イベント、パフォーマンス、健全性の監視
ONTAP 9

NetApp
April 24, 2024

目次

イベント、パフォーマンス、健全性の監視

System Managerを使用してクラスタパフォーマンスを監視する

System Manager を使用してクラスタパフォーマンスを監視する

このセクションのトピックでは、 ONTAP 9.7 以降のリリースで System Manager を使用してクラスタの健全性とパフォーマンスを管理する方法を説明します。

System Manager ダッシュボードでシステムに関する情報を表示することで、クラスタパフォーマンスを監視できます。ダッシュボードには、重要なアラートと通知に関する情報、ストレージ階層とボリュームの効率性と容量、クラスタで使用できるノード、 HA ペアのノードのステータス、最もアクティブなアプリケーションとオブジェクト、 およびクラスタまたはノードのパフォーマンス指標。

ダッシュボードでは、次の情報を確認できます。

- * Health * ：クラスタの健全性はどの程度ですか？
- * 容量 * ：クラスタで利用可能な容量
- * パフォーマンス * ：レイテンシ、 IOPS 、スループットを基準に、クラスタのパフォーマンスはどの程度向上していますか？
- * ネットワーク * ：ポート、インターフェイス、 Storage VM などのホストとストレージオブジェクトを使用してネットワークをどのように構成しますか？

健全性と容量の概要で、をクリックできます → 追加情報を表示してタスクを実行します。

パフォーマンスの概要では、時間、日、週、月、または年に基づく指標を表示できます。

ネットワークの概要では、ネットワーク内の各オブジェクトの数（「 8 NVMe/FC ポート」など）が表示されます。 番号をクリックすると、各ネットワークオブジェクトの詳細を確認できます。

クラスタダッシュボードにパフォーマンスを表示します

ダッシュボードを使用すると、追加または移動するワークロードについて、十分な情報に基づいて意思決定を下すことができます。また、ピーク使用時間を確認して、潜在的な変更を計画することもできます。

パフォーマンスの値は 3 秒ごとに更新され、パフォーマンスグラフは 15 秒ごとに更新されます。

手順

1. [* ダッシュボード *] をクリックします。
2. [* パフォーマンス *] で、間隔を選択します。

ホットボリュームやその他のオブジェクトを特定します

アクセス頻度の高いボリューム（ホットボリューム）とデータ（ホットオブジェクト）

を特定して、クラスタのパフォーマンスを向上させます。

> ONTAP 9.10.1以降では、ファイルシステム分析のアクティビティ追跡機能を使用してボリューム内のホットオブジェクトを監視できます。

手順

1. [ストレージ] 、 [ボリューム] の順にクリックします。
2. IOPS 、レイテンシ、およびスループットの列をフィルタリングして、アクセス頻度の高いボリュームとデータを表示します。

QoS を変更する

ONTAP 9.8以降では、ストレージのプロビジョニング時に サービス品質（QoS） はデフォルトで有効になっています。QoS を無効にするか、プロビジョニングプロセスでカスタムの QoS ポリシーを選択できます。ストレージのプロビジョニングが完了したあとに QoS を変更することもできます。

手順

1. System Managerで、**[**ストレージ**]***を選択し、[ボリューム]*を選択します。
2. QoSを変更するボリュームの横にあるを選択します。 ⋮ 次に*[編集]*をクリックします。

リスクを監視

ONTAP 9.10.0 以降では、 System Manager を使用して、 Active IQ デジタルアドバイザから報告されたリスクを監視できます。 ONTAP 9.10.1 以降の System Manager を使用してリスクを確認することもできます。

NetApp Active IQ Digital Advisor は、リスクを軽減し、ストレージ環境のパフォーマンスと効率を向上させる機会を報告します。 System Manager を使用すると、 Active IQ によって報告されるリスクを把握し、ストレージの管理や可用性の向上、セキュリティの向上、ストレージパフォーマンスの向上に役立つ実用的な情報を受け取ることができます。

Active IQ アカウントへのリンク

Active IQ からリスクに関する情報を受け取るには、まず System Manager から Active IQ アカウントにリンクします。

手順

1. System Manager で、 * Cluster > Settings * の順にクリックします。
2. [**Active IQ Registration**](登録 *) で '[*Register] (登録 *) をクリックします
3. Active IQ のクレデンシャルを入力します。
4. クレデンシャルの認証が完了したら、「 * 確認」をクリックして Active IQ と System Manager * をリンクします。

リスクの数を表示します

ONTAP 9.10.0 以降では、 System Manager のダッシュボードから Active IQ で報告されたリスクの数を確認できます。

作業を開始する前に

System Manager から Active IQ アカウントへの接続を確立する必要があります。 を参照してください Active IQ アカウントへのリンク。

手順

1. System Manager で、 * ダッシュボード * をクリックします。
2. * Health * セクションで、報告されたリスクの数を確認します。

> リスクの数を示すメッセージをクリックすると、各リスクの詳細情報を確認できます。 を参照してください リスクの詳細を表示します。

リスクの詳細を表示します

ONTAP 9.10.0 以降では、 Active IQ で報告されるリスクが影響領域別に分類される方法を System Manager で確認できます。 報告された各リスク、システムへの潜在的な影響、対処方法に関する詳細情報も確認できます。

作業を開始する前に

System Manager から Active IQ アカウントへの接続を確立する必要があります。 を参照してください Active IQ アカウントへのリンク。

手順

1. [* イベント]>[すべてのイベント *] をクリックします。
2. 概要 * セクションの * Active IQ 提案 * で、各インパクトエリアカテゴリのリスク数を表示します。 リスクカテゴリは次のとおりです。
   - パフォーマンスと効率性
   - 可用性と保護
   - 容量
   - 設定
   - セキュリティ
3. Active IQ Suggestions * （リスク提案 * ）タブをクリックして、以下を含む各リスクに関する情報を表示します。
   - システムへの影響のレベル
   - リスクのカテゴリ
   - 影響を受けるノード
   - 必要な軽減のタイプ
   - 対処方法

リスクを承認

ONTAP 9.10.1 以降のシステムでは、 System Manager を使用して開いているリスクを確認することができます。

手順

1. System Manager で、の手順を実行してリスクのリストを表示します リスクの詳細を表示します。
2. 承認する未完了リスクのリスク名をクリックします。
3. 次のフィールドに情報を入力します。
   - リマインダ（日付）
   - 理由
   - コメント
4. [* Acknowledge （確認）] をクリックし

> リスクを承認したあと、変更が Active IQ の提案リストに反映されるまでに数分かかります。

リスクの承認を取り消します

ONTAP 9.10.1 以降の System Manager を使用して、以前に確認されたリスクの承認を取り消すことができます。

手順

1. System Manager で、の手順を実行してリスクのリストを表示します リスクの詳細を表示します。
2. 承認を取り消すリスクの名前をクリックします。
3. 次のフィールドに情報を入力します。
   - 理由
   - コメント
4. [承認の取り消し *] をクリックします。

> リスクを承認しないと、 Active IQ の提案リストに変更が反映されるまでに数分かかります。

System Managerの分析情報

ONTAP 9.11.1以降では、システムのパフォーマンスとセキュリティの最適化に役立つ_insights_がSystem Managerに表示されます。

> インサイトの表示、カスタマイズ、応答については、 "システムの最適化に役立つ分析情報を取得できます"

容量に関する分析

System Managerでは、システムの容量の状況に応じて次の情報を表示できます。

インサイト	重大度	条件	の修正
ローカル階層のスペースが不足しています	リスクを修正	1つ以上のローカル階層の使用率が95%を超えており、急速に拡張しています。既存のワークロードを拡張できない場合や、極端な場合には、既存のワークロードのスペースが不足して失敗することがあります。	推奨される修正：次のいずれかのオプションを実行します。 • ボリュームリカバリキューをクリアします。 • シックプロビジョニングされたボリュームでシンプロビジョニングを有効にして、トラップされたストレージを解放します。 • 別のローカル階層にボリュームを移動します。 • 不要なSnapshotコピーを削除します。 • ボリューム内の不要なディレクトリまたはファイルを削除します。 • FabricPoolを有効にして、データをクラウドに階層化します。
アプリケーションにスペースが不足している	要注意	95%を超えていますが、自動拡張が有効になっていません。	推奨：現在の容量の150%まで自動拡張を有効にします。 その他のオプション： • Snapshotコピーを削除してスペースを再生します。 • ボリュームのサイズを変更します。 • ディレクトリまたはファイルを削除します。
FlexGroupボリュームの容量が不均衡になっています	ストレージの最適化	1つ以上のFlexGroupのコンスティチュエントボリュームのサイズが時間の経過とともに不均衡になっており、使用容量が不均衡になっています。 コンスティチュエントボリュームがフルになると、書き込みエラーが発生する可能性があります。	推奨：FlexGroupボリュームをリバランシングします。

Storage VMの容量が不足しています	ストレージの最適化	1つ以上のStorage VMが最大容量に近づいています。Storage VMが最大容量に達しても、新規または既存のボリュームに追加のスペースをプロビジョニングすることはできません。	推奨：可能であれば、Storage VMの最大容量を増やします。

セキュリティに関する分析情報

データやシステムのセキュリティを危険にさらす可能性がある状況に対して、System Managerでは次の分析情報を表示できます。

インサイト	重大度	条件	の修正
ボリュームは引き続きランサムウェア対策学習モード	要注意	1つ以上のボリュームが90日間Anti-Ransomware Learningモードになっています。	推奨：これらのボリュームに対して、ランサムウェア対策のアクティブモードを有効にします。
ボリュームでSnapshotコピーの自動削除が有効になる	要注意	Snapshotの自動削除が1つ以上のボリュームで有効になっています。	推奨：Snapshotコピーの自動削除を無効にします。そうしないと、ランサムウェア攻撃が発生した場合に、これらのボリュームのデータリカバリが不可能になる可能性があります。
ボリュームにSnapshotポリシーがありません	要注意	1つ以上のボリュームに適切なSnapshotポリシーが関連付けられていません。	推奨：Snapshotポリシーが割り当てられていないボリュームにSnapshotポリシーを適用します。そうしないと、ランサムウェア攻撃が発生した場合に、これらのボリュームのデータリカバリが不可能になる可能性があります。
ネイティブFPolicyが設定されていない	ベストプラクティス	ネイティブFPolicyが1つ以上のNAS Storage VMに設定されていません。	推奨：重要：拡張機能をブロックすると、予期しない結果になる可能性があります。9.11.1以降では、Storage VMに対してネイティブのFPolicyを有効にすることができます。これにより、ランサムウェア攻撃に使用されたことがわかっている3、000を超えるファイル拡張子がブロックされます。 "ネイティブFPolicyの設定" NAS Storage VMを使用して、環境内のボリュームへの書き込みを許可または許可しないファイル拡張子を制御します。

Telnetが有効	ベストプラクティス	セキュアなリモートアクセスには、Secure Shell（SSH）を使用する必要があります。	推奨：Telnetを無効にし、SSHを使用してセキュアなリモートアクセスを実現します。
設定されているNTPサーバが少なすぎます	ベストプラクティス	NTP用に設定されているサーバの数が3未満です。	推奨：少なくとも3台のNTPサーバをクラスタに関連付けます。 そうしないと、クラスタ時間の同期で問題が発生する可能性があります。
Remote Shell（RSH；リモートシェル）が有効	ベストプラクティス	セキュアなリモートアクセスには、Secure Shell（SSH）を使用する必要があります。	推奨：RSHを無効にし、SSHを使用してセキュアなリモートアクセスを実現します。
ログインバナーが設定されていません	ベストプラクティス	クラスタ、Storage VM、またはその両方に対してログインメッセージが設定されることはありません。	推奨：クラスタとStorage VMのログインバナーを設定し、使用を有効にします。
AutoSupportがセキュアでないプロトコルを使用している	ベストプラクティス	AutoSupportはHTTPS経由で通信するように設定されていません。	推奨：テクニカルサポートにAutoSupportメッセージを送信するためのデフォルトの転送プロトコルとしてHTTPSを使用することを強く推奨します。
デフォルトの管理ユーザがロックされていません	ベストプラクティス	デフォルトの管理アカウント（adminまたはdiag）を使用してログインしているユーザはおらず、これらのアカウントはロックされていません。	推奨：使用されていないデフォルトの管理アカウントをロックします。
Secure Shell（SSH）でセキュアでない暗号を使用	ベストプラクティス	現在の設定では、セキュアでないCBC暗号を使用しています。	推奨:訪問者との安全な通信を保護するために、Webサーバー上で安全な暗号のみを許可する必要があります。名前に「cbc」を含む暗号（「ais128-cbc」、「aes192-cbc」、「aes256-cbc」、「3DES-cbc」など）を削除します。
FIPS 140-2へのグローバルな準拠が無効になっている	ベストプラクティス	クラスタでFIPS 140-2へのグローバル準拠が無効になっています。	推奨：セキュリティ上の理由から、ONTAPが外部のクライアントまたはサーバクライアントと安全に通信できるように、グローバルFIPS 140-2準拠の暗号化を有効にする必要があります。

ボリュームがランサムウェア攻撃で監視されていない	要注意	Anti-ransomwareが1つ以上のボリュームで無効になっています。	推奨：ボリュームでランサムウェア対策を有効にします。そうしないと、ボリュームが脅威にさらされているときや攻撃を受けているときに気付かない可能性があります。
Storage VMはランサムウェア対策用に設定されていない	ベストプラクティス	ランサムウェア対策用に設定されていないStorage VMがあります。	推奨：Storage VMでランサムウェア対策を有効にします。そうしないと、Storage VMが脅威にさらされているときや攻撃を受けているときに気付かない可能性があります。

構成に関する分析情報

システム構成に関する懸念事項について、System Managerでは次の情報を表示できます。

インサイト	重大度	条件	の修正
通知用のクラスタが設定されていません	ベストプラクティス	Eメール、Webhook、またはSNMPトラップホストが、クラスタの問題に関する通知を受信できるように設定されていません。	推奨：クラスタの通知を設定します。
クラスタに自動更新が設定されていません。	ベストプラクティス	最新のディスク認定パッケージ、ディスクファームウェア、シェルフファームウェア、およびSP / BMCファームウェアファイルが利用可能な場合に自動更新を受信するようにクラスタが設定されていません。	推奨：この機能を有効にします。
クラスタファームウェアが最新ではありません	ベストプラクティス	お使いのシステムには、パフォーマンス向上のためにクラスタを保護するための改善策、セキュリティパッチ、または新機能が含まれている可能性のあるファームウェアに対する最新の更新がありません。	推奨：ONTAPファームウェアをアップデートします。

システムの最適化に役立つ分析情報を取得できます

System Managerでは、システムの最適化に役立つ分析情報を確認できます。

このタスクについて

ONTAP 9.11.0 以降では、システムの容量とセキュリティコンプライアンスの最適化に役立つ分析情報を System Manager で表示できます。

ONTAP 9.11.1以降では、システムの容量、セキュリティコンプライアンス、構成を最適化するための追加の分析情報を確認できます。

> 拡張機能をブロックすると、予期しない結果になる可能性があります。 ONTAP 9.11.1以降では、System Managerを使用してStorage VMのネイティブFPolicyを有効にできます。推奨されるSystem Manager Insightメッセージが表示される場合があります。 "ネイティブFPolicyの設定" （Storage VMの場合）。
>
> FPolicyネイティブモードでは、特定のファイル拡張子を許可または禁止できます。System Managerでは、過去にランサムウェア攻撃で使用されたファイル拡張子が3、000を超えることを推奨しています。 これらの拡張子の一部は、環境内の正規のファイルによって使用されている可能性があり、ブロックすると、予期しない問題が発生する可能性があります。
>
> したがって、環境のニーズに合わせて拡張子のリストを変更することを強くお勧めします。を参照してください "System Managerを使用してポリシーを再作成するためにSystem Managerで作成されたネイティブFPolicyの設定からファイル拡張子を削除する方法"。
>
> ネイティブFPolicyの詳細については、を参照してください。 "FPolicy の設定タイプ"。

これらの分析情報は、ベストプラクティスに基づいて 1 ページに表示され、システムを最適化するための緊急の操作を開始できます。各インサイトの詳細については、 "System Managerの分析情報"。

最適化のインサイトを表示

手順

1. System Manager で、左側のナビゲーション列の * Insights * をクリックします。

   [* Insights （インサイト）] ページには、インサイトのグループが表示されます 各インサイトグループには、 1 つ以上のインサイトが含まれる場合があります。 次のグループが表示されます。

   - 注意が必要です
   - リスクを修正
   - ストレージを最適化

2. （オプション）ページの右上隅にある以下のボタンをクリックして、表示されるインサイトをフィルタリングします。

   - セキュリティ関連の分析情報を表示します。
   - 容量に関する分析情報が表示されます。
   -

- 設定に関する分析情報を表示します。
- All すべてのインサイトを表示します。

分析情報に対応してシステムを最適化

System Manager では、分析情報を無視したり、さまざまな方法で問題を解決したり、プロセスを開始して問題を修正したりすることで、対応できます。

手順

1. System Manager で、左側のナビゲーション列の * Insights * をクリックします。
2. Insight にカーソルを合わせると、次の操作を実行するためのボタンが表示されます。
   - * Dismiss * ：ビューからインサイトを削除します。 洞察を「アン・却下」するには、を参照してください [customize-settings-insights]。
   - * Explore * ：洞察に言及されている問題を解決するさまざまな方法を見つけます。 このボタンは、複数の修復方法がある場合にのみ表示されます。
   - * 修正 *: インサイトで説明されている問題を修正するプロセスを開始します。修正の適用に必要なアクションを実行するかどうかを確認するメッセージが表示されます。

これらの処理の一部は System Manager の他のページから開始できますが、 * Insights * ページではこの 1 ページから実行できるため、日常業務を合理化できます。

インサイトの設定をカスタマイズします

System Managerで通知を受け取るインサイトをカスタマイズできます。

手順

1. System Manager で、左側のナビゲーション列の * Insights * をクリックします。
2. ページの右上にあるをクリックします ⋮をクリックし、*設定*を選択します。
3. [* 設定 *] ページで、通知を受けるインサイトの横にチェックボックスがあることを確認します。 以前にインサイトを却下したことがある場合は、チェックボックスをオンにすることで「アン却下」できます。
4. [保存（ Save ）] をクリックします。

インサイトを**PDF**ファイルとしてエクスポートします

適用可能なすべてのインサイトをPDFファイルとしてエクスポートできます。

手順

1. System Manager で、左側のナビゲーション列の * Insights * をクリックします。
2. ページの右上にあるをクリックします ⋮をクリックし、*エクスポート*を選択します。

ネイティブ**FPolicy**の設定

ONTAP 9.11.1以降では、ネイティブのFPolicyの実装を推奨するSystem Manager Insight

を受け取った場合は、そのInsightをStorage VMおよびボリュームに設定できます。

作業を開始する前に

System Manager Insightsにアクセスすると、*[ベストプラクティスの適用]*で、ネイティブのFPolicyが設定されていないことを示すメッセージが表示されることがあります。

FPolicy設定タイプの詳細については、を参照してください。 "FPolicy の設定タイプ"。

手順

1. System Manager で、左側のナビゲーション列の * Insights * をクリックします。
2. で、[ネイティブFPolicyは設定されていません]*を探します。
3. アクションを実行する前に、次のメッセージをお読みください。

> 拡張機能をブロックすると、予期しない結果になる可能性があります。 ONTAP 9.11.1以降では、System Managerを使用してStorage VMのネイティブFPolicyを有効にできます。FPolicyネイティブモードでは、特定のファイル拡張子を許可または禁止できます。System Managerでは、過去にランサムウェア攻撃で使用されたファイル拡張子が3、000を超えることを推奨しています。 これらの拡張子の一部は、環境内の正規のファイルによって使用されている可能性があり、ブロックすると、予期しない問題が発生する可能性があります。
>
> したがって、環境のニーズに合わせて拡張子のリストを変更することを強くお勧めします。を参照してください "System Managerを使用してポリシーを再作成するためにSystem Managerで作成されたネイティブFPolicyの設定からファイル拡張子を削除する方法"。

4. [修正]*をクリックします。
5. ネイティブFPolicyを適用するStorage VMを選択します。
6. 各Storage VMについて、ネイティブFPolicyを受け取るボリュームを選択します。
7. [**Configure**] をクリックします。

CLIを使用してクラスタパフォーマンスを監視および管理します

パフォーマンスの監視と管理の概要

基本的なパフォーマンスの監視と管理のタスクを設定し、一般的なパフォーマンスの問題を特定して解決することができます。

次の想定条件に該当する場合は、以下の手順に従ってクラスタのパフォーマンスを監視および管理してください。

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。
- ONTAP コマンドラインインターフェイスに加え、 Active IQ Unified Manager （旧 OnCommand Unified Manager ）を使用して、システムのステータスとアラートを表示し、クラスタのパフォーマンスを監視し、根本原因分析を実施する。
- ストレージサービス品質（ QoS ）の設定に ONTAP コマンドラインインターフェイスを使用している。

  QoS は、 System Manager 、 NSLM 、 WFA 、 VSC （ VMware プラグイン）、および API でも設定で

きます。

- Linux または Windows ベースのインストールではなく、仮想アプライアンスを使用して Unified Manager をインストールする。
- DHCP ではなく静的な設定を使用してソフトウェアをインストールする。
- ONTAP コマンドには、 advanced 権限レベルでアクセスできます。
- 「 admin 」ロールを持つクラスタ管理者である。

関連情報

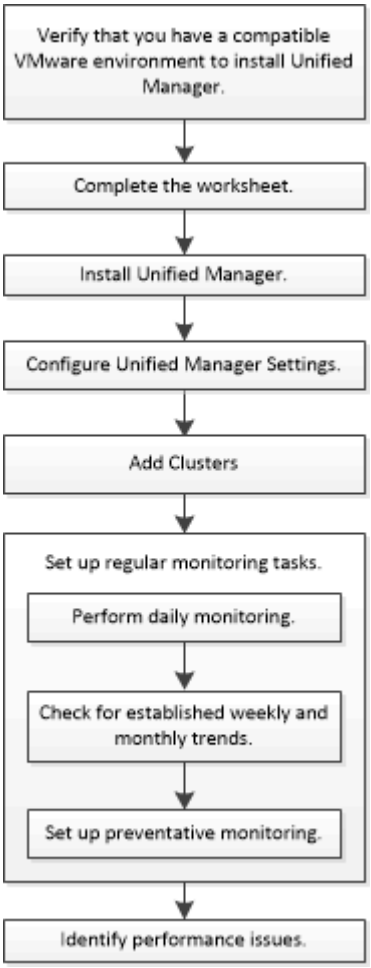
上記の想定条件に該当しない場合は、次の資料を参照してください。

- "Active IQ Unified Manager 9.8 のインストール"
- "システム管理"

パフォーマンスを監視

パフォーマンスの監視とメンテナンスのワークフローの概要

クラスタパフォーマンスの監視と保守では、Active IQ Unified Managerソフトウェアをインストールし、基本的な監視タスクを設定し、パフォーマンスの問題を特定して、必要に応じて調整を行います。



VMware 環境がサポートされていることを確認します

Active IQ Unified Manager を正しくインストールするには、VMware環境が要件を満たしていることを確認する必要があります。

手順

1. VMware インフラが Unified Manager のインストールに必要なサイジング要件を満たしていることを確認します。
2. にアクセスします "互換性マトリックス" 次のコンポーネントについて、サポートされている組み合わせであることを確認します。
   - ONTAPバージョン
   - ESXi オペレーティングシステムのバージョン
   - VMware vCenter Server のバージョン
   - VMware Tools のバージョン
   - ブラウザのタイプとバージョン

     。 "互換性マトリックス" に、 Unified Manager でサポートされる構成を示します。
3. 選択した構成の構成名をクリックします。

   その構成の詳細が [構成の詳細] ウィンドウに表示されます。
4. 次のタブの情報を確認します。
   - 注：

     お使いの構成に固有の重要なアラートおよび情報が表示されます。
   - ポリシーとガイドライン

     すべての構成に関する一般的なガイドラインが表示されます。

Active IQ Unified Manager ワークシート

Active IQ Unified Manager のインストール、設定、および接続に進む前に、環境に関する特定の情報を確認しておく必要があります。この情報はワークシートに記録できます。

Unified Manager のインストール情報

ソフトウェアが導入されている仮想マシン	あなたの価値
ESXi サーバの IP アドレス	
ホストの完全修飾ドメイン名	

ホストの IP アドレス	
ネットワークマスク	
ゲートウェイの IP アドレス	
プライマリ DNS アドレス	
セカンダリ DNS アドレス	
検索ドメイン	
メンテナンスユーザのユーザ名	
メンテナンスユーザのパスワード	

Unified Manager の設定情報

設定	あなたの価値
メンテナンスユーザの E メールアドレス	
NTPサーバ	
SMTP サーバのホスト名または IP アドレス	
SMTPユーザ名	
SMTPパスワード	
SMTP のデフォルトポート	25 （デフォルト値）
アラート通知の送信元 E メールアドレス	
LDAP のバインド識別名	
LDAP のバインドパスワード	
Active Directory の管理者名	
Active Directory のパスワード	

認証サーバのベース識別名	
認証サーバのホスト名または IP アドレス	

クラスタ情報

Unified Manager で各クラスタについて次の情報を確認します。

クラスタ 1 / N	あなたの価値
ホスト名またはクラスタ管理 IP アドレス	
ONTAP 管理者のユーザ名 管理者には「 admin 」ロールが割り当てられている必要があります。	
ONTAP 管理者のパスワード	
プロトコル（ HTTP または HTTPS ）	

関連情報

"管理者認証と RBAC"

Active IQ Unified Manager をインストールします

Active IQ Unified Manager をダウンロードして導入

ソフトウェアをインストールするには、仮想アプライアンス（ VA ）インストールファイルをダウンロードし、 VMware vSphere Client を使用して VMware ESXi サーバに導入する必要があります。VA は OVA ファイルとして提供されます。

手順

1. NetApp Support Siteソフトウェアのダウンロード * ページにアクセスし、 Active IQ Unified Manager を探します。

   https://mysupport.netapp.com/products/index.html

2. [Select Platform* （プラットフォームの選択）] ドロップダウンメニューで [* VMware vSphere* （ VMware vSphere * ）] を選択し、 [* Go!* （実行）] をクリックします
3. 「OVA」ファイルを、VMware vSphere Clientからアクセス可能なローカルまたはネットワーク上の場所に保存します。
4. VMware vSphere Client で、 * File * > * Deploy OVF Template * をクリックします。
5. 「OVA」ファイルを探し、ウィザードを使用してESXiサーバに仮想アプライアンスを導入します。

ウィザードの * Properties * タブを使用して、静的な構成情報を入力できます。

6. VM の電源をオンにします。
7. 最初の起動プロセスを表示するには、 * Console * タブをクリックします。
8. プロンプトに従って、 VM に VMware Tools をインストールします。
9. タイムゾーンを設定します。
10. メンテナンスユーザの名前とパスワードを入力します。
11. VM コンソールに表示された URL にアクセスします。

Active IQ Unified Manager の初期設定を行います

Web UI への初回アクセス時に Active IQ Unified Manager の初期セットアップダイアログボックスが表示されます。このダイアログボックスでは、いくつかの初期設定を行ったり、クラスタを追加したりできます。

手順

1. AutoSupport のデフォルトの有効設定をそのまま使用します。
2. NTP サーバの詳細、メンテナンスユーザの E メールアドレス、 SMTP サーバのホスト名、およびその他の SMTP オプションを入力し、 * Save * をクリックします。

完了後

初期セットアップが完了すると、クラスタデータソースページが表示され、クラスタの詳細を確認できます。

監視対象のクラスタを指定します

クラスタを監視対象に含め、クラスタの検出ステータスを確認したり、クラスタのパフォーマンスを監視したりするには、クラスタを Active IQ Unified Manager サーバに追加する必要があります。

必要なもの

- 次の情報が必要です。
  - ホスト名またはクラスタ管理 IP アドレス

    ホスト名は、 Unified Manager がクラスタへの接続に使用する完全修飾ドメイン名（ FQDN ）または短縮名です。このホスト名は、クラスタ管理 IP アドレスに解決される必要があります。

  クラスタ管理 IP アドレスは、管理用 Storage Virtual Machine （ SVM ）のクラスタ管理 LIF である必要があります。ノード管理 LIF を使用すると処理に失敗します。

  - ONTAP 管理者のユーザ名とパスワード
  - クラスタおよびクラスタのポート番号で設定できるプロトコルのタイプ（ HTTP または HTTPS ）
- アプリケーション管理者またはストレージ管理者のロールが必要です。
- ONTAP 管理者に ONTAPI と SSH の管理者ロールが必要です。
- Unified Manager の FQDN を使用して、 ONTAP に ping を実行できる必要があります。

これは、ONTAP コマンドを使用して確認できます `ping -node node_name -destination Unified_Manager_FQDN`。

このタスクについて

MetroCluster 構成では、ローカルクラスタとリモートクラスタの両方を追加し、クラスタを正しく設定する必要があります。

手順

1. [* Configuration * > * Cluster Data Sources *] をクリックします。
2. [クラスタ] ページで、 [* 追加] をクリックします。
3. Add Cluster * （クラスタの追加）ダイアログボックスで、クラスタのホスト名または IP アドレス（ IPv4 または IPv6 ）、ユーザ名、パスワード、通信プロトコル、ポート番号など、必要な値を指定します。

   デフォルトでは HTTPS プロトコルが選択されています。

   クラスタ管理 IP アドレスは、 IPv6 から IPv4 または IPv4 から IPv6 に変更できます。次の監視サイクルが完了すると、クラスタグリッドとクラスタ設定ページに新しい IP アドレスが反映されます。
4. [追加（ Add ）] をクリックします。
5. HTTPS を選択した場合は、次の手順を実行します。

   a. [* Authorize Host * （ホストの認証 * ）] ダイアログボックスで、 [* View Certificate * （証明書の表示）] をクリックしてクラスタに関する証明書情報を表示します。

   b. 「 * はい * 」をクリックします。

      Unified Manager で証明書がチェックされるのはクラスタを最初に追加したときだけですが、 ONTAP に対する API 呼び出しごとに確認されるわけではありません。

   証明書の期限が切れているクラスタは追加できません。SSL 証明書を更新してから、クラスタを追加する必要があります。
6. * オプション * ：クラスタ検出ステータスを表示します。

   a. クラスタセットアップ * ページでクラスタ検出ステータスを確認します。

   デフォルトの監視間隔である約 15 分後に、 Unified Manager データベースにクラスタが追加されます。

基本的な監視タスクを設定

日々の監視を実行します

監視を毎日実行することで、注意が必要なパフォーマンスの問題にすぐに対処することができます。

手順

1. Active IQ Unified Manager UI から * Event Inventory * ページに移動して、現在のイベントと廃止状態のイベントをすべて表示します。
2. [表示]*オプションで、を選択します `Active Performance Events` 必要なアクションを決定します。

週 / 月単位のパフォーマンスの傾向からパフォーマンスの問題を特定

パフォーマンスの傾向を特定すると、ボリュームレイテンシを分析して、クラスタの使用率が高すぎる / 低すぎる状況を特定するのに役立ちます。同様の手順に従って、 CPU やネットワークなど、システムのその他のボトルネックについても特定できます。

