    ## fluent-bit DB file path/location

    ##
    ## fluent-bit DB file path/location
    ## By default, fluent-bit is configured to use /var/log/netapp-
monitoring_flb_kube.db.  This path usually requires
```

```
    ## escalated privileges for read/write. Users who want to avoid
escalation privilege can use this option to specify
    ## a different DB file path/location. The custom path/location should
allow non-root users to read/write.
    ## Ideally, the path/location should be persistent.
    ##
    # fluent-bit-dbFile: '/var/log/netapp-monitoring_flb_kube.db'

    ##
    ## Additional tolerations for netapp-ci-event-exporter Deployment
    ## Inspect the netapp-ci-event-exporter Deployment to view the default
tolerations. If additional tolerations are
    ## needed, specify them here using the following abbreviated single
line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # event-exporter-tolerations: ''

    ##
    ## CPU/Mem limits and requests for netapp-ci-event-exporter Deployment
    ##
    # event-exporter-cpuLimit: '500m'
    # event-exporter-memLimit: '1Gi'
    # event-exporter-cpuRequest: '50m'
    # event-exporter-memRequest: '100Mi'

    ##
    ## Max age for events to be processed and exported; older events are
discarded
    ##
    # event-exporter-maxEventAgeSeconds: '10'

    ##
    ## Client-side throttling
    ## Set event-exporter-kubeBurst to roughly match event rate
    ## Set event-exporter-kubeQPS to approximately 1/5 of event-exporter-
kubeBurst
    ##
    # event-exporter-kubeQPS: 20
    # event-exporter-kubeBurst: 100

    ##
    ## Additional node selector terms for netapp-ci-event-exporter
Deployment
```

```
    ## Inspect the event-exporter Deployment to view the default node
selectors terms. If additional node selector terms
    ## are needed, specify them here using the following abbreviated
single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
    # event-exporter-nodeSelectorTerms: ''

  workload-map:
    ## Run workload-map container with escalation privilege to coordinate
memlocks
    ##
    ## Allow the netapp-ci-net-observer-l4-ds DaemonSet's net-observer
container to run with escalation privilege.
    ## This is needed to coordinate memlocks.
    ##
    # allowPrivilegeEscalation: 'true'

    ##
    ## CPU/Mem limits and requests for netapp-ci-net-observer-l4-ds
DaemonSet
    ##
    # cpuLimit: '500m'
    # memLimit: '500Mi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    ##
    ## Metric aggregation interval (in seconds)
    ## Set metricAggregationInterval between 30 and 120
    ##
    # metricAggregationInterval: '60'

    ##
    ## Interval for bpf polling
    ## Set bpfPollInterval between 3 and 15
    ##
    # bpfPollInterval: '8'

    ##
    ## Enable reverse DNS lookups on observed IPs
```

```
    ##
    # enableDNSLookup: 'true'

    ##
    ## Additional tolerations for netapp-ci-net-observer-l4-ds DaemonSet
    ## Inspect the netapp-ci-net-observer-l4-ds DaemonSet to view the
default tolerations. If additional tolerations
    ## are needed, specify them here using the following abbreviated
single line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # l4-tolerations: ''

    ##
    ## Run the netapp-ci-net-observer-l4-ds DaemonSet's net-observer
container in privileged mode
    ## Some environments impose restricts that prevent the net-observer
container from running.
    ## Unless those restrictions are lifted, users may need to run this
container in privileged mode.
    ##
    # runPrivileged: 'false'

  change-management:
    ##
    ## CPU/Mem limits and requests for netapp-ci-change-observer-watch-rs
ReplicaSet
    ##
    # cpuLimit: '1'
    # memLimit: '1Gi'
    # cpuRequest: '500m'
    # memRequest: '500Mi'

    ##
    ## Interval (in seconds) after which a non-successful deployment of a
workload will be marked as failed
    ##
    # workloadFailureDeclarationIntervalSeconds: '30'

    ##
    ## Frequency (in seconds) at which workload deployments are combined
and sent
    ##
    # workloadDeployAggrIntervalSeconds: '300'
```

```
    ##
    ## Frequency (in seconds) at which non-workload deployments are
combined and sent
    ##
    # nonWorkloadDeployAggrIntervalSeconds: '15'

    ##
    ## 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"'

    ##
    ## Additional node selector terms for netapp-ci-change-observer-watch-
rs ReplicaSet
    ## Inspect the netapp-ci-change-observer-watch-rs ReplicaSet to view
the default node selectors terms. If additional
    ## node selector terms are needed, specify them here using the
following abbreviated single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
    # nodeSelectorTerms: ''

    ##
    ## Comma-separated list of additional kinds to watch
    ## Each kind should be prefixed by its API group. This list in
addition to the default set of kinds watched by the
    ## collector.
    ##
    ## Example: '"authorization.k8s.io.subjectaccessreviews"'
    ##
    # additionalKindsToWatch: ''

    ##
    ## 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: ''

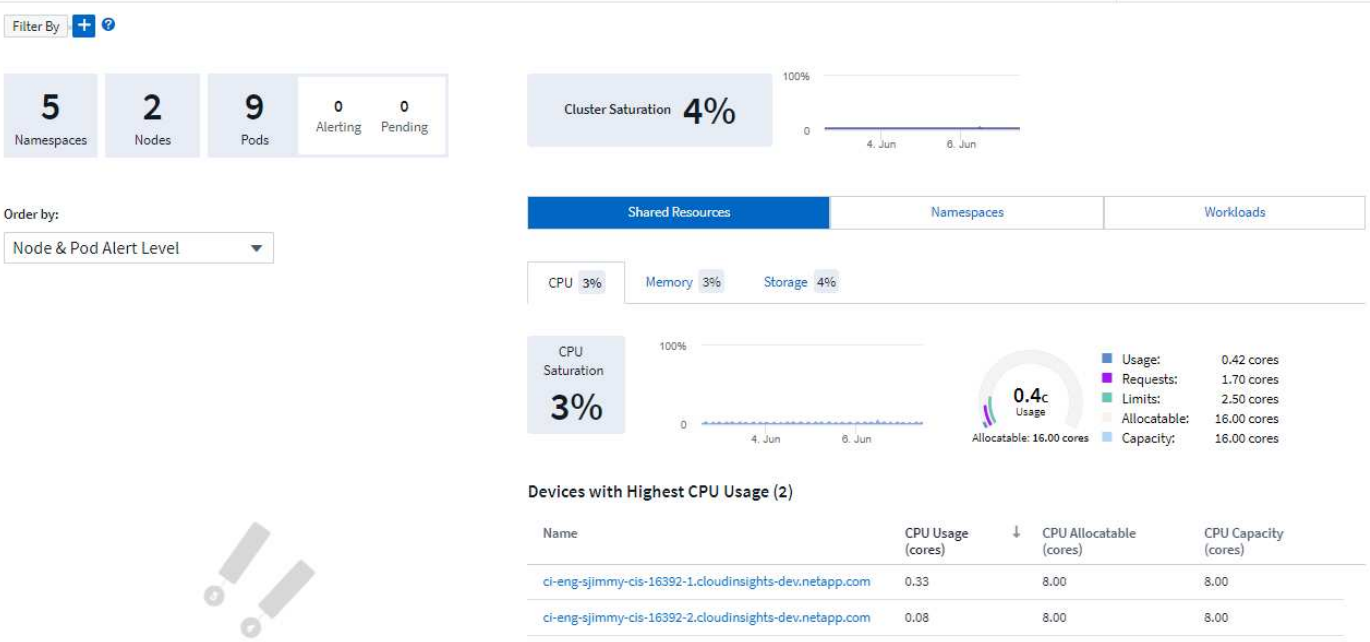
    ##
    ## Comma-separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
    ## Each kind should be prefixed by its API group.
    ##
    ## Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
    ##
    # kindsToIgnoreFromWatch: ''

    ##
    ## Frequency with which log records are sent to DII from the collector
    ##
    # logRecordAggrIntervalSeconds: '20'

    ##
    ## Additional tolerations for netapp-ci-change-observer-watch-rs
ReplicaSet
    ## Inspect the netapp-ci-change-observer-watch-rs ReplicaSet to view
the default tolerations. If additional
    ## tolerations are needed, specify them here using the following
abbreviated single line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # watch-tolerations: ''
```

Kubernetes クラスターの詳細ページ

Kubernetes クラスターの詳細ページには、Kubernetes クラスターの詳細な概要が表示されます。



名前空間、ノード、ポッドの数

ページ上部のカウントには、クラスター内の名前空間、ノード、ポッドの合計数と、現在アラートおよび保留中の popd の数が表示されます。

共有リソースと飽和

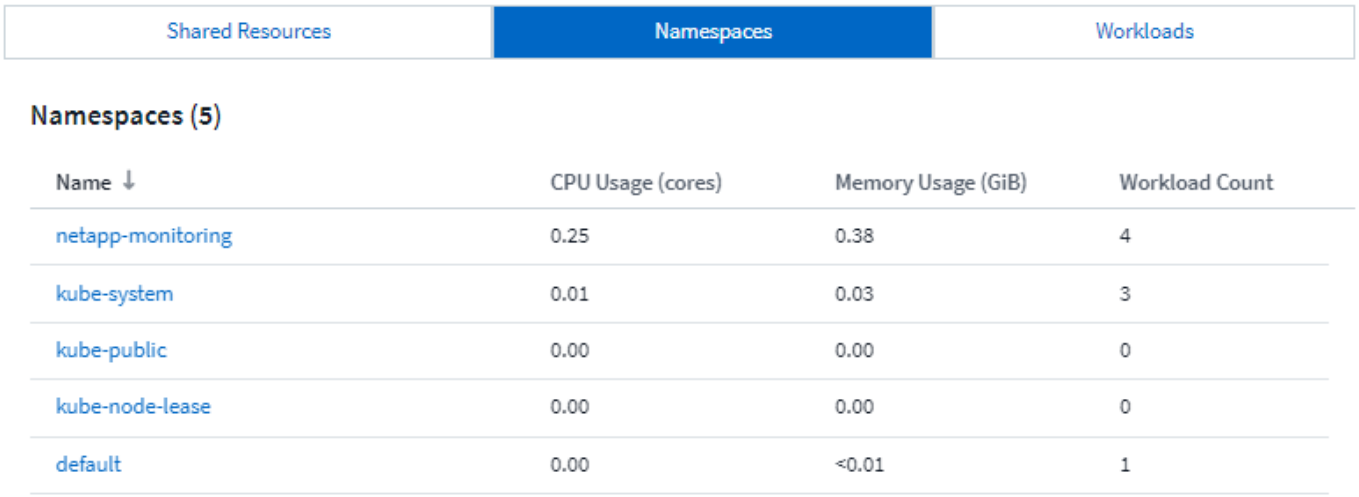
詳細ページの右上には、現在のクラスターの飽和度がパーセンテージで表示され、時間の経過に伴う最近の傾向を示すグラフも表示されます。クラスターの飽和度は、各時点での CPU、メモリ、またはストレージの飽和度のうち最も高い値です。

その下には、デフォルトで 共有リソース の使用状況が表示され、CPU、メモリ、ストレージのタブがあります。各タブには、飽和率と時間の経過に伴う傾向、および追加の使用状況の詳細が表示されます。ストレージの場合、表示される値は、個別に計算されるバックエンドとファイルシステムの飽和度のうち大きい方になります。

使用頻度が最も高いデバイスは下部の表に表示されます。これらのデバイスを調べるには、いずれかのリンクをクリックしてください。

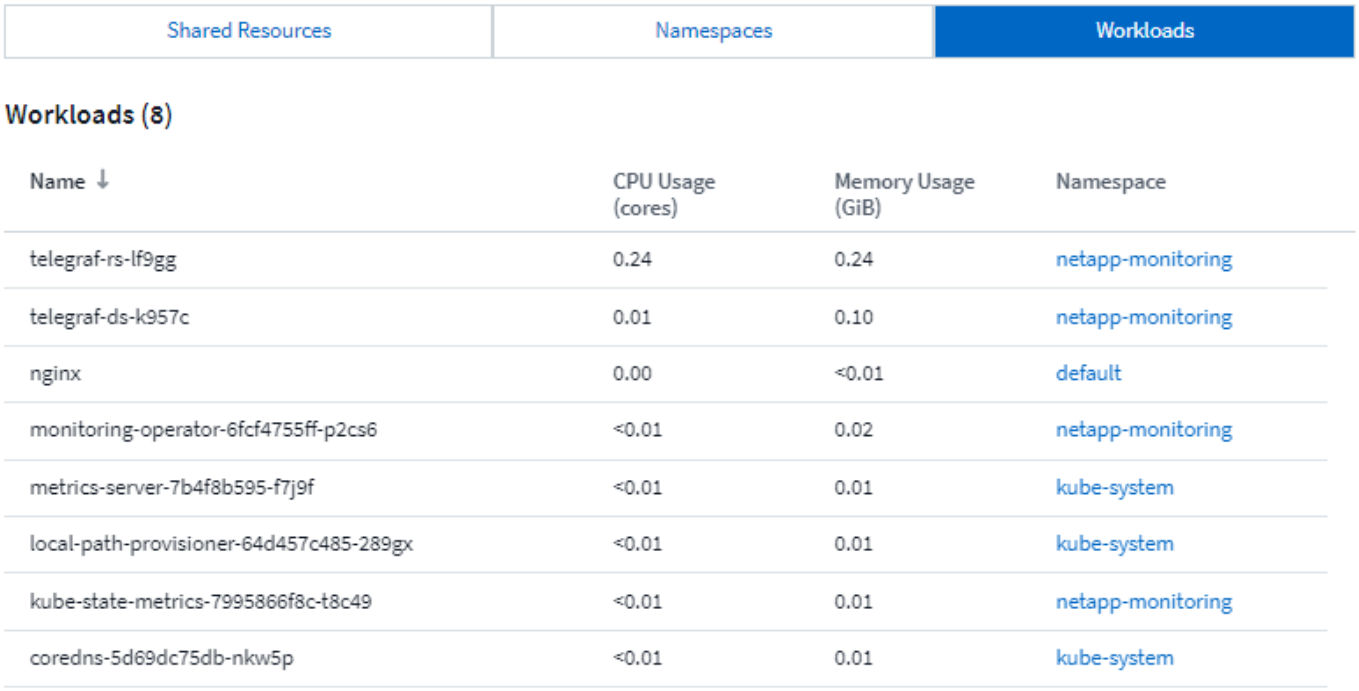
ネームスペース

「名前空間」タブには、Kubernetes 環境内のすべての名前空間のリストが表示され、CPU とメモリの使用率、および各名前空間のワークロード数が表示されます。名前リンクをクリックして、各名前空間を調べます。



ワークロード

同様に、[ワークロード] タブには、各名前空間のワークロードのリストが表示され、CPU とメモリの使用状況も表示されます。名前空間リンクをクリックすると、それぞれの詳細が表示されます。



クラスター「ホイール」



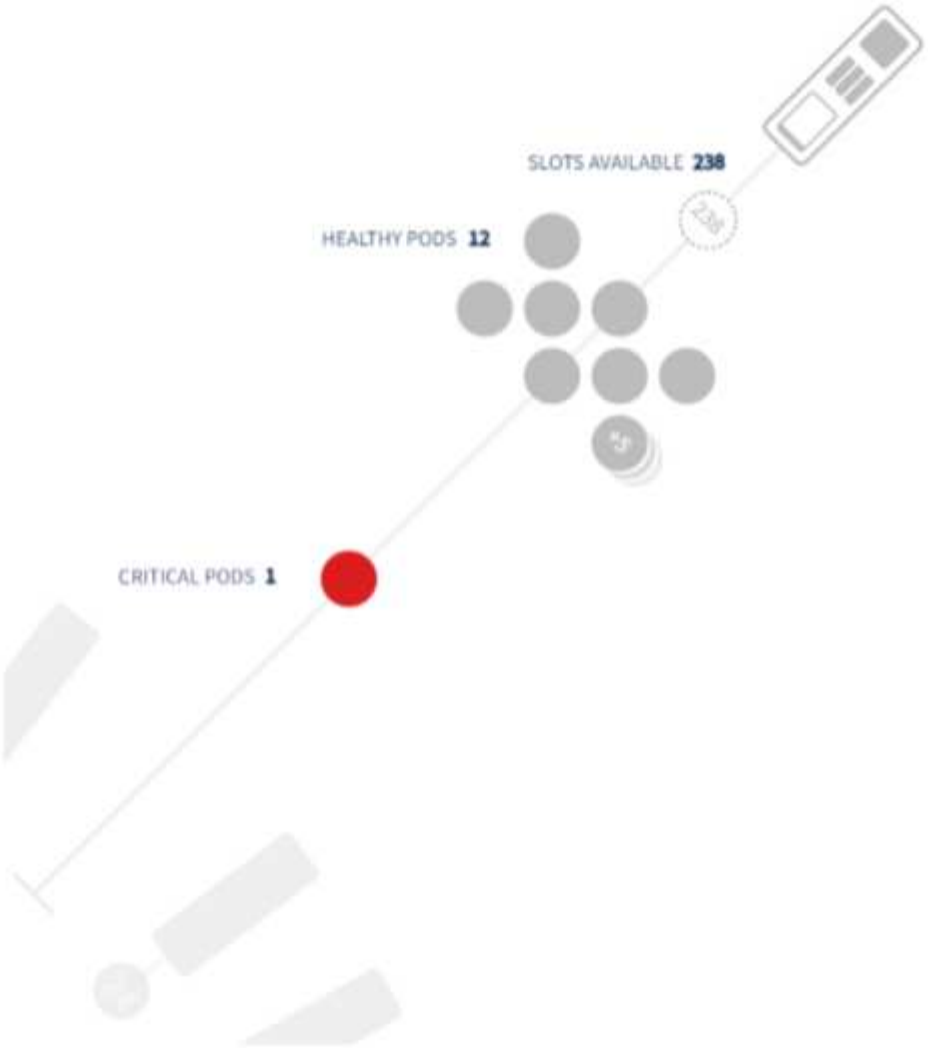
クラスターの「ホイール」セクションでは、ノードとポッドの健全性が一目でわかり、さらに詳しい情報にドリルダウンできます。クラスターにページのこの領域に表示できる数を超えるノードが含まれている場合は、使用可能なボタンを使用してホイールを回すことができます。

アラートを発しているポッドまたはノードは赤で表示されます。 「警告」エリアはオレンジ色で表示されます。スケジュールされていない (つまり、接続されていない) ポッドは、クラスターの「ホイール」の下隅に表示されます。

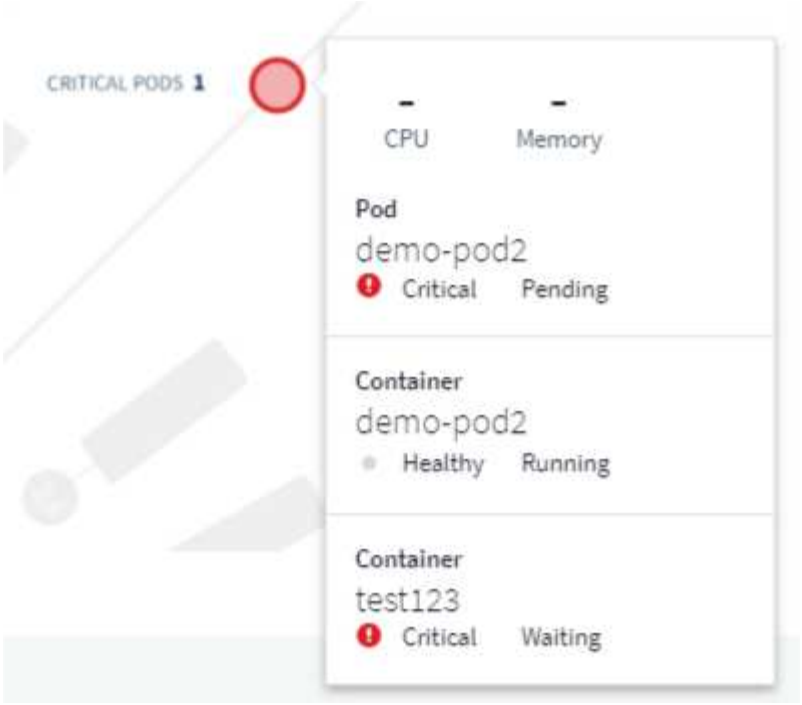
ポッド (円) またはノード (バー) の上にマウスを移動すると、ノードのビューが拡張されます。



そのビュー内のポッドまたはノードをクリックすると、拡張されたノード ビューが拡大表示されます。



ここから、要素の上にマウスを置くと、その要素の詳細が表示されます。たとえば、この例の重要なポッドにマウスを移動すると、そのポッドの詳細が表示されます。



ノード要素にマウスを移動すると、ファイルシステム、メモリ、CPU の情報を表示できます。



ゲージに関する注意

メモリ ゲージと CPU ゲージは、割り当て可能な容量 と 合計容量 の両方に関連して 使用済み を表示するため、3 色で表示されます。

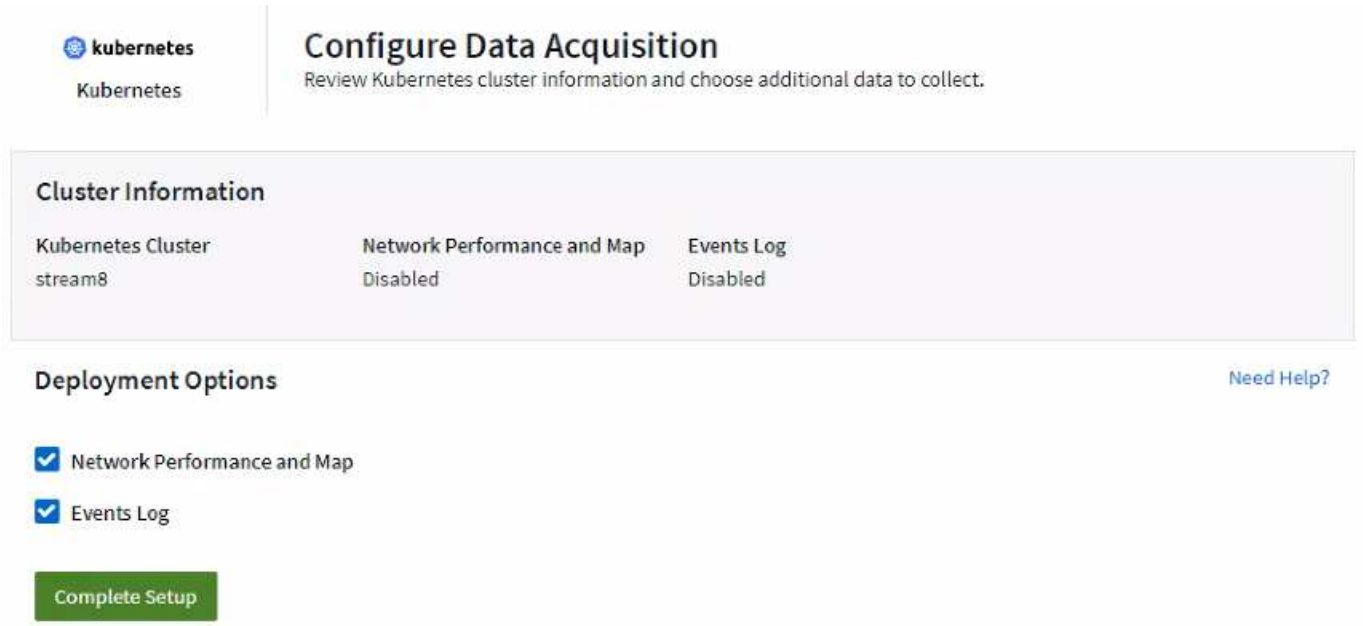
Kubernetes ネットワークパフォーマンス監視とマップ

Kubernetes ネットワーク パフォーマンス モニタリングおよびマップ機能は、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素化し、ネットワーク パフォーマンスの遅延と異常をリアルタイムで可視化して、ユーザーに影響が及ぶ前にパフォーマンスの問題を特定します。この機能により、組織は Kubernetes トラフィック フローを分析および監査して全体的なコストを削減できます。

主な機能: • 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強調表示します。 • 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。 • イングレス、エグレス、クロスリージョン、クロスゾーンのネットワーク 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ネットワークパフォーマンスモニタリングとマップを使用する前に、"NetApp Kubernetes 監視オペレーター"このオプションを有効にします。オペレーターのデプロイ中に、「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選択して有効にします。 Kubernetes ランディング ページに移動して「デプロイメントの変更」を選択することで、このオプションを有効にすることもできます。



モニター

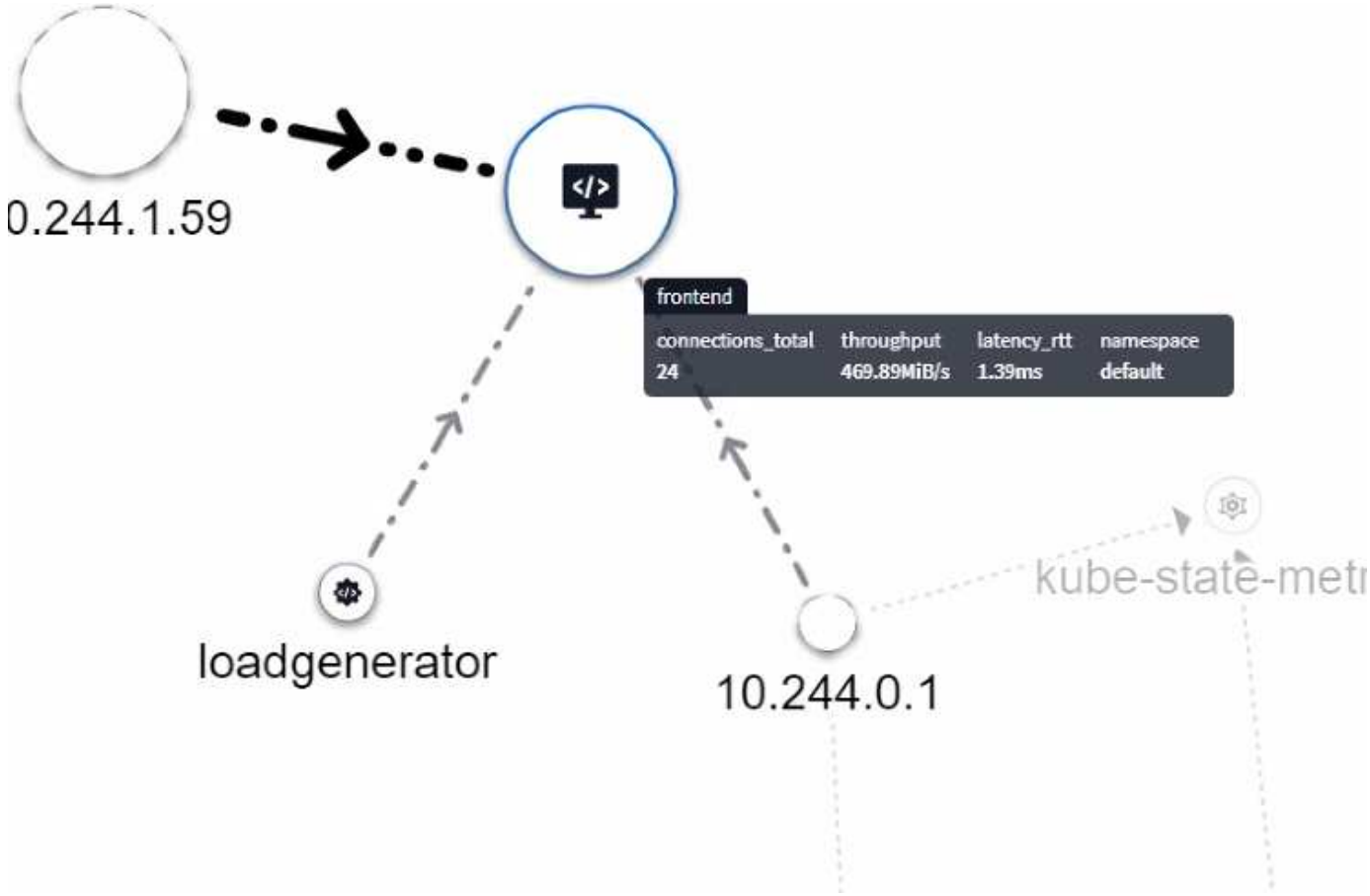
ワークロードマップは"監視"情報を導き出す。 Data Infrastructure Insights は、いくつかのデフォルトの Kubernetes モニターを提供します (これらはデフォルトで 一時停止 されている可能性があることに注意してください)。必要なモニターを 再開 (つまり有効化) することも、ワークロード マップでも使用される Kubernetes オブジェクト用のカスタム モニターを作成することもできます。

以下のいずれかのオブジェクト タイプに対して、 Data Infrastructure Insightsメトリック アラートを作成できます。データがデフォルトのオブジェクト タイプ別にグループ化されていることを確認します。

- kubernetes.ワークロード
- kubernetes.daemonset
- kubernetes.デプロイメント
- kubernetes.cronジョブ
- kubernetes.ジョブ
- kubernetes.レプリカセット
- 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ます。ワークロードの上にマウスを置くと、次の例のように、そのワークロードの概要情報が表示されます。



円内のアイコンは、さまざまなサービス タイプを表します。アイコンは、基礎となるオブジェクトがラベル。



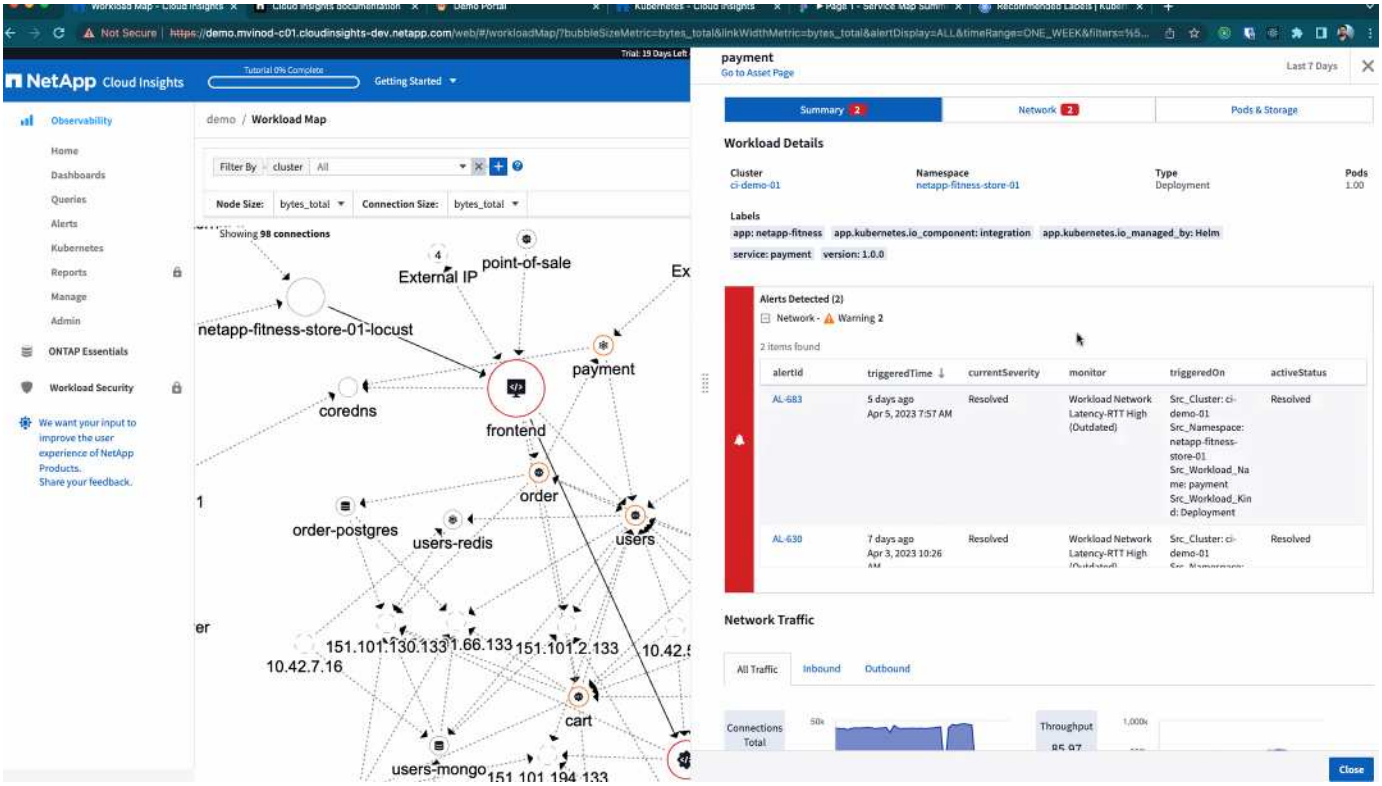
各円のサイズはノードのサイズを示します。これらのサイズは相対的なものであり、ブラウザのズーム レベルや画面サイズによって実際の円のサイズが変わる可能性があることに注意してください。同様に、トラフィック ライン スタイルを使用すると、接続サイズが一目でわかります。太い実線はトラフィック量が多く、細い点線はトラフィック量が少ないことを示します。

円内の数字は、現在サービスによって処理されている外部接続の数です。



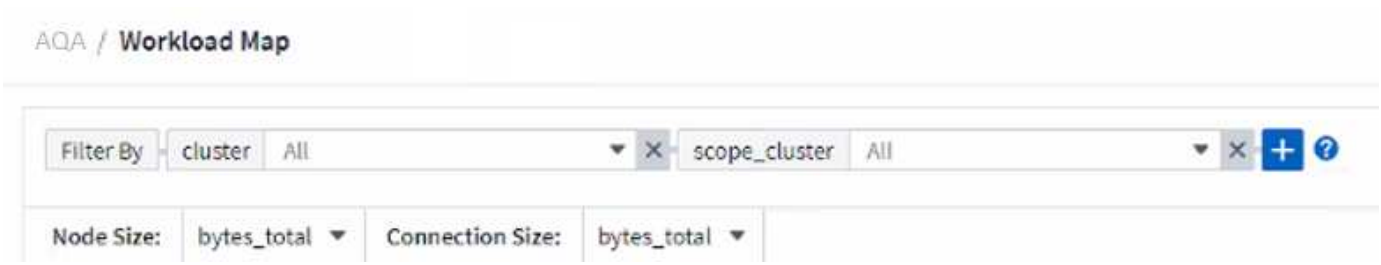
ワークロードの詳細とアラート

色で表示される円は、ワークロードの警告レベルまたは重大レベルのアラートを示します。問題の概要を表示するには円の上にマウスを移動するか、円をクリックして詳細を示すスライドアウト パネルを開きます。

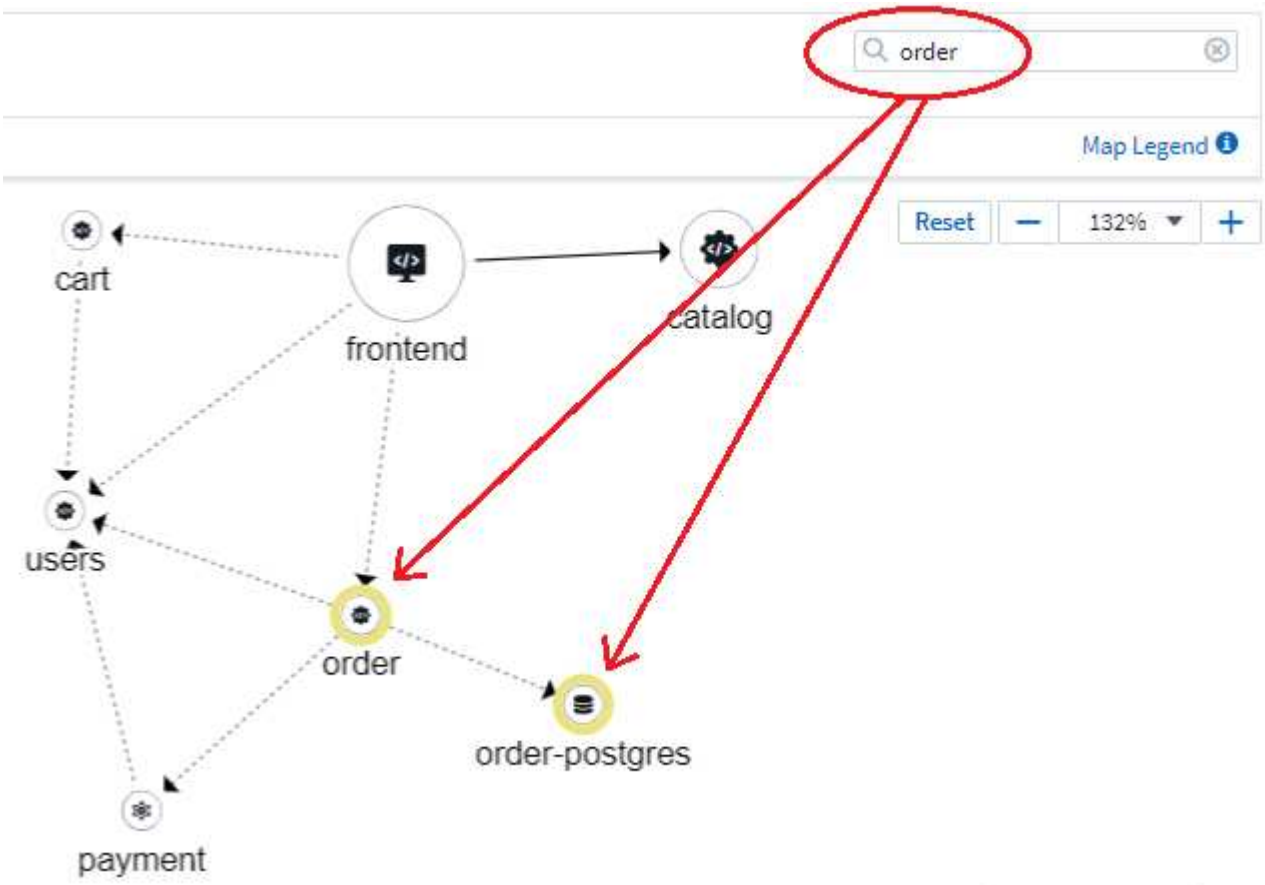


検索とフィルタリング

他のData Infrastructure Insights機能と同様に、必要な特定のオブジェクトまたはワークロード属性に焦点を絞るためのフィルターを簡単に設定できます。



同様に、[検索] 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強調表示されます。



ワークロードラベル

マップに表示されるワークロードの種類 (円形アイコンなど) を識別する場合は、ワークロード ラベルが必要です。ラベルは次のように生成されます。

- 実行中のサービス/アプリケーションの一般的な名前
- 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派生されます
  - ワークロードに期待されるラベル: 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

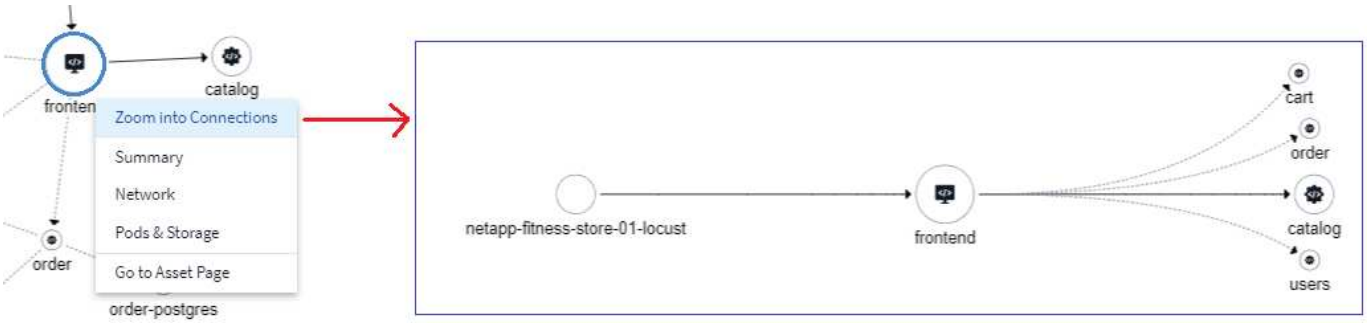
- バックエンド
- データベース
- キャッシュ
- キュー
- カフカ

- ソースが Kubernetes クラスターの外部にある場合:
  - Data Infrastructure Insights は、 DNS 解決された名前を解析してサービス タイプを抽出しようとします。

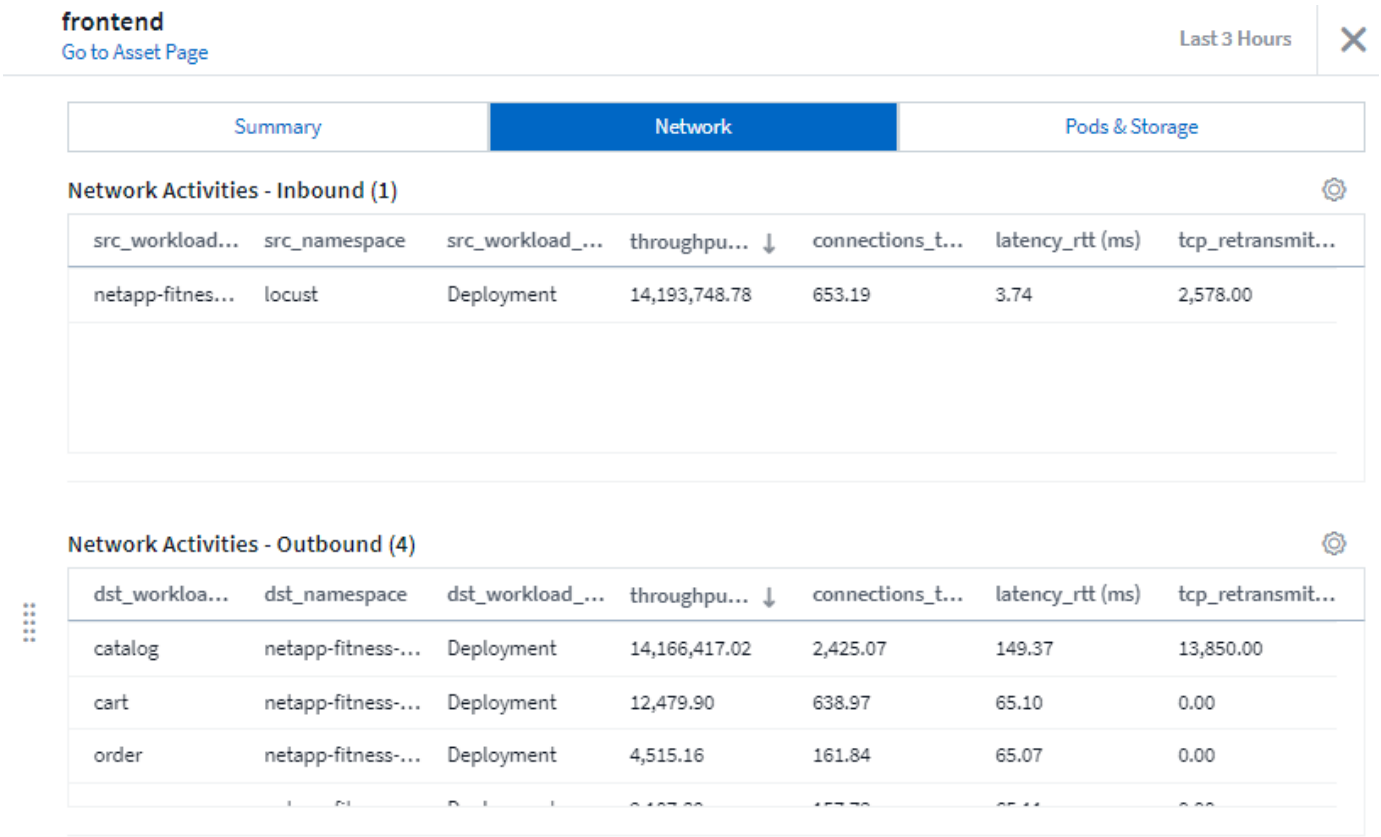
    たとえば、DNS 解決名が *s3.eu-north-1.amazonaws.com* の場合、解決された名前は解析され、サービス タイプとして *s3* が取得されます。

深く潜る

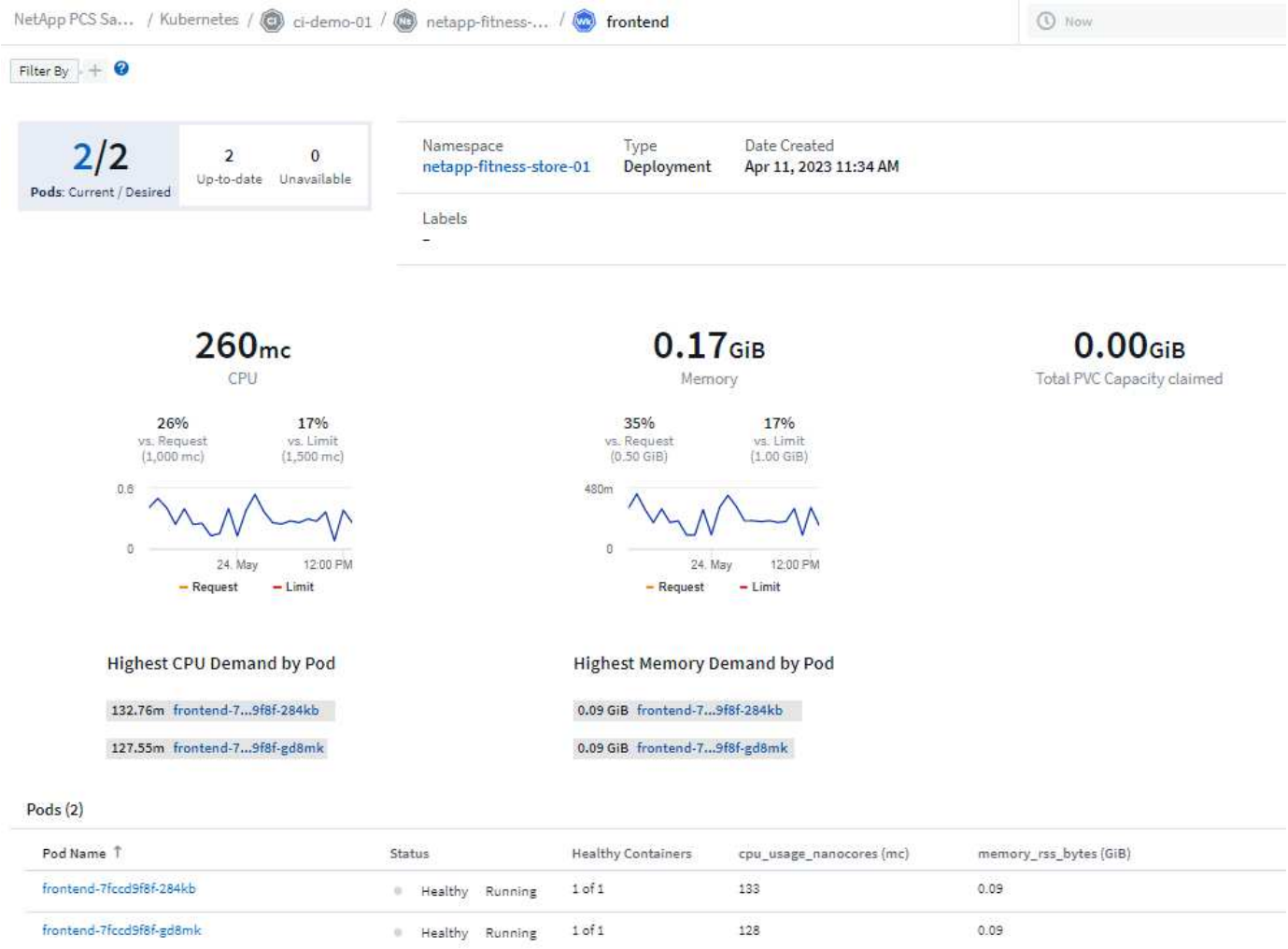
ワークロードを右クリックすると、さらに詳しく調べるための追加オプションが表示されます。たとえば、ここからズームインして、そのワークロードの接続を表示できます。



または、詳細スライドアウト パネルを開いて、[概要]、[ネットワーク]、または [ポッドとストレージ] タブを直接表示することもできます。



最後に、[アセット ページに移動] 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。



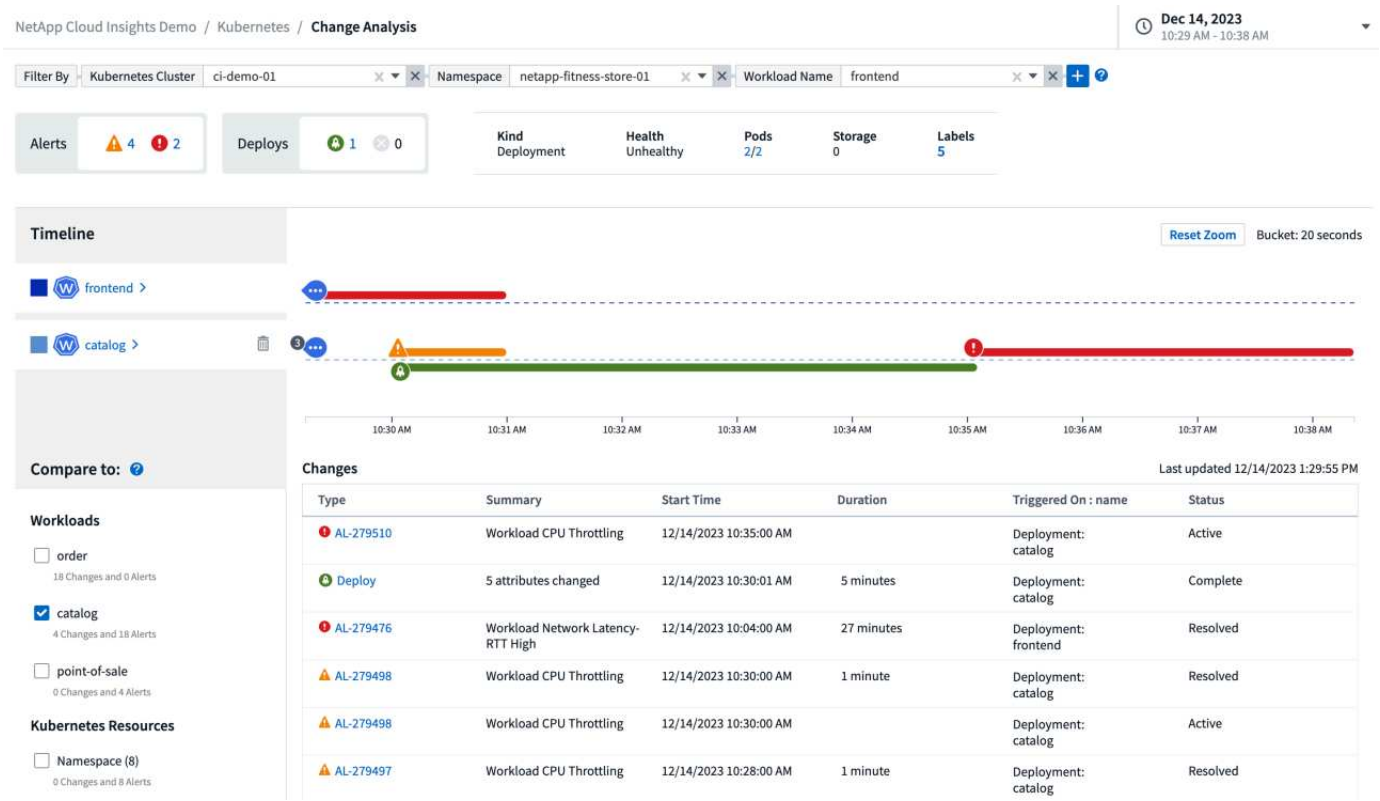
Kubernetes 変更分析

Kubernetes Change Analytics は、K8s 環境への最近の変更をワンストップで表示します。アラートと展開ステータスを簡単に確認できます。 Change Analytics を使用すると、すべてのデプロイメントと構成の変更を追跡し、それを K8s サービス、インフラストラクチャ、クラスターの健全性およびパフォーマンスと相関させることができます。

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、誤った構成変更により停止が発生する可能性があります。 Change Analytics は、ワークロードと構成の変更の健全性を表示して相関関係を調べるための単一のペインを提供することで、この作業を支援します。これは、動的な Kubernetes 環境のトラブルシューティングに役立つ可能性があります。

Kubernetes 変更分析を表示するには、**Kubernetes >** 変更分析 に移動します。



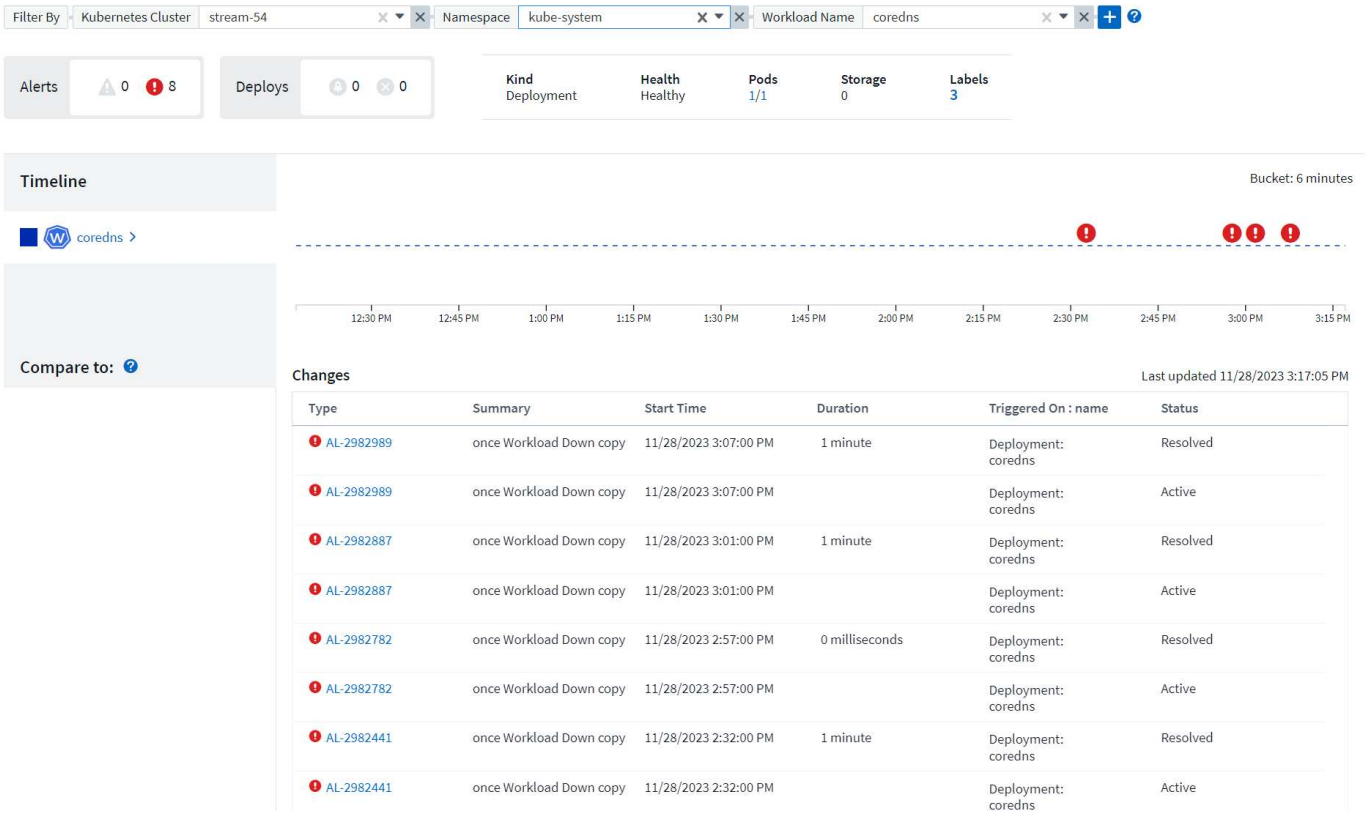
。

ページは、現在選択されているData Infrastructure Insightsの時間範囲に基づいて自動的に更新されます。時間範囲が狭いほど、画面の更新頻度が高くなります。

フィルタ

Data Infrastructure Insightsのすべての機能と同様に、変更リストのフィルタリングは直感的に行えます。ページの上部で、Kubernetes クラスター、名前空間、またはワークロードの値を入力または選択するか、[{+]] ボタンを選択して独自のフィルターを追加します。

特定のクラスター、名前空間、ワークロード (および設定したその他のフィルター) にフィルターすると、そのクラスターのその名前空間内のそのワークロードのデプロイメントとアラートのタイムラインが表示されます。グラフをクリックしてドラッグすると、さらに拡大して、より具体的な時間範囲に焦点を絞ることができます。



クイックステータス

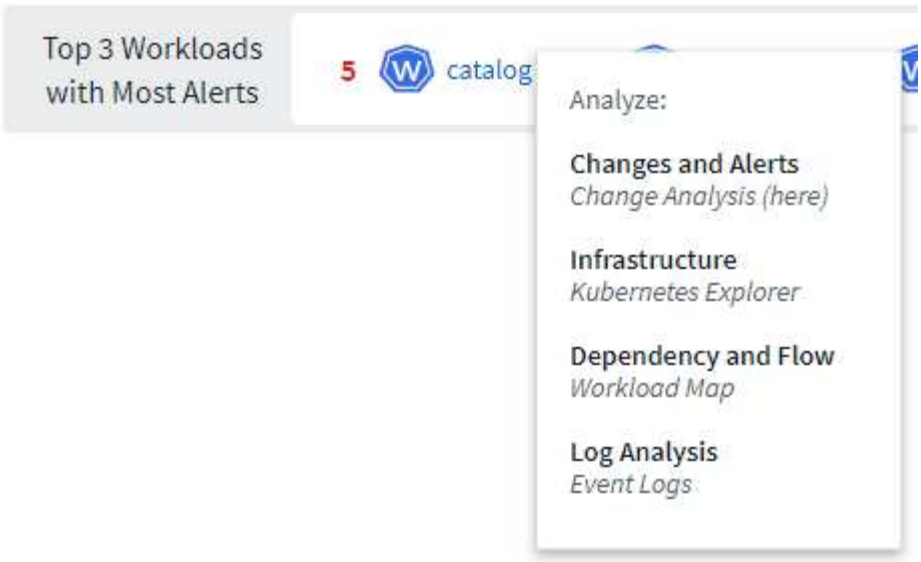
フィルタリング領域の下には、いくつかの高レベルインジケーターがあります。左側にはアラートの数（警告と重大）が表示されます。この数には、_アクティブ_アラートと_解決済み_アラートが含まれます。 _アクティブ_アラートのみを表示するには、「ステータス」のフィルターを設定し、「アクティブ」を選択します。



展開ステータスもここに表示されます。ここでも、デフォルトでは、開始、完了、および 失敗 のデプロイメントの数が表示されます。失敗したデプロイメントのみを表示するには、「ステータス」のフィルターを設定し、「失敗」を選択します。

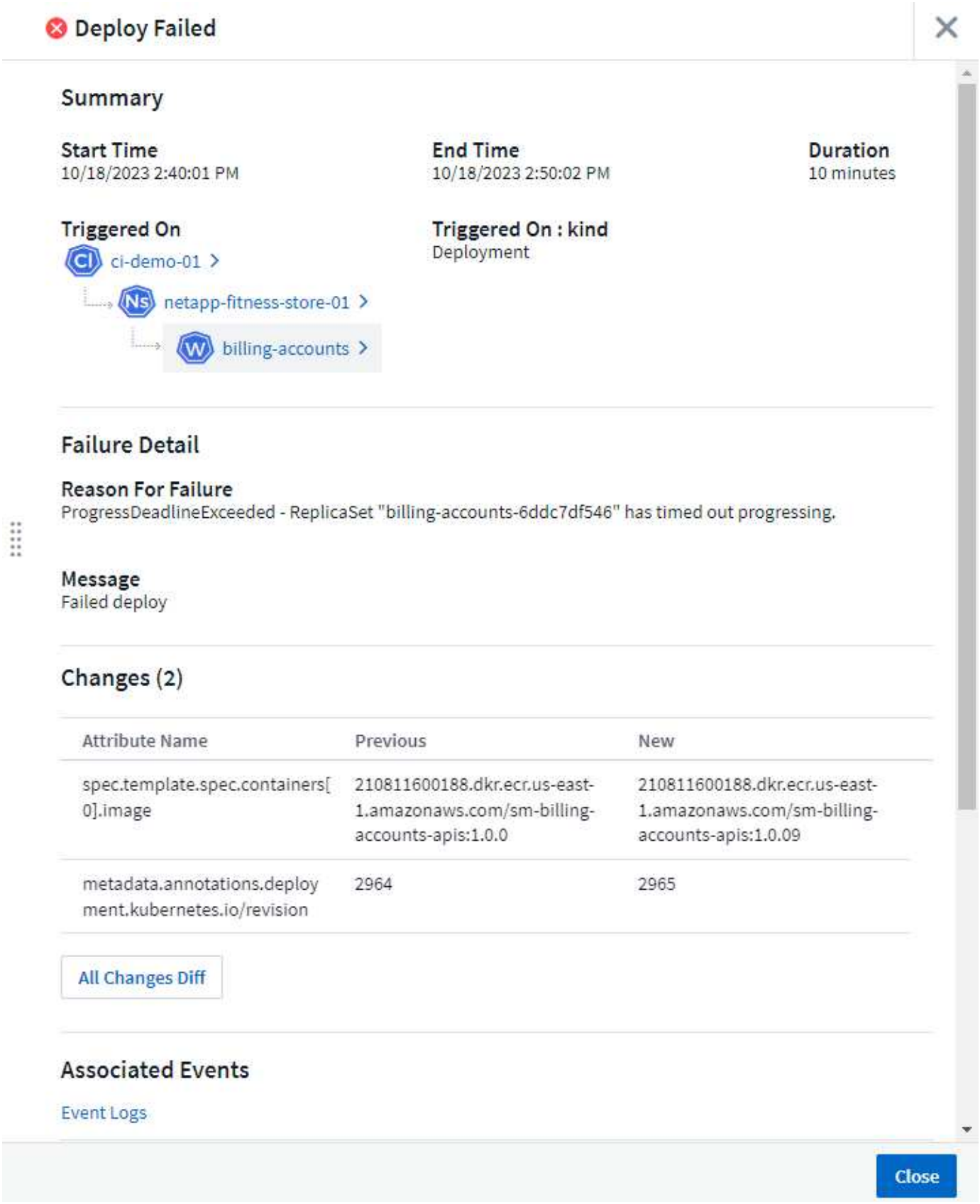


次に、アラートが最も多い上位 3 つのワークロードを示します。各ワークロードの横にある赤い数字は、そのワークロードに関連するアラートの数を示します。ワークロード リンクをクリックして、インフラストラクチャ (Kubernetes Explorer)、依存関係 (ワークロード マップ)、またはログ分析 (イベント ログ) を調べます。



詳細パネル

リスト内の変更を選択すると、変更の詳細を説明するパネルが開きます。たとえば、失敗したデプロイを選択すると、開始時刻と終了時刻、期間、デプロイがトリガーされた場所を含むデプロイの概要と、それらのリソースを調べ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、および関連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ーやアラートの視覚的なタイムラインを示すグラフなど、アラートに関する詳細が表示されます。

ONTAPエッセンシャル

ONTAP Essentials は、 ONTAP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 での作業時には、次の用語が使用されることがあります。

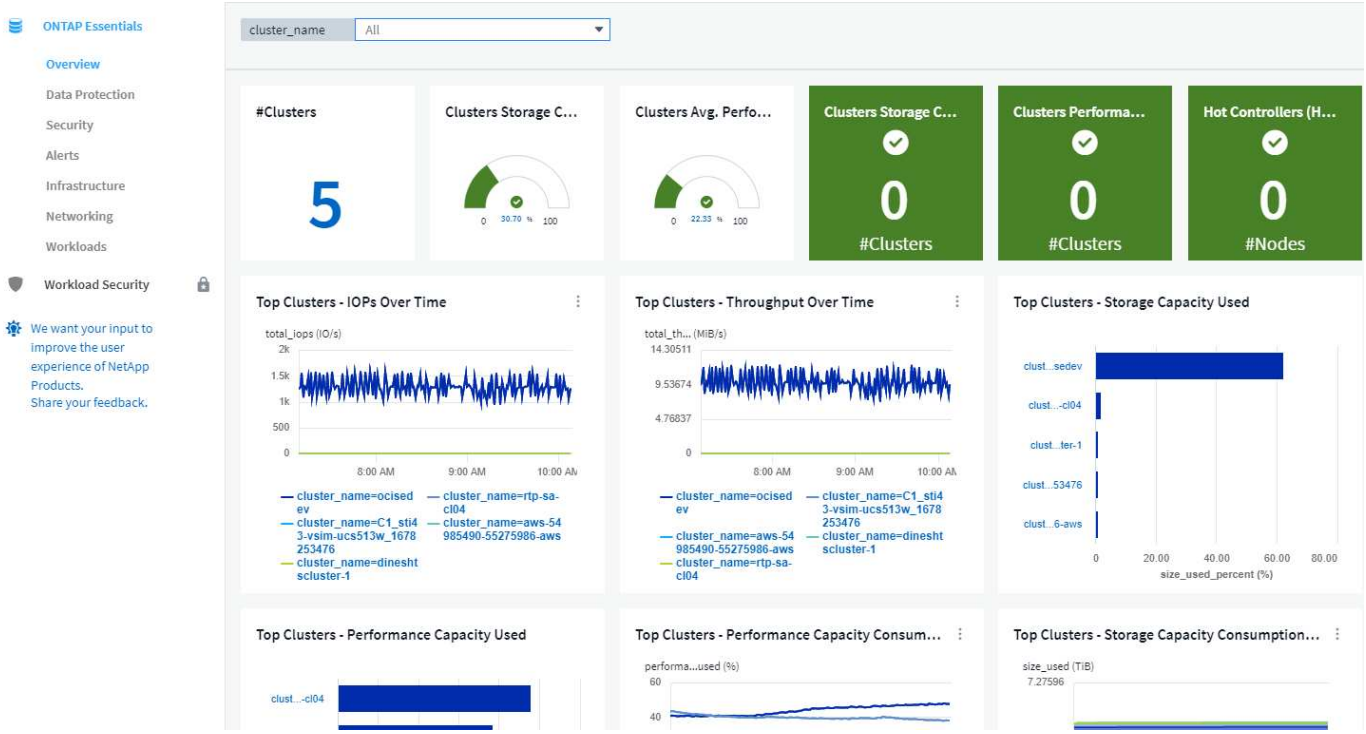
- インフラストラクチャ/インベントリ: ユーザーデータにストレージ/ネットワークサービスを提供するオブジェクト
- ワークロード: ユーザーにデータの読み取り/書き込みを行うためのインターフェースを提供するオブジェクト。
- データ保護: NetAppデータ保護テクノロジーを使用して保護できるオブジェクト

ONTAPに関連する追加の用語と定義については、"ONTAPデータコレクター"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、動作中のONTAPデータ コレクターが少なくとも 1 つ必要です。

概要

探索を開始するには、メインのData Infrastructure Insightsメニューから * ONTAP Essentials* を選択します。



*概要*ダッシュボードには、テナント上のクラスターの数、全体的な容量、パフォーマンスの割合などの有用な情報が表示されます。ストレージ容量またはパフォーマンス容量が不足するまでの予想日数に関する予測データも表示されます。さらに、インフラストラクチャ内のいずれかのコントローラの CPU 使用率が 65% を超えている場合 (フェイルオーバー時にクラスタが危険にさらされる可能性がある)、 ONTAP Essentials ではそれらのコントローラが「ホット」コントローラとして表示されます。

情報豊富なグラフにより、時間の経過に伴うパフォーマンスや容量使用状況の内訳を確認できます。これらの

グラフまたはデータ ポイントはそれぞれ、探索または調査の開始点として使用できます。

注: 「満杯までの日数」の数値が「0」(ゼロ) の場合、満杯までの日数が 90 日を超えると見積もられることを示します。つまり、システムの容量がすぐに不足する危険はありません。

データ保護

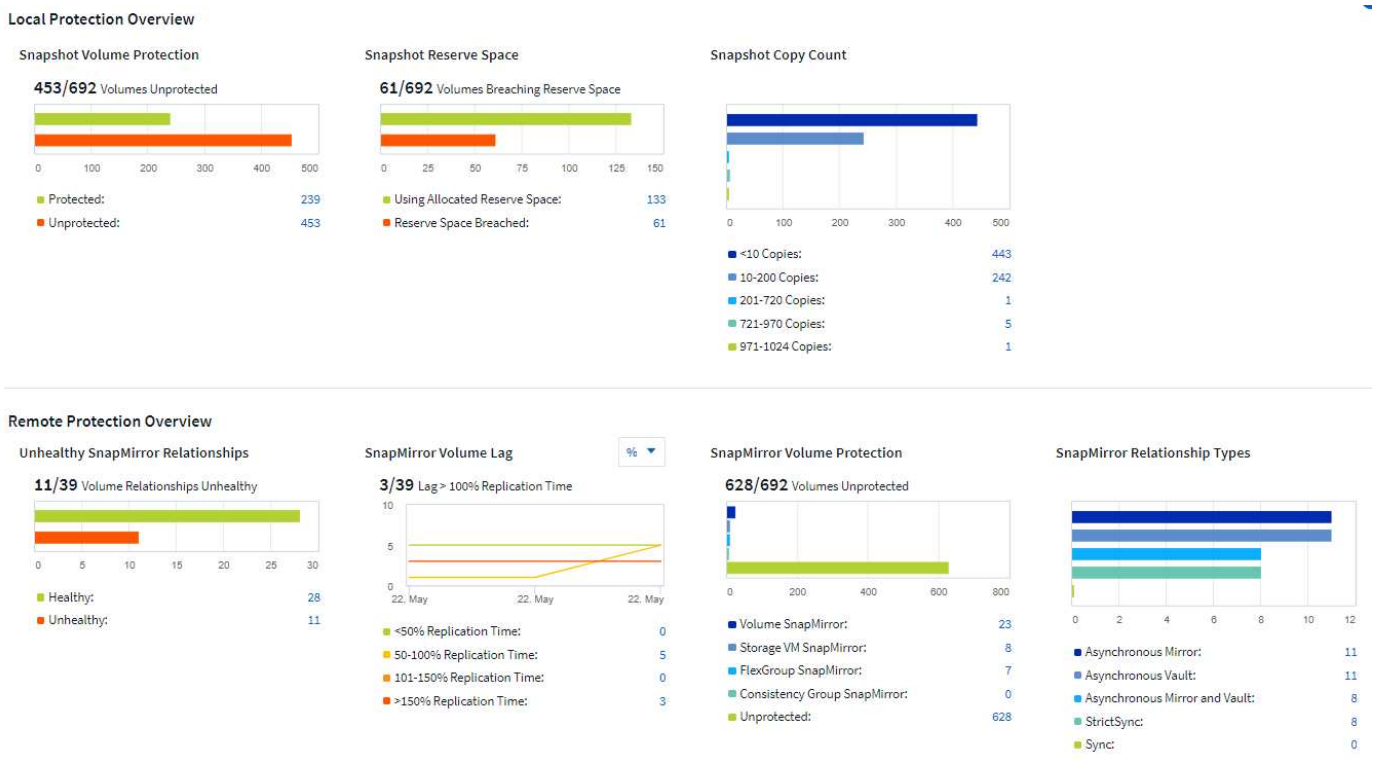
データ保護 ページには、スナップショット コピー または * SnapMirrorポリシー* によって保護されているボリュームのステータスが表示されます。

ローカル保護の概要 セクションでは、スナップショット コピーによって保護されているボリュームに関する次の情報がグラフに表示されます。

- スナップショット コピーによって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。
- スナップショット コピーの予約領域を使用しているか、その領域を超えているボリュームの数。
- スナップショット コピー数の特定の範囲 (つまり、10 コピー未満、10 ～ 200 コピーなど) 内のボリュームの数。

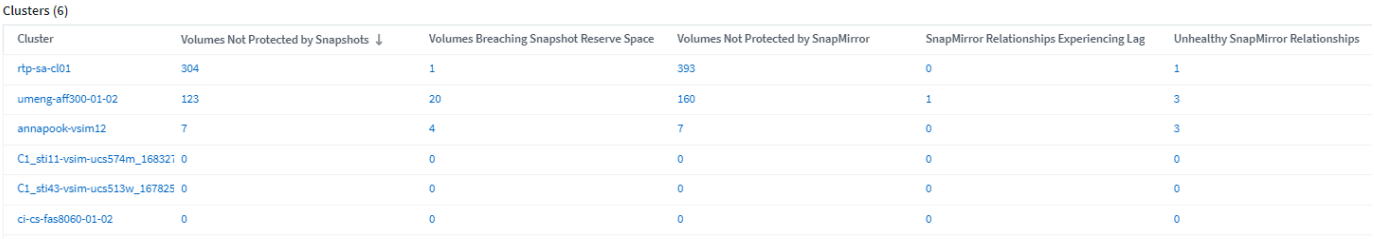
リモート保護の概要 セクションでは、 SnapMirrorポリシーによって保護されているボリュームに関連する情報がグラフに表示されます。

- 正常な SnapMirror 関係と異常なSnapMirror関係の数。
- 遅延ステータスに基づいて、リカバリポイント目標 (RPO) の遅延が発生しているSnapMirror関係の数。
- Volume SnapMirror、SVMDR 関係、 FlexGroup SnapMirror関係、 SnapMirror Business Continuity (SMBC) 整合性グループ関係などのSnapMirrorボリューム保護タイプによって保護されている関係、および保護されていないボリュームの数。
- 非同期ミラー、非同期ボールト、非同期ミラーボールト、StrictSync、同期などのSnapMirror関係タイプによって保護されている関係の数。



ページの下部にある [クラスター] グリッドには、次の詳細が表示されます。

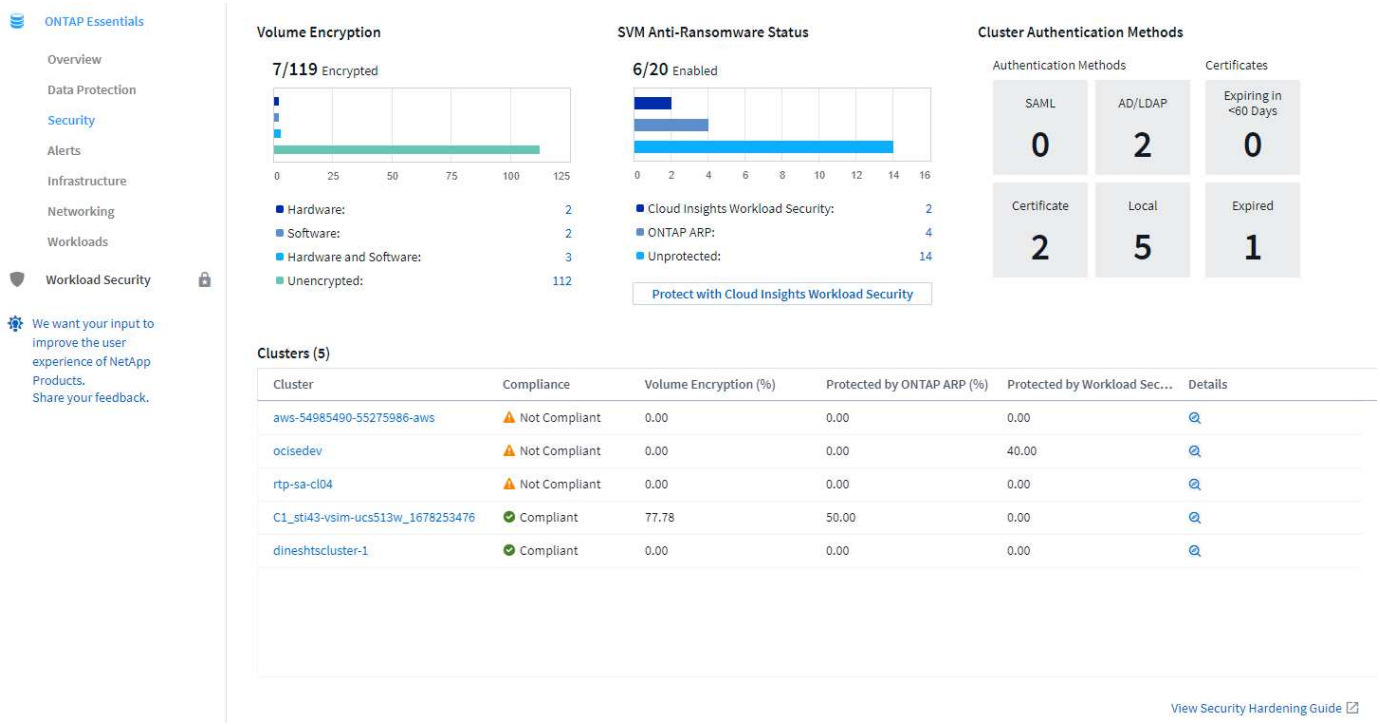
- スナップショットによって保護されていないボリューム。
- スナップショット予約領域を超えるボリューム。
- ボリュームは snapmirror ポリシーによって保護されておらず、遅延が発生しています。
- SnapMirror関係が正常ではありません。



セキュリティ

セキュリティダッシュボードでは、ハードウェアおよびソフトウェアによるボリューム暗号化、ファイル改ざん対策の状況、クラスター認証方法などのグラフが表示され、現在のセキュリティ状況を瞬時に確認できます。セキュリティ基準は、"* ONTAP 9 向けNetAppセキュリティ強化ガイド*"で定義された推奨事項に基づいて評価されます。

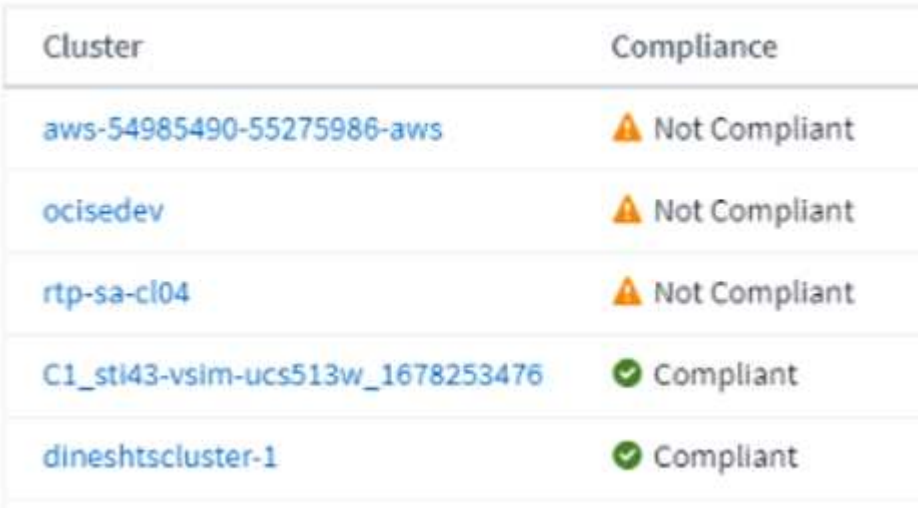
暗号化またはファイル改ざん防止カウントのいずれかを選択して、環境を詳しく調べます。



ONTAP Essentials Security 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。参照"クラスターコンプライアンスカテゴリ"詳細については、こちらをご覧ください。 ONTAP Essentials は、コンプライアンスを判断するために次のモニターを使用します。

モニター名	属性名（クラスターの詳細に表示される）	属性準拠値
FIPS モードが無効	FIPSモード	有効
SSH のクラスタ安全でない暗号	セキュアな SSH 設定	はい
Telnet プロトコルが有効	Telnet	無効
リモートシェルが有効	リモート シェル	無効
デフォルトのローカル管理ユーザが有効	デフォルトの管理ユーザ	無効
MD5ハッシュパスワード	MD5の使用	いいえ
クラスタ ピア通信が暗号化されていない	クラスタ ピアリング	暗号化/ピアなし
AutoSupport HTTPS転送が無効	HTTPSを使用したAutoSupport	はい
NTPサーバーが設定されていません	ネットワーク タイム プロトコル	設定
NTP サーバ数が不足	ネットワーク タイム プロトコル	設定
クラスターログインバナーが無効です	ログイン バナー	有効
ログ転送が暗号化されていない	ログ転送を暗号化	はい

上記のモニターが無効になっている場合、クラスターの詳細では、対応するセキュリティ コンプライアンス属性の値が「未チェック」と表示されることに注意してください。

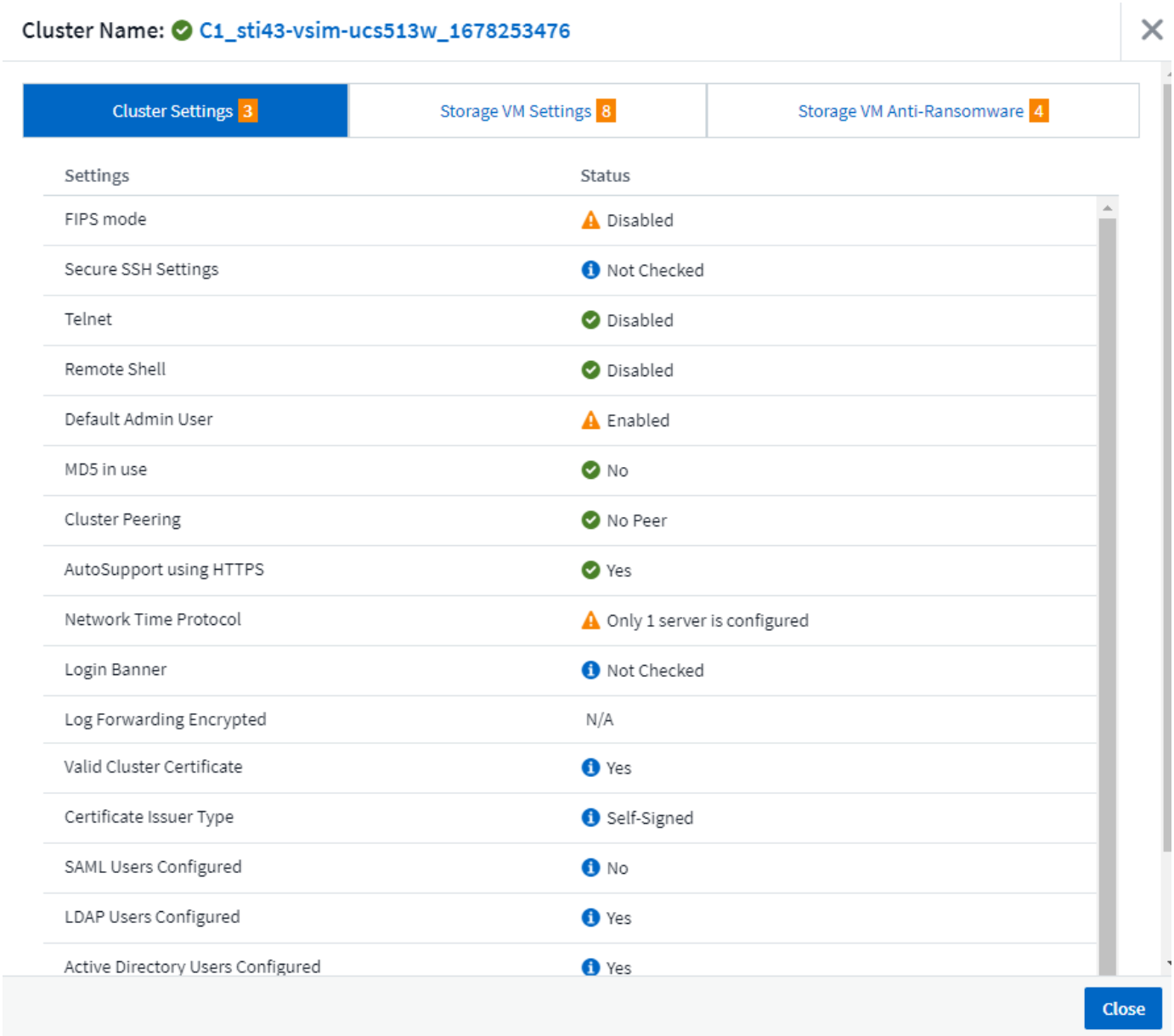


SVM の場合、セキュリティ ダッシュボードは次のモニターを確認します。

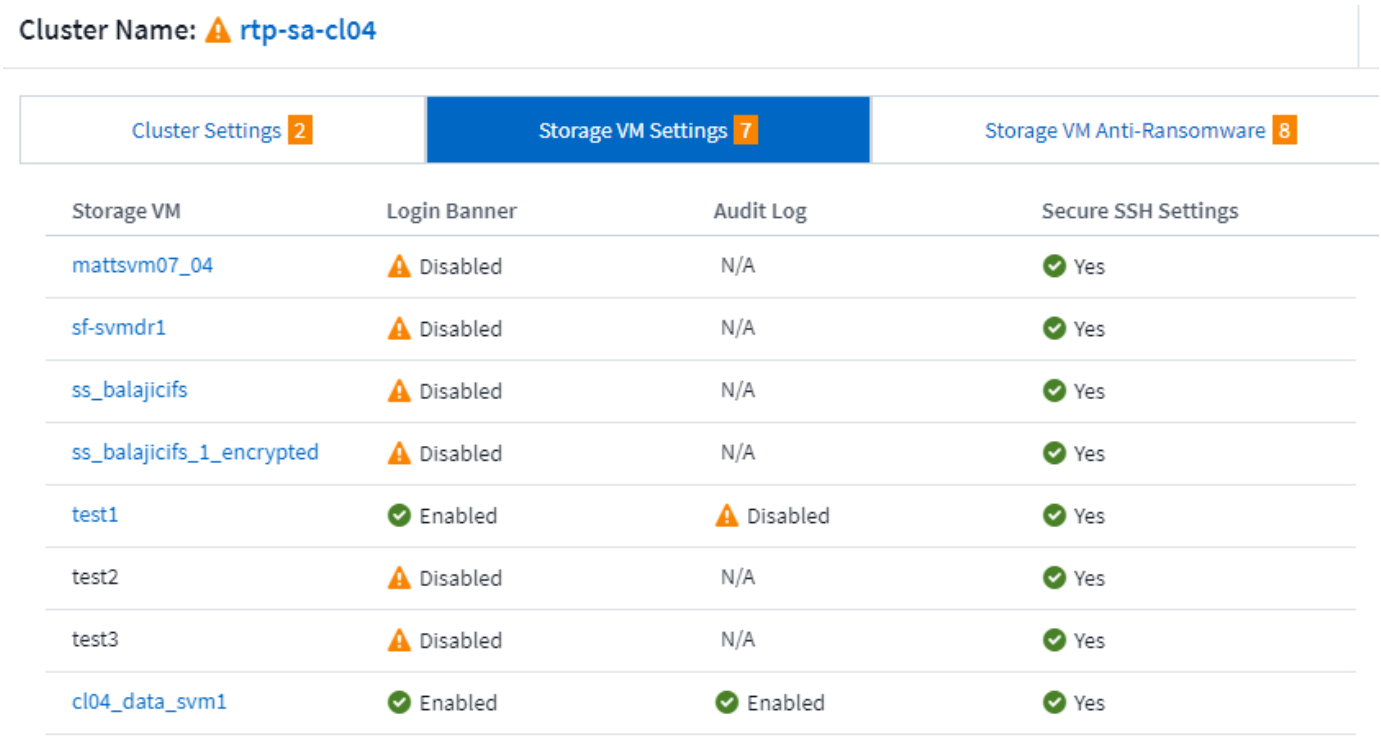
モニター名	属性名（ストレージ**VM**設定に表示される）	属性準拠値
ストレージ VM SSH の安全でない暗号	セキュアな SSH 設定	はい
ストレージ VM ログイン バナーが無効になっています	ログイン バナー	有効
ストレージ VM 監査ログが無効	監査ログ	有効

クラスター リストで、各クラスターの [詳細の表示] を選択すると、クラスター、ストレージ *VM*、_ランサムウェア対策 の現在の設定を示す「スライドアウト」パネルが開きます。

クラスターの詳細には、接続ステータス、証明書情報などが含まれます。



ストレージ VM の詳細には、監査と SSH 情報が表示されます。

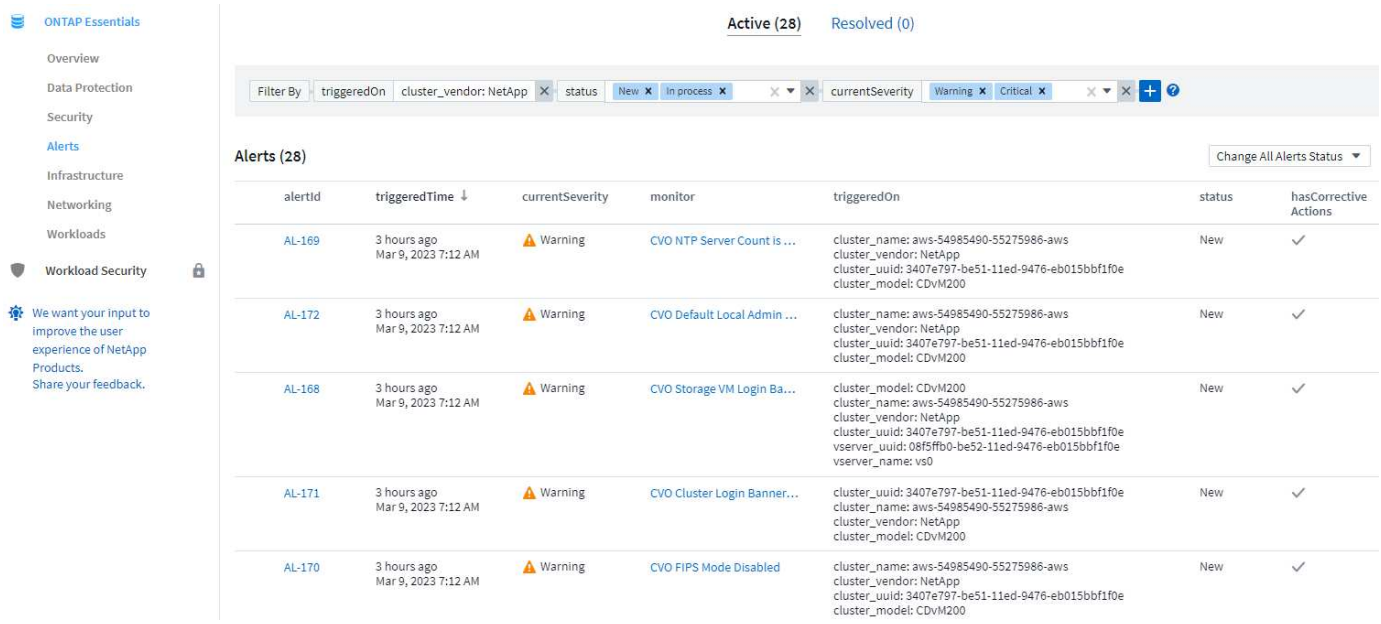


ランサムウェア対策の詳細には、ストレージ VM が ONTAP のランサムウェア対策保護またはData Infrastructure Insightsワークロード セキュリティによって保護されているかどうかが表示されます。 ONTAP ARP 列には、 ONTAPシステムで設定されている ONTAP のオンボード ランサムウェア対策の現在のステータスが表示されることに注意してください。その列で「保護」を選択すると、 Data Infrastructure Insightsワークロード セキュリティが有効になりま
す。



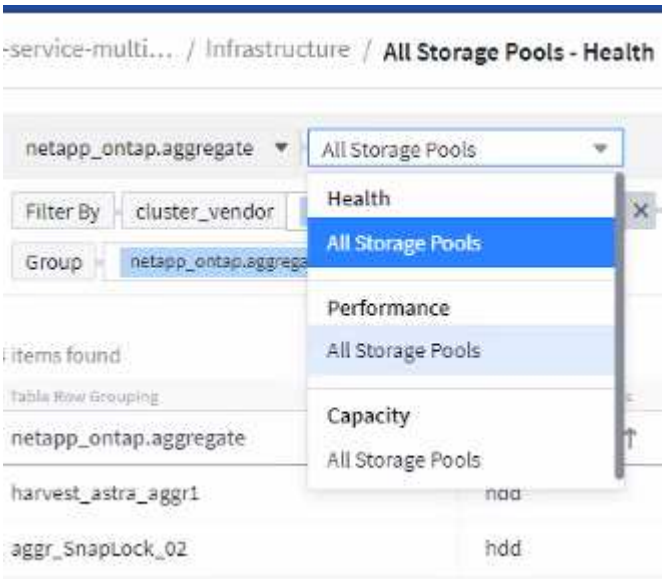
アラート

ここでは、テナント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ドリルダウンできます。解決されたアラートを表示するには、[解決済み] タブを選択します。

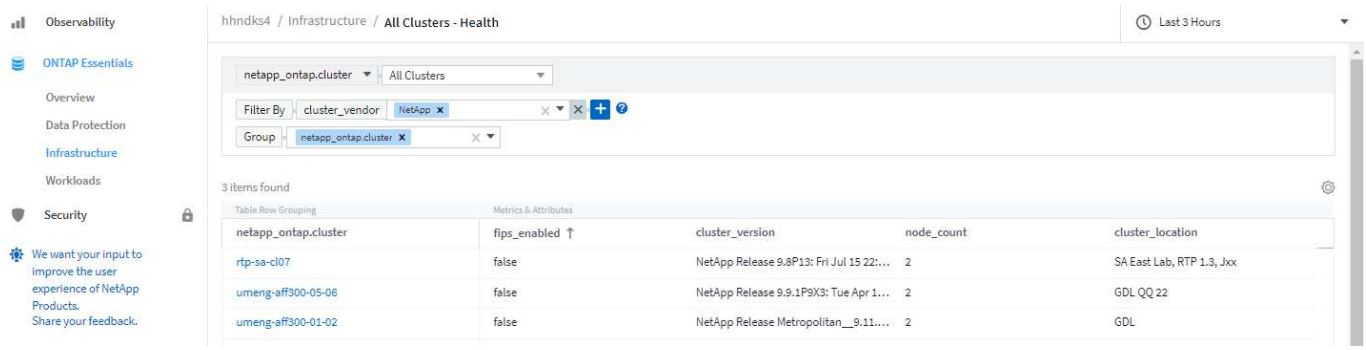


インフラ

ONTAP Essentials の **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) クエリを使用して、クラスタの健全性とパフォーマンスを確認できます。調査するオブジェクト タイプ (クラスター、ストレージ プールなど) を選択し、ヘルス情報またはパフォーマンス情報のどちらを表示するかを選択します。フィルターを設定して、個々のシステムを詳細に調べます。

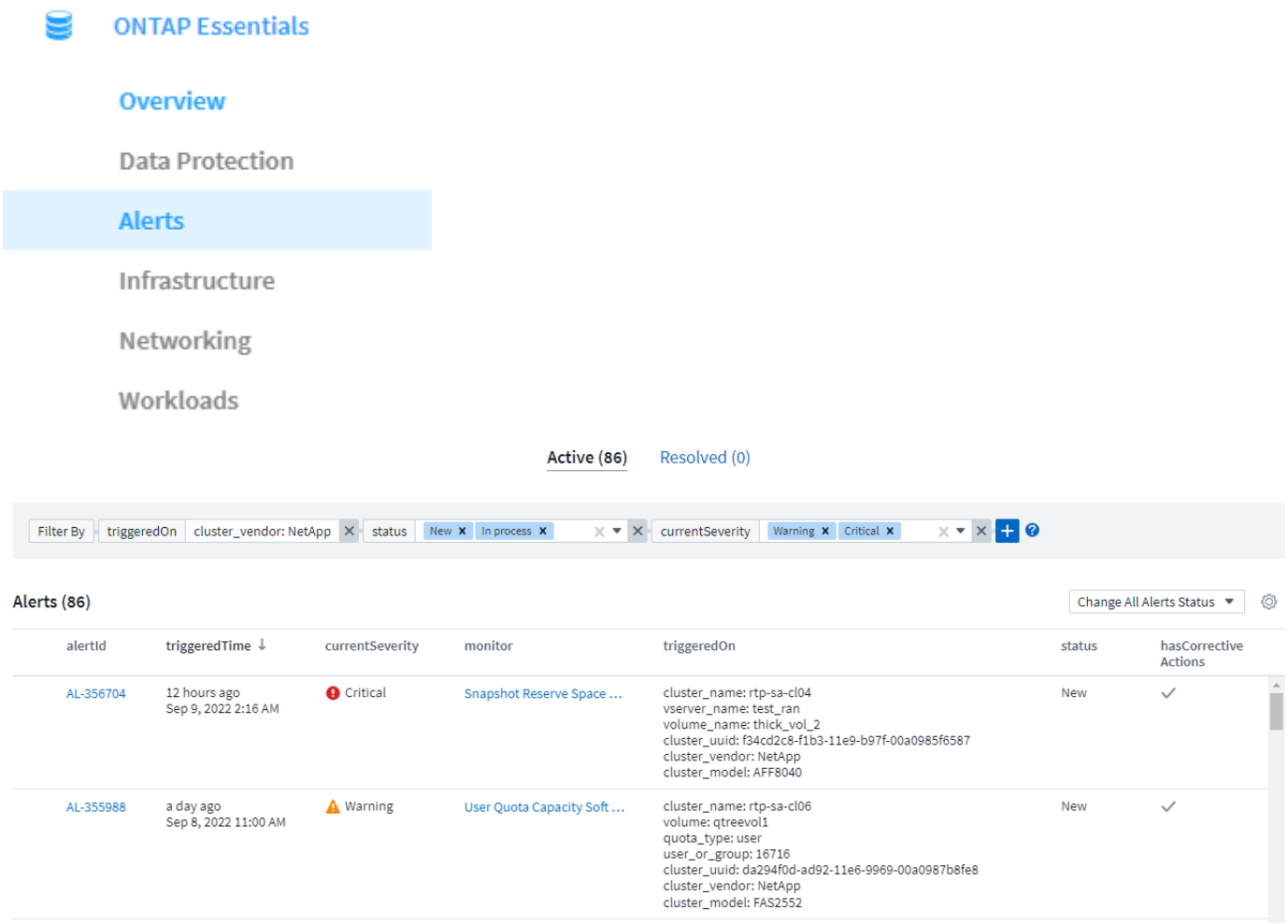


クラスターの健全性を示すインフラストラクチャ ページ
:



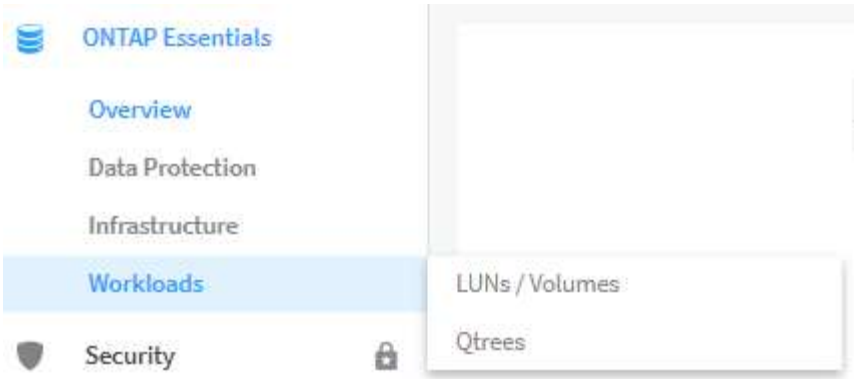
ネットワーク

ONTAP Essentials Networking を使用すると、FC、NVME FC、イーサネット、iSCSI インフラストラクチャを詳細に把握できます。これらのページでは、クラスター内のポートやそのノードなどを調べることができます。



ワークロード

テナント上の LUN/ボリューム、NFS または SMB 共有、または Qtree 上のワークロードを表示および調査します。



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

Data Infrastructure InsightsAPI

Data Infrastructure Insights API を使用すると、 NetApp の顧客と独立系ソフトウェア ベンダー (ISV)は、Data Infrastructure 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。

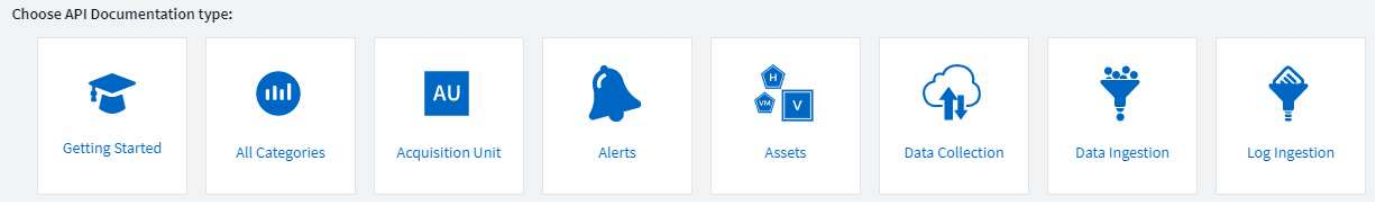
Data Infrastructure Insights"機能セットの役割"アクセスできる API を決定します。ユーザー ロールとゲスト ロールには、管理者ロールよりも権限が少なくなります。たとえば、Monitor and Optimize では管理者ロールを持ち、Reporting ではユーザーロールを持っている場合、データ ウェアハウスを除くすべての API タイプを管理できます。

APIアクセスの要件

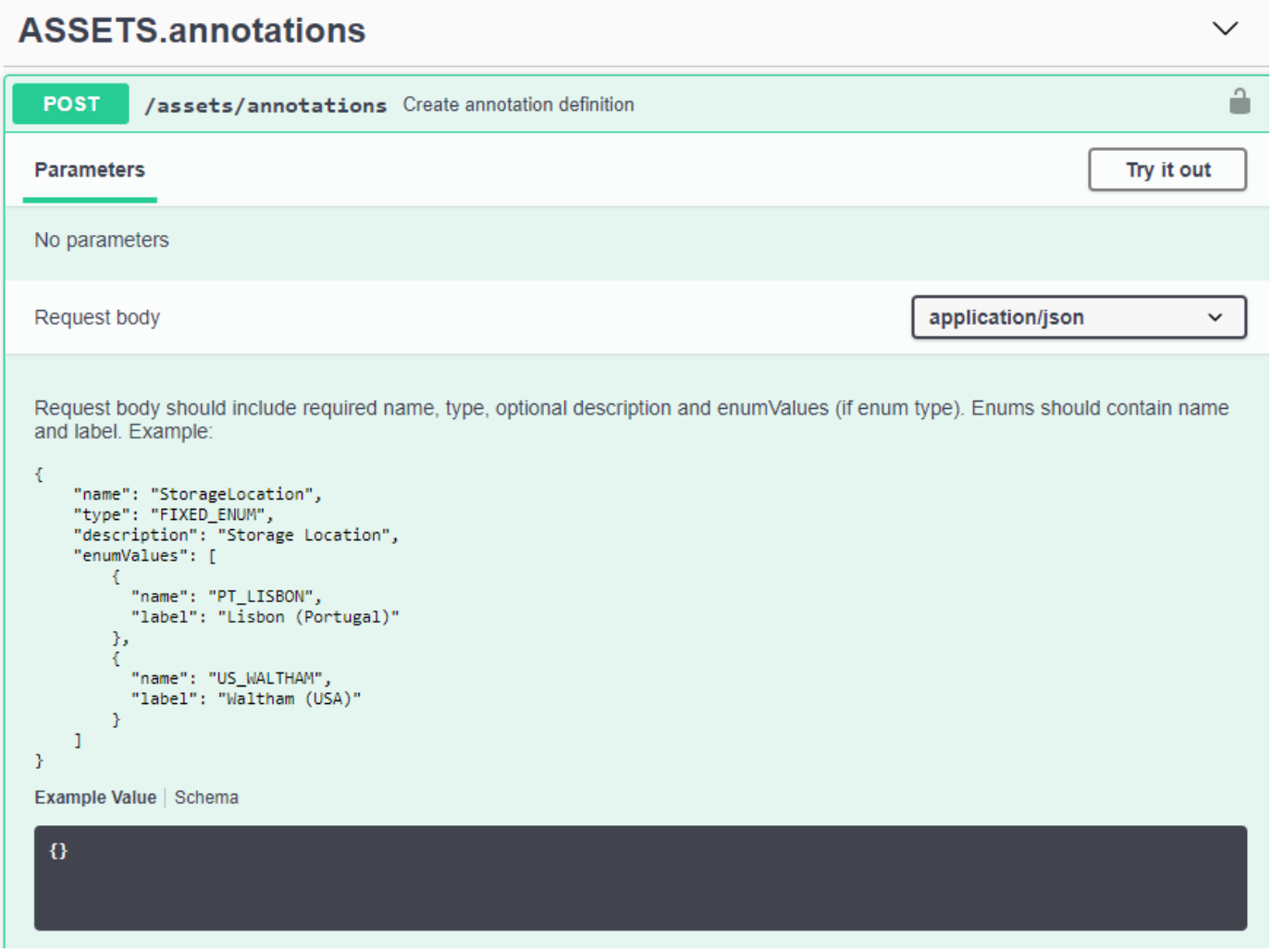
- アクセスを許可するには、API アクセス トークン モデルが使用されます。
- API トークンの管理は、管理者ロールを持つData Infrastructure Insightsユーザーによって実行されます。

APIドキュメント（Swagger）

最新の API 情報は、Data Infrastructure Insightsにログインし、管理 **> API** アクセス に移動すると見つかります。 **API** ドキュメント リンクをクリックします。



API ドキュメントは Swagger ベースであり、API の簡単な説明と使用方法の情報を提供し、テナントで試用することができます。ユーザー ロールやData Infrastructure Insightsエディションに応じて、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、読み取り権限や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。指定されたタイプのすべての API はアクセス トークンに対して有効です。各トークンにはユーザー名やパスワードはありません。

アクセス トークンを作成するには:

- *管理 > APIアクセス*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
  - APIタイプを選択
  - このAPIアクセスに付与する権限を指定します
  - トークンの有効期限を指定する

トークンは、作成プロセス中にクリップボードにコピーして保存するためにのみ使用できます。トークンは作成後に取得することはできないため、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に求められます。

トークンを無効化、有効化、取り消しできます。無効になっているトークンを有効にすることができます。

トークンは、顧客の観点から API への汎用アクセスを許可し、独自のテナントの範囲内で API へのアクセスを管理します。顧客管理者は、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付与したり取り消したりできます。

アプリケーションは、ユーザーが正常に認証してアクセスを承認するとアクセス トークンを受け取り、ターゲット API を呼び出すときにアクセス トークンを資格情報として渡します。渡されたトークンは、トークンの所有者が API にアクセスし、承認時に付与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することを承認されたことを API に通知します。

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、ストレージ アセットを取得するには、次を使用します。

```
 curl https://<tenant_host_name>/rest/v1/assets/storages -H 'X-
CloudInsights-ApiKey:<API_Access_Token>'
```

ここで、_<API_Access_Token>_ は、API アクセスの作成時に保存したトークンです。

使用したい 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、現在次のタイプが含まれています。

- ASSETS 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: 最上位レベル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クエリを取得および管理します。
  - インポート: 注釈またはアプリケーションをインポートし、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 または完全な名前を知らなくても、特定のオブジェクトを検索します。
- DATA COLLECTION タイプは、データ コレクターを取得および管理するために使用されます。
- DATA INGESTIONタイプは、Telegrafエージェントなどから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。
- LOG INGESTIONはログデータを取得および管理するために使用されます

今後、追加のタイプや API が利用可能になる可能性があります。最新のAPI情報は、"API Swaggerドキュメント" 。

ユーザーがアクセスできるAPIの種類は、"ユーザ ロール"各Data Infrastructure Insights機能セット (監視、ワークロード セキュリティ、レポート) に備わっています。

インベントリトラバーサル

このセクションでは、Data Infrastructure Insightsオブジェクトの階層を移動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、リクエスト内で一意のURL（JSONでは「self」と呼ばれます）によって識別され、オブジェクトタイプと内部IDの知識が必要です。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 URL は次のようになります。

```
https://mysite.c01.cloudinsights.netapp.com/rest/v1/assets/storages
```

子供と関連オブジェクト

ストレージなどの最上位オブジェクトは、他の子オブジェクトや関連オブジェクトに移動するために使用できます。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」と連結します。次に例を示します。

```
https://<tenant>/rest/v1/assets/storages/4537/disks
```

拡大

多くの API コマンドは、オブジェクトに関する追加の詳細または関連オブジェクトの URL を提供する **expand** パラメータをサポートしています。

共通する展開パラメータは *expands* です。応答には、オブジェクトに使用可能なすべての特定の展開のリストが含まれます。

たとえば、次のように要求するとします。

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=_expands
```

API は次のように、オブジェクトの利用可能なすべての展開を返します。

```
{
    "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 パラメータは、複数のネストされた属性をサポートします。例:

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=performance,storageResources.storage
```

展開を使用すると、1 つの応答で多くの関連データを取り込むことができます。
NetApp、一度に大量の情報を要求しないようにアドバイスしています。これにより、パフォーマンスが低下する可能性があります。

これを防ぐために、最上位レベルのコレクションのリクエストは拡張できません。たとえば、すべてのストレージ オブジェクトのデータ拡張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、展開する特定のオブジェクトを選択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、多数の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 は、1 時間ごとに (デフォルト) パフォーマンス サンプルを集計して要約します。

API を使用すると、サンプルと要約データの両方にアクセスできます。パフォーマンス データを持つオブジェクトの場合、パフォーマンスの概要は *expand=performance* として利用できます。パフォーマンス履歴の時系列は、ネストされた *expand=performance.history* を通じて利用できます。

パフォーマンス データ オブジェクトの例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
- ストレージプールパフォーマンス
- ポートパフォーマンス
- ディスクパフォーマンス

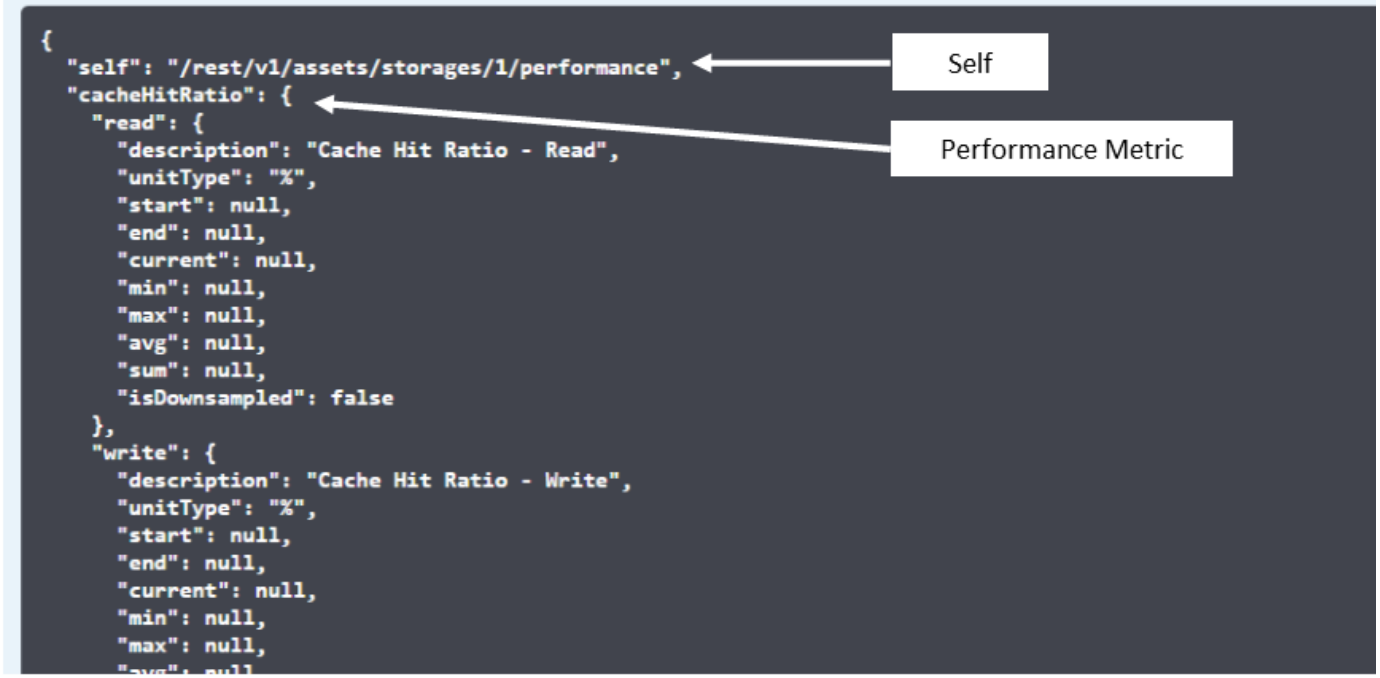
パフォーマンス メトリックには説明とタイプがあり、パフォーマンス サマリーのコレクションが含まれています。たとえば、レイテンシ、トラフィック、レートなどです。

パフォーマンス サマリーには、説明、単位、サンプルの開始時刻、サンプルの終了時刻、および時間範囲 (1 時間、24 時間、3 日間など) にわたって単一のパフォーマンス カウンターから計算された集計値 (現在値、最小値、最大値、平均値など) のコレクションが含まれます。

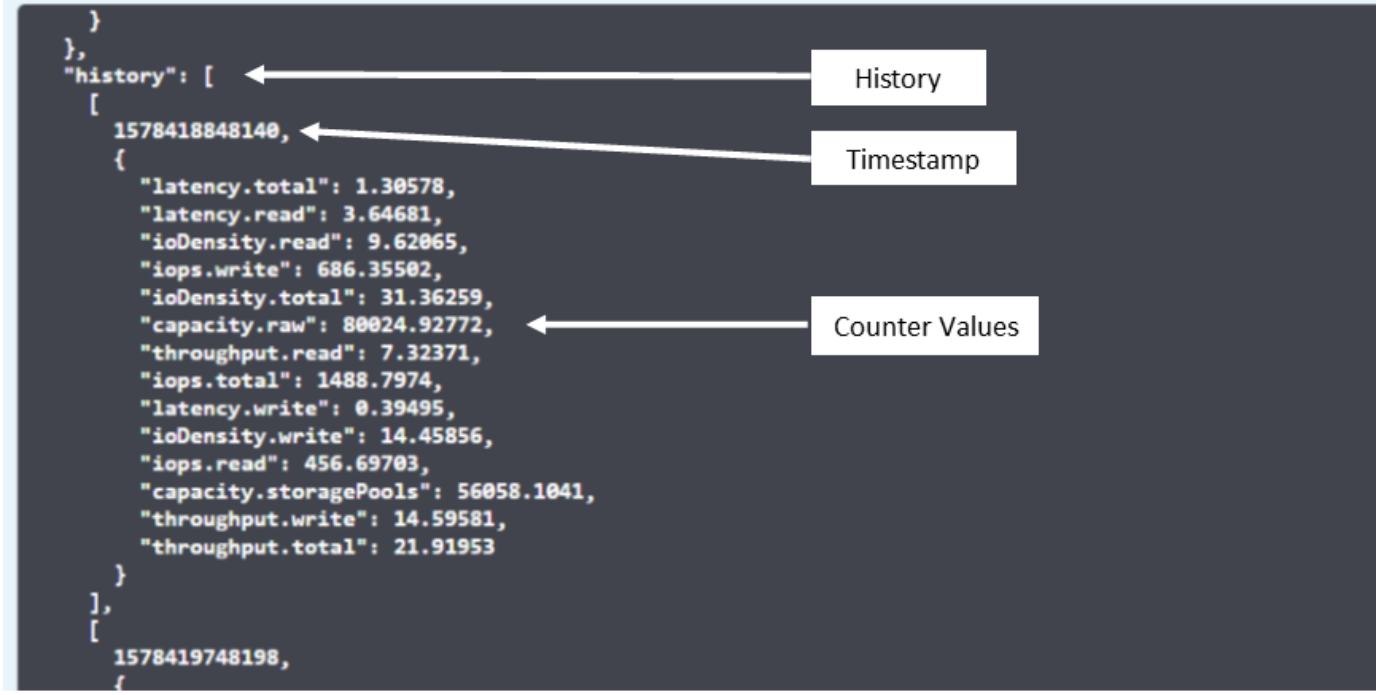
https://tenant.cloudinsights.netapp.com/rest/v1/assets/storages/1/performance?expand=history

