



モニターとアラート

Data Infrastructure Insights

NetApp
February 19, 2026

目次

モニターとアラート	1
モニターによるアラート	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ー?	1
モニターリスト	8
モニターグループ	9
システム定義モニター	11
モニター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
データが欠落している場合のアラート	13
「常時アクティブ」アラート	14
電子メール通知の設定	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
異常検出モニター	17
異常検出とは何ですか?	17
異常検出はいつ必要になるのでしょうか?	18
異常検出モニターの作成	18
異常の観察	20
システムモニター	21
モニターの説明	22
詳細情報	96
Webhook通知	96
Webhookを使用した通知	96
Discord の Webhook の例	100
PagerDuty の Webhook の例	102
Slack の Webhook の例	106
Microsoft Teams の Webhook の例	108

モニターとアラート

モニターによるアラート

インフラストラクチャ リソース全体のパフォーマンスしきい値、ログ イベント、および異常を追跡するようにモニターを構成します。ノードの書き込み遅延、ストレージ容量、アプリケーション パフォーマンスなどのメトリックのカスタム アラートを作成し、これらの条件が満たされたときに通知を受け取ります。

モニターを使用すると、ストレージ、VM、EC2、ポートなどの「インフラストラクチャ」オブジェクトによって生成されたメトリックや、Kubernetes、ONTAP の高度なメトリック、Telegraf プラグインなどで収集された「統合」データのしきい値を設定できます。これらのメトリック モニターは、警告レベルまたは重大レベルのしきい値を超えたときに警告を發します。

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

Data Infrastructure Insightsは、"[システム定義モニター](#)"環境に応じても同様です。

セキュリティのベストプラクティス

Data Infrastructure Insightsアラートは、テナント上のデータ ポイントと傾向を強調するように設計されており、Data Infrastructure Insightsでは、アラートの受信者として有効な電子メール アドレスを入力できます。安全な環境で作業している場合は、通知を受信するユーザーやアラートにアクセスできるユーザーについて特に注意してください。

メトリックまたはログモニター？

1. Data Infrastructure Insightsメニューから、*アラート>モニターの管理*をクリックします。

現在構成されているモニターを示すモニター リスト ページが表示されます。

2. 既存のモニターを変更するには、リスト内のモニター名をクリックします。
3. モニターを追加するには、[+ モニター] をクリックします。



新しいモニターを追加すると、メトリック モニターまたはログ モニターを作成するように求められます。

- *Metric* はインフラストラクチャまたはパフォーマンス関連のトリガーに関するアラートを監視します
- *Log* はログ関連のアクティビティに関するアラートを監視します

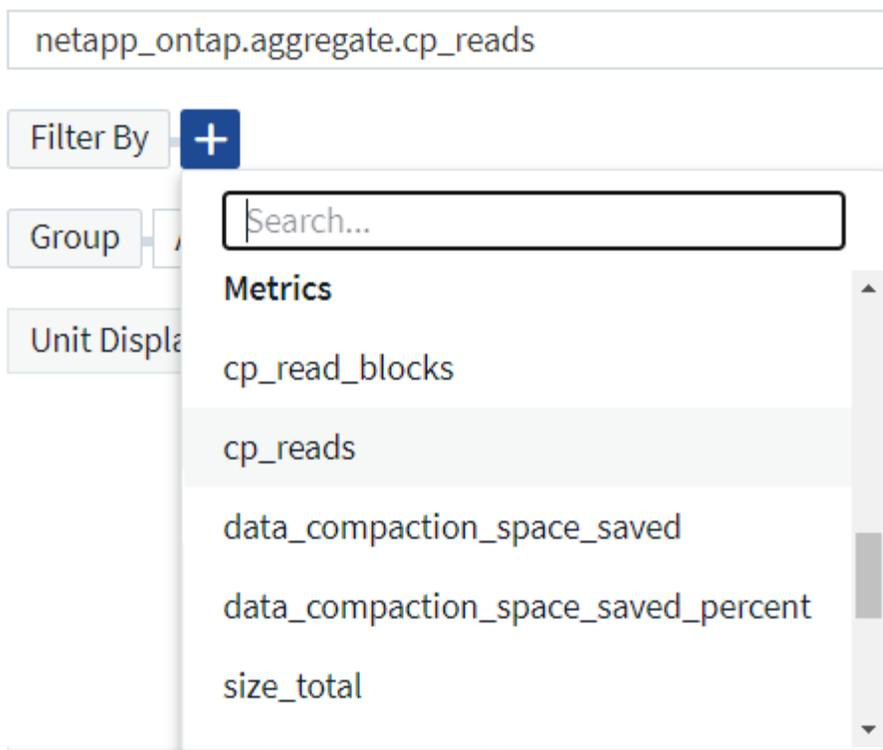
モニターの種類を選択すると、モニター構成ダイアログが表示されます。作成するモニターの種類に応じて構成が異なります。

メトリックモニター

1. ドロップダウンで、監視するオブジェクト タイプとメトリックを検索して選択します。

フィルターを設定して、監視するオブジェクト属性またはメトリックを絞り込むことができます。

1 Select a metric to monitor



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

メトリック モニターは、ストレージ、スイッチ、ホスト、VM などのインベントリ オブジェクト、およびONTAP Advanced や Kubernetes データなどの統合メトリックに適用されます。インベントリ オブジェクトを監視する場合、「グループ化」方法を選択できないことに注意してください。ただし、統合データを監視する場合はグループ化が許可されます。

マルチコンディションモニター

2 番目の条件を追加して、メトリック モニターをさらに絞り込むこともできます。「+ セカンダリメトリック条件の追加」プロンプトを展開し、追加の条件を構成するだけです。



両方の条件が満たされた場合、モニターは警告を発します。

2 番目の条件は「AND」のみで実行できることに注意してください。1 つの条件または他の条件に基づいてアラートを生成することはできません。

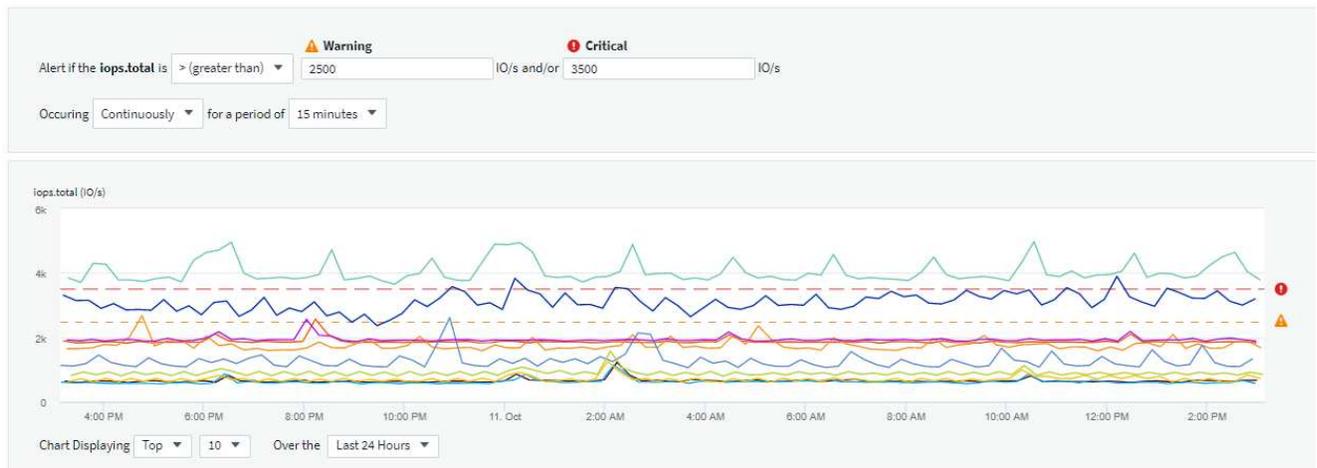
モニターの条件を定義します。

1. 監視するオブジェクトとメトリックを選択した後、警告レベルおよび/または重大レベルのしきい値を設定します。
2. 警告レベルには、この例では 200 と入力します。この警告レベルを示す破線がサンプルグラフに表示されます。
3. *Critical* レベルには 400 と入力します。この重大レベルを示す破線がサンプルグラフに表示されます。

グラフには履歴データが表示されます。グラフ上の警告レベルと重大レベルの線はモニターの視覚的な表現であるため、それぞれのケースでモニターがいつアラートをトリガーするかを簡単に確認できます。

4. 発生間隔には、[15 分] の期間で [連続] を選択します。

しきい値を超えた瞬間にアラートをトリガーするか、しきい値が一定期間継続して超過するまで待つかを選択できます。この例では、合計 IOPS が警告レベルまたは重大レベルを超えるたびに警告を受け取るのではなく、監視対象オブジェクトが少なくとも 15 分間、これらのレベルのいずれかを継続して超えた場合にのみ警告を受け取ります。



アラート解決動作を定義する

メトリック モニターのアラートを解決する方法を選択できます。次の 2 つの選択肢が表示されます。

- メトリックが許容範囲に戻ったら解決します。
- 指定された時間 (1 分から 7 日間) にわたってメトリックが許容範囲内にある場合に解決します。

ログモニター

*ログ モニター*を作成するときは、まず利用可能なログ リストから監視するログを選択します。上記のように、利用可能な属性に基づいてフィルタリングできます。1 つ以上の「グループ化」属性を選択することもできます。



ログ モニター フィルターは空にできません。

1 Select the log to monitor

Log Source logs.netapp.ems

Filter By ems.ems_message_type Nblade.vscanConnBackPressure x x ems.cluster_vendor NetApp x x

ems.cluster_model FAS* x AFF* x ASA* x FDvM* x x + ?

Group By ems.cluster_uuid x ems.cluster_vendor x ems.cluster_model x ems.cluster_name x x
ems.svm_uuid x ems.svm_name x

アラートの動作を定義する

上記で定義した条件が 1 回 (つまり即時) 発生したときに、重大度レベルが *Critical*、*Warning*、または *Informational* であるアラートを送信するモニターを作成するか、条件が 2 回以上発生するまでアラートを待機することができます。

アラート解決動作を定義する

ログ モニターのアラートを解決する方法を選択できます。次の 3 つの選択肢が表示されます。

- すぐに解決: アラートはすぐに解決され、それ以上のアクションは必要ありません
- 時間に基づいて解決: 指定された時間が経過するとアラートが解決されます
- ログ エントリに基づいて解決: 後続のログ アクティビティが発生すると、アラートが解決されます。たとえば、オブジェクトが「使用可能」としてログに記録される場合などです。

- 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 +

異常検出モニター

1. ドロップダウンで、監視するオブジェクト タイプとメトリックを検索して選択します。

フィルターを設定して、監視するオブジェクト属性またはメトリックを絞り込むことができます。

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。

- 監視するオブジェクトとメトリックを選択したら、異常が検出される条件を設定します。
 - 選択したメトリックが予測された境界を*上回った*場合、*その境界を下回った*場合、または境界を*上回ったか下回った*場合に異常を検出するかどうかを選択します。
 - 検出の*感度*を設定します。低 (検出される異常が少ない)、中、または高 (検出される異常が多い)。
 - アラートを*警告*または*重大*に設定します。
 - 必要に応じて、選択したメトリックが設定したしきい値を下回っている場合に異常を無視して、ノイズを減らすこともできます。

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

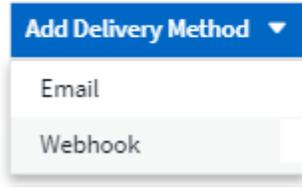
To reduce noise, ignore anomalies when **performance.iops.total** is below Optional IO/s

Chart Displaying Top 10 Over the Last 24 Hours

通知の種類と受信者を選択する

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

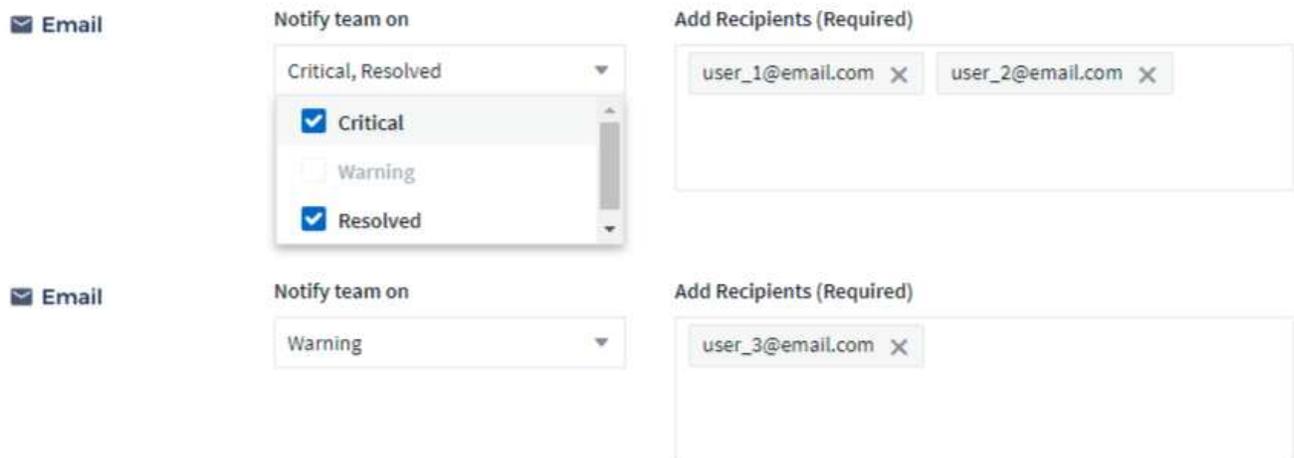
3 Set up team notification(s) (alert your team via email, or Webhook)



電子メールによるアラート:

アラート通知の電子メール受信者を指定します。必要に応じて、警告または重大なアラートに異なる受信者を選択できます。

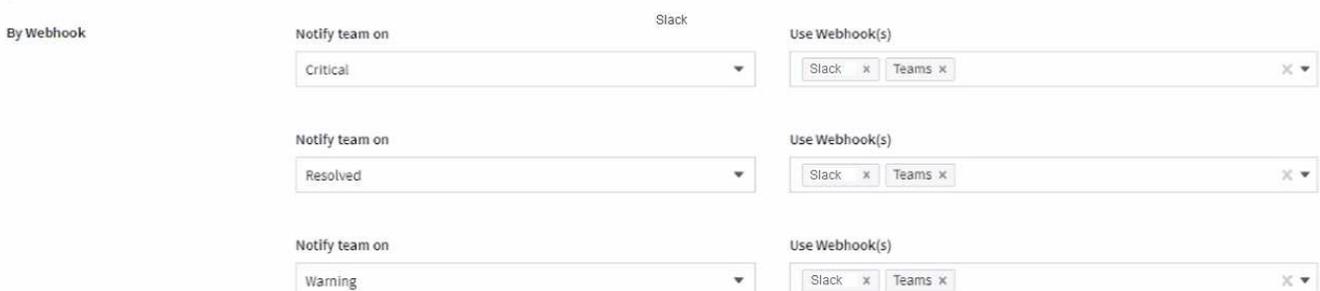
3 Set up team notification(s)

A screenshot of the configuration interface for email alerts. It shows two rows of settings. Each row starts with an "Email" icon and a "Notify team on" dropdown menu. The first row's dropdown is open, showing "Critical" (checked), "Warning" (unchecked), and "Resolved" (checked). To the right of each row is an "Add Recipients (Required)" field. The first row has two recipients: "user_1@email.com" and "user_2@email.com". The second row has one recipient: "user_3@email.com".

Webhook経由のアラート:

アラート通知用の Webhook を指定します。必要に応じて、警告または重大なアラートに異なる Webhook を選択できます。

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

A screenshot of the configuration interface for Webhook alerts. It shows three rows of settings. Each row starts with "By Webhook" and a "Notify team on" dropdown menu. The first row's dropdown is set to "Critical", the second to "Resolved", and the third to "Warning". To the right of each row is a "Use Webhook(s)" field. Each field contains two selected Webhooks: "Slack" and "Teams".



ONTAPデータ コレクターの通知は、クラスタ/データ コレクターに関連する特定のモニター通知よりも優先されます。データ コレクター自体に設定した受信者リストには、データ コレクターのアラートが送信されます。アクティブなデータ コレクター アラートがない場合、モニターによって生成されたアラートが特定のモニター受信者に送信されます。

是正措置または追加情報の設定

*アラートの説明を追加*セクションに入力することで、オプションの説明や追加の洞察や是正アクションを追加できます。説明は最大 1024 文字まで入力でき、アラートとともに送信されます。洞察/是正措置フィールドは最大 67,000 文字まで入力でき、アラート ランディング ページの概要セクションに表示されます。

これらのフィールドでは、アラートを修正または対処するためのメモ、リンク、または手順を入力できます。

任意のオブジェクト属性 (たとえば、ストレージ名) をアラートの説明にパラメータとして追加できます。たとえば、「ボリューム: `%%relatedObject.volume.name%%`、ストレージ: `%%relatedObject.storage.name%%` の待機時間が長い」のような説明で、ボリューム名とストレージ名のパラメータを設定できます。

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

モニターを保存する

1. 必要に応じて、モニターの説明を追加できます。
2. モニターにわかりやすい名前を付けて、[保存] をクリックします。

新しいモニターがアクティブなモニターのリストに追加されます。

モニターリスト

モニター ページには、現在構成されているモニターが一覧表示され、次の情報が表示されます。

- モニター名
- ステータス
- 監視対象のオブジェクト/メトリック

- モニターの条件

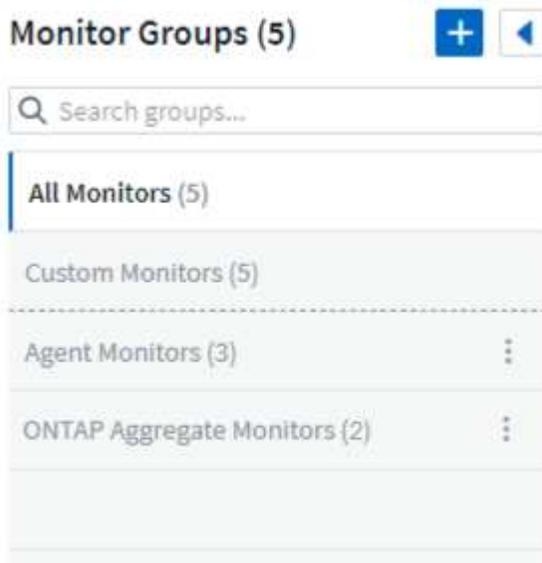
モニターの右側にあるメニューをクリックし、「一時停止」を選択すると、オブジェクトタイプの監視を一時的に一時停止できます。監視を再開する準備ができたなら、[再開] をクリックします。

メニューから*複製*を選択すると、モニターをコピーできます。その後、新しいモニターを変更し、オブジェクト/メトリック、フィルター、条件、電子メールの受信者などを変更できます。

モニターが不要になった場合は、メニューから*削除*を選択して削除できます。

モニターグループ

グループ化すると、関連するモニターを表示および管理できます。たとえば、テナント上のストレージ専用のモニターグループを作成したり、特定の受信者リストに関連するモニターを作成したりできます。



次のモニターグループが表示されます。グループに含まれるモニターの数、グループ名の横に表示されません。

- すべてのモニターにはすべてのモニターが一覧表示されます。
- カスタムモニターには、ユーザーが作成したすべてのモニターが一覧表示されます。
- 一時停止中のモニターには、Data Infrastructure Insightsによって一時停止されているシステムモニターが一覧表示されます。
- Data Infrastructure Insightsには、システム監視グループもいくつか表示されます。これには、"[システム定義モニター](#)" ONTAPインフラストラクチャおよびワークロードモニターなど。



カスタムモニターは、一時停止、再開、削除、または別のグループに移動できます。システム定義のモニターは一時停止および再開できますが、削除または移動することはできません。

サスペンドモニター

このグループは、Data Infrastructure Insights が1つ以上のモニターを一時停止している場合にのみ表示されます。過剰なアラートや継続的なアラートが生成されている場合、モニターは一時停止されることがあります。モニターがカスタムモニターの場合は、継続的なアラートを防止するために条件を変更してから、モニ

ターを再開します。一時停止の原因となった問題が解決されると、モニターは一時停止中のモニターグループから削除されます。

システム定義モニター

モニターに必要なデバイスやログの可用性が環境に含まれている限り、これらのグループには、Data Infrastructure Insightsによって提供されるモニターが表示されます。

システム定義のモニターは、変更したり、別のグループに移動したり、削除したりすることはできません。ただし、システムモニターを複製し、その複製を変更または移動することはできます。

システムモニターには、ONTAPインフラストラクチャ (ストレージ、ボリュームなど) やワークロード (ログモニターなど)、その他のグループのモニターが含まれる場合があります。NetAppは顧客のニーズと製品の機能を継続的に評価しており、必要に応じてシステムモニターとグループを更新または追加します。

カスタムモニターグループ

ニーズに応じて、モニターを含む独自のグループを作成できます。たとえば、ストレージ関連のすべてのモニターのグループが必要な場合があります。

新しいカスタムモニターグループを作成するには、["+"] 新しいモニターグループの作成] ボタンをクリックします。グループの名前を入力し、「グループの作成」をクリックします。その名前で空のグループが作成されます。

グループにモニターを追加するには、[すべてのモニター] グループ (推奨) に移動し、次のいずれかを実行します。

- 単一のモニターを追加するには、モニターの右側にあるメニューをクリックし、[グループに追加] を選択します。モニターを追加するグループを選択します。
- モニター名をクリックしてモニターの編集ビューを開き、[モニターグループに関連付ける] セクションでグループを選択します。