手順

1. 使用率が高すぎるか低すぎる疑いがあるボリュームを探します。
2. [ボリュームの詳細 **]** タブで、 **[*30 d**] をクリックして履歴データを表示します。
3. [データのブレークダウンの条件] ドロップダウンメニューで、 [**Latency**] を選択し、 [**Submit**] をクリックします。
4. クラスタコンポーネント比較グラフで「 * Aggregate 」を選択解除し、クラスタのレイテンシをボリュームレイテンシグラフと比較します。
5. アグリゲートを選択し、クラスタコンポーネント比較チャート内の他のすべてのコンポーネントの選択を解除して、アグリゲートのレイテンシをボリュームレイテンシチャートと比較します。
6. 読み取り / 書き込みレイテンシのグラフをボリュームレイテンシのグラフと比較します。
7. クライアントアプリケーションの負荷が原因でワークロードの競合が発生していないかどうかを確認し、必要に応じてワークロードのバランスを調整
8. アグリゲートの使用率が高すぎて競合を引き起こしていないかどうかを確認し、必要に応じてワークロードのバランスを調整

パフォーマンスしきい値を使用してイベント通知を生成

イベントは、事前に定義された状況が発生したとき、またはパフォーマンスカウンタの値がしきい値を超えたときに、 Active IQ Unified Manager で自動的に生成される通知です。イベントによって、監視しているクラスタ内のパフォーマンスの問題を特定できます。特定の重大度タイプのイベントが発生したときに自動的に E メール通知を送信するアラートを設定できます。

パフォーマンスしきい値を設定

重大なパフォーマンスの問題を監視するために、パフォーマンスしきい値を設定することができます。ユーザ定義のしきい値の場合、定義されたしきい値に近づいたとき、またはしきい値を超えたときに、警告または重大イベントの通知がトリガーされます。

手順

1. 警告イベントと重大イベントのしきい値を作成します。
   a. [* Configuration * > * Performance Thresholds *] を選択します。
   b. [作成（ Create ）] をクリックします。
   c. オブジェクトタイプを選択し、ポリシーの名前と概要を指定します。
   d. オブジェクトカウンタの条件を選択し、警告イベントと重大イベントの制限値を指定します。
   e. イベントを送信するために制限値に違反する必要がある期間を選択し、 [保存] をクリックします。
2. しきい値ポリシーをストレージオブジェクトに割り当てます。

a. 以前に選択したクラスタオブジェクトタイプのインベントリページに移動し、 View オプションから * Performance * を選択します。

b. しきい値ポリシーを割り当てるオブジェクトを選択し、 * しきい値ポリシーの割り当て * をクリックします。

c. 前の手順で作成したポリシーを選択し、 * ポリシーの割り当て * をクリックします。

例

重大なパフォーマンスの問題を特定するためにユーザ定義のしきい値を設定することができます。たとえば、ボリュームのレイテンシが20ミリ秒を超えるとMicrosoft Exchange Serverがクラッシュすることがわかっている場合は、警告しきい値を12ミリ秒、重大しきい値を15ミリ秒のように設定できます。このしきい値の設定を使用して、ボリュームのレイテンシが制限を超えたときに通知を受け取ることができます。

アラートを追加します

特定のイベントが生成されたときに通知するようにアラートを設定できます。アラートは、単一のリソース、リソースのグループ、または特定の重大度タイプのイベントについて設定することができます。通知を受け取る頻度を指定したり、アラートにスクリプトを関連付けたりできます。

必要なもの

- イベント生成時に Active IQ Unified Manager サーバからユーザに通知を送信できるように、通知に使用するユーザの E メールアドレス、 SMTP サーバ、 SNMP トラップホストなどを設定しておく必要があります。
- アラートをトリガーするリソースとイベント、および通知するユーザのユーザ名または E メールアドレスを確認しておく必要があります。
- イベントに基づいてスクリプトを実行する場合は、 Scripts ページを使用して Unified Manager にスクリプトを追加しておく必要があります。
- アプリケーション管理者またはストレージ管理者のロールが必要です。

このタスクについて

アラートは、ここで説明するように、 Alert Setup ページからアラートを作成するだけでなく、イベントを受信した後に Event Details ページから直接作成できます。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Alert Setup * をクリックします。
2. [* Alert Setup*] ページで、 [* Add] をクリックします。
3. [* アラートの追加 *] ダイアログボックスで、 [* 名前 *] をクリックし、アラートの名前と概要を入力します。
4. [* リソース] をクリックし、アラートに含めるリソースまたはアラートから除外するリソースを選択します。

   [* 次を含む名前（ * Name Contains ）] フィールドでテキスト文字列を指定してフィルタを設定し、リソースのグループを選択できます。指定したテキスト文字列に基づいて、フィルタルールに一致するリソー

スのみが使用可能なリソースのリストに表示されます。指定するテキスト文字列では、大文字と小文字が区別されます。

あるリソースが対象に含めるルールと除外するルールの両方に該当する場合は、除外するルールが優先され、除外されたリソースに関連するイベントについてはアラートが生成されません。

5. [*Events] をクリックし、アラートをトリガーするイベント名またはイベントの重大度タイプに基づいてイベントを選択します。

   複数のイベントを選択するには、 Ctrl キーを押しながら選択します。

6. [*Actions] をクリックし、通知するユーザを選択し、通知頻度を選択し、 SNMP トラップをトラップレシーバに送信するかどうかを選択し、アラートが生成されたときに実行するスクリプトを割り当てます。

   ユーザに対して指定されている E メールアドレスを変更し、アラートを再び開いて編集しようとすると、変更した E メールアドレスが以前に選択したユーザにマッピングされていないため、名前フィールドは空白になります。また、選択したユーザの E メールアドレスを Users ページで変更した場合、変更後の E メールアドレスは反映されません。

   SNMP トラップを使用してユーザに通知することもできます。

7. [保存（ Save ）] をクリックします。

アラートの追加例

この例は、次の要件を満たすアラートを作成する方法を示しています。

- アラート名： HealthTest
- リソース：名前に「 abc 」が含まれるすべてのボリュームを対象に含め、名前に「 xyz 」が含まれるすべてのボリュームを対象から除外する
- イベント：健全性に関するすべての重大なイベントを含みます
- アクション：「 sample@domain.com 」、「 Test 」スクリプトが含まれ、 15 分ごとにユーザに通知する必要があります

[Add Alert] ダイアログボックスで、次の手順を実行します。

1. [名前]をクリックし、と入力します `HealthTest` [アラート名]フィールドに入力します。
2. [* リソース] をクリックし、 [含める] タブで、ドロップダウン・リストから [* ボリューム] を選択します。
   a. 入力するコマンド `abc` [名前に次の文字を含む]*フィールドに、名前に「abc」を含むボリュームを表示します。
   b. 「 * + 」を選択します[All Volumes whose name contains 'abc']+* を使用可能なリソース領域から選択したリソース領域に移動します。
   c. [除外する]をクリックし、と入力します `xyz` [名前に*が含まれています]フィールドで、[*追加]をクリックします。
3. [* イベント **]** をクリックし、 **[** イベントの重要度 **]** フィールドから **[** クリティカル *] を選択します。
4. [Matching Events] 領域から [*All Critical Events] を選択し、 [Selected Events] 領域に移動します。

5. [アクション]をクリックし、と入力します `sample@domain.com` [これらのユーザーにアラートを送信]フィールドに入力します。
6. 15 分ごとにユーザに通知するには、「 * 15 分ごとに通知する」を選択します。

   指定した期間、受信者に繰り返し通知を送信するようにアラートを設定できます。アラートに対してイベント通知をアクティブにする時間を決める必要があります。

7. 実行するスクリプトの選択メニューで、 * テスト * スクリプトを選択します。
8. [保存（ Save ）] をクリックします。

アラートを設定

アラートについて、アラートをトリガーする Active IQ Unified Manager のイベント、アラートを受け取る E メール受信者、およびアラートの頻度を指定することができます。

必要なもの

アプリケーション管理者のロールが必要です。

このタスクについて

次のタイプのパフォーマンスイベントについて、固有のアラートを設定できます。

- 重大イベント：ユーザ定義のしきい値に違反したときにトリガーされます
- 警告イベント：ユーザ定義のしきい値、システム定義のしきい値、または動的なしきい値に違反したときにトリガーされます

デフォルトでは、すべての新しいイベントについて、 Unified Manager の管理者ユーザに E メールアラートが送信されます。他のユーザに E メールアラートを送信する場合は、それらのユーザの E メールアドレスを追加します。

> 特定のタイプのイベントに関するアラートの送信を無効にするには、そのイベントカテゴリですべてのチェックボックスをオフにする必要があります。この処理を実行しても、イベントがユーザインターフェイスに表示されるのを停止することはありません。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Alert Setup * を選択します。

   [Alert Setup] ページが表示されます。

2. [* 追加] をクリックし、各イベントタイプに適切な設定を行います。

   E メールアラートを複数のユーザに送信する場合は、各 E メールアドレスをカンマで区切って入力します。

3. [保存（ Save ）] をクリックします。

Active IQ Unified Manager のパフォーマンスの問題を特定する

パフォーマンスイベントが発生した場合は、 Active IQ Unified Manager で問題のソースを特定し、他のツールを使用して修正することができます。イベントの発生を知らせる

E メールを受信したり、日々の監視中にイベントに気付いたりすることがあります。

手順

1. E メール通知に記載されたリンクをクリックし、パフォーマンスイベントが発生しているストレージオブジェクトに直接移動します。

状況	作業
イベントの E メール通知を受信する	リンクをクリックしてイベントの詳細ページに直接移動します。
Event Inventory ページの分析中にイベントに注目してください	イベントを選択してイベントの詳細ページに直接移動します。

2. システム定義のしきい値を超えたイベントの場合は、画面に提示される対処方法に従って問題をトラブルシューティングします。
3. ユーザ定義のしきい値を超えたイベントの場合は、イベントを分析して対処が必要かどうかを判断します。
4. 問題が解決しない場合は、次の設定を確認します。
   - ストレージシステムのプロトコル設定
   - イーサネットスイッチまたはファブリックスイッチのネットワーク設定
   - ストレージシステムのネットワーク設定
   - ストレージシステムのディスクレイアウトとアグリゲートの指標を表示します
5. 問題が解除されない場合は、テクニカルサポートにお問い合わせください。

Active IQ デジタルアドバイザを使用して、システムのパフォーマンスを確認します

ネットアップにAutoSupport テレメトリを送信するONTAP システムについては、広範なパフォーマンスデータと容量データを表示できます。Active IQ には、 System Manager に表示されるよりも長時間にわたるシステムパフォーマンスが表示されます。

CPU 利用率、レイテンシ、 IOPS 、プロトコル別の IOPS 、およびネットワークスループットのグラフを表示できます。このデータは .csv 形式でダウンロードして、他のツールで分析することもできます。

Active IQ では、このパフォーマンスデータに加えて、ワークロード別のストレージ効率を表示して、そのワークロードタイプの想定される削減率と比較することができます。容量の傾向を確認して、特定の期間に追加する必要があるストレージの推定量を確認できます。

- Storage Efficiency は、メインダッシュボードの左側にあるお客様、クラスタ、ノードの各レベルで利用できます。
- パフォーマンスは、メインダッシュボードの左側のクラスタレベルとノードレベルで利用できます。

関連情報

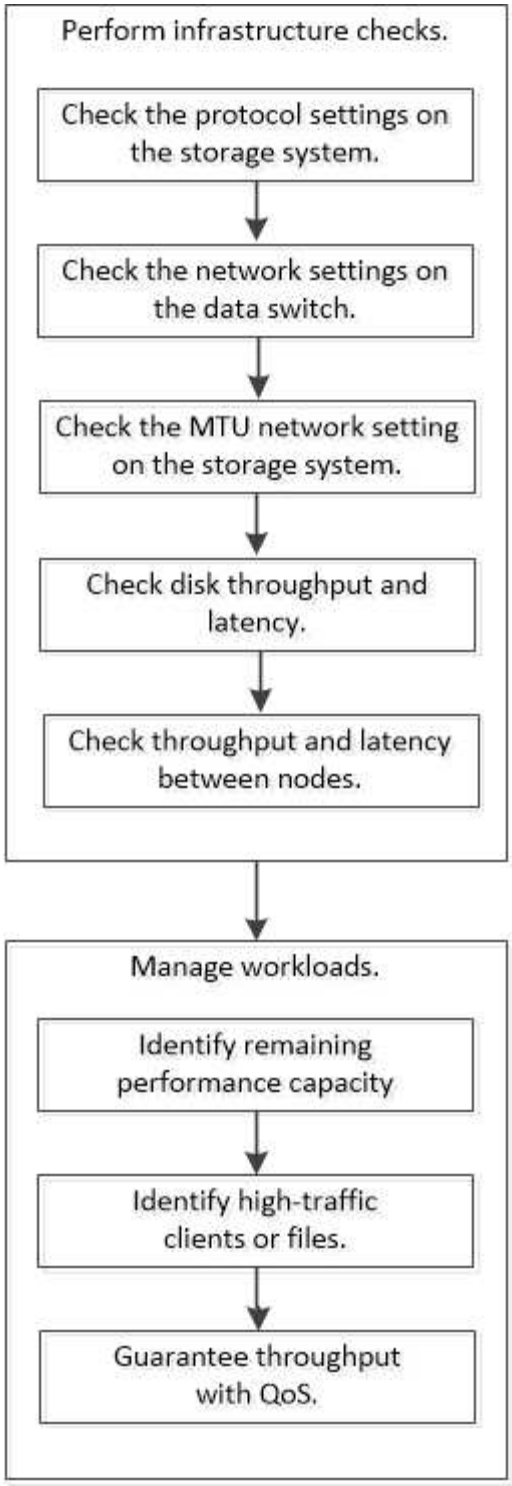
- "Active IQ デジタルアドバイザのドキュメント"

- "Active IQ デジタルアドバイザビデオ再生リスト"
- "Active IQ Web ポータル"

パフォーマンスの問題を管理

パフォーマンス管理ワークフロー

パフォーマンス問題を特定したら、インフラに関するいくつかの基本的な診断チェックを実施して明らかな構成エラーを排除できます。このチェックで問題が見つからなければ、ワークロード管理の問題について調べることができます。



基本的なインフラチェックを実施

ストレージシステムのプロトコル設定を確認してください

NFS の **TCP** 最大転送サイズを確認します

NFS の場合、読み取りと書き込みの TCP 最大転送サイズがパフォーマンス問題の原因になっていないかどうかを確認することができます。このサイズが原因でパフォーマンスが低下している可能性がある場合は、サイズを大きくして対処できます。

必要なもの

- このタスクを実行するには、クラスタ管理者の権限が必要です。
- このタスクを実行するには、 advanced 権限レベルのコマンドを使用する必要があります。

手順

1. advanced 権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. TCP 最大転送サイズを確認します。

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

3. TCP 最大転送サイズが小さすぎる場合は、サイズを大きくします。

   ```
   vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
   ```

4. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

次の例は、のTCP最大転送サイズを変更します `SVM1` 1048576まで：

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

iSCSI の TCP 読み取り / 書き込みサイズを確認します

iSCSI の場合、 TCP 読み取り / 書き込みサイズを確認して、サイズ設定がパフォーマンス問題を作成中であるかどうかを判断できます。サイズが問題のソースである場合は、サイズを変更して対処できます。

必要なもの

このタスクを実行するには、 advanced 権限レベルのコマンドが必要です。

手順

1. advanced 権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. TCP ウィンドウサイズの設定を確認します。

   ```
   vserver iscsi show -vserv,er vserver_name -instance
   ```

3. TCP ウィンドウサイズの設定を変更します。

   ```
   vserver iscsi modify -vserver vserver_name -tcp-window-size integer
   ```

4. admin 権限に戻ります。

   ```
   set -privilege admin
   ```

例

次の例は、のTCPウィンドウサイズを変更します `SVM1` 131、400バイトまで：

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

CIFS 多重化設定を確認します

低速な CIFS ネットワークが原因でパフォーマンス問題が発生する場合は、多重化設定を変更して対処することができます。

手順

1. CIFS 多重化設定を確認します。

   ```
   vserver cifs options show -vserver -vserver_name -instance
   ```

2. CIFS 多重化設定を変更します。

   ```
   vserver cifs options modify –vserver -vserver_name –max-mpx integer
   ```

例

次に、の最大多重化カウントを変更する例を示します `SVM1` 255まで：

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

FC アダプタのポート速度を確認します

パフォーマンスを最適化するには、アダプタのターゲットポートの速度を接続先デバイスの速度と同じにします。ポートに自動ネゴシエーションが設定されている場合、ギブバックやテイクオーバーなどの中断後の再接続に時間がかかる可能性があります。

必要なもの

このアダプタをホームポートとして使用しているすべての LIF をオフラインにする必要があります。

手順

1. アダプタをオフラインにします。

   ```
   network fcp adapter modify -node nodename -adapter adapter -state down
   ```

2. ポートアダプタの最大速度を確認します。

   ```
   fcp adapter show -instance
   ```

3. 必要に応じてポート速度を変更します。

   ```
   network fcp adapter modify -node nodename -adapter adapter -speed
   {1|2|4|8|10|16|auto}
   ```

4. アダプタをオンラインにします。

   ```
   network fcp adapter modify -node nodename -adapter adapter -state up
   ```

5. アダプタのすべての LIF をオンラインにします。

   ```
   network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }
   -status-admin up
   ```

例

次の例は、アダプタのポート速度を変更します `0d` オン `node1` 2 Gbpsまで：

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

データスイッチのネットワーク設定を確認します

クライアント、サーバ、ストレージシステム（ネットワークエンドポイント）で MTU 設定を同じにする必要がありますが、パフォーマンスに影響しないように、 NIC やスイッチなどの中間ネットワークデバイスを最大 MTU 値に設定する必要があります。

パフォーマンスを最大限に高めるには、ネットワーク内のすべてのコンポーネントでジャンボフレームを転送できる必要があります（ 9 、 000 バイトの IP 、 9022 バイトのイーサネットを含む）。データスイッチは 9022 バイト以上に設定する必要がありますが、ほとんどのスイッチでは 9216 という一般的な値があります。

手順

データスイッチの場合は、 MTU サイズが 9022 以上に設定されていることを確認します。

詳細については、スイッチベンダーのマニュアルを参照してください。

ストレージシステムの **MTU** ネットワーク設定を確認

ストレージシステムのネットワーク設定がクライアントや他のネットワークエンドポイントと同じでない場合は、設定を変更することができます。管理ネットワークの MTU 設定は 1500 に設定されていますが、データネットワークの MTU サイズは 9000 にしてください。

このタスクについて

管理トラフィックを処理する e0M ポートを除き、ブロードキャストドメイン内のすべてのポートの MTU サイズが同じです。ポートがブロードキャストドメインの一部である場合は、を使用します `broadcast-domain modify` コマンドを使用して、変更したブロードキャストドメイン内のすべてのポートのMTUを変更します。

NIC やデータスイッチなどの中間ネットワークデバイスの MTU サイズは、ネットワークエンドポイントよりも大きく設定できます。詳細については、を参照してください "データスイッチのネットワーク設定を確認します"。

手順

1. ストレージシステムの MTU ポート設定を確認します。

   ```
   network port show -instance
   ```

2. ポートで使用されているブロードキャストドメインのMTUを変更します。

   ```
   network port broadcast-domain modify -ipspace ipspace -broadcast-domain
   broadcast_domain -mtu new _mtu
   ```

例

次の例では、MTUポート設定を9000に変更します。

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain
Cluster -mtu 9000
```

ディスクのスループットとレイテンシを確認

ディスクのスループットとレイテンシの指標を確認すると、クラスタノードのトラブルシューティングに役立ちます。

このタスクについて

このタスクを実行するには、 advanced 権限レベルのコマンドが必要です。

手順

1. advanced 権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. ディスクのスループットとレイテンシの指標を確認します。

   ```
   statistics disk show -sort-key latency
   ```

例

次の例は、に対する各ユーザの読み取り/書き込み処理の合計を表示します `node2` オン `cluster1`：

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
                     Busy Total Read  Write  Read    Write   *Latency
  Disk       Node   (%)   Ops   Ops   Ops   (Bps)    (Bps)       (us)
------------ ----   ---- ----   ----- ----- ------   -----    -----

1.10.20      node2     4    5       3     2  95232  367616    23806
1.10.8       node2     4    5       3     2 138240  386048    22113

1.10.6       node2     3    4       2     2  48128  371712    19113
1.10.19      node2     4    6       3     2 102400  443392    19106

1.10.11      node2     4    4       2     2 122880  408576    17713
```

ノード間のスループットとレイテンシを確認

を使用できます `network test-path` コマンドを使用してネットワークのボトルネックを特定したり、ノード間のネットワークパスを事前に確認したりできます。このコマンドは、クラスタ間のノード間でもクラスタ内のノード間でも実行できます。

必要なもの

- このタスクを実行するには、クラスタ管理者である必要があります。
- このタスクを実行するには、 advanced 権限レベルのコマンドが必要です。
- クラスタ間のパスの場合、ソースクラスタとデスティネーションクラスタがピアリングされている必要があります。

このタスクについて

ノード間のネットワークパフォーマンスが、パス構成に対して期待される値にならない場合があります。たとえば、ソースクラスタとデスティネーションクラスタの間のリンクが 10GbE の場合でも、 SnapMirror レプリケーション処理による大量のデータ転送では 1Gbps の伝送速度が観察されることがあります。

を使用できます `network test-path` ノード間のスループットとレイテンシを測定するコマンド。このコマンドは、クラスタ間のノード間でもクラスタ内のノード間でも実行できます。

> このテストはネットワークパスが一杯になるまでデータを投入するため、システムがビジーでなく、ノード間のネットワークトラフィックが集中していないときに実行してください。テストは 10 秒後にタイムアウトします。このコマンドは、 ONTAP 9 のノード間でのみ実行できます。

。 `session-type` オプションは、ネットワークパスで実行する処理のタイプを指定します。たとえば、リモートデスティネーションへのSnapMirrorレプリケーションの場合は「AsyncMirrorRemote」と指定します。タイプによって、テストで使用されるデータの量が決まります。次の表に、セッションタイプを示します。

セッションタイプ（ Session Type ）	説明

AsyncMirrorLocal です	SnapMirrorによって同じクラスタ内のノード間で使用される設定
AsyncMirrorRemote	異なるクラスタのノード間のSnapMirrorで使用される設定（デフォルトタイプ）
RemoteDataTransfer	ONTAP が同じクラスタ内のノード間のリモートデータアクセスに使用する設定（たとえば、別のノードのボリュームに格納されたファイルを取得するためのノードへのNFS要求）

手順

1. advanced 権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. ノード間のスループットとレイテンシを測定します。

   ```
   network test-path -source-node source_nodename |local -destination-cluster
   destination_clustername -destination-node destination_nodename -session-type
   Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
   ```

   ソースノードはローカルクラスタにある必要があります。デスティネーションノードはローカルクラスタまたはピアクラスタに含めることができます。の値は「local」です `-source-node` コマンドを実行するノードを指定します。

   次のコマンドは、間のSnapMirrorタイプのレプリケーション処理のスループットとレイテンシを測定します `node1` ローカルクラスタおよび `node3` オン `cluster2`：

   ```
   cluster1::> network test-path -source-node node1 -destination-cluster
   cluster2 -destination-node node3 -session-type AsyncMirrorRemote
   Test Duration:      10.88 secs
   Send Throughput:    18.23 MB/sec
   Receive Throughput: 18.23 MB/sec
   MB sent:            198.31
   MB received:        198.31
   Avg latency in ms:  2301.47
   Min latency in ms:  61.14
   Max latency in ms:  3056.86
   ```

3. admin 権限に戻ります。

   ```
   set -privilege admin
   ```

完了後

パス構成に対して期待される値を得られない場合は、ノードのパフォーマンス統計の確認、ツールを使用した

ネットワークの問題の切り分け、スイッチ設定の確認などを行います。

ワークロードの管理

残りのパフォーマンス容量を特定します

パフォーマンス容量（ *headroom* ）は、リソースのワークロードのパフォーマンスにレイテンシの影響を受ける前にノードまたはアグリゲートに配置できる作業量を測定します。クラスタで利用可能なパフォーマンス容量を知っておくと、ワークロードのプロビジョニングと分散に役立ちます。

必要なもの

このタスクを実行するには、 advanced 権限レベルのコマンドが必要です。

このタスクについて

には次の値を使用できます `-object` ヘッドルームの統計を収集および表示するオプション：

- CPUの場合は、 `resource_headroom_cpu`。
- アグリゲートの場合 `resource_headroom_aggr`。

この作業は、 System Manager および Active IQ Unified Manager を使用して実行することもできます。

手順

1. advanced 権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. リアルタイムのヘッドルーム統計の収集を開始します。

   ```
   statistics start -object resource_headroom_cpu|aggr
   ```

   コマンド構文全体については、マニュアルページを参照してください。

3. リアルタイムのヘッドルーム統計情報を表示します。

   ```
   statistics show -object resource_headroom_cpu|aggr
   ```

   コマンド構文全体については、マニュアルページを参照してください。

4. admin 権限に戻ります。

   ```
   set -privilege admin
   ```

例

次の例は、クラスタノードの 1 時間あたりの平均ヘッドルーム統計を表示します。

ノードの使用可能なパフォーマンス容量は、を引いて計算できます `current_utilization` からカウンタを開きます `optimal_point_utilization` カウンタ。この例では、の利用率 `CPU_sti2520-213` IS-14%（72%~86%）は、CPUの過去1時間の平均利用率が高すぎることを示しています。

指定することもできました `ewma_daily`、 `ewma_weekly`または `ewma_monthly` 同じ情報をより長期間にわたって平均化することができます。

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
  (statistics show)

Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213

    Counter                                                     Value
    -------------------------------- ---------------------------------
    ewma_hourly                                                     -
                         current_ops                             4376
                     current_latency                            37719
                current_utilization                               86
                  optimal_point_ops                             2573
              optimal_point_latency                             3589
          optimal_point_utilization                               72
     optimal_point_confidence_factor                               1

Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214

    Counter                                                     Value
    -------------------------------- ---------------------------------
    ewma_hourly                                                     -
                         current_ops                                0
                     current_latency                                0
                current_utilization                                 0
                  optimal_point_ops                                 0
              optimal_point_latency                                 0
          optimal_point_utilization                                71
     optimal_point_confidence_factor                                1
2 entries were displayed.
```

トラフィックの多いクライアントやファイルを特定

ONTAP の Active Objects テクノロジを使用すると、クラスタのトラフィック量を著しく

増大させているクライアントやファイルを特定することができます。このような「上位」のクライアントやファイルを特定したら、クラスタワークロードをリバランシングするか、別の手順に従って問題を解決できます。

必要なもの

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. クラスタに最もアクセスする上位のクライアントを表示します。

   `statistics top client show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   コマンド構文全体については、マニュアルページを参照してください。

   次のコマンドは、アクセス頻度の高い上位のクライアントを表示します `cluster1`：

```
cluster1::> statistics top client show

cluster1 : 3/23/2016 17:59:10


                                                 *Total
         Client Vserver           Node Protocol    Ops
-------------- ------- -------------- -------- ------
172.17.180.170     vs4 siderop1-vsim4      nfs    668
172.17.180.169     vs3 siderop1-vsim3      nfs    337
172.17.180.171     vs3 siderop1-vsim3      nfs    142
172.17.180.170     vs3 siderop1-vsim3      nfs    137
172.17.180.123     vs3 siderop1-vsim3      nfs    137
172.17.180.171     vs4 siderop1-vsim4      nfs     95
172.17.180.169     vs4 siderop1-vsim4      nfs     92
172.17.180.123     vs4 siderop1-vsim4      nfs     92
172.17.180.153     vs3 siderop1-vsim3      nfs      0
```

2. クラスタで最も多くアクセスされる上位のファイルを表示します。

   `statistics top file show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   コマンド構文全体については、マニュアルページを参照してください。

   次のコマンドは、でアクセスされる上位のファイルを表示します `cluster1`：

