



## 監視とアラート

### Data Infrastructure Insights

NetApp  
September 09, 2025

# 目次

|                          |     |
|--------------------------|-----|
| 監視とアラート                  | 1   |
| モニタとのアラート                | 1   |
| セキュリティのベストプラクティス         | 1   |
| メトリックまたはログモニタ            | 1   |
| 監視リスト                    | 8   |
| グループを監視します               | 8   |
| システム定義のモニター              | 11  |
| モニタからのアラートの表示と管理         | 11  |
| アラートの表示と管理               | 11  |
| アラート詳細パネル                | 12  |
| データが見つからない場合に警告します       | 13  |
| 「Permanently Active」アラート | 14  |
| 電子メール通知を設定しています          | 14  |
| サブスクリプション通知の受信者          | 14  |
| アラートのグローバル受信者リスト         | 15  |
| ONTAP の通知の編集             | 15  |
| 異常検出モニタ                  | 17  |
| 異常検出とは                   | 17  |
| 異常検出はいつ必要ですか？            | 18  |
| 異常検出モニタの作成               | 18  |
| 異常の表示                    | 20  |
| システムモニタ                  | 21  |
| モニタの説明                   | 22  |
| 詳細情報                     | 92  |
| 電子メール通知を設定しています          | 92  |
| サブスクリプション通知の受信者          | 93  |
| アラートのグローバル受信者リスト         | 94  |
| ONTAP の通知の編集             | 94  |
| Webhook 通知               | 95  |
| webhook を使用した通知          | 95  |
| Discord のウェブフックの例        | 99  |
| PagerDuty の webhook の例   | 101 |
| Slack の Web フックの例        | 105 |
| Microsoft チームの Web フックの例 | 107 |

# 監視とアラート

## モニタとのアラート

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、そのような条件が満たされたときに通知を受け取ります。

監視を使用すると、ストレージ、VM、EC2、ポートなどの「インフラ」オブジェクトによって生成される指標や、Kubernetes、ONTAPの高度な指標、Telegrafプラグイン用に収集されたデータなどの「統合」データに対してしきい値を設定できます。これらの\_は、警告レベルまたは重大レベルのしきい値を超えたときにアラートを監視します。

また、警告レベル、重大レベル、または情報レベルのアラートをトリガーするモニタを作成して、指定されたログイベントが検出されたときに生成することもできます。

Data Infrastructure Insightsには、環境に応じて多数の機能もあり["システム定義のモニター"](#)ます。

## セキュリティのベストプラクティス

Data Infrastructure Insightsのアラートは、テナントのデータポイントや傾向を示すように設計されており、Data Infrastructure Insightsを使用すると、アラート受信者として有効なEメールアドレスを入力できます。セキュアな環境で作業する場合は、通知を受け取っているユーザ、またはアラートへのアクセス権があるユーザを特に意識してください。

## メトリックまたはログモニタ

1. [Data Infrastructure Insights]メニューで、\*[Alerts]>[Manage Monitors]\*をクリックします。  
[モニタ]リストページが表示され、現在設定されているモニタが表示されます。
2. 既存のモニタを変更するには、リストでモニタ名をクリックします。
3. モニタを追加するには、\*+ モニタ\*をクリックします。

**Metric Monitor**

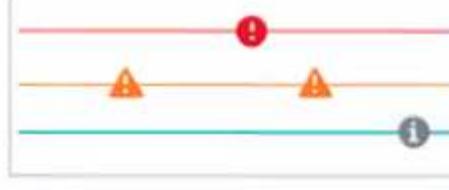
Set the high and low parameters that will trigger an alert if exceeded



Use when you know the upper and lower operating range

**Log Monitor**

Monitor logs and configure alerts



Use when you want to trigger alerts in response to log activity

新しいモニタを追加すると、メトリックモニタまたはログモニタを作成するよう求められます。

- `_Metric_` は、インフラまたはパフォーマンスに関するトリガーに関するアラートを監視します
- ログ関連のアクティビティに関するアラートを監視します

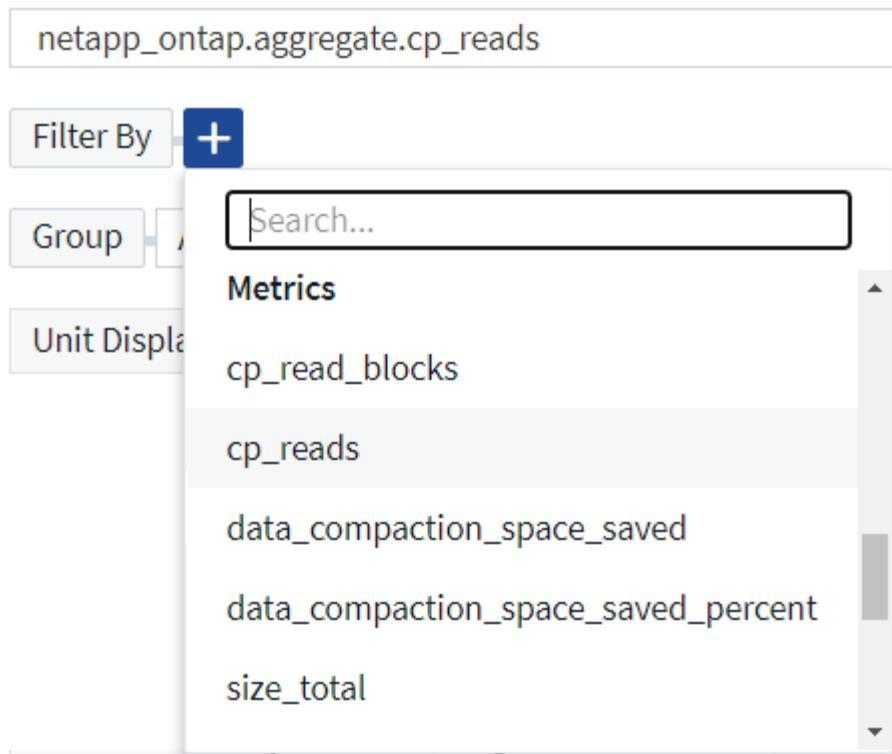
モニタタイプを選択すると、モニタ設定ダイアログが表示されます。構成は、作成するモニタのタイプによって異なります。

#### メートル法モニタ（Metric Monitor）

1. ドロップダウンで、監視するオブジェクトタイプと指標を検索して選択します。

フィルタを設定して、監視するオブジェクトの属性や指標を絞り込むことができます。

## 1 Select a metric to monitor



netapp\_ontap.aggregate.cp\_reads

Filter By +

Group

Metrics

Unit Display

Search...

cp\_read\_blocks

cp\_reads

data\_compaction\_space\_saved

data\_compaction\_space\_saved\_percent

size\_total

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



複数条件のモニタ（IOPS > X、レイテンシ > Yなど）を作成するには、最初の条件をしきい値、2番目の条件をフィルタとして定義します。

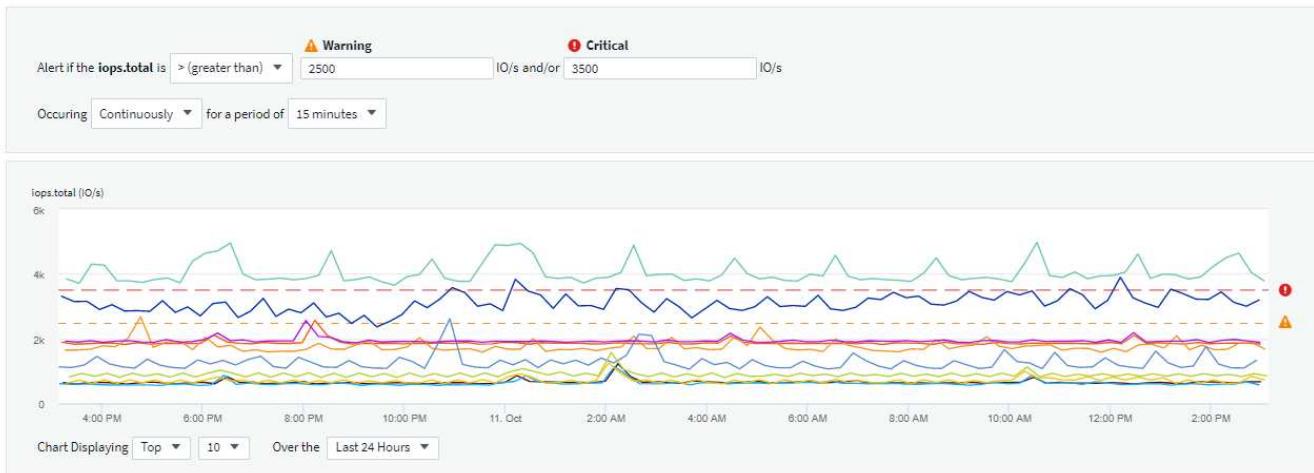
モニターの条件を定義します。

1. 監視するオブジェクトと指標を選択したら、警告レベルと重大レベルのしきい値、またはその両方を設定します。
2. Warning\_level には、この例に 200 を入力します。この警告レベルを示す破線がグラフの例に表示されます。
3. Critical\_level の場合は、400 と入力します。このクリティカルレベルを示す破線がグラフの例に表示されます。

このグラフには履歴データが表示されます。グラフ上の警告および重大レベルの線はモニタを視覚的に表しているため、モニタがアラートをトリガーするタイミングを簡単に確認できます。

4. 実行間隔には、15 分 Continuously を選択します。

しきい値を超えた時点でアラートをトリガーするか、しきい値が一定期間継続して違反になるまでアラートをトリガーするかを選択できます。この例では、合計 IOPS が警告レベルまたは重大レベルを超えるたびにアラートを表示する必要はありませんが、監視対象のオブジェクトがこれらのレベルの 1 つを 15 分以上継続して超えた場合にのみアラートを表示します。



アラート解決の動作を定義します

指標モニタのアラートの解決方法を選択できます。次の2つの選択肢が表示されます。

- メトリックが許容範囲に戻ったときに解決します。
- メトリックが、指定した時間（1分～7日）にわたって許容範囲内に収まった場合に解決します。

## ログモニタ

\*Log monitor \* を作成する場合は、まず使用可能なログリストから、監視するログを選択します。次に、前述のように使用可能な属性に基づいてフィルタできます。1つ以上の「グループ化」属性を選択することもできます。



ログモニタフィルタを空にすることはできません。

### 1 Select the log to monitor

アラートの動作を定義します

上記で定義した条件が1回（即刻）発生した場合に、重大度レベル\_Critical\_、\_Warning\_、または\_Informational\_でアラートを生成したり、条件が2回以上発生するまでアラートを待機したりするようにモニタを作成できます。

アラート解決の動作を定義します

ログモニタのアラートの解決方法を選択できます。次の3つの選択肢があります。

- \* 即時解決\*：このアラートは、対処不要で即座に解決されます

- ・ \* 時間に基づく解決 \* : アラートは指定した時間が経過すると解決されます
- ・ \* ログエントリに基づいて解決 \* : このアラートは、後続のログアクティビティが発生すると解決されます。たとえば、あるオブジェクトが「available」としてログされる場合などです。

- Resolve instantly
- Resolve based on time
- Resolve based on log entry

Log Source
logs.netapp.ems
▼

Filter By
ems.ems\_message\_type
"object.store.available"
X
▼
X
+

## 異常検出モニタ

1. ドロップダウンで、監視するオブジェクトタイプと指標を検索して選択します。

フィルタを設定して、監視するオブジェクトの属性や指標を絞り込むことができます。

### 1 Select a metric anomaly to monitor

Object
Storage
X
▼
Metric
iops.total
X
▼

Filter by Attribute
+
?

Filter by Metric
+
?

Group by
Storage
▼

Unit Displayed In
Whole Number
▼

モニターの条件を定義します。

1. 監視するオブジェクトとメトリックを選択した後、異常が検出される条件を設定します。
  - ・ 選択したメトリック\*スパイクが予測された境界を超えている場合、\*ドロップがそれらの境界を超えている場合、\*スパイクが境界を超えている場合、または\*スパイクが境界を下回っている場合に異常を検出するかどうかを選択します。
  - ・ 検出の\*感度\*を設定します。低（検出される異常が少ない）、中、または\*高\*（検出される異常が多い）。
  - ・ 警告をWither \* Warning または Critical \*に設定します。
  - ・ 必要に応じて、選択したメトリックが設定したしきい値を下回った場合に異常を無視して、ノイズを低減するように選択できます。

## 2 Define the monitor's conditions

Trigger alert when **performance.iops.total** Spikes above the predicted bounds.

Set sensitivity: Low (detect fewer anomalies)

Alert severity: Critical

To reduce noise, ignore anomalies when **performance.iops.total** is below Optional IO/s

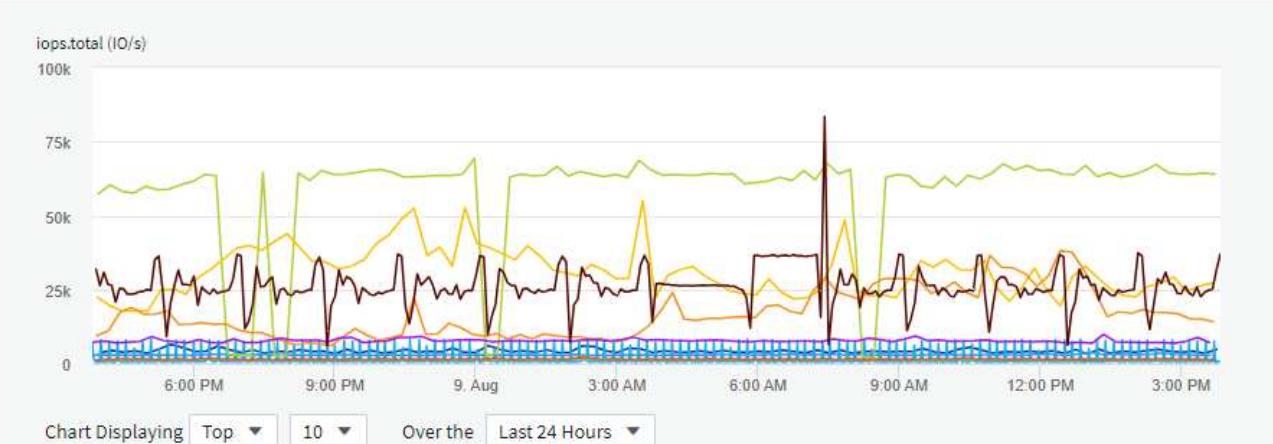


Chart Displaying Top 10 Over the Last 24 Hours

通知タイプと受信者を選択します

[チーム通知の設定] セクションでは、電子メールと Webhook のどちらでチームに通知するかを選択できます。

## 3 Set up team notification(s) (alert your team via email, or Webhook)

Add Delivery Method ▾

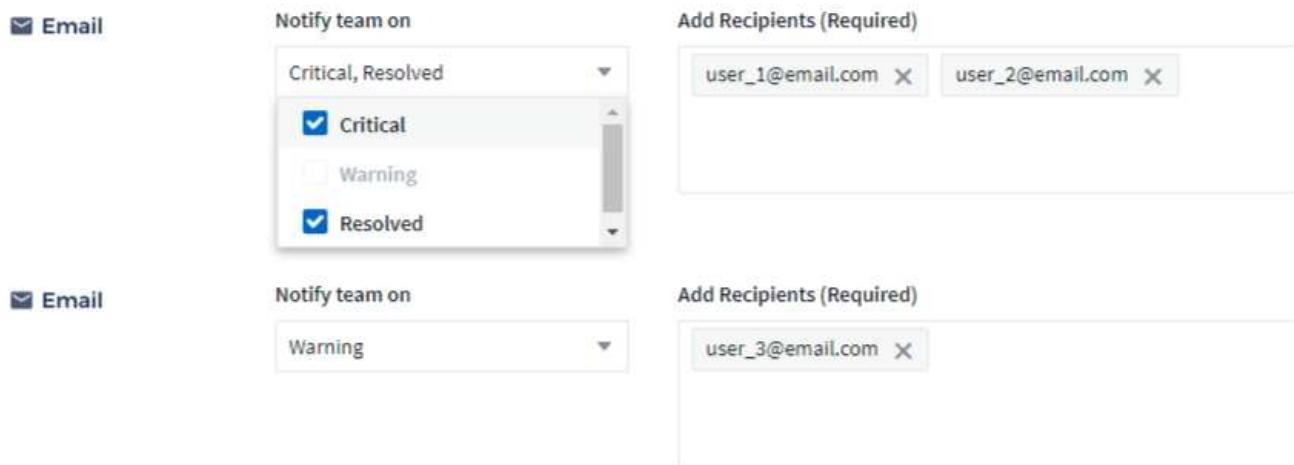
Email

Webhook

- 電子メールによる警告 :\*

アラート通知の E メール受信者を指定します。必要に応じて、警告または重大なアラートの受信者を別々に選択することもできます。

### 3 Set up team notification(s)



Configure team notifications via email:

- Notify team on:** Critical, Resolved
- Recipients:** user\_1@email.com, user\_2@email.com

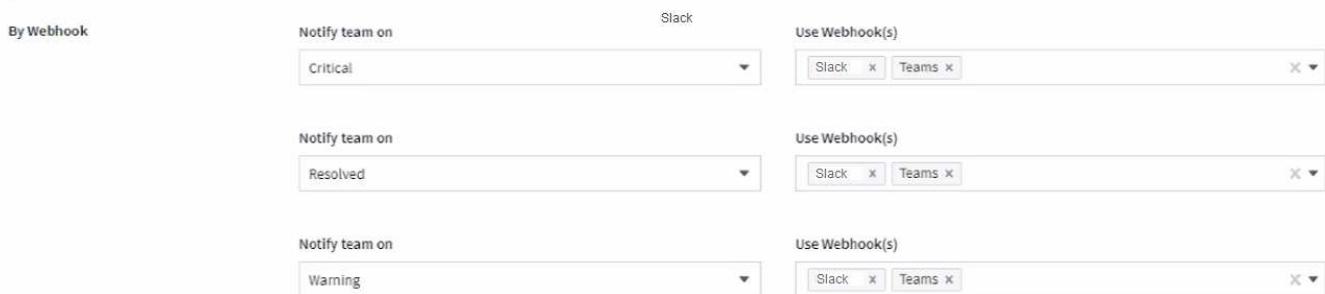
Configure team notifications via email:

- Notify team on:** Warning
- Recipients:** user\_3@email.com

- Webhookによる警告 :\*

アラート通知に使用する Web フックを指定します。必要に応じて、警告または重大なアラートに別のフックを選択できます。

### 3 Set up team notification(s) (alert your team via email, or Webhook)



Configure team notifications via webhook:

- Notify team on:** Critical
- Use Webhook(s):** Slack, Teams

Configure team notifications via webhook:

- Notify team on:** Resolved
- Use Webhook(s):** Slack, Teams

Configure team notifications via webhook:

- Notify team on:** Warning
- Use Webhook(s):** Slack, Teams

**ONTAP データコレクタ通知**は、クラスタ/データコレクタに関する特定のモニタ通知よりも優先されます。Data Collector自体に設定した受信者リストには、データコレクタアラートが送信されます。アクティブなデータコレクタアラートがない場合は、監視用に生成されたアラートが特定の監視受信者に送信されます。

対処方法または追加情報を設定しています

オプションの概要を追加したり、追加のインサイトや修正アクションを追加したりするには、「\*アラート概要の追加\*」セクションに入力します。概要是 1024 文字以内で指定し、アラートとともに送信されます。分析情報 / 対処方法のフィールドは最大 67,000 文字で、アラートランディングページの概要セクションに表示されます。

これらのフィールドには、アラートを修正したり対処したりするためのメモ、リンク、手順を入力できます。

アラートの説明にパラメータとして任意のオブジェクト属性（ストレージ名など）を追加できます。たとえば、ボリューム名とストレージ名のパラメータを次のような説明で設定できます。"High Latency for Volume : %% relatedObject.volume.name%%, Storage : %% relatedObject.storage.name%%"

#### 4 Add an alert description (optional)

|                                     |   |
|-------------------------------------|---|
| Add a description                   | Enter a description that will be sent with this alert (1024 character limit)            |
| Add insights and corrective actions | Enter a url or details about the suggested actions to fix the issue raised by the alert |

#### モニタを保存します

1. 必要に応じて、モニタの概要を追加できます。
2. モニターにわかりやすい名前を付け、 \* 保存 \* をクリックします。

新しいモニタがアクティブなモニタのリストに追加されます。

#### 監視リスト

[Monitor] ページには、現在設定されているモニタが一覧表示され、次の情報が示されます

- ・モニタ名
- ・ステータス
- ・監視対象のオブジェクト / 指標
- ・モニタの状態

モニターの右側にあるメニューをクリックし、 \* 一時停止 \* を選択すると、オブジェクトタイプの監視を一時的に停止できます。モニタリングを再開する準備ができたら、 \* Resume \* (続行) をクリックします。

モニタをコピーするには、メニューから「 \* Duplicate (複製) \* 」を選択します。その後、新しいモニタを変更して、オブジェクト / 指標、フィルタ、条件、 E メール受信者などを変更できます

モニタが不要になった場合は、メニューから \* Delete \* を選択して削除できます。

#### グループを監視します

グループ化により、関連するモニタを表示および管理できます。たとえば、テナントのストレージ専用の監視グループを設定したり、特定の受信者リストに関連する監視を設定したりできます。

Monitor Groups (5)

All Monitors (5)

Custom Monitors (5)

Agent Monitors (3)

ONTAP Aggregate Monitors (2)

次のモニタグループが表示されます。グループ名の横には、グループに含まれるモニタの数が表示されます。

- \* すべてのモニタ \* にすべてのモニタが一覧表示されます。
- \* カスタムモニター \* には、ユーザーが作成したすべてのモニターが一覧表示されます。
- \*一時停止中のモニター\*には、Data Infrastructure Insightsによって一時停止されたシステムモニターが表示されます。
- Data Infrastructure Insightsには複数の\*システム監視グループ\*も表示され、"システム定義のモニタ" "ONTAPインフラ監視やワーカロード監視など、の1つ以上のグループが表示されます。



カスタムモニタは、一時停止、再開、削除、または別のグループへの移動が可能です。システム定義のモニタは一時停止および再開できますが、削除または移動することはできません。

## 一時停止したモニタ

このグループは、Data Infrastructure Insightsが1つ以上のモニタを一時停止している場合にのみ表示されます。モニタが過度のアラートまたは継続的なアラートを生成している場合、モニタが一時停止することがあります。モニタがカスタムモニタの場合は、継続的なアラートの発生を防止する条件を変更してから、モニタを再開します。問題がサスペンションを引き起こしている状態が解消されると、モニタはサスペンド状態のモニタグループから削除されます。

## システム定義のモニター

これらのグループには、監視に必要なデバイスやログの可用性が環境に含まれている限り、Data Infrastructure Insightsが提供する監視が表示されます。

システム定義のモニタは、変更、別のグループへの移動、または削除できません。ただし、システムモニタを複製して、複製を変更または移動することはできます。

システムモニタには、ONTAP インフラストラクチャ（ストレージ、ボリュームなど）のモニタ、ワーカロード（ログモニタなど）、またはその他のグループが含まれます。ネットアップでは、お客様のニーズと製品の機能を常に評価しており、必要に応じてシステムの監視やグループの更新や追加を行います。

## カスタムモニタグループ

必要に応じてモニタを含めるための独自のグループを作成できます。たとえば、すべてのストレージ関連モニタのグループを作成する場合などです。

新しいカスタムモニタグループを作成するには、「+」「新規モニタグループの作成\*」ボタンをクリックします。グループの名前を入力し、「\* グループの作成\*」をクリックします。空のグループがその名前で作成されます。

モニタをグループに追加するには、\_all Monitors グループ（推奨）に移動し、次のいずれかの操作を行います。

- ・ 単一のモニタを追加するには、モニタの右側にあるメニューをクリックし、「\_グループに追加\_」を選択します。モニタを追加するグループを選択します。
- ・ モニタ名をクリックしてモニタの編集ビューを開き 'Associate to a monitor group' セクションでグループを選択します

## 5 Associate to a monitor group (optional)

ONTAP Monitors

モニタを削除するには、グループをクリックし、メニューから「\_グループから削除」を選択します。モニタを\_all Monitors\_ または \_Custom Monitors\_ グループから削除することはできませんこれらのグループからモニタを削除するには、モニタ自体を削除する必要があります。

グループからモニタを削除しても、そのモニタがData Infrastructure Insightsから削除されることはありません。モニタを完全に削除するには、モニタを選択し、Delete( 削除 )をクリックします。これにより、その所有者であるグループからも削除され、どのユーザからも使用できなくなります。

同様にモニタを別のグループに移動するには 'Move to Group' を選択します

グループ内のすべてのモニタを一度に一時停止または再開するには、グループのメニューを選択し、「\_Pause or Resume\_」をクリックします。

同じメニューを使用して、グループの名前変更または削除を行います。グループを削除しても、Data Infrastructure Insightsからモニタは削除されません。モニタは「すべてのモニタ」で引き続き使用できます。

The screenshot shows the AWS CloudWatch Metrics Metrics Explorer interface. At the top, it displays 'Monitor Groups (3)' with a '+' button and a back arrow. Below that is a search bar with the placeholder 'Agent Monitors' and a clear 'X' button. The main list area shows 'All Monitors (4)' and 'Custom Monitors (4)'. Under 'Agent Monitors (3)', a context menu is open, showing options: 'Pause', 'Resume', 'Rename', and 'Delete'. The 'Delete' option is highlighted in red.