5 Associate to a monitor group (optional)



グループをクリックし、メニューから [グループから削除] を選択して、モニターを削除します。すべてのモニター または カスタムモニターグループからモニターを削除することはできません。これらのグループからモニターを削除するには、モニター自体を削除する必要があります。

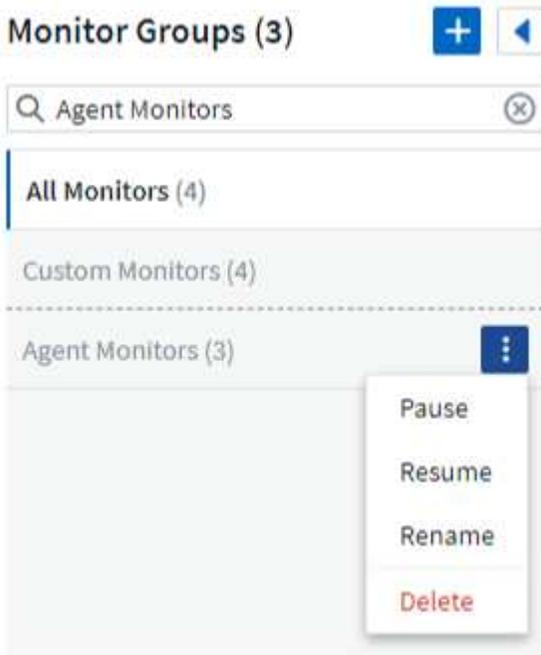


グループからモニターを削除しても、Data Infrastructure Insightsからモニターは削除されません。モニターを完全に削除するには、モニターを選択し、[削除] をクリックします。これにより、そのアイテムは所属していたグループからも削除され、どのユーザーも利用できなくなります。

同様に、[グループに移動] を選択して、モニターを別のグループに移動することもできます。

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

グループの名前を変更したり、グループを削除したりする場合にも、同じメニューを使用します。グループを削除しても、Data Infrastructure Insightsからモニターは削除されません。モニターは引き続き [すべてのモニター] で利用できます。



システム定義モニター

Data Infrastructure Insights には、メトリックとログの両方に対するシステム定義のモニターが多数含まれています。利用可能なシステム モニターは、テナントに存在するデータ コレクターによって異なります。そのため、データ コレクターが追加されたり、その構成が変更されたりすると、Data Infrastructure Insights で使用できるモニターが変わる可能性があります。

表示"[システム定義モニター](#)"Data Infrastructure Insightsに含まれるモニターの説明ページ。

詳細情報

- ["アラートの表示と消去"](#)

モニターからのアラートの表示と管理

Data Infrastructure Insightsは、次のような場合にアラートを表示します。"[監視対象の閾値](#)"超過しています。



モニターとアラートは、Data Infrastructure Insights Standard Edition 以上で利用できます。

アラートの表示と管理

アラートを表示および管理するには、次の手順を実行します。

1. アラート > すべてのアラート ページに移動します。
2. 最新の 1,000 件までのアラートのリストが表示されます。フィールドの列ヘッダーをクリックすると、このリストを任意のフィールドで並べ替えることができます。リストには次の情報が表示されます。これらの列のすべてがデフォルトで表示されるわけではないことに注意してください。「歯車」アイコンをクリックすると、表示する列を選択できます。
 - アラートID: システムによって生成された一意のアラートID
 - トリガー時刻: 関連するモニターがアラートをトリガーした時刻
 - 現在の重大度 (アクティブアラートタブ): アクティブアラートの現在の重大度
 - 最高重大度 (解決済みアラートタブ); 解決前のアラートの最大の重大度
 - モニター: アラートをトリガーするように設定されたモニター
 - トリガーオン: 監視対象のしきい値を超えたオブジェクト
 - ステータス: 現在のアラートのステータス、新規 または 処理中
 - アクティブ ステータス: アクティブ または 解決済み
 - 条件: アラートをトリガーしたしきい値条件
 - メトリック: 監視対象のしきい値を超えたオブジェクトのメトリック
 - モニターステータス: アラートをトリガーしたモニターの現在のステータス
 - 修正アクションあり: アラートには修正アクションが提案されています。これらを表示するにはアラート ページを開いてください。

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

- 処理中 アラートが調査中であるか、またはオープンのままにしておく必要があることを示します。
- *[閉じる]*をクリックすると、アクティブなアラートのリストからアラートが削除されます。

各アラートの左側にあるチェックボックスを選択し、「選択したアラートのステータスを変更」をクリックすると、複数のアラートを管理できます。

アラート ID をクリックすると、アラートの詳細ページが開きます。

アラート詳細パネル

任意のアラート行を選択すると、アラートの詳細パネルが開きます。アラートの詳細パネルには、アラートに関する追加の詳細が表示されます。これには、概要、オブジェクトのデータに関連するグラフを表示する_パフォーマンス_セクション、関連資産、アラート調査員が入力した_コメント_が含まれます。

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

altimeout

Attributes

Filters Applied: N/A

Description

No Description Provided

Resolution conditions

Resolve when metric is within acceptable range for 10 mins

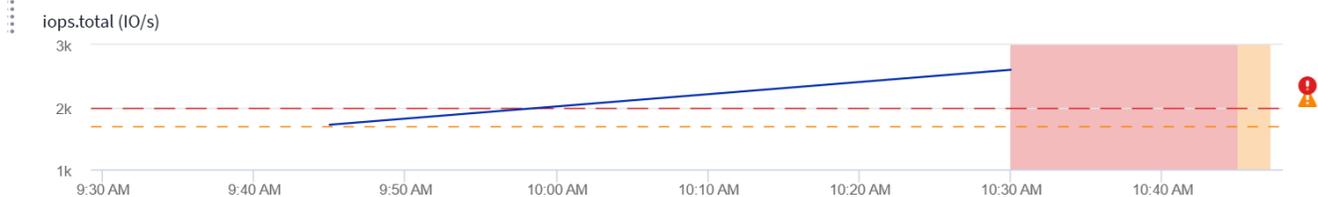
Status

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 [Settings](#)

Close

データが欠落している場合のアラート

Data Infrastructure Insightsなどのリアルタイム システムでは、モニターの分析をトリガーしてアラートを生成するかどうかを決定するために、次の2つのいずれかに依存します。

- 次に到着するデータポイント
- データポイントがなく、十分に待った場合に起動するタイマー

データの到着が遅い場合、またはデータが到着しない場合は、データ到着率が「リアルタイム」でアラートをトリガーするには不十分であるため、タイマー メカニズムが引き継ぐ必要があります。したがって、一般的な質問は、「分析ウィンドウを閉じて、結果を確認するまでにどれくらい待てばよいですか?」となります。待つ時間が長すぎると、役に立つほど速くアラートが生成されなくなります。

長期的なデータ損失が発生する前の最後のデータ ポイントで条件に違反していることを通知する 30 分のウィ

ンドウを持つモニターがある場合、モニターはメトリックの回復を確認するために使用する他の情報や条件が持続していることを通知する情報を受け取っていないため、アラートが生成されます。

「常時アクティブ」アラート

監視対象オブジェクトに条件が常に存在するようにモニターを構成することもできます (例: IOPS > 1 または レイテンシ > 0)。これらは多くの場合、「テスト」モニターとして作成され、その後忘れ去られます。このようなモニターは、構成オブジェクトに対して永続的に開いたままのアラートを作成するため、時間の経過とともにシステムのストレスや安定性の問題が発生する可能性があります。

これを防ぐために、Data Infrastructure Insights は、7 日後に「永続的にアクティブな」アラートを自動的に閉じます。基礎となるモニター条件は (おそらく) 引き続き存在し、新しいアラートがほぼ即座に発行される可能性があることに注意してください。ただし、この「常にアクティブな」アラートを閉じると、発生する可能性のあるシステム ストレスの一部が軽減されます。

電子メール通知の設定

サブスクリプション関連の通知用の電子メール リストと、パフォーマンス ポリシーしきい値違反の通知の受信者のグローバル電子メール リストを構成できます。

通知メールの受信者設定を構成するには、管理 > 通知 ページに移動し、メール タブを選択します。

Subscription Notification Recipients

Send subscription related notifications to the following:

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

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構成するには、「サブスクリプション通知の受信者」セクションに移動します。サブスクリプション関連のイベントに関する電子メール通知を、次の受信者のいずれかまたは全員に送信するように選択できます。

- すべてのアカウント所有者
- すべての _Monitor & Optimize_ 管理者

- 指定する追加のメールアドレス

以下は、送信される可能性のある通知の種類と、実行できるユーザーアクションの例です。

通知：	ユーザーアクション：
トライアルまたはサブスクリプションが更新されました	サブスクリプションの詳細を確認する" Subscription "ページ
サブスクリプションは90日後に期限切れになります サブスクリプションは30日後に期限切れになります	「自動更新」が有効になっている場合は、何もする必要はありません。サブスクリプションを更新するには、NetAppの営業担当者にお問い合わせください。
トライアルは2日後に終了します	トライアルの更新" Subscription "ページ。試用版は1回更新できます。サブスクリプションを購入するには、NetAppの営業担当者にお問い合わせください。
試用版またはサブスクリプションの有効期限が切れました。アカウントは48時間以内にデータ収集を停止します。アカウントは48時間後に削除されます。	サブスクリプションを購入するには、NetAppの営業担当者にお問い合わせください。



受信者がData Infrastructure Insightsから通知を確実に受信できるようにするには、次のメールアドレスを「許可」リストに追加します。

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

アラートのグローバル受信者リスト

アラートに関するアクションごとに、アラートの電子メール通知がアラート受信者リストに送信されます。アラート通知をグローバル受信者リストに送信することを選択できます。

グローバルアラートの受信者を設定するには、「グローバルモニター通知の受信者」セクションで目的の受信者を選択します。

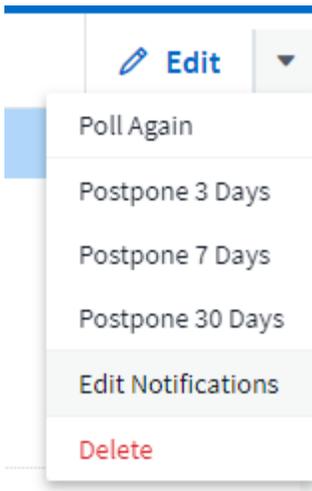
モニターを作成または変更するときに、いつでも個々のモニターのグローバル受信者リストを上書きできます。



ONTAPデータ コレクターの通知は、クラスター/データ コレクターに関連する特定のモニター通知よりも優先されます。データ コレクター自体に設定した受信者リストには、データ コレクターのアラートが送信されます。アクティブなデータ コレクター アラートがない場合、モニターによって生成されたアラートが特定のモニター受信者に送信されます。

ONTAPの通知の編集

ストレージ ランディング ページの右上にあるドロップダウンから [通知の編集] を選択すると、ONTAPクラスタの通知を変更できます。



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

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

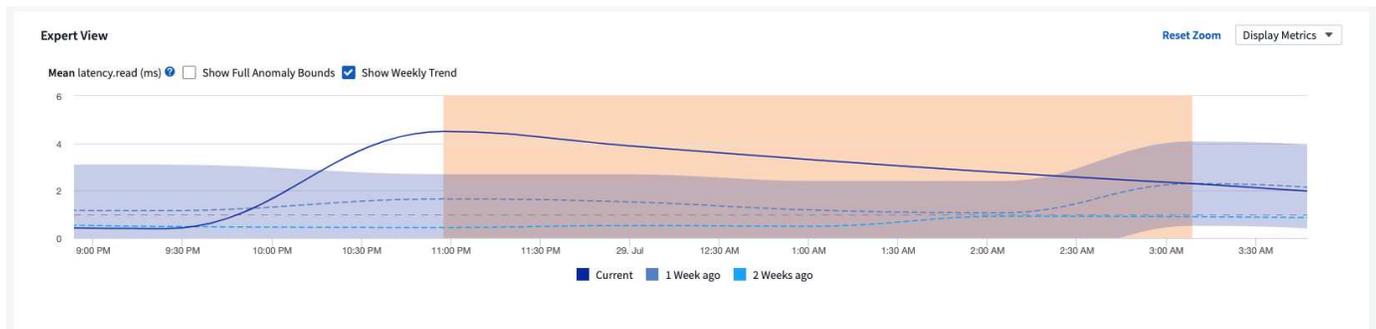
By Webhook

Enable webhook notification to add recipients

異常検出モニター

異常検出は、テナント上のデータ パターンの予期しない変化に関する洞察を提供します。異常は、オブジェクトの動作パターンが変化すると発生します。たとえば、オブジェクトが水曜日の特定の時間に特定のレベルのレイテンシを経験し、次の水曜日の同じ時間にレイテンシがそのレベルを超えて急上昇した場合、その急上昇は異常と見なされます。Data Infrastructure Insights を使用すると、このような異常が発生したときに警告を発するモニターを作成できます。

異常検出は、繰り返し発生する予測可能なパターンを示すオブジェクト メトリックに適しています。これらのオブジェクト メトリックが予想レベルを上回ったり下回ったりすると、Data Infrastructure Insights はアラートを生成して調査を促します。



異常検出とは何ですか？

異常は、メトリックの平均値が、過去数週間のそのメトリックの加重平均から標準偏差の数だけ離れており、最近の週が以前の週よりも重み付けが大きい場合に発生します。Data Infrastructure Insights は、データを監視し、異常が検出された場合に警告する機能を提供します。検出の「感度」レベルを設定することができます。たとえば、平均値と平均値からの標準偏差が少ないほど感度が高くなり、生成されるアラートが多くなります。逆に、感度が低い = 平均からの標準偏差が大きい = アラートが少ない。

異常検出監視はしきい値監視とは異なります。

- **しきい値ベースの監視***は、特定のメトリックに対して事前に定義されたしきい値がある場合に機能します。言い換えれば、何が期待されているか（つまり、正常範囲内）を明確に理解している場合です。

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***は、機械学習アルゴリズムを使用して、「正常」の定義が明確でない場合に、標準から逸脱する外れ値を識別します。

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になるのでしょうか？

異常検出モニタリングは、次のような多くの状況で役立つアラートを提供できます。

- 正常の定義が不明瞭な場合。たとえば、SAN エラー率はポートに応じて異なる量が予想される場合があります。1つのエラーについて警告するのはノイズが多く不必要ですが、突然のまたは大幅な増加は広範囲にわたる問題を示している可能性があります。
- 時間の経過とともに変化がある場所。季節性があるワークロード (つまり、特定の時間に忙しいか静かである)。これには、バッチの停止を示す可能性のある予期しない静かな期間が含まれる場合があります。
- しきい値を手動で定義および調整することが非現実的な大量のデータを扱う場合。たとえば、ワークロードが異なる多数のホストやボリュームを持つテナントなどです。それぞれ SLA が異なる場合があるため、標準を超える SLA を理解することが重要です。

異常検出モニターの作成

異常を警告するには、**Observability > Alerts > +Monitor** に移動してモニターを作成します。モニタータイプとして「異常検出モニター」を選択します。

Metric Monitor

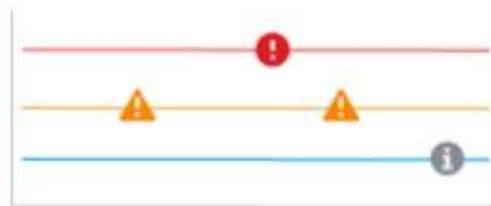
Set the high and low parameters that will trigger an alert if exceeded



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



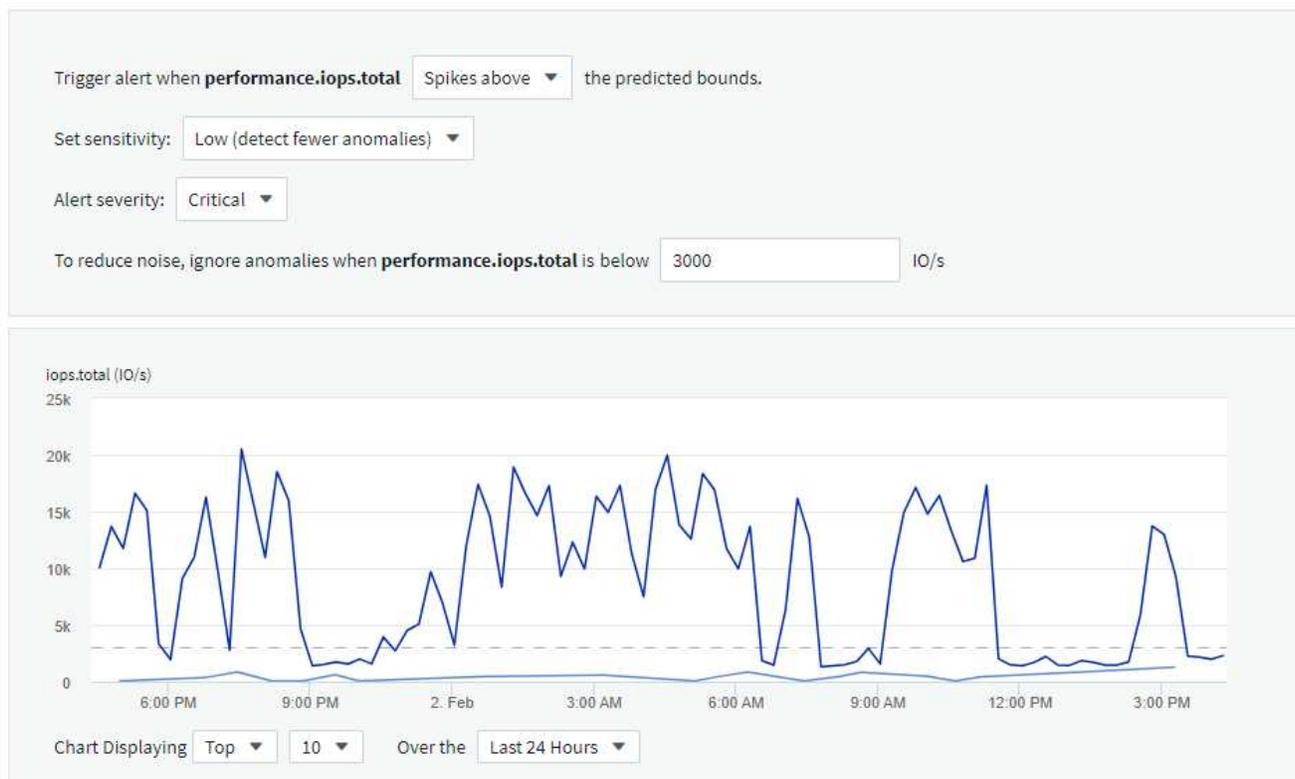
Use when you want to trigger alerts against performance spikes and drops

監視するオブジェクトとメトリックを選択します。他の種類のモニターと同様に、フィルターやグループ化を設定できます。

次にモニターの条件を設定します。

- 選択したメトリックが予測された境界を 上回る 場合、その境界を下回る場合、またはその両方の場合にアラートをトリガーします。
- 感度を「中」、「低」（より少ない異常が検出される）、または「高」（より多くの異常が検出される）に設定します。
- 警告レベルが *Critical* か *Warning* かを判断します。
- オプションで、その値を下回る異常は無視される値を設定します。これによりノイズを軽減できます。この値はサンプル グラフでは破線が表示されます。

2 Define the monitor's conditions



最後に、アラートの配信方法 (電子メール、Webhook、またはその両方) を構成し、モニターにオプションの説明や修正アクションを指定し、必要に応じてモニターをカスタム グループに追加できます。

モニターを意味のある名前前で保存すれば完了です。

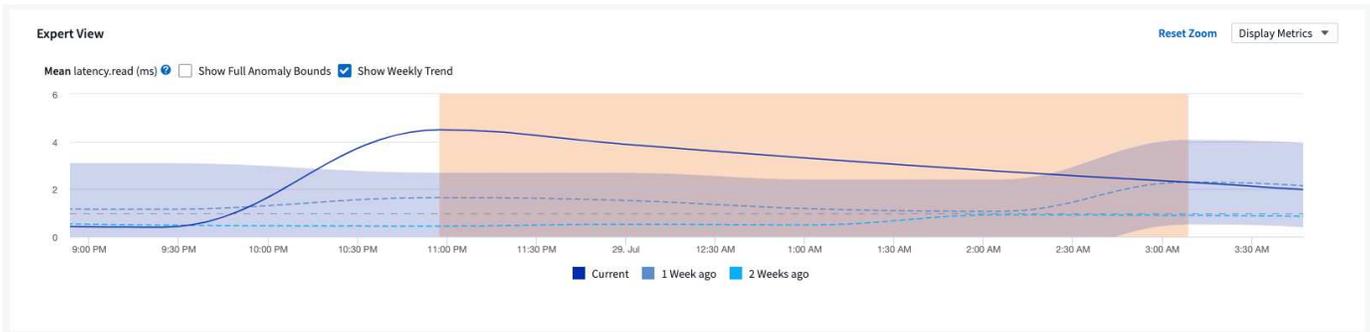
作成時に、モニターは前週のデータを分析して初期ベースラインを確立します。異常検出は、時間が経過し、履歴が増えるにつれて、より正確になります。



モニターが作成されると、DII は前の週の既存のデータを調べて、大幅なデータの急増や減少がないか調べます。これらは異常とみなされます。モニター作成後の最初の 1 週間 (「学習」フェーズ) は、アラートの「ノイズ」が増加する可能性があります。このノイズを軽減するために、30 分以上続く急上昇または急降下のみが異常とみなされ、アラートが生成されます。次の週には、より多くのデータが分析されるにつれて、通常、ノイズは減少し、一定期間続く大幅な急上昇または急降下は異常とみなされます。

異常の観察

アラート ランディング ページでは、異常が検出されたときにトリガーされるアラートにより、メトリックが予測された境界の外側に急上昇した時点から、その境界内に戻った時点までの、チャートに強調表示されたバンドが表示されます。



アラート ランディング ページで異常チャートを表示しているときに、次のオプションを選択できます。

- 週次傾向: 最大 5 週間前の同じ時刻、同じ日の値と比較します。
- 完全な異常境界: デフォルトでは、グラフはメトリック値に焦点を当てているため、メトリックの動作をより適切に分析できます。完全な異常境界（最大値など）を表示する場合に選択します

ランディング ページのパフォーマンス セクションでオブジェクトを選択して、異常の原因となったオブジェクトを表示することもできます。チャートには選択したオブジェクトの動作が表示されます。



システムモニター

Data Infrastructure Insights には、メトリックとログの両方に対するシステム定義のモニターが多数含まれています。利用可能なシステム モニターは、テナントに存在するデータ コレクターによって異なります。そのため、データ コレクターが追加されたり、その構成が変更されたりすると、Data Infrastructure Insights で使用できるモニターが変わる可能性があります。



多くのシステム モニターは、デフォルトでは一時停止 状態になっています。モニターの [再開] オプションを選択すると、システム モニターを有効にすることができます。データ コレクターで [Advanced Counter Data Collection] と [Enable ONTAP EMS log collection] が有効になっていることを確認します。これらのオプションは、ONTAP データ コレクターの [Advanced

Enable ONTAP EMS log collection

Configuration] にあります。

Opt in for Advanced Counter Data Collection rollout.

