管理と監視
ASA r2

NetApp
September 26, 2024

目次

管理と監視

ASA R2ストレージシステム上のStorage VMへのクライアントアクセスを管理します。

ASA R2システム上のストレージユニットは、Storage Virtual Machine（VM）内に格納されます。Storage VMは、SANクライアントにデータを提供するために使用されます。ONTAP System Managerを使用して、SANクライアントからStorage VMに接続してストレージユニットのデータにアクセスするためのLIF（ネットワークインターフェイス）を作成します。必要に応じて、サブネットを使用してLIFの作成を簡易化したり、IPspaceを使用してStorage VM専用のセキュアなストレージ、管理、ルーティングを実現したりできます。

IPspaceの作成

IPspaceは、Storage VMが配置される個別のIPアドレススペースです。IPspaceを作成すると、Storage VMに独自のセキュアなストレージ、管理、およびルーティングを設定できます。また、管理上分離されたネットワークドメイン内のクライアントで、同じIPアドレスサブネット範囲の重複するIPアドレスを使用できるようにします。

サブネットを作成する前にIPspaceを作成する必要があります。

手順

1. [ネットワーク]>[概要]*を選択します。
2. [IPspace]*で、を選択します + Add 。
3. IPspaceの名前を入力するか、デフォルトの名前をそのまま使用します。

   「all」はシステムで予約されている名前であるため、IPspace名を「all」にすることはできません。

4. [保存（ Save ）] を選択します。

次の手順

これでIPspaceが作成されました。これを使用してサブネットを作成できます。

サブネットの作成

サブネットを使用すると、LIF（ネットワークインターフェイス）の作成時に使用するIPv4またはIPv6アドレスの特定のブロックを割り当てることができます。サブネットを使用すると、LIFごとに特定のIPアドレスやネットワークマスクではなくサブネット名を指定できるため、LIFの作成が簡単になります。

開始する前に

- 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。
- "ブロードキャスト ドメイン"サブネットを追加するIPspaceとIPspaceがすでに存在している必要があります。

手順

1. [ネットワーク]>[概要]*を選択します。
2. [サブネット]*を選択し、を選択し + Add ます。
3. サブネット名を入力します。

   サブネット名はすべてIPspace内で一意である必要があります。

4. サブネットIPアドレスとサブネットマスクを入力します。
5. サブネットのIPアドレス範囲を指定します。

   サブネットのIPアドレス範囲を指定するときは、IPアドレスが他のサブネットと重複しないようにしてください。サブネットIPアドレスが重複し、異なるサブネットまたはホストが同じIPアドレスを使用しようとすると、ネットワークの問題が発生する可能性があります。

6. サブネットのブロードキャストドメインを選択してください。
7. 「 * 追加」を選択します。

次の手順

サブネットが作成されました。これを使用してLIFを簡単に作成できます。

LIFを作成する（ネットワークインターフェイス）

LIF（ネットワークインターフェイス）は、物理ポートまたは論理ポートに関連付けられたIPアドレスです。データへのアクセスに使用するポートにLIFを作成します。Storage VMは、1つ以上のLIFを介してクライアントにデータを提供します。コンポーネントに障害が発生しても、LIFは別の物理ポートにフェイルオーバーまたは移行できるため、ネットワーク通信が中断されません。

IPデータLIFを作成すると、デフォルトでiSCSIとNVMe/TCPの両方のトラフィックに対応できます。FCトラフィック用とNVMe/FCトラフィック用に、別 々 のデータLIFを作成する必要があります。

開始する前に

- 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。
- 基盤となる物理または論理ネットワークポートの管理 `up`ステータスがに設定されている必要があります。
- サブネット名を使用してLIFのIPアドレスとネットワークマスク値を割り当てる場合は、そのサブネットがすでに存在している必要があります。
- クラスタ内のノード間トラフィックを処理するLIFは、管理トラフィックを処理するLIFまたはデータトラフィックを処理するLIFと同じサブネット上には配置できません。