## システム定義のモニター

Data Infrastructure Insightsには、指標とログの両方について、システム定義の監視が多数含まれています。使用可能なシステムモニタは、テナントに存在するデータコレクタによって異なります。そのため、Data Infrastructure Insightsで使用できるモニタは、データコレクタの追加や設定の変更に応じて変更される場合があります。

ページを表示して、Data Infrastructure Insightsに含まれるモニタの説明を確認["システム定義のモニター"](#)します。

### 詳細情報

- ["アラートの表示と非表示"](#)

## モニタからのアラートの表示と管理

Data Infrastructure Insightsには、超過した場合にアラートが表示され["監視対象のしきい値"](#)ます。



監視とアラートは、Data Infrastructure Insights Standard Edition以上で利用できます。

### アラートの表示と管理

アラートを表示および管理するには、次の手順を実行します。

1. [\* Alerts] > [All Alerts] \* ページに移動します。
2. 最新の 1,000 個までのアラートのリストが表示されます。フィールドの列ヘッダーをクリックすると、任意のフィールドでこのリストをソートできます。リストには、次の情報が表示されます。デフォルトでは、すべての列が表示されるわけではありません。歯車アイコンをクリックすると、表示する列を選択できます。

- \* アラート ID\* : システムによって生成された一意のアラート ID
- \* Triggered Time \* : 該当するモニタがアラートをトリガーした時刻
- \* 現在の重大度 \* (アクティブなアラートタブ) : アクティブなアラートの現在の重大度
- \* 重大度上位 \* (解決済みアラートタブ) : 解決前のアラートの最大重大度
- **Monitor** : アラートをトリガーするように設定されたモニタ
- \* triggered on \* : 監視対象のしきい値に違反したオブジェクト
- \* ステータス \* : 現在のアラートステータス、 *New\_or\_in Process*
- \* アクティブステータス \* : *\_Active\_or\_Resolved\_*
- \* Condition \* : アラートをトリガーしたしきい値条件
- \* Metric \* : 監視対象のしきい値を超えたオブジェクトのメトリック
- **Monitor Status** : アラートをトリガーしたモニタの現在のステータス
- \* 対応処置あり \* : アラートで推奨される対処方法が提示されています。アラートページを開いて表示します。

アラートの右側にあるメニューをクリックし、次のいずれかを選択してアラートを管理できます。

- \* **処理中** \* : アラートが調査中であること、またはオープン状態を維持する必要があることを示します
- \* **Dismiss** \* を選択すると、アクティブなアラートのリストからアラートが削除されます。

各アラートの左側にあるチェックボックスをオンにして、 [選択したアラートステータスの変更] をクリックすると、複数のアラートを管理できます。

アラート ID をクリックすると、アラート詳細ページが開きます。

## アラート詳細パネル

アラートの行を選択すると、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、アラートに関する詳細情報 (概要、オブジェクトのデータに関するグラフを表示する\_エキスパートビュー\_、関連アセット、アラート調査担当者が入力した\_コメント\_など) が表示されます。

## Metric Alert

Jun 3, 2025  
9:29 AM - 10:47 AM



### ! Critical Alert AL-14930837

ACTIVE

[Collapse Details](#)

#### Triggered On

Storage:

CI-GDL1-OnTap-fas8080

#### Details

Top Severity: Critical

Condition: Average iops.total is > (greater than) 1,700 IO/s and/or 2,000 IO/s all the time in 15-minute window.

#### Monitor

alttimeout

#### Attributes

Filters Applied: N/A

#### Description

No Description Provided

#### Resolution conditions

Resolve when metric is within acceptable range for 10 mins

#### Status

New

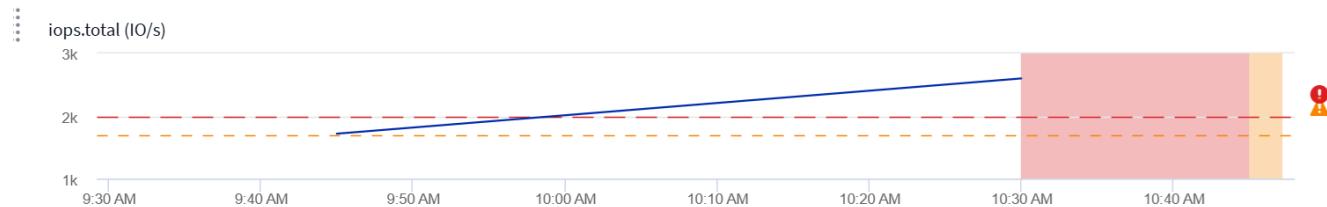
#### Time

Triggered time: Jun 3, 2025 10:44 AM Duration: 17m (Active)

Alert Summary

Alert Attributes

Jun 03, 2025 09:29 AM - 10:47 AM



[Close](#)

## データが見つからない場合に警告します

Data Infrastructure Insightsなどのリアルタイムシステムでは、監視の分析をトリガーしてアラートを生成するかどうかを判断するには、次の2つの要素のいずれかを使用します。

- 次のデータポイントに到達します
- データポイントがなく、十分な時間を持っているときに起動するタイマー

データの到着が遅い場合やデータの到着がない場合と同様に、「リアルタイム」でアラートをトリガーするにはデータの到着率が不十分であるため、タイマーメカニズムを引き継ぐ必要があります。そのため、通常は、「分析ウィンドウを閉じて所持しているものを確認するまで、どのくらい待つ必要があるか?」という質問になります。待機時間が長すぎると、アラートが生成されるまでの時間が長くなりません。

長期的なデータ損失が発生する前の最後のデータポイントによって条件が違反されていることを通知する30

分のウィンドウを備えたモニタがある場合、この状態が持続していることをモニタが確認するために使用する他の情報を受信しなかったため、アラートが生成されます。

## 「Permanently Active」アラート

監視対象オブジェクトでは、条件を「常に \*」にするようにモニタを設定できます。たとえば、IOPS>1 や Latency >0 などです。これらは頻繁に「テスト」モニターとして作成され、そして忘れられる。このような監視を実行すると、コンステイチュエントオブジェクトを永続的に開いたままにするアラートが作成されます。これにより、原因システムにかかる負荷や安定性の問題が時間の経過に

これを回避するために、Data Infrastructure Insightsは「永続的にアクティブな」アラートを7日後に自動的に閉じます。基本的なモニタ状態が（おそらく）継続して存在し、新しいアラートがほぼ即座に発行されることに注意してください。しかし、この「常時アクティブ」アラートを閉じることで、他の状況で発生する可能性のあるシステム負荷が軽減されます。

## 電子メール通知を設定しています

サブスクリプション関連の通知用の E メールリストや、パフォーマンスポリシーのしきい値違反の通知を受け取る受信者のグローバル E メールリストを設定できます。

通知メール受信者の設定を行うには、[\*Admin] > [Notifications] ページに移動し、[Email] タブを選択します。

### Subscription Notification Recipients

Send subscription related notifications to the following:

- All Account Owners
- All Monitor & Optimize Administrators
- Additional Email Addresses

name@email.com

Save

### Global Monitor Notification Recipients

Default email recipients for monitor related notifications:

- All Account Owners
- All Monitor & Optimize Administrators
- Additional Email Addresses

Save

## サブスクリプション通知の受信者

サブスクリプション関連のイベント通知の受信者を設定するには、「サブスクリプション通知の受信者」セクションに移動します。次の受信者のいずれかまたはすべてに、サブスクリプション関連イベントに関する E メール通知を送信するように選択できます。

- ・すべてのアカウント所有者
- ・すべての監視と最適化管理者

- ・指定する追加の E メールアドレス

送信される通知の種類と実行できるユーザアクションの例を次に示します。

| * 通知 : *  | * ユーザーアクション : *   |
|---|---|
| トライアルまたはサブスクリプションが更新されました   | ページでサブスクリプションの詳細を確認する <a href="#">"配信登録"</a>  |
| サブスクリプションの有効期限は 90 日ですサブスクリプションの有効期限は 30 日です                              | [Auto Renewal]が有効な場合、対応は不要です。NetAppセールスに連絡してサブスクリプションを更新してください。                                 |
| トライアルは 2 日で終了します  | ページからトライアルを更新し <a href="#">"配信登録"</a> ます。試用版は 1 回更新できます。サブスクリプションの購入については、NetApp営業担当にお問い合わせください |
| トライアルまたはサブスクリプションの有効期限が切れたアカウントは、48 時間以内にアカウントの収集を停止し、48 時間後にアカウントが削除されます | サブスクリプションの購入については、NetApp営業担当にお問い合わせください   |

受信者がData Infrastructure Insightsからの通知を受信できるようにするには、「許可」リストに次のEメールアドレスを追加します。



- ・\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

アラートの E メール通知は、アラートに対するすべての対処方法についてアラート受信者リストに送信されます。アラート通知をグローバル受信者リストに送信することもできます。

グローバルアラート受信者を設定するには、[\* Global Monitor Notification Recipients] セクションで目的の受信者を選択します。

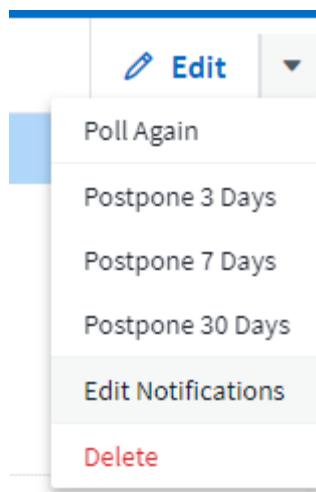
モニタを作成または変更するときは、各モニタのグローバル受信者リストを常に上書きできます。



ONTAP データコレクタ通知は、クラスタ/データコレクタに関連する特定のモニタ通知よりも優先されます。Data Collector自体に設定した受信者リストには、データコレクタアラートが送信されます。アクティブなデータコレクタアラートがない場合は、監視用に生成されたアラートが特定の監視受信者に送信されます。

## ONTAP の通知の編集

ONTAP クラスタの通知を変更するには、ストレージランディングページの右上のドロップダウンから[Edit Notifications]を選択します。



ここでは、重大、警告、情報、解決済みのアラートの通知を設定できます。各シナリオは、グローバル受信者リストまたは選択した他の受信者に通知できます。

## Edit Notifications

X

By Email

Notify team on

Critical, Warn...

Send to



- Global Monitor Recipient List  
 Other Email Recipients

email@email.one

email2@email2.two

Notify team on

Resolved

Send to



- Global Monitor Recipient List  
 Other Email Recipients

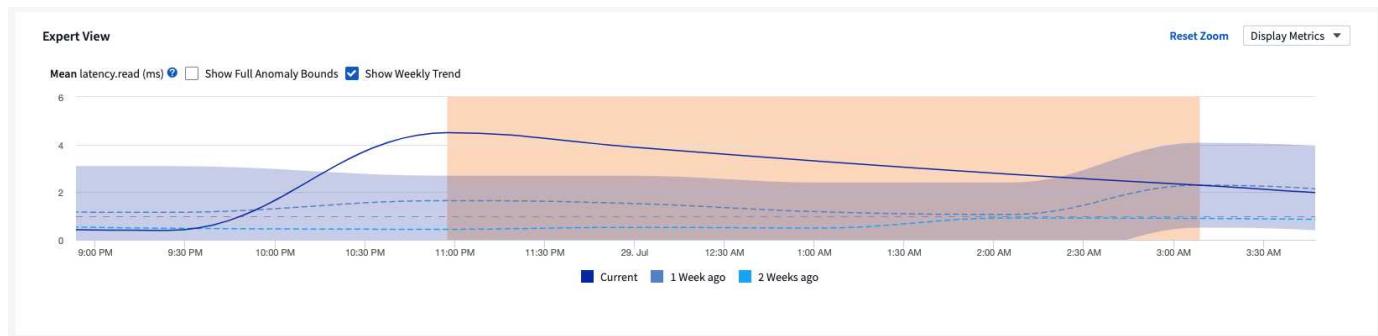
By Webhook

Enable webhook notification to add recipients

# 異常検出モニタ

異常検出では、テナント上のデータパターンの予期しない変化を分析できます。異常は、オブジェクトの動作のパターンが変化したときに発生します。たとえば、オブジェクトのレイテンシが水曜日のある時間に一定のレベルを超えていても、その次の水曜日のその時間にレイテンシが急増した場合、そのスパイクは異常とみなされます。Data Infrastructure Insightsでは、このような異常が発生したときにアラートを通知するモニタを作成できます。

異常検出は、予測可能な繰り返しパターンを示すオブジェクト指標に適しています。これらのオブジェクト指標が想定レベルを上回る、または下回ると、Data Infrastructure Insightsはアラートを生成して調査を促すことができます。



## 異常検出とは

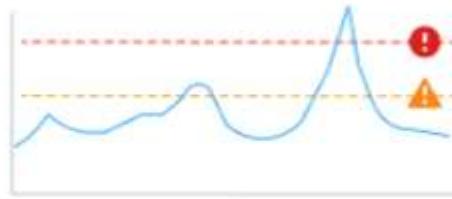
異常は、メトリックの平均値が、過去数週間のメトリックの加重平均からの標準偏差の数であり、最近の週の重みが前の週よりも大きい場合に発生します。Data Infrastructure Insightsは、データを監視し、異常の検出時にアラートを生成する機能を提供します。検出の「感度」レベルを設定することもできます。たとえば、平均値が平均からの標準偏差が少ない場合、より多くのアラートが生成されるようになります。逆に、感度が低い=平均からの標準偏差が多い=アラートの数が少ない。

異常検出の監視は、しきい値の監視とは異なります。

- \*しきい値ベースの監視\*は、特定のメトリックのしきい値が事前に定義されている場合に機能します。言い換えれば、何が期待されるのか(つまり、通常の範囲内)を明確に理解しているときです。

## Metric Monitor

Set the high and low parameters that will trigger an alert if exceeded



Use when you know the upper and lower operating range

- \*異常検出モニタリング\*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、標準から逸脱する異常値を特定します。

**Anomaly  
Detection Monitor**  
Detect and be alerted  
to abnormal  
performance changes



Use when you want to  
trigger alerts against  
performance spikes  
and drops

## 異常検出はいつ必要ですか？

異常検出の監視では、次のような多くの状況で役立つアラートが提供されます。

- `_normal` の定義が不明な場合。たとえば、ポートによっては、SANエラー率がさまざまに予想される場合があります。1つのエラーに関するアラートはノイズが多く、不要ですが、突然または大幅に増加した場合は、広範な問題が発生す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。季節的なワークロード（特定の時間にビジー状態または静かな状態）。これには、バッチの停止を示す可能性のある予期しない待機期間が含まれる可能性があります。
- しきい値を手動で定義して調整することが現実的ではない大量のデータを扱う。たとえば、さまざまなワークロードのホストやボリュームが多数あるテナントなどです。SLAはそれぞれ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。

## 異常検出モニタの作成

異常を警告するには、\*[Observability]>[Alerts]>[+Monitor]\*に移動してモニタを作成します。モニタタイプとして[*Anomaly Detection Monitor*]を選択します。

## Metric Monitor

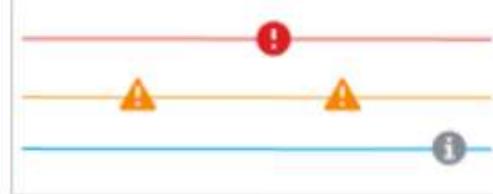
Set the high and low parameters that will trigger an alert if exceeded



Use when you know the upper and lower operating range

## Log Monitor

Monitor logs and configure alerts

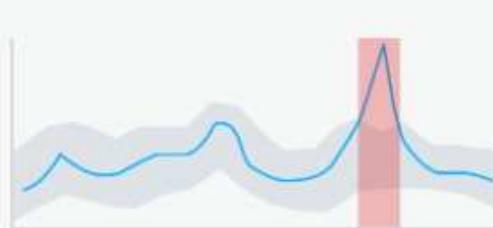


Use when you want to trigger alerts in response to log activity

## Anomaly

### Detection Monitor

Detect and be alerted to abnormal performance changes



Use when you want to trigger alerts against performance spikes and drops

監視するオブジェクトと指標を選択します。他のタイプのモニタと同様に、フィルタとグループ化を設定できます。

次に、モニタ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の上に\_Spike\_するか、\_drops below those bounds\_、またはその両方のいずれかの場合にアラートをトリガーします。
- 感度を\_Medium\_、\_Low\_（検出される異常が少ない）、または\_High\_（検出される異常が多い）に設定します。
- アラートレベルが\_Critical\_か\_Warning\_かを確認します。
- 必要に応じて、異常が\_ignored\_になる値を設定します。これはノイズを減らすのに役立ちます。この値は、サンプルグラフに破線で示されています。

## 2 Define the monitor's conditions

Trigger alert when **performance.iops.total** Spikes above the predicted bounds.

Set sensitivity: Low (detect fewer anomalies)

Alert severity: Critical

To reduce noise, ignore anomalies when **performance.iops.total** is below 3000 IO/s



Chart Displaying Top 10 Over the Last 24 Hours

最後に、アラートの配信方法（Eメール、Webhook、またはその両方）を設定したり、オプションの説明または修正アクションをモニタに指定したり、必要に応じてモニタをカスタムグループに追加したりできます。

モニタにわかりやすい名前を付けて保存すると、完了です。

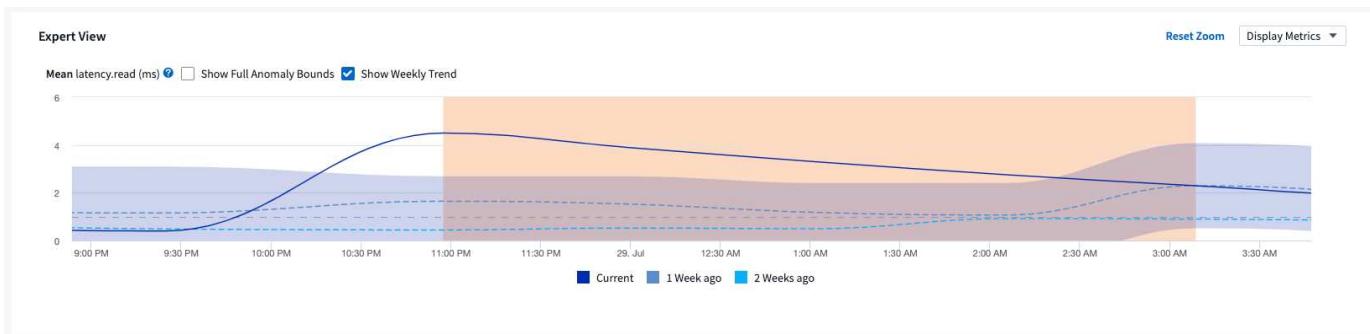
モニタを作成すると、前週のデータが分析され、初期ベースラインが確立されます。時間が経過して履歴が増えるにつれて、異常検出の精度が向上します。



モニターが作成されると、DIIは前週の既存データを確認し、顕著なデータの急上昇または急降下がないか確認します。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、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。

## 異常の表示

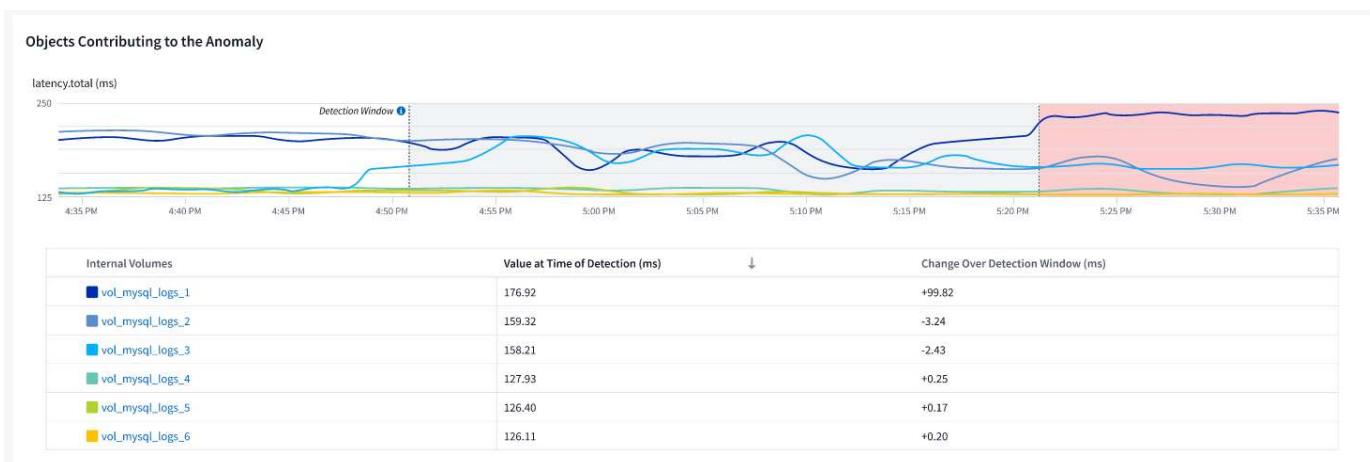
アラートランディングページでは、異常が検出されたときにトリガーされたアラートに、指標が予測範囲外に急増した時点から、その範囲内に戻った時点までのハイライトされた帯がグラフに表示されます。



アラートランディングページで異常チャートを表示する際には、次のオプションを選択できます。

- **Weekly Trend**（週ごとの傾向）：前の週の同じ時刻（前の週の同じ日）と最大5週間の値を比較します。
- **Full Anomaly Bounds**：デフォルトでは、指標の動作をより適切に分析できるように、グラフは指標値に焦点を当てています。異常境界全体（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エキスパートビュー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。グラフには、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

Data Infrastructure Insightsには、指標とログの両方について、システム定義の監視が多数含まれています。使用可能なシステムモニタは、テナントに存在するデータコレクタによって異なります。そのため、Data Infrastructure Insightsで使用できるモニタは、データコレクタの追加や設定の変更に応じて変更される場合があります。

多くのシステムモニタは、デフォルトでIN\_PAUSED\_STATEになっています。システムモニタを有効にするには、モニタの\_Resume\_optionを選択します。Data Collectorで\_Advanced Counter Data Collection\_and\_Enable ONTAP EMSログcollection\_が有効になっていることを確認します。これらのオプションは、ONTAP Data Collectorの\_Advanced Configuration\_にあり

**Enable ONTAP EMS log collection**

ます。 **Opt in for Advanced Counter Data Collection rollout.**

目次：[]