モニターの説明

システム定義のモニターは、事前定義されたメトリックと条件、および変更できないデフォルトの説明と修正アクションで構成されます。システム定義モニターの通知受信者リストを変更することができます。メトリック、条件、説明、修正アクションを表示したり、受信者リストを変更したりするには、システム定義のモニターグループを開き、リスト内のモニター名をクリックします。

システム定義のモニターグループは変更または削除できません。

以下のシステム定義モニターは、記載されているグループで使用できます。

- * ONTAPインフラストラクチャ* には、ONTAPクラスタのインフラストラクチャ関連の問題を監視するモニターが含まれています。
- * ONTAPワークロードの例* には、ワークロード関連の問題のモニターが含まれています。
- 両方のグループのモニターはデフォルトで一時停止状態になります。

以下は、現在Data Infrastructure Insightsに含まれているシステムモニターです。

メトリックモニター

モニター名	重大度	モニターの説明	対処方法
-------	-----	---------	------

<p>ファイバーチャネルポート使用率が高い</p>	<p>重大</p>	<p>ファイバー チャネル プロトコル ポートは、顧客のホスト システムとONTAP LUN 間の SAN トラフィックを受信および転送するために使用されます。ポートの使用率が高い場合、それがボトルネックとなり、最終的にはファイバー チャネル プロトコルのワークロードの重要なパフォーマンスに影響を及ぼします。...警告アラートは、ネットワークトラフィックを分散させるために計画されたアクションを実行する必要があることを示します。...重大なアラートは、サービスの中断が差し迫っており、サービスの継続性を確保するためにネットワークトラフィックを分散するための緊急措置を実行する必要があることを示します。</p>	<p>重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、直ちに次のアクションを検討してください。1.ワークロードを、使用率の低い別の FCP ポートに移動します。2. ONTAP のQoS ポリシーまたはホスト側の構成を使用して、特定の LUN のトラフィックを必要な作業のみに制限し、FCP ポートの使用率を軽減します。...警告しきい値を超えた場合は、次のアクションを実行するように計画します。1.ポート使用率がより多くのポートに分散されるように、データトラフィックを処理するためにさらに多くの FCP ポートを構成します。2.ワークロードを、使用率の低い別の FCP ポートに移動します。3. ONTAP のQoS ポリシーまたはホスト側の構成を使用して、特定の LUN のトラフィックを必要な作業のみに制限し、FCP ポートの使用率を軽減します。</p>
---------------------------	-----------	---	--

Lunレイテンシ高	重大	<p>LUN は、データベースなどのパフォーマンスが重視されるアプリケーションによって実行されることが多い I/O トラフィックを処理するオブジェクトです。LUN のレイテンシが高い場合、アプリケーション自体に問題が発生し、タスクを実行できなくなる可能性があります。...警告アラートは、LUN を適切なノードまたはアグリゲートに移動するために計画されたアクションを実行する必要があります。...重大なアラートは、サービスの中断が差し迫っており、サービスの継続性を確保するために緊急措置を講じる必要があることを示します。メディアの種類に応じて予想されるレイテンシは次のとおりです - SSD 最大 1~2 ミリ秒、SAS 最大 8~10 ミリ秒、SATA HDD 17~20 ミリ秒</p>	<p>重大なしきい値を超えた場合は、サービスの中断を最小限に抑えるために次のアクションを検討してください。LUN またはそのボリュームに QoS ポリシーが関連付けられている場合は、そのしきい値制限を評価し、それが LUN ワークロードの調整を引き起こしているかどうかを検証します。...警告しきい値を超えた場合は、次のアクションを実行するように計画します。1.アグリゲートの使用率も高い場合は、LUN を別のアグリゲートに移動します。2.ノードの使用率も高い場合は、ボリュームを別のノードに移動する、またはノードの合計ワークロードを削減します。3. LUN またはそのボリュームに QoS ポリシーが関連付けられている場合は、そのしきい値制限を評価し、それが LUN ワークロードの調整を引き起こしているかどうかを検証します。</p>
-----------	----	---	--

<p>ネットワークポート使用率が高い</p>	<p>重大</p>	<p>ネットワークポートは、顧客のホストシステムとONTAPボリューム間のNFS、CIFS、およびiSCSIプロトコルトラフィックを受信および転送するために使用されます。ポートの使用率が高い場合、それがボトルネックとなり、最終的にはNFS、CIFS、iSCSIワークロードのパフォーマンスに影響します。...警告アラートは、ネットワークトラフィックを分散させるために計画されたアクションを実行する必要があることを示します。...重大なアラートは、サービスの中断が差し迫っており、サービスの継続性を確保するためにネットワークトラフィックを分散するための緊急措置を実行する必要があります。</p>	<p>重大なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、次の即時アクションを検討してください。1. ONTAPのQoSポリシーまたはホスト側の分析を使用して、特定のボリュームのトラフィックを必要な作業のみに制限し、ネットワークポートの使用率を下げます。2. 使用率の低い別のネットワークポートを使用するように1つ以上のボリュームを構成します。...警告しきい値を超えた場合は、次の即時アクションを検討してください。1. ポート使用率がより多くのポートに分散されるように、データトラフィックを処理するためにさらに多くのネットワークポートを構成します。2. 使用率の低い別のネットワークポートを使用するように1つ以上のボリュームを構成します。</p>
------------------------	-----------	--	--

<p>NVMe名前空間レイテンシ高</p>	<p>重大</p>	<p>NVMe 名前空間は、データベースなどのパフォーマンスが重視されるアプリケーションによって実行される I/O トラフィックを処理するオブジェクトです。NVMe 名前空間のレイテンシが高いと、アプリケーション自体に問題が発生し、タスクを完了できなくなる可能性があります。...警告アラートは、LUN を適切なノードまたはアグリゲートに移動するために計画されたアクションを実行する必要がありますを示します。...重大なアラートは、サービスの中断が差し迫っており、サービスの継続性を確保するために緊急措置を講じる必要があることを示します。</p>	<p>重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるための即時のアクションを検討してください。NVMe 名前空間またはそのボリュームに QoS ポリシーが割り当てられている場合は、その制限しきい値が NVMe 名前空間のワークロードの調整を引き起こしていないかどうか確認してください。...警告しきい値を超えた場合は、次のアクションを実行することを検討してください。1.アグリゲートの使用率も高い場合は、LUN を別のアグリゲートに移動します。2.ノードの使用率も高い場合は、ボリュームを別のノードに移動する、またはノードの合計ワークロードを削減します。3. NVMe 名前空間またはそのボリュームに QoS ポリシーが割り当てられている場合は、そのポリシーによって NVMe 名前空間のワークロードが調整される可能性がないか、その制限しきい値を評価します。</p>
-----------------------	-----------	---	--

QTree 容量がいっぱい	重大	<p>qtree は、ボリューム内のルート ディレクトリの特別なサブディレクトリとして存在できる、論理的に定義されたファイルシステムです。各 qtree には、デフォルトのスペース クォータまたはクォータ ポリシーによって定義されたクォータがあり、ボリューム容量内でツリーに保存されるデータの量を制限します。...警告アラートは、スペースを増やすために計画されたアクションを実行する必要があります。...重大なアラートは、サービスの中断が差し迫っており、サービスの継続性を確保するためにスペースを解放する緊急措置を実行する必要があります。</p>	<p>重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、直ちに次のアクションを検討してください。1.成長に対応するために qtree のスペースを増やします。2.不要なデータを削除してスペースを解放します。...警告しきい値を超えた場合は、次の即時措置を講じる計画を立ててください。1.成長に対応するために qtree のスペースを増やします。2.不要なデータを削除してスペースを解放します。</p>
QTree 容量のハード制限	重大	<p>qtree は、ボリューム内のルート ディレクトリの特別なサブディレクトリとして存在できる、論理的に定義されたファイルシステムです。各 qtree には、KB 単位で測定されるスペース クォータがあり、これを使用してデータを保存します。これにより、ボリューム内のユーザー データの増加を制御し、合計容量を超えないようにします。...qtree は、qtree の合計容量クォータ制限に達してデータを保存できなくなる前に、ユーザーに事前に警告するソフトストレージ容量クォータを維持します。qtree 内に保存されているデータの量を監視することで、ユーザーは中断のないデータ サービスを受けることができます。</p>	<p>重大なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、次の即時アクションを検討してください。1.成長に対応するために、ツリーのスペース割り当てを増やします 2.スペースを解放するためにツリー内の不要なデータを削除するようにユーザーに指示します</p>

QTree 容量ソフト制限	警告	<p>qtree は、ボリューム内のルート ディレクトリの特別なサブディレクトリとして存在できる、論理的に定義されたファイルシステムです。各 qtree には、KB 単位で測定されるスペース クォータがあり、これを使用してデータを保存することで、ユーザー データの増加を制御し、合計容量を超えないようにします。...qtree は、qtree の合計容量クォータ制限に達してデータを保存できなくなる前に、ユーザーに事前に警告するソフト ストレージ容量クォータを維持します。qtree 内に保存されているデータの量を監視することで、ユーザーは中断のないデータ サービスを受けることができます。</p>	<p>警告しきい値を超えた場合は、次の即時アクションを検討してください。1.成長に対応するためにツリーのスペース割り当てを増やします。2.スペースを解放するために、ツリー内の不要なデータを削除するようにユーザーに指示します。</p>
QTree ファイルのハード制限	重大	<p>qtree は、ボリューム内のルート ディレクトリの特別なサブディレクトリとして存在できる、論理的に定義されたファイルシステムです。各 qtree には、ボリューム内で管理可能なファイルシステムサイズを維持するために含めることができるファイル数のクォータがあります。...qtree は、ツリー内の新しいファイルが拒否されるハード ファイル数クォータを維持します。qtree 内のファイル数を監視することで、ユーザーは中断のないデータ サービスを受けることができます。</p>	<p>重要なしきい値を超えた場合は、サービス中断を最小限に抑えるために、直ちに次のアクションを検討してください。1. qtree のファイル数クォータを増やします。2. qtree ファイルシステムから不要なファイルを削除します。</p>

<p>QTree ファイルのソフト制限</p>	<p>警告</p>	<p>qtree は、ボリューム内のルート ディレクトリの特 別なサブディレクトリと して存在できる、論理的 に定義されたファイルシ ステムです。各 qtree に は、ボリューム内で管理 可能なファイル システム サイズを維持するため に、格納できるファイル 数のクォータがありま す。...qtree は、qtree 内 のファイル制限に達して 追加のファイルを保存で きなくなる前に、ユーザ ーに事前に警告するた めにソフト ファイル数ク ォータを維持します。qtree 内のファイル数を監視す ることで、ユーザーは中 断のないデータ サービス を受けることができま す。</p>	<p>警告しきい値を超えた場 合は、次の即時措置を講 じる計画を立ててくださ い。1. qtree のファイル数 クォータを増やしま す。2. qtree ファイルシ ステムから不要なファイ ルを削除します。</p>
-------------------------	-----------	---	--

<p>スナップショット予約領域がいっぱいです</p>	<p>重大</p>	<p>アプリケーションと顧客データを保存するには、ボリュームのストレージ容量が必要です。スナップショット予約領域と呼ばれるその領域の一部は、データをローカルで保護できるようにするスナップショットを保存するために使用されます。ONTAPボリュームに保存される新規データや更新データが増えるほど、使用されるスナップショット容量が増え、将来の新規データや更新データに使用できるスナップショットストレージ容量は少なくなります。ボリューム内のスナップショットデータ容量が合計スナップショット予約領域に達すると、新しいスナップショットデータを保存できなくなり、ボリューム内のデータの保護レベルが低下する可能性があります。ボリュームの使用済みスナップショット容量を監視することで、データサービスの継続性が確保されます。</p>	<p>重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、直ちに次のアクションを検討してください。1.スナップショット予約がいっぱいになったときにボリューム内のデータ領域を使用するようにスナップショットを構成します。2.古くて不要なスナップショットをいくつか削除して、スペースを解放します。...警告しきい値を超えた場合は、次の即時措置を講じる計画を立ててください。1.成長に対応するために、ボリューム内のスナップショット予約領域を増やします。2.スナップショット予約がいっぱいになったときにボリューム内のデータ領域を使用するようにスナップショットを構成します。</p>
----------------------------	-----------	--	---

ストレージ容量制限	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 操作が遅くなり、最終的には停止して、ストレージ停止インシデントが発生します。警告アラートは、最小限の空き領域を回復するために計画されたアクションをすぐに実行する必要があることを示します。重大なアラートは、サービスが中断が差し迫っており、サービスの継続性を確保するためにスペースを解放するための緊急措置を講じる必要があることを示します。</p>	<p>重大なしきい値を超えた場合は、サービスが中断を最小限に抑えるために、直ちに次のアクションを検討してください。1.重要でないボリューム上のスナップショットを削除します。2.重要でないワークロードであり、オフストレージ コピーから復元できる可能性のあるボリュームまたは LUN を削除します。.....警告しきい値を超えた場合は、次の即時アクションを計画してください。1. 1 つ以上のボリュームを別の保存場所に移動します。2.ストレージ容量を追加します。3.ストレージ効率設定を変更するか、非アクティブなデータをクラウドストレージに階層化します。</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限界に達すると、操作が遅くなり、待ち時間が増加し、ワークロードとアプリケーションに障害が発生する可能性があります。ONTAP は、ワークロードのストレージ プールの使用率を評価し、消費されたパフォーマンスの割合を推定します。...警告アラートは、ワークロードのピークに対応するために十分なストレージ プール パフォーマンスを確保するために、ストレージ プールの負荷を軽減するための計画的なアクションを実行する必要があることを示します。...重大なアラートは、パフォーマンスの低下が差し迫っており、サービスの継続性を確保するためにストレージ プールの負荷を軽減するための緊急措置を実行する必要があることを示します。</p>	<p>重大なしきい値を超えた場合は、サービスが中断を最小限に抑えるために、次の即時アクションを検討してください。1. スナップショットやSnapMirrorレプリケーションなどのスケジュールされたタスクを一時停止します。2.重要でないワークロードをアイドル状態にします。...警告しきい値を超えた場合は、直ちに次の措置を講じてください。1. 1 つ以上のワークロードを別のストレージの場所に移動します。2.ストレージ ノード (AFF) またはディスク シェルフ (FAS) を追加し、ワークロードを再分配します 3.ワークロード特性 (ブロック サイズ、アプリケーション キャッシュ) を変更します。</p>

<p>ユーザークォータ容量のハード制限</p>	<p>重大</p>	<p>ONTAP は、ボリューム、ボリューム内のファイル、またはディレクトリにアクセスする権限を持つ Unix または Windows システムのユーザーを認識します。その結果、ONTAP を使用すると、顧客は Linux または Windows システムのユーザーまたはユーザーグループのストレージ容量を構成できるようになります。ユーザーまたはグループポリシークォータは、ユーザーが自身のデータに利用できるスペースの量を制限します。... このクォータのハード制限により、ボリューム内で使用されている容量が合計容量クォータに達する直前にユーザーに通知することができます。ユーザーまたはグループのクォータ内に保存されるデータの量を監視することで、ユーザーが中断のないデータ サービスを受けられるようになります。</p>	<p>重大なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、次の即時アクションを検討してください。1. 成長に対応するために、ユーザーまたはグループのクォータのスペースを増やします。2. 不要なデータを削除してスペースを解放するようにユーザーまたはグループに指示します。</p>
-------------------------	-----------	---	--

<p>ユーザークォータ容量ソフト制限</p>	<p>警告</p>	<p>ONTAP は、ボリューム、ボリューム内のファイル、またはディレクトリにアクセスする権限を持つ Unix または Windows システムのユーザーを認識します。その結果、ONTAP を使用すると、顧客は Linux または Windows システムのユーザーまたはユーザーグループのストレージ容量を構成できるようになります。ユーザーまたはグループポリシークォータは、ユーザーが自身のデータに利用できるスペースの量を制限します。... このクォータのソフト制限により、ボリューム内で使用されている容量が合計容量クォータに達したときに、ユーザーにプロアクティブに通知することができます。ユーザーまたはグループのクォータ内に保存されるデータの量を監視することで、ユーザーが中断のないデータサービスを受けられるようになります。</p>	<p>警告しきい値を超えた場合は、次の即時措置を講じる計画を立ててください。1.成長に対応するために、ユーザーまたはグループのクォータのスペースを増やします。2.不要なデータを削除してスペースを解放します。</p>
------------------------	-----------	---	---

<p>ボリューム容量がいっぱいです</p>	<p>重大</p>	<p>アプリケーションと顧客データを保存するには、ボリュームのストレージ容量が必要です。ONTAPボリュームに保存されるデータが増えるほど、将来のデータのストレージ可用性は低下します。ボリューム内のデータ保存容量が合計保存容量に達した場合、保存容量不足によりお客様がデータを保存できなくなる可能性があります。使用されたボリュームのストレージ容量を監視することで、データサービスの継続性が確保されます。</p>	<p>重大なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、次の即時アクションを検討してください。1. 成長に対応するためにボリュームのスペースを増やします。2. 不要なデータを削除してスペースを解放します。3. スナップショットのコピーがスナップショットリザーブよりも多くのスペースを占有している場合は、古いスナップショットを削除するか、ボリュームスナップショットの自動削除を有効にします。...警告しきい値を超えた場合は、次の即時アクションを実行するように計画してください。1. 成長に対応するためにボリュームのスペースを増やします 2. スナップショットのコピーがスナップショットリザーブよりも多くのスペースを占有する場合は、古いスナップショットを削除するか、ボリュームスナップショットの自動削除を有効にします。.....</p>
-----------------------	-----------	--	---

<p>ボリュームのiノード制限</p>	<p>重大</p>	<p>ファイルを保存するボリュームは、インデックスノード (inode) を使用してファイルのメタデータを保存します。ボリュームの inode 割り当てを使い果たすと、それ以上ファイルを追加できなくなります。...警告アラートは、使用可能な inode の数を増やすために計画されたアクションを実行する必要がありますを示します。...重大なアラートは、ファイル制限の使い果たしが差し迫っており、サービスの継続性を確保するために inode を解放する緊急措置を講じる必要があることを示します。</p>	<p>重大なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、次の即時アクションを検討してください。1. ボリュームの inode 値を増やします。inode 値がすでに最大値に達している場合は、ファイルシステムが最大サイズを超えているため、ボリュームを2つ以上のボリュームに分割します。2. FlexGroupを使用すると、大規模なファイルシステムに対応しやすくなります。警告しきい値を超えた場合は、次の即時措置を講じる計画を立ててください。1.ボリュームの inode 値を増やします。inode 値がすでに最大値に達している場合は、ファイルシステムが最大サイズを超えているため、ボリュームを2つ以上のボリュームに分割します。2. FlexGroupを使用すると、大規模なファイルシステムに対応できません。</p>
---------------------	-----------	--	---

<p>ボリュームレイテンシー 高</p>	<p>重大</p>	<p>ボリュームは、devOps アプリケーション、ホームディレクトリ、データベースなどのパフォーマンスが重視されるアプリケーションによって実行されることが多い I/O トラフィックを処理するオブジェクトです。大量の待ち時間が発生すると、アプリケーション自体に問題が発生し、タスクを完了できなくなる可能性があります。アプリケーションの一貫したパフォーマンスを維持するためには、ボリュームのレイテンシーを監視することが重要です。メディアタイプに基づいて予想されるレイテンシーは次のとおりです - SSD 最大 1 ~ 2 ミリ秒、SAS 最大 8 ~ 10 ミリ秒、SATA HDD 17 ~ 20 ミリ秒。</p>	<p>重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、次の即時アクションを検討してください。ボリュームに QoS ポリシーが割り当てられている場合は、ボリュームのワークロードが調整される原因となっていないか、その制限しきい値を評価します。...警告しきい値を超えた場合は、次の即時アクションを検討してください。1.アグリゲートの使用率も高い場合は、ボリュームを別のアグリゲートに移動します。2. ボリュームに QoS ポリシーが割り当てられている場合は、ボリュームのワークロードが調整される原因にならないように、その制限しきい値を評価します。3.ノードの使用率も高い場合は、ボリュームを別のノードに移動する、またはノードの合計ワークロードを削減します。</p>
<p>モニター名</p>	<p>重大度</p>	<p>モニターの説明</p>	<p>対処方法</p>