Details

Response body



Response body



結果として得られるパフォーマンス データ ディクショナリには、次のキーが含まれます。

- 「self」はオブジェクトの一意のURLです

- 「履歴」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。
- その他のすべての辞書キー (「diskThroughput」など) は、パフォーマンス メトリックの名前です。

各パフォーマンス データ オブジェクト タイプには、固有のパフォーマンス メトリックのセットがあります。たとえば、仮想マシン 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 ディクショナリに提示される特定の「performanceCategory」に属します。 Data Infrastructure Insights は、このドキュメントの後半にリストされているいくつかのパフォーマンス メトリック 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 メトリックの人間が判読できる説明である「説明」フィールドと、パフォーマンス サマリー カウンター エントリのセットも含まれます。

パフォーマンス サマリー カウンターは、パフォーマンス カウンターを要約したものです。カウンターの最小値、最大値、平均値などの一般的な集計値と、最新の観測値、要約データの時間範囲、カウンターの単位タイプ、データのしきい値が表示されます。しきい値のみがオプションであり、残りの属性は必須です。

パフォーマンス サマリーは、次の種類のカウンターで利用できます。

- 読み取り – 読み取り操作の概要
- 書き込み – 書き込み操作の概要
- 合計 – すべての操作の概要。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、他の操作が含まれることもあります。
- 合計最大値 – すべての操作の概要。これは指定された時間範囲内の最大合計値です。

オブジェクトパフォーマンスメトリック

API は、テナント上のオブジェクトの詳細なメトリックを返すことができます。次に例を示します。

- IOPS (1 秒あたりの入出力要求数)、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 メトリック。
- トラフィック使用率、BB クレジット ゼロ データ、ポート エラーなどのスイッチ パフォーマンス メトリック。

参照"API Swaggerドキュメント"各オブジェクト タイプのメトリックに関する情報。

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ー マップのペアのリストとしてパフォーマンス データ内に表示されます。

履歴カウンターは、パフォーマンス メトリック オブジェクト名に基づいて名前が付けられます。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.read」、「diskThroughput.write」、「diskThroughput.total」という名前のキーが含まれます。

タイムスタンプは UNIX 時間形式です。

以下は、ディスクのパフォーマンス データ JSON の例です。

```
"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

容量属性を持つオブジェクトは、基本データ型と CapacityItem を使用して表現します。

容量項目

CapacityItem は単一の論理容量単位です。親オブジェクトによって定義された単位で「value」と「highThreshold」を持ちます。また、容量値の構築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、100 TB のストレージ プールの合計容量は、値が 100 の CapacityItem になります。内訳には、「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ることが示される場合があります。

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。クライアントはこれを使用して、許容される構成範囲外の値に対してアラートまたは視覚的なキューを生成できます。

以下は、複数の容量カウンターを持つ StoragePool の容量を示しています。



検索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 への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リストが含まれます。タイプは、ストレージ、ホスト、データストアなど、インベントリとは異なる資産タイプです。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。

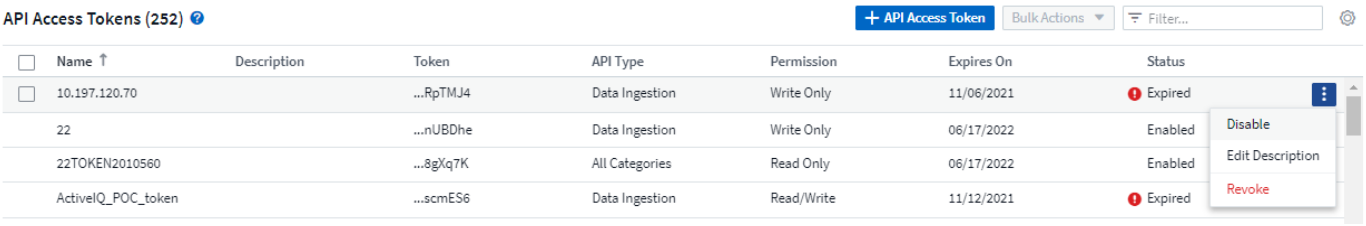
Data Infrastructure Insights は、サードパーティのオーケストレーション、ビジネス管理、変更管理、チケット発行システム、およびカスタム CMDB 統合との統合を可能にする拡張可能な (オープンな) ソリューションです。

Cloud Insight の RESTful API は、データのシンプルかつ効率的な移動を可能にするとともに、ユーザーがデータにシームレスにアクセスできるようにする主要な統合ポイントです。

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、「無効」を選択します。同じメニューを使用して [有効にする] を選択すると、いつでもトークンを再度有効にすることができます。

API トークンを完全に削除するには、メニューから「取り消し」を選択します。取り消されたトークンを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ローテーション

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 トークンの有効期限が切れると、ユーザーは新しいトークン (読み取り/書き込み権限を持つ データ インジェスチョン タイプ) を生成し、期限切れのトークンの代わりに新しく生成されたトークンを使用するように Telegraf を再構成する必要があります。その方法については、以下の手順で詳しく説明します。

Kubernetes

これらのコマンドはデフォルトの名前空間「netapp-monitoring」を使用していることに注意してください。独自の名前空間を設定している場合は、これらのコマンドと後続のすべてのコマンドおよびファイルでその名前空間を置き換えます。

注: 最新のNetApp Kubernetes Monitoring Operator がインストールされており、更新可能な API アクセス トークンを使用している場合、期限切れのトークンは新しい/更新された API アクセス トークンに自動的に置き換えられます。以下の手順を手動で実行する必要はありません。

- 新しい API トークンを作成します。
- 以下の手順に従ってください"手動アップグレード"、新しい API トークンを選択します。

注: Kustomize などの構成管理ツールを使用してNetApp Kubernetes Monitoring Operator を管理しているお客様は、同じ手順に従って、更新された YAML セットを生成してダウンロードし、リポジトリにプッシュできます。

RHEL/CentOS および 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
* Telegraf を再起動します。
```

```
sudo systemctl restart telegraf
```

Windows

- *C:\Program Files\telegraf\telegraf.d* 内の各 Telegraf 構成ファイルについて、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
```

- Telegraf 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) または予期しない変更 (トラブルシューティング用) を識別するには、 Data Infrastructure Insightsシステム イベントとユーザー アクティビティの監査証跡を表示できます。

監査対象イベントの表示

監査ページを表示するには、メニューの*管理>監査*をクリックします。監査ページが表示され、各監査エントリの次の詳細が提供されます。

- 時間 - イベントまたはアクティビティの日時
- 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におけるユーザーの役割 (ゲスト、ユーザー、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 - アクティビティの種類（例：ログイン、作成、更新）
- カテゴリー - アクティビティのカテゴリー
- 詳細 - アクティビティの詳細

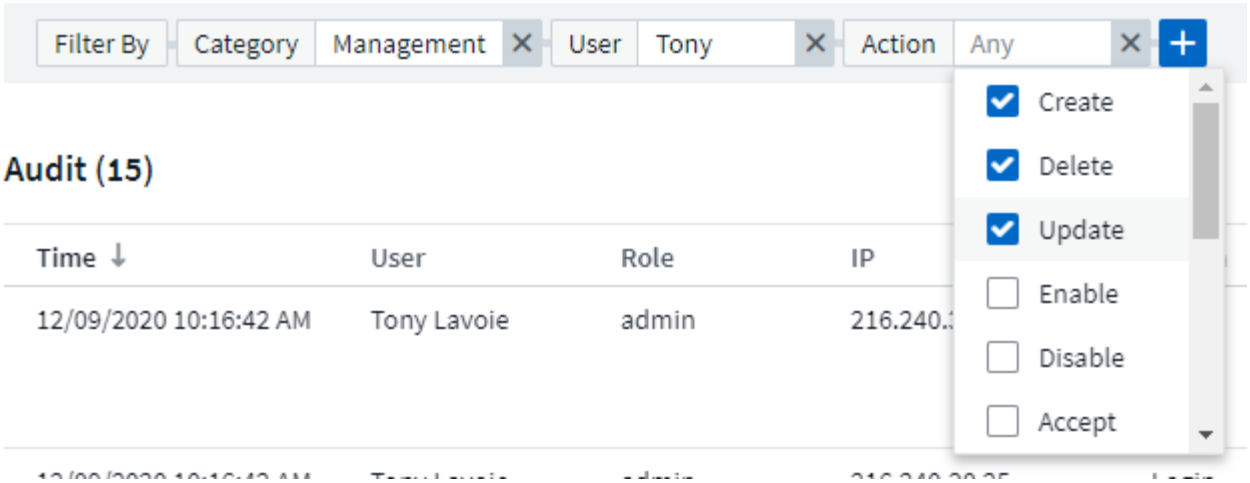
監査エントリの表示

監査エントリを表示するには、いくつかの方法があります。

- 特定の期間 (1 時間、24 時間、3 日間など) を選択して監査エントリを表示できます。
- 列ヘッダーの矢印をクリックすると、エントリの並べ替え順序を昇順 (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、テーブルにはエントリが降順で表示されます。

- フィルター フィールドを使用すると、必要なエントリのみをテーブルに表示できます。追加のフィルターを追加するには、[+]ボタンをクリックします。



フィルタリングの詳細

フィルターを絞り込むには、次のいずれかを使用できます。

フィルタ	何をするのか	例	結果
*（アスタリスク）	あらゆるものを検索できます	ヴォル*レル	「vol」で始まり「rhel」で終わるすべてのリソースを返します。
？（疑問符）	特定の文字数を検索できます	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る	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
ない	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」で始まらないものをすべて返します
なし	選択されたフィールドで空白/NULL/なしを検索します	なし	対象フィールドが空でない結果を返します
ない *	上記の_なし_と同様ですが、このフォームを使用して_テキストのみ_のフィールドのNULL値を検索することもできます。	ない *	ターゲット フィールドが空でない結果を返します。
""	完全一致を検索	「NetApp*」	正確なリテラル文字列 *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 は最初の引用符と最後の引用符の間のすべてを完全一致として扱います。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、「*」でフィルタリングすると、文字通りのアスタリスクである結果が返されます。この場合、アスタリスクはワイルドカードとして扱われません。演算子 OR と NOT も、二重引用符で囲むとリテラル文字列として扱われます。

監査対象のイベントとアクション

Data Infrastructure Insightsによって監査されるイベントとアクションは、次の広い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、役割の変更など。
- 取得単位: 作成、削除など

  例: 取得ユニット ***AU-Boston-1*** が削除されました。

- データコレクター: 追加、削除、変更、延期/再開、取得単位の変更、開始/停止など。

  例: データソース ** FlexPod Lab** が削除されました、ベンダー ** NetApp**、モデル ** ONTAP Data Management Software**、IP ***192.168.106.5***。

- アプリケーション: オブジェクトへの追加、割り当て、削除など。

  例: *Internal Volume* ***ocisedev:t1appSVM01:t1appFlexVol01*** がアプリケーション ***Test App*** に追加されました。

- 注釈: 追加、割り当て、削除、注釈ルールのアクション、注釈値の変更など。

  例: 注釈値 ***Boston*** が注釈タイプ ***SalesOffice*** に追加されました。

- クエリ: 追加、削除など

  例: クエリ ***TL Sales Query*** が追加されます。

- モニター: 追加、削除など

  例: モニター_Aggr Size - CI Alerts Notifications Dev_が更新されました

- 通知: メールの変更など

  例: 受信者 *ci-alerts-notifications-dl* が作成されました

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することができます。

手順

1. 監査ページで、希望する時間範囲と必要なフィルターを設定します。 Data Infrastructure Insights 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をエクスポートします。
2. _エクスポート_ボタンをクリックします表の右上にあります。

表示された監査イベントは、最大 10,000 行まで .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期間は、サブスクリプションによって異なります。

- トライアル環境: 監査データは30日間保持されます
- サブスクライブされた環境: 監査データは1年と1日間保持されます

保持期間より古い監査エントリは自動的に削除されます。ユーザーの操作は必要ありません。

保持期間より古い監査エントリは自動的に削除されます。ユーザーの操作は必要ありません。

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が見つかります。

問題：	これを試してみてください:
モニターがエクスポートされたことを通知する監査メッセージが表示されます。	カスタム モニター構成のエクスポートは通常、NetAppエンジニアが新機能の開発およびテスト中に使用します。このメッセージが表示されることを予期していなかった場合は、監査対象のアクションに指定されたユーザーのアクションを調べるか、サポートにお問い合わせください。

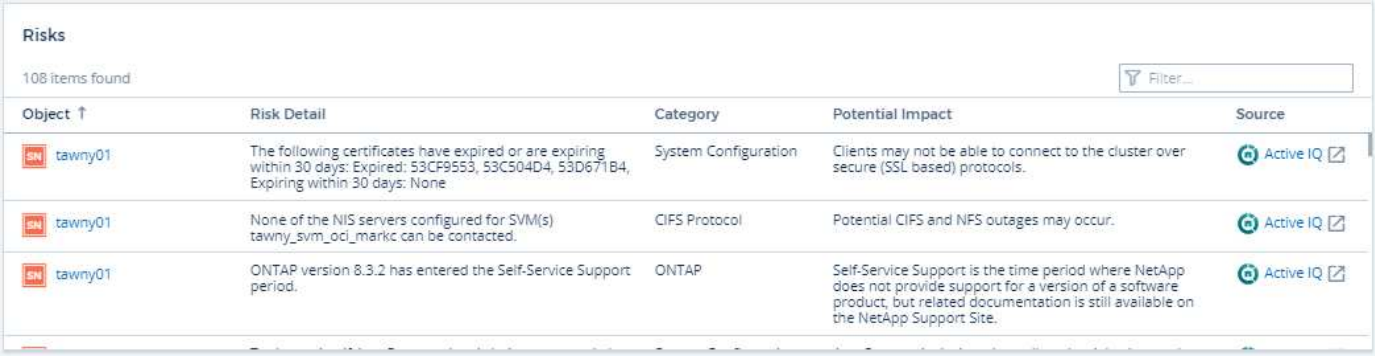
Active IQ Digital Advisor

NetApp"Active IQ Digital Advisor"(Digital Advisorとも呼ばれる) は、 NetAppの顧客のハードウェア/ソフトウェア システムに対して、一連の視覚化、分析、およびその他のサポート関連サービスを提供します。 Digital Advisorによって報告されるデータは、システムの問題のトラブルシューティングを強化し、デバイスに関連する最適化と予測分析に関する洞察も提供します。

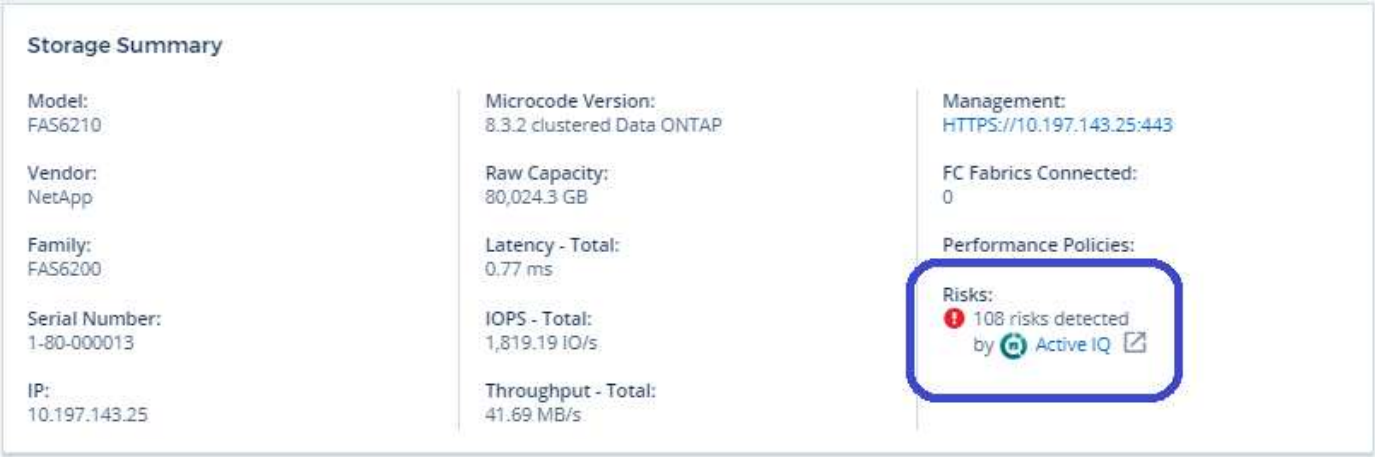
Data Infrastructure Insights は、 Digital Advisorによって監視およびレポートされるすべてのNetApp Clustered Data ONTAPストレージ システムの リスク を収集します。ストレージ システムについて報告されたリスクは、それらのデバイスからのデータ収集の一環として、Data Infrastructure Insightsによって自動的に収集されます。 Digital Advisor のリスク情報を収集するには、適切なデータ コレクターをData Infrastructure Insights に追加する必要があります。

Data Infrastructure Insights には、 Digital Advisorによって監視およびレポートされないONTAPシステムのリスク データは表示されません。

報告されたリスクは、Data Infrastructure Insightsの *storage* および *storage node* アセット ランディング ページの「リスク」テーブルに表示されます。表には、リスクの詳細、リスクのカテゴリ、リスクの潜在的な影響が表示され、ストレージ ノードのすべてのリスクをまとめたDigital Advisorページへのリンクも提供されます(NetAppサポート アカウントへのサインインが必要です)。



報告されたリスクの数は、適切なDigital Advisorページへのリンクとともに、ランディング ページの概要ウィジェットにも表示されます。ストレージ ランディング ページでは、カウントは基礎となるすべてのストレージ ノードからのリスクの合計になります。



Digital Advisorページを開く

Digital Advisorページへのリンクをクリックするときに、現在Digital Advisor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Digital Advisorページを表示する必要があります。

1. Data Infrastructure Insightsサイトの概要ウィジェットまたはリスク テーブルで、「Digital Advisor」リンクをクリックします。
2. NetAppサポート アカウントにSign in。 Digital Advisorのストレージ ノード ページに直接移動します。

リスクの問い合わせ

Data Infrastructure Insightsでは、ストレージまたはストレージ ノード クエリに **monitoring.count** 列を追加できます。返された結果にDigital Advisor監視対象ストレージ システムが含まれている場合、monitoring.count 列にはストレージ システムまたはノードのリスクの数が表示されます。

ダッシュボード

Digital Advisorによって監視されるNetApp Clustered Data ONTAPシステムのストレージおよびストレージ ノードのオブジェクト リスクを視覚化するために、ウィジェット (円グラフ、表ウィジェット、棒グラフ、列グラフ、散布図、単一値ウィジェットなど) を構築できます。ストレージまたはストレージ ノードがフォーカスのオブジェクトであるこれらのウィジェットでは、「オブジェクト リスク」を列またはメトリックとして選択できます。

Object Risks by Array

12 items found

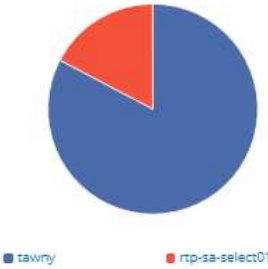
Name	Object Risks ↓
tawny	110
rtp-sa-select01	23
rtp-sa-cl02	N/A
rtp-sa-cl07	N/A
oci-phonehome	N/A
durlabprdsfc01	N/A
oci-3070-01	N/A

Object Risks by Node

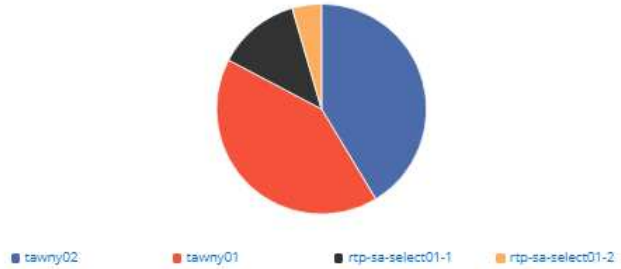
25 items found

Name	Object Risks ↓
tawny02	55
tawny01	55
rtp-sa-select01-1	17
rtp-sa-select01-2	6
tnode02	N/A
rtp-sa-cl06-01	N/A
rtp-sa-cl06-02	N/A

Object Risks by Storage



Object Risks by Storage Node



Total Storage Risks

133.00

Object Risks

ワークロードセキュリティ

ストレージワークロードセキュリティについて

Data Infrastructure Insights Storage Workload Security (旧称Cloud Secure) は、内部脅威に関する実用的なインテリジェンスによっ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 アクセスの集中的な可視性と制御を提供し、セキュリティとコンプライアンスの目標を確実に達成します。

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ー アクセスを一元的に可視化し、制御できます。

データへのアクセスと制御に関するタイムリーで正確な可視性を提供できないツールと手動プロセスを置き換えます。 Workload Security は、クラウドとオンプレミスの両方のストレージ システムで独自に動作し、悪意のあるユーザーの行動に関するアラートをリアルタイムで提供します。

保護

高度な機械学習と異常検出により、悪意のあるユーザーや侵害を受けたユーザーによる組織のデータの悪用を防ぎます。

高度な機械学習とユーザー行動の異常検出により、異常なデータアクセスを警告します。

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ー 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入門

Workload Security は、ユーザー アクティビティを監視し、ストレージ環境における潜在的なセキュリティ脅威を検出するのに役立ちます。監視を開始する前に、エージェント、データ コレクター、およびディレクトリ サービスを構成して、包括的なセキュリティ監視の基盤を確立する必要があります。

Workload Security システムはエージェントを使用して、ストレージ システムからのアクセス データとディレクトリ サービス サーバーからのユーザー情報を収集します。

データの収集を開始する前に、以下を構成する必要があります。

Task	関連情報

エージェントを構成する	"エージェントの要件" "エージェントを追加"
ユーザーディレクトリコネクタを構成する	"ユーザーディレクトリコネクタの追加"
データコレクターを構成する	ワークロード セキュリティ > コレクター をクリックし、設定するデータ コレクターをクリックします。コレクター情報については、ドキュメントのデータ コレクター ベンダー リファレンス セクションを参照してください。
ユーザーアカウントを作成する	"ユーザーアカウントの管理"

Workload Security は他のツールとも統合できます。例えば、"このガイドをご覧ください" Splunk との統合について。

ワークロード セキュリティ エージェントの要件

ワークロード・セキュリティ・エージェントは、OS、CPU、メモリ、ディスク容量の最小要件を満たす専用サーバーに導入することで、最適な監視および脅威検出パフォーマンスを確保できます。このガイドでは、"Workload Security エージェントのインストール"前に必要なハードウェアおよびネットワーク要件を規定しています。これには、サポート対象のLinuxディストリビューション、ネットワーク接続ルール、システムサイジングのガイダンスが含まれます。

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版を実行しているコンピュータ: * AlmaLinux 9.4 (64 ビット) ～ 9.5 (64 ビット)、10 (64 ビット) (SELinux を含む) * CentOS Stream 9 (64 ビット) * Debian 11 (64 ビット)、12 (64 ビット) (SELinux を含む) * OpenSUSE Leap 15.3 (64 ビット) ～ 15.6 (64 ビット) * Oracle Linux 8.10 (64 ビット) 、9.1 (64 ビット) ～ 9.6 (64 ビット) (SELinux を含む) * Red Hat Enterprise Linux 8.10 (64 ビット)、9.1 (64 ビット) ～ 9.6 (64 ビット)、10 (64 ビット) (SELinux を含む) * Rocky 9.4 (64 ビット) ～ 9.6 (64 ビット) (SELinux を含む) * SUSE Linux Enterprise Server 15 SP4 (64 ビット) ～ 15 SP6 (64 ビット)、SELinux を含む * Ubuntu 20.04 LTS (64 ビット)、22.04 LTS (64 ビット)、24.04 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。専用サーバーをお勧めします。
コマンド	インストールには「unzip」が必要です。さらに、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 su –」コマンドが必要です。
CPU	4つの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容量	ディスク領域は次のように割り当てる必要があります: /opt/netapp 36 GB (ファイルシステムの作成後に最低 35 GB の空き領域) 注: ファイルシステムの作成を可能にするために、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少なくとも 35 GB の空き領域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ーである場合は、ローカル ユーザーがこのフォルダーにアクセスできることを確認してください。ローカルユーザーにこのフォルダへの権限がない場合、エージェントまたはデータコレクタのインストールに失敗する可能性があります。"トラブルシューティング"詳細についてはセクションをご覧ください。
ネットワーク	100 Mbps ～ 1 Gbps のイーサネット接続、静的 IP アドレス、すべてのデバイスへの IP 接続、および Workload Security インスタンスへの必要なポート (80 または 443)。

注意: Workload Security エージェントは、Data Infrastructure Insights取得ユニット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がベストプラクティスです。これらを同じマシンにインストールする場合は、以下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容量	50～55 GB Linuxの場合、ディスク容量は次のように割り当てる必要があります: /opt/netapp 25～30 GB /var/log/netapp 25 GB

追加の推奨事項

- **Network Time Protocol (NTP)** または **Simple Network Time Protocol (SNTP)** を使用して、 ONTAPシステムとエージェント マシンの両方の時刻を同期することを強くお勧めします。

クラウドネットワークアクセスルール

*米国ベースの*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	デスティネーション	説明
TCP	443	ワークロードセキュリティエージェント	<サイト名>.cs01.cloudinsights.netapp.com <サイト名>.c01.cloudinsights.netapp.com <サイト名>.c02.cloudinsights.netapp.com	Data Infrastructure Insightsへのアクセス
TCP	443	ワークロードセキュリティエージェント	agentlogin.cs01.cloudinsights.netapp.com	認証サービスへのアクセス

*ヨーロッパベースの*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	デスティネーション	説明
TCP	443	ワークロードセキュリティエージェント	<サイト名>.cs01-eu-1.cloudinsights.netapp.com <サイト名>.c01-eu-1.cloudinsights.netapp.com <サイト名>.c02-eu-1.cloudinsights.netapp.com	Data Infrastructure Insightsへのアクセス
TCP	443	ワークロードセキュリティエージェント	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	デスティネーション	説明
TCP	443	ワークロードセキュリティエージェント	<サイト名>.cs01-ap-1.cloudinsights.netapp.com <サイト名>.c01-ap-1.cloudinsights.netapp.com <サイト名>.c02-ap-1.cloudinsights.netapp.com	Data Infrastructure Insightsへのアクセス
TCP	443	ワークロードセキュリティエージェント	エージェントログイン.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	デスティネーション	説明
TCP	389(LDAP) 636 (LDAP / start-tls)	ワークロードセキュリティエージェント	LDAP Server URL	LDAPに接続する
TCP	443	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 管理 IP アドレス (SVM コレクターの構成によって異なります)	ONTAPとのAPI通信

プロトコル	ポート	ソース	デスティネーション	説明
TCP	35000 - 55000	SVM データ LIF IP アドレス	ワークロードセキュリティエージェント	Fpolicy イベントのためのONTAPからWorkload Security Agent への通信。ONTAP がWorkload Security Agent にイベントを送信するには、Workload Security Agent 自体のファイアウォール（存在する場合）も含めてこれらのポートを Workload Security Agent に対して開く必要があります。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。まずは約 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。

プロトコル	ポート	ソース	デスティネーション	説明
TCP	35000-55000	クラスタ管理IP	ワークロードセキュリティエージェント	**EMS** イベント 用のONTAPクラスタ管理 IP 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Workload Security Agent に **EMS** イベント を送信するには、これらのポートを Workload Security Agent に対して開く必要があります。これには、Workload Security Agent 自体のファイアウォール (存在する場合) も含まれます。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。まずは約 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。
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 ユーザーのブロックに必要です。

システムのサイズ設定

参照"イベントレートチェッカー"サイズに関する情報についてはドキュメントを参照してください。

ワークロードセキュリティエージェントの導入

Workload Security エージェントは、ユーザー アクティビティを監視し、ストレージ インフラストラクチャ全体で潜在的なセキュリティ脅威を検出するために不可欠です。このガイドでは、ステップバイステップのインストール手順、エージェント管理のベストプラクティス (一時停止/再開、ピン留め/ピン留め解除機能を含む)、および展開後の構成要件について説明します。始める前に、エージェントサーバーが "システム要件"。

開始前の準備

- 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 ユーザー *cssys* とローカル グループ *cssys* がマシン上に作成されます。権限設定によりローカル ユーザーの作成が許可されず、代わりに Active Directory が必要な

場合は、ユーザー名が *cssys* のユーザーを Active Directory サーバーに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読むことができます"ここをクリックしてください。"。

ベストプラクティス

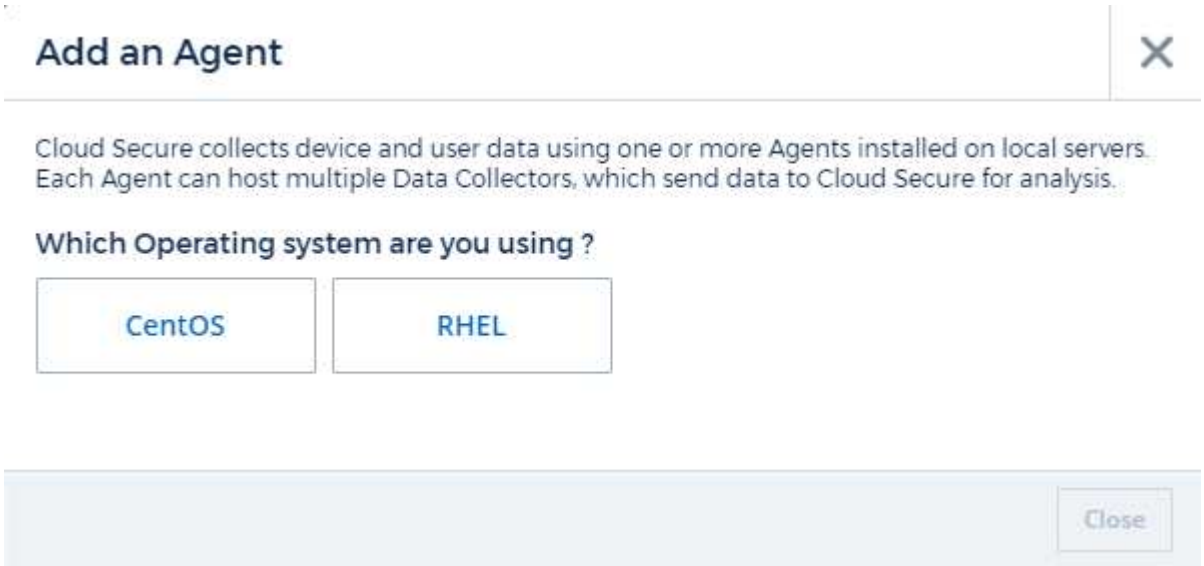
Workload Security エージェントを設定する前に、次の点に留意してください。

一時停止と再開	一時停止: ONTAPから fpolicies を削除します。通常、エージェント VM の再起動やストレージの交換など、かなりの時間を要する可能性がある長時間のメンテナンス アクティビティを顧客が実行する場合に使用されます。再開: fpolicies をONTAPに追加し直します。
ピン留めとピン留め解除	ピンを解除すると、すぐに最新バージョン (利用可能な場合) が取得され、エージェントとコレクターがアップグレードされます。このアップグレード中、fpolicies は切断され、再接続されます。この機能は、自動アップグレードのタイミングを制御したいお客様向けに設計されています。以下を参照ピン留め/ピン留め解除の手順。
推奨されるアプローチ	大規模な構成の場合、コレクターを一時停止するのではなく、Pin と Unpin を使用することをお勧めします。ピンとピン解除の使用中に一時停止したり再開したりする必要はありません。顧客はエージェントとコレクターを固定したままにして、新しいバージョンに関する電子メール通知を受信したら、30 日以内にエージェントを 1 つずつ選択的にアップグレードすることができます。このアプローチにより、fpolicies への遅延の影響が最小限に抑えられ、アップグレード プロセスをより細かく制御できるようになります。

エージェントのインストール手順

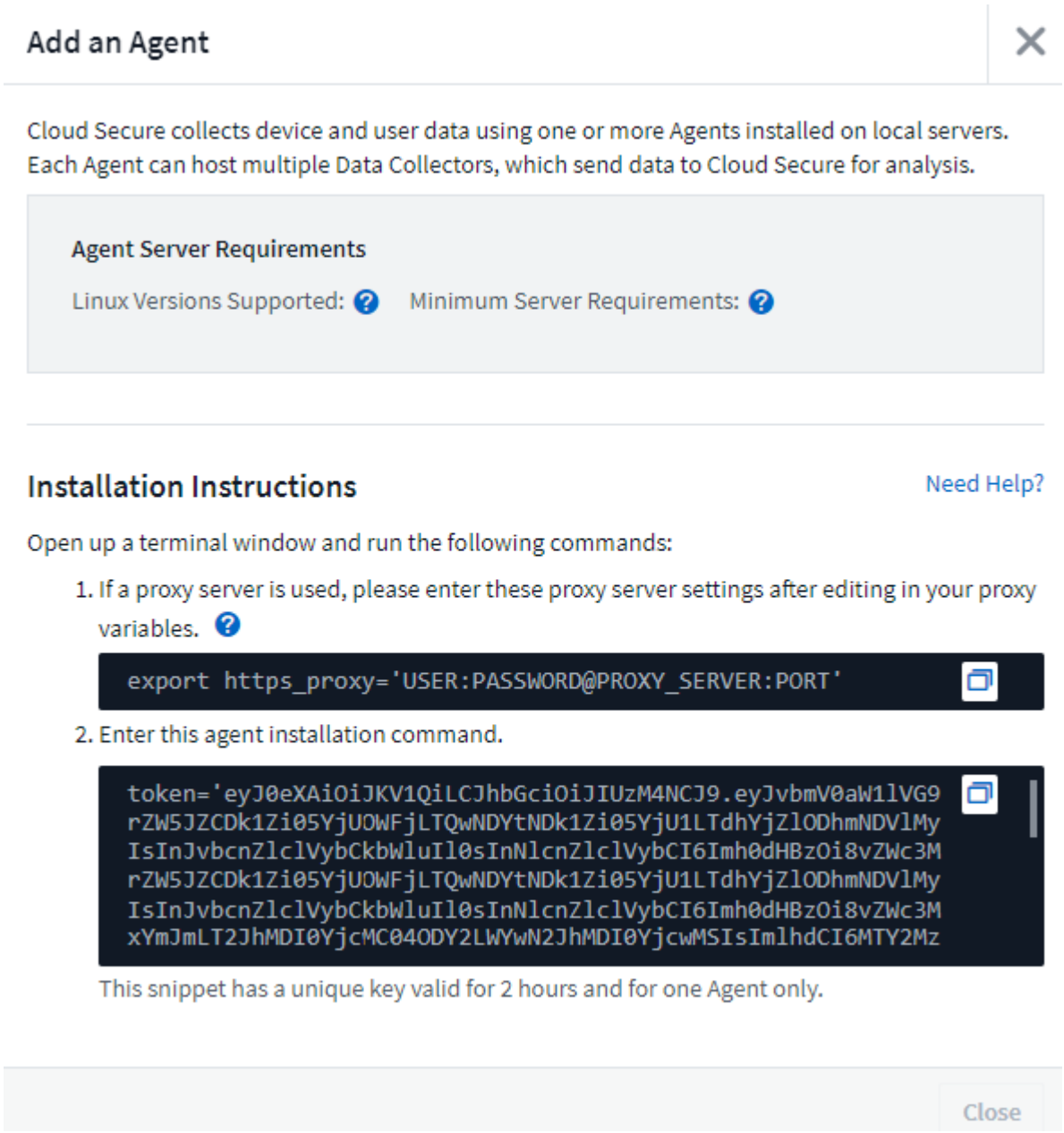
1. Workload Security 環境に管理者またはアカウント所有者としてログインします。
2. *コレクター > エージェント > +エージェント*を選択

   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 サーバー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 サーバーがサポートされているバージョンの Linux を実行し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 サーバー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 サーバーの詳細を設定してください。



6. インストール コマンドをコピーするには、[クリップボードにコピー] アイコンをクリックします。
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. 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ー"。
2. 1 つ以上のデータ コレクターを構成する必要があります。

ネットワーク構成

Workload Security で使用されるポートを開くには、ローカル システムで次のコマンドを実行します。ポート範囲に関してセキュリティ上の懸念がある場合は、*35000:35100* などのより狭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に従ってください。

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
```

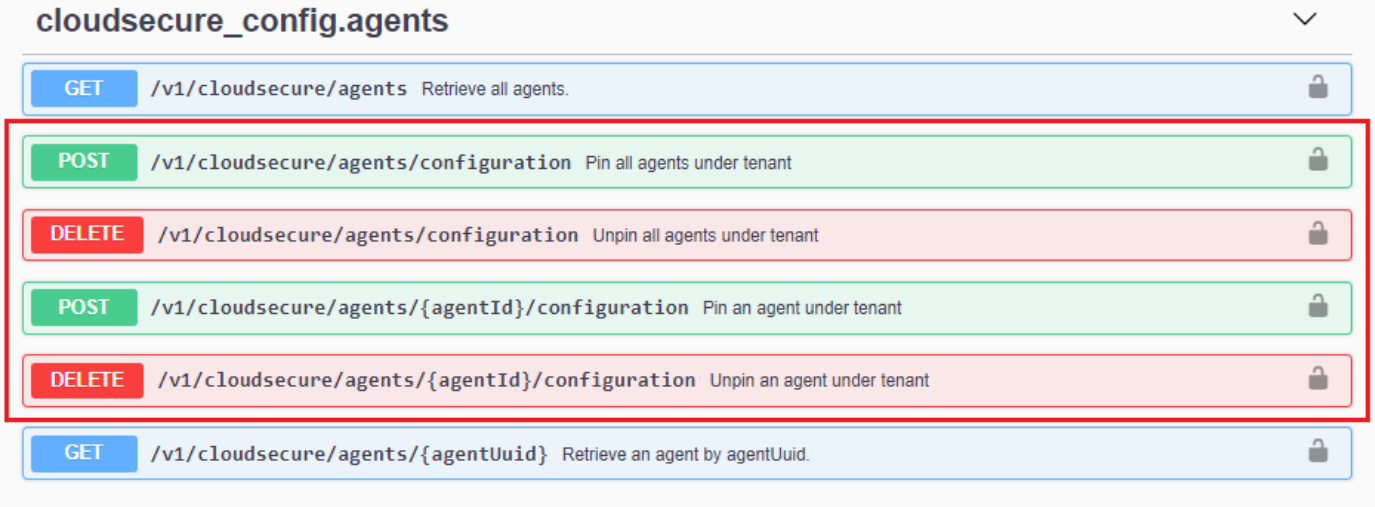
エージェントを現在のバージョンに「固定」する

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。自動更新を一時停止して、次のいずれかが発生するまでエージェントを現在のバージョンのままにすることを希望する顧客もいます。

- 顧客はエージェントの自動更新を再開します。
- 30日が経過しました。 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から始まることに注意してください。

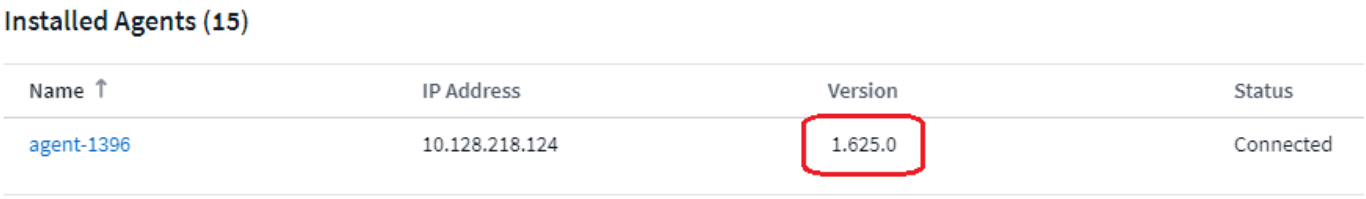
いずれの場合も、エージェントは次回の Workload Security 更新時に更新されます。

自動エージェント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アクションが有効になるまでに最大 5 分かかる場合があることに注意してください。

現在のエージェントのバージョンは、**Workload Security > Collectors** ページの **Agents** 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：
エージェントのインストールで /opt/netapp/cloudsecure/agent/logs/agent.log フォルダの作成に失敗し、install.log ファイルには関連情報が提供されません。	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。エラーはロガーが初期化される前に発生するため、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、サービスログで次のように表示されます。 `journalctl -u cloudsecure-agent.service`指示。このコマンドは、問題をさらにトラブルシューティングするために使用できます。
エージェントのインストールが「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」というメッセージで失敗します。インストールを終了します。	このエラーは、サポートされていないシステムにエージェントをインストールしようとしたときに表示されます。見る"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 をインストールしてから、インストール コマンドを再度実行します。マシンに Yum がインストールされている場合は、「yum install unzip」を実行して unzip ソフトウェアをインストールしてください。その後、エージェントのインストール UI からコマンドを再度コピーし、CLI に貼り付けてインストールを再度実行します。

問題：	解決：

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。	エージェント マシンに SSH で接続します。エージェントサービスのステータスを確認するには、 `sudo systemctl status cloudsecure-agent.service` 。1.ログに「Workload Security デーモン サービスを開始できませんでした」というメッセージが表示されているかどうかを確認します。2.エージェント マシンに cssys ユーザーが存在するかどうかを確認します。次のコマンドをルート権限で 1 つずつ実行し、cssys ユーザー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.存在しない場合は、集中監視ポリシーによって `cssys` ユーザー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` ユーザーとグループを手動で作成します。
	`sudo useradd cssys`
	`sudo groupadd cssys`5.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` 6.それでも実行されない場合は、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 50 個を超えるデータ コレクターを追加することはできません。	エージェントに追加できるデータ コレクターは 50 個のみです。これは、Active Directory、SVM、その他のコレクターなど、すべてのコレクター タイプの組み合わせになります。
UI には、エージェントが NOT_CONNECTED 状態にあることが示されます。	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 で接続します。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.エージェントサービスのステータスを確認するには、 `sudo systemctl status cloudsecure-agent.service` 。4.エージェントは CONNECTED 状態に移行する必要があります。
エージェント VM は Zscaler プロキシの背後にあり、エージェントのインストールが失敗します。 Zscaler プロキシの SSL 検査により、Workload Security 証明書は Zscaler CA によって署名された状態で提示されるため、エージェントは通信を信頼していません。	*.cloudinsights.netapp.com URL の Zscaler プロキシで SSL 検査を無効にします。 Zscaler が SSL 検査を実行して証明書を置き換えると、Workload Security は機能しなくなります。

問題：	解決：
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。エージェント インストール コマンドが非 root sudo ユーザーによって実行され、作業ディレクトリに別のユーザーに属するファイルがあり、それらのファイルの権限を変更できない場合、コマンドは失敗します。chmod コマンドが失敗したため、インストールの残りの部分は実行されません。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「token=…… …./cloudsecure-agent-install.sh」インストール コマンドをコピーして貼り付け、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。
それでもエージェントが Saas に接続できない場合は、 NetAppサポートにケースを開いてください。ケースを開くには、 Data Infrastructure Insights のシリアル番号を提供し、記載されているとおりにログをケースに添付します。	ログをケースに取り付けるには: 1.次のスクリプトをルート権限で実行し、出力ファイル (cloudsecure-agent-symptoms.zip) を共有します。a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2.ルート権限で次のコマンドを1つずつ実行し、出力を共有します。a. id cssys b. groups cssys 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 エージェント構成を収集しています 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 の作成に失敗しました	Zip ツールがインストールされていません。 「yum install zip」コマンドを実行して、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。
エージェントのインストールが useradd で失敗します: ディレクトリ /home/cssys を作成できません	このエラーは、権限不足のためにユーザーのログイン ディレクトリを /home の下に作成できない場合に発生する可能性があります。回避策としては、cssys ユーザーを作成し、次のコマンドを使用してそのログイン ディレクトリを手動で追加します: *sudo useradd user_name -m -d HOME_DIR* -m : ユーザーのホーム ディレクトリが存在しない場合は作成します。 -d : ユーザーのログイン ディレクトリの値として HOME_DIR を使用して新しいユーザーが作成されます。たとえば、*sudo useradd cssys -m -d /cssys* は、ユーザー *cssys* を追加し、ルートの下にそのログイン ディレクトリを作成します。

問題：	解決：
インストール後にエージェントが実行されていません。 *Systemctl status cloudsecure-agent.service* は次のように表示します: [root@demo ~]# systemctl status cloudsecure-agent.service agent.service – Workload Security Agent Daemon Service Loaded: loaded (/usr/lib/systemd/system/cloudsecure-agent.service; enabled; vendor preset: disabled) Active: activating (auto-restart) (Result: exit-code) since Tue 2021-08-03 21:12:26 PDT; 2 秒前 プロセス: 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent (コード = 終了、ステータス = 126) メイン PID: 25889 (コード = 終了、ステータス = 126)、8 月 03 日 21:12:26 demo systemd[1]: cloudsecure-agent.service: メイン プロセスが終了しました。コード = 終了、ステータス = 126/n/a 8 月 03 日 21:12:26 demo systemd[1]: ユニット cloudsecure-agent.service が失敗状態になりました。 8月3日 21:12:26 デモ systemd[1]: cloudsecure-agent.service が失敗しました。	*cssys* ユーザーにインストール権限がない可能性があるため、失敗する可能性があります。 /opt/netapp が NFS マウントであり、*cssys* ユーザーがこのフォルダー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、Workload Security インストーラによって作成されたローカル ユーザーであり、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ります。これを確認するには、*cssys* ユーザーを使用して /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent にアクセスしてみてください。 「Permission denied」が返された場合、インストール権限が存在しません。マウントされたフォルダーの代わりに、マシンのローカル ディレクトリにインストールします。
エージェントは最初にプロキシ サーバー経由で接続され、プロキシはエージェントのインストール中に設定されました。プロキシサーバーが変更されました。エージェントのプロキシ構成を変更するにはどうすればよいですか?	agent.properties を編集してプロキシの詳細を追加できます。次の手順に従ってください: 1.プロパティ ファイルが含まれているフォルダーに変更します: cd /opt/netapp/cloudsecure/conf 2.お気に入りのテキストエディターを使用して、*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

Workload Security エージェントを削除する場合は、まず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 コレクターを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 コレクターが削除されます。別のエージェントを使用してデータ コレクターを構成する予定の場合は、エージェントを削除する前に、データ コレクター構成のバックアップを作成する必要があります。

開始する前に

1. エージェントに関連付けられているすべてのデータ コレクターが Workload Security ポータルから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ーが STOPPED 状態の場合、この手順は無視してください。

エージェントを削除する手順:

1. エージェント VM に SSH で接続し、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. *ワークロードセキュリティ > コレクター > エージェント*をクリックします

   構成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*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、[削除] をクリックします。

Active Directory (AD) ユーザーディレクトリコレクターの構成

Workload Security は、Active Directory サーバーからユーザー属性を収集するように設定できます。

開始する前に

- このタスクを実行するには、 Data Infrastructure Insights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 サーバーをホストしているサーバーの IP アドレスが必要です。
- ユーザー ディレクトリ コネクタを構成する前に、エージェントを構成する必要があります。

ユーザーディレクトリコレクターを構成する手順

1. Workload Securityメニューで、*コレクター > ユーザーディレクトリコレクター > + ユーザーディレクトリコレクター*をクリックし、*Active Directory*を選択します。

   「ユーザー ディレクトリの追加」画面が表示されます。

次の表に必要なデータを入力して、ユーザー ディレクトリ コレクターを構成します。

Name	説明
Name	ユーザー ディレクトリの一意の名前。例えば_GlobalADCollector_
エージェント	リストから構成済みのエージェントを選択します

サーバーIP/ドメイン名	アクティブ ディレクトリをホストするサーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN)
森林名	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、次の両方の形式が許可されます: *x.y.z* ⇒ SVM にある直接のドメイン名。 [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、次のように指定することもできます: *OU=engineering*、*DC=hq*、*DC= companyname* 、*DC=com* [特定の OU engineering でフィルタリングする] *CN=username*、*OU=engineering* 、*DC=companyname*、*DC=netapp*、*DC=com* [OU <engineering> から <username> を持つ特定のユーザーのみを取得する] *CN=Acrobat Users*、*CN=Users* 、*DC=hq*、*DC=companyname*、*DC=com*、*O= companyname*、*L=Boston*、*S=MA*、*C=US* [その組織内のユーザー内のすべての Acrobat ユーザーを取得する] 信頼された Active Directory ドメインもサポートされています。
バインドDN	ディレクトリの検索を許可されたユーザー。たとえば、*username@companyname.com* または *username@domainname.com* です。さらに、ドメイン読み取り専用権限が必要です。ユーザーは、セキュリティ グループ 読み取り専用ドメイン コントローラー のメンバーである必要があります。
BINDのパスワード	ディレクトリ サーバーのパスワード (つまり、Bind DN で使用されるユーザー名のパスワード)
プロトコル	ldap、ldaps、ldap-start-tls
ポート	ポートを選択

Active Directory でデフォルトの属性名が変更されている場合は、次のディレクトリ サーバーの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 では変更されません。その場合は、デフォルトの属性名をそのまま使用して続行できます。

属性	ディレクトリサーバーの属性名
表示名	名前
SID	オブジェクトID
ユーザー名	sAMAccountName

次のいずれか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	ディレクトリサーバーの属性名
E メール アドレス	郵便
電話番号	電話番号
ロール	タイトル
国	共同

州	状態
部門	部門
写真	サムネイル写真
マネージャーDN	マネージャー
グループ	memberOf

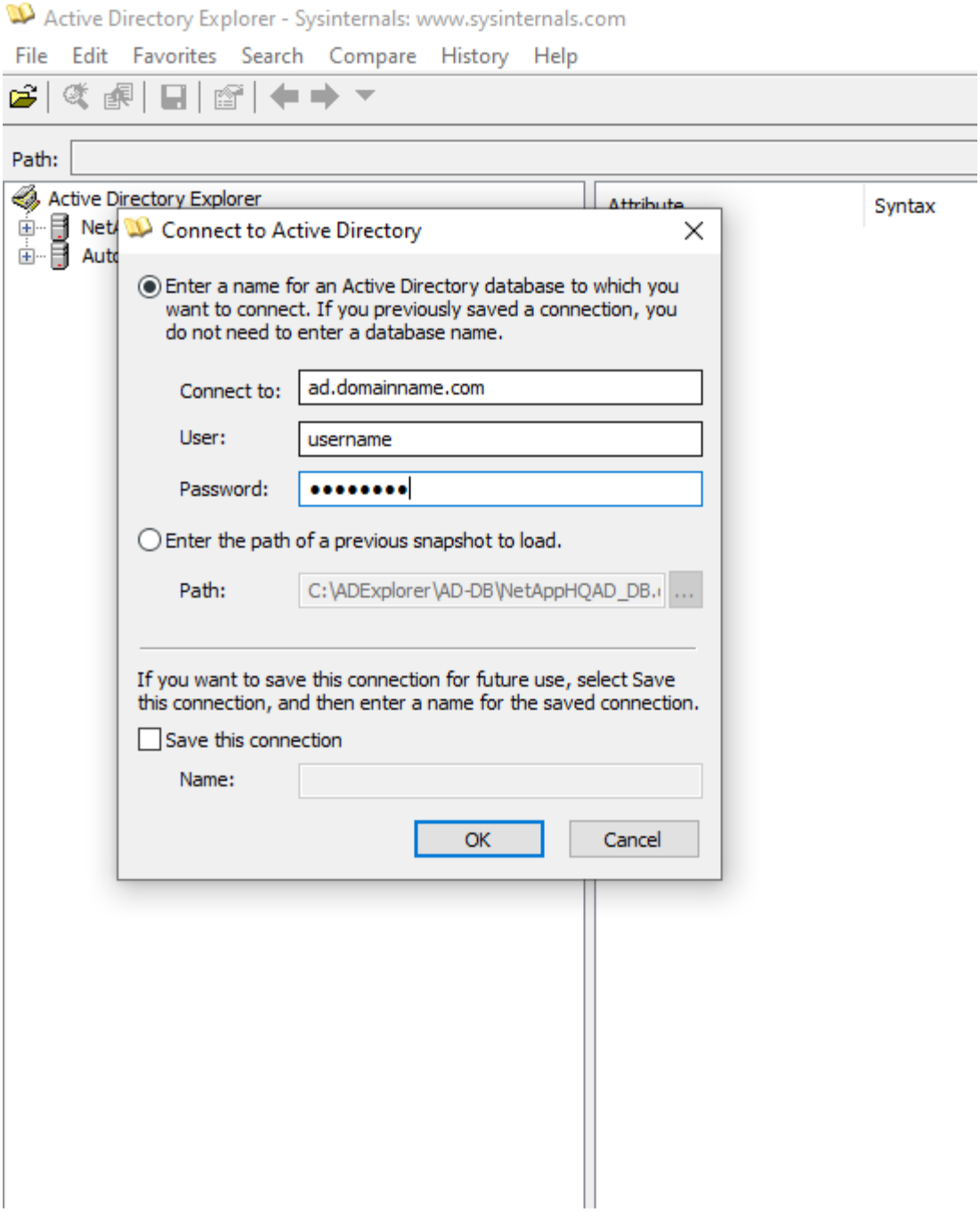
ユーザーディレクトリコレクターの構成のテスト

次の手順を使用して、LDAP ユーザー権限と属性定義を検証できます。

- Workload Security LDAP ユーザー権限を検証するには、次のコマンドを使用します。

```
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 を使用すると、AD データベースをナビゲートしたり、オブジェクトのプロパティと属性を表示したり、権限を表示したり、オブジェクトのスキーマを表示したり、保存して再実行できる高度な検索を実行したりできます。
  - インストール"広告エクスプローラー"AD サーバーに接続できる任意の Windows マシン上。
  - AD ディレクトリ サーバーのユーザー名とパスワードを使用して AD サーバーに接続します。



ユーザーディレクトリコレクターの構成エラーのトラブルシューティング

次の表では、コレクターの構成中に発生する可能性のある既知の問題と解決策について説明します。

問題：	解決：
ユーザー 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 サーバーに無効な資格情報が提供されました」というエラーが表示されます。	間違ったユーザー名またはパスワードが指定されました。正しいユーザー名とパスワードを編集して入力します。

問題：	解決：
ユーザー 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。エラーには、「フォレスト名として指定された DN=DC=hq、DC=domainname 、DC=com に対応するオブジェクトを取得できませんでした。」と表示されます。	指定され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属性が、Workload Security 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 に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ていないことが原因であると考えられます。正しいオプション属性名を編集して指定します。
データ コレクターが「LDAP ユーザーの取得に失敗しました」というエラー状態です。失敗の理由: サーバーに接続できません。接続が null です。	*Restart* ボタンをクリックしてコレクターを再起動します。
ユーザー 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 (サーバー、フォレスト名、バインド DN、バインド パスワード) に有効な値を指定していることを確認してください。バインド 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るようにします。
ユーザー ディレクトリ コネクタを追加すると、「再試行」状態になります。 「コレクターの状態を定義できません。理由: java.net.ConnectionException: 接続が拒否されたため、TCP コマンド [Connect(localhost:35012,None,List(),Some(,seconds),true)] が失敗しました。」というエラーが表示されます。	AD サーバーに指定された IP または FQDN が正しくありません。正しい IP アドレスまたは FQDN を編集して入力します。
ユーザー 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 接続を確立できませんでした」というエラーが表示されます。	AD サーバーに指定された IP または FQDN が正しくありません。正しい IP アドレスまたは FQDN を編集して入力します。
ユーザー 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。 「設定の読み込みに失敗しました」というエラーが表示されます。理由: データソース構成にエラーがあります。具体的な理由: /connector/conf/application.conf: 70: ldap.ldap-port のタイプは NUMBER ではなく STRING です	指定されたポートの値が正しくありません。 AD サーバー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。
必須属性から始めましたが、うまくいきました。オプションのものを追加した後、オプションの属性データが AD から取得されません。	これは、CloudSecure に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ていないことが原因であると考えられます。正しい必須またはオプションの属性名を編集して指定します。
コレクターを再起動した後、AD 同期はいつ行われますか?	コレクターが再起動するとすぐに AD 同期が行われます。約 30 万ユーザーのユーザーデータを取得するには約 15 分かかり、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。データはいつ削除されますか?	更新がない場合、ユーザーデータは 13 か月間保持されます。テナントが削除されると、データも削除されます。

問題：	解決：
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。 「コネクタはエラー状態です。サービス名: usersLdap。失敗の理由: LDAP ユーザーの取得に失敗しました。失敗の理由: 80090308: LdapErr: DSID-0C090453、コメント: AcceptSecurityContext エラー、データ 52e、v3839"	指定され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。
ユーザー プロフィール ページに電話番号が入力されません。	これは、Active Directory の属性マッピングの問題が原因であると考えられます。1. Active Directory からユーザーの情報を取得している特定の Active Directory コレクターを編集します。2.オプション属性の下に、Active Directory 属性「telephonenumber」にマップされたフィールド名「電話番号」があることに注意してください。4.ここで、上で説明した Active Directory Explorer 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、実際にユーザーの電話番号を持つ「telephonenumber」という名前の属性があることを確認します。5. Active Directory では「phonenumber」に変更されているとします。6.次に、CloudSecure ユーザー ディレクトリ コレクターを編集します。オプション属性セクションで、「telephonenumber」を「phonenumber」に置き換えます。7. Active Directory コレクターを保存すると、コレクターが再起動し、ユーザーの電話番号を取得して、ユーザー プロファイル ページに表示します。
Active Directory (AD) サーバーで暗号化証明書 (SSL) が有効になっている場合、Workload Security ユーザー ディレクトリ コレクターは AD サーバーに接続できません。	ユーザー ディレクトリ コレクターを構成する前に、AD サーバー暗号化を無効にします。ユーザーの詳細が取得されると、その情報は 13 か月間保存されます。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、AD に新しく追加されたユーザーは取得されません。再度取得するには、ユーザー ディレクトリ コレクターを AD に接続する必要があります。
Active Directory からのデータは CloudInsights Security に存在します。 CloudInsights からすべてのユーザー情報を削除します。	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。ユーザーを削除するには、テナント全体を削除する必要があります。

LDAPディレクトリサーバーコレクターの構成

Workload Security 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。

開始する前に

- このタスクを実行するには、 Data Infrastructure Insights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 サーバーをホストするサーバーの IP アドレスが必要です。

- LDAP ディレクトリ コネクタを構成する前に、エージェントを構成する必要があります。

ユーザーディレクトリコレクターを構成する手順

1. ワークロード セキュリティ メニューで、コレクター > ユーザー ディレクトリ コレクター > + ユーザー ディレクトリ コレクター をクリックし、**LDAP** ディレクトリ サーバー を選択します。

   「ユーザー ディレクトリの追加」画面が表示されます。

次の表に必要なデータを入力して、ユーザー ディレクトリ コレクターを構成します。

Name	説明
Name	ユーザー ディレクトリの一意の名前。例えば_GlobalLDAPCollector_
エージェント	リストから構成済みのエージェントを選択します
サーバーIP/ドメイン名	LDAP ディレクトリ サーバーをホストするサーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN)
検索ベース	LDAP サーバーの検索ベース検索ベースでは、次の両方の形式が許可されます: *x.y.z* ⇒ SVM にある直接のドメイン名。 [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、次のように指定することもできます: *OU=engineering,DC=hq,DC=companyname,DC=com* [特定の OU engineering でフィルタリングする] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [OU <engineering> から <username> を持つ特定のユーザーのみを取得する] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [その組織内のユーザー内のすべての Acrobat ユーザーを取得する]
バインドDN	ディレクトリの検索を許可されたユーザー。たとえば、ユーザー john@dorp.company.com の場合、uid=ldapuser、cn=users、cn=accounts、dc=domain、dc=companyname、dc=com uid=john 、cn=users、cn=accounts、dc=dorp、dc=company、dc=com となります。 dorp.company.com
--アカウント	--ユーザー
--ジョン	--アンナ
BINDのパスワード	ディレクトリ サーバーのパスワード (つまり、Bind DN で使用されるユーザー名のパスワード)
プロトコル	ldap、ldaps、ldap-start-tls
ポート	ポートを選択

LDAP ディレクトリ サーバーでデフォルトの属性名が変更されている場合は、次のディレクトリ サーバーの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 LDAP ディレクトリ サーバーで変更されませ

ん。その場合は、デフォルトの属性名でそのまま続行できます。

属性	ディレクトリサーバーの属性名
表示名	名前
UNIXID	uid番号
ユーザー名	uid

次のいずれか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	ディレクトリサーバーの属性名
E メール アドレス	郵便
電話番号	電話番号
ロール	タイトル
国	共同
州	状態
部門	部門番号
写真	写真
マネージャーDN	マネージャー
グループ	memberOf

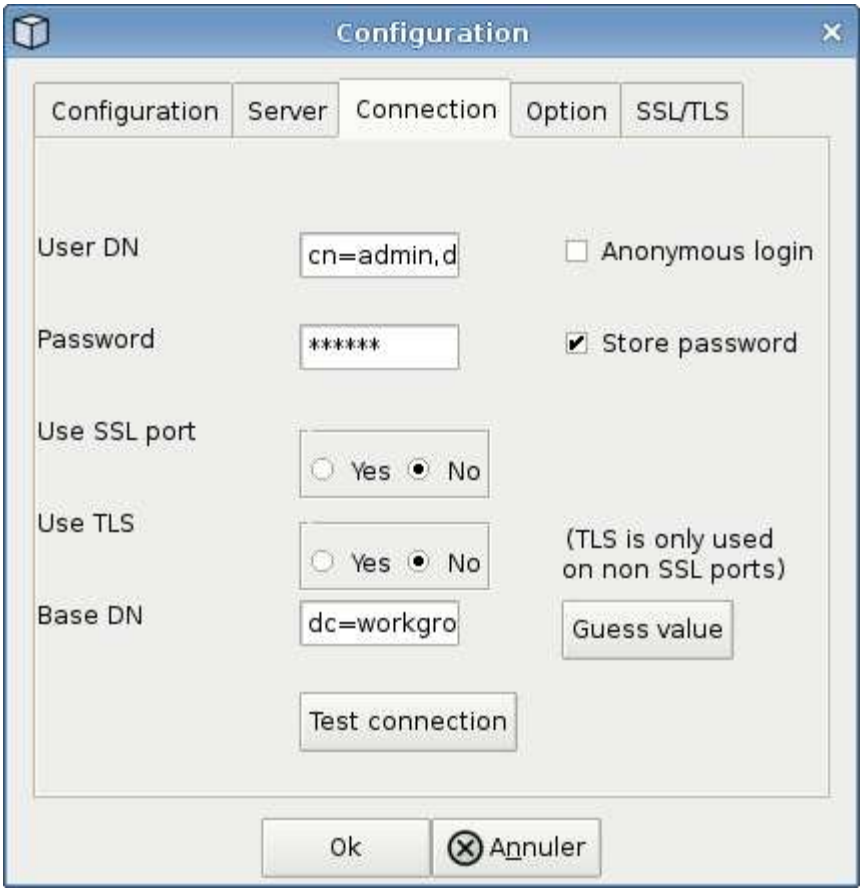
ユーザーディレクトリコレクターの構成のテスト

次の手順を使用して、LDAP ユーザー権限と属性定義を検証できます。

- Workload Security LDAP ユーザー権限を検証するには、次のコマンドを使用します。

```
 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 エクスプローラーを使用すると、LDAP
データベースをナビゲートしたり、オブジェクトのプロパティと属性を表示したり、権限を表示したり、オブジェクトのスキーマを表示したり、保存して再実行できる高度な検索を実行したりできます。
```

  - LDAPエクスプローラーをインストールする(http://ldaptool.sourceforge.net/) または Java LDAP エクスプローラー(http://jxplorer.org/) を、LDAP サーバーに接続できる任意の Windows マシンにインストールします。
  - LDAP ディレクトリ サーバーのユーザー名とパスワードを使用して LDAP サーバーに接続します。



LDAPディレクトリコレクターの設定エラーのトラブルシューティング

次の表では、コレクターの構成中に発生する可能性のある既知の問題と解決策について説明します。

問題：	解決：
LDAP 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 サーバーに無効な資格情報が提供されました」というエラーが表示されます。	指定されたバインド 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。正しい情報を編集して提供してください。
LDAP 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。エラーには、「フォレスト名として指定された DN=DC=hq、DC=domainname 、DC=com に対応するオブジェクトを取得できませんでした。」と表示されます。	間違った検索ベースが指定されました。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属性が、Workload Security 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 に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ていないことが原因であると考えられます。フィールドでは大文字と小文字が区別されます。正しいオプション属性名を編集して指定します。
データ コレクターが「LDAP ユーザーの取得に失敗しました」というエラー状態です。失敗の理由: サーバーに接続できません。接続が null です。	*Restart* ボタンをクリックしてコレクターを再起動します。

問題：	解決：
LDAP 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 (サーバー、フォレスト名、バインド DN、バインド パスワード) に有効な値を指定していることを確認してください。バインド DN 入力が常に uid=ldapuser、cn=users、cn=accounts、dc=domain、dc=companyname、dc=com として提供されるようにします。
LDAP ディレクトリ コネクタを追加すると、「再試行」状態になります。 「コレクターの正常性を判断できなかったため、再試行します」というエラーが表示されます	正しいサーバー IP と検索ベースが提供されていることを確認してください ////
LDAP ディレクトリの追加中に次のエラーが表示されます: 「2 回の再試行でコレクターの正常性を判断できませんでした。コレクターをもう一度再起動してください (エラー コード: AGENT008)」	正しいサーバーIPと検索ベースが提供されていることを確認してください
LDAP ディレクトリ コネクタを追加すると、「再試行」状態になります。 「コレクターの状態を定義できません。理由: java.net.ConnectionException: 接続が拒否されたため、TCP コマンド [Connect(localhost:35012,None,List(),Some(,seconds),true)] が失敗しました。」というエラーが表示されます。	AD サーバーに指定された IP または FQDN が正しくありません。正しい IP アドレスまたは FQDN を編集して入力します。 ////
LDAP 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 接続を確立できませんでした」というエラーが表示されます。	LDAP サーバーに指定された IP または FQDN が正しくありません。正しい IP アドレスまたは FQDN を編集して入力します。または、指定されたポートの値が正しくありません。 LDAP サーバー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。
LDAP 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。 「設定の読み込みに失敗しました」というエラーが表示されます。理由: データ ソース構成にエラーがあります。具体的な理由: /connector/conf/application.conf: 70: ldap.ldap-port のタイプは NUMBER ではなく STRING です	指定されたポートの値が正しくありません。 AD サーバー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。
必須属性から始めましたが、うまくいきました。オプションのものを追加した後、オプションの属性データが AD から取得されません。	これは、CloudSecure に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ていないことが原因であると考えられます。正しい必須またはオプションの属性名を編集して指定します。
コレクターを再起動した後、LDAP 同期はいつ行われますか?	コレクターが再起動するとすぐに LDAP 同期が実行されます。約 30 万ユーザーのユーザーデータを取得するには約 15 分かかり、12 時間ごとに自動的に更新されます。
ユーザーデータは LDAP から CloudSecure に同期されます。データはいつ削除されますか?	更新がない場合、ユーザーデータは 13 か月間保持されます。テナントが削除されると、データも削除されます。

問題：	解決：
LDAP ディレクトリ コネクタが「エラー」状態になります。 「コネクタはエラー状態です。サービス名: usersLdap。失敗の理由: LDAP ユーザーの取得に失敗しました。失敗の理由: 80090308: LdapErr: DSID-0C090453、コメント: AcceptSecurityContext エラー、データ 52e、v3839"	指定され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。
ユーザー プロフィール ページに電話番号が入力されません。	これは、Active Directory の属性マッピングの問題が原因であると考えられます。1. Active Directory からユーザーの情報を取得している特定の Active Directory コレクターを編集します。2.オプション属性の下に、Active Directory 属性「telephonenumber」にマップされたフィールド名「電話番号」があることに注意してください。4.ここで、上で説明した Active Directory Explorer ツールを使用して、LDAP ディレクトリ サーバーを参照し、正しい属性名を確認してください。3. LDAP ディレクトリに、実際にユーザーの電話番号を持つ「telephonenumber」という名前の属性があることを確認します。5. LDAP ディレクトリで「phonenumber」に変更されたとします。6.次に、CloudSecure ユーザー ディレクトリ コレクターを編集します。オプション属性セクションで、「telephonenumber」を「phonenumber」に置き換えます。7. Active Directory コレクターを保存すると、コレクターが再起動し、ユーザーの電話番号を取得して、ユーザー プロファイル ページに表示します。
Active Directory (AD) サーバーで暗号化証明書 (SSL) が有効になっている場合、Workload Security ユーザー ディレクトリ コレクターは AD サーバーに接続できません。	ユーザー ディレクトリ コレクターを構成する前に、AD サーバー暗号化を無効にします。ユーザーの詳細が取得されると、その情報は 13 か月間保存されます。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、AD に新しく追加されたユーザーは取得されません。再度取得するには、ユーザー ディレクトリ コレクターを AD に接続する必要があります。

ONTAP SVMデータコレクターの設定

ONTAP SVM データ コレクターを使用すると、Workload Security はNetApp ONTAPストレージ仮想マシン (SVM) 上のファイルおよびユーザー アクセス アクティビティを監視できます。このガイドでは、 ONTAP環境の包括的なセキュリティ監視を実現するための SVM データ コレクターの構成と管理について説明します。

開始する前に

- このデータ コレクターは以下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、 Data ONTAPバージョン 9.13.1 以降を使用してください。
  - SMB プロトコル バージョン 3.1 以前。

- NFS 4.1 までの NFS バージョン (NFS 4.1 はONTAP 9.15 以降でサポートされます)。
- FlexgroupはONTAP 9.4以降のバージョンでサポートされています
- FlexCache は、 ONTAP 9.7 以降のバージョンの NFS でサポートされます。
- FlexCache は、 ONTAP 9.14.1 以降のバージョンの SMB でサポートされます。
- ONTAP Selectがサポートされています

- データ型 SVM のみがサポートされます。無限ボリュームを持つ SVM はサポートされていません。
- SVM にはいくつかのサブタイプがあります。これらのうち、*default*、*sync_source*、および *sync_destination* のみがサポートされています。
- エージェント"設定する必要があります"データ コレクターを構成する前に。
- ユーザー ディレクトリ コネクタが適切に構成されていることを確認してください。適切に構成されていない場合、「アクティビティ フォレンジック」ページのイベントには、実際のユーザーの名前 (Active Directory に保存されている名前) ではなく、エンコードされたユーザー名が表示されます。
- ONTAP永続ストアは 9.14.1 からサポートされます。
- 最適なパフォーマンスを得るために、FPolicyサーバをストレージ システムと同一のサブネットに設定することを推奨します。
- Workload Security FPolicy設定に関する包括的なベストプラクティスと推奨事項については、"FPolicy ベストプラクティスに関する KB 記事" 。
- 次の 2 つの方法のいずれかを使用して SVM を追加する必要があります。
  - クラスタ IP、SVM 名、クラスタ管理ユーザー名とパスワードを使用します。 これが推奨される方法です。
    - SVM 名はONTAPに表示されているものと完全に一致している必要があり、大文字と小文字が区別されます。
  - SVM Vserver管理IP、ユーザー名、パスワードを使用する
  - 完全な管理者クラスタ/SVM管理ユーザー名とパスワードを使用できない場合、または使用したくない場合は、以下に記載されているように、より低い権限を持つカスタムユーザーを作成できます。「権限に関する注意事項」以下のセクションをご覧ください。このカスタム ユーザーは、SVM 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 ユーザーを使用することもできます。また、"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: clustershell:> `vserver cifs show`

  システムは、Vserver 名、CIFS サーバー名、および追加フィールドを返します。

- SVM vsadmin ユーザーのパスワードを設定します。カスタム ユーザーまたはクラスター管理者ユーザーを使用する場合は、この手順をスキップします。clustershell:> `security login password -username vsadmin -vserver svmname`
- 外部アクセス用に SVM vsadmin ユーザーのロックを解除します。カスタム ユーザーまたはクラスター管理者ユーザーを使用する場合は、この手順をスキップします。clustershell:> `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「mgmt」（「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、この手順をスキップしてください。clustershell:> `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 コレクターを使用するポートの 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。

  見る"エージェントの要件"構成情報については。これは、オンプレミスのエージェントとクラウドにインストールされたエージェントに適用されます。

- Cloud ONTAP SVM を監視するためにエージェントを AWS EC2 インスタンスにインストールする場合、エージェントとストレージは同じ VPC 内に存在する必要があります。別々の VPC にある場合は、VPC 間に有効なルートが必要です。

データコレクターの接続テスト

テスト接続機能 (2025 年 3 月に導入) は、 Data Infrastructure Insights (DII) ワークロード セキュリティでデータ コレクターを設定するときに、エンド ユーザーが障害の具体的な原因を特定できるようにすることを目的としています。これにより、ユーザーはネットワーク通信や役割の不足に関連する問題を自己修正できるようになります。

この機能は、データ コレクターを設定する前に、ネットワーク関連のすべてのチェックが実施されているかどうかをユーザーが確認するのに役立ちます。さらに、 ONTAPでユーザーに割り当てられたONTAP のバージョン、ロール、および権限に基づいて、ユーザーがアクセスできる機能についても通知します。

ユーザーディレクトリコレクターではテスト接続はサポートされていません

接続テストの前提条件

- この機能が完全に動作するには、クラスター レベルの認証情報が必要です。

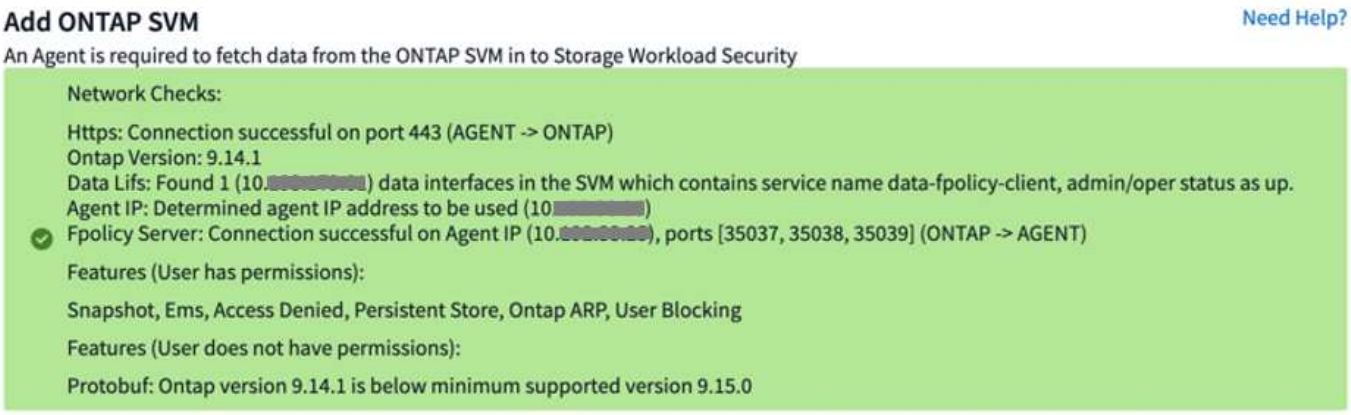
- SVM モードでは機能アクセス チェックはサポートされていません。
- クラスター管理資格情報を使用している場合は、新しい権限は必要ありません。
- カスタム ユーザー (例: *csuser*) を使用している場合は、使用する機能の必須権限と機能固有の権限を指定します。



必ず確認してください権限以下のセクションも同様です。

接続をテストする

ユーザーはコレクターの追加/編集ページに移動し、クラスター レベルの詳細 (クラスター モードの場合) または SVM レベルの詳細 (SVM モードの場合) を入力して、[接続のテスト] ボタンをクリックできます。Workload Security はリクエストを処理し、適切な成功または失敗のメッセージを表示します。



ONTAP Multi Admin Verify（MAV）の注意事項

スナップショットの作成と削除やユーザー ブロック（SMB）などの一部の機能は、ご使用のバージョンのONTAPに追加されたMAVコマンドによっては機能しない場合があります。

以下の手順に従って、MAV コマンドに除外を追加し、Workload Security がスナップショットを作成または削除したり、ユーザーをブロックしたりできるようにします。

スナップショットの作成と削除を許可するコマンド：

```
multi-admin-verify rule modify -operation "volume snapshot create" -query
"-snapshot !*cloudsecure_*"
multi-admin-verify rule modify -operation "volume snapshot delete" -query
"-snapshot !*cloudsecure_*"
```

ユーザーのブロックを許可するコマンド：

```
multi-admin-verify rule delete -operation set
```

ユーザーアクセスブロックの前提条件

以下の点に留意してください"ユーザーアクセスのブロック":

この機能が動作するには、クラスター レベルの資格情報が必要です。

クラスター管理資格情報を使用している場合は、新しい権限は必要ありません。

ユーザーに権限が付与されたカスタムユーザー（たとえば、*csuser*）を使用している場合は、次の手順に従ってください。"ユーザーアクセスのブロック" Workload Security にユーザーをブロックする権限を与えます。

権限に関する注意事項

*クラスタ管理**IP***経由で追加する場合の権限:

クラスタ管理管理者ユーザーを使用して Workload Security がONTAP SVM データ コレクターにアクセスできるようにできない場合は、以下のコマンドに示すように、ロールを持つ「csuser」という名前の新しいユーザーを作成できます。クラスタ管理 IP を使用するように Workload Security データ コレクターを構成するときは、ユーザー名「csuser」と「csuser」のパスワードを使用します。

注: カスタム ユーザーのすべての機能権限に使用する単一のロールを作成できます。既存のユーザーが存在する場合は、まず次のコマンドを使用して既存のユーザーとロールを削除します。

```
security login delete -user-or-group-name csuser -application *
security login role delete -role csrole -cmddirname *
security login rest-role delete -role csrestrole -api *
security login rest-role delete -role arwrole -api *
```

新しいユーザーを作成するには、クラスタ管理管理者のユーザー名/パスワードを使用してONTAPにログインし、 ONTAPサーバー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 role create -role csrole -cmddirname "cluster application-
record" -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
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole
```

Vserver 管理 **IP** 経由で追加する場合の権限:

クラスタ管理管理者ユーザーを使用して Workload Security がONTAP SVM データ コレクターにアクセスできるようにできない場合は、以下のコマンドに示すように、ロールを持つ「csuser」という名前の新しいユーザーを作成できます。 Vserver 管理 IP を使用するように Workload Security データ コレクターを構成するときは、ユーザー名「csuser」と「csuser」のパスワードを使用します。

注: カスタム ユーザーのすべての機能権限に使用する単一のロールを作成できます。既存のユーザーが存在する場合は、まず次のコマンドを使用して既存のユーザーとロールを削除します。

```
security login delete -user-or-group-name csuser -application * -vserver
<vservername>
security login role delete -role csrole -cmddirname * -vserver
<vservername>
security login rest-role delete -role csrestrole -api * -vserver
<vservername>
```

新しいユーザーを作成するには、クラスタ管理管理者のユーザー名/パスワードを使用してONTAPにログインし、 ONTAPサーバーで次のコマンドを実行します。簡単にするために、これらのコマンドをテキスト エディターにコピーし、<vservername> を Vserver 名に置き換えてから、 ONTAPでこれら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>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole -vserver <vservername>
```

プロトコルバッファモード

このオプションがコレクターの_詳細設定_設定で有効になっている場合、Workload Security は FPolicy エンジンを protobuf モードで設定します。 Protobuf モードは、 ONTAPバージョン 9.15 以降でサポートされています。

この機能の詳細については、"ONTAPのドキュメント" 。

protobuf 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既に存在している可能性があります)。

クラスターモード:

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Vserver モード:
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
```

ONTAP Autonomous Ransomware Protection および**ONTAP**アクセスの権限が拒否されました

クラスター管理資格情報を使用している場合は、新しい権限は必要ありません。

ユーザーに権限が付与されたカスタム ユーザー (たとえば、*csuser*) を使用している場合は、以下の手順に従って、Workload Security にONTAPから ARP 関連情報を収集する権限を付与します。

詳細については、以下をご覧ください。"ONTAPとの統合アクセスが拒否されました"

そして"ONTAP Autonomous Ransomware Protectionとの統合"

データコレクターを構成する

設定手順

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. ワークロード セキュリティ > コレクター > +データ コレクター をクリックします。

   システムは利用可能なデータ コレクターを表示します。

3. * NetApp SVM タイルにマウスを移動し、+ モニター をクリックします。

   ONTAP SVM 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
Name	データコレクターの一意の名前
エージェント	リストから構成済みの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のいずれかを選択します
クラスタ/SVM管理IPアドレス	上記の選択に応じて、クラスターまたは SVM の IP アドレス。
SVM 名	SVM の名前 (クラスタ IP 経由で接続する場合はこのフィールドが必須です)
ユーザー名	SVM/クラスターにアクセスするためのユーザー名。クラスター IP 経由で追加する場合のオプションは次のとおりです。1.クラスター管理者 2。 「csuser」3. csuser と同様の役割を持つ AD ユーザー。 SVM IP 経由で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。 csuser と同様の役割を持つ AD ユーザー名。
パスワード	上記のユーザー名のパスワード
シェア/ボリュームをフィルター	イベント収集に共有/ボリュームを含めるか除外するかを選択します
除外/含める完全な共有名を入力してください	イベント収集から除外または含める共有のコンマ区切りリスト（必要に応じて）
除外/含めるボリューム名を入力してください	イベント収集から除外または含めるボリュームのコンマ区切りリスト（必要に応じて）

フォルダーアクセスを監視する	チェックすると、フォルダー 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、フォルダーの作成/名前変更および削除は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する	ONTAP Fpolicy 送信バッファ サイズを設定します。9.8p7 より前のONTAPバージョンを使用していてパフォーマンスの問題が発生する場合は、 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ず、詳しく知りたい場合は、 NetAppサポートにお問い合わせください。

終了後の操作

- 「インストールされたデータ コレクター」ページで、各コレクターの右側にあるオプション メニューを使用して、データ コレクターを編集します。データ コレクターを再起動したり、データ コレクターの構成属性を編集したりできます。

MetroClusterの推奨構成

MetroClusterには以下が推奨されます。

1. 2 つのデータ コレクターを、1 つをソース SVM に、もう 1 つを宛先 SVM に接続します。
2. データ コレクターは *Cluster IP* によって接続する必要があります。
3. いつでも、現在「実行中」の SVM のデータ コレクターは「実行中」と表示されます。現在「停止」している SVM のデータ コレクターは、*Stopped* として表示されます。
4. 切り替えが発生するたびに、データ コレクターの状態は 実行中 から 停止 に変わり、その逆も同様になります。
5. データ コレクターが 停止 状態から 実行 状態に移行するまで最大 2 分かかります。

サービス ポリシー

ONTAP *バージョン 9.9.1 以降*でサービス ポリシーを使用する場合、データ ソース コレクターに接続するには、データ サービス *data-nfs* や *data-cifs* とともに *data-fpolicy-client* サービスが必要です。

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)
```

ONTAP 9.9.1 より前のバージョンでは、*data-fpolicy-client* を設定する必要はありません。

再生・一時停止データコレクター

データ コレクターが 実行中 状態の場合、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。コレクターが一時停止している間は、 ONTAPからデータは収集されず、コレクターからONTAPにデータは送信されません。つまり、Fpolicy イベントはONTAPからデータ コレクターに流れず、そこからData Infrastructure Insightsに流れません。

コレクターが一時停止中にONTAP上に新しいボリュームなどが作成された場合は、Workload Security はデータを収集せず、それらのボリュームなどは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。

> コレクターにユーザーが制限されている場合、コレクターを一時停止することはできません。コレクターを一時停止する前に、ユーザー アクセスを復元します。

次の事項に注意してください。

- 一時停止中のコレクターで構成された設定に従ってスナップショットの消去は実行されません。
- EMS イベント（ONTAP ARP など）は、一時停止中のコレクターでは処理されません。つまり、ONTAP がファイル改ざん攻撃を検知した場合、Data Infrastructure Insights Workload Security 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ーに対しては、ヘルス通知メールは送信されません。
- 一時停止中のコレクターでは、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のブロックなど) はサポートされません。
- エージェントまたはコレクターのアップグレード、エージェント VM の再起動、またはエージェント サービスの再起動が発生すると、一時停止中のコレクターは 一時停止 状態のままになります。
- データ コレクターが *Error* 状態の場合、コレクターを *Paused* 状態に変更することはできません。一時停止ボタンは、コレクターの状態が 実行中 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、コレクターを 一時停止 状態に変更することはできません。コレクターは 停止 状態になり、[一時停止] ボタンは無効になります。

永続ストア

永続ストアはONTAP 9.14.1 以降でサポートされています。ボリューム名の指示はONTAP 9.14 と 9.15 で異なることに注意してください。

コレクターの編集/追加ページでチェックボックスを選択することで、永続ストアを有効にできます。チェックボックスを選択すると、ボリューム名を入力するためのテキスト フィールドが表示されます。ボリューム名は、永続ストアを有効にするための必須フィールドです。

- ONTAP 9.14.1 の場合、機能を有効にする前にボリュームを作成し、[ボリューム名] フィールドに同じ名前を入力する必要があります。推奨ボリュームサイズは 16 GB です。
- ONTAP 9.15.1 の場合、*Volume Name* フィールドに指定された名前を使用して、コレクターによって 16 GB サイズのボリュームが自動的に作成されます。

永続ストア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既に存在している可能性があります)。

クラスターモード:

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "job show" -access
readonly
```

Vserver モード:

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"job show" -access readonly
```

コレクターの移行

Workload Security コレクターをあるエージェントから別のエージェントに簡単に移行できるため、エージェント間でコレクターの負荷を効率的に分散できます。

前提条件

- ソース エージェントは *connected* 状態である必要があります。
- 移行するコレクターは実行中状態である必要があります。

注：

- 移行は、データ コレクターとユーザー ディレクトリ コレクターの両方でサポートされています。
- 手動で管理されるテナントでは、コレクターの移行はサポートされません。

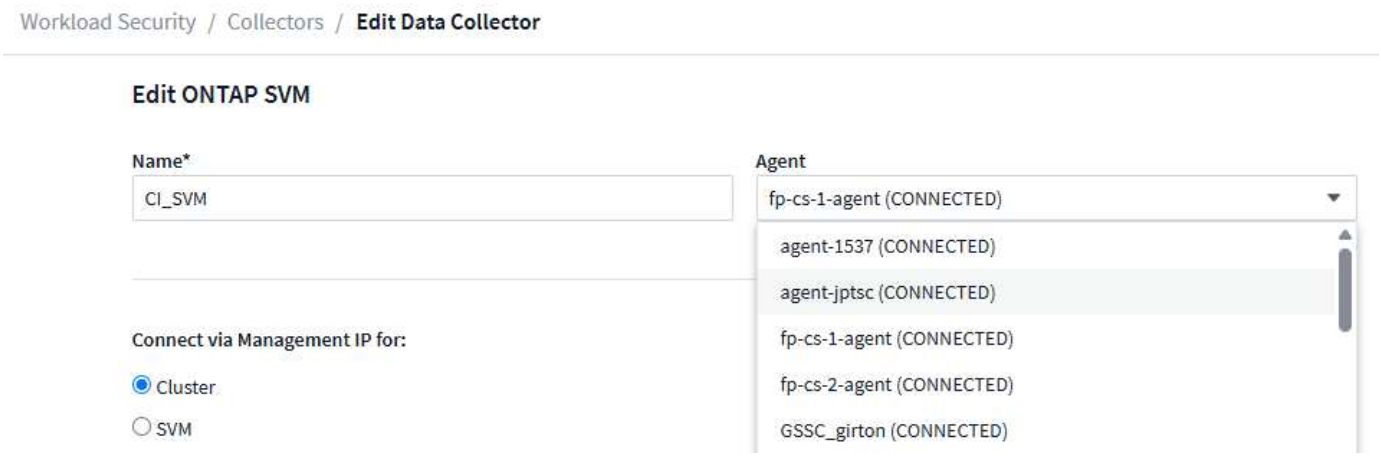
移行コレクター

コレクターを移行するには、次の手順に従います。

1. 「コレクターの編集」ページに移動します。
2. エージェント ドロップダウンから宛先エージェントを選択します。
3. 「コレクターを保存」ボタンをクリックします。

Workload Security がリクエストを処理します。移行が成功すると、ユーザーはコレクター リスト ページにリダイレクトされます。失敗した場合、編集ページに適切なメッセージが表示されます。

注意: 「コレクターの編集」ページで以前に行われた構成の変更は、コレクターが宛先エージェントに正常に移行されたときに適用されたままになります。



トラブルシューティング

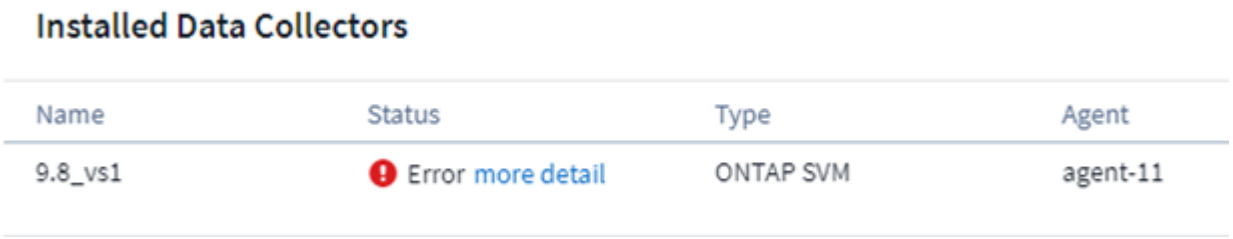
参照"SVMコレクターのトラブルシューティング"トラブルシューティングのヒントのページ。

ONTAP SVM データコレクタのトラブルシューティング

Workload Security はデータ コレクターを使用して、デバイスからファイルおよびユーザー アクセス データを収集します。ここでは、このコレクターに関する問題のトラブルシューティングのヒントを見つけることができます。

参照"SVMコレクターの設定"このコレクターを構成する手順については、このページをご覧ください。

エラーが発生した場合は、「インストールされたデータ コレクター」ページの [ステータス] 列の [詳細] をクリックすると、エラーの詳細が表示されます。



既知の問題とその解決策を以下に説明します。

問題: データ コレクターがしばらく実行され、ランダムな時間の経過後に停止し、次のエラーが発生します: 「エラー メッセージ: コネクタがエラー状態です。サービス名: 監査。失敗の理由: 外部ポリシー サーバーが過負荷です。これを試してください: ONTAPからのイベント レートは、エージェント ボックスが処理できるレートよりもはるかに高かったです。そのため接続は終了しました。

切断が発生したときの CloudSecure のピーク トラフィックを確認します。これは、**CloudSecure >** アクティビティフォレンジック **>** すべてのアクティビティ ページから確認できます。

ピーク集約トラフィックがエージェント ボックスで処理できる量を超える場合は、エージェント ボックスでのコレクター展開のサイズ設定方法について、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 日より前にエージェントがエージェント ボックスにインストールされていた場合は、エージェント ボックスで次のコマンドを実行します。

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

サイズ変更後、UI からコレクターを再起動します。

{空の}

問題: コレクターがエラー メッセージを報告します: 「SVM のデータ インターフェイスに到達できるコネクタにローカル IP アドレスが見つかりません」。 これを試してください: これは、 ONTAP側のネットワークの問題が原因である可能性が最も高いです。次の手順に従ってください。

1. SVM データ LIF または管理 LIF に SVM からの接続をブロックす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 経由で SVM を追加する場合は、SVM のデータ LIF と管理 LIF がエージェント VM から ping 可能であることを確認してください。問題が発生した場合は、LIF のゲートウェイ、ネットマスク、ルートを確認してください。

   クラスター管理 IP を使用して ssh 経由でクラスターにログインし、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、エージェント マシンが ping 可能であるように、 ONTAPのネットワーク設定が正しいことを確認します。

3. クラスタ IP 経由で接続しようとしたが機能しない場合は、SVM IP 経由で直接接続してみてください。SVM IP 経由で接続する手順については上記を参照してください。
4. SVM IP および vsadmin 資格情報を使用してコレクターを追加するときに、SVM Lif でデータ プラス Mgmt ロールが有効になっているかどうかを確認します。この場合、SVM Lif への ping は機能しますが、SVM Lif への SSH は機能しません。はいの場合は、SVM 管理専用 Lif を作成し、この SVM 管理専用 Lif 経由で接続してみます。
5. それでも動作しない場合は、新しい SVM Lif を作成し、その Lif を介して接続してみてください。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てください。
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 からデータ コレクターを SVM に接続してみます。
   c. エラーが表示されるまでお待ちください。 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。この場所で入手可能です

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. ONTAPからエージェント ボックスへの SYN があることを確認します。
.. ONTAPからの SYN がない場合、それはONTAPのファイアウォールに問題があります。
.. ONTAPでファイアウォールを開き、 ONTAP がエージェント
ボックスに接続できるようにします。
```

7. それでも動作しない場合は、ネットワーク チームに相談して、 ONTAPからエージェント ボックスへの接続が外部ファイアウォールによってブロックされていないことを確認してください。
8. 上記のいずれの方法でも問題が解決しない場合は、"NetApp サポート"さらにサポートが必要な場合はお問い合わせください。

{空の}

問題: メッセージ:「[ホスト名: <IP アドレス>] のONTAPタイプを判別できませんでした。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)" 次を試してください:

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. 接続先の SVM またはクラスターに SSH で接続します。接続したら、SVM またはクラスター名が正しいことを確認します。

{空の}

問題: 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: 監査。失敗の理由: 外部ポリシー サーバーが終了しました。 これを試してみてください:

1. おそらく、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ると考えられます。エージェント マシンが SVM から接続できるように、ポート範囲 35000 ～ 55000/tcp が開かれていることを確認します。また、 ONTAP側でエージェント 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も確認してください。
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 | grep 3500*
   ```

   サンプル出力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
   . 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確認する"ONTAP側で。

3. 監視する SVM/クラスターに SSH で接続します。 SVM データ LIF (CIFS、NFS プロトコルをサポート) からエージェント ボックスに ping を実行し、ping が機能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、エージェント マシンが ping 可能であるように、 ONTAPのネットワーク設定が正しいことを確認します。

4. 1 つの SVM が 2 つのデータ コレクターを介してテナントに 2 回追加されると、このエラーが表示されます。 UI を通じてデータ コレクターの 1 つを削除します。次に、UI を介して他のデータ コレクターを再起動します。その後、データ コレクターは「実行中」ステータスを表示し、SVM からのイベントの受信を開始します。

基本的に、テナントでは、1 つのデータ コレクターを介して 1 つの SVM を 1 回だけ追加する必要があります。 1 つの SVM を 2 つのデータ コレクター経由で 2 回追加しないでください。

5. 同じ SVM が 2 つの異なる Workload Security 環境 (テナント) に追加された場合には、最後の SVM が常に成功します。 2 番目のコレクターは独自の IP アドレスを使用して fpolicy を設定し、最初のコレクターを排除します。したがって、最初のコレクター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。これを防ぐには、各 SVM を単一の環境で構成します。
6. サービス ポリシーが正しく構成されていない場合にも、このエラーが発生する可能性があります。 ONTAP 9.8 以降では、データ ソース コレクターに接続するには、データ サービス data-nfs や data-cifs とともに、data-fpolicy-client サービスが必要です。さらに、data-fpolicy-client サービスは、監視対象 SVM のデータ lif に関連付けられている必要があります。

{空の}

問題: アクティビティ ページにイベントが表示されません。 これを試してみてください:

1. ONTAPコレクターが「RUNNING」状態であるかどうかを確認します。はいの場合は、いくつかのファイルを開いて、CIFS クライアント VM 上でいくつかの CIFS イベントが生成されていることを確認します。
2. アクティビティが見られない場合は、SVM にログインして次のコマンドを入力してください。

```
<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. アクティビティが見られない場合は、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「cloudsecure_」で名前が付けられた fpolicy ポリシーが設定されており、ステータスが「オン」になっているかどうかを確認します。設定されていない場合、エージェントは SVM でコマンドを実行できない可能性が高くなります。ページの冒頭に記載されているすべての前提条件が満たされていることを確認してください。

{空の}

問題: SVM データ コレクターがエラー状態にあり、エラー メッセージは「エージェントがコレクターへの接続に失敗しました」です。 次の操作を試してください:

1. おそらく、エージェントが過負荷になっており、データ ソース コレクターに接続できない状態です。
2. エージェントに接続されているデータ ソース コレクターの数を確認します。
3. また、UI の「すべてのアクティビティ」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 コレクターを新しいエージェントに移動します。

{空の}

問題: SVM データ コレクターに「fpolicy.server.connectError: ノードは FPolicy サーバー「12.195.15.146」との接続を確立できませんでした (理由:「選択がタイムアウトしました」)」というエラー メッセージが表示されます。 次のことを試してください: SVM/クラスター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 サーバーに接続できません。詳細情報を取得するために使用できるONTAPの CLI は次のとおりです。

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"ファイアウォールコマンドを確認する"ONTAP側で。

{空の}

問題: 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:監査。失敗の理由: SVM に有効なデータ インターフェイス (ロール: データ、データ プロトコル: NFS または CIFS またはその両方、ステータス: アップ) が見つかりません。 次のことを試してください: 動作可能なインターフェース (データとしての役割と CIFS/NFS としてのデータ プロトコルを持つ) があることを確認します。

{空の}

問題: データ コレクターがエラー状態になり、しばらくすると実行状態になり、その後再びエラー状態に戻ります。このサイクルが繰り返されます。 これを試してみてください: 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ーが追加されています。
2. このような動作を示すデータ コレクターには、1 つの SVM が追加されます。つまり、2 つ以上のデータ コレクターが 1 つの SVM に接続されます。
3. 1 つのデータ コレクターが 1 つの SVM にのみ接続す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 コレクターを削除します。

{空の}

問題: コネクタがエラー状態です。サービス名: 監査。失敗の理由: SVM svmname のポリシーの設定に失敗しました。理由: 'fpolicy.policy.scope-modify: "Federal" 内の 'shares-to-include' 要素に無効な値が指定されました。 次を試してください: *共有名は引用符なしで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。

共有を含めるおよび除外する は、共有名の長いリストを対象としていません。含めるまたは除外する株式が多数ある場合は、代わりに数量によるフィルタリングを使用します。

{空の}

問題: クラスター内に未使用の既存の fpolicies が存在します。 Workload Security をインストールする前に、これらに対して何をすべきでしょうか? これを試してください: 切断状態であっても、既存の未使用の fpolicy 設定をすべて削除することをお勧めします。 Workload Security は、プレフィックス「cloudsecure_」を持つ fpolicy を作成します。その他の未使用の fpolicy 構成はすべて削除できます。

fpolicy リストを表示する CLI コマンド:

```
 fpolicy show
fpolicy 構成を削除する手順:
```

```
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>
```

{空の}

問題: Workload Security を有効にすると、 ONTAP のパフォーマンスに影響が出ます。レイテンシが散発的に

高くなり、IOPS が散発的に低くなります。 これを試してください: ONTAP をWorkload Security とともに使用している場合、 ONTAPで遅延の問題が発生することがあります。これには、次に示すように、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 以降で修正されているため、これらの新しいバージョンのいずれかを使用することを強くお勧めします。

{空の}

問題: データ コレクターに次のエラー メッセージが表示されます:「エラー: 2 回の再試行でコレクターの状態を判別できませんでした。コレクターをもう一度再起動してください (エラー コード: AGENT008)」。 これを試してみてください:

1. 「データ コレクター」ページで、エラーが発生しているデータ コレクターの右までスクロールし、3 つのドット メニューをクリックします。 編集_を選択します。データコレクターのパスワードをもう一度入力してください。 _*Save* ボタンを押してデータ コレクターを保存します。データ コレクターが再起動し、エラーが解決されるはずです。
2. エージェント マシンに十分な CPU または RAM の余裕がないため、DSC が失敗する可能性があります。マシン内のエージェントに追加されているデータ コレクター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 および RAM 容量を増やしてください。 CPU と RAM が増加すると、DSC は自動的に初期化状態になり、その後実行状態になります。サイズガイドをご覧ください"このページ"。

{空の}

問題: SVM モードを選択すると、データ コレクターでエラーが発生します。 これを試してください: SVM モードで接続しているときに、SVM 管理 IP ではなくクラスター管理 IP を使用して接続すると、接続でエラーが発生します。正しい SVM IP が使用されていることを確認してください。

{空の}

問題: アクセス拒否機能が有効になっている場合、データ コレクターに次のエラー メッセージが表示されます:「コネクタはエラー状態です。サービス名: 監査。失敗の理由: SVM test_svm で fpolicy を設定できませんでした。理由: ユーザーは承認されていません。 これを試してください: ユーザーにアクセス拒否機能に必要な REST 権限がない可能性があります。以下の指示に従ってください"このページ"権限を設定します。

権限が設定されたら、コレクターを再起動します。

{空の}

問題: コレクターがエラー状態にあり、次のメッセージが表示されます: コネクタがエラー状態です。 失敗の理由: SVM <SVM 名> で永続ストアを構成できませんでした。 理由: SVM "<SVM Name>" 内のボリューム "<volumeName>" に適したアグリゲートが見つかりません。 理由: 集計 "<aggregateName>" のパフォーマンス情報は現在利用できません。サービス名: 監査。失敗の理由: SVM に永続的ストアを設定できませんでした。<svm name=""></svm>理由:ボリューム「」に適したアグリゲートが<volumename>SVM「<svm name="">」</svm>に</volumename>見つかりません。理由: アグリゲート「」のパフォーマンス情報<aggregatename>は現在使用できません。</aggregatename>数分待ってからもう一度コマンドを実行して

ください。

次の操作を試してください: 数分待ってからコレクターを再起動します。

{空の}

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。

Cloud Volumes ONTAPとAmazon FSx for NetApp ONTAPコレクターの構成

Cloud Volumes ONTAPおよびAmazon FSx for NetApp ONTAP用の Workload Security データコレクターを構成して、クラウド ストレージ インフラストラクチャ全体のファイルとユーザー アクセスを監視します。このガイドでは、AWS にエージェントをデプロイし、クラウド ストレージ インスタンスに接続するための手順を段階的に説明します。

Cloud Volumes ONTAPストレージ構成

Workload Security Agent をホストするための単一ノード/HA AWS インスタンスを構成するには、OnCommand Cloud Volumes ONTAP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 プロバイダーでサポートされています。例: Amazon、Azure、Google Cloud。
- ONTAP Amazon FSx

エージェントマシン構成

エージェント マシンは、クラウド サービス プロバイダーのそれぞれのサブネット内に構成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 でのエージェントのインストール手順です。インストールには、クラウド サービス プロバイダーに応じて、Azure または Google Cloud で同等の手順に従うことができます。

AWS では、次の手順に従って、マシンを Workload Security エージェントとして使用するように設定します。

Workload Security Agent として使用するマシンを設定するには、次の手順に従います。

手順

1. AWS コンソールにログインし、EC2 インスタンス ページに移動して、[インスタンスの起動] を選択します。
2. このページに記載されている適切なバージョンの 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. 割り当てリソースとして *t2.xlarge* (4 個の vCPU と 16 GB の 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 マネージャーを使用して必要な Linux パッケージをインストールします。
   a. ネイティブ Linux パッケージ *wget* および *unzip* をインストールします。

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する

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** に移動し、**Agents** タブをクリックします。
3. *+エージェント*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 インスタンスにエージェント インストール コマンドを貼り付けます。これにより、Workload Securityエージェントがインストールされ、"エージェントの前提条件"満たされます。

詳細な手順については、こ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
データコレクターによって「Workload Security: Amazon FxSN データコレクターのONTAPタイプを判別できませんでした」というエラーが表示されます。お客様は、新しい Amazon FSxN データコレクターを Workload Security に追加できません。エージェントからポート 443 上の FSxN クラスターへの接続がタイムアウトしています。ファイアウォールと AWS セキュリティグループには、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デプロイされており、同じ AWS アカウントに存在します。この同じエージェントは、残りのNetAppデバイス (すべて動作中) への接続と監視にも使用されます。	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。ポートが不明な場合は、すべてのポートを許可します。

ユーザー管理

Workload Security ユーザー アカウントは、Data Infrastructure Insightsを通じて管理されます。

Data Infrastructure Insights には、アカウント所有者、管理者、ユーザー、ゲストの 4 つのユーザー 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ー アカウントは、ユーザーを作成または変更し、各ユーザーに次のいずれかの Workload Security 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 コレクター、自動応答ポリシー、および Workload Security の API など、すべての Workload Security 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、割り当てることができるのは Workload Security のロールのみです。
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 ロールでは、アラートのステータスを変更したり、メモを追加したり、スナップショットを手動で取得したり、ユーザー アクセスを制限したりできます。
ゲスト	アラートと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 ステータスを変更したり、メモを追加したり、スナップショットを手動で取得したり、ユーザー アクセスを制限したりすることはできません。

手順

1. ワークロードセキュリティにログイン
2. メニューで*管理>ユーザー管理*をクリックします

   Data Infrastructure Insights のユーザー管理ページに転送されます。

3. 各ユーザーに対して希望するロールを選択します。

新しいユーザーを追加するときは、希望するロール (通常はユーザーまたはゲスト) を選択するだけです。

ユーザーアカウントとロールの詳細については、Data Infrastructure Insightsをご覧ください。"ユーザ ロール" ドキュメント。

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

データコレクタを導入する前に、SVM によって生成される NFS および SMB イベントレートを測定することで、最適な Agent マシンのサイジングを決定します。Event Rate Checker スクリプトは、容量制限（Agent あたり最大 50 のデータコレクタ）を理解し、Agent インフラストラクチャが予想されるイベント量を処理して信頼性の高い脅威検出を実現できることを確認するのに役立ちます。

要件：

- クラスターIP
- クラスター管理者のユーザー名とパスワード



このスクリプトを実行するときは、イベント レートを決定する SVM に対してONTAP SVM データ コレクターが実行されていない必要があります。

手順：

1. CloudSecure の指示に従ってエージェントをインストールします。
2. エージェントがインストールされたら、sudo ユーザーとして *server_data_rate_checker.sh* スクリプトを実行します。

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. このスクリプトを実行するには、Linux マシンに _sshpass_
がインストールされている必要があります。インストール方法は 2 つあります。
```

   a. 次のコマンドを実行します。

```
 linux_prompt> yum install sshpass
. . それでも問題が解決しない場合は、Web から Linux マシンに _sshpass_
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入力してください。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、スクリプトは SVM からのイベント レートを出力します。コンソール出力で 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 コレクターは単一の SVM に関連付けることができます。つまり、各データ コレクターは単一の SVM が生成するイベントの数を受信できるようになります。

次の事項に注意してください。

A) この表を一般的なサイズガイドとして使用してください。コア数やメモリ数を増やすと、サポートされるデータ コレクターの数を最大 50 個まで増やすことができます。

エージェントマシン構成	SVMデータコレクターの数	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人のデータ収集者	20Kイベント/秒
4コア、32GB	20人のデータ収集者	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間帯に実行されない場合、またはピークトラフィックを予測することが難しい場合

は、イベント レート バッファを 30% に維持します。

B + C は A より小さくなければなりません。そうでない場合、エージェント マシンは監視に失敗します。

つまり、単一のエージェント マシンに追加できるデータ コレクターの数は、次の式に従う必要があります。

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
```

参照link:concept_cs_agent_requirements.html["エージェントの要件"]追加の前提条件と要件については、ページをご覧ください。

例

それぞれ 1 秒あたり 100、200、300 イベントのイベント レートを生成する 3 つの SVMS があるとします。

次の式を適用します。

```
 (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。

次の場合には、スクリプトによって誤った結果が返される可能性があります。

- 不正な資格情報、IP、または SVM 名が指定されています。
- 同じ名前、シーケンス番号などを持つ既存の fpolicy はエラーになります。
- スクリプトは実行中に突然停止します。

スクリプトの実行例を以下に示します。

```
[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]#
```

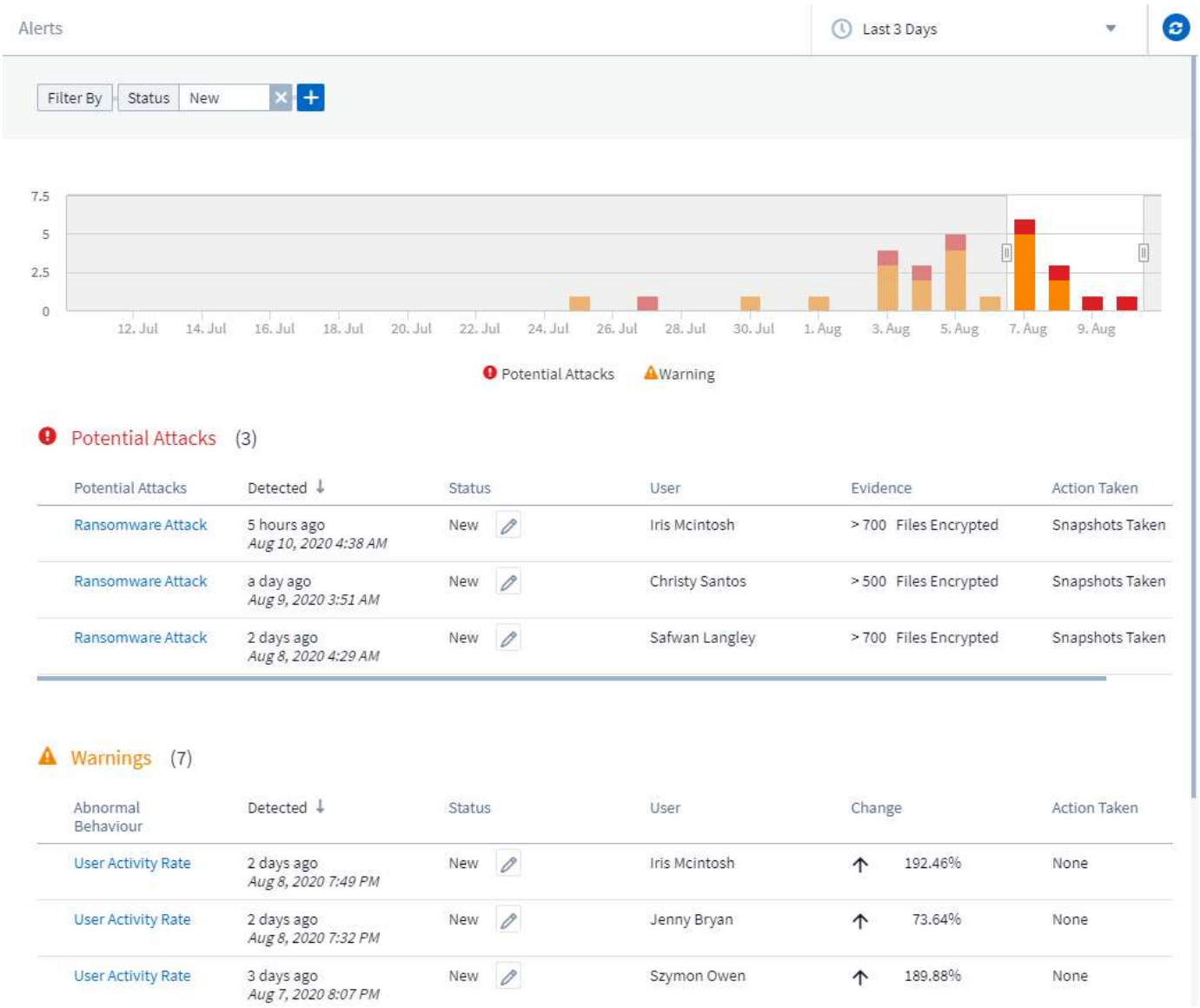
トラブルシューティング

質問	回答

Workload Security 用にすでに設定されている SVM でこのスクリプトを実行すると、SVM 上の既存の fpolicy 設定がそのまま使用されるのでしょうか、それとも一時的な設定が設定されてプロセスが実行されるのでしょうか?	イベント レート チェッカーは、すでに Workload Security 用に設定されている SVM でも正常に実行できます。影響はないはずです。
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?	○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も長くなりますか?	いいえ。SVM の数が増えても、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?	○スクリプトを編集し、SVM の最大数を 5 から任意の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も長くなりますか?	いいえ。SVM の数が増えても、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イベント レート チェッカー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と、SVM のレイテンシが増加する可能性があります。イベント レート チェッカーの実行中、この増加は一時的なものになります。

アラートの理解と調査

ワークロード セキュリティ アラート ページには、詳細な調査ツールとともに、検出された脅威と警告の包括的なタイムラインが表示されます。アラートの詳細を表示し、ステータスの更新を管理し、条件でフィルタリングし、ユーザー アクティビティを追跡して、セキュリティ インシデントを効率的に調査して対応します。



アラート

アラート リストには、選択した時間範囲内で発生した潜在的な攻撃および/または警告の合計数を示すグラフと、その時間範囲内で発生した攻撃および/または警告のリストが表示されます。グラフ内の開始時間と終了時間のスライダーを調整することで、時間範囲を変更できます。

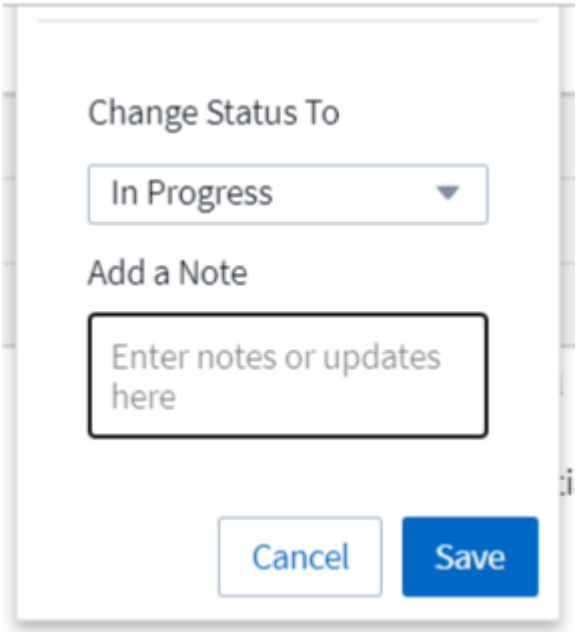
各アラートには次の内容が表示されます。

潜在的な攻撃:

- _潜在的な攻撃_の種類（例：ファイルの改ざんや妨害行為）
- 潜在的な攻撃が_検出された_日時
- アラートの_ステータス_:
  - 新規: これは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してマークされました。

◦ 無視: アラートは誤検知または予期された動作として無視されました。

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行動をした_ユーザー_
- 攻撃の_証拠_（例えば、大量のファイルが暗号化された）
- 実行されたアクション（例：スナップショットが取得された）

警告:

- 警告を引き起こした異常な行動
- 行動が_検出された_日時
- アラートのステータス（新規、進行中など）
- アラートをトリガーした行動をした_ユーザー_
- 変更の説明（例：ファイルアクセスの異常な増加）
- 取られた行動

フィルターオプション

アラートは次のようにフィルタリングできます。

- アラートのステータス
- *Note* 内の特定のテキスト
- _攻撃/警告_の種類
- アラート/警告を引き起こしたユーザー

アラートの詳細ページ

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、アラートの詳細ページが開きます。アラートの詳細は、攻撃またはアラートの種類によって異なる場合があります。たとえば、ファイル改ざん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。

概要セクション:

- 攻撃の種類（ファイル改ざん、妨害行為）とアラートID（Workload Securityによって割り当てられる）
- 攻撃が検出された日時
- 実行されたアクション (たとえば、自動スナップショットが取得されました)。スナップショットの時刻は、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）