## モニタの説明

システム定義のモニタは、事前に定義されたメトリックと条件に加えて、デフォルトの説明と修正アクションで構成されています。これらは変更できません。システム定義モニタの通知受信者リストを変更できます。メトリック、条件、概要、および修正アクションを表示したり、受信者リストを変更したりするには、システム定義のモニタグループを開き、リスト内のモニタ名をクリックします。

システム定義のモニタグループは変更または削除できません。

以下のシステム定義モニタは、記載されたグループで使用できます。

- \* ONTAP インフラストラクチャ \* は、ONTAP クラスタのインフラストラクチャ関連の問題を監視します。
- \* ONTAP ワークロードの例 \* には、ワークロード関連の問題のモニターが含まれています。
- 両方のグループのモニタのデフォルトは \_Paused \_ state です。

現在Data Infrastructure Insightsに含まれているシステム監視は次のとおりです。

### メトリックモニタ

| モニタ名               | 重大度 | 概要を監視します   | 対処方法   |
|--------------------|-----|--|--|
| ファイバチャネルポートの利用率が高い | 重大  | ファイバチャネルプロトコルポートは、お客様のホストシステムとONTAP LUNの間でSANトラフィックを送受信するために使用されます。ポートの利用率が高い場合は、そして、これはボトルネックになり、最終的にはファイバチャネルプロトコルの負荷の影響を受けやすいパフォーマンスに影響を与えます。...警告アラートは、ネットワークトラフィックのバランスを取るために計画されたアクションを実行する必要があることを示します。...重大アラートは、サービスの中断が差し迫っていること、およびネットワークのバランスを取るための緊急措置を示します サービスの継続性を確保するためのトラフィック。 | 重大の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緊急の対処方法を検討してください：1. 利用率の低い別のFCPポートにワークロードを移動します。2.特定のLUNのトラフィックは、ONTAPのQoSポリシーまたはホスト側の構成を使用して重要な作業のみに制限し、FCPポートの使用率を軽減します。警告しきい値を超えた場合は、次の操作を実行するように計画してください：1.データトラフィックを処理するFCPポートを増やして、ポート利用率をより多くのポートに分散させます。2.利用率の低い別のFCPポートにワークロードを移動します。3.特定のLUNのトラフィックは、ONTAPのQoSポリシーまたはホスト側設定を使用して重要な作業だけに制限し、FCPポートの利用率を軽減します。 |

|                    |    |   |   |
|--------------------|----|---|---|
| LUN レイテンシが高くなっています | 重大 | <p>LUN は、I/O トライフィックを処理するオブジェクトで、多くの場合、データベースなどのパフォーマンス重視のアプリケーションによって駆動されます。LUN のレイテンシが高いと、アプリケーション自体が影響を受け、タスクを実行できなくなる可能性があります。... 警告アラートは、LUN を適切なノードまたはアグリゲートに移動するため計画的なアクションが必要であることを示しています。... 重大アラートは、サービスの停止が差し迫っていること、および緊急時の措置を講じる必要があることを示してい サービスの継続性を確保します。次に、メディアタイプに基づく想定レイテンシを示します。これは、最大 1 ~ 2 ミリ秒の SSD、最大 8 ~ 10 ミリ秒の SAS、および 17 ~ 20 ミリ秒の SATA HDD です</p> | <p>重大しきい値を超えた場合は、サービスの中断を最小限に抑えるために次の操作を検討してください。LUN またはそのボリュームに QoS ポリシーが関連付けられている場合は、そのしきい値制限を評価し、LUN ワークロードが調整されているかどうかを確認します。警告しきい値を超えた場合は、次の操作を実行するように計画してください：</p> <ol style="list-style-type: none"> <li>1. アグリゲートの利用率も高い場合は、LUN を別のアグリゲートに移動してください。</li> <li>2. ノードの利用率も高い場合は、ボリュームを別のノードに移動するか、ノードの合計ワークロードを減らしてください。</li> <li>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て、LUN 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。</li> </ol> |
|--------------------|----|---|---|

|                  |    |  |   |
|------------------|----|--|---|
| ネットワークポートの利用率が高い | 重大 | <p>ネットワークポートは、NFS、CIFS、およびiSCSIのプロトコルトラフィックを受信して、お客様のホストシステムとONTAPの間で転送するために使用されます。ポート利用率が高いとボトルネックになり、最終的にはNFSのパフォーマンスに影響します。CIFSとiSCSIのワークロード。警告アラートは、ネットワークトラフィックのバランスを取るために計画されたアクションを実行する必要があることを示しています。重要アラートは、サービスの中止が差し迫っていることを示しており、サービスの継続性を確保するためにネットワークトラフィックの負荷を分散するために緊急措置を講じる</p> | <p>重大のしきい値を超えた場合は、サービスの停止を最小限に抑えるために次の緊急アクションを検討してください：</p> <ol style="list-style-type: none"> <li>1.ONTAPのQoSポリシーまたはホスト側の分析によって、ネットワークポートの利用率を下げるために、特定のボリュームのトラフィックを重要な処理のみに制限します。</li> <li>2.利用率の低い別のネットワークポートを使用するように、1つまたは複数のボリュームを設定します。...警告しきい値を超えた場合は、すぐに次の操作を実行することを検討してください。</li> </ol> <ol style="list-style-type: none"> <li>1.データトラフィックを処理するネットワークポートを増やして、ポート利用率をより多くのポートに分散させます。</li> <li>2.利用率の低い別のネットワークポートを使用するように1つ以上のボリュームを設定します。</li> </ol> |
|------------------|----|--|---|

|                       |    |   |   |
|-----------------------|----|---|---|
| NVMe ネームスペースレイテンシが高です | 重大 | <p>NVMe ネームスペースは、データベースなどのパフォーマンス重視のアプリケーションで I/O トラフィックを処理するオブジェクトです。NVMe ネームスペースのレイテンシが高いと、アプリケーション自体が影響を受けてタスクを実行できなくなる可能性があります。...警告アラートは、LUN を適切なノードまたはアグリゲートに移動するための計画的なアクションが必要であることを示しています。...重大アラートは、サービスの停止が迫っていること、および緊急時の措置を講じる必要があることを示しサービスの継続性を確保するため。</p> | <p>重大しきい値を超えた場合は、サービスの中断を最小限に抑えるための即時の対処を検討してください。NVMeネームスペースまたはそのボリュームにQoSポリシーが割り当てられている場合は、NVMeネームスペースのワークロードが調整されている場合に備えて、制限しきい値を評価してください。警告しきい値を超えた場合は、次の操作を実行することを検討してください。1.アグリゲートの利用率も高い場合は、LUN を別のアグリゲートに移動してください。2.ノードの利用率も高い場合は、ボリュームを別のノードに移動するか、ノードの合計ワークロードを減らしてください。3.NVMeネームスペースまたはそのボリュームにQoSポリシーが割り当てられている場合は、制限のしきい値が原因でNVMeネームスペースのワークロードが調整されないように評価します。</p> |
|-----------------------|----|---|---|

|                 |    |  |   |
|-----------------|----|--|---|
| qtree 容量がフルです   | 重大 | <p>qtree とは、論理的に定義されたファイルシステムで、ボリューム内のルートディレクトリに特別なサブディレクトリとして作成できます。各 qtree には、ボリューム容量内でツリーに格納されるデータ量を制限するため、クオータポリシーによって定義されるデフォルトスペースクオータがあります。.....警告アラートは、スペースを増やすために計画的な処理が必要であることを示します。...重大アラートは、サービスの停止が差し迫っていることを示します</p> <p>サービスの継続性を確保するために、スペースを空けるために緊急措置を講じる必要があります。</p>  | <p>重大の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緊急の対処方法を検討してください：1. この増加に対応するために、qtree のスペースを増やしてください。2. 不要なデータを削除してスペースを解放します。...警告のしきい値を超える場合は、すぐに次の操作を実行するように計画してください：1. この増加に対応するために、qtree のスペースを増やしてください。2. 不要なデータを削除してスペースを解放します。</p> |
| qtree 容量ハードリミット | 重大 | <p>qtree とは、論理的に定義されたファイルシステムで、ボリューム内のルートディレクトリに特別なサブディレクトリとして作成できます。各 qtree には、ボリューム内のユーザデータの増加を制御し、合計容量を超えないようにデータを格納するために使用される KB 単位のスペースクオータがあります。qtree は、ユーザにアラートを提供するソフトストレージ容量クオータを維持し、合計容量に達する前にユーザにアラートを送信します</p> <p>qtree 内の容量クオータ制限が超過したため、データを格納できなくなりました。qtree に格納されているデータ量を監視することで、ユーザに中断のないデータサービスを確実に提供できます。</p> | <p>重大のしきい値を超えた場合は、サービスの停止を最小限に抑えるために次の緊急アクションを検討してください：1. 増加に対応するために、ツリースペースクオータを増やします 2. ツリー内の不要なデータを削除してスペースを解放するよう指示します</p>  |

|                      |    |   |  |
|----------------------|----|---|--|
| qtree 容量のソフトリミット     | 警告 | <p>qtree とは、論理的に定義されたファイルシステムで、ボリューム内のルートディレクトリに特別なサブディレクトリとして作成できます。各 qtree には、ボリューム内のユーザデータの増加を制御し、その合計容量を超えないようにデータを格納するために使用できる、KB 単位のスペースクオータがあります。qtree は、に到達する前にユーザにプロアクティブにアラートを提供するソフトストレージ容量クオータを維持します qtree 内の容量クオータの合計制限で、データを格納できなくなります。qtree に格納されているデータ量を監視することで、ユーザに中断のないデータサービスを確実に提供できます。</p> | <p>警告しきい値を超えた場合は、すぐに次の操作を実行することを検討してください。1. 増加に対応するために、ツリースペースクオータを増やしてください。2. ツリー内の不要なデータを削除してスペースを解放するようにユーザーに指示します。</p> |
| qtree のファイル数のハードリミット | 重大 | <p>qtree とは、論理的に定義されたファイルシステムで、ボリューム内のルートディレクトリに特別なサブディレクトリとして作成できます。各 qtree には、ボリューム内で管理可能なファイルシステムサイズを維持するために含めることができるファイル数のクオータがあります。... qtree は、ツリー内の新しいファイルが拒否されるハードファイル数のクオータを保持します。qtree 内のファイル数を監視すると、ユーザには中断のないデータサービスが確実に提供されます。</p>  | <p>重大の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緊急の対処方法を検討してください：1. qtree のファイル数クオータを増やします。2. 不要なファイルを qtree ファイルシステムから削除します。</p>      |

|                      |    |  |   |
|----------------------|----|--|---|
| qtree のファイル数がソフトリミット | 警告 | <p>qtree とは、論理的に定義されたファイルシステムで、ボリューム内のルートディレクトリに特別なサブディレクトリとして作成できます。各 qtree には、ボリューム内の管理可能なファイルシステムサイズを維持するために、格納できるファイル数のクオータがあります。... qtree は、ソフトファイル番号のクオータを保持し、qtree および内のファイル数の上限に達する前にユーザにプロアクティブにアラートを送信します 追加のファイルを保存できません。qtree 内のファイル数を監視すると、ユーザには中断のないデータサービスが確実に提供されます。</p> | <p>警告のしきい値を超える場合は、すぐに次の操作を実行するように計画してください：1.qtree のファイル数クオータを増やします。2.不要なファイルをqtree ファイルシステムから削除します。</p> |
|----------------------|----|--|---|

|                        |    |  |   |
|------------------------|----|--|---|
| Snapshot リザーブスペースがフルです | 重大 | <p>アプリケーションとお客様のデータを格納するには、ボリュームのストレージ容量が必要です。Snapshot 予約領域と呼ばれる領域の一部は Snapshot の保存に使用され、データを一カカルで保護できます。ONTAP ボリュームに格納される新規データや更新データが多いほど、使用される Snapshot 容量は増えますが、今後追加または更新されるデータに使用できる Snapshot ストレージ容量は少なくなります。ボリューム内の Snapshot データ容量が Snapshot リザーブスペースの合計に達すると、新しい Snapshot データを格納できなくなり、ボリューム内のデータの保護レベルが低下する可能性があります。ボリュームの使用済み Snapshot 容量を監視して、データサービスの継続性を確保します。</p> | <p>重大の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緊急の対処方法を検討してください： 1. Snapshot リザーブがフルになったときにボリューム内のデータスペースを使用するように Snapshot を設定します。2. 古い不要な Snapshot をいくつか削除して、領域を解放してください。... 警告のしきい値を超える場合は、すぐに次の操作を実行するように計画してください： 1. この増加に対応するために、ボリューム内の Snapshot リザーブスペースを増やしてください。2. Snapshot リザーブがフルになったときにボリューム内のデータスペースを使用するように Snapshot を設定します。</p> |
| ストレージ容量の制限             | 重大 | <p>ストレージプール（アグリゲート）がいっぱいになると I/O 処理が低速化し、最後にストレージ停止インシデントが発生します。警告アラートは、最小限の空きスペースをリストアするために計画的な対処が必要であることを示しています。重大アラートは、サービスの停止が差し迫っていることを示しており、サービスの継続性を確保するためにスペースを解放するために緊急措置を講じる必要があることを示しています。</p>  | <p>重大のしきい値を超えた場合は、すぐに次の処理を実行してサービスの中断を最小限に抑えてください： 1. 重要なボリュームの Snapshot を削除します。2. 不要なワーカーロードであり、ストレージコピーからリストア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ていた場合は、すぐに次のアクションを計画します。1. 1つ以上のボリュームを別のストレージに移動します。2. ストレージ容量を追加します。3. Storage Efficiency の設定を変更するか、アクセス頻度の低いデータをクラウドストレージに階層化します。</p>                                    |

|                 |    |  |   |
|-----------------|----|--|---|
| ストレージパフォーマンスの制限 | 重大 | <p>ストレージシステムのパフォーマンスが上限に達すると、処理速度が低下し、レイテンシが増大し、ワークロードやアブリケーションで障害が発生する可能性があります。ONTAPは、ワークロードのストレージプールの使用率を評価し、パフォーマンスの消費率を推定します。...警告アラートは、ストレージプールの負荷を軽減するために、ワークロードのピークに対応できるだけの十分なストレージプールのパフォーマンスが確保されるように、計画されたアクションを実行する必要があることを示しますパフォーマンスの低下が切迫しており、サービスの継続性を確保するためにストレージプールの負荷を軽減するために緊急措置を講じる必要があります。</p> | <p>重大のしきい値を超えた場合は、サービスの停止を最小限に抑えるために次の緊急アクションを検討してください：</p> <ol style="list-style-type: none"> <li>1. Snapshot 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</li> <li>2. アイドル状態の重要ではないワークロード。警告しきい値を超えた場合は、すぐに次の操作を実行してください。</li> <li>1. 1つ以上のワークロードを別のストレージに移動します。</li> <li>2.ストレージノード (AFF) またはディスクシェルフ (FAS) を追加し、ワークロードを再配分する</li> <li>3. ワークロードの特性 (ブロックサイズ、アプリケーションのキャッシング) を変更する。</li> </ol> |
|-----------------|----|--|---|

|                   |    |   |   |
|-------------------|----|---|---|
| ユーザクォータ容量のハードリミット | 重大 | <p>ONTAP は、ボリューム内のボリューム、ファイル、またはディレクトリにアクセスする権限を持つ UNIX または Windows システムのユーザを認識します。その結果、ユーザやユーザグループが使用する Linux または Windows システムのストレージ容量を ONTAP で設定できるようになります。ユーザまたはグループのポリシークォータによって、ユーザが自身のデータに使用できるスペース量が制限されます。このクォータのハードリミットにより、ボリューム内で使用されている容量が適切である場合に、合計容量クォータに達する前にユーザに通知できます。ユーザクォータまたはグループクォータに保存されているデータ量を監視することで、ユーザに中断のないデータサービスを確実に提供できます。</p> | <p>重大のしきい値を超えた場合は、サービスの停止を最小限に抑えるために次の緊急アクションを検討してください：1.増加に対応するために、ユーザクォータまたはグループクォータのスペースを増やしてください。2.不要なデータを削除してスペースを解放するようにユーザまたはグループに指示します。</p> |
|-------------------|----|---|---|

|                   |    |  |  |
|-------------------|----|--|--|
| ユーザクォータ容量のソフトリミット | 警告 | <p>ONTAP は、ボリューム内のボリューム、ファイル、またはディレクトリにアクセスできる権限を持つ UNIX または Windows システムのユーザを認識します。その結果、ユーザやユーザグループが使用する Linux または Windows システムのストレージ容量を ONTAP で設定できるようになります。ユーザまたはグループのポリシークォータによって、ユーザが自身のデータに使用できるスペース量が制限されます。このクォータのソフトリミットにより、ボリューム内で使用されている容量が合計容量クォータに達したときにユーザにプロアクティブな通知が可能になります。ユーザクォータまたはグループクォータに保存されているデータ量を監視することで、ユーザに中断のないデータサービスを確実に提供できます。</p> | <p>警告のしきい値を超える場合は、すぐに次の操作を実行するように計画してください：1.増加に対応するために、ユーザクォータまたはグループクォータのスペースを増やしてください。2.不要なデータを削除してスペースを解放します。</p> |
|-------------------|----|--|--|

|               |    |  |   |
|---------------|----|--|---|
| ボリュームの容量がフルです | 重大 | <p>アプリケーションとお客様のデータを格納するには、ボリュームのストレージ容量が必要です。ONTAP ボリュームに格納されるデータが多いほど、以降のデータで使用できるストレージ容量は少なくなります。ボリューム内のデータストレージ容量が合計ストレージ容量に達すると、ストレージ容量の不足によりデータを格納できなくなる可能性があります。ボリュームの使用済みストレージ容量を監視して、データサービスの継続性を確保します。</p> | <p>重大のしきい値を超えた場合は、サービスの停止を最小限に抑えるために次の緊急アクションを検討してください： 1. 増加に対応するためにボリュームのスペースを増やしてください。 2. 不要なデータを削除してスペースを解放します。 3. Snapshot コピーが Snapshot リザーブよりも多くのスペースを占有している場合は、古い Snapshot を削除するか、ボリューム Snapshot の自動削除を有効にしてください。 ... 警告しきい値を超えている場合は、次のアクションをすぐに実行するように計画してください。 1. 増加に対応するために、ボリュームのスペースを増やしてください。 2. Snapshot コピーが Snapshot リザーブよりも多くのスペースを占有している場合は、古い Snapshot を削除するか、ボリュームの Snapshot の自動削除を有効にしています ...</p> |
|---------------|----|--|---|

|                 |    |   |   |
|-----------------|----|---|---|
| ボリュームの inode 制限 | 重大 | <p>ファイルを格納するボリュームでは、インデックスノード（inode）を使用してファイルメタデータが格納されます。ボリュームの inode 割り当てが使用されなくなった場合は、これ以上ファイルを追加できません。...警告アラートは、使用可能な inode の数を増やすために計画的なアクションを実行する必要があることを示しています。重要なアラートは、ファイル制限の枯渇が差し迫っていることを示しており、サービスの継続性を確保するために緊急対策を講じる必要があることを示しています。</p> | <p>重大のしきい値を超えた場合は、サービスの停止を最小限に抑えるために次の緊急アクションを検討してください：1.ボリュームの inode の値を増やします。inode の値がすでに最大値に達している場合は、ファイルシステムのサイズが最大サイズを超えていたため、ボリュームを複数のボリュームにスプリットします。2.FlexGroupを使用すると、大規模なファイルシステムに対応できます。警告のしきい値を超える場合は、すぐに次の操作を実行するように計画してください：1.ボリュームの inode の値を増やします。inode の値がすでに最大値に達している場合は、ファイルシステムのサイズが最大サイズを超えていたため、ボリュームを 2 つ以上のボリュームにスプリットします。2.FlexGroupを使用して大規模なファイルシステムに対応</p> |
|-----------------|----|---|---|

|                     |     |  |  |
|---------------------|-----|--|--|
| ボリュームレイテンシが高くなっています | 重大  | <p>ボリュームは、I/O トランザクションを処理するオブジェクトで、多くの場合、DevOps アプリケーション、ホームディレクトリ、データベースなどのパフォーマンス重視のアプリケーションによって駆動されます。ボリュームのレイテンシが高いと、アプリケーション自体に影響を及ぼし、タスクを実行できなくなる可能性があります。ボリュームのレイテンシを監視することは、アプリケーションの整合性を維持するうえで非常に重要です。メディアタイプに基づく想定レイテンシは、最大 1 ~ 2 ミリ秒、SAS は最大 8 ~ 10 ミリ秒、SATA HDD は 17 ~ 20 ミリ秒です</p> | <p>重大しきい値に違反した場合は、サービスの中断を最小限に抑えるためにすぐに実行することを検討してください。ボリュームにQoSポリシーが割り当てられている場合は、ボリュームのワークロードが調整されている場合に備えて、制限しきい値を評価します。警告しきい値を超えた場合は、すぐに次の操作を実行することを検討してください。</p> <ol style="list-style-type: none"> <li>1. アグリゲートの利用率も高い場合は、ボリュームを別のアグリゲートに移動します。</li> <li>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、制限のしきい値が原因でボリュームのワークロードが調整されていないかどうかを評価します。</li> <li>3. ノードの利用率も高い場合は、ボリュームを別のノードに移動するか、ノードの合計ワークロードを減らしてください。</li> </ol> |
| モニタ名                | 重大度 | 概要を監視します   | 対処方法   |

|            |         |   |   |
|------------|---------|---|---|
| ノードの高レイテンシ | 警告 / 重大 | <p>ノードのレイテンシが、ノード上のアプリケーションのパフォーマンスに影響する可能性があるレベルに達しました。ノードのレイテンシが低いため、アプリケーションのパフォーマンスが安定します。メディアタイプに基づく想定レイテンシは次のとおりです。SSD は最大 1 ~ 2 ミリ秒、SAS は最大 8 ~ 10 ミリ秒、SATA HDD は 17 ~ 20 ミリ秒。</p> | <p>重大しきい値を超える場合は、サービスの中断を最小限に抑えるためにただちに対処する必要があります： 1. スケジュールされたタスク、Snapshot、または SnapMirror レプリケーション 2 を一時停止 QoS 制限により、優先度の低いワークロードの需要を低減します。 3. 重要でないワークロードを非アクティビ化すると、警告しきい値を超えた場合の即時対処が考慮されます： 1. 1 つ以上のワークロードを別のストレージに移動します。 2. QoS 制限により、優先度の低いワークロードの需要を低減します。 3. ストレージノード（AFF）またはディスクシェルフ（FAS）を追加し、ワークロードを再配分します。 4. ワークロード特性（ブロックサイズ、アプリケーションキャッシングなど）の変更</p> |
|------------|---------|---|---|

|               |         |   |   |
|---------------|---------|---|---|
| ノードのパフォーマンス制限 | 警告 / 重大 | <p>ノードのパフォーマンス使用率が、IOS およびノードでサポートされているアプリケーションのパフォーマンスに影響する可能性があるレベルに達しました。ノードのパフォーマンス利用率が低いため、アプリケーションのパフォーマンスが安定します。</p> | <p>重大のしきい値を超えた場合にサービスの中断を最小限に抑えるために、ただちに対処する必要があります： 1. スケジュールされたタスク、Snapshot、または SnapMirror レプリケーション 2 を一時停止 QoS 制限により、優先度の低いワークロードの需要を低減します。 3. 重要でないワークロードを非アクティブ化すると、警告しきい値を超えた場合に次の処理が実行されることが考慮されます。 1. 1つ以上のワークロードを別のストレージに移動します。 2. QoS 制限により、優先度の低いワークロードの需要を低減します。 3. ストレージノード（AFF）またはディスクシェルフ（FAS）を追加し、ワークロードを再配分します。 4. ワークロード特性（ブロックサイズ、アプリケーションキャッシングなど）の変更</p> |
|---------------|---------|---|---|