<p>ノードの高レイテンシ</p>	<p>警告/重大</p>	<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を及ぼす可能性があるレベルに達しました。ノードのレイテンシが低い場合、アプリケーションの一貫したパフォーマンスが保証されます。メディアタイプに基づいて予想されるレイテンシは、SSDで最大1～2ミリ秒、SASで最大8～10ミリ秒、SATA HDDで17～20ミリ秒です。</p>	<p>重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、直ちに措置を講じる必要があります。1.スケジュールされたタスク、スナップショット、またはSnapMirrorレプリケーションを一時停止します 2. QoS 制限 3 を介して、優先度の低いワークロードの需要を下げます。重要でないワークロードを非アクティブ化します。警告しきい値を超えた場合は、直ちに次のアクションを検討してください。1. 1つ以上のワークロードを別のストレージの場所に移動します 2. QoS 制限 3 を介して、優先度の低いワークロードの需要を下げます。ストレージ ノード (AFF) またはディスク シェルフ (FAS) を追加し、ワークロードを再分配します 4. ワークロード特性の変更 (ブロックサイズ、アプリケーションキャッシュなど)</p>
-------------------	--------------	--	---

<p>ノードパフォーマンス制限</p>	<p>警告/重大</p>	<p>ノードのパフォーマンス使用率が、ノードでサポートされている IO およびアプリケーションのパフォーマンスに影響を及ぼす可能性があるレベルに達しました。ノードのパフォーマンス使用率が低いため、アプリケーションのパフォーマンスが一貫して確保されます。</p>	<p>重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、直ちに措置を講じる必要があります。1.スケジュールされたタスク、スナップショット、またはSnapMirrorレプリケーションを一時停止します 2. QoS 制限 3 を介して、優先度の低いワークロードの需要を下げます。重要でないワークロードを非アクティブ化します。警告しきい値を超えた場合は、次のアクションを検討してください。1. 1つ以上のワークロードを別のストレージの場所に移動します 2. QoS 制限 3 を介して、優先度の低いワークロードの需要を下げます。ストレージ ノード (AFF) またはディスク シェルフ (FAS) を追加し、ワークロードを再分配します 4. ワークロード特性の変更 (ブロックサイズ、アプリケーションキャッシュなど)</p>
---------------------	--------------	--	--

<p>ストレージVMの高レイテンシ</p>	<p>警告/重大</p>	<p>ストレージ VM (SVM) のレイテンシが、ストレージ VM 上のアプリケーションのパフォーマンスに影響を及ぼす可能性があります。ストレージ VM のレイテンシが低いため、アプリケーションの一貫したパフォーマンスが保証されます。メディア タイプに基づいて予想されるレイテンシは、SSD で最大 1 ~ 2 ミリ秒、SAS で最大 8 ~ 10 ミリ秒、SATA HDD で 17 ~ 20 ミリ秒です。</p>	<p>重大なしきい値を超えた場合は、QoS ポリシーが割り当てられたストレージ VM のボリュームのしきい値制限を直ちに評価し、ボリューム ワークロードの調整の原因になっているかどうかを確認します。警告しきい値を超えた場合は、次の即時アクションを検討してください。1.アグリゲートの使用率も高い場合は、ストレージ VM の一部のボリュームを別のアグリゲートに移動します。2. QoS ポリシーが割り当てられたストレージ VM のボリュームについては、しきい値制限によってボリューム ワークロードが調整されるかどうかを評価します 3. ノードの使用率が高い場合は、ストレージVMの一部のボリュームを別のノードに移動する、またはノードの全体的なワークロードを削減します。</p>
<p>ユーザークォータファイルハード制限</p>	<p>重大</p>	<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、追加のファイルを作成できません。保存されているファイルの数を監視することで、ユーザーは中断のないデータ サービスを受けることができます。</p>	<p>重大なしきい値を超えた場合は、サービスの中断を最小限に抑えるために即時の措置が必要です。...次の措置を検討してください。1.特定のユーザー 2 のファイル数クォータを増やします。不要なファイルを削除して、特定のユーザーのファイルクォータの負担を軽減します。</p>

<p>ユーザークォータファイルソフト制限</p>	<p>警告</p>	<p>ボリューム内に作成されたファイルの数がクォータのしきい値制限に達しており、重大な制限に近づいています。クォータが重大な制限に達した場合、追加のファイルを作成することはできません。ユーザーが保存するファイルの数を監視することで、ユーザーが中断のないデータ サービスを受けられるようになります。</p>	<p>警告しきい値を超えた場合は、直ちにアクションを検討してください。1. 特定のユーザー クォータ 2 のファイル数クォータを増やします。不要なファイルを削除して、特定のユーザーのファイルクォータの負担を軽減します。</p>
<p>ボリュームキャッシュミスマス率</p>	<p>警告/重大</p>	<p>ボリューム キャッシュ ミスマス率は、クライアント アプリケーションからの読み取り要求のうち、キャッシュから返されるのではなくディスクから返される要求の割合です。これは、音量が設定されたしきい値に達したことを意味します。</p>	<p>重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、直ちに措置を講じる必要があります。1. IO 負荷 2 を軽減するために、一部のワークロードをボリュームのノードから移動します。ボリュームのノードにまだない場合は、Flash Cache 3 を購入して追加し、WAFL キャッシュを増やします。QoS 制限を使用して、同じノード上の優先度の低いワークロードの需要を下げます。警告しきい値を超えた場合は、直ちに次のアクションを検討してください。1. IO 負荷 2 を軽減するために、一部のワークロードをボリュームのノードから移動します。ボリュームのノードにまだない場合は、Flash Cache 3 を購入して追加し、WAFL キャッシュを増やします。QoS 制限 4 を使用して、同じノード上の優先度の低いワークロードの需要を下げます。ワークロード特性の変更（ブロックサイズ、アプリケーションキャッシュなど）</p>

<p>ボリューム Qtree クォータ オーバーコミット</p>	<p>警告/重大</p>	<p>ボリューム qtree クォータ オーバーコミットは、ボリュームが qtree クォータによってオーバーコミットされていると見なされるパーセンテージを指定します。ボリュームの qtree クォータに設定されたしきい値に達しました。ボリューム qtree クォータのオーバーコミットを監視することで、ユーザーは中断のないデータ サービスを受けることができます。</p>	<p>重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、直ちに措置を講じる必要があります。1.ボリューム2のスペースを増やします。不要なデータを削除します。警告しきい値を超えた場合は、ボリュームのスペースを増やすことを検討してください。</p>
----------------------------------	--------------	--	---

[トップに戻る](#)

ログモニター

モニター名	重大度	説明	対処方法
<p>AWS 認証情報が初期化されていません</p>	<p>情報</p>	<p>このイベントは、モジュールがクラウド資格情報スレッドから Amazon Web Services (AWS) Identity and Access Management (IAM) ロールベースの資格情報にアクセスしようとしたときに、資格情報が初期化される前に発生します。</p>	<p>クラウド資格情報スレッドとシステムの初期化が完了するまで待ちます。</p>

クラウド層にアクセスできません	重大	ストレージ ノードは Cloud Tier オブジェクトストア API に接続できません。一部のデータにアクセスできなくなります。	オンプレミス製品を使用している場合は、次の修正アクションを実行してください。...「network interface show」コマンドを使用して、クラスタ間 LIF がオンラインで機能していることを確認します。...宛先ノードのクラスタ間 LIF で「ping」コマンドを使用して、オブジェクトストア サーバへのネットワーク接続を確認します。...次の点を確認してください。...オブジェクトストアの構成が変更されていないこと。...ログインおよび接続情報がまだ有効であること。...問題が解決しない場合は、NetAppテクニカル サポートにお問い合わせください。Cloud Volumes ONTAPを使用する場合は、次の修正アクションを実行します。...オブジェクトストアの構成が変更されていないことを確認します。...ログインおよび接続情報がまだ有効であることを確認してください。問題が解決しない場合は、NetAppテクニカル サポートにお問い合わせください。
ディスクが使用不可	情報	このイベントは、ディスクが障害としてマークされた、サニタイズされている、またはメンテナンス センターに入ったためにサービスから削除されたときに発生します。	なし。

FlexGroup構成員全員	重大	FlexGroupボリューム内の構成要素がいっぱいなので、サービスが中断される可能性があります。FlexGroupボリューム上でファイルを作成または拡張することは可能です。ただし、構成要素に保存されているファイルは変更できません。その結果、FlexGroupボリュームで書き込み操作を実行しようとする、ランダムに領域不足エラーが発生する可能性があります。	「volume modify -files +X」コマンドを使用して、FlexGroupボリュームに容量を追加することをお勧めします。または、FlexGroupボリュームからファイルを削除します。ただし、どのファイルが構成要素に到達したかを判断するのは困難です。
Flexgroupの構成員がほぼ満員	警告	FlexGroupボリューム内の構成要素のスペースがほとんど不足しており、サービスが中断される可能性があります。ファイルの作成と展開が可能です。ただし、構成要素のスペースが不足すると、構成要素上のファイルに追加したり変更したりできなくなる可能性があります。	「volume modify -files +X」コマンドを使用して、FlexGroupボリュームに容量を追加することをお勧めします。または、FlexGroupボリュームからファイルを削除します。ただし、どのファイルが構成要素に到達したかを判断するのは困難です。
FlexGroup構成要素のinode がほぼ不足しています	警告	FlexGroupボリューム内の構成要素のinode がほとんど不足しているため、サービスが中断される可能性があります。構成要素は平均よりも少ない作成要求を受け取ります。要求はより多くのinodeを持つ構成要素にルーティングされるため、FlexGroupボリュームの全体的なパフォーマンスに影響する可能性があります。	「volume modify -files +X」コマンドを使用して、FlexGroupボリュームに容量を追加することをお勧めします。または、FlexGroupボリュームからファイルを削除します。ただし、どのファイルが構成要素に到達したかを判断するのは困難です。

FlexGroup構成要素のinode 不足	重大	FlexGroupボリュームの構成要素の inode が不足しており、サービスが中断される可能性があります。この構成要素に新しいファイルを作成することはできません。これにより、FlexGroupボリューム全体でコンテンツの配分が全体的に不均衡になる可能性があります。	「volume modify -files +X」コマンドを使用して、FlexGroupボリュームに容量を追加することをお勧めします。または、FlexGroupボリュームからファイルを削除します。ただし、どのファイルが構成要素に到達したかを判断するのは困難です。
LUN はオフライン	情報	このイベントは、LUN が手動でオフラインになったときに発生します。	LUN をオンラインに戻します。
本体ファンの故障	警告	メインユニットの1つ以上のファンが故障しました。システムは引き続き動作します。...ただし、この状態が長時間続くと、過熱により自動シャットダウンがトリガーされる可能性があります。	故障したファンを取り付け直してください。エラーが解決しない場合は交換してください。
本体ファンが警告状態	情報	このイベントは、メインユニットの1つ以上のファンが警告状態にある場合に発生します。	過熱を防ぐため、指定されたファンを交換してください。
NVRAM バッテリ低下	警告	NVRAMバッテリー容量が極めて低くなっています。バッテリーが切れると、データが失われる可能性があります。...システムは、AutoSupportまたは「コール ホーム」メッセージを生成し、NetAppテクニカル サポートおよび設定された送信先（そのように設定されている場合は）に送信します。AutoSupportメッセージが正常に配信されると、問題の特定と解決が大幅に改善されます。	次の修正アクションを実行してください。... 「system node environment sensors show」コマンドを使用して、バッテリーの現在のステータス、容量、充電状態を表示します。...バッテリーを最近交換した場合、またはシステムが長期間動作していなかった場合は、バッテリーを監視して、適切に充電されていることを確認します。...バッテリーのランタイムが引き続き危険なレベルを下回り、ストレージシステムが自動的にシャットダウンする場合は、NetAppテクニカルサポートに問い合わせてください。

サービス プロセッサが未設定	警告	このイベントは毎週発生し、サービス プロセッサ (SP) を構成するよう通知します。SP は、リモート アクセスおよびリモート管理機能を提供するためにシステムに組み込まれる物理デバイスです。SP のすべての機能を使用するには、SP を構成する必要があります。	次の修正アクションを実行します。... 「system service-processor network modify」 コマンドを使用して SP を設定します。... オプションで、「system service-processor network show」 コマンドを使用して SP の MAC アドレスを取得します。... 「system service-processor network show」 コマンドを使用して SP ネットワーク設定を確認します。... 「system service-processor autosupport invoke」 コマンドを使用して SP が AutoSupport 電子メールを送信できることを確認します。注: このコマンドを発行する前に、ONTAP で AutoSupport 電子メール ホストと受信者を設定する必要があります。
サービス プロセッサはオフライン	重大	すべての SP リカバリアクションが実行されたにもかかわらず、ONTAP はサービス プロセッサ (SP) からハートビートを受信しなくなりました。ONTAP は SP なしではハードウェアの状態を監視できません。... ハードウェアの損傷とデータ損失を防ぐためにシステムはシャットダウンします。SP がオフラインになった場合に直ちに通知されるパニックアラートを設定します。	次の操作を実行して、システムの電源を入れ直します。... コントローラをシャーシから引き出します。... コントローラを押し込みます。... コントローラの電源を入れ直します。... 問題が解決しない場合は、コントローラ モジュールを交換します。

棚ファンが故障しました	重大	シェルフの指定された冷却ファンまたはファン モジュールに障害が発生しました。シェルフ内のディスクに十分な冷却気流が供給されず、ディスク障害が発生する可能性があります。	次の修正アクションを実行します。...ファン モジュールが完全に装着され、固定されていることを確認します。注:一部のディスクシェルフでは、ファンは電源モジュールに統合されています。...問題が解決しない場合は、ファン モジュールを交換してください。...それでも問題が解決しない場合は、NetAppテクニカル サポートにお問い合わせください。
本体ファンの故障によりシステムが動作不能	重大	1つ以上のメインユニットファンが故障し、システムの動作が中断されました。これにより、データが失われる可能性があります。	故障したファンを交換してください。
未割り当てのディスク	情報	システムには未割り当てのディスクがあり、容量が無駄になっており、システムに誤った構成や部分的な構成変更が適用されている可能性があります。	次の修正アクションを実行します。...「disk show -n」コマンドを使用して、割り当てられていないディスクを特定します。...「disk assign」コマンドを使用して、ディスクをシステムに割り当てます。
ウイルス対策サーバーがビジー状態です	警告	ウイルス対策サーバーがビジー状態のため、新しいスキャン要求を受け入れることができません。	このメッセージが頻繁に発生する場合は、SVM によって生成されるウイルス スキャン負荷を処理できる十分なウイルス対策サーバーがあることを確認してください。

IAM ロールの AWS 認証情報が期限切れです	重大	Cloud Volume ONTAPにアクセスできなくなりました。Identity and Access Management (IAM) のロールベースの認証情報の有効期限が切れました。認証情報は、IAM ロールを使用して Amazon Web Services (AWS) メタデータ サーバーから取得され、Amazon Simple Storage Service (Amazon S3) への API リクエストに署名するために使用されます。	以下の手順を実行します。...AWS EC2 マネジメントコンソールにログインします。...[インスタンス] ページに移動します。... Cloud Volumes ONTAPデプロイメントのインスタンスを見つけて、そのヘルスを確認します。...インスタンスに関連付けられた AWS IAM ロールが有効であり、インスタンスに対する適切な権限が付与されていることを確認します。
IAM ロールの AWS 認証情報が見つかりません	重大	クラウド資格情報スレッドは、AWS メタデータ サーバーから Amazon Web Services (AWS) Identity and Access Management (IAM) ロールベースの資格情報を取得できません。認証情報は、Amazon Simple Storage Service (Amazon S3) への API リクエストに署名するために使用されます。Cloud Volume ONTAPにアクセスできなくなりました。...	以下の手順を実行します。...AWS EC2 マネジメントコンソールにログインします。...[インスタンス] ページに移動します。... Cloud Volumes ONTAPデプロイメントのインスタンスを見つけて、そのヘルスを確認します。...インスタンスに関連付けられた AWS IAM ロールが有効であり、インスタンスに対する適切な権限が付与されていることを確認します。
IAM ロールの AWS 認証情報が無効です	重大	Identity and Access Management (IAM) のロールベースの認証情報が無効です。認証情報は、IAM ロールを使用して Amazon Web Services (AWS) メタデータ サーバーから取得され、Amazon Simple Storage Service (Amazon S3) への API リクエストに署名するために使用されます。Cloud Volume ONTAPにアクセスできなくなりました。	以下の手順を実行します。...AWS EC2 マネジメントコンソールにログインします。...[インスタンス] ページに移動します。... Cloud Volumes ONTAPデプロイメントのインスタンスを見つけて、そのヘルスを確認します。...インスタンスに関連付けられた AWS IAM ロールが有効であり、インスタンスに対する適切な権限が付与されていることを確認します。

AWS IAM ロールが見つかりません	重大	Identity and Access Management (IAM) ロール スレッドは、AWS メタデータ サーバーで Amazon Web Services (AWS) IAM ロールを見つけることができません。Amazon Simple Storage Service (Amazon S3) への API リクエストに署名するために使用されるロールベースの認証情報を取得するには、IAM ロールが必要です。Cloud Volume ONTAPにアクセスできなくなりました。...	次の操作を実行します。...AWS EC2 マネジメントコンソールにログインします。...[インスタンス] ページに移動します。... Cloud Volumes ONTAPデプロイメントのインスタンスを見つけて、その正常性を確認します。...インスタンスに関連付けられた AWS IAM ロールが有効であることを確認します。
AWS IAM ロールが無効です	重大	AWS メタデータ サーバーの Amazon Web Services (AWS) Identity and Access Management (IAM) ロールが無効です。Cloud Volume ONTAPにアクセスできなくなりました。	以下の手順を実行します。...AWS EC2 マネジメントコンソールにログインします。...[インスタンス] ページに移動します。... Cloud Volumes ONTAPデプロイメントのインスタンスを見つけて、そのヘルスを確認します。...インスタンスに関連付けられた AWS IAM ロールが有効であり、インスタンスに対する適切な権限が付与されていることを確認します。
AWS メタデータサーバーの接続失敗	重大	Identity and Access Management (IAM) ロール スレッドは、Amazon Web Services (AWS) メタデータ サーバーとの通信リンクを確立できません。Amazon Simple Storage Service (Amazon S3) への API リクエストに署名するために使用される必要な AWS IAM ロールベースの認証情報を取得するための通信を確立する必要があります。Cloud Volume ONTAPにアクセスできなくなりました。...	以下の手順を実行します。...AWS EC2 マネジメントコンソールにログインします。...[インスタンス] ページに移動します。... Cloud Volumes ONTAPデプロイメントのインスタンスを見つけて、そのヘルスを確認します。...

