System Managerを使用したクラスタパフォーマンスの監視

ONTAP 9

NetApp
December 20, 2024

目次

System Managerを使用したクラスタパフォーマンスの監視

System Managerを使用したクラスタパフォーマンスの監視

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について説明します。

タスクの内容

この手順は、FAS、AFF、および現在のASAシステムに適用されます。ASA R2システム（ASA A1K、ASA A70、またはASA A90）を使用している場合は、に従って"以下の手順を実行します"クラスタのパフォーマンスを監視します。ASA R2システムは、SANのみのお客様に特化したシンプルなONTAPエクスペリエンスを提供します。

System Managerのダッシュボードでシステムに関する情報を確認することで、クラスタの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、ストレージ階層とボリュームの効率性と容量、クラスタで使用可能なノード、HAペアを構成する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、クラスタやノードのパフォーマンス指標に関する情報が表示されます。

ダッシュボードでは、次の情報を確認できます。

- 健全性：クラスタの健全性
- 容量：クラスタで使用可能な容量を教えてください。
- 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れくらいですか？
- ネットワーク：ホストとストレージオブジェクト（ポート、インターフェイス、Storage VMなど）のネットワークはどのように設定されていますか？

健全性と容量の概要でをクリックすると、追加情報を表示したり、タスクを実行したりできます → 。

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

ネットワークの概要には、ネットワーク内の各オブジェクトの数が表示されます（例：「8 NVMe/FCポート」）。数字をクリックすると、各ネットワークオブジェクトの詳細が表示されます。

System Managerダッシュボードでクラスタの概要を表示する

System Managerダッシュボードを使用すると、ONTAPクラスタを1つの場所からすばやく包括的に把握できます。

System Managerダッシュボードを使用すると、重要なアラートと通知、ストレージ階層とボリュームの効率性と容量、クラスタで使用可能なノード、ハイアベイラビリティ（HA）ペアを構成する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、クラスタやノードのパフォーマンス指標に関する情報を一目で確認できます。

ダッシュボードは次の4つのパネルで構成されています。

健全性

[健全性]ビューには、クラスタ内の検出可能なすべてのノードの全体的な健常性に関する情報が表示されます。

[健全性]ビューには、クラスタレベルのエラーと警告（未設定のノードの詳細など）も表示され、クラスタのパフォーマンスを向上させるために変更できる特性が示されます。

をクリック → して[健全性]ビューを展開すると、クラスタの名前、バージョン、クラスタの作成日時など、クラスタの概要が表示されます。クラスタに関連付けられているノードの健常性に関連する統計を監視することもできます。タグを管理して、環境内のリソースをグループ化したり識別したりできます。[Insights]セクションでは、システムの容量、セキュリティコンプライアンス、構成を最適化できます。

容量

[容量]ビューには、クラスタのストレージスペースが表示されます。使用済み論理スペースの合計、使用済み物理スペースの合計、および使用可能なディスクスペースを確認できます。

Active IQに登録してクラスタの履歴データを表示することもできます。クリックし → て[容量]ビューを展開すると、クラスタに関連付けられている階層の概要が表示されます。各階層の容量情報（合計スペース、使用済みスペース、使用可能スペース）を確認できます。スループット、IOPS、およびレイテンシの詳細が表示されます。"容量の測定値の詳細については、System Managerを参照してください。"です。

[容量]ビューを使用して、ローカル階層とクラウド階層のどちらを追加するかを選択できます。[Capacity]ビューの詳細については、を参照して"クラスタの容量を表示する"ください。

ネットワーク

[ネットワーク]ビューには、ネットワークの一部である物理ポート、ネットワークインターフェイス、およびStorage VMが表示されます。

[ネットワーク]ビューには、ネットワークに接続されているクライアントのタイプが表示されます。ネットワークに接続された各クライアントは番号で表されます（「NVMe/FC 16」など）。番号を選択すると、これらの各ネットワーク要素の詳細が表示されます。

をクリックすると、ネットワークの全ページにわたる包括的なビューが表示されます。このビューには、 → ネットワーク上のポート、ネットワークインターフェイス、Storage VM、ホストが含まれます。

パフォーマンス

[パフォーマンス]ビューには、ONTAPクラスタの健常性と効率の監視に役立つパフォーマンス統計が表示されます。統計には、レイテンシ、スループット、IOPSなどの主要なクラスタパフォーマンス指標がグラフで表示されます。

[Performance]ビューには、日、時間、週、または年ごとに異なる時間間隔でパフォーマンス統計が表示されます。各種グラフを使用してクラスタのパフォーマンスを簡単に分析し、最適化が必要な特性を特定できます。このクイック分析は、ワークロードをどのように追加または移動するかを決定するのに役立ちます。使用量のピーク時間を確認して、潜在的な変化に備えて計画することもできます。

パフォーマンスビューには、レイテンシ、スループット、IOPSに関連するパフォーマンス指標の合計が表示されます。

9.15.1以降では、パフォーマンスビューが強化され、レイテンシ、スループット、IOPSに関連する読み取り、書き込み、その他、合計のパフォーマンス指標のグラフが表示されるようになりました。その他の指標には、読み取りまたは書き込み以外の処理が含まれます。