```
cluster1::> statistics top file show

cluster1 : 3/23/2016 17:59:10

                                    *Total
                     File Volume Vserver          Node    Ops
------------------------ ------ ------- -------------- ------
/vol/vol1/vm170-read.dat   vol1     vs4 siderop1-vsim4     22
/vol/vol1/vm69-write.dat   vol1     vs3 siderop1-vsim3      6
     /vol/vol2/vm171.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol2/vm169.dat   vol2     vs3 siderop1-vsim3      2
      /vol/vol2/p123.dat   vol2     vs4 siderop1-vsim4      2
      /vol/vol2/p123.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol1/vm171.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim3      2
      /vol/vol1/p123.dat   vol1     vs4 siderop1-vsim4      2
```

QoS でスループットを保証

QoS の概要を使用してスループットを保証

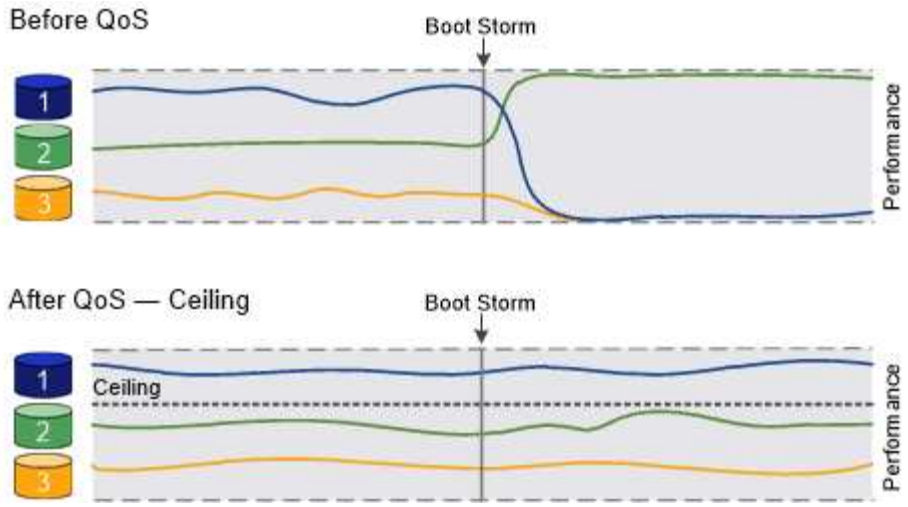
ストレージサービス品質（ QoS ）を使用して、重要なワークロードのパフォーマンスが競合するワークロードの影響を受けて低下しないようにすることができます。競合するワークロードに Throughput Ceil天 を設定して、システムリソースへの影響を制限したり、重要なワークロードに Throughput Floor_ を設定したりすることで、競合するワークロードによる要求に関係なく最小のスループットターゲットを満たすことができます。同じワークロードに対して上限と下限を設定することもできます。

スループットの上限（最大 **QoS** ）について

スループットの上限は、ワークロードのスループットを最大 IOPS / MBps 、または IOPS / MBps に制限します。次の図では、ワークロード 2 がワークロード 1 および 3 の Bully とならないようにスループットの上限が設定されています。

a_policy group_ は、 1 つ以上のワークロードに対するスループットの上限を定義します。ワークロードとは、 a_storage オブジェクト： _a ボリューム、ファイル、 qtree 、または LUN 、あるいは SVM 内のすべてのボリューム、ファイル、 qtree 、または LUN の I/O 処理のことです。上限はポリシーグループの作成時に指定できるほか、ワークロードをしばらく監視したあとで指定することもできます。

> ワークロードのスループットは、特にスループットが急激に変化した場合、指定された上限を 10% までは超過することができます。バースト時には、上限を 50% まで超過することができます。バーストは、トークンが 150% まで累積した場合に単一ノードで発生します



スループットの下限（最小 **QoS** ）について

スループットの下限は、ワークロードのスループットが最小IOPS、最小MBps、またはIOPSとMBpsを下回らないことを保証します。次の図では、ワークロード 1 とワークロード 3 のスループットの下限により、ワークロード 2 からの要求に関係なく、最小スループットが確保されています。

これらの例からわかるように、スループットの上限はスループットを直接調整するのに対し、スループットの下限は下限が設定されたワークロードを優先することでスループットを間接的に調整します。

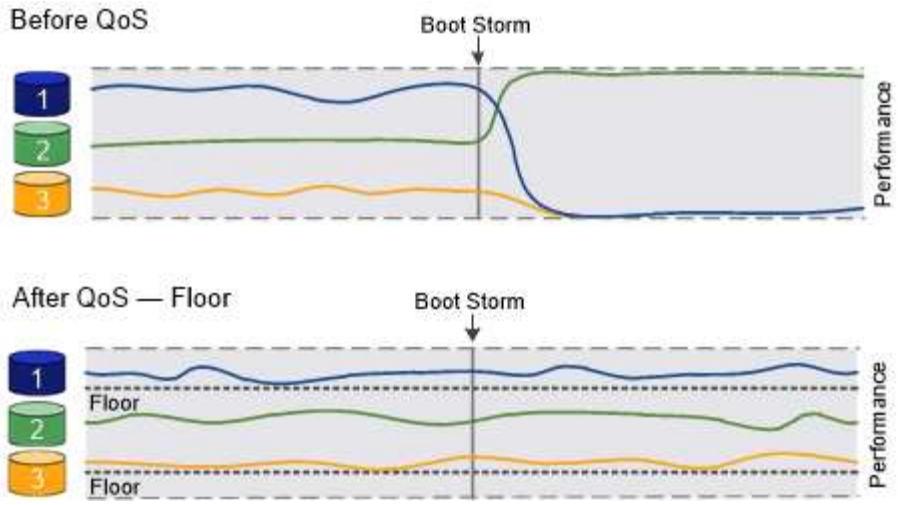
下限はポリシーグループの作成時に指定できるほか、ワークロードをしばらく監視したあとで指定することもできます。

ONTAP 9.13.1以降では、を使用してSVMスコープでスループットの下限を設定できます [adaptive-qos-templates]。ONTAP 9.13.1より前のリリースでは、スループットの下限を定義するポリシーグループはSVMに適用できません。

ONTAP 9.7 より前のリリースでは、使用可能なパフォーマンス容量が十分にある場合にスループットの下限が保証されます。

ONTAP 9.7 以降では、使用可能なパフォーマンス容量が不足している場合でもスループットの下限を保証できます。この新しいフロアビヘイビアをフロア v2 と呼びます。この保証を満たすために、 v2 のフロアを使用すると、スループットの下限や下限の設定を超える作業を行わなくても、ワークロードのレイテンシが高くなる可能性があります。QoS とアダプティブ QoS の両方をサポートするフロア v2 環境。

ONTAP 9.7P6以降では、下限v2の新しい動作を有効または無効にするオプションを使用できます。などの重要な処理の実行中は、ワークロードが指定された下限を下回ることがあります `volume move trigger-cutover`。利用可能な容量が十分にあり、重要な処理が実行されていない場合でも、ワークロードのスループットは指定された下限を 5% まで下回ることができます。オーバープロビジョニングされたフロアやパフォーマンス容量がないワークロードがある場合、指定された下限を下回ることがあります。



共有および非共有の **QoS** ポリシーグループについて

ONTAP 9.4 以降では、 _non-shared_QoS ポリシーグループを使用して、定義されたスループットの上限または下限の環境を各メンバーのワークロードごとに指定できます。_shared_policy グループの動作は ' ポリシー・タイプによって異なります

- スループットの上限については、共有ポリシーグループに割り当てられたワークロードの合計スループットが指定した上限以下でなければなりません。
- スループットの下限については、共有ポリシーグループを適用できるのは単一のワークロードのみです。

アダプティブ **QoS** について

通常、ストレージオブジェクトに割り当てたポリシーグループの値は固定値です。ストレージオブジェクトのサイズが変わったときは、値を手動で変更する必要があります。たとえば、ボリュームの使用スペースが増えた場合、通常は指定されているスループットの上限も増やす必要があります。

アダプティブ QoS _ ワークロードのサイズの変更に合わせてポリシーグループの値が自動的に調整され、 TB または GB あたりの IOPS が一定に維持されます。これは、何百何千という数のワークロードを管理する大規模な環境では大きなメリットです。

アダプティブ QoS は、主にスループットの上限の調整に使用しますが、下限の管理（ワークロードサイズが増えた場合）に使用することもできます。ワークロードのサイズは、ストレージオブジェクトに割り当てられたスペースまたはストレージオブジェクトで使用されているスペースのいずれかで表されます。

> ONTAP 9.5 以降では、使用済みスペースをスループットの下限に使用できます。ONTAP 9.4 以前では使用できません。

- 割り当て済みスペースのポリシーでは、ストレージオブジェクトの公称サイズを基準に IOPS と TB / GB の比率が維持されます。比率が 100 IOPS/GB の場合、 150GB のボリュームのスループットの上限はボリュームのサイズが変更されないかぎり 15 、 000 IOPS です。ボリュームのサイズが 300GB に変更されると、アダプティブ QoS によってスループットの上限が 30 、 000 IOPS に調整されます。
- a_used space-policy （デフォルト）は、ストレージ効率化前に格納されている実際のデータの量に基づいて、 IOPS/TB|GB の比率を維持します。比率が 100 IOPS/GB の場合、 100GB のデータが格納された 150GB のボリュームのスループットの上限は 10 、 000 IOPS です。使用済みスペースの量が変わると、アダプティブ QoS によって比率が一定になるようにスループットの上限が調整されます。

ONTAP 9.5 以降では、アプリケーションに I/O ブロックサイズを指定することで、スループット制限を IOPS と MBps の両方で指定できます。MBps の制限は、ブロックサイズに IOPS 制限を掛けて計算されます。たとえば、 32K の I/O ブロックサイズで IOPS の制限が 6144 IOPS/TB の場合、 MBps の制限は 192MBps になります。

以下は、スループットの上限と下限の両方に対して想定される動作です。

- アダプティブ QoS ポリシーグループにワークロードを割り当てると、上限または下限がただちに更新されます。
- アダプティブ QoS ポリシーグループに含まれるワークロードのサイズを変更すると、上限または下限が約 5 分で更新されます。

更新が実行されるためにはスループットが少なくとも 10 IOPS 増加する必要があります。

アダプティブ QoS ポリシーグループは常に非共有です。定義されているスループットの上限または下限の環境各メンバーワークロードを個別に定義します。

ONTAP 9.6以降では、SSDを使用するONTAP Select Premiumでスループットの下限がサポートされます。

アダプティブポリシーグループテンプレート

ONTAP 9.13.1以降では、アダプティブQoSテンプレートをSVMに設定できます。アダプティブポリシーグループテンプレートを使用すると、SVM内のすべてのボリュームにスループットの下限と上限を設定できます。

アダプティブポリシーグループテンプレートは、SVMの作成後にのみ設定できます。を使用します `vserver modify` コマンドにを指定します `-qos-adaptive-policy-group-template` ポリシーを設定するパラメータ。

アダプティブポリシーグループテンプレートを設定すると、ポリシーの設定後に作成または移行されたボリュームには自動的にポリシーが継承されます。ポリシーテンプレートを割り当てても、SVM上の既存のボリュームには影響しません。SVMでポリシーを無効にすると、以降SVMに移行または作成されたボリュームにポリシーは適用されません。アダプティブポリシーグループテンプレートを無効にしても、ポリシーテンプレートが保持されるため、そのポリシーテンプレートを継承したボリュームには影響しません。

詳細については、を参照してください アダプティブポリシーグループテンプレートを設定します。

一般的なサポート

次の表に、スループットの上限、スループットの下限、およびアダプティブ QoS のサポート状況を示します。

リソースまたは機能	スループットの上限	スループットの下限	スループットの下限 **v2**	アダプティブ **QoS**
ONTAP 9 バージョン	すべて	9.2以降	9.7以降	9.3以降

リソースまたは機能	スループットの上限	スループットの下限	スループットの下限 **v2**	アダプティブ **QoS**
プラットフォーム	すべて	• AFF • C190 * • ONTAP Select プレミアム SSD *	• AFF • C190 • SSD を使用する ONTAP Select Premium	すべて
プロトコル	すべて	すべて	すべて	すべて
FabricPool	はい。	階層化ポリシーが「 none 」に設定され、ブロックがクラウドにない場合は「 Yes 」です。	階層化ポリシーが「 none 」に設定され、ブロックがクラウドにない場合は「 Yes 」です。	いいえ
SnapMirror Synchronous	はい。	いいえ	いいえ	はい。

C190とONTAP Selectのサポートは、ONTAP 9.6リリースから開始されました。

スループットの上限がサポートされるワークロード

次の表に、スループットの上限がサポートされるワークロードを ONTAP 9 のバージョン別に示します。ルートボリューム、負荷共有ミラー、およびデータ保護ミラーはサポートされません。

ワークロード - 上限	**ONTAP 9.0**	**ONTAP 9.1**	**ONTAP 9.2**	**ONTAP 9.3**	**ONTAP 9.4~9.7**	**ONTAP 9.8**以降
ボリューム	はい。	はい。	はい。	はい。	はい。	はい。
ファイル。	はい。	はい。	はい。	はい。	はい。	はい。
LUN	はい。	はい。	はい。	はい。	はい。	はい。
SVM	はい。	はい。	はい。	はい。	はい。	はい。
FlexGroup ボリューム	いいえ	いいえ	いいえ	はい。	はい。	はい。
qtree *	いいえ	いいえ	いいえ	いいえ	いいえ	はい。

ワークロード - 上限	ONTAP 9.0	ONTAP 9.1	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4~9.7	ONTAP 9.8以降
ポリシーグループごとに複数のワークロードが割り当てられます	はい。	はい。	はい。	はい。	はい。	はい。
非共有のポリシーグループ	いいえ	いいえ	いいえ	いいえ	はい。	はい。

ONTAP 9.8以降では、NFSが有効なFlexVolおよびFlexGroupのqtreeでNFSアクセスがサポートされます。ONTAP 9.9.1以降では、SMBが有効なFlexVol およびFlexGroup ボリュームのqtreeでもSMBアクセスがサポートされます。

スループットの下限がサポートされるワークロード

次の表に、スループットの下限がサポートされるワークロードを ONTAP 9 のバージョン別に示します。ルートボリューム、負荷共有ミラー、およびデータ保護ミラーはサポートされません。

ワークロード - 下限	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4~9.7	ONTAP 9.8-9.13.0	ONTAP 9.13.1以降
ボリューム	はい。	はい。	はい。	はい。	はい。
ファイル。	いいえ	はい。	はい。	はい。	はい。
LUN	はい。	はい。	はい。	はい。	はい。
SVM	いいえ	いいえ	いいえ	いいえ	はい。
FlexGroup ボリューム	いいえ	いいえ	はい。	はい。	はい。
qtree *	いいえ	いいえ	いいえ	はい。	はい。
ポリシーグループごとに複数のワークロードが割り当てられます	いいえ	いいえ	はい。	はい。	はい。
非共有のポリシーグループ	いいえ	いいえ	はい。	はい。	はい。

* ONTAP 9.8以降では、NFSが有効なFlexVol およびFlexGroup のqtreeでNFSアクセスがサポートされます。ONTAP 9.9.1以降では、SMBが有効なFlexVol およびFlexGroup ボリュームのqtreeでもSMBアクセスがサポートされます。

アダプティブ **QoS** がサポートされるワークロード

次の表に、アダプティブ QoS がサポートされるワークロードを ONTAP 9 のバージョン別に示します。ルートボリューム、負荷共有ミラー、およびデータ保護ミラーはサポートされません。

ワークロード - アダプティブ **QoS**	**ONTAP 9.3**	**ONTAP 9.4-9.13.0**	**ONTAP 9.13.1**以降
ボリューム	はい。	はい。	はい。
ファイル。	いいえ	はい。	はい。
LUN	いいえ	はい。	はい。
SVM	いいえ	いいえ	はい。
FlexGroup ボリューム	いいえ	はい。	はい。
ポリシーグループごとに複数のワークロードが割り当てられます	はい。	はい。	はい。
非共有のポリシーグループ	はい。	はい。	はい。

ワークロードとポリシーグループの最大数

次の表に、ワークロードとポリシーグループの最大数を ONTAP 9 のバージョン別に示します。

ワークロードのサポート	**ONTAP 9.3**以前	**ONTAP 9.4**以降
クラスタあたりの最大ワークロード	12、000	4万だ
ノードあたりの最大ワークロード	12、000	4万だ
ポリシーグループの最大数	12、000	12、000

スループットの下限 **v2** を有効または無効にします

AFF のスループットの下限 v2 を有効または無効にすることができます。デフォルトは enabled です。フロア v2 を有効にした場合、他のワークロードのレイテンシが高くなってもコントローラを多用した場合はスループットの下限を満たすことができます。QoS とアダプティブ QoS の両方をサポートするフロア v2 環境。

手順

1. advanced 権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. 次のいずれかのコマンドを入力します。

状況	使用するコマンド
フロア v2 を無効にします	`qos settings throughput-floors-v2 -enable false`

状況	使用するコマンド
フロア v2 を有効にします	`qos settings throughput-floors-v2 -enable true`

> MetroCluster クラスタでスループットの下限 v2 を無効にするには、を実行する必要があります
>
> `qos settings throughput-floors-v2 -enable false`
>
> コマンドは、ソースとデスティネーションの両方のクラスタで実行します。

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

ストレージ **QoS** のワークフロー

QoS で管理するワークロードのパフォーマンス要件がすでにわかっている場合は、ポリシーグループを作成するときにスループットの制限を指定できます。それ以外の場合は、ワークロードを監視したうえで指定することができます。

QoS を使用してスループットの上限を設定する

を使用できます `max-throughput` ストレージオブジェクトのワークロードのスループットの上限（最大QoS）を定義するポリシーグループのフィールド。ポリシーグループは、ストレージオブジェクトを作成または変更するときに適用できます。

必要なもの

- ポリシーグループを作成するには、クラスタ管理者である必要があります。
- ポリシーグループを SVM に適用するには、クラスタ管理者である必要があります。

このタスクについて

- ONTAP 9.4 以降では、 _non-shared_QoS ポリシーグループを使用して、定義されたスループットの上限環境を各メンバーのワークロードごとに指定できます。ポリシーグループが _shared ：ポリシーグループに割り当てられているワークロードの合計スループットが指定した上限を超えることはできません。

  設定 `-is-shared=false` をクリックします `qos policy-group create` 非共有ポリシーグループを指定するコマンド。

- スループットの上限は、 IOPS 、 MB/ 秒、またはその両方で指定できますIOPS と MB/ 秒の両方を指定した場合、先に上限に達した方が適用されます。

  > 同じワークロードに対して上限と下限を設定する場合、スループット制限は IOPS 単位でのみ指定できます。

- QoS 制限の対象となるストレージオブジェクトは、ポリシーグループが属している SVM に含める必要が

あります。同じ SVM に複数のポリシーグループを作成することができます。

- 下位のオブジェクトまたは子オブジェクトがポリシーグループに属している場合は、そのストレージオブジェクトをポリシーグループに割り当てることはできません。
- ストレージオブジェクトのタイプごとに同じ QoS グループポリシーを適用することを推奨します。

手順

1. ポリシーグループを作成する。

   `qos policy-group create -policy-group` *`policy_group`* `-vserver` *`SVM`* `-max -throughput` *`number_of_iops`*`|Mb/S|iops,Mb/S -is-shared true|false`

   コマンド構文全体については、マニュアルページを参照してください。を使用できます `qos policy-group modify` コマンドを使用してスループットの上限を調整します。

   次のコマンドは、共有ポリシーグループを作成します `pg-vs1` 最大スループットが5、000 IOPSの場合：

   ```
   cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1
   -max-throughput 5000iops -is-shared true
   ```

   次のコマンドは、非共有ポリシーグループを作成します `pg-vs3` 最大スループットが100 IOPS、400KB/秒の場合：

   ```
   cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
   -max-throughput 100iops,400KB/s -is-shared false
   ```

   次のコマンドは、非共有ポリシーグループを作成します `pg-vs4` スループット制限なし：

   ```
   cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
   -is-shared false
   ```

2. ポリシーグループを SVM 、ファイル、ボリューム、または LUN に適用します。

   `storage_object` `create -vserver` *`SVM`* `-qos-policy-group` *`policy_group`*

   コマンド構文全体については、マニュアルページを参照してください。を使用できます *`storage_object`* `modify` ストレージオブジェクトに別のポリシーグループを適用するコマンド。

   次のコマンドは、ポリシーグループを適用します `pg-vs1` SVMに移動します `vs1`：

   ```
   cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
   ```

   次のコマンドは、ポリシーグループを適用します `pg-app` ボリュームに移動します `app1` および `app2`：

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app
```

3. ポリシーグループのパフォーマンスを監視します。

   `qos statistics performance show`

   コマンド構文全体については、マニュアルページを参照してください。

   > パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

   次のコマンドは、ポリシーグループのパフォーマンスを表示します。

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_vs1                   5008       19.56MB/s     2.45ms
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

4. ワークロードのパフォーマンスを監視します。

   `qos statistics workload performance show`

   コマンド構文全体については、マニュアルページを参照してください。

   > パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

   次のコマンドは、ワークロードのパフォーマンスを表示します。

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app1-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

を使用できます `qos statistics workload latency show` コマンドを使用してQoSワークロードの詳細なレイテンシ統計を表示します。

QoS を使用してスループットの下限を設定します

を使用できます `min-throughput` ストレージオブジェクトのワークロードのスループットの下限（最小QoS）を定義するポリシーグループのフィールド。ポリシーグループは、ストレージオブジェクトを作成または変更するときに適用できます。ONTAP 9.8 以降では、スループットの下限を IOPS または MBps で指定できるようになりました。

作業を開始する前に

- ONTAP 9.2 以降が実行されている必要があります。スループットの下限は ONTAP 9.2 以降で使用できます。
- ポリシーグループを作成するには、クラスタ管理者である必要があります。
- ONTAP 9.13.1以降では、を使用してSVMレベルでスループットの下限を適用できます アダプティブポリシーグループテンプレート。QoSポリシーグループを含むSVMにアダプティブポリシーグループテンプレートを設定することはできません。

このタスクについて

- ONTAP 9.4 以降では、 _non-shared_qos ポリシーグループを使用して、定義したスループットの下限を各メンバーワークロードに個別に適用するように指定できます。スループットの下限が定義されたポリシーグループを複数のワークロードに適用できるのは、この場合だけです。

  設定 `-is-shared=false` をクリックします `qos policy-group create` 共有されていないポリシーグループを指定するコマンド。

- ノードまたはアグリゲートに十分なパフォーマンス容量（ヘッドルーム）がない場合は、ワークロードのスループットが指定された下限を下回ることがあります。
- QoS 制限の対象となるストレージオブジェクトは、ポリシーグループが属している SVM に含める必要があります。同じ SVM に複数のポリシーグループを作成することができます。
- ストレージオブジェクトのタイプごとに同じ QoS グループポリシーを適用することを推奨します。
- スループットの下限を定義するポリシーグループは、 SVM には適用できません。

手順

1. の説明に従って、ノードまたはアグリゲートに十分なパフォーマンス容量があることを確認します "残りのパフォーマンス容量を特定しています"。

2. ポリシーグループを作成する。

   `qos policy-group create -policy group` *`policy_group`* `-vserver` *`SVM`* `-min -throughput` *`qos_target`* `-is-shared true|false`

   コマンド構文全体については、 ONTAP リリースのマニュアルページを参照してください。を使用できます `qos policy-group modify` スループットの下限を調整するコマンド。

   次のコマンドは、共有ポリシーグループを作成します `pg-vs2` 最小スループットが1、000 IOPSの場合：

   ```
   cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2
   -min-throughput 1000iops -is-shared true
   ```

   次のコマンドは、非共有ポリシーグループを作成します `pg-vs4` スループット制限なし：

   ```
   cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4
   -is-shared false
   ```

3. ポリシーグループをボリュームまたは LUN に適用します。

   `storage_object` `create -vserver` *`SVM`* `-qos-policy-group` *`policy_group`*

   コマンド構文全体については、マニュアルページを参照してください。を使用できます `_storage_object_modify` ストレージオブジェクトに別のポリシーグループを適用するコマンド。

   次のコマンドは、ポリシーグループを適用します `pg-app2` ボリュームに移動します `app2`：

   ```
   cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
   -qos-policy-group pg-app2
   ```

4. ポリシーグループのパフォーマンスを監視します。

   `qos statistics performance show`

   コマンド構文全体については、マニュアルページを参照してください。

   > パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

   次のコマンドは、ポリシーグループのパフォーマンスを表示します。

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_app2                  7216       28.19MB/s   420.00us
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

5. ワークロードのパフォーマンスを監視します。

   `qos statistics workload performance show`

   コマンド構文全体については、マニュアルページを参照してください。

   > パフォーマンスはクラスタから監視します。ホスト上のツールを使用してパフォーマンスを監視しないでください。

   次のコマンドは、ワークロードのパフォーマンスを表示します。

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app2-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

   > を使用できます `qos statistics workload latency show` コマンドを使用してQoSワークロードの詳細なレイテンシ統計を表示します。

アダプティブ **QoS** ポリシーグループを使用する

アダプティブ QoS ポリシーグループを使用すると、ボリュームサイズの変更に合わせてスループットの上限や下限を自動的に調整し、 TB または GB あたりの IOPS を一定に保つことができます。これは、何百何千という数のワークロードを管理する大規模な環境では大きなメリットです。

作業を開始する前に

- ONTAP 9.3以降が実行されている必要があります。アダプティブ QoS ポリシーグループは ONTAP 9.3 以降で使用できます。
- ポリシーグループを作成するには、クラスタ管理者である必要があります。

このタスクについて

ストレージオブジェクトは、アダプティブまたは非アダプティブどちらかのポリシーグループのメンバーにすることができますが、両方のメンバーにすることはできません。SVM はストレージオブジェクトとポリシーで同じである必要があります。ストレージオブジェクトはオンラインである必要があります。

アダプティブ QoS ポリシーグループは常に非共有です。定義されているスループットの上限または下限の環境各メンバーワークロードを個別に定義します。

ストレージオブジェクトサイズに対するスループット制限の比率は、以下に示すフィールドの組み合わせによって決まります。

- `expected-iops` は、割り当て済み（TB / GB）あたりの最小想定IOPSです。

> `expected-iops` は、`AFF` プラットフォームでのみ保証されます。`expected-iops` `FabricPool` については、階層化ポリシーが「`none`」に設定されていて、ブロックがクラウドにない場合にのみ保証されます。`expected-iops` は、`SnapMirror Synchronous`関係にないボリュームに対して保証されます。

- `peak-iops` は、割り当て済みまたは使用済み（TB / GB）あたりの最大IOPSです。
- `expected-iops-allocation` expected-iopsに割り当てスペース（デフォルト）と使用スペースのどちらを使用するかを示します。

> `expected-iops-allocation` ONTAP 9.5以降で使用できます。ONTAP 9.4 以前ではサポートされません。

- `peak-iops-allocation` に割り当てスペースと使用済みスペース（デフォルト）のどちらを使用するかを示します `peak-iops`。
- `absolute-min-iops` は、絶対最小IOPSです。このフィールドは非常に小さいストレージオブジェクトで使用します。両方を上書きします `peak-iops` および / または `expected-iops` いつ `absolute-min-iops` が計算されたよりも大きい `expected-iops`。

  たとえば、を設定した場合です `expected-iops` を1、000 IOPS/TBに設定し、ボリュームサイズが1GB未満である場合は、を計算します `expected-iops` 分数IOPになります。計算された `peak-iops` さらに小さな割合になりますこれを回避するには、を設定します `absolute-min-iops` 現実的な値に。

- `block-size` アプリケーションI/Oブロックサイズを指定します。デフォルトは32Kです。有効な値は、8K 、 16K 、 32K 、 64K 、 ANY です。ANY は、ブロックサイズが適用されないことを意味します。

次の表に示す 3 種類のアダプティブ QoS ポリシーグループがデフォルトで用意されています。これらのポリシーグループはボリュームに直接適用することができます。

デフォルトのポリシーグループ	想定 IOPS/TB	最大 IOPS/TB	絶対最小 IOPS
`extreme`	6,144	一二、二八八	1000
`performance`	2 、 048	四、〇 九六	500ドル

value	128	512	七五

下位のオブジェクトまたは子オブジェクトがポリシーグループに属している場合は、そのストレージオブジェクトをポリシーグループに割り当てることはできません。次の表に、制限事項を示します。

割り当て内容	以下のオブジェクトはポリシーグループに割り当てできない
SVM をポリシーグループに割り当てます	SVM に含まれているストレージオブジェクトのポリシーグループへの割り当て
ボリューム：ポリシーグループに割り当てます	そのボリュームを含む SVM または子 LUN
LUN	その LUN を含むボリュームまたは SVM
ファイルをポリシーグループに追加します	そのファイルを含むボリュームまたは SVM

手順

1. アダプティブ QoS ポリシーグループを作成します。

   `qos adaptive-policy-group create -policy group` *`policy_group`* `-vserver` *`SVM`* `-expected-iops` *`number_of_iops`*`/TB|GB -peak-iops` *`number_of_iops`*`/TB|GB -expected -iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-space -absolute-min-iops` *`number_of_iops`* `-block-size 8K|16K|32K|64K|ANY`

   コマンド構文全体については、マニュアルページを参照してください。

   > `-expected-iops-allocation` および `-block-size` ONTAP 9.5以降で使用できます。ONTAP 9.4 以前ではこれらのオプションがサポートされません。

   次のコマンドは、アダプティブQoSポリシーグループを作成します `adpg-app1` を使用 `-expected -iops` TBあたり300 IOPS/TBに設定 `-peak-iops` TBあたり1、000 IOPSに設定 `-peak-iops -allocation` をに設定します `used-space`` および ``-absolute-min-iops` 50 IOPSに設定：

   ```
   cluster1::> qos adaptive-policy-group create -policy group adpg-app1
   -vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
   -allocation used-space -absolute-min-iops 50iops
   ```

2. アダプティブ QoS ポリシーグループをボリュームに適用します。

   `volume create -vserver SVM -volume` *`volume`* `-aggregate` *`aggregate`* `-size` *`number_of`* `TB|GB -qos-adaptive-policy-group` *`policy_group`*

   コマンド構文全体については、マニュアルページを参照してください。

   次のコマンドは、アダプティブQoSポリシーグループを適用します `adpg-app1` ボリュームに移動します

app1：

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

次のコマンドは、デフォルトのアダプティブQoSポリシーグループを適用します extreme 新しいボリュームに移動します app4 および既存のボリュームに追加します app5。ポリシーグループの環境 ボリュームに対して定義されたスループットの上限 app4 および app5 個別：

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

アダプティブポリシーグループテンプレートを設定します

ONTAP 9.13.1以降では、アダプティブポリシーグループテンプレートを使用して、SVMレベルでスループットの下限と上限を適用できます。

このタスクについて

- アダプティブポリシーグループテンプレートはデフォルトポリシーです apg1。ポリシーはいつでも変更できます。CLIまたはONTAP REST APIでのみ設定でき、既存のSVMにのみ適用できます。
- アダプティブポリシーグループテンプレートは、ポリシーの設定後にSVMで作成またはSVMに移行されるボリュームにのみ影響します。SVM上の既存のボリュームのステータスは維持されます。

  アダプティブポリシーグループテンプレートを無効にした場合、SVM上のボリュームの既存のポリシーは保持されます。無効化の影響を受けるのは、あとでSVMに作成または移行されたボリュームだけです。

- QoSポリシーグループを含むSVMにアダプティブポリシーグループテンプレートを設定することはできません。
- アダプティブポリシーグループテンプレートは、AFF プラットフォーム向けに設計されています。アダプティブポリシーグループテンプレートは他のプラットフォームでも設定できますが、ポリシーによって最小スループットが適用されない場合があります。同様に、FabricPool アグリゲートまたは最小スループットをサポートしないアグリゲート内のSVMにアダプティブポリシーグループテンプレートを追加することもできますが、スループットの下限は適用されません。
- SVMがMetroCluster 構成またはSnapMirror関係に含まれている場合は、ミラーされたSVMにアダプティブポリシーグループテンプレートが適用されます。

手順

1. SVMを変更してアダプティブポリシーグループテンプレートを適用します。
   `vserver modify -qos-adaptive-policy-group-template apg1`
2. ポリシーが設定されたことを確認します。

```
vserver show -fields qos-adaptive-policy-group
```

Unified Manager を使用してクラスタパフォーマンスを監視する

Active IQ Unified Manager を使用すると、可用性を最大限に高め、ネットアップの AFF および FAS ストレージインフラの制御を維持できるため、拡張性、サポート性、パフォーマンス、セキュリティを向上させることができます。

Active IQ Unified Manager はシステムヘルスを継続的に監視し、アラートを送信するため、お客様の組織は IT スタッフのリソースを解放できます。1 つのダッシュボードでストレージのステータスを瞬時に確認し、推奨される対処方法を通じて問題に迅速に対処できます。

ストレージのプロアクティブな管理や問題の迅速な解決に役立つ通知を検出、監視、受信できるため、データ管理が簡易化されます。 ペタバイト規模のデータを単一のダッシュボードから監視して大規模なデータを管理できるため、管理効率が向上します。

Active IQ Unified Manager を使用すると、変動するビジネスニーズに対応し、パフォーマンスデータと高度な分析を使用してパフォーマンスを最適化できます。 レポート機能を使用すると、標準レポートにアクセスしたり、ビジネス固有のニーズに合わせてカスタムの運用レポートを作成したりできます。

関連リンク：

- "Active IQ Unified Managerの詳細はこちら"
- "Active IQ Unified Manager for VMwareの利用を開始する"
- "Active IQ Unified Manager for Linusの使用を開始する"
- "Active IQ Unified Manager for Windowsの使用を開始する"

Cloud Insights を使用してクラスタパフォーマンスを監視する

NetApp Cloud Insights は、インフラ全体を可視化する監視ツールです。Cloud Insights を使用すると、パブリッククラウドやプライベートデータセンターなど、すべてのリソースの監視、トラブルシューティング、最適化を行うことができます。

Cloud Insights には 2 つのエディションがあります

Cloud Insights 基本エディションは、ネットアップデータファブリック資産の監視と最適化を目的に設計されています。HCI を含むネットアップのすべてのリソースと、環境内の All Flash FAS （ AFF ）間の接続を無償で分析します。

Cloud Insights Standard エディションは、ネットアップデータファブリックに対応したインフラコンポーネントだけでなく、マルチベンダー / マルチクラウド環境にも焦点を当てています。豊富な機能により、 100 を超えるサービスとリソースのサポートにアクセスできます。

今日の世界では、オンプレミスのデータセンターから複数のパブリッククラウドにリソースを活用しているため、アプリケーション自体からストレージアレイのバックエンドディスクまで、完全なイメージを把握することが重要です。さらに、アプリケーションの監視（ Kafka 、 MongoDB 、 Nginx など）もサポートされているため、最適な利用率レベルと完全なリスクバッファで運用するために必要な情報と知識を得ることができま

す。

どちらのエディション（ Basic および Standard ）も NetApp Active IQ Unified Manager と統合できます。Active IQ Unified Managerを使用しているお客様は、Cloud Insightsユーザインターフェイス内で参加情報を確認できます。Active IQ Unified Managerに投稿された通知は見落とされず、Cloud Insightsのイベントに関連付けることができます。つまり、両方の世界を最大限に活用できます。