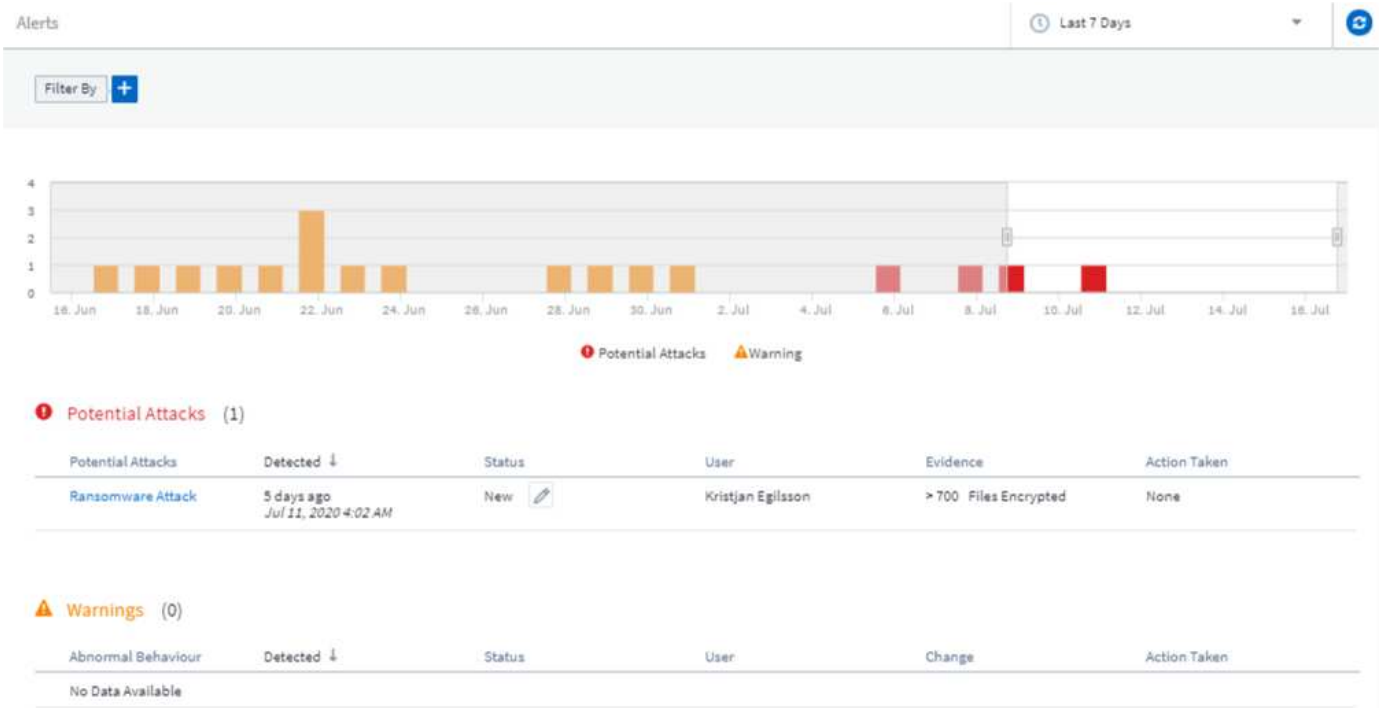
攻撃結果セクション:

- 影響を受けるボリュームとファイルの数
- 検出結果の要約
- 攻撃中のファイルアクティビティを示すグラフ

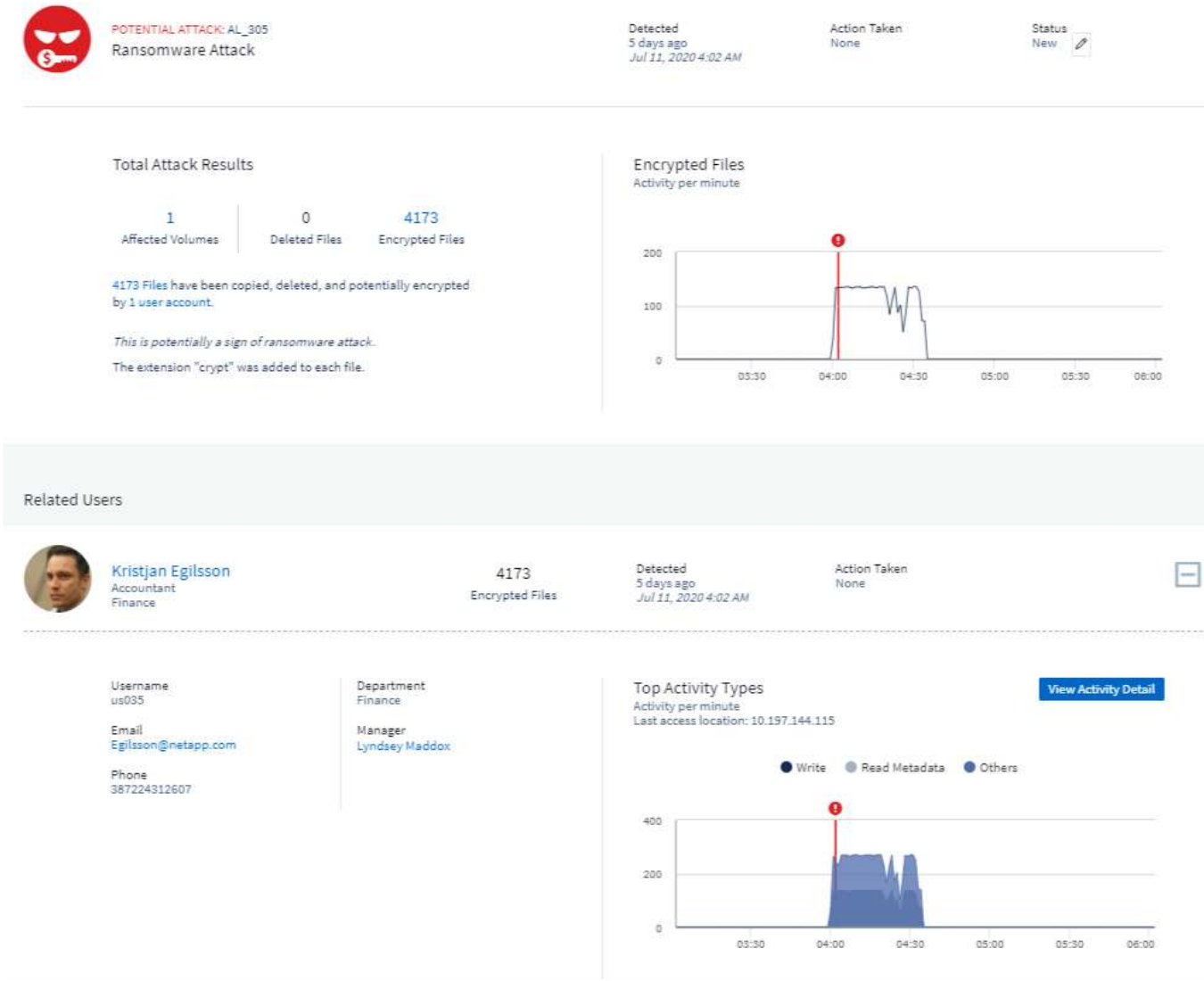
関連ユーザーセクション:

このセクションには、ユーザーのトップアクティビティのグラフなど、潜在的な攻撃に関与したユーザーの詳細が表示されます。

アラート ページ (この例では、潜在的なファイル改ざん攻撃を示しています):



詳細ページ (この例では、潜在的なファイル改ざん攻撃を示しています):

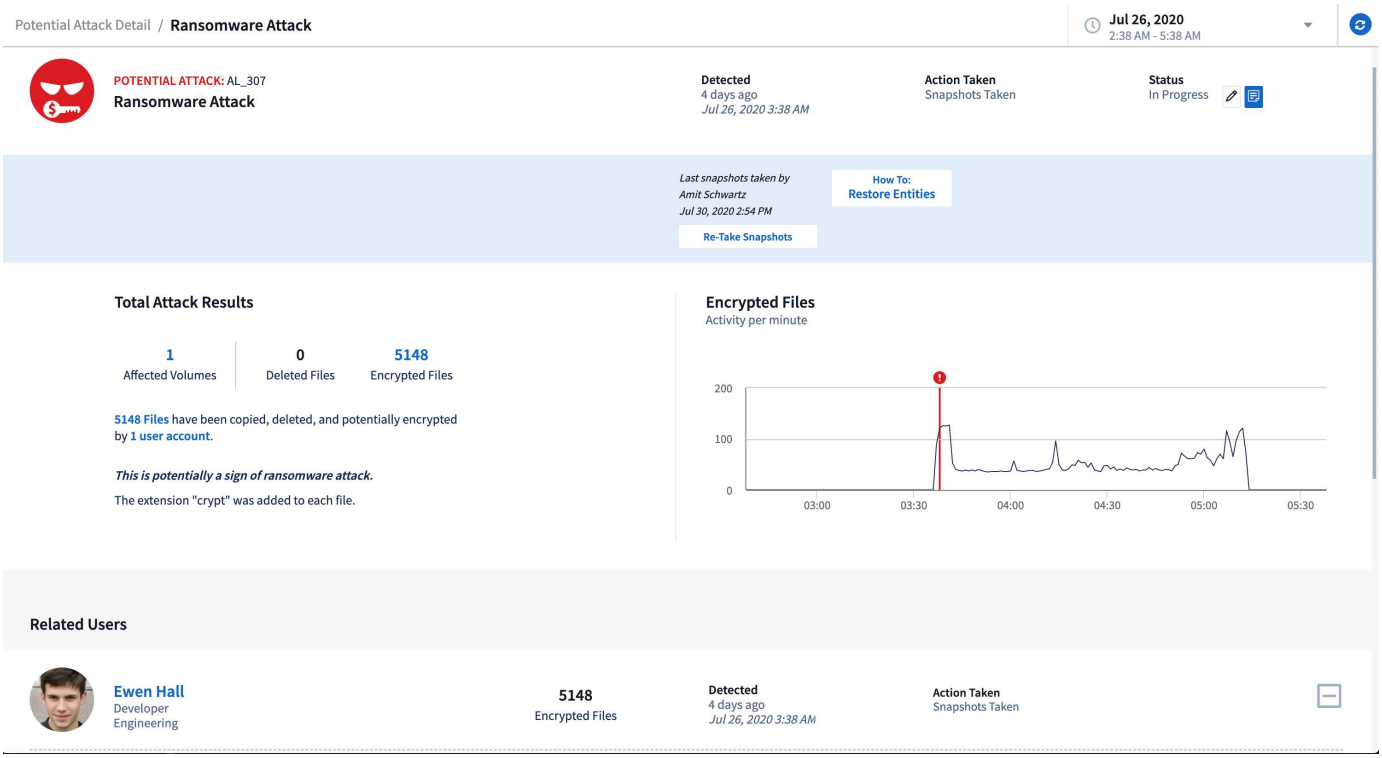


_スナップショットを撮る_アクション

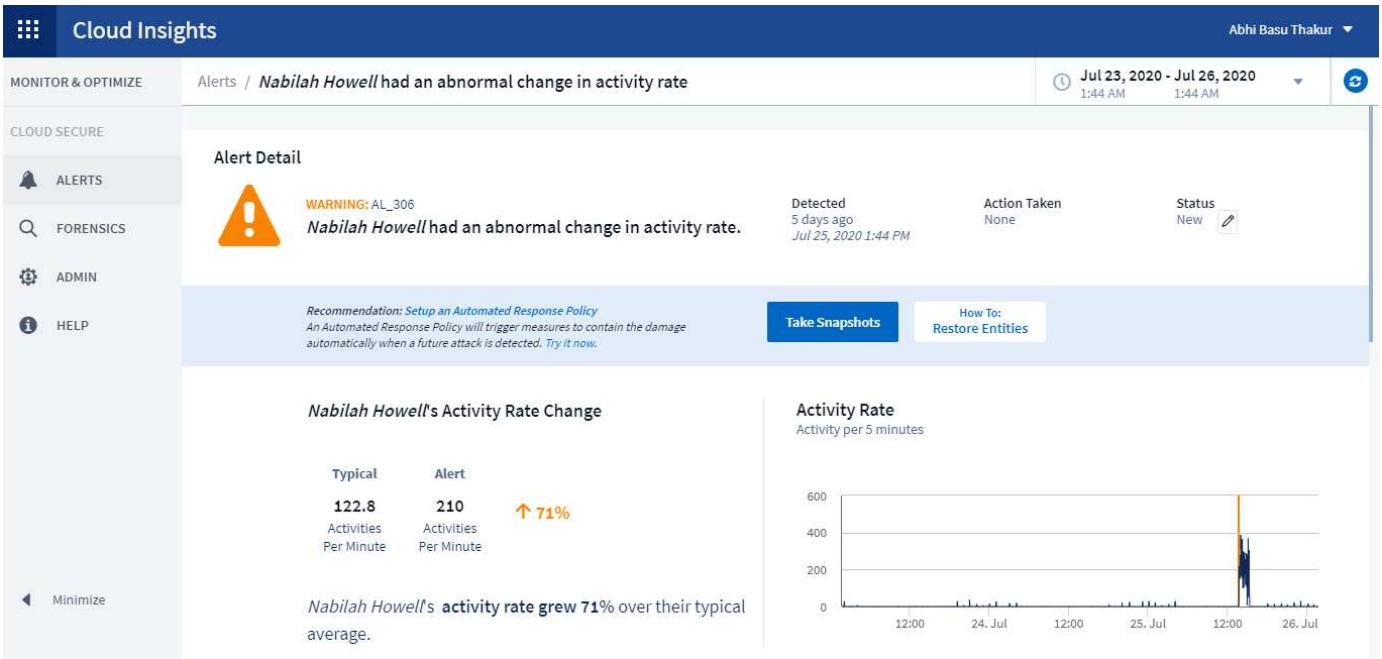
Workload Security は、悪意のあるアクティビティが検出されると自動的にスナップショットを取得してデータを保護し、データが安全にバックアップされることを保証します。

定義できます "自動応答ポリシー" ファイル改ざん攻撃やその他の異常なユーザー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得します。アラート ページから手動でスナップショットを取得することもできます。

自動スナップショットが取得されました
:



手動スナップショット
:



アラート通知

アラートに関するアクションごとに、アラートの電子メール通知がアラート受信者リストに送信されます。アラートの受信者を設定するには、管理 > 通知 をクリックし、各受信者の電子メール 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 か月間保持されます。 13 か月以上経過したアラートと警告は削除されます。 Workload

Security 環境が削除されると、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：	これを試してください:
ONTAP が1 日あたり 1 時間ごとにスナップショットを取得する状況があります。 Workload Security (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 1 時間ごとのスナップショットの場所を占めますか? デフォルトの 1 時間ごとのスナップショットは停止されますか?	Workload Security スナップショットは、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 1 時間ごとのスナップショット スペースを占有しないため、これまでどおり継続されるはずです。デフォルトの 1 時間ごとのスナップショットは停止されません。
ONTAPで最大スナップショット数に達するとどうなりますか?	最大スナップショット数に達すると、後続のスナップショットの取得は失敗し、スナップショットがいっぱいであることを示すエラー メッセージが Workload Security に表示されます。ユーザーは、最も古いスナップショットを削除するようにスナップショット ポリシーを定義する必要があります。そうしないと、スナップショットは作成されません。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。詳細については、 ONTAPのドキュメントを参照してください。"スナップショット削除ポリシーの設定" 。
Workload Security ではスナップショットをまったく取得できません。	スナップショットの作成に使用されているロールにリンク: 適切な権限が割り当てられていることを確認してください。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
Workload Security から削除され、その後再度追加された SVM 上の古いアラートのスナップショットが失敗します。 SVM が再度追加された後に発生する新しいアラートについては、スナップショットが取得されます。	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、古いアラートのスナップショットを手動で取得してください。
アラートの詳細 ページで、スナップショットの取得 ボタンの下に「前回の試行が失敗しました」というエラー メッセージが表示されます。エラーの上にマウスを置くと、「ID を持つデータ コレクターの Invoke API コマンドがタイムアウトしました」と表示されます。	これは、SVM の LIF がONTAPで *disabled* 状態の場合に、SVM 管理 IP を介してデータ コレクターが Workload Security に追加されたときに発生する可能性があります。 ONTAPで特定の LIF を有効にし、Workload Security から 手動でスナップショットを取得 をトリガーします。スナップショットアクションは成功します。

法医学

法医学 - すべての活動

「すべてのアクティビティ」ページは、Workload Security 環境内のエンティティに対し

て実行された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の調査

フォレンジック > アクティビティ フォレンジック をクリックし、すべてのアクティビティ タブをクリックして、すべてのアクティビティ ページにアクセスします。このページには、テナントでのアクティビティの概要が示され、次の情報が強調表示されます。

- アクティビティ履歴 を示すグラフ（選択したグローバル時間範囲に基づく）

  グラフ内で四角形をドラッグすると、グラフを拡大できます。ページ全体が読み込まれ、ズームされた時間範囲が表示されます。ズームインすると、ズームアウトできるボタンが表示されます。

- すべてのアクティビティ データのリスト。
- グループ化ドロップダウンでは、ユーザー、フォルダー、エンティティ タイプなどでアクティビティをグループ化するオプションが提供されます。
- テーブルの上に共通パス ボタンがあり、それをクリックするとエンティティ パスの詳細を含むスライドアウト パネルが表示されます。

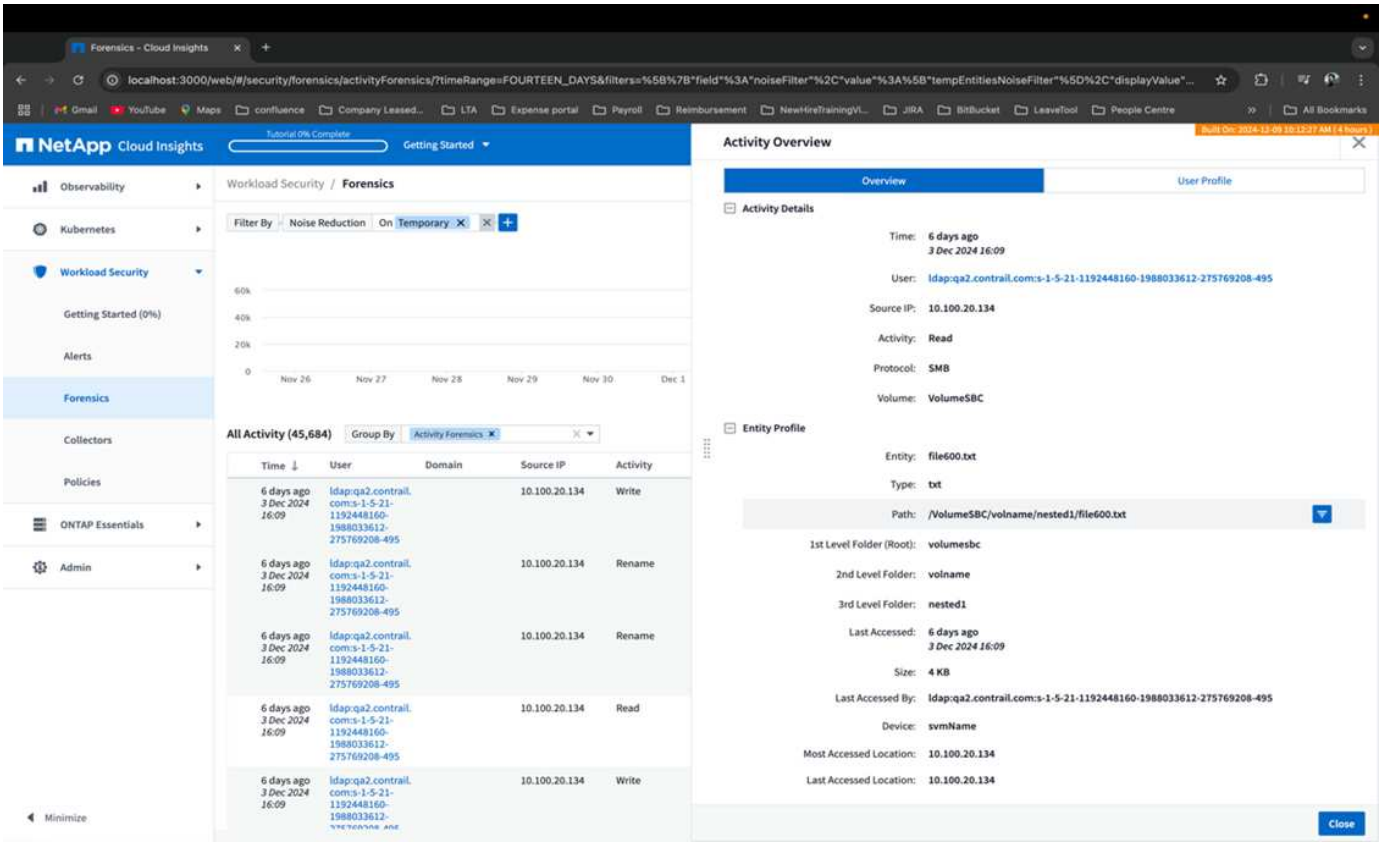
すべてのアクティビティ テーブルには次の情報が表示されます。これらの列のすべてがデフォルトで表示されるわけではないことに注意してください。 「歯車」アイコンをクリックすると、表示する列を選択できます。

- エンティティがアクセスされた 時間 (最終アクセスの年、月、日、時刻を含む)。
- リンクを使用してエンティティにアクセスした*ユーザー*"ユーザー情報"スライドアウトパネルとして。
- ユーザーが実行した*アクティビティ*。サポートされているタイプは次のとおりです:
  - グループ所有権の変更 - ファイルまたはフォルダーのグループ所有権が変更されます。グループの所有権の詳細については、以下を参照してください。"このリンク。"
  - 所有者の変更 - ファイルまたはフォルダーの所有権が別のユーザーに変更されます。
  - 権限の変更 - ファイルまたはフォルダーの権限が変更されます。
  - 作成 - ファイルまたはフォルダーを作成します。
  - 削除 - ファイルまたはフォルダを削除します。フォルダーが削除されると、そのフォルダーとサブフォルダー内のすべてのファイルに対して *delete* イベントが取得されます。
  - 読み取り - ファイルが読み取られました。
  - メタデータの読み取り - フォルダー監視オプションを有効にした場合のみ。 Windows でフォルダーを開くか、Linux でフォルダー内で「ls」を実行すると生成されます。
  - 名前の変更 - ファイルまたはフォルダーの名前を変更します。
  - 書き込み - データがファイルに書き込まれます。
  - メタデータの書き込み - 権限の変更など、ファイルのメタデータが書き込まれます。
  - 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。ファイルとフォルダーに適用できます。
- パス*は**_entity_**パスです。これは、正確なエンティティ パス **(**例**:** **"*/home/userX/nested1/nested2/abc.txt*")** または再帰検索のパスのディレクトリ部分 **(**例**:**

"/home/userX/nested1/nested2/") のいずれかである必要があります。注意: 正規表現のパス パターン (例: ***nested**) はここでは許可されません。あるいは、パス フィルタリングには、以下に示すような個別のパス フォルダー レベルのフィルターを指定することもできます。

- 第 **1** レベル フォルダー **(**ルート**)** は、小文字のエンティティ パスのルート ディレクトリです。
- **2** 番目のレベルのフォルダー は、小文字のエンティティ パスの 2 番目のレベルのディレクトリです。
- **3** 番目のレベルのフォルダー は、小文字のエンティティ パスの 3 番目のレベルのディレクトリです。
- **4** 番目のレベルのフォルダー は、小文字のエンティティ パスの 4 番目のレベルのディレクトリです。
- 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) を含む)。
- エンティティが存在する*デバイス*。
- イベントを取得するために使用される*プロトコル*。
- 元のファイルの名前が変更されたときに名前変更イベントに使用される 元のパス。この列はデフォルトではテーブルに表示されません。列セレクターを使用して、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*。この列はデフォルトではテーブルに表示されません。列セレクターを使用して、この列をテーブルに追加します。
- エンティティ名 は、エンティティ パスの最後のコンポーネントです。エンティティ タイプがファイルの場合、これはファイル名です。

テーブル行を選択すると、スライド アウト パネルが開き、1 つのタブにユーザー プロファイル、別のタブにアクティビティとエンティティの概要が表示されます。



デフォルトの *Group by* 方法は *Activity forensics* です。別の *Group By* 方法 (たとえば、エンティティ タイプ) を選択した場合は、エンティティの *Group By* テーブルが表示されます。選択が行われていない場合は、「グループ化」で すべて が表示されます。

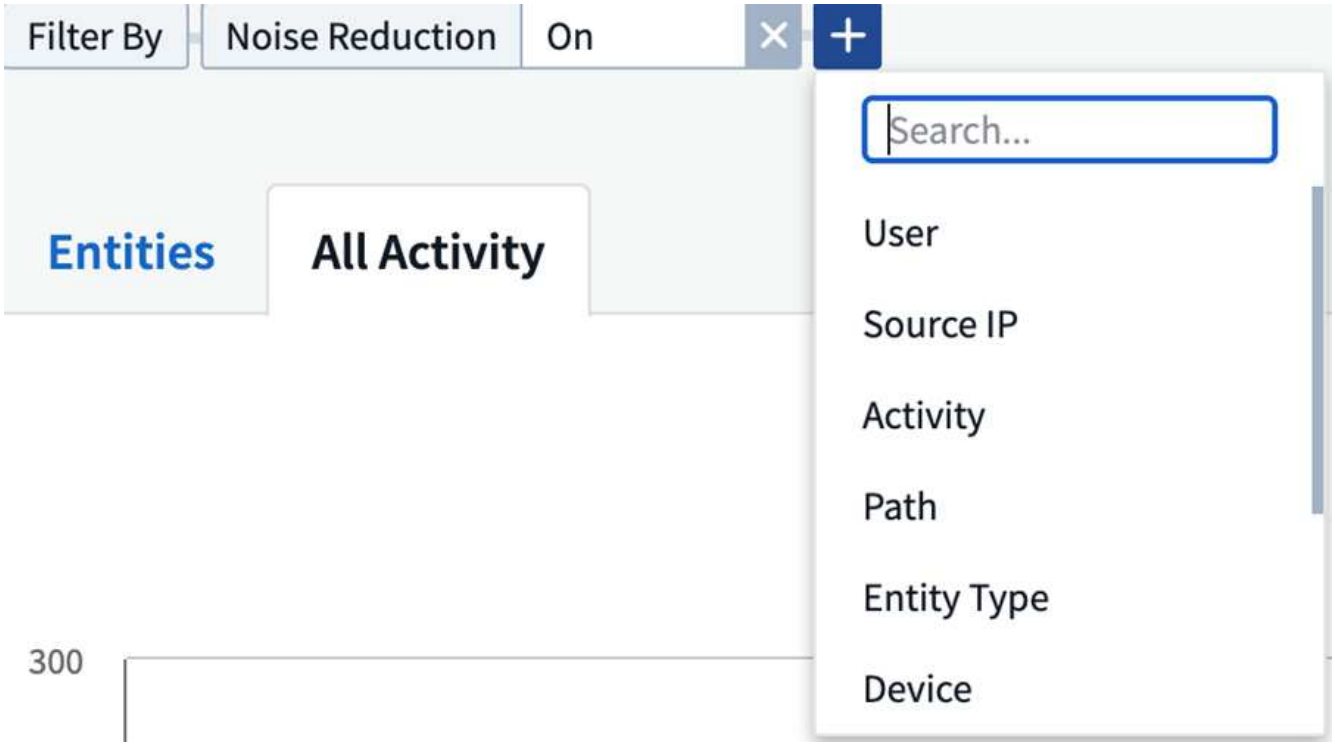
- アクティビティ数はハイパーリンクとして表示されます。これを選択すると、選択したグループがフィルターとして追加されます。そのフィルターに基づいてアクティビティ テーブルが更新されます。
- フィルターを変更したり、時間範囲を変更したり、画面を更新したりした場合は、フィルターを再度設定しないとフィルタリングされた結果に戻ることができないことに注意してください。
- エンティティ名がフィルターとして選択されている場合、グループ化ドロップダウンは無効になることに注意してください。また、ユーザーがすでにグループ化画面にいる場合、エンティティ名をフィルターとして使用することは無効になります。

フォレンジック活動履歴データのフィルタリング

データをフィルタリングするには 2 つの方法があります。

- フィルターはスライドアウト パネルから追加できます。値は、上部の [フィルター条件] リスト内の適切なフィルターに追加されます。
- *Filter By* フィールドに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、上部の [フィルター条件] ウィジェットから適切なフィルターを選択します。



  検索テキストを入力してください

  フィルターを適用するには、Enter キーを押すか、フィルター ボックスの外側をクリックします。

次のフィールドでフォレンジック アクティビティ データをフィルターできます。

- アクティビティ タイプ。
- プロトコル は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するユーザーの*ユーザー名*。フィルタリングするには正確なユーザー名を入力する必要があります。ユーザー名の一部、またはユーザー名の先頭または末尾に「*」が付いた部分的な検

索は機能しません。

- ノイズ低減 は、ユーザーが過去 2 時間以内に作成したファイルをフィルターします。また、ユーザーがアクセスする一時ファイル (.tmp ファイルなど) をフィルター処理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。フィルタリングするには*正確なドメイン*を指定する必要があります。部分的なドメイン、またはワイルドカード ('*') がプレフィックスまたはサフィックスとして付いた部分的なドメインの検索は機能しません。不足しているドメインを検索するには、*None* を指定できます。

次のフィールドには特別なフィルタリング 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) - 引用符で囲ん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。たとえば、「txt」。
- エンティティのパス - これは正確なエンティティ パス (例: "*/home/userX/nested1/nested2/abc.txt*") または再帰検索のパスのディレクトリ部分 (例: "*/home/userX/nested1/nested2/*") のいずれかである必要があります。注意: 正規表現のパス パターン (例: *nested*) はここでは許可されません。より速く結果を得るためには、最大 4 つのディレクトリの深さまでのディレクトリ パス フィルター (/ で終わるパス文字列) が推奨されます。たとえば、「*/home/userX/nested1/nested2/*」です。詳細については、以下の表を参照してください。
- 第 1 レベル フォルダー (ルート) - フィルターとしてのエンティティ パスのルート ディレクトリ。たとえば、エンティティ パスが /home/userX/nested1/nested2/ の場合、home または "home" を使用できます。
- 第 2 レベル フォルダー - エンティティ パス フィルターの第 2 レベル ディレクトリ。たとえば、エンティティ パスが /home/userX/nested1/nested2/ の場合、userX または "userX" を使用できます。
- 3 番目のレベルのフォルダー – エンティティ パス フィルターの 3 番目のレベルのディレクトリ。
- たとえば、エンティティ パスが /home/userX/nested1/nested2/ の場合、nested1 または "nested1" を使用できます。
- 4 番目のレベルのフォルダー - ディレクトリ エンティティ パス フィルターの 4 番目のレベルのディレクトリ。たとえば、エンティティ パスが /home/userX/nested1/nested2/ の場合、nested2 または "nested2" を使用できます。
- ユーザー アクティビティを実行します - 引用符で囲ん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、「管理者」などです。
- エンティティが存在する*デバイス*（SVM）
- エンティティが存在する*ボリューム*
- 元のファイルの名前が変更されたときに名前変更イベントに使用される 元のパス。
- エンティティにアクセスした ソース **IP**。
  - ワイルドカード * と？を使用できます。例: 10.0.0.、**10.0?.0.10**、**10.10**
  - 完全一致が必要な場合は、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..*」などの二重引用符で囲まれた不完全な IP は機能しません。
- エンティティ名 - フィルターとしてのエンティティ パスのファイル名。たとえば、エンティティ パスが /home/userX/nested1/testfile.txt の場合、エンティティ名は testfile.txt になります。正確なファイル名を引用符で囲んで指定することをお勧めします。ワイルドカード検索は避けてください。たとえば、「testfile.txt」。また、このエンティティ名フィルターは、より短い時間範囲 (最大 3 日間) に推奨されることに注意してください。

上記のフィールドは、フィルタリング時に次の条件に従います。

- 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を含めることはできません。例: searchtext、*searchtext* は、'searchtext' を含むすべての文字列をフィルターします。
- プレフィックス付きの文字列 (例: searchtext*) は、'searchtext' で始まるすべての文字列を検索します。

すべてのフィルター フィールドでは大文字と小文字が区別されない検索が行われることに注意してください。たとえば、適用されたフィルターが「searchtext」のエンティティ タイプである場合、エンティティ タイプが「searchtext」、「SearchText」、「SEARCHTEXT」である結果が返されます。

アクティビティフォレンジックフィルターの例:

ユーザーが適用したフィルター式	期待される結果	パフォーマンス評価	コメント
パス = "/home/userX/nested1/nested2/"	指定され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を再帰的に検索します	速い	最大 4 つのディレクトリまでのディレクトリ検索が高速になります。
パス = "/home/userX/nested1/"	指定され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を再帰的に検索します	速い	最大 4 つのディレクトリまでのディレクトリ検索が高速になります。
パス = "/home/userX/nested1/test"	パス値が /home/userX/nested1/test と一致する完全一致	遅い	完全一致検索では、ディレクトリ検索に比べて検索に時間がかかります。
パス = "/home/userX/nested1/nested2/nested3/"	指定され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を再帰的に検索します	遅い	4 つ以上のディレクトリを検索すると、検索速度が低下します。
その他の非パスベース フィルター。ユーザーおよびエンティティ タイプ フィルターは引用符で囲むことをお勧めします (例: User="Administrator" Entity Type="txt")。		速い	
エンティティ名 = "test.log"	ファイル名が test.log である完全一致	速い	完全一致なので
エンティティ名 = *test.log	test.log で終わるファイル名	遅い	ワイルドカードのため、遅くなる可能性があります。
エンティティ名 = test*.log	ファイル名は test で始まり .log で終わります	遅い	ワイルドカードのため、遅くなる可能性があります。
エンティティ名 = test.lo	test.loで始まるファイル名例えば、test.log 、test.log.1、test.log1に一致します。	遅い	最後にワイルドカードがあるため、遅くなる可能性があります。

ユーザーが適用したフィルター式	期待される結果	パフォーマンス評価	コメント
エンティティ名 = テスト	testで始まるファイル名	最も遅い	最後にワイルドカードがあり、より一般的な値が使用されるため、最も遅くなる可能性があります。

注：

1. [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、選択した時間範囲が 3 日を超える場合、30 分に切り上げられます。たとえば、時間範囲が「9 月 1 日午前 10 時 15 分から 9 月 7 日午前 10 時 15 分」の場合、9 月 1 日午前 10 時から 9 月 7 日午前 10 時 30 分までのアクティビティ数が表示されます。
2. 同様に、選択した時間範囲が 3 日を超える場合、アクティビティ履歴グラフに表示されるカウント メトリックは 30 分に切り上げられます。

フォレンジック活動履歴データの分類

アクティビティ履歴データは、時間、ユーザー、ソース *IP*、アクティビティ、、エンティティ タイプ、第 1 レベル フォルダー (ルート)、第 2 レベル フォルダー、第 3 レベル フォルダー、および第 4 レベル フォルダーで並べ替えることができます。デフォルトでは、テーブルは降順の 時間 順に並べ替えられ、最新のデータが最初に表示されます。 *Device* フィールドと *Protocol* フィールドでは並べ替えが無効になっています。

非同期エクスポートのユーザーガイド

概要

Storage Workload Security の非同期エクスポート機能は、大規模なデータの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によるデータのエクスポート

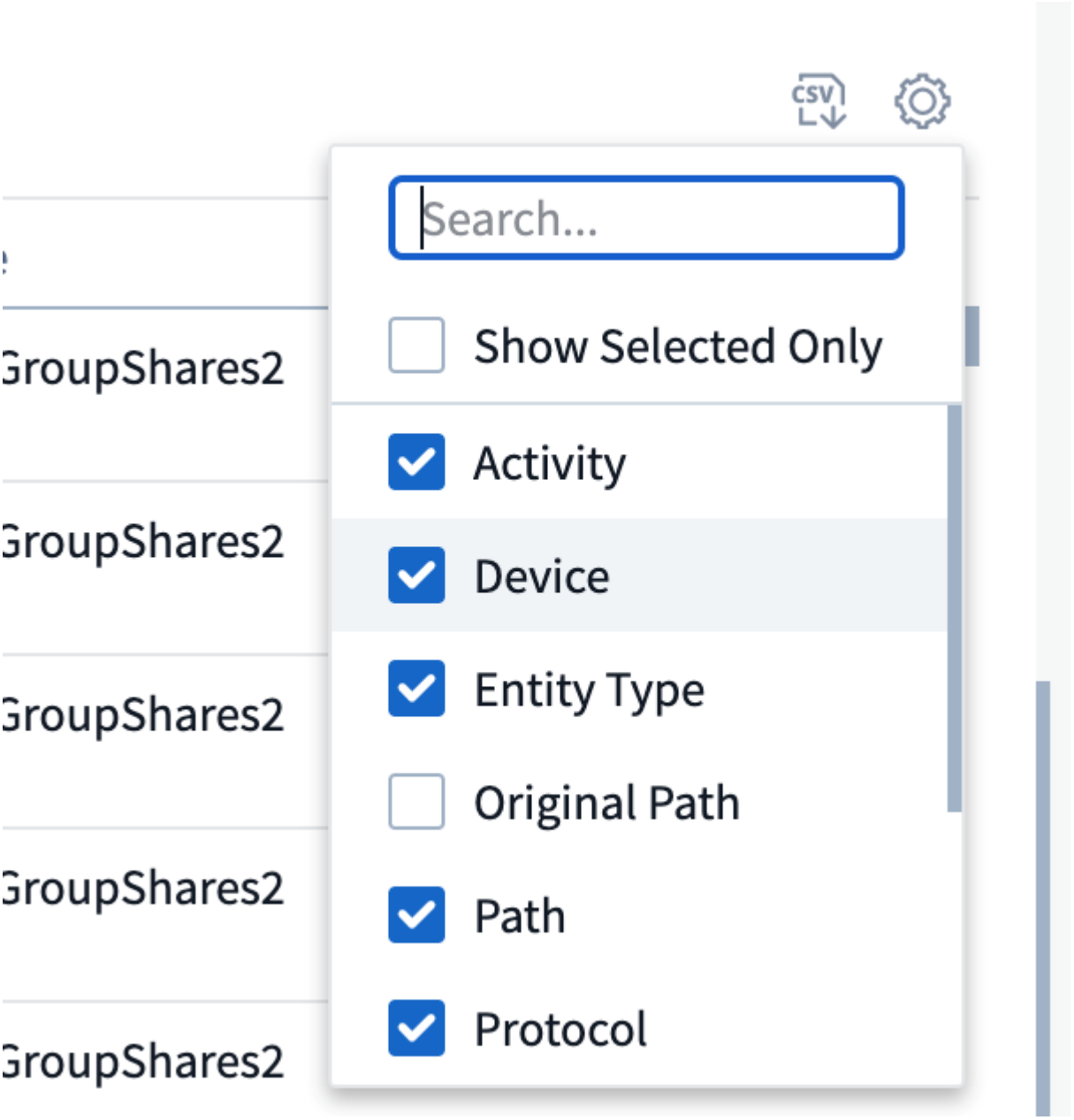
1. エクスポートの開始: エクスポートの希望する期間とフィルターを選択し、エクスポート ボタンをクリックします。
2. エクスポートが完了するまで待機: 処理時間は数分から数時間の範囲になります。フォレンジック ページを数回更新する必要がある場合があります。エクスポート ジョブが完了すると、「最後のエクスポート CSV ファイルをダウンロード」ボタンが有効になります。
3. ダウンロード: 「最後に作成されたエクスポート ファイルをダウンロード」ボタンをクリックすると、エクスポートされたデータが .zip 形式で取得されます。このデータは、ユーザーが別の非同期エクスポートを開始するか、3 日が経過するまで、いずれか早い方までダウンロードできます。別の非同期エクスポートが開始されるまで、ボタンは有効なままになります。
4. 制限事項:
    - 非同期ダウンロードの数は、現在、アクティビティおよびアクティビティ分析テーブルごとにユーザーあたり 1 回、テナントあたり 3 回に制限されています。
    - エクスポートされるデータは、アクティビティ テーブルの場合は最大 100 万レコードに制限されますが、グループ化の場合は 50 万レコードに制限されます。

API 経由でフォレンジック データを抽出するサンプル スクリプトは、エージェントの

/opt/netapp/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選択

すべてのアクティビティ テーブルには、デフォルトで選択した列が表示されます。列を追加、削除、または変更するには、表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

アクティブな Workload Security 環境のアクティビティ履歴は 13 か月間保持されます。

フォレンジックにおけるフィルターの適用性ページ

フィルタ	何をするのか	例	これらのフィルターに適用可能	これらのフィルターには適用されません	結果
*（アスタリスク）	あらゆるものを検索できます	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、括弧で囲んで表現を入力してください。例：svm-123を検索する場合は(svm*)	ユーザー、エンティティタイプ、デバイス、ボリューム、元のパス、第 1 レベル フォルダ、第 2 レベル フォルダ、第 3 レベル フォルダ、第 4 レベル フォルダ、エンティティ名、ソース IP		「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）	特定の文字数を検索できます	AutoSabotageUser1_03172022?	ユーザー、エンティティタイプ、デバイス、ボリューム、第 1 レベル フォルダ、第 2 レベル フォルダ、第 3 レベル フォルダ、第 4 レベル フォルダ、エンティティ名、ソース IP		AutoSabotageUser1_03172022A、AutoSabotageUser1_03172022B、AutoSabotageUser1_0317202 25などを返します。
または	複数のエンティティを指定できる	AutoSabotageUser1_03172022 または AutoRansomUser4_03162022	ユーザー、ドメイン、エンティティタイプ、元のパス、エンティティ名、ソースIP		AutoSabotageUser1_03172022 または AutoRansomUser4_03162022 のいずれかを返します
ない	検索結果からテキストを除外できます	NOT AutoRansomUser4_03162022	ユーザー、ドメイン、エンティティタイプ、元のパス、第 1 レベル フォルダ、第 2 レベル フォルダ、第 3 レベル フォルダ、第 4 レベル フォルダ、エンティティ名、ソース IP	デバイス	「AutoRansomUser4_03162022」で始まらない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		対象フィールドが空の場合の結果を返します

パス検索

/ の有無で検索結果は異なります

「/AutoDir1/AutoFile03242022」	完全一致検索のみが機能し、/AutoDir1/AutoFile03242022 という正確なパスを持つすべてのアクティビティを返します (大文字と小文字は区別されません)
「/AutoDir1/」	動作します。第 1 レベルのディレクトリが AutoDir1 と一致するすべてのアクティビティを返します (大文字と小文字は区別されません)。
「/AutoDir1/AutoFile03242022/」	動作します。第 1 レベルのディレクトリが AutoDir1 に一致し、第 2 レベルのディレクトリが AutoFile03242022 に一致するすべてのアクティビティを返します (大文字と小文字は区別されません)。
/AutoDir1/AutoFile03242022 または /AutoDir1/AutoFile03242022	動作しません
/AutoDir1/AutoFile03242022 ではありません	動作しません
/AutoDir1 ではない	動作しません
/AutoFile03242022 ではありません	動作しません
*	動作しません

ローカルルート**SVM**ユーザーアクティビティの変更

ローカル ルート SVM ユーザー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 がユーザー名に考慮されるようになり、フォレンジック アクティビティ ページとユーザー アクティビティ ページの両方で root@<ip-address-of-the-client> として表示されます。

例えば：

- SVM-1 が Workload Security によって監視され、その SVM の root ユーザーが IP アドレス 10.197.12.40 を持つクライアントに共有をマウントする場合、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ー名は *root@10.197.12.40* になります。
- 同じ SVM-1 が IP アドレス 10.197.12.41 を持つ別のクライアントに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ー名は *root@10.197.12.41* になります。

*• これは、NFS ルート ユーザーのアクティビティを IP アドレスによって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 IP の区別なく、*root* ユーザーのみによって実行されると考えられていました。

トラブルシューティング

問題	試してみてください

「すべてのアクティビティ」テーブルの「ユーザー」列に、ユーザー名は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:default:80038003」	考えられる理由は次のとおりです: 1.ユーザー ディレクトリ コレクターはまだ構成されていません。追加するには、**Workload Security > Collectors > User Directory Collectors** に移動し、**+User Directory Collector** をクリックします。 *Active Directory* または *LDAP* ディレクトリ サーバー を選択します。2.ユーザー ディレクトリ コレクターは構成されていますが、停止しているかエラー状態です。 コレクター **>** ユーザー ディレクトリ コレクター に移動して、ステータスを確認してください。参照"ユーザーディレクトリコレクター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、名前は 24 時間以内に自動的に解決されます。それでも解決しない場合は、正しいユーザー データ コレクターを追加したかどうかを確認してください。ユーザーが実際に追加された Active Directory/LDAP ディレクトリ サーバーの一部であることを確認します。
一部の NFS イベントは UI に表示されません。	次の点を確認してください。1. POSIX 属性が設定された AD サーバーのユーザー ディレクトリ コレクターは、UI から unixid 属性を有効にして実行する必要があります。2. UI 3 のユーザー ページで検索すると、NFS アクセスを行っているすべてのユーザーが表示されるはずです。生のイベント (ユーザーがまだ検出されていないイベント) は NFS 4 ではサポートされていません。 NFS エクスポートへの匿名アクセスは監視されません。5.使用されている NFS バージョンが 4.1 以下であることを確認してください。 (NFS 4.1 はONTAP 9.15 以降でサポートされています。)
フォレンジックの「すべてのアクティビティ」ページまたは「エンティティ」ページのフィルターにアスタリスク (*) などのワイルドカード文字を含む文字を入力すると、ページの読み込みが非常に遅くなります。	検索文字列にアスタリスク (*) を使用すると、すべてが検索されます。ただし、*<searchTerm> や *<searchTerm>* などの先頭のワイルドカード文字列を使用すると、クエリが遅くなります。パフォーマンスを向上させるには、代わりに <searchTerm>* の形式のプレフィックス文字列を使用します (つまり、検索語の 後 にアスタリスク (*) を追加します)。例: *testvolume や *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、特定のフォルダー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/」は、/path1/path2/path3 の下にあるすべてのアクティビティを再帰的に一覧表示します。または、[すべてのアクティビティ] タブの [フィルターに追加] オプションを使用します。
パス フィルターの使用時に、「ステータス コード 500/503 でリクエストが失敗しました」というエラーが発生します。	レコードをフィルタリングするには、より短い日付範囲を使用してみてください。

path フィルターを使用すると、Forensic UI のデータの読み込みが遅くなります。	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までのディレクトリ パス フィルター (/ で終わるパス文字列) をお勧めします。たとえば、ディレクトリ パスが /Aaa/Bbb/Ccc/Ddd の場合、データをより高速に読み込むには、「/Aaa/Bbb/Ccc/Ddd/」を検索してみてください。
フォレンジック UI はデータの読み込みが遅く、エンティティ名フィルターの使用時に障害が発生します。	時間範囲を狭めて、二重引用符で囲んだ正確な値の検索を試してください。たとえば、entityPath が「/home/userX/nested1/nested2/nested3/testfile.txt」の場合、エンティティ名フィルターとして「testfile.txt」を試してください。

フォレンジックユーザーの概要

各ユーザーの情報は、ユーザー概要に記載されています。これらのビューを使用して、ユーザーの特性、関連するエンティティ、最近のアクティビティを把握します。

ユーザープロフィール

ユーザー プロファイル情報には、ユーザー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含まれます。

- ユーザー名
- ユーザーのメールアドレス
- ユーザーのマネージャー
- ユーザーの電話連絡先
- ユーザーの所在地

ユーザーの行動

ユーザー行動情報は、ユーザーが最近実行したアクティビティと操作を識別します。この情報には以下が含まれます。

- 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日間の運用
  - 操作数

更新間隔

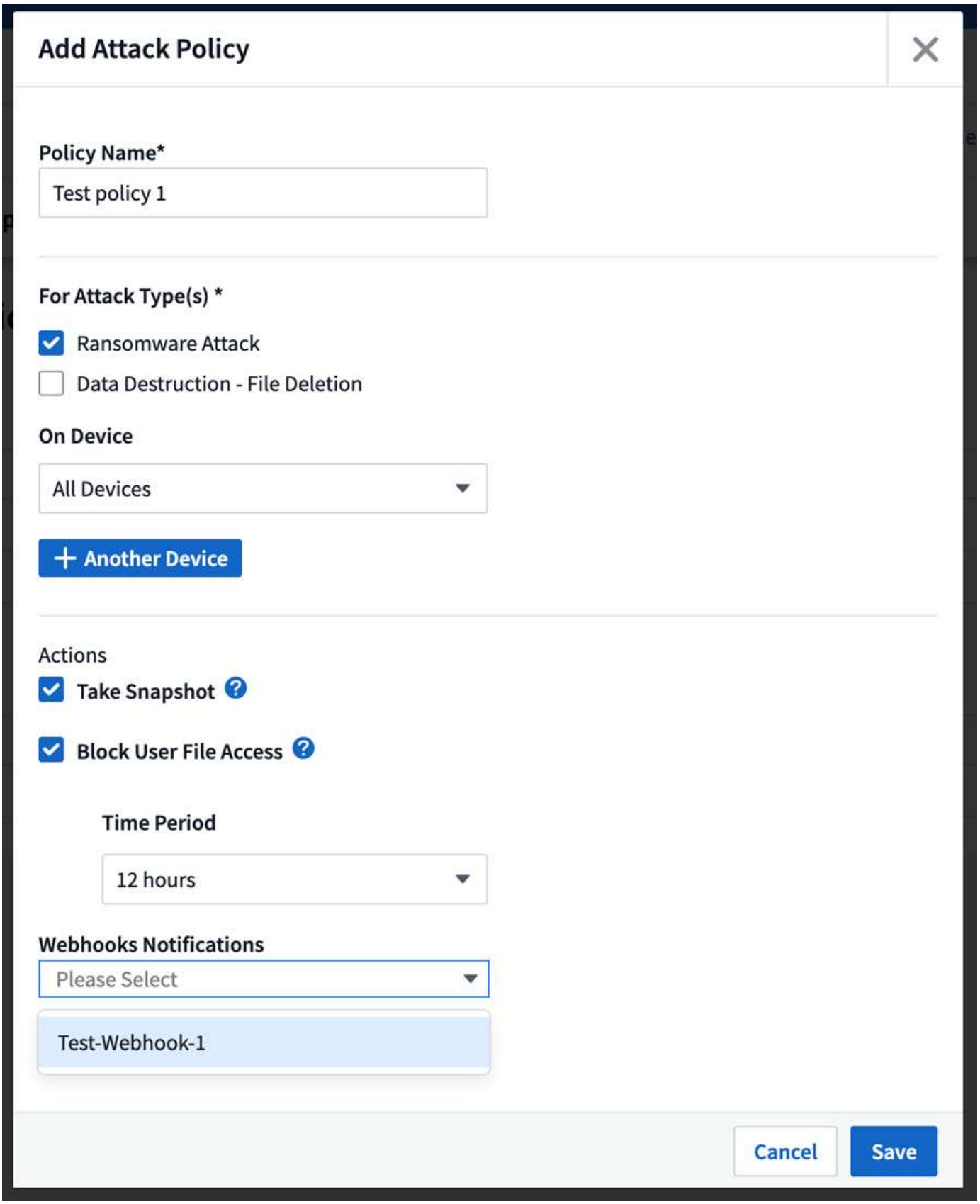
ユーザー リストは 12 時間ごとに更新されます。

再度更新されない場合、ユーザー リストは 13 か月間保持されます。 13 か月後にデータは削除されます。 Workload Security 環境が削除されると、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。

自動応答ポリシー

レスポンス ポリシーは、攻撃や異常なユーザー動作が発生した場合に、スナップショットを取得したり、ユーザー アクセスを制限したりする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、管理 **>** 自動応答ポリシー を選択し、適切な **+** ポリシー 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 (スナップショットの取得など) を無効にするには、アクションのチェックを外してポリシーを保存するだけです。

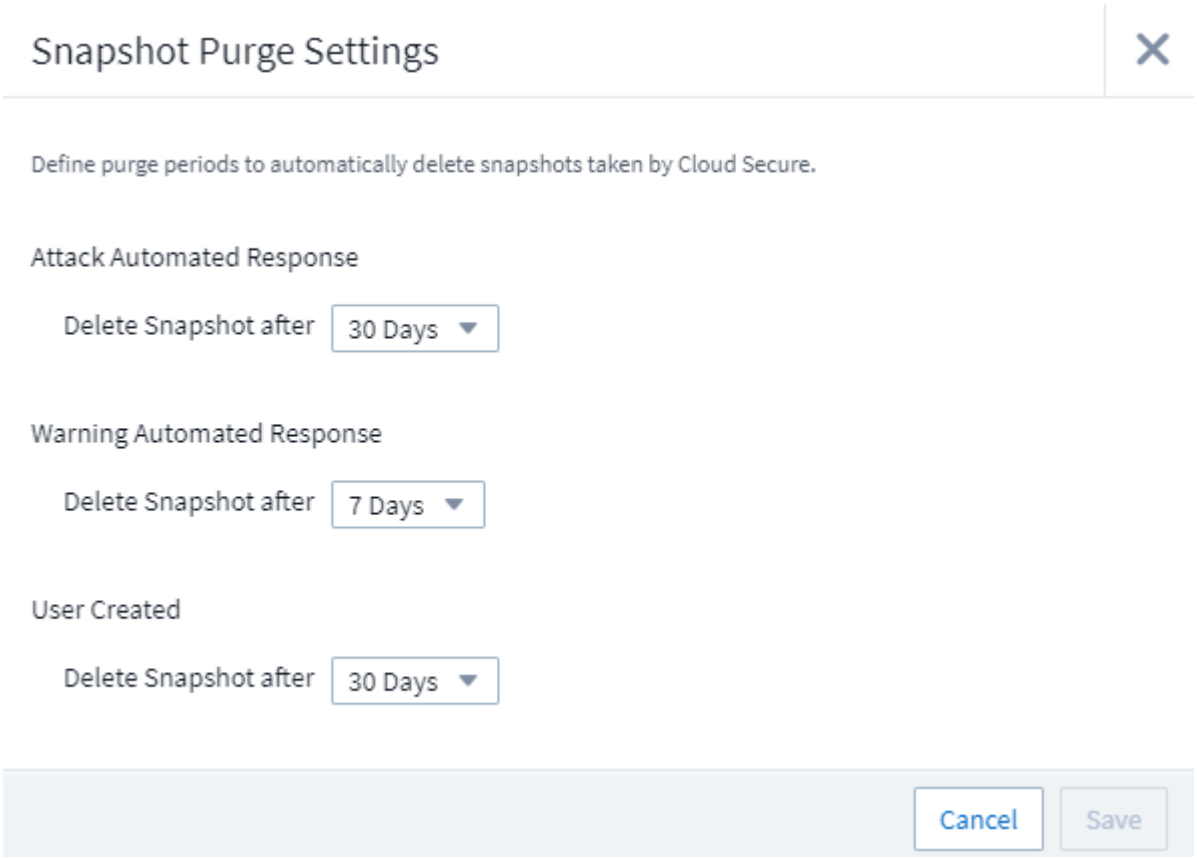
指定されたデバイス (または選択した場合はすべてのデバイス) に対してアラートがトリガーされると、自動応答ポリシーによってデータのスナップショットが作成されます。スナップショットのステータスは、"アラートの詳細ページ" 。

参照"ユーザーアクセスを制限する"IP によるユーザー アクセスの制限の詳細については、このページをご覧ください。

アラートが作成され、アクションが実行されたときに通知を受け取るために、ポリシーに 1 つ以上の Webhook を添付できます。ポリシーに追加する Webhook は 10 個以下にすることをお勧めします。ポリシーが一時停止されている場合、Webhook 通知はトリガーされないことに注意してください。

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すると、自動応答ポリシーを変更または一時停止できます。

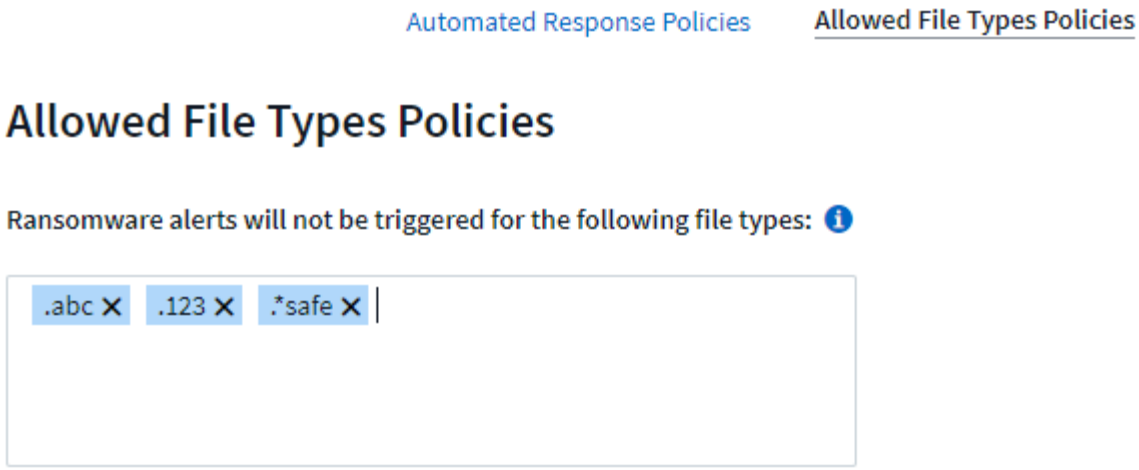
Workload Security は、スナップショット消去設定に基づいて、1 日に 1 回スナップショットを自動的に削除します。



許可されるファイルタイプのポリシー

既知のファイル拡張子に対するファイル改ざん攻撃が検出され、[アラート] 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 許可されたファイルの種類 リストに追加して、不要なアラートを防ぐことができます。

ワークロード セキュリティ > ポリシー に移動し、許可されたファイル タイプ ポリシー タブに移動します。



許可されたファイル タイプ リストに追加されると、その許可されたファイル タイプに対してファイル改ざん攻撃アラートは生成されなくなります。許可されるファイルの種類 ポリシーは、ファイルの改ざん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* に名前変更され、Workload Security が *.abc* 拡張子のためにファイル改ざん攻撃を検出した場合、*.abc* 拡張子を *allowed file types* リストに追加できます。リストに追加されると、*.abc* 拡張子を持つファイルに対してファイル改ざん攻撃が生成されなくなります。

許可されるファイル タイプは、完全一致 (例: 「.abc」) または表現 (例: 「.**type**」、「**.type**」、または「**type**」) にすることができます。 「.a*c」、「.p*f」型の式はサポートされていません。

ONTAP Autonomous Ransomware Protectionとの統合

ONTAP Autonomous Protection 機能は、NAS (NFS および SMB) 環境でのワークロード分析を使用して、悪意のある攻撃や不正なデータ変更を示唆する可能性のある異常なファイル内アクティビティをプロアクティブに検出し、警告します。

ARPに関する追加の詳細とライセンス要件については、以下をご覧ください。"ここをクリックしてください。" 。

Workload Security はONTAPと統合して ARP イベントを受信し、追加の分析および自動応答レイヤーを提供します。

Workload Security はONTAPから ARP イベントを受信し、次のアクションを実行します。

1. ボリューム暗号化イベントとユーザー アクティビティを相関させて、損害の原因を特定します。
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します:
    - 顧客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、より迅速な復旧とデータ侵害調査の実施に役立ちます。

前提条件

1. 最小ONTAPバージョン: 9.11.1
2. ARP 対応ボリューム。 ARPを有効にする方法の詳細については、"ここをクリックしてください。" 。 ARP はOnCommand System Manager経由で有効にする必要があります。 Workload Security では ARP を有効にできません。
3. Workload Security コレクターは、クラスター IP 経由で追加する必要があります。
4. この機能が動作するには、クラスター レベルの資格情報が必要です。つまり、SVM を追加するときは、クラスター レベルの認証情報を使用する必要があります。

ユーザー権限が必要です

クラスター管理資格情報を使用している場合は、新しい権限は必要ありません。

ユーザーに権限が付与されたカスタム ユーザー (たとえば、*csuser*) を使用している場合は、以下の手順に従って、Workload Security にONTAPから ARP 関連情報を収集する権限を付与します。

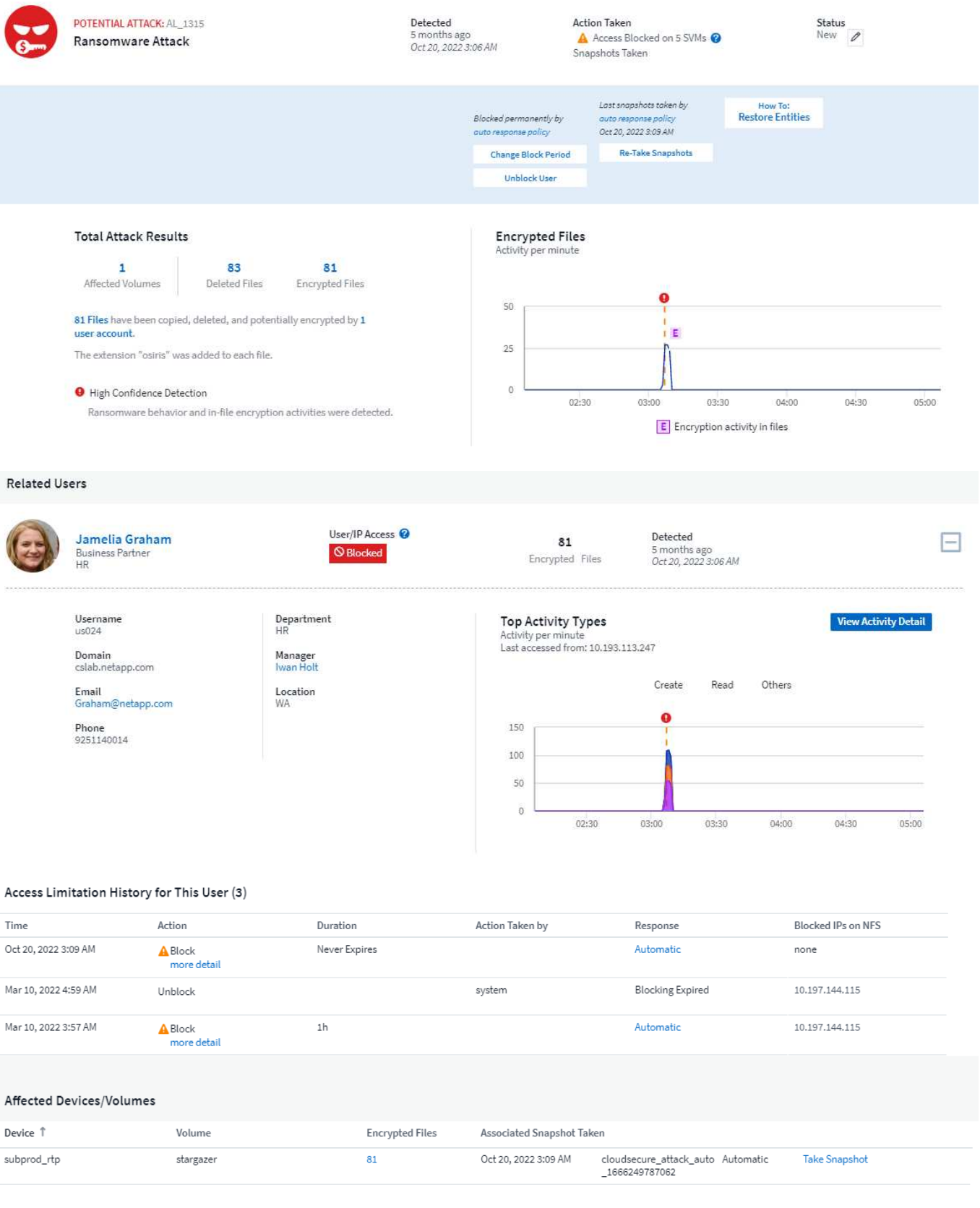
クラスタ認証情報を持つ *csuser* の場合は、 ONTAPコマンドラインから次の操作を実行します。

```
security login role create -role csrole -cmddirname "volume" -access
readonly
security login role create -role csrole -cmddirname "security anti-
ransomware volume" -access readonly
```

その他の設定についてはこちら"ONTAP権限"。

サンプルアラート

ARP イベントにより生成されたアラートのサンプルを以下に示します。



信頼性が高いバナーは、攻撃によってファイル暗号化アクティビティとともにファイル改ざん動作が行われたことを示します。暗号化されたファイルのグラフには、ARP ソリューション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。

制限事項

SVM が Workload Security によって監視されていないが、 ONTAPによって ARP イベントが生成されている場合でも、そのイベントは Workload Security によって受信され、表示されます。ただし、アラートに関連するフォレンジック情報やユーザー マッピングは取得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：
攻撃が検出されてから 24 時間以内に電子メールアラートが受信されます。 UI では、 Data Infrastructure Insights Workload Security が電子メールを受信する 24 時間前にアラートが表示されます。	ONTAP が_Ransomware Detected_ イベントをData Infrastructure Insights Workload Security (Workload Security) に送信すると、電子メールが送信されます。イベントには攻撃のリストとその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* イベントをData Infrastructure Insightsに送信します。したがって、UI にアラートが表示される時間と電子メールが送信される時間には差が生じる可能性があります。

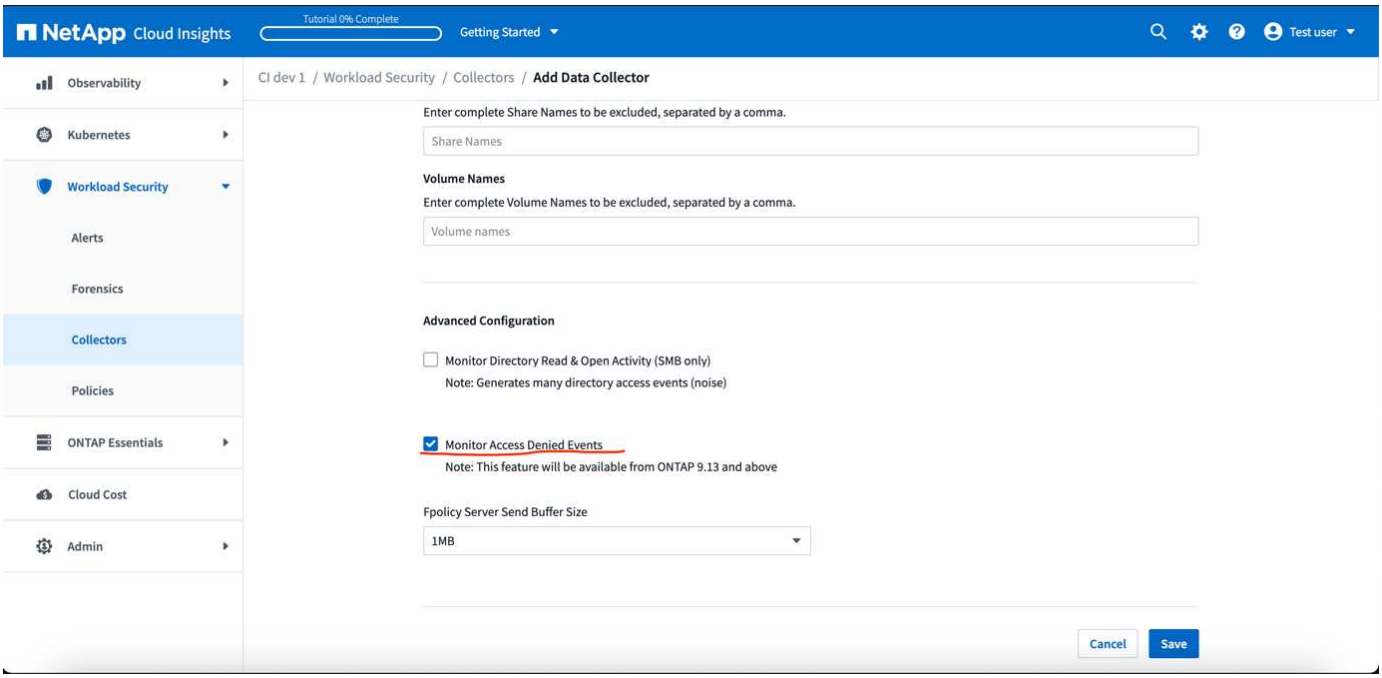
ONTAPとの統合アクセスが拒否されました

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、失敗したファイル操作 (つまり、ユーザーが権限のない操作を実行しようとしている) をプロアクティブに検出し、警告します。これらの失敗したファイル操作通知は、特にセキュリティ関連の障害の場合、早い段階で内部者による攻撃をブロックするのにさらに役立ちます。

Data Infrastructure Insights Workload Security 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ーを提供します。

前提条件

- 最小ONTAPバージョン: 9.13.0。
- Workload Security 管理者は、新しいコレクターを追加するとき、または既存のコレクターを編集するときに、[詳細設定] の [アクセス拒否イベントの監視] 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。



ユーザー権限が必要です

クラスター管理資格情報を使用してデータ コレクターを追加する場合、新しい権限は必要ありません。

ユーザーに権限が付与されたカスタム ユーザー (たとえば、*csuser*) を使用してコレクターを追加する場合は、次の手順に従って、 ONTAPでアクセス拒否イベントを登録するために必要な権限を Workload Security に付与します。

cluster 認証情報を持つ csuser 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。この権限はすでに存在している可能性があることに注意してください。

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
```

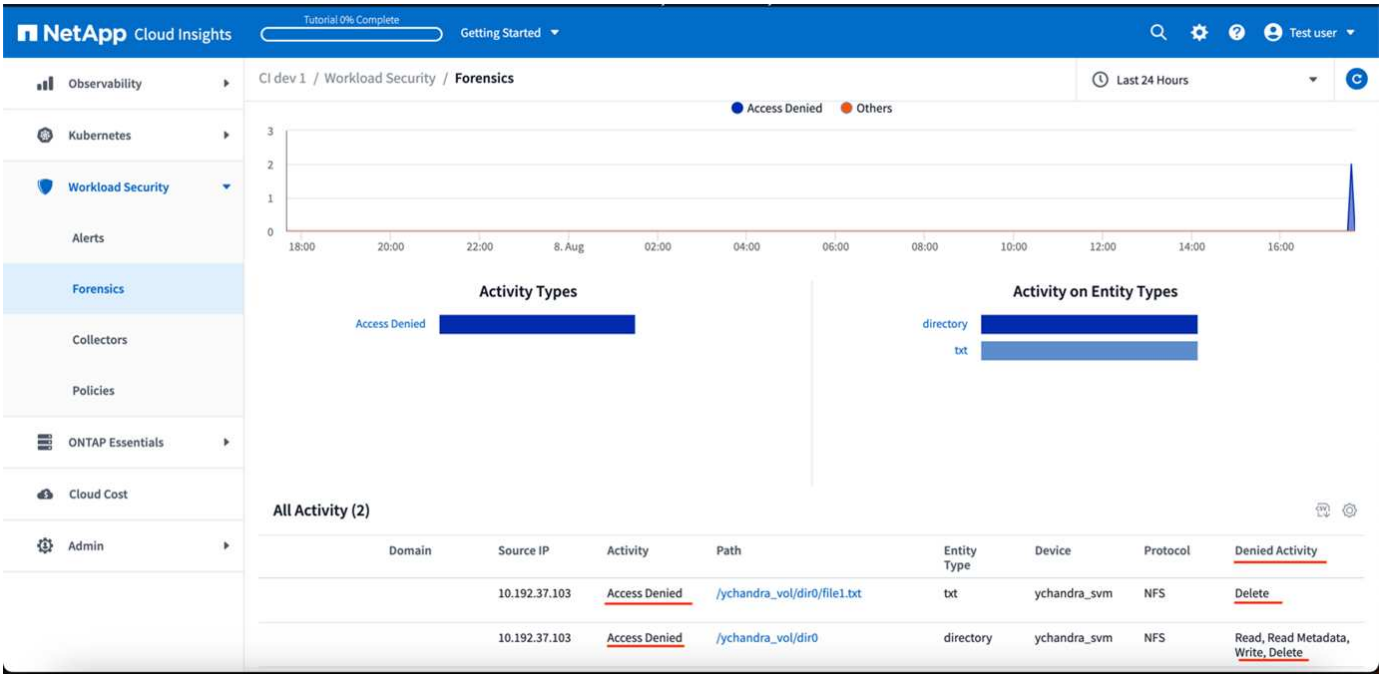
SVM 認証情報を持つ `csuser` の場合は、
ONTAPコマンドラインから次のコマンドを実行します。この権限はすでに存在している可能性があることに注意してください。

```
 security login role create -vserver <vservername> -role csrole
-cmddirname "vserver fpolicy" -access all
```

その他の設定についてはこちらlink:task_add_collector_svm.html["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、Workload Security Forensics 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、歯車アイコンからテーブルに「必要なアクティビティ」列を追加することで、特定の操作に不足しているユーザー権限を表示できます。



攻撃を阻止するためにユーザーアクセスをブロックする

侵害を受けたユーザーからのアクセスをブロックして検出された攻撃を直ちに停止し、さらなるデータの損傷や流出を防ぎます。Workload Security では、自動応答ポリシーによる自動ブロックと、アラートまたはユーザー詳細ページからの手動介入の両方が可能になり、セキュリティ対応を柔軟に制御できます。アクセス制限は、監視対象のすべてのストレージ ボリュームに自動的に適用され、自動復元には時間制限があります。

ユーザーは SMB に対して直接ブロックされ、攻撃の原因となっているホスト マシンの IP アドレスは NFS に対してブロックされます。これらのマシン IP アドレスは、Workload Security によって監視されるストレージ仮想マシン (SVM) へのアクセスがブロックされます。

たとえば、Workload Security が 10 個の SVM を管理しており、そのうち 4 個の SVM に対して自動応答ポリシーが設定されているとします。攻撃が 4 つの SVM のいずれかから発生した場合、ユーザーのアクセスは 10 個の SVM すべてでブロックされます。スナップショットは元の SVM で引き続き作成されます。

4 つの SVM があり、そのうち 1 つの SVM が SMB 用、1 つの SVM が NFS 用、残りの 2 つが NFS と SMB の両方用に設定されている場合、攻撃が 4 つの SVM のいずれかから発生した場合、すべての SVM がブロックされます。

ユーザーアクセスブロックの前提条件

この機能が動作するには、クラスター レベルの資格情報が必要です。

クラスター管理資格情報を使用している場合は、新しい権限は必要ありません。

ユーザーに権限が付与されたカスタム ユーザー (たとえば、*csuser*) を使用している場合は、以下の手順に従って、Workload Security にユーザーをブロックする権限を付与します。

クラスタ認証情報を持つ csuser の場合は、 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
```

必ず権限セクションを確認してください。"ONTAP SVMデータコレクターの設定"ページも同様です。

この機能を有効にするにはどうすればいいですか?

- Workload Security で、**Workload Security >** ポリシー **>** 自動応答ポリシー に移動します。 *+攻撃ポリシー*を選択します。
- _ユーザーファイルアクセスをブロック_を選択（チェック）します。

自動ユーザーアクセスブロックを設定するにはどうすればいいですか?

- 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クリックします。これを選択すると機能が有効になります。
- 「期間」の下で、ブロックを適用する期間を選択します。
- 自動ユーザーブロックをテストするには、"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たユーザーがいるかどうかを知るにはどうすればいいですか?

- アラート リスト ページでは、ユーザーがブロックされている場合に画面上部にバナーが表示されます。
- バナーをクリックすると、「ユーザー」ページに移動し、ブロックされたユーザーのリストが表示されます。
- 「ユーザー」ページに、「ユーザー/IP アクセス」という列があります。その列には、ユーザーのブロックの現在の状態が表示されます。

ユーザーアクセスを手動で制限および管理する

- アラートの詳細画面またはユーザーの詳細画面に移動し、それらの画面からユーザーを手動でブロックまたは復元することができます。

ユーザーアクセス制限履歴

アラートの詳細とユーザーの詳細ページのユーザー パネルでは、ユーザーのアクセス制限履歴の監査を表示できます。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、手動/自動、NFS の

影響を受ける IP などが表示されます。

機能を無効にするにはどうすればいいですか?

この機能はいつでも無効にすることができます。システムに制限されたユーザーが存在する場合は、まずそのユーザーのアクセスを復元する必要があります。

- Workload Security で、**Workload Security >** ポリシー **>** 自動応答ポリシー に移動します。 *+攻撃ポリシー*を選択します。
- _ユーザーファイルアクセスをブロック_を選択解除します。

この機能はすべてのページで非表示になります。

NFSのIPを手動で復元する

Workload Security のトライアルの有効期限が切れた場合、またはエージェント/コレクターがダウンしている場合は、次の手順に従ってONTAPから IP を手動で復元します。

1. SVM 上のすべてのエクスポート ポリシーを一覧表示します。

```
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. それぞれの RuleIndex を指定して、クライアント マッチとして「cloudsecure_rule」を持つ SVM 上のすべてのポリシーのルールを削除します。ワークロード セキュリティ ルールは通常 1 になります。

```
 contrail-qa-fas8020:*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Workload Security 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のユーザーを手動で復元する

Workload Security のトライアルの有効期限が切れた場合、またはエージェント/コレクターがダウンしている場合は、次の手順に従ってONTAPからユーザーを手動で復元します。

Workload Security でブロックされている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. クラスタ *admin* 認証情報を使用して、 ONTAPクラスタ (ユーザーのブロックを解除するクラスタ) にログインします。 (Amazon FSxの場合は、FSx 認証情報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 で Workload Security for SMB によってブロックされているすべてのユーザーを一覧表示します。

```
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、ドメイン CSLAB で 2 人のユーザー (US030、US040) がブロックされました。

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>
```
. 次のコマンドを実行して、ユーザーがブロック解除されていることを確認します。

```
vserver name-mapping show -direction win-unix -replacement " "
```

以前にブロックされたユーザーについてはエントリが表示されません。

トラブルシューティング

問題	試してみてください
攻撃があるにもかかわらず、一部のユーザーは制限を受けていません。	1.SVM のデータ コレクターとエージェントが 実行中状態であることを確認します。データコレクタとエージェントが停止している場合、Workload Security はコマンドを送信できません。2.これは、ユーザーがこれまで使用されたことのない新しい 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、ユーザーがストレージにアクセスしているホストの IP アドレスによって行われます。制限されている IP アドレスのリストについては、UI (アラートの詳細 > このユーザーのアクセス制限履歴 > 影響を受ける IP) で確認してください。ユーザーが制限された IP とは異なる IP を持つホストからストレージにアクセスしている場合でも、ユーザーは制限されていない IP を通じてストレージにアクセスできます。ユーザーが 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。
「アクセスの制限」を手動でクリックすると、「このユーザーの IP アドレスは既に制限されています」というメッセージが表示されます。	制限対象の IP は既に別のユーザー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: そのコマンドを実行する権限がありません。	csuser を使用している場合は、上記のようにユーザーに権限が付与されていることを確認します。

問題	試してみてください
NFS のユーザー (IP アドレス) ブロックは機能しますが、SMB/CIFS の場合は、「SID から DomainName への変換に失敗しました」というエラー メッセージが表示されます。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、*csuser* に ssh を実行する権限がない場合に発生する可能性があります。 (クラスター レベルでの接続を確認し、ユーザーが ssh を実行できることを確認します)。 *csuser* ロール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クラスタ認証情報を持つ *csuser* の場合は、 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* が使用されず、クラスタ レベルの管理者ユーザが使用される場合は、管理者ユーザがONTAPへの SSH 権限を持っていることを確認します。
ユーザーがブロックされるはずなのに、エラー メッセージ「*SID* の変換に失敗しました。 理由:*255:*エラー*:* コマンドが失敗しました*:* このコマンドに対して権限がありませんエラー*: "access-check"* は認識されたコマンドではありません」が表示されます。	これは、*csuser* に適切な権限がない場合に発生する可能性があります。見る"ユーザーアクセスブロックの前提条件"詳細についてはこちらをご覧ください。権限を適用した後、 ONTAPデータ コレクターとユーザー ディレクトリ データ コレクターを再起動することをお勧めします。必要な権限コマンドは以下のとおりです。 ---- 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 ----

ワークロードセキュリティ: ファイル改ざんのシミュレーション

このページの手順を使用すると、付属のファイル改ざんシミュレーション スクリプトを使用して、Workload Security のテストまたはデモンストレーションのためにファイル改ざんをシミュレートできます。

始める前に注意すべきこと

- ファイル改ざんシミュレーション スクリプトは Linux でのみ動作します。シミュレーション スクリプトは、ユーザーがONTAP ARP を Workload Security と統合した場合に、高信頼度アラートも生成する必要があります。
- Workload Security は、 ONTAPバージョンが 9.15 以上の場合にのみ、NFS 4.1 で生成されたイベントと

アラートを検出します。

- スクリプトは、Workload Security エージェントのインストール ファイルに付属しています。 Workload Security エージェントがインストールされているどのマシンでも利用できます。
- Workload Security エージェント マシン自体でスクリプトを実行できます。別の Linux マシンを準備する必要はありません。ただし、別のシステムでスクリプトを実行したい場合は、スクリプトをコピーしてそこで実行するだけです。
- ユーザーは、自分の好みやシステム要件に応じて、Python スクリプトまたはシェル スクリプトのいずれかを選択できます。
- Python スクリプトには前提条件となるインストールがあります。 Python を使用したくない場合は、シェル スクリプトを使用します。

ガイドライン:

このスクリプトは、暗号化するファイルが多数 (理想的にはサブフォルダー内のファイルを含む 100 個以上) 含まれているフォルダーを含む SVM で実行する必要があります。ファイルが空でないことを確認してください。

アラートを生成するには、テスト データの作成前にコレクターを一時的に停止します。サンプル ファイルが生成されたら、コレクターを再開し、暗号化プロセスを開始します。

手順：

システムを準備します。

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 または CIFS エクスポートのいずれか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:

```
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 をマウントしないでください。これは 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:

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```

ONTAP Autonomous Ransomware Protection を有効にする（オプション）：

ONTAPクラスタのバージョンが 9.11.1 以上の場合は、 ONTAPコマンド コンソールで次のコマンドを実行して、 ONTAPランサムウェア保護サービスを有効にできます。

```
 security anti-ransomware volume enable -volume [volume_name] -vserver
[svm_name]
```
次に、データ コレクターを設定します。

1. Workload Security エージェントをまだ設定していない場合は設定します。
2. まだ行っていない場合は、SVM データ コレクターを構成します。
3. データ コレクターを構成するときに、マウント プロトコルが選択されていることを確認します。

プログラムでサンプル ファイルを生成します。

ファイルを作成する前に、まず停止するか、"データ収集装置を一時停止する"処理。

シミュレーションを実行する前に、まず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ターゲット フォルダーに手動でコピーするか、付属のスクリプトのいずれか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する場合でも、暗号化するファイルが少なくとも 100 個あることを確認してください。

プログラムでファイルを作成する場合は、シェルまたは Python を使用できます。

シェル：

1. エージェント ボックスにログインします。
2. ファイラーの SVM からエージェント マシンに NFS または CIFS 共有をマウントします。そのフォルダに CD します。
3. エージェントのインストール ディレクトリ (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/create_dataset.sh) からスクリプトをターゲットのマウント場所にコピーします。
4. マウントされたディレクトリ (例: /root/demo) 内のスクリプトを使用して次のコマンドを実行し、テスト データセット フォルダーとファイルを作成します。

   ```
    './create_dataset.sh'
   ```
   . これにより、「test_dataset」というディレクトリの下のマウント フォルダー内に、さまざまな拡張子を持つ空でないファイル 100 個が作成されます。

パイソン:

Python スクリプトの前提条件:

- Python をインストールします (まだインストールされていない場合)。
  - Python 3.5.2以上をダウンロード https://www.python.org/。
  - Pythonのインストールを確認するには、以下を実行します。 `python --version` 。
  - Python スクリプトはバージョン 3.5.2 以降でテストされています。
- まだインストールされていない場合は pip をインストールします。

- get-pip.pyスクリプトを以下からダウンロードします。 https://bootstrap.pypa.io/ 。
- pipをインストールするには `python get-pip.py`。
- pipのインストールを確認する `pip --version`。

- PyCryptodome ライブラリ:
  - このスクリプトは PyCryptodome ライブラリを使用します。
  - PyCryptodomeをインストールする `pip install pycryptodome`。
  - PyCryptodomeのインストールを確認するには、 `pip show pycryptodome` 。

Python ファイル作成スクリプト:

1. エージェント ボックスにログインします。
2. ファイラーの SVM からエージェント マシンに NFS または CIFS 共有をマウントします。そのフォルダに CD します。
3. エージェントのインストール ディレクトリ (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/create_dataset.py) からターゲットのマウント場所にスクリプトをコピーします。
4. マウントされたディレクトリ (例: /root/demo) 内のスクリプトを使用して次のコマンドを実行し、テスト データセット フォルダーとファイルを作成します。

   `'python create_dataset.py'` . これにより、「`test_dataset`」というディレクトリの下のマウントフォルダ内に、さまざまな拡張子を持つ`100`個の空でないファイルが作成されます。

コレクターを再開する

これらの手順を実行する前にコレクターを一時停止した場合は、サンプル ファイルが作成されたら必ずコレクターを再開してください。

プログラムでサンプル ファイルを生成します。

ファイルを作成する前に、まず停止するか、"データ収集装置を一時停止する"処理。

ファイル改ざんアラートを生成するには、Workload Security でファイル改ざんアラートをシミュレートする付属のスクリプトを実行します。

シェル：

1. エージェントのインストール ディレクトリ (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/simulate_attack.sh) からスクリプトをターゲットのマウント場所にコピーします。
2. マウントされたディレクトリ (例: /root/demo) 内のスクリプトを使用して次のコマンドを実行し、テスト データセットを暗号化します。

```
'./simulate_attack.sh'
```
. これにより、「test_dataset」ディレクトリの下に作成されたサンプルファイルが暗号化されます。

パイソン:

1. エージェントのインストール ディレクトリ (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/simulate_attack.py) からスクリプトをターゲットのマウント場所にコピーします。
2. Pythonの前提条件は、Pythonスクリプトの前提条件セクションに従ってインストールされていることに注意してください。
3. マウントされたディレクトリ (例: /root/demo) 内のスクリプトを使用して次のコマンドを実行し、テストデータセットを暗号化します。