|                            |         |  |   |
|----------------------------|---------|--|---|
| Storage VM のレイテンシが高くなっています | 警告 / 重大 | <p>Storage VM ( SVM ) のレイテンシが Storage VM のアプリケーションのパフォーマンスに影響する可能性があるレベルに達しました。Storage VM のレイテンシが低いため、アプリケーションのパフォーマンスが安定します。メディアタイプに基づく想定レイテンシは次のとおりです。SSD は最大 1 ~ 2 ミリ秒、SAS は最大 8 ~ 10 ミリ秒、SATA HDD は 17 ~ 20 ミリ秒。</p> | <p>重大しきい値を超えた場合は、QoS ポリシーが割り当てられた Storage VM のボリュームについてすぐにしきい値を評価して、ボリュームワークロードの負荷が調整されているかどうかを確認し、警告しきい値を超えた場合の即時対処方法として次の点を考慮します：1. アグリゲートの利用率も高い場合は、Storage VM の一部のボリュームを別のアグリゲートに移動します。2. QoS ポリシーが割り当てられている Storage VM のボリュームについて、しきい値制限が原因でボリュームワークロードが調整されている場合は評価します。3. ノードの利用率が高い場合は、Storage VM の一部のボリュームを別のノードに移動するか、ノードの合計ワークロードを減らします</p> |
| ユーザクォータのファイル数のハードリミット      | 重大      | <p>ボリューム内に作成されたファイル数が重大な制限に達したため、追加ファイルを作成できません。保存されたファイル数を監視することで、ユーザに中断のないデータサービスを確実に提供できます。</p>   | <p>重大のしきい値を超えた場合にサービスの中断を最小限に抑えるには、即時アクションが必要です。次のアクションを実行することを検討してください。1. 特定のユーザのファイル数クォータを増やします。2. 不要なファイルを削除して、特定のユーザのファイルクォータに対する圧力を軽減します</p>   |
| ユーザクォータのファイル数がソフトリミット      | 警告      | <p>ボリューム内に作成されたファイル数がクォータのしきい値に達し、重大な制限に近づいています。クォータが重大の上限に達した場合、追加のファイルを作成できません。ユーザが保存するファイル数を監視することで、ユーザに中断のないデータサービスが確実に提供されます。</p>   | <p>警告しきい値を超えた場合は、ただちに対処することを検討してください。1. 特定のユーザクォータ 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、特定のユーザのファイルクォータに対する圧力を軽減します</p>  |

|                           |         |   |   |
|---------------------------|---------|---|---|
| ボリュームキャッシュミス率             | 警告 / 重大 | <p>ボリュームキャッシュミス率は、クライアントアプリケーションからの読み取り要求に対してキャッシュからではなくディスクからデータが返される割合です。これは、ボリュームが設定されたしきい値に達したことを意味します。</p>   | <p>重大しきい値を超える場合は、サービスの中断を最小限に抑えるためにただちに対処する必要があります： 1。ボリュームのノードから一部のワークロードを移動して、IO負荷を軽減してください 2。ボリュームのノードに Flash Cache 3 がない場合は、Flash Cache 3 を購入して追加し、WAFL キャッシュを拡張します。QoS 制限を使用して同じノードに対する優先度の低いワークロードの要求を下げ、警告しきい値を超えた場合の即時対処を検討します。 1. ボリュームのノードから一部のワークロードを移動して、IO 负荷を軽減してください 2. ボリュームのノードに Flash Cache 3 がない場合は、Flash Cache 3 を購入して追加し、WAFL キャッシュを拡張します。QoS 制限により、同じノードでの優先度の低いワークロードの要求を軽減します。 4. ワークロード特性（ブロックサイズ、アプリケーションキャッシングなど）の変更</p> |
| ボリュームの qtree クオータオーバーコミット | 警告 / 重大 | <p>ボリュームの qtree クオータオーバーコミットは、ボリュームが qtree クオータによってオーバーコミットされているとみなす割合を示します。ボリュームの qtree クオータの設定しきい値に達しました。ボリューム qtree クオータオーバーコミットを監視することで、ユーザに中断のないデータサービスが確実に提供されます。</p> | <p>重大しきい値を超える場合は、サービスの中断を最小限に抑えるためにただちに対処する必要があります： 1. ボリューム 2 のスペースを増やします。警告しきい値を超えたときに不要なデータを削除してから、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。</p>  |

[トップに戻る](#)

## ログモニタ

| モニタ名               | 重大度 | 製品説明   | 対処方法   |
|--------------------|-----|--|--|
| AWS クレデンシャルが初期化されて | 情報  | <p>このイベントは、モジュールが初期化される前に、クラウドクレデンシャルスレッドから Amazon Web Services ( AWS ) の Identity and Access Management ( IAM ) ロールベースクレデンシャルにアクセスしようとした場合に発生します。</p> | " クラウドクレデンシャルのスレッドとシステムの初期化が完了するまで待ちます。  |
| クラウド階層に到達不能です      | 重大  | <p>ストレージノードからクラウド階層のオブジェクトストア API に接続することはできません。一部のデータにアクセスできません。</p>  | <p>オンプレミス製品を使用している場合は、次の対処策を実施します。 ... 「 network interface show 」コマンドを使用して、クラスタ間 LIF がオンラインで機能していることを確認します。 ... デステイネーションノードのクラスタ間 LIF で「 ping 」コマンドを使用して、オブジェクトストアサーバへのネットワーク接続を確認します。 ... オブジェクトストアの設定が変更されていないことを確認します。ログインおよび接続の情報はです それでも有効です。問題が解決しない場合は、ネットアップのテクニカルサポートにお問い合わせください。 Cloud Volumes ONTAP を使用する場合は、次の対処方法を実行します。 ... オブジェクトストアの設定が変更されていないことを確認します。 ... ログイン情報と接続情報がまだ有効であることを確認してください。問題が解決しない場合は、NetAppテクニカルサポートにお問い合わせください。</p> |

|                             |    |   |   |
|-----------------------------|----|---|---|
| ディスクがサービスを停止しています           | 情報 | 「このイベントは、ディスクが障害としてマークされているか、完全消去中であるか、Maintenance Center に入力されたためにサービスから削除された場合に発生します。」  | ありません。  |
| FlexGroup 構成要素がフルです         | 重大 | 「FlexGroup ボリューム内のコンステイチュエントがいっぱいになっているため、原因がサービスを停止する可能性があります。この場合も、FlexGroup ボリュームでファイルを作成または拡張できます。ただし、コンステイチュエントに格納されているファイルを変更することはできません。その結果、FlexGroup ボリュームに対して書き込み処理を実行しようとしたときに、ランダムなスペース不足エラーが発生することがあります。」 | 「volume modify -files +X」コマンドを使用して、FlexGroup ボリュームに容量を追加することを推奨します。または、FlexGroup ボリュームからファイルを削除することもできます。しかし、どのファイルがコンステイチュエントに置かれているかを特定するのは難しい」 |
| FlexGroup コンステイチュエントがほぼフルです | 警告 | 「FlexGroup ボリューム内のコンステイチュエントのスペースがほとんどなくなると、原因によってサービスが停止する可能性があります。ファイルを作成して展開できます。ただし、コンステイチュエントのスペースが不足すると、コンステイチュエントにファイルを追加したり変更したりできなくなる可能性があります。」  | 「volume modify -files +X」コマンドを使用して、FlexGroup ボリュームに容量を追加することを推奨します。または、FlexGroup ボリュームからファイルを削除することもできます。しかし、どのファイルがコンステイチュエントに置かれているかを特定するのは難しい」 |

|   |    |   |   |
|---|----|---|---|
| FlexGroup コンステイチュエントの inode がほぼなくなっています | 警告 | 「FlexGroup ボリューム内のコンステイチュエントは inode がほとんどなくなっています。原因がサービスの停止を招く可能性があります。コンステイチュエントに平均よりも少ない作成要求が送信されます。FlexGroup ボリュームの全体的なパフォーマンスに影響することがあります。これは、inode が多いコンステイチュエントに要求がルーティングされるためです。」 | 「volume modify -files +X」コマンドを使用して、FlexGroup ボリュームに容量を追加することを推奨します。または、FlexGroup ボリュームからファイルを削除することもできます。しかし、どのファイルがコンステイチュエントに置かれているかを特定するのは難しい」 |
| FlexGroup コンステイチュエントの inode が不明です       | 重大 | 「FlexGroup ボリュームのコンステイチュエントの inode が不足しており、原因によってサービスが停止する可能性があります。この構成要素には新しいファイルを作成できません。これにより、FlexGroup ボリューム間でコンテンツが全体的に不均衡な状態に分散される可能性があります。」  | 「volume modify -files +X」コマンドを使用して、FlexGroup ボリュームに容量を追加することを推奨します。または、FlexGroup ボリュームからファイルを削除することもできます。しかし、どのファイルがコンステイチュエントに置かれているかを特定するのは難しい」 |
| LUNはオフライン                               | 情報 | このイベントは、LUN が手動でオフラインになった場合に発生します。  | LUN をオンラインに戻します。  |
| メインユニットファンに障害が発生しました                    | 警告 | 1つ以上のメインユニットファンで障害が発生しました。システムは動作し続けます。しかし、状態が長く続くと、過熱によって自動シャットダウンがトリガーされることがあります。   | "障害が発生したファンを取り付け直します。エラーが解消されない場合は、交換します。   |
| 警告状態のメインユニットファン                         | 情報 | このイベントは、1つまたは複数のメインユニットファンが警告状態のときに発生します。   | 過熱を防ぐため、示されたファンを交換してください。   |

|               |    |  |   |
|---------------|----|--|---|
| NVRAM バッテリ低下  | 警告 | <p>NVRAM バッテリ容量が非常に少なくなっています。バッテリの電力が不足すると、データが失われる可能性があります。</p> <p>...NetApp テクニカルサポートと設定済みの送信先（該当する場合）に、AutoSupport または「call home」というメッセージが生成されて送信されます。AutoSupport メッセージが正常に配信されると、問題の特定と解決方法が大幅に改善されます。</p> | <p>「system node environment sensors show」コマンドを使用して、バッテリの現在のステータス、容量、および充電状態を表示します。バッテリを最近交換した場合や、システムが長時間にわたって動作していない場合は、次の対処方法を実行します。バッテリを監視して、適切に充電されていることを確認してください。...バッテリの稼働時間が引き続きクリティカルなレベルを下回ると、ストレージシステムが自動的にシャットダウンする場合は、ネットアップテクニカルサポートにお問い合わせください。</p>   |
| サービスプロセッサが未設定 | 警告 | <p>「このイベントは毎週発生し、サービスプロセッサ（SP）の設定を通知するために使用されます。SP は、システムに組み込まれている物理デバイスであり、リモートアクセス機能とリモート管理機能を提供します。すべての機能を使用できるように SP を設定する必要があります。</p>   | <p>次の対処方法を実行します。...「system service-processor network modify」コマンドを使用して SP を設定します。オプションで、「system service-processor network show」コマンドを使用して、SP の MAC アドレスを取得します。...「system service-processor network show」コマンドを使用して、SP ネットワーク設定を確認します。「system service-processor AutoSupport invoke」コマンドを使用して、SP から AutoSupport E メールを送信できることを確認します。注 AutoSupport：このコマンドを実行する前に、ONTAP E メールホストと受信者を問題で設定する必要があります。</p> |

|                               |    |   |  |
|-------------------------------|----|---|--|
| 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ても、ONTAP はサービスプロセッサ (SP) からハートビートを受信しなくなります。ONTAP は、SP なしでハードウェアの状態を監視できません。システムはシャットダウンして、ハードウェアの損傷やデータの損失を防ぎます。SP がオフラインになった場合にすぐに通知されるようにパニック・アラートを設定する | 次の操作を実行して、システムの電源を再投入します。…コントローラをシャーシから引き出します。…コントローラをもう一度押し込みます。…コントローラをオンに戻します。問題が解決しない場合は、コントローラモジュールを交換します。  |
| シェルフのファンに障害があります              | 重大 | " シェルフの冷却ファンまたはファンモジュールに障害が発生しました。シェルフ内のディスクに十分な通気による冷却が確保されないと、ディスク障害が発生する可能性があります。"   | 次の対処方法を実行します。ファンモジュールが完全に装着され、固定されていることを確認します。メモ：一部のディスクシェルフの電源装置モジュールにファンが内蔵されています。問題が解決しない場合は、ファンモジュールを交換してください。それでも問題が解決しない場合は、ネットアップのテクニカルサポートにお問い合わせください。 |
| メインユニットファンの障害により、システムは動作できません | 重大 | 「1つまたは複数のメインユニットファンで障害が発生し、システムの動作が中断しました。これにより、データが失われる可能性があります。」  | 障害が発生したファンを交換します。  |
| 未割り当てディスク                     | 情報 | システムに未割り当てのディスクがあります - 容量が無駄になっており、構成の設定ミスや部分的な変更がシステムに適用されている可能性があります。   | 次の対処方法を実行します。「disk show -n」コマンドを使用して、どのディスクが割り当てられていないかを確認します。「disk assign」コマンドを使用して、ディスクをシステムに割り当てます。   |

|                               |    |  |  |
|-------------------------------|----|--|--|
| アンチウイルスサーバービジー                | 警告 | ウィルス対策サーバがビジーのため、新しいスキャン要求を受け入れることができません。  | このメッセージが頻繁に表示される場合は、SVMで生成されるウィルススキャンの負荷を処理できるだけの十分なウィルス対策サーバがあることを確認してください。   |
| IAM ロールの AWS クレデンシャルの期限が切れました | 重大 | Cloud Volume ONTAP にアクセスできなくなりました。ID およびアクセス管理 ( IAM ) ロールベースのクレデンシャルの期限が切れている。クレデンシャルは、IAM ロールを使用して Amazon Web Services ( AWS ) メタデータサーバから取得され、Amazon Simple Storage Service ( Amazon S3 ) への API 要求に署名するために使用されます。                             | 次の手順を実行します。... AWS EC2 管理コンソールにログインします。... インスタンスページに移動します。... Cloud Volumes ONTAP 導入のインスタンスを探してその健常性を確認します。... インスタンスに関連付けられている AWS IAM ロールが有効であり、インスタンスに適切な権限が付与されていることを確認します。 |
| IAM ロールの AWS クレデンシャルが見つかりません  | 重大 | クラウドクレデンシャルスレッドで、Amazon Web Services ( AWS ) の Identity and Access Management ( IAM ) ロールベースのクレデンシャルを AWS メタデータサーバから取得することはできません。クレデンシャルは、Amazon Simple Storage Service ( Amazon S3 ) への API 要求への署名に使用されます。Cloud Volume ONTAP にアクセスできなくなりました。... | 次の手順を実行します。... AWS EC2 管理コンソールにログインします。... インスタンスページに移動します。... Cloud Volumes ONTAP 導入のインスタンスを探してその健常性を確認します。... インスタンスに関連付けられている AWS IAM ロールが有効であり、インスタンスに適切な権限が付与されていることを確認します。 |
| IAM ロールの AWS クレデンシャルが無効です     | 重大 | ID およびアクセス管理 ( IAM ) ロールベースのクレデンシャルが無効です。クレデンシャルは、IAM ロールを使用して Amazon Web Services ( AWS ) メタデータサーバから取得され、Amazon Simple Storage Service ( Amazon S3 ) への API 要求に署名するために使用されます。Cloud Volume ONTAP にアクセスできなくなりました。                                 | 次の手順を実行します。... AWS EC2 管理コンソールにログインします。... インスタンスページに移動します。... Cloud Volumes ONTAP 導入のインスタンスを探してその健常性を確認します。... インスタンスに関連付けられている AWS IAM ロールが有効であり、インスタンスに適切な権限が付与されていることを確認します。 |

|                         |    |  |  |
|-------------------------|----|--|--|
| AWS IAM ロールが見つかりません     | 重大 | Identity and Access Management ( IAM ) ロールスレッドで、AWS メタデータサーバに Amazon Web Services ( AWS ) IAM ロールが見つかりません。 IAM ロールは、 Amazon Simple Storage Service ( Amazon S3 ) への API 要求の署名に使用するロールベースのクレデンシャルを取得する必要があります。 Cloud Volume ONTAP にアクセスできなくなりました。 ...       | 次の手順を実行します。 ... AWS EC2 管理コンソールにログインします。 ... インスタンスページに移動します。 ... Cloud Volumes ONTAP 導入のインスタンスを探してその健常性を確認します。 ... インスタンスに関連付けられている AWS IAM ロールが有効であることを確認します。                      |
| AWS IAM ロールが無効です        | 重大 | AWS メタデータサーバの Amazon Web Services ( AWS ) Identity and Access Management ( IAM ) ロールが無効です。 Cloud Volume ONTAP にアクセスできなくなりました。 ...  | 次の手順を実行します。 ... AWS EC2 管理コンソールにログインします。 ... インスタンスページに移動します。 ... Cloud Volumes ONTAP 導入のインスタンスを探してその健常性を確認します。 ... インスタンスに関連付けられている AWS IAM ロールが有効であり、インスタンスに適切な権限が付与されていることを確認します。 |
| AWS メタデータサーバに接続できませんでした | 重大 | Identity and Access Management ( IAM ) 役割スレッドで、 Amazon Web Services ( AWS ) メタデータサーバとの通信リンクを確立できません。 Amazon Simple Storage Service ( Amazon S3 ) への API 要求の署名に使用する AWS IAM ロールベースの必要なクレデンシャルを取得するために通信を確立する必要があります。 Cloud Volume ONTAP にアクセスできなくなりました。 ... | 次の手順を実行します。 ... AWS EC2 管理コンソールにログインします。 ... インスタンスページに移動します。 ... Cloud Volumes ONTAP 導入のインスタンスを探してその健全性を確認します。  |

|                              |    |  |   |
|------------------------------|----|--|---|
| FabricPool のスペース使用制限にほぼ達しました | 警告 | <p>容量ライセンスのあるプロバイダが提供するオブジェクトストアでのクラスタ全体の FabricPool スペースの使用量が、ライセンスで許可された上限にほぼ達しています。</p> | <p>次の対処方法を実行します。... 「storage aggregate object-store show-space」コマンドを使用して、各 FabricPool ストレージ階層で使用されているライセンス容量の割合を確認します。</p> <p>... 「volume snapshot delete」コマンドを使用して、階層化ポリシー「snapshot」または「backup」が設定されたボリュームから Snapshot コピーを削除します。...新しいライセンスをインストールします クラスタ上でライセンス容量を拡張します。</p> |
| FabricPool のスペース使用制限に達しました   | 重大 | <p>容量ライセンスプロバイダが提供するオブジェクトストアでのクラスタ全体の FabricPool スペースの使用量がライセンスの上限に達しました。</p>             | <p>次の対処方法を実行します。... 「storage aggregate object-store show-space」コマンドを使用して、各 FabricPool ストレージ階層で使用されているライセンス容量の割合を確認します。</p> <p>... 「volume snapshot delete」コマンドを使用して、階層化ポリシー「snapshot」または「backup」が設定されたボリュームから Snapshot コピーを削除します。...新しいライセンスをインストールします クラスタ上でライセンス容量を拡張します。</p> |

|                     |    |   |   |
|---------------------|----|---|---|
| アグリゲートのギブバックに失敗しました | 重大 | <p>ストレージフェイルオーバー (SFO) ギブバックの一環としてアグリゲートを移行したときに、デスティネーションノードがオブジェクトストアに到達できない場合に発生します。</p> | <p>次の対処方法を実行します。... 「network interface show」コマンドを使用して、インターフェース LIF がオンラインで機能していることを確認します。... デスティネーションノードのクラスタ間 LIF で「ping」コマンドを使用して、オブジェクトストアサーバへのネットワーク接続を確認します。... 「aggregate object-store config show」コマンドを使用して、オブジェクトストアの設定が変更されておらず、ログインおよび接続の情報が正確であることを確認してください。または、このエラーを無効にするには、giveback コマンドの「require-partner-waiting」パラメータに false を指定します。詳細やサポートについては、ネットアップテクニカルサポートにお問い合わせください。</p> |
|---------------------|----|---|---|

|                     |    |   |
|---------------------|----|---|
| HA インターコネクトが停止しています | 警告 | <p>ハイアベイラビリティ ( HA ) インターコネクトが停止しています。フェイルオーバーを利用できない場合、サービスが停止するリスクがあります。</p> <p>対処方法は、プラットフォームでサポートされている HA インターコネクトリンクの数と種類、およびインターフェースが停止している理由によって異なります。</p> <ul style="list-style-type: none"> <li>リンクがダウンしている場合:       <ul style="list-style-type: none"> <li>HA ペアの両方のコントローラが動作していることを確認します。外部接続リンクの場合は、相互接続ケーブルが正しく接続されていること、および小型フォームファクタプラグアダプタ ( 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。</li> <li>内部接続されているリンクの場合は、リンクを無効にし、リンクを有効にします。</li> <li>一方は、「IC LINK OFF」コマンドと「IC LINK ON」コマンドを使用して行います。</li> <li>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。</li> <li>ピアが接続されていない場合は、「ic link off」コマンドと「ic link on」コマンドを使用して、一方のリンクを無効にし、再度有効にします。</li> </ul> </li> <li>問題が解決しない場合は、ネットアップのテクニカルサポートにお問い合わせください。</li> </ul> |
|---------------------|----|---|

|                        |    |  |
|------------------------|----|--|
| ユーザあたりの最大セッション数を超えるました | 警告 | <p>TCP 接続でのユーザあたりの最大許容セッション数を超えるました。セッションを確立する要求は、一部のセッションが解放されるまで拒否されます。...</p> <p>次の対処策を実行します。...クライアントで実行されているすべてのアプリケーションを検査し、正常に動作していないアプリケーションを終了します。...クライアントを再起動します。...問題が新規または既存のアプリケーションによって発生しているかどうかを確認します。アプリケーションが新規の場合は、「cifs option modify -max-opense-opense-file-per-tree」コマンドを使用して、クライアントのしきい値を大きく設定します。クライアントが想定どおりに動作していても、しきい値の上昇が必要となる場合があります。クライアントのしきい値を高く設定するには、advanced 権限が必要です。...問題が既存のアプリケーションに起因している場合は、クライアントに問題が存在する可能性があります。詳細またはサポートについては、ネットアップテクニカルサポートにお問い合わせください。</p> |
|------------------------|----|--|

|                        |    |  |   |
|------------------------|----|--|---|
| ファイルあたりの最大オーブン回数を超えました | 警告 | <p>TCP 接続でファイルを開くことができる最大回数を超えました。このファイルを開く要求は、ファイルの開いているインスタンスをいくつか閉じるまでは拒否されます。これは通常、異常なアプリケーション動作を示します。</p> | <p>次の修正アクションを実行します。この TCP 接続を使用してクライアントで実行されているアプリケーションを検査します。クライアントが正しく動作していない可能性があります。クライアントを再起動します。クライアントが新規または既存のアプリケーションによって問題が発生しているかどうかを確認します。アプリケーションが新規である場合は、「<code>cifs option modify -max -opense-opense-file-per-tree</code>」コマンドを使用して、クライアントのしきい値を大きく設定します。クライアントが想定どおりに動作していても、しきい値の上昇が必要となる場合があります。クライアントのしきい値を高く設定するには、<code>advanced</code> 権限が必要です。...問題が既存のアプリケーションに起因している場合は、クライアントに問題が存在する可能性があります。詳細またはサポートについては、ネットアップテクニカルサポートにお問い合わせください。</p> |
|------------------------|----|--|---|