すべてのリソースの監視、トラブルシューティング、最適化を行います

Cloud Insights を使用すると、問題の解決にかかる時間を大幅に短縮し、エンドユーザへの影響を防ぐことができます。 また、クラウドインフラのコスト削減にも役立ちます。 実用的な情報でデータを保護することで、内部の脅威にさらされる危険性が軽減されます。

Cloud Insights を使用すると、パブリッククラウドからデータセンターまで、ハイブリッドインフラ全体を 1 箇所で可視化できます。 必要に応じてカスタマイズできる関連ダッシュボードを瞬時に作成できます。また、組織のニーズに合わせて、ターゲットを絞ったアラートや条件付きアラートを作成することもできます。

高度な異常検出機能により、問題が発生する前にプロアクティブに解決できます。 リソースの競合と低下を自動的に確認して、影響を受けたワークロードを迅速にリストアできます。 スタック内のさまざまなコンポーネント間の関係を自動的に構築することで、トラブルシューティングがより迅速になります。

使用されていないリソースや放置されたリソースを環境全体で特定することで、インフラの規模を適正化し、支出全体を最適化する機会を見つけ出すことができます。

Cloud Insights は、システムトポロジを可視化し、 Kubernetes アーキテクチャを把握します。Kubernetes クラスタの健常性を監視できます。問題が発生しているノードを監視し、問題が発生したときにズームインすることができます。

Cloud Insights は、高度な機械学習と異常検出機能により、悪意のあるユーザや侵害されたユーザによる組織データの不正利用を防止し、内部の脅威に関する実用的な情報を提供します。

Cloud Insights は Kubernetes 指標を可視化することで、ポッド、ノード、クラスタ間の関係を完全に把握できるようになります。クラスタまたは作業ポッドの正常性、および現在処理中の負荷を評価できます。これにより、 K8S クラスタのコマンドを実行し、展開の健全性とコストの両方を制御できます。

関連リンク

- "Cloud Insightsの詳細はこちら"
- "Cloud Insightsの使用を開始する"

監査ロギング

ONTAP での監査ログの実装方法

監査ログに記録された管理アクティビティは標準の AutoSupport レポートに、特定のログアクティビティは EMS メッセージに含まれています。監査ログを指定の場所に転送したり、 CLI や Web ブラウザを使用して監査ログファイルを表示することもできます。

ONTAP 9.11.1以降では、System Managerを使用して監査ログの内容を表示できます。

ONTAP 9.12.1以降では、ONTAPで監査ログの改ざんアラートが提供されます。ONTAPは、audit.logファイルの改ざんをチェックするために毎日のバックグラウンドジョブを実行し、変更または改ざんされたログファイルが見つかるとEMSアラートを送信します。

ONTAP では、クラスタで実行された管理アクティビティについて、発行された要求、要求を発行したユーザ、ユーザのアクセス方法、要求が発行された時間などの情報が記録されます。

管理アクティビティには次のタイプがあります。

- set要求。通常は表示以外のコマンドや操作が該当します
  - これらの要求は、を実行したときに発行されます `create`、 `modify`または `delete` たとえば、コマンドです。
  - set 要求はデフォルトで記録されます。
- get要求。情報を取得して管理インターフェイスに表示します
  - これらの要求は、を実行したときに発行されます `show` たとえば、コマンドです。
  - GET要求はデフォルトでは記録されませんが、ONTAP CLIから送信されるGET要求を制御できます (`-cliget`）、ONTAP APIから (`-ontapiget`）、またはREST APIから (`-httpget`）がファイルに記録されます。

ONTAP は、の管理アクティビティを記録します `/mroot/etc/log/mlog/audit.log` ノードのファイル。CLI コマンドの 3 つのシェル（クラスタシェル、ノードシェル、および非対話型システムシェル）からのコマンドに加え、 API コマンドがここに記録されます（対話型システムシェルのコマンドは記録されません）。監査ログには、クラスタ内のすべてのノードの時刻が同期しているかどうかを示すタイムスタンプが含まれています。

。 `audit.log` ファイルは、AutoSupport ツールによって指定された受信者に送信されます。また、 Splunk や syslog サーバなど、指定した外部の送信先にコンテンツを安全に転送することもできます。

。 `audit.log` ファイルは1日単位でローテーションされます。また、サイズが 100MB に達したときにもローテーションが実行されます。以前の 48 個のコピーは保持されます（最大合計 49 個のファイル）。監査ファイルが 1 日単位のローテーションを実行するときは、 EMS メッセージは生成されません。監査ファイルのサイズが上限を超えたためにローテーションが実行された場合は、 EMS メッセージが生成されます。

ONTAP 9 における監査ログの変更点

ONTAP 9以降では、を参照してください `command-history.log` ファイルはに置き換えられます `audit.log`および `mgwd.log` ファイルに監査情報が含まれなくなりました。ONTAP 9 にアップグレードする場合は、これらの従来のファイルとその中身を参照するスクリプトやツールを見直す必要があります。

ONTAP 9へのアップグレード後、既存 `command-history.log` ファイルは保持されます。これらは新規として回転（削除）されます `audit.log` ファイルはローテーションされます（作成されます）。

をチェックするツールとスクリプト `command-history.log` からのソフトリンクがあるため、ファイルは引き続き機能する場合があります `command-history.log` 終了： `audit.log` は、アップグレード時に作成されます。ただし、をチェックするツールとスクリプト `mgwd.log` ファイルに監査情報が含まれなくなったため、ファイルは失敗します。

また、 ONTAP 9 以降の監査ログでは、以下のエントリは有用な情報とはみなされず、原因の不要なログアク

ティビティでもあるため、記録されなくなりました。

- ONTAP によって実行される内部コマンド（ username=root のコマンド）
- コマンドのエイリアス（元のコマンドとは別に）

ONTAP 9 以降では、 TCP プロトコルと TLS プロトコルを使用して監査ログを外部の宛先に安全に送信できます。

監査ログの内容を表示します

クラスタの内容を表示できます `/mroot/etc/log/mlog/audit.log` ONTAP CLI 、System Manager、またはWebブラウザを使用して実行します。

クラスタのログファイルには、次のエントリが含まれます。

時間
: ログエントリのタイムスタンプ。

アプリケーション
: クラスタへの接続に使用するアプリケーション。指定可能な値の例はです `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, および `service-processor`。

ユーザ
: リモートユーザのユーザ名。

状態
: 監査要求の現在の状態 `success`, `pending`, または `error`。

メッセージ
: コマンドのステータスに関するエラーまたは追加情報 を含むオプションのフィールド。

セッション**ID**
: 要求を受信したセッションID。各SSH_SESSION_ISにはセッションIDが割り当てられ、各HTTP 、ONTAPI、またはSNMP_REQUESTには一意のセッションIDが割り当てられます。

Storage VM
: ユーザの接続に使用するSVM。

適用範囲
: 表示されます `svm` 要求がデータStorage VM上にある場合。それ以外の場合はと表示されます `cluster`。

コマンド**ID**
: CLIセッションで受信した各コマンドのID。これにより、要求と応答を関連付けることができます。ZAPI、HTTP、SNMPの各要求にはコマンドIDはありません。

クラスタのログエントリは、ONTAP CLIから、Webブラウザから、ONTAP 9.11.1以降のSystem Managerから表示できます。

System Manager の略

- インベントリを表示するには、[* Events & Jobs]>[Audit Logs]を選択します。[+]
  各列には、カテゴリのフィルタ、並べ替え、検索、表示、およびインベントリを制御できます。インベントリの詳細は、Excelブックとしてダウンロードできます。
- フィルタを設定するには、右上の*[Filter]*ボタンをクリックし、目的のフィールドを選択します。[+]
  セッションIDリンクをクリックして、障害が発生したセッションで実行されたすべてのコマンドを表示することもできます。

CLI の使用

クラスタ内の複数のノードからマージされた監査エントリを表示するには、+と入力します
`security audit log show [parameters]`

を使用できます `security audit log show` 個 々 のノードの監査エントリを表示するコマンド、またはクラスタ内の複数のノードの監査エントリをマージするコマンド。の内容を表示することもできます `/mroot/etc/log/mlog` Webブラウザを使用して、単一のノード上のディレクトリを作成します。詳細については、のマニュアルページを参照してください。

Web ブラウザ

の内容を表示できます `/mroot/etc/log/mlog` Webブラウザを使用して、単一のノード上のディレクトリを作成します。 "Webブラウザを使用してノードのログファイル、コアダンプファイル、MIBファイルにアクセスする方法について説明します"。

監査GET要求の設定を管理します

set要求はデフォルトで記録されますが、get要求は記録されません。ただし、ONTAP HTMLから送信されるGET要求を制御することはできます (`-httpget`）、ONTAP CLI (`-cliget`）、またはONTAP APIからアクセスできます (`-ontapiget`）がファイルに記録されます。

監査ログ設定は、ONTAP CLIから、ONTAP 9.11.1以降の監査ログ設定は、System Managerから変更できます。

System Manager の略

1. [* Events & Jobs]>[Audit Logs]を選択します。
2. をクリックします ⚙ 右上にあるをクリックし、追加または削除する要求を選択します。

CLI の使用

- デフォルトのset要求に加えて、ONTAP CLIまたはAPIからのget要求を監査ログ（audit.logファイル）に記録するように指定するには、+と入力します
  `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- 現在の設定を表示するには、+と入力します
  `security audit show`

詳細については、マニュアルページを参照してください。

監査ログの送信先を管理します

監査ログは最大で10箇所に転送できます。たとえば、 Splunk や syslog サーバにログを転送し、監視や分析、バックアップなどの目的で使用できます。

このタスクについて

転送を設定するには、転送されたログに使用するsyslogまたはSplunkホストのIPアドレス、ポート番号、転送プロトコル、syslog機能を指定する必要があります。 "syslogファシリティについて説明します"。

次のいずれかの送信値を選択できます。

UDP暗号化なし

セキュリティなしのユーザデータグラムプロトコル（デフォルト）

TCP暗号化なし

セキュリティなしのTransmission Control Protocol

TCP暗号化

Transport Layer Security（TLS）を使用したTransmission Control Protocol
[TCP暗号化プロトコル]が選択されている場合は、[VERIFY SERVER]オプションを使用できます。

監査ログは、ONTAP CLIから転送できます。ONTAP 9.11.1以降は、System Managerから転送できます。

System Manager の略

- 監査ログの送信先を表示するには、* Cluster > Settings の順に選択します。**[+]**
  ログデスティネーションの数は、[通知管理]タイル*に表示されます。をクリックします ⋮ 詳細を表示します。
- 監査ログの送信先を追加、変更、または削除するには、[**Events & Jobs]>[Audit Logs]**を選択し、画面右上の**[*Manage Audit Destinations**]をクリックします。[+]
  をクリックします + Add またはをクリックします ⋮ エントリを編集または削除するには、* Host Address *列に入力します。

CLI の使用

1. 監査ログの転送先ごとに、デスティネーション IP アドレスまたはホスト名、およびセキュリティオプションを指定します。

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

   - 状況に応じて `cluster log-forwarding create` コマンドが接続を確認するためにデスティネーションホストにpingを実行できない場合、エラーが表示されてコマンドが失敗します。推奨されませんが、を使用してください `-force` パラメータを指定すると、接続の検証が省略されます。
   - を設定した場合 `-verify-server` パラメータの値 `true`では、ログの転送先の`ID`は、証明書を検証することによって検証されます。この値はに設定できます `true` を選択した場合のみ `tcp-encrypted` の値 `-protocol` フィールド。

2. を使用して、宛先レコードが正しいことを確認します `cluster log-forwarding show` コマンドを実行します

```
cluster1::> cluster log-forwarding show

                                                   Verify Syslog
Destination Host          Port   Protocol         Server Facility
------------------------- ------ --------         ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            514    tcp-encrypted   true   user
2 entries were displayed.
```

詳細については、マニュアルページを参照してください。

AutoSupport

System Manager を使用して AutoSupport 設定を管理します

System Managerを使用して、AutoSupportアカウントの設定を管理できます。

次の手順を実行できます。

AutoSupport 設定を表示します

System Manager を使用して、 AutoSupport アカウントの設定を表示できます。

手順

1. System Manager で、 * Cluster > Settings * の順にクリックします。

   「 * AutoSupport * 」セクションには、次の情報が表示されます。

   - ステータス
   - 転送プロトコル
   - プロキシサーバ
   - 送信元 E メールアドレス

2. AutoSupport セクションで、 ⋮をクリックし、[その他のオプション]*を選択します。

   AutoSupport 接続と E メール設定については、追加情報が表示されます。また、メッセージの転送履歴も表示されます。

AutoSupport データを生成して送信します

System Manager では、 AutoSupport メッセージの生成を開始して、データを収集するクラスタノードを選択できます。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. AutoSupport セクションで、 ⋮をクリックし、[生成して送信]*を選択します。
3. 件名を入力します。
4. [データの収集元]*のチェックボックスをオンにして、データの収集元のノードを指定します。

AutoSupport への接続をテストします

System Manager からテストメッセージを送信して、 AutoSupport への接続を確認できます。

手順

1. System Manager で、 * Cluster > Settings * の順にクリックします。
2. AutoSupport セクションで、 ⋮をクリックし、[Test Connectivity]*を選択します。
3. メッセージの件名を入力します。

AutoSupport を有効または無効にします

AutoSupportは、可能性のある構成上の問題をプロアクティブに特定し、サポートケースを迅速に解決するなど、NetAppのお客様に実証済みのビジネスメリットを提供します。 新しいシステムでは、AutoSupportはデフォルトで有効になっています。必要に応じて、System Managerを使用して、ストレージシステムのヘルスを監視して通知メッセージを送信するAutoSupportの機能を無効にすることができます。 AutoSupport を無効にしたあとで再度有効にすることができます。

このタスクについて

AutoSupportを無効にする前に、NetAppコールホームシステムをオフにすると、次の利点が失われることに注意してください。

- ヘルスモニタリング：AutoSupportはストレージシステムのヘルスを監視し、テクニカルサポートおよび社内のサポート部門に通知を送信します。
- 自動化：AutoSupportはサポートケースのレポートを自動化します。ほとんどのサポートケースは、お客様が問題に気付く前に自動的にオープンされます。
- 迅速な解決: AutoSupportデータを送信するシステムでは、AutoSupportデータを送信しないシステムと比較して、サポートケースが半分の時間で解決されます。
- アップグレードの高速化：AutoSupportは、System Managerのバージョンアップグレード、アドオン、更新、ファームウェア更新の自動化など、お客様のセルフサービスワークフローを強化します。
- その他の機能：他のツールの特定の機能（BlueXPの一部のワークフローなど）は、AutoSupportが有効な場合にのみ機能します。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. AutoSupport セクションで、 ⋮をクリックし、[無効化]*を選択します。
3. AutoSupportを再度有効にする場合は、* AutoSupport セクションで ⋮をクリックし、[有効化]*を選択します。

サポートケースの生成を抑制します

ONTAP 9.10.1 以降の場合、 System Manager から AutoSupport に要求を送信して、サポートケースの生成を抑制することができます。

このタスクについて

サポートケースの生成を抑制するには、抑制を実行するノードと時間数を指定します。

システムのメンテナンス中に AutoSupport で自動ケースを作成しない場合は、サポートケースを抑制することが特に役立ちます。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. AutoSupport セクションで、 ⋮をクリックし、[Suppress Support Case Generation]*を選択します。
3. 抑制を実行する時間数を入力します。
4. 抑制を実行するノードを選択します。

サポートケースの生成を再開

ONTAP 9.10.1 以降では、 System Manager を使用してサポートケースが抑制されていれば AutoSupport から生成を再開できます。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. AutoSupport セクションで、 ⋮をクリックし、[Resume Support Case Generation]*を選択します。
3. 生成を再開するノードを選択します。

AutoSupport の設定を編集します

System Manager を使用して、 AutoSupport アカウントの接続や E メールの設定を変更することができます。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. AutoSupport セクションで、 ⋮をクリックし、[その他のオプション]*を選択します。
3. [接続]セクションまたは[電子メール]セクションで、 Edit をクリックして、いずれかのセクションの設定を変更します。

CLI を使用して AutoSupport を管理します

Manage AutoSupport の概要

AutoSupport は、システムヘルスをプロアクティブに監視し、ネットアップテクニカルサポート、社内のサポート部門、およびサポートパートナーにメッセージを自動的に送信します。テクニカルサポートへの AutoSupport メッセージの送信はデフォルトで有効になりますが、メッセージを社内のサポート部門に送信する場合は、適切なオプションを設定し、有効なメールホストを指定する必要があります。

AutoSupport 管理を実行できるのはクラスタ管理者だけです。Storage Virtual Machine （ SVM ）管理者には AutoSupport へのアクセス権はありません。

AutoSupport は、ストレージシステムの初回設定時にデフォルトで有効になります。AutoSupport は、AutoSupport が有効になってから 24 時間後にテクニカルサポートへのメッセージ送信を開始します。この間隔を 24 時間よりも短くするには、システムをアップグレードまたはリバートするか、 AutoSupport 設定を変更するか、システムの時間を 24 時間以外の時間に変更します。

> AutoSupport はいつでも無効にできますが、常に有効にしておく必要があります。AutoSupport を有効にしておくと、ストレージ・システムに問題が発生したときに、迅速に原因を判断し解決できます。デフォルトでは、 AutoSupport を無効にした場合でも、 AutoSupport の情報が収集されてローカルに格納されます。

AutoSupport の詳細については、NetApp Support Siteを参照してください。

関連情報

- "ネットアップサポート"

- "ONTAP コマンドの詳細については、 AutoSupport の CLI を参照してください"

AutoSupport と **Active IQ Digital Advisor** を使用します

ONTAP の AutoSupport コンポーネントはテレメトリを収集し、分析用に送信します。Active IQ デジタルアドバイザは AutoSupport からデータを分析し、プロアクティブなサポートと最適化を提供します。Active IQ は、人工知能を使用して潜在的な問題を特定し、ビジネスに影響が及ぶ前に解決を支援します。

Active IQ では、クラウドベースのポータルとモバイルアプリを通じて、実用的な予測分析とプロアクティブなサポートを提供することで、グローバルハイブリッドクラウド全体でデータインフラを最適化できます。SupportEdge との契約が締結されているネットアップのすべてのお客様は、 Active IQ が提供するデータ主体の分析情報と推奨事項を利用できます（機能は製品やサポートレベルによって異なります）。

Active IQ でできることは次のとおりです。

- アップグレードを計画する。Active IQ では、 ONTAP の新しいバージョンにアップグレードすることで解決可能な問題が環境内で特定されます。また、アップグレードを計画する際に役立つ Upgrade Advisor コンポーネントも用意されています。
- システムの健全性を表示します。Active IQ ダッシュボードで、健全性に関する問題が報告されるため、それらの問題の解決に役立ちます。システム容量を監視して、ストレージスペースが不足しないようにします。システムのサポートケースを表示します。
- パフォーマンスを管理Active IQ には、 System Manager に表示されるよりも長時間にわたるシステムパフォーマンスが表示されます。パフォーマンスに影響を与えている構成やシステムの問題を特定します。
- 効率性の最大化Storage Efficiency 指標を表示し、より多くのデータをより少ないスペースに格納する方法を特定します。
- インベントリと構成を表示します。Active IQ は、インベントリおよびソフトウェアとハードウェアの構成に関するすべての情報を表示します。サービス契約がいつ期限切れになるかを確認し、サービス契約を更新してサポートを継続するかを確認します。

関連情報

"ネットアップのマニュアル： Active IQ Digital Advisor"

"Active IQ を起動します"

"SupportEdge サービス"

AutoSupport メッセージが送信されるタイミングおよび場所

AutoSupport は、メッセージの種類に応じた宛先にメッセージを送信します。AutoSupport がメッセージを送信するタイミングと場所を知ると、 E メールで受信するメッセージまたは Active IQ （旧 My AutoSupport ） Web サイトに表示されるメッセージを把握するのに役立ちます。

特に指定がないかぎり、次の表に示す設定はのパラメータです `system node autosupport modify` コマンドを実行します

イベントトリガー型メッセージ

修正措置を必要とするシステムでイベントが発生した場合には、 AutoSupport からイベントトリガー型メッセージが自動的に送信されます。

メッセージが送信されたとき	メッセージの送信先
AutoSupport は、 EMS のトリガーイベントに応答します	で指定されたアドレス `-to` および `-noteto`。（送信されるのはサービスに影響する重要なイベントのみ）。 で指定されたアドレス `-partner-address` テクニカルサポート（該当する場合 `-support` がに設定されます `enable`

スケジュールされたメッセージ

AutoSupport は、定期的に複数のメッセージを自動的に送信します。

メッセージが送信されたとき	メッセージの送信先
毎日（デフォルトでは、午前 12 時からチェックする必要がありますログメッセージとして送信される）	で指定されたアドレス `-partner-address` テクニカルサポート（該当する場合 `-support` がに設定されます `enable`
毎日（デフォルトでは、午前 12 時からチェックする必要がありますパフォーマンスメッセージとして送信されます） `-perf` パラメータはに設定されます `true`	partner-address で指定されているアドレス テクニカルサポート（該当する場合 `-support` がに設定されます `enable`
毎週（デフォルトでは、日曜日の午前 0 時から午前 1 時までの間に送信されます）	で指定されたアドレス `-partner-address` テクニカルサポート（該当する場合 `-support` がに設定されます `enable`

手動でトリガーされるメッセージ

AutoSupport メッセージは、手動で送信または再送信できます。

メッセージが送信されたとき	メッセージの送信先
を使用して、手動でメッセージを送信します `system node autosupport invoke` コマンドを実行します	を使用してURIを指定した場合 `-uri` のパラメータを指定します `system node autosupport invoke` コマンドを実行すると、メッセージがそのURIに送信されます。 状況 `-uri` を省略すると、で指定したアドレスにメッセージが送信されます `-to` および `-partner -address`。このメッセージは、の場合はテクニカルサポートにも送信されます `-support` がに設定されます `enable`。
を使用して、手動でメッセージを送信します `system node autosupport invoke-core-upload` コマンドを実行します	を使用してURIを指定した場合 `-uri` のパラメータを指定します `system node autosupport invoke-core-upload` コマンドを実行すると、メッセージがそのURIに送信され、コアダンプファイルがそのURIにアップロードされます。 状況 `-uri` では省略されています `system node autosupport invoke-core-upload` コマンドを実行すると、メッセージがテクニカルサポートに送信され、コアダンプファイルがテクニカルサポートサイトにアップロードされます。 どちらのシナリオでもそれが必要です `-support` がに設定されます `enable` および `-transport` がに設定されます `https` または `http`。 コアダンプファイルのサイズが大きいため、メッセージはで指定されたアドレスに送信されません `-to` および `-partner-addresses` パラメータ

メッセージが送信されたとき	メッセージの送信先
を使用して、手動でメッセージを送信します `system node autosupport invoke-performance-archive` コマンドを実行します	を使用してURIを指定した場合 `-uri` のパラメータを指定します `system node autosupport invoke-performance-archive` コマンドを実行すると、メッセージがそのURIに送信され、パフォーマンスアーカイブファイルがそのURIにアップロードされます。 状況 `-uri` では省略されています `system node autosupport invoke-performance-archive`メッセージがテクニカルサポートに送信され、パフォーマンスアーカイブファイルがテクニカルサポートサイトにアップロードされます。 どちらのシナリオでもそれが必要です `-support` がに設定されます `enable` および `-transport` がに設定されます `https` または `http`。 パフォーマンスアーカイブファイルはサイズが大きいため、で指定したアドレスにメッセージが送信されません `-to` および `-partner-addresses` パラメータ
を使用して手動で過去のメッセージを再送信した `system node autosupport history retransmit` コマンドを実行します	で指定したURIだけに送信されます `-uri` のパラメータ `system node autosupport history retransmit` コマンドを実行します

テクニカルサポートによってトリガーされるメッセージです

テクニカルサポートは、 AutoSupport OnDemand 機能を使用して、 AutoSupport からのメッセージを要求できます。

メッセージが送信されたとき	メッセージの送信先
AutoSupport が新しい AutoSupport メッセージを生成するという送信指示を取得したとき	で指定されたアドレス `-partner-address` テクニカルサポート（該当する場合 `-support` がに設定されます `enable` および `-transport` がに設定されます `https`
過去の AutoSupport メッセージを再送信するという送信指示を AutoSupport が受け取ったとき	テクニカルサポート（該当する場合 `-support` がに設定されます `enable` および `-transport` がに設定されます `https`
コアダンプファイルまたはパフォーマンスアーカイブファイルをアップロードする新しい AutoSupport メッセージを生成するという送信指示を AutoSupport が受け取ったとき	テクニカルサポート（該当する場合 `-support` がに設定されます `enable` および `-transport` がに設定されます `https`。テクニカルサポートサイトにコアダンプファイルまたはパフォーマンスアーカイブファイルがアップロードされます。

AutoSupport でイベントトリガー型メッセージが作成されて送信される仕組み

AutoSupport では、トリガーイベントの処理時にイベントトリガー型 AutoSupport メッセージが作成されます。イベントトリガー型 AutoSupport メッセージは、対応処置が必要な問題を受信者に通知します。問題に関連する情報だけが含まれています。含めるコンテンツと、メッセージの受信者をカスタマイズできます。

AutoSupport では、次のプロセスを使用してイベントトリガー型 AutoSupport メッセージを作成し、送信します。

1. EMS がトリガーイベントを処理すると、 EMS は AutoSupport に要求を送信します。

   トリガーイベントは、AutoSupport のデスティネーションとで始まる名前を含むEMSイベントです `callhome.` プレフィックス。

2. AutoSupport により、イベントトリガー型 AutoSupport メッセージが作成されます。

   AutoSupport は、トリガーに関連付けられたサブシステムから基本的な情報とトラブルシューティング情報を収集し、トリガーイベントに関連する情報のみが含まれたメッセージを作成します。

   各トリガーには一連のデフォルトのサブシステムが関連付けられています。ただし、を使用して、追加のサブシステムをトリガーに関連付けることもできます `system node autosupport trigger modify` コマンドを実行します

3. AutoSupport は、で定義された受信者にイベントトリガー型AutoSupport メッセージを送信します `system node autosupport modify` コマンドにを指定します `-to`、 `-noteto`、 `-partner -address`および `-support` パラメータ

   を使用して、特定のトリガーに対するAutoSupport メッセージの配信を有効または無効にできます `system node autosupport trigger modify` コマンドにを指定します `-to` および `-noteto` パラメータ

特定のイベントについて送信されるデータの例

。 `storage shelf PSU failed` EMSイベントによって、必須、ログファイル、ストレージ、RAID、HA、プラットフォームサブシステム、ネットワークサブシステム、および必須サブシステム、ログファイル、およびストレージサブシステムからのトラブルシューティングデータ。

将来の対応として送信されるAutoSupport メッセージにNFSに関するデータを含めることを決定します `storage shelf PSU failed` イベント：のNFSのトラブルシューティングレベルのデータを有効にするには、次のコマンドを入力します `callhome.shlf.ps.fault` イベント：

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

を参照してください `callhome.` プレフィックスはからドロップされます `callhome.shlf.ps.fault` を使用する場合のイベント `system node autosupport trigger` （CLIのAutoSupport イベントおよびEMSイベントで参照されている場合）。

AutoSupport メッセージの種類とその内容

AutoSupport メッセージには、サポートされているサブシステムに関するステータス情報が含まれていAutoSupport メッセージの内容を把握しておくと、 E メールで受信したメッセージまたは Active IQ （旧 My AutoSupport ） Web サイトに表示されたメッセージを解釈したり、応答したりするときに役立ちます。

メッセージのタイプ	メッセージに含まれるデータのタイプ
イベントトリガー型	イベントが発生した特定のサブシステムに関するコンテキスト依存データが含まれるファイル
毎日	ログファイル
パフォーマンス	過去 24 時間以内にサンプリングされたパフォーマンスデータ
毎週	設定データおよびステータスデータ
によってトリガーされます `system node autosupport invoke` コマンドを実行します	で指定した値によって異なります `-type` パラメータ： • `test` いくつかの基本データを含むユーザトリガー型メッセージを送信します。 また、を使用して、テクニカルサポートからの自動応答Eメールが指定したEメールアドレス宛てに送信されます `-to` オプション。AutoSupport メッセージが受信されていることを確認できます。 • `performance` パフォーマンスデータを送信します。 • `all` 各サブシステムのトラブルシューティングデータを含む、週次メッセージと同様の一連のデータを含むユーザトリガー型メッセージを送信します。 通常、テクニカルサポートからはこのメッセージが要求されます。
によってトリガーされます `system node autosupport invoke-core-upload` コマンドを実行します	ノードのコアダンプファイル
によってトリガーされます `system node autosupport invoke-performance-archive` コマンドを実行します	指定された期間のパフォーマンスアーカイブファイル

メッセージのタイプ	メッセージに含まれるデータのタイプ
AutoSupport OnDemand によってトリガーされます	AutoSupport OnDemand では、新しいメッセージまたは過去のメッセージを要求できます。 • 新しいメッセージは、AutoSupport 収集のタイプに応じてにすることができます `test`、 `all`または `performance`。 • 過去のメッセージは、再送信されるメッセージの種類によって異なります。 AutoSupport OnDemand では、NetApp Support Site に次のファイルをアップロードする新しいメッセージを要求できます "mysupport.netapp.com"： • コアダンプ • パフォーマンスアーカイブ

AutoSupport サブシステムとは

各サブシステムは、 AutoSupport がメッセージに使用する基本情報およびトラブルシューティング情報を提供します。各サブシステムはトリガーイベントとも関連付けられており、 AutoSupport はトリガーイベントに関連する情報のみをサブシステムから収集できます。

AutoSupport は、状況に応じたコンテンツを収集します。を使用して、サブシステムおよびトリガーイベントに関する情報を表示できます `system node autosupport trigger show` コマンドを実行します

AutoSupport のサイズ割当量と時間割当量

AutoSupport は、サブシステム別に情報を収集し、各サブシステムのコンテンツにサイズ割当量と時間割当量を適用します。ストレージシステムが拡張すると、 AutoSupport の割当量によって AutoSupport のペイロードが制御され、拡張性の高い AutoSupport データの配信が可能になります。

サブシステムのコンテンツがサイズ割当量または時間割当量を超えた場合、 AutoSupport は情報の収集を停止し、 AutoSupport のコンテンツを切り捨てます。コンテンツを切り捨てるのが容易ではない場合（バイナリファイルなど）、 AutoSupport はそのコンテンツを除外します。

デフォルトのサイズ割当量と時間割当量の変更は、ネットアップサポートから指示があった場合にのみ行うようにしてください。を使用して、サブシステムのデフォルトのサイズ割当量と時間割当量を確認することもできます `autosupport manifest show` コマンドを実行します

イベントトリガー型 **AutoSupport** メッセージで送信されるファイル

イベントトリガー型 AutoSupport メッセージには、 AutoSupport でメッセージが生成される原因となったイベントに関連付けられたサブシステムからの基本情報とトラブルシューティング情報のみが含まれています。特定のデータは、ネットアップサポートおよ

びサポートパートナーによる問題のトラブルシューティングに役立ちます。

AutoSupport では、イベントトリガー型 AutoSupport メッセージの内容の制御に次の基準を使用します。

- 含まれているサブシステム

  データは、ログファイルなどの共通サブシステムや、 RAID などの特定のサブシステムといったサブシステムにグループ化されます。各イベントは、特定のサブシステムのデータのみを含むメッセージをトリガーします。