```
'python simulate_attack.py'
```
. これにより、「test_dataset」ディレクトリの下に作成されたサンプルファイルが暗号化されます。

ワークロードセキュリティでアラートを生成する

シミュレータ スクリプトの実行が終了すると、数分以内に Web UI にアラートが表示されます。

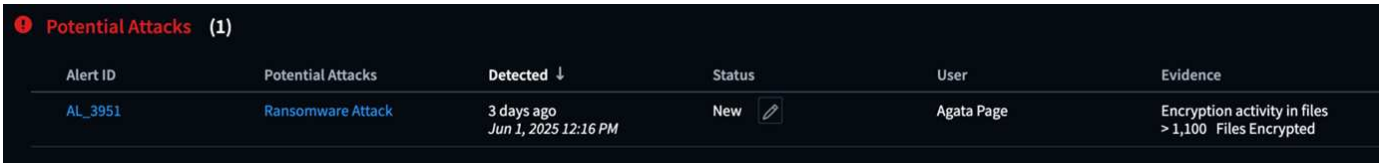
注意: 以下の条件がすべて満たされた場合、高信頼度アラートが生成されます。

1. 監視対象SVMのONTAPバージョンが9.11.1以上
2. ONTAP Autonomous Ransomware Protection が構成済み
3. Workload Security データ コレクターがクラスター モードに追加されました。

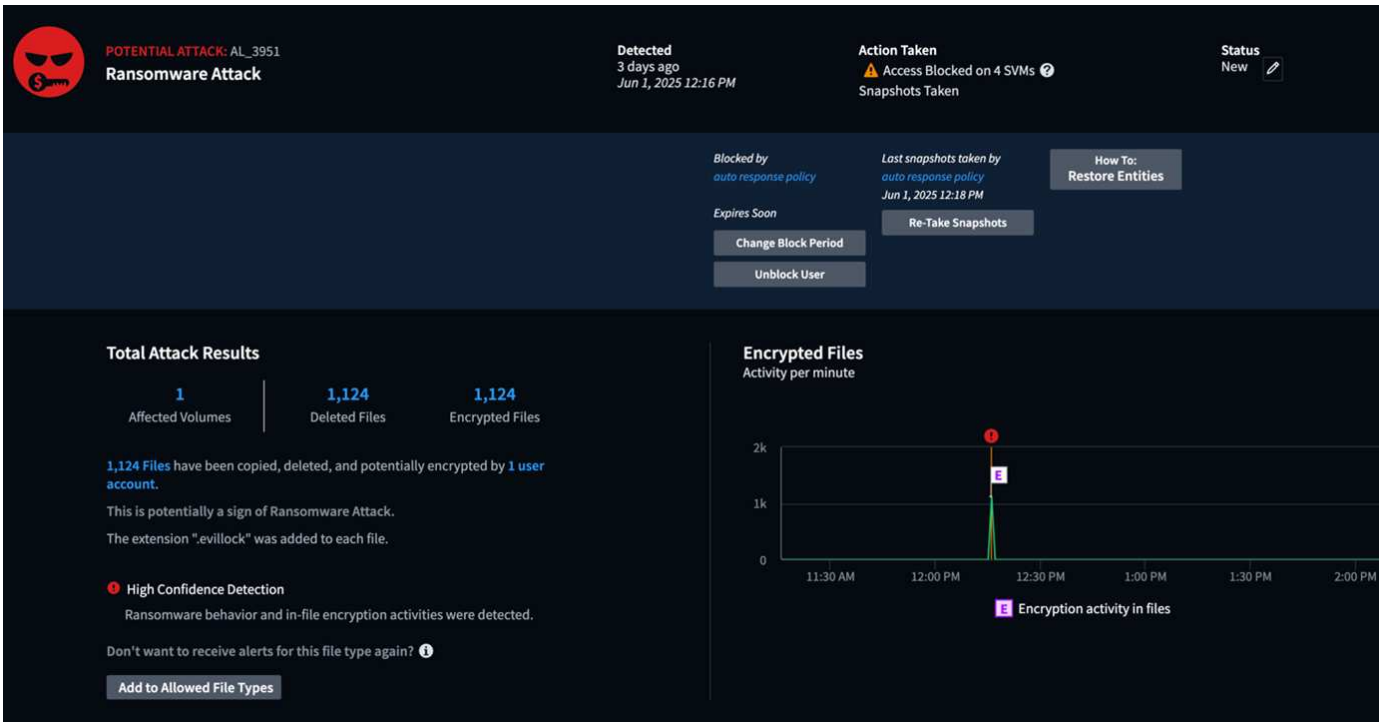
Workload Security はユーザーの行動に基づいてファイルの改ざんパターンを検出し、 ONTAP ARP はファイル内の暗号化アクティビティに基づいてファイルの改ざんアクティビティを検出します。

条件が満たされると、Workload Security はアラートを高信頼度アラートとしてマークします。

アラート リスト ページの高信頼度アラートの例:



高信頼度アラートの詳細の例:



アラートを複数回トリガーする

Workload Security はユーザーの行動を学習し、同じユーザーに対して 24 時間以内にファイル改ざん攻撃が繰り返された場合、アラートを生成しません。

別のユーザーで新しいアラートを生成するには、同じ手順（テスト データを作成し、テスト データを暗号化する）を再度実行してください。

アラート、警告、エージェント/データソースコレクターの正常性に関する電子メール通知の構成

電子メール通知により、潜在的な攻撃、セキュリティ警告、インフラストラクチャの健全性の問題が発生したときに、それらについて最新情報を入手できます。各受信者の責任に合わせたリアルタイムアラートを受信するには、[管理] > [通知] 設定で受信者の電子メール アドレスを構成します。

潜在的な攻撃の警告と警告

潜在的な攻撃 アラート通知を送信するには、[潜在的な攻撃アラートの送信] セクションに受信者のメール アドレスを入力します。アラートのすべてのアクションについて、アラート受信者リストに電子メール通知が送信されます。

警告 通知を送信するには、[警告アラートの送信] セクションに受信者のメール アドレスを入力します。

エージェントとデータコレクターのヘルスモニタリング

通知を通じてエージェントとデータ ソースの正常性を監視できます。

エージェントまたはデータ ソース コレクターが機能していない場合に通知を受信するには、[データ収集ヘルス アラート] 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。

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/コレクターが少なくとも 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 コレクターが長期間切断された場合でも、指定された 24 時間以内に対象の受信者に送信される電子メール通知は 1 件のみです。
- エージェントに障害が発生した場合、1 つのアラートが送信されます (コレクターごとに 1 つではありません)。電子メールには、影響を受けるすべての SVM のリストが含まれます。
- Active Directory コレクションの失敗は警告として報告されますが、脅威の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」フェーズが追加されました。

エージェントとデータコレクターのアップグレード通知の受信

- 「データ収集ヘルスアラート」にメール ID を入力します。
- 「アップグレード通知を有効にする」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データ コレクターのアップグレードに関する電子メール通知は、計画されたアップグレードの 1 日前に電子メール ID に送信されます。

トラブルシューティング

問題：	これを試してみてください:
「データ コレクターのヘルス アラート」に電子メール ID が表示されますが、通知を受信できません。	通知メールは、 NetApp Data Infrastructure Insightsドメイン (*accounts@service.cloudinsights.netapp.com*) から送信されます。一部の企業では、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。

Webhook通知

Webhookを使用したワークロードセキュリティ通知

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重大なアラート通知や警告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は、Slack、PagerDuty、Teams、Discord など、標準の入力インターフェースとして Webhook をサポートしています。汎用的でカスタマイズ可能な Webhook チャネルをサポートすることで、Workload Security はこれらの配信チャネルの多くをサポートできます。 Webhook の設定に関する情報は、それぞれのアプリケーションの Web サイトで確認できます。例えば、Slackは"この便利なガイド"。

複数の Webhook チャネルを作成し、各チャネルを異なる目的、個別のアプリケーション、異なる受信者などを対象にすることができます。

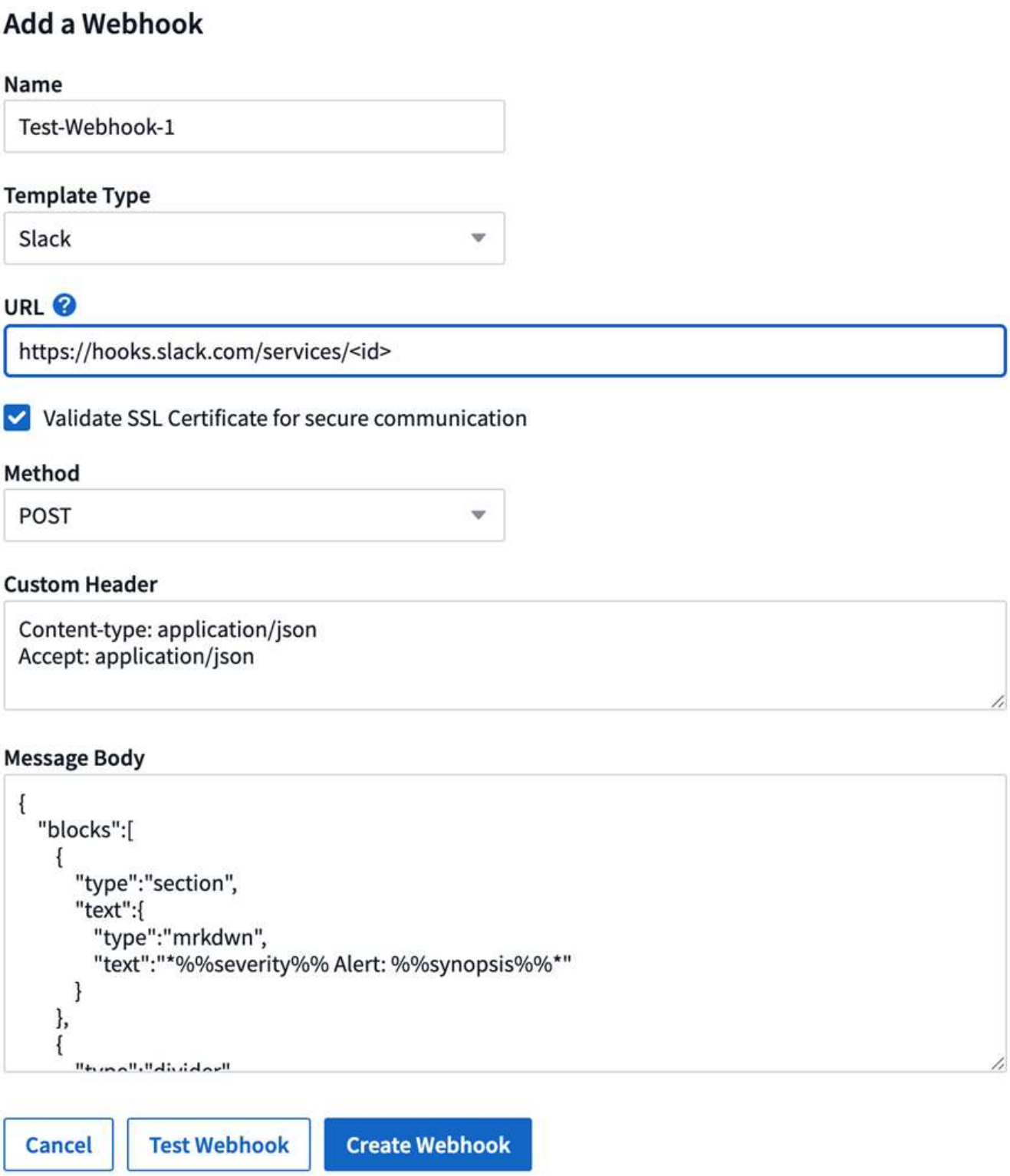
Webhookチャネルインスタンスは次の要素で構成されています

Name	説明
URL	Webhook ターゲット 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）
方法	GET/POST - デフォルトはPOST
カスタムヘッダー	ここでカスタムヘッダーを指定します
メッセージ本文	メッセージの本文をここに入力してください
デフォルトのアラートパラメータ	Webhookのデフォルトパラメータを一覧表示します
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、固有のパラメータやパスワードなどの安全な要素を追加できます。

Webhookの作成

Workload Security Webhook を作成するには、「管理」>「通知」に移動し、「Workload Security Webhooks」タブを選択します。次の画像は、Slack Webhook 作成画面のサンプルを示しています。

注意: Workload Security Webhook を作成および管理するには、ユーザーは Workload Security *Admin* である必要があります。



- 各フィールドに適切な情報を入力し、「保存」をクリックします。
- 「Webhook 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、選択したメソッドに従って、定義された URL に「メッセージ本文」（置換なし）が送信されることに注意してください。
- SWS Webhook は、いくつかのデフォルト パラメータで構成されています。さらに、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。

パラメーター: パラメーターとは何か、どのように使用するのか?

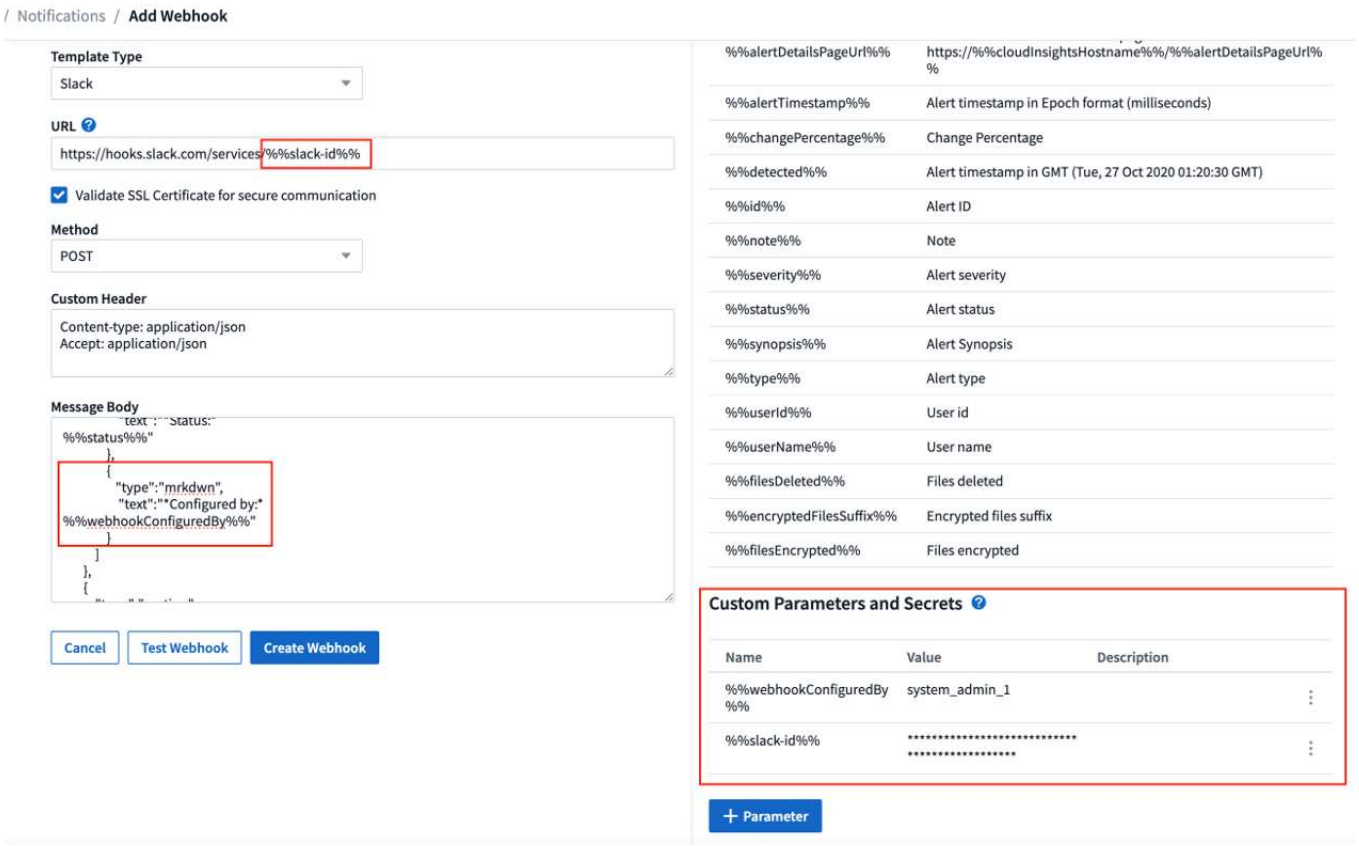
アラート パラメータは、アラートごとに設定される動的な値です。たとえば、*%%severity%%* パラメータは、アラートの重大度タイプに置き換えられます。

「Test Webhook」ボタンをクリックしたときには置換は実行されないことに注意してください。テストでは、パラメータのプレースホルダー (*%%<param-name>%%*) を表示するペイロードが送信されますが、データに置き換えられることはありません。

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、必要なカスタム パラメータやシークレットを追加できます。カスタム パラメータまたはシークレットは、URL またはメッセージ本文に含めることができます。シークレットを使用すると、ユーザーはパスワード、apiKey などの安全なカスタム パラメータを設定できます。

次のサンプル画像は、Webhook の作成時にカスタム パラメータがどのように使用されるかを示しています。



ワークロード セキュリティ **Webhook** リスト ページ

Webhook リスト ページには、名前、作成者、作成日、ステータス、セキュリティ、最終報告のフィールドが表示されます。注: 「ステータス」列の値は、最後の Webhook トリガーの結果に基づいて変化し続けます。以下はステータス結果の例です。

ステータス	説明
OK	通知を正常に送信しました。
403	禁止されています。

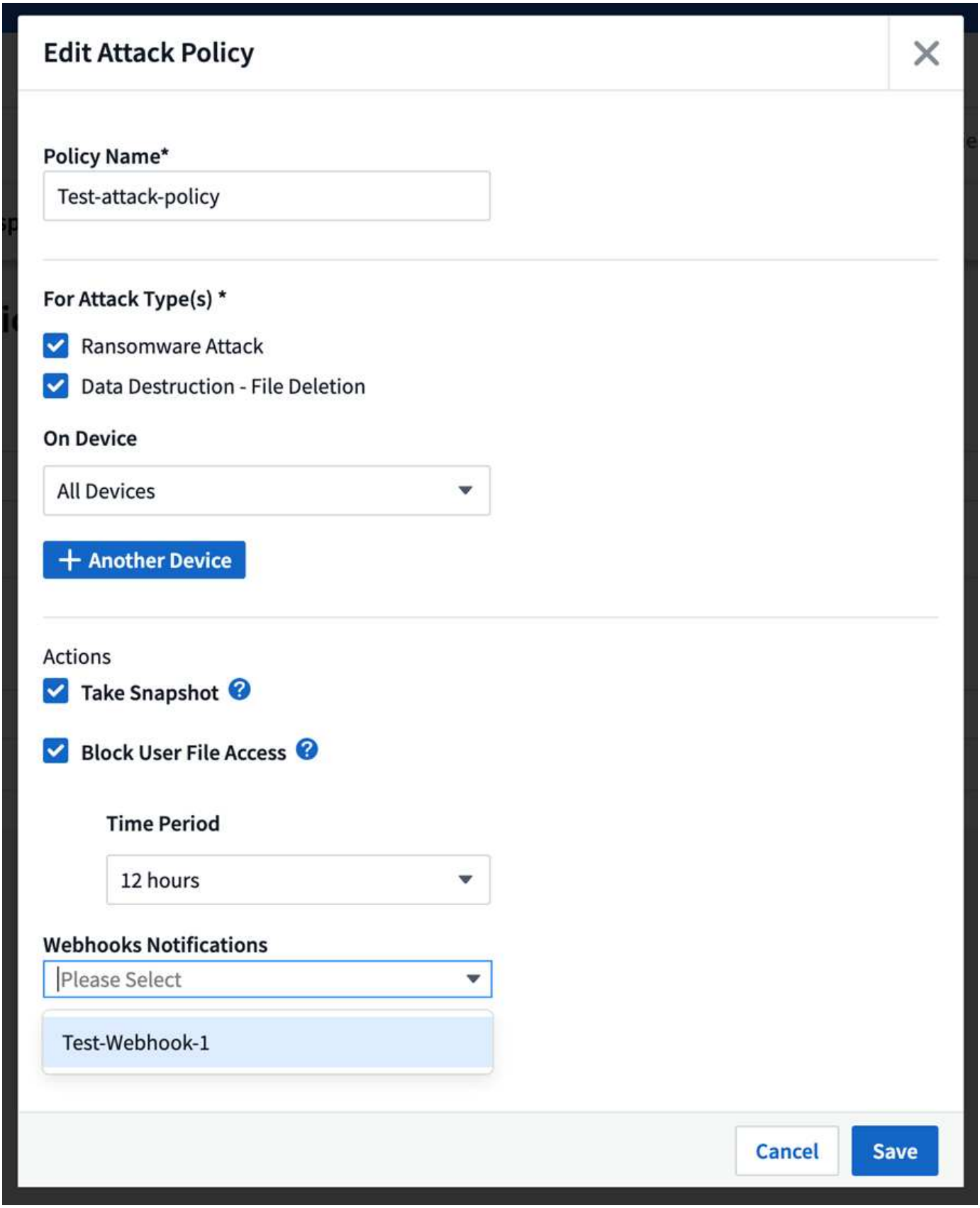
404	URLが見つかりません。
400	要求の形式が正しくありません。メッセージ本文にエラーがある場合、このステータスが表示されることがあります。例: • 形式が不適切な json。 • 予約済みのキーに無効な値を指定しています。たとえば、PagerDuty は「重大度」として、critical/warning/error/info のみを受け入れます。その他の結果の場合は、400 ステータスが返される可能性があります。 • アプリケーション固有の検証エラー。たとえば、Slack ではセクション内に最大 10 個のフィールドが許可されます。 10 個を超えると、400 ステータスになる可能性があります。
410	リソースは利用できなくなりました

「最終報告」列には、Webhook が最後にトリガーされた時刻が示されます。

ウェブフック一覧ページから、ユーザーはウェブフックを編集/複製/削除することもできます。

アラートポリシーで**Webhook**通知を構成する

アラート ポリシーに Webhook 通知を追加するには、「ワークロード セキュリティ」>「ポリシー」に移動し、既存のポリシーを選択するか、新しいポリシーを追加します。 アクション セクション > *Webhook* 通知ドロップダウンで、必要な Webhook を選択します。



Webhook 通知はポリシーに関連付けられています。攻撃 (RW/DD/WARN) が発生すると、設定されたアクション (スナップショットの取得/ユーザーのブロック) が実行され、関連する Webhook 通知がトリガーされます。

注: 電子メール通知はポリシーとは無関係であり、通常どおりトリガーされます。

- ポリシーが一時停止されている場合、Webhook 通知はトリガーされません。
- 複数の Webhook を 1 つのポリシーにアタッチできますが、ポリシーにアタッチする Webhook は 5 つ以下にすることをお勧めします。

ワークロードセキュリティ**Webhook**の例

Webhooksの"スラック"

Webhooksの"ページャーデューティ"Webhooksの"チーム"Webhooksの"不和"

Discord 向けワークロード セキュリティ Webhook の例

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。このページでは、Discord 用の Webhook を設定する例を示します。

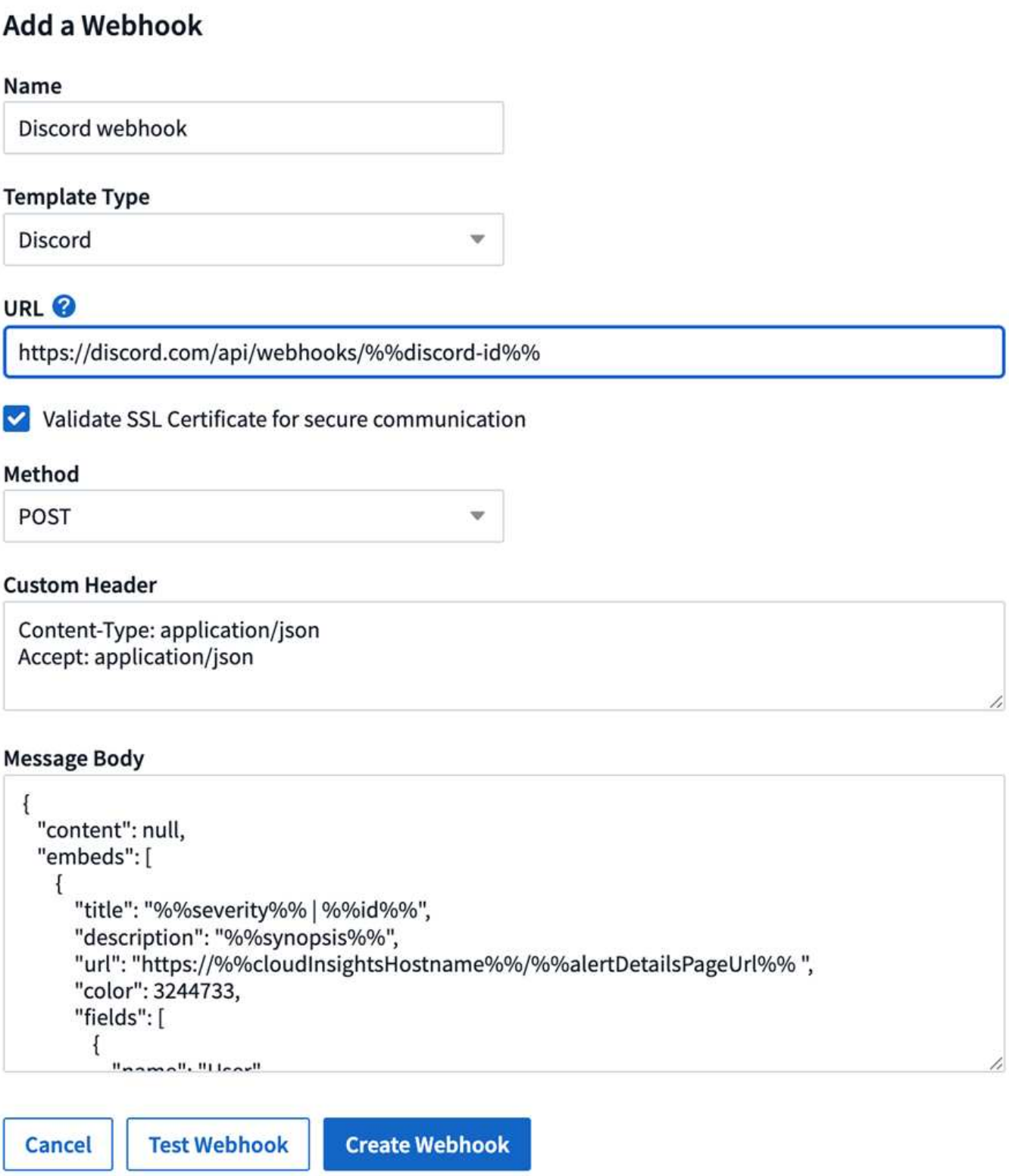
このページはサードパーティの指示を参照しており、変更される可能性があります。参照"Discordドキュメント"最新情報についてはこちらをご覧ください。

Discordの設定:

- Discordでサーバーを選択し、テキストチャンネルの下にあるチャンネル編集（歯車アイコン）を選択します。
- *統合 > Webhookの表示*を選択し、*新しいWebhook*をクリックします。
- Webhook URL をコピーします。これを Workload Security Webhook 設定に貼り付ける必要があります。

ワークロード セキュリティ **Webhook** を作成します。

1. 「管理」>「通知」に移動し、「*Workload Security Webhooks*」タブを選択します。新しい Webhook を作成するには、「+ Webhook」をクリックします。
2. Webhook に意味のある名前を付けます。
3. テンプレート タイプ ドロップダウンで、**Discord** を選択します。
4. 上記の Discord URL を *URL* フィールドに貼り付けます。



Webhook をテストするには、メッセージ本文の URL 値を有効な URL (*https://netapp.com* など) に一時的に置き換えて、[*Test Webhook*] ボタンをクリックします。 Discord では、テスト Webhook 機能が動作するために有効な URL を指定する必要があります。

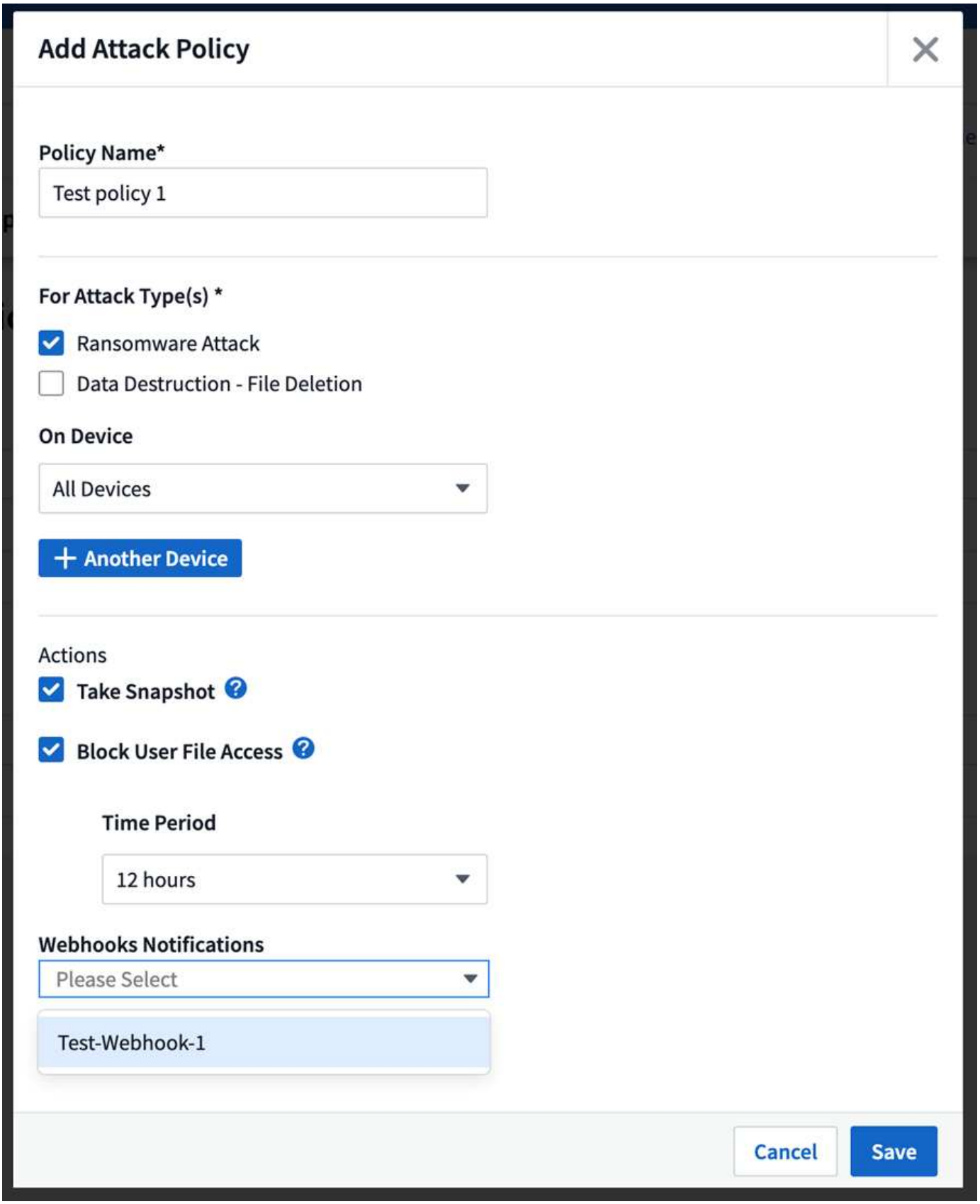
テストが完了したら、必ずメッセージ本文を元に戻してください。

Webhook経由の通知

Webhook 経由でイベントを通知するには、[*Workload Security*] > [ポリシー] に移動します。 +攻撃ポリシー_ または+警告ポリシー_をクリックします。

- 意味のあるポリシー名を入力します。
- 必要な攻撃タイプ、ポリシーを適用するデバイス、および必要なアクションを選択します。
- [*Webhooks Notifications*] ドロップダウンで、必要な Discord Webhook を選択して保存します。

注: Webhook は、編集することで既存のポリシーに添付することもできます。



PagerDuty のワークロード セキュリティ **Webhook** の例

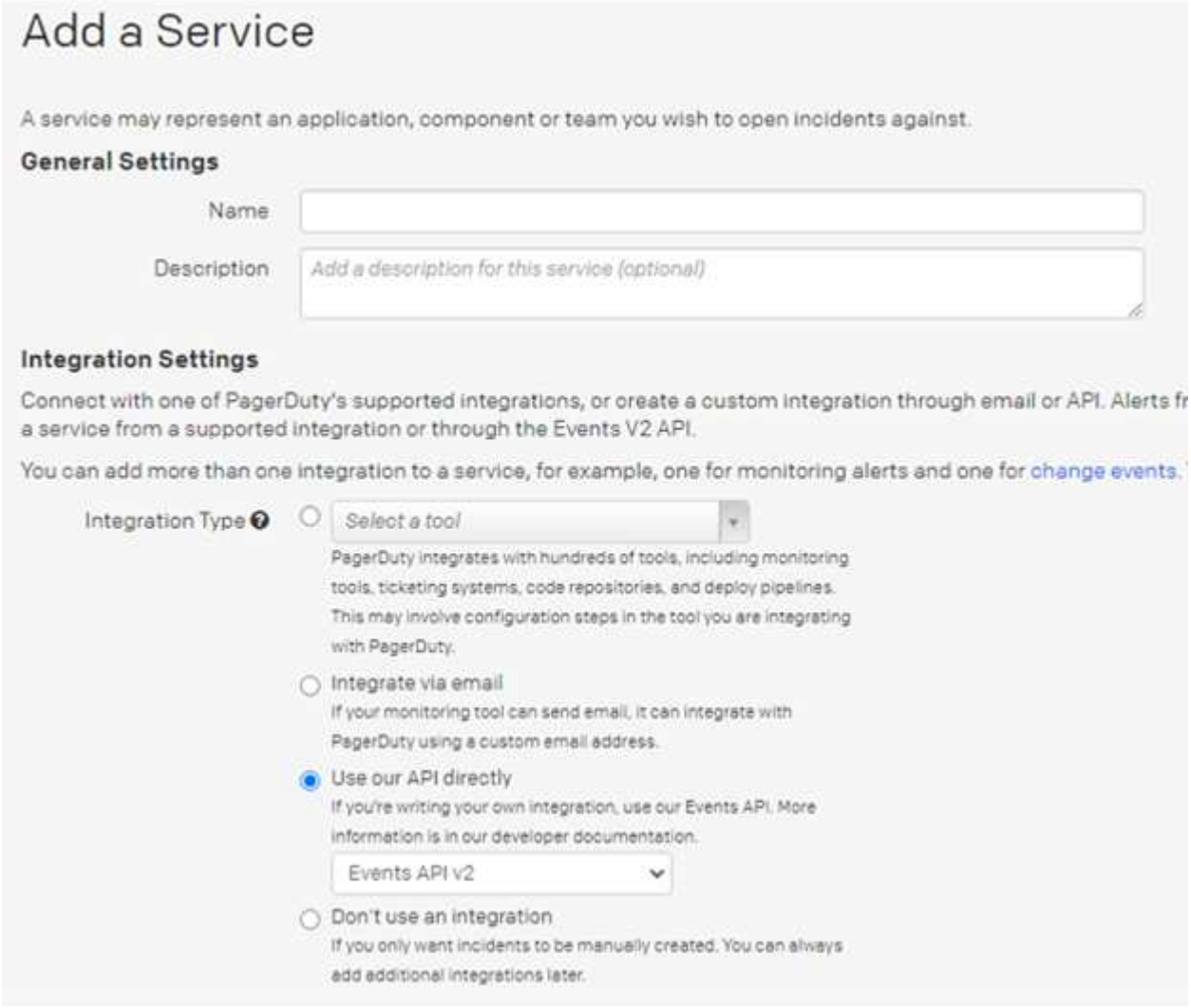
Webhook を使用すると、ユーザーはカスタマイズされた Webhook チャネルを使用して

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。このページでは、PagerDuty の Webhook を設定する例を示します。

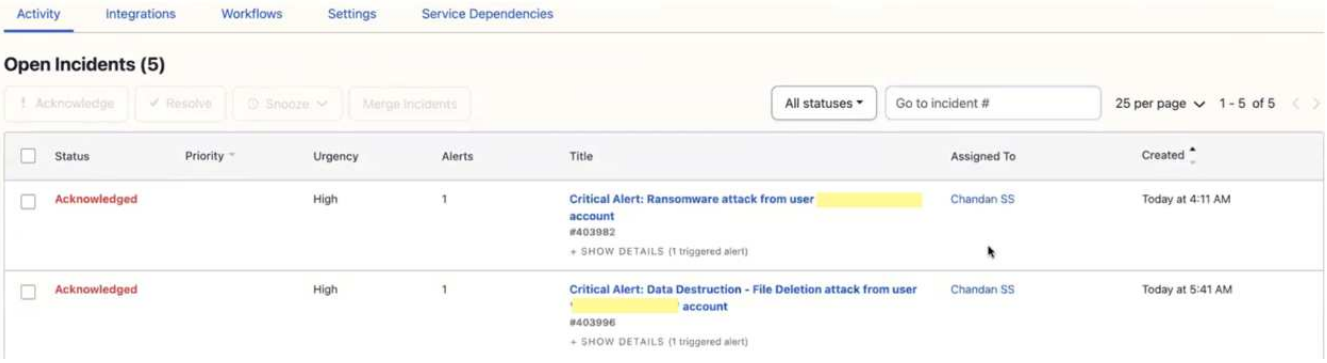
このページはサードパーティの指示を参照しており、変更される可能性があります。参照"PagerDutyのドキュメント"最新情報についてはこちらをご覧ください。

PagerDutyのセットアップ**:**

1. PagerDuty で、サービス **>** サービス ディレクトリ に移動し、**+** 新しいサービス ボタンをクリックします。
2. _名前_を入力し、_API を直接使用_を選択します。 _サービスの追加_を選択します。

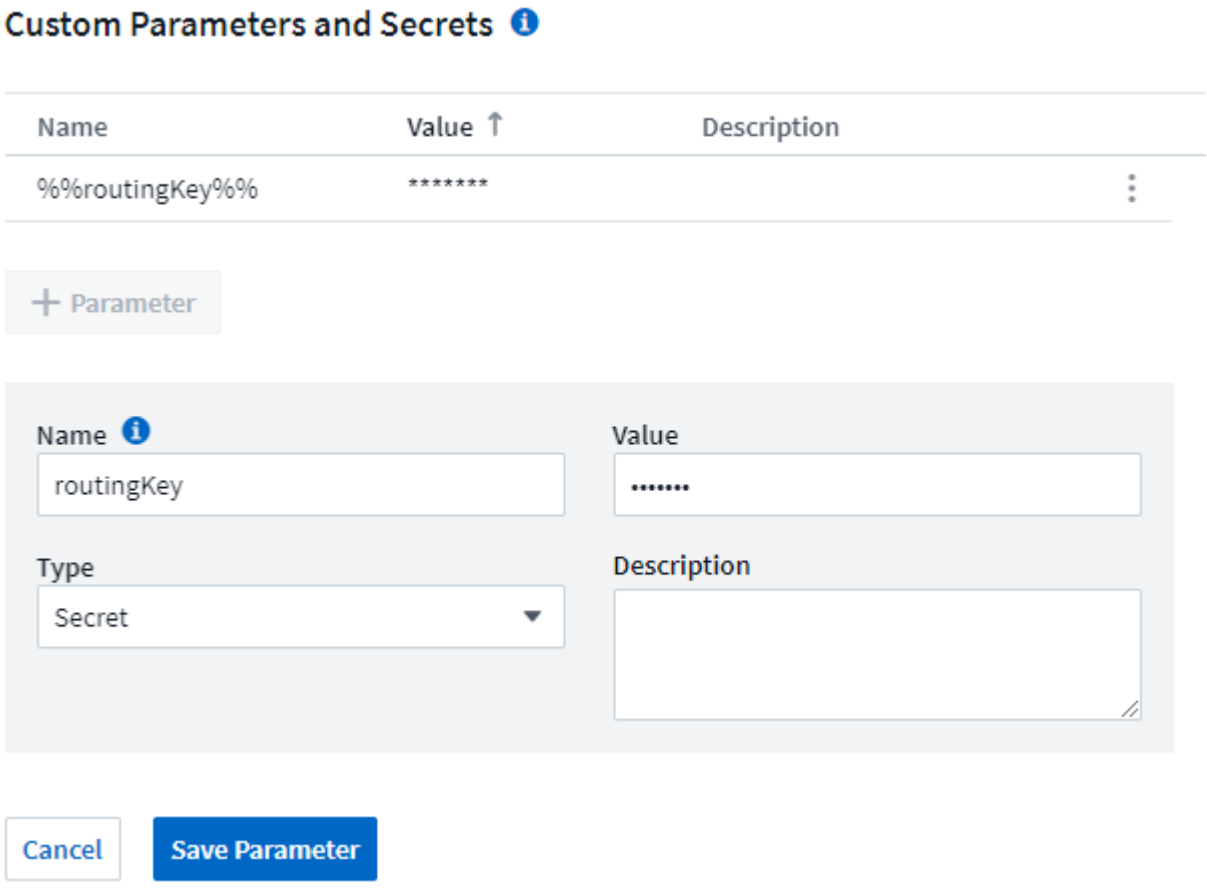


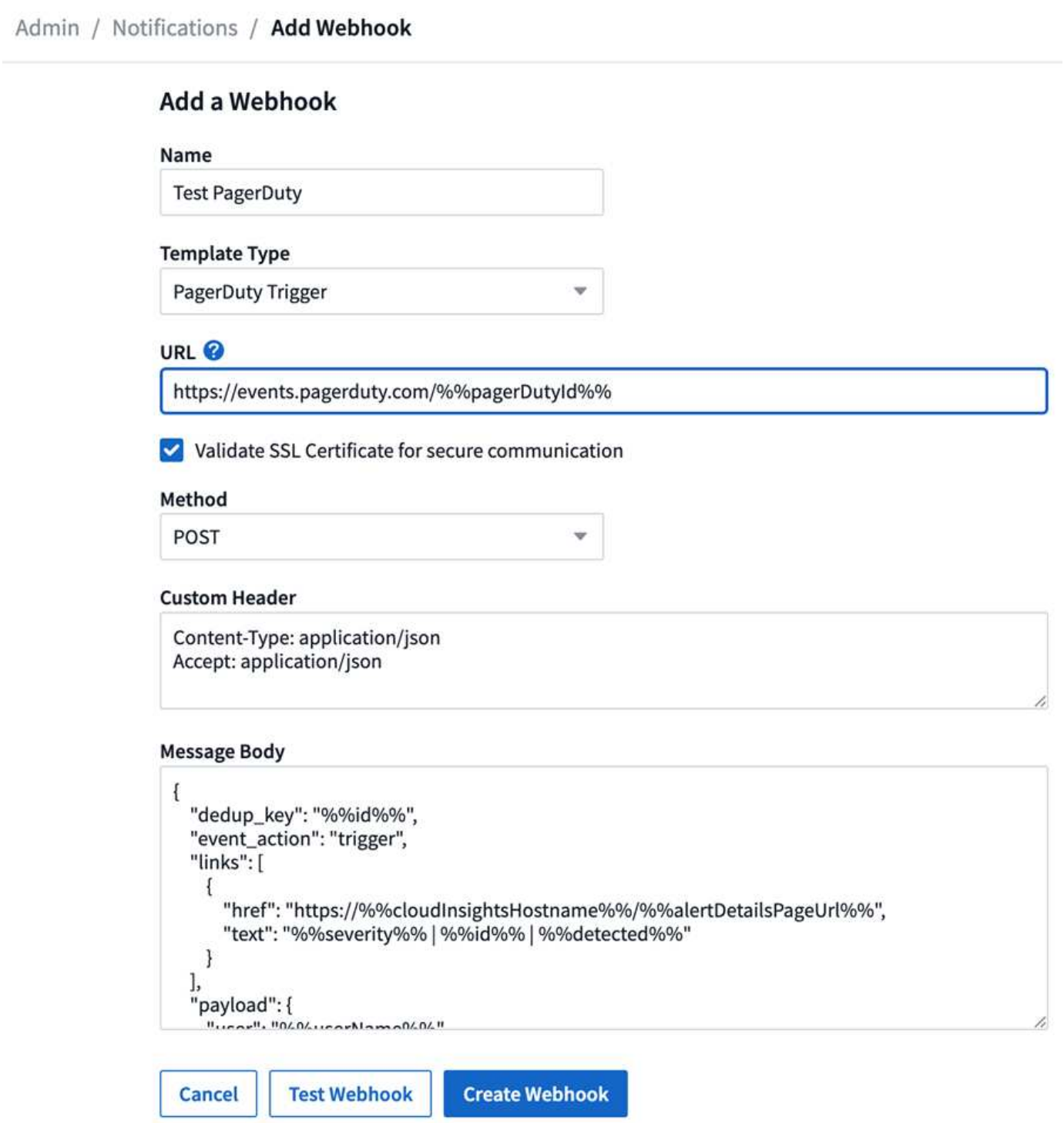
3. *統合キー*を表示するには、[統合] タブを選択します。以下の Workload Security Webhook を作成するときに、このキーが必要になります。
4. アラートを表示するには、「インシデント」または「サービス」に移動します。



Workload Security PagerDuty Webhook を作成します。

- 「管理」>「通知」に移動し、「*Workload Security Webhooks*」タブを選択します。新しい Webhook を作成するには、「+ Webhook」を選択します。
- Webhook に意味のある名前を付けます。
- テンプレート タイプ ドロップダウンで、*PagerDuty* トリガー を選択します。
- *routingKey* という名前のカスタム パラメータ シークレットを作成し、その値を上記で作成した PagerDuty *Integration Key* に設定します。

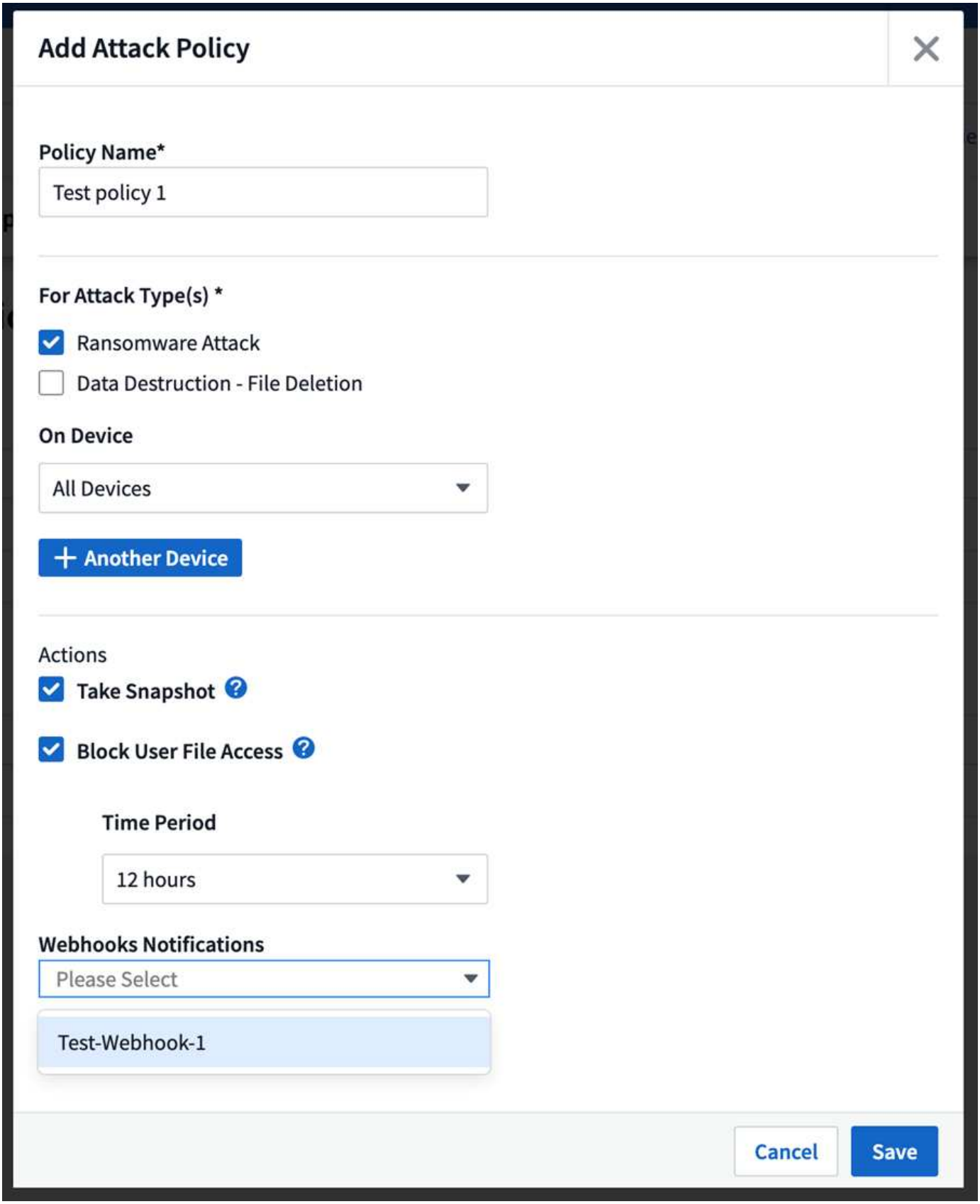




Webhook経由の通知

- Webhook 経由でイベントを通知するには、[*Workload Security*] > [ポリシー] に移動します。 +攻撃ポリシー_または+警告ポリシー_を選択します。
- 意味のあるポリシー名を入力します。
- 必要な攻撃タイプ、ポリシーを適用するデバイス、および必要なアクションを選択します。
- [*Webhooks Notifications*] ドロップダウンで、必要な PagerDuty Webhook を選択します。ポリシーを保存します。

注: Webhook は、編集することで既存のポリシーに添付することもできます。



Slack 向けワークロード セキュリティ Webhook の例

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。このページでは、Slack 用の Webhook を設定する例を示します。

このページはサードパーティの指示を参照しており、変更される可能性があります。最新情報については、Slack のドキュメントを参照してください。

Slackの例

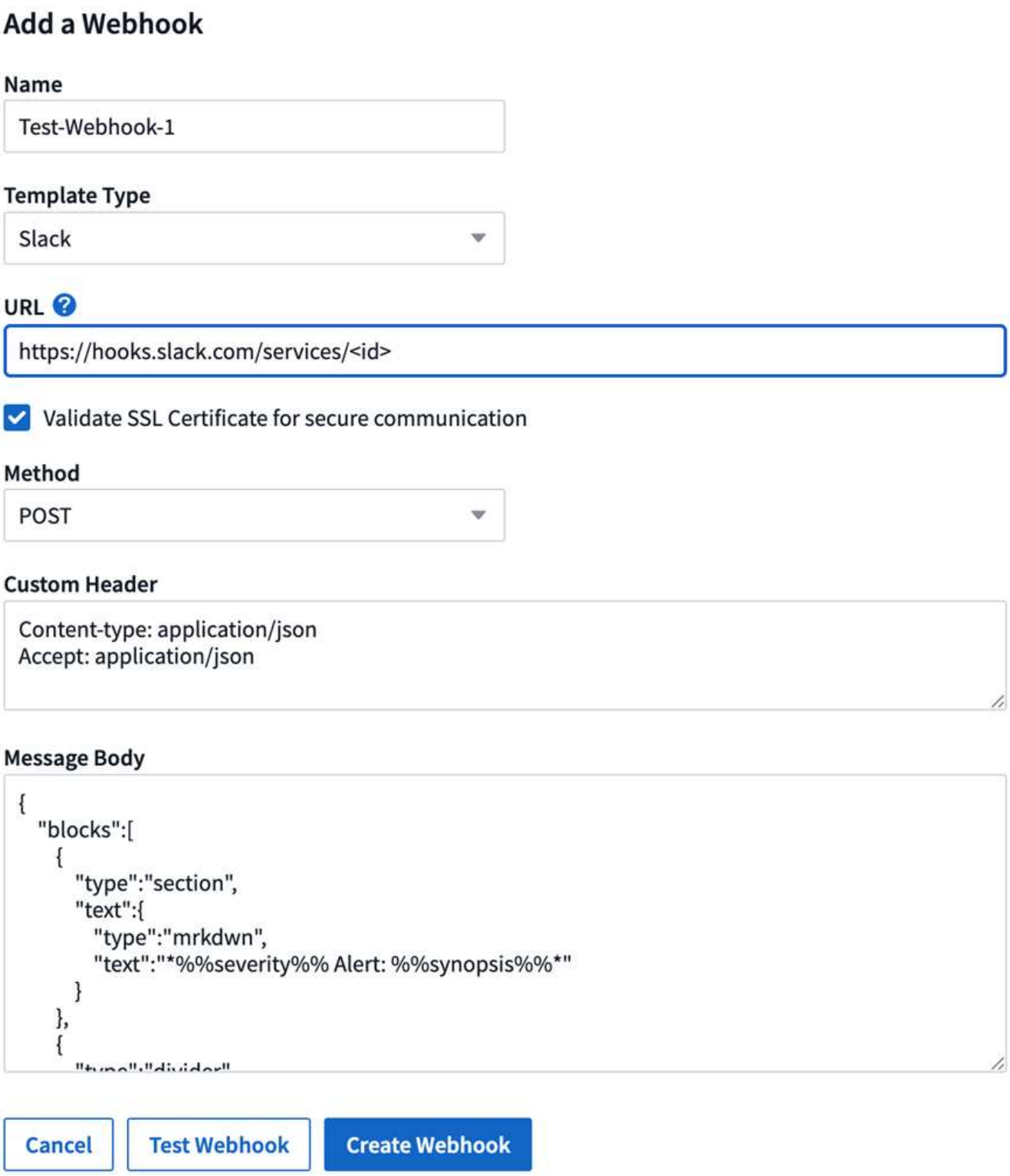
- へ移動 https://api.slack.com/apps新しいアプリを作成します。意味のある名前を付けて、ワークスペースを選択します。



- 「Incoming Webhooks」に移動し、「*Activate Incoming Webhooks*」をクリックし、「*Add New Webhook*」を選択して、投稿するチャネルを選択します。
- Webhook URL をコピーします。この URL は、Workload Security Webhook を作成するときに提供されます。

ワークロードセキュリティ **Slack Webhook** を作成する

1. 「管理」>「通知」に移動し、「*Workload Security Webhooks*」タブを選択します。新しい Webhook を作成するには、[+ *Webhook*] を選択します。
2. Webhook に意味のある名前を付けます。
3. テンプレート タイプ ドロップダウンで、*Slack* を選択します。
4. 上記からコピーしたURLを貼り付けます。

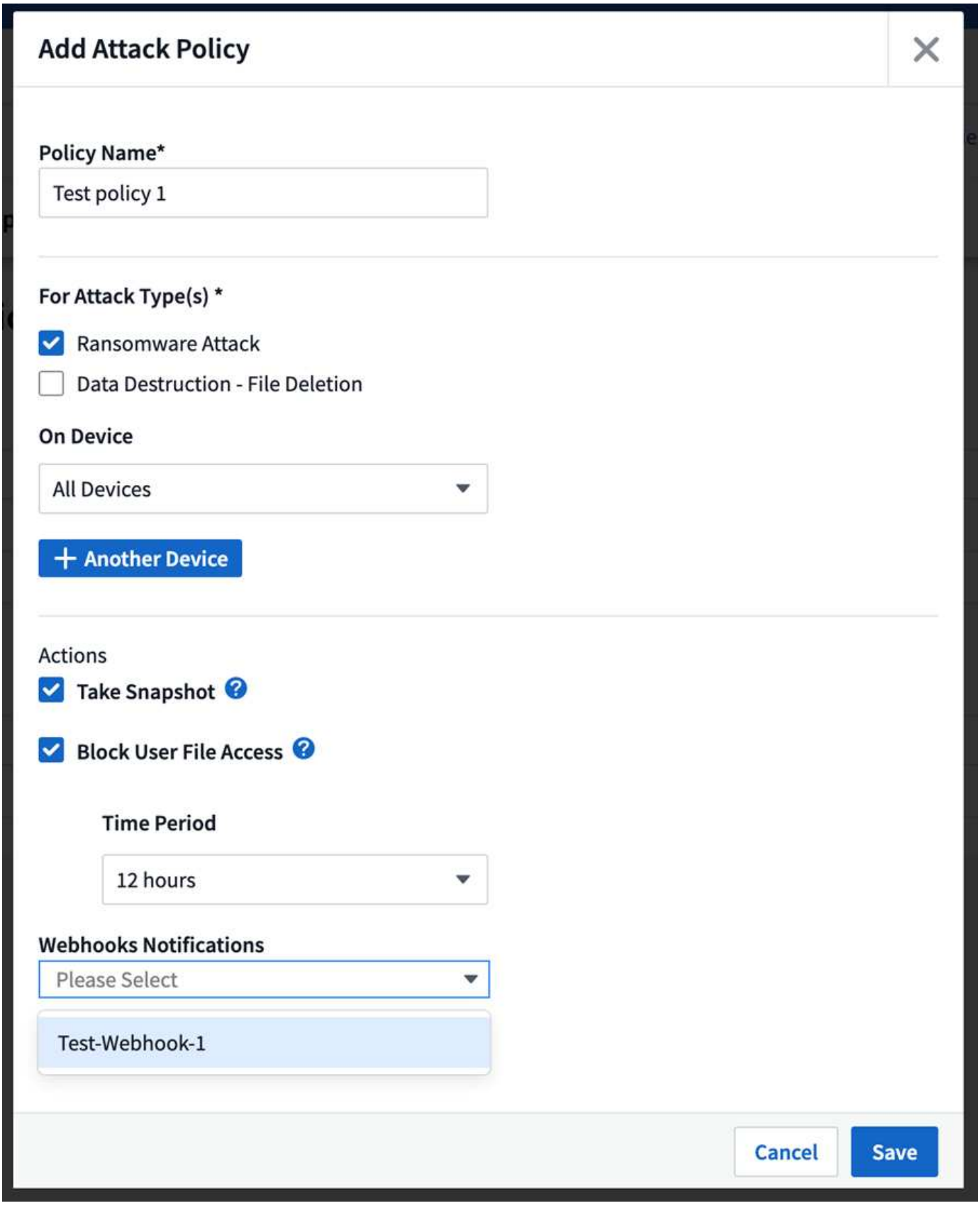


Webhook経由の通知

- Webhook 経由でイベントを通知するには、[*Workload Security*] > [ポリシー] に移動します。 +攻撃ポリシー_または+警告ポリシー_をクリックします。
- 意味のあるポリシー名を入力します。
- 必要な攻撃タイプ、ポリシーを適用するデバイス、および必要なアクションを選択します。

- [*Webhooks Notifications*] ドロップダウンで、必要な Webhook を選択します。ポリシーを保存します。

注: Webhook は、編集することで既存のポリシーに添付することもできます。



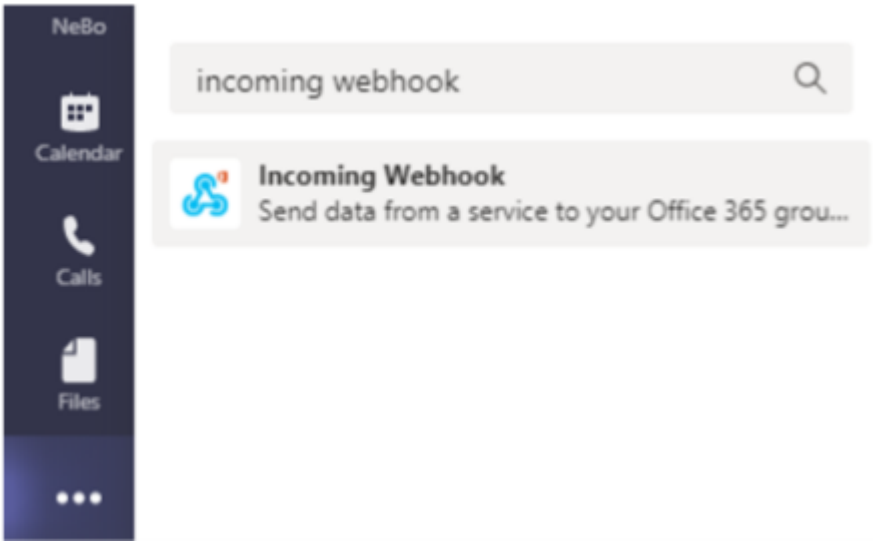
Microsoft Teams のワークロード セキュリティ Webhook の例

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。このページでは、Teams の Webhook を設定する例を示します。

このページはサードパーティの指示を参照しており、変更される可能性があります。参照"Teamsドキュメント"最新情報についてはこちらをご覧ください。

Teams のセットアップ**:**

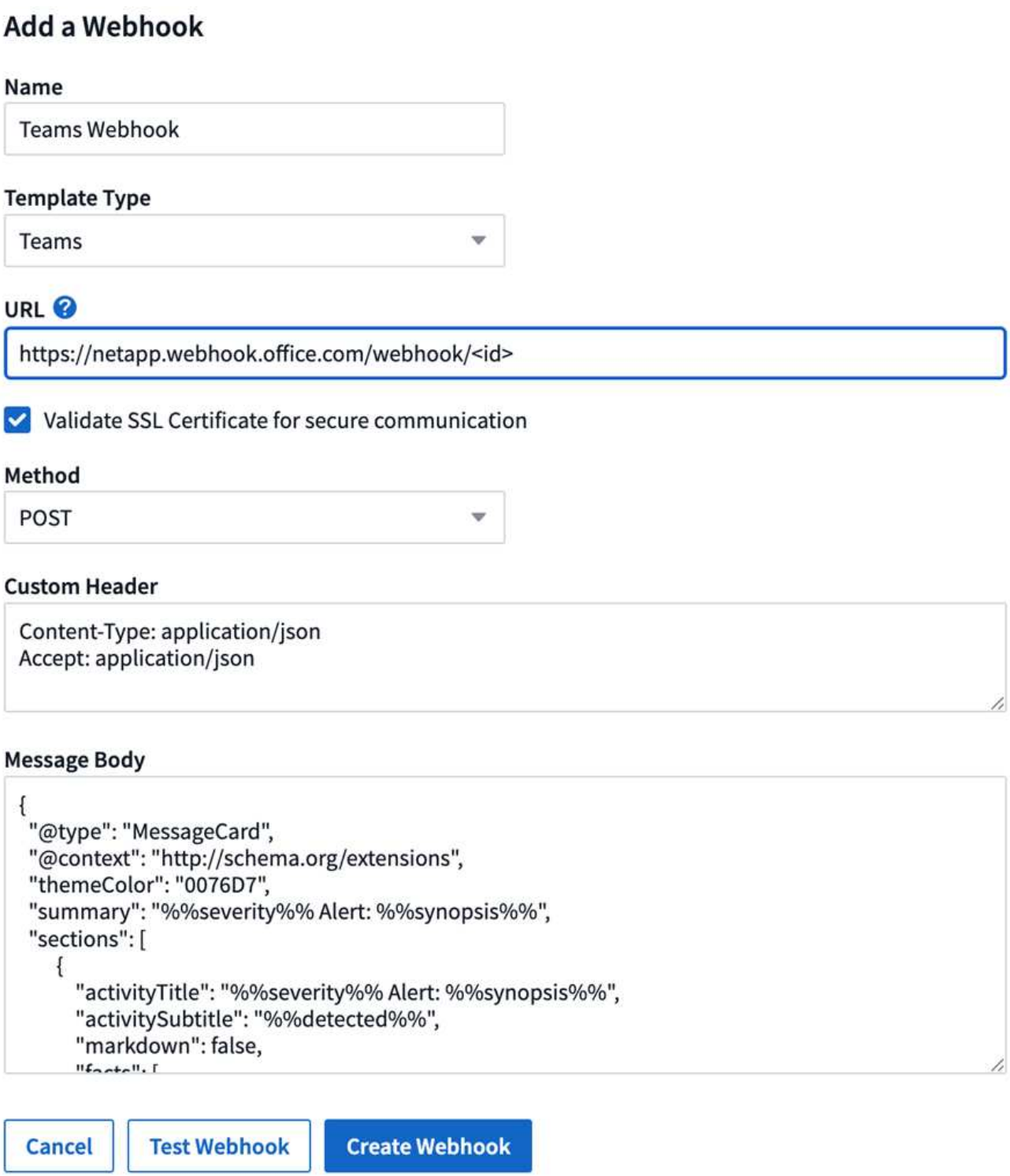
1. Teams でケバブを選択し、Incoming Webhook を検索します。



2. *チームに追加 > チームを選択 > コネクタの設定*を選択します。
3. Webhook URL をコピーします。これを Workload Security Webhook 設定に貼り付ける必要があります。

ワークロード セキュリティ チームの **Webhook** を作成します。

1. 「管理」>「通知」に移動し、「Workload Security Webhooks」タブを選択します。新しい Webhook を作成するには、[+ *Webhook*] を選択します。
2. Webhook に意味のある名前を付けます。
3. [テンプレート タイプ] ドロップダウンで、[**Teams**] を選択します。



4. 上記の URL を *URL* フィールドに貼り付けます。

アダプティブカードテンプレートを使用して**Teams**通知を作成する手順

1. メッセージ本文を次のテンプレートに置き換えます：

```
{
"type": "message",
```

```
"attachments": [
  {
    "contentType": "application/vnd.microsoft.card.adaptive",
    "content": {
      "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
      "type": "AdaptiveCard",
      "version": "1.2",
      "body": [
        {
          "type": "TextBlock",
          "text": "%%severity%% Alert: %%synopsis%%",
          "wrap": true,
          "weight": "Bolder",
          "size": "Large"
        },
        {
          "type": "TextBlock",
          "text": "%%detected%%",
          "wrap": true,
          "isSubtle": true,
          "spacing": "Small"
        },
        {
          "type": "FactSet",
          "facts": [
            {
              "title": "User",
              "value": "%%userName%%"
            },
            {
              "title": "Attack/Abnormal Behavior",
              "value": "%%type%%"
            },
            {
              "title": "Action taken",
              "value": "%%actionTaken%%"
            },
            {
              "title": "Files encrypted",
              "value": "%%filesEncrypted%%"
            },
            {
              "title": "Encrypted files suffix",
              "value": "%%encryptedFilesSuffix%%"
            },
            {
```

```
                "title": "Files deleted",
                "value": "%%filesDeleted%%"
              },
              {
                "title": "Activity Change Rate",
                "value": "%%changePercentage%%"
              },
              {
                "title": "Severity",
                "value": "%%severity%%"
              },
              {
                "title": "Status",
                "value": "%%status%%"
              },
              {
                "title": "Notes",
                "value": "%%note%%"
              }
            ]
          }
        ],
        "actions": [
          {
            "type": "Action.OpenUrl",
            "title": "View Details",
            "url":
"https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%"
          }
        ]
      }
    }
  ]
}
```

2. Power Automate Flows を使用している場合、URL 内のクエリパラメータはエンコードされた形式になります。入力する前に URL をデコードする必要があります。
3. 「Webhook をテスト」をクリックして、エラーがないことを確認します。
4. Webhook を保存します。

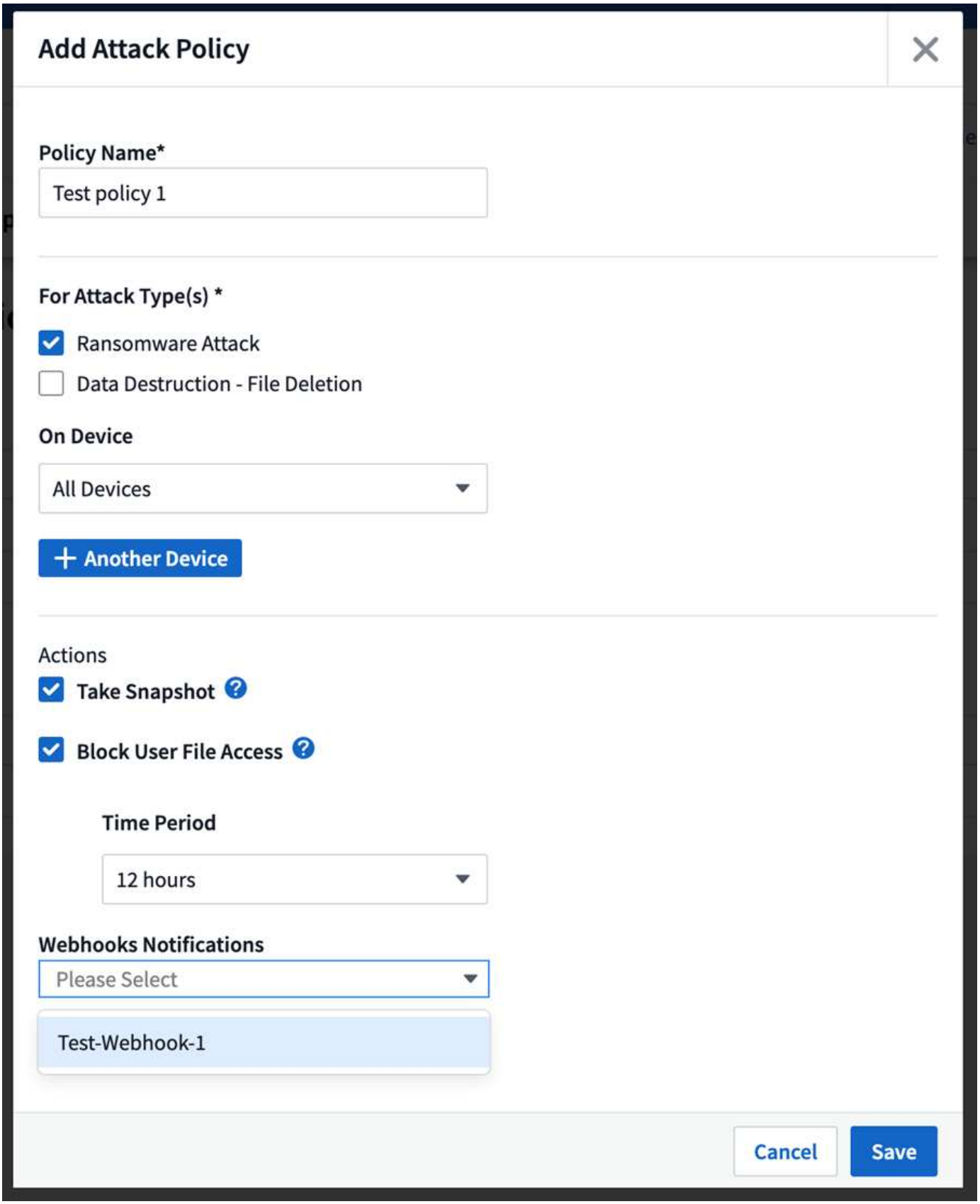
Webhook経由の通知

Webhook 経由でイベントを通知するには、[*Workload Security*] > [ポリシー] に移動します。 +攻撃ポリシー_ または+警告ポリシー_を選択します。

- 意味のあるポリシー名を入力します。

- 必要な攻撃タイプ、ポリシーを適用するデバイス、および必要なアクションを選択します。
- [*Webhooks Notifications*] ドロップダウンで、必要な Teams Webhook を選択します。ポリシーを保存します。

注: Webhook は、編集することで既存のポリシーに添付することもできます。



ワークロードセキュリティ**API**

安全なトークンベース認証で保護された REST API を使用して、Workload Security をエ

ンタープライズ エコシステムに統合できます。フォレンジック アクティビティ データの取得、API アクセス トークンの管理、CMDB、チケット システム、その他のアプリケーションとのカスタム統合の開発が可能です。インタラクティブな Swagger ドキュメントでは、完全な API 仕様が提供されており、エンドポイントを直接テストできます。

API アクセスの要件:

- アクセスを許可するには、API アクセス トークン モデルが使用されます。
- API トークンの管理は、管理者ロールを持つ Workload Security ユーザー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、Workload Security にログインし、管理 **> API** アクセス に移動すると見つかります。 **API** ドキュメント リンクをクリックします。 API ドキュメントは Swagger ベースであり、API の簡単な説明と使用方法の情報を提供し、テナントで試用することができます。

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 を複数回呼び出す場合は、呼び出しが並列ではなく順番に行われるようにしてください。複数の並列呼び出しにより、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

Workload Security 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:

- *管理 > APIアクセス*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*を入力してください
- *トークンの有効期限*を指定します

トークンは、作成プロセス中にクリップボードにコピーして保存するためにのみ使用できます。トークンは作成後に取得することはできないため、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に求められます。

トークンを無効化、有効化、取り消しできます。無効になっているトークンを有効にすることができます。

トークンは、顧客の観点から API への汎用アクセスを許可し、独自のテナントの範囲内で API へのアクセスを管理します。

アプリケーションは、ユーザーが正常に認証してアクセスを承認するとアクセス トークンを受け取り、ターゲット API を呼び出すときにアクセス トークンを資格情報として渡します。渡されたトークンは、トークンの所有者が API にアクセスし、承認時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することを承認されたことを API に通知します。

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、ストレージ アセットを取得するには、次を使用します。

```
 curl https://<Workload Security tenant>/rest/v1/cloudsecure/activities -H
'X-CloudInsights-ApiKey: <API_Access_Token>'
```

ここで、_<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あり、_<Workload Security Tenant>_ は Workload Security 環境のテナント URL です。

詳細情報は、管理 > **API** アクセス の *API* ドキュメント リンクで確認できます。

API経由でデータを抽出するスクリプト

Workload Security エージェントには、要求された時間範囲をより小さなバッチに分割することで、v2 API への並列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。同じディレクトリにある README ファイルに使用方法が記載されています。

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 <Workload Security tenant>
--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
```

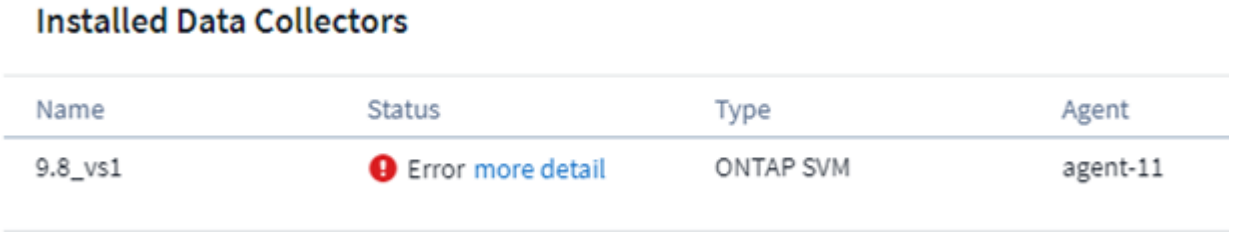
主なパラメータ: - `--iteration_interval 12` : 要求された時間範囲を 12 時間間隔に分割します。 - `--num_workers 3` : 3 つのスレッドを使用してこれらの間隔を並列に取得します。

ONTAP SVM データコレクタのトラブルシューティング

Workload Security はデータ コレクターを使用して、デバイスからファイルおよびユーザー アクセス データを収集します。ここでは、このコレクターに関する問題のトラブルシューティングのヒントを見つけることができます。

参照"SVMコレクターの設定"このコレクターを構成する手順については、このページをご覧ください。

エラーが発生した場合は、「インストールされたデータ コレクター」ページの [ステータス] 列の [詳細] をクリックすると、エラーの詳細が表示されます。



既知の問題とその解決策を以下に説明します。

問題: データ コレクターがしばらく実行され、ランダムな時間の経過後に停止し、次のエラーが発生します: 「エラー メッセージ: コネクタがエラー状態です。サービス名: 監査。失敗の理由: 外部ポリシー サーバーが過負荷です。これを試してください: ONTAPからのイベント レートは、エージェント ボックスが処理できるレートよりもはるかに高かったです。そのため接続は終了しました。

切断が発生したときの CloudSecure のピーク トラフィックを確認します。これは、**CloudSecure >** アクティビティフォレンジック **>** すべてのアクティビティ ページから確認できます。

ピーク集約トラフィックがエージェント ボックスで処理できる量を超える場合は、エージェント ボックスでのコレクター展開のサイズ設定方法について、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 日より前にエージェントがエージェント ボックスにインストールされていた場合は、エージェント ボックスで次のコマンドを実行します。

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

サイズ変更後、UI からコレクターを再起動します。

{空の}

問題: コレクターがエラー メッセージを報告します: 「SVM のデータ インターフェイスに到達できるコネクタにローカル IP アドレスが見つかりません」。 これを試してください: これは、 ONTAP側のネットワークの問題が原因である可能性が最も高いです。次の手順に従ってください。

1. SVM データ LIF または管理 LIF に SVM からの接続をブロックす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 経由で SVM を追加する場合は、SVM のデータ LIF と管理 LIF がエージェント VM から ping 可能であることを確認してください。問題が発生した場合は、LIF のゲートウェイ、ネットマスク、ルートを確認してください。

   クラスター管理 IP を使用して ssh 経由でクラスターにログインし、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、エージェント マシンが ping 可能であるように、 ONTAPのネットワーク設定が正しいことを確認します。
3. クラスタ IP 経由で接続しようとしたが機能しない場合は、SVM IP 経由で直接接続してみてください。SVM IP 経由で接続する手順については上記を参照してください。

4. SVM IP および vsadmin 資格情報を使用してコレクターを追加するときに、SVM Lif でデータ プラス Mgmt ロールが有効になっているかどうかを確認します。この場合、SVM Lif への ping は機能しますが、SVM Lif への SSH は機能しません。はいの場合は、SVM 管理専用 Lif を作成し、この SVM 管理専用 Lif 経由で接続してみます。
5. それでも動作しない場合は、新しい SVM Lif を作成し、その Lif を介して接続してみてください。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てください。
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 からデータ コレクターを SVM に接続してみます。
    c. エラーが表示されるまでお待ちください。 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。この場所で入手可能です

        https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
        .. ONTAPからエージェント ボックスへの SYN があることを確認します。
        .. ONTAPからの SYN がない場合、それはONTAPのファイアウォールに問題があります。
        .. ONTAPでファイアウォールを開き、 ONTAP がエージェント ボックスに接続できるようにします。

7. それでも動作しない場合は、ネットワーク チームに相談して、 ONTAPからエージェント ボックスへの接続が外部ファイアウォールによってブロックされていないことを確認してください。
8. 上記のいずれの方法でも問題が解決しない場合は、"NetApp サポート"さらにサポートが必要な場合はお問い合わせください。

{空の}

問題: メッセージ:「[ホスト名: <IP アドレス>] のONTAPタイプを判別できませんでした。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)" 次を試してください:

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. 接続先の SVM またはクラスターに SSH で接続します。接続したら、SVM またはクラスター名が正しいことを確認します。

{空の}

問題: 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: 監査。失敗の理由: 外部ポリシー サーバーが終了しました。 これを試してみてください:

1. おそらく、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ると考えられます。エージェント マシンが SVM から接続できるように、ポート範囲 35000 ～ 55000/tcp が開かれていることを確認します。また、 ONTAP側でエージェント 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も確認してください。

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 | grep 3500*
```

サンプル出力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
. 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確認する"ONTAP側で。

3. 監視する SVM/クラスターに SSH で接続します。 SVM データ LIF (CIFS、NFS プロトコルをサポート) からエージェント ボックスに ping を実行し、ping が機能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、エージェント マシンが ping 可能であるように、 ONTAPのネットワーク設定が正しいことを確認します。

4. 1 つの SVM が 2 つのデータ コレクターを介してテナントに 2 回追加されると、このエラーが表示されます。 UI を通じてデータ コレクターの 1 つを削除します。次に、UI を介して他のデータ コレクターを再起動します。その後、データ コレクターは「実行中」ステータスを表示し、SVM からのイベントの受信を開始します。

   基本的に、テナントでは、1 つのデータ コレクターを介して 1 つの SVM を 1 回だけ追加する必要があります。 1 つの SVM を 2 つのデータ コレクター経由で 2 回追加しないでください。

5. 同じ SVM が 2 つの異なる Workload Security 環境 (テナント) に追加された場合には、最後の SVM が常に成功します。 2 番目のコレクターは独自の IP アドレスを使用して fpolicy を設定し、最初のコレクターを排除します。したがって、最初のコレクター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。これを防ぐには、各 SVM を単一の環境で構成します。

6. サービス ポリシーが正しく構成されていない場合にも、このエラーが発生する可能性があります。 ONTAP 9.8 以降では、データ ソース コレクターに接続するには、データ サービス data-nfs や data-cifs とともに、data-fpolicy-client サービスが必要です。さらに、data-fpolicy-client サービスは、監視対象 SVM のデータ lif に関連付けられている必要があります。

{空の}

問題: アクティビティ ページにイベントが表示されません。 これを試してみてください:

1. ONTAPコレクターが「RUNNING」状態であるかどうかを確認します。はいの場合は、いくつかのファイルを開いて、CIFS クライアント VM 上でいくつかの CIFS イベントが生成されていることを確認します。
2. アクティビティが見られない場合は、SVM にログインして次のコマンドを入力してください。

   ```
   <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. アクティビティが見られない場合は、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「cloudsecure_」で名前が付けられた fpolicy ポリシーが設定されており、ステータスが「オン」になっているかどうかを確認します。設定されていない場合、エージェントは SVM でコマンドを実行できない可能性が高くなります。ページの冒頭に記載されているすべての前提条件が満たされていることを確認してください。

{空の}

問題: SVM データ コレクターがエラー状態にあり、エラー メッセージは「エージェントがコレクターへの接続に失敗しました」です。 次の操作を試してください:

1. おそらく、エージェントが過負荷になっており、データ ソース コレクターに接続できない状態です。
2. エージェントに接続されているデータ ソース コレクターの数を確認します。
3. また、UI の「すべてのアクティビティ」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 コレクターを新しいエージェントに移動します。

{空の}

問題: SVM データ コレクターに「fpolicy.server.connectError: ノードは FPolicy サーバー「12.195.15.146」との接続を確立できませんでした (理由:「選択がタイムアウトしました」)」というエラー メッセージが表示されます。 次のことを試してください: SVM/クラスター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 サーバーに接続できません。詳細情報を取得するために使用できるONTAPのCLI は次のとおりです。

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"ファイアウォールコマンドを確認する"ONTAP側で。

{空の}

問題: 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:監査。失敗の理由: SVM に有効なデータ インターフェイス (ロール: データ、データ プロトコル: NFS または CIFS またはその両方、ステータス: アップ) が見つかりません。 次のことを試してください: 動作可能なインターフェース (データとしての役割と CIFS/NFS としてのデータ プロトコルを持つ) があることを確認します。

{空の}

問題: データ コレクターがエラー状態になり、しばらくすると実行状態になり、その後再びエラー状態に戻ります。このサイクルが繰り返されます。 これを試してみてください: 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ーが追加されています。
2. このような動作を示すデータ コレクターには、1 つの SVM が追加されます。つまり、2 つ以上のデータ コレクターが 1 つの SVM に接続されます。
3. 1 つのデータ コレクターが 1 つの SVM にのみ接続す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 コレクターを削除します。

{空の}

問題: コネクタがエラー状態です。サービス名: 監査。失敗の理由: SVM svmname のポリシーの設定に失敗しました。理由: 'fpolicy.policy.scope-modify: "Federal" 内の 'shares-to-include' 要素に無効な値が指定されました。 次を試してください: *共有名は引用符なしで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。

共有を含めるおよび除外する は、共有名の長いリストを対象としていません。含めるまたは除外する株式が多数ある場合は、代わりに数量によるフィルタリングを使用します。

{空の}

問題: クラスター内に未使用の既存の fpolicies が存在します。 Workload Security をインストールする前に、これらに対して何をすべきでしょうか? これを試してください: 切断状態であっても、既存の未使用の fpolicy 設定をすべて削除することをお勧めします。 Workload Security は、プレフィックス「cloudsecure_」を持つ fpolicy を作成します。その他の未使用の fpolicy 構成はすべて削除できます。

fpolicy リストを表示する CLI コマンド:

```
 fpolicy show
```

fpolicy 構成を削除する手順:

```
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>
```

{空の}

問題: Workload Security を有効にすると、 ONTAP のパフォーマンスに影響が出ます。レイテンシが散発的に高くなり、IOPS が散発的に低くなります。 これを試してください: ONTAP をWorkload Security とともに使用している場合、 ONTAPで遅延の問題が発生することがあります。これには、次に示すように、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 以降で修正されているため、これらの新しいバージョンのいずれかを使用することを強くお勧めします。

{空の}

問題: データ コレクターに次のエラー メッセージが表示されます:「エラー: 2 回の再試行でコレクターの状態を判別できませんでした。コレクターをもう一度再起動してください (エラー コード: AGENT008)」。 これを試してみてください:

1. 「データ コレクター」ページで、エラーが発生しているデータ コレクターの右までスクロールし、3 つのドット メニューをクリックします。 編集_を選択します。データコレクターのパスワードをもう一度入力してください。 _*Save* ボタンを押してデータ コレクターを保存します。データ コレクターが再起動し、エラーが解決されるはずです。
2. エージェント マシンに十分な CPU または RAM の余裕がないため、DSC が失敗する可能性があります。マシン内のエージェントに追加されているデータ コレクター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 および RAM 容量を増やしてください。 CPU と RAM が増加すると、DSC は自動的に初期化状態になり、その後実行状態になります。サイズガイドをご覧ください"このページ"。

{空の}

問題: SVM モードを選択すると、データ コレクターでエラーが発生します。 これを試してください: SVM モードで接続しているときに、SVM 管理 IP ではなくクラスター管理 IP を使用して接続すると、接続でエラーが発生します。正しい SVM IP が使用されていることを確認してください。

{空の}

問題: アクセス拒否機能が有効になっている場合、データ コレクターに次のエラー メッセージが表示されます:「コネクタはエラー状態です。サービス名: 監査。失敗の理由: SVM test_svm で fpolicy を設定できませんでした。理由: ユーザーは承認されていません。 これを試してください: ユーザーにアクセス拒否機能に必要

な REST 権限がない可能性があります。以下の指示に従ってください"このページ"権限を設定します。

権限が設定されたら、コレクターを再起動します。

{空の}

問題**:** コレクターがエラー状態にあり、次のメッセージが表示されます: コネクタがエラー状態です。 失敗の理由: SVM <SVM 名> で永続ストアを構成できませんでした。 理由: SVM "<SVM Name>" 内のボリューム "<volumeName>" に適したアグリゲートが見つかりません。 理由: 集計 "<aggregateName>" のパフォーマンス情報は現在利用できません。サービス名: 監査。失敗の理由: SVM に永続的ストアを設定できませんでした。<svm name=""></svm>理由:ボリューム「」に適したアグリゲートが<volumename>SVM「<svm name="">」</svm>に</volumename>見つかりません。理由: アグリゲート「」のパフォーマンス情報<aggregatename>は現在使用できません。</aggregatename>数分待ってからもう一度コマンドを実行してください。

次の操作を試してください**:** 数分待ってからコレクターを再起動します。

{空の}

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。

トラブルシューティング

一般的なData Infrastructure Insightsの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提案を紹介します。

参照"Linux 取得ユニットの問題のトラブルシューティング"そして"Windows 取得ユニットの問題のトラブルシューティング"。

ログインに関する問題

問題：	これを試してみてください:
Data Infrastructure Insightsは6時間ごとに自動的にログアウトします	これはブラウザのサードパーティ Cookie が無効になっているために発生します。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 Cookie を有効にすることも、より狭い例外リストを使用してData Infrastructure Insightsの Cookie のみを有効にすることもできます。例: ブラウザの設定を開き、「すべての Cookie を許可する」オプションを選択します。 または「サードパーティの Cookie をブロックする」を選択し、*[*.]auth0.com* と *[*.]netapp.com* の例外を追加します。 Microsoft Edge は、例外に関して Chrome と同じ形式に従います。 Firefox では、Cookie 例外は単に *auth0.com* と *netapp.com* として指定されます。
コンソールアカウントを持っていますが、ログインできません。	チケットを開く https://mysupport.netapp.com/site/help。カテゴリ「console.netapp.com > アカウント/ログインの問題」または「console.netapp.com > フェデレーションの問題」を選択します。これらは、コンソールの問題や質問に特化しています。その他のData Infrastructure Insightsのテクニカルサポートの問題については、"NetAppサポート" 。
Data Infrastructure Insightsに招待されましたが、「承認されていません」というメッセージが表示されます。	コンソール アカウントにサインアップしていること、または組織がコンソールで SSO ログインを使用していることを確認します。コンソール プロファイルの電子メール アドレスが、 Data Infrastructure Insightsのウェルカム メールに記載されている電子メール アドレスと一致していることを確認します。メールアドレスが一致しない場合は、正しいメールアドレスで新しい招待をリクエストしてください。

問題：	これを試してみてください:
コンソールからログアウトすると、 Data Infrastructure Insightsからも自動的にログアウトされました。	NetAppクラウド サービス全体のシングル サインオン (SSO) により、すべてのData Infrastructure Insights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、いずれか 1 つのアカウントからログアウトすると、すべてのアクティブなセッションがログアウトされます。アカウントにアクセスするには再度ログインしてください。
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 (現在のコンソール設定は 7 日です)。アカウントにアクセスするには再度ログインしてください。
「ログインする権限がありません」というエラーメッセージが表示されます。	Data Infrastructure Insightsへのアクセスを確認するには、アカウント管理者に問い合わせてください。コンソール プロファイルのメール アドレスが、 Data Infrastructure Insightsのウェルカム メールに記載されているメール アドレスと一致していることを確認します。
その他のログインエラー	Chrome でシークレット モードを試すか、ブラウザの履歴、Cookie、キャッシュを消去してください。別のブラウザ プロファイル (Chrome - Person を追加など) を試してください。

その他の問題

質問：	答え：
Qtree ハード クォータはクエリで正しく表示されますが、ソフト クォータはボリュームの合計容量として表示されます。それは正しいですか？	設定されたクォータとして表示されるのは、手動で設定されたか、またはTridentを通じて設定されたハード クォータのみです。ハード クォータが指定されていない場合、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。これは正しいですか?	はい、ハード クォータが指定されている場合は、それが合計容量として表示されます。
Cognos レポートのスケジュール時間を入力すると、スケジュール時間に余分な「m」が入ってしまうことがあります。たとえば、時間を「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ることがあります。外側をクリックすると、「午前 2:15」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、スケジュール時間に AM と PM のどちらを入力したかに関係なく、スケジュール時間は AM (午前) として表示されます。	スケジュール時刻を再入力します。「AM」または「PM」の文字をすべて入力しないように注意してください。「AM」の場合は「A」、「PM」の場合は「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、スケジュール時間は正しく設定されています。

リソース

追加のトラブルシューティングのヒントについては、"NetAppナレッジベース" (サポートへのサインインが必

要です)。

追加のサポート情報は、Data Infrastructure Insightsから入手できます。"サポート"ページ。

アクティブなData Infrastructure Insightsサブスクリプションをお持ちの場合は、次のサポート オプションを使用できます。

"電話番号" "サポートチケット"

詳細については、 "Data Infrastructure Insightsサポートドキュメント" 。

Linux での取得ユニットの問題のトラブルシューティング

ここでは、Linux サーバー上の Acquisition Units 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紹介します。

問題：	これを試してみてください:
Observability > Collectors ページの **Acquisition Units** タブの AU ステータスに、「証明書の有効期限が切れました」または「証明書が取り消されました」と表示されます。	AU の右側にあるメニューをクリックし、*接続の復元*を選択します。取得ユニットを復元するには、次の手順に従ってください。1. Acquisition Unit (AU) サービスを停止します。 [停止コマンドのコピー] ボタンをクリックすると、コマンドをクリップボードにすばやくコピーし、このコマンドを取得ユニット 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/cloudinsights/acq/conf* フォルダーに「token」という名前のファイルを作成します。3. [トークンをコピー] ボタンをクリックし、このトークンを作成したファイルに貼り付けます。4.AUサービスを再開します。 [再起動コマンドのコピー] ボタンをクリックし、コマンドを AU のコマンド プロンプトに貼り付けます。
取得ユニット サーバー サービスの起動時にアクセスが拒否されました	AU を SELINUX にインストールする場合、SE を *permissive* モードに設定する必要があります。 *Enforcing* モードはサポートされていません。 SELINUX を許可モードに設定した後、AU サービスを再起動します。
サーバー要件が満たされていません	取得ユニットサーバーまたはVMが以下の要件を満たしていることを確認してください。"要件"

ネットワーク要件が満たされていません	Acquisition Unit サーバー/VM がポート 443 経由の SSL 接続を介してData Infrastructure Insights環境 (<environment-name>.c01.cloudinsights.netapp.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ください: *ping <environment-name>.c01.cloudinsights.netapp.com traceroute <environment-name>.c01.cloudinsights.netapp.com curl https://<environment-name>.c01.cloudinsights.netapp.com wget https://<environment-name>.c01.cloudinsights.netapp.com* AU からData Infrastructure Insightsへの「アウトバウンド」でポート 443 を開く必要があることに注意してください。
プロキシサーバーが正しく構成されていません	プロキシ設定を確認し、正しいプロキシ設定を入力するために、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ください。1. 「curl」を試してください。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 は多くのプロキシ設定をサポートしているため、ワイルドカード「*」です)。2. 「wget」を試してください。プロキシ オプションについてはドキュメントを確認してください。
取得サービスの開始中に資格情報エラーが発生し、Data Infrastructure Insightsで取得ユニットのインストールに失敗しました (acq.log に表示されます)。	これは、プロキシ資格情報に特殊文字が含まれていることが原因で発生する可能性があります。 AU をアンインストールし (*sudo cloudinsights-uninstall.sh*)、特殊文字を使用せずに再インストールします。
Linux: ライブラリが見つからない / ファイルが見つからない	Linux Acquisition Unit サーバー/VM に必要なライブラリがすべて揃っていることを確認します。たとえば、サーバーに *unzip* ライブラリがインストールされている必要があります。 *unzip* ライブラリをインストールするには、Acquisition Unit インストール スクリプトを実行する前に、コマンド **sudo yum install unzip** を実行します。
権限の問題	_sudo_権限を持つユーザーとしてログインしていることを確認してください
取得が実行されていません:	/opt/netapp/cloudinsights/acq/logs から acq.log を収集します (Linux) 取得サービスを再起動します: sudo cloudinsights-service.sh restart acquisition
データ収集の問題:	「エラーレポートを送信」ボタンをクリックして、データコレクターのランディングページから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Data Infrastructure Insightsにハートビートを送信します。ネットワークの問題または応答しないData Infrastructure Insights が原因でハートビート呼び出しが失敗した場合、AU のリース時間は更新されません。 AU のリースの期限が切れると、Data Infrastructure Insights に「ハートビート失敗」というステータスが表示されます。トラブルシューティングの手順: Acquisition Unit サーバーと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。取得ユニット ログ (/var/log/netapp/cloudinsights/acq/acq.log) をチェックして、エラーがある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ます	このエラーは、ネットワークの中断により、Acquisition Unit とData Infrastructure Insights環境間の通信が 1 分以上中断された場合に発生する可能性があります。 AU とData Infrastructure Insights間の接続が安定しておりアクティブであることを確認します。
取得ユニットを再インストールすると、「ValueError: File context for /opt/netapp/cloudinsights(/.*)? already defined」というメッセージが表示されます。	SELinux搭載のシステムでは、このエラーメッセージは `cloudinsights-uninstall.sh -p`が実行され、取得ユニットが再インストールされます。コマンドを実行する `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

組織でインターネット アクセスにプロキシの使用が必要な場合は、組織のプロキシの動作を理解し、 Data Infrastructure Insightsが機能するための特定の例外を探す必要がある場合があります。次の事項に注意してください。

- まず、組織ではデフォルトでアクセスをブロックし、例外的に特定の Web サイト/ドメインへのアクセスのみを許可していますか? 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取得ユニット、および Web ブラウザーでのData Infrastructure Insightsとのやり取りはすべて、そのドメイン名を持つホストに送信されます。

- 2 番目に、一部のプロキシは、 NetAppから生成されていないデジタル証明書を使用してData Infrastructure Insights Web サイトになりすまして TLS/SSL 検査を実行しようとします。Data Infrastructure Insights取得ユニットのセキュリティ 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。また、 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容易にするには、上記のドメイン名をこの機能から除外する必要があります。

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、プロキシ環境とツールによって異

なりますが、一般的には、AU がこれらのサーバーと適切に通信できるようにするには、 Data Infrastructure Insightsサーバーの URL をこの例外リストに追加する必要があります。

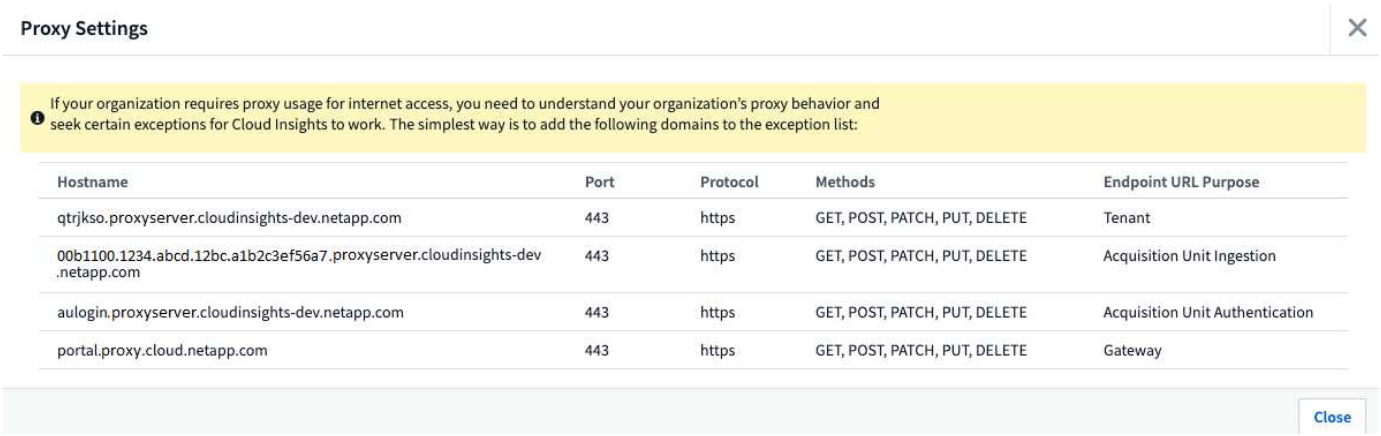
これを行う最も簡単な方法は、Data Infrastructure Insightsドメイン自体を例外リストに追加することです。

```
*.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、例外リストが必要になる場合と、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不明な場合、またはプロキシやファイアウォールの構成により`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問い合わせて、プロキシの `SSL` インターセプト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

オンボーディング中にデータ コレクターを選択するときに [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 エンドポイントを表示できます。次のような表が表示されます。環境に Workload Security がある場合は、設定されたエンドポイント URL もこのリストに表示されます。



リソース

追加のトラブルシューティングのヒントについては、"NetAppナレッジベース" (サポートへのサインインが必要です)。

追加のサポート情報は、Data Infrastructure Insightsから入手できます。"サポート"ページ。

Windows での取得ユニットの問題のトラブルシューティング

ここでは、Windows サーバー上の Acquisition Units 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紹介します。

問題：	これを試してみてください:

Observability > Collectors ページの **Acquisition Units** タブの AU ステータスに、「証明書の有効期限が切れました」または「証明書が取り消されました」と表示されます。	AU の右側にあるメニューをクリックし、*接続の復元*を選択します。取得ユニットを復元するには、次の手順に従ってください。1. Acquisition Unit (AU) サービスを停止します。 [停止コマンドのコピー] ボタンをクリックすると、コマンドをクリップボードにすばやくコピーし、このコマンドを取得ユニット 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* フォルダーに「token」という名前のファイルを作成します。3. [トークンをコピー] ボタンをクリックし、このトークンを作成したファイルに貼り付けます。4.AUサービスを再開します。 [再起動コマンドのコピー] ボタンをクリックし、コマンドを AU のコマンド プロンプトに貼り付けます。
サーバー要件が満たされていません	取得ユニットサーバーまたはVMが以下の要件を満たしていることを確認してください。"要件"
ネットワーク要件が満たされていません	Acquisition Unit サーバー/VM がポート 443 経由の SSL 接続を介してData Infrastructure Insights環境 (<environment-name>.c01.cloudinsights.netapp.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ください: *ping <environment-name>.c01.cloudinsights.netapp.com traceroute <environment-name>.c01.cloudinsights.netapp.com curl https://<environment-name>.c01.cloudinsights.netapp.com wget https://<environment-name>.c01.cloudinsights.netapp.com* AU からData Infrastructure Insightsへの「アウトバウンド」でポート 443 を開く必要があることに注意してください。
プロキシサーバーが正しく構成されていません	プロキシ設定を確認し、正しいプロキシ設定を入力するために、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ください。1. 「curl」を試してください。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 は多くのプロキシ設定をサポートしているため、ワイルドカード「*」です)。2. 「wget」を試してください。プロキシ オプションについてはドキュメントを確認してください。
取得サービスの開始中に資格情報エラーが発生し、Data Infrastructure Insightsで取得ユニットのインストールに失敗しました (acq.log に表示されます)。	これは、プロキシ資格情報に特殊文字が含まれていることが原因で発生する可能性があります。 AU をアンインストールし (*sudo cloudinsights-uninstall.sh*)、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ーとしてログインしていることを確認してください
取得が実行されていません	情報は、<インストール ディレクトリ>\ *Cloud Insights\Acquisition Unit\log* フォルダーの acq.log で見つかります。 Windowsサービス経由で取得を再開する

データ収集の問題	「エラーレポートを送信」ボタンをクリックして、データコレクターのランディングページから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Data Infrastructure Insightsにハートビートを送信します。ネットワークの問題または応答しないData Infrastructure Insights が原因でハートビート呼び出しが失敗した場合、AU のリース時間は更新されません。 AU のリースの期限が切れると、Data Infrastructure Insights に「ハートビート失敗」というステータスが表示されます。トラブルシューティングの手順: * Acquisition Unit サーバーと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 ログ (<Install dir>:\Program Files\ Cloud Insights\Acquisition Unit\log\acq.log) をチェックして、エラーがある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ます	このエラーは、ネットワークの中断により、Acquisition Unit とData Infrastructure Insights環境間の通信が 1 分以上中断された場合に発生する可能性があります。 AU とData Infrastructure Insights間の接続が安定しており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

組織でインターネット アクセスにプロキシの使用が必要な場合は、組織のプロキシの動作を理解し、 Data Infrastructure Insightsが機能するための特定の例外を探す必要がある場合があります。次の事項に注意してください。

- まず、組織ではデフォルトでアクセスをブロックし、例外的に特定の Web サイト/ドメインへのアクセスのみを許可していますか? 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
  ```

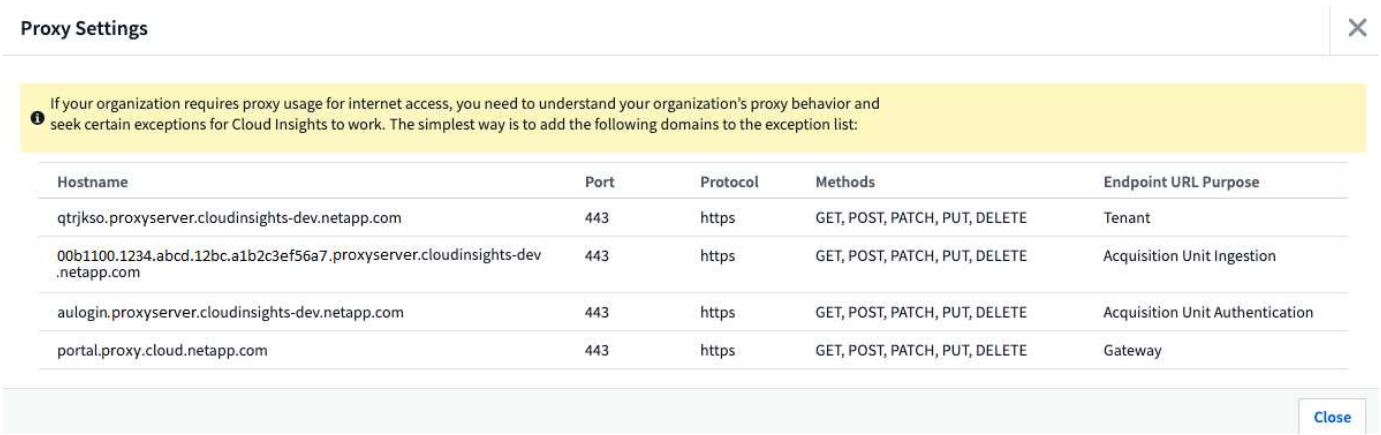
  Data Infrastructure Insights取得ユニット、および Web ブラウザーでのData Infrastructure Insightsとのやり取りはすべて、そのドメイン名を持つホストに送信されます。

- 2 番目に、一部のプロキシは、 NetAppから生成されていないデジタル証明書を使用してData Infrastructure Insights Web サイトになりすまして TLS/SSL 検査を実行しようとします。Data Infrastructure Insights取得ユニットのセキュリティ 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。また、 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容易にするには、上記のドメイン名をこの機能から除外する必要があります。

プロキシエンドポイントの表示

オンボーディング中にデータ コレクターを選択するときに [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 エンドポイントを表示できま

す。次のような表が表示されます。環境に Workload Security がある場合は、設定されたエンドポイント URL もこのリストに表示されます。



リソース

追加のトラブルシューティングのヒントについては、"NetAppナレッジベース" (サポートへのサインインが必要です)。

追加のサポート情報は、Data Infrastructure Insightsから入手できます。"サポート"ページ。

失敗したデータ収集装置の調査

データ コレクターに失敗メッセージがあり、影響度が高または中程度の場合、リンクされた情報を含むデータ コレクターの概要ページを使用してこの問題を調査する必要があります。

データ コレクターの障害の原因を特定するには、次の手順に従います。データ コレクターの障害メッセージは、管理者 メニューと インストールされたデータ コレクター ページに表示されます。

手順

1. 管理者 > データ コレクター > インストールされたデータ コレクター をクリックします。
2. 障害が発生したデータ コレクターのリンクされた名前をクリックして、[概要] ページを開きます。
3. [概要] ページで、[コメント] 領域をチェックして、この障害を調査している可能性のある別のエンジニアが残したメモを読んでください。
4. パフォーマンス メッセージがあればメモします。
5. イベント タイムライン グラフのセグメントの上にマウス ポインターを移動すると、追加情報が表示されます。
6. イベント タイムラインの下に表示されるデバイスのエラー メッセージを選択し、メッセージの右側に表示されるエラーの詳細アイコンをクリックします。

   エラーの詳細には、エラー メッセージのテキスト、最も可能性の高い原因、使用中の情報、問題を修正するために試すことができる内容の提案が含まれます。

7. 「このデータ コレクターによって報告されたデバイス」領域では、リストをフィルターして関心のあるデバイスのみを表示できます。また、デバイスのリンクされた 名前 をクリックして、そのデバイスの資産

ページを表示できます。

8. データ コレクター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] 領域をチェックして、最近の変更が問題の原因になっているかどうかを確認します。

Data Infrastructure Insightsデータコレクターサポートマトリックス

データ コレクター サポート マトリックスには、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 コレクターのリファレンスが提供されます。

HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ ストレージ

このデータコレクターでサポートされてい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 7200 • HPE_3PAR 7200c • HPE_3PAR 7400 • HPE_3PAR 7400c • 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 7440c • HP_3PAR 7450c • HP_3PAR 8200 • HP_3PAR 8400 • HP_3PAR 8440 • InServ F200 • InServ F400 • InServ T400 • InServ T800 • InServ V400 • InServ V800	• 3.1.1（MU1） • 3.1.2（MU3） • 3.1.3（MU1） • 3.1.3（MU2） • 3.2.1（MU2） • 3.2.1（MU3） • 3.2.1（MU5） • 3.2.2（MU4） • 3.2.2（MU6） • 3.3.1 • 3.3.1（MU1） • 3.3.1（MU2） • 3.3.1（MU3） • 3.3.1（MU5） • 3.3.2（MU1） • 4.3.1 • 4.3.3 • 4.4.1 リリースタイプ：標準サポートリリース • 4.5.15 リリースタイプ：延長サポートリリース • 4.5.18 リリースタイプ：延長サポートリリース • 4.5.21 リリースタイプ：延長サポートリリース • 4.5.24 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 • 4.6.1 リリースタイプ：延長サポートリリース • 9.5.15 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 • 9.6.1 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ーでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		トローラー			
		ストレージポート	実装済み	SSH	
製品	カテゴリ	特徴/属性 タイプ	ステータス ギャップ	使用されるプロトコル SSH	追加情報
	ボリュームマスク	イニシエータ	実装済み	SSH	
		プロトコルコントローラー	実装済み	SSH	
		ストレージポート	実装済み	SSH	
		タイプ	ギャップ	SSH	
	ボリューム参照	Name	実装済み	SSH	
		ストレージIP	実装済み	SSH	
	WWNエイリアス	ホストエイリアス	実装済み	SSH	
		オブジェクト タイプ	実装済み	SSH	
		ソース	実装済み	SSH	
		WWN	実装済み	SSH	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		スループット書き込み	実装済み	SMI-S	
製品	カテゴリ	書き込み保留中 特徴/属性	実装済み 実装ステータス	SMI-S 使用されるプロトコル	合計書き込み保留中 追加情報
	Volume	キャッシュヒット率読み取り	実装済み	SMI-S	
		キャッシュヒット率合計	実装済み	SMI-S	
		キャッシュヒット率書き込み	実装済み	SMI-S	
		物理容量	実装済み	SMI-S	
		総容量	実装済み	SMI-S	
		使用容量	実装済み	SMI-S	
		書面による能力	実装済み	SMI-S	
		使用容量比率	実装済み	SMI-S	
		容量比率書き込み	実装済み	SMI-S	
		総圧縮節約	実装済み	SMI-S	
		IOPS読み取り	実装済み	SMI-S	ディスク上の読み取りIOPS数
		IOP合計	実装済み	SMI-S	
		IOPS書き込み	実装済み	SMI-S	
		鍵	実装済み	SMI-S	
		レイテンシ読み取り	実装済み	SMI-S	
		レイテンシ合計	実装済み	SMI-S	
		レイテンシ書き込み	実装済み	SMI-S	
		部分ブロック率	実装済み	SMI-S	
		サーバ ID	実装済み	SMI-S	
		スループット読み取り	実装済み	SMI-S	
		スループット合計	実装済み	SMI-S	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	SMI-S	
		書き込み保留中	実装済み	SMI-S	合計書き込み保留中

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
3Par SMI-S	SMI-S	HTTP / HTTPS	5988/5989		true	true	true	true
3Par CLI	SSH	SSH	22		true	false	true	true

アマゾンAWSEC2

このデータコレクターでサポートされているモデルとバージョン: API バージョン:

- 2014/10/01

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		メーカー	実装済み	HTTPS	
		Name	実装済み	HTTPS	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		OID	実装済み	HTTPS	
	情報	APIの説明	実装済み	HTTPS	
		API名	実装済み	HTTPS	
		APIバージョン	実装済み	HTTPS	
		データソース名	実装済み	HTTPS	情報
		日付	実装済み	HTTPS	
		発信者ID	実装済み	HTTPS	
		発信者キー	実装済み	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

					と書き込み）（MB/秒）
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
		特徴/属性	実装ステータス	HTTPS	
	vm	合計CPU使用率	実装済み	HTTPS	
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		ディスクIops合計	実装済み	HTTPS	
		ディスクIOPS書き込み	実装済み	HTTPS	
		レイテンシ読み取り	実装済み	HTTPS	
		レイテンシ合計	実装済み	HTTPS	
		レイテンシ書き込み	実装済み	HTTPS	
		ディスクスループット読み取り	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	ディスクスループット合計読み取り
		ディスクスループット書き込み	実装済み	HTTPS	
		IPスループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	IPスループット合計
		ipThroughput.write	実装済み	HTTPS	
	VM	総容量	実装済み	HTTPS	
		鍵	実装済み	HTTPS	
		サーバ ID	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
EC2 API	HTTPS	HTTPS	443		true	true	true	true

アマゾンAWSS3

このデータコレクターでサポートされてい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ーでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					合計）
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
	ストレージ プール	DWH容量に含める	実装済み	HTTPS	ACQからDWH容量に関心のあるストレージプールを制御する方法
		Name	実装済み	HTTPS	
		物理ディスク容量（MB）	実装済み	HTTPS	ストレージプールの生の容量として使用
		レイドグループ	実装済み	HTTPS	このストレージプールがRAIDグループであるかどうかを示します
		原材料と使用可能量の比率	実装済み	HTTPS	使用可能容量から生の容量に変換する比率
		ストレージプールID	実装済み	HTTPS	
		シンプロビジョニングをサポート	実装済み	HTTPS	この内部ボリュームがその上のボリューム層に対してシンプロビジョニングをサポートしているかどうか
		割り当て済み容量の合計	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?
パフォーマンス	内部容積	総容量	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		使用容量比率	実装済み	HTTPS	
		鍵	実装済み	HTTPS	
		合計オブジェクト数	実装済み	HTTPS	
		サーバ ID	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
S3 API	HTTPS	HTTPS	443		true	true	true	true

Microsoft Azure NetApp Files

このデータコレクターでサポートされているモデルとバージョン:

API バージョン	モデル
2019年6月1日 2024年7月1日	Azure NetApp Files

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					合計）
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
	ストレージ プール	データ割り当て容量	ギャップ	HTTPS	データに割り当てられた容量
		データ使用容量	実装済み	HTTPS	
		DWH容量に含める	実装済み	HTTPS	ACQからDWH容量に関心のあるストレージプールを制御する方法
		Name	実装済み	HTTPS	
		物理ディスク容量（MB）	実装済み	HTTPS	ストレージプールの生の容量として使用
		レイドグループ	実装済み	HTTPS	このストレージプールがRAIDグループであるかどうかを示します
		原材料と使用可能量の比率	実装済み	HTTPS	使用可能容量から生の容量に変換する比率
		ステータス	実装済み	HTTPS	
		ストレージプールID	実装済み	HTTPS	
		シンプロビジョニングをサポート	実装済み	HTTPS	この内部ボリュームがその上のボリューム層に対してシンプロビジョニングをサポートしているかどうか
		割り当て済み容量の合計	実装済み	HTTPS	
		総使用容量	実装済み	HTTPS	総容量（MB）
		タイプ	ギャップ	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?
		コメント	ギャップ	HTTPS	状態: SVMを説明する自由形式のテキストコメント

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

					と書き込み）（MB/秒）
製品	カテゴリ	特徴/属性	実装済み/テスト書き込み	実装済み/テスト	使用されるプロトコル	追加情報
	ストレージプールディスク	IOPS読み取り	実装済み		ディスク上の読み取りIOPS数
		IOPS書き込み	実装済み		
		スループット読み取り	実装済み		
		スループット書き込み	実装済み		
		スループット合計	実装済み		平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		IOP合計	実装済み		

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
Azure NetApp ファイル REST API	HTTPS	HTTPS	443		true	true	true	true

Brocadeファイバーチャネルスイッチ

このデータコレクターでサポートされてい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
• 176.51 • 183.0 • Brocade 200E • Brocade 300E • Brocade 4024 Embedded • Brocade 5000 • Brocade 5100 • Brocade 5300 • Brocade 5480 Embedded • Brocade 6505 • Brocade 6510 • Brocade 6520 • Brocade 6546 • Brocade 6547 Embedded • Brocade 6548 • Brocade 6558 • Brocade 7800 • Brocade 7810 Extension Switch • 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 G730 • Brocade M5424 Embedded • Brocade VA-40FC • Brocade X6-4 • Brocade X6-8 • Brocade X7-4 • Brocade X7-8	• v6.2.2b • v6.2.2f • v6.2.2g • v6.4.1b • v6.4.2a • v6.4.3 • v6.4.3d • v6.4.3f3 • v7.0.1 • v7.0.1b • v7.0.2 • v7.0.2b1 • v7.0.2c • v7.0.2e • v7.0.2e1 • v7.1.0a • v7.1.0b • v7.2.0a • v7.2.0d • v7.2.1 • v7.2.1c • v7.2.1c1 • v7.2.1d • v7.3.0a • v7.3.0c • v7.3.1 • v7.3.1c • v7.3.1d • v7.3.2a • v7.4.0a • v7.4.1 • v7.4.1d • v7.4.1e • v7.4.2 • v7.4.2a • v7.4.2a4 v7.4.2c v7.4.2d

このデータコレクターでサポートされている製品:

-
- v7.4.2e
- v7.4.2f
- v7.4.2g
- v7.4.2g_cvr_824494_01
- v7.4.2h
- v7.4.2j1
- v8.0.2c
- v8.0.2d
- v8.0.2f
- v8.1.0b
- v8.1.1a
- v8.1.2a
- v8.1.2d
- v8.1.2f
- v8.1.2g
- v8.1.2h
- v8.1.2j
- v8.1.2k
- v8.2.0
- v8.2.0a
- v8.2.0a1
- v8.2.0b
- v8.2.1
- v8.2.1a
- 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
- v8.2.3a_cvr_855776_01
- v8.2.3b

v8.2.3c

v8.2.3c1

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団			• v8.2.3e • v8.2.3e1 • v8.2.3e2 • v9.0.0a • v9.0.1a • v9.0.1b • v9.0.1b4 • v9.0.1c • v9.0.1d • v9.0.1e • v9.0.1e1 • v9.1.0b • v9.1.1 • v9.1.1a • v9.1.1b • v9.1.1b_lw • v9.1.1c • v9.1.1d • v9.1.1d1 • v9.1.1d2 • v9.1.1d2_lw • v9.1.1d5 • v9.2.0a • v9.2.0b • v9.2.0b1_lw • v9.2.0c • v9.2.0c1 • v9.2.1a • v9.2.1a1 • v9.2.2		

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

	ゾーン	ゾーン名	実装済み	SSH	
	ゾーンメンバー	タイプ	ギャップ	SSH	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		WWN	実装済み	SSH	
	ゾーニング機能	アクティブ構成	実装済み	SSH	
		構成名	実装済み	SSH	
		デフォルトのゾーニング動作	実装済み	SSH	
		WWN	実装済み	SSH	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		ウト			
		合計ポートエラー数	実装済み	SNMP	合計ポートエラー
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		サーバ ID	実装済み	SNMP	
		トラフィックフレームレート	実装済み	SNMP	
		総トラフィックフレームレート	実装済み	SNMP	
		トラフィックフレームレート	実装済み	SNMP	
		平均フレームサイズ	実装済み	SNMP	トラフィックの平均フレームサイズ
		TXフレーム	実装済み	SNMP	トラフィックの平均フレームサイズ
		トラフィック受信率	実装済み	SNMP	
		総トラフィックレート	実装済み	SNMP	
		トラフィック送信速度	実装済み	SNMP	
		受信トラフィック使用率	実装済み	SNMP	
		総トラフィック使用率	実装済み	SNMP	総トラフィック使用率
		トラフィック送信使用率	実装済み	SNMP	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
Brocade SNMP	SNMP	SNMPv1、SNMPv2、SNMPv3	161		true	true	true	true
Brocade SSH	SSH	SSH	22		false	false	true	true
データソースウィザードの構成	手動入力				true	true	true	true

Brocadeネットワークアドバイザー HTTP

このデータコレクターでサポートされているモデルとバージョン:

API バージョン	モデル	ファームウェアバージョン
14.4.3 14.4.4	Brocade 6520、 Brocade DCX 8510-4、 Brocade G620、 Brocade X6-8、EMC Connectrix DS-6510B	v7.3.0b v7.4.1b v8.2.3c1 v9.0.1e1

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
760					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		不明な接続	実装済み	HTTP/S	
		ブレード	実装済み	HTTP/S	
製品	カテゴリ	特徴/属性 GBIC タイプ	ステータス 実装済み	使用されるプロトコル HTTP/S	追加情報
	スイッチ	WWN	実装済み	HTTP/S	
		IP	実装済み	HTTP/S	
		ファームウェアバージョン	実装済み	HTTP/S	
		メーカー	実装済み	HTTP/S	
		モデル	実装済み	HTTP/S	
		Name	実装済み	HTTP/S	
		役割を切り替える	実装済み	HTTP/S	
		タイプ	ギャップ	HTTP/S	
		シリアル番号	実装済み	HTTP/S	
		URLの管理	実装済み	HTTP/S	
		スイッチ状態	実装済み	HTTP/S	
		スイッチステータス	実装済み	HTTP/S	
		ドメインID	実装済み	HTTP/S	
		VSAN 有効	実装済み	HTTP/S	
	不明	WWN	実装済み	HTTP/S	
		メーカー	実装済み	HTTP/S	
		ファームウェア	実装済み	HTTP/S	
		ドライバ	実装済み	HTTP/S	
		モデル	実装済み	HTTP/S	
	WWNエイリアス	ホストエイリアス	実装済み	HTTP/S	
		オブジェクト タイプ	実装済み	HTTP/S	
		ソース	実装済み	HTTP/S	
		WWN	実装済み	HTTP/S	
	ゾーン	ゾーン名	実装済み	HTTP/S	
	ゾーンメンバー	タイプ	ギャップ	HTTP/S	
		WWN	実装済み	HTTP/S	
	ゾーニング機能	アクティブ構成	実装済み	HTTP/S	
		構成名	実装済み	HTTP/S	
		WWN	実装済み	HTTP/S	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス	ポート	BBクレジットゼロ送信	実装済み	HTTP/S	BBクレジットゼロ送信
		BBクレジットゼロ合計	実装済み	HTTP/S	BBクレジットゼロ合計
		BBクレジットゼロMS送信	実装済み	HTTP/S	BBクレジットゼロMS送信

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
Brocadeネットワークアドバイザー REST API	HTTP / HTTPS	HTTP / HTTPS	80/443		true	true	true	true

BrocadeFOS REST

このデータコレクターでサポートされてい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
• 183.0 • 184.0 • 190.0 • Brocade 6505 • Brocade 6510 • Brocade 6520 • Brocade 7810 Extension Switch • Brocade 7840 • Brocade DCX8510-4 • Brocade DCX8510-8 • Brocade G610 • Brocade G620 • Brocade G630 • Brocade G720 • Brocade G730 • Brocade X6-4 • Brocade X6-8 • Brocade X7-4 • Brocade X7-8	• v8.2.2a • v8.2.2d • v8.2.2d4 • v8.2.3 • v8.2.3a • v8.2.3b • v8.2.3c • v8.2.3c1 • v8.2.3d • v8.2.3e • v8.2.3e1 • v9.0.0b • v9.0.1a • v9.0.1b • v9.0.1b4 • v9.0.1c • v9.0.1d • v9.0.1e • v9.0.1e1 • v9.1.0b • v9.1.1a • v9.1.1b • v9.1.1c • v9.1.1c3 • v9.1.1d • v9.1.1d1 • v9.1.1d1_lw • v9.1.1d2 • v9.1.1d3_cvr_861742_01 • v9.2.0a • v9.2.0b • v9.2.0b1 • v9.2.0b_cvr_857687_01 • v9.2.0c • v9.2.0c3 • v9.2.1 v9.2.1a v9.2.1b

このデータコレクターでサポートされている製品:	• • v9.2.2

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

	ゾーン	ゾーン名	実装済み	HTTPS	
	ゾーンメンバー	タイプ	ギャップ	HTTPS	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		WWN	実装済み	HTTPS	
	ゾーニング機能	アクティブ構成	実装済み	HTTPS	
		構成名	実装済み	HTTPS	
		デフォルトのゾーニング動作	実装済み	HTTPS	
		WWN	実装済み	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		ー数			ー
		サーバ ID	実装済み	HTTPS	
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
		総トラフィックフレームレート	実装済み	HTTPS	
		総トラフィックフレームレート	実装済み	HTTPS	
		トラフィックフレームレート	実装済み	HTTPS	
		平均フレームサイズ	実装済み	HTTPS	トラフィックの平均フレームサイズ
		TXフレーム	実装済み	HTTPS	トラフィックの平均フレームサイズ
		トラフィック受信率	実装済み	HTTPS	
		総トラフィックレート	実装済み	HTTPS	
		トラフィック送信速度	実装済み	HTTPS	
		受信トラフィック使用率	実装済み	HTTPS	
		総トラフィック使用率	実装済み	HTTPS	総トラフィック使用率
		トラフィック送信使用率	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
BrocadeFOS REST API	HTTPS		443		true	true	true	true

Cisco MDS および Nexus ファブリック スイッチ

このデータコレクターでサポートされてい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
• DS-C9124-2-K9 • DS-C9124-K9 • DS-C9132T-K9 • DS-C9148-16P-K9 • DS-C9148-32P-K9 • DS-C9148-48P-K9 • DS-C9148S-K9 • DS-C9148T-K9 • DS-C9148V-K9 • DS-C9220I-K9 • DS-C9222I-K9 • DS-C9250I-K9 • DS-C9396S-K9 • DS-C9396T-K9 • DS-C9396V-K9 • DS-C9506 • DS-C9509 • DS-C9513 • DS-C9706 • DS-C9710 • DS-C9718 • DS-HP-8GFC-K9 • DS-HP-FC-K9 • N5K-C5548UP • N5K-C5596UP • N5K-C5696Q • UCS-FI-6248UP • UCS-FI-6296UP • UCS-FI-6332 • UCS-FI-6332-16UP • UCS-FI-64108 • UCS-FI-6454	• 3.3(1c) • 4.1（3a） • 4.2（1a） • 5.0（1a） • 5.0(3)N2(3.11e) • 5.0(3)N2(4.01d) • 5.0(3)N2(4.13i) • 5.0(3)N2(4.21e) • 5.0(3)N2(4.21j) • 5.0(3)N2(4.21k) • 5.0(3)N2(4.22c) • 5.0(3)N2(4.23f) • 5.0(3)N2(4.23g) • 5.0(3)N2(4.34a) • 5.0(8) • 5.2(2d) • 5.2(8) • 5.2（8a） • 5.2(8b) • 5.2(8c) • 5.2(8d) • 5.2(8f) • 5.2（8g） • 5.2（8h） • 5.2(8i) • 6.2(11) • 6.2(11b) • 6.2(11c) • 6.2(13) • 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)

このデータコレクターでサポートされている製品:

-
- 6.2(31)
- 6.2(33)
- 6.2（5a）
- 6.2(7)
- 6.2(9)
- 6.2（9a）
- 6.2(9b)
- 7.0(3)N2(4.04e)
- 7.0(3)N2(4.13b)
- 7.0(3)N2(4.13g)
- 7.3(0)D1(1)
- 7.3(1)DY(1)
- 7.3(13)N1(1)
- 7.3(8)N1(1)
- 8.1(1)
- 8.1（1a）
- 8.2(1)
- 8.2(2)
- 8.3(1)
- 8.3(2)
- 8.4(1)
- 8.4（1a）
- 8.4(2)
- 8.4（2a）
- 8.4(2b)
- 8.4(2c)
- 8.4(2d)
- 8.4(2e)
- 8.4(2f)
- 8.5(1)
- 9.2（1a）
- 9.2(2)
- 9.3(1)
- 9.3(2)
- 9.3（2a）

  9.3(5)I42(1b)

  9.3(5)I42(1g)

  9.3(5)I42(1j)

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団			• 9.3(5)I42(3f) • 9.3(5)I43(4b) • 9.4(1) • 9.4（1a） • 9.4(2) • 9.4（2a） • 9.4(3)		

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		タイプ	ギャップ	SNMP	
		VSAN 有効	実装済み	SNMP	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		WWN	実装済み	SNMP	
	不明	ドライバ	実装済み	SNMP	
		ファームウェア	実装済み	SNMP	
		生成された	実装済み	SNMP	
		メーカー	実装済み	SNMP	
		モデル	実装済み	SNMP	
		Name	実装済み	SNMP	
		WWN	実装済み	SNMP	
	WWNエイリアス	ホストエイリアス	実装済み	SNMP	
		オブジェクト タイプ	実装済み	SNMP	
		ソース	実装済み	SNMP	
		WWN	実装済み	SNMP	
	ゾーン	ゾーン名	実装済み	SNMP	
		ゾーンタイプ	実装済み	SNMP	
	ゾーンメンバー	タイプ	ギャップ	SNMP	
		WWN	実装済み	SNMP	
	ゾーニング機能	アクティブ構成	実装済み	SNMP	
		構成名	実装済み	SNMP	
		デフォルトのゾーニング動作	実装済み	SNMP	
		マージコントロール	実装済み	SNMP	
		WWN	実装済み	SNMP	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		トラフィックフレームレート	実装済み	SNMP	
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
		総トラフィックフレームレート	実装済み	SNMP	
		トラフィックフレームレート	実装済み	SNMP	
		平均フレームサイズ	実装済み	SNMP	トラフィックの平均フレームサイズ
		TXフレーム	実装済み	SNMP	トラフィックの平均フレームサイズ
		トラフィック受信率	実装済み	SNMP	
		総トラフィックレート	実装済み	SNMP	
		トラフィック送信速度	実装済み	SNMP	
		受信トラフィック使用率	実装済み	SNMP	
		総トラフィック使用率	実装済み	SNMP	総トラフィック使用率
		トラフィック送信使用率	実装済み	SNMP	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	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		true	true	true	true

結束力

このデータコレクターでサポートされてい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
C4000 コンピューティングノード C4600 C5036 C5066 C6025 C6035 C6055 CX8405 PXG1 UCS-C240M5H10 仮想ROBO	6.8.1_u1_release-20221022_6f58ed2a 6.8.2_u1_release-20240509_a5da4644 7.1.2_u2_release-20240925_66722648 7.1.2_u3_release-20241231_bb47fe77 7.2.1_release-20241114_794eae46 7.2.2_release-20250228_63e93ccf

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
786					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		割り当て済み容量の合計	実装済み		
		総使用容量	実装済み		総容量（MB）
製品	カテゴリ	特徴/属性タイプ	ステータスギャップ	使用されるプロトコル	追加情報
		バーチャル	実装済み		これはストレージ仮想化デバイスですか?
		暗号化	実装済み		
パフォーマンス	ストレージ	失敗した生の容量	実装済み		
		物理容量	実装済み		
		予備の生の容量	実装済み		スペアディスクの生の容量（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	実装済み		
		IOPS読み取り	実装済み		ディスク上の読み取りIOPS数
		IOP合計	実装済み		
		IOPS書き込み	実装済み		
		鍵	実装済み		
		レイテンシ読み取り	実装済み		
		レイテンシ合計	実装済み		
		レイテンシ書き込み	実装済み		
		サーバ ID	実装済み		
		スループット読み取り	実装済み		
		スループット合計	実装済み		平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み		
		利用合計	実装済み		

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
コヒーシティREST API	HTTPS	HTTPS	443		true	true	true	true

EMC Celerra (SSH)

このデータコレクターでサポートされているモデルとバージョン:

モデル	ファームウェアバージョン
NSX VG8 VNX5200 VNX5300 VNX5400 VNX5500	5.5.38-1 7.1.76-4 7.1.79-8 7.1.83-2 8.1.21-266 8.1.9-155

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		割り当て済み容量の合計	実装済み	SSH	
		総使用容量	実装済み	SSH	総容量（MB）
製品	カテゴリ	特徴/属性タイプ	ステータスギャップ	使用されるプロトコル	追加情報
		バーチャル	実装済み	SSH	これはストレージ仮想化デバイスですか?

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
Celerra CLI	SSH	SSH			true	false	true	true

EMC CLARiX (NaviCLI)

このデータコレクターでサポートされているモデルとバージョン:

API バージョン	モデル	ファームウェアバージョン
• 6.26 • 6.28 • 7.32 • 7.33	• CX3-40f • CX4-480 • VNX5100 • VNX5200 • VNX5300 • VNX5400 • VNX5500 • VNX5600 • VNX5700 • VNX5800 • VNX7600	• 04.28.000.5.710 • 05.32.000.5.206 • 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 • 05.33.008.5.119 • 05.33.009.5.155 • 05.33.009.5.184 • 05.33.009.5.186 • 05.33.009.5.231 • 05.33.009.5.238 • 05.33.021.5.256 • 05.33.021.5.266 • 05.33.021.5.322 • 3.26.40.5.029

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
802					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		タイプ	ギャップ	CLI	
		UUID	実装済み	CLI	
製品	カテゴリ	特徴/属性 使用容量	ステータス 実装済み	使用されるプロトコル CLI	追加情報
	ボリュームマップ	LUN	実装済み	CLI	バックエンド LUN の名前
		プロトコルコントローラー	実装済み	CLI	
		ストレージポート	実装済み	CLI	
		タイプ	ギャップ	CLI	
	ボリュームマスク	イニシエータ	実装済み	CLI	
		プロトコルコントローラー	実装済み	CLI	
		ストレージポート	実装済み	CLI	
		タイプ	ギャップ	CLI	
	ボリュームメンバー	容量	実装済み	CLI	スナップショット使用容量（MB）
		Name	実装済み	CLI	
		順位	実装済み	CLI	
		合計物理容量	実装済み	CLI	総生容量（アレイ上のすべてのディスクの合計）
		冗長性	実装済み	CLI	冗長レベル
		ストレージプールID	実装済み	CLI	
		使用容量	実装済み	CLI	
	WWNエイリアス	ホストエイリアス	実装済み	CLI	
		IP	実装済み	CLI	
		オブジェクト タイプ	実装済み	CLI	
		ソース	実装済み	CLI	
		WWN	実装済み	CLI	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					
808					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		読み取り使用率	実装済み	CLI	
		利用合計	実装済み	CLI	
製品	カテゴリ	特徴/属性 利用書き込み	ステータス 実装済み	使用されるプロトコル CLI	追加情報
	Volume	キャッシュヒット率読み取り	実装済み	CLI	
		キャッシュヒット率合計	実装済み	CLI	
		キャッシュヒット率書き込み	実装済み	CLI	
		物理容量	実装済み	CLI	
		総容量	実装済み	CLI	
		使用容量	実装済み	CLI	
		使用容量比率	実装済み	CLI	
		IOPS読み取り	実装済み	CLI	ディスク上の読み取りIOPS数
		IOP合計	実装済み	CLI	
		IOPS書き込み	実装済み	CLI	
		レイテンシ読み取り	実装済み	CLI	
		レイテンシ合計	実装済み	CLI	
		レイテンシ書き込み	実装済み	CLI	
		部分ブロック率	実装済み	CLI	
		スループット読み取り	実装済み	CLI	
		スループット合計	実装済み	CLI	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	CLI	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
ナビ CLI	CLI		6389,2162,2163,443(HTTPS)/80(HTTP)		true	true	true	false

EMC データドメイン (SSH)

このデータコレクターでサポートされてい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 • DD2500 • DD3300 • DD4200 • DD6300 • DD6400 • DD6800 • DD6900 • DD7200 • DD9300 • DD9400 • DD9410 • DD9500 • DD9800 • DD990 • DD9900 • DD9910	• 6.0.2.30-606339 • 6.1.2.051-633576 • 6.1.2.20-606786 • 6.2.1.30-663869 • 6.2.1.40-671977 • 6.2.1.60-686365 • 7.10.0.20-1023227 • 7.10.1.0-1042928 • 7.10.1.1-1049892 • 7.10.1.10-1068159 • 7.10.1.15-1078832 • 7.10.1.20-1090468 • 7.10.1.30-1105324 • 7.10.1.40-1126469 • 7.10.1.50-1146826 • 7.11.0.0-1035502 • 7.13.0.20-1082704 • 7.2.0.20-658029 • 7.2.0.60-682124 • 7.2.0.70-686759 • 7.2.0.90-692270 • 7.7.4.0-1017976 • 7.7.5.1-1040473 • 7.7.5.11-1046187 • 7.7.5.25-1078970 • 7.7.5.30-1091295 • 8.0.0.10-1097914 • 8.1.0.10-1127744

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		ト			ボリューム層に対してシンプロビジョニングをサポートしているかどうか
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		割り当て済み容量の合計	実装済み	SSH	
		総使用容量	実装済み	SSH	総容量（MB）
		タイプ	ギャップ	SSH	
		バーチャル	実装済み	SSH	これはストレージ仮想化デバイスですか?

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
データドメイン CLI	SSH	SSH	22		true	true	true	true

EMC ECS

このデータコレクターでサポートされてい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	3.6.1.3 3.6.2.1 3.7.0.0 3.7.0.3 3.7.0.4 3.7.0.6 3.8.0.1 3.8.0.2 3.8.0.3 3.8.0.4 3.8.0.5 3.8.0.6 3.8.1.1 3.8.1.2 3.8.1.3

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		ド容量使用率（MB）	実装済み	HTTPS	
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
	ストレージ プール	DWH容量に含める	実装済み	HTTPS	ACQからDWH容量に関心のあるストレージプールを制御する方法
		Name	実装済み	HTTPS	
		物理ディスク容量（MB）	実装済み	HTTPS	ストレージプールの生の容量として使用
		レイドグループ	実装済み	HTTPS	このストレージプールがRAIDグループであるかどうかを示します
		原材料と使用可能量の比率	実装済み	HTTPS	使用可能容量から生の容量に変換する比率
		ストレージプールID	実装済み	HTTPS	
		シンプロビジョニングをサポート	実装済み	HTTPS	この内部ボリュームがその上のボリューム層に対してシンプロビジョニングをサポートしているかどうか
		割り当て済み容量の合計	実装済み	HTTPS	
		総使用容量	実装済み	HTTPS	総容量（MB）
		タイプ	ギャップ	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					スクの読み取りと書き込み）（MB/秒）
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
	ストレージプールディスク	プロビジョニングされた容量	実装済み	HTTPS	
		物理容量	実装済み	HTTPS	
		総容量	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		オーバーコミット容量比率	実装済み	HTTPS	時系列で報告
		使用容量比率	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
EMC ECS REST API	HTTPS	HTTPS	443		true	true	true	true

Dell EMC IsilonとPowerScale Rest

このデータコレクターでサポートされてい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
• A100 • A200 • A2000 • A300 • A3000 • F200 • F600 • F800 • F900 • H400 • H500 • H5600 • H600 • H700 • NL410 • S210 • X210 • X410	• 9.1.0.10 • 9.1.0.6 • 9.1.0.9 • 9.2.1.10 • 9.2.1.11 • 9.2.1.12 • 9.2.1.13 • 9.2.1.19 • 9.2.1.4 • 9.2.1.9 • 9.4.0.11 • 9.4.0.13 • 9.4.0.14 • 9.4.0.15 • 9.4.0.16 • 9.4.0.17 • 9.4.0.18 • 9.5.0.3 • 9.5.0.5 • 9.5.0.6 • 9.5.0.7 • 9.5.0.8 • 9.5.1.0 • 9.5.1.1 • 9.5.1.2 • 9.7.1.0 • 9.7.1.2 • 9.7.1.3 • 9.7.1.4 • 9.7.1.5 • v8.0.0.4 • v8.0.0.6 • v8.0.0.7 • v8.1.0.4 • v8.1.2.0 • v9.0.0.0

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		Snapshot 使用済み容量	実装済み	HTTPS	
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
		集合ストレージプールID	実装済み	HTTPS	
		シンプロビジョニングをサポート	実装済み	HTTPS	この内部ボリュームがその上のボリューム層に対してシンプロビジョニングをサポートしているかどうか
		割り当て済み容量の合計	実装済み	HTTPS	
		総使用容量	実装済み	HTTPS	総容量（MB）
		タイプ	ギャップ	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					（MB/秒）
		スループット書き込み	実装済み	HTTPS	
製品	カテゴリ	特徴/属性 利用合計	ステータス 実装済み	使用されるプロトコル HTTPS	追加情報
	ストレージプールディスク	プロビジョニングされた容量	実装済み	HTTPS	
		物理容量	実装済み	HTTPS	
		総容量	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		オーバーコミット容量比率	実装済み	HTTPS	時系列で報告
		使用容量比率	実装済み	HTTPS	
		合計データ容量	実装済み	HTTPS	
		データ使用容量	実装済み	HTTPS	
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOP合計	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		その他の総容量	実装済み	HTTPS	
		その他の使用容量	実装済み	HTTPS	
		スナップショット予約容量	実装済み	HTTPS	
		Snapshot 使用済み容量	実装済み	HTTPS	
		スナップショット使用容量比率	実装済み	HTTPS	時系列で報告
		スループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	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		true	true	true	true

Dell EMC Isilon / PowerScale (CLI)

このデータコレクターでサポートされてい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 • H400 • H500 • NL400 • NL410 • S210 • X200 • X400 • X410	• 9.1.0.18 • 9.1.0.19 • 9.2.1.12 • 9.2.1.13 • 9.2.1.15 • 9.4.0.17 • 9.5.0.3 • 9.5.0.6 • 9.5.0.8 • 9.7.1.2 • 9.8.0.2 • 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

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					を説明するフリーテキスト
		UUID	実装済み	SSH	
製品	カテゴリ	特徴/属性 管理IPアドレス	ステータス 実装済み	使用されるプロトコル SSH	追加情報
	ストレージ プール	データ割り当て容量	ギャップ	SSH	データに割り当てられた容量
		データ使用容量	実装済み	SSH	
		DWH容量に含める	実装済み	SSH	ACQからDWH容量に関心のあるストレージプールを制御する方法
		Name	実装済み	SSH	
		物理ディスク容量（MB）	実装済み	SSH	ストレージプールの生の容量として使用
		レイドグループ	実装済み	SSH	このストレージプールがRAIDグループであるかどうかを示します
		原材料と使用可能量の比率	実装済み	SSH	使用可能容量から生の容量に変換する比率
		スナップショット割り当て容量	ギャップ	SSH	スナップショットの割り当て容量（MB）
		Snapshot 使用済み容量	実装済み	SSH	
		ストレージプールID	実装済み	SSH	
		シンプロビジョニングをサポート	実装済み	SSH	この内部ボリュームがその上のボリューム層に対してシンプロビジョニングをサポートしているかどうか
		割り当て済み容量の合計	実装済み	SSH	
		総使用容量	実装済み	SSH	総容量（MB）
		タイプ	ギャップ	SSH	
		バーチャル	実装済み	SSH	これはストレージ仮想化デバイスですか?