パフォーマンス値は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。クラスタのパフォーマンスに関する情報がない場合、グラフは表示されません。

クリックする と、時間、日、週、月、年ごとのパフォーマンス指標の全ページビューが表示されます。ローカルシステムのパフォーマンス指標のレポートをダウンロードすることもできます。

ホットボリュームやその他のオブジェクトの特定

アクセス頻度の高いボリューム（ホットボリューム）やデータ（ホットオブジェクト）を特定して、クラスタパフォーマンスを高速化できます。

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]*をクリックします。
2. IOPS、レイテンシ、およびスループットの列をフィルタして、アクセス頻度の高いボリュームやデータを表示します。

QoSの変更

ONTAP 9 8以降では、ストレージのプロビジョニング時にがサービス品質（QoS）デフォルトで有効になります。プロビジョニングプロセスでは、QoSを無効にしたり、カスタムのQoSポリシーを選択したりできます。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*[編集]*を選択します 。

リスクの監視

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（デジタルアドバイザ）によって報告されるリスクを監視できます。ONTAP 9 .10.1以降では、System Managerを使用してリスクを承認することもできます。

NetAppデジタルアドバイザは、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、Digital Advisorによって報告されるリスクを確認し、ストレージ管理、可用性の向上、セキュリティの強化、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。

Digital Advisorアカウントへのリンク

Digital Advisorからリスクに関する情報を受け取るには、最初にSystem ManagerからDigital Advisorアカウントにリンクする必要があります。

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. Digital Advisor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。

リスク数を表示する

ONTAP 9 .10.0以降では、Digital Advisorによって報告されたリスクの数をSystem Managerのダッシュボードで確認できます。

開始する前に

System ManagerからDigital Advisor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 Digital Advisor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 リスクの詳細を表示

リスクの詳細を表示

ONTAP 9 .10.0以降では、Digital Advisorから報告されるリスクが影響範囲別に分類される仕組みをSystem Managerで確認できます。また、報告された各リスク、システムへの潜在的な影響、および対処方法に関する詳細情報も表示できます。

開始する前に

System ManagerからDigital Advisor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 Digital Advisor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。リスクカテゴリには次のものがあります。
   - パフォーマンスと効率性
   - 可用性と保護
   - 容量

- 構成
- 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
   - 必要な緩和策のタイプ
   - 対処方法

リスクを承認

ONTAP 9 .10.1以降では、System Managerを使用して未解決のリスクを承認できます。

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。
2. 承認する未完了の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。
   - リマインダー（日付）
   - 位置合わせ
   - コメント
4. [* Acknowledge （確認）] をクリックし

> リスクを承認してから、Digital Advisor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。

リスクの承認を取り消し

ONTAP 9 .10.1以降では、以前に承認し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。
2. 承認を取り消す承認済み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。
   - 位置合わせ
   - コメント
4. [承認の取り消し *] をクリックします。

> リスクの承認を取り消してから、Digital Advisor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"

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	リスクの修正	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、次の分析情報がSystem Managerに表示されることがあります。

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

システムの構成に関する懸念事項に対して、次の分析情報がSystem Managerに表示されることがあります。

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、SP / BMCファームウェア、またはセキュリティファイルが利用可能なとき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

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。

タスクの内容

この手順は、FAS、AFF、および現在のASAシステムに適用されます。ASA R2システム（ASA A1K、ASA A70、またはASA A90）を使用している場合は、に従って"以下の手順を実行します"システムの最適化に役立つインサイトを確認してください。ASA R2システムは、SANのみのお客様に特化したシンプルなONTAPエクスペリエンスを提供します。

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に表示できます。

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、構成の最適化に役立つ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。.11.1以降では、System Managerを使用して、Storage VMのネイティブONTAP 9を有効にすることができます。Storage VMを推奨する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"。

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つのページに表示され、すぐにシステムを最適化するためのアクションを開始できます。各インサイトの詳細については、を参照してください"System Managerの分析情報"。

最適化に関するインサイトを表示

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ている場合があります。次のグループが表示されます。

   - Needs your attention
   - リスクの修正
   - 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次のボタンをクリックして、表示されるインサイトを絞り込みます。
   -  セキュリティ関連のインサイトを表示します。
   -  容量関連の分析情報が表示されます。
   -  構成関連のインサイトを表示します。
   -  すべてのインサイトが表示されます。

分析情報に対応してシステムを最適化

System Managerでは、分析情報を却下するか、問題のさまざまな解決方法を探るか、問題を修正するプロセスを開始することで、分析情報に対応できます。

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. インサイト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。インサイトを「却下解除」する方法については、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、修正方法が複数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。修正を適用するため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する

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. ページの右上隅にあるをクリックし、*[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する

該当する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. ページの右上隅にあるをクリックし、*エクスポート*を選択します。

ネイティブ**FPolicy**の設定

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。.11.1以降では、System Managerを使用して、Storage VMのネイティブONTAP 9を有効にすることができます。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. Storage VMごとに、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。

著作権に関する情報

商標に関する情報