FabricPool のスペース使用制限にほぼ達しました	警告	容量ライセンス プロバイダーからのオブジェクトストアのクラスター全体のFabricPoolスペース使用量の合計が、ライセンス制限にほぼ達しています。	次の修正アクションを行います。... 「storage aggregate object-store show-space」コマンドを使用して、各FabricPoolストレージ層で使用されているライセンス容量の割合を確認します。... 「volume snapshot delete」コマンドを使用して、階層化ポリシーが「snapshot」または「backup」であるボリュームから Snapshot コピーを削除し、スペースを解放します。... クラスターに新しいライセンスをインストールして、ライセンス容量を増やします。
FabricPool のスペース使用制限に達しました	重大	容量ライセンス プロバイダーからのオブジェクトストアのクラスター全体のFabricPoolスペース使用量の合計がライセンス制限に達しました。	次の修正アクションを行います。... 「storage aggregate object-store show-space」コマンドを使用して、各FabricPoolストレージ層で使用されているライセンス容量の割合を確認します。... 「volume snapshot delete」コマンドを使用して、階層化ポリシーが「snapshot」または「backup」であるボリュームから Snapshot コピーを削除し、スペースを解放します。... クラスターに新しいライセンスをインストールして、ライセンス容量を増やします。

<p>集計のギブバックに失敗しました</p>	<p>重大</p>	<p>このイベントは、ストレージ フェイルオーバー (SFO) ギブバックの一環としてアグリゲートを移行しているときに、宛先ノードがオブジェクトストアに到達できない場合に発生します。</p>	<p>次の修正アクションを実行します。... 「network interface show」 コマンドを使用して、クラスタ間 LIF がオンラインで機能していることを確認します。...宛先ノードのクラスタ間 LIF で「ping」 コマンドを使用して、オブジェクト ストア サーバへのネットワーク接続を確認します。... 「aggregate object-store config show」 コマンドを使用して、オブジェクト ストアの構成が変更されておらず、ログインおよび接続情報が正確であることを確認してください。... または、giveback コマンドの「require-partner-waiting」パラメータに false を指定してエラーを無効にすることもできます。... 詳細またはサポートについては、NetApp テクニカル サポートにお問い合わせください。</p>
------------------------	-----------	---	---

HA相互接続ダウン	警告	<p>高可用性 (HA) 相互接続がダウンしています。フェイルオーバーが利用できない場合、サービス停止のリスクがあります。</p>	<p>修正アクションは、プラットフォームでサポートされている HA 相互接続リンクの数とタイプ、および相互接続がダウンしている理由によって異なります。リンクがダウンしている場合: HA ペアの両方のコントローラが動作していることを確認します。外部接続リンクの場合は、相互接続ケーブルが正しく接続されていること、および該当する場合は Small Form-Factor Pluggable (SFP) が両方のコントローラに正しく装着されていることを確認します。内部接続リンクの場合は、「ic link off」コマンドと「ic link on」コマンドを使用して、リンクを順番に無効にしてから再度有効にします。...リンクが無効になっている場合は、「ic link on」コマンドを使用してリンクを有効にします。...ピアが接続されていない場合は、「ic link off」コマンドと「ic link on」コマンドを使用して、リンクを順番に無効にしてから再度有効にします。...問題が解決しない場合は、NetAppテクニカルサポートにお問い合わせください。</p>
-----------	----	---	---

<p>ユーザーあたりの最大セッション数を超過しました</p>	<p>警告</p>	<p>TCP 接続でユーザーごとに許可されるセッションの最大数を超過しました。いくつかのセッションが解放されるまで、セッションを確立する要求はすべて拒否されます。...</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。...クライアントを再起動します。...問題の原因が新しいアプリケーションか既存のアプリケーションかを確認します。...アプリケーションが新しい場合は、「cifs option modify -max-opens-same-file-per-tree」コマンドを使用して、クライアントのしきい値を高く設定します。場合によっては、クライアントは期待どおりに動作しますが、より高いしきい値が必要になります。クライアントに対してより高いしきい値を設定するには、高度な権限が必要です。...問題が既存のアプリケーションによって発生している場合は、クライアントに問題がある可能性があります。詳細情報やサポートについては、NetAppテクニカル サポートにお問い合わせください。</p>
--------------------------------	-----------	--	---

<p>ファイルあたりの最大オープン回数を超過しました</p>	<p>警告</p>	<p>TCP 接続経由でファイルを開くことができる最大回数を超過しました。ファイルの開いているインスタンスをいくつか閉じるまで、このファイルを開く要求はすべて拒否されます。これは通常、異常なアプリケーションの動作を示します。...</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るアプリケーションを検査します。クライアント上で実行されているアプリケーションが原因で、クライアントが正しく動作していない可能性があります。...クライアントを再起動してください。...問題の原因が新しいアプリケーションか既存のアプリケーションかを確認してください。...アプリケーションが新しい場合は、「cifs option modify -max-opens -same-file-per-tree」コマンドを使用して、クライアントのしきい値を高く設定してください。場合によっては、クライアントは期待どおりに動作しますが、より高いしきい値が必要になります。クライアントに対してより高いしきい値を設定するには、高度な権限が必要です。...問題が既存のアプリケーションによって発生している場合は、クライアントに問題がある可能性があります。詳細情報やサポートについては、NetAppテクニカルサポートにお問い合わせください。</p>
--------------------------------	-----------	---	---

NetBIOS名の競合	重大	<p>NetBIOS ネーム サービスは、リモート マシンからの名前登録要求に対する否定応答を受信しました。これは通常、NetBIOS 名またはエイリアスの競合によって発生します。その結果、クライアントはデータにアクセスできないか、クラスター内の適切なデータ提供ノードに接続できない可能性があります。</p>	<p>次のいずれかの修正処置を実行してください。...NetBIOS 名またはエイリアスに競合がある場合は、次のいずれかを実行してください。... 「vserver cifs delete -aliases alias -vserver vserver」コマンドを使用して、重複した NetBIOS エイリアスを削除します。... 「vserver cifs create -aliases alias -vserver vserver」コマンドを使用して、重複した名前を削除し、新しい名前のエイリアスを追加することで、NetBIOS エイリアスの名前を変更します。...エイリアスが設定されておらず、NetBIOS 名が競合している場合は、「vserver cifs delete -vserver vserver」および「vserver cifs create -cifs-server netbiosname」コマンドを使用して CIFS サーバの名前を変更します。注意: CIFS サーバを削除すると、データにアクセスできなくなる可能性があります。...NetBIOS 名を削除するか、リモートマシン上の NetBIOS の名前を変更します。</p>
NFSv4 ストア プールが枯渇しました	重大	<p>NFSv4 ストア プールが使い果たされました。</p>	<p>このイベント後、NFS サーバが 10 分以上応答しない場合は、NetAppテクニカル サポートにお問い合わせください。</p>

登録済みのスキャンエンジンがありません	重大	ウイルス対策コネクタは、登録済みのスキャンエンジンがないことをONTAPに通知しました。「スキャン必須」オプションが有効になっている場合、データが利用できなくなる可能性があります。	次の修正アクションを実行します。...ウイルス対策サーバにインストールされているスキャンエンジンソフトウェアがONTAPと互換性があることを確認します。...スキャンエンジンソフトウェアが実行されており、ローカルループバックを介してウイルス対策コネクタに接続するように設定されていることを確認します。
Vscan接続なし	重大	ONTAPには、ウイルススキャン要求を処理するためのVscan接続がありません。「スキャン必須」オプションが有効になっている場合、データが利用できなくなる可能性があります。	スキャナプールが適切に設定されており、ウイルス対策サーバがアクティブでONTAPに接続されていることを確認します。
ノードルートボリュームの空き容量が少ない	重大	システムはルートボリュームの空き容量が危険なほど少ないことを検出しました。ノードは完全に動作していません。データLIFがクラスター内でフェイルオーバーした可能性があります。そのため、ノード上のNFSおよびCIFSアクセスが制限されています。管理機能は、ルートボリューム上のスペースをクリアするためのノードのローカル回復手順に制限されません。	次の修正アクションを実行してください。...古いスナップショットコピーを削除するか、/mrootディレクトリから不要になったファイルを削除するか、ルートボリュームの容量を拡張して、ルートボリュームのスペースを解放します。...コントローラを再起動します。...詳細またはサポートについては、NetAppテクニカルサポートにお問い合わせください。
管理者共有が存在しません	重大	Vscanの問題: クライアントが存在しない ONTAP_ADMIN\$共有に接続しようとして失敗しました。	指定されたSVM IDに対してVscanが有効になっていることを確認します。SVMでVscanを有効にすると、SVMに対してONTAP_ADMIN\$共有が自動的に作成されます。
NVMe名前空間のスペース不足	重大	スペース不足による書き込み失敗のため、NVMe名前空間がオフラインになりました。	ボリュームにスペースを追加し、「vserver nvme namespace modify」コマンドを使用してNVMe名前空間をオンラインにします。

NVMe-oF の猶予期間 - アクティブ	警告	このイベントは、NVMe over Fabrics (NVMe-oF) プロトコルが使用されており、ライセンスの猶予期間がアクティブな場合に毎日発生します。ライセンスの猶予期間が終了した後、NVMe-oF 機能にはライセンスが必要になります。ライセンスの猶予期間が終了すると、NVMe-oF 機能は無効になります。	営業担当者に連絡して NVMe-oF ライセンスを取得し、それをクラスターに追加するか、クラスターから NVMe-oF 構成のすべてのインスタンスを削除してください。
NVMe-oF の猶予期間 - 終了	警告	NVMe over Fabrics (NVMe-oF) ライセンスの猶予期間が終了し、NVMe-oF 機能が無効になっています。	営業担当者に連絡して NVMe-oF ライセンスを取得し、クラスターに追加してください。
NVMe-oF 猶予期間の開始	警告	ONTAP 9.5 ソフトウェアへのアップグレード中に、NVMe over Fabrics (NVMe-oF) 構成が検出されました。ライセンスの猶予期間が終了した後、NVMe-oF 機能にはライセンスが必要になります。	営業担当者に連絡して NVMe-oF ライセンスを取得し、クラスターに追加してください。
オブジェクトストアホストが解決できません	重大	オブジェクトストアサーバーのホスト名を IP アドレスに解決できません。オブジェクトストアクライアントは、IP アドレスを解決しないとオブジェクトストアサーバーと通信できません。その結果、データにアクセスできなくなる可能性があります。	DNS 構成をチェックして、ホスト名が IP アドレスで正しく設定されていることを確認します。

<p>オブジェクトストアのクラスタ間LIFがダウンしています</p>	<p>重大</p>	<p>オブジェクトストアクライアントは、オブジェクトストアサーバーと通信するための動作可能なLIFを見つけることができません。インタークラスタLIFが動作可能になるまで、ノードはオブジェクトストアクライアントトラフィックを許可しません。その結果、データにアクセスできなくなる可能性があります。</p>	<p>次の修正アクションを実行します。...「network interface show -role intercluster」コマンドを使用して、クラスタ間LIFのステータスを確認します。...クラスタ間LIFが正しく設定され、動作していることを確認します。...クラスタ間LIFが設定されていない場合は、「network interface create -role intercluster」コマンドを使用して追加します。</p>
<p>オブジェクトストアの署名の不一致</p>	<p>重大</p>	<p>オブジェクトストアサーバーに送信された要求署名が、クライアントによって計算された署名と一致しません。その結果、データにアクセスできなくなる可能性があります。</p>	<p>シークレットアクセスキーが正しく設定されていることを確認します。正しく設定されている場合は、NetAppテクニカルサポートにお問い合わせください。</p>
<p>READDIR タイムアウト</p>	<p>重大</p>	<p>READDIR ファイル操作が、WAFLで実行できるタイムアウトを超えました。これは、ディレクトリが非常に大きいか、またはディレクトリがまばらであるために発生する可能性があります。是正措置をお勧めします。</p>	<p>次の修正アクションを実行します。...次の「diag」権限ノードシェルCLIコマンドを使用して、READDIR ファイル操作の有効期限が切れた最近のディレクトリに固有の情報を検索します: wafll readdir notice show。...ディレクトリがスパースとして示されているかどうかを確認します。...ディレクトリがスパースとして示されている場合は、ディレクトリファイルのスパース性を削除するために、ディレクトリの内容を新しいディレクトリにコピーすることをお勧めします。...ディレクトリがスパースとして示されておらず、ディレクトリが大きい場合は、ディレクトリ内のファイルエントリの数を減らして、ディレクトリファイルのサイズを小さくすることをお勧めします。</p>

<p>集計の再配置に失敗しました</p>	<p>重大</p>	<p>このイベントは、集約の再配置中に、宛先ノードがオブジェクトストアに到達できない場合に発生します。</p>	<p>次の修正アクションを実行します。... 「network interface show」 コマンドを使用して、クラスタ間 LIF がオンラインで機能していることを確認します。...宛先ノードのクラスタ間 LIF で「ping」 コマンドを使用して、オブジェクトストアサーバへのネットワーク接続を確認します。... 「aggregate object-store config show」 コマンドを使用して、オブジェクトストアの構成が変更されておらず、ログインおよび接続情報が正確であることを確認してください。...または、再配置コマンドの「override-destination-checks」パラメータを使用してエラーを無効にすることもできます。...詳細またはサポートについては、NetAppテクニカルサポートにお問い合わせください。</p>
<p>シャドウコピーに失敗しました</p>	<p>重大</p>	<p>Microsoft Server のバックアップおよび復元サービス操作であるボリュームシャドウコピーサービス (VSS) が失敗しました。</p>	<p>イベントメッセージに提供される情報を使用して、次の点を確認してください。...シャドウコピー構成は有効になっていますか?...適切なライセンスがインストールされていますか?...シャドウコピー操作はどの共有で実行されますか?...共有名は正しいですか?...共有パスは存在しますか?...シャドウコピーセットとそのシャドウコピーの状態はどうですか?</p>

ストレージスイッチの電源が故障しました	警告	クラスタ スwitchに電源がありません。冗長性が低下し、さらなる停電で停電の危険が生じます。	次の修正アクションを実行してください。...クラスタ スwitchに電力を供給する電源装置のメインがオンになっていることを確認します。...電源コードが電源装置に接続されていることを確認します。...問題が解決しない場合は、NetAppテクニカル サポートに問い合わせてください。
CIFS認証が多すぎる	警告	多くの認証ネゴシエーションが同時に発生しました。このクライアントからの不完全な新規セッション要求が 256 件あります。	クライアントが 256 個以上の新しい接続要求を作成した理由を調査します。エラーが発生した原因を特定するには、クライアントまたはアプリケーションのベンダーに問い合わせる必要がある場合があります。
管理者共有への不正ユーザーアクセス	警告	ログインしているユーザーが許可されたユーザーではないにもかかわらず、クライアントは特権のある ONTAP_ADMIN\$ 共有に接続しようとしてしました。	次の修正アクションを実行します。...指定されたユーザー名と IP アドレスがアクティブな Vscan スキャナ プールの 1 つに設定されていることを確認します。...「vserver vscan scanner pool show-active」コマンドを使用して、現在アクティブなスキャナ プールの設定を確認します。
ウイルスが検出されました	警告	Vscan サーバーがストレージ システムにエラーを報告しました。これは通常、ウイルスが見つかったことを示します。ただし、Vscan サーバー上の他のエラーがこのイベントの原因となる場合があります。...ファイルへのクライアント アクセスが拒否されました。Vscan サーバーは、設定と構成に応じて、ファイルを消去したり、隔離したり、削除したりする場合があります。	「syslog」イベントで報告された Vscan サーバーのログをチェックして、感染したファイルを正常にクリーンアップ、隔離、または削除できたかどうかを確認します。それができなかった場合、システム管理者が手動でファイルを削除しなければならぬ可能性があります。

ボリュームはオフライン	情報	このメッセージは、ボリュームがオフラインになっていることを示します。	ボリュームをオンラインに戻します。
ボリュームは制限状態	情報	このイベントは、フレキシブル ボリュームが制限されたことを示します。	ボリュームをオンラインに戻します。
ストレージ VM の停止に成功しました	情報	このメッセージは、「vserver stop」操作が成功したときに表示されます。	'vserver start' コマンドを使用して、ストレージ VM 上のデータ アクセスを開始します。
ノードパニック	警告	このイベントはパニックが発生したときに発行されます	NetAppカスタマー サポートにお問い合わせください。

[トップに戻る](#)

ランサムウェア対策ログモニター

モニター名	重大度	説明	対処方法
ストレージ VM のランサムウェア対策監視が無効	警告	ストレージ VM のランサムウェア対策監視が無効になっています。ランサムウェア対策を有効にして、ストレージ VM を保護します。	なし
ストレージ VM のランサムウェア対策監視が有効 (学習モード)	情報	ストレージ VM のランサムウェア対策監視が学習モードで有効になっています。	なし
ボリュームランサムウェア対策監視が有効	情報	ボリュームのランサムウェア対策監視が有効になっています。	なし
ボリュームランサムウェア対策監視が無効	警告	ボリュームのランサムウェア対策監視は無効になっています。ボリュームを保護するためにランサムウェア対策を有効にします。	なし
ボリュームランサムウェア対策監視が有効 (学習モード)	情報	ボリュームのランサムウェア対策監視が学習モードで有効になっています。	なし
ボリュームランサムウェア対策監視の一時停止 (学習モード)	警告	ボリュームのランサムウェア対策監視は学習モードで一時停止されています。	なし

ボリュームランサムウェア対策監視の一時停止	警告	ボリュームのランサムウェア対策監視が一時停止されています。	なし
ボリュームランサムウェア対策監視の無効化	警告	ボリュームのランサムウェア対策監視が無効になっています。	なし
ランサムウェア活動が検出されました	重大	検出されたランサムウェアからデータを保護するために、元のデータを復元するために使用できるスナップショット コピーが作成されました。システムはAutoSupportまたは「コール ホーム」メッセージを生成し、NetAppテクニカル サポートおよび設定された送信先に送信します。AutoSupportメッセージにより、問題の特定と解決が向上します。	ランサムウェア活動に対する是正措置を講じるには、「FINAL-DOCUMENT-NAME」を参照してください。

[トップに戻る](#)

NetApp ONTAPモニターの FSx

モニター名	しきい値	モニターの説明	対処方法
FSxボリュームの容量がいっぱいです	警告 @ > 85 %...重大 @ > 95 %	アプリケーションと顧客データを保存するには、ボリュームのストレージ容量が必要です。ONTAPボリュームに保存されるデータが増えるほど、将来のデータのストレージ可用性は低下します。ボリューム内のデータ保存容量が合計保存容量に達した場合、保存容量不足によりお客様がデータを保存できなくなる可能性があります。使用されたボリュームのストレージ容量を監視することで、データサービスの継続性が確保されます。	重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、直ちにアクションを実行する必要があります。...1.スペースを空けるために、不要になったデータを削除することを検討してください

<p>FSxボリュームの高レイテンシー</p>	<p>警告 @ > 1000 μs...重大 @ > 2000 μs</p>	<p>ボリュームは、devOps アプリケーション、ホームディレクトリ、データベースなどのパフォーマンスが重視されるアプリケーションによって発生することが多いIOトラフィックを処理するオブジェクトです。大量の待ち時間が発生すると、アプリケーション自体に問題が発生し、タスクを完了できなくなる可能性があります。アプリケーションの一貫したパフォーマンスを維持するためには、ボリュームのレイテンシを監視することが重要です。</p>	<p>重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、直ちにアクションを実行する必要があります。...1.ボリュームにQoSポリシーが割り当てられている場合は、ボリュームのワークロードが調整される原因にならないように、その制限しきい値を評価します.....警告しきい値を超えた場合は、すぐに次のアクションを実行するように計画します:...1.ボリュームにQoSポリシーが割り当てられている場合は、ボリュームのワークロードが調整される原因にならないように、その制限しきい値を評価します。...2.ノードの使用率も高い場合は、ボリュームを別のノードに移動する、またはノードの合計ワークロードを削減します。</p>
-------------------------	--	--	--

<p>FSxボリュームのiノード制限</p>	<p>警告 @ > 85 %...重大 @ > 95 %</p>	<p>ファイルを保存するボリュームは、インデックスノード (inode) を使用してファイルのメタデータを保存します。ボリュームの inode 割り当てを使い果たすと、それ以上のファイルを追加できなくなります。警告アラートは、利用可能な inode の数を増やすために計画されたアクションを実行する必要があることを示します。重大なアラートは、ファイル制限の枯渇が差し迫っており、サービスの継続性を確保するために、iノードを解放するための緊急措置を講じる必要があることを示します。</p>	<p>重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、直ちにアクションを実行する必要があります。...1.ボリュームの inode 値を増やすことを検討してください。inode 値がすでに最大値に達している場合は、ファイルシステムが最大サイズを超えているため、ボリュームを2つ以上のボリュームに分割することを検討してください.....警告しきい値を超えた場合は、すぐに次のアクションを実行するように計画してください:...1.ボリュームの inode 値を増やすことを検討してください。inode値がすでに最大値に達している場合は、ファイルシステムが最大サイズを超えているため、ボリュームを2つ以上のボリュームに分割することを検討してください。</p>
<p>FSx ボリューム Qtree クォータ オーバーコミット</p>	<p>警告 @ > 95 %...重大 @ > 100 %</p>	<p>ボリューム qtree クォータ オーバーコミットは、ボリュームが qtree クォータによってオーバーコミットされていると見なされるパーセンテージを指定します。ボリュームの qtree クォータに設定されたしきい値に達しました。ボリューム qtree クォータのオーバーコミットを監視することで、ユーザーは中断のないデータ サービスを受けることができます。</p>	<p>重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、直ちに措置を講じる必要があります。1.不要なデータを削除します...警告しきい値を超えた場合は、ボリュームのスペースを増やすことを検討してください。</p>

<p>FSxスナップショットの予約スペースがいっぱいです</p>	<p>警告 @ > 90 %...重大 @ > 95 %</p>	<p>アプリケーションと顧客データを保存するには、ボリュームのストレージ容量が必要です。スナップショット予約領域と呼ばれるその領域の一部は、データをローカルで保護できるようにするスナップショットを保存するために使用されます。ONTAPボリュームに保存される新規データや更新データが増えるほど、使用されるスナップショット容量が増え、将来の新規データや更新データに使用できるスナップショットストレージ容量は少なくなります。ボリューム内のスナップショットデータ容量が合計スナップショット予約領域に達すると、顧客が新しいスナップショットデータを保存できなくなり、ボリューム内のデータの保護レベルが低下する可能性があります。ボリュームの使用済みスナップショット容量を監視することで、データサービスの継続性が確保されます。</p>	<p>重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、直ちにアクションを実行する必要があります。...1.スナップショット予約がいっぱいになったときにボリューム内のデータ領域を使用するようにスナップショットを構成することを検討してください...2.スペースを解放するために、不要になった可能性のある古いスナップショットを削除することを検討してください.....警告しきい値を超えた場合は、すぐに次のアクションを実行するように計画してください:...1.成長に対応するためにボリューム内のスナップショット予約領域を増やすことを検討してください...2.スナップショットの予約領域がいっぱいになったときにボリューム内のデータ領域を使用するようにスナップショットを構成することを検討してください</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のうち、キャッシュから返されるのではなくディスクから返される要求の割合です。これは、音量が設定されたしきい値に達したことを意味します。	重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために、直ちに措置を講じる必要があります。1. IO 負荷 2 を軽減するために、一部のワークロードをボリュームのノードから移動します。QoS 制限を使用して、同じノード上の優先度の低いワークロードの需要を下げます... 警告しきい値を超えた場合は、直ちにアクションを検討してください。1. IO 負荷 2 を軽減するために、一部のワークロードをボリュームのノードから移動します。QoS 制限 3 を使用して、同じノード上の優先度の低いワークロードの需要を下げます。ワークロード特性の変更（ブロックサイズ、アプリケーションキャッシュなど）
------------------	----------------------------	--	---

[トップに戻る](#)