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					（MB/秒）
		スループット書き込み	実装済み	SSH	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		利用合計	実装済み	SSH	
	ストレージプールディスク	総容量	実装済み	SSH	
		使用容量比率	実装済み	SSH	
		合計データ容量	実装済み	SSH	
		プロビジョニングされた容量	実装済み	SSH	
		データ使用容量	実装済み	SSH	
		使用容量	実装済み	SSH	
		物理容量	実装済み	SSH	
		オーバーコミット容量比率	実装済み	SSH	時系列で報告
		Snapshot 使用済み容量	実装済み	SSH	
		スナップショット予約容量	実装済み	SSH	
		スナップショット使用容量比率	実装済み	SSH	時系列で報告

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
アイシロン SSH	SSH	SSH	22		true	false	true	true

EMC PowerStore REST

このデータコレクターでサポートされてい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 5200T • PowerStore 9000T • PowerStore 9200T	• 2.1.0.1 • 2.1.1.0 • 3.2.0.1 • 3.2.1.0 • 3.2.1.1 • 3.5.0.1 • 3.5.0.2 • 3.6.0.0 • 3.6.1.0 • 3.6.1.1 • 3.6.1.2 • 3.6.1.3 • 3.6.1.4 • 4.0.0.1 • 4.0.0.2 • 4.0.1.0

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		タイプ	ギャップ		
		バーチャル	実装済み		これはストレージ仮想化デバイスですか?
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
	Volume	容量	実装済み		スナップショット使用容量（MB）
		ジャンクションパス	実装済み		
		Name	実装済み		
		合計物理容量	実装済み		総生容量（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	実装済み		
		シンプロビジョニング	実装済み		
		タイプ	ギャップ		
		UUID	実装済み		
		使用容量	実装済み		
		QoS - ポリシー	実装済み		
	ボリュームマップ	LUN	実装済み		バックエンド LUN の名前
		マスクが必要	実装済み		
		プロトコルコントローラー	実装済み		
		ストレージポート	実装済み		
		タイプ	ギャップ		
	ボリュームマスク	イニシエータ	実装済み		
		プロトコルコントローラー	実装済み		
		タイプ	ギャップ		
	WWNエイリアス	ホストエイリアス	実装済み		
		オブジェクト タイプ	実装済み		
		ソース	実装済み		
		WWN	実装済み		

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					と書き込み）（MB/秒）
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
	Volume	物理容量	実装済み		
		総容量	実装済み		
		使用容量	実装済み		
		使用容量比率	実装済み		
		IOPS読み取り	実装済み		ディスク上の読み取りIOPS数
		IOP合計	実装済み		
		IOPS書き込み	実装済み		
		鍵	実装済み		
		レイテンシ読み取り	実装済み		
		レイテンシ合計	実装済み		
		レイテンシ書き込み	実装済み		
		サーバ ID	実装済み		
		スループット読み取り	実装済み		
		スループット合計	実装済み		平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み		

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
EMC PowerStore REST API	HTTPS	HTTPS	443		true	true	true	true

EMC RecoverPoint (HTTP)

このデータコレクターでサポートされてい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
リカバリポイント	5.1.SP4.P1(h.89) 5.1.SP4.P2(h.101) 5.1.SP4.P3(h.109) 5.1.SP4.P4(h.97) 5.1.SP4.P5(h.138)

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
876					

					合計）
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
	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）
		モデル	実装済み	HTTPS	
		Name	実装済み	HTTPS	
		プロセッサ数	実装済み	HTTPS	デバイスCPU
		シリアル番号	実装済み	HTTPS	
		州	実装済み	HTTPS	デバイスの状態を説明するフリーテキスト
		UUID	実装済み	HTTPS	
		version	実装済み	HTTPS	ソフトウェアバージョン
	ストレージ同期	モード	実装済み	HTTPS	
		モード列挙型	実装済み	HTTPS	
		ソースストレージ	実装済み	HTTPS	
		ソース ボリューム	実装済み	HTTPS	
		州	実装済み	HTTPS	デバイスの状態を説明するフリーテキスト
		状態列挙型	実装済み	HTTPS	
		ターゲットストレージ	実装済み	HTTPS	
		ターゲット ボリューム	実装済み	HTTPS	
		テクノロジ	実装済み	HTTPS	ストレージ効率の変化をもたらす技術

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
RecoverPoint REST API	HTTPS	HTTPS	443		true	true	true	true

EMC ScaleIO および PowerFlex REST

このデータコレクターでサポートされてい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
スケールIO	R3_5.1201.101 R3_6.1000.134

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		タイプ	ギャップ	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
	Volume	容量	実装済み	HTTPS	スナップショット使用容量（MB）
		ジャンクションパス	実装済み	HTTPS	
		Name	実装済み	HTTPS	
		合計物理容量	実装済み	HTTPS	総生容量（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	実装済み	HTTPS	
		シンプロビジョニング	実装済み	HTTPS	
		UUID	実装済み	HTTPS	
		ホストIP	実装済み	HTTPS	
パフォーマンス	ストレージ	失敗した生の容量	実装済み		
		物理容量	実装済み		
		予備の生の容量	実装済み		スペアディスクの生の容量（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	実装済み		
		IOPS読み取り	実装済み		ディスク上の読み取りIOPS数
		IOP合計	実装済み		
		IOPS書き込み	実装済み		
		鍵	実装済み		
		サーバ ID	実装済み		
		スループット読み取り	実装済み		
		スループット合計	実装済み		平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み		

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
EMC ScaleIO & PowerFlex REST API	HTTPS	HTTPS	443		true	true	true	true

EMC Symmetrix CLI

このデータコレクターでサポートされているモデルとバージョン:

API バージョン	モデル	ファームウェアバージョン
• V10.0.0.0 • V10.0.1.1 • V10.1.0.0 • V10.1.0.1 • V10.1.0.3 • V10.1.0.5 • V10.2.0.0 • V8.3.0.6 • V8.4.0.7 • V8.4.0.9 • V9.1.0.5 • V9.1.0.6 • V9.2.1.0 • V9.2.2.0 • V9.2.3.0 • V9.2.3.1 • V9.2.3.4 • V9.2.3.6 • V9.2.4.1 • V9.2.4.2 • V9.2.4.3 • V9.2.4.6 • V9.2.4.7 • V9.2.4.8	• PMax8000 • PowerMax_2000 • PowerMax_8000 • VMAX-1 • VMAX100K • VMAX10K • VMAX200K • VMAX250F • VMAX400K • VMAX40K • VMAX450F • VMAX850F • VMAX950F	• 5876.286.194(16F40000) build 115 • 5876.309.196(16F40000) build 153 • 5876.309.196(16F40000) build 162 • 5876.309.196(16F40000) build 94 • 5977.1151.1151（17590000）build 45 • 5977.1151.1151（17590000）build 60 • 5977.1151.1151（17590000）ビルド9 • 5978.711.711(175A0000) build 320 • 5978.711.711(175A0000) build 335 • 5978.711.711(175A0000) build 365 • 5978.711.711（175A0000）ビルド 416 • 5978.711.711(175A0000) build 436 • 5978.711.711(175A0000) build 438 • 5978.711.711(175A0000) build 448 • 5978.711.711(175A0000) build 484 • 5978.711.711(175A0000) build 542 • 5978.711.711(175A0000) build 581 • 5978.714.714(175A0000) build 1 • 5978.714.714(175A0000) build 101 • 5978.714.714(175A0000) build 108 • 5978.714.714(175A0000) build 117 5978.714.714（175A0000）ビルド137
		5978.714.714(175A0000) build

このデータコレクターでサポートされている製品:

- 145
- 5978.714.714（175A0000）ビルド34
- 5978.714.714(175A0000) build 49
- 5978.714.714(175A0000) build 53
- 5978.714.714(175A0000) build 79

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		トローラー			
		ストレージポート	実装済み		
製品	カテゴリ	特徴/属性タイプ	ステータスギャップ	使用されるプロトコル	追加情報
	ボリュームメンバー	自動階層化	実装済み		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	実装済み		スナップショット使用容量（MB）
		シリンダー	実装済み		
		Name	実装済み		
		順位	実装済み		
		合計物理容量	実装済み		総生容量（アレイ上のすべてのディスクの合計）
		冗長性	実装済み		冗長レベル
		ストレージプールID	実装済み		
		UUID	実装済み		
	ボリューム参照	Name	実装済み		
		ストレージIP	実装済み		
	WWNエイリアス	ホストエイリアス	実装済み		
		オブジェクト タイプ	実装済み		
		ソース	実装済み		
		WWN	実装済み		

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		スループット書き込み	実装済み		
製品	カテゴリ	書き込み保留中特徴/属性	実装ステータス	使用されるプロトコル	合計書き込み保留中追加情報
	Volume	キャッシュヒット率読み取り	実装済み		
		キャッシュヒット率合計	実装済み		
		キャッシュヒット率書き込み	実装済み		
		物理容量	実装済み		
		総容量	実装済み		
		使用容量	実装済み		
		書面による能力	実装済み		
		使用容量比率	実装済み		
		容量比率書き込み	実装済み		
		IOPS読み取り	実装済み		ディスク上の読み取りIOPS数
		IOP合計	実装済み		
		IOPS書き込み	実装済み		
		鍵	実装済み		
		レイテンシ読み取り	実装済み		
		レイテンシ合計	実装済み		
		レイテンシ書き込み	実装済み		
		サーバ ID	実装済み		
		スループット読み取り	実装済み		
		スループット合計	実装済み		平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み		
		書き込み保留中	実装済み		合計書き込み保留中

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
シンクリ	CLI		2707		true	true	true	true
Symmetrix SMI-S	SMI-S	HTTP / HTTPS	5988/5989		true	false	false	true

Dell ユニスフィア REST

このデータコレクターでサポートされているモデルとバージョン:

API バージョン	モデル	ファームウェアバージョン
• V10.0.0.5 • V10.0.1.5 • V10.1.0.1 • V10.1.0.5 • V10.1.0.6 • V10.1.0.8 • V10.2.0.1 • V10.2.0.2 • V9.2.3.15 • V9.2.3.20 • V9.2.3.22 • V9.2.3.4 • V9.2.4.1 • V9.2.4.10 • V9.2.4.11 • V9.2.4.12 • V9.2.4.3 • V9.2.4.6 • V9.2.4.7 • V9.2.4.9	• PowerMax_2000 • PowerMax_2500 • PowerMax_8000 • PowerMax_8500 • VMAX200K • VMAX250F • VMAX400K • VMAX450F • VMAX950F	• 5977.1131.1131 build 615 • 5977.1151.1151 build 60 build 60 • 5978.711.711 build 205 • 5978.711.711 build 335 build 335 • 5978.711.711 build 365 • 5978.711.711 build 416 • 5978.711.711 build 436 build 436 • 5978.711.711 build 438 • 5978.711.711 build 448 • 5978.711.711 build 471 • 5978.711.711 build 484 • 5978.711.711 build 484 build 484 • 5978.711.711 build 542 • 5978.711.711 build 542 build 542 • 5978.711.711 build 581 • 5978.711.711 build 75 • 5978.711.711 build 8 build 8 • 5978.714.711 build 49 • 5978.714.714 build 1 build 1 • 5978.714.714 build 101 build 101 • 5978.714.714 build 108 • 5978.714.714 build 117 • 5978.714.714 build 117 build 117 • 5978.714.714 build 131 build 131 • 5978.714.714 build 137 • 5978.714.714 build 137 build 137 • 5978.714.714 build 145 • 5978.714.714 ビルド149 ビルド149 • 5978.714.714 build 34 5978.714.714 build 49 5978.714.714 build 49 build 49

このデータコレクターでサポートされている製品:

-
- 5978.714.714 build 79
- 5978.714.714 build 79 build 79
- 6079.175.0 build 161 build 161
- 6079.175.0 ビルド 259 ビルド 259
- 6079.225.0 build 127 build 127
- 6079.225.0 build 216 build 216
- 6079.225.0 build 218 build 218
- 6079.225.0 build 291 build 291
- 6079.225.0 build 331 build 331
- 6079.225.0 build 86 build 86
- 6079.275.0 build 221 build 221

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
908					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		トローラー			
		ストレージポート	実装済み	HTTPS	
製品	カテゴリ	特徴/属性タイプ	ステータスギャップ	使用されるプロトコル	追加情報
	WWNエイリアス	ホストエイリアス	実装済み	HTTPS	
		オブジェクト タイプ	実装済み	HTTPS	
		ソース	実装済み	HTTPS	
		WWN	実装済み	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					と書き込み）（MB/秒）
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
		スループット書き込み	実装済み	HTTPS	
	Volume	鍵	実装済み	HTTPS	
		サーバ ID	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット書き込み	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		レイテンシ読み取り	実装済み	HTTPS	
		レイテンシ書き込み	実装済み	HTTPS	
		レイテンシ合計	実装済み	HTTPS	
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOPS書き込み	実装済み	HTTPS	
		IOP合計	実装済み	HTTPS	
		総容量	実装済み	HTTPS	
		物理容量	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		使用容量比率	実装済み	HTTPS	
		総圧縮節約	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
Dell Unisphere API	HTTPS	HTTPS	443		true	true	true	true

EMC VNX (SSH)

このデータコレクターでサポートされてい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 VNX5500 VNX5700	05.32.000.5.216 05.32.000.5.221 05.32.000.5.249 7.1.76-4 7.1.80-3

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
922					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		ト			
		プロトコルコントローラー	実装済み	SSH	
製品	カテゴリ	特徴/属性タイプ	ステータスギャップ	使用されるプロトコル	追加情報
	ボリュームマスク	ストレージポート	実装済み	SSH	
		イニシエータ	実装済み	SSH	
		プロトコルコントローラー	実装済み	SSH	
		タイプ	ギャップ	SSH	
	ボリュームメンバー	Name	実装済み	SSH	
		ストレージプールID	実装済み	SSH	
		順位	実装済み	SSH	
		容量	実装済み	SSH	スナップショット使用容量（MB）
		合計物理容量	実装済み	SSH	総生容量（アレイ上のすべてのディスクの合計）
		使用容量	実装済み	SSH	
		冗長性	実装済み	SSH	冗長レベル
	WWNエイリアス	ソース	実装済み	SSH	
		ホストエイリアス	実装済み	SSH	
		WWN	実装済み	SSH	
		オブジェクト タイプ	実装済み	SSH	
		IP	実装済み	SSH	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		プロビジョニングされた容量	実装済み	SSH	
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	時系列で報告
		コミット容量比率	実装済み	SSH	追加情報
	Volume	レイテンシ合計	実装済み	SSH	
		部分ブロック率	実装済み	SSH	
		レイテンシ読み取り	実装済み	SSH	
		IOPS書き込み	実装済み	SSH	
		スループット読み取り	実装済み	SSH	
		IOP合計	実装済み	SSH	
		レイテンシ書き込み	実装済み	SSH	
		IOPS読み取り	実装済み	SSH	ディスク上の読み取りIOPS数
		キャッシュヒット率読み取り	実装済み	SSH	
		キャッシュヒット率合計	実装済み	SSH	
		キャッシュヒット率書き込み	実装済み	SSH	
		スループット書き込み	実装済み	SSH	
		スループット合計	実装済み	SSH	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
VNX SSH と CLI	SSH	SSH	22		true	false	true	true

EMC VNXe と Unity Unisphere (CLI)

このデータコレクターでサポートされてい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 480 • Unity 480F • Unity 500 • Unity 550F • Unity 600F • Unity 650F • Unity 680F • Unity 880 • Unity 880F • UnityVSA • VNXe3200	• 3.1.17.10229825 • 4.1.2.9257522 • 5.0.6.0.5.008 • 5.0.8.0.5.007 • 5.1.2.0.5.007 • 5.2.1.0.5.013 • 5.2.2.0.5.004 • 5.3.0.0.5.120 • 5.3.1.0.5.008 • 5.3.1.0.6.028 • 5.4.0.0.5.094 • 5.4.1.0.5.006

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		シンプロビジョニング	実装済み	HTTPS	
		UUID	実装済み	HTTPS	
製品	カテゴリ	特徴/属性 使用容量	ステータス 実装済み	使用されるプロトコル HTTPS	追加情報
	ボリュームマップ	LUN	実装済み	HTTPS	バックエンド LUN の名前
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実装済み	HTTPS	
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					と書き込み）（MB/秒）
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
	Volume	スループット書き込み	実装済み	HTTPS	
		物理容量	実装済み	HTTPS	
		総容量	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		使用容量比率	実装済み	HTTPS	
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOP合計	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		レイテンシ合計	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
VNXe と Unisphere CLI	HTTPS	HTTPS	443		true	true	true	true

EMC VPLEX

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団	情報	データソース名	実装済み	HTTP/S	情報
		日付	実装済み	HTTP/S	
		発信者ID	実装済み	HTTP/S	
		発信者キー	実装済み	HTTP/S	
パフォーマンス	ストレージノードデータ	キャッシュヒット率合計	実装済み	SSH	
		鍵	実装済み	SSH	
		サーバ ID	実装済み	SSH	
		利用合計	実装済み	SSH	
	Volume	物理容量	実装済み	SSH	
		総容量	実装済み	SSH	
		IOP合計	実装済み	SSH	
		鍵	実装済み	SSH	
		レイテンシ読み取り	実装済み	SSH	
		レイテンシ合計	実装済み	SSH	
		レイテンシ書き込み	実装済み	SSH	
		サーバ ID	実装済み	SSH	
		スループット読み取り	実装済み	SSH	
		スループット合計	実装済み	SSH	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	SSH	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
EMC VPLEX CLI	SSH	SSH	22		true	true	true	true

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
EMC VPLEX API	HTTP / HTTPS	HTTP / HTTPS	80/443		true	true	true	true

EMC XtremIO (HTTP)

このデータコレクターでサポートされているモデルとバージョン:

API バージョン	モデル	ファームウェアバージョン
• 6.2.1 • 6.3.2 • 6.3.3 • 6.4.0 • 6.4.1 • 6.4.2	• 1 Bricks＆125TB • 1 Bricks＆24TB • 1 個のブリックと 31TB • 1 Bricks＆8TB • 1X10TB • 1X20TB • 1X40TB • 2 Bricks＆83TB • 3 Bricks ＆ 146TB • 3 Bricks＆251TB • 3 Bricks ＆ 283TB • 4 Bricks＆628TB • 4ブリック＆754TB • 4X20TB • 6X40TB	• 4.0.27-1 • 4.0.31-11 • 6.3.3-8_X2 • 6.4.0-36_hotfix_2_X2

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		ターゲット ボリューム	実装済み	HTTPS	
		テクノロジ	実装済み	HTTPS	ストレージ効率の有効化もたらす技術
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
	Volume	容量	実装済み	HTTPS	スナップショット使用容量（MB）
		ディスク サイズ	実装済み	HTTPS	ディスクサイズ（GB）のコンマ区切りリスト
		ディスク速度	実装済み	HTTPS	ディスク速度（rpm）のコンマ区切りリスト
		ディスクタイプ	利用不可	HTTPS	
		Name	実装済み	HTTPS	
		合計物理容量	実装済み	HTTPS	総生容量（アレイ上のすべてのディスクの合計）
		冗長性	実装済み	HTTPS	冗長レベル
		ストレージプールID	実装済み	HTTPS	
		シンプロビジョニング	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
		UUID	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?
	ボリュームマップ	LUN	実装済み	HTTPS	バックエンド LUN の名前
		プロトコルコントローラー	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実装済み	HTTPS	
		プロトコルコントローラー	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					と書き込み）（MB/秒）
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
	Volume	物理容量	実装済み	HTTPS	
		総容量	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		使用容量比率	実装済み	HTTPS	
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOP合計	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		鍵	実装済み	HTTPS	
		レイテンシ読み取り	実装済み	HTTPS	
		レイテンシ合計	実装済み	HTTPS	
		レイテンシ書き込み	実装済み	HTTPS	
		部分ブロック率	実装済み	HTTPS	
		サーバ ID	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
EMC XtremIO REST API	HTTPS	HTTPS	443		true	true	true	true

NetApp Eシリーズ

このデータコレクターでサポートされてい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
• 2660 • 2680 • 2702 • 2704 • 2800B • 2804 • 2806 • 3000 • 4000 • 5486 • 5488 • 5504 • 5564 • 5600 • 5700 • 5700B • 6000 • 7999	• 08.40.60.01 • 08.80.00.00 • 7.84.46.0 • 8.20.16.0 • 8.20.27.0 • 8.20.30.0 • 8.20.8.0 • 8.25.14.0 • 8.25.6.0 • 8.40.0.1 • 8.40.20.0 • 8.40.30.4 • 8.40.40.0 • 8.40.50.0 • 8.40.60.1 • 8.40.60.2 • 8.40.60.3 • 8.42.30.5 • 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 • 8.70.0.2 • 8.70.0.3 • 8.71.2.0 • 8.71.3.0 • 8.72.0.0 • 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ーでサポートされている製品:	• • 8.75.0.1 • 8.75.1.0 • 8.80.0.0 • 8.80.1.0 • 8.81.0.3 • 8.81.1.0 • 8.81.2.0 • 8.81.3.0 • 8.90.0.0

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
970					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		ト			ボリューム層に対してシンプロビジョニングをサポートしているかどうか
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		割り当て済み容量の合計	実装済み	RMI	
		総使用容量	実装済み	RMI	総容量（MB）
		タイプ	ギャップ	RMI	
		バーチャル	実装済み	RMI	これはストレージ仮想化デバイスですか?
	Volume	容量	実装済み	RMI	スナップショット使用容量（MB）
		ディスクタイプ	利用不可	RMI	
		Name	実装済み	RMI	
		合計物理容量	実装済み	RMI	総生容量（アレイ上のすべてのディスクの合計）
		冗長性	実装済み	RMI	冗長レベル
		ストレージプールID	実装済み	RMI	
		シンプロビジョニング	実装済み	RMI	
		タイプ	ギャップ	RMI	
		UUID	実装済み	RMI	
		使用容量	実装済み	RMI	
		バーチャル	実装済み	RMI	これはストレージ仮想化デバイスですか?
		書面による能力	実装済み	RMI	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）
	ボリュームマップ	LUN	実装済み	RMI	バックエンド LUN の名前
		ストレージポート	実装済み	RMI	
		タイプ	ギャップ	RMI	
	ボリュームマスク	イニシエータ	実装済み	RMI	
		ストレージポート	実装済み	RMI	
		タイプ	ギャップ	RMI	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					
976					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		読み取り使用率	実装済み	RMI	
		利用合計	実装済み	RMI	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		利用書き込み	実装済み	RMI	
	Volume	キャッシュヒット率読み取り	実装済み	RMI	
		キャッシュヒット率合計	実装済み	RMI	
		キャッシュヒット率書き込み	実装済み	RMI	
		物理容量	実装済み	RMI	
		総容量	実装済み	RMI	
		使用容量	実装済み	RMI	
		書面による能力	実装済み	RMI	
		使用容量比率	実装済み	RMI	
		容量比率書き込み	実装済み	RMI	
		IOPS読み取り	実装済み	RMI	ディスク上の読み取りIOPS数
		IOP合計	実装済み	RMI	
		IOPS書き込み	実装済み	RMI	
		レイテンシ読み取り	実装済み	RMI	
		レイテンシ合計	実装済み	RMI	
		レイテンシ書き込み	実装済み	RMI	
		スループット読み取り	実装済み	RMI	
		スループット合計	実装済み	RMI	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	RMI	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
SANtricity API	RMI	TCP			true	true	false	false

ピュアストレージ フラッシュブレード **REST**

このデータコレクターでサポートされてい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
フラッシュブレード フラッシュブレード//S200	純度//FB 4.1.5 純度//FB 4.3.0 純度//FB 4.3.11 純度//FB 4.3.6 純度//FB 4.4.3

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
982					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					サポートしているかどうか
製品	カテゴリ	割り当て済み容量の合計	実装済み	HTTPS	追加情報
		総使用容量	実装済み	HTTPS	総容量（MB）
		タイプ	ギャップ	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

		ト使用容量比率			
		圧縮によるスペース節約	実装済み	HTTPS	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		総圧縮節約	実装済み	HTTPS	
	ストレージ	失敗した生の容量	実装済み	HTTPS	
		物理容量	実装済み	HTTPS	
		予備の生の容量	実装済み	HTTPS	スペアディスクの生の容量（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	実装済み	HTTPS	
		IOPsその他	実装済み	HTTPS	
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOP合計	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		鍵	実装済み	HTTPS	
		レイテンシ読み取り	実装済み	HTTPS	
		レイテンシ合計	実装済み	HTTPS	
		レイテンシ書き込み	実装済み	HTTPS	
		サーバ ID	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
ピュアストレージフラッシュブレード API	HTTPS	HTTPS	443		true	true	true	true

Google Cloud コンピューティング

このデータコレクターでサポートされているモデルとバージョン: API バージョン:

- v1

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
992					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		メーカー	実装済み	HTTPS	
		Name	実装済み	HTTPS	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		OID	実装済み	HTTPS	
	情報	APIの説明	実装済み	HTTPS	
		API名	実装済み	HTTPS	
		APIバージョン	実装済み	HTTPS	
		データソース名	実装済み	HTTPS	情報
		日付	実装済み	HTTPS	
		発信者ID	実装済み	HTTPS	
		発信者キー	実装済み	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス	vm	総容量	実装済み	HTTPS	
		使用容量比率	実装済み	HTTPS	
		合計CPU使用率	実装済み	HTTPS	
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		ディスクIops合計	実装済み	HTTPS	
		ディスクIOPS書き込み	実装済み	HTTPS	
		レイテンシ合計	実装済み	HTTPS	
		ディスクスループット読み取り	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	ディスクスループット合計読み取り
		ディスクスループット書き込み	実装済み	HTTPS	
		IPスループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	IPスループット合計
		ipThroughput.write	実装済み	HTTPS	
		合計メモリ使用率	実装済み	HTTPS	
		スワップレート.inRate	実装済み	HTTPS	
		スワップレート	実装済み	HTTPS	
		トータルスワップレート	実装済み	HTTPS	
		待ち時間をスケジュールする	実装済み	HTTPS	スケジュール待ち時間（パーセント）
	VM	総容量	実装済み	HTTPS	
		使用容量比率	実装済み	HTTPS	
		鍵	実装済み	HTTPS	
		サーバ ID	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
Google コンピューティングプラットフォーム REST API	HTTPS		443		true	true	true	true

HDS HCP (HTTPS)

このデータコレクターでサポートされてい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
日立コンテンツプラットフォーム	9.6.2.37 9.6.3.33 9.7.2.27 9.7.3.14

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					ジ仮想化デバイスですか?
製品	ストレージ ノード カテゴリ	Name 特徴/属性 UUID	実装済み ステータス 実装済み	HTTPS 使用されるプロトコル HTTPS	追加情報
	ストレージ プール	DWH容量に含める	実装済み	HTTPS	ACQからDWH容量に関心のあるストレージプールを制御する方法
		Name	実装済み	HTTPS	
		物理ディスク容量（MB）	実装済み	HTTPS	ストレージプールの生の容量として使用
		レイドグループ	実装済み	HTTPS	このストレージプールがRAIDグループであるかどうかを示します
		原材料と使用可能量の比率	実装済み	HTTPS	使用可能容量から生の容量に変換する比率
		ソフト制限（MB）	実装済み	HTTPS	ボリュームの作成またはサイズ変更操作中に定義される論理ボリュームのサイズ
		ストレージプールID	実装済み	HTTPS	
		シンプロビジョニングをサポート	実装済み	HTTPS	この内部ボリュームがその上のボリューム層に対してシンプロビジョニングをサポートしているかどうか
		割り当て済み容量の合計	実装済み	HTTPS	
		総使用容量	実装済み	HTTPS	総容量（MB）
		タイプ	ギャップ	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス	ストレージ	失敗した生の容量	実装済み		
		物理容量	実装済み		
		予備の生の容量	実装済み		スペアディスクの生の容量（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	実装済み		
		鍵	実装済み		
		サーバ ID	実装済み		
	ストレージノードデータ	鍵	実装済み		
		サーバ ID	実装済み		
		スループット読み取り	実装済み		
		スループット合計	実装済み		平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み		
		利用合計	実装済み		

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
HDS HCP REST API	HTTPS	HTTPS	9090		true	true	true	true

HiCommand デバイス マネージャー

このデータコレクターでサポートされているモデルとバージョン:

API バージョン	モデル	ファームウェアバージョン
• 7.6.1 • 8.0 • 8.7.1 • 8.7.3 • 8.7.6 • 8.8.3	• DF850MH • DF850S • HM800 • HM850 • P9500 • RAID800 • VSP5000 • XP24000 • XP8	• 0983/A-H • 0984/B-H • 0985/B-S • 0986/A-H • 0988/H-S • DKC:60-08-22 • DKC：60-08-65 • DKC：70-06-43 • DKC:80-06-80-00/02 • DKC:80-06-91-00/00 • DKC:80-06-96-00/00 • DKC:83-05-46-60/00 • DKC:83-05-50-60/00 • DKC:83-05-53-60/00 • DKC:88-08-08-60/00 • DKC:88-08-10-60/00 • DKC:88-08-12-60/00 • DKC:88-08-13-60/00 • DKC:88-08-13-60/01 • DKC:90-08-81-00/00 • DKC:90-09-21-00/00 • DKC:90-09-23-00/00 • DKC:90-09-24-00/00 • DKC:90-09-24-00/01 • DKC：90-09-25 • SVP：60-08-21/00 • SVP:60-08-54/00 • SVP：70-06-30/00 • SVP:80-06-76/02 • SVP:80-06-86/00 • SVP:80-06-91/00 • SVP：83-05-50-60/00 • SVP：83-05-54-60/00 • SVP：83-05-57-60/00 • SVP：88-08-10-60/00 SVP：88-08-12-60/00 SVP:88-08-14-60/00 SVP：88-08-15-60/00

このデータコレクターでサポートされている製品:

-
- SVP:90-08-81/00
- SVP:90-09-21/00
- SVP：90-09-23/00
- SVP：90-09-24/00
- SVP:90-09-25/00

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
1004					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		シンプロビジョニング	実装済み	HDS XML API	
		タイプ	ギャップ	HDS XML API	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		使用容量	実装済み	HDS XML API	
	ボリュームマップ	LUN	実装済み	HDS XML API	バックエンド LUN の名前
		マスクが必要	実装済み	HDS XML API	
		プロトコルコントローラー	実装済み	HDS XML API	
		ストレージポート	実装済み	HDS XML API	
	ボリュームマスク	イニシエータ	実装済み	HDS XML API	
		プロトコルコントローラー	実装済み	HDS XML API	
		ストレージポート	実装済み	HDS XML API	
	ボリュームメンバー	容量	実装済み	HDS XML API	スナップショット使用容量（MB）
		シリンダー	実装済み	HDS XML API	
		Name	実装済み	HDS XML API	
		順位	実装済み	HDS XML API	
		合計物理容量	実装済み	HDS XML API	総生容量（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	実装済み	HDS XML API	
		使用容量	実装済み	HDS XML API	
	WWNエイリアス	ホストエイリアス	実装済み	HDS XML API	
		オブジェクト タイプ	実装済み	HDS XML API	
		ソース	実装済み	HDS XML API	
		WWN	実装済み	HDS XML API	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		使用容量	実装済み	エクスポート/CLI	
製品	カテゴリ	使用容量比率 特徴/属性	実装済み 実装ステータス	エクスポート/CLI 使用されるプロトコル	追加情報
	Volume	鍵	実装済み	エクスポート/CLI	
		サーバ ID	実装済み	エクスポート/CLI	
		総容量	実装済み	エクスポート/CLI	
		物理容量	実装済み	エクスポート/CLI	
		使用容量	実装済み	エクスポート/CLI	
		使用容量比率	実装済み	エクスポート/CLI	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	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				false	false	false	false
HiCommand デバイス マネージャー XML API	HDS XML API	HTTP / HTTPS	2001		true	true	true	true

日立オプスセンター

このデータコレクターでサポートされてい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 5600 • VSP 5600H • VSP E1090 • VSP E590 • VSP E790 • VSP E790H • VSP F1500 • VSP F400 • VSP F900 • VSP G1000 • VSP G1500 • VSP G600 • VSP G800 • VSP G900 • XP8	• 80-06-91-00/00:01-71-03/02 • 80-06-94-00/00:01-70-03/04 • 80-06-96-00/00:01-71-03/02 • 80-06-96-00/00:01-76-03/03 • 83-05-49-40/01:01-69-03/02 • 83-05-49-60/01:01-65-03/05 • 83-05-49-60/01:01-69-03/02 • 83-05-51-40/00:01-70-03/04 • 83-05-51-40/00:01-71-03/02 • 83-05-51-40/00:01-76-03/03 • 88-08-08-60/00:01-65-03/05 • 88-08-08-60/00:01-70-03/04 • 88-08-11-60/00:01-65-03/05 • 88-08-11-60/00:01-70-03/04 • 88-08-13-60/00:01-65-03/05 • 88-08-13-60/01:01-65-03/05 • 88-08-13-60/01:01-70-03/04 • 88-08-13-60/01:01-71-03/02 • 88-08-13-60/01:01-76-03/03 • 90-08-82-00/00:01-65-03/05 • 90-08-82：01.70.04 • 90-09-01-00/01:01-65-03/05 • 90-09-22-00/00:01-65-03/05 • 90-09-22-00/00:01-70-03/04 • 90-09-22-00/00:01-71-03/02 • 90-09-24-00/01:01-65-03/05 • 90-09-24-00/01:01-71-03/02 • 90-09-24-00/01:01-76-03/03 • 90-09-24：01.65.05 • 90-09-25-00/00:01-76-03/03 • 90-09-25：01.70.04 • 90-09-26-00/00:01-65-03/05 • 90-09-26-00/00:01-71-03/02 • 90-09-26-00/00:01-76-03/03 • 93-07-01-80/00:01-70-03/04 • 93-07-22-40/00:01-65-03/05 93-07-22-40/00:01-69-03/02 93-07-22-80/00:01-70-03/04

このデータコレクターでサポートされている製品:	• • 93-07-22-80/00:01-71-03/02 • 93-07-23-80/00:01-71-03/02 • 93-07-23-80/01:01-71-03/02 • 93-07-24-40/00:01-76-03/03 • 93-07-24-80/00:01-70-03/04 • null：null

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
1020					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		トローラー			
		ストレージポート	実装済み		
製品	カテゴリ	特徴/属性タイプ	ステータスギャップ	使用されるプロトコル	追加情報
	ボリュームマスク	イニシエータ	実装済み		
		プロトコルコントローラー	実装済み		
		ストレージポート	実装済み		
		タイプ	ギャップ		

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					
1026					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		スループット合計	実装済み		平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
	Volume	キャッシュヒット率読み取り	実装済み		
		キャッシュヒット率合計	実装済み		
		IOPS読み取り	実装済み		ディスク上の読み取りIOPS数
		IOP合計	実装済み		
		IOPS書き込み	実装済み		
		鍵	実装済み		
		レイテンシ読み取り	実装済み		
		レイテンシ合計	実装済み		
		レイテンシ書き込み	実装済み		
		サーバ ID	実装済み		
		スループット読み取り	実装済み		
		スループット合計	実装済み		平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み		

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
日立オプスセンターREST API	HTTPS	HTTPS	443		true	true	true	true

HDS HNAS (CLI)

このデータコレクターでサポートされてい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
ファイル 34 G600 G800 HNAS 4060 HNAS 4080 HNAS 4100 N800	14.6.7520.04 14.7.7623.07 14.9.7916.07 15.1.8030.03 15.1.8030.05 15.2.8128.05 15.2.8128.07 15.2.8128.09 15.3.8224.02

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					ーテキスト
		UUID	実装済み	SSH	
		version	実装済み	SSH	
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
	ストレージ プール	データ使用容量	実装済み	SSH	
		重複排除が有効	実装済み	SSH	ストレージプールで重複排除が有効になっていますか
		DWH容量に含める	実装済み	SSH	ACQからDWH容量に関心のあるストレージプールを制御する方法
		Name	実装済み	SSH	
		レイドグループ	実装済み	SSH	このストレージプールがRAIDグループであるかどうかを示します
		原材料と使用可能量の比率	実装済み	SSH	使用可能容量から生の容量に変換する比率
		Snapshot 使用済み容量	実装済み	SSH	
		ストレージプールID	実装済み	SSH	
		シンプロビジョニングをサポート	実装済み	SSH	この内部ボリュームがその上のボリューム層に対してシンプロビジョニングをサポートしているかどうか
		割り当て済み容量の合計	実装済み	SSH	
		総使用容量	実装済み	SSH	総容量（MB）
		タイプ	ギャップ	SSH	
		バーチャル	実装済み	SSH	これはストレージ仮想化デバイスですか?

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
HDS HNAS CLI	SSH	SSH	22		true	true	true	true

HPE Nimble / Alletra 6000 ストレージ

このデータコレクターでサポートされているモデルとバージョン:

API バージョン	モデル	ファームウェアバージョン
v1	5050 6070 AF1000 AF20Q AF40 AF60 AF80 CS1000 CS300 CS3000 CS500 HF20 HF20C HF20H HF40 HF60	5.0.8.0-677726-opt 5.2.1.1100-1027043-opt 5.2.1.400-796142-opt 5.2.1.700-882343-opt 5.2.1.800-930936-opt 6.0.0.400-991061-opt 6.0.0.500-1005932-opt 6.1.1.200-1020304-opt 6.1.1.300-1028597-opt 6.1.2.300-1042680-opt 6.1.2.400-1048557-opt 6.1.2.500-1053701-opt 6.1.2.502-1057650-opt 6.1.2.600-1064273-opt

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		トローラー			
		ストレージポート	実装済み	HTTPS	
製品	カテゴリ	特徴/属性タイプ	ステータスギャップ	使用されるプロトコル	追加情報
	ボリュームマスク	イニシエータ	実装済み	HTTPS	
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
	WWNエイリアス	ホストエイリアス	実装済み	HTTPS	
		オブジェクト タイプ	実装済み	HTTPS	
		ソース	実装済み	HTTPS	
		WWN	実装済み	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					
1048					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					と書き込み）（MB/秒）
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
		書き込み		HTTPS	
	ストレージプールディスク	IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOP合計	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	HTTPS	
	Volume	物理容量	実装済み	HTTPS	
		総容量	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		使用容量比率	実装済み	HTTPS	
		総圧縮節約	実装済み	HTTPS	
		圧縮によるスペース節約	実装済み	HTTPS	
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOP合計	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		レイテンシ読み取り	実装済み	HTTPS	
		レイテンシ合計	実装済み	HTTPS	
		レイテンシ書き込み	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
HP ニンブル REST API	HTTPS	HTTPS	5392		true	false	true	true

Huawei OceanStor（REST/HTTPS）

このデータコレクターでサポートされてい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
18800 V5 2600 V3 5310 V5 5500 V3 5500 V5 5800 V3 6800 V3 Dorado 18000 V6 NVMe Dorado 3000 V6 Dorado 5000 V3 Dorado 6000 V3 Dorado 6000 V6 NVMe	V300R001C01 V300R002C10 V300R006C10 V300R006C20 V300R006C50 V500R007C10 V500R007C30 V500R007C60 クンペン V500R007C61 V500R007C71 クンペン V600R003C00 V600R005C11 V600R005C26 V600R005C27

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
1052					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		タイプ	ギャップ	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
	Volume	容量	実装済み	HTTPS	スナップショット使用容量（MB）
		ジャンクションパス	実装済み	HTTPS	
		Name	実装済み	HTTPS	
		合計物理容量	実装済み	HTTPS	総生容量（アレイ上のすべてのディスクの合計）
		冗長性	実装済み	HTTPS	冗長レベル
		ストレージプールID	実装済み	HTTPS	
		シンプロビジョニング	実装済み	HTTPS	
		UUID	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?
	ボリュームマップ	LUN	実装済み	HTTPS	バックエンド LUN の名前
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実装済み	HTTPS	
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					と書き込み）（MB/秒）
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
		スループット書き込み	実装済み	HTTPS	
	Volume	キャッシュヒット率読み取り	実装済み	HTTPS	
		キャッシュヒット率合計	実装済み	HTTPS	
		キャッシュヒット率書き込み	実装済み	HTTPS	
		物理容量	実装済み	HTTPS	
		総容量	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		使用容量比率	実装済み	HTTPS	
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOP合計	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		鍵	実装済み	HTTPS	
		レイテンシ読み取り	実装済み	HTTPS	
		レイテンシ合計	実装済み	HTTPS	
		レイテンシ書き込み	実装済み	HTTPS	
		サーバ ID	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
Huawei OceanStor REST API	HTTPS	HTTPS	8088		true	true	true	true

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	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		true	false	true	true

IBM クレバーセーフ

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		UUID	実装済み	HTTPS	
		version	実装済み	HTTPS	ソフトウェアバージョン
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		管理IPアドレス	実装済み	HTTPS	
	ストレージ プール	DWH容量に含める	実装済み	HTTPS	ACQからDWH容量に関心のあるストレージプールを制御する方法
		Name	実装済み	HTTPS	
		物理ディスク容量（MB）	実装済み	HTTPS	ストレージプールの生の容量として使用
		レイドグループ	実装済み	HTTPS	このストレージプールがRAIDグループであるかどうかを示します
		原材料と使用可能量の比率	実装済み	HTTPS	使用可能容量から生の容量に変換する比率
		ストレージプールID	実装済み	HTTPS	
		シンプロビジョニングをサポート	実装済み	HTTPS	この内部ボリュームがその上のボリューム層に対してシンプロビジョニングをサポートしているかどうか
		割り当て済み容量の合計	実装済み	HTTPS	
		総使用容量	実装済み	HTTPS	総容量（MB）
		タイプ	ギャップ	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
IBM クレバーセーフ REST API	HTTPS	HTTPS	443		true	true	true	true

IBM DS 8K (DSCLI)

このデータコレクターでサポートされてい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 2107-993 2107-994 2107-996 2107-A05	7.10.1.8 7.6.31.4250 7.7.51.1400 7.9.32.101 7.9.33.132 7.9.33.95 7.9.40.251 7.9.41.65

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
1074					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		タイプ	ギャップ	DSNI	
		バーチャル	実装済み	DSNI	これはストレージ仮想化デバイスですか?
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
	Volume	容量	実装済み	DSNI	スナップショット使用容量（MB）
		ディスクタイプ	利用不可	DSNI	
		ジャンクションパス	実装済み	DSNI	
		Name	実装済み	手動入力	
		合計物理容量	実装済み	DSNI	総生容量（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	実装済み	DSNI	
		シンプロビジョニング	実装済み	DSNI	
		タイプ	ギャップ	DSNI	
		使用容量	実装済み	DSNI	
	ボリュームマップ	LUN	実装済み	DSNI	バックエンド LUN の名前
		プロトコルコントローラー	実装済み	DSNI	
		ストレージポート	実装済み	DSNI	
	ボリュームマスク	イニシエータ	実装済み	DSNI	
		プロトコルコントローラー	実装済み	DSNI	
		ストレージポート	実装済み	DSNI	
	WWNエイリアス	ホストエイリアス	実装済み	DSNI	
		ホスト OS	実装済み	DSNI	
		オブジェクト タイプ	実装済み	DSNI	
		ソース	実装済み	DSNI	
		WWN	実装済み	DSNI	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					
1078					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		物理容量	実装済み	DSNI	
		使用容量	実装済み	DSNI	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		使用容量比率	実装済み	DSNI	
	Volume	キャッシュヒット率読み取り	実装済み	DSNI	
		キャッシュヒット率合計	実装済み	DSNI	
		キャッシュヒット率書き込み	実装済み	DSNI	
		物理容量	実装済み	DSNI	
		総容量	実装済み	DSNI	
		使用容量	実装済み	DSNI	
		使用容量比率	実装済み	DSNI	
		IOPS読み取り	実装済み	DSNI	ディスク上の読み取りIOPS数
		IOP合計	実装済み	DSNI	
		IOPS書き込み	実装済み	DSNI	
		鍵	実装済み	DSNI	
		レイテンシ読み取り	実装済み	DSNI	
		レイテンシ合計	実装済み	DSNI	
		レイテンシ書き込み	実装済み	DSNI	
		サーバ ID	実装済み	DSNI	
		スループット読み取り	実装済み	DSNI	
		スループット合計	実装済み	DSNI	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	DSNI	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	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構成	手動入力				true	true	true	true
IBM DS CLI	DSNI	DSNI			true	true	true	true

IBM PowerVM (SSH)

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
1084					

		Name	実装済み	SSH	
		OID	実装済み	SSH	
製品	カテゴリ	特徴/属性タイプ	ステータスギャップ	使用されるプロトコル	追加情報
	仮想マシン	DNS名	実装済み	SSH	
		ゲスト州	実装済み	SSH	
		ホスト OID	実装済み	SSH	
		IPアドレス	実装済み	SSH	
		モイド	実装済み	SSH	
		メモリ	実装済み	SSH	
		Name	実装済み	SSH	
		OID	実装済み	SSH	
		OS	実装済み	SSH	
		電源状態	実装済み	SSH	
		状態変化時間	実装済み	SSH	
		プロセッサ	実装済み	SSH	
	仮想マシンディスク	OID	実装済み	SSH	
		仮想ディスクOID	実装済み	SSH	
		仮想マシンOID	実装済み	SSH	
	ホスト	ホストCPU数	実装済み	SSH	
		ホストにインストールされているメモリ	実装済み	SSH	
		ホストモデル	実装済み	SSH	
		NICの数	実装済み	SSH	
		IPアドレス	実装済み	SSH	
		メーカー	実装済み	SSH	
		Name	実装済み	SSH	
		OID	実装済み	SSH	
		プラットフォーム タイプ	実装済み	SSH	
	情報	データソース名	実装済み	SSH	情報
		日付	実装済み	SSH	
		発信者ID	実装済み	SSH	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
IBM ハードウェア管理コンソール SSH アクセス	SSH	SSH	22		true	false	true	true

IBM SVC (CLI)

このデータコレクターでサポートされてい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 • 2072-12G • 2072-224 • 2072-24C • 2072-24E • 2072-24F • 2072-24G • 2072-2N4 • 2072-324 • 2072-3H4 • 2072-3N2 • 2072-3N4 • 2072-92F • 2072-92G • 2076-124 • 2076-12F • 2076-224 • 2076-24F • 2076-24G • 2076-524 • 2076-624 • 2076-724 • 2076-824 • 2076-AF6 • 2076-AFF • 2077-24F • 2077-24G • 2077-424 • 2077-4H4 • 2078-12F • 2078-12G • 2078-224 • 2078-24C • 2078-24F • 2078-24G • 2078-324 2078-424 2078-4H4	• 1.5.2.7 • 1.6.1.2 • 1.6.1.4 • 1.6.1.5 • 7.7.1.8 • 7.8.1.11 • 7.8.1.12 • 7.8.1.13 • 7.8.1.14 • 7.8.1.16 • 7.8.1.5 • 7.8.1.6 • 7.8.1.7 • 7.8.1.8 • 8.2.1.10 • 8.2.1.8 • 8.2.1.9 • 8.3.1.10 • 8.3.1.2 • 8.3.1.5 • 8.3.1.6 • 8.3.1.7 • 8.3.1.8 • 8.3.1.9 • 8.4.0.10 • 8.4.0.11 • 8.4.0.13 • 8.4.0.15 • 8.4.0.2 • 8.4.0.5 • 8.4.0.6 • 8.4.0.9 • 8.4.2.0 • 8.5.0.10 • 8.5.0.11 • 8.5.0.12 8.5.0.13 8.5.0.14

このデータコレクターでサポートされている製品:

- 2078-92G
- 2078-AF3
- 4657-24G
- 4657-924
- 4662-12G
- 4662-24G
- 4662-6H2
- 4666-AH8
- 4666-UH8
- 4680-24H
- 4680-2P4
- 4680-3P4
- 4680-92H
- 4983-AH8
- 9843-AE2
- 9843-AE3
- 9846-AG8
- 9848-AF7
- 9848-AF8
- 9848-AG8
- 9848-UG8
- SVC

- 8.5.0.5
- 8.5.0.6
- 8.5.0.7
- 8.5.0.8
- 8.5.0.9
- 8.6.0.0
- 8.6.0.2
- 8.6.0.3
- 8.6.0.4
- 8.6.0.5
- 8.7.0.0
- 8.7.0.1
- 8.7.0.2
- 8.7.0.3

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
1090					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					に書き込まれた合計容量（MB）
		圧縮が有効	実装済み	SSH	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		暗号化	実装済み	SSH	
	ボリュームマップ	LUN	実装済み	SSH	バックエンド LUN の名前
		プロトコルコントローラー	実装済み	SSH	
		ストレージポート	実装済み	SSH	
	ボリュームマスク	イニシエータ	実装済み	SSH	
		プロトコルコントローラー	実装済み	SSH	
		ストレージポート	実装済み	SSH	
		タイプ	ギャップ	SSH	
	WWNエイリアス	ホストエイリアス	実装済み	SSH	
		オブジェクト タイプ	実装済み	SSH	
		ソース	実装済み	SSH	
		WWN	実装済み	SSH	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		読み取り使用率	実装済み	SSH	
		利用合計	実装済み	SSH	
製品	カテゴリ	特徴/属性 利用書き込み	ステータス 実装済み	使用されるプロトコル SSH	追加情報
	Volume	キャッシュヒット率読み取り	実装済み	SSH	
		キャッシュヒット率合計	実装済み	SSH	
		キャッシュヒット率書き込み	実装済み	SSH	
		物理容量	実装済み	SSH	
		総容量	実装済み	SSH	
		使用容量	実装済み	SSH	
		書面による能力	実装済み	SSH	
		使用容量比率	実装済み	SSH	
		容量比率書き込み	実装済み	SSH	
		IOPS読み取り	実装済み	SSH	ディスク上の読み取りIOPS数
		IOP合計	実装済み	SSH	
		IOPS書き込み	実装済み	SSH	
		レイテンシ読み取り	実装済み	SSH	
		レイテンシ合計	実装済み	SSH	
		レイテンシ書き込み	実装済み	SSH	
		スループット読み取り	実装済み	SSH	
		スループット合計	実装済み	SSH	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	SSH	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
IBM SVC CLI	SSH	SSH	22		true	false	true	true

IBM XIV & A9000 (XIVCLI)

このデータコレクターでサポートされてい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
A14	10.2.4.e

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
1104					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		トローラー			
	ボリュームマスク	イニシエータ	実装済み	XIV CLI	
		ポートコントローラー	実装済み	XIV CLI	
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
	WWNエイリアス	ソース	実装済み	XIV CLI	
		ホストエイリアス	実装済み	XIV CLI	
		WWN	実装済み	XIV CLI	
		オブジェクト タイプ	実装済み	XIV CLI	
		ホスト OS	実装済み	XIV CLI	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
IBM DS CLI	DSNI	DSNI			true	true	true	true
IBM XIV CLI	XIV CLI	TCP	7778		true	false	true	false

インフィニダット インフィニボックス (HTTP)

このデータコレクターでサポートされてい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
F4303 F6230 F6240	6.0.20.40 6.0.31.0 7.1.14.0 7.1.15.0 7.3.20.90 8.1.0.280

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		トローラー			
		ストレージポート	実装済み	HTTPS	
製品	カテゴリ	特徴/属性タイプ	ステータスギャップ	使用されるプロトコル	追加情報
	WWNエイリアス	ホストエイリアス	実装済み	HTTPS	
		オブジェクト タイプ	実装済み	HTTPS	
		ソース	実装済み	HTTPS	
		WWN	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
インフィニダット REST API	HTTPS	HTTPS	443		true	true	true	true

Microsoft Azure コンピューティング

このデータコレクターでサポートされているモデルとバージョン: API バージョン:

- 2018/06/01

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		メーカー	実装済み	HTTPS	
		Name	実装済み	HTTPS	
製品	カテゴリ	特徴/属性 OID	ステータス 実装済み	使用されるプロトコル HTTPS	追加情報
	情報	APIの説明	実装済み	HTTPS	
		API名	実装済み	HTTPS	
		APIバージョン	実装済み	HTTPS	
		データソース名	実装済み	HTTPS	情報
		日付	実装済み	HTTPS	
		発信者ID	実装済み	HTTPS	
		発信者キー	実装済み	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					
1120					

		スループット合計	実装済み	HTTPS	IPスループット合計
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
		ipThroughput.write	実装済み	HTTPS	
	VM	総容量	実装済み	HTTPS	
		鍵	実装済み	HTTPS	
		サーバ ID	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
Microsoft Azure コンピューティング REST API	HTTPS	HTTPS	443		true	true	true	true

Microsoft Hyper-V

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
1122					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

	仮想マシンディスク	OID	実装済み	WMI	
		仮想ディスクOID	実装済み	WMI	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		仮想マシンOID	実装済み	WMI	
	ホスト	ホストCPU数	実装済み	WMI	
		ホストCPU速度	実装済み	WMI	
		ホストドメイン	実装済み	WMI	
		ホストにインストールされているメモリ	実装済み	WMI	
		ホストモデル	実装済み	WMI	
		NICの数	実装済み	WMI	
		NIC速度	実装済み	WMI	
		IPアドレス	実装済み	WMI	
		メーカー	実装済み	WMI	
		Name	実装済み	WMI	
		OID	実装済み	WMI	
		プラットフォーム タイプ	実装済み	WMI	
	ISCSI ノード	ホストエイリアス	実装済み	WMI	
		Node Name	実装済み	WMI	
		OID	実装済み	WMI	
		タイプ	ギャップ	WMI	
	情報	データソース名	実装済み	WMI	情報
		日付	実装済み	WMI	
		発信者ID	実装済み	WMI	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					
1126					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					と書き込み）（MB/秒）
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
	vm	総容量	実装済み	WS-マネジメント	
		使用容量	実装済み	WS-マネジメント	
		使用容量比率	実装済み	WS-マネジメント	
		合計CPU使用率	実装済み	WS-マネジメント	
		IOPS読み取り	実装済み	WS-マネジメント	ディスク上の読み取りIOPS数
		ディスクIops合計	実装済み	WS-マネジメント	
		ディスクIOPS書き込み	実装済み	WS-マネジメント	
		レイテンシ合計	実装済み	WS-マネジメント	
		ディスクスループット読み取り	実装済み	WS-マネジメント	
		スループット読み取り	実装済み	WS-マネジメント	ディスクスループット合計読み取り
		ディスクスループット書き込み	実装済み	WS-マネジメント	
		IPスループット読み取り	実装済み	WS-マネジメント	
		スループット合計	実装済み	WS-マネジメント	IPスループット合計
		ipThroughput.write	実装済み	WS-マネジメント	
	VM	総容量	実装済み	WS-マネジメント	
		使用容量	実装済み	WS-マネジメント	
		使用容量比率	実装済み	WS-マネジメント	
		鍵	実装済み	WS-マネジメント	
		サーバ ID	実装済み	WS-マネジメント	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
PowerShell	WS-マネジメント	HTTP	5985		true	false	false	true
WMI	WMI	WMI	135		true	false	true	true

NetApp 7 モード

このデータコレクターでサポートされているモデルとバージョン:

API バージョン	モデル	ファームウェアバージョン
1.12 1.17 1.19 1.20 1.21	FAS2040 FAS2220 FAS2240-4 FAS2520 FAS2552 FAS2554 FAS3140 FAS3160 FAS3250 FAS3270 FAS6240 FAS6250 FAS8020 FAS8040 FAS8060 N6070 N6240 N6270	8.1.1 7モード 8.1.4P9D18 7モード 8.2.2 7モード 8.2.3 7モード 8.2.3P2 7モード 8.2.3P3 7モード 8.2.4 7モード 8.2.4P4 7モード 8.2.4P5 7モード 8.2.4P6 7モード 8.2.5 7モード 8.2.5P3 7モード 8.2.5P4 7モード 8.2.5P5 7モード 8.2P3 7モード 8.2P4 7モードData ONTAPリリース 7.3.3 Data ONTAPリリース 8.2.5 7モードData ONTAPリリース 8.2.5P1 7モード

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
1132					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		シンプロビジョニング	実装済み		
		タイプ	ギャップ		
製品	カテゴリ	特徴/属性 使用容量	ステータス 実装済み	使用されるプロトコル	追加情報
	ボリュームマップ	LUN	実装済み		バックエンド LUN の名前
		プロトコルコントローラー	実装済み		
		タイプ	ギャップ		
	ボリュームマスク	イニシエータ	実装済み		
		プロトコルコントローラー	実装済み		
		ストレージポート	実装済み		
		タイプ	ギャップ		

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		読み取り使用率	実装済み		
		利用合計	実装済み		
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		利用書き込み	実装済み		
	Volume	物理容量	実装済み		
		総容量	実装済み		
		使用容量	実装済み		
		使用容量比率	実装済み		
		IO密度読み取り	実装済み		
		IO密度合計	実装済み		
		書き込みIO密度	実装済み		
		IOPS読み取り	実装済み		ディスク上の読み取りIOPS数
		IOP合計	実装済み		
		IOPS書き込み	実装済み		
		レイテンシ読み取り	実装済み		
		レイテンシ合計	実装済み		
		レイテンシ書き込み	実装済み		
		部分ブロック率	実装済み		
		スループット読み取り	実装済み		
		スループット合計	実装済み		平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み		
		書き込み保留中	実装済み		合計書き込み保留中

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
NetApp 7 モード ZAPI	ZAPI	ZAPI			true	true	true	true

NetApp Eシリーズ REST

このデータコレクターでサポートされてい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
2800B 2806 5700	08.71.03.00 08.73.00.00 08.74.02.00 08.75.00.00 08.75.00.01 08.80.00.00 08.81.00.03 08.81.02.00 08.81.03.00 08.90.00.00

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		ト			ボリューム層に対してシンプロビジョニングをサポートしているかどうか
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		割り当て済み容量の合計	実装済み	HTTPS	
		総使用容量	実装済み	HTTPS	総容量（MB）
		タイプ	ギャップ	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?
		暗号化	実装済み	HTTPS	
	Volume	容量	実装済み	HTTPS	スナップショット使用容量（MB）
		ディスクタイプ	利用不可	HTTPS	
		Name	実装済み	HTTPS	
		合計物理容量	実装済み	HTTPS	総生容量（アレイ上のすべてのディスクの合計）
		冗長性	実装済み	HTTPS	冗長レベル
		ストレージプールID	実装済み	HTTPS	
		シンプロビジョニング	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
		UUID	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?
		暗号化	実装済み	HTTPS	
	ボリュームマップ	LUN	実装済み	HTTPS	バックエンド LUN の名前
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス	ストレージ	キャッシュヒット率読み取り	実装済み	HTTPS	
		キャッシュヒット率合計	実装済み	HTTPS	
		キャッシュヒット率書き込み	実装済み	HTTPS	
		失敗した生の容量	実装済み	HTTPS	
		物理容量	実装済み	HTTPS	
		予備の生の容量	実装済み	HTTPS	スペアディスクの生の容量（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	実装済み	HTTPS	
		IOPsその他	実装済み	HTTPS	
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOP合計	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		鍵	実装済み	HTTPS	
		レイテンシ読み取り	実装済み	HTTPS	
		レイテンシ合計	実装済み	HTTPS	
		レイテンシ書き込み	実装済み	HTTPS	
		サーバ ID	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
NetApp E シリーズ REST API	HTTPS	HTTPS	443		true	true	true	true

Amazon FSx for NetApp ONTAP

このデータコレクターでサポートされてい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
ONTAP向け FSx	Data ONTAP

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

	レージプール IRef	ルID			
製品	仮想マシン/ボリューム参照	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
	Volume	容量	実装済み	HTTPS	
		ディスクグループ	実装済み	HTTPS	
		ジャンクションパス	実装済み	HTTPS	
		最終アクセス時刻	実装済み	HTTPS	
		Name	実装済み	HTTPS	
		qtree ID	実装済み	HTTPS	
		合計物理容量	実装済み	HTTPS	
		ストレージプールID	実装済み	HTTPS	
		シンプロビジョニング	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
		UUID	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		暗号化	実装済み	HTTPS	
	ボリュームマップ	LUN	実装済み	HTTPS	
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実装済み	HTTPS	
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					
1172					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					（MB/秒）
		スループット書き込み	実装済み	HTTPS	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		利用合計	実装済み	HTTPS	
	ストレージプールディスク	総容量	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		物理容量	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		IOP合計	実装済み	HTTPS	
		スナップショット使用容量比率	実装済み	HTTPS	時系列で報告
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		使用容量比率	実装済み	HTTPS	
		合計データ容量	実装済み	HTTPS	
		プロビジョニングされた容量	実装済み	HTTPS	
		データ使用容量	実装済み	HTTPS	
		リザーブ容量	実装済み	HTTPS	部分予約（データ割り当て容量に含まれる）
		スループット書き込み	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		オーバーコミット容量比率	実装済み	HTTPS	時系列で報告
		Snapshot 使用済み容量	実装済み	HTTPS	
		スナップショット予約容量	実装済み	HTTPS	
	仮想マシン	総容量	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		鍵	実装済み	HTTPS	
		サーバ ID	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
NetApp ONTAP API	HTTP / HTTPS	HTTP / HTTPS	80/443		true	true	true	true

NetAppクラスタ化Data ONTAP 8.1.1+

このデータコレクターでサポートされてい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-A1K • AFF-A20 • AFF-A200 • AFF-A220 • AFF-A250 • AFF-A300 • AFF-A320 • AFF-A400 • AFF-A70 • AFF-A700 • AFF-A700s • AFF-A800 • AFF-A90 • AFF-A900 • AFF-C190 • AFF-C250 • AFF-C400 • AFF-C60 • AFF-C80 • AFF-C800 • AFF8020 • AFF8040 • AFF8060 • AFF8080 • ASA-A250 • ASA-A400 • ASA-A800 • ASA-A900 • ASA-C250 • ASA-C400 • ASA-C800 • CDvM100 • CDvM200 • DM5000H • DM7100F FAS2240-2 FAS2520	• 8.2.3P4 • 8.2.3P5 • 8.3.1P2 • 8.3.2 • 8.3.2P12 • 8.3.2P5 • 9.0.0 • 9.1.0 • 9.1.0P1 • 9.1.0P11 • 9.1.0P15 • 9.1.0P17 • 9.1.0P19 • 9.1.0P2 • 9.1.0P20 • 9.1.0P3 • 9.1.0P6 • 9.1.0P7 • 9.1.0P8 • 9.1.0P9 • 9.10.0 • 9.10.1 • 9.10.1P1 • 9.10.1P10 • 9.10.1P11 • 9.10.1P12 • 9.10.1P13 • 9.10.1P14 • 9.10.1P15 • 9.10.1P16 • 9.10.1P17 • 9.10.1P18 • 9.10.1P19 • 9.10.1P2 • 9.10.1P20 • 9.10.1P3 9.10.1P4 9.10.1P5

このデータコレクターでサポートされている製品:

- FAS2552
- FAS2554
- FAS2620
- FAS2650
- FAS2720
- FAS2750
- FAS2820
- FAS3220
- FAS3250
- FAS3270
- FAS500f
- FAS6210
- FAS8020
- FAS8040
- FAS8060
- FAS8080
- FAS8200
- FAS8300
- FAS8700
- FAS90
- FAS9000
- FAS9500
- FASDvM300
- SIMBOX

- 9.10.1P6
- 9.10.1P7
- 9.10.1P8
- 9.10.1P9
- 9.11.0P1
- 9.11.1
- 9.11.1P1
- 9.11.1P10
- 9.11.1P11
- 9.11.1P12
- 9.11.1P13
- 9.11.1P14
- 9.11.1P15
- 9.11.1P16
- 9.11.1P17
- 9.11.1P18
- 9.11.1P2
- 9.11.1P3
- 9.11.1P4
- 9.11.1P5
- 9.11.1P6
- 9.11.1P7
- 9.11.1P8
- 9.11.1P9
- 9.12.1
- 9.12.1P1
- 9.12.1P10
- 9.12.1P11
- 9.12.1P12
- 9.12.1P13
- 9.12.1P14
- 9.12.1P15
- 9.12.1P16
- 9.12.1P17
- 9.12.1P2
- 9.12.1P3

9.12.1P4

9.12.1P5

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団			• 9.12.1P7 • 9.12.1P8 • 9.12.1P9 • 9.13.0 • 9.13.0P1 • 9.13.0P3 • 9.13.1 • 9.13.1D1 • 9.13.1P1 • 9.13.1P10 • 9.13.1P11 • 9.13.1P12 • 9.13.1P13 • 9.13.1P14 • 9.13.1P2 • 9.13.1P3 • 9.13.1P4 • 9.13.1P5 • 9.13.1P6 • 9.13.1P7 • 9.13.1P8 • 9.13.1P9 • 9.14.0 • 9.14.0P1 • 9.14.0P2 • 9.14.1 • 9.14.1P1 • 9.14.1P10 • 9.14.1P11 • 9.14.1P2 • 9.14.1P4 • 9.14.1P5 • 9.14.1P6 • 9.14.1P7 • 9.14.1P8 9.14.1P8D5 9.14.1P9		
1180					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
			• 9.15.0P2 • 9.15.1 • 9.15.1P1 • 9.15.1P2 • 9.15.1P2D2 • 9.15.1P3 • 9.15.1P4 • 9.15.1P5 • 9.15.1P6 • 9.15.1P7 • 9.15.1P7D4 • 9.15.1P8 • 9.16.1 • 9.16.1P1 • 9.17.1 • 9.2.0P3 • 9.2.0P4 • 9.3.0P15 • 9.3.0P18 • 9.3.0P20 • 9.3.0P21 • 9.3.0P6 • 9.3.0P7 • 9.3.0P8 • 9.4.0 • 9.4.0P2 • 9.4.0P5 • 9.5.0 • 9.5.0P1 • 9.5.0P10 • 9.5.0P14 • 9.5.0P16 • 9.5.0P17 • 9.5.0P18 • 9.5.0P19 9.5.0P2 9.5.0P3		

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
			• 9.5.0P7 • 9.5.0P9 • 9.6.0 • 9.6.0P11 • 9.6.0P18 • 9.6.0P2 • 9.6.0P3 • 9.6.0P5 • 9.7.0 • 9.7.0P10 • 9.7.0P11 • 9.7.0P12 • 9.7.0P13 • 9.7.0P14 • 9.7.0P15 • 9.7.0P16 • 9.7.0P17 • 9.7.0P18 • 9.7.0P19 • 9.7.0P20 • 9.7.0P21 • 9.7.0P22 • 9.7.0P23 • 9.7.0P4 • 9.7.0P5 • 9.7.0P6 • 9.7.0P7 • 9.7.0P8 • 9.7.0P9 • 9.8.0 • 9.8.0P1 • 9.8.0P10 • 9.8.0P11 • 9.8.0P12 • 9.8.0P13 9.8.0P14 9.8.0P15		

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
			• 9.8.0P17 • 9.8.0P18 • 9.8.0P19 • 9.8.0P2 • 9.8.0P20 • 9.8.0P21 • 9.8.0P3 • 9.8.0P4 • 9.8.0P6 • 9.8.0P7 • 9.8.0P8 • 9.8.0P9 • 9.9.0 • 9.9.1 • 9.9.1P10 • 9.9.1P11 • 9.9.1P12 • 9.9.1P13 • 9.9.1P14 • 9.9.1P15 • 9.9.1P16 • 9.9.1P17 • 9.9.1P18 • 9.9.1P19 • 9.9.1P2 • 9.9.1P20 • 9.9.1P3 • 9.9.1P6 • 9.9.1P7 • 9.9.1P9		

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		QoS 制限 MBPS	実装済み	HTTPS	
		QoS 制限（生）	実装済み	HTTPS	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		QoS - ポリシー	実装済み	HTTPS	
	ボリュームマップ	LUN	実装済み	HTTPS	バックエンド LUN の名前
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実装済み	HTTPS	
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					
1198					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		使用容量	実装済み	HTTPS	
		鍵	実装済み	HTTPS	
製品	カテゴリ	特徴/属性 サーバ ID	ステータス 実装済み	使用されるプロトコル HTTPS	追加情報
	Volume	物理容量	実装済み	HTTPS	
		総容量	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		使用容量比率	実装済み	HTTPS	
		IO密度読み取り	実装済み	HTTPS	
		IO密度合計	実装済み	HTTPS	
		書き込みIO密度	実装済み	HTTPS	
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOP合計	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		レイテンシ読み取り	実装済み	HTTPS	
		レイテンシ合計	実装済み	HTTPS	
		レイテンシ書き込み	実装済み	HTTPS	
		部分ブロック率	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
NetApp ONTAP API	HTTP / HTTPS	HTTP / HTTPS	80/443		true	true	true	true

ASA

このデータコレクターでサポートされてい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
ASA-A1K ASA-A20 ASA-A90	NetAppリリース 9.16.1: 2025年1月18日(土) 19:31:15 UTC NetAppリリース 9.16.1RC1: 2024年11月4日(月) 10:39:46 UTC

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		トローラー			
		ストレージポート	実装済み	HTTPS	
製品	カテゴリ	特徴/属性タイプ	ステータスギャップ	使用されるプロトコル	追加情報
	ボリュームマスク	イニシエータ	実装済み	HTTPS	
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
パフォーマンス	ディスク	IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOP合計	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		鍵	実装済み	HTTPS	
		サーバ ID	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	HTTPS	
		読み取り使用率	実装済み	HTTPS	
		利用合計	実装済み	HTTPS	
		利用書き込み	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
NetApp ASA API	HTTPS	HTTPS	443		true	true	true	true

NetApp ONTAP REST

このデータコレクターでサポートされてい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-A220 • AFF-A250 • AFF-A300 • AFF-A400 • AFF-A70 • AFF-A700 • AFF-A700s • AFF-A800 • AFF-A90 • AFF-A900 • AFF-C190 • AFF-C250 • AFF-C400 • AFF-C800 • ASA-A250 • ASA-A400 • ASA-A800 • ASA-C250 • ASA-C800 • CDvM200 • FAS2720 • FAS2750 • FAS2820 • FAS8200 • FAS8300 • FAS8700 • FAS9000 • FAS9500 • FASDvM300 • SIMBOX	• NetAppリリース 9.14.1P10: 2024年11月28日(木) 12:32:16 UTC • NetAppリリース 9.14.1P11: 2025年1月22日(水) 11:55:28 UTC • NetAppリリース 9.14.1P1: 2024年2月15日(木) 00:45:21 UTC • NetAppリリース 9.14.1P4: 2024年4月18日(木) 15:59:10 UTC • NetAppリリース 9.14.1P5: 2024年5月18日(土) 19:42:16 UTC • NetAppリリース 9.14.1P6: 2024年6月18日火曜日 16:11:44 UTC • NetAppリリース 9.14.1P7: 2024年8月1日(木) 03:07:44 UTC • NetAppリリース 9.14.1P8: 2024年9月13日金曜日 07:12:27 UTC • NetAppリリース 9.14.1P9: 2024年10月21日月曜日 18:04:05 UTC • NetAppリリース 9.15.1: 2024年7月4日(木) 12:21:07 UTC • NetAppリリース 9.15.1P1: 2024年7月30日火曜日 05:15:49 UTC • NetAppリリース 9.15.1P2: 2024年8月27日火曜日 16:35:16 UTC • NetAppリリース 9.15.1P3: 2024年9月25日(水) 22:33:44 UTC • NetAppリリース 9.15.1P4: 2024年10月27日(日) 20:15:53 UTC • NetAppリリース 9.15.1P5: 2024年11月24日(日) 16:31:37 UTC • NetAppリリース 9.15.1P6: 2024年12月4日水曜日 01:42:39 UTC • NetAppリリース 9.15.1P7: 2025年1月18日(土) 21:34:02 UTC • NetAppリリース 9.15.1RC2: 2024年6月24日月曜日 04:49:55 UTC • NetAppリリース 9.16.1: 2025年1月18日(土) 19:31:15 UTC • NetAppリリース 9.16.1P1: 2025年2月14日金曜日 03:53:50 UTC • NetAppリリース 9.16.1RC1: 2024年11月4日月曜日 10:39:46 UTC • NetAppリリース Clawhammer__9.14.1: 2024 年 5 月 18 日土曜日 09:23:49 UTC

このデータコレクターでサポートされている製品:

-
- NetAppリリース Cloudstream__9.16.1: 2024年11月4日月曜日 05:51:46 UTC
- NetAppリリース Cloudstream__9.16.1: 2025 年 3 月 13 日木曜日 20:55:54 UTC
- NetAppリリース Electricjellyfish__9.17.1: 2025 年 3 月 3 日月曜日 05:57:49 UTC
- NetAppリリース Electricjellyfish__9.17.1: 2025 年 3 月 9 日(日) 05:56:14 UTC
- NetAppリリース Electricjellyfish__9.17.1: 日曜日 3月16日 04:54:53 UTC 2025
- NetAppリリース Electricjellyfish__9.17.1: 2025 年 1 月 28 日火曜日 11:48:14 UTC
- NetAppリリース Electricjellyfish__9.17.1: 2025 年 3 月 18 日火曜日 04:59:54 UTC
- NetAppリリース Electricjellyfish__9.17.1: 2025 年 3 月 12 日水曜日 04:42:03 UTC
- NetAppリリース Mightysquirrel__9.15.1: 2024年5月24日金曜日 05:03:10 UTC
- NetAppリリース Mightysquirrel__9.15.1: 2025年1月18日(土) 11:39:42 UTC
- NetAppリリース Tropicallightning__9.18.0: 2025年2月21日(金) 14:02:58 UTC
- NetAppリリース Tropicallightning__9.18.0: 2025 年 2 月 17 日月曜日 08:18:14 UTC
- NetAppリリース Tropicallightning__9.18.0: 2025 年 2 月 20 日(木) 08:11:55 UTC
- NetAppリリース Tropicallightning__9.18.0: 2025 年 2 月 27 日(木) 04:15:40 UTC
- NetAppリリース Tropicallightning__9.18.0: 2025 年 2 月 18 日火曜日 14:00:54 UTC
- NetAppリリース Tropicallightning__9.18.0: 2025 年 2 月 26 日水曜日 08:19:21 UTC
- NetAppリリース Tropicallightning__9.18.0: 2025 年 1 月 29 日水曜日 08:34:06 UTC

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		トローラー			
		ストレージポート	実装済み	HTTPS	
製品	カテゴリ	特徴/属性タイプ	ステータスギャップ	使用されるプロトコル	追加情報
	ボリュームマスク	イニシエータ	実装済み	HTTPS	
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					
1242					

		読み取り使用率	実装済み	HTTPS	
		利用合計	実装済み	HTTPS	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		利用書き込み	実装済み	HTTPS	
	ストレージ プール	プロビジョニングされた容量	実装済み	HTTPS	
		物理容量	実装済み	HTTPS	
		総容量	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		オーバーコミット容量比率	実装済み	HTTPS	時系列で報告
		使用容量比率	実装済み	HTTPS	
		圧縮節約率合計	実装済み	HTTPS	
		総圧縮スペース	実装済み	HTTPS	
		総圧縮節約	実装済み	HTTPS	
		圧縮によるスペース節約	実装済み	HTTPS	
		合計データ容量	実装済み	HTTPS	
		データ使用容量	実装済み	HTTPS	
		重複排除による節約率合計	実装済み	HTTPS	
		重複排除によるスペース節約	実装済み	HTTPS	
		故障したディスク	実装済み	HTTPS	
		鍵	実装済み	HTTPS	
		サーバ ID	実装済み	HTTPS	
		スナップショット予約容量	実装済み	HTTPS	
		Snapshot 使用済み容量	実装済み	HTTPS	
		スナップショット使用容量比率	実装済み	HTTPS	時系列で報告

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
NetApp ONTAP REST API	HTTPS	HTTPS	443		true	true	true	true

NetApp SolidFire 8.1 以上

このデータコレクターでサポートされてい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-0 • H410S-1 • H410S-2 • H500S • H610S-1 • H610S-2 • H610S-4 • SF19210 • SF2405 • SF38410 • SF4805 • SF9605 • SF9608	• 11.1.0.72 • 11.7.0.76 • 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ーでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		QoS 制限 IOPS	実装済み	HTTPS	
		QoS 最小 IOPS	実装済み	HTTPS	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		QoS - ポリシー	実装済み	HTTPS	
	ボリュームマップ	LUN	実装済み	HTTPS	バックエンド LUN の名前
		マスクが必要	実装済み	HTTPS	
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実装済み	HTTPS	
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					（MB/秒）
		スループット書き込み	実装済み	HTTPS	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		利用合計	実装済み	HTTPS	
	Volume	物理容量	実装済み	HTTPS	
		総容量	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		使用容量比率	実装済み	HTTPS	
		総圧縮節約	実装済み	HTTPS	
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOP合計	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		鍵	実装済み	HTTPS	
		レイテンシ読み取り	実装済み	HTTPS	
		レイテンシ合計	実装済み	HTTPS	
		レイテンシ書き込み	実装済み	HTTPS	
		部分ブロック率	実装済み	HTTPS	
		サーバ ID	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	HTTPS	
		利用合計	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
SolidFire REST API	HTTPS	HTTPS	443		true	true	true	true

NetAppStorageGRID(HTTPS)

このデータコレクターでサポートされているモデルとバージョン:

API バージョン	モデル	ファームウェアバージョン
• 3.2 • 3.3 • 3.4 • 3.5 • 4.0 • 4.1	• Webscale	• 11.4.0 • 11.5.0.11 • 11.5.0.6 • 11.5.0.7 • 11.5.0.9 • 11.6.0 • 11.6.0.10 • 11.6.0.11 • 11.6.0.12 • 11.6.0.13 • 11.6.0.14 • 11.6.0.15 • 11.6.0.16 • 11.6.0.4 • 11.6.0.5 • 11.6.0.7 • 11.6.0.8 • 11.6.0.9 • 11.7.0 • 11.7.0.11 • 11.7.0.12 • 11.7.0.13 • 11.7.0.3 • 11.7.0.4 • 11.7.0.5 • 11.7.0.6 • 11.7.0.8 • 11.7.0.9 • 11.8.0 • 11.8.0.1 • 11.8.0.2 • 11.8.0.3 • 11.8.0.5 • 11.8.0.6 • 11.8.0.7 • 11.8.0.8 11.8.0.9 11.9.0

このデータコレクターでサポートされている製品:

-
- 11.9.0.1
- 11.9.0.2
- 11.9.0.3
- 11.9.0.4

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		ノード容量使用率使用メタデータ（MB）	実装済み	HTTPS	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		サイト名	実装済み	HTTPS	
	ストレージ プール	DWH容量に含める	実装済み	HTTPS	ACQからDWH容量に関心のあるストレージプールを制御する方法
		Name	実装済み	HTTPS	
		物理ディスク容量（MB）	実装済み	HTTPS	ストレージプールの生の容量として使用
		レイドグループ	実装済み	HTTPS	このストレージプールがRAIDグループであるかどうかを示します
		原材料と使用可能量の比率	実装済み	HTTPS	使用可能容量から生の容量に変換する比率
		ストレージプールID	実装済み	HTTPS	
		シンプロビジョニングをサポート	実装済み	HTTPS	この内部ボリュームがその上のボリューム層に対してシンプロビジョニングをサポートしているかどうか
		割り当て済み容量の合計	実装済み	HTTPS	
		総使用容量	実装済み	HTTPS	総容量（MB）
		タイプ	ギャップ	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					と書き込み）（MB/秒）
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
	ストレージノードデータ	鍵	実装済み		
		ノード容量使用率許可メタデータ	実装済み		
		ノード容量使用率合計	実装済み		
		ノード容量使用率使用可能	実装済み		
		ノード容量使用率	実装済み		
		ノード容量使用率使用メタデータ	実装済み		
		サーバ ID	実装済み		
		スループット読み取り	実装済み		
		スループット合計	実装済み		平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み		
	ストレージプールディスク	プロビジョニングされた容量	実装済み		
		物理容量	実装済み		
		総容量	実装済み		
		使用容量	実装済み		
		オーバーコミット容量比率	実装済み		時系列で報告
		使用容量比率	実装済み		

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
ストレージグリッド REST API	HTTPS	HTTPS	443		true	false	true	true

Nutanix ストレージ (REST)

このデータコレクターでサポートされてい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
NX-3170-G7 NX-8155-G7 HPE DX380 12LFF G11 HPE DX380-24 G10 HPE DX385-12 Gen10 Plus NX-3060-G6 NX-3060-G7 NX-3060-G8 NX-3155G-G7 NX-3155G-G8 NX-3170-G6 NX-8035-G8 NX-8150-G7 NX-8150-G8 NX-8155-G8 XF3070 XF8050 コア	5.20.1.1 6.10 6.10.1 6.5.3.7 6.5.4 6.5.5.1 6.5.5.7 6.5.6 6.5.6.5 6.5.6.6 6.5.6.7 6.7.1.6 7.0

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		タイプ	ギャップ	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
	Volume	容量	実装済み	HTTPS	スナップショット使用容量（MB）
		ジャンクションパス	実装済み	HTTPS	
		Name	実装済み	HTTPS	
		qtree ID	実装済み	HTTPS	qtreeの一意のID
		合計物理容量	実装済み	HTTPS	総生容量（アレイ上のすべてのディスクの合計）
		冗長性	実装済み	HTTPS	冗長レベル
		ストレージプールID	実装済み	HTTPS	
		シンプロビジョニング	実装済み	HTTPS	
		UUID	実装済み	HTTPS	
	ボリュームマップ	LUN	実装済み	HTTPS	バックエンドLUN の名前
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
	ボリュームマスク	イニシエータ	実装済み	HTTPS	
		プロトコルコントローラー	実装済み	HTTPS	
		ストレージポート	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					と書き込み）（MB/秒）
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
		書き込み		HTTPS	
	ストレージプールディスク	IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOP合計	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	HTTPS	
	Volume	レイテンシ合計	実装済み	HTTPS	
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		レイテンシ読み取り	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット書き込み	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		IOP合計	実装済み	HTTPS	
		レイテンシ書き込み	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
Nutanix REST API	HTTPS	HTTPS	443		true	true	true	true

Oracle ZFS (HTTPS)

このデータコレクターでサポートされてい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 7120 • Sun ZFS Storage 7320 • Sun ZFS Storage 7330 • Sun ZFS Storage 7335 • Sun ZFS Storage 7350 • Sun ZFS Storage 7370 • Sun ZFS Storage 7390 • Sun ZFS Storage 7420	• 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 • 2013.06.05.7.29 • 2013.06.05.8.0 • 2013.06.05.8.26 • 2013.06.05.8.29 • 2013.06.05.8.37 • 2013.06.05.8.44 • 2013.06.05.8.50 • 2013.06.05.8.53 • 2013.06.05.8.56 • 2013.06.05.8.6 • 2013.06.05.8.61 • 2013.06.05.8.65 • 2013.06.05.8.7 • 2013.06.05.8.72 • 2013.06.05.8.74 • 2013.06.05.8.76

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		使用容量	実装済み	HTTP/S	
		バーチャル	実装済み	HTTP/S	これはストレージ仮想化デバイスですか?
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
	ボリュームマップ	LUN	実装済み	HTTP/S	バックエンド LUN の名前
		マスクが必要	実装済み	HTTP/S	
		プロトコルコントローラー	実装済み	HTTP/S	
		ストレージポート	実装済み	HTTP/S	
		タイプ	ギャップ	HTTP/S	
	ボリュームマスク	イニシエータ	実装済み	HTTP/S	
		プロトコルコントローラー	実装済み	HTTP/S	
		ストレージポート	実装済み	HTTP/S	
		タイプ	ギャップ	HTTP/S	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					
1296					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		ストレージプールの容量	実装済み		
		鍵	実装済み		
製品	カテゴリ	特徴/属性 サーバ ID	ステータス 実装済み	使用されるプロトコル	追加情報
	ストレージ ノード	IOPS読み取り	実装済み		ディスク上の読み取りIOPS数
		IOPS書き込み	実装済み		
		IOP合計	実装済み		
		キャッシュヒット率合計	実装済み		
		スループット合計	実装済み		平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		利用合計	実装済み		
		スループット書き込み	実装済み		
		スループット読み取り	実装済み		
	ストレージノードデータ	キャッシュヒット率合計	実装済み		
		IOPS読み取り	実装済み		ディスク上の読み取りIOPS数
		IOP合計	実装済み		
		IOPS書き込み	実装済み		
		鍵	実装済み		
		サーバ ID	実装済み		
		スループット読み取り	実装済み		
		スループット合計	実装済み		平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み		
		利用合計	実装済み		
	ストレージプールディスク	IOP合計	実装済み		

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
Oracle ZFS REST API	HTTP / HTTPS	HTTP / HTTPS	215		true	true	true	true

ピュアストレージ フラッシュアレイ (HTTP)

このデータコレクターでサポートされてい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-450 • FA-C40R3 • FA-C50R4 • FA-C60 • FA-C60R3 • FA-C70R4 • FA-C90R4 • FA-X10R2 • FA-X10R3 • FA-X20R2 • FA-X20R3 • FA-X20R4 • FA-X50R2 • FA-X50R3 • FA-X50R4 • FA-X70R2 • FA-X70R3 • FA-X70R4 • FA-X90R2 • FA-X90R3 • FA-X90R4 • FA-XL130 • FA-XL170 • FA-m20 • FA-m20r2 • FA-m50 • FA-m70 • FA-m70r2 • 酸素	• 5.3.14 • 5.3.20 • 6.1.10 • 6.1.14 • 6.1.18 • 6.1.19 • 6.1.21 • 6.1.22 • 6.1.23 • 6.2.10 • 6.3.10 • 6.3.11 • 6.3.12 • 6.3.13 • 6.3.14 • 6.3.15 • 6.3.16 • 6.3.17 • 6.3.18 • 6.3.3 • 6.3.6 • 6.3.7 • 6.3.9 • 6.4.10 • 6.4.2 • 6.4.3 • 6.4.7 • 6.4.8 • 6.4.9 • 6.5.0 • 6.5.1 • 6.5.2 • 6.5.3 • 6.5.4 • 6.5.5 • 6.5.6 6.5.7 6.5.8

このデータコレクターでサポートされている製品:	• • 6.5.9 • 6.6.10 • 6.6.11 • 6.6.5 • 6.6.6 • 6.6.7 • 6.7.0 • 6.7.1 • 6.8.1 • 6.8.2 • 6.8.3

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		トローラー			
		ストレージポート	実装済み	HTTP/S	
製品	カテゴリ	特徴/属性タイプ	ステータスギャップ	使用されるプロトコル	追加情報
	ボリュームマスク	イニシエータ	実装済み	HTTP/S	
		プロトコルコントローラー	実装済み	HTTP/S	
		ストレージポート	実装済み	HTTP/S	
		タイプ	ギャップ	HTTP/S	
	WWNエイリアス	ホストエイリアス	実装済み	HTTP/S	
		オブジェクト タイプ	実装済み	HTTP/S	
		ソース	実装済み	HTTP/S	
		WWN	実装済み	HTTP/S	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					と書き込み）（MB/秒）
製品	カテゴリ	特徴/属性	実装済み/ステータス	使用されるプロトコル	追加情報
	ストレージプールディスク	プロビジョニングされた容量	実装済み		
		物理容量	実装済み		
		総容量	実装済み		
		使用容量	実装済み		
		オーバーコミット容量比率	実装済み		時系列で報告
		使用容量比率	実装済み		
		合計データ容量	実装済み		
		データ使用容量	実装済み		
		その他の使用容量	実装済み		
		Snapshot 使用済み容量	実装済み		
		スナップショット使用容量比率	実装済み		時系列で報告
	Volume	物理容量	実装済み		
		総容量	実装済み		
		使用容量	実装済み		
		使用容量比率	実装済み		
		IOPS読み取り	実装済み		ディスク上の読み取りIOPS数
		IOP合計	実装済み		
		IOPS書き込み	実装済み		
		レイテンシ読み取り	実装済み		
		レイテンシ合計	実装済み		
		レイテンシ書き込み	実装済み		
		スループット読み取り	実装済み		
		スループット合計	実装済み		平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み		

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
ピュアストレージREST API	HTTP / HTTPS	HTTP / HTTPS	80/443		true	true	true	true

レッドハット **RHV (REST)**

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		Name	実装済み	HTTP/S	
		OID	実装済み	HTTP/S	
		ポート	実装済み	HTTP/S	
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
		プラットフォーム タイプ			
	ISCSI ノード	Node Name	実装済み	HTTP/S	
		OID	実装済み	HTTP/S	
		タイプ	ギャップ	HTTP/S	
	情報	データソース名	実装済み	HTTP/S	情報
		日付	実装済み	HTTP/S	
		発信者ID	実装済み	HTTP/S	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
レッドハット RHEV REST API	HTTPS	HTTPS	443		true	true	true	true

ルーブリックストレージ

このデータコレクターでサポートされているモデルとバージョン: ファームウェアバージョン:

- 8.1.3-p12-25506
- 8.1.3-p13-25544
- 8.1.3-p2-24912
- 9.0.3-p10-25744
- 9.0.3-p5-25595
- 9.0.3-p6-25611
- 9.1.1-27527
- 9.1.2-27824
- 9.1.2-p1-27870
- 9.1.2-p1-27870_HP1473894
- 9.1.3-p1-28075
- 9.1.3-p8-28434
- 9.2.2-p1-29213
- 9.2.3-29313
- 9.2.3-p1-29368

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
1320					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		（MB）			
		ノード容量使用率（MB）	実装済み	HTTPS	
製品	カテゴリ	特徴/属性 サイト名	ステータス 実装済み	使用されるプロトコル HTTPS	追加情報
	ストレージ プール	データ使用容量	実装済み	HTTPS	
		DWH容量に含める	実装済み	HTTPS	ACQからDWH容量に関心のあるストレージプールを制御する方法
		Name	実装済み	HTTPS	
		その他使用容量（MB）	実装済み	HTTPS	データとスナップショット以外の容量
		物理ディスク容量（MB）	実装済み	HTTPS	ストレージプールの生の容量として使用
		レイドグループ	実装済み	HTTPS	このストレージプールがRAIDグループであるかどうかを示します
		原材料と使用可能量の比率	実装済み	HTTPS	使用可能容量から生の容量に変換する比率
		Snapshot 使用済み容量	実装済み	HTTPS	
		ストレージプールID	実装済み	HTTPS	
		シンプロビジョニングをサポート	実装済み	HTTPS	この内部ボリュームがその上のボリューム層に対してシンプロビジョニングをサポートしているかどうか
		割り当て済み容量の合計	実装済み	HTTPS	
		総使用容量	実装済み	HTTPS	総容量（MB）
		タイプ	ギャップ	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?
		有効使用容量の割合	実装済み	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					
1324					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					（MB/秒）
		スループット書き込み	実装済み	HTTPS	
製品	カテゴリ	特徴/属性利用合計	ステータス実装済み	使用されるプロトコル HTTPS	追加情報
	ストレージプールディスク	IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOPS書き込み	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット書き込み	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		IOP合計	実装済み	HTTPS	
		総容量	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
		その他の使用容量	実装済み	HTTPS	
		物理容量	実装済み	HTTPS	
		使用容量比率	実装済み	HTTPS	
		データ使用容量	実装済み	HTTPS	
		Snapshot 使用済み容量	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	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		true	true	true	true

VAST データストア

このデータコレクターでサポートされてい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
VA2437096 VASTデータ	ビルド バージョン:release-5.0.0-sp24-1389206 ビルド バージョン:release-5.0.0-sp24-1389206 ビルド バージョン:release-5.0.0-sp70-1532643 ビルド バージョン:release-5.1.0-sp50-1578267 ビルド バージョン:release-5.1.0-sp51-hf3-1643358 ビルド バージョン:release-5.1.0-sp56-1630237 ビルド バージョン:release-5.1.0-sp56-hf10-1682647 ビルド バージョン:release-5.1.0-sp56-hf14-1700467 システム バージョン:5.0.0.94 システム バージョン:5.0.0.133 システム バージョン:5.0.0.94 システム バージョン: 5.1.0.210 システムバージョン: 5.1.0.231

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

					サポートしているかどうか
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
		割り当て済み容量の合計	実装済み	HTTPS	
		総使用容量	実装済み	HTTPS	総容量（MB）
		タイプ	ギャップ	HTTPS	
		バーチャル	実装済み	HTTPS	これはストレージ仮想化デバイスですか?
		暗号化	実装済み	HTTPS	
	ストレージ仮想マシン	割り当てられた容量（MB）	実装済み	HTTPS	スナップショットの割り当て容量
		コメント	実装済み	HTTPS	
		ガイドキー	実装済み	HTTPS	ストレージ仮想マシンのグローバル一意キー
		Name	実装済み	HTTPS	
		タイプ	ギャップ	HTTPS	
		UUID	実装済み	HTTPS	
		使用容量	実装済み	HTTPS	
	仮想マシン内部ボリューム参照	内部ボリュームID	実装済み	HTTPS	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス	ストレージ	失敗した生の容量	実装済み	HTTPS	
		物理容量	実装済み	HTTPS	
		予備の生の容量	実装済み	HTTPS	スペアディスクの生の容量（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	実装済み	HTTPS	
		IO密度読み取り	実装済み	HTTPS	
		IO密度合計	実装済み	HTTPS	
		書き込みIO密度	実装済み	HTTPS	
		IOPsその他	実装済み	HTTPS	
		IOPS読み取り	実装済み	HTTPS	ディスク上の読み取りIOPS数
		IOP合計	実装済み	HTTPS	
		IOPS書き込み	実装済み	HTTPS	
		鍵	実装済み	HTTPS	
		レイテンシ読み取り	実装済み	HTTPS	
		レイテンシ合計	実装済み	HTTPS	
		レイテンシ書き込み	実装済み	HTTPS	
		サーバ ID	実装済み	HTTPS	
		スループット読み取り	実装済み	HTTPS	
		スループット合計	実装済み	HTTPS	平均ディスク合計速度（全ディスクの読み取りと書き込み）（MB/秒）
		スループット書き込み	実装済み	HTTPS	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
VAST データストア API	HTTPS	HTTPS	443		true	true	true	true

NetApp HCI仮想センター

このデータコレクターでサポートされているモデルとバージョン: API バージョン:

- VMware vCenter Server 6.7.0 ビルド 10244857
- VMware vCenter Server 7.0.3 ビルド 20395099

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

	仮想マシンディスク	OID	実装済み	ウェブサービス	
		仮想マシンOID	実装済み	ウェブサービス	
		仮想ディスクOID	実装済み	ウェブサービス	
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報
	ホスト	ホストCPU数	実装済み	ウェブサービス	
		ホストCPU速度	実装済み	ウェブサービス	
		ホストドメイン	実装済み	ウェブサービス	
		ホストにインストールされているメモリ	実装済み	ウェブサービス	
		ホストモデル	実装済み	ウェブサービス	
		NICの数	実装済み	ウェブサービス	
		NIC速度	実装済み	ウェブサービス	
		IPアドレス	実装済み	ウェブサービス	
		メーカー	実装済み	ウェブサービス	
		Name	実装済み	ウェブサービス	
		OID	実装済み	ウェブサービス	
		プラットフォーム タイプ	実装済み	ウェブサービス	
	ISCSI ノード	ホストエイリアス	実装済み	ウェブサービス	
		Node Name	実装済み	ウェブサービス	
		OID	実装済み	ウェブサービス	
		タイプ	ギャップ	ウェブサービス	
	情報	APIの説明	実装済み	ウェブサービス	
		API名	実装済み	ウェブサービス	
		APIバージョン	実装済み	ウェブサービス	
		クライアントAPI名	実装済み	ウェブサービス	
		クライアント API バージョン	実装済み	ウェブサービス	
		データソース名	実装済み	ウェブサービス	情報
		日付	実装済み	ウェブサービス	
		発信者ID	実装済み	ウェブサービス	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		待ち時間をスケジュールする	実装済み	ウェブサービス	スケジュール待ち時間（パーセント）
製品	カテゴリ	特徴/属性	実装済み	使用されるプロトコル	追加情報
		合計ops	実装済み	ウェブサービス	
		トータルスワップレート	実装済み	ウェブサービス	
		スループット読み取り	実装済み	ウェブサービス	ディスクスループット合計読み取り

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
VMware REST API	ウェブサービス	HTTP / HTTPS	80/443		true	true	true	true

VMware Cloud on AWS

このデータコレクターでサポートされているモデルとバージョン: API バージョン:

- VMware vCenter Server 7.0.3 ビルド 21477706
- VMware vCenter Server 7.0.3 ビルド 24322018
- VMware vCenter Server 8.0.0 ビルド 22877852
- VMware vCenter Server 8.0.1 ビルド 22161730
- VMware vCenter Server 8.0.1 ビルド 23525738
- VMware vCenter Server 8.0.3 ビルド 24322831

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

	仮想マシンディスク	OID	実装済み	ウェブサービス	
		仮想ディスクOID	実装済み	ウェブサービス	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		仮想マシンOID	実装済み	ウェブサービス	
	ホスト	ホストCPU数	実装済み	ウェブサービス	
		ホストCPU速度	実装済み	ウェブサービス	
		ホストドメイン	実装済み	ウェブサービス	
		ホストにインストールされているメモリ	実装済み	ウェブサービス	
		ホストモデル	実装済み	ウェブサービス	
		NICの数	実装済み	ウェブサービス	
		NIC速度	実装済み	ウェブサービス	
		IPアドレス	実装済み	ウェブサービス	
		メーカー	実装済み	ウェブサービス	
		Name	実装済み	ウェブサービス	
		OID	実装済み	ウェブサービス	
		プラットフォーム タイプ	実装済み	ウェブサービス	
	情報	APIの説明	実装済み	ウェブサービス	
		API名	実装済み	ウェブサービス	
		APIバージョン	実装済み	ウェブサービス	
		クライアントAPI名	実装済み	ウェブサービス	
		クライアント API バージョン	実装済み	ウェブサービス	
		データソース名	実装済み	ウェブサービス	情報
		日付	実装済み	ウェブサービス	
		発信者ID	実装済み	ウェブサービス	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス	ホスト	合計CPU使用率	実装済み	ウェブサービス	
		IOPS読み取り	実装済み	ウェブサービス	ディスク上の読み取りIOPS数
		ディスクIops合計	実装済み	ウェブサービス	
		ディスクIOPS書き込み	実装済み	ウェブサービス	
		レイテンシ読み取り	実装済み	ウェブサービス	
		レイテンシ合計	実装済み	ウェブサービス	
		レイテンシ書き込み	実装済み	ウェブサービス	
		ディスクスループット読み取り	実装済み	ウェブサービス	
		スループット読み取り	実装済み	ウェブサービス	ディスクスループット合計読み取り
		ディスクスループット書き込み	実装済み	ウェブサービス	
		IPスループット読み取り	実装済み	ウェブサービス	
		スループット合計	実装済み	ウェブサービス	IPスループット合計
		ipThroughput.write	実装済み	ウェブサービス	
		鍵	実装済み	ウェブサービス	
		合計メモリ使用率	実装済み	ウェブサービス	
		サーバ ID	実装済み	ウェブサービス	
		スワップレート.inRate	実装済み	ウェブサービス	
		スワップレート	実装済み	ウェブサービス	
		トータルスワップレート	実装済み	ウェブサービス	

このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
VMware REST API	ウェブサービス	HTTP / HTTPS	80/443		true	true	true	true

VMware vSphere (Web サービス)

このデータコレクターでサポートされているモデルとバージョン: API バージョン:

- VMware ESXi 6.0.0 ビルド 10474991
- VMware ESXi 6.0.0 ビルド 10719132
- VMware ESXi 6.0.0 ビルド 13635687
- VMware ESXi 6.0.0 ビルド 2494585
- VMware ESXi 6.0.0 ビルド 3620759
- VMware ESXi 6.0.0 ビルド 5050593
- VMware ESXi 6.0.0 ビルド 5224934
- VMware ESXi 6.0.0 ビルド 9239799
- VMware ESXi 6.5.0 ビルド 5310538
- VMware ESXi 7.0.3 ビルド 20036589
- VMware ESXi 7.0.3 ビルド 20328353
- VMware ESXi 8.0.0 ビルド 21203435
- VMware ESXi 8.0.1 ビルド 21495797
- VMware vCenter Server 5.0.0 ビルド 623373
- 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 3252642
- 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 5183551
- 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 12863991
- VMware vCenter Server 6.5.0 ビルド 15259038
- 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 20510539
- VMware vCenter Server 6.5.0 ビルド 22499743
- VMware vCenter Server 6.5.0 ビルド 5973321
- 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 14070654
- VMware vCenter Server 6.7.0 ビルド 14792544
- VMware vCenter Server 6.7.0 ビルド 15679289
- VMware vCenter Server 6.7.0 ビルド 17137232
- VMware vCenter Server 6.7.0 ビルド 17137327
- VMware vCenter Server 6.7.0 ビルド 18010560
- 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 19832280
- VMware vCenter Server 6.7.0 ビルド 20504301
- VMware vCenter Server 6.7.0 ビルド 20504362
- VMware vCenter Server 6.7.0 ビルド 22509751
- VMware vCenter Server 6.7.0 ビルド 24323669
- VMware vCenter Server 6.7.0 ビルド 8170161
- VMware vCenter Server 7.0.2 ビルド 17958471
- VMware vCenter Server 7.0.2 ビルド 18356314
- VMware vCenter Server 7.0.2 ビルド 18455184
- VMware vCenter Server 7.0.2 ビルド 22781136
- VMware vCenter Server 7.0.3 ビルド 18778458
- VMware vCenter Server 7.0.3 ビルド 19234570
- VMware vCenter Server 7.0.3 ビルド 19480866
- VMware vCenter Server 7.0.3 ビルド 19717403

- VMware vCenter Server 7.0.3 ビルド 20150588
- VMware vCenter Server 7.0.3 ビルド 20395099
- VMware vCenter Server 7.0.3 ビルド 20845200
- VMware vCenter Server 7.0.3 ビルド 20990077
- VMware vCenter Server 7.0.3 ビルド 21290409
- VMware vCenter Server 7.0.3 ビルド 21477706
- VMware vCenter Server 7.0.3 ビルド 21784236
- VMware vCenter Server 7.0.3 ビルド 21958406
- VMware vCenter Server 7.0.3 ビルド 22357613
- VMware vCenter Server 7.0.3 ビルド 22837322
- VMware vCenter Server 7.0.3 ビルド 23085514
- VMware vCenter Server 7.0.3 ビルド 23788036
- VMware vCenter Server 7.0.3 ビルド 24026615
- VMware vCenter Server 7.0.3 ビルド 24201990
- VMware vCenter Server 7.0.3 ビルド 24322018
- VMware vCenter Server 8.0.0 ビルド 20519528
- VMware vCenter Server 8.0.0 ビルド 20920323
- VMware vCenter Server 8.0.0 ビルド 21216066
- VMware vCenter Server 8.0.0 ビルド 21457384
- VMware vCenter Server 8.0.1 ビルド 21560480
- VMware vCenter Server 8.0.1 ビルド 21815093
- VMware vCenter Server 8.0.1 ビルド 21860503
- VMware vCenter Server 8.0.1 ビルド 22088981
- VMware vCenter Server 8.0.1 ビルド 22368047
- VMware vCenter Server 8.0.1 ビルド 24005165
- VMware vCenter Server 8.0.2 ビルド 22385739
- VMware vCenter Server 8.0.2 ビルド 22617221
- VMware vCenter Server 8.0.2 ビルド 23319993
- VMware vCenter Server 8.0.2 ビルド 23504390
- VMware vCenter Server 8.0.2 ビルド 23929136
- VMware vCenter Server 8.0.2 ビルド 24321653
- VMware vCenter Server 8.0.3 ビルド 24022515
- VMware vCenter Server 8.0.3 ビルド 24091160
- VMware vCenter Server 8.0.3 ビルド 24262322

- VMware vCenter Server 8.0.3 ビルド 24305161
- VMware vCenter Server 8.0.3 ビルド 24322831

このデータコレクターでサポートされている製品:

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
財団					
1358					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

	仮想マシンディスク	OID	実装済み	ウェブサービス	
		仮想ディスクOID	実装済み	ウェブサービス	
製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
		仮想マシンOID	実装済み	ウェブサービス	
	ホスト	ホストCPU数	実装済み	ウェブサービス	
		ホストCPU速度	実装済み	ウェブサービス	
		ホストドメイン	実装済み	ウェブサービス	
		ホストにインストールされているメモリ	実装済み	ウェブサービス	
		ホストモデル	実装済み	ウェブサービス	
		NICの数	実装済み	ウェブサービス	
		NIC速度	実装済み	ウェブサービス	
		IPアドレス	実装済み	ウェブサービス	
		メーカー	実装済み	ウェブサービス	
		Name	実装済み	ウェブサービス	
		OID	実装済み	ウェブサービス	
		プラットフォーム タイプ	実装済み	ウェブサービス	
	ISCSI ノード	ホストエイリアス	実装済み	ウェブサービス	
		Node Name	実装済み	ウェブサービス	
		OID	実装済み	ウェブサービス	
		タイプ	ギャップ	ウェブサービス	
	情報	APIの説明	実装済み	ウェブサービス	
		API名	実装済み	ウェブサービス	
		APIバージョン	実装済み	ウェブサービス	
		クライアントAPI名	実装済み	ウェブサービス	
		クライアント API バージョン	実装済み	ウェブサービス	
		データソース名	実装済み	ウェブサービス	情報
		日付	実装済み	ウェブサービス	
		発信者ID	実装済み	ウェブサービス	

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報
パフォーマンス					
1362					

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

製品	カテゴリ	特徴/属性	ステータス	使用されるプロトコル	追加情報

		スループット合計	実装済み	ウェブサービス	IPスループット合計	
製品	カテゴリ	特徴/属性	実装ステータス	使用されるプロトコル	追加情報	
		ipThroughput.write	実装済み	ウェブサービス		
		合計メモリ使用率	実装済み	ウェブサービス		
		スワップレート.inRate	実装済み	ウェブサービス		
		スワップレート	実装済み	ウェブサービス		
		トータルスワップレート	実装済み	ウェブサービス		
		待ち時間をスケジュールする	実装済み	ウェブサービス	スケジュール待ち時間（パーセント）	

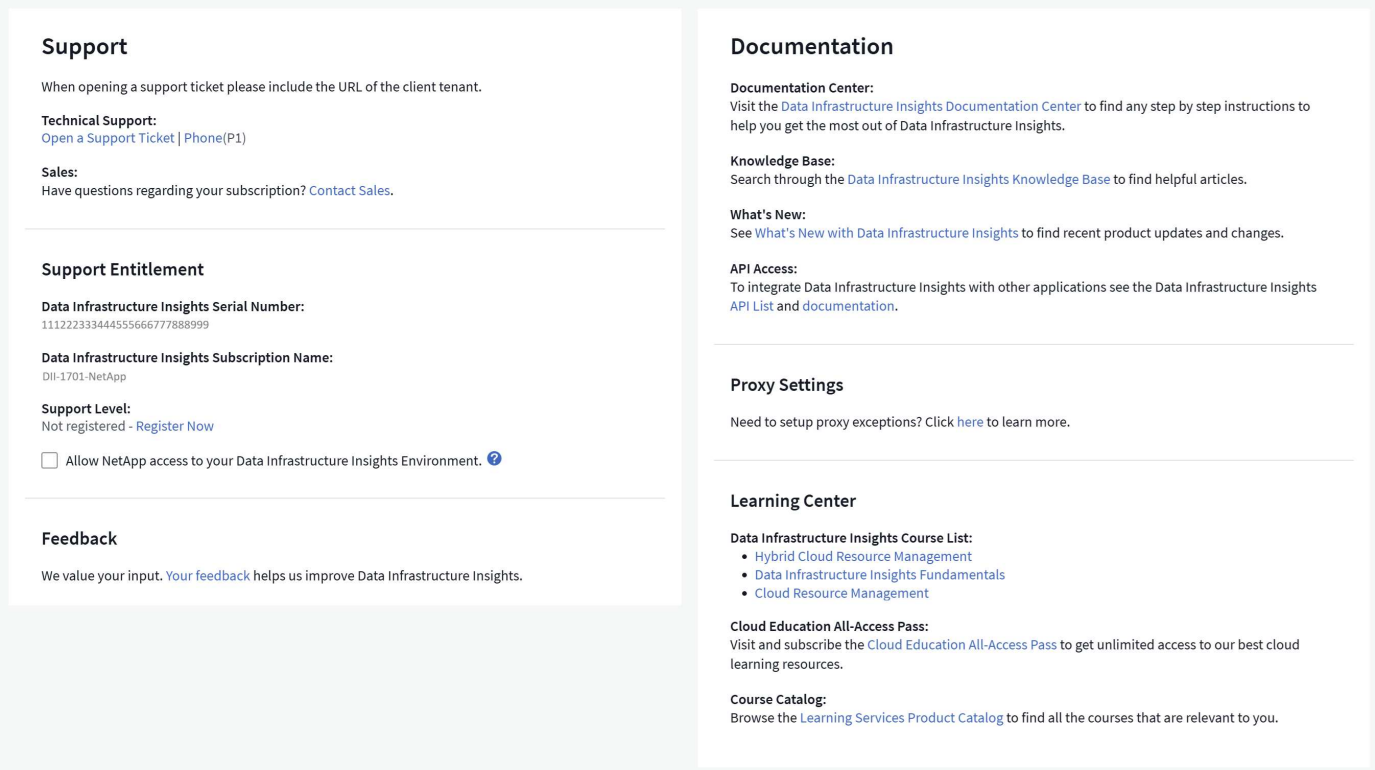
このデータ コレクターで使用される管理 API:

API	使用されるプロトコル	使用されるトランスポート層プロトコル	使用される受信ポート	使用される送信ポート	認証をサポート	「読み取り専用」の資格情報のみが必要です	暗号化をサポート	ファイアウォール対応（静的ポート）
VMware REST API	ウェブサービス	HTTP / HTTPS	80/443		true	true	true	true

リファレンスとサポート

サポートのリクエスト

ヘルプ > サポート を選択すると、 Data Infrastructure Insightsで利用可能なサポート オプションにアクセスできます。



サポート資格の有効化

Data Infrastructure Insights は、試用モードで実行しているときにセルフサービス サポートと電子メール サポートを提供します。サービスに加入したら、サポート資格を有効にすることを強くお勧めします。サポート資格を有効にすると、Web チケット システムと電話を介してテクニカル サポートにアクセスできるようになります。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。見る詳細下に。

最初のサブスクリプション プロセス中に、 Data Infrastructure Insightsインスタンスによって、「950」で始まる 20 桁のNetAppシリアル番号が生成されます。このNetAppシリアル番号は、アカウントに関連付けられているData Infrastructure Insightsサブスクリプションを表します。サポート資格を有効にするには、 NetApp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 2 つのオプションがあります。

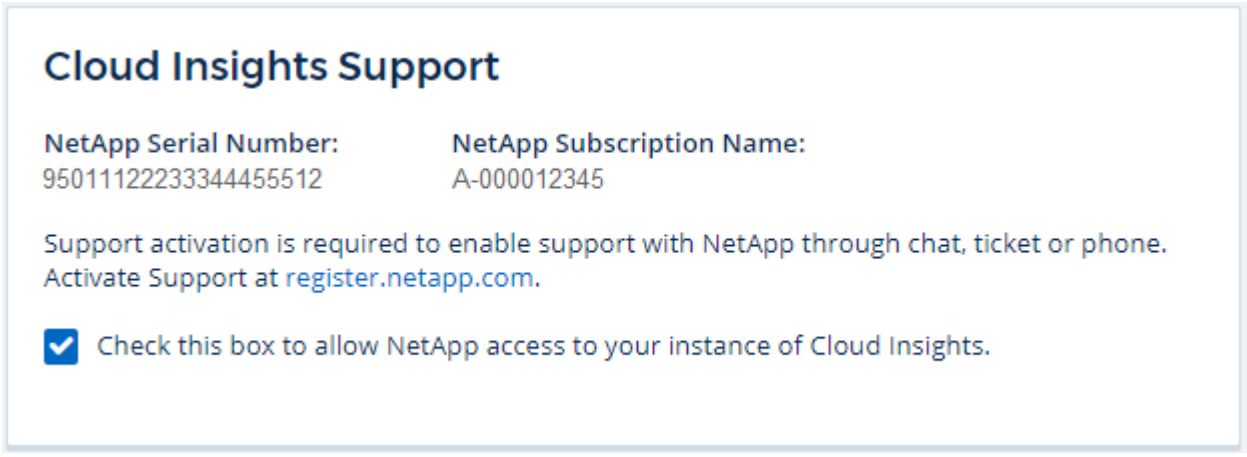
1. 既存のNetAppサポート サイト (NSS) SSO アカウントを持つユーザー (例: 現在のNetApp顧客)
2. 既存のNetAppサポート サイト (NSS) SSO アカウントを持たない新しいNetApp顧客

オプション **1:** 既存の**NetApp**サポート サイト **(NSS) SSO** アカウントを持つユーザーの手順

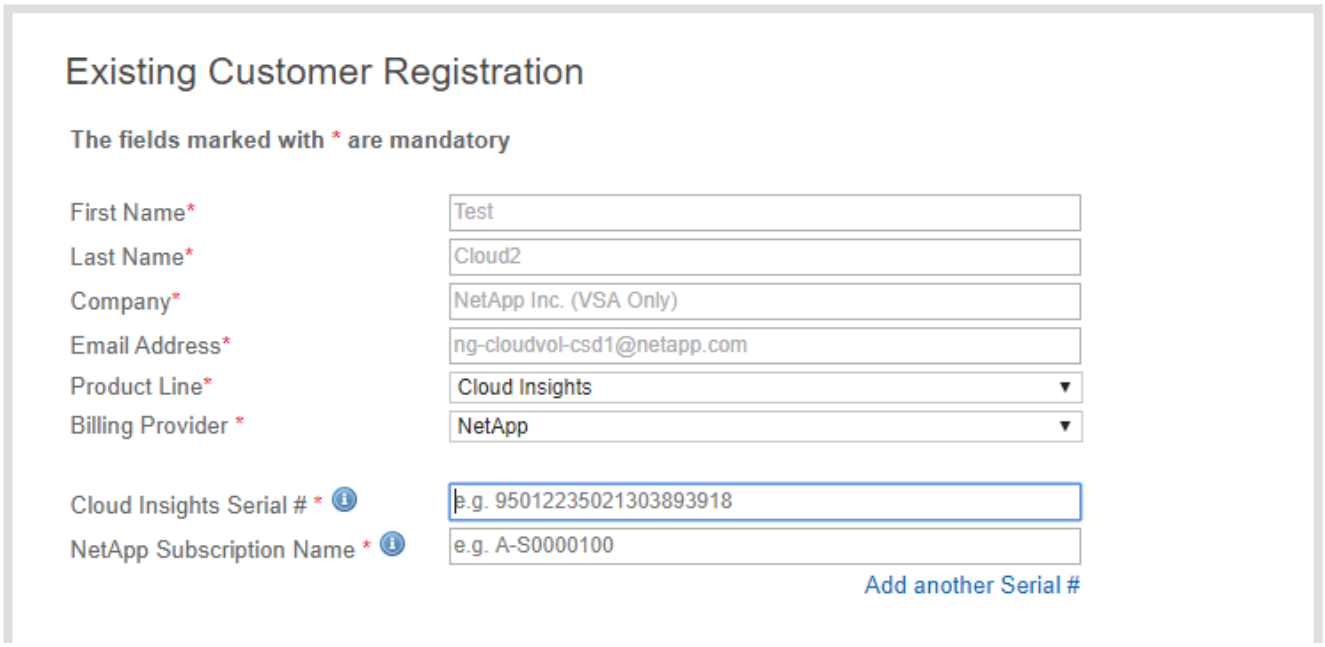
手順

1. NetApp登録ウェブサイトへアクセスします https://register.netapp.com

2. 「すでにNetApp顧客として登録されています」を選択し、製品ラインとして [*Data Infrastructure Insights*] を選択します。請求プロバイダー (NetAppまたは AWS) を選択し、 Data Infrastructure Insightsユーザーインターフェイス内の [ヘルプ > サポート] メニューを参照して、シリアル番号とNetAppサブスクリプション名または AWS 顧客 ID を入力します。



3. 既存顧客登録フォームに記入し、「送信」をクリックします。

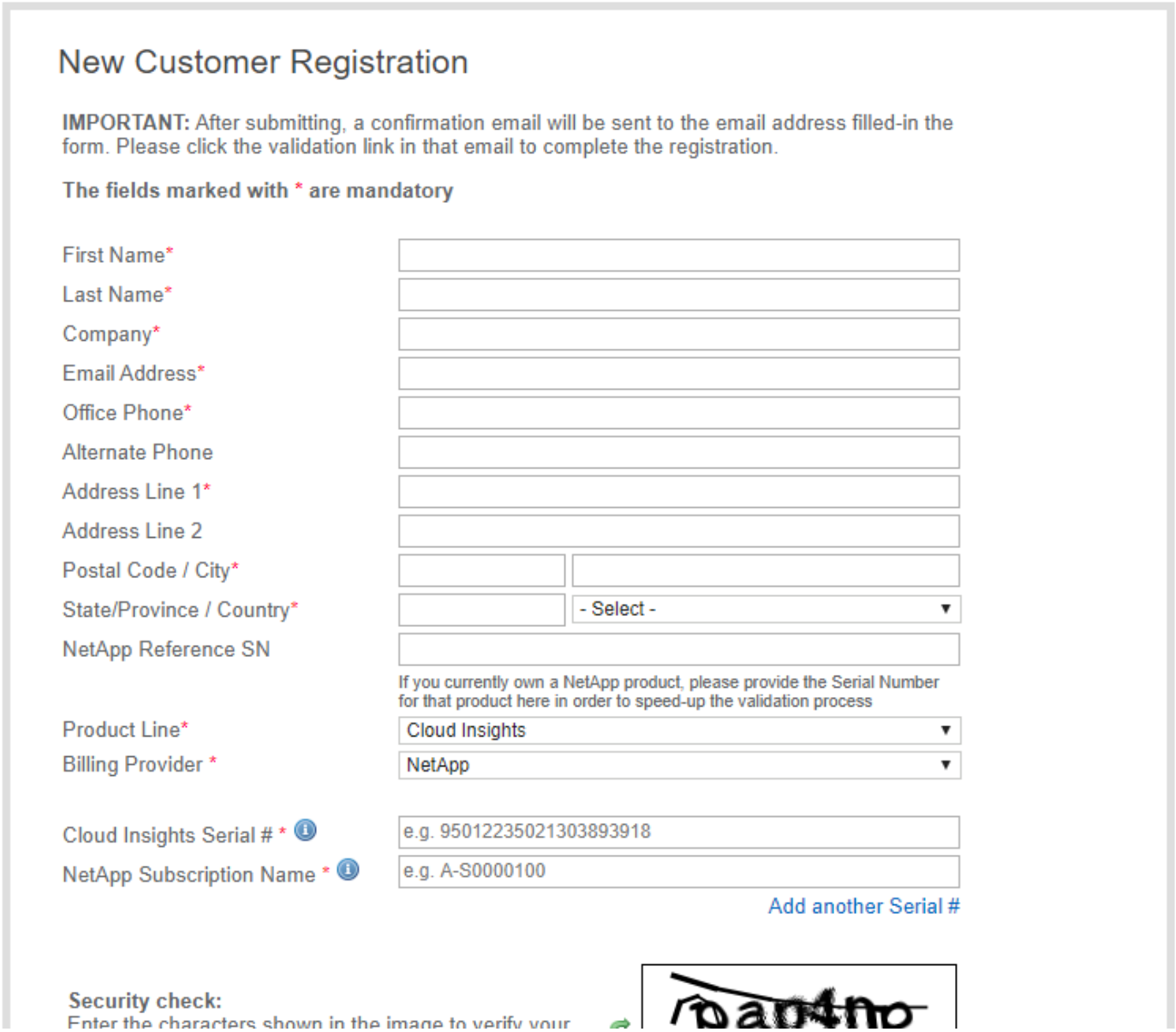


4. エラーが発生しない場合、ユーザーは「登録が正常に送信されました」ページに移動します。登録に使用した NSS SSO ユーザー名に関連付けられた電子メール アドレスに、数分以内に「お使いの製品はサポート対象になりました」という内容の電子メールが届きます。
5. これは、Data Infrastructure Insights NetAppシリアル番号の 1 回限りの登録です。