|                       |    |   |  |
|-----------------------|----|---|--|
| NetBIOS 名が競合しています     | 重大 | <p>NetBIOS ネームサービスが、リモートマシンから名前登録要求に対して否定的な応答を受信しました。これは通常、NetBIOS 名またはエイリアスの競合が原因です。その結果、クライアントがデータにアクセスできなくなったり、クラスタ内の適切なデータを提供しているノードに接続できなくなったりすることがあります。</p> | <p>次のいずれかの修正処置を実行します。...</p> <p>NetBIOS 名またはエイリアスに競合がある場合、次のいずれかを実行します。... 「vserver cifs delete -aliases alias -vserver vserver」コマンドを使用して、重複するNetBIOS エイリアスを削除します。... 「vserver cifs create -aliases alias -vserver vserver」コマンドを使用して、重複する名前を削除し、新しい名前のエイリアスを追加して、NetBIOS エイリアスの名前を変更します。...</p> <p>NetBIOS 名にエイリアスが設定されておらず、競合がある場合は、「vserver cifs delete -vserver vserver」コマンドと「vserver cifs create -cifs -server netbiosname」コマンドを使用してCIFS サーバの名前を変更します。メモ：CIFS サーバを削除すると、データにアクセスできなくなる可能性があります。...</p> <p>リモートマシンのNetBIOS 名を削除するか、NetBIOS 名を変更します。</p> |
| NFSv4 ストアプールを使い果たしました | 重大 | NFSv4 ストアプールを使い果たしました。  | NFS サーバが応答しなくなつてから 10 分以上が経過した場合は、ネットアップテクニカルサポートにお問い合わせください。  |

|                           |    |  |  |
|---------------------------|----|--|--|
| 登録済みのスキャンエンジンがありません       | 重大 | Antivirus Connector は、スキャンエンジンが登録されていないことをONTAPに通知しました。「scan-mandatory」オプションを有効にすると、原因データを使用できなくなることがあります。   | 次の対処方法を実行します。...アンチウイルスサーバーにインストールされているスキャンエンジンソフトウェアがONTAPと互換性があることを確認します。スキャンエンジンソフトウェアが実行中で、ローカルループバックを介してアンチウイルスコネクタに接続するように設定されていることを確認します。                           |
| Vscan 接続なし                | 重大 | ONTAPでは、ウィルススキャン要求への対応に関するVscan接続はありません。「scan-mandatory」オプションを有効にすると、原因データを使用できなくなることがあります。  | スキャナプールが正しく設定され、ウィルス対策サーバがアクティブでONTAPに接続されていることを確認します。   |
| ノードのルートボリュームのスペースが不足しています | 重大 | ルートボリュームのスペースが危険なほど少なくなっていることが検出されました。ノードが完全には動作していません。ノードで NFS アクセスと CIFS アクセスが制限されているため、クラスタ内でデータ LIF がフェイルオーバーされる可能性があります。管理機能は、ノードがルートボリューム上のスペースをクリアするためのローカルリカバリ手順に限定されます。 | 次の対処方法を実行します。...古い Snapshot コピーを削除してルートボリュームのスペースをクリアする、/mrootDirectory から不要になったファイルを削除する、またはルートボリュームの容量を拡張する。...コントローラをリブートする...詳細やサポートについては、ネットアップのテクニカルサポートにお問い合わせください。 |
| 存在しない管理共有です               | 重大 | vscan 問題：クライアントが、存在しないONTAP_ADMIN\$ 共有に接続しようとしました。   | 指定した SVM ID で Vscan が有効になっていないことを確認してください。SVM で Vscan を有効にすると、SVM 用にONTAP_ADMIN\$ 共有が自動的に作成されます。   |
| NVMe ネームスペースのスペースが不足しています | 重大 | スペース不足が原因の書き込みエラーが原因で NVMe ネームスペースがオフラインになりました。  | ボリュームにスペースを追加し、「vserver nvme namespace modify」コマンドを使用して NVMe ネームスペースをオンラインにします。  |

|                    |    |   |  |
|--------------------|----|---|--|
| NVMe の猶予期間 - アクティブ | 警告 | <p>このイベントは、 NVMe over Fabrics ( NVMe-oF ) プロトコルを使用して いてライセンスの猶予期間がアクティブになっている場合に毎日発生します。 NVMe-oF 機能には、 ライセンスの猶予期間が 終了したあとにライセンスが必要です。 ライセンスの猶予期間が終了すると、 NVMe-oF 機能は無効になります。</p> | 営業担当者に連絡して NVMe-oF ライセンスを取得し、 クラスタに追加するか、 NVMe-oF 構成のすべてのインスタンスを クラスタから削除してください。 |
| NVMe の猶予期間 - 終了    | 警告 | <p>NVMe over Fabrics ( NVMe-oF ) ライセンスの 猶予期間が終了し、 NVMe-oF 機能は無効になります。</p>   | 営業担当者に連絡して NVMe-oF ライセンスを取得し、 クラスタに追加してください。                                     |
| NVMe の猶予期間 - 開始    | 警告 | <p>ONTAP 9.5 ソフトウェア へのアップグレード中に NVMe over Fabrics ( NVMe-oF ) 設定が検出されました。 NVMe-oF 機能を使用するには、 ライセンスの猶予期間が終了したあとにライセンスが必要です。</p>  | 営業担当者に連絡して NVMe-oF ライセンスを取得し、 クラスタに追加してください。                                     |
| オブジェクトストアのホスト解決不可  | 重大 | <p>オブジェクトストアサー バのホスト名を IP アドレスに解決できません。 オブジェクトストアクライアントが IP アドレスに解決しないとオブジェクトストアサーバと通信できません。 その結果、 データにアクセスできなくなる可能性があります。</p>  | DNS 設定を調べて、 ホスト名が IP アドレスで正しく設定されていることを確認します。                                    |

|                              |    |  |   |
|------------------------------|----|--|---|
| オブジェクトストアのクラスタ間 LIF が停止しています | 重大 | オブジェクトストアクライアントが、オブジェクトストアサーバと通信するための稼働している LIF を見つけることができません。クラスタ間 LIF が動作可能になるまで、このノードはオブジェクトストアクライアントトラフィックを許可しません。その結果、データにアクセスできなくなる可能性があります。 | 次の対処方法を実行します。... 「network interface show -role intercluster」コマンドを使用して、クラスタ間 LIF のステータスを確認します。... クラスタ間 LIF が正しく設定されていて動作していることを確認します。... クラスタ間 LIF が設定されていない場合は、「network interface create -role intercluster」コマンドを使用して追加します。  |
| オブジェクトストアシグネチャの不一致           | 重大 | オブジェクトストアサーバに送信された要求の署名が、クライアントで計算された署名と一致しません。その結果、データにアクセスできなくなる可能性があります。  | シークレットアクセキーが正しく設定されていることを確認します。正しく設定されている場合は、ネットアップテクニカルサポートにお問い合わせください。  |
| REaddir タイムアウト               | 重大 | REaddir ファイル処理が、WAFL で実行が許可されているタイムアウトを超えました。これは、ディレクトリが非常に大きく、スペースであるためです。対処方法を推奨します。   | 次の対処方法を実行します。... REaddir ファイル操作が期限切れになった最近のディレクトリに関する情報を検索するには、次の 'diag' 特権ノードシェル CLI コマンドを使用します。WAFL readdir notice show... ディレクトリが sparse または not: 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 sparse として示されている場合は、ディレクトリの内容を新しいディレクトリにコピーしてディレクトリファイルの sparsess を削除することをお勧めします。... ディレクトリがスペースとして示されておらず、ディレクトリが大きい場合は、ディレクトリ内のファイルエントリの数を減らすことでディレクトリファイルのサイズを小さくすることをお勧めします。 |

|                   |    |  |  |
|-------------------|----|--|--|
| アグリゲートの再配置に失敗しました | 重大 | このイベントは、アグリゲートの再配置時にデスティネーションノードがオブジェクトストアに到達できない場合に発生します。                       | 次の対処方法を実行します。... 「network interface show」コマンドを使用して、インターフェース LIF がオンラインで機能していることを確認します。... デスティネーションノードのクラスタ間 LIF で「ping」コマンドを使用して、オブジェクトストアサーバへのネットワーク接続を確認します。... 「aggregate object-store config show」コマンドを使用して、オブジェクトストアの設定が変更されておらず、ログインおよび接続の情報が正確であることを確認してください。または、再配置コマンドの「override-destination-checks」パラメータを使用してエラーを無効にすることもできます。詳細やサポートについては、ネットアップのテクニカルサポートにお問い合わせください。 |
| シャドウコピーに失敗しました    | 重大 | ボリュームシャドウコピーサービス (VSS) の実行に失敗しました。VSS は、Microsoft Server のバックアップおよびリストアサービス処理です。 | イベントメッセージに表示される情報を使用して、次の項目を確認します。... Is shadow copy configuration enabled? ... 適切なライセンスがインストールされているか? ... どの共有でシャドウコピー操作が実行されますか? 共有名は正しいですか? 共有名は正しいですか? 共有名は正しいですか? シャドウコピーセットとそのシャドウコピーの状態はどうなっていますか?  |

|                          |    |  |  |
|--------------------------|----|--|--|
| ストレージスイッチの電源装置に障害が発生しました | 警告 | クラスタスイッチに電源装置がありません。冗長性が低下し、停電が発生するリスクが高まります。  | 次の対処方法を実行します。クラスタスイッチに電力を供給する電源装置の電源がオンになっていることを確認します。電源コードが電源装置に接続されていることを確認します。問題が解決しない場合は、ネットアップのテクニカルサポートにお問い合わせください。                                  |
| CIFS 認証が多すぎます            | 警告 | 多数の認証ネゴシエーションが同時に行われています。このクライアントからの新規セッション要求は 256 個あります。  | クライアントが新しい接続要求を 256 個以上作成した理由を調べます。エラーの原因を特定するために、クライアントまたはアプリケーションのベンダーに問い合わせなければならない場合があります。   |
| 管理共有への権限のないユーザアクセス       | 警告 | クライアントが ONTAP_ADMIN\$ 共有に接続しようとしたが、ログインしているユーザが許可されていません。  | 次の対処方法を実行します。...指定したユーザ名と IP アドレスがアクティブな Vscan スキヤナプールの 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ヤナプールの設定を確認します。 |
| ウイルスを検出しました              | 警告 | Vscan サーバからストレージシステムにエラーが報告されました。通常は、ウイルスが検出されたことを示します。ただし、Vscan サーバでその他のエラーが発生すると、このイベントを原因できます。ファイルへのクライアントアクセスは拒否されます。Vscan サーバは、設定に応じて、ファイルをクリーンアップするか、ファイルを隔離するか、または削除する可能性があります。 | 「syslog」イベントで報告された Vscan サーバのログを調べて、感染ファイルのクリーンアップ、隔離、削除が正常に完了したかどうかを確認します。削除できなかった場合は、システム管理者が手動でファイルを削除しなければならないことがあります。                                 |
| ボリュームはオフライン              | 情報 | ボリュームがオフラインになりました。   | ボリュームをオンラインに戻します。  |

|                   |    |  |  |
|-------------------|----|--|--|
| ボリュームは制限状態        | 情報 | フレキシブルボリュームが制限されたことを示すイベントです。            | ボリュームをオンラインに戻します。                                    |
| Storage VMが停止しました | 情報 | このメッセージは、「vserver stop」処理が成功した場合に表示されます。 | Storage VMでデータアクセスを開始するには、「vserver start」コマンドを使用します。 |
| ノードのパニック          | 警告 | このイベントはパニック状態になった場合に生成されます               | ネットアップカスタマーサポートにお問い合わせください。                          |

[トップに戻る](#)

## ランサムウェア対策ログモニタ

| モニタ名                                       | 重大度 | 製品説明  | 対処方法 |
|--|-----|---|------|
| Storage VM ランサムウェア対策監視が無効になっています           | 警告  | Storage VM のランサムウェア対策監視は無効になっています。Storage VM を保護するには、ランサムウェア対策を有効にしてください。 | なし   |
| Storage VM ランサムウェア対策監視有効（ラーニングモード）         | 情報  | Storage VM のランサムウェア対策監視は、学習モードで有効になっています。                                 | なし   |
| Volume Anti-Ransomware Monitoring を有効にしました | 情報  | ボリュームのランサムウェア対策監視が有効になっている。   | なし   |
| ボリュームのアンチランサムウェア監視が無効になっています               | 警告  | ボリュームのランサムウェア対策監視は無効になっています。ランサムウェア対策を有効にしてボリュームを保護                       | なし   |
| ボリュームでのランサムウェア対策監視の有効化（ラーニングモード）           | 情報  | ボリュームのランサムウェア対策監視は、学習モードで有効になっています。                                       | なし   |
| ボリュームのアンチランサムウェア監視が一時停止されました（ラーニングモード）     | 警告  | ボリュームのアンチランサムウェアモニタリングが学習モードで一時停止しています。                                   | なし   |
| ボリュームのアンチランサムウェアモニタリングが一時停止されました           | 警告  | ボリュームのランサムウェア対策監視が一時停止されています。   | なし   |

|  |    |  |  |
|--|----|--|--|
| Volume Anti-Ransomware Monitoring Disabling の略 | 警告 | ボリュームのアンチランサムウェア監視が無効になっています。  | なし   |
| ランサムウェアのアクティビティが検出され                           | 重大 | 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、元のデータをリストアするために使用できる Snapshot コピーが作成されました。システムによって AutoSupport または「コールホーム」メッセージが生成され、ネットアップテクニカルサポートおよび設定された宛先に送信されます。AutoSupport メッセージを使用すると、問題の特定と解決方法が向上します | ランサムウェアの活動を修復する方法については、「final-document-name」を参照してください。 |

[トップに戻る](#)

## NetApp ONTAP モニタの FSX

| モニタ名             | しきい値              | 概要を監視します  | 対処方法   |
|------------------|-------------------|---|--|
| FSX ボリューム容量がフルです | 警告@>85%...重大@>95% | アプリケーションとお客様のデータを格納するには、ボリュームのストレージ容量が必要です。ONTAP ボリュームに格納されるデータが多いほど、以降のデータで使用できるストレージ容量は少なくなります。ボリューム内のデータストレージ容量が合計ストレージ容量に達すると、ストレージ容量の不足によりデータを格納できなくなる可能性があります。ボリュームの使用済みストレージ容量を監視して、データサービスの継続性を確保します。 | 重大のしきい値を超えた場合にサービスの中断を最小限に抑えるには、即時アクションが必要です。1.スペースを解放するため、不要になったデータを削除することを検討してください |

|                     |   |   |  |
|---------------------|---|---|--|
| FSX ボリューム高レイテンシ     | 警告 @> 1000 $\mu$ s ... クリティカル @> 2000 $\mu$ s | <p>ボリュームとは、多くの場合、 DevOps アプリケーション、ホームディレクトリ、データベースなどのパフォーマンス重視のアプリケーションによって I/O トラフィックを処理するオブジェクトです。ボリュームのレイテンシが高いと、アプリケーション自体に影響を及ぼし、タスクを実行できなくなる可能性があります。ボリュームのレイテンシを監視することは、アプリケーションの整合性を維持するうえで非常に重要です。</p>   | <p>重大のしきい値を超えた場合にサービスの中断を最小限に抑えるには、即時アクションが必要です。 1. ボリュームに QoS ポリシーが割り当てられている場合は、ボリュームのワークロードが抑制される原因になった場合に制限しきい値を評価します。 ..... 警告しきい値を超えた場合には、すぐに次の処理を実行するよう計画してください。 1. ボリュームに QoS ポリシーが割り当てられている場合は、ボリュームのワークロードが調整される原因となった場合に備えて、制限のしきい値を評価します。 ... 2. ノードの利用率も高い場合は、ボリュームを別のノードに移動するか、ノードの合計ワークロードを減らしてください。</p>           |
| FSX ボリュームの inode 制限 | 警告@>85%...重大@>95%                             | <p>ファイルを格納するボリュームでは、インデックスノード（inode）を使用してファイルメタデータが格納されます。ボリュームが inode の割り当てを使用しなくなると、そのボリュームにはこれ以上ファイルを追加できません。警告アラートは、使用可能な inode の数を増やすために計画的な処理が必要であることを示しています。重大アラートは、ファイル制限の枯渇が差し迫っていることを示し、サービスの継続性を確保するために inode を解放するための緊急対策を講じる必要があることを示しています</p> | <p>重大のしきい値を超えた場合にサービスの中断を最小限に抑えるには、即時アクションが必要です。 1. ボリュームの inode の値を増やすことを検討してください。 inode の値がすでに最大値に達している場合は、ファイルシステムが最大サイズを超えていたため、ボリュームを 2 つ以上のボリュームに分割することを検討してください。次の処理は、警告しきい値に違反した場合にすぐに実行されます。 1. ボリュームの inode の値を増やすことを検討してください。 inode の値がすでに最大値に達している場合は、ファイルシステムの最大サイズを超えたためにボリュームを 2 つ以上のボリュームにスプリットすることを検討してください</p> |

|                               |                    |  |  |
|-------------------------------|--------------------|--|--|
| FSX ボリュームの qtree クォータオーバーコミット | 警告@>95%...重大@>100% | <p>ボリュームの qtree クォータオーバーコミットは、ボリュームが qtree クォータによってオーバーコミットされているとみなす割合を示します。ボリュームの qtree クォータの設定しきい値に達しました。ボリューム qtree クォータオーバーコミットを監視することで、ユーザに中断のないデータサービスが確実に提供されます。</p>  | <p>重大しきい値を超える場合は、サービスの中断を最小限に抑えるためにただちに対処する必要があります：1。不要なデータを削除してください。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。</p>  |
| FSX Snapshot リザーブス ペースがフルです   | 警告@>90%...重大@>95%  | <p>アプリケーションとお客様のデータを格納するには、ボリュームのストレージ容量が必要です。Snapshot 予約領域と呼ばれる領域の一部は Snapshot の保存に使用され、データをローカルで保護できます。ONTAP ボリュームに格納される新規データや更新データが多いほど、使用される Snapshot 容量は増えますが、今後追加または更新されるデータに使用できる Snapshot ストレージ容量は少なくなります。ボリューム内の Snapshot データ容量が Snapshot リザーブの合計スペースに達すると、新しい Snapshot データを格納できなくなり、ボリューム内のデータの保護レベルが低下する可能性があります。ボリュームの使用済み Snapshot 容量を監視して、データサービスの継続性を確保します。</p> | <p>重大のしきい値を超えた場合にサービスの中断を最小限に抑えるには、即時アクションが必要です。1. Snapshot 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 Snapshot を設定することを検討してください。2. 容量を解放するために不要になった古い Snapshot を削除することを検討してください……警告しきい値を超えた場合には、すぐに次のアクションを実行するよう計画してください。...1. ボリューム内の Snapshot 予約容量を増やして、増加に対応することを検討してください。2. Snapshot リザーブがフルになったときにボリューム内のデータスペースを使用するように Snapshot を設定することを検討してください</p> |

|                   |                    |  |   |
|-------------------|--------------------|--|---|
| 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に対してキャッシュからではなくディスクからデータが返される割合です。これは、ボリュームが設定されたしきい値に達したことを意味します。 | 重大しきい値を超える場合は、サービスの中断を最小限に抑えるためにただちに対処する必要があります：1。ボリュームのノードから一部のワークロードを移動して、IO負荷を軽減してください2。QoS制限により、同じノードでの優先度の低いワークロードの要求を軽減...警告しきい値を超えた場合の即時対処を検討する。1.ボリュームのノードから一部のワークロードを移動して、IO負荷を軽減してください2。QoS制限により、同じノードでの優先度の低いワークロードの要求を軽減します。3.ワークロード特性（ブロックサイズ、アプリケーションキャッシングなど）の変更 |
|-------------------|--------------------|--|---|

[トップに戻る](#)

## K8s モニタ

| モニタ名 | 製品説明 | 対処方法 | 重大度/しきい値 |
|------|------|------|----------|
|------|------|------|----------|

|                 |   |   |                              |
|-----------------|---|---|------------------------------|
| 永続ボリュームレイテンシが高い | 高レイテンシの永続ボリュームは、アプリケーション自体に影響を及ぼし、タスクを実行できない可能性があることを意味します。アプリケーションの一貫したパフォーマンスを維持するには、永続ボリュームのレイテンシを監視することが重要です。メディアタイプに基づく想定レイテンシは、最大 1 ~ 2 ミリ秒、SAS は最大 8 ~ 10 ミリ秒、SATA HDD は 17 ~ 20 ミリ秒です | 即時アクション重大しきい値を超えた場合は、すぐに実行できるアクションを検討してサービスの中断を最小限に抑えます。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ている場合に備えて、制限しきい値を評価します。すぐに実行するアクション警告しきい値に違反した場合は、すぐに次のアクションを計画します。ストレージプールの利用率も高い場合は、ボリュームを別のストレージプールに移動します。2.ボリュームにQoSポリシーが割り当てられている場合は、制限のしきい値が原因でボリュームのワークロードが調整されていないかどうかを評価します。3.コントローラの利用率も高い場合は、ボリュームを別のコントローラに移動するか、コントローラの総ワークロードを減らしてください。 | 警告@>6, 000 μs 重大@>12, 000 μs |
| クラスタメモリ飽和度高     | クラスタの割り当て可能なメモリの飽和度が高くなっています。クラスタのCPU飽和度は、メモリ使用量の合計をすべてのKubernetesノードの割り当て可能なメモリの合計で割った値です。   | ノードを追加します。スケジュールされていないノードを修正します。適切なサイズのポッドでノードのメモリを解放   | 警告 @>80% 重大 @>90%            |
| ポッドの接続に失敗しました   | このアラートは、ポッドとのボリューム接続に失敗した場合に発生します。  |   | 警告                           |

|                   |                             |  |                    |
|-------------------|-----------------------------|--|--------------------|
| 高い再送信レート          | 高いTCP再送信レート                 | ネットワークの輻輳を確認する-ネットワーク帯域幅を大量に消費するワークロードを特定します。PodのCPU利用率が高いかどうかを確認します。ハードウェアネットワークのパフォーマンスを確認します。 | 警告 @>10% 重大 @>25%  |
| ノードファイルシステム容量上限   | ノードファイルシステム容量上限             | -アプリケーションファイル用の十分なスペースを確保するために、ノードディスクのサイズを拡張します。-アプリケーションファイルの使用量を削減します。                        | 警告 @>80% 重大 @>90%  |
| ワークロードネットワークジッタ上限 | 高いTCPジッタ（レイテンシ/応答時間の変動が大きい） | ネットワークの輻輳を確認します。ネットワーク帯域幅を大量に消費するワークロードを特定します。PodのCPU利用率が高いかどうかを確認します。ハードウェアネットワークのパフォーマンスの確認    | 警告@>30 ms重大@>50 ms |

|                                 |  |  |                                |
|---------------------------------|--|--|--------------------------------|
| 永続的ボリュームのスループット                 | 永続ボリュームの MBps のしきい値を使用して、永続ボリュームが事前に定義されたパフォーマンスの期待値を超えたときに管理者にアラートを送信し、他の永続ボリュームに影響を及ぼしている可能性があるこのモニタをアクティブにすると、SSD 上の永続的ボリュームの一般的なスループットプロファイルに適したアラートが生成されます。このモニタはテナントのすべての永続ボリュームに対応します。警告および重大のしきい値は、監視目標に基づいてこのモニタを複製し、ストレージクラスに適したしきい値を設定することで調整できます。複製されたモニタは、テナント上の永続ボリュームのサブセットにさらにターゲットを絞ることができます。 | 即時アクション重大しきい値を超えた場合は、サービスの中止を最小限に抑えるための即時アクションを計画します。ボリュームに対して QoS MBps の制限を適用します。2. ボリュームのワークロードを処理しているアプリケーションに異常がないかどうかを確認します。すぐに実行するアクション警告しきい値に違反した場合は、次のアクションを直ちに実行することを計画してください。1. ボリュームに対して QoS MBps の制限を適用します。2. ボリュームのワークロードを処理しているアプリケーションに異常がないかどうかを確認します。 | 警告@>10,000 MB/秒重大@>15,000 MB/秒 |
| OOMが終了する危険性のあるコンテナ              | コンテナのメモリ制限が低すぎます。コンテナが削除される可能性があります (Out of Memory Kill)。  | コンテナメモリの上限を引き上げます。   | 警告@> 95%                       |
| ワークロード停止                        | ワークロードに正常なポッドがありません。   |  | 重大@< 1                         |
| 永続的ボリューム要求のバインドに失敗しました          | このアラートは、PVC でバインディングが失敗した場合に発生します。   |  | 警告                             |
| リソースクォータのメモリ制限を超えるようとしています      | ネームスペースのメモリ制限がResourceQuotaを超えようとしています   |  | 警告 @>80% 重大 @>90%              |
| ResourceQuotaのメモリ要求が超過しようとしています | ネームスペースのメモリ要求がResourceQuotaを超えようとしています   |  | 警告 @>80% 重大 @>90%              |
| ノード作成に失敗しました                    | 設定エラーのため、ノードをスケジュールできませんでした。   | Kubernetesイベントログで、設定エラーの原因を確認します。  | 重大                             |
| 永続的ボリュームの再生に失敗しました              | ボリュームの自動再生に失敗しました。   |  | 警告@>0 B                        |