K8sモニター

モニター名	説明	対処方法	重大度/閾値
-------	----	------	--------

<p>永続ボリュームのレイテンシが高い</p>	<p>永続ボリュームのレイテンシが高いということは、アプリケーション自体に問題が発生し、タスクを完了できなくなる可能性があることを意味します。アプリケーションの一貫したパフォーマンスを維持するためには、永続ボリュームのレイテンシを監視することが重要です。メディアタイプに基づいて予想されるレイテンシは次のとおりです - SSD 最大 1 ~ 2 ミリ秒、SAS 最大 8 ~ 10 ミリ秒、SATA HDD 17 ~ 20 ミリ秒。</p>	<p>即時アクション 重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるための即時アクションを検討してください。ボリュームに QoS ポリシーが割り当てられている場合は、ボリュームのワークロードが調整される原因となっていないか、その制限しきい値を評価します。すぐに行うべきアクション 警告しきい値を超えた場合は、次の即時アクションを計画してください。1.ストレージプールの使用率も高い場合は、ボリュームを別のストレージプールに移動します。2.ボリュームに QoS ポリシーが割り当てられている場合は、ボリュームのワークロードが調整される原因にならないように、その制限しきい値を評価します。3.コントローラの使用率も高い場合は、ボリュームを別のコントローラに移動する、またはコントローラの全体的なワークロードを減らします。</p>	<p>警告 @ > 6,000 μs 重大 @ > 12,000 μs</p>
<p>クラスタメモリ飽和度が高い</p>	<p>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 K8s ノード全体の割り当て可能なメモリの合計で割って計算されます。</p>	<p>ノードを追加します。スケジュールされていないノードを修正します。ポッドのサイズを適正化してノード上のメモリを解放します。</p>	<p>警告 @ > 80 % 重大 @ > 90 %</p>
<p>POD接続に失敗しました</p>	<p>このアラートは、POD を使用したボリューム接続が失敗したときに発生します。</p>		<p>警告</p>

高い再送信率	高いTCP再送信率	ネットワークの輻輳をチェックする - ネットワーク帯域幅を大量に消費するワークロードを特定します。Pod の CPU 使用率が高くないか確認します。ハードウェアのネットワークパフォーマンスを確認します。	警告 @ > 10 % 重大 @ > 25 %
ノードファイルシステム容量高	ノードファイルシステム容量高	- アプリケーション ファイルに十分なスペースを確保するために、ノードディスクのサイズを増やします。 - アプリケーション ファイルの使用量を減らします。	警告 @ > 80 % 重大 @ > 90 %
ワークロードネットワークジッター高	高い TCP ジッター (高いレイテンシ/応答時間の変動)	ネットワークの混雑を確認します。ネットワーク帯域幅を大量に消費するワークロードを特定します。Pod の CPU 使用率が高くないか確認します。ハードウェアネットワークのパフォーマンスを確認する	警告 @ > 30 ms 重大 @ > 50 ms

永続ボリュームのスループット	永続ボリュームの MBPS しきい値を使用すると、永続ボリュームが事前定義されたパフォーマンスの期待値を超え、他の永続ボリュームに影響を及ぼす可能性がある場合に管理者に警告することができます。このモニターを有効にすると、SSD 上の永続ボリュームの一般的なスループット プロファイルに適したアラートが生成されます。このモニターは、テナント上のすべての永続ボリュームをカバーします。このモニターを複製し、ストレージクラスに適したしきい値を設定することで、監視目標に基づいて警告および重大なしきい値を調整できます。複製されたモニターは、テナント上の永続ボリュームのサブセットをさらにターゲットにすることができます。	即時のアクション 重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために即時のアクションを計画します。1.ボリュームに QoS MBPS 制限を導入します。2.ボリューム上のワークロードを実行しているアプリケーションに異常がないか確認します。すぐに行うべきアクション 警告しきい値を超えた場合は、次の即時アクションを実行するように計画してください。1.ボリュームに QoS MBPS 制限を導入します。2.ボリューム上のワークロードを実行しているアプリケーションに異常がないか確認します。	警告 @ > 10,000 MB/s 重大 @ > 15,000 MB/s
OOM になる危険性のあるコンテナが強制終了される	コンテナのメモリ制限が低すぎます。コンテナは、排除される危険があります (メモリ不足による強制終了)。	コンテナのメモリ制限を増やします。	警告 @ > 95 %
作業負荷の減少	ワークロードには正常なポッドがありません。		クリティカル @ < 1
永続ボリュームの要求のバインドに失敗しました	このアラートは、PVC でバインディングが失敗したときに発生します。		警告
リソースクォータのメモリ制限を超過します	名前空間のメモリ制限が ResourceQuota を超えようとしています		警告 @ > 80 % 重大 @ > 90 %
リソースクォータメモリ要求が超過しそうです	名前空間のメモリ要求がリソースクォータを超えようとしています		警告 @ > 80 % 重大 @ > 90 %
ノードの作成に失敗しました	構成エラーのため、ノードをスケジュールできませんでした。	構成失敗の原因については、Kubernetes イベントログを確認してください。	致命的
永続ボリュームの再利用に失敗しました	ボリュームの自動再利用が失敗しました。		警告 @ > 0 B

コンテナのCPUスロットリング	コンテナの CPU 制限が低すぎます。コンテナのプロセスが遅くなります。	コンテナの CPU 制限を増やします。	警告 @ > 95 % 重大 @ > 98 %
サービス ロードバランサの削除に失敗しました			警告
永続ボリュームIOPS	永続ボリュームの IOPS しきい値を使用すると、永続ボリュームが事前定義されたパフォーマンス期待値を超えたときに管理者に警告することができます。このモニターを有効にすると、永続ボリュームの一般的な IOPS プロファイルに適したアラートが生成されます。このモニターは、テナント上のすべての永続ボリュームをカバーします。このモニターを複製し、ワークロードに適したしきい値を設定することで、監視目標に基づいて警告および重大しきい値を調整できます。	即時のアクション 重要なしきい値を超えた場合は、サービスの中断を最小限に抑えるために即時のアクションを計画します。1.ボリュームに QoS IOPS 制限を導入します。2.ボリューム上のワークロードを実行しているアプリケーションに異常がないか確認します。すぐに行うべきアクション 警告しきい値を超えた場合は、次の即時アクションを計画してください。1.ボリュームに QoS IOPS 制限を導入します。2.ボリューム上のワークロードを実行しているアプリケーションに異常がないか確認します。	警告 @ > 20,000 IO/s 重大 @ > 25,000 IO/s
サービス ロードバランサの更新に失敗しました			警告
PODマウント失敗	このアラートは、POD のマウントが失敗したときに発生します。		警告
ノードPID圧力	(Linux) ノード上の使用可能なプロセス ID が、削除しきい値を下回りました。	多くのプロセスを生成し、使用可能なプロセス ID のノードを枯渇させるポッドを見つけて修正します。過剰なプロセスを生成するポッドまたはコンテナからノードを保護するには、PodPidsLimit を設定します。	クリティカル @ > 0

ポッドイメージのプル失敗	Kubernetes はポッド コンテナ イメージのプルに失敗しました。	- ポッド構成でポッドのイメージが正しく入力されていることを確認します。 - レジストリにイメージタグが存在することを確認します。 - イメージ レジストリの資格情報を確認します。 - レジストリ接続の問題がないか確認します。 - パブリック レジストリ プロバイダーによって課せられたレート制限に達していないことを確認します。	警告
ジョブの実行時間が長すぎる	ジョブの実行時間が長すぎます		1時間以上で警告、5時間以上で重大
ノードメモリ高	ノードのメモリ使用量が高い	ノードを追加します。スケジュールされていないノードを修正します。ポッドのサイズを適正化してノード上のメモリを解放します。	警告 @ > 85 % 重大 @ > 90 %
リソースクォータCPU制限を超過しそうです	名前空間の CPU 制限が ResourceQuota を超えようとしています		警告 @ > 80 % 重大 @ > 90 %
ポッドクラッシュループバックオフ	ポッドがクラッシュし、複数回再起動を試行しました。		クリティカル @ > 3
ノードCPU高	ノードの CPU 使用率が高くなっています。	ノードを追加します。スケジュールされていないノードを修正します。ポッドのサイズを適正化して、ノード上の CPU を解放します。	警告 @ > 80 % 重大 @ > 90 %
ワークロードネットワーク遅延RTT高	TCP RTT (ラウンドトリップタイム) の遅延が高い	ネットワークの輻輳を確認する  ネットワーク帯域幅を大量に消費するワークロードを特定します。Pod の CPU 使用率が高くないか確認します。ハードウェアのネットワークパフォーマンスを確認します。	警告 @ > 150 ms 重大 @ > 300 ms
ジョブが失敗しました	ノードのクラッシュまたは再起動、リソースの枯渇、ジョブのタイムアウト、またはポッドのスケジュール失敗のため、ジョブは正常に完了しませんでした。	Kubernetes イベント ログで失敗の原因を確認します。	警告 @ > 1

数日で永続ボリュームがいっぱいになる	永続ボリュームの容量は数日で不足します	- アプリケーション ファイルに十分なスペースを確保するためにボリューム サイズを増やします。 - アプリケーションに保存されるデータの量を削減します。	警告 @ < 8日 重大 @ < 3日
ノードメモリの圧力	ノードのメモリが不足しています。使用可能なメモリが削除しきい値に達しました。	ノードを追加します。スケジュールされていないノードを修正します。ポッドのサイズを適正化してノード上のメモリを解放します。	クリティカル @ > 0
ノードが準備完了ではありません	ノードは5分間準備されていません	ノードに十分な CPU、メモリ、ディスク リソースがあることを確認します。ノードのネットワーク接続を確認します。Kubernetes イベント ログで失敗の原因を確認します。	クリティカル @ < 1
永続ボリューム容量大	永続ボリュームのバックエンドの使用容量が高くなっています。	- アプリケーション ファイルに十分なスペースを確保するためにボリューム サイズを増やします。 - アプリケーションに保存されるデータの量を減らします。	警告 @ > 80 % 重大 @ > 90 %
サービス ロードバランサの作成に失敗しました	サービス ロードバランサの作成に失敗しました		致命的
ワークロードレプリカの不一致	一部のポッドは現在、デプロイメントまたは DaemonSet で使用できません。		警告 @ > 1
リソースクォータCPU要求が超過しそうです	名前空間のCPU要求がリソースクォータを超えようとしています		警告 @ > 80 % 重大 @ > 90 %
高い再送信率	高いTCP再送信率	ネットワークの輻輳をチェックする - ネットワーク帯域幅を大量に消費するワークロードを特定します。Pod の CPU 使用率が高くないか確認します。ハードウェアのネットワークパフォーマンスを確認します。	警告 @ > 10 % 重大 @ > 25 %

ノードディスク圧力	ノードのルート ファイルシステムまたはイメージファイル システムのいずれかで使用可能なディスク領域と inode が、削除しきい値を満たしました。	- アプリケーション ファイルに十分なスペースを確保するために、ノードディスクのサイズを増やします。 - アプリケーション ファイルの使用量を減らします。	クリティカル @ > 0
クラスターCPU飽和度が高い	クラスターの割り当て可能な CPU 飽和度が高くなっています。クラスターの CPU 飽和度は、CPU 使用量の合計をすべての K8s ノード全体の割り当て可能な CPU の合計で割って計算されます。	ノードを追加します。スケジュールされていないノードを修正します。ポッドのサイズを適正化して、ノード上の CPU を解放します。	警告 @ > 80 % 重大 @ > 90 %

[トップに戻る](#)

変更ログモニター

モニター名	重大度	モニターの説明
内部ボリュームを発見	情報	このメッセージは、内部ボリュームが検出された場合に発生します。
内部ボリュームが変更されました	情報	このメッセージは、内部ボリュームが変更されたときに発生します。
ストレージノードが検出されました	情報	このメッセージは、ストレージ ノードが検出されたときに表示されます。
ストレージノードが削除されました	情報	このメッセージは、ストレージ ノードが削除されたときに表示されます。
ストレージプールが検出されました	情報	このメッセージは、ストレージ プールが検出されたときに表示されます。
ストレージ仮想マシンが検出されました	情報	このメッセージは、ストレージ仮想マシンが検出されたときに表示されます。
ストレージ仮想マシンが変更されました	情報	このメッセージは、ストレージ仮想マシンが変更されたときに発生します。

[トップに戻る](#)

データ収集モニター

モニター名	説明	対処方法
-------	----	------

買収ユニットのシャットダウン	Data Infrastructure Insights取得ユニットは、新しい機能を導入するために、アップグレードの一環として定期的に再起動されます。通常環境では、これは月に1回以下発生します。取得ユニットがシャットダウンしたという警告アラートの直後には、新しく再起動された取得ユニットがData Infrastructure Insightsへの登録を完了したことを通知する解決策が続く必要があります。通常、このシャットダウンから登録までのサイクルには5～15分かかります。	アラートが頻繁に発生する場合、または15分以上続く場合は、Acquisition Unitをホストするシステム、ネットワーク、およびAUをインターネットに接続しているプロキシの動作を確認してください。
コレクターが失敗しました	データコレクターのポーリングで予期しない障害状況が発生しました。	状況の詳細については、Data Infrastructure Insightsのデータコレクターページをご覧ください。
コレクターの警告	このアラートは通常、データコレクターまたはターゲットシステムの構成が誤っているために発生する可能性があります。今後のアラートを防ぐために構成を見直してください。また、データ収集者が収集可能なすべてのデータを収集したにもかかわらず、不完全なデータを取得したことが原因である可能性もあります。これは、データ収集中に状況が変化した場合に発生する可能性があります(たとえば、データ収集の開始時に存在していた仮想マシンが、データ収集中、データがキャプチャされる前に削除された場合など)。	データコレクターまたはターゲットシステムの構成を確認します。コレクター警告のモニターは他のモニタータイプよりも多くのアラートを送信する可能性があるため、トラブルシューティングを行わない限り、アラート受信者を設定しないことをお勧めします。

[トップに戻る](#)

セキュリティモニター

モニター名	しきい値	モニターの説明	対処方法
-------	------	---------	------

AutoSupport HTTPS 転送が無効	警告 @ < 1	AutoSupportは、転送プロトコルとしてHTTPS、HTTP、およびSMTPをサポートします。AutoSupportメッセージは機密性が高いため、NetAppでは、NetAppサポートにAutoSupportメッセージを送信する際のデフォルト転送プロトコルとして、HTTPSを使用することを強く推奨しています。	AutoSupportメッセージのトランスポートプロトコルとしてHTTPSを設定するには、次のONTAPコマンドを実行します。...system node autosupport modify -transport https
SSH のクラスタ安全でない暗号	警告 @ < 1	SSH が安全でない暗号 (例: *cbc で始まる暗号) を使用していることを示します。	CBC暗号を削除するには、次のONTAPコマンドを実行します。...security ssh remove -vserver <admin vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
クラスタログインバナーが無効です	警告 @ < 1	ONTAPシステムにアクセスするユーザーに対してログインバナーが無効になっていることを示します。ログインバナーを表示すると、システムへのアクセスと使用に関する期待を確立するのに役立ちます。	クラスタのログインバナーを設定するには、次のONTAPコマンドを実行します:...security login banner modify -vserver <admin svm> -message "Access limited to authorized users"
クラスタピア通信が暗号化されていない	警告 @ < 1	ディザスタリカバリ、キャッシュ、またはバックアップの目的でデータをレプリケートする場合は、あるONTAPクラスタから別のONTAPクラスタへの転送時にそのデータを保護する必要があります。暗号化は、ソースクラスタと宛先クラスタの両方で構成する必要があります。	ONTAP 9.6 よりも前に作成されたクラスタピア関係に対して暗号化を有効にするには、ソースとデスティネーションのクラスタを 9.6 にアップグレードする必要があります。次に、「cluster peer modify」コマンドを使用して、ソースクラスタピアと宛先クラスタピアの両方がクラスタピアリング暗号化を使用するように変更します。詳細については、『NetAppセキュリティ強化ガイド for ONTAP 9』を参照してください。

デフォルトのローカル管理ユーザが有効	警告 @ > 0	NetApp、lock コマンドを使用して、不要なデフォルトの管理者ユーザー (組み込み) アカウントをロック (無効化) することを推奨しています。これらは主に、パスワードが更新または変更されたことのないデフォルトのアカウントです。	組み込みの「admin」アカウントをロックするには、次のONTAPコマンドを実行します。...security login lock -username admin
FIPS モードが無効	警告 @ < 1	FIPS 140-2 への準拠を有効にすると、TLSv1 と SSLv3 は無効になり、TLSv1.1 と TLSv1.2 のみが引き続き有効になりますONTAPでは、FIPS 140-2への準拠が有効な場合、TLSv1とSSLv3を有効にすることはできません。	クラスターでFIPS 140-2準拠を有効にするには、次のONTAPコマンドを詳細権限モードで実行します。...security config modify -interface SSL -is -fips-enabled true
ログ転送が暗号化されていない	警告 @ < 1	情報の流出を単一のシステムまたはソリューションに限定するためには、syslog情報をオフロードする必要があります。そのため、syslog情報を安全な保管場所にオフロードすることを推奨します。	ログ転送先を作成したら、そのプロトコルを変更することはできません。暗号化されたプロトコルに変更するには、次のONTAPコマンドを使用してログ転送先を削除して再作成します。...cluster log-forwarding create -destination <destination ip> -protocol tcp-encrypted
MD5ハッシュパスワード	警告 @ > 0	NetApp、ONTAPユーザー アカウント パスワードには、より安全な SHA-512 ハッシュ関数を使用することを強くお勧めします。安全性の低い MD5 ハッシュ関数を使用しているアカウントは、SHA-512 ハッシュ関数に移行する必要があります。	NetAppは、ユーザーにパスワードを変更させることで、ユーザーアカウントをより安全なSHA-512ソリューションに移行することを強く推奨しています。...MD5ハッシュ関数を使用するパスワードでアカウントをロックするには、次のONTAPコマンドを実行します。...security login lock -vserver * -username * -hash-function md5

NTPサーバーが設定されていません	警告 @ < 1	クラスターに NTP サーバーが構成されていないことを示します。冗長性と最適なサービスを確保するために、NetApp少なくとも3台の NTP サーバーをクラスターに関連付けることを推奨しています。	NTPサーバをクラスターに関連付けるには、次のONTAPコマンドを実行します: cluster time-service ntp server create -server <ntp server host name or ip address>
NTP サーバ数が不足しています	警告 @ < 3	クラスターに構成されている NTP サーバーが3台未満であることを示します。冗長性と最適なサービスを確保するために、NetApp少なくとも3台の NTP サーバーをクラスターに関連付けることを推奨しています。	NTPサーバをクラスターに関連付けるには、次のONTAPコマンドを実行します。...cluster time-service ntp server create -server <ntpサーバのホスト名またはIPアドレス>
リモートシェルが有効	警告 @ > 0	リモート シェルは、ONTAPソリューションへのコマンド ライン アクセスを確立するための安全な方法ではありません。安全なリモート アクセスを実現するには、リモート シェルを無効にする必要があります。	NetAppは、安全なリモートアクセスのためにセキュアシェル (SSH) を推奨しています。...クラスターでリモートシェルを無効にするには、次のONTAPコマンドを高度な権限モードで実行します。...security protocol modify -application rsh-enabled false
ストレージ VM 監査ログが無効	警告 @ < 1	SVM の監査ログが無効になっていることを示します。	Vserver の監査ログを設定するには、次のONTAPコマンドを実行します:...vserver audit enable -vserver <svm>
ストレージ VM SSH の安全でない暗号	警告 @ < 1	SSH が安全でない暗号 (例: *cbc で始まる暗号) を使用していることを示します。	CBC暗号を削除するには、次のONTAPコマンドを実行します。...security ssh remove -vserver <vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
ストレージ VM ログインバナーが無効になっています	警告 @ < 1	システム上の SVM にアクセスするユーザーに対してログインバナーが無効になっていることを示します。ログインバナーを表示すると、システムへのアクセスと使用に関する期待を確立するのに役立ちます。	クラスターのログインバナーを設定するには、次のONTAPコマンドを実行します:...security login banner modify -vserver <svm> -message "Access limited to authorized users"

Telnet プロトコルが有効	警告 @ > 0	Telnet は、ONTAPソリューションへのコマンドラインアクセスを確立するための安全な方法ではありません。安全なリモートアクセスのために、Telnet を無効にする必要があります。	セキュアなリモートアクセスを確立するために、Secure Shell (SSH) を推奨します。クラスタ上でTelnetを無効にするには、次のONTAPコマンドを詳細権限モードで実行します。...security protocol modify -application telnet -enabled false
-----------------	----------	--	---

[トップに戻る](#)

データ保護モニター

モニター名	しきい値	モニターの説明	対処方法
LUNスナップショットコピー用のスペースが不足しています	(フィルター contains_luns = Yes) 警告 @ > 95 %... 重大 @ > 100 %	アプリケーションと顧客データを保存するには、ボリュームのストレージ容量が必要です。スナップショット予約領域と呼ばれるその領域の一部は、データをローカルで保護できるようにするスナップショットを保存するために使用されます。ONTAPボリュームに保存される新規データや更新データが増えるほど、使用されるスナップショット容量が増え、将来の新規データや更新データに使用できるスナップショットストレージ容量は少なくなります。ボリューム内のスナップショットデータ容量が合計スナップショット予約領域に達すると、顧客が新しいスナップショットデータを保存できなくなり、ボリューム内の LUN のデータの保護レベルが低下する可能性があります。ボリュームの使用済みスナップショット容量を監視することで、データサービスの継続性が確保されません。	即時のアクション 重要なしきい値を超えた場合は、サービス中断を最小限に抑えるために、即時のアクションを検討してください。1.スナップショット予約がいっぱいになったときにボリューム内のデータ領域を使用するようにスナップショットを構成します。2.古くて不要なスナップショットをいくつか削除して、スペースを解放します。すぐに行うべきアクション 警告しきい値を超えた場合は、次の即時アクションを実行するように計画してください。1.成長に対応するために、ボリューム内のスナップショット予約領域を増やします。2.スナップショット予約がいっぱいになったときにボリューム内のデータ領域を使用するようにスナップショットを構成します。