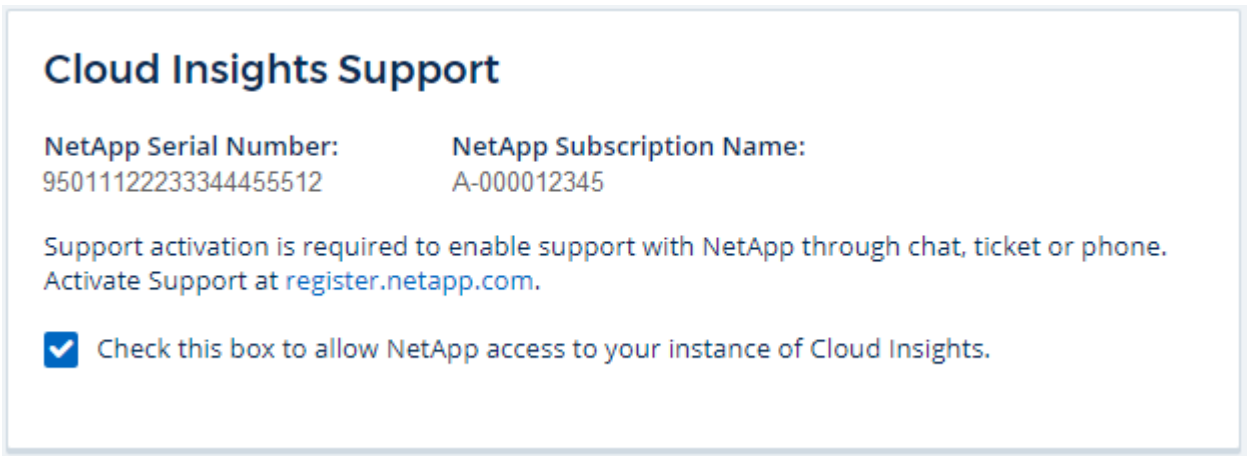
オプション **2:** 既存の**NetApp**サポート サイト **(NSS) SSO** アカウントを持たない新しい**NetApp**顧客向けの手順

手順

1. NetApp登録ウェブサイトへアクセスします https://register.netapp.com
2. 「私はNetAppの登録顧客ではありません」を選択し、以下のサンプル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。請求プロバイダー (NetAppまたは AWS) を選択し、 Data Infrastructure Insightsユーザー インターフェイス内の [ヘルプ > サポート] メニューを参照して、シリアル番号とNetAppサブスクリプション名または AWS 顧客 ID を入力します。



2. エラーが発生しない場合、ユーザーは「登録が正常に送信されました」ページに移動します。登録に使用した NSS SSO ユーザー名に関連付けられた電子メール アドレスに、数時間以内に「お使いの製品はサポート対象になりました」という内容の電子メールが届きます。
3. NetApp の新規顧客として、今後の登録やテクニカル サポートおよび Web チケット用サポート ポータルへのアクセスのために、 NetAppサポート サイト (NSS) ユーザー アカウントも作成する必要があります。このリンクは次の場所にあります https://mysupport.netapp.com/eservice/public/now.do。プロセスを迅速化するために、新しく登録したData Infrastructure Insights のシリアル番号を提供できます。
4. これは、Data Infrastructure Insights NetApp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

NetApp は、さまざまな方法でData Infrastructure Insightsのサポートを提供します。ナレッジベース (KB) 記事やNetAppコミュニティなど、豊富な無料のセルフサポート オプションが 24 時間 365 日ご利用いただけます。Data Infrastructure Insightsに加入しているユーザーは、電話または Web チケットを通じてテクニカル サポートを受けることができます。Web チケットとケース管理には、 NetAppサポート サイト (NSS) SSO アカウントが必要です。

セルフサービスサポート:

以下のサポート オプションは試用モードで利用可能で、24 時間 365 日無料でご利用いただけます。

- ナレッジベース

  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、関連する記事やハウツーなどを検索できます。

- *"ドキュメント" *

  「ドキュメント」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コミュニティに移動し、そこで同僚や専門家とつながることができます。

提供するためのリンクもあります"フィードバック"Data Infrastructure Insights の改善にご協力ください。

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サブスクリプション、または監視対象のNetApp製品やサービスの有料サポートをお持ちの場合は、 NetAppサポート エンジニアと協力して問題を解決することができます。

登録が必要ですサポートを有効にするNetApp Cloud 製品向け。登録するには、NetAppの"クラウドデータサービスサポート登録"。

サポート セッション中にNetAppサポート エンジニアがData Infrastructure Insightsテナントにアクセスできるようにするには、ボックスをオンにすることを強くお勧めします。これにより、エンジニアが問題をトラブルシューティングし、迅速に解決できるようになります。問題が解決した場合、またはサポート セッションが終了したら、ボックスのチェックを外すことができます。

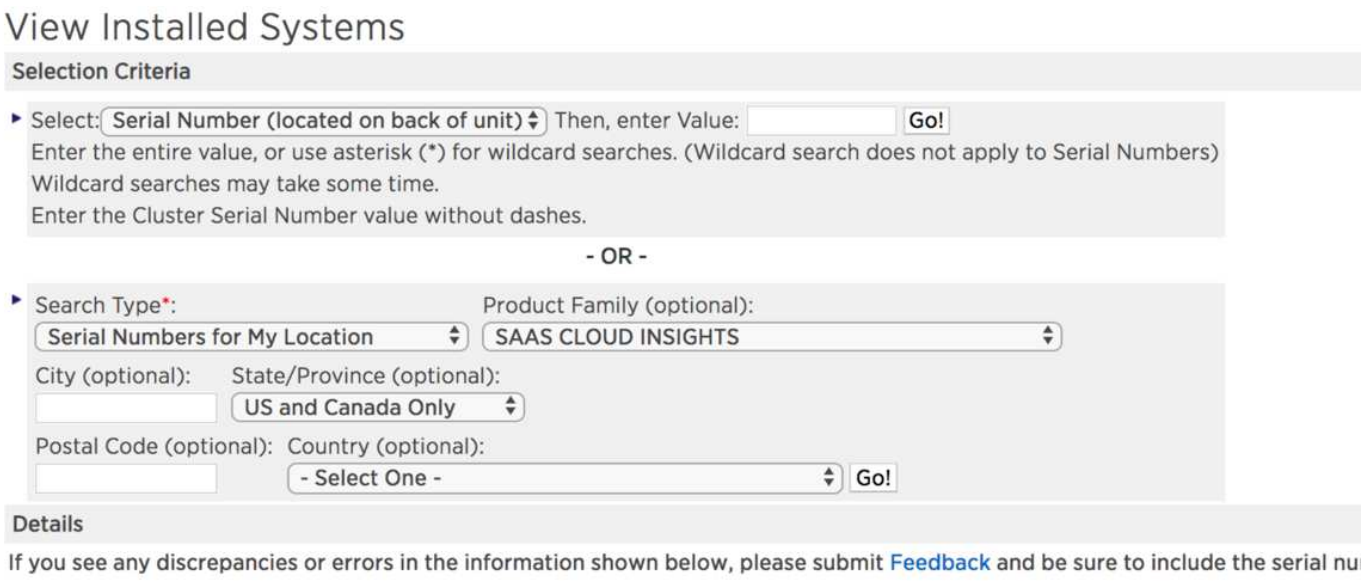
以下のいずれかの方法でサポートをリクエストできます。これらのサポート オプションを使用するには、アクティブなData Infrastructure Insightsサブスクリプションが必要です。

- "電話"
- "サポートチケット"

*営業部に問い合わせる*リンクをクリックして営業サポートをリクエストすることもできます。

Data Infrastructure Insights のシリアル番号は、サービス内の 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に問題があり、以前にNetAppにシリアル番号を登録している場合は、次のようにしてNetAppサポート サイトからData Infrastructure Insightsシリアル番号のリストを表示することもできます。

- mysupport.netapp.comにログイン
- [製品] > [マイ製品] メニュー タブから、製品ファミリー「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見つけます。



Data Infrastructure Insightsデータコレクター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ーに関する情報や詳細は、**Data Infrastructure Insights**データ コレクター サポート マトリックス、role= 。

ラーニングセンター

サブスクリプションの種類に関係なく、ヘルプ > サポート には、Data Infrastructure Insightsを最大限に活用するのに役立ついくつかのNetApp University コースへのリンクがあります。ぜひチェックしてみてください！

データコレクターリファレンス - インフラストラクチャ

ベンダー固有のリファレンス

このセクションのトピックでは、ベンダー固有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 コレクターの構成は簡単です。場合によっては、データ コレクターを適切に構成するために追加の情報や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 ベンダー をクリックすると、そのデータ コレクターの情報が表示されます。

Amazon EC2 データコレクターの設定

Data Infrastructure Insights は、 Amazon EC2 データコレクターを使用して、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 アカウントの **IAM** ロール。 IAM ロールは、取得ユニットが 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 アクセスキー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** アクセスキー ID とシークレットアクセスキー。
- 「リスト組織」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 (あまり自然ではないが) ホストとして報告できます。 EBS ボリュームは、VM によって使用される仮想ディスクとしてだけでなく、仮想ディスクの容量を提供するデータストアとしても報告できます。

アクセス キーは、アクセス キー ID (例: AKIAIOSFODNN7EXAMPLE) とシークレット アクセス キー (例: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY) で構成されます。 Amazon EC2 SDK、REST、またはクエリ API オペレーションを使用する場合は、アクセスキーを使用して EC2 に対して行うプログラムによるリクエストに署名します。これらのキーは、Amazon との契約で提供されます。

構成

以下の表に従って、データ コレクター フィールドにデータを入力します。

フィールド	説明
AWS Region	AWSリージョンを選択
IAM ロール	AWS の AU で取得した場合のみ使用できます。詳細については以下をご覧ください。IAM ロール 。
AWS IAM Access Key ID	AWS IAM アクセスキー 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 シークレットアクセスキー	AWS IAM シークレットアクセスキーを入力します。 IAM ロールを使用しない場合は必須です。
AWSがAPIリクエストに対して料金を請求することを理解しています	これをチェックして、 Data Infrastructure Insightsポーリングによって行われた API リクエストに対して AWS が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
追加リージョンを含める	ポーリングに含める追加の地域を指定します。
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
タグによる VM のフィルタリングを適用するには、「除外」または「含める」を選択します	データを収集するときに、タグによって VM を含めるか除外するかを指定します。 「含める」を選択した場合、タグ キー フィールドを空にすることはできません。
VM をフィルタリングするためのタグキーと値	**+** フィルター タグ をクリックし、VM 上のタグのキーと値に一致するキーと値をフィルターして、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が、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 エージェントメトリクス名前空間	データを収集する EC2/EBS 内の名前空間。この名前空間内のデフォルトのメトリックの名前が変更された場合、 Data Infrastructure Insights は名前が変更されたデータを収集できない可能性があることに注意してください。デフォルトのメトリック名のままにしておくことをお勧めします。

IAMアクセス キー

アクセスキーは、IAM ユーザーまたは AWS アカウントのルートユーザーの長期的な認証情報です。アクセスキーは、AWS CLI または AWS API へのプログラムによるリクエスト (直接または AWS SDK を使用) に署名するために使用されます。

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* アクセスキー 認証を使用する場合 (*IAM* ロール 認証ではなく)、リクエスト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併用する必要があります。詳細については、Amazonのドキュメントをご覧ください。"アクセスキー" 。

IAM ロール

IAM ロール 認証 (IAM アクセスキー認証ではなく) を使用する場合は、作成または指定するロールに、リソースにアクセスするために必要な適切な権限があることを確認する必要があります。

たとえば、*InstanceEc2ReadOnly* という名前の IAM ロールを作成する場合は、この IAM ロールのすべての EC2 リソースに対する EC2 読み取り専用リストアクセス権限を付与するポリシーを設定する必要があります。さらに、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) アクセスを付与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その IAM ロールをアタッチできます。

IAM ロール *InstanceEc2ReadOnly* を EC2 インスタンスにアタッチすると、IAM ロール名でインスタンス メタデータを通じて一時的な認証情報を取得し、それを使用してこの EC2 インスタンスで実行されている任意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のドキュメントをご覧ください。"IAM ロール" 。

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

Amazon タグを**Data Infrastructure Insights**アノテーションにマッピングする

Amazon EC2 データコレクターには、EC2 で設定されたタグを使用してData Infrastructure Insights の注釈を入力できるオプションが含まれています。アノテーションの名前は EC2 タグとまったく同じにする必要があります。 Data Infrastructure Insights は、常に同じ名前のテキスト タイプの注釈を入力し、他のタイプ (数値、ブール値など) の注釈を入力するように「最善の試み」を行います。注釈が別のタイプであり、データ コレクターが注釈を入力できない場合は、注釈を削除してテキスト タイプとして再作成する必要がある場合があります。

AWS では大文字と小文字が区別されますが、 Data Infrastructure Insightsでは大文字と小文字は区別されないことに注意してください。したがって、 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、EC2 の「owner」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 データコレクターの 詳細設定 セクションで、追加のリージョンを含める フィールドを設定して、コンマまたはセミコロンで区切られた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、すべての米国 AWS リージョンで収集されます。すべての地域で収集するには、このフィールドを *.** に設定します。 *追加のリージョンを含める*フィールドが空の場合、データコレクターは*構成*セクションで指定された*AWSリージョン*フィールドで指定されたアセットを収集します。

AWS子アカウントからの収集

Data Infrastructure Insights は、単一の AWS データコレクター内での AWS の子アカウントの収集をサポートします。このコレクションの構成は、AWS 環境で実行されます。

- メインアカウント ID が子アカウントの EC2 の詳細にアクセスできるようにする AWS ロールを各子アカウントに設定する必要があります。
- 各子アカウントのロール名は、同じ文字列として設定されている必要があります。
- このロール名文字列を、 Data Infrastructure Insights AWS Data Collector の 詳細設定 セクションの クロスアカウントロール フィールドに入力します。
- コレクターがインストールされているアカウントには、代理アクセス管理者 権限が必要です。詳細については、"AWS 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 で事前定義された *AmazonEC2ReadOnlyAccess* ポリシーを EC2 メイン アカウントに割り当てることを強くお勧めします。また、AWS をクエリするには、データ ソースで構成されたユーザーには、少なくとも事前定義された *AWSOrganizationsReadOnlyAccess* ポリシーが割り当てられている必要があります。

Data Infrastructure Insights がAWS 子アカウントから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 ロールを使用して AWS アカウント間でアクセスを委任する"

"AWS のセットアップ: 自分が所有する別の AWS アカウントの IAM ユーザーにアクセスを許可する"

"IAM ユーザーに権限を委任するロールの作成"

トラブルシューティング

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

Amazon FSx for NetApp ONTAPデータコレクター

このデータコレクターは、Amazon FSx for NetApp ONTAPからインベントリとパフォーマンスデータを取得します。このデータ コレクターは、Data Infrastructure Insightsサービス リージョン全体で段階的に利用可能になります。 Data Infrastructure Insights環境にこのコレクター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コレクターには、*Filesystem-Scoped* ロールを持つONTAPユーザーが必要です。 AWSを確認してください"役割とルール"利用可能なオプションのドキュメント。現時点では、AWS はファイルシステムスコープを持つユーザーロールとして *fsxadmin* の 1 種類のみをサポートしています。これは、 Data Infrastructure Insightsコレクターに使用する適切なロールです。ユーザーには、http、ontapi、ssh の 3 つのアプリケーションもすべて割り当てられている必要があります。

用語

Data Infrastructure Insights は、 FSx- NetAppデータ コレクターからインベントリとパフォーマンス データを取得します。取得した資産の種類ごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
クラスタ	ストレージ
LUN	Volume
Volume	内部容積

FSx- NetApp用語

次の用語は、FSx- NetAppストレージ アセット ランディング ページに表示されるオブジェクトまたは参照に適用されます。これらの条件の多くは、他のデータ収集者にも適用されます。

ストレージ

- モデル – このクラスター内の一意の個別のモデル名のカンマ区切りリスト。
- ベンダー – AWS
- シリアル番号 – アレイのシリアル番号。

- IP – 通常は、データ ソースで構成されている IP またはホスト名になります。
- 生の容量 – FSx ファイルシステムに割り当てられたすべての SSD ストレージの 2 を底とする合計。
- レイテンシ – 読み取りと書き込みの両方において、ホスト側のワークロードが経験している状況を表します。理想的には、 Data Infrastructure Insightsがこの値を直接取得しますが、多くの場合そうではありません。アレイがこれを提供する代わりに、 Data Infrastructure Insightsは通常、個々の内部ボリュームの統計から導き出された IOPS 加重計算を実行します。
- スループット – 内部ボリュームから集計されます。管理 – これにはデバイスの管理インターフェイスへのハイパーリンクが含まれる場合があります。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

- ストレージ – このプールが存在するストレージ アレイ。必須。
- タイプ – 可能性のある列挙リストからの説明的な値。最も一般的なのは「アグリゲート」または「RAID グループ」です。
- 容量 – ここでの値は、論理的に使用されている容量、使用可能な容量、論理的な合計容量、およびこれらの間で使用されている割合です。
- IOPS – このストレージ プールに割り当てられたすべてのボリュームの合計 IOPS。
- スループット – このストレージ プールに割り当てられた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 コレクターを構成して使用するための要件は次のとおりです。

- 「fsxadmin」ロールを持つアカウントにアクセスでき、それには ssh、ontapi、http の 3 つのアプリケーションが割り当てられている必要があります。
- アカウントの詳細にはユーザー名とパスワードが含まれます。
- ポート要件: 443

構成

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

高度なメトリクス

このデータ コレクターは、FSx for NetApp ONTAPストレージから次の高度なメトリックを収集します。

- fpolicy
- nfsv3
- nfsv3:ノード

- nfsv4
- nfsv4_1
- nfsv4_1:ノード
- nfsv4:ノード
- ポリシーグループ
- qtree
- 音量
- ワークロードボリューム

FSx CLI および API コマンドは、Data Infrastructure Insights ZAPI が収集しない一部の容量値を取得するため、特定の容量値 (ストレージ プールの値など) はData Infrastructure Insightsと FSx 自体で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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
401 HTTP 応答または 13003 ZAPI エラー コードを受信し、ZAPI が「権限が不十分です」または「このコマンドは許可されていません」を返します。	ユーザー名とパスワード、およびユーザー権限/許可を確認します。
ZAPI は「クラスタ ロールが cluster_mgmt LIF ではありません」を返します	AU はクラスター管理 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に変更します
再試行後にZAPIコマンドが失敗する	AU はクラスターとの通信に問題があります。ネットワーク、ポート番号、IP アドレスを確認します。ユーザーは、AU マシンのコマンド ラインからコマンドを実行することも試みる必要があります。
AUはHTTP経由でZAPIに接続できませんでした	ZAPI ポートがプレーンテキストを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、通信は失敗します。
SSLException により通信が失敗しました	AU は、ファイラー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 ポートが SSL を受け入れるかどうかを確認するか、別のポートを使用します。
追加の接続エラー: ZAPI 応答にエラー コード 13001、「データベースが開いていません」が含まれています。ZAPI エラー コードは 60 で、応答には「API が時間どおりに終了しませんでした」が含まれています。ZAPI 応答には「initialize_session() が NULL 環境を返しました」が含まれています。ZAPI エラー コードは 14007 で、応答には「ノードが正常ではありません」が含まれています。	ネットワーク、ポート番号、IP アドレスを確認します。ユーザーは、AU マシンのコマンド ラインからコマンドを実行することも試みる必要があります。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Azure コンピューティング データ コレクターの構成

Data Infrastructure Insights は、 Azure コンピューティング データ コレクターを使用して、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 データを取得します。

要件

このデータ コレクターを構成するには、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 管理 REST IP (management.azure.com)
- Azure リソース マネージャー 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 ロールが必要)
- Azure サービス プリンシパル認証キー (ユーザー 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。

  アカウントが適切に構成され、アプリケーションを Azure に登録すると、 Data Infrastructure Insightsを使用して Azure インスタンスを検出するために必要な資格情報が得られます。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[]

構成

以下の表に従って、データ コレクター 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 ロールが必要)	Azure へのサインイン ID。リーダー ロールの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 プリンシパル認証キー	ログイン認証キー
私は、MicrosoftがAPIリクエストに対して料金を請求することを理解しています	Insight ポーリングによって行われた API リクエストに対して Microsoft が課金することを理解していることを確認するには、これにチェックを入れます。

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
タグによる VM のフィルタリングを適用するには、「除外」または「含める」を選択します	データを収集するときに、タグによって VM を含めるか除外するかを指定します。 「含める」を選択した場合、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 をフィルタリングするためのタグキーと値	+ フィルター タグ をクリックし、VM 上のタグのキーと値に一致するキーと値をフィルターして、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が、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300です

トラブルシューティング

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

Broadcom

Brocade Network Advisor データコレクター

Data Infrastructure Insights は、 Brocade Network Advisor データ コレクターを使用して、 Brocadeスイッチからインベントリとパフォーマンス データを取得します。

用語

Data Infrastructure Insights は、 Brocade Network Advisor データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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
論理スイッチ	論理スイッチ

注: 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 コレクターのすべてのケースを反映しているわけではありません。

要件

このデータ コレクターを構成するには、次のものが必要です。

- Data Infrastructure Insights取得ユニットは、BNA サーバー上の TCP ポート 443 への接続を開始します。 BNA サーバーはバージョン 14.2.1 以上を実行している必要があります。
- Brocade Network Advisor サーバーの IP アドレス
- 管理者アカウントのユーザー名とパスワード
- ポート要件: HTTP/HTTPS 443

構成

フィールド	説明
Brocadeネットワークアドバイザーサーバー IP	ネットワークアドバイザーサーバーのIPアドレス
ユーザー名	スイッチのユーザー名
ユーザー名	管理者ユーザー名
パスワード	管理者のパスワード

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）
接続ポートのオーバーライド	空白の場合は、接続タイプフィールドの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
インベントリポーリング間隔（分）	デフォルトは40です
レポートアクセスゲートウェイ	アクセスゲートウェイモードにデバイスを含めるにはチェックを入れます
パフォーマンスポーリング間隔（秒）	デフォルトは1800です

トラブルシューティング

このデータ コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
1 つ以上のノードが Access Gateway ポートにログインしている、またはデータ コレクターが Access Gateway デバイスの検出に失敗したというメッセージが表示されます。	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 が想定されてい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。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Brocade FCスイッチデータコレクター

Data Infrastructure Insights は、 Brocade FC スイッチ (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 モードとアクセス ゲートウェイ モードの両方のデバイスがサポートされています。

用語

Data Infrastructure Insights は、 Brocade FC スイッチ データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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
論理スイッチ	論理スイッチ
仮想ボリューム	Volume
LSANゾーン	IVRゾーン

注: 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 コレクターのすべてのケースを反映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 データを収集するために 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に IP 接続する必要があります。 [ファブリック内のすべてのスイッチを検出する] チェック ボックスをオンにすると、 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。ただし、これらの追加スイッチを検出するには、それらのスイッチへの 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グローバルに同じアカウントが必要です。アクセスを確認するには、PuTTY (オープンソースのターミナルエミュレーター) を使用できます。
- SNMP パフォーマンス ポーリングを行うには、ファブリック内のすべてのスイッチに対してポート 161 と 162 が開いている必要があります。
- SNMP読み取り専用コミュニティ文字列

構成

フィールド	説明
スイッチIP	EFCサーバーのIPアドレスまたは完全修飾ドメイン名
ユーザー名	スイッチのユーザー名
パスワード	スイッチのパスワード
SNMP	SNMPバージョン
SNMPコミュニティ文字列	スイッチへのアクセスに使用されるSNMP読み取り専用コミュニティ文字列

フィールド	説明
SNMPユーザー名	SNMPユーザー名
SNMP パスワード	SNMPのパスワード

高度な設定

フィールド	説明
生地名	データ コレクター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 として報告するに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 ポーリングの間隔。デフォルトは 15 です。
除外されたデバイス	ポーリングから除外するデバイス ID のコンマ区切りリスト
管理ドメインがアクティブ	管理ドメインを使用する場合に選択
MPRデータの取得	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する	デバイスから SNMP トラップを受信したときに取得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 も有効にする必要があります。
トラップ間の最小時間（秒）	トラップによってトリガーされる取得試行間の最小時間。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する	ファブリック内のすべてのスイッチを検出するには選択します
HBA を優先するかゾーン エイリアスを優先するかを選択する	HBA またはゾーン 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 ポーリングの間隔。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	SNMP再試行回数

トラブルシューティング

このデータ コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
Brocadeデータソースのインベントリ取得が次のエラーで失敗しました: <日付> <時刻> ERROR [com.onaro.sanscreen.acquisition.framework.datasource.BaseDataSource] エラー 2 / 2: <データソース名> [内部エラー] - 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 ([デバイス名 <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）	この問題は、 Brocadeスイッチがプロンプトを返すまでに時間がかかり、デフォルトのタイムアウトである 5 秒を超えた場合に発生する可能性があります。 Data Infrastructure Insightsのデータ コレクターの詳細構成設定で、*SSH* バナー待機タイムアウト *(秒)* の値を高くしてみてください。
エラー: 「Data Infrastructure Insights が無効なシャーシ ロールを受信しました」	このデータ ソースで構成されたユーザーにシャーシ ロール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」	DII は、原則として、取得ユニットとデバイス間のネットワーク アドレス変換またはポート アドレス変換をサポートしません。 DII は、コレクター構成内のホスト名/IP アドレスが、デバイスが認識しているアドレスのいずれとも一致しないことを検出している可能性があります。
アクセスゲートウェイポートに1つ以上のノードがログインしているというメッセージを受信する	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 が想定されてい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。
エラー: ....ログインの最大リモート セッション数...	FOS では、ユーザー ロールごとにサポートされる同時 SSH セッションの数に異なる制限があります。これらの制限に違反しているため、このデバイスへの DII の SSH セッションはログイン時に拒否されます。これは、同じ資産を発見したコレクターが重複していることを示す兆候である可能性があり、これを避ける必要があります。

パフォーマンス

問題：	これを試してください:
「SNMP 要求の送信中にタイムアウトしました」というエラーでパフォーマンス収集が失敗します。	クエリ変数とスイッチ構成によっては、一部のクエリがデフォルトのタイムアウトを超える場合があります。"詳細情報" 。
パフォーマンス収集が失敗し、「...SNMP テーブルに行の重複が見つかりました...」というメッセージが表示される	DII は不正な SNMP 応答を検出しました。おそらく FOS 8.2.3e を実行していると思われます。 8.2.3e2 以上にアップグレードしてください。
パフォーマンス収集が「...不明なユーザー名...」で失敗しました	DII コレクターを、SNMPv3 ユーザー スロットの 1 つに挿入されていない「SNMP ユーザー名」値で構成しました。 Brocade FOS でユーザーを作成しただけでは、必ずしも SNMPv3 ユーザーとして有効になるわけではありません。v3 ユーザー スロットの 1 つに配置する必要があります。

問題：	これを試してください:
パフォーマンス収集が「…サポートされていないセキュリティ レベル…」で失敗します	DII コレクターを SNMPv3 を使用するように構成しましたが、問題のデバイスでは暗号化 (プライバシーとも呼ばれます) や認証の設定が有効になっていません。
パフォーマンス収集が失敗しました…空のプライバシー パスワードは、プライバシー プロトコル NONE でのみ許可されます	DIIコレクターを暗号化（別名プライバシープロトコル（AESなど））付きのSNMPv3を使用するように構成しましたが、「SNMPプライバシーパスワード」値が空であるため、DIIはこのデバイスと暗号化されたSNMPv3データフローをネゴシエートできません。
パフォーマンス収集が …..VF:nn、エラー: アクセスなし… で失敗しました	複数の仮想ファブリックが有効になっているデバイスで SNMPv3 を使用するように DII コレクターを構成しましたが、SNMPv3 ユーザーに VF NN の権限がありません。 DII は物理資産の部分的な検出をサポートしていません。DII は常に特定の物理デバイス上の既存の VF のパフォーマンス データを取得しようとするため、常に 128 個の可能な VF すべてに DII アクセスを許可する必要があります。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Brocade FOS REST データコレクター

Data Infrastructure Insights は、 Brocade FOS REST コレクターを使用して、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。初期の 8.2 FOS リリースには REST API バグが含まれている可能性があるので注意してください。プラットフォームがサポートする最新の FOS リリースを実行することを強くお勧めします。

注意: FOS のデフォルトの「ユーザー」レベルでは、Data Infrastructure Insightsがデバイスの論理的側面をすべて表示するには機能が不十分です。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に加えて、「シャーシ ロール」が有効になっているユーザー アカウントが必要です。

以下は、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」ユーザー アカウントを作成する方法の例です。

userConfig --add NetAppCIUser -r user -l 1-128 -c user -p Qwerty!

これにより、パスワードが「Qwerty!」であるユーザー「NetAppCIUser」が作成されます。このユーザーには、128 個のすべての仮想ファブリック (-l) にわたる「ユーザー」ロール (-r) が与えられます。このユーザーには、ユーザー レベルのアクセスが割り当てられた、必要な「シャーシ」ロール (-c) も追加で付与されます。

デフォルトでは、このコレクターは、スイッチが属するすべてのファブリックに含まれるすべての FOS デバイスを検出しようとします。

注意: FOS のデフォルトの読み取り専用ユーザー「ユーザー」には、すべての仮想ファブリックに対する表示権限はなく、「シャーシ ロール」権限もありません。つまり、FOS デバイスの物理構成と論理構成の両方を理解する必要があるData Infrastructure Insightsで「ユーザー」を使用しても成功する可能性は低くなります。

用語

Data Infrastructure Insights は、 Brocade FOS REST データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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
論理スイッチ	論理スイッチ
LSANゾーン	IVRゾーン

注: 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 コレクターのすべてのケースを反映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 接続が必要です。このデータ コレクター 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。 [ファブリック内のすべてのスイッチを検出する] チェック ボックスをオンにすると、 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。ただし、これらの追加スイッチを検出するには、それらのスイッチへの 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グローバルに同じアカウントが必要です。アクセスを確認するには、デバイスの Web インターフェースを使用できます。

構成

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
ユーザー名	スイッチのユーザー名
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	ポーリングから除外するデバイスの IPv4 アドレスのコンマ区切りリスト。
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。デフォルトは 60 です。
ファブリック内のすべてのスイッチを検出する	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 を優先するかゾーン エイリアスを優先するかを選択する	HBA エイリアスとゾーン エイリアスのどちらを優先するかを選択します。
接続の種類	HTTP または HTTPS。
この設定は、デバイスごとにCIが最初に使用しようとするプロトコルを変更するだけであることに注意してください。CIは、デフォルトで失敗した場合、自動的に反対のプロトコルを試みます。	TCPポートの上書き
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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
テスト機能でプロトコルにアクセスできないという警告が表示される	特定のBrocade FOS 8.2+ デバイスは、HTTP または HTTPS でのみ通信しようとします。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 または HTTPS を使用して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 の両方で通信を試行します。テストで 1 つのプロトコルが成功したことが示された場合は、コレクターを安全に保存でき、他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。コレクター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: 401 不正アクセスによりインベントリが失敗しました…無効なセッション キーです…	これは、HTTP 基本認証を適切にサポートしていない 8.2.1c などの非常に初期の 8.2 FOS リリースに特有のバグです。 8.2 または 9.* 以降のリリースにアップグレードします
エラー: 「Data Infrastructure Insights が無効なシャーシ ロールを受信しました」	このデータ ソースで構成されたユーザーにシャーシ ロール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 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。
在庫が403 Forbiddenで失敗する	これは単に資格情報が正しくないこと、または不十分な権限を持つ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」権限や、デフォルト以外の仮想ファブリックへの表示アクセス権がないことを覚えておいてください。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクター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 コレクター

Data Infrastructure Insights は、 Cisco MDS ファブリック スイッチ データ コレクターを使用して、 Cisco MDS ファブリック スイッチのインベントリと、FC サービスが有効になっているさまざまなCisco Nexus FCoE スイッチを検出します。

さらに、このデータ コレクターを使用すると、NPV モードで実行されているCiscoデバイスの多くのモデルを検出できます。

用語

Data Infrastructure Insights は、 Cisco FC スイッチ データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
スイッチ	スイッチ
ポート	ポート
VSAN	ファブリック
ゾーン	ゾーン
論理スイッチ	論理スイッチ
ネームサーバーエントリ	ネームサーバーエントリ
VSAN間ルーティング（IVR）ゾーン	IVRゾーン

注: 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 コレクターのすべてのケースを反映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有効にする）
- SNMP V2を使用する場合、読み取り専用コミュニティ文字列
- ポート161はデバイスへのアクセスに使用されます

構成

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。パフォーマンス取得にはV2以降が必要です。
SNMPコミュニティ文字列	スイッチへのアクセスに使用されるSNMP読み取り専用コミュニティ文字列（SNMP v3には適用されません）

フィールド	説明
ユーザー名	スイッチのユーザー名（SNMP v3のみ）
パスワード	スイッチに使用するパスワード（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）	インベントリポーリングの間隔（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	SNMP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5000ミリ秒）
トラッピングを有効にする	トラッピングを有効にするには選択します。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）	トラップによってトリガーされる取得試行間の最小時間（デフォルトは10秒）
すべてのファブリックスイッチを見る	ファブリック内のすべてのスイッチを検出するには選択します
除外されたデバイス	ポーリングから除外するデバイス IP のコンマ区切りリスト
含まれるデバイス	ポーリングに含めるデバイス IP のコンマ区切りリスト
デバイスの種類を確認する	明示的にCiscoデバイスとしてアドバタイズされているデバイスのみを受け入れるように選択します
最初のエイリアスタイプ	エイリアスの解決に最優先を指定します。次の中から選択します: デバイス アレイ これは、必要に応じてすべての構成コマンドで使用できるポート WWN (pWWN) のユーザーフレンドリな名前です。 Cisco MDS 9000 ファミリのすべてのスイッチは、分散デバイス エイリアス サービス (デバイス エイリアス) をサポートしています。 なし エイリアスを報告しません。 ポートの説明 ポートのリスト内でポートを識別するのに役立つ説明。 ゾーン エイリアス (すべて) アクティブな構成にのみ使用できるポートのユーザーフレンドリな名前。これがデフォルトです。
2番目のエイリアスタイプ	エイリアスの解決に2番目の優先順位を指定する
3番目のエイリアスタイプ	エイリアスの解決に3番目の優先順位を与える

フィールド	説明
SANTapプロキシモードのサポートを有効にする	Ciscoスイッチがプロキシ モードで SANTap を使用している場合に選択します。 EMC RecoverPoint を使用している場合は、おそらく SANTap を使用しているでしょう。
パフォーマンスポーリング間隔（秒）	パフォーマンスポーリングの間隔（デフォルトは300秒）

トラブルシューティング

このデータ コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
エラー: シャーシの検出に失敗しました - スイッチが検出されませんでした	• IPアドレスが設定されているデバイスに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ウォークを実行します。
エラー: デバイスは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 はスイッチの WWN を取得できません。	これは FC または FCoE スイッチではない可能性があり、そのためサポートされない可能性があります。データ ソースに設定されている IP/FQDN が実際に FC/FCoE スイッチであることを確認します。
エラー: NPV スイッチ ポートにログインしているノードが複数見つかりました	NPVスイッチの直接取得を無効にする
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する • IPアドレスとリスニングポートを確認する • デバイスにpingを実行する • Cisco Device Manager GUIを使用してデバイスにログインする • CLIを使用してデバイスにログインする • SNMPウォークを実行する

パフォーマンス

問題：	これを試してください:
エラー: パフォーマンス取得はSNMP v1ではサポートされていません	• 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。• データソースとスイッチ構成を変更して、SNMP v2以上を使用します。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Cohesity SmartFiles データコレクター

この REST API ベースのコレクターは、Cohesity クラスターを取得し、「ビュ

ー」(Data Infrastructure Insightsの内部ボリュームとして) やさまざまなノードを検出し、パフォーマンス メトリックを収集します。

構成

フィールド	説明
Cohesity クラスタ IP	Cohesity クラスタの IP アドレス
ユーザー名	Cohesity クラスタのユーザー名
パスワード	Cohesity クラスタで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 ポーリングの間隔。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 ポーリングの間隔。デフォルトは900秒です。

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Dell

Dell EMC XCシリーズデータコレクター

Data Infrastructure Insights は、このデータ コレクターを使用して、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情報を検出します。

構成

フィールド	説明
Prism外部IPアドレス	XCサーバーのIPアドレス
ユーザー名	XCサーバーのユーザー名
パスワード	XCサーバーで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	XCサーバーとの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 ポーリングの間隔。デフォルトは60分です。

フィールド	説明
パフォーマンスポーリング間隔（分）	パフォーマンス ポーリングの間隔。デフォルトは300秒です。

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Dell EMC

DELL EMC Data Domain データコレクター

このデータ コレクターは、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情報を収集します。このデータ コレクターを構成するには、特定の構成手順と使用上の推奨事項に従う必要があります。

用語

Data Infrastructure Insights は、 Data Domain データ コレクターから次のインベントリ情報を取得します。Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ディスク	ディスク
アレイ	ストレージ
FCポート	ポート
ファイルシステム	内部容積
クォータ	クォータ
NFSとCIFSの共有	ファイルシェア

注: これらは一般的な用語のマッピングのみであり、このデータ収集ツールのすべてのケースを反映しているわけではありません。

要件

このデータ コレクターを構成するには、次の情報が必要です。

- Data DomainデバイスのIPアドレス
- Data Domainストレージへの読み取り専用ユーザー名とパスワード
- SSH、ポート22

構成

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ー名
パスワード	Data Domainストレージアレイのパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。デフォルトは 20 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

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

EMC ECS データコレクターの構成

このデータ コレクターは、EMC ECS 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 データを取得します。構成には、データ コレクターに ECS クラスターの IP アドレスまたはホスト名とユーザー名およびパスワードが必要です。

Dell EMC ECS は、管理対象ユニットとは異なる Raw TB レートで計測されます。フォーマットされていないECS容量40TBごとに1として課金されます。"管理ユニット（MU）"。

用語

Data Infrastructure Insights は、 ECS データ コレクターから次のインベントリ情報を取得します。取得した資産の種類ごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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	内部容積
ディスク	ディスク

注: 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 コレクターのすべてのケースを反映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システムのユーザー名とパスワード
- ポート 4443 (HTTPS)。 ECS システムの TCP ポート 4443 への送信接続が必要です。

構成

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するポート
ECS ユーザーID	ECSのユーザーID
パスワード	ECS で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360分です。

トラブルシューティング

このデータ コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
エラー: ユーザー認証に失敗しました。	このデバイスの資格情報が正しいことを確認してください。

パフォーマンス

問題：	これを試してください:
エラー: 十分なデータが収集されませんでした。	* 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。* より長い時間待機します。
エラー: パフォーマンス 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ます。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Dell EMC PowerScaleデータコレクター

Data Infrastructure Insights は、 Dell EMC PowerScale (旧 Isilon) SSH データ コレクターを使用して、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 データを取得します。

用語

Data Infrastructure Insights は、このデータ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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
ファイルシステム	内部容積

注: 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 コレクターのすべてのケースを反映しているわけではありません。

要件

このデータ コレクターを構成するには、次の情報が必要です。

- PowerScaleストレージへの管理者権限
- PowerScaleクラスターのIPアドレス
- ポート22へのSSHアクセス

構成

フィールド	説明
IPアドレス	PowerScale クラスターの IP アドレスまたは完全修飾ドメイン名
ユーザー名	PowerScaleクラスターのユーザー名
パスワード	PowerScaleクラスターで使用するパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。デフォルトは 20 です。
パフォーマンスポーリング間隔（秒）	パフォーマンス ポーリングの間隔。デフォルトは 300 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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
「無効なログイン資格情報」とエラー メッセージ「ロールベースの管理で有効になっていないコマンドには、ルート ユーザーのアクセスが必要です」	* ユーザーがデバイス上で以下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 version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * ウィザードで使用されている資格情報がデバイスの資格情報と一致していることを確認します
「内部エラー」とエラー メッセージ「コマンド <コマンド> の実行が権限: <現在の権限> で失敗しました。」 Sudoコマンドの実行権限の問題	ユーザーがデバイス上で次のコマンドを実行するためのsudo権限を持っていることを確認します。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Dell EMC Isilon / PowerScale REST データコレクター

Data Infrastructure Insights は、 Dell EMC Isilon / PowerScale REST データ コレクターを使用して、Dell EMC Isilon または PowerScale ストレージからインベントリとパフォーマンス データを取得します。このコレクターは、OneFS 8.0.0 以降を実行するアレイをサポートします。

用語

Data Infrastructure Insights は、このデータ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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	内部容積
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マッピングのみであり、このデータ コレクターのすべてのケースを反映しているわけではありません。

要件

このデータ コレクターを構成するには、次の情報が必要です。

- ユーザーアカウントとパスワード。このアカウントは管理者/ルートである必要はありませんが、サービスアカウントにかなりの数の読み取り専用権限を付与する必要があります - 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 クラスター

権限名	説明	**r(**読み取り**)**または**rw(**読み取り**+**書き込み**)**
ISI_PRIV_LOGIN_PAPI	プラットフォームAPI	r
ISI_PRIV_SYS_TIME	Time	r
ISI_PRIV_AUTH	認証	r
ISI_PRIV_ROLE	権限	r
ISI_PRIV_DEVICES	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を構成する	r
ISI_PRIV_QUOTA	クォータ	r
ISI_PRIV_SMARTPOOLS	スマートプール	r
ISI_PRIV_SMB	SMB	r
ISI_PRIV_統計	統計	r
ISI_PRIV_SWIFT	迅速	r
ISI_PRIV_JOB_ENGINE	求人エンジン	r

構成

フィールド	説明
アイシロン 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
ユーザー名	Isilonのユーザー名
パスワード	Isilonで使用するパスワード

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 ポーリングの間隔。デフォルトは 20 です。

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 ポーリングの間隔。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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
「無効なログイン資格情報」とエラー メッセージ「ロールベースの管理で有効になっていないコマンドには、ルート ユーザーのアクセスが必要です」	* ユーザーがデバイス上で以下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 version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * ウィザードで使用されている資格情報がデバイスの資格情報と一致していることを確認します
「内部エラー」とエラー メッセージ「コマンド <コマンド> の実行が権限: <現在の権限> で失敗しました。」 Sudoコマンドの実行権限の問題	ユーザーがデバイス上で次のコマンドを実行するためのsudo権限を持っていることを確認します。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Dell EMC PowerStoreデータコレクター

EMC PowerStore データ コレクターは、EMC PowerStore ストレージからインベントリ情報を収集します。構成の場合、データ コレクターには、ストレージ プロセッサの IP アドレスと読み取り専用のユーザー名とパスワードが必要です。

EMC PowerStore データ コレクターは、PowerStore が他のストレージ アレイ間で調整するボリューム間のレプリケーション関係を収集します。 Data Infrastructure Insights は、各 PowerStore クラスターのストレージ アレイを表示し、そのクラスター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 データは収集されません。

用語

Data Infrastructure Insights は、このデータ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ホスト	ホスト
ホストボリュームマッピング	ホストボリュームマッピング
ハードウェア（「extra_details」オブジェクトの下にドライブがあります）: ドライブ	ディスク
アプライアンス	ストレージプール

ベンダー/モデル用語	**Data Infrastructure Insights**用語
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
音量	Volume
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マッピングのみであり、このデータ コレクターのすべてのケースを反映しているわけではありません。

要件

このデータ コレクターを構成するには、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ー名とパスワード

構成

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
ユーザー名	PowerStoreのユーザー名
パスワード	PowerStoreで使用するパスワード

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 ポーリングの間隔。デフォルトは60分です。

Cloud Insight の PowerStore パフォーマンス収集では、PowerStore の 5 分単位のソース データが使用されます。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が、これは構成できません。

トラブルシューティング

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

Dell EMC RecoverPointデータコレクター

EMC RecoverPoint データ コレクターの主な使用例は、RecoverPoint ストレージ アプライアンスによって実現されるボリューム間のレプリケーション関係を検出することで

す。このコレクターは、Recoverpoint アプライアンス自体も検出します。 Dell/EMC はVMwareのVMwareバックアップソリューション「RecoverPoint for VMs」を販売していますが、このコレクターではサポートされていません。

構成の場合、データ コレクターには、ストレージ プロセッサの IP アドレスと読み取り専用のユーザー名とパスワードが必要です。

EMC RecoverPoint データ コレクターは、RecoverPoint が他のストレージ アレイ間で調整するボリューム間のレプリケーション関係を収集します。 Data Infrastructure Insights は、各 RecoverPoint クラスターのストレージ アレイを表示し、そのクラスター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 データは収集されません。

要件

このデータ コレクターを構成するには、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ー名とパスワード
- ポート443経由のREST APIアクセス

構成

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
ユーザー名	RecoverPointクラスタのユーザー名
パスワード	RecoverPointクラスタに使用されるパスワード

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される TCP ポート
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。デフォルトは20分です。
除外されたクラスター	ポーリング時に除外するクラスター ID または名前のコンマ区切りリスト。

トラブルシューティング

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

DELL EMC ScaleIO / PowerFlex データコレクター

ScaleIO/PowerFlex データ コレクターは、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 コレクターを構成するに

は、ScaleIO/PowerFlex ゲートウェイ アドレスと管理者のユーザー名とパスワードが必要です。

用語

Data Infrastructure Insights は、 ScaleIO/PowerFlex データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
MDM（メタデータマネージャー）クラスター	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
Volume	Volume
デバイス	ディスク

注: 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 コレクターのすべてのケースを反映しているわけではありません。

要件

- 管理者ユーザー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

構成

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 (;) で区切る）
ユーザー名	ScaleIO/PowerFlexデバイスにログインするために使用される管理者ユーザー名
パスワード	ScaleIO/PowerFlexデバイスにログインするために使用するパスワード

高度な設定

インベントリ収集を有効にするには、[インベントリ] チェックボックスをクリックします。

フィールド	説明
HTTPS ポート	443
インベントリポーリング間隔（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。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

EMC Unityデータコレクターの構成

DELL EMC Unity (旧称 VNXe) データ コレクターは、VNXe 統合ストレージ 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 および NAS プロトコルをサポートしています。

要件

- Unity データ コレクターは CLI ベースです。VNXe データ コレクターが存在する取得ユニットに Unisphere for Unity CLI (uemcli.exe) をインストールする必要があります。
- uemcli.exe はトランスポート プロトコルとして HTTPS を使用するため、取得ユニットは 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 コレクターが使用するには、少なくとも読み取り専用ユーザーが必要です。
- ポート443のHTTPSが必要です
- EMC Unity データ コレクターは、インベントリに NAS および iSCSI サポートを提供します。ファイバー 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、またはストレージ ポートを報告しません。

用語

Data Infrastructure Insights は、 Unity データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ディスク	ディスク
ストレージ アレイ	ストレージ
プロセッサ	ストレージ ノード
ストレージ プール	ストレージ プール
一般的な iSCSI ブロック情報、VMware VMFS	共有
レプリケーションリモートシステム	同期
iSCSIノード	iSCSIターゲットノード
iSCSI Initiator	iSCSI ターゲット イニシエーター

注: 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 ソースのすべてのケースを反映しているわけではありません。

構成

フィールド	説明
ユニティストレージ	UnityデバイスのIPアドレスまたは完全修飾ドメイン名
ユーザー名	Unityデバイスのユーザー名
パスワード	Unityデバイスのパスワード
実行可能ファイル UEMCLI へのフルパス	*uemcli.exe* 実行ファイルを含むフォルダーへのフルパス

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 ポーリングの間隔。デフォルトは40分です
Unity CLI ポート	Unity CLI で使用されるポート
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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
「外部ユーティリティの実行に失敗しました」というエラー メッセージが表示され、「Unisphere 実行可能ファイル uemcli が見つかりませんでした」というエラー メッセージが表示される	* IP アドレス、ユーザー名、およびパスワードが正しいことを確認します。 * 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 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 から CMD を開き、構成されたインストール ディレクトリ ${INSTALLDIR.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

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Dell EMC VMAXおよび**PowerMax**デバイスファミリーのデータコレクター

Data Infrastructure Insights は、環境内の既存の Solutions Enabler サーバーと組み合わせて Solutions Enabler symcli コマンドを使用することで、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 サーバーは、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 コレクターを構成する前に、 Data Infrastructure Insights が既存の Solutions Enabler サーバー上のポート 2707 に TCP 接続できることを確認する必要があります。 Data Infrastructure Insights は、そのサーバーからの「symcfg list」出力に表示される、このサーバーに「ローカル」であるすべての Symmetrix アレイを検出します。

- SMI-S プロバイダー アプリケーションを備えた EMC Solutions Enabler (CLI) は、Acquisition Unit サーバーにインストールする必要があり、そのバージョンは Solutions Enabler サーバーで実行されているバージョンと一致するか、それより前である必要があります。
- 適切に構成された {installdir}\EMC\SYMAPI\config\netcnfg ファイルが必要です。このファイルは、Solutions Enabler サーバー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/書き込みの遅延が必要な場合、SMI-S プロバイダーは、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。
- 管理ソリューション イネーブラ サーバーの IP アドレス
- Solutions Enabler (SE) サーバーの管理者権限
- SEソフトウェアへの読み取り専用ユーザー名とパスワード
- UNISPHERE for VMAXアプリケーションが実行され、SMI-Sプロバイダーのインストールによって管理されるEMC VMAXおよびPowerMaxストレージアレイの統計情報を収集する必要があります。
- パフォーマンスのアクセス検証: 取得ユニットの Web ブラウザーで、*https://<SMI-S* ホスト名または *IP>:5989/ecomconfig* にアクセスします。ここで、「SMI-S ホスト名または IP」は SMI-S サーバーの IP アドレスまたはホスト名です。この URL は、EMC SMI-S (別名「ECOM」) サービスの管理ポータル用です。ログイン ポップアップが表示されます。
- 権限は、Solutions Enabler サーバーのデーモン構成ファイルで宣言する必要があります。このファイルは通常、次の場所にあります: */var/symapi/config/daemon_users*

  適切な cisys 権限を持つファイルの例を次に示します。

```
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

Data Infrastructure Insights 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。取得した資産の種類ごとに、その資産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

クターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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
監督	ストレージ ノード
デバイス プール、ストレージ リソース プール (SRP)	ストレージ プール
デバイスTDev	Volume

注: 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 コレクターのすべてのケースを反映しているわけではありません。

構成

注**:** SMI-S ユーザー認証が有効になっていない場合、 Data Infrastructure Insightsデータ コレクター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* ファイルに指定されたサービス名
CLIへのフルパス	Symmetrix CLI を含むフォルダへのフルパス
SMI-Sホスト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 ポーリングの間隔。デフォルトは40分です。
リストを指定するには「除外」または「含める」を選択します	データを収集するときに、以下の配列リストを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ーデバイスリスト	含めるまたは除外するデバイス ID のコンマ区切りリスト

フィールド	説明
接続キャッシュ	接続キャッシュ方法を選択します: * LOCAL は、Cloud Insights Acquisition サービスが Solutions Enabler サーバー上で実行されており、検出対象の Symmetrix アレイへのファイバー チャネル接続があり、ゲートキーパー ボリュームにアクセスできることを意味します。これは、一部のリモート取得ユニット (RAU) 構成で発生する可能性があります。 * REMOTE_CACHED はデフォルトであり、ほとんどの場合に使用する必要があります。これには、NETCNFG ファイル設定を使用して、IP を使用して Solutions Enabler サーバーに接続します。このサーバーは、検出対象の Symmetrix アレイへのファイバ チャネル接続を持ち、Gatekeeper ボリュームにアクセスできる必要があります。 * REMOTE_CACHED オプションにより 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。取得プロセスが遅くなることに注意してください (極端な場合には数時間または数日かかる可能性があります)。 NETCNFG ファイル設定は、検出対象の Symmetrix アレイへのファイバー チャネル接続を持つ Solutions Enabler サーバーへの IP 接続に引き続き使用されます。 注: この設定では、「symcfg list」出力で REMOTE としてリストされているアレイに関するData Infrastructure Insights の動作は変更されません。 Data Infrastructure Insights は、このコマンドによって LOCAL として表示されるデバイス上でのみデータを収集します。
SMI-Sプロトコル	SMI-S プロバイダーに接続するために使用されるプロトコル。使用されるデフォルトのポートも表示します。
SMISポートの上書き	空白の場合は、接続タイプフィールドの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プロバイダーホストのユーザー名
SMI-Sパスワード	SMI-Sプロバイダーホストのユーザー名
パフォーマンスポーリング間隔（秒）	パフォーマンスポーリングの間隔（デフォルトは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	パフォーマンスデータを収集するときに、以下のアレイリストを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ーデバイスリスト	含めるまたは除外するデバイス ID のコンマ区切りリスト

トラブルシューティング

このデータ コレクターで問題が発生した場合に試すことができるいくつかのこと:

問題：	これを試してください:
エラー: 要求された機能は現在ライセンスされていません	SYMAPI サーバー 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	Symmetrix デバイスが Solutions Enabler サーバー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。 - 構成されている Symmetrix デバイスのリストを表示するには、symcfg list -v を実行します。
エラー: 要求されたネットワーク サービスがサービス ファイルに見つかりません	Solutions Enabler の netcnfg ファイルで Solutions Enabler サービス名が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 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/サーバー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 ホスト上の最新の 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 サーバー上の *hosts* ファイルを編集して、Acquisition Unit のホスト名が Solutions Enabler サーバー上の storsrvd.log に報告されている IP アドレスに解決されるようにします。
エラー: 関数はメモリを取得できませんでした	Solutions Enablerを実行するためにシステムに十分な空きメモリが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の健全性状態と負荷プロファイルを調査する
エラー: • Solutions Enabler サーバー 8.x から Solutions Enabler 7.x を使用して収集した場合、「symcfg list -tdev」CLI コマンドは誤ったデータを返す場合があります。 • Solutions Enabler 8.3 以降から Solutions Enabler 8.1.0 以前を使用して収集された場合、「symcfg list -srp」 CLI コマンドは誤ったデータを返すことがあります。	同じSolutions Enablerメジャーリリースを使用していることを確認してください
「不明なコード」というメッセージとともにデータ収集エラーが表示されます	Solutions Enablerサーバー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、このメッセージが表示されることがあります（要件その上。）これは、SE クライアントのバージョンが SE サーバー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、*cisys* ユーザー (Solutions Enabler コマンドを実行する) に /var/symapi/config/daemon_users 構成ファイルで必要なデーモン権限が設定されていない場合にも発生する可能性があります。これを修正するには、/var/symapi/config/daemon_users ファイルを編集し、cisys ユーザーに 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/daemon_users … cisys storapid <all>

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Dell EMC VNX ブロック ストレージ (NaviCLI) データ コレクター

Data Infrastructure Insights は、 Dell EMC VNX Block Storage (NaviSec) データ コレク

ター (旧 CLARiiON) を使用して、インベントリとパフォーマンス データを取得します。

用語

Data Infrastructure Insights は、 EMC VNX ブロック ストレージ データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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	Volume

注: 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 ソースのすべてのケースを反映しているわけではありません。

要件

データを収集するには、次の要件を満たす必要があります。

- 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への読み取り専用のNavisphereユーザー名とパスワード
- NaviSecCliはData Infrastructure Insights AUにインストールする必要があります
- アクセス検証: 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。
- パフォーマンスを確保するには、統計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ーフェース構文

naviseccli.exe -h <IPアドレス> -user <ユーザー> -password <パスワード> -scope <スコープ、グローバルスコープの場合は0を使用> -port <デフォルトでは443を使用> コマンド

構成

フィールド	説明
VNX ブロック ストレージ 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
ユーザー名	VNX ブロック ストレージ デバイスにログインするために使用される名前。

フィールド	説明
パスワード	VNX ブロック ストレージ デバイスにログインするために使用されるパスワード。
naviseccli.exe への CLI パス	*naviseccli.exe* 実行ファイルを含むフォルダへのフルパス

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 ポーリングの間隔。デフォルトは40分です。
Scope	安全なクライアントスコープ。デフォルトはグローバルです。
パフォーマンスポーリング間隔（秒）	パフォーマンス ポーリングの間隔。デフォルトは300秒です。

トラブルシューティング

このデータ コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
エラー： • エージェントが実行されていません • naviseccli が見つかりませんでした • コマンドの実行に失敗しました	• NaviSphere CLIがCloud Insight Acquisition Unitにインストールされていることを確認します。 • データ コレクター構成ウィザードで「セキュア クライアントを使用する」オプションを選択しておらず、Naviphere CLI の非セキュア バージョン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します。 • データ コレクター構成で 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取得ユニットより: ◦ CMDを開きます。 ◦ 設定され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みます（{ip}を実際のIPに置き換えてください）。

問題：	これを試してください:
エラー: 4.29 emc235848 emc241018 getall ホストエイリアス情報の解析に失敗しました	これは、アレイ自体のホスト イニシエーター データベースの FLARE 29 破損問題によって発生したものと考えられます。 EMC ナレッジベースの記事 emc235848、emc241018 を参照してください。確認することもできます https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128
エラー: メタ 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ーの構成を変更します (推奨) • navicli.exe または naviseccli.exe の CLI パスに navicli.jar をインストールします。 • 注意: navicli.jar は EMC Navisphere バージョン 6.26 以降では非推奨です。 • navicli.jarは\http://powerlink.emc.comで入手できるかもしれない。
エラー: ストレージ プールが、構成された IP アドレスのサービス プロセッサ上のディスクを報告していません	両方のサービスプロセッサIPをコンマで区切ってデータコレクターを構成します。
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を更新したが、NaviCLI.exe のインストールを更新していないために発生します。これは、異なるファームウェアを搭載したさまざまなデバイスがあるにもかかわらず、(異なるファームウェア バージョンを備えた) 1 つの CLI のみがインストールされていることが原因である可能性もあります。 • 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取得ユニットからコマンドラインウィンドウを開きます ◦ 設定され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CLARiiONデバイスに接続します。 ◦ 最初の数行のバージョン番号を探します。例:「エージェント Rev: 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 リビジョン 6.07.00.04.07」

問題：	これを試してください:
エラー: サポートされていない構成 - ファイバーチャネルポートがありません	デバイスにはファイバー チャネル ポートが構成されていません。現在、FC 構成のみがサポートされています。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。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

DELL EMC VNX File（旧Celerra Unified Storage System）データコレクター

このデータ コレクターは、VNX ファイル ストレージ システムからインベントリ情報を取得します。このデータ コレクターを構成するには、ストレージ プロセッサの IP アドレスと読み取り専用のユーザー名とパスワードが必要です。

用語

Data Infrastructure Insights は、 VNX ファイル データ コレクターから次のインベントリ情報を取得します。Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
Celerra ネットワーク サーバ/Celerra ストレージ プール	ストレージ プール
ファイルシステム	内部容積
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マッピングのみであり、このデータ コレクターのすべてのケースを反映しているわけではありません。

要件

このデータ コレクターを構成するには、次のものが必要です。

- 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ー名とパスワード
- SSH、ポート22

構成

フィールド	説明
VNXファイルのIPアドレス	VNX ファイル デバイスの IP アドレスまたは完全修飾ドメイン名
ユーザー名	VNXファイルデバイスにログインするために使用する名前
パスワード	VNXファイルデバイスにログインするために使用するパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。デフォルトは20分です。

トラブルシューティング

このデータ コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
エラー: DART の更新中は続行できません	考えられる解決策: データ コレクターを一時停止し、DART アップグレードが完了するまで待ってから、別の取得要求を試行します。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Dell EMC VNX 統合データコレクターの構成

構成には、Dell EMC VNX Unified (SSH) データ コレクターに、コントロール ステーションの IP アドレスと読み取り専用のユーザー名とパスワードが必要です。

用語

Data Infrastructure Insights は、このデータ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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	内部容積
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

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ストレージプール、RAIDグループ	ストレージ プール
LUN	Volume
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 コレクターを構成するには、次のものが必要です。

- Celerra コントロール ステーションへの VNX IP アドレスと資格情報。
- 読み取り専用のユーザー名とパスワード。
- データコレクターは、DART OS NASヘッドを利用して、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。

構成

フィールド	説明
VNX IPアドレス	VNXコントロールステーションのIPアドレスまたは完全修飾ドメイン名
ユーザー名	VNXコントロールステーションのユーザー名
パスワード	VNXコントロールステーションのパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。デフォルトは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 ポーリングの間隔。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ーに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

EMC VPLEXデータコレクターの構成

このデータ コレクターは、EMC VPLEX ストレージ システム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。データ コレクターを構成するには、VPLEX サーバーの IP アドレスと管理レベルのドメイン アカウントが必要です。

Data Infrastructure Insightsによる Vplex クラスターからのパフォーマンス収集では、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 ファイルとログを入力するために、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。NetApp は、多くの Vplex ファームウェア アップグレード/管理ステーションの更新によってこの機能が動作しなくなることを確認しました。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使用できなくなるかどうか、またそうなる場合は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この機能を再度有効にできるかを Dell/EMC に事前に問い合わせることをお勧めします。 Cloud Insight の Vplex パフォーマンス コードは、各ポーリングで、予想されるすべてのファイルが存在するかどうか、およびそれらが適切に更新されているかどうかを評価します。ファイルが欠落しているか古くなっている場合、 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

Data Infrastructure Insights は、VPLEX データ コレクターから次のインベントリ情報を取得します。取得した資産の種類ごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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、システム範囲	バックエンドストレージプール
仮想ボリューム	Volume
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
ストレージ容量	バックエンドLUN
ITL	バックエンドパス

注: 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 コレクターのすべてのケースを反映しているわけではありません。

要件

- VPLEX管理コンソールのIPアドレス
- VPLEX サーバーの管理レベル 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 への送信接続が必要です。
- パフォーマンス上の理由から、ssh/scp アクセス用の読み取り専用のユーザー名とパスワード。
- パフォーマンスのためにはポート 22 が必要です。

構成

フィールド	説明
VPLEX管理コンソールのIPアドレス	VPLEX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
ユーザー名	VPLEX CLIのユーザー名
パスワード	VPLEX CLI で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管理コンソールのパフォーマンスリモートIPアドレス
パフォーマンスリモートユーザー名	VPLEX管理コンソールのパフォーマンスリモートユーザー名
パフォーマンスリモートパスワード	VPLEX管理コンソールのパフォーマンスリモートパスワード

高度な設定

フィールド	説明
通信ポート	VPLEX CLI に使用されるポート。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 ポーリングの間隔。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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
エラー: ユーザー認証に失敗しました。	このデバイスの資格情報が正しいことを確認してください。

パフォーマンス

問題：	これを試してください:
エラー: バージョン 5.3 未満の 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する
エラー: 十分なデータが収集されませんでした。	• 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。• より長い時間待機します。
エラー: 永続ログ ファイルが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。

問題：	これを試してください:
エラー: パフォーマンス 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ます。
エラー: VPLEX 管理コンソールのパフォーマンス リモート 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 管理コンソールのパフォーマンス リモート IP アドレスを設定します。
エラー: ディレクターからパフォーマンスデータが報告されません	• システムパフォーマンスモニターが正しく動作していることを確認してください。 • システムパフォーマンスモニターの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。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Dell EMC XtremeIO データコレクター

EMC XtremIO データ コレクターは、EMC XtremIO 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。

要件

EMC XtremIO (HTTP) データ コレクターを構成するには、次のものが必要です。

- XtremIO 管理サーバー (XMS) ホスト アドレス
- 管理者権限を持つアカウント
- ポート443（HTTPS）へのアクセス

用語

Data Infrastructure Insights は、 EMC XtremIO データ コレクターから次のインベントリ情報を取得します。Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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
Volume	Volume
LUN マップ	ボリュームマップ
ターゲットFCイニシエーター	ボリュームマスク

注: 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 ソースのすべてのケースを反映しているわけではありません。

要件

- XtremIO 管理サーバー (XMS) ホストの IP アドレス
- XtremIOの管理者ユーザー名とパスワード

構成

フィールド	説明
XMSホスト	XtremIO 管理サーバーの IP アドレスまたは完全修飾ドメイン名
ユーザ名	XtremIO管理サーバーのユーザー名
パスワード	XtremIO管理サーバーのパスワード

高度な設定

フィールド	説明
TCP ポート	XTremIO 管理サーバーに接続するために使用される TCP 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 ポーリングの間隔。デフォルトは60分です。
パフォーマンスポーリング間隔（秒）	パフォーマンス ポーリングの間隔。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ーに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

富士通 **Eternus** データコレクター

Fujitsu Eternus データ コレクターは、ストレージ システムへの管理レベルの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

Data Infrastructure Insights は、 Fujitsu Eternus ストレージから以下のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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、フレキシブルティアプール、レイドグループ	ストレージ プール

ベンダー/モデル用語	**Data Infrastructure Insights**用語
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 ティア ボリューム (FTV)、ワイド ストライピング ボリューム (WSV)	Volume
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マッピングのみであり、このデータ コレクターのすべてのケースを反映しているわけではありません。

要件

このデータ コレクターを構成するには、次のものが必要です。

- EternusストレージのIPアドレス（カンマ区切り不可）
- SSH 管理レベルのユーザー名とパスワード
- 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）

構成

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
ユーザー名	Eternusストレージのユーザー名
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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
「データ取得エラー」と「CLI プロンプト検索エラー」または「シェル結果の最後にプロンプト検索エラー」というエラー メッセージが表示される	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。考えられる解決策: * 次のコマンドを実行して、ページスクロールを無効にしてみてください: set clienv-show-more -scroll disable

問題：	これを試してください:
「接続エラー」と「ストレージへの SSH 接続のインスタンス化に失敗しました」または「VirtualCenter への接続のインスタンス化に失敗しました」というエラー メッセージが表示される	考えられる原因: * 資格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。 * ストレージがダウンしているか、応答しない可能性があります。考えられる解決策: * 入力した資格情報と IP アドレスを確認します。 * SSH クライアントを使用してストレージとの通信を試みます。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

NetApp Google Compute データコレクター

このデータ コレクターは、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。このコレクターは、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を使用して検出する Google 組織が複数ある場合は、組織ごとに 1 つのData Infrastructure Insightsコレクターをデプロイする必要があります。

サービスアカウントの要件

- 以下の手順に従ってサービスアカウントを作成する必要があります。"サービスアカウントの作成/管理" 。このようなサービス アカウントは、*clientId* と呼ばれる一意の ID によって識別され、ユーザー名として使用されます。
- さらに、以下の手順に従ってサービスアカウントキーを作成します。"サービス アカウント キーの作成/管理" 。このキーは json ファイルとしてダウンロードでき、その内容がパスワードとして使用されます。
- サービス アカウントのスコープは、*compute.readonly*、*monitoring.read*、および *cloud-platform* に設定する必要があります。

構成

フィールド	説明
組織ID	このコレクターで検出する組織 ID。サービスアカウントが複数の組織を参照できる場合、このフィールドは必須です
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に取り込まれるプロジェクトのリソースを制限する場合。
プロジェクトID	「除外を選択…」の値に応じて、検出対象としてフィルター処理するプロジェクト ID のリスト。デフォルトのリストは空です
クライアントID	Google Cloud Platform 構成のクライアント ID
Google認証情報ファイルの内容をコピーしてここに貼り付けます	Cloud Platform アカウントの Google 認証情報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
ラベルによるVMのフィルタリングを適用するには、「除外」または「含める」を選択します	データ収集時にラベルごとに VM を含めるか除外するかを指定します。 「含める」を選択した場合、ラベル キー フィールドを空にすることはできません。
VM をフィルタリングするためのラベルキーと値	+ フィルター ラベル をクリックし、VM 上のラベルのキーと値に一致するキーと値をフィルターして、含める/除外する VM (および関連ディスク) を選択します。ラベル キーは必須ですが、ラベル値はオプションです。ラベル値が空の場合、ラベル 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秒です

トラブルシューティング

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

Google Cloud NetApp Volumesデータコレクター

このデータ コレクターは、Google Cloud NetApp Volumes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。コレクターは、Google 組織内のすべてのプロジェクトにわたってNetAppボリュームとストレージ リソースを検出します。 Data Infrastructure Insightsを使用して監視する Google 組織が複数ある場合は、組織ごとに 1 つのコレクターをデプロイします。

サービスアカウントの要件

- 以下の手順に従ってサービスアカウントを作成する必要があります。"サービスアカウントの作成/管理" 。このサービス アカウントは、*clientId* と呼ばれる一意の ID によって識別され、ユーザー名として使用されます。
- さらに、以下の手順に従ってサービスアカウントキーを作成します。"サービス アカウント キーの作成/管理" 。このキーは json ファイルとしてダウンロードでき、その内容がパスワードとして使用されます。
- サービス アカウントのスコープは、*compute.readonly*、*monitoring.read*、および *cloud-platform* に設定する必要があります。

構成

フィールド	説明
組織ID	このコレクターで検出する組織 ID。サービスアカウントが複数の組織を参照できる場合、このフィールドは必須です

フィールド	説明
GCNV資産を場所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	このコレクターはデフォルトで組織内の世界中のすべての GCNV ボリュームを検出することを目的としているため、デフォルトでは除外に設定されています。
GCNV 除外/含める場所	デフォルトでは空になっており、「除外」または「含める」オプションを選択するときに使用されます。特定のリージョン内のアセットのみを検出する場合は、これら 2 つのオプションを使用してこのコレクターの範囲を制限します。
プロジェクトID	「除外を選択…」の値に応じて、検出対象としてフィルター処理するプロジェクト ID のリスト。デフォルトのリストは空です
クライアントID	Google Cloud Platform 構成のクライアント ID
Google認証情報ファイルの内容をコピーしてここに貼り付けます	Cloud Platform アカウントの Google 認証情報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
REST API呼び出しにAUプロキシを使用する	コレクターが、コレクターが存在する取得ユニットと同じプロキシを使用するようにするには、このオプションを選択します。デフォルトでは無効になっており、コレクターは HTTPS API 呼び出しを Google に直接送信しようとします。
VM をフィルタリングするためのラベルキーと値	+ フィルター ラベル をクリックし、VM 上のラベルのキーと値に一致するキーと値をフィルターして、含める/除外する VM (および関連ディスク) を選択します。ラベル キーは必須ですが、ラベル値はオプションです。ラベル値が空の場合、ラベル 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300秒です

トラブルシューティング

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

HPエンタープライズ

HP Enterprise Alletra 9000 / Primera ストレージデータコレクター

Data Infrastructure Insights は、 HP Enterprise Alletra 9000 / HP Enterprise Primera (旧称 3PAR) データ コレクターを使用して、インベントリとパフォーマンスを検出します。

用語

Data Infrastructure Insights は、このデータ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

フィールド	説明
物理ディスク	ディスク
Storage System	ストレージ
コントローラーノード	ストレージ ノード
共通プロビジョニンググループ	ストレージ プール
仮想ボリューム	Volume

注: 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 コレクターのすべてのケースを反映しているわけではありません。

要件

このデータ コレクターを構成するには、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、StoreServサーバーの読み取り専用ユーザー名とパスワード
- パフォーマンスのために、StoreServサーバーへのユーザー名とパスワードの読み取り/書き込み
- ポート要件: 22 (インベントリ収集)、5988 または 5989 (パフォーマンス収集) [注: パフォーマンスは StoreServ OS 3.x 以降でサポートされます]
- パフォーマンス収集の場合は、SSH 経由でアレイにログインして SMI-S が有効になっていることを確認します。

構成

フィールド	説明
ストレージIPアドレス	StoreServ クラスターのストレージ IP アドレスまたは完全修飾ドメイン名
ユーザー名	StoreServサーバーのユーザー名
パスワード	StoreServサーバーで使用するパスワード
SMI-Sユーザー名	SMI-Sプロバイダーホストのユーザー名
SMI-Sパスワード	SMI-Sプロバイダーホストに使用するパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。デフォルトは40分です。

フィールド	説明
SMI-S接続	SMI-Sプロバイダーへの接続に使用されるプロトコル
SMI-Sデフォルトポートを上書きする	空白の場合は、SMI-S接続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。
パフォーマンスポーリング間隔（秒）	パフォーマンス ポーリングの間隔。デフォルトは300秒です。

トラブルシューティング

このデータ コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
「showsys」コマンドは結果を返しません。	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：	これを試してください:
接続またはログインに失敗しました。プロバイダーの初期化に失敗しました。	すべて数字のアレイ名を使用すると、SMI-S サーバーで問題が発生する可能性があります。アレイ名を変更してみてください。
構成されたSMI-Sユーザーにはドメインがありません	構成されたSMI-Sユーザーに適切なドメイン権限を付与します
Data Infrastructure Insights、 SMI-S サービスに接続/ログインできないと表示されます。	CI AU とアレイの間に、CI AU が 5988 または 5989 に TCP 接続するの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。それが完了し、ファイアウォールがないことを確認したら、アレイに SSH で接続し、「showcim」コマンドを使用して確認する必要があります。次の点を確認してください: * サービスが有効になっている * HTTPS が有効になっている * HTTPS ポートは 5989 である必要があります。これらすべてが正しい場合は、「stopcim」を実行してから「startcim」を実行して CIM (つまり SMI-S サービス) を再起動してみてください。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

HP Enterprise Command View データコレクター

HP Enterprise Command View Advanced Edition データ コレクターは、Command View Advanced Edition (CVAE) サーバー経由で XP および P9500 アレイの検出をサポートします。 Data Infrastructure Insights は、標準の Command View API を使用して CVAE と通信し、インベントリとパフォーマンス データを収集します。

用語

Data Infrastructure Insights は、 HP Enterprise Command View データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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
ポートコントローラー	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）	Volume

注: 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 コレクターのすべてのケースを反映しているわけではありません。

在庫要件

インベントリ データを収集するには、次のものが必要です。

- CVAEサーバーのIPアドレス
- CVAE ソフトウェアおよびピア権限の読み取り専用ユーザー名とパスワード
- 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、次の要件を満たす必要があります。

- HDS USP、USP V、およびVSPのパフォーマンス
  - パフォーマンス モニターのライセンスが必要です。
  - 監視スイッチを有効にする必要があります。
  - エクスポート ツール (Export.exe) をData Infrastructure Insights AU にコピーし、特定の場所に抽出する必要があります。 CI Linux AU では、「cisys」に読み取り権限と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は、ターゲット アレイのマイクロコード バージョンと一致する必要があります。
- AMS パフォーマンス:
  - パフォーマンス モニター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ます。
- 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 を使用して配列と通信します。これらのツールは、

呼び出しごとに送信元および宛先 TCP ポートを動的にネゴシエートする可能性があるため、ファイアウォール対応ではない可能性があります。また、異なるモデルアレイのエクスポートツールはネットワーク上で異なる動作をする場合があります。モデルの要件についてはHPEにお問い合わせください。

構成

フィールド	説明
コマンドビューサーバー	Command View サーバーの IP アドレスまたは完全修飾ドメイン名
ユーザー名	Command View サーバーのユーザー名。
パスワード	Command View サーバーに使用されるパスワード。
デバイス - VSP G1000 (R800)、VSP (R700)、HUS VM (HM700)、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。各ストレージには次の情報が必要です: * 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。各ストレージには次の情報が必要です: * アレイのIP: ストレージのIPアドレス * ストレージナビゲータCLIパス: SNM2 CLIパス * アカウント認証有効: 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
パフォーマンスのためにチューニングマネージャーを選択する	他のパフォーマンスオプションを上書きする
チューニングマネージャーホスト	チューニングマネージャーのIPアドレスまたは完全修飾ドメイン名
チューニングマネージャーポート	チューニングマネージャーで使用されるポート
チューニングマネージャーのユーザー名	チューニングマネージャーのユーザー名
チューニングマネージャーのパスワード	チューニングマネージャーのパスワード

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
コマンドビューサーバーポート	Command View Server で使用されるポート
HTTPS 有効	HTTPSを有効にするには選択してください
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。デフォルトは 40 です。
リストを指定するには「除外」または「含める」を選択します	データを収集するときに、以下の配列リストを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	含めるまたは除外するデバイス ID またはアレイ名のコンマ区切りリスト
クエリホストマネージャー	ホストマネージャを照会するには選択してください
パフォーマンスポーリング間隔（秒）	パフォーマンス ポーリングの間隔。デフォルトは 300 です。

トラブルシューティング

このデータ コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
エラー: ユーザーに十分な権限がありません	より高い権限を持つ別のユーザー アカウントを使用するか、データ コレクターで構成されているユーザー 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、ユーザーに十分な権限がありません	* DeviceManager を使用して、デバイスが構成されているかどうかを確認します。 * より高い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ます
エラー: HDS ストレージ アレイが数日間更新されていません	HP CommandView AE でこのアレイが更新されない理由を調査します。

パフォーマンス

問題：	これを試してください:
エラー: * エクスポート ユーティリティの実行エラー * 外部コマンドの実行エラー	*Data Infrastructure Insightsアクイジション ユニットにエクスポート ユーティリティがインストールされていることを確認します。 * データ コレクター構成でエクスポート ユーティリティの場所が正しいことを確認します。 * データ コレクター構成で USP/R600 アレイの IP が正しいことを確認します。 * データ コレクター構成でユーザー名とパスワードが正しいことを確認します。 * エクスポート ユーティリティのバージョンがストレージ 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します。 *Data Infrastructure Insightsアクイジション ユニットから、CMD プロンプトを開き、次の操作を行います。 - ディレクトリを構成されたインストール ディレクトリに変更します。 - バッチ ファイル runWin.bat を実行して、構成されたストレージ アレイとの接続を試みます。
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 * このHDSデータコレクター専用のユーザーIDを作成します * このアレイを取得するために他のデータコレクターが設定されていないことを確認します

問題：	これを試してください:
エラー: エクスポート ツールで「監視の時間範囲を取得できません」というログが記録されました。	* 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ます。
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、「フィルター デバイス リスト」を使用します。
エラー: * 外部コマンドの実行エラー * 構成エラー: ストレージアレイがインベントリによって報告されません * 構成エラー: 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 Command View サーバーで構成されているかどうかを確認します。 * パフォーマンス ポーリング間隔を 60 秒の倍数に設定します。
エラー: * Storage navigator CLI エラー * auperform コマンド実行エラー * 外部コマンド実行エラー	* Storage Navigator Modular 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 コレクター構成で、Storage Navigator Modular CLI の場所が正しいことを確認します。 * データ コレクターの構成で、WMS/SMS/SMS アレイの IP が正しいことを確認します。 * Storage Navigator Modular CLI のバージョンが、データ コレクターで構成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します。 * Data Infrastructure Insights Acquisition Unit から、CMD プロンプトを開き、次の操作を行います。 - ディレクトリを構成されたインストール ディレクトリに変更します。 - 次のコマンド「auunitref.exe」を実行して、構成されたストレージ アレイとの接続を試みます。
エラー: 構成エラー: ストレージアレイがインベントリによって報告されません	問題のストレージアレイがCommand Viewサーバーで構成されているかどうかを確認します。
エラー: * Storage Navigator Modular 2 CLI にアレイが登録されていません * 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、構成されたパスにディレクトリを変更します。 * コマンド「set=STONAVM_HOME=」を実行します。 * コマンド「auunitref」を実行します。 * コマンド出力に IP を含む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、Storage Navigator CLI を使用してアレイを登録します。 - コマンド プロンプトを開き、構成されたパスにディレクトリを変更します。 - コマンド「set=STONAVM_HOME=」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に置き換えます

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

HPE Alletra 6000 データコレクター

HP Enterprise Alletra 6000 (旧 Nimble) データ コレクターは、Alletra 6000 ストレージ ア

レイのインベントリおよびパフォーマンス データをサポートします。

用語

Data Infrastructure Insights は、このコレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
アレイ	ストレージ
ディスク	ディスク
Volume	Volume
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マッピングのみであり、このデータ コレクターのすべてのケースを反映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および構成データを収集するには、次のものが必要です。

- アレイはインストールおよび構成されており、完全修飾ドメイン名 (FQDN) またはアレイ管理 IP アドレスを通じてクライアントからアクセスできる必要があります。
- アレイでは NimbleOS 2.3.x 以降が実行されている必要があります。
- 少なくとも「オペレータ」レベルのロールを持つアレイへの有効なユーザー名とパスワードが必要です。「ゲスト」ロールには、イニシエーターの構成を理解するための十分なアクセス権がありません。
- アレイ上でポート 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、次のものが必要です。

- アレイは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構成されている必要があります。 NimbleOS が持つ唯一のパフォーマンス API はボリューム用であり、統計Data Infrastructure Insightsレポートはボリュームの統計から派生します。

構成

フィールド	説明
アレイ管理IPアドレス	完全修飾ドメイン名 (FQDN) またはアレイ管理 IP アドレス。
ユーザー名	アレイのユーザー名
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 で使用されるポート。デフォルトは 5392 です。
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。デフォルトは60分です。

注: デフォルトのパフォーマンス ポーリング間隔は 300 秒であり、変更することはできません。これは、HPE Alletra 6000 でサポートされている唯一の間隔です。

日立データシステムズ

日立ヴァンタラコマンドスイートデータコレクター

Hitachi Vantara Command Suite データ コレクターは、HiCommand Device Manager サーバーをサポートします。 Data Infrastructure Insights は、標準の HiCommand API を使用して HiCommand Device Manager サーバーと通信します。

用語

Data Infrastructure Insights は、 Hitachi Vantara Command Suite データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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
ポートコントローラー	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）	Volume

注: 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 コレクターのすべてのケースを反映しているわけではありません。

ストレージ

以下の用語は、HDS ストレージ アセット ランディング ページに表示されるオブジェクトまたは参照に適用されます。これらの条件の多くは他のデータ収集者にも適用されます。

- 名前 – GetStorageArray XML API呼び出しを介してHDS HiCommandデバイスマネージャの「name」属性から直接取得されます。
- モデル - GetStorageArray XML API呼び出しを介してHDS HiCommandデバイスマネージャの「arrayType」属性から直接取得されます。

- ベンダー – HDS
- ファミリー - GetStorageArray XML API呼び出しを介してHDS HiCommandデバイスマネージャの「arrayFamily」属性から直接取得されます。
- IP – これはアレイの管理IPアドレスであり、アレイ上のすべてのIPアドレスの網羅的なリストではありません。
- 生の容量 – 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

以下の用語は、HDS ストレージ プール アセット ランディング ページに表示されるオブジェクトまたは参照に適用されます。これらの条件の多くは他のデータ収集者にも適用されます。

- タイプ: ここでの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（ジャーナリング、スナップショットなど）専用である場合
  - シンプロビジョニング - HDPプールの場合
  - レイド グループ – いくつかの理由により、これらは表示されない可能性があります。

    Data Infrastructure Insights は、いかなる犠牲を払ってでも容量の二重カウントを回避するという強い姿勢をとっています。 HDS では通常、ディスクから RAID グループを構築し、それらの RAID グループ上にプール 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 (多くの場合は HDP ですが、特殊目的の場合もあります) 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そのまま報告した場合、それらの生の容量の合計はディスクの合計を大幅に超過することになります。

  代わりに、 Data Infrastructure Insightsの HDS Command Suite データ コレクターは、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。この結果、 Data Infrastructure Insights がRaid グループをまったく報告しなくなる可能性があります。さらに、結果として得られる Raid グループには、 Data Infrastructure Insights WebUI には表示されないようにフラグが付けられますが、 Data Infrastructure Insightsデータ ウェアハウス (DWH) には流れ込みます。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事柄によって UI が乱雑になるのを避けることです。HDS アレイに 50 MB の空き容量がある RAID グループがある場合、その空き領域を意味のある結果に使用することはできない可能性があります。

- ノード - N/A（HDS プールは特定のノードに結び付けられていないため）
- 冗長性 - プールの RAID レベル。複数の RAID タイプで構成された HDP プールの場合は複数の値が存在する可能性があります
- 容量 % - データ使用量にプールが使用されている割合（使用済み GB とプールの合計論理 GB サイズ）
- オーバーコミット容量 - 「このプールの論理容量は、このパーセンテージでプールの論理容量を超える論理ボリュームの合計によって、このパーセンテージでオーバーサブスクライブされています」という派生値
- スナップショット - このプールのスナップショット使用のために予約されている容量を表示します

ストレージ ノード

次の用語は、HDS ストレージ ノード アセット ランディング ページに表示されるオブジェクトまたは参照に

適用されます。これらの条件の多くは他のデータ収集者にも適用されます。

- 名前 – モノリシック アレイ上のフロントエンド ディレクター (FED) またはチャネル アダプターの名前、またはモジュラー アレイ上のコントローラーの名前。特定のHDSアレイには2つ以上のストレージノードが含まれます
- ボリューム – ボリュームテーブルには、このストレージノードが所有するポートにマッピングされたボリュームが表示されます。

在庫要件

インベントリ データを収集するには、次のものが必要です。

- HiCommand Device Manager サーバーの IP アドレス
- HiCommand Device Manager ソフトウェアおよびピア権限の読み取り専用ユーザー名とパスワード
- ポート要件: 2001 (http) または 2443 (https)
- ユーザー名とパスワードを使用してHiCommandデバイスマネージャーソフトウェアにログインします。
- HiCommand Device Manager へのアクセスを確認します http://<HiCommand_Device_Manager_IP>:2001/service/StorageManager

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、次の要件を満たす必要があります。

- HDS USP、USP V、およびVSPのパフォーマンス
  - パフォーマンス モニターのライセンスが必要です。
  - 監視スイッチを有効にする必要があります。
  - 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は、ターゲット アレイのマイクロコード バージョンと一致する必要があります。
- AMS パフォーマンス:
  - NetApp、Data Infrastructure Insights がパフォーマンス データを取得するため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お勧めします。 Storage Navigator では、ユーザー アカウントがアレイに同時にログインできるのは 1 回のみです。 Data Infrastructure Insights が管理スクリプトまたは HiCommand と同じユーザー アカウントを使用すると、同時ログインできるユーザー アカウントが 1 つに制限されるため、 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可能性があります。
  - パフォーマンス モニターのライセンスが必要です。
  - Storage Navigator Modular 2 (SNM2) CLI ユーティリティをData Infrastructure Insights AU にインストールする必要があります。

構成

フィールド	説明
HiCommand サーバー	HiCommand Device Manager サーバーの IP アドレスまたは完全修飾ドメイン名

フィールド	説明
ユーザー名	HiCommand Device Manager サーバーのユーザー名。
パスワード	HiCommand Device Manager サーバーに使用されるパスワード。
デバイス - VSP G1000 (R800)、VSP (R700)、HUS VM (HM700)、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。各ストレージには次の情報が必要です: * 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。各ストレージには次の情報が必要です: * アレイのIP: ストレージのIPアドレス * ストレージナビゲータCLIパス: SNM2 CLIパス * アカウント認証有効: 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
パフォーマンスのためにチューニングマネージャーを選択する	他のパフォーマンスオプションを上書きする
チューニングマネージャーホスト	チューニングマネージャーのIPアドレスまたは完全修飾ドメイン名
チューニングマネージャーポートの上書き	空白の場合は、「パフォーマンスのためのチューニングマネージャの選択」フィールドのデフォルトのポートを使用します。それ以外の場合は、使用するポートを入力します。
チューニングマネージャーのユーザー名	チューニングマネージャーのユーザー名
チューニングマネージャーのパスワード	チューニングマネージャーのパスワード

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、デフォルトのポートも表示します
HiCommand サーバーポート	HiCommand デバイス マネージャーで使用されるポート
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。デフォルトは 40 です。
リストを指定するには「除外」または「含める」を選択します	データを収集するときに、以下の配列リストを含めるか除外するかを指定します。
フィルターデバイスリスト	含めるまたは除外するデバイスのシリアル番号のコンマ区切りリスト

パフォーマンスポーリング間隔（秒）	パフォーマンス ポーリングの間隔。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 ユーティリティのタイムアウト。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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
エラー: ユーザーに十分な権限がありません	より高い権限を持つ別のユーザー アカウントを使用するか、データ コレクターで構成されているユーザー 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、ユーザーに十分な権限がありません	* DeviceManager を使用して、デバイスが構成されているかどうかを確認します。 * より高い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ます
エラー: HDS ストレージ アレイが数日間更新されていません	このアレイが HDS HiCommand で更新されない理由を調査します。

パフォーマンス

問題：	これを試してください:
エラー: * エクスポート ユーティリティの実行エラー * 外部コマンドの実行エラー	*Data Infrastructure Insightsアクイジション ユニットにエクスポート ユーティリティがインストールされていることを確認します。 * データ コレクター構成でエクスポート ユーティリティの場所が正しいことを確認します。 * データ コレクター構成で USP/R600 アレイの IP が正しいことを確認します。 * データ コレクター構成でユーザー名とパスワードが正しいことを確認します。 * エクスポート ユーティリティのバージョンがストレージ 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します。 *Data Infrastructure Insightsアクイジション ユニットから、CMD プロンプトを開き、次の操作を行います。 - ディレクトリを構成されたインストール ディレクトリに変更します。 - バッチ ファイル runWin.bat を実行して、構成されたストレージ アレイとの接続を試みます。
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 * このHDSデータコレクター専用のユーザーIDを作成します * このアレイを取得するために他のデータコレクターが設定されていないことを確認します

問題：	これを試してください:
エラー: エクスポート ツールで「監視の時間範囲を取得できません」というログが記録されました。	* 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ます。
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、「フィルター デバイス リスト」を使用します。
エラー: * 外部コマンドの実行エラー * 構成エラー: ストレージアレイがインベントリによって報告されません * 構成エラー: 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 サーバーで構成されているかどうかを確認します。 * パフォーマンス ポーリング間隔を 60 秒の倍数に設定します。
エラー: * Storage navigator CLI エラー * auperform コマンド実行エラー * 外部コマンド実行エラー	* Storage Navigator Modular 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 コレクター構成で、Storage Navigator Modular CLI の場所が正しいことを確認します。 * データ コレクターの構成で、WMS/SMS/SMS アレイの IP が正しいことを確認します。 * Storage Navigator Modular CLI のバージョンが、データ コレクターで構成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します。 * Data Infrastructure Insights Acquisition Unit から、CMD プロンプトを開き、次の操作を行います。 - ディレクトリを構成されたインストール ディレクトリに変更します。 - 次のコマンド「auunitref.exe」を実行して、構成されたストレージ アレイとの接続を試みます。
エラー: 構成エラー: ストレージアレイがインベントリによって報告されません	問題のストレージアレイがHiCommandサーバーで構成されているかどうかを確認します
エラー: * Storage Navigator Modular 2 CLI にアレイが登録されていません * 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、構成されたパスにディレクトリを変更します。 * コマンド「set=STONAVM_HOME=」を実行します。 * コマンド「auunitref」を実行します。 * コマンド出力に IP を含む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、Storage Navigator CLI を使用してアレイを登録します。 - コマンド プロンプトを開き、構成されたパスにディレクトリを変更します。 - コマンド「set=STONAVM_HOME=」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。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Hitachi Vantara NASデータコレクターの構成

Hitachi Vantara NAS データ コレクターは、HDS NAS クラスターの検出をサポートするインベントリおよび構成データ コレクターです。 Data Infrastructure Insights は、 NFS

および CIFS 共有、ファイル システム (内部ボリューム)、およびスパン (ストレージ プール) の検出をサポートします。

用語

Data Infrastructure Insights は、 HNAS データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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	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	内部容積

注: 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 コレクターのすべてのケースを反映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
- ユーザー名とパスワード - 権限レベル: スーパーバイザー
- 注: このデータ コレクターは SSH ベースであるため、これをホストする AU は、HNAS 自体の TCP 22 またはクラスターが接続されているシステム管理ユニット (SMU) への SSH セッションを開始できる必要があります。

構成

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
ユーザー名	HNAS CLIのユーザー名
パスワード	HNAS CLI で使用するパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。デフォルトは30分です。

トラブルシューティング

このデータ コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
「接続エラー」と「シェル チャネルの設定エラー:」または「シェル チャネルを開くエラー」というエラー メッセージが表示される	ネットワーク接続の問題または SSH の設定ミスが原因である可能性があります。代替SSHクライアントで接続を確認する
「タイムアウト」または「データの取得エラー」、および「コマンド: XXX がタイムアウトしました。」というエラー メッセージが表示される。	* 別のSSHクライアントでコマンドを試す * タイムアウトを増やす
「接続エラー」または「ログイン資格情報が無効です」というエラー メッセージが表示され、「デバイスと通信できませんでした:」	* IPアドレスを確認する * ユーザー名とパスワードを確認する * 代替SSHクライアントで接続を確認する

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

日立オプスセンターデータコレクター

このデータ コレクターは、Hitachi Ops Center の統合アプリケーション 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およびパフォーマンス データにアクセスします。インベントリと容量の検出のために、Ops Center インストールには「Common Services」コンポーネントと「Administrator」コンポーネントの両方が含まれている必要があります。パフォーマンス収集には、「Analyzer」を追加で導入する必要があります。

用語

Data Infrastructure Insights は、このデータ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ストレージ システム	ストレージ
Volume	Volume
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（Thin、SNAP）
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
ホストグループ	ボリュームマッピングとマスキング

ベンダー/モデル用語	**Data Infrastructure Insights**用語
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マッピングのみであり、このデータ コレクターのすべてのケースを反映しているわけではありません。

在庫要件

インベントリ データを収集するには、次のものが必要です。

- 「共通サービス」コンポーネントをホストする Ops Center サーバーの IP アドレスまたはホスト名
- Ops Center コンポーネントをホストするすべてのサーバーに存在する root/sysadmin ユーザー アカウントとパスワード。 HDS は、Ops Center 10.8 以降まで、LDAP/SSO ユーザーによる使用のための REST API サポートを実装していませんでした。

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、次の要件を満たす必要があります。

HDS Ops Center「アナライザ」モジュールをインストールする必要があります。ストレージアレイはOps Center「アナライザ」モジュールにデータを供給する必要があります。

構成

フィールド	説明
日立オプスセンターIPアドレス	「共通サービス」コンポーネントをホストする Ops Center サーバーの IP アドレスまたは完全修飾ドメイン名
ユーザー名	Ops Center サーバーのユーザー名。
パスワード	Ops Center サーバーに使用されるパスワード。

高度な設定

フィールド	説明
接続タイプ	HTTPS（ポート443）がデフォルトです
TCPポートの上書き	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 ポーリングの間隔。デフォルトは 40 です。
リストを指定するには「除外」または「含める」を選択します	データを収集するときに、以下の配列リストを含めるか除外するかを指定します。
フィルターデバイスリスト	含めるまたは除外するデバイスのシリアル番号のコンマ区切りリスト
パフォーマンスポーリング間隔（秒）	パフォーマンス ポーリングの間隔。デフォルトは 300 です。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Infinidat InfiniBox データコレクター

Infinidat InfiniBox (HTTP) データ コレクターは、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されます。

用語

Data Infrastructure Insights は、 Infinidat InfiniBox データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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
Filesystem	内部容積
Filesystem	ファイル共有
ファイルシステムのエクスポート	共有

要件

このデータ コレクターを構成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
- 管理者のユーザーIDとパスワード
- REST API経由のポート443

構成

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
ユーザー名	InfiniBox管理ノードのユーザー名
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 サーバーに接続するために使用される TCP 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	インベントリ ポーリングの間隔。デフォルトは60分です。

トラブルシューティング

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

Huawei OceanStorデータコレクター

Data Infrastructure Insights は、 Huawei OceanStor (REST/HTTPS) データ コレクターを使用して、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

Data Infrastructure Insights は、 Huawei OceanStor から次のインベントリとパフォーマンス情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ストレージ プール	ストレージ プール
ファイルシステム	内部容積
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 イニシエーター (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 イニシエーター	iSCSI イニシエーターノード
ディスク	ディスク
LUN	Volume

要件

このデータ コレクターを構成するには、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ーにアクセスするための資格情報
- ポート8088が利用可能である必要があります

構成

フィールド	説明
OceanStorホストIPアドレス	OceanStorデバイスマネージャのIPアドレスまたは完全修飾ドメイン名

フィールド	説明
ユーザー名	OceanStorデバイスマネージャにログインするために使用する名前
パスワード	OceanStorデバイスマネージャにログインするため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 デバイス マネージャーに接続するために使用される 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 ポーリングの間隔。デフォルトは60分です。
パフォーマンス ポーリング間隔 (秒)。	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ーに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

IBM

IBM Cleversafe データコレクター

Data Infrastructure Insights は、このデータ コレクターを使用して、IBM Cleversafe ストレージ システムのインベントリとパフォーマンス データを検出します。

IBM Cleversafe は、管理対象ユニットに対して異なる Raw TB レートで計測されます。フォーマットされていないIBM Cleversafeの容量40TBごとに1として課金されます。"管理ユニット（MU）"。

用語

Data Infrastructure Insights は、 IBM Cleversafe データ コレクターから次のインベントリ情報を取得します。Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ストレージ プール	ストレージ プール
Container	内部容積
Container	ファイル共有
NFS 共有	共有

注: 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 コレクターのすべてのケースを反映している

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IPアドレス
- 管理者のユーザ名とパスワード
- ポート9440

構成

フィールド	説明
マネージャーのIP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	スーパーユーザーまたはシステム管理者の役割を持つユーザーアカウントのユーザー名
パスワード	スーパーユーザーまたはシステム管理者の役割を持つユーザーアカウントのパスワード

高度な設定

フィールド	説明
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。
HTTP接続タイムアウト（秒）	HTTP タイムアウト（秒単位）。

トラブルシューティング

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

IBM CS データコレクター

Data Infrastructure Insights は、このデータ コレクターを使用して、IBM CS ストレージ システムのインベントリとパフォーマンス データを検出します。

用語

Data Infrastructure Insights は、 IBM CS データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ストレージ プール	ストレージ プール
Container	内部容積
Container	ファイル共有
NFS 共有	共有

注: 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 コレクターのすべてのケースを反映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IPアドレス
- 管理者のユーザ名とパスワード
- ポート9440

構成

フィールド	説明
Prism外部IPアドレス	クラスタの外部データサービスIPアドレス
ユーザ名	管理者アカウントのユーザー名
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 アレイに接続するために使用される TCP ポート。デフォルトは 9440 です。
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。デフォルトは60分です。
パフォーマンスポーリング間隔(秒)	パフォーマンス ポーリングの間隔。デフォルトは300秒です。

トラブルシューティング

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

IBM System Storage DS8000 シリーズ データコレクター

IBM DS (CLI) データ コレクターは、DS6xxx および DS8xxx デバイスのインベントリおよびパフォーマンス データの取得をサポートします。

DS3xxx、DS4xxx、およびDS5xxxデバイスは、"NetApp Eシリーズデータコレクター" 。サポートされてい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

Data Infrastructure Insights は、 IBM DS データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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	Volume
ホスト FC イニシエーター (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マッピングのみであり、このデータ収集者のすべてのケースを反映しているわけではない可能性があります。

要件

このデータ コレクターを構成するには、次のものが必要です。

- 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ー名とパスワード
- Data Infrastructure Insights AU にインストールされているサードパーティ製ソフトウェア: IBM *dscli*
- アクセス検証: ユーザー名とパスワードを使用して_dscli_コマンドを実行します
- ポート要件: 80、443、および 1750

構成

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
ユーザー名	DS CLI のユーザー名
パスワード	DS CLI のパスワード
dscli 実行可能パス	*dscli* 実行可能ファイルへのフルパス

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 ポーリングの間隔 (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	インベントリ収集から除外するデバイスのシリアル番号のコンマ区切りリスト
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ータイプ	含める: リスト上のデバイスからのみ収集されたデータ。除外: これらのデバイスからのデータは収集されません

フィールド	説明
パフォーマンスフィルターデバイスリスト	パフォーマンス収集に含めるか除外するデバイス ID のコンマ区切りリスト

トラブルシューティング

このデータ コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
次のエラーが含まれています: CMUC00192E 、CMUC00191E、または CMUC00190E	* 入力した資格情報と IP アドレスを確認します。 * Web 管理コンソール https://<ip>:8452/DS8000/Console を介してアレイとの通信を試みます。 <ip> をデータ コレクターが設定した IP に置き換えます。
エラー: * プログラムを実行できません * コマンド実行エラー	*Data Infrastructure Insights取得ユニットから CMD を開きます。 * CLI のホーム ディレクトリ/ライブラリにある CLI.CFG ファイルを開き、プロパティ JAVA_INSTALL を確認して、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。 * 発行された CLI コマンドで指定された IBM ストレージ デバイスの IP アドレスを ping します。 * 上記のすべてがうまくいった場合は、CLIコマンドを手動で実行します

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

IBM SANボリュームコントローラデータコレクターの構成

IBM SAN ボリューム コントローラー (SVC) データ コレクターは、SSH を使用してインベントリとパフォーマンス 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。

サポートされているデバイスのリストには、SVC、v7000、v5000、v3700 などのモデルが含まれています。サポートされてい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

Data Infrastructure Insights は、 IBM SVC データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ドライブ	ディスク

ベンダー/モデル用語	**Data Infrastructure Insights**用語
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	Volume
Mディスク	バックエンドLUNとパス

注: 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 コレクターのすべてのケースを反映しているわけではありません。

在庫要件

- 各SVCクラスタのIPアドレス
- ポート22が利用可能
- 読み取り専用のユーザー名とパスワード

パフォーマンス要件

- SVC コンソールは、すべての SVC クラスターに必須であり、SVC 検出基盤パッケージに必要です。
- 資格情報には、クラスター 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場合にのみ管理アクセス レベルが必要です。
- SSHでSVCクラスターに接続し、次のコマンドを実行してデータ収集を有効にします: *svctask startstats -interval 1*

  注: または、SVC 管理ユーザー インターフェイスを使用してデータ収集を有効にします。

構成

フィールド	説明
クラスター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
インベントリユーザー名	SVC CLI のユーザー名
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 ポーリングの間隔。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 ポーリングの間隔。デフォルトは300秒です。
ダンプされた統計ファイルをクリーンアップするには	ダンプされた統計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選択します

トラブルシューティング

このデータ コレクターで問題が発生した場合に試すことができるいくつかのこと:

問題：	これを試してください:
エラー:「コマンドは構成ノードで実行されなかったため、開始できません。」	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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

問題：	これを試してください:
エラー:「コマンドは構成ノードで実行されなかったため、開始できません。」	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ーに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

IBM XIV/A9000 データコレクターの構成

IBM XIV および A9000 (CLI) データ コレクターは、XIV コマンド ライン インターフェースを使用してインベントリ データを収集し、パフォーマンス収集は、ポート 7778 で SMI-S プロバイダーを実行する XIV/A9000 アレイへの SMI-S 呼び出しによって実行されます。

用語

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ディスク	ディスク
Storage System	ストレージ
ストレージ プール	ストレージ プール
Volume	Volume

要件

このデータ コレクターを構成して使用するには、次の要件を満たす必要があります。

- ポート要件: TCP ポート 7778
- 読み取り専用のユーザー名とパスワード
- XIV CLIはAUにインストールする必要があります

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エージェント1.4以上
- アレイ上で実行される SMI-S 互換の CIMService。ほとんどの XIV アレイには、CIMServer がデフォルト

でインストールされています。

- CIMServer にユーザー ログインを提供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への完全な読み取りアクセス権が必要です。
- SMI-S 名前空間。デフォルトは root/ibm です。これは CIMServer で設定可能です。
- 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を作成する方法については、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

構成

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
ユーザー名	XIVストレージのユーザー名
パスワード	XIVストレージのパスワード
XIV CLI ディレクトリへのフルパス	XIV CLI を含むフォルダーへのフルパス
SMI-Sホスト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 ポーリングの間隔。デフォルトは40分です。
SMI-Sプロトコル	SMI-S プロバイダーに接続するために使用されるプロトコル。デフォルトのポートも表示します。
SMI-Sポートのオーバーライド	空白の場合は、接続タイプフィールドの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。
ユーザー名	SMI-Sプロバイダーホストのユーザー名
パスワード	SMI-Sプロバイダー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 ポーリングの間隔。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ーに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

Lenovoデータコレクター

Data Infrastructure Insights は、 Lenovo データ コレクターを使用して、Lenovo HX ストレージ システムのインベントリとパフォーマンス データを検出します。

注: これらは一般的な用語のマッピングのみであり、このデータ コレクターのすべてのケースを反映している

わけではありません。

要件

- Prism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

構成

フィールド	説明
Prism外部IPアドレス	クラスタの外部データサービスIPアドレス
ユーザ名	管理者アカウントのユーザー名
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	アレイに接続するために使用される TCP ポート。デフォルトは 9440 です。
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。デフォルトは60分です。
パフォーマンスポーリング間隔（秒）	パフォーマンス ポーリングの間隔。デフォルトは300秒です。

トラブルシューティング

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

Microsoft

Azure NetApp Filesデータ コレクターの構成

Data Infrastructure Insights は、 Azure NetApp Filesデータ コレクターを使用して、インベントリとパフォーマンス データを取得します。

要件

このデータ コレクターを構成するには、次の情報が必要です。

- ポート要件: 443 HTTPS
- Azure 管理 REST IP (management.azure.com)
- Azure サービス プリンシパル クライアント ID (ユーザー アカウント)
- Azure サービス プリンシパル認証キー (ユーザー 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。

  アカウントが適切に構成され、アプリケーションを Azure に登録すると、 Data Infrastructure Insightsを使用して Azure インスタンスを検出するために必要な資格情報が得られます。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ています。

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

構成

以下の表に従って、データ コレクター 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
Azure サービス プリンシパル認証キー	ログイン認証キー
私は、MicrosoftがAPIリクエストに対して料金を請求することを理解しています	Insight ポーリングによって行われた API リクエストに対して Microsoft が課金することを理解していることを確認するには、これにチェックを入れます。

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 コレクターが使用する資格情報には、ANF ボリュームを含むすべての Azure サブスクリプションへのアクセス権が必要です。
- 読者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 レベルで共同作成者アクセスを付与してみてください。

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

Microsoft Hyper-V データコレクター

Microsoft Hyper-V データ コレクターは、仮想化されたサーバー 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 データを取得します。このデータ コレクターは、スタンドアロン Hyper-V ホストまたはクラスター全体を検出できます。スタンドアロン ホストまたはクラスターごとに 1 つのコレクターを作成します。

用語

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によって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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
クラスター共有ボリューム（CSV）、パーティション ボリューム	データ ストア
インターネット SCSI デバイス、マルチパス SCSI LUN	LUN
ファイバーチャネルポート	ポート

注: 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 コレクターのすべてのケースを反映しているわけではありません。

要件

このデータ コレクターを構成するには、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/管理のためにポート 5985 を開く必要があります。
- クラスター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 クラスターのホスト名または IP を使用することは、クラスター内の特定の 1 つのノードのみにコレクターを向ける場合よりも、最も信頼性の高いアプローチであると考えられます。
- クラスター内のすべてのハイパーバイザーで機能する管理レベルのユーザー アカウント。
- WinRMはすべてのハイパーバイザーで有効化され、リッスンする必要がある
- ポート要件: WMI 経由のポート 135、および Windows 2003 以前では 1024 ～ 65535、Windows 2008 では 49152 ～ 65535 に割り当てられた動的 TCP ポート。
- データコレクターがIPアドレスのみを指している場合でも、DNS解決は成功する必要がある
- 各 Hyper-V ハイパーバイザーでは、すべてのホスト上のすべての VM に対して「リソース メータリング」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、各ゲストのData Infrastructure Insightsにさらに多くのデータを利用できるようになります。これを設定しないと、ゲストごとに取得されるパフォーマンス メトリックの数が少なくなります。リソースメータリングの詳細については、Microsoft のドキュメントを参照してください。

  "Hyper-V リソースメータリングの概要"

  "VMリソースメータリングを有効にする"

Hyper-V データ コレクターには Windows Acquisition Unit が必要です。

構成

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	クラスタまたはスタンドアロンの非クラスタ化ハイパーバイザの IP アドレスまたは完全修飾ドメイン名

フィールド	説明
ユーザー名	ハイパーバイザーの管理者ユーザー名
パスワード	ハイパーバイザーのパスワード
DNSドメインサフィックス	単純なホスト名と組み合わせてハイパーバイザーのFQDN を表現する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

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

NetApp

NetApp Cloud Volumes ONTAPデータコレクター

このデータ コレクターは、Cloud Volumes ONTAP構成からのインベントリ収集をサポートします。

構成

フィールド	説明
NetApp管理 IP アドレス	Cloud Volumens ONTAPの IP アドレス
ユーザー名	Cloud Volumes ONTAPのユーザー名
パスワード	上記ユーザーのパスワード

高度な設定

フィールド	説明
接続タイプ	HTTPS を推奨します。デフォルトのポートも表示されます。
通信ポートのオーバーライド	デフォルトでない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。
インベントリ同時スレッド数	同時実行スレッドの数。
HTTPSにTLSを強制する	HTTPS 経由の TLS を強制する
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
HTTP読み取りタイムアウト秒数	デフォルトは30秒です

フィールド	説明
応答を UTF-8 として強制する	応答を UTF-8 として強制する
パフォーマンスポーリング間隔（分）	デフォルトは 900 秒です。
パフォーマンス同時スレッド数	同時実行スレッドの数。
高度なカウンターデータ収集	これをチェックすると、 Data Infrastructure Insights によって以下のリストから高度なメトリックが収集されます。

トラブルシューティング

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

NetApp ONTAP AFX データコレクター

このデータ コレクターは、REST API 呼び出しを使用して、 ONTAP 9.16.0 以降を実行しているストレージ システムからインベントリ、EMS ログ、およびパフォーマンス データを取得します。

要件

このデータ コレクターを構成して使用するための要件は次のとおりです。

- 必要なアクセス レベルを持つユーザー アカウントにアクセスできる必要があります。新しい REST ユーザー/ロールを作成する場合は、管理者権限が必要であることに注意してください。
  - 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、いくつかの書き込み権限が必要です。すぐ下の「権限に関する注意」を参照してください。
- ONTAPバージョン 9.16.0 以上。
- ポート要件: 443

権限に関する注意事項

Data Infrastructure InsightsのONTAPダッシュボードの多くは高度なONTAPカウンターに依存しているため、データ コレクターの詳細設定セクションで 高度なカウンター データ収集を有効にする を有効のままにしておく必要があります。

クラスタ レベルでData Infrastructure Insightsのローカル アカウントを作成するには、クラスタ管理管理者のユーザー名とパスワードを使用してONTAPにログインし、 ONTAPサーバーで次のコマンドを実行します。

1. 開始する前に、_管理者_アカウントでONTAPにサインインし、_診断レベルのコマンド_を有効にする必要があります。
2. タイプが *admin* である vserver の名前を取得します。後続のコマンドではこの名前を使用します。

```
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ーを作成します。作成コマンドを実行すると、このユーザーのパスワードを入力するよう求められます。

```
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、コマンドは

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
```