|                        |  |   |                                |
|------------------------|--|---|--------------------------------|
| コンテナのCPUスロットリング        | コンテナのCPU制限が低すぎます。コンテナプロセスの速度が低下します。  | コンテナのCPU制限を引き上げます。  | 警告 @>95% 重大 @>98%              |
| サービスロードバランサを削除できませんでした |  |   | 警告                             |
| 永続ボリューム IOPS           | 永続ボリュームの IOPS しきい値を使用すると、永続ボリュームが事前に定義されたパフォーマンスの期待値を超えたときに管理者に通知することができます。このモニタをアクティブにすると、永続ボリュームの一般的な IOPS プロファイルに適したアラートが生成されます。このモニタはテナントのすべての永続ボリュームに対応します。警告および重大のしきい値は、このモニタを複製し、ワークロードに適したしきい値を設定することで、監視の目標に基づいて調整できます。 | 即時アクション重大しきい値を超えた場合は、サービスの中止を最小限に抑えるために即時アクションを計画します。ボリュームのQoS IOPS制限を導入します。2.ボリュームのワークロードを処理しているアプリケーションに異常がないかどうかを確認します。すぐに実行するアクション警告しきい値に違反した場合は、すぐに次のアクションを計画します。ボリュームのQoS IOPS制限を導入します。2.ボリュームのワークロードを処理しているアプリケーションに異常がないかどうかを確認します。 | 警告@>20,000 IO/秒重大@>25,000 IO/秒 |
| サービスロードバランサを更新できませんでした |  |   | 警告                             |
| ポッドのマウントに失敗しました        | このアラートは、ポッドでマウントに失敗したときに発生します。   |   | 警告                             |
| ノードPID圧力               | (Linux) ノードで使用可能なプロセス識別子が削除しきい値を下回っています。   | 多数のプロセスを生成し、使用可能なプロセスIDのノードを枯渇させるポッドを検索して修正します。プロセスを生成するポッドやコンテナからノードを保護するには、PodPidsLimitを設定します。  | 重大@>0                          |

|                                |  |   |                        |
|--------------------------------|--|---|------------------------|
| ポッドイメージのプルエラー                  | Kubernetesがポッドコンテナイメージを取得できませんでした。   | -ポッド構成でポッドのイメージのスペルが正しいことを確認します。-レジストリにイメージタグが存在することを確認してください。-イメージレジストリのクレデンシャルを確認します。-レジストリ接続の問題を確認します。-公共のレジストリプロバイダーによって課されたレート制限に達していないことを確認します。 | 警告                     |
| ジョブの実行時間が長すぎます                 | ジョブの実行時間が長すぎます   |   | 警告 @>1時間重大 @>5時間       |
| ノードメモリ上限                       | ノードのメモリ使用率が高くなっています  | ノードを追加します。スケジュールされていないノードを修正します。適切なサイズのポッドでノードのメモリを解放   | 警告 @>85% 重大 @>90%      |
| ResourceQuotaのCPU制限を超えようとしています | ネームスペースのCPU制限がリソースクォータを超えようとしています  |   | 警告 @>80% 重大 @>90%      |
| ポッドクラッシュループバックオフ               | ポッドがクラッシュし、何度も再起動しようとした。   |   | 重大 @>3                 |
| ノードCPU高                        | ノードのCPU使用率が高くなっています。   | ノードを追加します。スケジュールされていないノードを修正します。適切なサイズのポッドでノードのCPUを解放   | 警告 @>80% 重大 @>90%      |
| ワークロードネットワークレイテンシのRTTが高い       | 高いTCP RTT (Round Trip Time) 遅延   | Check for Network congestion : ネットワーク帯域幅を大量に消費するワークロードを特定します。PodのCPU利用率が高いかどうかを確認します。ハードウェアネットワークのパフォーマンスを確認します。                                      | 警告 @>150 ms重大 @>300 ms |
| ジョブ失敗                          | ノードのクラッシュまたはリブート、リソースの枯渇、ジョブのタイムアウト、またはポッドのスケジュール設定エラーが原因で、ジョブが正常に完了しませんでした。 | Kubernetesイベントログで障害の原因を確認します。   | 警告 @>1                 |

|                                 |   |  |                   |
|---------------------------------|---|--|-------------------|
| 永続的ボリュームが数日でフル                  | 永続的ボリュームのスペースが数日後に不足します                   | -ボリュームサイズを大きくして、アプリケーションファイル用の十分な空き容量を確保します。-アプリケーションに保存されるデータ量を削減します。                           | 警告@< 8日重大@< 3日    |
| ノードのメモリ圧力                       | ノードのメモリが不足しています。使用可能なメモリが削除しきい値に達しました。    | ノードを追加します。スケジュールされていないノードを修正します。適切なサイズのポッドでノードのメモリを解放  | 重大@>0             |
| ノード-準備完了                        | ノードの準備が5分間完了していません                        | ノードに十分なCPU、メモリ、およびディスクリソースがあることを確認します。ノードのネットワーク接続を確認してください。Kubernetesイベントログで障害の原因を確認します。        | 重大@< 1            |
| 永続的ボリュームの容量が上限です                | 永続的ボリュームバックエンドの使用容量が多くなっています。             | -ボリュームサイズを大きくして、アプリケーションファイル用の十分な空き容量を確保します。-アプリケーションに保存されるデータ量を削減します。                           | 警告 @>80% 重大 @>90% |
| サービスロードバランサを作成できませんでした          | サービスロードバランサの作成に失敗しました                     |  | 重大                |
| ワークロードレプリカの不一致                  | 現在、一部のポッドはDeploymentまたはDaemonSetで使用できません。 |  | 警告@>1             |
| ResourceQuota CPU要求が超過しようとしています | ネームスペースのCPU要求がリソースクォータを超えようとしています         |  | 警告 @>80% 重大 @>90% |
| 高い再送信レート                        | 高いTCP再送信レート                               | ネットワークの輻輳を確認する-ネットワーク帯域幅を大量に消費するワークロードを特定します。PodのCPU利用率が高いかどうかを確認します。ハードウェアネットワークのパフォーマンスを確認します。 | 警告 @>10% 重大 @>25% |

|                |   |   |                   |
|----------------|---|---|-------------------|
| ノードディスク圧力      | ノードのルートファイルシステムまたはイメージファイルシステムで使用可能なディスクスペースとinodeが削除しきい値を超えていいます。                            | -アプリケーションファイル用の十分なスペースを確保するために、ノードディスクのサイズを拡張します。-アプリケーションファイルの使用量を削減します。 | 重大@>0             |
| クラスタのCPU飽和度-上限 | クラスタの割り当て可能なCPU使用率が高くなっています。クラスタのCPU使用率は、CPU使用率の合計をすべてのKubernetesノードの割り当て可能なCPUの合計で割って算出されます。 | ノードを追加します。スケジュールされていないノードを修正します。適切なサイズのポッドでノードのCPUを解放                     | 警告 @>80% 重大 @>90% |

[トップに戻る](#)

## 変更ログモニタ

| モニタ名                       | 重大度 | 概要を監視します   |
|----------------------------|-----|--|
| 内部ボリュームが検出されました            | 情報  | このメッセージは、内部ボリュームが検出された場合に表示されます。                 |
| 内部ボリュームが変更されました            | 情報  | このメッセージは、内部ボリュームが変更された場合に表示されます。                 |
| ストレージノードを検出                | 情報  | このメッセージは、ストレージノードが検出された場合に表示されます。                |
| ストレージノードが削除されました           | 情報  | このメッセージは、ストレージノードが削除された場合に表示されます。                |
| ストレージプールが検出されました           | 情報  | このメッセージは、ストレージプールが検出された場合に表示されます。                |
| Storage Virtual Machineを検出 | 情報  | このメッセージは、Storage Virtual Machineが検出された場合に表示されます。 |
| Storage Virtual Machineを変更 | 情報  | このメッセージは、Storage Virtual Machineが変更された場合に表示されます。 |

[トップに戻る](#)

## データ収集モニタ

| モニタ名 | 製品説明 | 対処方法 |
|------|------|------|
|      |      |      |

|                           |   |   |
|---------------------------|---|---|
| Acquisition Unit のシャットダウン | Data Infrastructure Insights<br>Acquisition Unitは、アップグレードの一環として定期的に再起動し、新機能を導入します。これは、一般的な環境で月に1回以下の頻度で発生します。Acquisition Unitがシャットダウンしたという警告アラートのすぐ後に、新しく再起動したAcquisition UnitがData Infrastructure Insightsへの登録を完了したことを示す解決策が表示されます。通常、このシャットダウンと登録のサイクルには5~15分かかります。 | このアラートが頻繁に発生する場合や15分以上続く場合は、Acquisition Unit、ネットワーク、およびAUをインターネットに接続するプロキシをホストしているシステムの動作を確認してください。             |
| コレクタでエラーが                 | データコレクタのポーリングで予期しない障害が発生しました。   | Data Infrastructure Insightsのデータコレクタページにアクセスして、状況の詳細を確認してください。  |
| コレクタ警告                    | このアラートは通常、データコレクタまたはターゲットシステムの設定に誤りがある場合に発生します。今後のアラートを防止するために、設定を再確認してください。また、データコレクタがすべてのデータを収集した、完了していないデータの取得が原因の可能性もあります。これは、データ収集中に状況が変化した場合に発生します（データ収集の開始時に存在する仮想マシンが、データ収集の実行中とキャプチャの前に削除された場合など）。   | データコレクタまたはターゲットシステムの設定を確認します。コレクタ警告のモニタは他のモニタタイプよりも多くのアラートを送信できるため、トラブルシューティングを行っていない限り、アラート受信者を設定しないことをお勧めします。 |

[トップに戻る](#)

## セキュリティモニタ

| モニタ名                   | しきい値   | 概要を監視します  | 対処方法   |
|------------------------|--------|---|--|
| AutoSupport HTTPS転送が無効 | 警告@<1. | AutoSupportでは、転送プロトコルとしてHTTPS、HTTP、およびSMTPがサポートされます。AutoSupportメッセージは機密性が高いため、NetAppでは、AutoSupportメッセージをNetAppサポートに送信するためのデフォルトの転送プロトコルとしてHTTPSを使用することを強く推奨します。 | AutoSupport メッセージの転送プロトコルとしてHTTPSを設定するには、次のONTAP コマンドを実行します。...system node AutoSupport modify -transport https |

|                          |        |  |   |
|--------------------------|--------|--|---|
| SSH用のクラスタのセキュアでない暗号      | 警告@<1. | SSHでセキュアでない暗号（たとえば、*CBCで始まる暗号）が使用されていることを示します。   | CBC暗号を削除するには、次のONTAP コマンドを実行します。...security ssh remove -vserver <admin vserver>-ciphers aes256-cbc、aes192-cbc、aes128-cbc、3des-cbc   |
| クラスタでログインbannerが無効になりました | 警告@<1. | ONTAP システムにアクセスするユーザに対してログインbannerが無効になっていることを示します。ログインbannerを表示すると、システムに期待されるアクセス方法や使用方法を設定するのに役立ちます。                             | クラスタにログインbannerを設定するには、次のONTAP コマンドを実行します。...security login banner modify -vserver <admin SVM>-message "権限のあるユーザだけがアクセスできます"  |
| クラスタピア通信が暗号化されていません      | 警告@<1. | ディザスタリカバリ、キヤッシュ、またはバックアップのためにデータをレプリケートする場合は、ONTAPクラスタ間でネットワークを介して転送するときに、そのデータを保護する必要があります。ソースとデスティネーションの両方のクラスタで暗号化を設定する必要があります。 | ONTAP 9.6より前に作成されたクラスタピア関係で暗号化を有効にするには、ソースクラスタとデスティネーションクラスタを9.6にアップグレードする必要があります。その後、「cluster peer modify」コマンドを使用して、クラスタピアリング暗号化を使用するようソースとデスティネーション両方のクラスタピアを変更します。詳細については、『ONTAP 9セキュリティ設定ガイド』を参照してください。 |
| デフォルトのローカル管理ユーザが有効       | 警告@>0  | ロックコマンドを使用して、不要なデフォルトの管理ユーザ（組み込み）アカウントをロック（無効化）することを推奨します。これらは主に、パスワードが更新または変更されていないデフォルトアカウントです。                                  | 組み込みの「admin」アカウントをロックするには、次のONTAP コマンドを実行します。...security login lock-username admin  |

|                  |        |   |   |
|------------------|--------|---|---|
| FIPSモードが無効       | 警告@<1. | FIPS 140-2への準拠を有効にすると、TLSv1とSSLv3は無効になります。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準拠モードを有効にするには、次のONTAP コマンドをadvanced権限モードで実行します。...security config modify -interface SSL -is-fips-enabled true  |
| ログ転送が暗号化されていない   | 警告@<1. | 違反の範囲やフットプリントを単一のシステムまたはソリューションに限定するには、syslog情報のオフロードが必要です。そのため、NetAppでは、syslog情報を安全なストレージまたは保持場所に安全にオフロードすることを推奨しています。         | ログの転送先を作成したあとにプロトコルを変更することはできません。暗号化されたプロトコルに変更するには、次のONTAP コマンドを使用して、ログの転送先を削除して再作成します。...cluster log-forwarding create -destination <destination ip>-protocol tcp-encrypted |
| MD5ハッシュ化パスワード    | 警告@>0  | ONTAP ユーザアカウントのパスワードには、より安全なSHA-512ハッシュ関数を使用することを推奨します。安全性の低いMD5ハッシュ関数を使用するアカウントは、SHA-512ハッシュ関数に移行する必要があります。                    | ユーザに解決策 MD5ハッシュ関数を使用するパスワードでアカウントをロックするには、次のONTAP コマンドを実行します。...security login lock -vserver *-username *-hash-function MD5   |
| NTPサーバが設定されていません | 警告@<1. | クラスタにNTPサーバが設定されていないことを示します。冗長性と最適なサービスを実現するために、最低3台のNTPサーバをクラスタに関連付けることを推奨します。   | クラスタにNTPサーバを関連付けるには、次のONTAP コマンドを実行します。cluster time-service ntp server create -server <ntp server host name or ip address>  |
| NTPサーバ数が不足しています  | 警告@<3. | クラスタに設定されているNTPサーバが3台未満であることを示します。冗長性と最適なサービスを実現するために、最低3台のNTPサーバをクラスタに関連付けることを推奨します。   | クラスタにNTPサーバを関連付けるには、次のONTAP コマンドを実行します。...cluster time-service ntp server create -server <ntp server host name or ip address>   |

|                              |        |  |   |
|------------------------------|--------|--|---|
| リモートシェルが有効です                 | 警告@>0  | リモートシェルは、ONTAP 解決策へのコマンドラインアクセスを確立するためのセキュアな方法ではありません。セキュアなリモートアクセスのために、リモートシェルを無効にする必要があります。  | ネットアップでは、セキュアなリモートアクセスのためにSecure Shell (SSH) を推奨しています。クラスタでリモートシェルを無効にするには、advanced権限モードで次のONTAP コマンドを実行します。...security protocol modify -application rsh -enabled false |
| Storage VM監査ログが無効になりました      | 警告@<1. | SVMで監査ログが無効になっていることを示します。  | SVMの監査ログを設定するには、次のONTAP コマンドを実行します。...vserver audit enable -vserver <svm>   |
| SSH用のStorage VMのセキュアでない暗号    | 警告@<1. | SSHでセキュアでない暗号（たとえば、*CBCで始まる暗号）が使用されていることを示します。   | CBC暗号を削除するには、次のONTAP コマンドを実行します。...security ssh remove -vserver <vserver>-ciphers aes256-cbc、aes192-cbc、aes128-cbc、3des-cbc   |
| Storage VMのログインバナーが無効になっています | 警告@<1. | システムでSVMにアクセスするユーザに対してログインバナーが無効になっていることを示します。ログインバナーを表示すると、システムに期待されるアクセス方法や使用方法を設定するのに役立ちます。 | クラスタにログインバナーを設定するには、次のONTAP コマンドを実行します。...security login banner modify -vserver <svm>-message "権限のあるユーザだけがアクセスできます"   |
| Telnetプロトコルが有効               | 警告@>0  | Telnetは、ONTAP 解決策へのコマンドラインアクセスを確立するためのセキュアな方法ではありません。セキュアなリモートアクセスのためにTelnetを無効にする必要があります。     | NetAppでは、セキュアなリモートアクセスにセキュアシェル (SSH) を推奨しています。クラスタでTelnetを無効にするには、次のONTAP コマンドをadvanced権限モードで実行します。...security protocol modify -application telnet -enabled false       |

[トップに戻る](#)

## データ保護モニタ

| モニタ名                           | しきい値   | 概要を監視します   | 対処方法  |
|--------------------------------|--|--|---|
| LUN Snapshotコピー用の十分なスペースがありません | (contains_luns = Yes ) Warning @> 95%...Critical @> 100% | アプリケーションとお客様のデータを格納するには、ボリュームのストレージ容量が必要です。Snapshot予約領域と呼ばれる領域の一部はSnapshotの保存に使用され、データをローカルで保護できます。ONTAPボリュームに格納される新規データや更新データが多いほど、使用されるSnapshot容量は増えますが、今後追加または更新されるデータに使用できるSnapshotストレージ容量は少なくなります。ボリューム内のSnapshotデータ容量がSnapshotリザーブスペースの合計に達すると、新しいSnapshotデータを格納できなくなり、ボリューム内のLUN内のデータの保護レベルが低下する可能性があります。ボリュームの使用済みSnapshot容量を監視して、データサービスの継続性を確保します。 | 緊急アクション重大しきい値に違反した場合は、サービスの中断を最小限に抑えるための即時アクションを考慮してください。1.Snapshotリザーブがフルになったときにボリューム内のデータスペースを使用するようにSnapshotを設定します。2.不要な古いSnapshotをいくつか削除してスペースを解放してください。すぐに実行するアクション警告しきい値に違反した場合は、次のアクションを直ちに実行することを計画してください。1.この増加に対応するために、ボリューム内のSnapshotリザーブスペースを増やしてください。2.Snapshotリザーブがフルになったときにボリューム内のデータスペースを使用するようにSnapshotを設定します。 |
| SnapMirror関係の遅延                | 警告@>150%...重大@>300%                                      | SnapMirror関係の遅延は、Snapshotのタイムスタンプとデスティネーションシステムの時間の差です。lag_time_percentは、SnapMirrorポリシーのスケジュール間隔に対する遅延時間の比率です。遅延時間がスケジュール間隔と等しい場合、lag_time_パーセントは100%になります。SnapMirrorポリシーにスケジュールが設定されていない場合、lag_time_percentは計算されません。  | snapmirror showコマンドを使用して、SnapMirrorのステータスを監視します。snapmirror show-historyコマンドを使用して、SnapMirror転送の履歴を確認します  |

[トップに戻る](#)

## Cloud Volume (CVO) モニタ

| モニタ名                              | CI の重大度 | 概要を監視します   | 対処方法   |
|-----------------------------------|---------|--|--|
| CVO Disk Out of Service』を参照してください | 情報      | 「このイベントは、ディスクが障害としてマークされているか、完全消去中であるか、Maintenance Center に入力されたためにサービスから削除された場合に発生します。」 | なし   |
| ストレージプールのCVO ギブバックに失敗しました         | 重大      | ストレージフェイルオーバー (SFO) ギブバックの一環としてアグリゲートを移行したときに、デスティネーションノードがオブジェクトストアに到達できない場合に発生します。     | 次の対処方法を実行します。 network interface show コマンドを使用して、インタークラスタ LIF がオンラインで機能していることを確認します。 デスティネーションノードのクラスタ間 LIF で「ping」コマンドを使用して、オブジェクトストアサーバへのネットワーク接続を確認してください。 aggregate object-store config show コマンドを使用して、オブジェクトストアの設定が変更されておらず、ログインおよび接続の情報がまだ正確であることを確認してください。 また、 giveback コマンドの「require-partner-waiting」パラメータに false を指定して、エラーを無効にすることもできます。 詳細またはサポートについては、ネットアップテクニカルサポートにお問い合わせください。 |

|                       |    |   |  |
|-----------------------|----|---|--|
| CVO HAインターネクトが停止しています | 警告 | <p>ハイアベイラビリティ（HA）インターネクトが停止しています。フェイルオーバーを利用できない場合、サービスが停止するリスクがあります。</p> | <p>対処方法は、プラットフォームでサポートされている HA ハイアベイラビリティ（HA）インターネクトリンクの数と種類、およびインターネクトが停止している理由によって異なります。リンクが停止している場合：HA ペアの両方のコントローラが動作していることを確認します。外部接続リンクの場合は、インターネクトケーブルが正しく接続されていることと、Small Form-Factor Pluggable (SFP) がある場合は、両方のコントローラに正しく取り付けられていることを確認してください。内部接続リンクの場合は、「ic link off」コマンドと「ic link on」コマンドを使用して、一方のリンクを無効にし、再度有効にします。リンクが無効になっている場合は、「ic link on」コマンドを使用してリンクを有効にします。ピアが接続されていない場合は、「IC link off」コマンドと「IC link on」コマンドを使用して、一方のリンクをディセーブルにし、再度イネーブルにします。問題が解決しない場合は、ネットアップテクニカルサポートにお問い合わせください。</p> |
|-----------------------|----|---|--|

|                            |    |   |   |
|----------------------------|----|---|---|
| ユーザあたりのCVOの最大セッション数を超えるました | 警告 | <p>TCP 接続でのユーザあたりの最大許容セッション数を超えるました。セッションを確立する要求は、一部のセッションが解放されるまで拒否されます。</p> | <p>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。クライアントをリブートします。問題が新規または既存のアプリケーションに起因しているかどうかを確認します。アプリケーションが新規の場合は、「cifs option modify -max-opens -opense-file-per-tree」コマンドを使用して、クライアントのしきい値を高く設定します。クライアントが想定どおりに動作していても、しきい値の上昇が必要となる場合があります。クライアントのしきい値を高く設定するには、advanced 権限が必要です。既存のアプリケーションが問題の原因である場合は、クライアントに問題がある可能性があります。詳細またはサポートについては、ネットアップテクニカルサポートにお問い合わせください。</p> |
|----------------------------|----|---|---|

|                           |    |  |  |
|---------------------------|----|--|--|
| CVO NetBIOS名が競合しています      | 重大 | NetBIOS ネームサービスが、リモートマシンから名前登録要求に対して否定的な応答を受信しました。これは通常、NetBIOS 名またはエイリアスの競合が原因です。その結果、クライアントがデータにアクセスできなくなったり、クラスタ内の適切なデータを提供しているノードに接続できなくなったりすることがあります。 | 次のいずれかの対処策を実行します。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 -alias alias -vserver vserver」コマンドを使用して、重複するNetBIOSエイリアスを削除します。「vserver cifs create -aliases alias alias -vserver vserver」コマンドを使用して、重複する名前を削除し、新しい名前のエイリアスを追加してNetBIOSエイリアスの名前を変更します。エイリアスが設定されておらず、NetBIOS名に競合がある場合は、「vserver cifs delete -vserver vserver」コマンドと「vserver cifs create -cifs -server netbiosname」コマンドを使用してCIFSサーバの名前を変更します。メモ：CIFS サーバを削除すると、データにアクセスできなくなる可能性があります。NetBIOS名を削除するか、リモートマシンのNetBIOS名を変更します。 |
| CVO NFSv4のストアプールを使い果たしました | 重大 | NFSv4 ストアプールを使い果たしました。   | NFS サーバが応答しなくなってから 10 分以上が経過した場合は、ネットアップテクニカルサポートにお問い合わせください。  |
| CVOノードのパニック               | 警告 | このイベントはパニック状態になった場合に生成されます   | ネットアップカスタマーサポートにお問い合わせください。  |