SnapMirror関係の遅延	警告 @ > 150%...重大 @ > 300%	SnapMirror関係の遅延は、スナップショットのタイムスタンプと宛先システムの時間の差です。lag_time_percent は、SnapMirrorポリシーのスケジュール間隔に対する遅延時間の比率です。遅延時間がスケジュール間隔と等しい場合、lag_time_percent は100% になります。SnapMirrorポリシーにスケジュールがない場合、lag_time_percent は計算されません。	「snapmirror show」コマンドを使用してSnapMirrorのステータスを監視します。 「snapmirror show-history」コマンドを使用してSnapMirrorの転送履歴を確認します。
-----------------	---------------------------	--	---

[トップに戻る](#)

クラウドボリューム (CVO) モニター

モニター名	CIの重症度	モニターの説明	対処方法
CVO ディスクがサービス停止中	情報	このイベントは、ディスクが障害としてマークされた、サニタイズされている、またはメンテナンスセンターに入ったためにサービスから削除されたときに発生します。	なし

<p>ストレージプールの CVO ギブバックに失敗しました</p>	<p>重大</p>	<p>このイベントは、ストレージ フェイルオーバー (SFO) ギブバックの一環としてアグリゲートを移行しているときに、宛先ノードがオブジェクトストアに到達できない場合に発生します。</p>	<p>次の修正アクションを実行します。「network interface show」コマンドを使用して、クラスタ間 LIF がオンラインで機能していることを確認します。宛先ノードのクラスタ間 LIF 経由で「ping」コマンドを使用して、オブジェクトストア サーバーへのネットワーク接続を確認します。</p> <p>「aggregate object-store config show」コマンドを使用して、オブジェクトストアの構成が変更されておらず、ログインおよび接続情報がまだ正確であることを確認します。あるいは、giveback コマンドの「require-partner-waiting」パラメータに false を指定してエラーを無効にすることもできます。詳細情報やサポートについては、NetAppテクニカル サポートにお問い合わせください。</p>
-----------------------------------	-----------	---	---

CVO HA相互接続ダウン	警告	<p>高可用性 (HA) 相互接続がダウンしています。フェイルオーバーが利用できない場合、サービス停止のリスクがあります。</p>	<p>修正アクションは、プラットフォームでサポートされている HA 相互接続リンクの数とタイプ、および相互接続がダウンしている理由によって異なります。リンクがダウンしている場合: HA ペアの両方のコントローラが動作していることを確認します。外部接続リンクの場合は、相互接続ケーブルが正しく接続されていること、および該当する場合は Small Form-Factor Pluggable (SFP) が両方のコントローラに正しく装着されていることを確認します。内部的に接続されたリンクの場合は、「ic link off」コマンドと「ic link on」コマンドを使用して、リンクを順番に無効にしてから再度有効にします。リンクが無効になっている場合は、「ic link on」コマンドを使用してリンクを有効にします。ピアが接続されていない場合は、「ic link off」コマンドと「ic link on」コマンドを使用して、リンクを順番に無効にしてから再度有効にします。問題が解決しない場合は、NetAppテクニカルサポートにお問い合わせください。</p>
---------------	----	---	---

<p>ユーザーあたりの CVO 最大セッション数を超過しました</p>	<p>警告</p>	<p>TCP 接続でユーザーごとに許可されるセッションの最大数を超過しました。いくつかのセッションが解放されるまで、セッションを確立する要求はすべて拒否されます。</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。クライアントをリポートします。問題の原因が新しいアプリケーションか既存のアプリケーションかを確認します。アプリケーションが新しい場合は、「cifs option modify -max-opens -same-file-per-tree」コマンドを使用して、クライアントのしきい値を高く設定します。場合によっては、クライアントは期待どおりに動作しますが、より高いしきい値が必要になります。クライアントに対してより高いしきい値を設定するには、高度な権限が必要です。問題が既存のアプリケーションによって発生している場合は、クライアントに問題がある可能性があります。詳細情報やサポートについては、NetAppテクニカル サポートにお問い合わせください。</p>
-------------------------------------	-----------	---	--

CVO NetBIOS 名が競合	重大	NetBIOS ネーム サービスは、リモート マシンからの名前登録要求に対する否定応答を受信しました。これは通常、NetBIOS 名またはエイリアスの競合によって発生します。その結果、クライアントはデータにアクセスできないか、クラスター内の適切なデータ提供ノードに接続できない可能性があります。	次のいずれかの修正アクションを実行します。NetBIOS 名またはエイリアスに競合がある場合は、次のいずれかを実行します。「vserver cifs delete -aliases alias -vserver vserver」コマンドを使用して、重複した NetBIOS エイリアスを削除します。重複した名前を削除し、「vserver cifs create -aliases alias -vserver vserver」コマンドを使用して新しい名前のエイリアスを追加することで、NetBIOS エイリアスの名前を変更します。エイリアスが設定されておらず、NetBIOS 名が競合している場合は、「vserver cifs delete -vserver vserver」および「vserver cifs create -cifs-server netbiosname」コマンドを使用して CIFS サーバの名前を変更します。注意: CIFS サーバを削除すると、データにアクセスできなくなる可能性があります。NetBIOS 名を削除するか、リモート マシン上の NetBIOS の名前を変更します。
CVO NFSv4 ストア プールが枯渇しました	重大	NFSv4 ストア プールが使い果たされました。	このイベント後、NFS サーバが 10 分以上応答しない場合は、NetAppテクニカル サポートにお問い合わせください。
CVOノードパニック	警告	このイベントはパニックが発生したときに発行されます	NetAppカスタマー サポートにお問い合わせください。

CVO ノードルートボリュームスペース不足	重大	システムはルート ボリュームの空き容量が危険なほど少ないことを検出しました。ノードは完全には動作していません。データ LIF がクラスター内でフェイルオーバーした可能性があります。そのため、ノード上の NFS および CIFS アクセスが制限されています。管理機能は、ルート ボリューム上のスペースをクリアするためのノードのローカル回復手順に制限されます。	次の修正アクションを実行します。古いスナップショット コピーを削除するか、/mroot ディレクトリから不要になったファイルを削除するか、ルート ボリュームの容量を拡張して、ルート ボリュームのスペースを解放します。コントローラーを再起動します。詳細情報やサポートについては、NetAppテクニカル サポートにお問い合わせください。
CVO 存在しない管理者共有	重大	Vscan の問題: クライアントが存在しない ONTAP_ADMIN\$ 共有に接続しようとしてしました。	指定された SVM ID に対して Vscan が有効になっていることを確認します。SVM で Vscan を有効にすると、SVM に対して ONTAP_ADMIN\$ 共有が自動的に作成されます。
CVO オブジェクト ストア ホストが解決できません	重大	オブジェクト ストア サーバーのホスト名を IP アドレスに解決できません。オブジェクト ストア クライアントは、IP アドレスを解決しないとオブジェクト ストア サーバーと通信できません。その結果、データにアクセスできなくなる可能性があります。	DNS 構成をチェックして、ホスト名が IP アドレスで正しく設定されていることを確認します。
CVO オブジェクト ストア インタークラスタ LIF ダウン	重大	オブジェクト ストア クライアントは、オブジェクト ストア サーバーと通信するための動作可能な LIF を見つけることができません。インタークラスタ LIF が動作可能になるまで、ノードはオブジェクト ストア クライアントトラフィックを許可しません。その結果、データにアクセスできなくなる可能性があります。	次の修正アクションを実行します。「network interface show -role intercluster」コマンドを使用して、クラスタ間 LIF のステータスを確認します。クラスタ間 LIF が正しく設定され、動作していることを確認します。クラスタ間 LIF が設定されていない場合は、「network interface create -role intercluster」コマンドを使用して追加します。

CVO オブジェクト ストア署名の不一致	重大	オブジェクト ストア サーバーに送信された要求署名が、クライアントによって計算された署名と一致しません。その結果、データにアクセスできなくなる可能性があります。	シークレット アクセス キーが正しく設定されていることを確認します。正しく設定されている場合は、NetAppテクニカルサポートにお問い合わせください。
CVO QoS モニターのメモリが上限に達しました	重大	QoS サブシステムの動的メモリが、現在のプラットフォーム ハードウェアの限界に達しました。一部の QoS 機能は制限された容量で動作する場合があります。	アクティブなワークロードまたはストリームをいくつか削除して、メモリを解放します。 「statistics show -object workload -counter ops」コマンドを使用して、どのワークロードがアクティブであるかを確認します。アクティブなワークロードにはゼロ以外の操作が表示されます。次に、「workload delete <workload_name>」コマンドを複数回使用して、特定のワークロードを削除します。または、「stream delete -workload <workload name> *」コマンドを使用して、アクティブなワークロードから関連付けられているストリームを削除します。

<p>CVO READDIR タイムアウト</p>	<p>重大</p>	<p>READDIR ファイル操作が、WAFLで実行できるタイムアウトを超えました。これは、ディレクトリが非常に大きいか、またはディレクトリがまばらであるために発生する可能性があります。是正措置をお勧めします。</p>	<p>次の修正アクションを実行します。次の「diag」権限ノードシェル CLI コマンドを使用し、READDIR ファイル操作の有効期限が切れた最近のディレクトリに固有の情報を検索します: waf readdir notification show。ディレクトリがスパースとして示されているかどうかを確認します。ディレクトリがスパースとして示されている場合は、ディレクトリの内容を新しいディレクトリにコピーして、ディレクトリファイルのスパース性を解除することをお勧めします。ディレクトリがスパースとして示されておらず、ディレクトリが大きい場合は、ディレクトリ内のファイル エントリの数を減らして、ディレクトリファイルのサイズを小さくすることをお勧めします。</p>
---------------------------	-----------	---	--

CVO ストレージ プールの再配置に失敗しました	重大	このイベントは、集約の再配置中に、宛先ノードがオブジェクトストアに到達できない場合に発生します。	次の修正アクションを実行します。「network interface show」コマンドを使用して、クラスタ間 LIF がオンラインで機能していることを確認します。宛先ノードのクラスタ間 LIF 経由で「ping」コマンドを使用して、オブジェクトストア サーバーへのネットワーク接続を確認します。 「aggregate object-store config show」コマンドを使用して、オブジェクトストアの構成が変更されておらず、ログインおよび接続情報がまだ正確であることを確認します。あるいは、再配置コマンドの「override-destination-checks」パラメータを使用してエラーを無効にすることもできます。詳細情報やサポートについては、NetApp テクニカル サポートにお問い合わせください。
CVO シャドウコピーに失敗しました	重大	Microsoft Server のバックアップおよび復元サービス操作であるボリューム シャドウ コピー サービス (VSS) が失敗しました。	イベント メッセージに提供される情報を使用して、次の点を確認します。シャドウ コピー構成は有効になっていますか？適切なライセンスがインストールされていますか？シャドウ コピー操作はどの共有で実行されますか？共有名は正しいですか？共有パスは存在しますか？シャドウ コピー セットとそのシャドウ コピーの状態はどうなっていますか？
CVO ストレージ VM の停止に成功しました	情報	このメッセージは、「vserver stop」操作が成功したときに表示されます。	'vserver start' コマンドを使用して、ストレージ VM 上のデータ アクセスを開始します。

CVO CIFS 認証が多すぎる	警告	多くの認証ネゴシエーションが同時に発生しました。このクライアントからの不完全な新規セッション要求が 256 件あります。	クライアントが 256 個以上の新しい接続要求を作成した理由を調査します。エラーが発生した原因を特定するには、クライアントまたはアプリケーションのベンダーに問い合わせる必要がある場合があります。
CVO 未割り当てディスク	情報	システムには未割り当てのディスクがあり、容量が無駄になっており、システムに誤った構成や部分的な構成変更が適用されている可能性があります。	次の修正アクションを実行します。「disk show-n」コマンドを使用して、割り当てられていないディスクを特定します。「disk assign」コマンドを使用してディスクをシステムに割り当てます。
CVO 管理者共有への不正ユーザーアクセス	警告	ログインしているユーザーが許可されたユーザーではないにもかかわらず、クライアントは特権のある ONTAP_ADMIN\$ 共有に接続しようとしていました。	次の修正アクションを実行します。指定されたユーザー名と IP アドレスがアクティブな Vscan スキャナー プールの 1 つに設定されていることを確認します。「vserver vscan scanner pool show-active」コマンドを使用して、現在アクティブなスキャナー プールの構成を確認します。
CVO ウイルスが検出されました	警告	Vscan サーバーがストレージシステムにエラーを報告しました。これは通常、ウイルスが見つかったことを示します。ただし、Vscan サーバー上の他のエラーによってこのイベントが発生する場合があります。ファイルへのクライアント アクセスが拒否されました。Vscan サーバーは、設定と構成に応じて、ファイルを消去したり、隔離したり、削除したりする場合があります。	「syslog」イベントで報告された Vscan サーバーのログをチェックして、感染したファイルを正常にクリーンアップ、隔離、または削除できたかどうかを確認します。それができなかった場合、システム管理者が手動でファイルを削除しなければならない可能性があります。
CVO ボリュームオフライン	情報	このメッセージは、ボリュームがオフラインになっていることを示します。	ボリュームをオンラインに戻します。

CVO ボリューム制限	情報	このイベントは、フレキシブル ボリュームが制限されたことを示します。	ボリュームをオンラインに戻します。
-------------	----	------------------------------------	-------------------

[トップに戻る](#)

SnapMirror for Business Continuity (SMBC) メディエーター ログ モニター

モニター名	重大度	モニターの説明	対処方法
ONTAPメディエーターが追加されました	情報	このメッセージは、ONTAP Mediator がクラスに正常に追加されたときに表示されます。	なし
ONTAPメディエーターにアクセスできません	重大	このメッセージは、ONTAP Mediator が再利用されたか、Mediator パッケージが Mediator サーバーにインストールされなくなった場合に表示されます。その結果、SnapMirrorフェイルオーバーは不可能になります。	「snapmirror mediator remove」コマンドを使用して、現在のONTAP Mediator の設定を削除します。「snapmirror mediator add」コマンドを使用して、ONTAP Mediator へのアクセスを再設定します。
ONTAPメディエーターが削除されました	情報	このメッセージは、ONTAP Mediator がクラスから正常に削除されたときに表示されます。	なし
ONTAPメディエーターにアクセスできません	警告	このメッセージは、クラス上でONTAP Mediator にアクセスできない場合に表示されます。その結果、SnapMirrorフェイルオーバーは不可能になります。	「network ping」および「network traceroute」コマンドを使用して、ONTAP Mediator へのネットワーク接続を確認します。問題が解決しない場合は、「snapmirror mediator remove」コマンドを使用して、現在のONTAP Mediator の設定を削除します。「snapmirror mediator add」コマンドを使用して、ONTAP Mediator へのアクセスを再設定します。

SMBC CA証明書の有効期限が切れました	重大	このメッセージは、ONTAP Mediator 証明機関 (CA) 証明書の有効期限が切れたときに表示されます。その結果、ONTAP Mediator への以降の通信はすべてできなくなります。	「snapmirror mediator remove」コマンドを使用して、現在のONTAP Mediator の設定を削除します。ONTAP Mediator サーバー上の新しい CA 証明書を更新します。 「snapmirror mediator add」コマンドを使用して、ONTAP Mediator へのアクセスを再設定します。
SMBC CA証明書の有効期限切れ	警告	このメッセージは、ONTAP Mediator の証明機関 (CA) 証明書の有効期限が 30 日以内に切れる場合に表示されます。	この証明書の有効期限が切れる前に、「snapmirror mediator remove」コマンドを使用して、現在のONTAP Mediator の設定を削除します。ONTAP Mediator サーバー上の新しい CA 証明書を更新します。「snapmirror mediator add」コマンドを使用して、ONTAP Mediator へのアクセスを再設定します。
SMBCクライアント証明書の有効期限が切れました	重大	このメッセージは、ONTAP Mediator クライアント証明書の有効期限が切れたときに表示されます。その結果、ONTAP Mediator への以降の通信はすべてできなくなります。	「snapmirror mediator remove」コマンドを使用して、現在のONTAP Mediator の設定を削除します。「snapmirror mediator add」コマンドを使用して、ONTAP Mediator へのアクセスを再設定します。
SMBCクライアント証明書の有効期限切れ	警告	このメッセージは、ONTAP Mediator クライアント証明書の有効期限が 30 日以内に切れる場合に表示されます。	この証明書の有効期限が切れる前に、「snapmirror mediator remove」コマンドを使用して、現在のONTAP Mediator の設定を削除します。 「snapmirror mediator add」コマンドを使用して、ONTAP Mediator へのアクセスを再設定します。

SMBC関係の同期が取れていない注:UMにはこれがありません	重大	このメッセージは、SnapMirror for Business Continuity (SMBC) 関係のステータスが「同期中」から「非同期」に変更されたときに表示されます。このため、RPO=0 のデータ保護は中断されま	ソースボリュームと宛先ボリューム間のネットワーク接続を確認します。宛先では「snapmirror show」コマンドを使用し、ソースでは「snapmirror list-destinations」コマンドを使用して、SMBC 関係のステータスを監視します。自動再同期は、関係を「同期中」の状態に戻そうとします。再同期が失敗した場合は、クラスター内のすべてのノードがクォーラム状態にあり、正常であることを確認します。
SMBC サーバー証明書の有効期限が切れました	重大	このメッセージは、ONTAP Mediator サーバ証明書の有効期限が切れたときに表示されます。その結果、ONTAP Mediator への以降の通信はすべてできなくなります。	「snapmirror mediator remove」コマンドを使用して、現在のONTAP Mediator の設定を削除します。ONTAP Mediator サーバ上の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 Mediator 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切れ	警告	このメッセージは、ONTAP Mediator サーバ証明書の有効期限が 30 日以内に切れる場合に表示されます。	この証明書の有効期限が切れる前に、「snapmirror mediator remove」コマンドを使用して、現在のONTAP Mediator の設定を削除します。ONTAP Mediator サーバ上の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 Mediator へのアクセスを再設定します。

[トップに戻る](#)

追加の電源、ハートビート、およびその他のシステムモニター

モニター名	重大度	モニターの説明	対処方法
ディスクシェルフ電源装置を検出しました	情報	このメッセージは、ディスクシェルフに電源ユニットが追加されたときに発生します。	NONE
ディスクシェルフ電源を取り外しました	情報	このメッセージは、電源ユニットがディスクシェルフから取り外されたときに表示されます。	NONE
MetroClusterの自動計画外スイッチオーバーが無効	重大	このメッセージは、計画外の自動切り替え機能が無効になっている場合に表示されます。	自動スイッチオーバーを有効にするには、クラスター内の各ノードに対して「metrocluster modify -node-name <nodename> -automatic-switchover -onfailure true」コマンドを実行します。
MetroClusterストレージブリッジに到達できません	重大	ストレージブリッジは管理ネットワーク経由でアクセスできません	1) ブリッジがSNMPによって監視されている場合は、「network interface show」コマンドを使用して、ノード管理LIFが起動していることを確認します。「network ping」コマンドを使用して、ブリッジが動作していることを確認します。2) ブリッジがインバンドで監視されている場合は、ブリッジへのファブリックケーブルを確認し、ブリッジの電源がオンになっていることを確認します。
MetroClusterブリッジ温度異常 - 危険未満	重大	ファイバーチャネルブリッジのセンサーは、重大なしきい値を下回る温度を報告しています。	1) ストレージブリッジ上のファンの動作状態を確認します。2) ブリッジが推奨温度条件下で動作していることを確認します。
MetroClusterブリッジ温度異常 - 危険域以上	重大	ファイバーチャネルブリッジのセンサーが、重大なしきい値を超える温度を報告しています。	1) コマンド「storage bridge show -cooling」を使用して、ストレージブリッジ上のシャーシ温度センサーの動作状態を確認します。2) ストレージブリッジが推奨温度条件下で動作していることを確認します。

モニター名	重大度	モニターの説明	対処方法
MetroCluster で残ったアグリゲートあり	警告	骨材はスイッチバック中に取り残されました。	1) コマンド「aggr show」を使用してアグリゲートの状態を確認します。2) アグリゲートがオンラインの場合は、「metrocluster switchback」コマンドを使用して、アグリゲートを元の所有者に戻します。
メトロクラスターパートナー間のすべてのリンクがダウン	重大	RDMA 相互接続アダプタおよびクラスター間 LIF とピア クラスターとの接続が切断されているか、ピアクラスターがダウンしています。	1) クラスター間 LIF が稼働していることを確認します。クラスター間 LIF がダウンしている場合は修復します。2) 「cluster peer ping」コマンドを使用して、ピアクラスターが起動して実行されていることを確認します。ピアクラスターがダウンしている場合は、『MetroCluster ディザスタリカバリ ガイド』を参照してください。3) ファブリック MetroCluster の場合、バックエンド ファブリック ISL が稼働していることを確認します。バックエンド ファブリック ISL がダウンしている場合は修復します。4) 非ファブリック MetroCluster 構成の場合、RDMA 相互接続アダプタ間のケーブル接続が正しいことを確認します。リンクがダウンしている場合は、ケーブルを再構成してください。