結果として得られるロールとユーザー
ログインは次のようになります。実際の出力は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
```

移住

以前のONTAP (ontapi) データ コレクターから新しいONTAP REST コレクターに移行するには、次の手順を実行します。

1. REST コレクターを追加します。以前のコレクターに設定されたユーザーとは異なるユーザーの情報を入力することをお勧めします。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ーを使用します。
2. 前のコレクターを一時停止して、データの収集を継続しないようにします。
3. 新しい REST コレクターが少なくとも 30 分間データを取得するようにします。この期間中に「正常」と見えないデータはすべて無視します。
4. 休止期間後、REST コレクターが引き続きデータを取得し、データが安定するはずです。

必要に応じて、同じプロセスを使用して、前のコレクターに戻ることができます。

構成

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。クラスター管理 IP/FQDN である必要があります。
ONTAP RESTユーザー名	NetAppクラスタのユーザー名
ONTAP REST パスワード	NetApp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。
高度なカウンターデータ収集	ポーリングにONTAPアドバンスド カウンタ データを含めるには、これを選択します。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 データを含めるにはこれを選択します。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

Data Infrastructure Insights は、 ONTAPデータ コレクターからインベントリ、ログ、パフォーマンス データを取得します。取得した資産の種類ごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
クラスタ	ストレージ
ノード	ストレージノード

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ボリューム/ FlexVol/ FlexGroup	内部ボリューム
Qtree/フレックスツリー	Qtree (タイプ: Explixit/Default)
S3 バケット	Qtree (タイプ: バケット)
ストレージポッド/ストレージ可用性ゾーン	ストレージプール
共有	共有
クォータ	クォータ
SVM (ストレージ仮想マシン)	Storage Virtual Machine

ONTAPデータ管理用語

次の用語は、 ONTAP Data Management ストレージ アセットのランディング ページに表示されるオブジェクトまたは参照に適用されます。これらの条件の多くは他のデータ収集者にも適用されます。

ストレージ

- モデル – このクラスター内の一意の個別のノード モデル名のカンマ区切りリスト。クラスター内のすべてのノードが同じモデル タイプである場合、モデル名が 1 つだけ表示されます。
- ベンダー – 新しいデータ ソースを構成する場合に表示されるのと同じベンダー名。
- シリアル番号 – アレイUUID
- IP – 通常は、データ ソースで構成されている IP またはホスト名になります。
- マイクロコード バージョン - ファームウェア。
- 生の容量 – 役割に関係なく、システム内のすべての物理ディスクの 2 を底とする合計。
- レイテンシ – 読み取りと書き込みの両方において、ホスト側のワークロードが経験している状況を表します。理想的には、 Data Infrastructure Insightsがこの値を直接取得しますが、多くの場合そうではありません。アレイがこれを提供する代わりに、 Data Infrastructure Insightsは通常、個々の内部ボリュームの統計から導き出された IOPS 加重計算を実行します。
- スループット – 内部ボリュームから集計されます。管理 – これにはデバイスの管理インターフェイスへのハイパーリンクが含まれる場合があります。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

- ストレージ – このプールが存在するストレージ アレイ。必須。
- タイプ – 可能性のある列挙リストからの説明的な値。最も一般的なのは「アグリゲート」または「RAID グループ」です。
- ノード – このストレージ アレイのアーキテクチャで、プールが特定のストレージ ノードに属している場合、その名前は独自のランディング ページへのハイパーリンクとしてここに表示されます。
- フラッシュ プールの使用 – はい/いいえの値 – この SATA/SAS ベースのプールには、キャッシュ アクセラレーションに使用される SSD がありますか?
- 冗長性 – RAID レベルまたは保護スキーム。 RAID_DP はデュアル パリティ、RAID_TP はトリプル パリティです。

- 容量 – ここでの値は、論理的に使用されている容量、使用可能な容量、論理的な合計容量、およびこれらの間で使用されている割合です。
- 過剰コミット容量 – 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容量の合計を割り当てた場合、ここでのパーセンテージ値は 0% より大きくなります。
- スナップショット – ストレージ プール アーキテクチャが容量の一部をスナップショット専用のセグメント領域に割り当てている場合の、スナップショットの使用済み容量と合計容量。 MetroCluster構成のONTAPではこの問題が発生する可能性が高くなりますが、他のONTAP構成ではこの問題は発生しにくくなります。
- 使用率 – このストレージ プールに容量を提供しているディスクのうち最も高いディスク使用率を示すパーセンテージ値。ディスク使用率は、必ずしもアレイのパフォーマンスと強い相関関係があるわけではありません。ホスト駆動型のワークロードがない場合、ディスクの再構築、重複排除アクティビティなどにより、使用率が高くなる可能性があります。また、多くのアレイのレプリケーション実装では、内部ボリュームまたはボリュームのワークロードとして表示されずにディスク使用率が向上する場合があります。
- IOPS – このストレージ プールに容量を提供しているすべてのディスクの合計 IOPS。スループット – このストレージ プールに容量を提供しているすべてのディスクの合計スループット。

ストレージ ノード

- ストレージ – このノードが属するストレージ アレイ。必須。
- HA パートナー - ノードが他の 1 つのノードにのみフェールオーバーするプラットフォームでは、通常ここに表示されます。
- 状態 – ノードの健全性。アレイがデータ ソースによってインベントリされるのに十分正常な場合にのみ使用できます。
- モデル – ノードのモデル名。
- バージョン – 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 – 使用可能な場合は 2 進メモリ。
- 使用率 – ONTAPでは、これは独自のアルゴリズムによるコントローラ ストレス インデックスです。すべてのパフォーマンス ポーリングでは、 WAFLディスク競合または平均 CPU 使用率のいずれか大きい方の 0 ～ 100% の数値が報告されます。継続的に 50% を超える値が観測される場合は、サイズ不足を示しています。つまり、書き込みワークロードを吸収するのに十分な大きさのコントローラー/ノードがないか、回転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電力メトリクス

いくつかのONTAPモデルでは、監視やアラートに使用できるData Infrastructure Insightsの電力メトリックが提供されます。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なものではありませんが、何らかのガイダンスを提供します。一般に、モデルがリストにあるモデルと同じファミリーに属している場合、サポートは同じです。

対応モデル:

A200 A220 A250 A300 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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

問題：	これを試してください:
ONTAP REST データコレクター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: 構成: 10.193.70.14: 10.193.70.14 のONTAP REST API は使用できません: 10.193.70.14 が GET /api/cluster に失敗しました: 400 不正な要求	これは、REST API 機能がない古いONTAPアレイ (たとえば、 ONTAP 9.6) が原因である可能性があります。 ONTAP 9.14.1 は、 ONTAP REST コレクターでサポートされる最小のONTAPバージョンです。 REST ONTAPより前のリリースでは、「400 Bad Request」応答が予想されます。 REST をサポートしているが 9.14.1 以降ではないONTAPバージョンの場合、次のような類似のメッセージが表示されることがあります: 構成: 10.193.98.84: 10.193.98.84 のONTAP REST API は使用できません: 10.193.98.84: 10.193.98.84 のONTAP REST API は使用できます: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 ただし、最小バージョン 9.14.1 ではありません。
ONTAP ontapi コレクターがデータを表示する場所に、空または「0」のメトリックが表示されます。	ONTAP REST は、 ONTAPシステムでのみ内部的に使用されるメトリックを報告しません。たとえば、システム アグリゲートはONTAP REST によって収集されず、「データ」タイプの SVM のみが収集されます。ゼロまたは空のデータを報告する可能性があるONTAP REST メトリックのその他の例: InternalVolumes: REST は vol0 を報告しなくなりました。集計: REST は aggr0 を報告しなくなりました。ストレージ: ほとんどのメトリックは内部ボリュームメトリックのロールアップであり、上記の影響を受けます。ストレージ仮想マシン: REST は、「データ」以外のタイプ (「クラスター」、「管理」、「ノード」など) の SVM を報告しなくなりました。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、データがあるグラフの外観が変わる場合があります。ポーリングの頻度が高ければ、プロットするデータ ポイントの数も多くなります。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

NetApp ONTAP ASA r2（オール**SAN**アレイ）データコレクター

このデータ コレクターは、REST API 呼び出しを使用して、 ONTAP 9.16.0 以降を実行しているストレージ システムからインベントリ、EMS ログ、およびパフォーマンス データを取得します。

要件

このデータ コレクターを構成して使用するための要件は次のとおりです。

- 必要なアクセス レベルを持つユーザー アカウントにアクセスできる必要があります。新しい REST ユーザー/ロールを作成する場合は、管理者権限が必要であることに注意してください。
  - 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、いくつかの書き込み権限が必要です。すぐ下の「権限に関する注意」を参照してください。
- ONTAPバージョン 9.16.0 以上。
- ポート要件: 443

ASA R2 は、 ONTAP ASAストレージ プラットフォームの最新世代モデルを表します。これには、アレイ モデルASA A1K、A90、A70、A50、A30、および A20 が含まれます。

以前の世代のASAシステムについては、"ONTAPレスト"コレクタ。

権限に関する注意事項

Data Infrastructure InsightsのONTAPダッシュボードの多くは高度なONTAPカウンターに依存しているため、データ コレクターの詳細設定セクションで 高度なカウンター データ収集を有効にする を有効のままにしておく必要があります。

クラスタ レベルでData Infrastructure Insightsのローカル アカウントを作成するには、クラスタ管理管理者のユーザー名とパスワードを使用してONTAPにログインし、 ONTAPサーバーで次のコマンドを実行します。

1. 開始する前に、_管理者_アカウントでONTAPにサインインし、_診断レベルのコマンド_を有効にする必要があります。
2. タイプが *admin* である vserver の名前を取得します。後続のコマンドではこの名前を使用します。

```
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ーを作成します。作成コマンドを実行すると、このユーザーのパスワードを入力するよう求められます。

```
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、コマンドは

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
```

結果として得られるロールとユーザー
ログインは次のようになります。実際の出力は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
```

移住

以前のONTAP (ontapi) データ コレクターから新しいONTAP REST コレクターに移行するには、次の手順を実行します。

1. REST コレクターを追加します。以前のコレクターに設定されたユーザーとは異なるユーザーの情報を入力することをお勧めします。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ーを使用します。
2. 前のコレクターを一時停止して、データの収集を継続しないようにします。
3. 新しい REST コレクターが少なくとも 30 分間データを取得するようにします。この期間中に「正常」と見えないデータはすべて無視します。
4. 休止期間後、REST コレクターが引き続きデータを取得し、データが安定するはずです。

必要に応じて、同じプロセスを使用して、前のコレクターに戻ることができます。

構成

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。クラスター管理 IP/FQDN である必要があります。
ONTAP RESTユーザー名	NetAppクラスタのユーザー名
ONTAP REST パスワード	NetApp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。
高度なカウンターデータ収集	ポーリングにONTAPアドバンスド カウンタ データを含めるには、これを選択します。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 データを含めるにはこれを選択します。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

Data Infrastructure Insights は、 ONTAPデータ コレクターからインベントリ、ログ、パフォーマンス データを取得します。取得した資産の種類ごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ディスク	ディスク
レイドグループ	ディスクグループ

ベンダー/モデル用語	**Data Infrastructure Insights**用語
クラスタ	ストレージ
ノード	ストレージ ノード
Aggregate	ストレージ プール
LUN	Volume
Volume	内部容積
ストレージ仮想マシン/Vserver	Storage Virtual Machine

ONTAPデータ管理用語

次の用語は、 ONTAP Data Management ストレージ アセットのランディング ページに表示されるオブジェクトまたは参照に適用されます。これらの条件の多くは他のデータ収集者にも適用されます。

ストレージ

- モデル – このクラスター内の一意の個別のノード モデル名のカンマ区切りリスト。クラスター内のすべてのノードが同じモデル タイプである場合、モデル名が 1 つだけ表示されます。
- ベンダー – 新しいデータ ソースを構成する場合に表示されるのと同じベンダー名。
- シリアル番号 – アレイUUID
- IP – 通常は、データ ソースで構成されている IP またはホスト名になります。
- マイクロコード バージョン - ファームウェア。
- 生の容量 – 役割に関係なく、システム内のすべての物理ディスクの 2 を底とする合計。
- レイテンシ – 読み取りと書き込みの両方において、ホスト側のワークロードが経験している状況を表します。理想的には、 Data Infrastructure Insightsがこの値を直接取得しますが、多くの場合そうではありません。アレイがこれを提供する代わりに、 Data Infrastructure Insightsは通常、個々の内部ボリュームの統計から導き出された IOPS 加重計算を実行します。
- スループット – 内部ボリュームから集計されます。管理 – これにはデバイスの管理インターフェイスへのハイパーリンクが含まれる場合があります。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

- ストレージ – このプールが存在するストレージ アレイ。必須。
- タイプ – 可能性のある列挙リストからの説明的な値。最も一般的なのは「アグリゲート」または「RAID グループ」です。
- ノード – このストレージ アレイのアーキテクチャで、プールが特定のストレージ ノードに属している場合、その名前は独自のランディング ページへのハイパーリンクとしてここに表示されます。
- フラッシュ プールの使用 – はい/いいえの値 – この SATA/SAS ベースのプールには、キャッシュ アクセラレーションに使用される SSD がありますか?
- 冗長性 – RAID レベルまたは保護スキーム。 RAID_DP はデュアル パリティ、RAID_TP はトリプル パリティです。
- 容量 – ここでの値は、論理的に使用されている容量、使用可能な容量、論理的な合計容量、およびこれらの間で使用されている割合です。

- 過剰コミット容量 – 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容量の合計を割り当てた場合、ここでのパーセンテージ値は 0% より大きくなります。
- スナップショット – ストレージ プール アーキテクチャが容量の一部をスナップショット専用のセグメント領域に割り当てている場合の、スナップショットの使用済み容量と合計容量。 MetroCluster構成のONTAPではこの問題が発生する可能性が高くなりますが、他のONTAP構成ではこの問題は発生しにくくなります。
- 使用率 – このストレージ プールに容量を提供しているディスクのうち最も高いディスク使用率を示すパーセンテージ値。ディスク使用率は、必ずしもアレイのパフォーマンスと強い相関関係があるわけではありません。ホスト駆動型のワークロードがない場合、ディスクの再構築、重複排除アクティビティなどにより、使用率が高くなる可能性があります。また、多くのアレイのレプリケーション実装では、内部ボリュームまたはボリュームのワークロードとして表示されずにディスク使用率が向上する場合があります。
- IOPS – このストレージ プールに容量を提供しているすべてのディスクの合計 IOPS。スループット – このストレージ プールに容量を提供しているすべてのディスクの合計スループット。

ストレージ ノード

- ストレージ – このノードが属するストレージ アレイ。必須。
- HA パートナー - ノードが他の 1 つのノードにのみフェールオーバーするプラットフォームでは、通常ここに表示されます。
- 状態 – ノードの健全性。アレイがデータ ソースによってインベントリされるのに十分正常な場合にのみ使用できます。
- モデル – ノードのモデル名。
- バージョン – 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 – 使用可能な場合は 2 進メモリ。
- 使用率 – ONTAPでは、これは独自のアルゴリズムによるコントローラ ストレス インデックスです。すべてのパフォーマンス ポーリングでは、 WAFLディスク競合または平均 CPU 使用率のいずれか大きい方の 0 ～ 100% の数値が報告されます。継続的に 50% を超える値が観測される場合は、サイズ不足を示しています。つまり、書き込みワークロードを吸収するのに十分な大きさのコントローラー/ノードがないか、回転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電力メトリクス

いくつかのONTAPモデルでは、監視やアラートに使用できるData Infrastructure Insightsの電力メトリックが提供されます。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なものではありませんが、何らかのガイダンスを提供します。一般に、モデルがリストにあるモデルと同じファミリーに属している場合、サポートは同じです。

対応モデル:

A200 A220 A250 A300 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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

問題：	これを試してください:
ONTAP REST データコレクター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: 構成: 10.193.70.14: 10.193.70.14 のONTAP REST API は使用できません: 10.193.70.14 が GET /api/cluster に失敗しました: 400 不正な要求	これは、REST API 機能がない古いONTAPアレイ (たとえば、 ONTAP 9.6) が原因である可能性があります。 ONTAP 9.14.1 は、 ONTAP REST コレクターでサポートされる最小のONTAPバージョンです。 REST ONTAPより前のリリースでは、「400 Bad Request」応答が予想されます。 REST をサポートしているが 9.14.1 以降ではないONTAPバージョンの場合、次のような類似のメッセージが表示されることがあります: 構成: 10.193.98.84: 10.193.98.84 のONTAP REST API は使用できません: 10.193.98.84: 10.193.98.84 のONTAP REST API は使用できます: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 ただし、最小バージョン 9.14.1 ではありません。
ONTAP ontapi コレクターがデータを表示する場所に、空または「0」のメトリックが表示されます。	ONTAP REST は、 ONTAPシステムでのみ内部的に使用されるメトリックを報告しません。たとえば、システム アグリゲートはONTAP REST によって収集されず、「データ」タイプの SVM のみが収集されます。ゼロまたは空のデータを報告する可能性があるONTAP REST メトリックのその他の例: InternalVolumes: REST は vol0 を報告しなくなりました。集計: REST は aggr0 を報告しなくなりました。ストレージ: ほとんどのメトリックは内部ボリューム メトリックのロールアップであり、上記の影響を受けます。ストレージ仮想マシン: REST は、「データ」以外のタイプ (「クラスター」、「管理」、「ノード」など) の SVM を報告しなくなりました。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、データがあるグラフの外観が変わる場合があります。ポーリングの頻度が高ければ、プロットするデータ ポイントの数も多くなります。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

NetApp ONTAPデータ管理ソフトウェア データコレクター

このデータ コレクターは、 ONTAPアカウントからの読み取り専用 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およびパフォーマンス データを取得します。このデータ コレクターは、サポートを高速化するために、ク

ラスター アプリケーション レジストリにレコードも作成します。

用語

Data Infrastructure Insights は、 ONTAPデータ コレクターからインベントリとパフォーマンス データを取得します。取得した資産の種類ごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ディスク	ディスク
レイドグループ	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
Aggregate	ストレージ プール
LUN	Volume
Volume	内部容積

ONTAPデータ管理用語

次の用語は、 ONTAP Data Management ストレージ アセットのランディング ページに表示されるオブジェクトまたは参照に適用されます。これらの条件の多くは他のデータ収集者にも適用されます。

ストレージ

- モデル – このクラスター内の一意の個別のノード モデル名のカンマ区切りリスト。クラスター内のすべてのノードが同じモデル タイプである場合、モデル名が 1 つだけ表示されます。
- ベンダー – 新しいデータ ソースを構成する場合に表示されるのと同じベンダー名。
- シリアル番号 – アレイのシリアル番号。 ONTAP Data Management 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役に立たない場合があります。
- IP – 通常は、データ ソースで構成されている IP またはホスト名になります。
- マイクロコード バージョン - ファームウェア。
- 生の容量 – 役割に関係なく、システム内のすべての物理ディスクの 2 を底とする合計。
- レイテンシ – 読み取りと書き込みの両方において、ホスト側のワークロードが経験している状況を表します。理想的には、 Data Infrastructure Insightsがこの値を直接取得しますが、多くの場合そうではありません。アレイがこれを提供する代わりに、 Data Infrastructure Insightsは通常、個々の内部ボリュームの統計から導き出された IOPS 加重計算を実行します。
- スループット – 内部ボリュームから集計されます。管理 – これにはデバイスの管理インターフェイスへのハイパーリンクが含まれる場合があります。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

- ストレージ – このプールが存在するストレージ アレイ。必須。

- タイプ – 可能性のある列挙リストからの説明的な値。最も一般的なのは「アグリゲート」または「RAID グループ」です。
- ノード – このストレージ アレイのアーキテクチャで、プールが特定のストレージ ノードに属している場合、その名前は独自のランディング ページへのハイパーリンクとしてここに表示されます。
- フラッシュ プールの使用 – はい/いいえの値 – この SATA/SAS ベースのプールには、キャッシュ アクセラレーションに使用される SSD がありますか?
- 冗長性 – RAID レベルまたは保護スキーム。 RAID_DP はデュアル パリティ、RAID_TP はトリプル パリティです。
- 容量 – ここでの値は、論理的に使用されている容量、使用可能な容量、論理的な合計容量、およびこれらの間で使用されている割合です。
- 過剰コミット容量 – 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容量の合計を割り当てた場合、ここでのパーセンテージ値は 0% より大きくなります。
- スナップショット – ストレージ プール アーキテクチャが容量の一部をスナップショット専用のセグメント領域に割り当てている場合の、スナップショットの使用済み容量と合計容量。 MetroCluster構成のONTAPではこの問題が発生する可能性が高くなりますが、他のONTAP構成ではこの問題は発生しにくくなります。
- 使用率 – このストレージ プールに容量を提供しているディスクのうち最も高いディスク使用率を示すパーセンテージ値。ディスク使用率は、必ずしもアレイのパフォーマンスと強い相関関係があるわけではありません。ホスト駆動型のワークロードがない場合、ディスクの再構築、重複排除アクティビティなどにより、使用率が高くなる可能性があります。また、多くのアレイのレプリケーション実装では、内部ボリュームまたはボリュームのワークロードとして表示されずにディスク使用率が向上する場合があります。
- IOPS – このストレージ プールに容量を提供しているすべてのディスクの合計 IOPS。スループット – このストレージ プールに容量を提供しているすべてのディスクの合計スループット。

ストレージ ノード

- ストレージ – このノードが属するストレージ アレイ。必須。
- HA パートナー - ノードが他の 1 つのノードにのみフェールオーバーするプラットフォームでは、通常ここに表示されます。
- 状態 – ノードの健全性。アレイがデータ ソースによってインベントリされるのに十分正常な場合にのみ使用できます。
- モデル – ノードのモデル名。
- バージョン – 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 – 使用可能な場合は 2 進メモリ。
- 使用率 – ONTAPでは、これは独自のアルゴリズムによるコントローラ ストレス インデックスです。すべてのパフォーマンス ポーリングでは、 WAFLディスク競合または平均 CPU 使用率のいずれか大きい方の 0 ～ 100% の数値が報告されます。継続的に 50% を超える値が観測される場合は、サイズ不足を示しています。つまり、書き込みワークロードを吸収するのに十分な大きさのコントローラー/ノードがないか、回転ディスクが足りない可能性があります。
- IOPS – ノード オブジェクト上のONTAP ZAPI 呼び出しから直接導出されます。
- レイテンシ – ノード オブジェクトに対するONTAP ZAPI 呼び出しから直接導出されます。

- スループット – ノード オブジェクトに対するONTAP ZAPI 呼び出しから直接導出されます。
- プロセッサ – CPU 数。

要件

このデータ コレクターを構成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 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ー名とパスワードが含まれます。
- ポート要件: 80 または 443
- アカウント権限:
  - デフォルトの Vserver への ontapi アプリケーションへの読み取り専用ロール名
  - オプションで追加の書き込み権限が必要になる場合があります。以下の権限に関する注意事項を参照してください。
- ONTAPライセンス要件:
  - ファイバーチャネル検出には FCP ライセンスとマップ/マスクされたボリュームが必要です

ONTAPスイッチメトリックの収集に必要な権限

Data Infrastructure Insightsは、コレクターのオプションとしてONTAPクラスタスイッチデータを収集する機能を持っています。詳細設定設定。 Data Infrastructure Insightsコレクターでこれを有効にすることに加えて、 ONTAPシステム自体も*設定*して提供する必要があります。"スイッチ情報" 、正しいことを確認する権限スイッチ データをData Infrastructure Insightsに送信できるようにするために、設定されています。

構成

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

高度な設定

フィールド	説明
接続の種類	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
通信ポートのオーバーライド	デフォルトを使用しない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。
HTTPSのTLSの場合	HTTPS を使用する場合はプロトコルとして TLS のみを許可する

フィールド	説明
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自動ネットグループ検索を有効にする
ネットグループの拡張	ネットグループの拡大戦略。 *file* または *shell* を選択します。デフォルトは *shell* です。
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 として強制する	データコレクターコードに、CLIからの応答をUTF-8として解釈するように強制します。
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。
高度なカウンターデータ収集	ONTAP統合を有効にします。ポーリングにONTAPアドバンスド カウンタ データを含めるには、これを選択します。リストから必要なカウンターを選択します。
クラスタスイッチメトリック	Data Infrastructure Insights がクラスター スイッチ データを収集できるようにします。 Data Infrastructure Insights側でこれを有効にすることに加えて、ONTAPシステムも設定する必要があることに注意してください。"スイッチ情報" 、正しいことを確認する権限スイッチ データをData Infrastructure Insightsに送信できるようにするために、設定されています。以下の「権限に関する注意事項」を参照してください。

ONTAP電力メトリクス

いくつかのONTAPモデルでは、監視やアラートに使用できるData Infrastructure Insightsの電力メトリックが提供されます。

> これらのリストは包括的なものではなく、変更される可能性があります。一般に、モデルがリストにあるモデルと同じファミリーに属する場合、サポートは同じになるはずですが、必ずしも同じになるとは限りません。ご使用のモデルが電力メトリックをサポートしているかどうか不明な場合は、 ONTAPサポートにお問い合わせください。

対応モデル:

A200 A220 A250 A300 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

権限に関する注意事項

Data Infrastructure InsightsのONTAPダッシュボードの多くは高度なONTAPカウンターに依存しているため、データ コレクターの詳細設定セクションで 高度なカウンター 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、これには必要な権限を持つクラスター レベルのアカウントが必要です。

クラスタ レベルでData Infrastructure Insightsのローカル アカウントを作成するには、クラスタ管理管理者のユーザー名とパスワードを使用してONTAPにログインし、 ONTAPサーバーで次のコマンドを実行します。

1. 開始する前に、_管理者_アカウントでONTAPにサインインし、_診断レベルのコマンド_を有効に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ーを作成します。作成コマンドを実行すると、このユーザーのパスワードを入力するよう求められます。

```
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、コマンドは

```
 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 データを収集する場合：

```
security login rest-role create -role ci_readonly_rest -api
/api/network/ethernet -access readonly
security login create -user-or-group-name ci_user -application http
-authmethod password -role ci_readonly_rest
```

結果として得られるロールとユーザー ログインは次のようになります。実際の出力は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場合、 Data Infrastructure Insights 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コレクターで有効にしたが、 ONTAPで権限を設定していない場合、取得は失敗します。さらに、ロールが以前にONTAPで定義されていて、Rest API 機能を追加する場合は、ロールに *http* が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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
401 HTTP 応答または 13003 ZAPI エラー コードを受信し、ZAPI が「権限が不十分です」または「このコマンドは許可されていません」を返します。	ユーザー名とパスワード、およびユーザー権限/許可を確認します。
クラスタバージョンは 8.1 未満です	クラスターの最小サポートバージョンは 8.1 です。サポートされている最小バージョンにアップグレードします。
ZAPI は「クラスタ ロールが cluster_mgmt LIF ではありません」を返します	AU はクラスター管理 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に変更します
エラー:「7 モード ファイラーはサポートされていません」	このデータ コレクターを使用して 7 モード ファイラーを検出すると、この問題が発生する可能性があります。代わりに、IP を変更して cdot クラスターを指すようにします。
再試行後にZAPIコマンドが失敗する	AU はクラスターとの通信に問題があります。ネットワーク、ポート番号、IP アドレスを確認します。ユーザーは、AU マシンのコマンド ラインからコマンドを実行することも試みる必要があります。
AUはHTTP経由でZAPIに接続できませんでした	ZAPI ポートがプレーンテキストを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、通信は失敗します。
SSLException により通信が失敗しました	AU は、ファイラー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 ポートが SSL を受け入れるかどうかを確認するか、別のポートを使用します。

問題：	これを試してください:
追加の接続エラー: ZAPI 応答にエラー コード 13001、「データベースが開いていません」が含まれています。ZAPI エラー コードは 60 で、応答には「API が時間どおりに終了しませんでした」が含まれています。ZAPI 応答には「initialize_session() が NULL 環境を返しました」が含まれています。ZAPI エラー コードは 14007 で、応答には「ノードが正常ではありません」が含まれています。	ネットワーク、ポート番号、IP アドレスを確認します。ユーザーは、AU マシンのコマンド ラインからコマンドを実行することも試みる必要があります。

パフォーマンス

問題：	これを試してください:
「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	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試してください: *> system node systemshell -node * -command "spmctl -h cmd –stop; spmctl -h cmd –exec"*

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

NetApp ONTAP REST データコレクター

このデータ コレクターは、REST API 呼び出しを使用して、 ONTAP 9.14.1 以降を実行しているストレージ システムからインベントリ、EMS ログ、およびパフォーマンス データを取得します。以前のリリースのONTAPシステムの場合は、ZAPI ベースの「NetApp ONTAPデータ管理ソフトウェア」コレクター タイプを使用します。

ONTAP REST コレクターは、以前の ONTAPI ベースのコレクター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メトリックに違いが生じる可能性があります。 ONTAPI とRESTの違いの詳細については、"ONTAP 9.14.1 ONTAPIからRESTへのマッピング"ドキュメント。

要件

このデータ コレクターを構成して使用するための要件は次のとおりです。

- 必要なアクセス レベルを持つユーザー アカウントにアクセスできる必要があります。新しい REST ユーザー/ロールを作成する場合は、管理者権限が必要であることに注意してください。
  - 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、いくつかの書き込み権限が必要です。すぐ下の「権限に関する注意」を参照してください。
- ONTAPバージョン 9.14.1 以上。
- ポート要件: 443
- ONTAP REST コレクターでは FPolicy メトリックはサポートされていないことに注意してください (Workload Security データ コレクターは FPolicy サーバーを使用し、FPolicy メトリックを使用すると Workload Security データ収集アクティビティを監視できます)。Fpolicyメトリックをサポートするには、"ONTAPデータ管理" コレクタ。

Data Infrastructure InsightsのONTAPダッシュボードの多くは高度なONTAPカウンターに依存しているため、データ コレクターの詳細設定セクションで 高度なカウンター データ収集を有効にする を有効のままにしておく必要があります。

クラスタ レベルでData Infrastructure Insightsのローカル アカウントを作成するには、クラスタ管理管理者のユーザー名とパスワードを使用してONTAPにログインし、 ONTAPサーバーで次のコマンドを実行します。

1. 開始する前に、_管理者_アカウントでONTAPにサインインし、_診断レベルのコマンド_を有効にする必要があります。
2. タイプが *admin* である vserver 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}
```

3. 次のコマンドを使用して読み取り専用ユーザーを作成します。作成コマンドを実行すると、このユーザーのパスワードを入力するよう求められます。次のコマンドでは、ロールが *ci_readonly* に設定されていることに注意してください。上記の手順 3 で別の名前のロールを作成する場合は、代わりにそのカスタム ロール名を使用します。

```
 security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
```

AD/LDAPアカウントを使用する場合、コマンドは

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
```

結果として得られるロールとユーザー
ログインは次のようになります。実際の出力は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
```

必要に応じて spi アクセスを確認できます。

```
**Vserver:> vserver services web access show -name spi
 Vserver                      Type     Service Name     Role
--------------- -------- ---------------- ----------------
<vserver name >     admin             spi           admin
<vserver name >     admin             spi           csrestrole

2 entries were displayed.**
```

移住

以前のONTAP (ontapi) データ コレクターから新しいONTAP REST コレクターに移行するには、次の手順を実行します。

1. REST コレクターを追加します。以前のコレクターに設定されたユーザーとは異なるユーザーの情報を入力することをお勧めします。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ーを使用します。
2. 前のコレクターを一時停止して、データの収集を継続しないようにします。
3. 新しい REST コレクターが少なくとも 30 分間データを取得するようにします。この期間中に「正常」と見えないデータはすべて無視します。
4. 休止期間後、REST コレクターが引き続き取得を続けると、データが安定するはずです。

必要に応じて、同じプロセスを使用して、前のコレクターに戻ることができます。

構成

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。クラスター管理 IP/FQDN である必要があります。
ONTAP RESTユーザー名	NetAppクラスタのユーザー名
ONTAP REST パスワード	NetApp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。
高度なカウンターデータ収集	ポーリングにONTAPアドバンスド カウンタ データを含めるには、これを選択します。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 データを含めるにはこれを選択します。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

Data Infrastructure Insights は、 ONTAPデータ コレクターからインベントリ、ログ、パフォーマンス データを取得します。取得した資産の種類ごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ディスク	ディスク
レイドグループ	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
Aggregate	ストレージ プール
LUN	Volume
Volume	内部容積
ストレージ仮想マシン/Vserver	Storage Virtual Machine

ONTAPデータ管理用語

次の用語は、 ONTAP Data Management ストレージ アセットのランディング ページに表示されるオブジェクトまたは参照に適用されます。これらの条件の多くは他のデータ収集者にも適用されます。

ストレージ

- モデル – このクラスター内の一意の個別のノード モデル名のカンマ区切りリスト。クラスター内のすべてのノードが同じモデル タイプである場合、モデル名が 1 つだけ表示されます。
- ベンダー – 新しいデータ ソースを構成する場合に表示されるのと同じベンダー名。
- シリアル番号 – アレイUUID
- IP – 通常は、データ ソースで構成されている IP またはホスト名になります。
- マイクロコード バージョン - ファームウェア。
- 生の容量 – 役割に関係なく、システム内のすべての物理ディスクの 2 を底とする合計。
- レイテンシ – 読み取りと書き込みの両方において、ホスト側のワークロードが経験している状況を表します。理想的には、 Data Infrastructure Insightsがこの値を直接取得しますが、多くの場合そうではありません。アレイがこれを提供する代わりに、 Data Infrastructure Insightsは通常、個々の内部ボリュームの統計から導き出された IOPS 加重計算を実行します。
- スループット – 内部ボリュームから集計されます。
- 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る場合があります。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で作成されます。

ストレージ プール

- ストレージ – このプールが存在するストレージ アレイ。必須。
- タイプ – 可能性のある列挙リストからの説明的な値。最も一般的なのは「アグリゲート」または「RAID グループ」です。
- ノード – このストレージ アレイのアーキテクチャで、プールが特定のストレージ ノードに属している場合、その名前は独自のランディング ページへのハイパーリンクとしてここに表示されます。
- フラッシュ プールの使用 – はい/いいえの値 – この SATA/SAS ベースのプールには、キャッシュ アクセラレーションに使用される SSD がありますか?
- 冗長性 – RAID レベルまたは保護スキーム。 RAID_DP はデュアル パリティ、RAID_TP はトリプル パリティです。
- 容量 – ここでの値は、論理的に使用されている容量、使用可能な容量、論理的な合計容量、およびこれらの間で使用されている割合です。
- 過剰コミット容量 – 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容量の合計を割り当てた場合、ここでのパーセンテージ値は 0% より大きくなります。
- スナップショット – ストレージ プール アーキテクチャが容量の一部をスナップショット専用のセグメント領域に割り当てている場合の、スナップショットの使用済み容量と合計容量。 MetroCluster構成のONTAPではこの問題が発生する可能性が高くなりますが、他のONTAP構成ではこの問題は発生しにくくなります。
- 使用率 – このストレージ プールに容量を提供しているディスクのうち最も高いディスク使用率を示すパーセンテージ値。ディスク使用率は、必ずしもアレイのパフォーマンスと強い相関関係があるわけではありません。ホスト駆動型のワークロードがない場合、ディスクの再構築、重複排除アクティビティなどにより、使用率が高くなる可能性があります。また、多くのアレイのレプリケーション実装では、内部ボリュームまたはボリュームのワークロードとして表示されずにディスク使用率が向上する場合があります。
- IOPS – このストレージ プールに容量を提供しているすべてのディスクの合計 IOPS。スループット – このストレージ プールに容量を提供しているすべてのディスクの合計スループット。

ストレージ ノード

- ストレージ – このノードが属するストレージ アレイ。必須。
- HA パートナー - ノードが他の 1 つのノードにのみフェールオーバーするプラットフォームでは、通常ここに表示されます。
- 状態 – ノードの健全性。アレイがデータ ソースによってインベントリされるのに十分正常な場合にのみ使用できます。
- モデル – ノードのモデル名。
- バージョン – 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 – 使用可能な場合は 2 進メモリ。
- 使用率 – ONTAPでは、これは独自のアルゴリズムによるコントローラ ストレス インデックスです。すべてのパフォーマンス ポーリングでは、 WAFLディスク競合または平均 CPU 使用率のいずれか大きい方の 0 ～ 100% の数値が報告されます。継続的に 50% を超える値が観測される場合は、サイズ不足を示しています。つまり、書き込みワークロードを吸収するのに十分な大きさのコントローラー/ノードがないか、回転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電力メトリクス

いくつかのONTAPモデルでは、監視やアラートに使用できるData Infrastructure Insightsの電力メトリックが提供されます。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なものではありませんが、何らかのガイダンスを提供します。一般に、モデルがリストにあるモデルと同じファミリーに属している場合、サポートは同じです。

対応モデル:

A200 A220 A250 A300 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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

問題：	これを試してください:
ONTAP REST データコレクター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: 構成: 10.193.70.14: 10.193.70.14 のONTAP REST API は使用できません: 10.193.70.14 が GET /api/cluster に失敗しました: 400 不正な要求	これはおそらく、REST API機能を持たない古いONTAPアレイ（例：ONTAP 9.6）が原因です。ONTAP 9.14.1は、ONTAP RESTコレクターでサポートされる最小のONTAPバージョンです。RESTより前のONTAPリリースでは、「400 Bad Request」レスポンスが想定されます。RESTをサポートしているが9.14.1以降ではないONTAPバージョンの場合、次のような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 at 10.193.98.84 is not available: 10.193.98.84: ONTAP rest API at 10.193.98.84 is available: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 but is not of minimum version 9.14.1.
ONTAP ontapi コレクターがデータを表示する場所に、空または「0」のメトリックが表示されます。	ONTAP REST は、 ONTAPシステムでのみ内部的に使用されるメトリックを報告しません。たとえば、システム アグリゲートはONTAP REST によって収集されず、「データ」タイプの SVM のみが収集されます。ゼロまたは空のデータを報告する可能性があるONTAP REST メトリックのその他の例: InternalVolumes: REST は vol0 を報告しなくなりました。集計: REST は aggr0 を報告しなくなりました。ストレージ: ほとんどのメトリックは内部ボリュームメトリックのロールアップであり、上記の影響を受けます。ストレージ仮想マシン: REST は、「データ」以外のタイプ (「クラスター」、「管理」、「ノード」など) の SVM を報告しなくなりました。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、データがあるグラフの外観が変わる場合があります。ポーリングの頻度が高ければ、プロットするデータ ポイントの数も多くなります。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

7-Mode データコレクターで動作する**NetApp Data ONTAP**

7-Mode で動作するData ONTAPソフトウェアを使用するストレージ システムの場合は、CLI を使用して容量とパフォーマンス データを取得する 7-Mode データ コレクタを使用します。

用語

Data Infrastructure Insights は、 NetApp 7 モード データ コレクターから次のインベントリ情報を取得します。取得した資産の種類ごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

このデータ収集者は"非推奨"。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ディスク	ディスク
レイドグループ	ディスクグループ
ファイラー	ストレージ
ファイラー	ストレージ ノード
Aggregate	ストレージ プール
LUN	Volume
Volume	内部容積

注: 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 コレクターのすべてのケースを反映しているわけではありません。

要件

このデータ コレクターを構成して使用するには、次のものが必要です。

- FASストレージ コントローラとパートナーの IP アドレス。
- ポート443
- 7-Mode の次のロール機能を持つコントローラおよびパートナー コントローラのカスタム管理者レベルのユーザー名とパスワード:
  - 「api-*」: これを使用すると、 OnCommand Insight はすべてのNetAppストレージ API コマンドを実行できるようになります。
  - 「login-http-admin」: これを使用して、 OnCommand Insight がHTTP 経由でNetAppストレージに接続できるようにします。
  - 「security-api-vfiler」: これを使用して、 OnCommand Insight 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します。
  - 「cli-options」: これを使用してストレージ システムのオプションを読み取ります。
  - 「cli-lun」: LUN を管理するにはこれらのコマンドにアクセスします。指定された LUN または LUN のクラスのステータス (LUN パス、サイズ、オンライン/オフライン状態、共有状態) を表示します。
  - 「cli-df」: 空きディスク容量を表示するにはこれを使用します。
  - 「cli-ifconfig」: インターフェースと IP アドレスを表示するにはこれを使用します。

構成

フィールド	説明
ストレージシステムのアドレス	NetApp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
ユーザー名	NetAppストレージシステムのユーザー名
パスワード	NetAppストレージシステムのパスワード
クラスタ内の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

フィールド	説明
クラスタ内のHAパートナーのユーザー名	HAパートナーのユーザー名
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 ポーリングの間隔。デフォルトは20分です。
接続タイプ	HTTPSまたはHTTP、デフォルトのポートも表示します
接続ポートのオーバーライド	空白の場合は、接続タイプフィールドの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 ポーリングの間隔。デフォルトは300秒です。

ストレージシステムの接続

このデータ コレクターのデフォルトの管理ユーザーを使用する代わりに、このデータ コレクターがNetAppストレージ システムからデータを取得できるように、 NetAppストレージ システム上で直接管理権限を持つユーザーを構成することもできます。

NetAppストレージ システムに接続するには、メイン pfiler (ストレージ システムが存在する) を取得するときに指定されるユーザーが次の条件を満たしている必要があります。

- ユーザーは vfiler0 (ルート ファイラー/pfiler) 上にいる必要があります。

  ストレージ システムは、メイン pfiler を取得するときに取得されます。

- 次のコマンドは、ユーザー ロールの機能を定義します。
  - 「api-*」: これを使用すると、 Data Infrastructure Insights がすべてのNetAppストレージ API コマンドを実行できるようになります。

    ZAPI を使用するにはこのコマンドが必要です。

  - 「login-http-admin」: これを使用して、 Data Infrastructure Insights がHTTP 経由でNetAppストレージに接続できるようにします。 ZAPI を使用するにはこのコマンドが必要です。
  - 「security-api-vfiler」: これを使用して、 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します。
  - "cli-options": "options" コマンド用で、パートナー IP および有効なライセンスに使用されます。
  - 「cli-lun」: LUN を管理するにはこれらのコマンドにアクセスします。指定された LUN または LUN のクラスのステータス (LUN パス、サイズ、オンライン/オフライン状態、共有状態) を表示します。
  - 「cli-df」: 「df -s」、「df -r」、「df -A -r」コマンドで空き領域を表示するために使用されます。
  - 「cli-ifconfig」: 「ifconfig -a」コマンド用で、ファイラー IP アドレスを取得するために使用されます。

- "cli-rdfile": "rdfile /etc/netgroup" コマンド用で、ネットグループを取得するために使用されます。
- 「cli-date」:「date」コマンド用で、スナップショット コピーを取得するための完全な日付を取得するために使用されます。
- 「cli-snap」:「snap list」コマンド用で、スナップショット コピーを取得するために使用されます。

cli-date または cli-snap 権限が付与されていない場合、取得は完了しますが、スナップショット 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、次のコマンド文字列のいずれかを使用してユーザー ロールを定義する必要があります。ここにリストされている 2 番目の文字列は、最初の文字列の簡素化されたバージョンです。

- ログイン-http-admin、api-*、セキュリティ-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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
401 HTTP 応答または 13003 ZAPI エラー コードを受信し、ZAPI が「権限が不十分です」または「このコマンドは許可されていません」を返します。	ユーザー名とパスワード、およびユーザー権限/許可を確認します。
「コマンドの実行に失敗しました」というエラー	ユーザーがデバイスに対して以下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 また、 ONTAPのバージョンがData Infrastructure Insightsでサポートされているかどうかを確認し、使用されている資格情報がデバイスの資格情報と一致しているかどうかを確認します。
クラスタバージョンは 8.1 未満です	クラスターの最小サポートバージョンは 8.1 です。サポートされている最小バージョンにアップグレードします。
ZAPI は「クラスタ ロールが cluster_mgmt LIF ではありません」を返します	AU はクラスター管理 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に変更します
エラー:「7 モード ファイラーはサポートされていません」	このデータ コレクターを使用して 7 モード ファイラーを検出すると、この問題が発生する可能性があります。代わりに、IP を変更して cdot ファイラーを指すようにします。
再試行後にZAPIコマンドが失敗する	AU はクラスターとの通信に問題があります。ネットワーク、ポート番号、IP アドレスを確認します。ユーザーは、AU マシンのコマンド ラインからコマンドを実行することも試みる必要があります。

問題：	これを試してください:
AUはZAPIへの接続に失敗しました	IP/ポート接続を確認し、ZAPI 構成を確認します。
AUはHTTP経由でZAPIに接続できませんでした	ZAPI ポートがプレーンテキストを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、通信は失敗します。
SSLException により通信が失敗しました	AU は、ファイラー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 ポートが SSL を受け入れるかどうかを確認するか、別のポートを使用します。
追加の接続エラー: ZAPI 応答にエラー コード 13001、「データベースが開いていません」が含まれています。ZAPI エラー コードは 60 で、応答には「API が時間どおりに終了しませんでした」が含まれています。ZAPI 応答には「initialize_session() が NULL 環境を返しました」が含まれています。ZAPI エラー コードは 14007 で、応答には「ノードが正常ではありません」が含まれています。	ネットワーク、ポート番号、IP アドレスを確認します。ユーザーは、AU マシンのコマンド ラインからコマンドを実行することも試みる必要があります。
ZAPI のソケットタイムアウトエラー	ファイラーの接続を確認し、タイムアウトを増やしてください。
「Cモードクラスタは7モードデータソースではサポートされていません」というエラー	IP を確認し、IP を 7 Mode クラスターに変更します。
「vFilerへの接続に失敗しました」エラー	取得するユーザーの機能に少なくとも以下が含まれていることを確認します: api-* security-api-vfiler login-http-admin ファイラーが少なくとも ONTAPI バージョン 1.7 を実行していることを確認します。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

NetApp Eシリーズ レガシー **Santricity API** データコレクター

NetApp E シリーズ レガシー Santricity API データ コレクターは、インベントリとパフォーマンス データを収集します。コレクターは、同じ構成を使用して同じデータを報告するファームウェア 7.x+ をサポートします。

用語

Cloud Insights は、 NetApp E シリーズ データ コレクターから次のインベントリ情報を取得します。取得した資産の種類ごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ボリューム グループ	ストレージ プール
Volume	Volume

注: 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 コレクターのすべてのケースを反映しているわけではありません。

Eシリーズ用語集（ランディングページ）

次の用語は、 NetApp E シリーズ アセット ランディング ページに表示されるオブジェクトまたは参照に適用されます。これらの条件の多くは、他のデータ収集者にも適用されます。

ストレージ

- モデル – デバイスのモデル名。
- ベンダー – 新しいデータソースを構成する場合に表示されるのと同じベンダー名
- シリアル番号 – アレイのシリアル番号。 NetApp Clustered Data Ontapのような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」のシリアル番号ほど役に立たない場合があります。
- IP – 通常はデータソースで設定されたIPまたはホスト名になります
- マイクロコードバージョン – ファームウェア
- 生の容量 – システム内のすべての物理ディスクの2を底とする合計（役割に関係なく）
- レイテンシ – 読み取りと書き込みの両方において、ホスト側のワークロードが経験している状況を表します。理想的には、 Data Infrastructure Insightsがこの値を直接取得しますが、多くの場合そうではありません。アレイがこれを提供する代わりに、 Data Infrastructure Insights は通常、個々のボリュームの統計から導き出された IOPS 加重計算を実行します。
- スループット – アレイのホスト側スループットの合計。理想的にはアレイから直接取得されますが、利用できない場合は、Data Infrastructure Insightsがボリュームのスループットを合計してこの値を導き出します。
- 管理 – これにはデバイスの管理インターフェイスへのハイパーリンクが含まれる場合があります。在庫レポートの一部として、Data Infrastructure Insightsサイト データソースによってプログラム的に作成されます。

ストレージ プール

- ストレージ – このプールが存在するストレージ アレイ。必須
- タイプ – 可能性のある列挙リストからの説明的な値。最も一般的なのは「シンプロビジョニング」または「RAIDグループ」です。
- ノード – このストレージアレイのアーキテクチャで、プールが特定のストレージノードに属している場合、その名前は独自のランディングページへのハイパーリンクとしてここに表示されます。
- フラッシュプールを使用する – はい/いいえの値
- 冗長性 – RAID レベルまたは保護スキーム。 EシリーズはDDPプールに対して「RAID 7」を報告します
- 容量 – ここでの値は、論理的に使用されている容量、使用可能な容量、論理的な合計容量、およびこれらの間で使用されている割合です。これらの値にはEシリーズの「保存」容量が含まれており、数値とパー

センテージはEシリーズのユーザーインターフェースに表示されるものよりも高くなります。

- 過剰コミット容量 – 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容量の合計を割り当てた場合、ここでのパーセンテージ値は 0% より大きくなります。
- スナップショット – ストレージプールアーキテクチャがスナップショット専用のセグメント領域に容量の一部を割り当てている場合、使用されているスナップショット容量と合計容量
- 使用率 – このストレージ プールに容量を提供しているディスクのうち最も高いディスク使用率を示すパーセンテージ値。ディスク使用率は、必ずしもアレイのパフォーマンスと強い相関関係があるわけではありません。ホスト駆動型のワークロードがない場合、ディスクの再構築、重複排除アクティビティなどにより、使用率が高くなる可能性があります。また、多くのアレイのレプリケーション実装では、ボリュームのワークロードとして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 プールに容量を提供し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でディスクIOPSが利用できない場合、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。
- スループット – このストレージ プールに容量を提供しているすべてのディスクの合計スループット。特定のプラットフォームでディスクスループットが利用できない場合、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スループットの合計から取得されます。

ストレージ ノード

- ストレージ – このノードが属するストレージ アレイ。必須
- HAパートナー – ノードが他の1つのノードにのみフェイルオーバーするプラットフォームでは、通常ここに表示されます。
- 状態 – ノードの健全性。アレイがデータソースによってインベントリされるのに十分健全な場合にのみ使用可能
- モデル – ノードのモデル名
- バージョン – 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 – 利用可能な場合は2進メモリ
- 使用率 – 通常は CPU 使用率の数値ですが、 NetApp Ontap の場合はコントローラのストレス インデックスです。 NetApp Eシリーズでは現在利用できません
- IOPS – このコントローラー上のホスト駆動 IOPS を表す数値。理想的にはアレイから直接取得されますが、利用できない場合は、このノードに排他的に属するボリュームのすべての IOP を合計することによって計算されます。
- レイテンシ – このコントローラー上の典型的なホストレイテンシまたは応答時間を表す数値。理想的にはアレイから直接取得されますが、利用できない場合は、このノードに排他的に属するボリュームから IOPS 加重計算を実行して計算されます。
- スループット – このコントローラー上のホスト駆動スループットを表す数値。理想的にはアレイから直接取得されますが、利用できない場合は、このノードに排他的に属するボリュームのすべてのスループットを合計することによって計算されます。
- プロセッサ – CPU数

要件

- アレイ上の各コントローラのIPアドレス
- ポート要件 2463

構成

フィールド	説明
アレイSANtricityコントローラIPのコンマ区切りリスト	アレイコントローラのIPアドレスおよび/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は最大3600秒	デフォルトは300秒です

トラブルシューティング

このデータ収集装置に関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

NetApp Eシリーズ **REST**データコレクター

NetApp E シリーズ REST データ コレクターは、インベントリ、ログ、パフォーマンス データを収集します。コレクターは、同じ構成を使用して同じデータを報告するファームウェア 7.x+ をサポートします。 REST コレクターは、ストレージ プール、ディスク、ボリュームの暗号化ステータス、ストレージ ノードの CPU 使用率を監視し、従来のSANtricity E シリーズ コレクターでは提供されていないログ機能も提供します。

用語

Data Infrastructure Insights 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。取得した資産の種類ごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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
Volume	Volume

注: 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 コレクターのすべてのケースを反映している

わけではありません。

要件

- アレイ上の各コントローラのIPアドレス
- このコレクターは、*ネイティブ 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 シリーズ組織は、古い E シリーズ アレイ用に、アレイ外でインストール可能な REST API ディストリビューションを出荷します。このコレクターでは、そのシナリオはサポートされていません。古いアレイをお使いのユーザーは、引き続きData Infrastructure Insightsを使用してください。"EシリーズSANtricity API"コレクタ。
- 「E シリーズ コントローラの IP アドレス」フィールドは、2 つの IP/ホスト名のコンマ区切り文字列をサポートします。コレクターは、最初の IP/ホスト名にアクセスできない場合、インテリジェントに 2 番目の IP/ホスト名を試行します。
- HTTPS ポート: デフォルトは 8443 です。

構成

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カンマ区切りの IP アドレスおよび/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は最大3600秒	デフォルトは300秒です

Eシリーズ用語集（ランディングページ）

次の用語は、 NetApp E シリーズ アセット ランディング ページに表示されるオブジェクトまたは参照に適用されます。これらの条件の多くは、他のデータ収集者にも適用されます。

ストレージ

- モデル – デバイスのモデル名。
- ベンダー – 新しいデータソースを構成する場合に表示されるのと同じベンダー名
- シリアル番号 – アレイのシリアル番号。 NetApp Clustered Data Ontapのような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」のシリアル番号ほど役に立たない場合があります。
- IP – 通常はデータソースで設定されたIPまたはホスト名になります
- マイクロコードバージョン – ファームウェア
- 生の容量 – システム内のすべての物理ディスクの2を底とする合計（役割に関係なく）
- レイテンシ – 読み取りと書き込みの両方において、ホスト側のワークロードが経験している状況を表します。理想的には、 Data Infrastructure Insightsがこの値を直接取得しますが、多くの場合そうではありません。アレイがこれを提供する代わりに、 Data Infrastructure Insights は通常、個々のボリュームの統計から導き出された IOPS 加重計算を実行します。

- スループット – アレイのホスト側スループットの合計。理想的にはアレイから直接取得されますが、利用できない場合は、Data Infrastructure Insightsがボリュームのスループットを合計してこの値を導き出します。
- 管理 – これにはデバイスの管理インターフェイスへのハイパーリンクが含まれる場合があります。在庫レポートの一部として、Data Infrastructure Insightsサイト データソースによってプログラム的に作成されます。

ストレージ プール

- ストレージ – このプールが存在するストレージ アレイ。必須
- タイプ – 可能性のある列挙リストからの説明的な値。最も一般的なのは「シンプロビジョニング」または「RAIDグループ」です。
- ノード – このストレージアレイのアーキテクチャで、プールが特定のストレージノードに属している場合、その名前は独自のランディングページへのハイパーリンクとしてここに表示されます。
- フラッシュプールを使用する – はい/いいえの値
- 冗長性 – RAID レベルまたは保護スキーム。 EシリーズはDDPプールに対して「RAID 7」を報告します
- 容量 – ここでの値は、論理的に使用されている容量、使用可能な容量、論理的な合計容量、およびこれらの間で使用されている割合です。これらの値にはEシリーズの「保存」容量が含まれており、数値とパーセンテージはEシリーズのユーザーインターフェースに表示されるものよりも高くなります。
- 過剰コミット容量 – 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容量の合計を割り当てた場合、ここでのパーセンテージ値は 0% より大きくなります。
- スナップショット – ストレージプールアーキテクチャがスナップショット専用のセグメント領域に容量の一部を割り当てている場合、使用されているスナップショット容量と合計容量
- 使用率 – このストレージ プールに容量を提供しているディスクのうち最も高いディスク使用率を示すパーセンテージ値。ディスク使用率は、必ずしもアレイのパフォーマンスと強い相関関係があるわけではありません。ホスト駆動型のワークロードがない場合、ディスクの再構築、重複排除アクティビティなどにより、使用率が高くなる可能性があります。また、多くのアレイのレプリケーション実装では、ボリュームのワークロードとして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 プールに容量を提供し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でディスクIOPSが利用できない場合、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。
- スループット – このストレージ プールに容量を提供しているすべてのディスクの合計スループット。特定のプラットフォームでディスクスループットが利用できない場合、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スループットの合計から取得されます。

ストレージ ノード

- ストレージ – このノードが属するストレージ アレイ。必須
- HAパートナー – ノードが他の1つのノードにのみフェイルオーバーするプラットフォームでは、通常ここに表示されます。
- 状態 – ノードの健全性。アレイがデータソースによってインベントリされるのに十分健全な場合にのみ使用可能
- モデル – ノードのモデル名
- バージョン – 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 – 利用可能な場合は2進メモリ
- 使用率 – 通常は CPU 使用率の数値ですが、 NetApp Ontap の場合はコントローラのストレス インデックスです。 NetApp Eシリーズでは現在利用できません
- IOPS – このコントローラー上のホスト駆動 IOPS を表す数値。理想的にはアレイから直接取得されますが、利用できない場合は、このノードに排他的に属するボリュームのすべての IOP を合計することによって計算されます。
- レイテンシ – このコントローラー上の典型的なホストレイテンシまたは応答時間を表す数値。理想的にはアレイから直接取得されますが、利用できない場合は、このノードに排他的に属するボリュームから IOPS 加重計算を実行して計算されます。
- スループット – このコントローラー上のホスト駆動スループットを表す数値。理想的にはアレイから直接取得されますが、利用できない場合は、このノードに排他的に属するボリュームのすべてのスループットを合計することによって計算されます。
- プロセッサ – CPU数

トラブルシューティング

このデータ収集装置に関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

NetApp HCI管理サーバーのデータコレクターの構成

NetApp HCI管理サーバーのデータ コレクターは、 NetApp HCIホスト情報を収集し、管理サーバー内のすべてのオブジェクトに対する読み取り専用権限を必要とします。

このデータ コレクターは、* NetApp HCI管理サーバーからのみ* を取得します。ストレージシステムからデータを収集するには、"NetApp SolidFire"データ収集者。

用語

Data Infrastructure Insights は、このデータ コレクターから次のインベントリ情報を取得します。取得した資産の種類ごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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	Volume
ファイバーチャネルポート	ポート

これらは一般的な用語のマッピングのみであり、このデータ コレクターのすべてのケースを反映しているわけではありません。

要件

このデータ コレクターを構成するには、次の情報が必要です。

- NetApp HCI管理サーバーの IP アドレス
- NetApp HCI管理サーバーの読み取り専用のユーザー名とパスワード
- NetApp HCI管理サーバー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管理サーバー上の SDK アクセス – 通常は既に設定されています。
- ポート要件: http-80 https-443
- アクセスを検証:
  - 上記のユーザー名とパスワードを使用してNetApp HCI管理サーバーにログインします。
  - 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
Name	データコレクターの一意の名前
買収ユニット	買収ユニット名

構成

フィールド	説明
NetApp HCIストレージ クラスター 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管理サーバーにアクセスするために使用するユーザー名
パスワード	NetApp HCI管理サーバーにアクセスするために使用するパスワード
VCenterユーザー名	VCenterのユーザー名
VCenter パスワード	VCenterのパスワード

高度な設定

詳細構成画面で、**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	クラスタ、データセンター、またはESXホストを選択
リストを指定するには「除外」または「含める」を選択します	VMを含めるか除外するかを指定する

デバイスリストをフィルタリング	ESX_HOST、CLUSTER、および DATACENTER のみによるフィルタリングの場合、フィルタリングする VM のリスト (カンマ区切り、または値にカンマが使用されている場合はセミコロン区切り)
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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
エラー: VM をフィルタリングするための包含リストは空にできません	包含リストを選択した場合は、VM をフィルタリングするために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ください。
エラー: IP の 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: * 入力した資格情報と IP アドレスを確認します。 * Infrastructure Client を使用して Virtual Center との通信を試みます。 * 管理対象オブジェクト ブラウザー (MOB など) を使用して仮想センターとの通信を試みます。
エラー: IP の VirtualCenter には、JVM に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 (例: 1024 ビット) RSA キーを使用して、Virtual Center の証明書を再生成します。 * 非推奨: JVM java.security 構成を変更して、制約 jdk.certpath.disabledAlgorithms を活用し、512 ビットの RSA キーを許可します。 JDK 7アップデート40のリリースノートについては、"http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

NetApp SolidFireオールフラッシュアレイ データコレクター

NetApp SolidFireオールフラッシュ アレイ データ コレクターは、iSCSI とファイバー チャネルの両方の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 コレクターはSolidFire REST API を利用します。データ コレクターが存在する取得ユニットは、 SolidFireクラスター管理 IP アドレスの TCP ポート 443 への HTTPS 接続を開始できる必要があります。データ コレクターには、 SolidFireクラスターで REST API クエリを実行できる資格情報が必要です。

用語

Data Infrastructure Insights は、 NetApp SolidFire All-Flash Array データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするとき

は、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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
Volume	Volume
ファイバーチャネルポート	ポート
ボリュームアクセスグループ、LUN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マッピングのみであり、このデータ コレクターのすべてのケースを反映しているわけではありません。

要件

このデータ コレクターを構成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ー名と資格情報
- ポート443

構成

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
ユーザー名	SolidFireクラスタにログインするために使用する名前
パスワード	SolidFireクラスタにログインするため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
通信ポート	NetApp API に使用されるポート
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 がエラーを報告すると、 Data Infrastructure Insightsに次のように表示されます。

データを取得しようとしたときに、 *SolidFire*デバイスからエラー メッセージが受信されました。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 *(*デバイスのマニュアルを確認してください*):* <メッセージ>

各値の意味は次のとおりです。

- <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のコンマ区切りリストです。
- <message> は、デバイスがエラー メッセージとして返した内容です。

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

NetApp StorageGRIDデータコレクター

NetApp StorageGRIDデータ コレクターは、 StorageGRID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。

> 基盤となるハードウェア トポロジと構成に関係なく、すべてのStorageGRIDシステムにわたって DII 権限に対する一貫した計測を提供するために、 Data Infrastructure Insights は、物理ディスク レイアウトに基づく RAW 容量ではなく、使用可能な合計容量 (storagegrid_storage_utilization_total_space_bytes) を使用します。
>
> 容量ベースのライセンス モデルを使用しているお客様の場合、 StorageGRIDは「オブジェクト」ストレージとして計測されます。
>
> 従来の (MU) ライセンス モデルを使用しているお客様の場合、 StorageGRIDはセカンダリ ストレージとして 40TiB から 1 MU のレートで計測されます。

用語

Data Infrastructure Insights は、 NetApp StorageGRIDコレクターから次のインベントリ情報を取得します。取得した資産の種類ごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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	内部容積

要件

このデータ ソースを構成するための要件は次のとおりです。

- StorageGRIDホスト IP アドレス
- メトリッククエリとテナントアクセスのロールが割り当てられたユーザーのユーザー名とパスワード
- ポート 443（または設定されている場合は 8443）

構成

フィールド	説明
StorageGRIDホスト IP アドレス	StorageGRID（Grid Manager）の管理IPアドレス
ユーザー名	StorageGRID（Grid Manager）へのログインに使用する名前
パスワード	StorageGRID（Grid Manager）へのログインに使用するパスワード

高度な設定

フィールド	説明
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**）

その"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バージョン	シングルサインオン（SSO）をサポート
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

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

Nutanix NX データコレクター

Data Infrastructure Insights は、 Nutanix データ コレクターを使用して、Nutanix NX ストレージ システムのインベントリとパフォーマンス データを検出します。

用語

Data Infrastructure Insights は、 Nutanix データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ストレージ プール	ストレージ プール

ベンダー/モデル用語	**Data Infrastructure Insights**用語
Nutanixコンテナ	内部容積
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マッピングのみであり、このデータ コレクターのすべてのケースを反映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IPアドレス
- 読み取り専用のユーザー名とパスワード（ボリューム グループが使用されていない場合）。ボリューム グループが使用されている場合は、管理者のユーザー名とパスワードが必要です。
- ポート要件: HTTPS 443

構成

フィールド	説明
Prism外部IPアドレス	クラスタの外部データサービスIPアドレス
ユーザ名	管理者アカウントのユーザー名
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 アレイに接続するために使用される TCP ポート。デフォルトは 9440 です。
インベントリポーリング間隔（分）	インベントリ ポーリングの間隔。デフォルトは60分です。
パフォーマンスポーリング間隔(秒)	パフォーマンス ポーリングの間隔。デフォルトは300秒です。

トラブルシューティング

このデータコレクターに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

Oracle ZFS Storage Appliance データコレクター

Data Infrastructure Insights は、 Oracle ZFS Storage Appliance データ コレクターを使用して、インベントリおよびパフォーマンス データを収集します。

用語

Data Infrastructure Insights は、 Oracle ZFS データ コレクターを使用してインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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	Volume
LUN マップ	ボリュームマップ
イニシエーター、ターゲット	ボリュームマスク
共有	内部容積

注: 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 ソースのすべてのケースを反映しているわけではありません。

要件

- ZFS コントローラ 1 と ZFS コントローラ 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メトリック

Oracle ZFS アプライアンスは、ストレージ管理者にパフォーマンス統計をキャプチャするための大きな柔軟性を提供します。 Data Infrastructure Insights、高可用性ペアの各コントローラーが次のメトリックをキャプチャするように構成されている必要があります。

- smb2.ops[共有]
- nfs3.ops[共有]
- nfs4.ops[共有]
- nfs4-1.ops[共有]

コントローラーがこれらのいずれかまたはすべてをキャプチャできない場合、 Data Infrastructure Insights は「内部ボリューム」のワークロードを把握しないか、または過少に報告する可能性があります。

構成

フィールド	説明
ZFSコントローラ1のホスト名	ストレージコントローラ1のホスト名
ZFSコントローラ2のホスト名	ストレージコントローラ2のホスト名

フィールド	説明
ユーザ名	ストレージ システム管理者ユーザー アカウントのユーザー名
パスワード	管理者ユーザー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、デフォルトのポートも表示します
接続ポートのオーバーライド	空白の場合は、接続タイプフィールドの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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
「ログイン資格情報が無効です」	Zfsユーザーアカウントとパスワードを検証する
「リクエストはステータス 404 で失敗しました https://…..:215/api/access/v1」	ZFS アレイが古すぎて、REST API をサポートできない可能性があります。 AK 2013.1.3.0 は、REST API 対応の最初の ZFS OS リリースであり、すべての ZFS アプライアンスがこのリリースにアップグレードできるわけではありません。
「構成エラー」と「REST サービスが無効です」というエラー メッセージ	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。

問題：	これを試してください:
「構成エラー」とエラーメッセージ「コマンドを実行する権限のないユーザー」	このエラーは、構成されたユーザーに特定のロール (たとえば、「advanced_analytics」) が含まれていないことが原因であ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可能性があります。次の手順を実行します。 1. ZFsシステムでは、「構成」→「ユーザー」画面で、マウスをロールの上に移動し、ダブルクリックして編集を許可します。 2. 「スコープ」ドロップダウン メニューから「分析」を選択します。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。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Pure Storage FlashArray データコレクター

Data Infrastructure Insights は、Pure Storage FlashArray データ コレクターを使用して、インベントリとパフォーマンス データを収集します。

用語

Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**用語
ドライブ（SSD）	ディスク
アレイ	ストレージ
コントローラ	ストレージ ノード
Volume	Volume
LUN マップ	ボリュームマップ
イニシエーター、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マッピングのみであり、このデータ コレクターのすべてのケースを反映している

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 システムの管理者アカウントのユーザー名とパスワード。
- ポート要件: HTTP/HTTPS 80/443

構成

フィールド	説明
FlashArrayホストIPアドレス	ストレージシステムのIPアドレス
ユーザ名	管理者権限を持つユーザー名
管理者権限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
接続の種類	[HTTP]または[HTTPS]を選択します。デフォルトのポートも表示します。
TCPポートを上書きする	空白の場合は、接続タイプフィールドの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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
「無効なログイン資格情報」と「ポリシーにより許可されていません」または「権限がありません」というエラー メッセージが表示される	Pure http インターフェース経由で Pure ユーザー アカウントとパスワードを検証します

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Red Hat Virtualization データコレクター

Data Infrastructure Insights は、 Red Hat Virtualization データコレクターを使用して、仮想化された Linux および Microsoft Windows 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

Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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
論理ユニット	LUN

注: 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 コレクターのすべてのケースを反映しているわけではありません。

要件

- REST API 経由のポート 443 経由の RHEV サーバーの IP アドレス
- 読み取り専用のユーザー名とパスワード
- RHEV バージョン 3.0 以上

構成

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	管理者権限を持つユーザー名
管理者権限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ーに関する追加情報は、"サポート"ページまたは"データコレクターサポートマトリックス"。

Rubrik CDM データコレクター

Data Infrastructure Insights は、 Rubrik データ コレクターを使用して、Rubrik ストレージ アプライアンスからインベントリ データとパフォーマンス データを取得します。

用語

Data Infrastructure Insights は、 Rubrik データ コレクターから次のインベントリ情報を取得します。 Data Infrastructure Insightsによって取得された資産タイプごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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マッピングのみであり、このデータ ソースのすべてのケースを反映しているわけではありません。

要件

このデータ コレクターを構成するには、次のものが必要です。

- Data Infrastructure Insights取得ユニットは、Rubrik クラスターへの TCP ポート 443 への接続を開始します。クラスターごとに 1 つのコレクター。
- Rubrik クラスターの IP アドレス。
- クラスターへのユーザー名とパスワード。
- Rubrik クラスターの IP アドレスまたはホスト名。
- 基本認証の場合、クラスターへのユーザー名とパスワード。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、組織IDが必要です。
- ポート要件: HTTPS 443

構成

フィールド	説明
IP	Rubrik クラスタの IP アドレス
ユーザー名 / サービスアカウント	クラスターのユーザー名
パスワード/シークレット	クラスターのパスワード
サービスアカウントの組織ID	これは、「Organization:::nnnnnn-nnnn.....」のような完全な文字列である必要があります。

高度な設定

インベントリポーリング間隔（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 コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
複数のストレージが作成されたというメッセージが表示されました。	クラスターが正しく構成され、コレクターが単一のクラスターを指していることを確認します。
ポーリングが 400 [Bad Request] で失敗しました… .ManagedId が無効です….	組織 ID フィールドに値を入力しましたが、Rubrik からのエラー メッセージで「ManagedId」と表示されているにもかかわらず、Rubrik クラスターではそれが有効な組織 ID であると認識されません。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

VMware VSphere データコレクターの構成

VMware vSphere のデータ コレクターは、VM ゲストおよび ESXi ホストのパフォーマンスと構成情報を収集し、vSphere 内のすべてのオブジェクトに対する読み取り専用権限を必要とします。 2024 年 8 月現在、vSphere コレクターは vSphere 環境からのログメッセージと、VMware 固有のメトリックも追加で取得します。 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ることに注意してください。同様に、ベンダー固有のメトリックは vSphere 7 以降の環境でのみサポートされます。そのため、特定のコレクターが古い vSphere インスタンスを指している場合は、そのコレクター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をお勧めします。

用語

Data Infrastructure Insights は、 VMware vSphere データ コレクターから次のインベントリ情報を取得します。取得した資産の種類ごとに、その資産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 コレクターを表示またはトラブルシューティングするときは、次の用語に留意してください。

ベンダー/モデル用語	**Data Infrastructure Insights**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	Volume
ファイバーチャネルポート	ポート

これらは一般的な用語のマッピングのみであり、このデータ コレクターのすべてのケースを反映しているわけではありません。

要件

このデータ コレクターを構成するには、次の情報が必要です。

- Virtual CenterサーバーのIPアドレス
- 仮想センターの読み取り専用のユーザー名とパスワード
- 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 サーバー上の SDK アクセス – 通常はすでに設定されています。
- ポート要件: http-80 https-443
- アクセスを検証:
  - 上記のユーザー名とパスワードを使用してVirtual Centerクライアントにログインします。
  - 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
Name	データコレクターの一意の名前
買収ユニット	買収ユニット名

構成

フィールド	説明
仮想センターIPアドレス	仮想センターのIPアドレス
ユーザ名	仮想センターへのアクセスに使用するユーザー名
パスワード	仮想センターにアクセスするために使用するパスワード

高度な設定

詳細構成画面で、**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をフィルタリングする	クラスタ、データセンター、またはESXホストを選択
リストを指定するには「除外」または「含める」を選択します	フィルター リスト (CLUSTER、DATACENTER、ESX_HOST) を作成します。
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 リストをフィルター…	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 の両方で報告される ESX ホストの正確な「名前」のコンマ区切りリストを作成する必要があります。これらの「名前」は、IP アドレス、単純なホスト名、または完全修飾ドメイン名 (FQDN) のいずれかになります。これは、これらのホストが最初に vSphere に追加されたときにどのように命名されたかによって決まります。 CLUSTER でフィルタリングする場合は、ハイパーバイザー上の CI によって報告されるData Infrastructure Insightsスタイルのクラスター名を使用します - Data Infrastructure Insights はvSphere クラスター名の前に vSphere データセンター名とスラッシュを追加します - 「DC1/clusterA」は、データセンター DC1 内の clusterA のハイパーバイザーについてData Infrastructure Insightsが報告するクラスター名です。
パフォーマンスポーリング間隔（秒）	デフォルトは300です

VMware タグを**Data Infrastructure Insights** のアノテーションにマッピングする

VMware データ コレクターを使用すると、VMware で構成されたタグを使用して、 Data Infrastructure Insights の注釈を入力できます。 DII アノテーション名は VMware カテゴリ 名と同一である必要があります。タグは、カテゴリと同じ名前の DII アノテーションのアノテーション値として適用されます。 Data Infrastructure Insights は、常に同じ名前のテキスト タイプの注釈を入力し、他のタイプ (数値、ブール値など) の注釈を入力するように「最善の試み」を行います。注釈が別のタイプであり、データ コレクターが注釈を入力できない場合は、注釈を削除してテキスト タイプとして再作成する必要がある場合があります。

VMware タグでは大文字と小文字が区別される場合がありますが、 Data Infrastructure Insightsタグでは大文字と小文字は区別されないことに注意してください。したがって、 Data Infrastructure Insightsで「OWNER」という名前の注釈を作成し、VMware で「OWNER」、「Owner」、「owner」という名前のタグを作成すると、「owner」のこれらすべてのバリエーションが Cloud Insight の「OWNER」注釈にマッピングされます。

次の事項に注意してください。

- Data Infrastructure Insights は現在、 NetAppデバイスのサポート情報のみを自動公開します。
- このサポート情報は注釈形式で保持されるため、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。
- ユーザーが注釈の値を上書きまたは空にした場合、 Data Infrastructure Insightsが注釈を更新するときに (1 日に 1 回)、値が再度自動入力されます。

トラブルシューティング

このデータ コレクターで問題が発生した場合に試すことができるいくつかのこと:

インベントリ

問題：	これを試してください:
エラー: VM をフィルタリングするための包含リストは空にできません	包含リストを選択した場合は、VM をフィルタリングするために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ください。
エラー: IP の 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: * 入力した資格情報と IP アドレスを確認します。 * VMware Infrastructure Client を使用して Virtual Center との通信を試みます。 * 管理対象オブジェクト ブラウザー (MOB など) を使用して仮想センターとの通信を試みます。
エラー: IP の VirtualCenter には、JVM に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 (例: 1024 ビット) RSA キーを使用して、Virtual Center の証明書を再生成します。 * 非推奨: JVM java.security 構成を変更して、制約 jdk.certpath.disabledAlgorithms を活用し、512 ビットの RSA キーを許可します。見る"JDK 7 アップデート 40 リリースノート" 。
「VMware ログ パッケージは、VMware バージョン 8.0.1 未満ではサポートされていません」というメッセージが表示されます。	ログ収集は、VMware バージョン 8.0.1 より前ではサポートされていません。 Data Infrastructure Insights 内のログ収集機能を使用する場合は、VI Center Infrastructure をバージョン 8.0.1 以降にアップグレードしてください。詳細については、こちらをご覧ください"こちらの技術情報"。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

データコレクターリファレンス - サービス

ノードデータ収集

Data Infrastructure Insights は、エージェントがインストールされているノードからメトリックを収集します。

インストール

1. **Observability > Collectors** から、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 コレクター (Kubernetes、Docker、Apache など) をインストールすると、ノード データ収集も構成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構成します。手順は、データ収集に使用し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の種類によって異なります。

オブジェクトとカウンター

次のオブジェクトとそのカウンターがノード メトリックとして収集されます。

オブジェクト	識別子:	属性:	データポイント:
ノードファイルシステム	ノードUUIDデバイスパスタイプ	ノードIP ノード名 ノードOSモード	空きiノード 空きiノード使用済みiノード合計 使用済み合計 使用済み合計

オブジェクト	識別子:	属性:	データポイント:
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 進行中の合計IOPS 読み取りバイト数（秒あたり） 読み取り時間 合計読み取り数（秒あたり） 加重IO時間 合計書き込みバイト数（秒あたり） 書き込み時間 合計書き込み数（秒あたり） 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
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 ユーザー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:	データポイント:
ノード	ノードUUID	ノードIP ノード名 ノードOS	カーネルのブート時間、カーネルのコンテキストスイッチ（1秒あたり）カーネルの使用可能なエントロピー、カーネル割り込み（1秒あたり）フォークされたカーネルプロセス（1秒あたり）メモリ、アクティブメモリ、使用可能メモリ、合計メモリ、使用可能メモリ、バッファメモリ、キャッシュメモリ、コミット制限、コミット済みメモリ、ダーティメモリ、空きメモリ上限、空きメモリ上限、合計メモリ、ヒュージページサイズ、メモリ、ヒュージページ、空きメモリ、ヒュージページ、合計メモリ下限、空きメモリ下限、合計メモリ、マップメモリ、ページテーブル、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、スワップ空きメモリ、スワップ合計メモリ、使用済みメモリ合計、使用済みメモリ合計、メモリ、vmallocチャンクメモリ、vmalloc使用済みメモリ合計、vmallocメモリ、使用済みメモリ、メモリ、ワイヤードメモリ、ライトバック、合計メモリ、ライトバック一時メモリ、メモリキャッシュフォールト、メモリ需要、ゼロフォールト、メモリページフォールト、メモリページ、メモリ、非ページメモリ、ページメモリ、キャッシュコアメモリ、スタンバイキャッシュ、通常メモリ、スタンバイキャッシュ、予約メモリ、遷移フォールト、プロセス、ブロックされたプロセス、デッドプロセス、アイドルプロセス、ページングプロセス、実行中のプロセススリープ中のプロセ

オブジェクト	識別子:	属性:	データポイント:
ノードネットワーク	ネットワークインターフェースノードUUID	ノード名 ノードIP ノードOS	受信バイト数 送信バイト数 送信パケット数 破棄された送信パケット数 エラー数 受信パケット数 破棄された受信パケット数 エラー数 受信パケット数 送信パケット数

セットアップ

セットアップとトラブルシューティングに関する情報は、"エージェントの設定"ページ。

ActiveMQ データコレクター

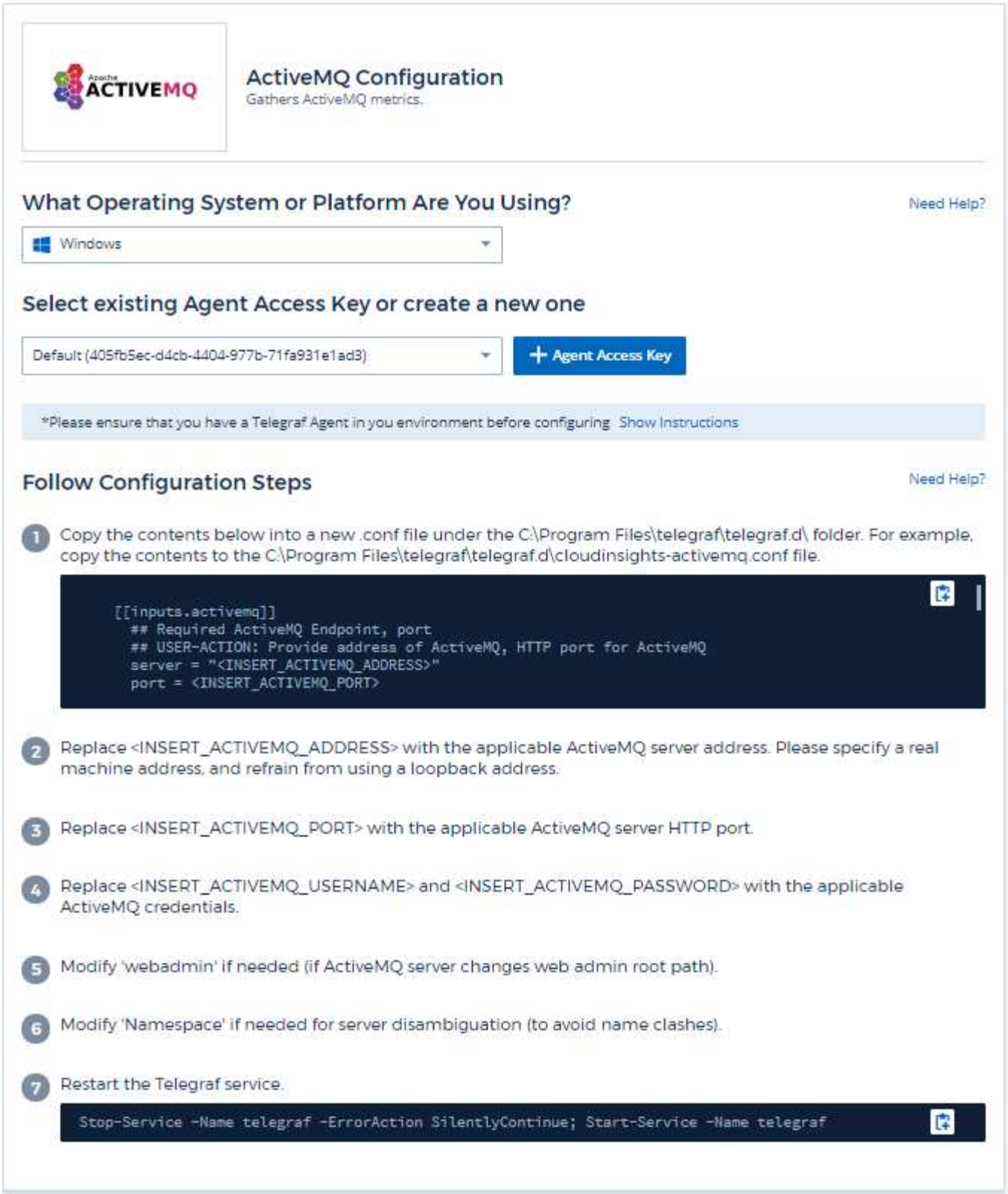
Data Infrastructure Insights は、このデータ コレクターを使用して ActiveMQ からメトリックを収集します。

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 ActiveMQを選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

詳細は以下をご覧ください。 "ActiveMQドキュメント"

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
ActiveMQ キュー	名前空間キューポートサーバー	ノード名 ノードIP ノードUUID	コンシューマー数 デキュー数 エンキュー数 キューサイズ
ActiveMQ サブスクライバー	クライアントID 接続ID ポート サーバー 名前空間	アクティブ宛先ノード名 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	デキュー数、ディスパッチ数、ディスパッチキューサイズ、エンキュー数、保留キューサイズ
ActiveMQトピック	トピックポートサーバー 名前空間	ノード名 ノードIP ノードUUID ノードOS	コンシューマー数 デキュー数 エンキュー数 サイズ

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

Apache データコレクター

このデータ コレクターを使用すると、テナント上の Apache サーバーからデータを収集できます。

前提条件

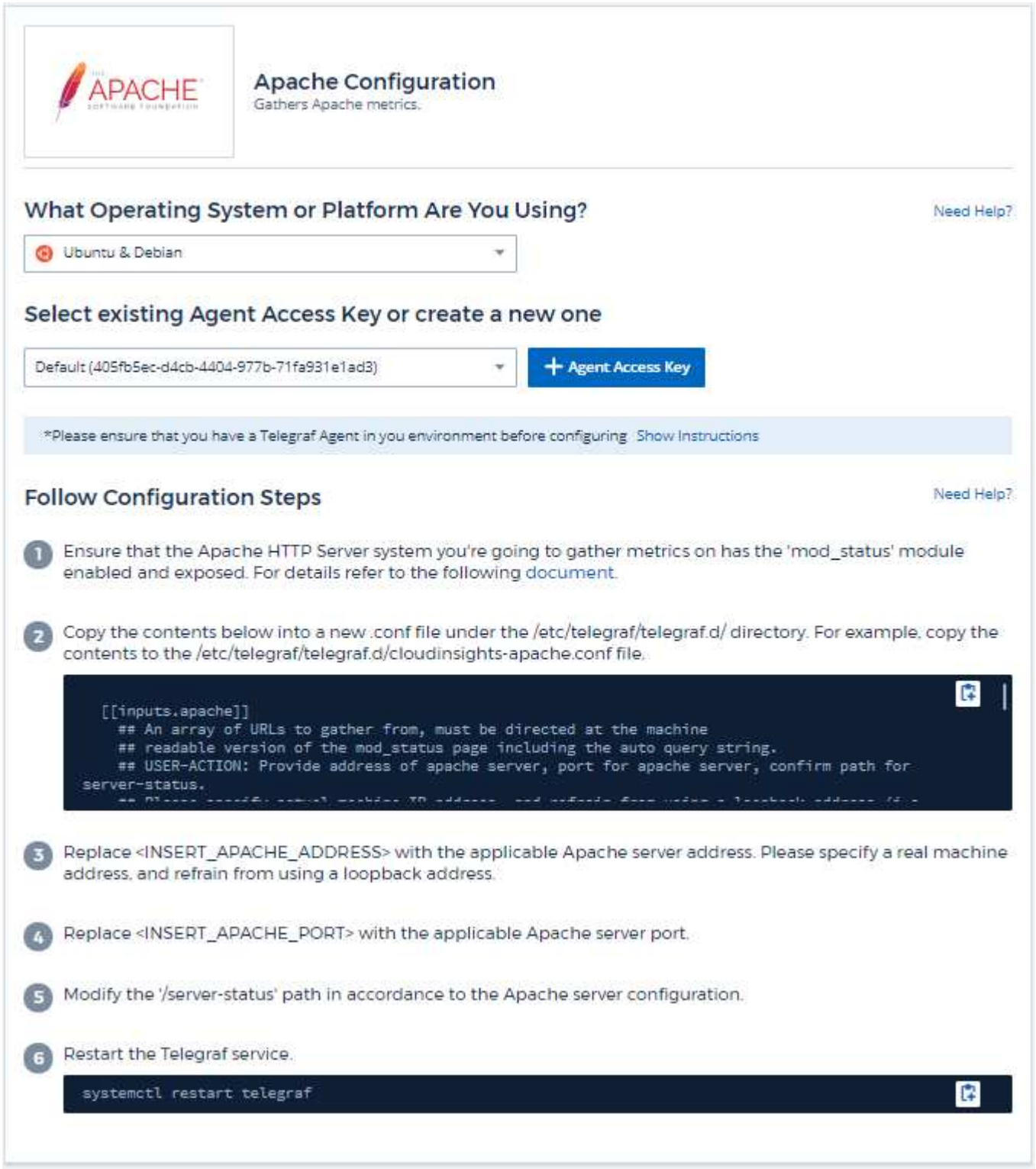
- Apache HTTP Serverがセットアップされ、適切に実行されている必要があります。
- エージェントホスト/VMに対するsudoまたは管理者権限が必要です
- 通常、Apache *mod_status* モジュールは、Apache サーバーの '/server-status?auto' の場所にページを公開するように構成されます。利用可能なすべてのフィールドを収集するには、*ExtendedStatus* オプションを有効にする必要があります。サーバーの設定方法については、Apache モジュールのドキュメントを参照してください。 https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 Apacheを選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

Apache の HTTP サーバー用の Telegraf プラグインは、'mod_status' モジュールが有効になっていることを前提としています。これを有効にすると、Apache の HTTP サーバーは、ブラウザーで表示したり、Apache の HTTP サーバーのすべての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る HTML エンドポイントを公開します。

互換性:

構成は、Apache の HTTP サーバー バージョン 2.4.38 に対して開発されました。

mod_status を有効にする:

「mod_status」モジュールを有効にして公開するには、次の 2 つの手順が必要です。

- 有効化モジュール
- モジュールから統計を公開する

有効化モジュール:

モジュールの読み込みは、「/usr/local/apache/conf/httpd.conf」の下の設定ファイルによって制御されます。設定ファイルを編集し、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
```

モジュールから統計を公開する:

'mod_status' の公開は、'/usr/local/apache2/conf/extra/httpd-info.conf' の下の設定ファイルによって制御されます。構成ファイルに次の内容が含まれてい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は含まれている必要があります)。

```
# 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
```

「mod_status」モジュールの詳細な手順については、"Apacheドキュメント"

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
アパッチ	名前空間サーバー	ノードIP ノード名 ポート 親サーバー構成生成 親サーバーMPM生成 サーバー稼働停止中	ビジーワーカー リクエストあたりのバイト数 1秒あたりのバイト数 CPU 子プロセス システム CPU 子プロセス ユーザープロセス CPU 負荷 システム CPU ユーザー 非同期接続 非同期接続のクローズ 維持 非同期接続 書き込み接続 リクエストあたりの合計継続時間 アイドルワーカー 平均負荷 (過去 1 分) 平均負荷 (過去 15 分) 平均負荷 (過去 5 分) プロセス 1 秒あたりのリクエスト数 合計アクセス数 合計継続時間 合計キロバイト数 スコアボード クローズ中 スコアボード DNS ルックアップ スコアボード 終了中 スコアボード アイドル クリーンアップ スコアボード 維持 スコアボード ログ記録中 スコアボード オープン中 スコアボード 読み取り中 スコアボード 送信中 スコアボード 開始中 スコアボード 待機中

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

領事データコレクター

Data Infrastructure Insights は、このデータ コレクターを使用して Consul からメトリックを収集します。

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。領事を選択してください。

   収集用のエージェントを設定していない場合は、"エージェントをインストールする"テナントに。

   エージェントがすでに構成されている場合は、適切なオペレーティング システムまたはプラットフォームを選択し、[続行] をクリックします。

2. Consul 構成画面の指示に従って、データ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。

セットアップ

詳細は以下をご覧ください。"領事文書" 。

領事館のオブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
領事	名前空間チェックID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 チェック名 サービスID ステータス	クリティカルパス警告

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

Couchbase データコレクター

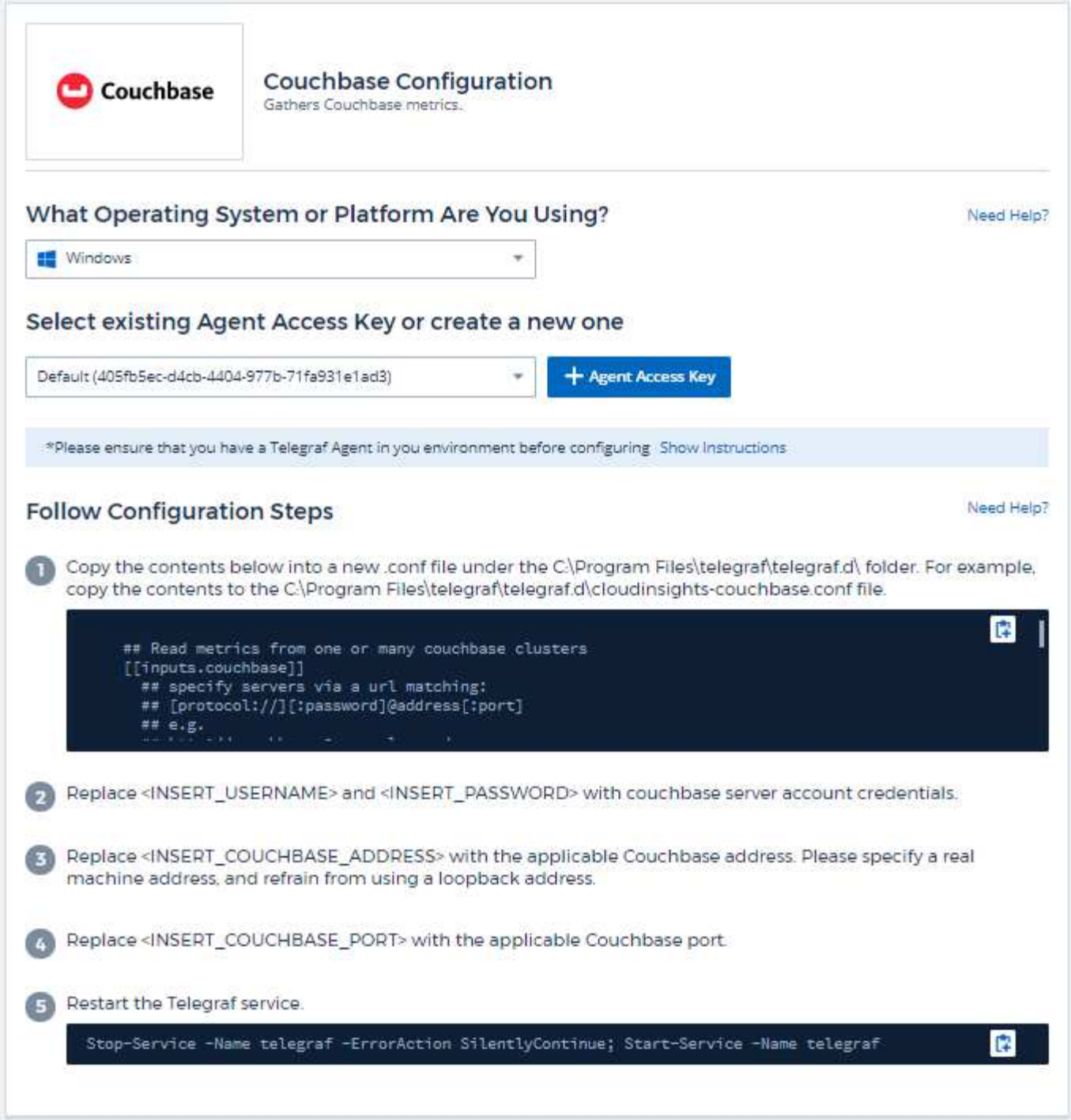
Data Infrastructure Insights は、このデータ コレクターを使用して Couchbase からメトリックを収集します。

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 Couchbaseを選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

詳細は以下をご覧ください。"Couchbaseのドキュメント" 。

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
カウチベースノード	名前空間 クラスタ Couchbase ノード ホスト名	ノード名 ノードIP	メモリ空き容量合計メモリ
カウチベースバケット	名前空間バケットクラスター	ノード名 ノードIP	使用データ データフェッチ 使用ディスク アイテム数 使用メモリ 1秒あたりの操作数 使用クォータ

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

CouchDB データコレクター

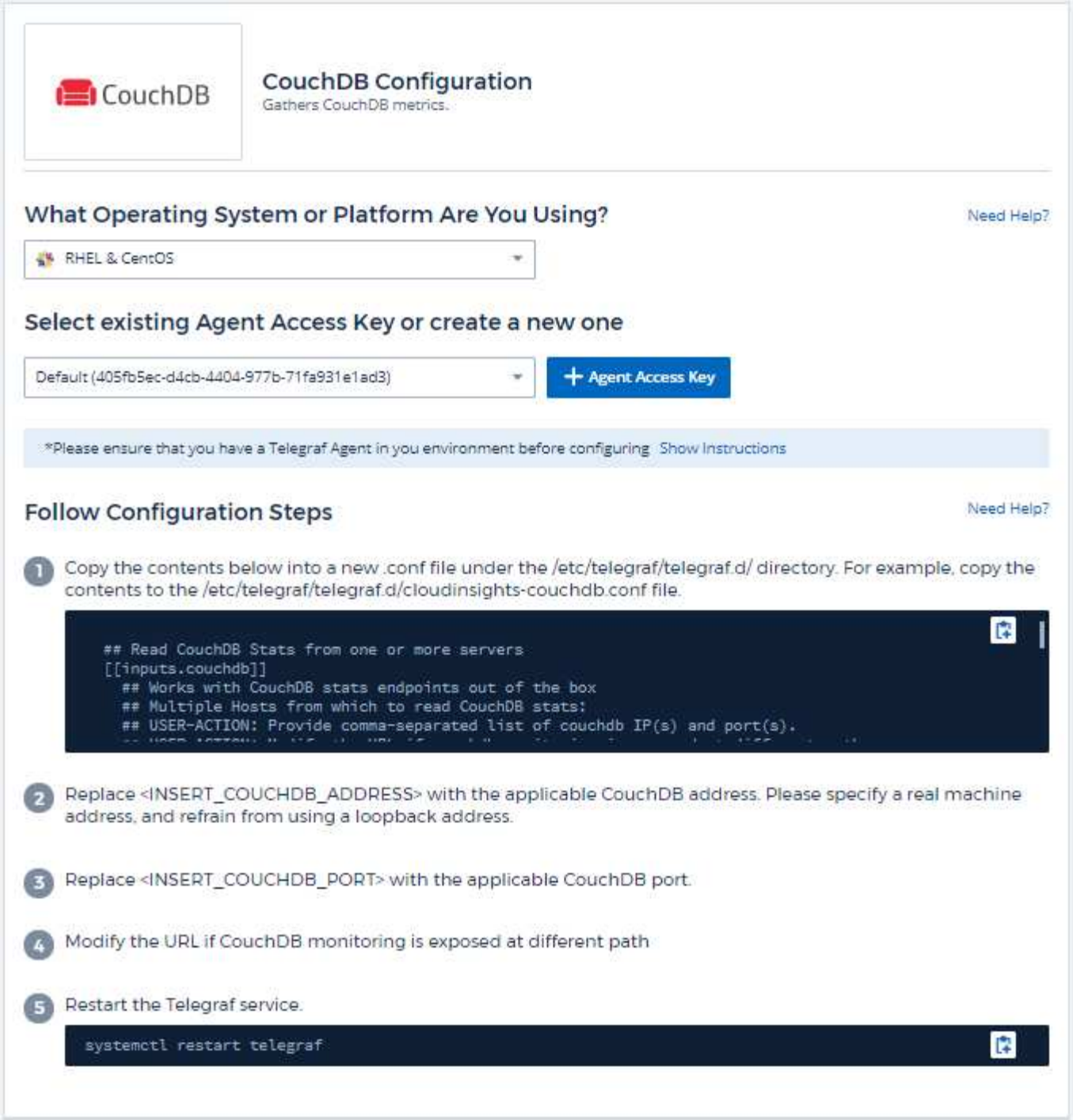
Data Infrastructure Insights は、このデータ コレクターを使用して CouchDB からメトリックを収集します。

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 CouchDB を選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

詳細は以下をご覧ください。"CouchDBのドキュメント" 。

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
カウチDB	名前空間サーバー	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 データベース読み取り データベース書き込み データベースオープン OS ファイル最大リクエスト時間 最小リクエスト時間 HTTP リクエストメソッド コピー HTTP リクエストメソッド 削除 HTTP リクエストメソッド 取得 HTTP リクエストメソッド ヘッド HTTP リクエストメソッド ポスト HTTP リクエストメソッド プット 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

追加情報は以下からご覧いただけます。"サポート"ページ。

Docker データコレクター

Data Infrastructure Insights は、このデータ コレクターを使用して Docker からメトリックを収集します。

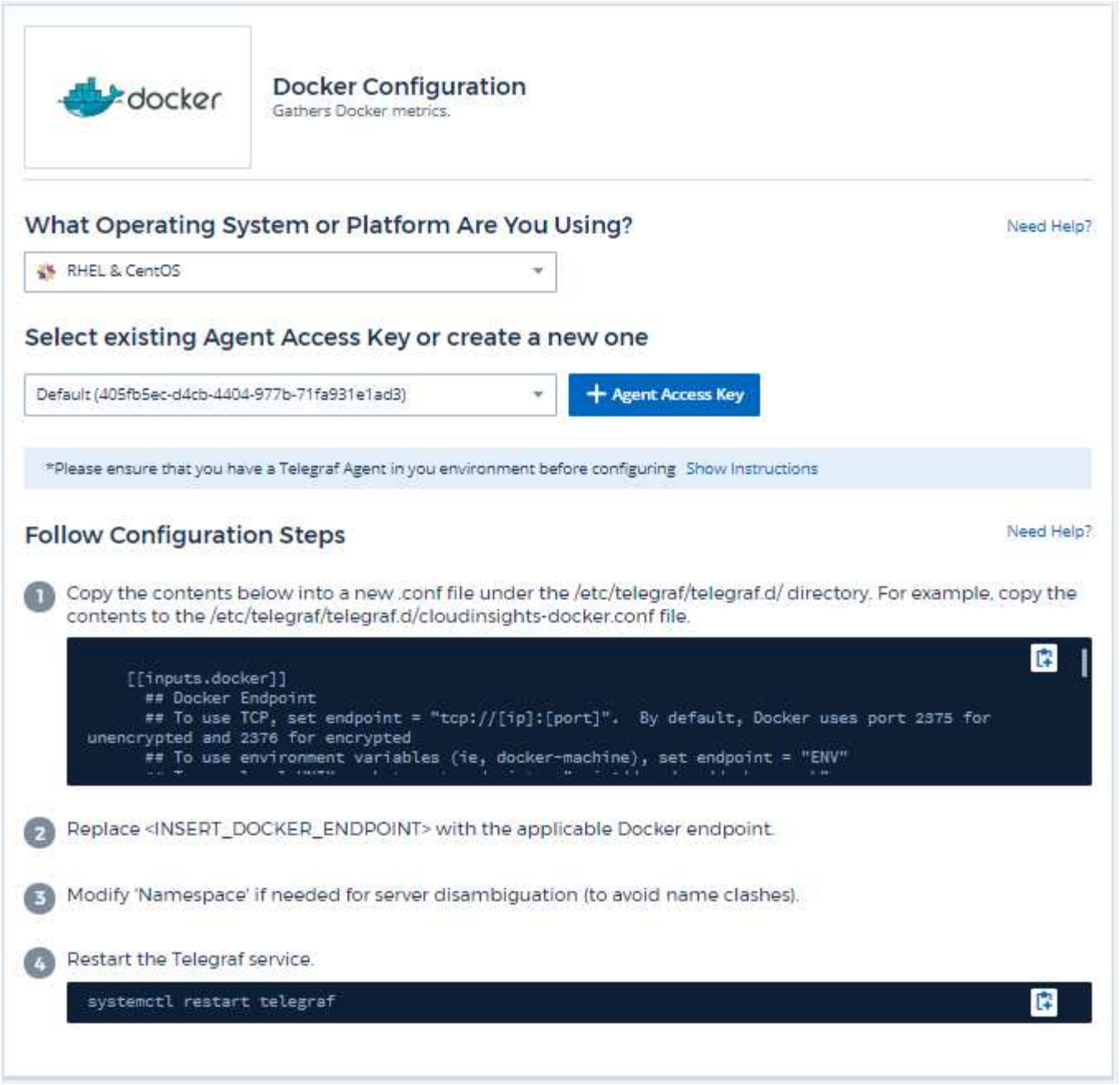
インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 Dockerを選択します。

   収集用のエージェントを設定していない場合は、"エージェントをインストールする"テナントに。

   エージェントがすでに構成されている場合は、適切なオペレーティング システムまたはプラットフォームを選択し、[続行] をクリックします。

2. Docker 構成画面の指示に従って、データ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

Docker 用の Telegraf 入力プラグインは、指定された UNIX ソケットまたは TCP エンドポイントを通じてメトリックを収集します。

互換性

構成は Docker バージョン 1.12.6 に対して開発されました。

セットアップ

UNIXソケット経由で**Docker**にアクセスする

Telegraf エージェントがベアメタル上で実行されている場合は、次のコマンドを実行して、telegraf Unix ユーザーを 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、ソケットをボリュームとしてポッドにマッピングし、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 に以下を追加します。

```
volumes:
...
- name: docker-sock
hostPath:
path: /var/run/docker.sock
type: File
```

次に、コンテナーに次の内容を追加します。

```
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インストーラーがこのマッピングを自動的に処理することに注意してください。

TCPエンドポイント経由で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ー

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
Dockerエンジン	名前空間 Docker エンジン	ノード名 ノードIP ノードUUID ノードOS Kubernetes クラスター Docker バージョン ユニット	メモリ コンテナ 一時停止中のコンテナ 実行中のコンテナ 停止中のコンテナ CPU Go ルーチン イメージ リスナー 使用中のイベント ファイル記述子 使用可能なデータ 使用済みデータ合計 使用可能なメタデータ 使用可能なメタデータ 使用済みメタデータ合計 プール ブロックサイズ

オブジェクト	識別子:	属性:	データポイント:
Dockerコンテナ	名前空間 コンテナ名 Docker エンジン	Kubernetes コンテナ ハッシュ、Kubernetes コンテナ ポート、Kubernetes コンテナの再起動回数、Kubernetes コンテナの終了メッセージ パス、Kubernetes コンテナの終了メッセージ ポリシー、Kubernetes ポッドの終了猶予期間、コンテナ イメージ、コンテナの状態、コンテナのバージョン、ノード名、Kubernetes コンテナのログ パス、Kubernetes コンテナ名、Kubernetes Docker タイプ、Kubernetes ポッド名、Kubernetes ポッド名前空間、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 構成の確認、Kubernetes IO 構成ソース、OpenShift IO SCC、Kubernetes の説明、Kubernetes 表示名、OpenShift タグ、Kompose サービス、ポッド テンプレート ハッシュ、コントローラー リビジョン ハッシュ、ポッド テンプレートの生成、ライセンス スキーマのビルド日、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、メンテナー、顧客ポッド、Kubernetes StatefulSet、ポッド名、テナント、Web コンソール、アーキテクチャ、権限のあるソース URL、ビルド日、RH ビルド ホスト、RH コンポーネント ディストリビューション、スコープ、インストール、リリース、実行の概要、アンインストー	メモリ アクティブ匿名メモリ 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 メモリ マップファイルメモリ 最大使用量 メモリ ページフォールトメモリ ページメジャーフォールトメモリ ページインメモリ ページアウトメモリ 常駐セットサイズ メモリ常駐セットサイズ 巨大メモリ合計 アクティブ匿名メモリ合計 アクティブファイルメモリ合計 キャッシュメモリ合計 非アクティブ匿名メモリ合計 非アクティブファイルメモリ合計 マップファイルメモリ合計 ページフォールトメモリ合計 ページメジャーフォールトメモリ合計 ページインメモリ合計 ページアウトメモリ合計 常駐セットサイズ メモリ合計 常駐セットサイズ巨大メモリ合計 排除不可能メモリ 排除不可能メモリ使用量 メモリ使用量の割合 終了コード OOM 強制終了 PID 開始時 失敗ストリーク

オブジェクト	識別子:	属性:	データポイント:
DockerコンテナブロックIO	名前空間 コンテナ名 デバイス Docker エンジン	Kubernetes コンテナ ハッシュ、Kubernetes コンテナ ポート、Kubernetes コンテナの再起動回数、Kubernetes コンテナの終了メッセージ パス、Kubernetes コンテナの終了メッセージ ポリシー、Kubernetes ポッドの終了猶予期間、コンテナ イメージ、コンテナの状態、コンテナのバージョン、ノード名、Kubernetes コンテナのログ パス、Kubernetes コンテナ名、Kubernetes Docker タイプ、Kubernetes ポッド名、Kubernetes ポッド名前空間、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 構成情報、Kubernetes 構成ソース、OpenShift SCC、Kubernetes の説明、Kubernetes 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、コントローラー 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 Web コンソール ビルド日、ライセンス ベンダー、アーキテクチャ、信頼できるソース URL、RH ビルド ホスト、RH コンポーネント ディストリビューション スコープ、インストール、メンテナー、リリース、実行、概要、アンインストール、VCS 参照、VCS タイプ バージョ	IO サービス バイト数 (再帰非同期)、IO サービス バイト数 (再帰読み取り)、IO サービス バイト数 (再帰同期)、IO サービス バイト数 (再帰合計)、IO サービス バイト数 (再帰書き込み)、IO サービス数 (再帰非同期)、IO サービス数 (再帰読み取り)、IO サービス数 (再帰同期)、IO サービス数 (再帰合計)、IO サービス数 (再帰書き込み)

オブジェクト	識別子:	属性:	データポイント:
Dockerコンテナネットワーク	名前空間 コンテナ名 ネットワーク Docker エンジン	コンテナイメージ コンテナステータス 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 K8s クラスタ Dockerバージョン コンテナID	RXドロップ RXバイト RXエラー RXパケット TXドロップ TXバイト TXエラー TXパケット

オブジェクト	識別子:	属性:	データポイント:
DockerコンテナCPU	名前空間 コンテナ名 CPU Dockerエンジン	Kubernetes コンテナ ハッシュ、Kubernetes コンテナ ポート、Kubernetes コンテナの再起動回数、Kubernetes コンテナの終了メッセージ パス、Kubernetes コンテナの終了メッセージ ポリシー、Kubernetes ポッドの終了猶予期間、Kubernetes 構成の確認、Kubernetes 構成ソース、OpenShift SCC コンテナ イメージ、コンテナ 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 ポッド名前空間、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 クラスター Docker バージョン、Kubernetes の説明、Kubernetes 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、コントローラー 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 Web コンソール ビルド日、ライセンス ベンダー、アーキテクチャ、権限のあるソース URL、RH ビルド ホスト、RH コンポーネント ディストリビューション スコープ、インストール、メンテナー、リリース、実行、サマリー、アンインストール、VCS 参照、VCS タイプ バージョ	スロットル期間 スロットル スロットル期間 スロットル スロットル時間 カーネルモードでの使用量 ユーザーモードでの使用量 使用量の割合 システム使用量 合計

問題：	これを試してください:
構成ページの指示に従った後、 Data Infrastructure Insightsに Docker メトリックが表示されません。	Telegraf エージェント ログをチェックして、次のエラーが報告されているかどうかを確認します: E! プラグイン [inputs.docker] のエラー: Docker デーモン ソケットへの接続中に権限が拒否されました。その場合は、上記のように、Telegraf エージェントに Docker Unix ソケットへのアクセスを提供するために必要な手順を実行してください。

追加情報は以下からご覧いただけます。"サポート"ページ。

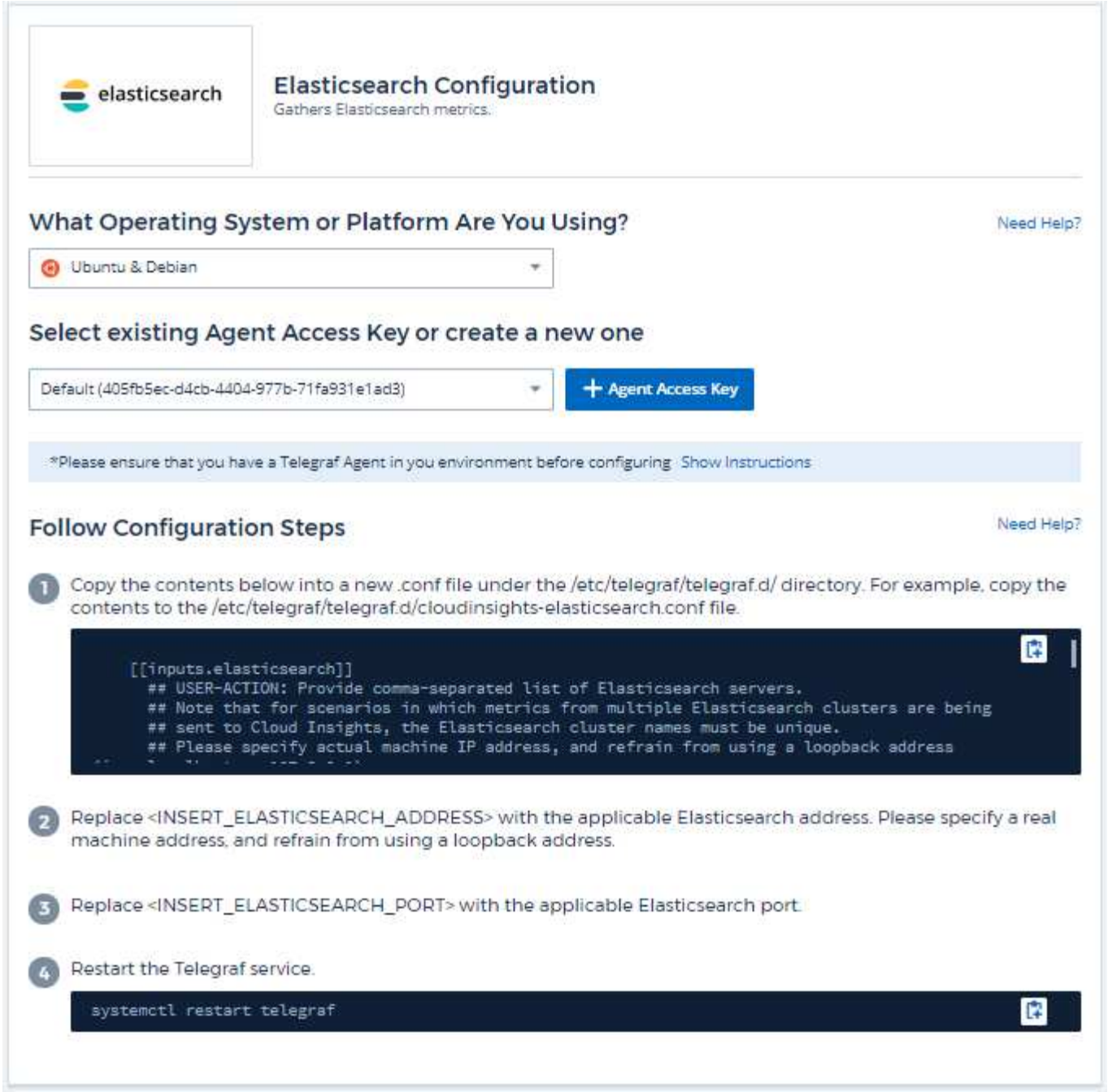
Elasticsearch データコレクター

Data Infrastructure Insights は、このデータ コレクターを使用して Elasticsearch からメトリックを収集します。

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 Elasticsearch を選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

詳細は以下をご覧ください。"Elasticsearch ドキュメント" 。

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:
Elasticsearch クラスター	名前空間クラスター	ノードIP ノード名 クラスタステータス

オブジェクト	識別子:	属性:
Elasticsearchノード	名前空間 クラスター ES ノード ID ES ノード IP ES ノード	ゾーンID

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

Flinkデータコレクター

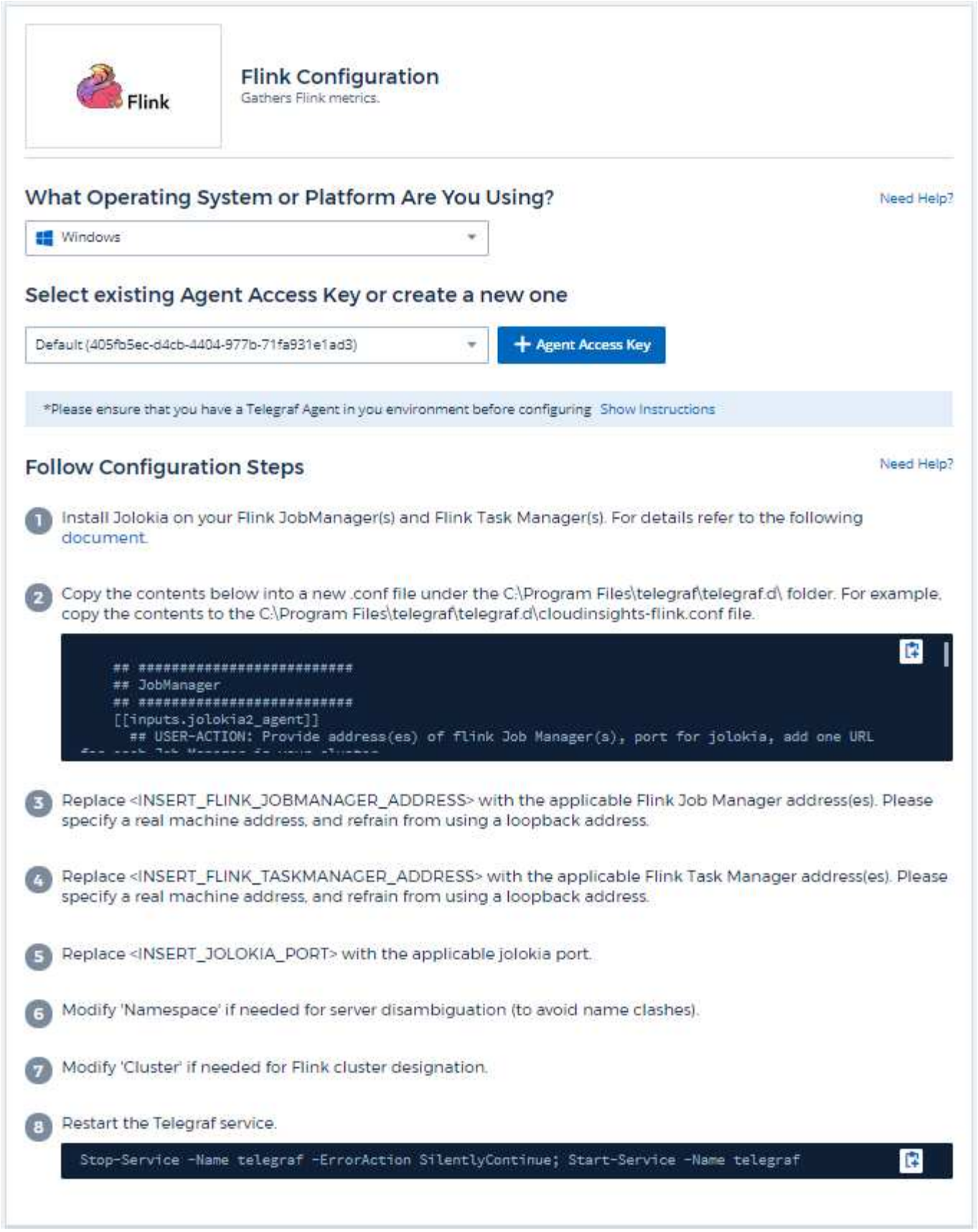
Data Infrastructure Insights は、このデータ コレクターを使用して Flink からメトリックを収集します。

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 Flinkを選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

完全な Flink デプロイメントには、次のコンポーネントが含まれます。

JobManager: Flink プライマリ システム。一連の TaskManager を調整します。高可用性設定では、システムには複数の JobManager が存在します。 TaskManager: ここで Flink オペレーターが実行されます。 Flink プラグインは、Telegraf 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必要があるため、すべてのコンポーネントで Jolokia を介して JMX を構成して公開する必要があります。

互換性

構成は Flink バージョン 1.7.0 に対して開発されました。

セットアップ

ジョロキアエージェントジャー

すべての個別コンポーネントについて、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"Jolokia エージェント 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/' の場所に配置されていることを前提としています。

ジョブマネージャー

JobManager が Jolokia API を公開するように設定するには、ノードに次の環境変数を設定し、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` をロックするための内部 `IP` がある場合は、「すべてをキャッチ」する `0.0.0.0` を独自の `IP` に置き換えることができます。この `IP` は `Telegraf` プラグインからアクセスできる必要があることに注意してください。

タスクマネージャー

Jolokia API を公開するように TaskManager を構成するには、ノードで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` をロックするための内部 `IP` がある場合は、「すべてをキャッチ」する `0.0.0.0` を独自の `IP` に置き換えることができます。この `IP` は `Telegraf` プラグインからアクセスできる必要があることに注意してください。

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
Flinkタスクマネージャー	クラスター名前空間サーバー	ノード名 タスクマネージャーID ノードIP	ネットワーク使用可能メモリセグメント ネットワーク合計メモリセグメント ガベージコレクション PS マークスイープ数 ガベージコレクション PS マークスイープ時間 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 コミット済みヒープメモリ ヒープメモリ初期化ヒープメモリ 最大使用ヒープメモリ スレッド数 デーモンスレッド数 ピークスレッド数 開始済みスレッド数合計
フリンクジョブ	クラスタ名前空間サーバジョブID	ノード名 ジョブ名 ノードIP 最終チェックポイント 外部パス 再起動時間	ダウンタイム 完全再起動 最終チェックポイント アライメント バッファリング 最終チェックポイントの持続時間 最終チェックポイントのサイズ 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 稼働時間
Flinkジョブマネージャー	クラスター名前空間サーバー	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 時間 ガベージ コレクション PS Scavenge 数 ガベージ コレクション PS Scavenge 時間 コミットされたヒープ メモリ ヒープ メモリの初期値 ヒープ メモリの最大使用ヒープ メモリ 登録されたタスク マネージャーの数 実行中のジョブの数 使用可能なタスク スロットの数 合計スレッド数 デーモン スレッド数 ピーク スレッド数 合計開始スレッド数