|                               |    |  |   |
|-------------------------------|----|--|---|
| CVOノードのルートボリュームのスペースが不足しています  | 重大 | ルートボリュームのスペースが危険なほど少なくなっていることが検出されました。ノードが完全には動作していません。ノードで NFS アクセスと CIFS アクセスが制限されているため、クラスタ内でデータ LIF がフェイルオーバーされる可能性があります。管理機能は、ノードがルートボリューム上のスペースをクリアするためのローカルリカバリ手順に限定されます。 | 次の対処策を実行します。古いSnapshotコピーを削除するか、/mrootdirectoryから不要になったファイルを削除するか、ルートボリュームの容量を拡張して、ルートボリュームのスペースをクリアします。コントローラをリブートします。詳細またはサポートについては、ネットアップテクニカルサポートにお問い合わせください。   |
| CVOが存在しない管理者共有です              | 重大 | vscan 問題：クライアントが、存在しない ONTAP_ADMIN\$ 共有に接続しようとしました。  | 指定した SVM ID で Vscan が有効になっていないことを確認してください。SVM で Vscan を有効にすると、SVM 用に ONTAP_ADMIN\$ 共有が自動的に作成されます。   |
| CVOオブジェクトストアのホスト解決不可          | 重大 | オブジェクトストアサーバのホスト名を IP アドレスに解決できません。オブジェクトストアクライアントが IP アドレスに解決しないとオブジェクトストアサーバと通信できません。その結果、データにアクセスできなくなる可能性があります。  | DNS 設定を調べて、ホスト名が IP アドレスで正しく設定されていることを確認します。  |
| CVOオブジェクトストアのクラスタ間LIFが停止しています | 重大 | オブジェクトストアクライアントが、オブジェクトストアサーバと通信するための稼働している LIF を見つけることができません。クラスタ間 LIF が動作可能になるまで、このノードはオブジェクトストアクライアントトラフィックを許可しません。その結果、データにアクセスできなくなる可能性があります。                               | 次の対処方法を実行します。「network interface show -role intercluster」コマンドを使用して、クラスタ間LIFのステータスを確認します。クラスタ間LIFが正しく設定され、動作していることを確認してください。インターラクラスタLIFが設定されていない場合は、「network interface create -role intercluster」コマンドを使用して追加します。 |

|                       |    |  |  |
|-----------------------|----|--|--|
| CVOオブジェクトストアシグネチャの不一致 | 重大 | オブジェクトストアサーバに送信された要求の署名が、クライアントで計算された署名と一致しません。その結果、データにアクセスできなくなる可能性があります。  | シークレットアクセスキーが正しく設定されていることを確認します。正しく設定されている場合は、ネットアップテクニカルサポートにお問い合わせください。  |
| CVO QoS監視メモリの最大化      | 重大 | 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上限に達しました。一部の QoS 機能は、制限された容量で動作する場合があります。 | いくつかのアクティブなワークロードまたはストリームを削除してメモリを解放してください。アクティブなワークロードを判別するには、「statistics show -object workloads counter ops」コマンドを使用します。アクティブなワークロードに対する処理がゼロ以外の処理を示しています。次に、「workload delete <workloads name>」コマンドを複数回使用して、特定のワークロードを削除します。または、「stream delete-workload <workload name>*」コマンドを使用して、アクティブなワークロードから関連するストリームを削除します。 |

|                   |    |  |   |
|-------------------|----|--|---|
| CVO REaddirタイムアウト | 重大 | <p>REaddir ファイル処理が、 WAFL で実行が許可されているタイムアウトを超えました。これは、ディレクトリが非常に大きく、スペースであるためです。対処方法を推奨します。</p> | <p>次の対処方法を実行します。Find information specific to recent directories that have REaddir file operations expire using the following 'diag' privilege nodeshell CLIコマンド：WAFL readdir notice showディレクトリがスペースとして示されているかどうかを確認します。ディレクトリがスペースとして示されている場合は、ディレクトリの内容を新しいディレクトリにコピーしてディレクトリファイルのsparsessを削除することをお勧めします。ディレクトリがスペースとして示されておらず、ディレクトリが大きい場合は、ディレクトリ内のファイルエントリの数を減らすことでディレクトリファイルのサイズを縮小することを推奨します。</p> |
|-------------------|----|--|---|

|                         |    |   |  |
|-------------------------|----|---|--|
| ストレージプールのCVOの再配置に失敗しました | 重大 | このイベントは、アグリゲートの再配置時にデスティネーションノードがオブジェクトストアに到達できない場合に発生します。                    | 次の対処方法を実行します。network interface showコマンドを使用して、インターラスタLIFがオンラインで機能していることを確認します。デスティネーションノードのクラスタ間LIFで「ping」コマンドを使用して、オブジェクトストアサーバへのネットワーク接続を確認してください。aggregate object-store config showコマンドを使用して、オブジェクトストアの設定が変更されておらず、ログインおよび接続の情報がまだ正確であることを確認してください。また、再配置コマンドの「override -destination -checks」パラメータを使用して、このエラーを無視することもできます。詳細またはサポートについては、ネットアップテクニカルサポートにお問い合わせください。 |
| CVOシャドウコピーが失敗しました       | 重大 | ボリュームシャドウコピーサービス（VSS）の実行に失敗しました。VSSは、Microsoft Server のバックアップおよびリストアサービス処理です。 | イベントメッセージに表示された情報を使用して、次のことを確認します。ls shadow copy configuration enabled ? 適切なライセンスがインストールされているか。どの共有でシャドウコピー処理が実行されますか。共有名は正しいですか？共有パスが存在するか。シャドウコピー設定とそのシャドウコピーの状態   |
| CVO Storage VMが停止されました  | 情報 | このメッセージは、「vserver stop」処理が成功した場合に表示されます。                                      | Storage VMでデータアクセスを開始するには、「vserver start」コマンドを使用します。   |

|                                  |    |  |   |
|----------------------------------|----|--|---|
| CVOにCIFS認証が多すぎます                 | 警告 | 多数の認証ネゴシエーションが同時に行われています。このクライアントからの新規セッション要求は 256 個あります。  | クライアントが新しい接続要求を 256 個以上作成した理由を調べます。エラーの原因を特定するために、クライアントまたはアプリケーションのベンダーに問い合わせなければならない場合があります。  |
| CVOの未割り当てディスク                    | 情報 | システムに未割り当てのディスクがあります - 容量が無駄になっており、構成の設定ミスや部分的な変更がシステムに適用されている可能性があります。  | 次の対処方法を実行します。disk show -nコマンドを使用して、割り当てが解除されたディスクを確認します。disk assignコマンドを使用して、ディスクをシステムに割り当てます。  |
| CVO : 管理者共有への不正なユーザアクセス          | 警告 | クライアントがONTAP_ADMIN\$ 共有に接続しようとしたが、ログインしているユーザが許可されていません。   | 次の対処策を実行します。指定したユーザ名とIPアドレスがアクティブなVscanスキャナプールの1つに設定されていることを確認します。vserver vscan scanner-pool show-activeコマンドを使用して、現在アクティブなスキャナプールの設定を確認します。 |
| CVO Virus Detected. (CVOウイルスが検出) | 警告 | Vscan サーバからストレージシステムにエラーが報告されました。通常は、ウイルスが検出されたことを示します。ただし、Vscan サーバで発生したその他のエラーではこのイベントを原因処理できます。ファイルへのクライアントアクセスが拒否されました。Vscan サーバは、設定に応じて、ファイルをクリーンアップするか、ファイルを隔離するか、または削除する可能性があります。 | 「syslog」イベントで報告されたVscan サーバのログを調べて、感染ファイルのクリーンアップ、隔離、削除が正常に完了したかどうかを確認します。削除できなかった場合は、システム管理者が手動でファイルを削除しなければならぬことがあります。                    |
| CVO Volumeオフライン                  | 情報 | ボリュームがオフラインになりました。   | ボリュームをオンラインに戻します。   |
| CVO Volumeは制限付きです                | 情報 | フレキシブルボリュームが制限されたことを示すイベントです。  | ボリュームをオンラインに戻します。   |

[トップに戻る](#)

## ビジネス継続性 (SMBC) メディエーターログモニタ用SnapMirror

| モニタ名                    | 重大度 | 概要を監視します  | 対処方法   |
|-------------------------|-----|---|--|
| ONTAP メディエーターが追加されました   | 情報  | このメッセージは、ONTAP メディエーターがクラスタに追加された場合に表示されます。   | なし   |
| ONTAP メディエーターにアクセスできません | 重大  | このメッセージは、ONTAP メディエーターが転用された場合、またはメディエーターパッケージがメディエーターサーバにインストールされなくなった場合に表示されます。そのため、SnapMirrorフェイルオーバーを実行できません。 | 「snapmirror mediator remove」コマンドを使用して、現在のONTAP メディエーターの設定を削除します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。  |
| ONTAP メディエーターが削除されました   | 情報  | このメッセージは、ONTAP メディエーターがクラスタから削除された場合に表示されます。  | なし   |
| ONTAP メディエーターに到達できません   | 警告  | このメッセージは、クラスタでONTAP メディエーターに到達できない場合に表示されます。そのため、SnapMirrorフェイルオーバーを実行できません。                                      | 「network ping」コマンドと「network traceroute」コマンドを使用して、ONTAP メディエーターへのネットワーク接続を確認します。問題が解除されない場合は、「snapmirror mediator remove」コマンドを使用して現在のONTAP メディエーターの設定を削除します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。 |

|                        |    |   |   |
|------------------------|----|---|---|
| SMBC CA証明書期限切れ         | 重大 | <p>このメッセージは、ONTAP メディエーター認証局 (CA) 証明書の有効期限が切れた場合に表示されます。そのため、ONTAP メディエーターへの以降のすべての通信を行うことができません。</p> | <p>「snapmirror mediator remove」コマンドを使用して、現在のONTAP メディエーターの設定を削除します。ONTAP メディエーターサーバで新しいCA 証明書を更新します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。</p>                 |
| SMBC CA証明書の有効期限が切れて    | 警告 | <p>このメッセージは、ONTAP メディエーター認証局 (CA) 証明書の有効期限が30日以内になった場合に表示されます。</p>                                    | <p>この証明書の有効期限が切れる前に、「snapmirror mediator remove」コマンドを使用して現在のONTAP メディエーターの設定を削除します。ONTAP メディエーターサーバで新しいCA 証明書を更新します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。</p> |
| SMBCクライアント証明書期限切れ      | 重大 | <p>このメッセージは、ONTAP メディエータークライアント証明書の有効期限が切れた場合に表示されます。そのため、ONTAP メディエーターへの以降のすべての通信を行うことができません。</p>    | <p>「snapmirror mediator remove」コマンドを使用して、現在のONTAP メディエーターの設定を削除します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。</p>  |
| SMBCクライアント証明書の有効期限が切れて | 警告 | <p>このメッセージは、ONTAP メディエータークライアント証明書の有効期限が30日以内に切れると表示されます。</p>   | <p>この証明書の有効期限が切れる前に、「snapmirror mediator remove」コマンドを使用して現在のONTAP メディエーターの設定を削除します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。</p>                                  |

|                                 |    |  |   |
|---------------------------------|----|--|---|
| SMBC関係が同期していない場合の注意：UMにはこれがあります | 重大 | このメッセージは、SnapMirror for Business Continuity (SMBC) 関係のステータスが「In-Sync」から「Out-of-sync」に変わると表示されます。このRPO = 0のため、データ保護は中断されます。 | ソースボリュームとデスティネーションボリュームの間のネットワーク接続を確認します。デスティネーションで「snapmirror show」コマンドを使用し、ソースで「snapmirror list-destinations」コマンドを使用して、SMBC関係のステータスを監視します。自動再同期では、関係のステータスが「同期中」に戻ります。再同期に失敗した場合は、クラスタ内のすべてのノードがクオーラムにあること、および正常な状態であることを確認します。 |
| SMBCサーバ証明書期限切れ                  | 重大 | このメッセージは、ONTAP メディエーターサーバ証明書の有効期限が切れた場合に表示されます。そのため、ONTAP メディエーターへの以降のすべての通信を行うことができません。                                   | 「snapmirror mediator remove」コマンドを使用して、現在のONTAP メディエーターの設定を削除します。ONTAP メディエーターサーバで新しいサーバ証明書を更新します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。  |
| SMBCサーバ証明書の有効期限が切れて             | 警告 | このメッセージは、ONTAP メディエーターサーバ証明書の有効期限が30日以内になった場合に表示されます。  | この証明書の有効期限が切れる前に、「snapmirror mediator remove」コマンドを使用して現在のONTAP メディエーターの設定を削除します。ONTAP メディエーターサーバで新しいサーバ証明書を更新します。snapmirror mediator addコマンドを使用してONTAP メディエーターへのアクセスを再設定します。  |

[トップに戻る](#)

その他の電源、ハートビート、およびその他のシステムモニタ

| モニタ名                              | 重大度 | 概要を監視します                                    | 対処方法  |
|-----------------------------------|-----|---|---|
| ディスクシェルフの電源装置が検出されました             | 情報  | このメッセージは、電源装置をディスクシェルフに追加した場合に表示されます。       | なし  |
| ディスクシェルフの電源装置が取り外されました            | 情報  | このメッセージは、電源装置をディスクシェルフから取り外すと表示されます。        | なし  |
| MetroClusterの自動計画外スイッチオーバーが無効     | 重大  | このメッセージは、自動計画外スイッチオーバー機能が無効になっている場合に表示されます。 | クラスタ内の各ノードで「MetroCluster modify -node -name <nodename> -automatic -switchover -onfailure true」コマンドを実行して、自動スイッチオーバーを有効にします。  |
| MetroClusterストレージブリッジに到達不能        | 重大  | ストレージブリッジに管理ネットワーク経由でアクセスできません              | 1) ブリッジをSNMPで監視している場合は、「network interface show」コマンドを使用して、ノード管理LIFが動作していることを確認します。「network ping」コマンドを使用して、ブリッジがアクティブであることを確認します。2) ブリッジがインバンドで監視されている場合は、ブリッジへのファブリックケーブル接続を確認し、ブリッジの電源が入っていることを確認します。 |
| MetroClusterブリッジの温度が異常-重大を下回っています | 重大  | ファイバチャネルブリッジのセンサーが重大しきい値を下回っている温度を報告しています。  | 1)ストレージブリッジのファンの動作ステータスを確認します。2)ブリッジが推奨される温度条件で動作していることを確認します。  |
| MetroClusterブリッジの温度が異常-重大を超えてています | 重大  | ファイバチャネルブリッジのセンサーが重大しきい値を超えている温度を報告しています。   | 1)ストレージブリッジのシャーシ温度センサーの動作ステータスを確認するには、コマンド「storage bridge show -Cooling」を使用します。2)ストレージブリッジが推奨される温度条件で動作していることを確認します。  |

| モニタ名                                | 重大度 | 概要を監視します   | 対処方法  |
|-------------------------------------|-----|--|---|
| MetroClusterで取り残されたアグリゲート           | 警告  | アグリゲートはスイッチバック時にリストアされませんでした。                                | 1) コマンド「aggr show」を使用して、アグリゲートの状態を確認します。2) アグリゲートがオンラインの場合、コマンド「MetroCluster switchback」を使用して、アグリゲートを元の所有者に戻します。  |
| MetroCluster パートナー間のすべてのリンクが停止しています | 重大  | RDMAインターフェクトアダプタとクラスタ間LIFがピアクラスタへの接続を切断しているか、ピアクラスタが停止しています。 | 1) クラスタ間LIFが動作していることを確認します。インタークラスタLIFが停止している場合は修復します。2) 「cluster peer ping」コマンドを使用して、ピアクラスタが稼働中であることを確認します。ピアクラスタが停止している場合は、『MetroCluster ディザストリカバリガイド』を参照してください。3) Fabric MetroCluster の場合は、バックエンドファブリックISLが稼働していることを確認します。バックエンドファブリックISLが停止している場合は、ISLを修復します。4) 非ファブリックMetroCluster 構成の場合は、RDMAインターフェクトアダプタ間のケーブル接続が正しいことを確認します。リンクがダウンしている場合は、ケーブル接続を再設定します。 |

| モニタ名  | 重大度 | 概要を監視します  | 対処方法  |
|---|-----|---|---|
| ピアリングネットワーク<br>経由でMetroClusterパート<br>ナーにアクセスできない        | 重大  | ピアクラスタへの接続が<br>切断されています。                          | 1)ポートが正しいネット<br>ワーク/スイッチに接続さ<br>れていることを確認しま<br>す。2) クラスタ間LIFが<br>ピアクラスタに接続され<br>ていることを確認3)<br>cluster peer pingコマンド<br>を使用して、ピアクラス<br>タが稼働中であることを<br>確認します。ピアクラス<br>タが停止している場合<br>は、『MetroCluster ディ<br>ザスタリカバリガイド』<br>を参照してください。 |
| MetroCluster スイッチ間<br>のすべてのリンクが停止<br>しています              | 重大  | ストレージスイッチのす<br>べてのスイッチ間リンク<br>(ISL) が停止していま<br>す。 | 1)ストレージスイッチの<br>バックエンドファブリッ<br>クISLを修復します。2)<br>パートナースイッチが稼<br>働し、ISLが動作してい<br>ることを確認します。3)<br>xWDMデバイスなどの中<br>間機器が動作してい<br>ることを確認します。  |
| MetroCluster ノードから<br>ストレージスタックへ<br>のSASリンクが停止して<br>います | 警告  | SASアダプタまたは接続<br>されているケーブルに問<br>題がある可能性がありま<br>す。  | 1.SASアダプタがオンライン<br>で稼働していること<br>を確認します。2.物理的<br>なケーブル接続が固定さ<br>れ、動作していることを<br>確認し、必要に応じてケ<br>ーブルを交換しま<br>す。3.SASアダプタがデ<br>ィスクシェルフに接続さ<br>れている場合は、IOMと<br>ディスクが適切に装着さ<br>れていることを確認しま<br>す。   |
| MetroClusterFCイニシエ<br>ータリンクガテイシシテ<br>イル                 | 重大  | FCイニシエータアダプタ<br>に障害が発生していま<br>す。                  | 1.FCイニシエータリンク<br>が改ざんされていないこ<br>とを確認しま<br>す。2.system node run<br>-node local -command<br>storage show adapterコマ<br>ンドを使用して、FCイニ<br>シエータアダプタの動作<br>ステータスを確認しま<br>す。  |

| モニタ名                                | 重大度 | 概要を監視します                        | 対処方法   |
|-------------------------------------|-----|---------------------------------|--|
| FC-VIインターフェクトリンクが停止しています            | 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.コマンド「MetroCluster interconnect adapter show」を使用して、FC-VIアダプタの物理ステータスが「up」になっていることを確認します。3.構成にファブリックスイッチが含まれている場合は、それらが適切にケーブル接続および設定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             | 警告  | スペアディスクはスイッチバック中にリストアされませんでした。  | ディスクで障害が発生していない場合は、コマンド「MetroCluster switchback」を使用してディスクを元の所有者に戻します。  |
| MetroClusterストレージブリッジのポートが停止しています   | 重大  | ストレージブリッジのポートはオフラインです。          | 1) コマンド「storage bridge show -ports」を使用して、ストレージブリッジのポートの動作ステータスを確認します。2)ポートへの論理接続と物理接続を確認します。   |
| MetroClusterストレージスイッチのファンに障害が発生しました | 重大  | ストレージスイッチのファンで障害が発生しました。        | 1) コマンドstorage switch show -Coolingを使用して、スイッチのファンが正しく動作していることを確認します。2)ファンFRUが正しく挿入され、動作していることを確認します。   |
| MetroClusterストレージスイッチに到達不能です        | 重大  | ストレージスイッチに管理ネットワーク経由でアクセスできません。 | 1) 「network interface show」コマンドを使用して、ノード管理LIFが動作していることを確認します。2)「network ping」コマンドを使用して、スイッチが有効であることを確認します。3)スイッチにログインした後、SNMP経由でスイッチにアクセスできることを確認します。                            |

| モニタ名                                 | 重大度 | 概要を監視します  | 対処方法  |
|--------------------------------------|-----|---|---|
| MetroCluster スイッチの電源装置に障害が発生しました     | 重大  | ストレージスイッチの電源装置が正常に動作していません。   | 1) コマンド「storage switch show -error-switch -name <switch name>」を使用して、エラーの詳細を確認します。2) コマンド「storage switch show power-switch-name <switch name>」を使用して、障害のある電源装置ユニットを特定します。3) 電源装置のunitisがストレージスイッチのシャーシに正しく挿入され、完全に動作していることを確認します。 |
| MetroCluster スイッチの温度センサーに障害が発生しました   | 重大  | Fibre Channelスイッチのセンサーに障害が発生しました。   | 1) コマンドstorage switch show -Coolingを使用して、ストレージスイッチの温度センサーの動作ステータスを確認します。2) スイッチが推奨される温度条件で動作していることを確認します。   |
| MetroCluster スイッチの温度が異常です            | 重大  | Fibre Channelスイッチの温度センサーが異常な温度を報告しました。  | 1) コマンドstorage switch show -Coolingを使用して、ストレージスイッチの温度センサーの動作ステータスを確認します。2) スイッチが推奨される温度条件で動作していることを確認します。   |
| Service Processor Heartbeat Missedの略 | 情報  | このメッセージは、ONTAP がサービスポートセッサ (SP) から想定される「ハートビート」信号を受信しなかった場合に表示されます。このメッセージに加えて、SPからのログファイルがデバッグのために送信されます。ONTAP は SP をリセットして通信を回復しようとします。SP のリブート中は、最大2分間は SP を使用できません。 | ネットアップテクニカルサポートにお問い合わせください。   |

| モニタ名                   | 重大度 | 概要を監視します  | 対処方法  |
|------------------------|-----|---|---|
| サービスプロセッサハートビートを停止しました | 警告  | <p>このメッセージは、ONTAP がサービスプロセッサ (SP) からハートビートを受信しなくなった場合に表示されます。ハードウェアの設計によっては、システムは引き続きデータを提供することも、データ損失やハードウェアの破損を防ぐためにシャットダウンすることもあります。システムはデータを提供し続けますが、SPが動作していない可能性があるため、システムは停止しているアプライアンス、ポートエラー、またはOpen Firmware (OFW) のPower-on Self-Test (POST) エラーの通知を送信できません。システムが設定されている場合は、AutoSupport (「コールホーム」) メッセージを生成してネットアップテクニカルサポートおよび設定された宛先に送信します。AutoSupport メッセージが正常に配信されると、問題の特定と解決方法が大幅に改善されます。</p> | <p>システムがシャットダウンした場合は、ハード電源の再投入を試みます。コントローラをシャーシから引き出し、押し込んでから、システムの電源を入れます。電源再投入後も問題が解決しない場合、または注意が必要な他の状況については、ネットアップテクニカルサポートにお問い合わせください。</p> |

[トップに戻る](#)

## 詳細情報

- ・ "アラートの表示と非表示"

## 電子メール通知を設定しています

サブスクリプション関連の通知用の E メールリストや、パフォーマンスポリシーのしきい値違反の通知を受け取る受信者のグローバル E メールリストを設定できます。

通知メール受信者の設定を行うには、 [\*Admin] > [Notifications] ページに移動し、 [Email] タブを選択します。

## Subscription Notification Recipients

Send subscription related notifications to the following:

- All Account Owners
- All Monitor & Optimize Administrators
- Additional Email Addresses

X

Save

## Global Monitor Notification Recipients

Default email recipients for monitor related notifications:

- All Account Owners
- All Monitor & Optimize Administrators
- Additional Email Addresses

Save

## サブスクリプション通知の受信者

サブスクリプション関連のイベント通知の受信者を設定するには、「サブスクリプション通知の受信者」セクションに移動します。次の受信者のいずれかまたはすべてに、サブスクリプション関連イベントに関する E メール通知を送信するように選択できます。

- ・ すべてのアカウント所有者
- ・ すべての監視と最適化管理者
- ・ 指定する追加の E メールアドレス

送信される通知の種類と実行できるユーザアクションの例を次に示します。

| * 通知 : *  | * ユーザーアクション : *   |
|---|---|
| トライアルまたはサブスクリプションが更新されました   | ページでサブスクリプションの詳細を確認する <a href="#">"配信登録"</a>  |
| サブスクリプションの有効期限は 90 日です<br>サブスクリプションの有効期限は 30 日です                          | [Auto Renewal]が有効な場合、対応は不要です。NetAppセールスに連絡してサブスクリプションを更新してください。                                 |
| トライアルは 2 日で終了します  | ページからトライアルを更新し <a href="#">"配信登録"</a> ます。試用版は 1 回更新できます。サブスクリプションの購入については、NetApp営業担当にお問い合わせください |
| トライアルまたはサブスクリプションの有効期限が切れたアカウントは、48 時間以内にアカウントの収集を停止し、48 時間後にアカウントが削除されます | サブスクリプションの購入については、NetApp営業担当にお問い合わせください   |

受信者がData Infrastructure Insightsからの通知を受信できるようにするには、「許可」リストに次のEメールアドレスを追加します。



- \ 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

アラートのEメール通知は、アラートに対するすべての対処方法についてアラート受信者リストに送信されます。アラート通知をグローバル受信者リストに送信することもできます。

グローバルアラート受信者を設定するには、[\* Global Monitor Notification Recipients] セクションで目的の受信者を選択します。

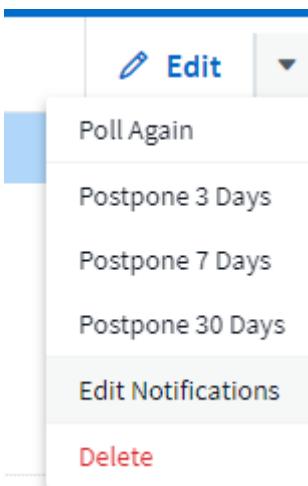
モニタを作成または変更するときは、各モニタのグローバル受信者リストを常に上書きできます。



ONTAP データコレクタ通知は、クラスタ/データコレクタに関連する特定のモニタ通知よりも優先されます。Data Collector自体に設定した受信者リストには、データコレクタアラートが送信されます。アクティブなデータコレクタアラートがない場合は、監視用に生成されたアラートが特定の監視受信者に送信されます。

## ONTAP の通知の編集

ONTAP クラスタの通知を変更するには、ストレージランディングページの右上のドロップダウンから[Edit Notifications]を選択します。



ここでは、重大、警告、情報、解決済みのアラートの通知を設定できます。各シナリオは、グローバル受信者リストまたは選択した他の受信者に通知できます。

## Edit Notifications



### By Email

Notify team on

Critical, Warn...