- 含まれている各サブシステムの詳細レベル

  含まれている各サブシステムのデータは、基本レベルまたはトラブルシューティングレベルで提供されます。

を使用して、考えられるすべてのイベントを表示し、各イベントに関するメッセージにどのサブシステムが含まれているかを確認できます `system node autosupport trigger show` コマンドにを指定します `-instance` パラメータ

各イベントにデフォルトで含まれるサブシステムのほかに、を使用して基本レベルまたはトラブルシューティングレベルでサブシステムを追加できます `system node autosupport trigger modify` コマンドを実行します

AutoSupport メッセージで送信されるログファイルです

AutoSupport メッセージには、ネットアップのテクニカルサポート担当者が最近のシステムアクティビティを確認できる、複数の主要ログファイルを含めることができます。

ログファイルサブシステムが有効になっている場合は、すべてのタイプの AutoSupport メッセージに次のログファイルが含まれる可能性があります。

ログファイル	ファイルから含まれているデータの量
• からのログファイル `/mroot/etc/log/mlog/` ディレクトリ • MESSAGES ログファイル	最後の AutoSupport メッセージ以降にログに追加された、指定最大数までの新しい行のみこれにより、AutoSupport メッセージに、一意で関連性のあるデータが重複しないようになります。 （パートナーからのログファイルは例外です。パートナーについては、最大許容データが含まれます）。
• からのログファイル `/mroot/etc/log/shelflog/` ディレクトリ • からのログファイル `/mroot/etc/log/acp/` ディレクトリ • Event Management System （ EMS ；イベント管理システム）ログデータ	指定された最大数までの最新のデータ行。

AutoSupport メッセージの内容は、 ONTAP のリリースによって変わる場合があります。

週単位の **AutoSupport** メッセージで送信されるファイル

週単位の AutoSupport メッセージには、追加の設定およびステータスが含まれ、時間の経過に伴うシステム内の変更の追跡に役立ちます。

週単位の AutoSupport メッセージでは、次の情報が送信されます。

- 各サブシステムに関する基本情報
- 選択したの内容 `/mroot/etc` ディレクトリファイル
- ログファイル
- システム情報を表示するコマンドの出力
- レプリケートされたデータベース（ RDB ）情報、サービス統計情報などの追加情報

AutoSupport OnDemand がテクニカルサポートから送信指示を取得する仕組み

AutoSupport OnDemand はテクニカルサポートと定期的に通信し、 AutoSupport メッセージの送信、再送信、拒否に関する配信指示を取得するとともに、NetApp Support Site に大容量ファイルをアップロードします。AutoSupport OnDemand を使用すると、週単位の AutoSupport ジョブの実行を待たずに AutoSupport メッセージをオンデマンドで送信できます。

AutoSupport OnDemand は、次のコンポーネントで構成されています。

- 各ノードで稼働する AutoSupport OnDemand クライアント
- テクニカルサポートで稼働する AutoSupport OnDemand サービス

AutoSupport OnDemand クライアントは、 AutoSupport OnDemand サービスを定期的にポーリングし、テクニカルサポートから送信指示を取得します。たとえば、テクニカルサポートは、 AutoSupport OnDemand サービスを使用して、新しい AutoSupport メッセージを生成するよう要求できます。AutoSupport OnDemand クライアントは、 AutoSupport OnDemand サービスをポーリングして、配信指示を取得し、要求に応じて新しい AutoSupport メッセージをオンデマンドで送信します。

AutoSupport OnDemand は、デフォルトで有効になっています。ただし、 AutoSupport OnDemand がテクニカルサポートとの通信を継続するかどうかは、いくつかの AutoSupport 設定によって決まります。次の要件を満たしている場合、 AutoSupport OnDemand はテクニカルサポートと自動的に通信を行います。

- AutoSupport が有効になっている
- AutoSupport は、テクニカルサポートにメッセージを送信するように設定されています。
- AutoSupport は、 HTTPS 転送プロトコルを使用するように設定されています。

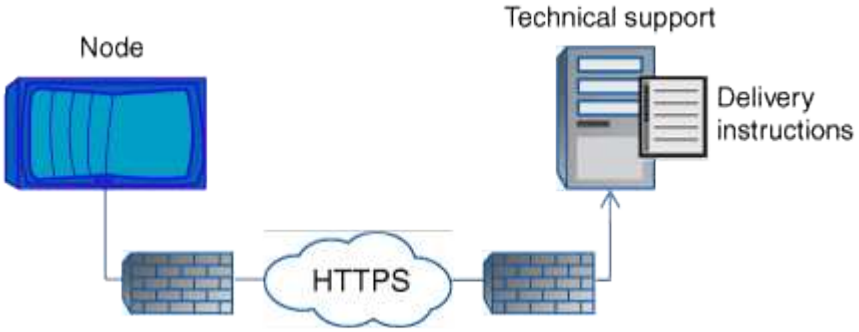
AutoSupport OnDemand クライアントは、 AutoSupport メッセージの送信先と同じ場所のテクニカルサポートに HTTPS 要求を送信します。AutoSupport OnDemand クライアントは、着信接続は受け入れません。

> AutoSupport OnDemand は、「 AutoSupport 」ユーザーアカウントを使用してテクニカルサポートと通信します。ONTAP では、このアカウントを削除することはできません。

AutoSupport OnDemandを無効にし、AutoSupportは有効なままにする場合は、次のコマンドを使用しま

す。link：https://docs.netapp.com/us-en/ontap-cli-9121/system-node-autosupport-modify.html#parameters[`system node autosupport modify -ondemand-state disable`]。

次の図は、 AutoSupport OnDemand がテクニカルサポートに HTTPS 要求を送信して送信指示を取得する方法を示しています。



配信指示には、 AutoSupport が行う処理として、次のようなものがあります。

- 新しい AutoSupport メッセージの生成

  テクニカルサポートからは、問題の優先度を選別できるように、新たな AutoSupport メッセージが要求されることが

- コアダンプファイルまたはパフォーマンスアーカイブファイルをNetApp Support Siteにアップロードする新しい AutoSupport メッセージの生成

  問題の優先度を選別できるように、テクニカルサポートからコアダンプファイルまたはパフォーマンスアーカイブファイルを要求されることがあります。

- 以前に生成した AutoSupport メッセージの再送信

  この要求は、配信エラーが原因でメッセージが受信されなかった場合に自動的に行われます。

- 特定のトリガーイベントに対する AutoSupport メッセージ配信を無効にします。

  テクニカルサポートは、使用されていないデータの配信を無効にすることがあります。

E メールで送信される **AutoSupport** メッセージの構造

AutoSupport メッセージを E メールで送信すると、メッセージには標準的な件名、簡単な本文、およびデータが含まれた 7z ファイル形式の大きな添付ファイルが含められます。

> プライベートデータを非表示にするように AutoSupport が設定されている場合は、ヘッダー、件名、本文、添付ファイル内のホスト名などの特定の情報が省略されるか、マスクされます。

件名

AutoSupport メカニズムによって送信されたメッセージの件名行には、通知の理由を特定するテキスト文字列が含まれています。件名行の形式は次のとおりです。

HA グループ通知の送信元 _ システム _ 名前 _ （ _ メッセージ _ ） _ 重大度 _

- *System_Name* は、 AutoSupport の設定に応じてホスト名またはシステム ID です

ボディ（ **Body** ）

AutoSupport メッセージの本文には、次の情報が含まれます。

- メッセージの日付とタイムスタンプ
- メッセージを生成したノード上の ONTAP のバージョン
- メッセージを生成したノードのシステム ID 、シリアル番号、およびホスト名
- AutoSupport シーケンス番号
- SNMP の連絡先名と場所（指定されている場合）
- HA パートナーノードのシステム ID とホスト名

添付ファイル

AutoSupport メッセージの重要な情報は、という名前の7zファイルに圧縮されたファイルに含まれています `body.7z` メッセージに添付されています。

添付ファイルに含まれるファイルは、 AutoSupport メッセージのタイプに固有です。

AutoSupport の重大度のタイプ

AutoSupport メッセージには、各メッセージの目的を示す重大度のタイプが設定されます。たとえば、緊急の問題にすぐに対処する場合や、情報提供のみを目的とした場合などです。

メッセージには次のいずれかの重大度が設定されます。

- * 警告 * ：アラートメッセージは、何らかの処置を行わないと、より高いレベルのイベントが発生する可能性があることを示します。

  アラートメッセージに対しては、 24 時間以内に対処を行う必要があります。

- * 緊急 * ：システム停止が発生すると、緊急メッセージが表示されます。

  緊急メッセージに対しては、すぐに対処する必要があります。

- * エラー * ：エラー状態は、無視した場合に発生する可能性がある問題を示します。
- * 通知 * ：通常の状態だが重要な状態。
- * 情報 * ：情報メッセージは、問題に関する詳細情報を提供しますが、これは無視してかまいません。
- * デバッグ *: デバッグレベルのメッセージには、実行する必要がある手順が記載されています。

社内のサポート部門が AutoSupport メッセージを E メールで受信する場合、重大度は E メールメッセージの件名に表示されます。

AutoSupport を使用するための要件

セキュリティを最適化し、AutoSupportの最新の機能をすべてサポートするには、AutoSupportメッセージの配信にHTTPSとTLSv1.2またはセキュアSMTPを使用する必要があります。他のプロトコルで配信されたAutoSupportメッセージは拒否されます。

サポートされているプロトコル

これらのプロトコルはいずれも、名前が解決されるアドレスファミリーに応じて IPv4 または IPv6 で実行されます。

プロトコルとポート	説明
ポート 443 で HTTPS を使用します	これがデフォルトのプロトコルです。できるだけこのプロトコルを使用することを推奨します。 このプロトコルでは、 AutoSupport OnDemand と大容量ファイルのアップロードがサポートされます。 検証を無効にしないかぎり、リモートサーバからの証明書がルート証明書に照らして検証されます。 配信にはHTTPS PUT要求が使用されます。PUT では、要求の転送中にエラーが発生した場合に、停止した場所から要求が再開されます。要求を受信したサーバがPUTをサポートしていない場合は、HTTPS POST要求が使用されます。
ポート 80 の HTTP	このプロトコルは SMTP よりも推奨されます。 このプロトコルでは、大容量ファイルのアップロードがサポートされますが、 AutoSupport OnDemand はサポートされません。 配信にはHTTPS PUT要求が使用されます。PUT では、要求の転送中にエラーが発生した場合に、停止した場所から要求が再開されます。要求を受信したサーバがPUTをサポートしていない場合は、HTTPS POST要求が使用されます。

プロトコルとポート	説明
SMTP ：ポート 25 または別のポート	このプロトコルは、ネットワーク接続でHTTPSが許可されていない場合にのみ使用してください。 デフォルトのポート値は 25 ですが、別のポートを使用するように AutoSupport を設定できます。 SMTP を使用する場合は、次の制限事項に注意してください。 • AutoSupport OnDemand と大容量ファイルのアップロードはサポートされません。 • データは暗号化されません。 SMTP ではデータがクリアテキストで送信されるため、 AutoSupport メッセージ内のテキストの傍受や読み取りが容易になります。 • メッセージの長さや行の長さの制限が生じることがあります。

AutoSupport に社内のサポート部門またはサポートパートナーの E メールアドレスを指定した場合、それらのメッセージは常に SMTP で送信されます。

たとえば、推奨されるプロトコルを使用してテクニカルサポートにメッセージを送信し、同時に社内のサポート部門にもメッセージを送信する場合は、それぞれ HTTPS と SMTP を使用して転送されます。

AutoSupport では、プロトコルごとに最大ファイルサイズが制限されます。HTTP および HTTPS 転送のデフォルト設定は 25MB です。SMTP 転送のデフォルト設定は 5MB です。AutoSupport メッセージのサイズが設定された上限を超えると、 AutoSupport はできるだけ多くのメッセージを配信します。最大サイズは、AutoSupport の設定を変更することで編集できます。を参照してください `system node autosupport modify` のマニュアルページを参照してください。

> コアダンプファイルやパフォーマンスアーカイブファイルをNetApp Support Siteや指定の URI にアップロードする AutoSupport メッセージを生成して送信すると、 HTTPS プロトコルと HTTP プロトコルの最大ファイルサイズの上限は自動的に無視されます。自動オーバーライドは、を使用してファイルをアップロードする場合にのみ適用されます `system node autosupport invoke-core-upload` または `system node autosupport invoke-performance-archive` コマンド

設定要件

ネットワーク構成によっては、HTTPSプロトコルでプロキシURLの追加設定が必要になる場合があります。テクニカルサポートへのAutoSupportメッセージの送信にHTTPSを使用し、プロキシを使用している場合は、そのプロキシのURLを指定する必要があります。プロキシがデフォルトのポート（ 3128 ）以外のポートを使用する場合は、そのプロキシのポートを指定できます。プロキシ認証のユーザ名とパスワードを指定することもできます。

SMTP を使用して社内のサポート部門やテクニカルサポートに AutoSupport メッセージを送信する場合は、外部のメールサーバを設定する必要があります。ストレージシステムはメールサーバとしては機能しないた

め、メール送信用に外部のメールサーバが別途必要になります。このメールサーバを SMTP ポート（ 25 ）または別のポートを監視するホストにして、 8 ビットの Multipurpose Internet Mail Extensions （ MIME ）エンコーディングを送受信するように設定する必要があります。メール・ホストの例としては 'sendmail プログラムなどの SMTP サーバを実行する UNIX ホストと 'Microsoft Exchange サーバを実行する Windows サーバがありますメールホストは 1 つでも複数でもかまいません。

AutoSupport をセットアップする

テクニカルサポートまたは社内のサポート部門に AutoSupport 情報を送信するかどうかおよびその方法を管理し、その設定が正しいことをテストできます。

このタスクについて

ONTAP 9.5 以降のリリースでは、クラスタのすべてのノードで AutoSupport を有効にし、その設定を同時に変更できます。新しいノードがクラスタに追加されると、そのノードは AutoSupport クラスタ設定を自動的に継承します。各ノードの設定を個別に更新する必要はありません。

> ONTAP 9.5以降では、の対象となります `system node autosupport modify` コマンドはクラスタ全体に適用されます。AutoSupport 設定がクラスタ内のすべてのノードで変更されます。これには、が含まれます `-node` オプションが指定されています。このオプションは無視されますが、 CLI の下位互換性を維持するために保持されています。
>
> ONTAP 9.4以前のリリースでは、の対象となります `system node autosupport modify` コマンドはノードに固有です。クラスタ内の各ノードで AutoSupport 設定を変更する必要があります。

デフォルトでは、各ノードで AutoSupport が有効になっており、 HTTPS 転送プロトコルを使用してテクニカルサポートにメッセージを送信できます。

セキュリティを最適化し、AutoSupportの最新の機能をすべてサポートするには、AutoSupportメッセージの配信にHTTPSとTLSv1.2またはセキュアSMTPを使用する必要があります。

手順

1. AutoSupport が有効になっていることを確認します。

   ```
   system node autosupport modify -state enable
   ```

2. テクニカルサポートに AutoSupport メッセージを送信するには、次のコマンドを使用します。

   ```
   system node autosupport modify -support enable
   ```

   AutoSupport を AutoSupport OnDemand と連携できるようにする場合、またはコアダンプファイルやパフォーマンスアーカイブファイルなどの大容量ファイルをテクニカルサポートまたは指定の URL にアップロードする場合は、このオプションを有効にする必要があります。

3. テクニカルサポートが AutoSupport メッセージを受信できるようになっている場合は、メッセージに使用する転送プロトコルを指定します。

   次のオプションから選択できます。

状況	次に、の次のパラメータを設定します `system node autosupport modify` コマンド…
デフォルトの HTTPS プロトコルを使用します	a. 設定 `-transport` 終了： `https`。 b. プロキシを使用する場合は、を設定します `-proxy-url` にプロキシのURLを入力します。この設定では、 AutoSupport OnDemand との通信および大容量ファイルのアップロードがサポートされます。
SMTP を使用する	設定 `-transport` 終了： `smtp`。 この設定では、 AutoSupport OnDemand や大容量ファイルのアップロードはサポートされません。

4. 社内のサポート部門またはサポートパートナーに AutoSupport メッセージを送信するには、次の操作を実行します。
   a. 組織内の受信者を特定するには、の次のパラメータを設定します `system node autosupport modify` コマンドを実行します

設定するパラメータ	パラメータの値
`-to`	重要な AutoSupport メッセージを受け取る社内サポート部門の、カンマで区切った 5 つまでの個別 E メールアドレスまたは配信リスト
`-noteto`	重要な AutoSupport メッセージの携帯電話やその他のモバイルデバイス用の短縮版を受け取る社内サポート部門の、カンマで区切った 5 つまでの個別 E メールアドレスまたは配信リスト
`-partner-address`	すべての AutoSupport メッセージを受け取るサポートパートナー部門の、カンマで区切った 5 つまでの個別 E メールアドレスまたは配信リスト

   b. を使用して送信先をリストし、アドレスが正しく設定されていることを確認します `system node autosupport destinations show` コマンドを実行します
5. メッセージを社内のサポート部門に送信するか、テクニカルサポートへのメッセージにSMTP転送を選択した場合は、の次のパラメータを設定してSMTPを設定します `system node autosupport modify` コマンドを実行します

   - 設定 `-mail-hosts` をカンマで区切って1つ以上のメールホストに転送します。

     最大 5 つのを設定できます。

   メールホスト名のあとにコロンとポート番号を指定することで、各メールホストのポート値を設定できます。次に例を示します。 `mymailhost.example.com:5678`では、5678はメールホストのポートです。

- 設定 `-from` AutoSupport メッセージを送信するEメールアドレスに送信します。

6. DNS を設定します。
7. 特定の設定を変更する場合は、必要に応じてコマンドオプションを追加します。

実行する処理	次に、の次のパラメータを設定します `system node autosupport modify` コマンド...
メッセージ内の機密データを削除、マスキング、またはエンコードすることによって、プライベートデータを非表示にします	設定 `-remove-private-data` 終了： `true`。から変更した場合 `false` 終了： `true`をクリックすると、すべてのAutoSupport 履歴とすべての関連ファイルが削除されます。
定期的な AutoSupport メッセージでのパフォーマンスデータの送信を停止します	設定 `-perf` 終了： `false`。

8. を使用して設定全体を確認します `system node autosupport show` コマンドにを指定します `-node` パラメータ
9. を使用してAutoSupport の動作を確認します `system node autosupport check show` コマンドを実行します

   問題が報告された場合は、を使用してください `system node autosupport check show-details` コマンドを使用して詳細情報を表示します。

10. AutoSupport メッセージが送受信されていることをテストします。

    a. を使用します `system node autosupport invoke` コマンドにを指定します `-type` パラメータをに設定します `test`。

    ```
    cluster1::> system node autosupport invoke -type test -node node1
    ```

    b. ネットアップが AutoSupport メッセージを受信していることを確認します。

    system node AutoSupport history show -node local コマンドを実行します

    最新の発信AutoSupport メッセージのステータスは、最終的ににに変わります `sent-successful` すべての適切なプロトコルの宛先に対して。

    a. 必要に応じて、AutoSupportメッセージが社内のサポート部門またはサポートパートナーに送信されていることを確認します。そのためには、用に設定したアドレスのEメールを確認します `-to`、`-noteto`または `-partner-address` のパラメータ `system node autosupport modify` コマンドを実行します

コアダンプファイルをアップロードする

コアダンプファイルが保存されると、イベントメッセージが生成されます。AutoSupport サービスが有効であり、ネットアップサポートにメッセージを送信するように設定されている場合は、 AutoSupport メッセージが送信され、自動応答メールが返信されます。

必要なもの

- 次の設定を使用して AutoSupport をセットアップしておく必要があります。
  - ノードで AutoSupport が有効になっている。
  - AutoSupport は、テクニカルサポートにメッセージを送信するように設定されています。
  - HTTP または HTTPS 転送プロトコルを使用するように AutoSupport が設定されている。

    コアダンプファイルなどの大容量ファイルを含むメッセージを送信する場合、 SMTP 転送プロトコルはサポートされません。

このタスクについて

を使用して、HTTPS経由のAutoSupport サービスを通じてコアダンプファイルをアップロードすることもできます `system node autosupport invoke-core-upload` コマンド（ネットアップサポートから要求された場合）。

"ネットアップにファイルをアップロードする方法"

手順

1. を使用して、ノードのコアダンプファイルを表示します `system node coredump show` コマンドを実行します

   次の例では、ローカルノードのコアダンプファイルが表示されます。

   ```
   cluster1::> system node coredump show -node local
   Node:Type Core Name Saved Panic Time
   --------- ------------------------------------------- -----
   -----------------
   node:kernel
   core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
   ```

2. を使用して、AutoSupport メッセージを生成し、コアダンプファイルをアップロードします `system node autosupport invoke-core-upload` コマンドを実行します

   次の例では、 AutoSupport メッセージが生成されてデフォルトの場所（テクニカルサポート）に送信されます。コアダンプファイルは、NetApp Support Siteであるデフォルトの場所にアップロードされます。

   ```
   cluster1::> system node autosupport invoke-core-upload -core-filename
   core.4073000068.2013-09-11.15_05_01.nz -node local
   ```

   次の例では、 AutoSupport メッセージが生成され、 URI に指定した場所に送信されます。コアダンプファイルはその URI にアップロードされます。

```
cluster1::> system node autosupport invoke-core-upload -uri
https//files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

パフォーマンスアーカイブファイルをアップロードします

パフォーマンスアーカイブを含む AutoSupport メッセージを生成して送信できます。デフォルトでは、 AutoSupport メッセージはネットアップテクニカルサポートに送信され、パフォーマンスアーカイブはNetApp Support Siteにアップロードされます。メッセージの送信先とアップロード先には別の場所を指定できます。

必要なもの

- 次の設定を使用して AutoSupport をセットアップしておく必要があります。
  - ノードで AutoSupport が有効になっている。
  - AutoSupport は、テクニカルサポートにメッセージを送信するように設定されています。
  - HTTP または HTTPS 転送プロトコルを使用するように AutoSupport が設定されている。

    パフォーマンスアーカイブファイルなどの大容量ファイルを含むメッセージの送信では、 SMTP 転送プロトコルはサポートされません。

このタスクについて

アップロードするパフォーマンスアーカイブデータの開始日を指定する必要があります。ほとんどのストレージシステムでは、パフォーマンスアーカイブが 2 週間保存されるため、 2 週間前までの開始日を指定できます。たとえば、今日が 1 月 15 日の場合は、 1 月 2 日の開始日を指定できます。

ステップ

1. を使用して、AutoSupport メッセージを生成し、パフォーマンスアーカイブファイルをアップロードします `system node autosupport invoke-performance-archive` コマンドを実行します

   次の例では、 2015 年 1 月 12 日から 4 時間分のパフォーマンスアーカイブファイルが AutoSupport メッセージに追加され、NetApp Support Siteのデフォルトの場所にアップロードされます。

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

   次の例では、 2015 年 1 月 12 日から 4 時間分のパフォーマンスアーカイブファイルが AutoSupport メッセージに追加され、 URI で指定した場所にアップロードされます。

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h -uri
   https://files.company.com
   ```

AutoSupport メッセージの説明を取得する

受信したAutoSupport メッセージの説明は、ONTAP のSyslog Translatorを使用して参照できます。

手順

1. にアクセスします "Syslog Translator"。
2. [リリース]フィールドに、使用しているONTAP のバージョンを入力します。検索文字列フィールドに「callhome」と入力します。[*平行移動（Translate）]を選択し
3. Syslog Translatorには、入力したメッセージ文字列に一致するすべてのイベントがアルファベット順に表示されます。

AutoSupport を管理するためのコマンド

を使用します `system node autosupport` AutoSupport の設定を変更または表示したり、以前のAutoSupport メッセージに関する情報を表示したり、AutoSupport メッセージを送信、再送信、またはキャンセルしたりするコマンド。

AutoSupport を設定します

状況	使用するコマンド
AutoSupport メッセージを送信するかどうかを制御します	`system node autosupport modify` を使用 `-state` パラメータ
AutoSupport メッセージをテクニカルサポートに送信するかどうかを制御します	`system node autosupport modify` を使用 `-support` パラメータ
AutoSupport をセットアップするか、 AutoSupport の設定を変更します	`system node autosupport modify`
個々のトリガーイベントについて、 AutoSupport メッセージを社内のサポート部門に送信するかどうかを指定する。また、各トリガーイベントで送信されるメッセージに含める追加のサブシステムレポートを指定する	`system node autosupport trigger modify`

AutoSupport の設定に関する情報を表示します

状況	使用するコマンド
AutoSupport の設定を表示します	`system node autosupport show` を使用 `-node` パラメータ
AutoSupport メッセージを受信するすべてのアドレスと URL の概要を表示します	`system node autosupport destinations show`

状況	使用するコマンド
個々のトリガーイベントについて社内のサポート部門に送信される AutoSupport メッセージを表示します	`system node autosupport trigger show`
AutoSupport の設定およびさまざまな宛先への配信のステータスを表示します	`system node autosupport check show`
AutoSupport の設定およびさまざまな宛先への配信の詳細なステータスを表示します	`system node autosupport check show-details`

過去の **AutoSupport** メッセージに関する情報を表示する

状況	使用するコマンド
1 つ以上の最新の 50 件の AutoSupport メッセージに関する情報を表示する	`system node autosupport history show`
テクニカルサポートサイトまたは指定の URI にコアダンプファイルまたはパフォーマンスアーカイブファイルをアップロードするために生成された最新の AutoSupport メッセージに関する情報を表示します	`system node autosupport history show-upload-details`
AutoSupport メッセージ内の情報を表示します。メッセージ用に収集された各ファイルの名前とサイズのほか、エラーがある場合はその情報も表示されます	`system node autosupport manifest show`

AutoSupport メッセージを送信、再送信、またはキャンセルします

状況	使用するコマンド
ローカルに保存されている AutoSupport メッセージを、 AutoSupport シーケンス番号で識別して再転送します AutoSupport メッセージを再送信し、サポート部門がすでにそのメッセージを受信している場合、サポートシステムは重複するケースを作成しません。一方、サポート部門がそのメッセージを受信しなかった場合、 AutoSupport システムはメッセージを分析し、必要に応じてケースを作成します。	`system node autosupport history retransmit`

状況	使用するコマンド
テストなどの目的で、 AutoSupport メッセージを生成して送信します	`system node autosupport invoke` を使用します `-force` AutoSupport が無効な場合でもメッセージを送信するためのパラメータ。を使用します `-uri` 設定されている宛先ではなく、指定した宛先にメッセージを送信するためのパラメータ。
AutoSupport メッセージをキャンセルします	`system node autosupport history cancel`

関連情報

"ONTAP 9コマンド"

AutoSupport マニフェストに含まれる情報

AutoSupport マニフェストでは、各 AutoSupport メッセージについて収集されるファイルの詳細が表示されます。AutoSupport マニフェストには、 AutoSupport が必要なファイルを収集できない場合の収集エラーに関する情報も含まれています。

AutoSupport マニフェストには次の情報が含まれています。

- AutoSupport メッセージのシーケンス番号
- AutoSupport メッセージに含まれている AutoSupport ファイル
- 各ファイルのサイズ（バイト単位）
- AutoSupport マニフェストによる収集のステータス
- 概要が 1 つ以上のファイルの収集に失敗した場合は、エラー AutoSupport

を使用してAutoSupport マニフェストを表示できます `system node autosupport manifest show` コマンドを実行します

AutoSupport マニフェストは、すべての Active IQ メッセージに含まれ、 XML 形式で表示されます。つまり、一般的な XML ビューアを使用してメッセージを読んだり、 AutoSupport （旧 My AutoSupport ）ポータルを使用して表示したりできます。

スケジュールされたメンテナンス時間中の **AutoSupport** ケースの抑制

AutoSupport ケースの抑制を使用すると、スケジュールされたメンテナンス時間中にトリガーされる AutoSupport メッセージによって不要なケースが作成されるのを阻止できます。

AutoSupport ケースを抑制するには、特別な形式のテキスト文字列を使用してAutoSupport メッセージを手動で呼び出す必要があります。 `MAINT=xh`。 `x` には、メンテナンス時間の長さを時間単位で指定します。

関連情報

"スケジュールされたメンテナンス時間中にケースの自動作成を停止する方法"

メッセージを受信しない場合は、 **AutoSupport** のトラブルシューティングを行います

システムから AutoSupport メッセージが送信されない場合は、 AutoSupport がメッセージを生成できないためであるか、配信できないためであるかを判別できます。

手順

1. を使用して、メッセージの配信ステータスを確認します `system node autosupport history show` コマンドを実行します
2. ステータスを読みます。

このステータスです	はい
初期化中です	収集プロセスが開始しています。この状態が一時的なものであれば問題はありません。ただし、この状態が解消されない場合は、問題が存在します。
コレクション - 失敗しました	AutoSupport は、スプールディレクトリに AutoSupport コンテンツを作成できません。AutoSupport が収集しようとしている内容を表示するには、を入力します `system node autosupport history show -detail` コマンドを実行します
収集を実行中です	AutoSupport は AutoSupport コンテンツを収集しています。AutoSupport が収集している情報を表示するには、を入力します `system node autosupport manifest show` コマンドを実行します
キューに登録され	AutoSupport メッセージは配信のためにキューに登録されますが、まだ配信されていません。
送信中です	AutoSupport は現在メッセージを配信しています。
Sent - 成功しました	AutoSupport がメッセージを正常に配信しました。AutoSupport がメッセージを配信した場所を確認するには、を入力します `system node autosupport history show -delivery` コマンドを実行します
無視します	AutoSupport にメッセージの送信先がありません。配信の詳細を表示するには、を入力します `system node autosupport history show -delivery` コマンドを実行します
再キューイングされました	AutoSupport はメッセージの配信を試みましたが、失敗しました。その結果、AutoSupport は別の試行のためにメッセージを配信キューに戻しました。エラーを表示するには、を入力します `system node autosupport history show` コマンドを実行します
トランスミッション - 不合格	AutoSupport は、指定された回数メッセージの配信に失敗し、メッセージ配信の試行を停止しました。エラーを表示するには、を入力します `system node autosupport history show` コマンドを実行します

このステータスです	はい
OnDemand - 無視されます	AutoSupport メッセージは正常に処理されましたが、 AutoSupport OnDemand サービスによって無視されました。

3. 次のいずれかを実行します。

をクリックします	手順
initializing または collection-failed	AutoSupport でメッセージを生成できないため、ネットアップサポートにお問い合わせください。次のナレッジベース記事に言及してください。 "AutoSupport の配信に失敗しました：ステータスが「初期化中にエラーが発生しました"
ignore 、 re-queued 、または transmission failed のいずれかです	AutoSupport はメッセージを配信できないため、SMTP 、 HTTP 、または HTTPS のデスティネーションが正しく設定されていることを確認します。

HTTP または **HTTPS** を使用した **AutoSupport** メッセージ配信のトラブルシューティング

HTTP または HTTPS を使用していて、想定される AutoSupport メッセージが送信されない場合や自動更新機能が動作しない場合は、いくつかの設定を確認することで問題を解決できます。

必要なもの

基本的なネットワーク接続と DNS ルックアップについて、以下の点を確認しておきます。

- ノード管理 LIF の動作ステータスおよび管理ステータスが up になっている。
- 同じサブネット上の機能しているホストに、（ノード上の LIF ではなく）クラスタ管理 LIF から ping を実行できる。
- サブネットの外部の機能しているホストに、クラスタ管理 LIF から ping を実行できる。
- サブネットの外部の機能しているホストに、（ IP アドレスではなく）ホストの名前を使用してクラスタ管理 LIF から ping を実行できる。