オブジェクト	識別子:	属性:	データポイント:
フリンクタスク	クラスター名前空間ジョブIDタスクID	サーバーノード名 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 現在の入力ウォーターマーク	プール内バッファー使用量、キュー内バッファー長、プール外バッファー使用量、キュー内バッファー長、ローカル内バッファー数、ローカル内バッファー数 (秒あたり)、ローカル内バッファー数 (秒あたり)、速度、リモート内バッファー数、リモート内バッファー数 (秒あたり)、リモート内バッファー数 (秒あたり)、速度、出力バッファー数、秒あたり出力バッファー数、秒あたり出力バッファー数、速度、ローカル内バイト数、ローカル内バイト数 (秒あたり)、速度、リモート内バイト数、リモート内バイト数 (秒あたり)、速度、出力バイト数、秒あたり出力バイト数、秒あたり出力バイト数、秒あたり出力バイト数、速度、入力レコード数、秒あたり入力レコード数、秒あたり入力レコード数、秒あたり出力レコード数、秒あたり出力レコード数、秒あたり出力レコード数

オブジェクト	識別子:	属性:	データポイント:
Flinkタスクオペレーター	クラスター名前空間ジョブIDオペレーターIDタスクID	サーバーノード名 ジョブ名 オペレータ名 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	現在の入力ウォーターマーク 現在の出力ウォーターマーク 入力レコード数 1秒あたりの入力レコード数 1秒あたりの入力レコード数 レート 出力レコード数 1秒あたりの出力レコード数 1秒あたりの出力レコード数 レート 遅延レコード数 ドロップされた割り当て済みパーティション 消費バイト数 レート コミット待ち時間 平均コミット待ち時間 最大コミットレート 失敗したコミット数 成功したコミット数 接続クローズレート 接続数 接続作成レート数 フェッチ待ち時間 平均フェッチ待ち時間 最大フェッチレート フェッチサイズ 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時間平均（ナノ秒） IO待機比率 IO待機時間平均（ナノ秒） 参加レート 参加時間平均前回ハートビート前 ネットワークIOレート 送信バイトレート 消費レコード数 レコード遅延 リクエストあたりの最大レコード数 平均リクエストレート リクエストサイズ 平均リクエストサイズ 最大レスポンスレート 選択レート 同期レート 同期時間 平均ハートビートレスポンス時間最大参加時間 最大同期時間 最大

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

Hadoop データコレクター

Data Infrastructure Insights は、このデータ コレクターを使用して Hadoop からメトリッ

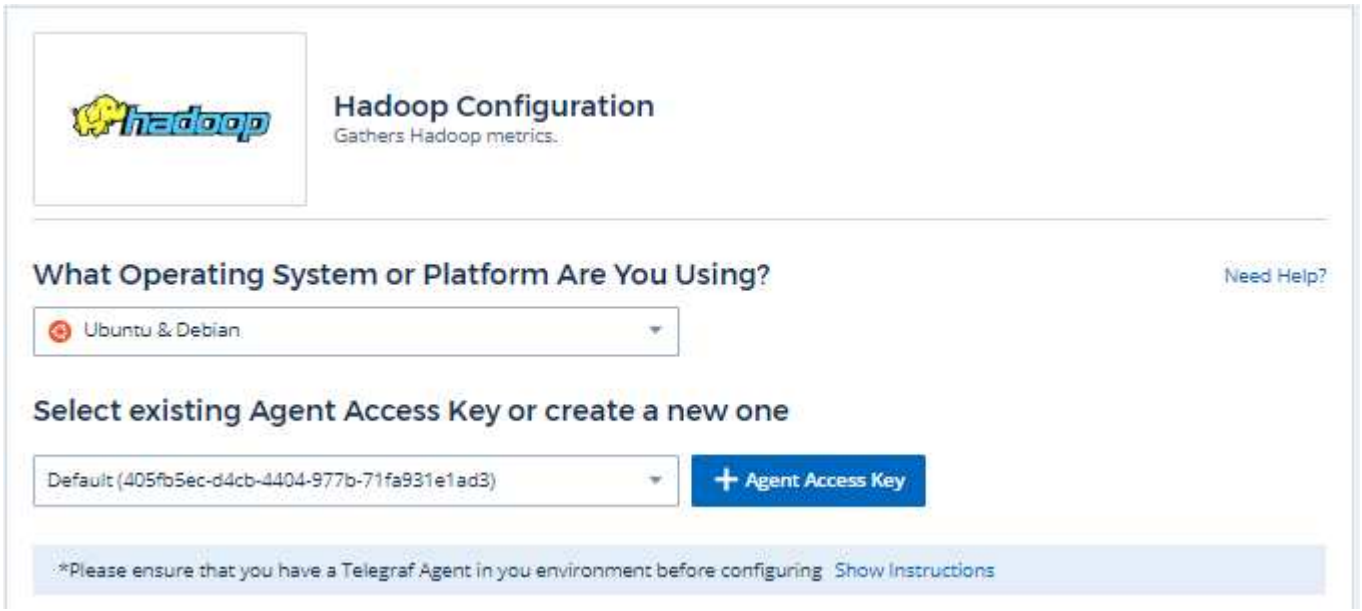
クを収集します。

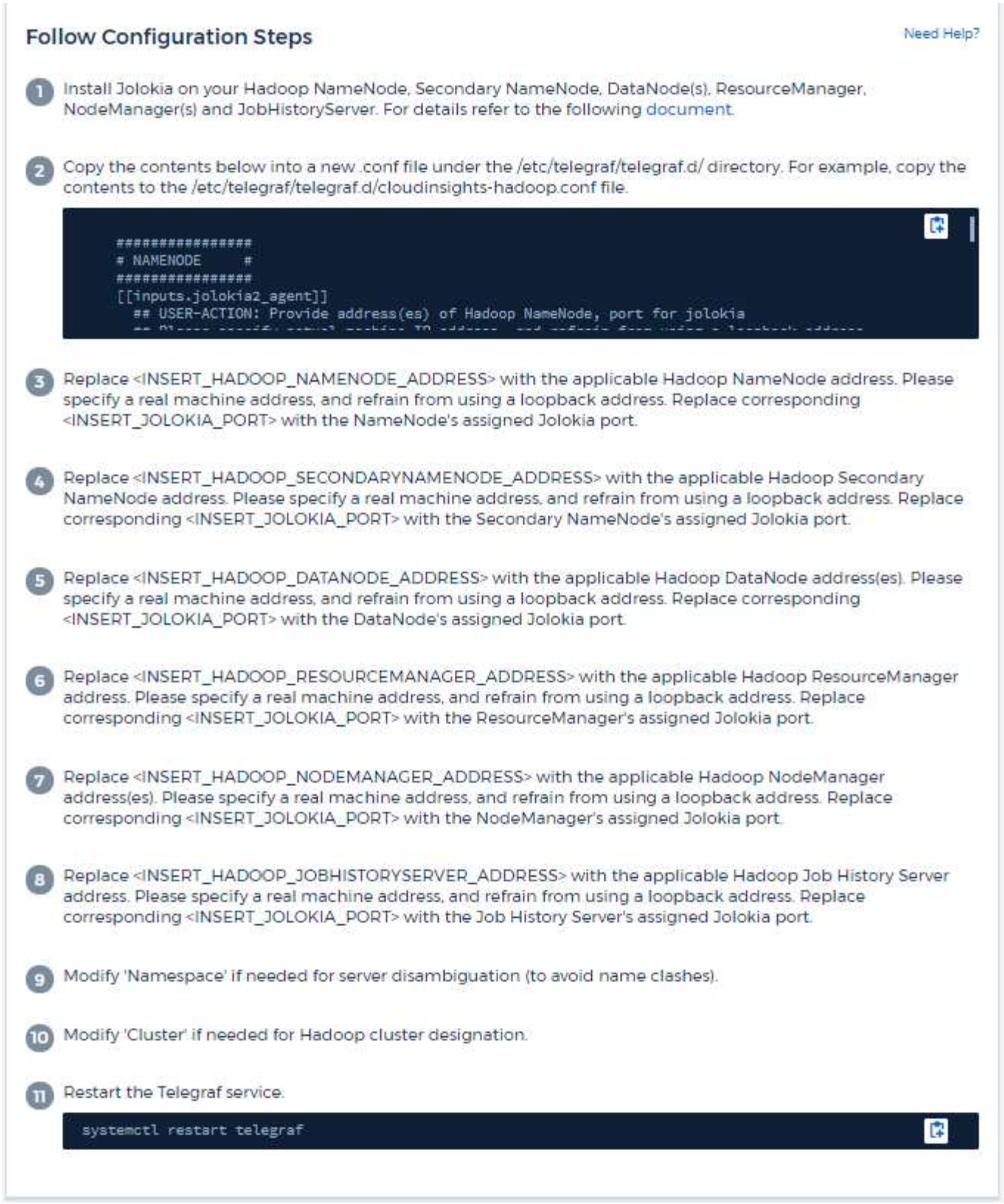
インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 Hadoop を選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。





セットアップ

完全な Hadoop の展開には、次のコンポーネントが含まれます。

- NameNode: Hadoop 分散ファイル システム (HDFS) のプライマリ 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、必要に応じて昇格できるように 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 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のリソース。アプリケーションを実行する実際の場所。
- JobHistoryServer: すべてのジョブ履歴関連のリクエストを処理する役割を担います。

Hadoop プラグインは、Telegraf 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必要があるため、すべてのコンポーネントで Jolokia 経由で JMX を構成して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

ジョロキアエージェントジャー

すべての個別コンポーネントについて、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"Jolokia エージェント 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/' の場所に配置されていることを前提としています。

ネームノード

NameNode を設定して Jolokia API を公開するには、<HADOOP_HOME>/etc/hadoop/hadoop-env.sh で次のように設定します。

```
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.
```

セカンダリネームノード

セカンダリ NameNode が 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.
```

データノード

Jolokia API を公開するように DataNode を構成するには、<HADOOP_HOME>/etc/hadoop/hadoop-env.sh で次のように設定します。

```
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.
```

リソースマネージャー

ResourceManager が 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 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.
```

ノードマネージャー

Jolokia API を公開するように NodeManagers を構成するには、<HADOOP_HOME>/etc/hadoop/hadoop-env.sh で次のように設定します。

```
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.
```

ジョブ履歴サーバー

JobHistoryServer が 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_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ー

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:
Hadoop セカンダリネームノード	クラスター名前空間サーバー	ノード名 ノードIP コンパイル情報 バージョン
Hadoop ノードマネージャー	クラスター名前空間サーバー	ノード名 ノードIP
Hadoop リソースマネージャー	クラスター名前空間サーバー	ノード名 ノードIP
Hadoop データノード	クラスター名前空間サーバー	ノード名 ノードIP クラスタID バージョン
Hadoop ネームノード	クラスター名前空間サーバー	ノード名 ノードIP トランザクションID 最終書き込み 最終ロード以降の時間 編集 HA状態 ファイルシステム状態 ブロックプールID クラスタID コンパイル情報 個別バージョン数 バージョン
Hadoop ジョブ履歴サーバー	クラスター名前空間サーバー	ノード名 ノードIP

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

HAProxy データコレクター

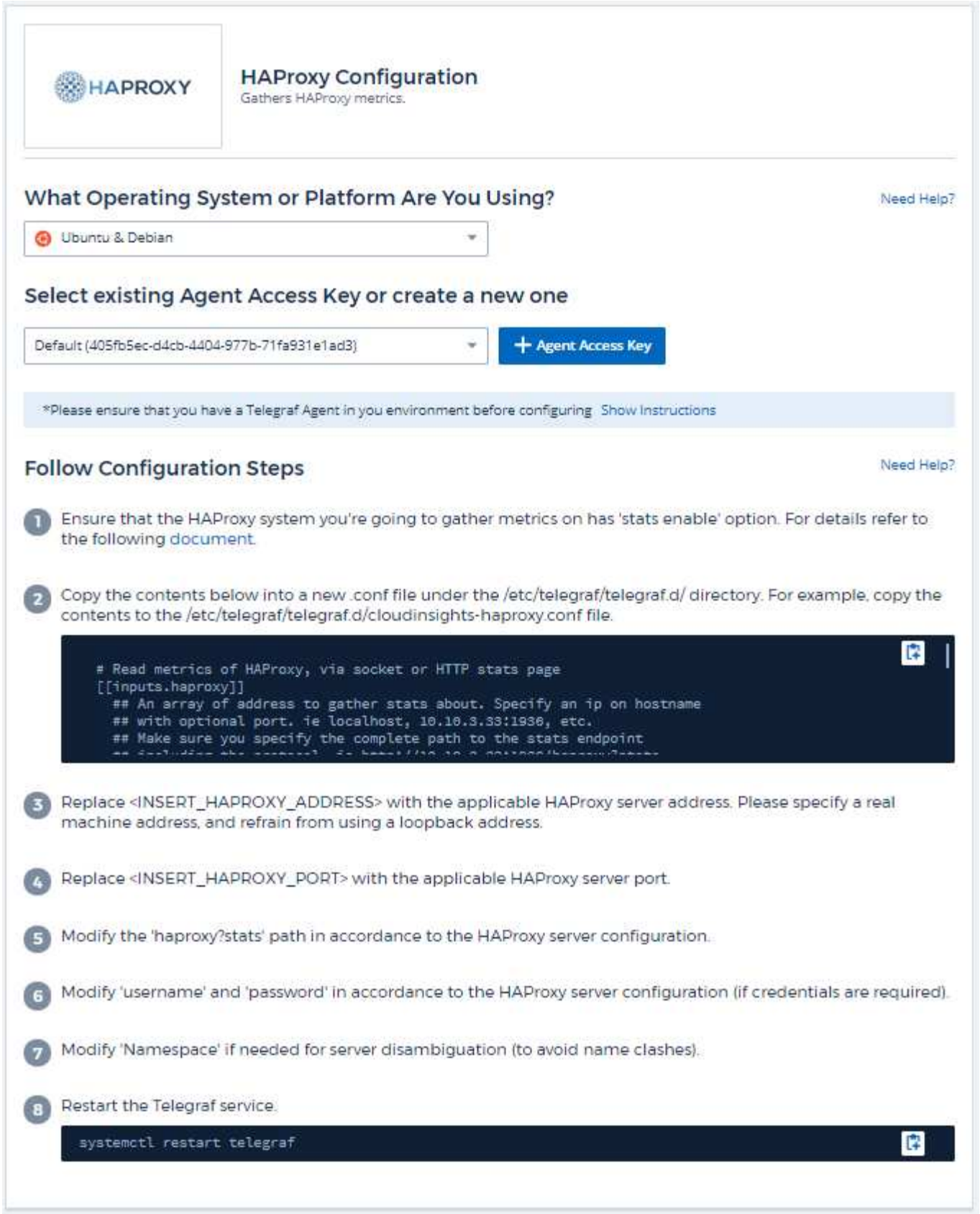
Data Infrastructure Insights は、このデータ コレクターを使用して HAProxy からメトリックを収集します。

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 HAProxyを選択します。

Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 + エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

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 に組み込まれた構成ですが、そのままでは有効になっていません。有効にすると、HAProxy はブラウザで表示した

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る HTML エンドポイントを公開します。

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。

セットアップ:

統計を有効にするには、haproxy 構成ファイルを編集し、独自のユーザー名/パスワードおよび/または haproxy URL を使用して、 'defaults' セクションの後に次の行を追加します。

```
stats enable
stats auth myuser:mypassword
stats uri  /haproxy?stats
```

以下は、統計が有効になっている簡略化された構成ファイルの例です。

```
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
```

完全かつ最新の手順については、"HAProxyドキュメント" 。

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
HAProxy フロントエンド	名前空間アドレスプロキシ	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 サーバーID セッション制限 ステータス	受信バイト数 送信バイト数 キャッシュヒット数 キャッシュルックアップ数 圧縮バイト数 バイパス圧縮バイト数 受信バイト数 圧縮バイト数 出力バイト数 圧縮レスポンス数 接続率 接続率 最大接続数 合計リクエスト数 接続ルールにより拒否されたリクエスト数 セキュリティ上の懸念により拒否されたリクエスト数 セキュリティ上の懸念により拒否されたレスポンス数 セッションルールにより拒否されたリクエスト数 エラーレスポンス数 1xxレスポンス数 2xxレスポンス数 3xxレスポンス数 4xxレスポンス数 5xxレスポンス数 その他のリクエスト数 インターセプトされたリクエスト数 セッション率 セッション率 最大リクエスト数 リクエスト率 最大リクエスト数 合計セッション数 セッション数 最大セッション数 合計リクエスト数 書き換え

オブジェクト	識別子:	属性:	データポイント:
HAProxyサーバー	名前空間アドレスプロキシサーバー	ノードIP ノード名 チェック完了時間 チェック下降構成チェック ヘルス値チェック上昇構成チェック ステータス プロキシID 最終変更時間 最終セッション時間 モード プロセスID サーバーID ステータス 重み	アクティブサーバー バックアップサーバー 受信バイト数 送信バイト数 チェックダウン数 チェック失敗数 クライアントの中止 接続数 接続平均時間 ダウンタイム 合計拒否数 応答数 接続エラー数 応答エラー数 応答数 1xx 応答数 2xx 応答数 3xx 応答数 4xx 応答数 5xx 応答数 選択されたその他のサーバー 合計キュー数 現在のキュー数 最大キュー数 平均時間 1秒あたりのセッション数 1秒あたりの最大セッション数 接続再利用数 応答時間 平均セッション数 最大セッション数 サーバー転送中止数 セッション数 合計セッション数 合計時間 平均リクエスト数 再ディスパッチ数 リクエスト数 再試行数 リクエスト数 書き換え数

オブジェクト	識別子:	属性:	データポイント:
HAProxyバックエンド	名前空間アドレスプロキシ	ノードIP ノード名 プロキシID 最終変更時刻 最終セッション時刻 モード プロセスID サーバーID セッション制限 ステータス 重み	アクティブサーバー バックアップサーバー 受信バイト数 送信バイト数 キャッシュヒット数 キャッシュ検索数 チェックダウン数 クライアントによる圧縮中止数 圧縮バイパス数 圧縮受信バイト数 圧縮送信バイト数 圧縮レスポンス数 接続数 接続平均時間 ダウンタイム合計 セキュリティ上の懸念により拒否されたリクエスト数 セキュリティ上の懸念により拒否されたレスポンス数 接続エラー数 レスポンスエラー数 レスポンス数 1xxレスポンス数 2xxレスポンス数 3xxレスポンス数 4xxレスポンス数 5xxレスポンス数 選択されたその他のサーバー キュー合計数 現在のキュー数 最大キュー数 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数 最大リクエスト数 合計接続再利用数 レスポンス時間 平均セッション数 最大セッション数 サーバー転送中止数 セッション数 合計セッション数 合計時間 平均リクエスト数 再ディスパッチ数 リクエスト数 再試行数 リクエスト数 書き換え数

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

JVMデータコレクター

Data Infrastructure Insights は、このデータ コレクターを使用して JVM からメトリックを収集します。

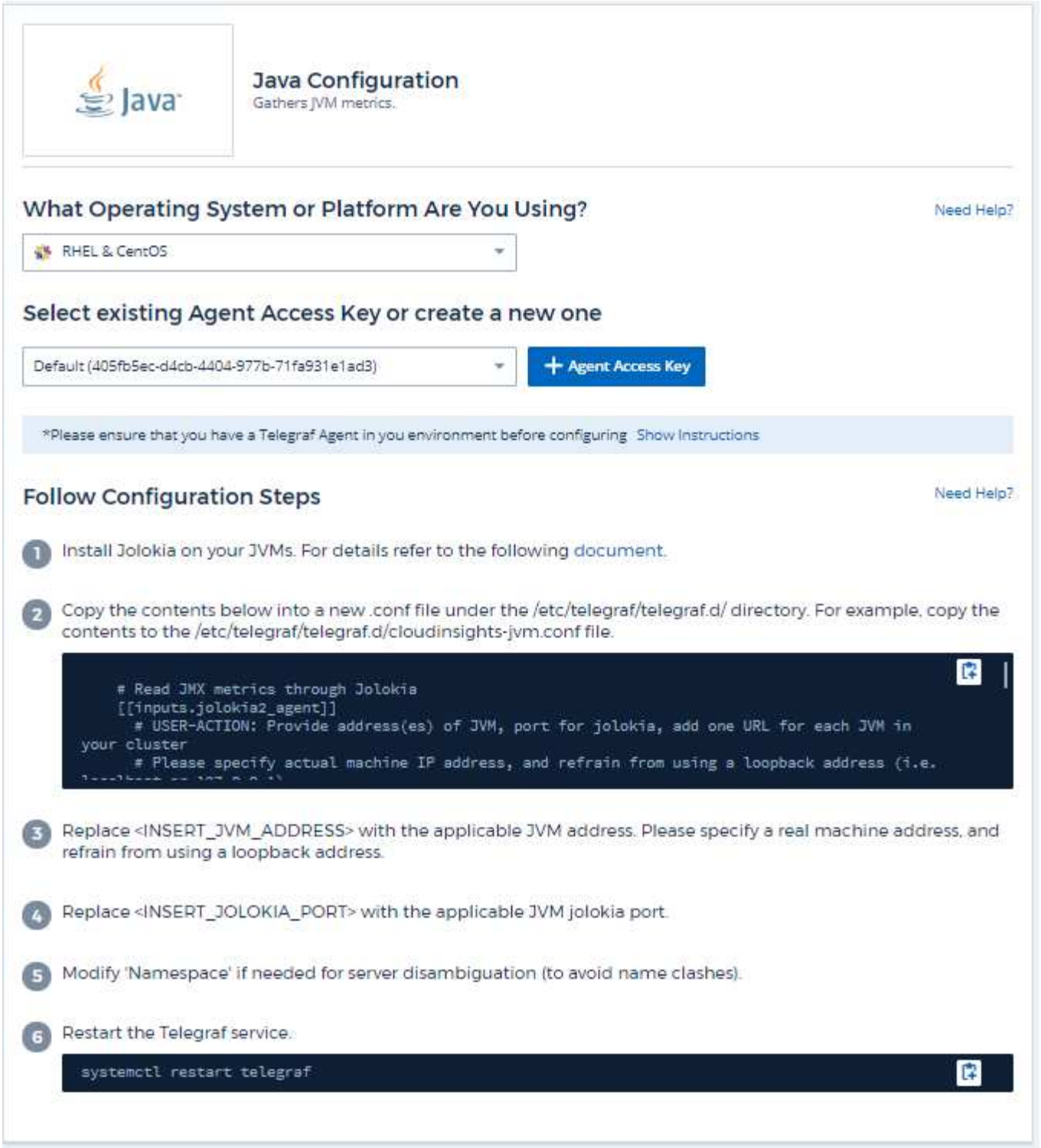
インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 JVM を選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 + エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

情報は以下をご覧ください"JVMのドキュメント"。

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
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 稼働時間 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	ロードされたクラス ロードされたクラスの合計 クラスがアンロードされたメモリ ヒープ コミットされたメモリ ヒープ初期メモリ 使用済みヒープ最大メモリ 使用済みメモリ 非ヒープ コミットされたメモリ 非ヒープ初期メモリ 非ヒープ最大メモリ 非ヒープ 使用済みメモリ ファイナライズ保留中のメモリ オブジェクト 使用可能な OS プロセッサ OS コミット済み仮想メモリ サイズ OS 空き物理メモリ サイズ OS 空きスワップ領域サイズ OS 最大ファイル記述子数 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 システム平均負荷 OS 合計物理メモリ サイズ OS 合計スワップ領域サイズ スレッド デーモン数 スレッド ピーク数 スレッド数 開始されたスレッド数 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 コピー コレクション時間 ガベージ コレクタ マークスイープ コレクション数 ガベージ コレクタ マークスイープ コレクション時間 ガベージ コレクタ G1 Old Generation コレクション数 ガベージ コレクタ G1 Old Generation コレクション時間 ガベージ コレクタ G1 Young Generation コレクション数 ガベージ コレクタ G1 Young Generation コレクション時間 ガベージ コレクタ同時マークスイープ コレクション数 ガベージ コレクター同時マークスイープ コレクション時間 ガベージ コレクター並列コレクション数 ガベージ コレクター並列コレクション時

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

Kafka データコレクター

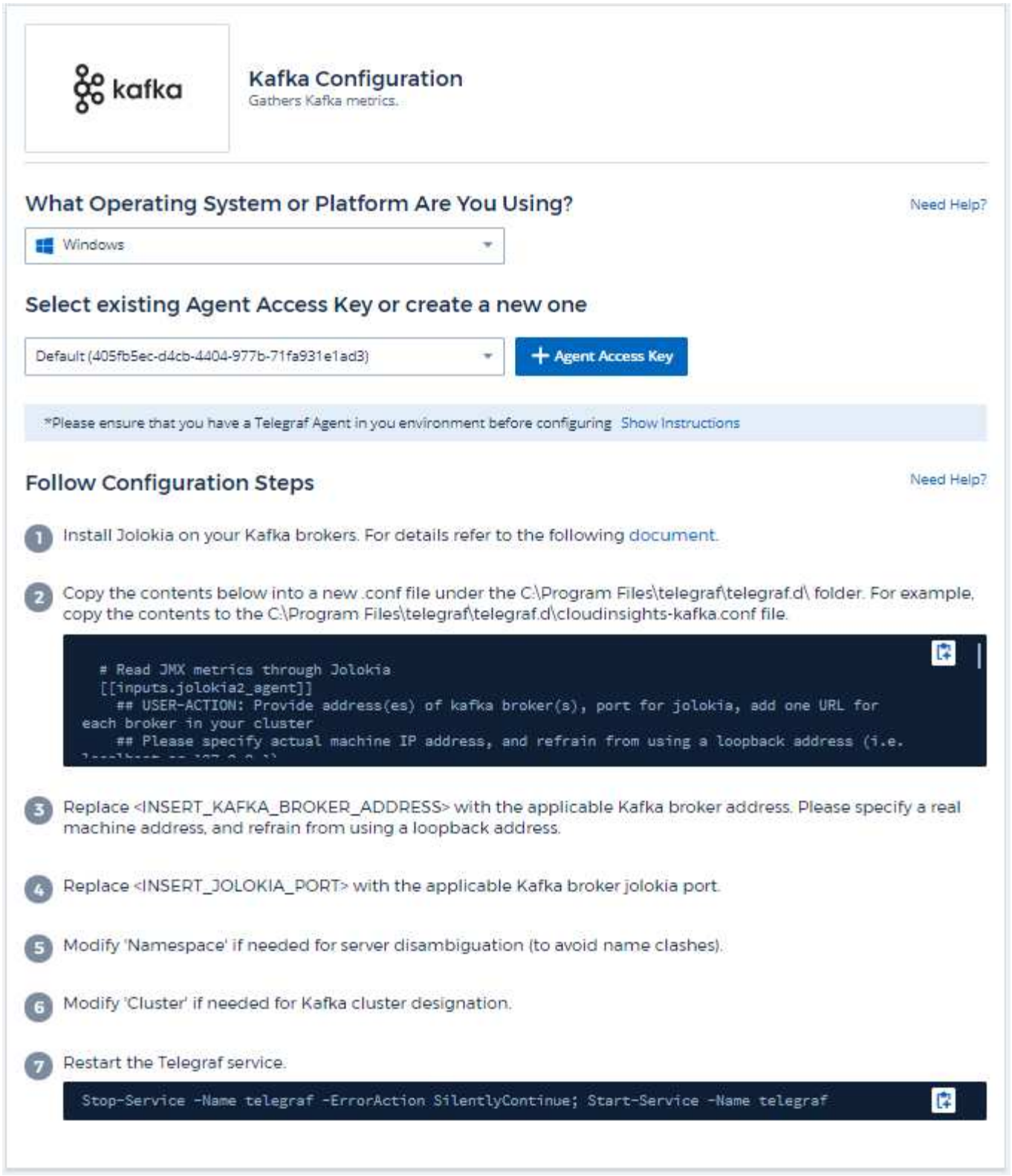
Data Infrastructure Insights は、このデータ コレクターを使用して Kafka からメトリックを収集します。

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 Kafka を選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

Kafka プラグインは、Telegraf 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、すべてのコンポーネントで Jolokia 経由で JMX を構成して公開する必要があります。

互換性

構成は Kafka バージョン 0.11.0.2 に対して開発されました。

セットアップ

以下のすべての手順では、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。以下の手順をインストール場所に合わせて調整できます。

ジョロキアエージェントジャー

Jolokiaエージェントjarファイルのバージョン"ダウンロード済み"。テスト対象のバージョンは Jolokia エージェント 1.6.0 です。

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/' の場所に配置されていることを前提としています。

Kafkaブローカー

Jolokia API を公開するように Kafka Brokers を構成するには、<KAFKA_HOME>/bin/kafka-server-start.sh の 'kafka-run-class.sh' 呼び出しの直前に以下を追加します。

```
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ることに注意してください。複数の IP を持つマシンでは、RMI 接続に必要な IP を収集するためにこれを調整する必要があります。

JMX (上記 9999) と Jolokia (8778) には異なるポートを選択できます。 Jolokia をロックするための内部 IP がある場合は、「すべてをキャッチ」する 0.0.0.0 を独自の IP に置き換えることができます。この IP は Telegraf プラグインからアクセスできる必要があることに注意してください。認証したくない場合は、オプション「-Dcom.sun.management.jmxremote.authenticate=false」を使用できます。自己責任でご使用ください。

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:
Kafkaブローカー	クラスター名前空間ブローカー	ノード名 ノードIP

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

Kibana データコレクター

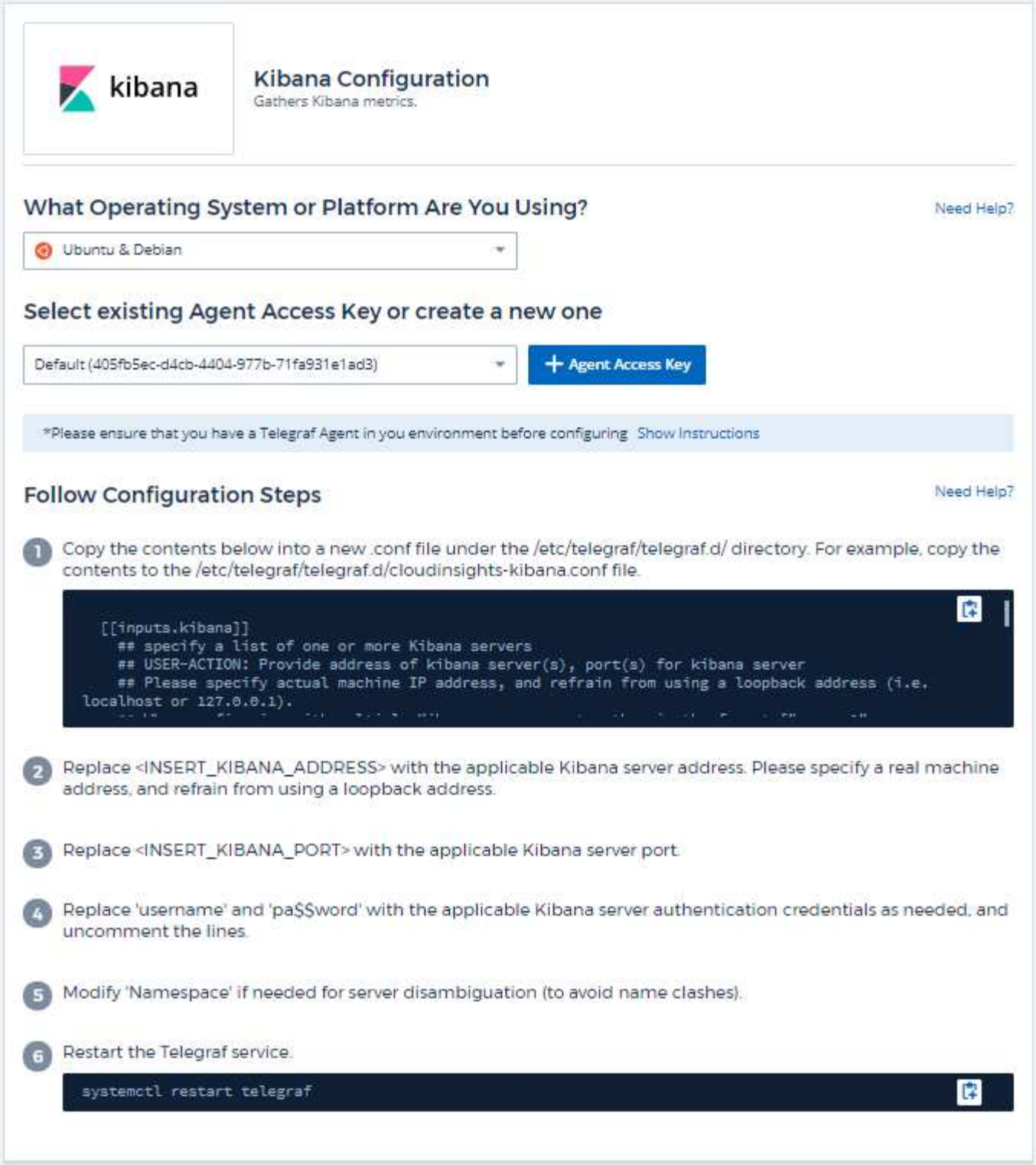
Data Infrastructure Insights は、このデータ コレクターを使用して Kibana からメトリックを収集します。

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 Kibanaを選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

詳細は以下をご覧ください。"Kibanaのドキュメント" 。

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
キバナ	名前空間アドレス	ノードIP ノード名 バージョン ステータス	同時接続数 ヒープ最大使用数 1秒あたりのリクエスト数 応答時間平均応答時間最大稼働時間

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

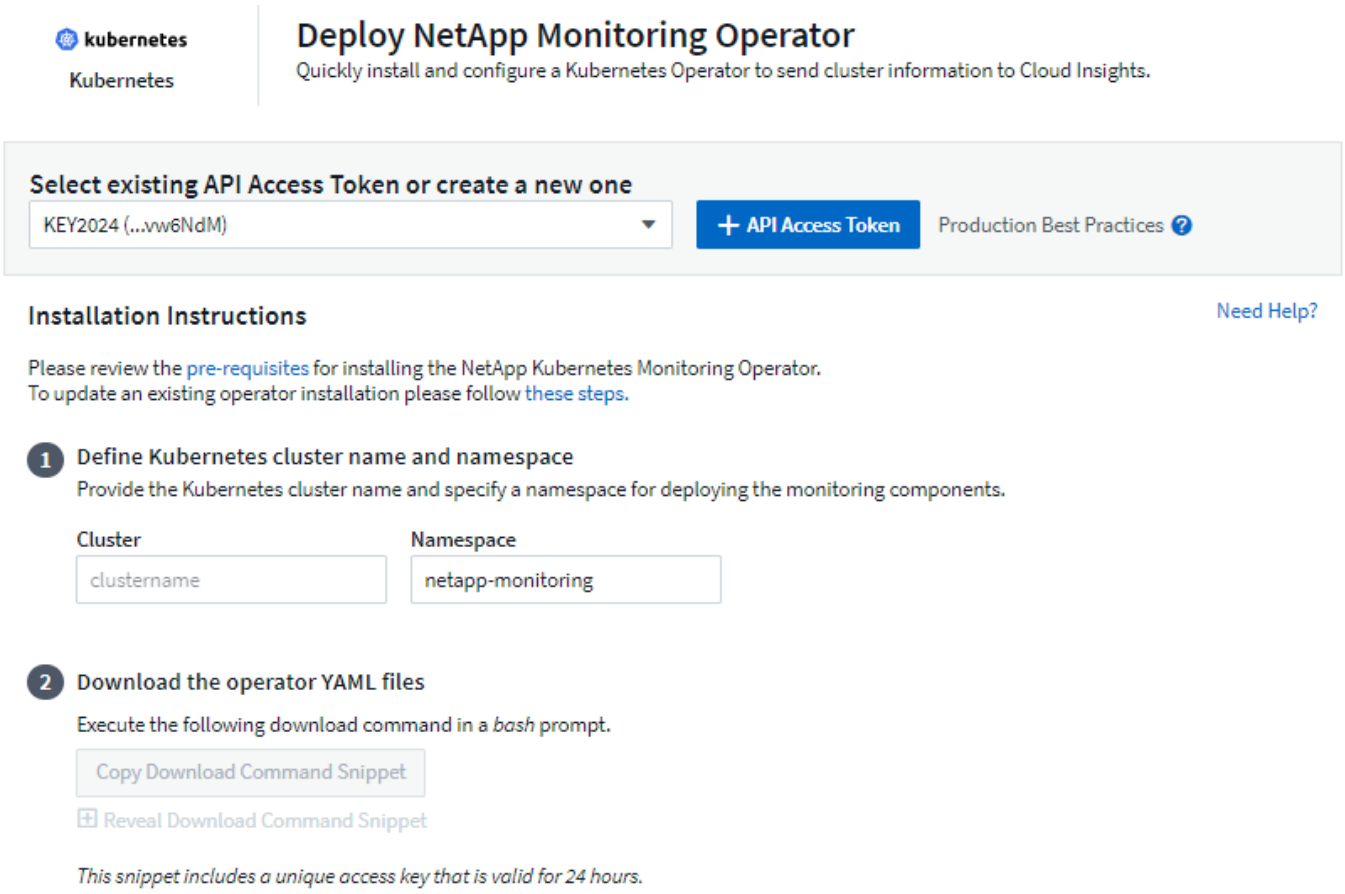
Kubernetes モニタリング オペレーターのインストールと構成

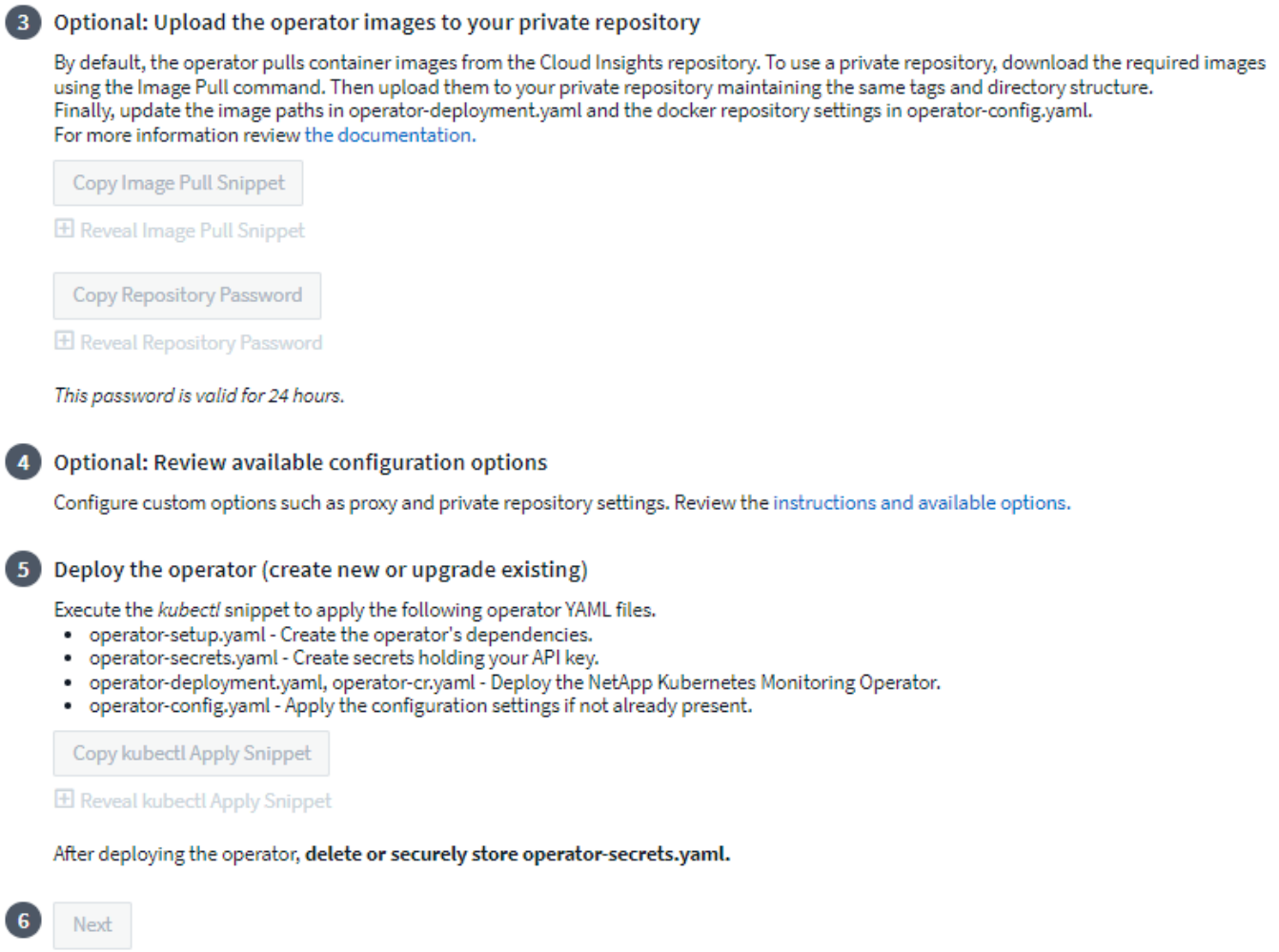
Data Infrastructure Insights は、 Kubernetes コレクション用の **Kubernetes Monitoring Operator** を提供します。新しいオペレーターをデプロイするには、**Kubernetes > Collectors > +Kubernetes Collector** に移動します。

Kubernetesモニタリングオペレーターをインストールする前に

参照"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に、ドキュメントを参照してください。

Kubernetes モニタリング オペレーターのインストール





Kubernetes に **Kubernetes Monitoring Operator** エージェントをインストールする手順:

1. 一意のクラスター名と名前空間を入力します。もしあなたがアップグレード以前の Kubernetes Operator からの場合は、同じクラスター名と名前空間を使用します。
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 *bash* ウィンドウに貼り付けて実行します。 Operator インストール ファイルがダウンロードされます。スニペットには一意のキーがあり、24 時間有効であることに注意してください。
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、*bash* シェルに貼り付けて実行します。イメージをプルしたら、それをプライベート リポジトリにコピーします。必ず同じタグとフォルダー構造を維持してください。 *operator-deployment.yaml* 内のパスと、*operator-config.yaml* 内の 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 リポジトリ設定などの利用可能な構成オプションを確認します。詳細については、"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、ダウンロードして実行して、Operator をデプロイします。
7. インストールは自動的に進行します。完了したら、[次へ] ボタンをクリックします。
8. インストールが完了したら、[次へ] ボタンをクリックします。 *operator-secrets.yaml* ファイルも必ず削除するか、安全に保存してください。

カスタムリポジトリをお持ちの場合は、以下をお読みください。カスタム/プライベートDockerリポジトリを

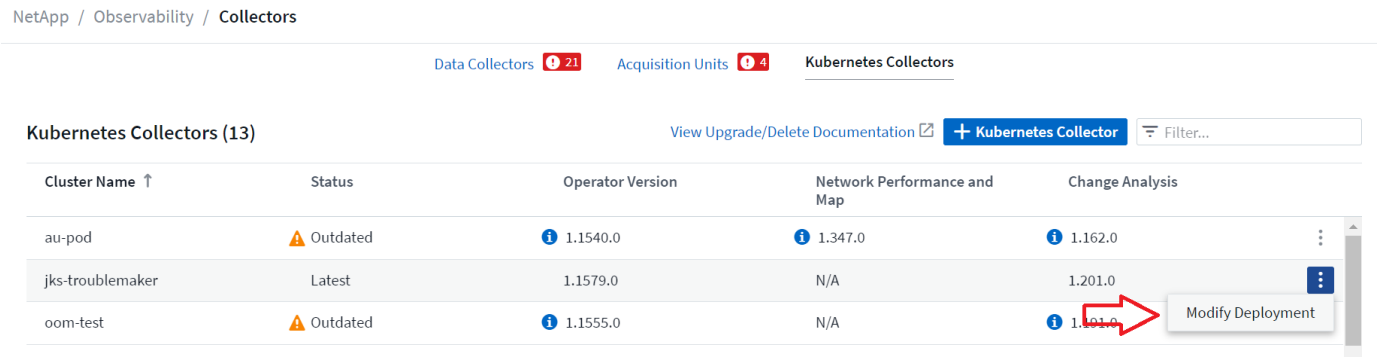
使用する 。

Kubernetes 監視コンポーネント

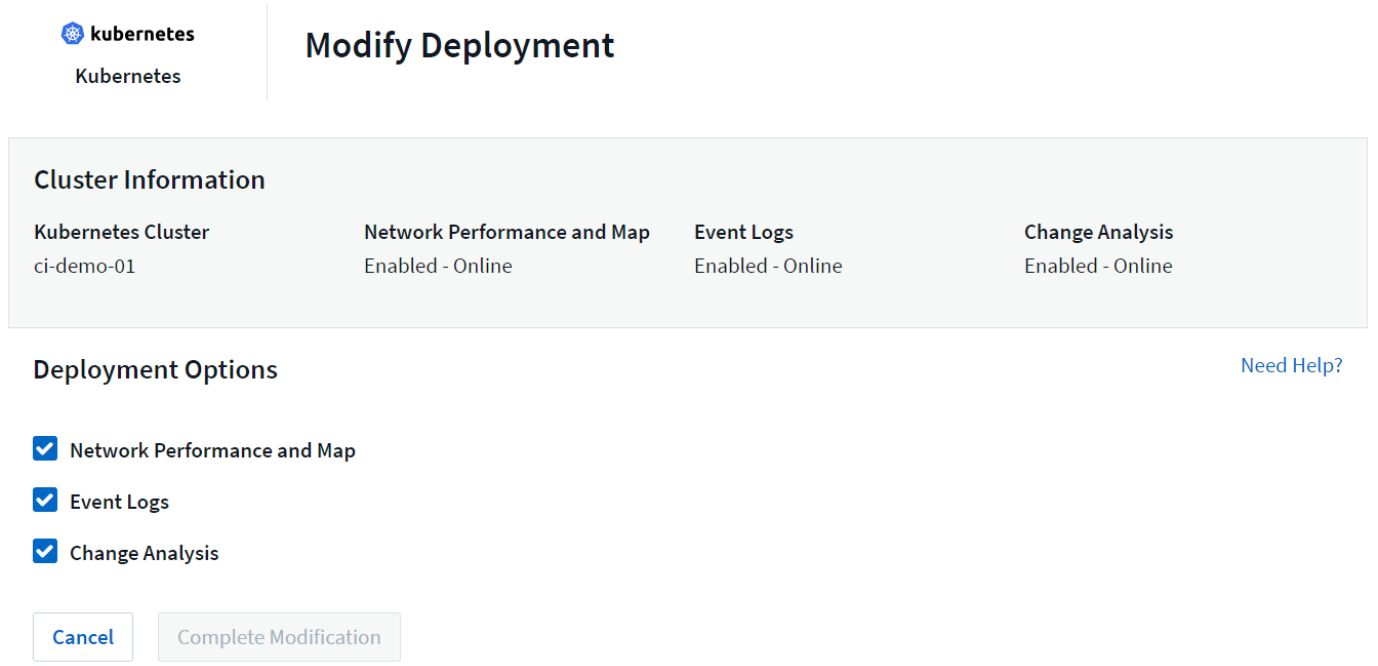
Data Infrastructure Insights Kubernetes モニタリングは、次の 4 つのモニタリング コンポーネントで構成されています。

- クラスターメトリック
- 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 コレクターに対してデフォルトで有効になっています。特定のコレクターに対して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、画面の右側にあるコレクターの「3 つのドット」メニューから *Modify Deployment* を選択して無効にすることができます。



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ー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。



最新のKubernetesモニタリングオペレーターへのアップグレード

DII プッシュボタンアップグレード

DII Kubernetes Collectors ページから Kubernetes Monitoring Operator をアップグレードできます。アップグレードするクラスターの横にあるメニューをクリックし、「アップグレード」を選択します。オペレーターはイメージ署名を検証し、現在のインストールのスナップショットを実行して、アップグレードを実行します。数分以内に、オペレーターのステータスが「アップグレード進行中」から「最新」へと進行していくのが確認できます。エラーが発生した場合は、詳細を表示するにはエラー ステータスを選択し、以下のプッシュ ボタン アップグレードのトラブルシューティング表を参照してください。

プライベートリポジトリによるプッシュボタンアップグレード

オペレーターがプライベート リポジトリを使用するように構成されている場合は、オペレーターの実行に必要なすべてのイメージとその署名がリポジトリで使用可能であることを確認してください。アップグレードプロセス中にイメージが不足しているためにエラーが発生した場合は、イメージをリポジトリに追加して、アップグレードを再試行してください。リポジトリにイメージ署名をアップロードするには、次のようにcosignツールを使用してください。3 オプション: 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 > イメージプルスニペットで指定されたすべてのイメージの署名をアップロードしてください。

```
cosign copy example.com/src:v1 example.com/dest:v1
#Example
cosign copy <DII container registry>/netapp-monitoring:<image version>
<private repository>/netapp-monitoring:<image version>
```

以前実行していたバージョンにロールバックする

プッシュボタン アップグレード機能を使用してアップグレードし、アップグレード後 7 日以内に現在のバージョンのオペレーターに問題が発生した場合は、アップグレード プロセス中に作成されたスナップショットを使用して、以前実行していたバージョンにダウングレードできます。ロールバックするクラスターの横にあるメニューをクリックし、[ロールバック] を選択します。

手動アップグレード

既存の Operator に *AgentConfiguration* が存在するかどうかを判断します（名前空間がデフォルトの *netapp-monitoring* でない場合は、適切な名前空間に置き換えます）：

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
_AgentConfiguration_ が存在する場合：
```

- インストール既存のオペレータよりも最新のオペレータを優先します。
  - 必ず最新のコンテナイメージを取得するカスタム リポジトリを使用している場合。

AgentConfiguration が存在しない場合：

- Data Infrastructure Insightsによって認識されるクラスター名をメモします (名前空間がデフォルトの netapp-monitoring でない場合は、適切な名前空間に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（名前空間がデフォルトの netapp-
monitoring でない場合は、適切な名前空間に置き換えます）。
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-operator,アンインストール
>>既存のオペレータ。
* <<installing-the-kubernetes-monitoring-operator,インストール
>>最新のオペレーター。
```

- 同じクラスター名を使用します。
- 最新の Operator YAML ファイルをダウンロードした後、デプロイする前に、*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。
- 必ず最新のコンテナイメージを取得するカスタム リポジトリを使用している場合。

Kubernetes モニタリング オペレーターの停止と起動

Kubernetes モニタリング オペレーターを停止するには:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Kubernetes モニタリング オペレーターを起動するには:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

アンインストール

Kubernetesモニタリングオペレーターを削除するには

Kubernetes モニタリング オペレーターのデフォルトの名前空間は「netapp-monitoring」であることに注意してください。独自の名前空間を設定している場合は、これらのコマンドと後続のすべてのコマンドおよびファイルでその名前空間を置き換えます。

監視オペレーターの新しいバージョンは、次のコマンドで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>
```

監視オペレーターが専用のネームスペースにデプロイされている場合は、ネームスペースを削除します。

```
 kubectl delete ns <NAMESPACE>
```

注：
最初のコマンドで「リソースが見つかりません」と返された場合は、次の手順に従って、監視オペレーターの古いバージョンをアンインストールしてください。

以下の各コマンドを順番に実行します。現在のインストールによっては、これらのコマンドの一部が「オブジェクトが見つかりません」というメッセージを返す場合があります。これらのメッセージは無視しても問題ありません。

```
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以前に作成されている場合:

```
kubectl delete scc telegraf-hostaccess
```

Kube-state-metricsについて

NetApp Kubernetes Monitoring Operator は、他のインスタンスとの競合を避けるために独自の kube-state-metrics をインストールします。

Kube-State-Metricsの詳細については、以下を参照してください。"このページ" 。

オペレーターの設定/カスタマイズ

これらのセクションには、オペレーター構成のカスタマイズ、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 の操作に関する情報が含まれています。

設定オプション

最も頻繁に変更される設定は、*AgentConfiguration* カスタム リソースで構成できます。オペレーターをデプロイする前に、*operator-config.yaml* ファイル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の例が含まれています。リストを見る"利用可能な設定"オペレーターの最新バージョン。

オペレーターをデプロイした後、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
```

デプロイされたオペレーターのバージョンが _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
```

「サーバーからのエラー (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ーをアップグレードする必要があります。

プロキシサポートの設定

Kubernetes モニタリング オペレーターをインストールするために、テナント上でプロキシを使用できる場所は 2 つあります。これらは同じプロキシ システムである場合もあれば、別のプロキシ システムである場合もあります。

- インストール コード スニペットの実行中（「curl」を使用）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 Kubernetes クラスターが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、まずプロキシがData Infrastructure Insights環境との良好な通信を許可するように構成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ー/VM からData Infrastructure Insightsにアクセスできる場合は、プロキシは適切に構成されている可能性があります。

Kubernetes オペレーティング モニター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* 環境変数を設定します。一部のプロキシ環境では、*no_proxy environment* 変数も設定する必要がある場合があります。

変数を設定するには、Kubernetes モニタリング オペレーター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. 現在のユーザーの *https_proxy* および/または *http_proxy* 環境変数を設定します。
   a. セットアップするプロキシに認証 (ユーザー名/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 （ユーザー名/パスワード）がある場合は、次のコマンドを実行します。

      ```
      export http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_port>
      ```

Kubernetes クラスターがData Infrastructure Insights環境と通信するために使用するプロキシについては、これらの手順をすべて読んだ後、Kubernetes Monitoring Operator をインストールしてください。

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**Docker**リポジトリの使用

デフォルトでは、Kubernetes Monitoring Operator はData Infrastructure Insightsリポジトリからコンテナ イメージをプルします。監視のターゲットとして Kubernetes クラスターが使用されており、そのクラスターがカスタムまたはプライベート Docker リポジトリまたはコンテナー レジストリからのみコンテナー イメージをプルするように構成されている場合は、Kubernetes 監視オペレーターに必要なコンテナーへのアクセスを構成する必要があります。

NetApp Monitoring Operator インストール タイルから「イメージ プル スニペット」を実行します。このコマンドは、 Data Infrastructure Insightsリポジトリにログインし、オペレーターのすべてのイメージ依存関係をプルし、 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、提供され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ているかについては、以下を参照してください。

コアオペレーター機能とKubernetesモニタリング

- netapp 監視
- ci-kube-rbac-プロキシ
- ci-ksm

- ci-telegraf
- ディストロレスルートユーザー

イベントログ

- ci-fluent-bit
- ci-kubernetes-イベントエクスポーター

ネットワークパフォーマンスとマップ

- ci-net-オブザーバー

企業ポリシーに従って、オペレーターの 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リポジトリのものと一致していることを確認します。

operator-deployment.yaml の monitoring-operator デプロイメントを編集し、すべてのイメージ参照を変更してプライベート Docker リポジトリを使用します。

```
image: <docker repo of the enterprise/corp docker repo>/ci-kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

新しい docker リポジトリの場所を反映するように、*operator-config.yaml* の *AgentConfiguration* を編集します。プライベートリポジトリ用の新しい 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
```

長期パスワード用の **API** アクセストークン

一部の環境（プロキシリポジトリなど）では、Data Infrastructure Insights docker リポジトリの長期パスワードが必要です。インストール時に UI で提供されるパスワードは 24 時間のみ有効です。それを使用する代わりに、API アクセストークンを docker リポジトリパスワードとして使用できます。このパスワードは、API アクセストークンが有効である限り有効です。この特定の目的のために新しい API アクセストークンを生成

することも、既存のものを使用することもできます。

"こちらをお読みください"新しいAPIアクセストークンを作成する手順については、こちらをご覧ください。

ダウンロードした *operator-secrets.yaml* ファイルから既存の API アクセス トークンを抽出するには、ユーザーは以下を実行できます：

```
grep '\.dockerconfigjson' operator-secrets.yaml |sed 's/.*\.dockerconfigjson:
//g' |base64 -d |jq
```

実行中のオペレーターインストールから既存のAPIアクセストークンを抽出するには、ユーザーは以下を実行できます：

```
kubectl -n netapp-monitoring get secret netapp-ci-docker -o
jsonpath='{.data.\.dockerconfigjson}' |base64 -d |jq
```

OpenShift の手順

OpenShift 4.6 以降で実行している場合は、*operator-config.yaml* の *AgentConfiguration* を編集して *runPrivileged* 設定を有効に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。

寛容と汚点

netapp-ci-telegraf-ds、*netapp-ci-fluent-bit-ds*、および *netapp-ci-net-observer-l4-ds* DaemonSets は、すべてのノードでデータを正しく収集するために、クラスター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。オペレーターは、いくつかのよく知られた 汚染 を許容するように設定されています。ノードにカスタムテイントを設定して、ポッドがすべてのノードで実行されないようにしている場合は、それらのテイントに対して*許容*を作成できます。"_AgentConfiguration_内" 。クラスター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、オペレーター ポッドをスケジュールして実行できるように、オペレーター デプロイメントに必要な許容値も追加する必要があります。

Kubernetesについて詳しく知る"汚名と寛容"。

戻る"* NetApp Kubernetes Monitoring Operator のインストール* ページ"

秘密についてのメモ

Kubernetes モニタリング オペレーターがクラスター全体でシークレットを表示する権限を削除するには、インストール前に *operator-setup.yaml* ファイルから次のリソースを削除します。

```
ClusterRole/netapp-ci<namespace>-agent-secret
ClusterRoleBinding/netapp-ci<namespace>-agent-secret
```

アップグレードの場合は、クラスター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* または *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。この行における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 モニタリング オペレーター イメージ署名の検証

オペレータのイメージとそれが展開するすべての関連イメージは、 NetAppによって署名されています。インストール前に cosign ツールを使用してイメージを手動で検証したり、Kubernetes アドミッション コントローラーを構成したりすることができます。詳細については、"Kubernetesドキュメント" 。

イメージ署名の検証に使用される公開鍵は、モニタリング オペレーターのインストール タイルの「オプション: オペレーター イメージをプライベート リポジトリにアップロード > イメージ署名公開鍵」で入手できます。

イメージ署名を手動で検証するには、次の手順を実行します。

1. 画像プルスニペットをコピーして実行する
2. リポジトリパスワードをコピーしてプロンプトが表示されたら入力します
3. イメージ署名公開鍵（例では dii-image-signing.pub）を保存します。
4. cosign を使用してイメージを検証します。共同署名の使用例を参照してください

```
$ cosign verify --key dii-image-signing.pub --insecure-ignore-sct
--insecure-ignore-tlog <repository>/<image>:<tag>
Verification for <repository>/<image>:<tag> --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - The signatures were verified against the specified public key
[{"critical":{"identity":{"docker-
reference":"<repository>/<image>"},"image":{"docker-manifest-
digest":"sha256:<hash>"},"type":"cosign container image
signature"},"optional":null}]
```

トラブルシューティング

Kubernetes モニタリング オペレーターの設定中に問題が発生した場合に試すことは次のとおりです。

問題：	これを試してください:
Kubernetes 永続ボリュームと対応するバックエンド ストレージ デバイス間のハイパーリンク/接続が表示されません。私の Kubernetes 永続ボリュームは、ストレージ サーバーのホスト名を使用して構成されています。	手順に従って既存の Telegraf エージェントをアンインストールし、最新の Telegraf 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 以降を使用している必要があり、Kubernetes クラスター 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：	これを試してください:
ログには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: *v1.MutatingWebhookConfiguration の一覧を取得できませんでした: 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: *v1.Lease の一覧を取得できませんでした: 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、Kubernetes バージョン 1.20 未満で kube-state-metrics バージョン 2.0.0 以上を実行している場合に表示されることがあります。 Kubernetes のバージョンを取得するには: *kubectl version* kube-state-metrics のバージョンを取得するには: *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* これらのメッセージが表示されないようにするには、ユーザーは kube-state-metrics デプロイメントを変更して、次のリースを無効にすることができます: *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* 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,nodes,persistentvolumeclaims,persistentvolumes, poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas, secrets、services 、statefulsets、storageclasses 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、horizontalpodautoscalers、ingresses、jobs、leases、limitranges 、mutatingwebhookconfigurations、namespaces、networkpolicies、nodes、persistentvolumeclaims、persistentvolumes、poddisruptionbudgets、pods、replicasets、replicationcontrollers、resourcequotas、secrets 、services、statefulsets、storageclasses、validatingwebhookconfigurations、volumeattachments"
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: Oct 11 14:23:41 ip-172-31-39-47 systemd[1]: Started The plugin-driven server agent for reporting metrics into InfluxDB. 10月11日 14:23:41 ip-172-31-39-47 telegraf[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。無視されました\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="開けませんでした。無視されました。open /etc/telegraf/.cache/snowflake/ocsp_response_cache.json: そのようなファイルまたはディレクトリはありません\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021-10-11T14:23:41Z I! Telegraf 1.19.3 の起動	これは既知の問題です。参照"このGitHubの記事"詳細についてはこちらをご覧ください。 Telegraf が稼働している限り、ユーザーはこれらのエラー メッセージを無視できます。

問題：	これを試してください:
Kubernetes では、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 が有効になっていて強制されている場合、Telegraf ポッドが Kubernetes ノード上の /proc/1/mountstats ファイルにアクセスできない可能性があります。この制限を克服するには、エージェント構成を編集し、runPrivileged 設定を有効にします。詳細については、OpenShift の手順を参照してください。
Kubernetes では、Telegraf ReplicaSet ポッドが次のエラーを報告しています: [inputs.prometheus] プラグインのエラー: キーペア /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: そのような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 として指定されたノード上で実行されることを目的としています。 ReplicaSet ポッドがこれらのノードのいずれかで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 taint があるかどうかを確認します。そうなる場合は、Telegraf ReplicaSet (telegraf-rs) に必要な許容範囲を追加します。たとえば、ReplicaSet を編集します… kubectl edit rs telegraf-rs …そして、適切な許容値を仕様に追加します。次に、ReplicaSet ポッドを再起動します。
PSP/PSA環境があります。これは監視オペレーターに影響しますか?	Kubernetes クラスターが Pod Security Policy (PSP) または Pod Security Admission (PSA) を適用した状態で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 をサポートする現在の Operator にアップグレードするには、次の手順に従います。1. アンインストール以前の監視オペレーター: kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com 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. インストール監視オペレータの最新バージョン。
PSP/PSA を使用しているのですが、Operator を展開しようとして問題が発生しました。	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> edit agent 2. 「security-policy-enabled」を「false」としてマークします。これにより、ポッド セキュリティ ポリシーとポッド セキュリティ アドミッションが無効になり、オペレーターがデプロイ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 が削除されたことが表示されます) kubectl get all -n <namespace>
grep -i psp (何も見つからないことが表示されます)	「ImagePullBackoff」エラーが発生
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 モニタリング オペレーターがそれを適切に認識するようにまだ構成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 リポジトリの構成について。	モニタリング オペレーターのデプロイメントで問題が発生していますが、現在のドキュメントでは解決できません。

問題：	これを試してください:
次のコマンドの出力をキャプチャまたはメモして、テクニカル サポート チームに連絡してください。 ``` 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) ポッドは CrashLoopBackOff にあります
これらのポッドは、ネットワーク可観測性のワークロード マップ データ コレクターに対応します。以下を試してください: • いずれかのポッドのログをチェックして、最小カーネル 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 は、最小カーネル バージョン 4.18.0 より小さいです","time":"2022-11-09T08:23:08Z"} ---- • Net-observer ポッドでは、Linux カーネル バージョンが少なくとも 4.18.0 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。	ポッドはオペレーター名前空間（デフォルト：netapp-monitoring）で実行されていますが、ワークロードマップのUIやクエリのKubernetesメトリックにデータが表示されません。
K8S クラスターのノード上の時刻設定を確認します。正確な監査とデータ レポートを実現するために、ネットワーク タイム プロトコル (NTP) または簡易ネットワーク タイム プロトコル (SNTP) を使用してエージェント マシンの時刻を同期することを強くお勧めします。	オペレーター名前空間内の一部のネットオブザーバー ポッドが保留状態になっています
Net-observer は DaemonSet であり、k8s クラスターの各ノードでポッドを実行します。 • 保留中の状態のポッドに注意し、CPU またはメモリのリソースの問題が発生しているかどうかを確認します。ノードで必要なメモリと CPU が使用可能であることを確認します。	Kubernetes モニタリング オペレーターをインストールした直後、ログに次の内容が表示されます: [inputs.prometheus] プラグインでエラーが発生しました: http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics への HTTP リクエストの作成エラー: http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics を取得: tcp をダイヤル: kube-state-metrics.<namespace>.svc.cluster.local を検索: そのようなホストはありません

問題：	これを試してください:
このメッセージは通常、新しいオペレータがインストールされ、*ksm* ポッドが起動する前に *telegraf-rs* ポッドが起動している場合にのみ表示されます。すべてのポッドが実行されると同時に、これらのメッセージは停止します。	クラスター内に存在する Kubernetes CronJobs に対して収集されているメトリックが表示されません。
Kubernetesのバージョンを確認してください（つまり `kubectl version`）。 v1.20.x 以下の場合、これは予想される制限です。 Kubernetes Monitoring Operator とともにデプロイされた kube-state-metrics リリースは、v1.CronJob のみをサポートします。 Kubernetes 1.20.x 以下では、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。	オペレーターをインストールすると、telegraf-ds ポッドは CrashLoopBackOff 状態になり、ポッド ログに「su: 認証失敗」と表示されます。
AgentConfiguration の telegraf セクションを編集し、*dockerMetricCollectionEnabled* を false に設定します。詳細については、オペレーターの"設定オプション"を参照してください。… spec：… telegraf：…-name：docker run-mode：- DaemonSet substitutions：- key：DOCKER_UNIX_SOCK_PLACEHOLDER value：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: E! [エージェント] 出力への書き込みエラー: http: Post "https://<tenant_url>/rest/v1/lake/ingest/influxdb": コンテキストの期限が切れました (ヘッダーの待機中に Client.Timeout を超えました)
AgentConfiguration の telegraf セクションを編集し、*outputTimeout* を 10 秒に増やします。詳細については、オペレーターの"設定オプション"。	一部のイベント ログの *involvedobject* データが見つかりません。
必ず、"権限"上記のセクション。	netapp-ci-monitoring-operator-<pod> と monitoring-operator-<pod> という名前の 2 つの監視オペレータ ポッドが実行されているのはなぜですか?
2023年10月12日現在、 Data Infrastructure Insights は、ユーザーへのサービス向上のため、オペレーターをリファクタリングしました。これらの変更を完全に適用するには、古い演算子を削除するそして新しいものをインストールする。	Kubernetes イベントが予期せずData Infrastructure Insightsへのレポートを停止しました。
イベント エクスポーター ポッドの名前を取得します。 `kubectl -n netapp-monitoring get pods`	grep event-exporter

問題：	これを試してください:
awk '{print $1}'	sed 's/event-exporter./event-exporter/'` 「netapp-ci-event-exporter」または「event-exporter」のいずれかである必要があります。次に、監視エージェントを編集します `kubectl -n netapp-monitoring edit agent`、LOG_FILE の値を、前の手順で見つかった適切なイベント エクスポーター ポッド名を反映するように設定します。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 … …. あるいは、uninstallそして再インストールエージェント。
Kubernetes モニタリング オペレーターによってデプロイされたポッドが、リソース不足のためにクラッシュしているのがわかります。	Kubernetesモニタリングオペレーターを参照してください"設定オプション"必要に応じて CPU および/またはメモリの制限を増やします。
イメージが欠落しているか、構成が無効であるため、netapp-ci-kube-state-metrics ポッドの起動または準備ができませんでした。現在、StatefulSet はスタックしており、構成の変更が netapp-ci-kube-state-metrics ポッドに適用されていません。	StatefulSetは"壊れた"州。構成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 ポッドは、Kubernetes Operator のアップグレードを実行した後に起動に失敗し、ErrImagePull (イメージのプルに失敗します) をスローします。	ポッドを手動でリセットしてみてください。
ログ分析の Kubernetes クラスターで、「イベントは maxEventAgeSeconds より古いため破棄されました」というメッセージが表示されています。	Operator の *agentconfiguration* を変更し、*event-exporter-maxEventAgeSeconds* (つまり 60 秒)、*event-exporter-kubeQPS* (つまり 100)、および *event-exporter-kubeBurst* (つまり 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、"設定オプション"ページ。

問題：	これを試してください:
Telegraf は、ロック可能なメモリが不足しているために警告を発したりクラッシュしたりします。	基盤となるオペレーティング システム/ノードで Telegraf のロック可能なメモリの制限を増やしてみてください。制限を増やすことができない場合は、NKMO エージェント構成を変更し、*unprotected* を *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されます。復号化された秘密がディスクにスワップアウトされる可能性があるため、セキュリティ上のリスクが生じ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の実行が可能になります。*unprotected* 設定オプションの詳細については、"設定オプション"ページ。
Telegraf から次のような警告メッセージが表示されます: *W! [inputs.diskio] "vdc"* のディスク名を収集できません*: /dev/vdc* の読み取りエラー*:* そのようなファイルまたはディレクトリはありません	Kubernetes Monitoring Operator の場合、これらの警告メッセージは無害であり、無視しても問題ありません。または、AgentConfiguration の telegraf セクションを編集し、*runDsPrivileged* を true に設定します。詳細については、"オペレータの設定オプション"を参照してください。

問題：	これを試してください:
Fluent-bit ポッドが次のエラーで失敗しています: [2024/10/16 14:16:23] [error] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] 開いているファイルが多すぎます [2024/10/16 14:16:23] [error] 入力 tail.0 の初期化に失敗しました [2024/10/16 14:16:23] [error] [engine] 入力の初期化に失敗しました	クラスター内の *fsnotify* 設定を変更してみます。 ``` sudo sysctl fs.inotify.max_user_instances (take note of setting) sudo sysctl fs.inotify.max_user_instances=<something larger than current setting> sudo sysctl fs.inotify.max_user_watches (take note of setting) sudo sysctl fs.inotify.max_user_watches=<something larger than current setting> ``` Fluent-bit を再起動します。 注意: これらの設定をノードの再起動後も維持するには、*/etc/sysctl.conf* に次の行を追加する必要があります。 ``` fs.inotify.max_user_instances=<something larger than current setting> fs.inotify.max_user_watches=<something larger than current setting> ```
Telegraf DS ポッドは、TLS 証明書を検証できないために kubernetes 入力プラグインが HTTP リクエストを実行できないことに関連するエラーを報告しています。例: E! [inputs.kubernetes] プラグインのエラー: HTTPリクエストの送信中にエラーが発生しました"<a href="https://<kubelet_IP>:10250/stats/summary":" class="bare">https://<kubelet_IP>:10250/stats/summary":得る"<a href="https://<kubelet_IP>:10250/stats/summary":" class="bare">https://<kubelet_IP>:10250/stats/summary":tls: 証明書の検証に失敗しました: x509: IP SANが含まれていないため、<kubelet_IP>の証明書を検証できません	これは、kubelet が自己署名証明書を使用している場合、および/または指定された証明書の証明書の *Subject Alternative Name* リストに <kubelet_IP> が含まれていない場合に発生します。これを解決するには、ユーザーは"エージェント構成"、*telegraf:insecureK8sSkipVerify* を *true* に設定します。これにより、Telegraf 入力プラグインが検証をスキップするように設定されます。あるいは、ユーザーはkubeletを次のように設定することができます。"サーバーTLSブートストラップ"これにより、「certificates.k8s.io」API からの証明書要求がトリガーされます。

問題：	これを試してください:
Fluent-bit ポッドで次のエラーが発生し、ポッドを起動できません：026/01/12 20:20:32] [error] [sqldb] error=unable to open database file [2026/01/12 20:20:32] [error] [input:tail:tail.0] db: could not create 'in_tail_files' table [2026/01/12 20:20:32] [error] [input:tail:tail.0] could not open/create database [2026/01/12 20:20:32] [error] failed initialize input tail.0 [2026/01/12 20:20:32] [error] [engine] input initialization failed	DBファイルが存在するホストディレクトリに適切な読み取り / 書き込み権限があることを確認してください。具体的には、ホストディレクトリは非ルートユーザーに読み取り / 書き込み権限を付与する必要があります。デフォルトのDBファイルの場所は、fluent-bit-dbFile *agentconfiguration* オプションで上書きされない限り、/var/log/ です。SELinuxが有効になっている場合は、fluent-bit-seLinuxOptionsType agentconfigurationオプションを 'spc_t' に設定してみてください。

追加情報は以下からご覧いただけます。"サポート"ページまたは"データコレクターサポートマトリックス"。

Memcached データコレクター

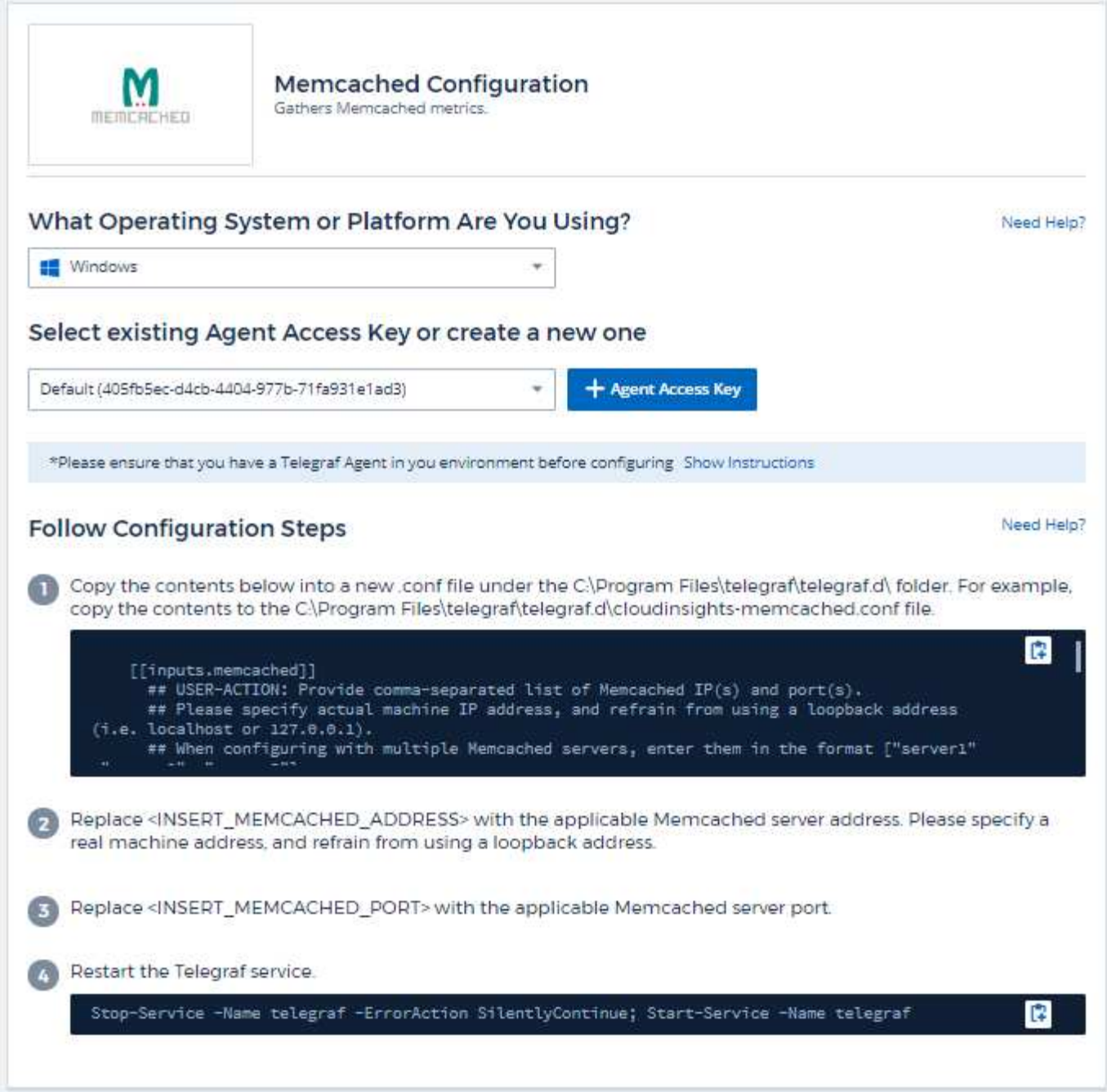
Data Infrastructure Insights は、このデータ コレクターを使用して Memcached からメトリックを収集します。

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 Memcached を選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

詳細は以下をご覧ください。"Memcached ウィキ" 。

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
メムキャッシュ	名前空間サーバー	ノードIPノード名	受け入れる接続 処理された認証要求 失敗した認証 使用バイト数 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) CAS 無効 CAS ヒット数 CAS ミス数 フラッシュ要求数 (1 秒あたり) 取得要求数 (1 秒あたり) セット要求数 (1 秒あたり) タッチ要求数 (1 秒あたり) 接続解放数 (1 秒あたり) 接続構造 オープン接続 現在保存されているアイテム 減少要求ヒット数 (1 秒あたり) 減少要求ミス数 (1 秒あたり) 削除要求ヒット数 (1 秒あたり) 削除要求ミス数 (1 秒あたり) 追い出されたアイテム 有効な追い出し 期限切れアイテム 取得ヒット数 (1 秒あたり) 取得ミス数 (1 秒あたり) 使用ハッシュバイト数 ハッシュが拡張中 ハッシュ電力レベル 増加要求ヒット数 (1 秒あたり) 増加要求ミス数 (1 秒あたり) サーバー最大バイト数 リッスン無効 再利用されたワーカースレッド数 オープン接続合計数 保存されたアイテム合計数 タッチヒット数 タッチミス数 サーバー稼働時間

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

MongoDB データコレクター

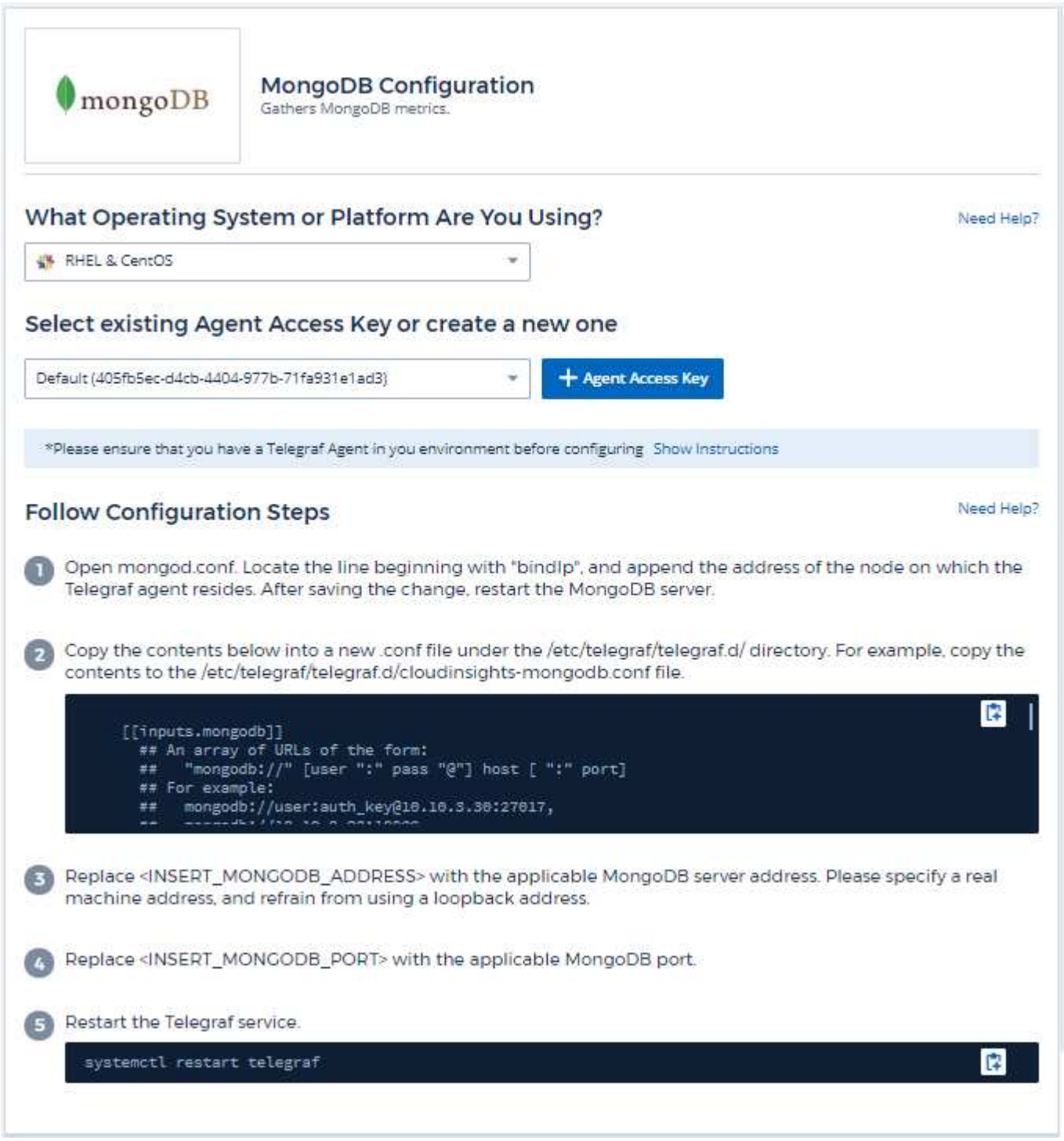
Data Infrastructure Insights は、このデータ コレクターを使用して MongoDB からメトリックを収集します。

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 MongoDB を選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 + エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

詳細は以下をご覧ください。"MongoDBのドキュメント" 。

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
MongoDB	名前空間ホスト名		
MongoDB データベース	名前空間 ホスト名 データベース名		

トラブルシューティング

情報は以下から入手できます。"サポート"ページ。

MySQL データコレクター

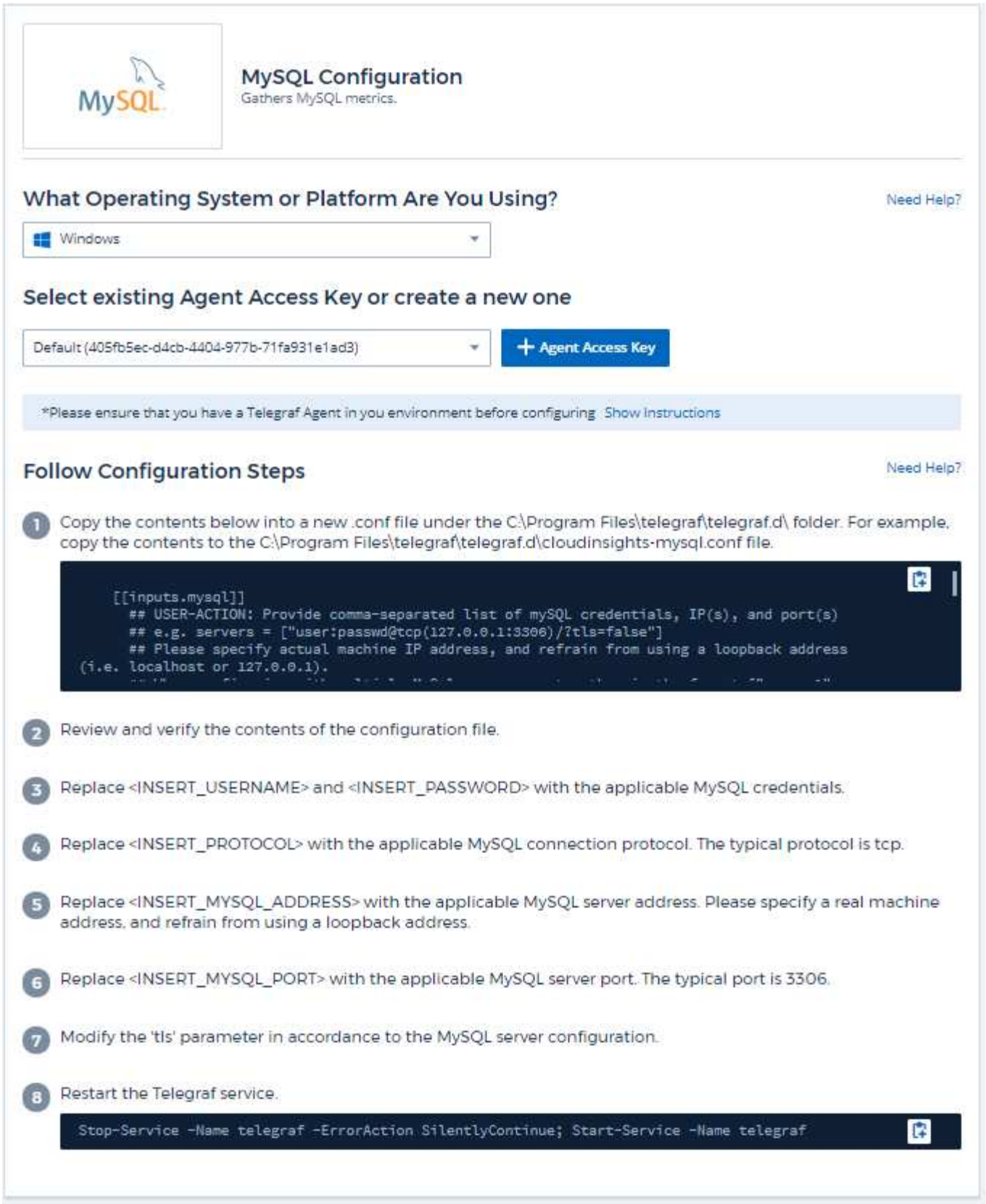
Data Infrastructure Insights は、このデータ コレクターを使用して MySQL からメトリックを収集します。

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 MySQLを選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

詳細は以下をご覧ください。"MySQLドキュメント" 。

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
MySQL	名前空間 MySQL サーバー	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） 中止された接続数（1秒あたり） 受信バイト数（1秒あたり） 送信バイト数（1秒あたり） 管理コマンド数（1秒あたり） イベント変更コマンド 関数変更コマンド インスタンス変更コマンド プロシージャ変更コマンド サーバー変更コマンド テーブル変更コマンド テーブルスペース変更コマンド ユーザー変更コマンド 分析コマンド キーキャッシュへの割り当てコマンド 開始コマンド バイナリログコマンド プロシージャ呼び出しコマンド DB変更コマンド マスター変更コマンド レプリケーションフィルター変更コマンド チェックコマンド チェックサムコマンド コミットコマンド DB作成コマンド イベント作成コマンド 関数作成コマンド インデックス作成コマンド プロシージャ作成コマンド サーバー作成コマンド テーブル作成コマンド トリガー作成コマンド UDF作成コマンド ユーザー作成コマンド ビュー作成コマンド SQL接続エラーの割り当て解除 作成された一時ディスクテーブルの受け入れ 遅延エラー フラッシュコマンド ハンドラーコミット Innodbバッファプールバイトデータ フラッシュされていないキーブロック キー読み取り要求 キー書き込み要求 キー書き込み最大実行時間使用中の接続の最大数を超えました 開いているファイル パフォーマンス スキーマ アカウント 失われました 準備されたステートメントの数 Qcache 空きブロック クエリ 質問 フル結合の選択 フル範囲結合の選択 範

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

Netstat データコレクター

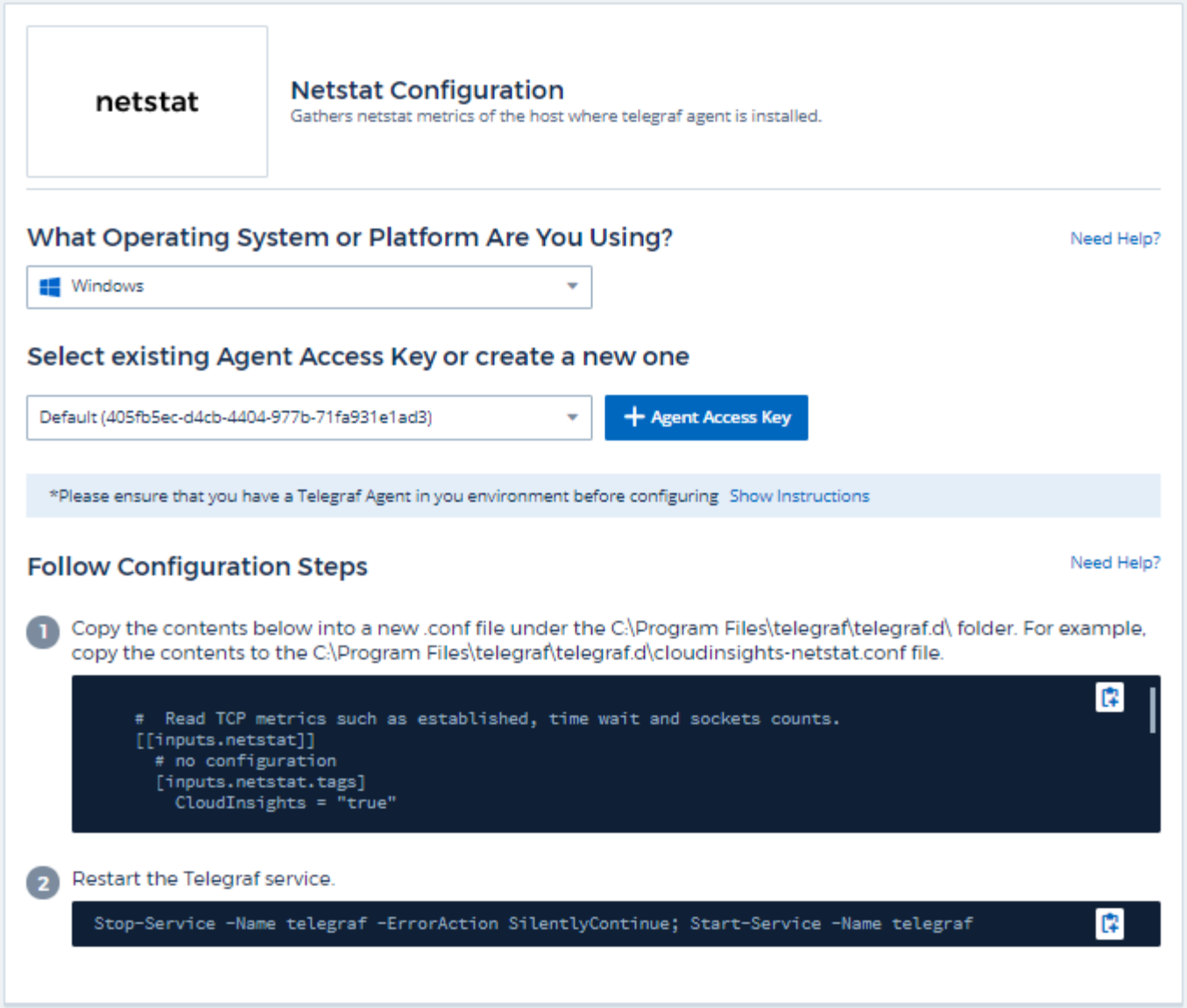
Data Infrastructure Insights は、このデータ コレクターを使用して Netstat メトリックを収集します。

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 Netstat を選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
ネットスタット	ノードUUID	ノードIPノード名	

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

Nginx データコレクター

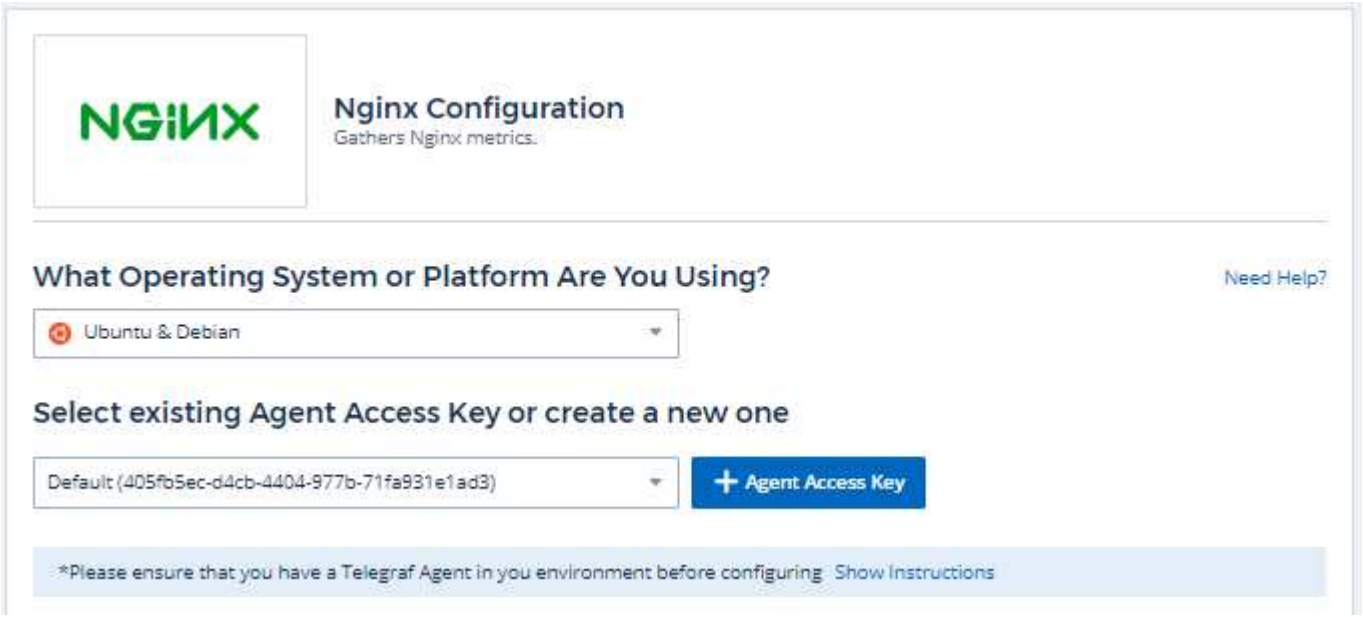
Data Infrastructure Insights は、このデータ コレクターを使用して Nginx からメトリックを収集します。

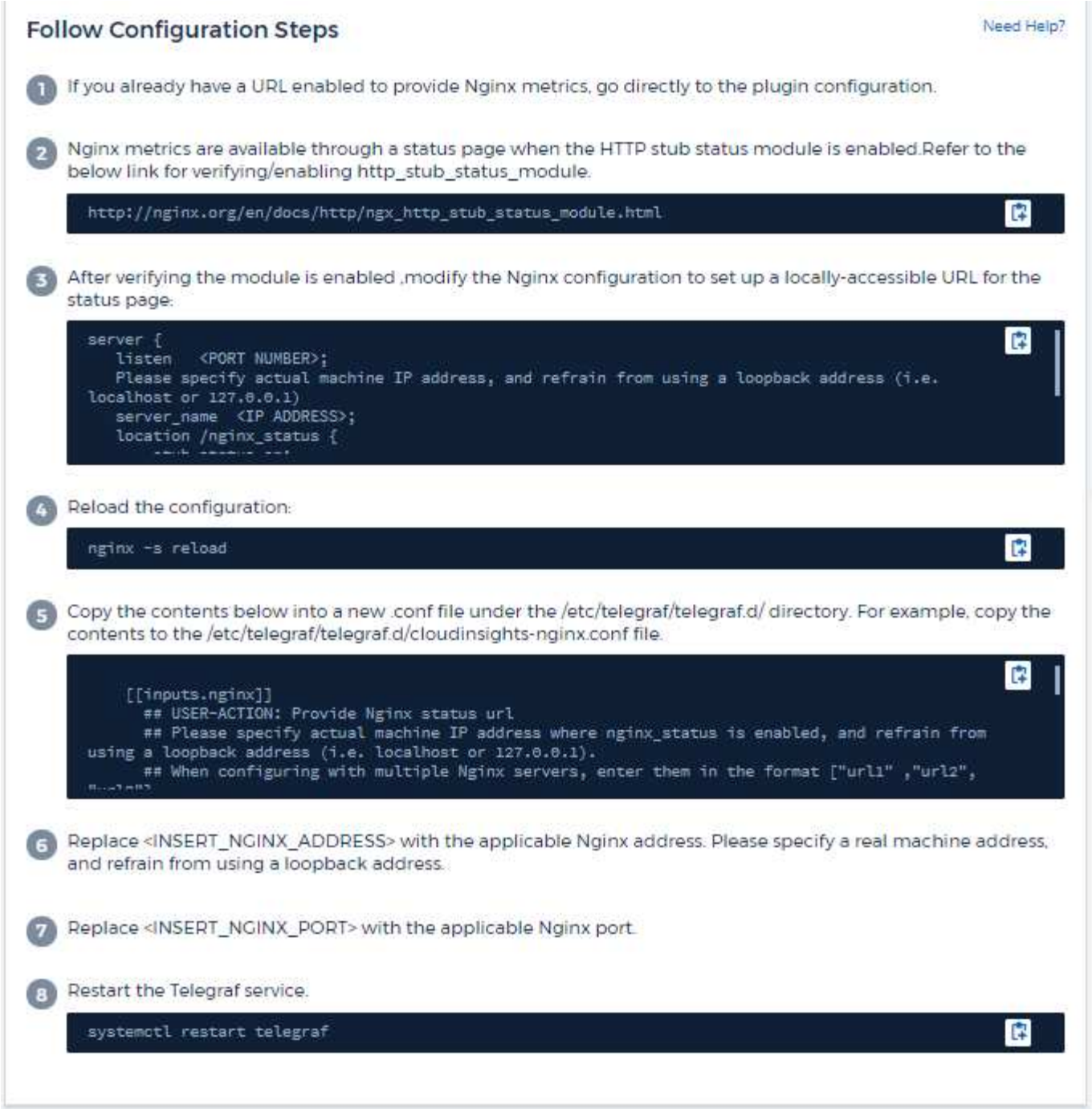
インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 Nginx を選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。





セットアップ

Nginxのメトリック収集には、Nginx"http_stub_status_module"有効になります。

追加情報は以下をご覧ください。"Nginxのドキュメント" 。

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
Nginx	名前空間サーバー	ノードIP ノード名 ポート	アクティブに処理された読み取り要求を受け入れ、書き込みを待機

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

PostgreSQL データコレクター

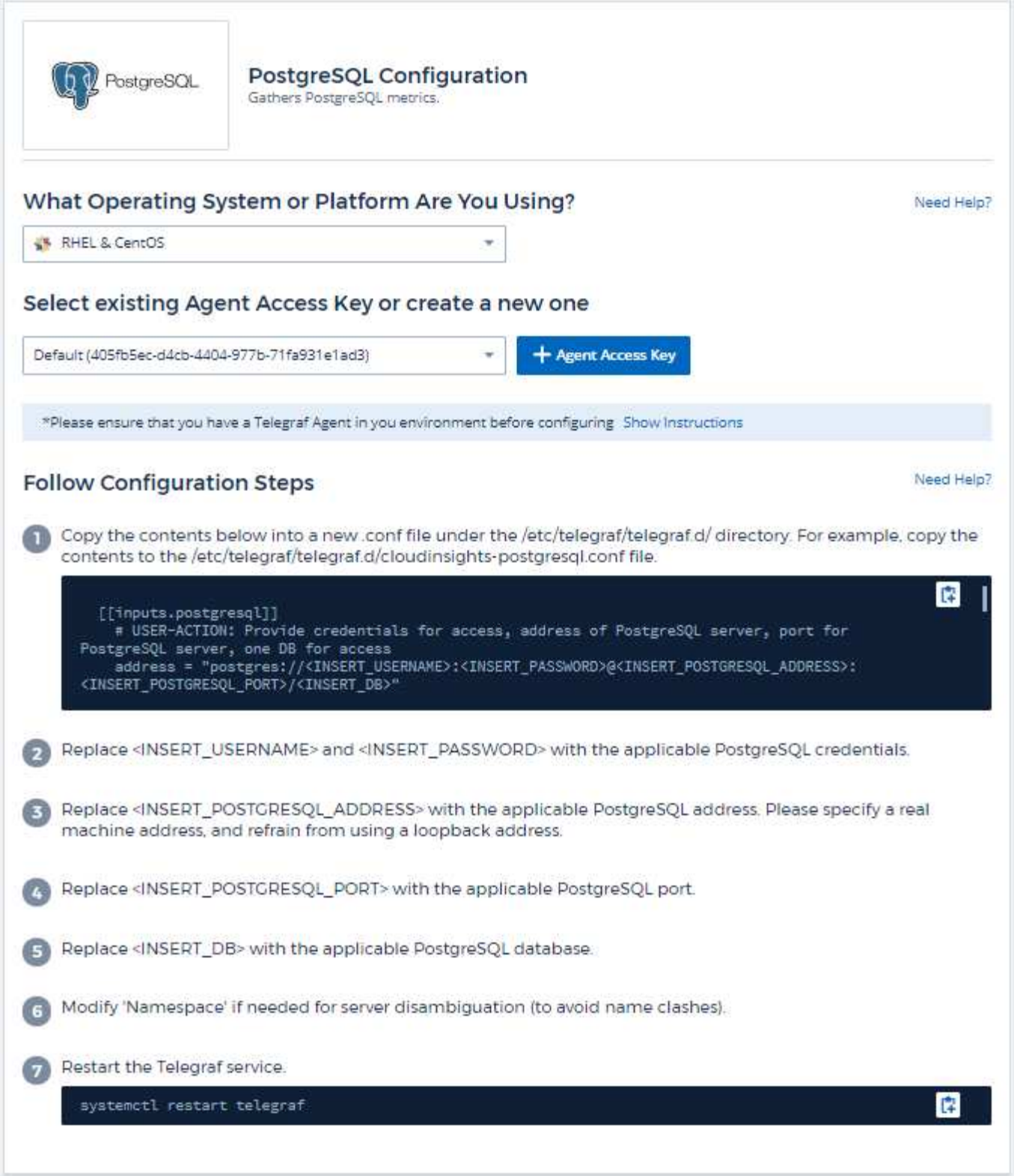
Data Infrastructure Insights は、このデータ コレクターを使用して PostgreSQL からメトリックを収集します。

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 PostgreSQLを選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

詳細は以下をご覧ください。"PostgreSQLドキュメント" 。

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
PostgreSQLサーバー	名前空間データベースサーバー	ノード名 ノードIP	バッファ 割り当てられたバッファ バックエンドバッファ 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 クリーンチェックポイント 同期時間 チェックポイント書き込み時間 チェックポイント 要求 チェックポイント 時間指定 最大書き込みクリーン
PostgreSQLデータベース	名前空間データベースサーバー	データベースOID ノード名 ノードIP	ブロック読み取り時間、ブロック書き込み時間、ブロックヒット数、ブロック読み取り数、競合数、デッドロック数、クライアント数、一時ファイル数、バイト数、一時ファイル数、削除された行数、フェッチされた行数、挿入された行数、返された行数、更新されたトランザクション数、コミットされたトランザクション数、ロールバックされたトランザクション数

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

Puppet エージェント データコレクター

Data Infrastructure Insights は、このデータ コレクターを使用して、Puppet Agent からメトリックを収集します。

インストール

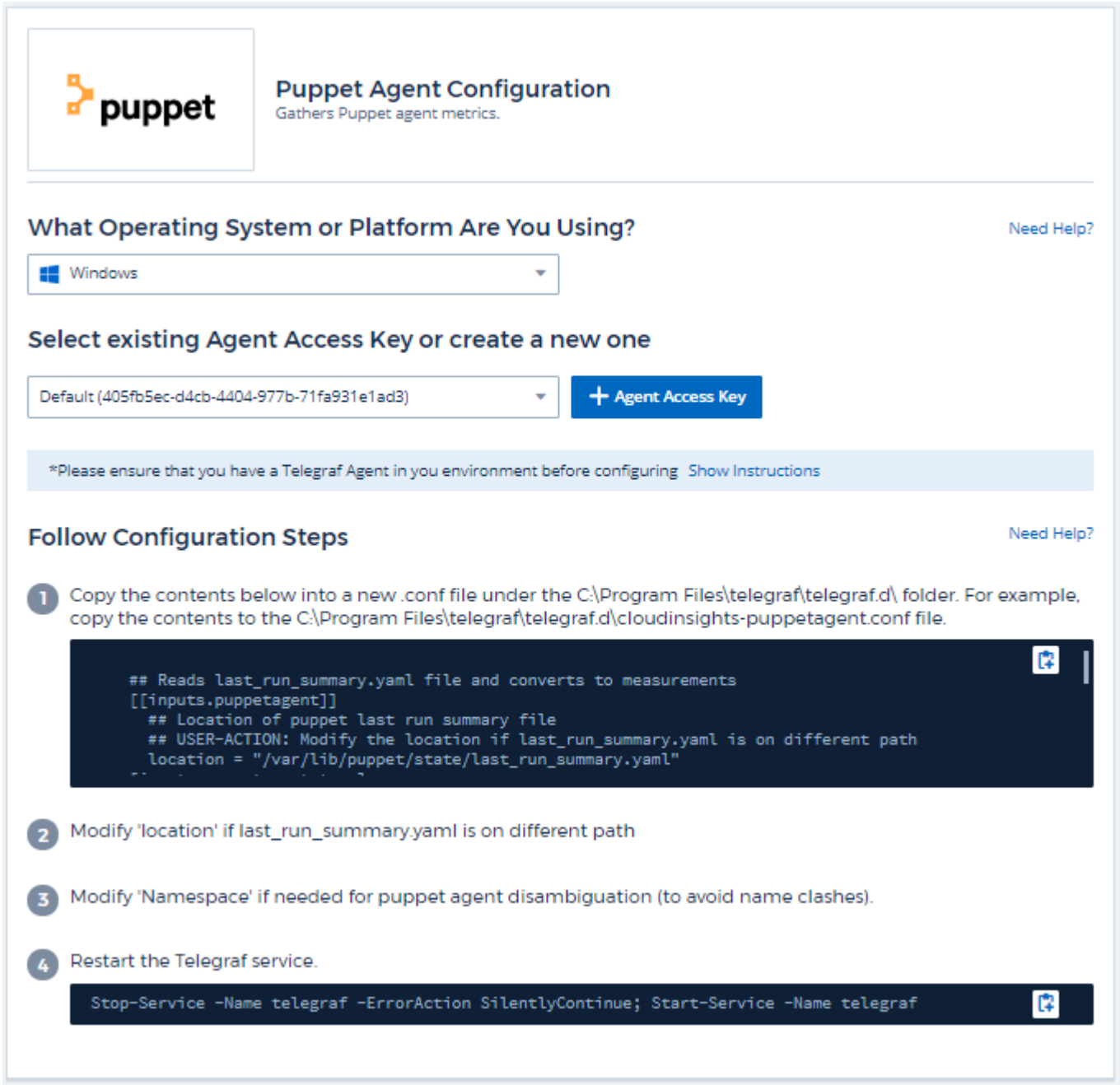
1. **Observability > Collectors** から、**+ Data Collector** をクリックします。パペットを選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント

アクセス キーを使用します。

4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

詳細は以下をご覧ください。 "Puppetのドキュメント"

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:

操り人形エージェント	名前空間ノードUUID	ノード名 場所 ノードIP バージョン Configstring バージョン Puppet	変更合計イベント 失敗イベント 成功イベント 合計リソース 変更されたリソース 失敗したリソース 再起動に失敗したリソース 同期していないリソース 再起動されたリソース スケジュールされたリソース スキップされたリソース 合計時間 アンカー時間 Configretrieval時間 Cron時間 Exec時間 ファイル時間 ファイルバケット時間 最終実行時間 パッケージ時間 スケジュール時間 サービス時間 sshauthorizedkey時間 合計時間 ユーザー

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

Redis データコレクター

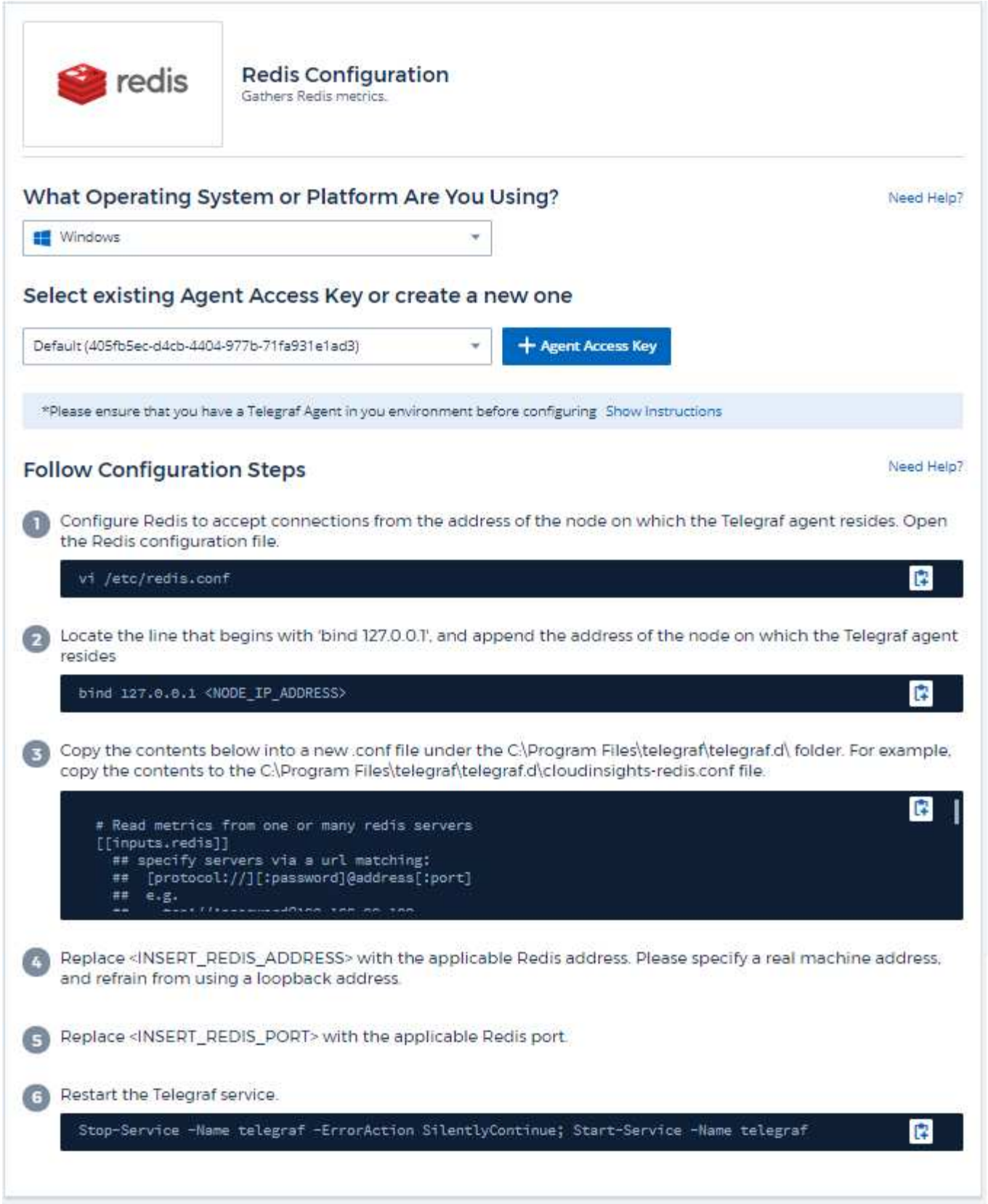
Data Infrastructure Insights は、このデータ コレクターを使用して Redis からメトリックを収集します。 Redis は、データベース、キャッシュ、メッセージ ブローカーとして使用されるオープン ソースのインメモリ データ構造ストアであり、文字列、ハッシュ、リスト、セットなどのデータ構造をサポートしています。

インストール

1. **Observability > Collectors** から、**+ Data Collector** をクリックします。 Redis を選択します。

   Telegraf 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. 収集用のエージェント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用のエージェントをインストールする場合は、[手順を表示] をクリックして展開します。"エージェントのインストール"説明書。
3. このデータ コレクターで使用するエージェント アクセス キーを選択します。 **+** エージェント アクセス キー 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: データ コレクターを OS/プラットフォーム別などにグループ化する場合にのみ、異なるエージェント アクセス キーを使用します。
4. 構成手順に従ってデータ コレクターを構成します。手順は、データ収集に使用し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の種類によって異なります。



セットアップ

詳細は以下をご覧ください。"Redisのドキュメント" 。

オブジェクトとカウンター

次のオブジェクトとそのカウンターが収集されます。

オブジェクト	識別子:	属性:	データポイント:
レディス	名前空間サーバー		

トラブルシューティング

追加情報は以下からご覧いただけます。"サポート"ページ。

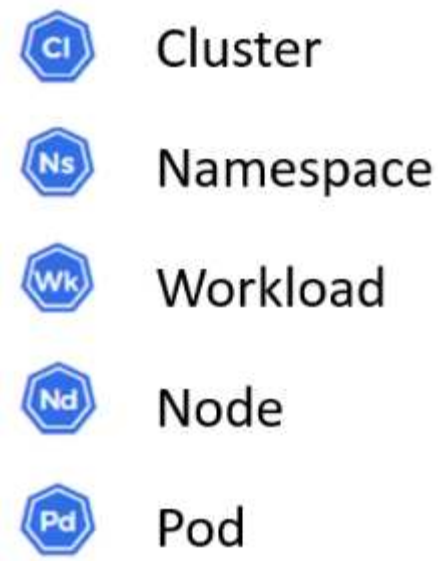
オブジェクトアイコンリファレンス

Data Infrastructure Insightsで使用されるオブジェクト アイコン。

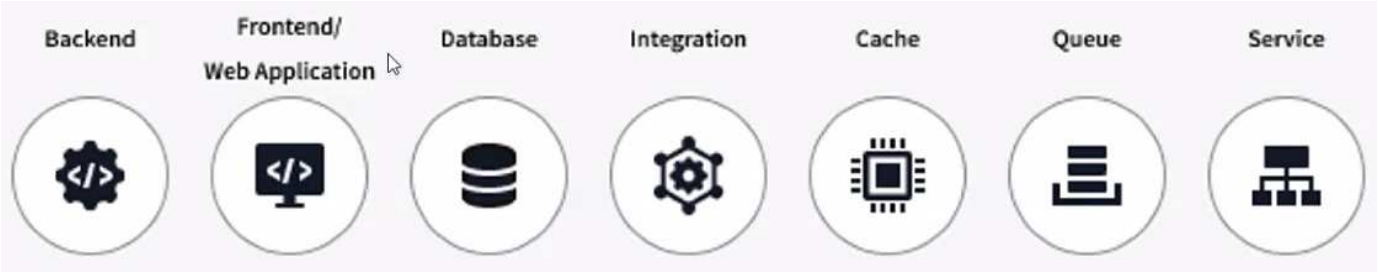
インフラストラクチャアイコン:



Kubernetes アイコン:



Kubernetes ネットワーク パフォーマンス監視とマップ アイコン**:**



法律上の表示

法的通知から、著作権情報、商標、特許などを確認できます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp、NetAppのロゴ、NetAppの商標一覧のページに掲載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

現在NetAppが所有する特許の一覧は以下のページから閲覧できます。

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、 NetApp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提供されます。

Data Infrastructure Insights （旧Cloud Insights）に関するお知らせ、window=_blank

Workload Security（旧Cloud Secure）に関するお知らせ、window=_blank

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

商標に関する情報

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