Send to



- Global Monitor Recipient List
- Other Email Recipients

email@email.one

email2@email2.two

Notify team on

Resolved

Send to



- Global Monitor Recipient List
- Other Email Recipients

### By Webhook

Enable webhook notification to add recipients

## 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では、標準入力インターフェイスとして Webhook がサポートされています。たとえば、Slack、PagerDuty、Teams、および Discord は、すべてのウェブフックをサポートしています。Data Infrastructure Insightsは、カスタマイズ可能な汎用Webhookチャネルをサポートすることで、これらの配信チャネルの多くのサポートできます。Web フックの情報は、これらのアプリケーション Web サイトに掲載されています。たとえば、Slackには"この便利なガイドです"次のような機能があります。

複数の Web フックチャネルを作成できます。各チャネルは異なる目的に合わせて、アプリケーションや受信者などを個別に指定できます

webhook チャネルインスタンスは、次の要素で構成されています。

|                  |  |
|------------------|--|
| 名前               | 一意の名前  |
| URL              | URLパラメータとともに _http:// または <a href="https://">https://</a> プレフィックスを含む Webhook ターゲット URL |
| 方法               | GET、POST-DEFAULT は POST です   |
| カスタムヘッダー         | ここで任意のカスタムヘッダー行を指定します  |
| メッセージ本文          | メッセージの本文をここに入力します  |
| デフォルトのアラートパラメータ  | に、 webhook のデフォルトパラメータを示します  |
| カスタムパラメータとシークレット | カスタムパラメータとシークレットを使用すると、一意のパラメータとパスワードなどのセキュアな要素を追加できます                                 |

## Webhook の作成

Data Infrastructure Insights の Webhook を作成するには、 \* Admin > Notifications に移動し、 Webhooks \* タブを選択します。

次の図は、 Slack 用に設定された webhook の例を示しています。

## Edit a Webhook

### Name

### Template Type

### URL

### Method

### Custom Header

```
Content-Type: application/json
Accept: application/json
```

### Message Body

```
{
  "blocks": [
    {
      "type": "section",
      "text": {
        "type": "mrkdwn",
        "text": "*Cloud Insights Alert - %%alertId%%*\nSeverity - *%%severity%%*"
      }
    }
  ]
}
```

各フィールドに適切な情報を入力し、完了したら[保存]をクリックします。

また、[Webフックのテスト]ボタンをクリックして、接続をテストすることもできます。これにより、選択されたメソッドに従って、定義されたURLに「Message Body」（置換なし）が送信されます。

Data Infrastructure InsightsのWebhookは、多数のデフォルトパラメータで構成されています。また、独自のカスタムパラメータまたはシークレットを作成することもできます。

## Default Alert Parameters

| Name                      | Description   |
|---------------------------|---|
| %%alertDescription%%      | Alert description   |
| %%alertId%%               | Alert ID  |
| %%alertRelativeUrl%%      | Relative URL to the Alert page. To build alert link use <a href="https://%%cloudInsightsHostName%%/%%alertRelativeUrl%%">https://%%cloudInsightsHostName%%/%%alertRelativeUrl%%</a> |
| %%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 i

| Name  | Value | Description |
|---|-------|-------------|
| No Data Available   |       |             |
| <a href="#" style="background-color: #0070C0; color: white; padding: 5px 10px; border-radius: 5px;">+ Parameter</a> |       |             |

パラメータ：パラメータとは何ですか？また、パラメータの使用方法を教えてください。

アラートパラメータは、アラートごとに動的に設定される値です。たとえば、%%TriggeredOn%% の \_Parameter はアラートがトリガーされたオブジェクトで置き換えられます。

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の説明でボリューム名とストレージ名のパラメータを次のように設定できます。"High Latency for Volume : %%relatedObject.volume.name%%、Storage : %%relatedObject.storage.name%%"

このセクションでは、置換は「Test Webhook」ボタンをクリックしたときに`_not_performed`になります。このボタンは、`_%_substitutions`を示すペイロードを送信しますが、これらをデータに置き換えません。

カスタムパラメータとシークレット

このセクションでは、任意のカスタムパラメータやシークレットを追加できます。セキュリティ上の理由から、シークレットが定義されている場合は、 webhook 作成者だけがこの webhook チャネルを変更できます。他のユーザに対しては読み取り専用です。URL/ ヘッダーのシークレットは、`%%<secret_name>%%`として使用できます。

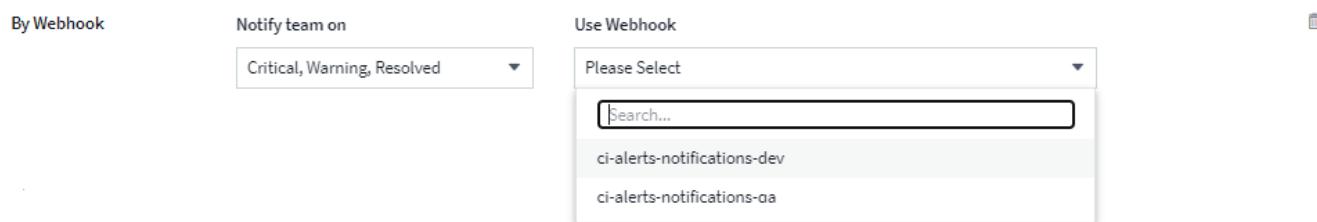
#### Webhookリストページ

Webhookのリストページには、Name、Created By、Created On、Status、Secure、およびLast Reportedフィールド。

モニタで [Webhook Notification] を選択します

でWebhook通知を選択するには"監視する"、\*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。警告レベル（重大、警告、解決済み）を選択し、目的のウェブフックを選択します。

#### ③ Set up team notification(s) (alert your team via email, or Webhook)



Webhook の例：

Webhook用Webhook "PagerDuty"用Webhook用Webhook用Webhook用Webhook用Webhook"Slack"用"チーム""切断"

#### Discord のウェブフックの例

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 用のウェブフックを設定する例を示します。



このページでは、変更される可能性があるサードパーティの手順について説明します。最新の情報については、を参照して"ディスコードの説明"ください。

ディスコード設定：

- Discord（コード解除）でサーバーを選択し、Text Channels（テキストチャンネル）でEdit Channel（チャネルの編集）（歯車アイコン）を選択します。

- ・「統合」>「Web フックの表示」と選択し、「新規 Webhook」をクリックします
- ・Webhook URL をコピーします。この設定をData Infrastructure InsightsのWebhook設定に貼り付ける必要があります。

データインフラに関するインサイトを作成Webhook：

1. Data Infrastructure Insightsで、\* Admin > Notifications に移動し、Webhooks タブを選択します。  
[+Webhook\*] をクリックして、新しい Web フックを作成します。
2. Web フックに「Discord」などのわかりやすい名前を付けます。
3. [Template Type] ドロップダウンで、[\* Discord] を選択します。
4. 上の URL を \_url\_field に貼り付けます。

## Edit a Webhook

### Name

Discord Webhook

### Template Type

Discord

### URL

<https://discord.com/api/webhooks/> <token string>

### Method

POST

### Custom Header

Content-Type: application/json  
Accept: application/json

### Message Body

```
{
  "content": null,
  "embeds": [
    {
      "title": "%severity% | %alertId% | %triggeredOn%",
      "description": "%monitorName%",
      "url": "https://%%cloudInsightsHostname%%%alertRelativeUrl%%",
      "color": 3244733,
      "fields": [
        {
          "name": "%%CloudInsightsMetricName%%"
        }
      ]
    }
  ]
}
```

Cancel

Test Webhook

Save Webhook



Webhookをテストするには、メッセージ本文のhttps://netapp.com\_)値を任意の有効なURL（\_など）に一時的に置き換えてから、\_Test Webhook\_ボタンをクリックします。テストが完了したら、必ずメッセージの本文を元に戻してください。

## Webhook で通知します

Webhookでイベントを通知するには、[Data Infrastructure Insights ]で\*[Alerts]>[Monitors]に移動し、[+Monitor]\*をクリックして新しいを作成し"監視する"ます。

- ・メトリックを選択し、モニタの条件を定義します。
- ・チーム通知の設定（\_Set up team notification(s)）で、 \* Webhook \* 配信方法を選択します。
- ・目的のイベント（クリティカル、警告、解決済み）の「コード解除」ウェブフックを選択します。

### 3 Set up team notification(s) (alert your team via email, or Webhook)



## 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 のウェブフックの設定例を示します。



このページでは、変更される可能性があるサードパーティの手順について説明します。最新の情報については、を参照して"PagerDuty のドキュメント"ください。

### PagerDuty 設定：

1. PagerDuty で、 [Services] > [Service Directory] に移動し、 [+New Service\*] ボタンをクリックします
2. 「A\_Name\_」と入力し、「\_」を選択して API を直接使用します\_。[ サービスの追加 ] をクリックします。

# Add a Service

A service may represent an application, component or team you wish to open incidents against.

## General Settings

Name:

Description:

Add a description for this service (optional)

## Integration Settings

Connect with one of PagerDuty's supported integrations, or create a custom integration through email or API. Alerts from a service from a supported integration or through the Events V2 API.

You can add more than one integration to a service, for example, one for monitoring alerts and one for change events.

Integration Type:

Select a tool

PagerDuty integrates with hundreds of tools, including monitoring tools, ticketing systems, code repositories, and deploy pipelines. This may involve configuration steps in the tool you are integrating with PagerDuty.

Integrate via email

If your monitoring tool can send email, it can integrate with PagerDuty using a custom email address.

Use our API directly

If you're writing your own integration, use our Events API. More information is in our developer documentation.

Events API v2

Don't use an integration

If you only want incidents to be manually created. You can always add additional integrations later.

- [Integrations] タブをクリックして、\*統合キー\*を表示します。このキーは、以下のData Infrastructure Insights Web フックを作成する際に必要になります。
- [インシデント\*] または [サービス\*] に移動して、アラートを表示します。

PagerDuty

Incidents on All Teams

| Your open Incidents                                  |                            | All open Incidents                                   |                            |
|--|----------------------------|--|----------------------------|
| Assigned to  | Incident ID                | Assigned to  | Incident ID                |
| <input type="checkbox"/> <a href="#">Edwin Chung</a> | <a href="#">#123456789</a> | <input type="checkbox"/> <a href="#">Edwin Chung</a> | <a href="#">#123456789</a> |
| <input type="checkbox"/> <a href="#">Edwin Chung</a> | <a href="#">#123456789</a> | <input type="checkbox"/> <a href="#">Edwin Chung</a> | <a href="#">#123456789</a> |
| <input type="checkbox"/> <a href="#">Edwin Chung</a> | <a href="#">#123456789</a> | <input type="checkbox"/> <a href="#">Edwin Chung</a> | <a href="#">#123456789</a> |
| <input type="checkbox"/> <a href="#">Edwin Chung</a> | <a href="#">#123456789</a> | <input type="checkbox"/> <a href="#">Edwin Chung</a> | <a href="#">#123456789</a> |
| <input type="checkbox"/> <a href="#">Edwin Chung</a> | <a href="#">#123456789</a> | <input type="checkbox"/> <a href="#">Edwin Chung</a> | <a href="#">#123456789</a> |
| <input type="checkbox"/> <a href="#">Edwin Chung</a> | <a href="#">#123456789</a> | <input type="checkbox"/> <a href="#">Edwin Chung</a> | <a href="#">#123456789</a> |
| <input type="checkbox"/> <a href="#">Edwin Chung</a> | <a href="#">#123456789</a> | <input type="checkbox"/> <a href="#">Edwin Chung</a> | <a href="#">#123456789</a> |

データインフラに関するインサイトを作成Webhook：

1. Data Infrastructure Insightsで、\* Admin > Notifications に移動し、Webhooks タブを選択します。[+Webhook\*] をクリックして、新しい Web フックを作成します。
2. Webhook に "PagerDuty Trigger" などのわかりやすい名前を付けます。このウェブフックは、クリティカル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、値を上記の PagerDuty\_Integration Key\_value に設定します。

### Custom Parameters and Secrets i

| Name           | Value ↑ | Description |
|----------------|---------|-------------|
| %%routingKey%% | *****   | ⋮           |

+ Parameter

|  |             |
|--|-------------|
| Name <span style="color: blue;">i</span> | Value       |
| routingKey                               | .....       |
| Type                                     | Description |
| Secret                                   |             |

Cancel Save Parameter

この手順を繰り返して、解決済みイベントの "PagerDuty Resolve" ウェブフックを作成します。

### PagerDutyとData Infrastructure Insightsのフィールドマッピング

次の表と画像は、PagerDutyとData Infrastructure Insightsの間のフィールドのマッピングを示しています。

| PagerDuty | データインフラの分析情報 |
|-----------|--------------|
| アラートキー    | アラートID       |
| ソース       | でトリガされます     |
| 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    |

|           |              |
|-----------|--------------|
| PagerDuty | データインフラの分析情報 |
| クラス       | モニタ名         |

### 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 で通知します

Webhookでイベントを通知するには、[Data Infrastructure Insights]で\*[Alerts]>[Monitors]に移動し、[+Monitor]\*をクリックして新しいを作成し"監視する"ます。

- メトリックを選択し、モニタの条件を定義します。
- チーム通知の設定（\_Set up team notification(s)）で、\* Webhook \* 配信方法を選択します。
- クリティカルレベルおよび警告レベルのイベントには、"PagerDuty Trigger" Web フックを選択します。
- 解決されたイベントの「PagerDuty Resolve」を選択します。

#### 3 Set up team notification(s) (alert your team via email, or Webhook)

|            |                   |  |
|------------|-------------------|--|
| By Webhook | Notify team on    | Use Webhook(s)   |
|            | Critical, Warning | PagerDuty Trigger <span style="border: 1px solid #ccc; padding: 2px;">×</span> |
|            | Resolved          | PagerDuty Resolve <span style="border: 1px solid #ccc; padding: 2px;">×</span> |



PagerDuty ではトリガーイベントが解決済みイベントとは異なる方法で処理されるため、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をお勧めします。

## Slack の Web フックの例

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 Web フックを設定する例を示します。



このページでは、変更される可能性があるサードパーティの手順について説明します。最新の情報については、["ドキュメントのたるみ"](#)ください。

たわみ率の例：

- に移動 <https://api.slack.com/apps> し、新しいアプリを作成します。わかりやすい名前を付けて、[ たわみ率 ( Slack ) ] ワークスペースを選択する。

**Create a Slack App** ×

**App Name**  
e.g. Super Service

Don't worry; you'll be able to change this later.

**Development Slack Workspace**  
Development Slack Workspace ▼

Your app belongs to this workspace—leaving this workspace will remove your ability to manage this app. Unfortunately, this can't be changed later.

By creating a Web API Application, you agree to the [Slack API Terms of Service](#).

Cancel Create App

- 受信したウェブフックに移動し、[on\_Activate incoming webhooks]、[Request to Add New Webhook] の順にクリックして、投稿するチャネルを選択します。
- Webhook URL をコピーします。この設定をData Infrastructure InsightsのWebhook設定に貼り付ける必要があります。

データインフラに関するインサイトを作成Webhook：

1. Data Infrastructure Insightsで、\* Admin > Notifications に移動し、Webhooks タブを選択します。  
[+Webhook\*] をクリックして、新しい Web フックを作成します。
2. Web フックに「Slack 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 \_ (Template Type)] ドロップダウンで、[\* Slack \* (\* Slack \*)] を選択する。
4. 上の URL を \_url\_field に貼り付けます。

## Edit a Webhook

Name

Template Type

URL

Method

Custom Header

```
Content-Type: application/json
Accept: application/json
```

Message Body

```
{
  "blocks": [
    {
      "type": "section",
      "text": {
        "type": "mrkdwn",
        "text": "Cloud Insights Alert - %%alertId%%\nSeverity - %%severity%%"
      }
    }
  ]
}
```

[Cancel](#) [Test Webhook](#) [Save Webhook](#)

## Webhook で通知します

Webhookでイベントを通知するには、[Data Infrastructure Insights]で\*[Alerts]>[Monitors]に移動し、[+Monitor]\*をクリックして新しいを作成し"監視する"ます。

- ・メトリックを選択し、モニタの条件を定義します。
- ・チーム通知の設定（\_Set up team notification(s)）で、\* Webhook \* 配信方法を選択します。
- ・目的のイベントに対応する「Slack」Web フックを選択します（Critical、Warning、Resolved）

③ **Set up team notification(s)** (alert your team via email, or Webhook)

|            |                             |   |
|------------|-----------------------------|---|
| By Webhook | Notify team on              | Use Webhook(s)  |
|            | Critical, Warning, Resolved | Slack <span style="border: 1px solid black; padding: 0 2px;">X</span> |
|            |                             | X ▾   |

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、を参照してください。 <https://api.slack.com/messaging/composing>
- ・エラー処理：[https://api.slack.com/messaging/webhooks#handling\\_errors](https://api.slack.com/messaging/webhooks#handling_errors)

## Microsoft チームの Web フックの例

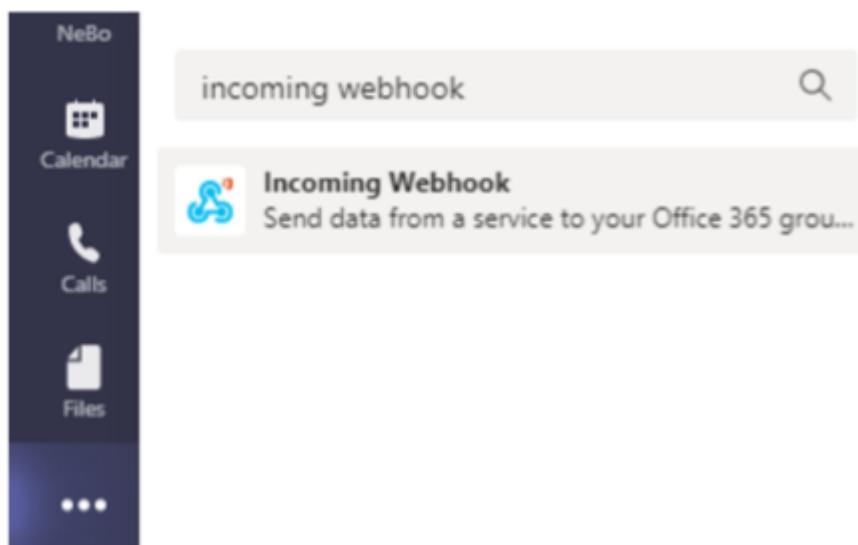
Webhook を使用すると、ユーザーはカスタマイズされた webhook チャネルを使用して、さまざまなアプリケーションにアラート通知を送信できます。このページでは、チームの Web フックを設定する例を示します。



このページでは、変更される可能性があるサードパーティの手順について説明します。最新の情報については、を参照して"チームのドキュメント"ください。

チームの設定：

1. チームで、kebab を選択し、着信 Webhook を検索します。



2. [チームに追加（Add to a Team）] > [チームを選択（Select a Team）] > [コネクタのセットアップ（Setup a Connector）]

3. Webhook URL をコピーします。この設定をData Infrastructure InsightsのWebhook設定に貼り付ける必要があります。

データインフラに関するインサイトを作成Webhook：

1. Data Infrastructure Insightsで、\* Admin > Notifications に移動し、Webhooks タブを選択します。  
[+Webhook\*] をクリックして、新しい Web フックを作成します。
2. Web フックに「Teams Webhook」などのわかりやすい名前を付けます。
3. [Template Type] ドロップダウンで、[\*Teams] を選択します。

## Edit a Webhook

Name  
Teams Webhook

Template Type  
Teams

URL  
https://netapp.webhook.office.com/webhookb2/<token string>

Method  
POST

Custom Header  
Content-Type: application/json  
Accept: application/json

Message Body

```
{  
  "@type": "MessageCard",  
  "@context": "http://schema.org/extensions",  
  "themeColor": "0076D7",  
  "summary": "Cloud Insights Alert",  
  "sections": [  
    {  
      "activityTitle": "%%severity%% | %%alertId%% | %%triggeredOn%%",  
      "activitySubtitle": "%%triggerTime%%",  
      "markdown": false,  
      "text": "%%message%%"  
    }  
  ]  
}
```

**Cancel** **Test Webhook** **Save Webhook**

1. 上の URL を \_url\_field に貼り付けます。

## Webhook で通知します

Webhookでイベントを通知するには、[Data Infrastructure Insights]で\*[Alerts]>[Monitors]に移動し、[+Monitor]\*をクリックして新しいを作成し"監視する"ます。

- ・メトリックを選択し、モニタの条件を定義します。
- ・チーム通知の設定（\_Set up team notification(s)）で、\* Webhook \* 配信方法を選択します。
- ・目的のイベント（重要、警告、解決済み）の「チーム」ウェブフックを選択します。

### ③ Set up team notification(s) (alert your team via email, or Webhook)

|            |                               |                   |
|------------|-------------------------------|-------------------|
| By Webhook | Notify team on                | Use Webhook(s)    |
|            | Critical, Warning, Resolved ▾ | Teams - Edwin X ▾ |

## 著作権に関する情報

Copyright © 2025 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隨時、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 5225.227-19（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。