モニター名	重大度	モニターの説明	対処方法
MetroClusterパートナーがピアリング ネットワーク経由でアクセスできない	重大	ピア クラスタへの接続が切断されました。	1) ポートが正しいネットワーク/スイッチに接続されていることを確認します。2) クラスタ間 LIF がピア クラスタに接続されていることを確認します。3) コマンド「cluster peer ping」を使用して、ピア クラスタが起動して実行されていることを確認します。ピア クラスタがダウンしている場合は、『MetroClusterディザスタリカバリ ガイド』を参照してください。
MetroClusterスイッチ間全リンクダウン	重大	ストレージ スイッチ上のすべてのスイッチ間リンク (ISL) がダウンしています。	1) ストレージ スイッチ上のバックエンド ファブリック ISL を修復します。2) パートナー スイッチが起動しており、その ISL が動作していることを確認します。3) xWDM デバイスなどの中間機器が動作していることを確認します。
MetroClusterノードからストレージスタックへのSASリンクがダウンしています	警告	SAS アダプタまたはそれに接続されたケーブルに障害がある可能性があります。	1.SAS アダプターがオンラインで実行されていることを確認します。2.物理的なケーブル接続が安全で動作していることを確認し、必要に応じてケーブルを交換します。3. SAS アダプタがディスクシェルフに接続されている場合は、IOM とディスクが正しく取り付けられていることを確認します。
MetroClusterFCイニシエーターリンクダウン	重大	FC イニシエーター アダプターに障害があります。	1.FC イニシエーター リンクが改ざんされていないことを確認します。2. 「system node run -node local -command storage show adapter」 コマンドを使用して、FC イニシエーター アダプターの動作ステータスを確認します。

モニター名	重大度	モニターの説明	対処方法
FC-VIインターコネクトリンクダウン	重大	FC-VI ポート上の物理リンクがオフラインです。	1.FC-VI リンクが改ざんされていないことを確認します。2. 「metrocluster interconnect adapter show」 コマンドを使用して、FC-VI アダプタの物理ステータスが「Up」であることを確認します。3.構成にファブリックスイッチが含まれている場合は、それらが正しくケーブル接続され、構成されていることを確認します。
MetroCluster で残ったスペア ディスクあり	警告	スイッチバック中にスペア ディスクが残されました。	ディスクに障害が発生していない場合は、「metrocluster switchback」 コマンドを使用して、ディスクを元の所有者に戻します。
MetroClusterストレージブリッジポートがダウンしています	重大	ストレージブリッジのポートがオフラインです。	1) コマンド「storage bridge show -ports」を使用して、ストレージブリッジ上のポートの動作状態を確認します。2) ポートへの論理的および物理的な接続を確認します。
MetroClusterストレージスイッチファンの故障	重大	ストレージスイッチのファンが故障しました。	1) コマンド「storage switch show -cooling」を使用して、スイッチ内のファンが正しく動作していることを確認します。2) ファンFRUが正しく挿入され、動作していることを確認します。
MetroClusterストレージスイッチにアクセスできません	重大	ストレージスイッチは管理ネットワーク経由ではアクセスできません。	1) コマンド「network interface show」を使用して、ノード管理LIFが起動していることを確認します。2) 「network ping」コマンドを使用して、スイッチが動作していることを確認します。3) スイッチにログインした後、SNMP設定をチェックして、スイッチがSNMP経由で到達可能であることを確認します。

モニター名	重大度	モニターの説明	対処方法
MetroClusterスイッチの電源装置に障害が発生しました	重大	ストレージスイッチの電源ユニットが動作していません。	1) コマンド「storage switch show -error -switch -name <スイッチ名>」を使用してエラーの詳細を確認します。 2) コマンド「storage switch show -power -switch-name <switch name>」を使用して、障害のある電源ユニットを特定します。 3) 電源ユニットがストレージスイッチのシャーシに正しく挿入され、完全に動作していることを確認します。
MetroClusterスイッチの温度センサーが故障しました	重大	ファイバーチャネルスイッチのセンサーに障害が発生しました。	1) コマンド「storage switch show -cooling」を使用して、ストレージスイッチの温度センサーの動作状態を確認します。 2) スイッチが推奨温度条件下で動作していることを確認します。
MetroClusterスイッチの温度異常	重大	ファイバーチャネルスイッチの温度センサーが異常な温度を報告しました。	1) コマンド「storage switch show -cooling」を使用して、ストレージスイッチの温度センサーの動作状態を確認します。 2) スイッチが推奨温度条件下で動作していることを確認します。
サービスプロセッサのハートビートが失われました	情報	このメッセージは、ONTAPがサービスプロセッサ(SP)から予期される「ハートビート」信号を受信しなかった場合に表示されます。このメッセージとともに、SPからのログファイルがデバッグ用に送信されます。ONTAPはSPをリセットして通信を復元しようとします。SPは再起動中、最大2分間使用できなくなります。	NetAppテクニカルサポートにお問い合わせください。

モニター名	重大度	モニターの説明	対処方法
サービス プロセッサのハートビートが停止しました	警告	このメッセージは、ONTAP がサービス プロセッサ (SP) からハートビートを受信しなくなったときに表示されます。ハードウェアの設計に応じて、システムはデータの提供を継続するか、データの損失やハードウェアの損傷を防ぐためにシャットダウンすることを決定する場合があります。システムは引き続きデータを提供しますが、SPが動作していない可能性があるため、ダウンしたアプライアンス、ブートエラー、または Open Firmware (OFW) 電源投入時セルフテスト (POST) エラーに関する通知を送信できません。システムがそのように構成されている場合、AutoSupport (または「コール ホーム」) メッセージが生成され、NetAppテクニカル サポートと構成された送信先に送信されます。AutoSupportメッセージが正常に配信されると、問題の特定と解決が大幅に改善されます。	システムがシャットダウンした場合は、ハードパワーサイクルを試してください。コントローラをシャーシから引き出し、押し戻して、システムの電源を入れます。電源を入れ直しても問題が解決しない場合、または他に注意が必要な状況がある場合は、NetAppテクニカル サポートにお問い合わせください。

[トップに戻る](#)

詳細情報

- ["アラートの表示と消去"](#)

Webhook通知

Webhookを使用した通知

Webhook を使用すると、ユーザーはカスタマイズされた Webhook チャンネルを使用してさまざまなアプリケーションにアラート通知を送信できます。

多くの商用アプリケーションは、標準入力インターフェースとして Webhook をサポートしています。たとえば、Slack、PagerDuty、Teams、Discord はすべて Webhook をサポートしています。汎用的でカスタマイズ可能な Webhook チャンネルをサポートすることで、Data Infrastructure Insights はこれらの配信チャンネルの多

くをサポートできます。Webhook に関する情報は、これらのアプリケーション Web サイトで参照できます。例えば、Slackは["この便利なガイド"](#)。

複数の Webhook チャンネルを作成し、各チャンネルを異なる目的 (個別のアプリケーション、異なる受信者など) に向けることができます。

Webhook チャンネル インスタンスは、次の要素で構成されます。

Name	一意の名前
URL	Webhook ターゲット URL (URL パラメータとともに <i>http://</i> または <i>https://</i> プレフィックスを含む)
方法	GET、POST - デフォルトはPOST
カスタムヘッダー	ここでカスタムヘッダー行を指定します
メッセージ本文	メッセージの本文をここに入力してください
デフォルトのアラートパラメータ	Webhookのデフォルトパラメータを一覧表示します
カスタムパラメータとシークレット	カスタムパラメータとシークレットを使用すると、固有のパラメータやパスワードなどの安全な要素を追加できます。

Webhookの作成

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

次の画像は、Slack 用に構成された Webhook の例を示しています。

Edit a Webhook

Name

Slack Test

Template Type

Slack

URL

https://hooks.slack.com/services/<token>

Method

POST

Custom Header

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

Message Body

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

Cancel

Test Webhook

Save Webhook

各フィールドに適切な情報を入力し、完了したら「保存」をクリックします。

「Webhook のテスト」ボタンをクリックして接続をテストすることもできます。これにより、選択したメソッドに従って、定義された URL に「メッセージ本文」（置換なし）が送信されることに注意してください。

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

Default Alert Parameters

Name	Description
%%alertDescription%%	Alert description
%%alertId%%	Alert ID
%%alertRelativeUrl%%	Relative URL to the Alert page. To build alert link use https://%%cloudInsightsHostName%%%%alertRelativeUrl%%
%%metricName%%	Monitored metric
%%monitorName%%	Monitor name
%%objectType%%	Monitored object type
%%severity%%	Alert severity level
%%alertCondition%%	Alert condition
%%triggerTime%%	Alert trigger time in GMT ("Tue, 27 Oct 2020 01:20:30 GMT")
%%triggerTimeEpoch%%	Alert trigger time in Epoch format (milliseconds)
%%triggeredOn%%	Triggered On (key:value pairs separated by commas)
%%value%%	Metric value that triggered the alert
%%cloudInsightsLogoUrl%%	Cloud Insights logo URL
%%cloudInsightsHostname%%	Cloud Insights Hostname (concatenate with relative URL to build alert link)

Custom Parameters and Secrets

Name	Value	Description
No Data Available		

[+ Parameter](#)

パラメーター: パラメーターとは何ですか? また、どのように使用しますか?

アラート パラメータは、アラートごとに設定される動的な値です。たとえば、`%%TriggeredOn%%` パラメータは、アラートがトリガーされたオブジェクトに置き換えられます。

任意のオブジェクト属性 (ストレージ名など) をパラメータとして Webhook に追加できます。たとえば、Webhook の説明に、次のようにボリューム名とストレージ名のパラメータを設定できます: 「ボリューム: `%%relatedObject.volume.name%%`、ストレージ: `%%relatedObject.storage.name%%` の待機時間が長い」。

このセクションでは、「Webhook をテスト」ボタンをクリックしたときに置換は実行されないことに注意してください。ボタンは、%% 置換を示すペイロードを送信しますが、データに置き換えません。

カスタムパラメータとシークレット

このセクションでは、必要なカスタムパラメータやシークレットを追加できます。セキュリティ上の理由から、シークレットが定義されている場合、この Webhook チャンネルを変更できるのは Webhook 作成者のみです。他のユーザーにとっては読み取り専用となります。URL/ヘッダーでは、%%<secret_name>% のようにシークレットを使用できます。

Webhooks リストページ

Webhook リスト ページには、名前、作成者、作成日、ステータス、セキュリティ、最終報告のフィールドが表示されます。

モニターで Webhook 通知を選択する

ウェブフック通知を選択するには"monitor"、アラート > モニターの管理 に移動して目的のモニターを選択するか、新しいモニターを追加します。チーム通知の設定 セクションで、配信方法として Webhook を選択します。アラート レベル (重大、警告、解決済み) を選択し、目的の Webhook を選択します。

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

By Webhook

Notify team on

Critical, Warning, Resolved

Use Webhook

Please Select

Search...

ci-alerts-notifications-dev

ci-alerts-notifications-qa

Webhook の例:

Webhooksの"スラック"Webhooksの"ページャーデューティ"Webhooksの"チーム"Webhooksの"不和"

Discord の Webhook の例

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



このページはサードパーティの指示を参照しており、変更される可能性があります。参照"Discordドキュメント"最新情報についてはこちらをご覧ください。

Discordの設定:

- Discordでサーバーを選択し、テキストチャンネルの下にあるチャンネル編集（歯車アイコン）を選択します。
- *統合 > Webhookの表示*を選択し、*新しいWebhook*をクリックします。

- Webhook URL をコピーします。これをData Infrastructure Insights のWebhook 構成に貼り付ける必要があります。

Data Infrastructure Insights Webhook を作成します。

1. Data Infrastructure Insightsで、管理 > 通知 に移動し、**Webhooks** タブを選択します。新しい Webhook を作成するには、[+Webhook] をクリックします。
2. Webhook に「Discord」などの意味のある名前を付けます。
3. テンプレート タイプ ドロップダウンで、**Discord** を選択します。
4. 上記の URL を *URL* フィールドに貼り付けます。

Edit a Webhook

Name

Template Type

URL

Method

Custom Header

Message Body

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



Webhook をテストするには、メッセージ本文の URL 値を有効な URL (<https://netapp.com> など) に一時的に置き換えて、[Test Webhook] ボタンをクリックします。テストが完了したら、必ずメッセージ本文を元に戻してください。

Webhook 経由の通知

Webhook 経由でイベントを通知するには、Data Infrastructure Insights で*アラート>モニター*に移動し、*+モニター*をクリックして新しいモニターを作成します。"monitor"。

- メトリックを選択し、モニターの条件を定義します。
- [チーム通知の設定] の下で、**Webhook** 配信方法を選択します。
- 必要なイベント（重大、警告、解決済み）の「Discord」Webhookを選択します。

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

The screenshot shows a configuration interface for team notifications. It includes a 'By Webhook' label, a 'Notify team on' dropdown menu with 'Critical, Warning, Resolved' selected, and a 'Use Webhook(s)' section with a 'Discord' button and a close icon.

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 チャンネルを使用してさまざまなアプリケーションにアラート通知を送信できます。このページでは、PagerDuty の Webhook を設定する例を示します。



このページはサードパーティの指示を参照しており、変更される可能性があります。参照"[PagerDutyのドキュメント](#)"最新情報についてはこちらをご覧ください。

PagerDutyのセットアップ:

1. PagerDutyで*サービス>サービスディレクトリ*に移動し、*+新しいサービス*ボタンをクリックします。
2. 名前_を入力し、[_API を直接使用] を選択します。 _サービスの追加_をクリックします。

Data Infrastructure Insights Webhook を作成します。

1. Data Infrastructure Insightsで、管理 > 通知 に移動し、**Webhooks** タブを選択します。新しい Webhook を作成するには、[+Webhook] をクリックします。
2. Webhook に「PagerDuty Trigger」などの意味のある名前を付けます。この Webhook は、重大レベルおよび警告レベルのイベントに使用します。
3. テンプレート タイプ ドロップダウンで、**PagerDuty** を選択します。
4. *routingKey* という名前のカスタム パラメータ シークレットを作成し、その値を上記の PagerDuty *Integration Key* 値に設定します。

Custom Parameters and Secrets ⓘ

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

+ Parameter

Name ⓘ

Value

Type

Description

Cancel

Save Parameter

これらの手順を繰り返して、解決されたイベントの「PagerDuty Resolve」 Webhook を作成します。

PagerDuty からData Infrastructure Insightsへのフィールド マッピング

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

ページャーデューティ	Data Infrastructure Insights
アラートキー	Alert ID
ソース	トリガーオン
コンポーネント	メトリック名
グループ	オブジェクト タイプ

ページャーデューティ	Data Infrastructure Insights
クラス	モニター名

Message Body

```
{
  "dedup_key": "%%alertId%%",
  "event_action": "trigger",
  "links": [
    {
      "href": "https://%%cloudInsightsHostname%%/%%alertRelativeUrl%%",
      "text": "%%metricName%%' value of %%value%% (%%alertCondition%%) for
%%triggeredOn%%"
    }
  ],
  "payload": {
    "class": "%%monitorName%%",
    "component": "%%metricName%%",
    "group": "%%objectType%%",
    "severity": "critical",
    "source": "%%triggeredOn%%",
    "summary": "%%severity%% | %%alertId%% | %%triggeredOn%%"
  },
  "routing_key": "%%routingKey%%"
}
```

Webhook経由の通知

Webhook経由でイベントを通知するには、Data Infrastructure Insightsで*アラート>モニター*に移動し、*+モニター*をクリックして新しいモニターを作成します。"monitor"。

- メトリックを選択し、モニターの条件を定義します。
- [チーム通知の設定] の下で、**Webhook** 配信方法を選択します。
- 重大レベルおよび警告レベルのイベントには、「PagerDuty トリガー」Webhook を選択します。
- 解決されたイベントには「PagerDuty Resolve」を選択します。

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

By Webhook	Notify team on Critical, Warning	Use Webhook(s) PagerDuty Trigger x	
	Notify team on Resolved	Use Webhook(s) PagerDuty Resolve x	



PagerDuty はトリガー イベントを解決済みイベントとは異なる方法で処理するため、トリガー イベントと解決済みイベントに別々の通知を設定することがベスト プラクティスです。

Slack の Webhook の例

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



このページはサードパーティの指示を参照しており、変更される可能性があります。参照"[Slackドキュメント](#)"最新情報についてはこちらをご覧ください。

Slackの例:

- へ移動 <https://api.slack.com/apps>新しいアプリを作成します。意味のある名前を付けて、Slack ワークスペースを選択します。

Create a Slack App ×

App Name

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

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](#).

- 「受信 Webhooks」に移動し、「受信 Webhook のアクティブ化」をクリックし、「新しい Webhook の追加」をリクエストして、投稿するチャンネルを選択します。
- Webhook URL をコピーします。これをData Infrastructure Insights のWebhook 構成に貼り付ける必要があります。

Data Infrastructure Insights Webhook を作成します。

1. Data Infrastructure Insightsで、管理 > 通知 に移動し、**Webhooks** タブを選択します。新しい Webhook を作成するには、[+Webhook] をクリックします。
2. Webhook に「Slack Webhook」などの意味のある名前を付けます。
3. テンプレート タイプ ドロップダウンで、**Slack** を選択します。
4. 上記の URL を URL フィールドに貼り付けます。

Edit a Webhook

Name

Slack

Template Type

Slack

URL

https://hooks.slack.com/services/<token string>

Method

POST

Custom Header

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

Message Body

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

Cancel

Test Webhook

Save Webhook

Webhook経由の通知

Webhook経由でイベントを通知するには、Data Infrastructure Insightsで*アラート>モニター*に移動し、*+モニター*をクリックして新しいモニターを作成します。"monitor"。

- メトリックを選択し、モニターの条件を定義します。
- [チーム通知の設定] の下で、**Webhook** 配信方法を選択します。
- 必要なイベント（重大、警告、解決済み）の「Slack」 Webhookを選択します。

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

By Webhook	Notify team on Critical, Warning, Resolved	Use Webhook(s) Slack 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、 <https://api.slack.com/messaging/composing>
- エラー処理: https://api.slack.com/messaging/webhooks#handling_errors

Microsoft Teams の Webhook の例

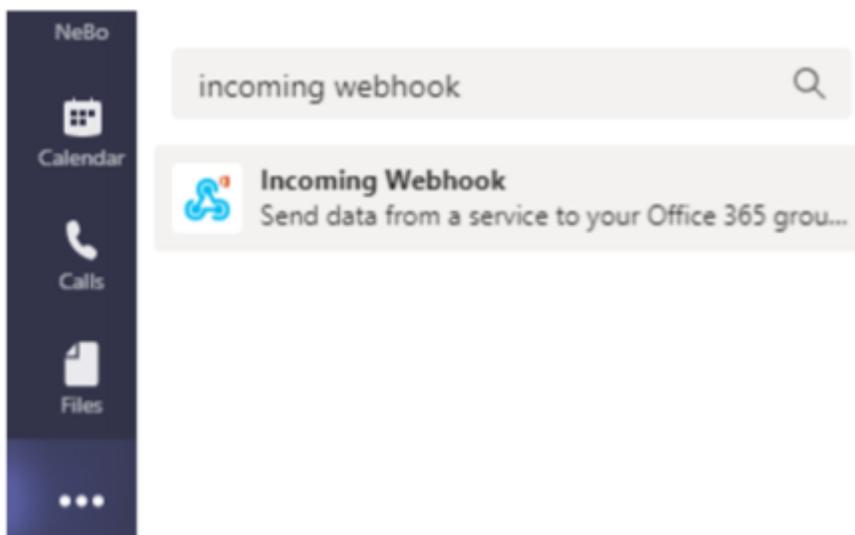
Webhook を使用すると、ユーザーはカスタマイズされた Webhook チャンネルを使用してさまざまなアプリケーションにアラート通知を送信できます。このページでは、Teams の Webhook を設定する例を示します。



このページはサードパーティの指示を参照しており、変更される可能性があります。参照"Teamsドキュメント"最新情報についてはこちらをご覧ください。

Teams のセットアップ:

1. Teams でケバブを選択し、Incoming Webhook を検索します。



2. *チームに追加 > チームを選択 > コネクタの設定*を選択します。
3. Webhook URL をコピーします。これをData Infrastructure Insights のWebhook 構成に貼り付ける必要があります。

Data Infrastructure Insights Webhook を作成します。

1. Data Infrastructure Insightsで、管理 > 通知 に移動し、**Webhooks** タブを選択します。新しい Webhook を作成するには、[+Webhook] をクリックします。
2. Webhook に「Teams Webhook」などのわかりやすい名前を付けます。
3. [テンプレート タイプ] ドロップダウンで、[Teams] を選択します。

Edit a Webhook

Name

Template Type

URL

Method

Custom Header

Message Body

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

1. 上記の URL を URL フィールドに貼り付けます。

Webhook経由の通知

Webhook経由でイベントを通知するには、Data Infrastructure Insightsで*アラート>モニター*に移動し、*+モ

モニター*をクリックして新しいモニターを作成します。"monitor"。

- メトリックを選択し、モニターの条件を定義します。
- [チーム通知の設定] の下で、**Webhook** 配信方法を選択します。
- 必要なイベント（重大、警告、解決済み）の「Teams」Webhookを選択します。

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

By Webhook

Notify team on

Critical, Warning, Resolved ▼

Use Webhook(s)

Teams - Edwin x ▼

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

商標に関する情報

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