このタスクについて

以下の手順は、 AutoSupport でメッセージを生成できているが、 HTTP または HTTPS 経由でメッセージを配信できていないと判断した場合に実行します。

エラーが発生したり、この手順の手順を完了できない場合は、問題を特定し、対処してから次の手順に進んでください。

手順

1. AutoSupport サブシステムの詳細なステータスを表示します。

```
system node autosupport check show-details
```

たとえば、テストメッセージを送信して AutoSupport デスティネーションへの接続を検証したり、AutoSupport の設定で発生する可能性のあるエラーのリストを指定したりします。

2. ノード管理 LIF のステータスを確認します。

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   。 `status-oper` および `status-admin` フィールドは「up」を返す必要があります。

3. あとで使用できるように、 SVM 名、 LIF 名、および LIF の IP アドレスを書き留めておきます。
4. DNS が有効になっていて正しく設定されていることを確認します

   ```
   vserver services name-service dns show
   ```

5. AutoSupport メッセージからエラーが返された場合は、対処します。

   ```
   system node autosupport history show -node * -fields node,seq-
   num,destination,last-update,status,error
   ```

   返されたエラーのトラブルシューティングについては、を参照してください "ONTAP AutoSupport（Transport HTTPSおよびHTTP）解決ガイド"。

6. クラスタが必要なサーバとインターネットの両方に正常にアクセスできることを確認します。

   a. `network traceroute -lif node-management_LIF -destination DNS server`

   b. `network traceroute -lif node_management_LIF -destination support.netapp.com`

   > 住所 `support.netapp.com` それ自体はpingやtracerouteに応答しませんが、ホップ単位の情報は重要です。

   c. `system node autosupport show -fields proxy-url`

   d. `network traceroute -node node_management_LIF -destination proxy_url`

   これらのルートのいずれかが機能していない場合は、ほとんどのサードパーティ製ネットワーククライアントで検出された「 traceroute 」または「 tracert 」ユーティリティを使用して、クラスタと同じサブネット上の機能しているホストから同じルートを試してください。これにより、問題がネットワーク構成とクラスタ構成のどちらに含まれているかを判断できます。

7. AutoSupport 転送プロトコルに HTTPS を使用する場合は、 HTTPS トラフィックがネットワークから送信可能であることを確認します。

   a. クラスタ管理 LIF と同じサブネットに Web クライアントを設定します。

      プロキシサーバ、ユーザ名、パスワード、ポートを含む、すべての設定パラメータの値が AutoSupport の設定と同じであることを確認します。

   b. にアクセスします `https://support.netapp.com` Webクライアントを使用します。

      アクセスが成功します。成功しない場合は、 HTTPS トラフィックと DNS トラフィックを許可するようにすべてのファイアウォールが設定されていること、およびプロキシサーバが正しく設定されてい

ることを確認します。support.netapp.comの静的な名前解決の設定の詳細については、サポート技術情報の記事を参照してください "ONTAP for support.netapp.com? でホストエントリを追加する方法を説明します"

8. ONTAP 9.10.1 以降では、自動更新機能を有効にした場合、次の URL への HTTPS 接続が確立されていることを確認してください。
   - https://support-sg-emea.netapp.com
   - https://support-sg-naeast.netapp.com
   - https://support-sg-nawest.netapp.com

SMTP を使用した **AutoSupport** メッセージ配信のトラブルシューティング

システムが SMTP 経由で AutoSupport メッセージを配信できない場合は、いくつかの設定を確認することで問題を解決できます。

必要なもの

基本的なネットワーク接続と DNS ルックアップについて、以下の点を確認しておきます。

- ノード管理 LIF の動作ステータスおよび管理ステータスが up になっている。
- 同じサブネット上の機能しているホストに、（ノード上の LIF ではなく）クラスタ管理 LIF から ping を実行できる。
- サブネットの外部の機能しているホストに、クラスタ管理 LIF から ping を実行できる。
- サブネットの外部の機能しているホストに、（ IP アドレスではなく）ホストの名前を使用してクラスタ管理 LIF から ping を実行できる。

このタスクについて

以下の手順は、 AutoSupport でメッセージを生成できているが、 SMTP 経由でメッセージを配信できていないと判断した場合に実行します。

エラーが発生したり、この手順の手順を完了できない場合は、問題を特定し、対処してから次の手順に進んでください。

特に指定がないかぎり、すべてのコマンドを ONTAP の CLI に入力します。

手順

1. ノード管理 LIF のステータスを確認します。

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   。 `status-oper` および `status-admin` フィールドが返される必要があります `up`。

2. あとで使用できるように、 SVM 名、 LIF 名、および LIF の IP アドレスを書き留めておきます。
3. DNS が有効になっていて正しく設定されていることを確認します

   ```
   vserver services name-service dns show
   ```

4. AutoSupport で使用するように設定されているすべてのサーバを表示します。

system node autosupport show -fields mail-hosts

表示されたすべてのサーバ名を記録します。

5. 前の手順で表示された各サーバについて、およびを参照してください `support.netapp.com`ノードからサーバまたはURLにアクセスできることを確認します。

   network traceroute -node local -destination *server_name*

   これらのルートのいずれかが機能していない場合は、ほとんどのサードパーティ製ネットワーククライアントで検出された「 traceroute 」または「 tracert 」ユーティリティを使用して、クラスタと同じサブネット上の機能しているホストから同じルートを試してください。これにより、問題がネットワーク構成とクラスタ構成のどちらに含まれているかを判断できます。

6. メールホストとして指定したホストにログインし、このホストが SMTP 要求を処理できることを確認します。

   netstat -aAn|grep 25

   `25` は、リスナーのSMTPポート番号です。

   次のようなメッセージが表示されます。

   ```
   ff64878c tcp        0      0  *.25    *.*    LISTEN.
   ```

7. 他のホストで、メールホストの SMTP ポートを使用した Telnet セッションを開始します。

   telnet *mailhost* 25

   次のようなメッセージが表示されます。

   ```
   220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
   10:49:04 PST
   ```

8. Telnet のプロンプトで、メールホストからメッセージをリレーできることを確認します。

   HELO *domain_name*

   MAIL FROM: *your_email_address*

   RCPT TO: autosupport@netapp.com

   `domain_name` は、ネットワークのドメイン名です。

   リレーが拒否されたというエラーが返された場合は、メールホストでリレーが有効になっていません。システム管理者に問い合わせてください。

9. Telnet のプロンプトで、テストメッセージを送信します。

```
DATA

SUBJECT: TESTING
THIS IS A TEST

.
```

> 行の最後のピリオド（ . ）を単独で入力してください。このピリオドは、メッセージが完了したことをメールホストに示します。

エラーが返された場合は、メールホストが正しく設定されていません。システム管理者に問い合わせてください。

10. ONTAP のコマンドラインインターフェイスから、アクセス可能な信頼できる E メールアドレスに AutoSupport テストメッセージを送信します。

    ```
    system node autosupport invoke -node local -type test
    ```

11. テストのシーケンス番号を確認します。

    ```
    system node autosupport history show -node local -destination smtp
    ```

    タイムスタンプに基づいて、シーケンス番号を探します。おそらく、最新の試みです。

12. テストメッセージに関するエラーを表示します。

    ```
    system node autosupport history show -node local -seq-num seq_num -fields
    error
    ```

    表示されたエラーは、です `Login denied`、SMTPサーバがクラスタ管理LIFからの送信要求を受け入れていません。転送プロトコルを HTTPS に変更しない場合は、サイトのネットワーク管理者に連絡して、この問題に対応するように SMTP ゲートウェイを設定してください。

    このテストが成功しても mailto ： autosupport@netapp.com に同じメッセージが送信されない場合は、すべての SMTP メールホストで SMTP リレーが有効になっていることを確認するか、転送プロトコルとして HTTPS を使用してください。

    ローカルで管理されている E メールアカウントへのメッセージの送信も失敗する場合は、次の両方の条件に該当する添付ファイルを転送するように SMTP サーバが設定されていることを確認してください。

    - サフィックスが「 7z
    - MIME タイプが「 application/x-7x-compressed 」。

AutoSupport サブシステムのトラブルシューティングを行います

。 `system node check show` コマンドを使用すると、AutoSupport の設定と配信に関連する問題の検証とトラブルシューティングを行うことができます。

ステップ

1. 次のコマンドを使用して、 AutoSupport サブシステムのステータスを表示します。

使用するコマンド	作業
system node autosupport check show	AutoSupport HTTP または HTTPS デスティネーション、 AutoSupport SMTP デスティネーション、 AutoSupport OnDemand サーバ、 AutoSupport 設定など、 AutoSupport サブシステムの全体的なステータスを表示します
system node autosupport check show-details	エラーの詳細な説明や対処方法など、 AutoSupport サブシステムの詳細なステータスを表示する

健全性の監視

システムの健常性の概要を監視

ヘルスモニタは、クラスタ内の特定のクリティカルな状態をプロアクティブに監視し、障害やリスクが検出された場合にアラートを生成します。アクティブなアラートがある場合、クラスタのヘルスステータスはデグレードと報告されます。アラートには、デグレードしたシステムヘルスへの対応に必要な情報が含まれています。

ステータスがデグレードになっている場合は、考えられる原因や推奨されるリカバリアクションなど、問題の詳細を表示できます。問題を解決すると、システムヘルスステータスは自動的に OK に戻ります。

システムヘルスステータスには、複数の異なるヘルスモニタの結果が反映されます。1 つのヘルスモニタのステータスがデグレードになると、システムヘルス全体のステータスがデグレードになります。

クラスタ内のシステムヘルスの監視におけるクラスタスイッチのサポート状況 ONTAP については、Hardware Universe を参照してください。

"Hardware Universe でサポートされるスイッチ"

Cluster Switch Health Monitor （ CSHM ） AutoSupport メッセージの原因とアラートの解決方法に関する詳細については、技術情報アーティクルを参照してください。

"AutoSupport メッセージ：ヘルスモニタプロセス CSHM"

ヘルスモニタの仕組み

個々のヘルスモニタには、特定の条件に該当する場合にアラートをトリガーする一連のポリシーがあります。ヘルスモニタの仕組みを理解しておくと、問題に対応し、将来のアラートを制御するのに役立ちます。

ヘルスモニタは、次のコンポーネントで構成されています。

- 特定のサブシステム用のヘルスモニタ。各ヘルスモニタには独自のヘルスステータスがあります

  たとえば、ストレージサブシステムにはノード接続ヘルスモニタがあります。

- 個々のヘルスモニタのヘルスステータスを統合したシステム全体のヘルスモニタ

  1 つのサブシステムのステータスがデグレードになると、システム全体のステータスがデグレードになります。サブシステムにアラートがない場合、システム全体のステータスは OK です。

各ヘルスモニタは、次の主要な要素で構成されています。

- ヘルスモニタが発生させる可能性があるアラート

  各アラートには、アラートの重大度や原因の可能性などの詳細が定義されています。

- 各アラートをいつトリガーするかを特定するヘルスポリシー

  各ヘルスポリシーには、アラートをトリガーする正確な条件または変更であるルール式があります。

ヘルスモニタは、サブシステム内のリソースの条件または状態の変化を継続的に監視し、検証します。条件または状態の変化がヘルスポリシーのルール式に一致すると、ヘルスモニタはアラートを生成します。アラートにより、サブシステムのヘルスステータスおよびシステム全体のヘルスステータスがデグレードします。

システムヘルスアラートへの対応方法

システムヘルスアラートが発生した場合は、確認して詳細を確認し、原因となった状態を修復して、再発を防止できます。

ヘルスモニタからアラートが発せられた場合、次のいずれかの方法で対応できます。

- 影響を受けるリソース、アラートの重大度、原因の可能性、考えられる影響、対処方法など、アラートに関する情報を入手する
- アラートが発せられた時間、すでに誰かが承認しているかどうかなど、アラートに関する詳細情報を入手する
- 特定のシェルフやディスクなど、影響を受けるリソースまたはサブシステムの状態に関するヘルス関連の情報を取得する
- アラートを承認して、問題に対応中のユーザがいることを示し、自分自身を「承認者」と指定します。
- ケーブル接続を修正して接続の問題を解決するなど、アラートで指定された対処方法を実施することで、問題を解決する
- アラートが自動的に解除されない場合は、そのアラートを削除します。
- サブシステムのヘルスの状態に影響しないようにアラートを抑制する

  問題を把握した場合は、抑制が役に立ちます。アラートを抑制すると、そのアラートは引き続き発生する可能性がありますが、抑制されたアラートが発生すると、サブシステムのヘルスは「 ok-with-suppressed 」と表示されます。

システムヘルスアラートのカスタマイズ

ヘルスモニタが生成するアラートは、アラートをいつトリガーするかを定義するシステムヘルスポリシーを有効または無効にすることによって制御できます。これにより、環境に合わせてヘルス監視システムをカスタマイズできます。

ポリシーの名前は、生成されたアラートの詳細情報を表示するか、特定のヘルスモニタ、ノード、またはアラート ID のポリシー定義を表示することによって確認できます。

ヘルスポリシーの無効化と、アラートの抑制は違います。アラートを抑制した場合はサブシステムのヘルスステータスには影響しませんが、アラートは発生します。

ポリシーを無効にした場合に、そのポリシールール式に定義されている条件または状態によるアラートがトリガーされなくなります。

無効にするアラートの例

たとえば、役に立たないアラートが発生するとします。を使用します `system health alert show -instance` コマンドを使用してアラートのポリシーIDを取得します。ポリシーIDはで使用します `system health policy definition show` コマンドを使用してポリシーに関する情報を表示します。ポリシーのルール式およびその他の情報を確認したら、ポリシーを無効にすることにします。を使用します `system health policy definition modify` コマンドを使用してポリシーを無効にします。

ヘルスアラートによる **AutoSupport** メッセージおよびイベントのトリガー方法

システムヘルスアラートは Event Management System （ EMS ；イベント管理システム）の AutoSupport メッセージとイベントをトリガーし、ヘルス監視システムを直接使用することに加え、 AutoSupport メッセージと EMS を使用してシステムのヘルスを監視できます。

アラートから 5 分以内に AutoSupport メッセージが送信されます。AutoSupport メッセージには、前の AutoSupport メッセージ以降に生成されたすべてのアラートが含まれます。ただし、同じリソースで前週に原因と同じであると考えられるアラートは除きます。

一部のアラートでは AutoSupport メッセージがトリガーされません。ヘルスポリシーで AutoSupport メッセージの送信が無効になっている場合は、アラートが発生しても AutoSupport メッセージがトリガーされません。たとえば、問題の発生時に AutoSupport ですでにメッセージが生成されているという理由で、ヘルスポリシーによってデフォルトで AutoSupport メッセージを無効にすることができます。を使用して、AutoSupport メッセージをトリガーしないようにポリシーを設定できます `system health policy definition modify` コマンドを実行します

を使用して、前の週に送信されたアラートトリガー型AutoSupport メッセージのすべてのリストを表示できます `system health autosupport trigger history show` コマンドを実行します

アラートは EMS へのイベントの生成もトリガーします。イベントは、アラートが作成されるたび、およびアラートがクリアされるたびに生成されます。

使用可能なクラスタヘルスモニタ

ヘルスモニタは複数あり、それぞれがクラスタの異なる部分を監視します。ヘルスモニタは、イベント検出、アラート送信、およびクリアされたイベントの削除を行い、ONTAP システム内で発生したエラーからのリカバリに役立ちます。

ヘルスモニタ名（識別子）	サブシステム名（識別子）	目的
クラスタスイッチ（ cluster -switch ）	スイッチ（ Switch-Health ）	温度、利用率、インターフェイスの設定、冗長性（クラスタネットワークスイッチのみ）、ファンおよび電源の動作に関して、クラスタネットワークスイッチと管理ネットワークスイッチを監視します。クラスタスイッチヘルスモニタは SNMP でスイッチと通信します。デフォルトの設定は SNMPv2c です。 ONTAP 9.2 以降では、最後のポーリング期間以降のクラスタスイッチのリブートをこのモニタで検出して報告できるようになりました。
MetroCluster ファブリック	スイッチ	MetroCluster 構成のバックエンドファブリックトポロジを監視して、間違ったケーブル接続およびゾーニングなどの設定ミスや、 ISL の障害を検出します。
MetroCluster の健常性	インターコネクト、 RAID 、ストレージ	FC-VI アダプタ、 FC イニシエータアダプタ、取り残されたアグリゲートやディスク、およびクラスタ間ポートを監視します
ノード接続（ node-connect ）	CIFS のノンストップオペレーション（ CIFS-NDO ）	SMB 接続を監視して、 Hyper-V アプリケーションへのノンストップオペレーションを実現します。
ストレージ（ SAS-connect ）	ノードレベルでシェルフ、ディスク、およびアダプタを監視して、適切なパスと接続を維持します。	システム
該当なし	他のヘルスモニタからの情報を集約します。	システム接続（ system-connect ）

システムヘルスアラートを自動的に受信する

を使用して、システムヘルスアラートを手動で表示できます `system health alert show` コマンドを実行しますただし、ヘルスモニタがアラートを生成したときに通知を自動的に受信するには、特定の Event Management System （ EMS ；イベント管理システム）メッセージに登録する必要があります。

このタスクについて

次の手順は、すべての hm.alert.raised メッセージ、およびすべての hm.alert.cleared メッセージに対する通知のセットアップ方法を示しています。

すべての hm.alert.raised メッセージおよび hm.alert.cleared メッセージには SNMP トラップが含まれています。SNMPトラップの名前はです `HealthMonitorAlertRaised` および `HealthMonitorAlertCleared`。SNMP トラップについては、 _ ネットワーク管理ガイド _ を参照してください。

手順

1. を使用します `event destination create` コマンドを使用して、EMSメッセージの送信先を定義します。

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. を使用します `event route add-destinations` コマンドを使用してをルーティングします `hm.alert.raised` メッセージおよび `hm.alert.cleared` 宛先へのメッセージ。

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

関連情報

"Network Management の略"

デグレードしたシステムヘルスに対応する

システムのヘルスステータスがデグレードした場合は、アラートを表示して考えられる原因および対処方法について一読し、デグレードしたサブシステムに関する情報を表示して、問題を解決できます。抑制されたアラートも表示されるため、変更して承認済みかどうかを確認できます。

このタスクについて

AutoSupport メッセージやEMSイベントを表示するか、を使用すると、アラートが生成されたことを確認できます `system health` コマンド

手順

1. を使用します `system health alert show` コマンドを使用して、システムヘルスを侵害しているアラートを表示します。
2. アラートに示された原因の考えられる影響、考えられる影響、および対処方法を一読し、問題を解決できるか、または詳細情報が必要かを判断します。
3. 詳細情報が必要な場合は、を使用してください `system health alert show -instance` アラートで使用可能な追加情報 を表示するコマンド。
4. を使用します `system health alert modify` コマンドにを指定します `-acknowledge` パラメータを

指定して、特定のアラートに対して作業中であることを示します。

5. の説明に従って、問題を解決するための対処方法を実行します `Corrective Actions` フィールドに入力します。

   対処方法にはシステムのリブートが含まれている場合があります。

   問題が解決すると、アラートは自動的にクリアされます。サブシステムに他のアラートがない場合は、サブシステムのヘルスがに変わります `OK`。すべてのサブシステムのヘルスがOKの場合は、システム全体のヘルスステータスがに変わります `OK`。

6. を使用します `system health status show` コマンドを入力して、システムヘルスステータスがであることを確認します `OK`。

   システムのヘルスステータスがでない場合 `OK`、この手順 を繰り返します。

デグレードしたシステムヘルスへの対応の例

ノードへの 2 つのパスが不足しているシェルフが原因でデグレードしたシステムヘルスの特定の例を使用して、アラートに対応するときに CLI に表示される内容を確認します。

ONTAP を起動したあと、システムヘルスを確認すると、ステータスがデグレードしていることがわかります。

```
cluster1::>system health status show
  Status
  ---------------
  degraded
```

アラートを表示して、問題箇所を見つけ、シェルフ 2 にノード 1 へのパスが 2 つないことを確認します。

```
      cluster1::>system health alert show
               Node: node1
           Resource: Shelf ID 2
           Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

アラートの詳細を表示して、アラート ID などの詳細情報を取得します。

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
           Acknowledge: false
              Suppress: false
                Policy: DualPathToDiskShelf_Policy
          Acknowledger: -
            Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

アラートを確認して対応中であることを示します。

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

シェルフ 2 とノード 1 との間のケーブルを修正してから、システムをリブートします。次に、システムヘルスを再度確認し、ステータスがになっていることを確認します `OK`：

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

クラスタと管理ネットワークスイッチの検出を設定します

クラスタスイッチヘルスモニタは、 Cisco Discovery Protocol （ CDP ）を使用して、クラスタと管理ネットワークスイッチの検出を自動的に試みます。ヘルスモニタがスイッチを自動的に検出できない場合、または CDP を自動検出に使用することを望まない場合は、ヘルスモニタを設定する必要があります。

このタスクについて

。 `system cluster-switch show` コマンドは、ヘルスモニタが検出したスイッチをリスト表示します。想定していたスイッチがこのリストに表示されない場合、ヘルスモニタは自動的にスイッチを検出できません。

手順

1. CDPを自動検出に使用する場合は、次の手順を実行します。

   a. スイッチで Cisco Discovery Protocol （ CDP ）が有効になっていることを確認します。

      手順については、スイッチのマニュアルを参照してください。

   b. クラスタ内の各ノードで次のコマンドを実行し、 CDP が有効か無効かを確認します。

      run -node *node_name* -command options cdpd.enable

      CDP が有効になっている場合は、手順 d に進みますCDP が無効になっている場合は、手順 c に進みます

   c. 次のコマンドを実行して CDP を有効にします。

      run -node *node_name* -command options cdpd.enable on

   5 分待ってから次の手順に進みます。

   a. を使用します `system cluster-switch show` コマンドを使用して、ONTAP がスイッチを自動的に検出できるようになったかどうかを確認します。

2. ヘルスモニタがスイッチを自動的に検出できない場合は、を使用します `system cluster-switch create` スイッチの検出を設定するコマンドは次のとおりです。

   ```
   cluster1::> system cluster-switch create -device switch1 -address
   192.0.2.250 -snmp-version SNMPv2c -community cshm1! -model NX5020 -type
   cluster-network
   ```

5 分待ってから次の手順に進みます。

3. を使用します `system cluster-switch show` コマンドを使用して、情報を追加したスイッチをONTAP が検出できることを確認します。

完了後

ヘルスモニタがスイッチを監視できることを確認します。

クラスタと管理ネットワークスイッチの監視を確認

クラスタスイッチヘルスモニタは検出されたスイッチの監視を自動的に試みますが、スイッチが正しく設定されていないと監視が自動的に行われないことがあります。ヘルスモニタが使用中のスイッチを監視するように適切に設定されていることを確認してください。

手順

1. クラスタスイッチヘルスモニタによって検出されたスイッチを特定するには、次のコマンドを入力します。

   ONTAP 9.8以降

   ```
   system switch ethernet show
   ```

   ONTAP 9.7以前

   ```
   system cluster-switch show
   ```

   状況に応じて `Model` 列に値が表示されます `OTHER`の場合、`ONTAP` はスイッチを監視できません。`ONTAP` は、値をに設定します `OTHER` 自動検出されたスイッチがヘルスモニタでサポートされていない場合。

   > コマンド出力にスイッチが表示されない場合は、そのスイッチの検出を設定する必要があります。

2. NetApp Support Siteで、サポートされている最新のスイッチソフトウェアとリファレンス構成ファイル（RCF）にアップグレードします。

   "ネットアップサポートのダウンロードページ"

   スイッチの RCF 内のコミュニティストリングは、使用するヘルスモニタが構成されているコミュニティストリングと一致する必要があります。デフォルトでは、ヘルスモニタはコミュニティストリングを使用します `cshm1!`。

   > 現時点では、ヘルスモニタはSNMPv2のみをサポートしています。

   クラスタが監視するスイッチの情報を変更する必要がある場合は、次のコマンドを使用して、ヘルスモニタが使用するコミュニティストリングを変更できます。

ONTAP 9.8以降

```
system switch ethernet modify
```

ONTAP 9.7以前

```
system cluster-switch modify
```

3. スイッチの管理ポートが管理ネットワークに接続されていることを確認します。

   この接続は、 SNMP クエリを実行するために必要です。

システムの健常性を監視するためのコマンドです

を使用できます `system health` システムリソースの健全性に関する情報を表示し、アラートに対応し、以降のアラートを設定するためのコマンド。CLI コマンドを使用すると、ヘルスモニタの設定に関する詳細情報を表示できます。詳細については、各コマンドのマニュアルページを参照してください。

システムヘルスのステータスを表示します

状況	使用するコマンド
個々のヘルスモニタの全体的なステータスを反映した、システムのヘルスステータスを表示する	`system health status show`
ヘルス監視が可能なサブシステムのヘルスステータスを表示する	`system health subsystem show`

ノード接続のステータスを表示します

状況	使用するコマンド
ノードからストレージシェルフへの接続に関する詳細を表示します。これには、ポート情報、 HBA ポート速度、 I/O スループット、 1 秒あたりの I/O 処理数などの情報が含まれます	`storage shelf show -connectivity` を使用します `-instance` 各シェルフに関する詳細情報を表示するためのパラメータ。
使用可能なスペース、シェルフとベイの番号、所有ノード名など、ドライブとアレイ LUN に関する情報を表示します	`storage disk show` を使用します `-instance` 各ドライブに関する詳細情報を表示するためのパラメータ。
ポートのタイプ、速度、ステータスなど、ストレージシェルフポートに関する詳細情報を表示します	`storage port show` を使用します `-instance` 各アダプタに関する詳細情報を表示するためのパラメータ。

クラスタ、ストレージ、および管理ネットワークスイッチの検出を管理します

状況	使用するコマンド（**ONTAP 9.8**以降）	使用するコマンド（**ONTAP 9.7**以前）
クラスタが監視するスイッチを表示します	`system switch ethernet show`	`system cluster-switch show`
削除したスイッチ（コマンド出力の Reason 列に表示）を含む、クラスタが現在監視しているスイッチ、およびクラスタや管理ネットワークスイッチへのネットワークアクセスに必要な設定情報を表示します。 このコマンドは、 advanced 権限レベルで使用できます。	`system switch ethernet show-all`	`system cluster-switch show-all`
未検出のスイッチの検出を設定します	`system switch ethernet create`	`system cluster-switch create`
クラスタが監視するスイッチに関する情報（デバイス名、 IP アドレス、 SNMP バージョン、コミュニティストリングなど）を変更する	`system switch ethernet modify`	`system cluster-switch modify`
スイッチの監視を無効にします	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
スイッチの検出と監視を無効にし、スイッチの設定情報を削除します	`system switch ethernet delete`	`system cluster-switch delete`
データベースに格納されているスイッチ設定情報を完全に削除する（これにより、スイッチの自動検出が再度有効になる）	`system switch ethernet delete -force`	`system cluster-switch delete -force`
AutoSupport メッセージで送信するには、自動ロギングを有効にします。	`system switch ethernet log`	`system cluster-switch log`

生成されたアラートに対応する

状況	使用するコマンド
アラートがトリガーされたリソースやノード、アラートの重大度や原因など、生成されたアラートに関する情報を表示する	`system health alert show`
生成された各アラートの情報を表示する	`system health alert show -instance`
アラートに対して作業中であることを示します	`system health alert modify`
アラートを確認します	`system health alert modify -acknowledge`
サブシステムのヘルスステータスに影響しないように、以降のアラートを抑制する	`system health alert modify -suppress`
自動的に消去されなかったアラートを削除します	`system health alert delete`
あるアラートで AutoSupport メッセージがトリガーされたかどうかを確認するためなど、過去 1 週間にアラートによってトリガーされた AutoSupport メッセージに関する情報を表示する	`system health autosupport trigger history show`

以後のアラートを設定

状況	使用するコマンド
リソースの状態に応じて特定のアラートを発行するかどうかを制御するポリシーを有効または無効にします	`system health policy definition modify`

ヘルスモニタの設定に関する情報を表示します

状況	使用するコマンド
ヘルスモニタについて、ノード、名前、サブシステム、ステータスなどの情報を表示する	`system health config show` を使用します `-instance` 各ヘルスモニタに関する詳細情報を表示するためのパラメータ。
ヘルスモニタで生成される可能性があるアラートの情報を表示する	`system health alert definition show` を使用します `-instance` 各アラート定義に関する詳細情報を表示するためのパラメータ。

状況	使用するコマンド
アラートが発行されるタイミングを決定する、ヘルスモニタのポリシーに関する情報を表示する	`system health policy definition show` を使用します `-instance` 各ポリシーに関する詳細情報を表示するためのパラメータ。ポリシーのステータス（有効または無効）、ヘルスモニタ、アラートなどによってアラートのリストをフィルタリングするには、その他のパラメータを使用します。

環境情報を表示します

センサーを使用すると、システムの環境コンポーネントを監視できます。環境センサーについて表示できる情報には、タイプ、名前、状態、値、しきい値警告などがあります。

ステップ

1. 環境センサーに関する情報を表示するには、を使用します `system node environment sensors show` コマンドを実行します

File System Analytics の略

File System Analytics の概要

ONTAP 9.8で初めてFSA（ファイルシステム分析）が導入され、ONTAP FlexGroup またはFlexVol ボリューム内のファイル使用状況やストレージ容量の傾向をリアルタイムで可視化できるようになりました。この標準搭載の機能により、外部ツールが不要になり、ストレージの利用状況や、ビジネスニーズに合わせてストレージを最適化できるかどうかに関する重要な分析情報を得ることができます。

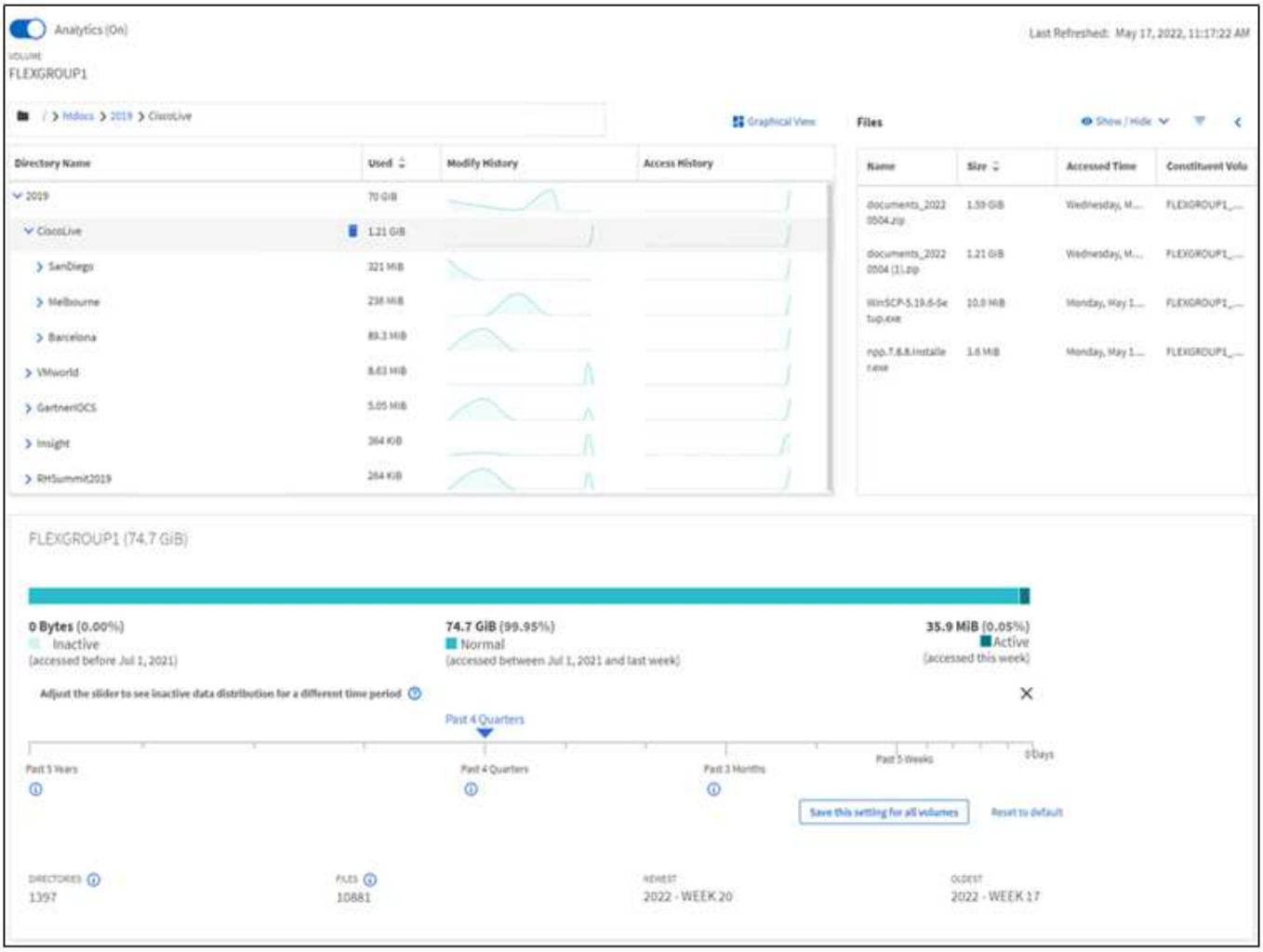
FSAを使用すると、NAS内のボリュームのファイルシステム階層のすべてのレベルが可視化されます。たとえば、Storage VM（SVM）、ボリューム、ディレクトリ、ファイルの各レベルで使用状況と容量を分析できます。FSAを使用して回答 に関する次のような質問をすることができます

- ストレージがいっぱいになっているのは何ですか？また、別のストレージに移動できる大きなファイルはありますか？
- 最もアクティブなボリューム、ディレクトリ、およびファイルはどれですか？ストレージのパフォーマンスはユーザのニーズに合わせて最適化されていますか？
- 先月に追加されたデータの量
- 最もアクティブなストレージユーザと最もアクティブでないストレージユーザのどちらを探していますか？
- プライマリストレージには、どのくらいの非アクティブデータまたは休止データがありますか？そのデータを低コストのコールド階層に移動できますか。

- 計画したサービス品質の変更は、重要で頻繁にアクセスされるファイルへのアクセスに悪影響を及ぼしますか？

ファイルシステム分析は、ONTAP システムマネージャに統合されています。System Managerには次の機能があります。

- リアルタイムで可視化できるため、効果的なデータ管理と運用が可能です
- リアルタイムのデータ収集と集約
- サブディレクトリとファイルのサイズと数、および関連付けられているパフォーマンスプロファイル
- 変更履歴およびアクセス履歴のファイル経過時間ヒストグラム



サポートされているボリュームタイプ

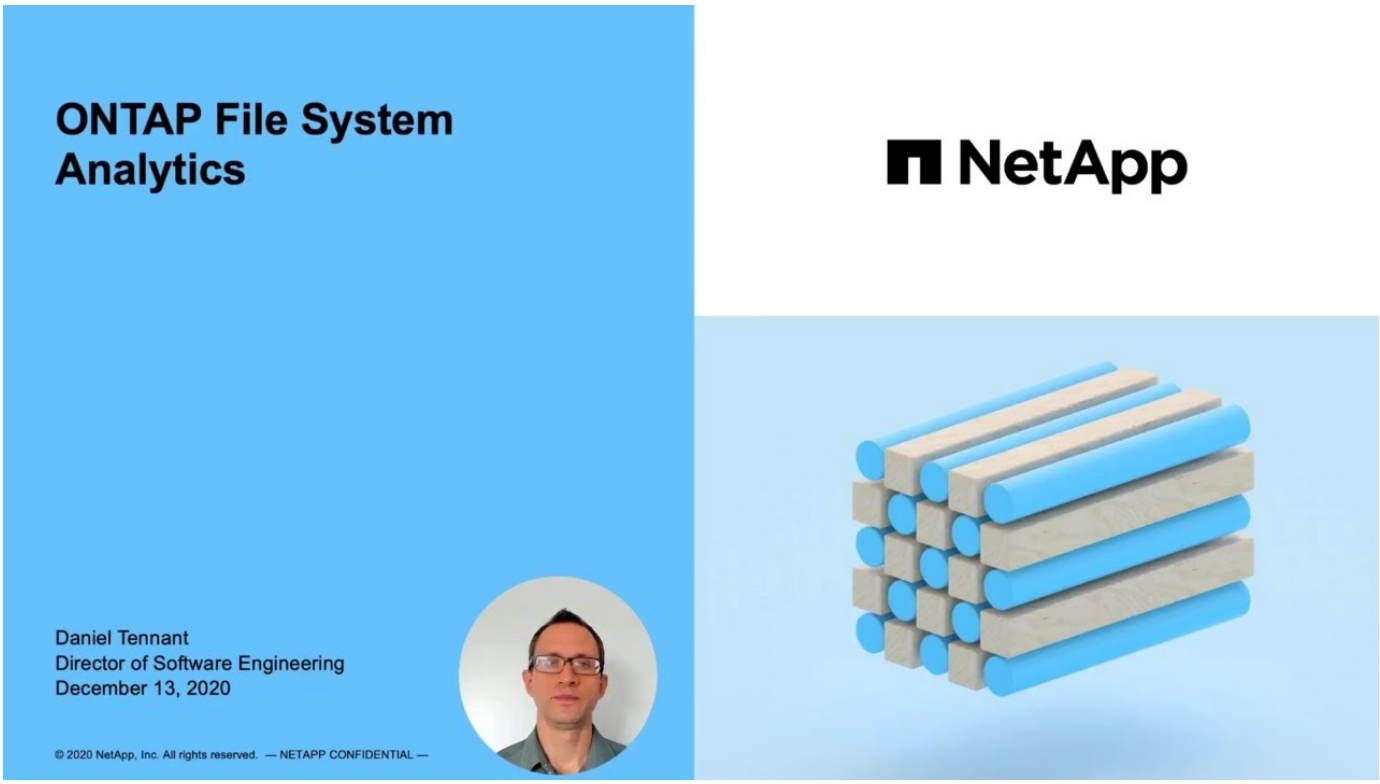
ファイルシステム分析は、 FlexCache キャッシュと SnapMirror デスティネーションボリュームを除き、アクティブな NAS データがあるボリュームで可視化を実現するように設計されています。

ファイルシステム分析機能の可用性

ONTAPの各リリースでは、ファイルシステム分析の範囲が拡張されます。

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
System Manager での表示	✓	✓	✓	✓	✓	✓	✓
容量分析	✓	✓	✓	✓	✓	✓	✓
アクセス頻度の低いデータの情報	✓	✓	✓	✓	✓	✓	✓
Data ONTAP 7-Modeから移行されたボリュームのサポート	✓	✓	✓	✓	✓	✓	
System Managerで非アクティブ期間をカスタマイズできます	✓	✓	✓	✓	✓	✓	
ボリュームレベルのアクティビティトラッキング	✓	✓	✓	✓	✓		
アクティビティトラッキングデータをCSVにダウンロードします	✓	✓	✓	✓	✓		
SVMレベルのアクティビティ追跡	✓	✓	✓	✓			
タイムライン	✓	✓	✓	✓			
使用状況分析	✓	✓	✓				
オプションを選択して、ファイルシステム分析をデフォルトで有効にします	✓	✓					
初期化スキャン進行状況モニタ	✓						

ファイルシステム分析の詳細をご覧ください



詳細はこちら

- "TR-4687 ：『 Best Practices guidelines for ONTAP File System Analytics 』"
- "ナレッジベース：NetApp ONTAP ファイルシステム分析をオンにしたあとにレイテンシが大きく変動する、または変動する"

File System Analytics を有効にします

容量分析などの使用状況データを収集して表示するには、ボリュームでファイルシステム分析を有効にする必要があります。

このタスクについて

- ONTAP 9.8以降では、新規または既存のボリュームでファイルシステム分析を有効にできます。システムをONTAP 9.8以降にアップグレードする場合は、ファイルシステム分析を有効にする前に、すべてのアップグレードプロセスが完了していることを確認してください。
- ボリュームのサイズと内容によっては、 ONTAP がボリューム内の既存データを処理する間、分析を有効にするのに時間がかかることがあります。完了すると、 System Manager に進捗状況が表示され、分析データが表示されます。初期化の進捗状況に関する詳細情報が必要な場合は、ONTAP CLIコマンドを使用します `volume analytics show`。

  ONTAP 9.14.1以降のONTAPでは、スキャンの進行状況に影響するスロットルイベントに関する通知に加えて、初期化スキャンの進行状況を追跡できます。

  初期化スキャンに関するその他の考慮事項については、を参照してください スキャンに関する考慮事項。

手順

ONTAP システムマネージャまたはCLIを使用して、ファイルシステム分析を有効にできます。

System Manager の略

ONTAP 9.8 および **9.9.1** では	**ONTAP 9.10.1** 以降でサポートされます
1. 「 * Storage 」 > 「 Volumes 」を選択します。 2. 目的のボリュームを選択し、 * エクスプローラ * を選択します。 3. 「 * 分析を有効にする * 」または「 * 分析を無効にする * 」を選択します。	1. 「 * Storage 」 > 「 Volumes 」を選択します。 2. 目的のボリュームを選択します。個別のボリューム・メニューから、 * ファイル・システム > エクスプローラ * を選択します。 3. 「 * 分析を有効にする * 」または「 * 分析を無効にする * 」を選択します。

CLI の使用

CLI を使用してファイルシステム分析を有効にします

1. 次のコマンドを実行します。
   `volume analytics on -vserver` *`svm_name`* `-volume` *`volume_name`* `[-foreground {true|false}]`
   デフォルトでは、このコマンドはフォアグラウンドで実行されます。 ONTAP は進捗状況を表示し、完了すると分析データを表示します。より正確な情報が必要な場合は、を使用してコマンドをバックグラウンドで実行できます `-foreground false` オプションを選択し、を使用します `volume analytics show` CLIに初期化の進行状況を表示するコマンド。
2. ファイルシステム分析を有効にしたら、System ManagerまたはONTAP REST APIを使用して分析データを表示します。

ファイルシステム分析のデフォルト設定を変更します

ONTAP 9.13.1以降では、SVMまたはクラスタの設定を変更して、新しいボリュームに対してデフォルトでファイルシステム分析を有効にすることができます。

System Manager の略

System Managerを使用している場合は、Storage VMまたはクラスタの設定を変更して、ボリューム作成時に容量分析とアクティビティ追跡をデフォルトで有効にすることができます。設定の変更後に作成された環境ボリュームのみがデフォルトで有効になり、既存のボリュームは有効になりません。

クラスタのファイルシステム分析の設定を変更します

1. System Managerで、***[**クラスタ設定]に移動します。
2. クラスタ設定で、[ファイルシステム設定]タブを確認します。設定を変更するには、を選択します ⚙ をクリックします。
3. [***Activity Tracking**]フィールドに、アクティビティ追跡をデフォルトで有効にするSVMの名前を入力します。このフィールドを空白のままにすると、すべてのSVMでアクティビティ追跡が無効のままになります。

   新しいStorage VMでアクティビティ追跡をデフォルトで無効にするには、[**Enable on new Storage VMs]**ボックスをオフにします。

4. [***Analytics**]フィールドに、容量分析をデフォルトで有効にするStorage VMの名前を入力します。このフィールドを空白のままにすると、すべてのSVMで容量分析が無効なままになります。

   新しいStorage VMに対して容量分析をデフォルトで無効にするには、[**Enable on new Storage VMs]**ボックスをオフにします。

5. 保存を選択します。

SVMのファイルシステム分析設定を変更します

1. 変更するSVMを選択し、 **Storage VM**設定を選択します。
2. [* **File System Analytics**]カードで、トグルを使用して、Storage VM上のすべての新しいボリュームに対してアクティビティ追跡と容量分析を有効または無効にします。

CLI の使用

ONTAP CLIを使用して、新しいボリュームでファイルシステム分析をデフォルトで有効にするようにStorage VMを設定できます。

SVMでファイルシステム分析をデフォルトで有効にします

1. SVMを変更して、新しく作成したすべてのボリュームで容量分析とアクティビティ追跡をデフォルトで有効にします。
   ```
   vserver modify -vserver svm_name -auto-enable-activity-tracking true -auto
   -enable-analytics true
   ```

ファイルシステムのアクティビティを表示します

File System Analytics（FSA）を有効にすると、選択したボリュームのルートディレクトリの内容を各サブツリーで使用されているスペースでソートして表示できます。

ファイルシステムを参照したり、ディレクトリ内の各オブジェクトに関する詳細情報を表示したりするには、任意のファイルシステムオブジェクトを選択します。ディレクトリの情報をグラフィカルに表示することもできます。時間の経過とともに、各サブツリーの履歴データが表示されます。ディレクトリ数が 3000 を超える

場合、使用済みスペースはソートされません。

エクスプローラ（ **Explorer** ）

File System Analytics * Explorer * 画面は、次の 3 つの領域で構成されています。

- ディレクトリとサブディレクトリのツリービュー。名前、サイズ、変更履歴、アクセス履歴を示す展開可能なリスト。
- ファイル。ディレクトリリストで選択したオブジェクトの名前、サイズ、アクセス日時を表示します。
- ディレクトリリストで選択したオブジェクトのアクティブデータと非アクティブデータの比較。

  ONTAP 9.9.1以降では、レポート対象の範囲をカスタマイズできます。デフォルト値は 1 年です。これらのカスタマイズ内容に基づいて、ボリュームの移動や階層化ポリシーの変更などの対処を実行できます。

デフォルトでは、アクセス時間が表示されます。ただし、CLIから（を設定して）ボリュームのデフォルトを変更した場合は `-atime-update` オプションをに設定します `false` を使用 `volume modify` コマンド）を入力した場合は、最終変更時刻のみが表示されます。例：

- ツリービューには、 * アクセス履歴 * は表示されません。
- ファイルビューが変更されます。
- 変更後の時刻に基づいてアクティブ/非アクティブデータビューが表示されます (`mtime`）。

これらの表示を使用して、次のことを確認できます。

- ファイルシステムの場所が最も多くのスペースを消費している
- ディレクトリおよびサブディレクトリ内のファイル数やサブディレクトリ数など、ディレクトリツリーに関する詳細情報
- 古いデータを含むファイルシステムの場所（スクラッチ、一時、ログツリーなど）

FSA の出力を解釈するときは、次の点に留意してください。

- データの使用場所と使用時期は、処理されるデータ量ではなく、 FSA によって示されます。たとえば、最近アクセスされたファイルや変更されたファイルによる大量のスペース消費は、必ずしもシステムの処理負荷が高いことを示すわけではありません。
- [ボリュームエクスプローラ *] タブで FSA のスペース消費を計算する方法は、他のツールとは異なる場合があります。特に、ボリュームで Storage Efficiency 機能が有効になっている場合、ボリューム概要 * で報告される消費量と大きく異なる可能性があります。これは、 * ボリュームエクスプローラ * タブには効率化による削減効果がないためです。
- ディレクトリ表示のスペースに制限があるため、 *List View* で 8 レベルを超えるディレクトリ階層を表示することはできません。8 レベルを超えるディレクトリを詳細に表示するには、 *Graphical View* に切り替え、目的のディレクトリを見つけて、 *List View* に切り替える必要があります。これにより、ディスプレイに画面スペースが追加されます。

手順

1. 選択したボリュームのルートディレクトリの内容を表示します。

ONTAP 9.8 および 9.9.1 では	ONTAP 9.10.1 以降でサポートされます
[* ストレージ] 、 [ボリューム] の順にクリックし、目的のボリュームを選択して、 [* エクスプローラ *] をクリックします。	[* Storage] > [Volumes] を選択し、目的のボリュームを選択します。個別のボリューム・メニューから、 * ファイル・システム > エクスプローラ * を選択します。

アクティビティトラッキングを有効にします

ONTAP 9.10.1以降のファイルシステム分析にはアクティビティ追跡機能が含まれています。この機能を使用すると、ホットオブジェクトを特定してデータをCSVファイルとしてダウンロードできます。ONTAP 9.11.1以降では、アクティビティトラッキングがSVMスコープに拡張されています。また、ONTAP 9.11.1以降、System Managerではアクティビティ追跡のタイムラインが表示され、最大5分間のアクティビティ追跡データを確認できます。

アクティビティ追跡では、次の 4 つのカテゴリでモニタリングが可能です。

- ディレクトリ
- ファイル
- クライアント
- ユーザ

監視対象のカテゴリごとに、読み取り IOPS 、書き込み IOPS 、読み取りスループット、書き込みスループットが表示されます。アクティビティトラッキングに関するクエリーは、過去 5 秒間にシステムに表示されたホットスポットに関連する 10 〜 15 秒ごとに更新されます。

アクティビティ追跡情報は概算値であり、データの正確性は受信 I/O トラフィックの分散に依存します。

System Managerでボリュームレベルでアクティビティ追跡を表示している場合は、展開されたボリュームのメニューだけがアクティブに更新されます。ボリュームのビューが縮小されている場合、ボリュームの表示が展開されるまで表示は更新されません。更新を停止するには、 * 更新を一時停止 * ボタンを使用します。アクティビティデータは CSV 形式でダウンロードでき、選択したボリュームについて収集されたすべてのポイントインタイムデータが表示されます。

タイムライン機能を使用できるONTAP 9.11.1以降では、ボリュームまたはSVM上のホットスポットアクティビティの記録を保持し、約5秒ごとに継続的に更新し、過去5分間のデータを保持できます。タイムラインデータは、ページの表示領域にあるフィールドに対してのみ保持されます。追跡カテゴリを折りたたむかスクロールしてタイムラインが表示されないようにすると、タイムラインはデータの収集を停止します。デフォルトでは、タイムラインは無効になっており、[アクティビティ]タブから移動すると自動的に無効になります。

1つのボリュームのアクティビティトラッキングを有効にします

アクティビティ追跡は、ONTAP System ManagerまたはCLIを使用して有効にできます。

このタスクについて

ONTAP REST API または System Manager で RBAC を使用する場合は、アクティビティ追跡へのアクセスを管理するためのカスタムロールを作成する必要があります。を参照してください ロールベースアクセス制御 をクリックしてください。

System Manager の略

手順

1. Storage > Volumes （ストレージ）を選択します。目的のボリュームを選択します。個々のボリュームメニューから、ファイルシステムを選択し、アクティビティタブを選択します。
2. 上位のディレクトリ、ファイル、クライアント、およびユーザに関する個々のレポートを表示するには、 * Activity Tracking * をオンにします。
3. 更新を行わずにデータをより詳細に分析するには、 * 更新を一時停止 * を選択します。データをダウンロードして、レポートの CSV レコードを取得することもできます。

CLI の使用

手順

1. アクティビティトラッキングを有効にする：

   ```
   volume activity-tracking on -vserver svm_name -volume volume_name
   ```

2. 次のコマンドを使用して、ボリュームのアクティビティ追跡の状態がオンまたはオフになっているかどうかを確認します。

   ```
   volume activity-tracking show -vserver svm_name -volume volume_name -state
   ```

3. 有効にしたら、 ONTAP システムマネージャまたは ONTAP REST API を使用してアクティビティ追跡データを表示します。

複数のボリュームのアクティビティ追跡を有効にします

System ManagerまたはCLIを使用して、複数のボリュームのアクティビティ追跡を有効にすることができます。

このタスクについて

ONTAP REST API または System Manager で RBAC を使用する場合は、アクティビティ追跡へのアクセスを管理するためのカスタムロールを作成する必要があります。を参照してください ロールベースアクセス制御 をクリックしてください。

System Manager の略

特定のボリュームに対して有効にします

1. Storage > Volumes （ストレージ）を選択します。目的のボリュームを選択します。個々のボリュームメニューから、ファイルシステムを選択し、アクティビティタブを選択します。
2. アクティビティトラッキングを有効にするボリュームを選択します。ボリュームリストの上部で、その他のオプション*ボタンを選択します。［*アクティビティトラッキングを有効にする］を選択します。
3. SVMレベルでアクティビティの追跡を表示するには、表示するSVMを* Storage > Volumes *から選択します。[ファイルシステム]タブに移動して[アクティビティ]を選択すると、アクティビティ追跡が有効になっているボリュームのデータが表示されます。

すべてのボリュームでを有効にします

1. Storage > Volumes （ストレージ）を選択します。メニューからSVMを選択します。
2. 「* File System 」タブに移動し、「 More *」タブを選択して、SVM内のすべてのボリュームでアクティビティの追跡を有効にします。

CLI の使用

ONTAP 9.13.1以降では、ONTAP CLIを使用して複数のボリュームのアクティビティ追跡を有効にすることができます。

手順

1. アクティビティトラッキングを有効にする：

   ```
   volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
   ```

   使用 * 指定したStorage VM上のすべてのボリュームに対してアクティビティ追跡を有効にします。

   使用 ！続けてボリューム名を指定し、指定したボリュームを除くSVM上のすべてのボリュームに対してアクティビティ追跡を有効にします。

2. 処理が成功したことを確認します。

   ```
   volume show -fields activity-tracking-state
   ```

3. 有効にしたら、 ONTAP システムマネージャまたは ONTAP REST API を使用してアクティビティ追跡データを表示します。

使用状況分析を実現

ONTAP 9.12.1以降では、使用状況分析を有効にして、ボリューム内のどのディレクトリが最もスペースを使用しているかを確認できます。ボリューム内のディレクトリの総数、またはボリューム内のファイルの総数を表示できます。Reportingは、最もスペースを使用する25個のディレクトリに制限されます。

大規模ディレクトリの分析は15分ごとに更新されます。ページ上部の[Last refreshed]のタイムスタンプを確認すると、最新の更新を監視できます。[ダウンロード]ボタンをクリックして、Excelブックにデータをダウンロードすることもできます。ダウンロード処理はバックグラウンドで実行され、選択したボリュームについて最

新の情報が表示されます。結果が表示されずにスキャンが戻った場合は、ボリュームがオンラインであることを確認します。SnapRestore などのイベントが発生すると、原因 ファイルシステム分析は大きなディレクトリのリストを再構築します。

手順

1. Storage > Volumes （ストレージ）を選択します。目的のボリュームを選択します。
2. 個別のボリューム・メニューから、ファイル・システム*を選択します。次に、 Usage *タブを選択します。
3. 使用状況の分析を有効にするには、* Analytics *スイッチを切り替えます。
4. System Managerでは、最大サイズのディレクトリを降順に示す棒グラフが表示されます。

> ONTAP では、上位ディレクトリのリストの収集中に、部分データが表示されたり、まったくデータが表示されないことがあります。スキャンの進行状況は、スキャン中に表示される[**Usage**]タブで確認できます。

特定のディレクトリに関する詳細な情報を得るには、次の手順を実行します。 ファイルシステム上のアクティビティを表示する。

分析に基づいて修正措置を講じる

ONTAP 9.9.1以降では、ファイルシステム分析画面から、現在のデータと期待される結果に基づいて直接対処できます。

ディレクトリとファイルを削除します

エクスプローラの表示で、削除するディレクトリまたは個々のファイルを選択できます。低レイテンシの高速ディレクトリ削除機能により、ディレクトリが削除されます。（高速ディレクトリ削除は、分析を有効にしない ONTAP 9.9.1 以降でも使用できます）。

手順

1. [* ストレージ] 、 [ボリューム] の順にクリックし、 [* エクスプローラ *] をクリックします。

   ファイルまたはフォルダにカーソルを合わせると、削除するオプションが表示されます。一度に削除できるオブジェクトは 1 つだけです。

> ディレクトリとファイルを削除しても、新しいストレージ容量の値はすぐには表示されません。

ストレージ階層にメディアコストを割り当てて、使用頻度の低いデータストレージのコストを比較します

メディアコストは、ストレージコストの評価に基づいて割り当てた値であり、 GB あたりの通貨を選択したものとして表されます。設定すると、 System Manager は割り当てられているメディアコストを使用して、ボリュームを移動するときの推定削減量を計算します。

設定したメディアコストは永続的ではなく、 1 つのブラウザセッションにのみ設定できます。

手順

1. [ストレージ]>[階層]をクリックし、ローカル階層（アグリゲート）のタイルで[メディアコストの設定]*を

クリックします。

アクティブな階層と非アクティブな階層を選択して、比較を有効にしてください。

2. 通貨タイプと金額を入力します。

   メディアコストを入力または変更すると、すべてのメディアタイプで変更が行われます。

ボリュームを移動してストレージコストを削減

分析画面やメディアコストの比較に基づいて、ローカル階層内の低コストのストレージにボリュームを移動できます。

一度に 1 つのボリュームのみを比較および移動できます。

手順

1. メディアコストの表示を有効にしたら、 [* ストレージ > 階層 *] をクリックし、 [* ボリューム *] をクリックします。
2. ボリュームのデスティネーションオプションを比較するには、をクリックします ⋮ ボリュームの場合は、 * 移動 * をクリックします。
3. [Select Destination Local Tier] （宛先ローカル階層の選択）画面で、推定コスト差異を表示する宛先階層を選択します。
4. オプションを比較したら、目的の階層を選択し、 * 移動 * をクリックします。

ファイルシステム分析を使用したロールベースアクセス制御

ONTAP 9.12.1以降では、ONTAP に、という名前の事前定義されたロールベースアクセス制御（RBAC）ロールが含まれています `admin-no-fsa`。。 `admin-no-fsa` ロールは管理者レベルの権限を付与しますが、に関連する処理は実行できません `files` ONTAP CLI、REST API、およびSystem Managerのエンドポイント（ファイルシステム分析など）

詳細については、を参照してください `admin-no-fsa` ロール。を参照してください クラスタ管理者の事前定義されたロール。

ONTAP 9.12.1よりも前のバージョンのONTAP を使用している場合は、ファイルシステム分析へのアクセスを制御する専用のロールを作成する必要があります。ONTAP 9.12.1よりも前のバージョンのONTAP では、ONTAP CLIまたはONTAP REST APIを使用してRBAC権限を設定する必要があります。

System Manager の略

ONTAP 9.12.1以降では、System Managerを使用してファイルシステム分析用のRBAC権限を設定できます。

手順

1. [* Cluster]>[Settings]（設定）を選択します。**[***セキュリティ]で、[ユーザーと役割]に移動し、を選択します →。
2. [役割（ Roles）]でを選択します + Add 。
3. ロールの名前を指定します。Role Attributesで、適切なを指定してユーザロールのアクセスまたは制限を設定します "APIエンドポイント"。File System Analyticsアクセスまたは制限を設定するためのプライマリパスとセカンダリパスについては、次の表を参照してください。

制限	プライマリパス	セカンダリパス
ボリュームのアクティビティ追跡	`/api/storage/volumes`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
SVMのアクティビティ追跡	`/api/svm/svms`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
すべてのファイルシステム分析処理	`/api/storage/volumes`	`/:uuid/files`

を使用できます `/*/` エンドポイントのすべてのボリュームまたはSVMにポリシーを設定する場合は、UUIDの代わりにUUIDが設定されます。

各エンドポイントのアクセス権限を選択します。

4. [保存（ Save ）] を選択します。
5. ユーザにロールを割り当てる手順については、を参照してください 管理者アクセスの制御。

CLI の使用

ONTAP 9.12.1よりも前のバージョンのONTAP を使用している場合は、ONTAP CLIを使用してカスタム

ロールを作成します。

手順

1. すべての機能にアクセスできるようにデフォルトのロールを作成します。

   この作業は ' ロールがアクティビティの追跡のみに限定されるようにするために ' 制限的なロールを作成する前に実行する必要があります

   ```
   security login role create -cmddirname DEFAULT -access all -role
   storageAdmin
   ```

2. 制限付きロールを作成します。

   ```
   security login role create -cmddirname "volume file show-disk-usage"
   -access none -role storageAdmin
   ```

3. ロールに SVM の Web サービスへのアクセスを許可します。

   - `rest` （REST API呼び出しの場合）
   - `security` パスワード保護のため
   - `sysmgr` System Managerへのアクセスに使用します

     ```
     vserver services web access create -vserver svm-name -name_ -name rest
     -role storageAdmin
     ```

     ```
     vserver services web access create -vserver svm-name -name security
     -role storageAdmin
     ```

   ```
   vserver services web access create -vserver svm-name -name sysmgr -role
   storageAdmin
   ```

4. ユーザを作成します。

   ユーザに適用するアプリケーションごとに個別の create コマンドを問題 に設定する必要があります。同じユーザで create を複数回呼び出すと、すべてのアプリケーションがそのユーザに適用されるだけで、毎回新しいユーザが作成されることはありません。。 `http` アプリケーションタイプのパラメータは、ONTAP REST APIおよびSystem Managerに適用されます。

   ```
   security login create -user-or-group-name storageUser -authentication
   -method password -application http -role storageAdmin
   ```

5. 新しいユーザクレデンシャルを使用して、System Managerにログインするか、ONTAP REST APIを使用してファイルシステム分析データにアクセスできるようになりました。

詳細情報

- クラスタ管理者の事前定義されたロール
- System Managerで管理者アクセスを制御します
- "RBACロールとONTAP REST APIの詳細については、こちらをご覧ください"

ファイルシステム分析に関する考慮事項

ファイルシステム分析の実装に伴う使用の制限とパフォーマンスへの潜在的な影響について理解しておく必要があります。

SVMで保護されている関係

保護関係にある SVM を含むボリュームでファイルシステム分析を有効にしている場合、分析データはデスティネーション SVM にレプリケートされません。リカバリ処理でソース SVM を再同期する必要がある場合は、リカバリ後に目的のボリュームの分析を手動で再度有効にする必要があります。

パフォーマンスに関する考慮事項

場合によっては、File System Analyticsを有効にすると、メタデータの初回収集時のパフォーマンスに悪影響を及ぼすことがあります。この状況は、通常、使用率が最大のシステムで発生します。このようなシステムでは、分析を有効にしないように、ONTAP System Managerのパフォーマンス監視ツールを使用できます。

レイテンシが著しく増加している場合は、ナレッジベースの記事を参照してください "NetApp ONTAP ファイルシステム分析を有効にしたあとにレイテンシが増減する"。

スキャンに関する考慮事項

容量分析を有効にすると、ONTAPは容量分析の初期化スキャンを実行します。スキャンは、容量分析が有効になっているボリューム内のすべてのファイルのメタデータにアクセスします。スキャン中にファイルデータは読み取られません。ONTAP 9.14.1以降では、REST API、System Managerの[* **Explorer**]タブ、または `volume analytics show` CLIコマンド。スロットルイベントが発生した場合は、ONTAPから通知が送信されます。

スキャンが完了すると、ファイルシステムの変更に応じてファイルシステム分析がリアルタイムで継続的に更新されます。スキャンを再度実行する必要はありません。

スキャンに必要な時間は、ボリューム上のディレクトリとファイルの数に比例します。スキャンではメタデータが収集されるため、ファイルサイズはスキャン時間に影響しません。

初期化スキャンの詳細については、を参照してください "TR-4867：『Best Practice Guidelines for File System Analytics』"。

ベストプラクティス

アグリゲートを共有していないボリュームでスキャンを開始する必要があります。現在どのアグリゲートがどのボリュームをホストしているかは、コマンドを使用して確認できます。

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

スキャンの実行中も、ボリュームは引き続きクライアントトラフィックを処理します。クライアントトラフィックが低いと予想される期間にスキャンを開始することをお勧めします。

クライアントトラフィックが増加すると、システムリソースが消費され、原因 スキャンにかかる時間が長くなります。

ONTAP 9.12.1以降では、System ManagerおよびONTAP CLIでデータ収集を一時停止できます。

- ONTAP CLIを使用する場合は、次の手順を実行します。
  - 次のコマンドを使用してデータ収集を一時停止できます。 `volume analytics initialization pause -vserver *svm_name* -volume *volume_name*`
  - クライアントトラフィックの速度が低下したら、次のコマンドを使用してデータ収集を再開できます。 `volume analytics initialization resume -vserver *svm_name* -volume *volume_name*`
- System Managerを使用している場合は、ボリュームメニューの*ビューで[データ収集の一時停止]および[データ収集の再開]*ボタンを使用してスキャンを管理します。

EMSノセツテイ

EMS設定の概要

早急な対応が必要なシステムの問題をすぐに通知するように、イベント管理システム（EMS）の重要なイベント通知をEメールアドレス、syslogサーバ、簡易管理ネットワークプロトコル（SNMP）トラップホスト、またはWebhookアプリケーションに直接送信するようにONTAP 9を設定できます。

重要なイベント通知はデフォルトでは有効になっていないため、Eメールアドレス、syslogサーバ、SNMPトラップホスト、またはWebhookアプリケーションのいずれかに通知を送信するようにEMSを設定する必要があります。

のリリース固有のバージョンを確認します "ONTAP 9 EMSリファレンス"。

EMSイベントのマッピングで廃止されたONTAP コマンドセット（イベントの送信先、イベントルートなど）を使用している場合は、マッピングを更新することを推奨します。 "廃止されたONTAP コマンドからEMSマッピングを更新する方法について説明します"。

System Manager で EMS イベントの通知とフィルタを設定します

System Manager を使用して、早急な対応を要するシステムの問題を通知するために、Event Management System （ EMS ；イベント管理システム）でのイベント通知の配信方法を設定できます。

ONTAPバージョン	System Manager で実行できる作業
ONTAP 9.12.1以降	リモートsyslogサーバにイベントを送信するときに、Transport Layer Security（TLS）プロトコルを指定します。
ONTAP 9.10.1 以降	SNMPトラップホストに加え、Eメールアドレス、syslogサーバ、Webフックアプリケーションを設定します。
ONTAP 9.7 から 9.10.0	SNMP トラップホストのみを設定する。 ONTAP CLI を使用して他の EMS デスティネーションを設定できます。 を参照してください "EMS設定の概要"。

次の手順を実行できます。

- [add-ems-destination]
- [create-ems-filter]
- [edit-ems-destination]
- [edit-ems-filter]
- [delete-ems-destination]
- [delete-ems-filter]

関連情報

- "ONTAP EMSリファレンス"
- "CLI を使用して、イベント通知を受信する SNMP トラップホストを設定します"

EMS イベント通知の送信先を追加します

System Manager を使用して、 EMS メッセージの送信先を指定できます。

ONTAP 9.12.1以降では、EMSイベントをTransport Layer Security（TLS）プロトコル経由でリモートsyslogサーバの指定ポートに送信できます。詳細については、を参照してください `event notification destination create` のマニュアルページ。

手順

1. [**Cluster] > [Settings**] の順にクリックします。
2. [*Notifications Management] セクションで、をクリックします ⋮をクリックし、 * イベントの送信先の表示 * をクリックします。
3. [* 通知管理 **]** ページで、 **[** イベントの送信先 *] タブを選択します。
4. をクリックします + Add 。
5. 名前、 EMS デスティネーションタイプ、およびフィルタを指定します。

> ⓘ 必要に応じて、新しいフィルタを追加できます。 [新しいイベントフィルタの追加 *] をクリックします。

6. 選択した EMS デスティネーションのタイプに応じて、次の情報を指定します。

構成する	指定または選択 …
SNMP トラップホスト	• トラップホスト名
E メール （ 9.10.1 以降）	• 送信先 E メールアドレス • メールサーバ • 送信元 E メールアドレス

syslog サーバ （ 9.10.1 以降）	• サーバのホスト名または IP アドレス • Syslogポート（9.12.1以降） • Syslog転送（9.12.1以降） TCP Encrypted を選択すると、**Transport Layer Security**（**TLS**）プロトコルが有効になります。**syslog**ポート*に値を入力しない場合は、「 Syslog transport *」の選択に基づいてデフォルトが使用されます。
ウェブフック （ 9.10.1 以降）	• webhook URL • クライアント認証（クライアント証明書を指定する場合はこのオプションを選択します）

新しい **EMS** イベント通知フィルタを作成します

ONTAP 9.10.1 以降の System Manager を使用して、 EMS 通知の処理ルールを指定する、カスタマイズされた新しいフィルタを定義できます。

手順

1. [**Cluster] > [Settings**] の順にクリックします。
2. [**Notifications Management]** セクションで、をクリックします ⋮をクリックし、[イベントの送信先の表示]*をクリックします。
3. [* 通知管理 *] ページで、 [* イベント・フィルタ *] タブを選択します。
4. をクリックします ＋ Add 。
5. 名前を指定し、既存のイベントフィルタからルールをコピーするか、新しいルールを追加するかを選択します。
6. 選択した手順に応じて、次の手順を実行します。

選択した場合	次に、次の手順を実行します。
• 既存のイベントフィルタからルールをコピー *	1. 既存のイベントフィルタを選択します。 2. 既存のルールを変更します。 3. 必要に応じて、をクリックして他のルールを追加します ＋ Add 。
• 新しいルールを追加 *	新しいルールごとに、タイプ、名前パターン、重大度、および SNMP トラップのタイプを指定します。

EMS イベント通知の送信先を編集します

ONTAP 9.10.1 以降では、 System Manager を使用してイベント通知の送信先情報を変更できます。

手順

1. [**Cluster] > [Settings**] の順にクリックします。
2. [*Notifications Management] セクションで、をクリックします ⋮をクリックし、 * イベントの送信先の表示 * をクリックします。
3. [**Notifications Management]** ページで、 **[*Events Destinations**] タブを選択します。
4. イベントの送信先の名前の横にあるをクリックします ⋮をクリックし、 * 編集 * をクリックします。
5. イベントの送信先情報を変更し、 * 保存 * をクリックします。

EMS イベント通知フィルタを編集します

ONTAP 9.10.1 以降の System Manager を使用して、カスタマイズしたフィルタを変更して、イベント通知の処理方法を変更できるようになりました。

> システム定義のフィルタは変更できません。

手順

1. [**Cluster] > [Settings**] の順にクリックします。
2. [**Notifications Management]** セクションで、をクリックします ⋮をクリックし、[イベントの送信先の表示]*をクリックします。
3. [* 通知管理 *] ページで、 [* イベント・フィルタ *] タブを選択します。
4. イベントフィルタの名前の横にあるをクリックします ⋮をクリックし、 * 編集 * をクリックします。
5. イベントフィルタの情報を変更し、 [保存（ Save ）] をクリックします。

EMS イベント通知の送信先を削除します

ONTAP 9.10.1 以降の場合、 System Manager を使用して EMS イベント通知の送信先を削除できます。

> SNMP 送信先は削除できません。

手順

1. [**Cluster] > [Settings**] の順にクリックします。
2. [**Notifications Management]** セクションで、をクリックします ⋮をクリックし、[イベントの送信先の表示]*をクリックします。
3. [* 通知管理 **]** ページで、 **[** イベントの送信先 *] タブを選択します。
4. イベントの送信先の名前の横にあるをクリックします ⋮をクリックし、*[削除]*をクリックします。

EMS イベント通知フィルタを削除します

ONTAP 9.10.1 以降の System Manager を使用して、カスタマイズしたフィルタを削除できるようになりました。

> システム定義のフィルタは削除できません。

手順

1. [**Cluster] > [Settings**] の順にクリックします。

2. **[Notifications Management]** セクションで、をクリックします ⋮をクリックし、[イベントの送信先の表示]*をクリックします。
3. [* 通知管理 *] ページで、 [* イベント・フィルタ *] タブを選択します。
4. イベントフィルタの名前の横にあるをクリックします ⋮をクリックし、 * 削除 * をクリックします。

CLI を使用して EMS イベント通知を設定します

EMSの設定ワークフロー

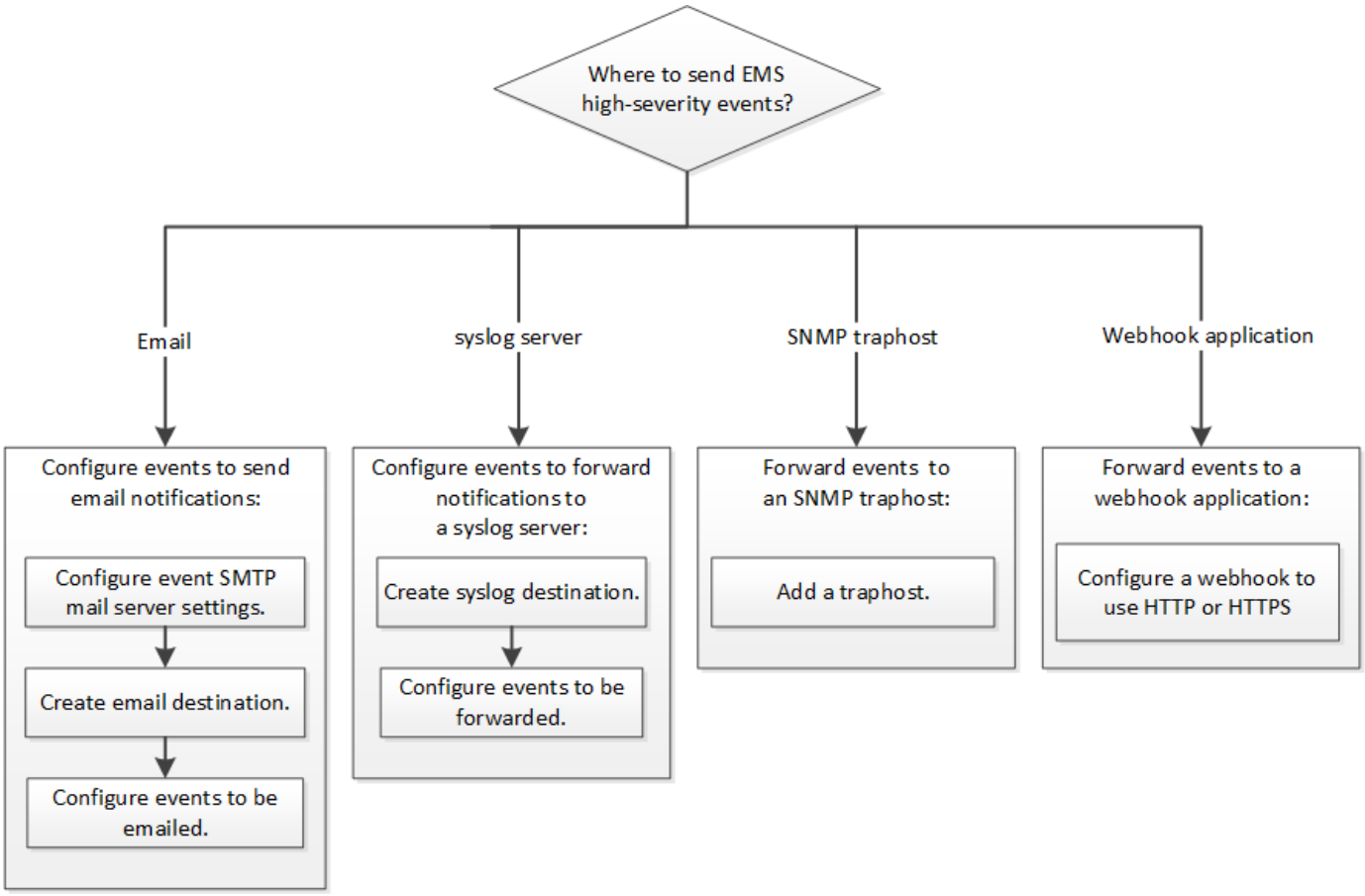
重要なEMSイベント通知は、Eメールで送信されるか、syslogサーバに転送されるか、SNMPトラップホストに転送されるか、またはWebフックアプリケーションに転送されるように設定する必要があります。これにより、適切な修正措置を講じてシステムの停止を回避できます。

このタスクについて

サーバやアプリケーションなどの他のシステムで記録されたイベントを集約するためにすでに syslog サーバを使用している場合は、ストレージシステムの重要なイベントの通知にもその syslog サーバを使用すると簡単です。

syslog サーバがまだない場合は、重要なイベントの通知に E メールを使用すると便利です。

イベント通知をすでに SNMP トラップホストに転送している場合は、そのトラップホストで重要なイベントについても監視できます。



選択肢

- イベント通知を送信するように EMS を設定します。

状況	参照先
EMS の重要なイベント通知を E メールアドレスに送信します	重要な EMS イベントの通知を E メールで送信するように設定します
EMS の重要なイベント通知を syslog サーバに転送します	重要な EMS イベントの通知を syslog サーバに転送するように設定します
EMS のイベント通知を SNMP トラップホストに転送する	SNMP トラップホストでイベント通知を受信するように設定します
EMSでイベント通知をwebhookアプリケーションに転送する場合	重要なEMSイベントについて、通知をWebフックアプリケーションに転送するように設定します

重要な **EMS** イベントの通知を **E** メールで送信するように設定します

重要なイベントの通知を E メールで受信するには、重要なアクティビティを示すイベントに関する E メールメッセージを送信するように EMS を設定する必要があります。

必要なもの

クラスタで E メールアドレスを解決するように DNS が設定されている必要があります。

このタスクについて

このタスクは、クラスタの実行中であれば、 ONTAP コマンドラインでコマンドを入力していつでも実行できます。

手順

1. イベント用の SMTP メールサーバを設定します。

   ```
   event config modify -mail-server mailhost.your_domain -mail-from
   cluster_admin@your_domain
   ```

2. イベントの通知に使用する E メール送信先を作成します。

   ```
   event notification destination create -name storage-admins -email
   your_email@your_domain
   ```

3. 重要なイベントの通知を E メールで送信するように設定します。

   ```
   event notification create -filter-name important-events -destinations storage-
   admins
   ```

重要な **EMS** イベントの通知を **syslog** サーバに転送するための設定

重大なイベントの通知を syslog サーバに記録するには、重要なアクティビティを示すイベントに関する通知を転送するように EMS を設定する必要があります。

必要なもの

クラスタで syslog サーバ名を解決するように DNS が設定されている必要があります。

このタスクについて

イベント通知用の syslog サーバがまだない場合は、先に syslog サーバを作成する必要があります。他のシステムのイベントを記録するためにすでに syslog サーバを使用している場合は、重要なイベントの通知にも同じ syslog サーバを使用できます。

このタスクは、クラスタの実行中であれば、ONTAP CLIでコマンドを入力していつでも実行できます。

ONTAP 9.12.1以降では、EMSイベントをTransport Layer Security（TLS）プロトコル経由でリモートsyslogサーバの指定ポートに送信できます。次の2つの新しいパラメータを使用できます。

`tcp-encrypted`

いつ `tcp-encrypted` にを指定します `syslog-transport`ONTAP は、デスティネーションホストの証明書を検証することで、そのホストの`ID`を検証します。デフォルト値はです `udp-unencrypted`。

`syslog-port`

デフォルト値 `syslog-port` パラメータは、の設定によって異なります `syslog-transport` パラメータ状況 `syslog-transport` がに設定されます `tcp-encrypted`、 `syslog-port` のデフォルト値は6514です。

詳細については、を参照してください `event notification destination create` のマニュアルページ。

手順

1. 重要なイベントの転送先の syslog サーバを作成します。

   `event notification destination create -name` *`syslog-ems`* `-syslog` *`syslog-server-address`* `-syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}`

   ONTAP 9.12.1以降では、に次の値を指定できます `syslog-transport`：

   - `udp-unencrypted` -セキュリティなしのユーザデータグラムプロトコル
   - `tcp-unencrypted` -セキュリティなしのTransmission Control Protocol
   - `tcp-encrypted` - Transport Layer Security（TLS）を使用したTransmission Control Protocol

   デフォルトのプロトコルはです `udp-unencrypted`。

2. 重要なイベントについて、 syslog サーバに通知を転送するように設定します。

   `event notification create -filter-name` *`important-events`* `-destinations` *`syslog-ems`*

SNMP トラップホストでイベント通知を受信するように設定します

SNMP トラップホストでイベント通知を受信するには、トラップホストを設定する必要があります。

必要なもの

- クラスタで SNMP トラップと SNMP トラップが有効になっている必要があります。

  SNMP トラップと SNMP トラップはデフォルトで有効になっています。

- クラスタでトラップホスト名を解決するように DNS が設定されている必要があります。

このタスクについて

イベント通知（ SNMP トラップ）を受信するように設定した SNMP トラップホストがまだない場合は、SNMP トラップホストを追加する必要があります。

このタスクは、クラスタの実行中であれば、 ONTAP コマンドラインでコマンドを入力していつでも実行できます。

ステップ

1. イベント通知を受信するように設定された SNMP トラップホストがまだない場合は、次のいずれかを追加します。

   ```
   system snmp traphost add -peer-address snmp_traphost_name
   ```

   SNMP でデフォルトでサポートされるすべてのイベント通知が SNMP トラップホストに転送されます。

重要な**EMS**イベントについて、通知を**Web**フックアプリケーションに転送するように設定します

重要なイベント通知をwebhookアプリケーションに転送するようにONTAP を設定できます。必要な設定手順は、選択したセキュリティのレベルによって異なります。

EMSイベント転送を設定するための準備をします

イベント通知をWebフックアプリケーションに転送するようにONTAP を設定する前に、いくつかの概念と要件を考慮する必要があります。

Webhookアプリケーション

ONTAP イベント通知を受信できるWebフックアプリケーションが必要です。webhookは、実行するリモートアプリケーションまたはサーバの機能を拡張するユーザ定義のコールバックルーチンです。webhookは、宛先URLにHTTP要求を送信することによって、クライアント（この場合はONTAP ）によって呼び出されるか、アクティブになります。具体的には、ONTAP は、webhookアプリケーションをホストするサーバにHTTP POST要求を送信し、イベント通知の詳細をXML形式で送信します。

セキュリティオプション

Transport Layer Security（TLS）プロトコルの使用方法に応じて、いくつかのセキュリティオプションがあります。選択するオプションによって、必要なONTAP 設定が決まります。

TLSは、インターネットで広く使用されている暗号化プロトコルです。1つ以上の公開鍵証明書を使用して、プライバシー、データの整合性、および認証を実現します。証明書は、信頼された認証局によって発行されます。

HTTP

HTTPを使用してイベント通知を転送できます。この設定では、接続はセキュアではありません。ONTAP クライアントおよびWebフックアプリケーションのIDは検証されません。さらに、ネットワークトラフィックは暗号化も保護もされません。を参照してください "HTTPを使用するようにwebhookの宛先を設定します" をクリックして設定の詳細を確認します

HTTPS

セキュリティを強化するために、webhookルーチンをホストするサーバーに証明書をインストールできます。HTTPSプロトコルは、ONTAP によって、WebフックアプリケーションサーバのIDおよびネットワークトラフィックのプライバシーと整合性を確保するために、両当事者によって使用されます。を参照してください "HTTPSを使用するようにWebhookの宛先を設定する" をクリックして設定の詳細を確認します

HTTPSを相互認証で使用

Webブック要求を発行するONTAP システムにクライアント証明書をインストールすると、HTTPSセキュリティをさらに強化できます。ONTAP がWebフックアプリケーションサーバのIDを検証し、ネットワークトラフィックを保護することに加えて、webhookアプリケーションはONTAP クライアントのIDを確認します。この双方向ピア認証は、_Mutual TLS_と呼ばれています。を参照してください "相互認証でHTTPSを使用するようにwebhookの宛先を設定します" をクリックして設定の詳細を確認します

関連情報

- "Transport Layer Security（TLS）プロトコルバージョン1.3"

HTTPを使用するように**webhook**の宛先を設定します

HTTPを使用してイベント通知をWebフックアプリケーションに転送するようにONTAP を設定できます。これは最も安全性の低いオプションですが、設定が最も簡単です。

手順

1. 新しい保存先を作成します `restapi-ems` イベントを受信するには：

   ```
   event notification destination create -name restapi-ems -rest-api-url
   http://<webhook-application>
   ```

   上記のコマンドでは、デスティネーションに* HTTP *スキームを使用する必要があります。

2. をリンクする通知を作成します `important-events` でフィルタリングします `restapi-ems` 目的地：

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

HTTPSを使用するように**Webhook**の宛先を設定する

HTTPSを使用してイベント通知をWebhookアプリケーションに転送するようにONTAP を設定できます。ONTAP は、サーバ証明書を使用して、WebフックアプリケーションのIDを確認し、ネットワークトラフィックを保護します。

作業を開始する前に

- webhookアプリケーションサーバの秘密鍵と証明書を生成します
- ルート証明書をONTAP にインストールできるようにします

手順

1. webhookアプリケーションをホストしているサーバに、適切なサーバ秘密鍵と証明書をインストールします。具体的な設定手順は、サーバによって異なります。
2. サーバのルート証明書をONTAP にインストールします。

   ```
   security certificate install -type server-ca
   ```

   このコマンドでは証明書を要求します。

3. を作成します `restapi-ems` イベントの受信先：

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application>
   ```

   上記のコマンドでは、デスティネーションに* HTTPS *スキームを使用する必要があります。

4. をリンクする通知を作成します `important-events` 新しいでフィルタリングします `restapi-ems` 目的地：

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

相互認証で**HTTPS**を使用するように**webhook**の宛先を設定します

相互認証を使用したHTTPSを使用してイベント通知をWebhookアプリケーションに転送するようにONTAP を設定できます。この構成では、2つの証明書があります。ONTAP は、サーバ証明書を使用して、Webフックアプリケーションの IDを確認し、ネットワークトラフィックを保護します。また、webhookをホストするアプリケーションは、クライアント証明書を使用してONTAP クライアントのIDを確認します。

作業を開始する前に

ONTAP を設定する前に、次の作業を実行する必要があります。

- webhookアプリケーションサーバの秘密鍵と証明書を生成します
- ルート証明書をONTAP にインストールできるようにします
- ONTAP クライアントの秘密鍵と証明書を生成します

手順

1. タスクの最初の2つの手順を実行します "HTTPSを使用するようにWebhookの宛先を設定する" ONTAP がサーバの識別情報を確認できるようにサーバ証明書をインストールする。
2. 適切なルート証明書と中間証明書をwebhookアプリケーションにインストールして、クライアント証明書を検証します。
3. ONTAP にクライアント証明書をインストールします。

   ```
   security certificate install -type client
   ```

秘密鍵と証明書を入力するよう求められます。

4. を作成します `restapi-ems` イベントの受信先：

```
event notification destination create -name restapi-ems -rest-api-url
https://<webhook-application> -certificate-authority <issuer of the client
certificate> -certificate-serial <serial of the client certificate>
```

上記のコマンドでは、デスティネーションに* HTTPS *スキームを使用する必要があります。

5. をリンクする通知を作成します `important-events` 新しいでフィルタリングします `restapi-ems` 目的地：

```
event notification create -filter-name important-events -destinations restapi-
ems
```

廃止された **EMS** イベントマッピングを更新します

EMS イベントのマッピングモデル

ONTAP 9.0 よりも前のバージョンでは、 EMS イベントはイベント名のパターンマッチングに基づいてイベントデスティネーションにのみマッピングできました。ONTAP コマンドセット (`event destination`、 `event route`）は、最新バージョンのONTAP でも引き続きこのモデルを使用できますが、ONTAP 9.0以降では廃止されています。

ONTAP 9.0以降ではONTAP 、拡張性に優れたイベントフィルタモデルを使用して、を使用して複数のフィールドに対してパターンマッチングを実行することを推奨します `event filter`、 `event notification`` および ``event notification destination` コマンドセット。

廃止されたコマンドを使用してEMSマッピングが設定されている場合は、を使用するようにマッピングを更新する必要があります `event filter`、 `event notification`` および ``event notification destination` コマンドセット。

イベントの送信先には、次の 2 種類があります。

1. * システムで生成される送信先 * ：システムで生成される 5 つのイベントの送信先があります（デフォルトで作成）。
   - `allevents`
   - `asup`
   - `criticals`
   - `pager`
   - `traphost`

     システムで生成される宛先の一部は、特別な目的に使用されます。たとえば、 ASUP デスティネーションは、 callhome.* イベントを ONTAP の AutoSupport モジュールにルーティングして AutoSupport メッセージを生成します。

2. ユーザが作成した送信先：を使用して手動で作成します `event destination create` コマンドを実行

します

```
cluster-1::event*> destination show
                                                                    Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
traphost         -                 -                  -
false
5 entries were displayed.
+
cluster-1::event*> destination create -name test -mail test@xyz.com
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
+
cluster-1::event*> destination show
+
Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

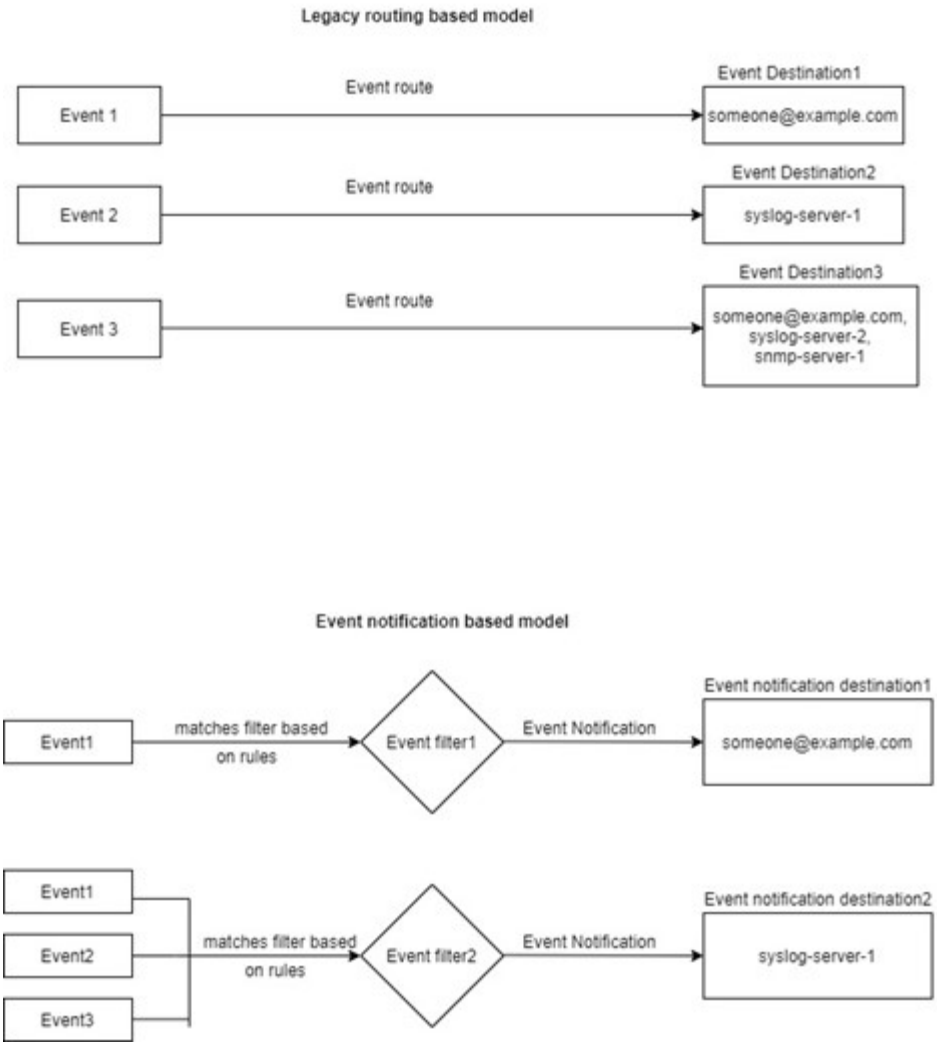
廃止されたモデルでは、EMSイベントはを使用して個別にデスティネーションにマッピングされます `event route add-destinations` コマンドを実行します

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
                                                                    Freq
Time
Message                           Severity       Destinations   Threshd
Threshd
--------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort          NOTICE         test           0       0
raid.aggr.autoGrow.success        NOTICE         test           0       0
raid.aggr.lock.conflict           INFORMATIONAL  test           0       0
raid.aggr.log.CP.count            DEBUG          test           0       0
4 entries were displayed.
```

拡張性に優れた新しい EMS イベント通知メカニズムは、イベントフィルタとイベント通知の送信先に基づいています。新しいイベント通知メカニズムの詳細については、次の技術情報アーティクルを参照してください。

- "ONTAP 9 のイベント管理システムの概要"



廃止された **ONTAP** コマンドから **EMS** イベントマッピングを更新します

廃止されたONTAP コマンドセットを使用してEMSイベントマッピングが設定されている場合 (`event destination`、 `event route`を使用するには、この手順 に従ってマッピングを更新する必要があります `event filter`、 `event notification`および `event notification destination` コマンドセット。

手順

1. を使用して、システム内のすべてのイベントの送信先を一覧表示します `event destination show` コマンドを実行します

```
cluster-1::event*> destination show

Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ---------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
test              test@xyz.com      -                  -
false
traphost          -                 -                  -
false
6 entries were displayed.
```

2. 各送信先について、を使用してマッピングされているイベントを一覧表示します `event route show -destinations <destination name>` コマンドを実行します

```
cluster-1::event*> route show -destinations test
                                                                    Freq
Time
Message                           Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort          NOTICE         test           0       0
raid.aggr.autoGrow.success        NOTICE         test           0       0
raid.aggr.lock.conflict           INFORMATIONAL  test           0       0
raid.aggr.log.CP.count            DEBUG          test           0       0
4 entries were displayed.
```

3. 対応するを作成します `event filter` これには、これらすべてのイベントのサブセットが含まれます。たとえば、のみを含める場合などです `raid.aggr.*`イベントの場合は、にワイルドカードを使用します `message-name` フィルタ作成時のパラメータ。単一のイベントに対するフィルタを作成することもできます。

> 最大 50 個のイベントフィルタを作成できます。

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
test_events
            1        include   raid.aggr.*            *               *
            2        exclude   *                      *               *
2 entries were displayed.
```

4. を作成します `event notification destination` をクリックします `event destination` エンドポイント（SMTP、SNMP、syslogなど）

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name            Type        Destination
--------------  ----------  ---------------------
dest1           email       test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost   snmp        - (from "system snmp traphost")
2 entries were displayed.
```

5. イベントフィルタをイベント通知の送信先にマッピングして、イベント通知を作成します。

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID   Filter Name                      Destinations
---- ------------------------------  -----------------
1    default-trap-events             snmp-traphost
2    asup_events                     dest1
2 entries were displayed.
```

6. それぞれについて、手順1 ~ 5を繰り返します `event destination` が搭載されています `event route`

マッピング：

> SNMPの送信先にルーティングされたイベントは、にマッピングする必要があります `snmp-traphost` イベント通知の送信先。SNMP トラップホストの送信先では、システムで設定された SNMP トラップホストを使用します。

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
        scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>    Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

                Destination Name: snmp-traphost
             Type of Destination: snmp
                     Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
       Client Certificate Valid?: -
```