手順

1. [ネットワーク]>[概要]*を選択します。
2. [ネットワークインターフェイス]*を選択し、を選択し + Add ます。
3. インターフェイスタイプとプロトコルを選択し、Storage VMを選択します。
4. LIFの名前を入力するか、デフォルトの名前をそのまま使用します。
5. ネットワークインターフェイスのホームノードを選択し、IPアドレスとサブネットマスクを入力します。
6. [保存（ Save ）] を選択します。

結果

データアクセス用のLIFを作成しておきます。

LIFを変更する（ネットワークインターフェイス）

LIFは、必要に応じて無効にしたり名前を変更したりできます。LIFのIPアドレスとサブネットマスクを変更することもできます。

手順

1. [ネットワーク]>[概要]を選択し、[ネットワークインターフェイス]*を選択します。
2. 編集するネットワークインターフェイスにカーソルを合わせ、を選択します。
3. 「 * 編集 * 」を選択します。
4. ネットワークインターフェイスを無効にしたり、ネットワークインターフェイスの名前を変更したり、IPアドレスを変更したり、サブネットマスクを変更したりできます。
5. [保存（ Save ）] を選択します。

結果

LIFが変更されました。

ASA R2ストレージシステムのクラスタネットワークを管理します。

ONTAPシステムマネージャを使用して、ASA R2システムで基本的なストレージネットワーク管理を実行できます。たとえば、ブロードキャストドメインを追加したり、ポートを別のブロードキャストドメインに再割り当てしたりできます。

ブロードキャストドメインを追加する

ブロードキャストドメインを使用すると、同じレイヤ2ネットワークに属するネットワークポートをグループ化してクラスタネットワークの管理を簡易化できます。その後、Storage Virtual Machine（VM）は、グループ内のポートをデータトラフィックまたは管理トラフィックに使用できます。

「Default」ブロードキャストドメインと「Cluster」ブロードキャストドメインは、クラスタのセットアップ時に作成します。「Default」ブロードキャストドメインには、「Default」IPspace内のポートが含まれています。これらのポートは、主にデータの提供に使用されます。クラスタ管理ポートとノード管理ポートも、このブロードキャスト ドメインに含まれています。「Cluster」ブロードキャストドメインには、「Cluster」IPspace内のポートが含まれています。これらのポートはクラスタ通信に使用され、クラスタ内のすべてのノードのすべてのクラスタポートが含まれます。

クラスタが初期化されたら、追加のブロードキャストドメインを作成できます。ブロードキャストドメインを作成すると、同じポートを含むフェイルオーバーグループが自動的に作成されます。

タスクの内容

ブロードキャストドメインに追加されたポートのMaximum Transmission Unit（MTU；最大伝送ユニット）は、ブロードキャストドメインに設定されているMTU値に更新されます。

手順

1. System Managerで、*[ネットワーク]>[概要]*を選択します。
2. [ブロードキャスト]*[ドメイン]で、を選択します + Add 。
3. ブロードキャストドメインの名前を入力するか、デフォルトの名前をそのまま使用します。

   ブロードキャストドメイン名はすべてIPspace内で一意である必要があります。

4. ブロードキャストドメインのIPspaceを選択します。

   IPspace名を指定しない場合、ブロードキャストドメインは「Default」IPspaceに作成されます。

5. 最大伝送ユニット（MTU）を入力します。

   MTUは、ブロードキャストドメインで受け入れられる最大のデータパケットです。

6. 目的のポートを選択し、*[保存]*を選択します。

結果

新しいブロードキャストドメインを追加しておきます。

別のブロードキャストドメインへのポートの再割り当て

ポートが属することができるブロードキャストドメインは1つだけです。ポートが属するブロードキャストドメインを変更する場合は、ポートを既存のブロードキャストドメインから新しいブロードキャストドメインに再割り当てする必要があります。

手順

1. System Managerで、*[ネットワーク]>[概要]*を選択します。
2. で、⋮ドメイン名の横にあるを選択し、[編集]*を選択します。
3. 別のドメインに再割り当てするイーサネットポートの選択を解除します。
4. ポートを再割り当てするブロードキャストドメインを選択し、*[再割り当て]*を選択します。
5. [保存（ Save ）] を選択します。

結果

ポートを別のブロードキャストドメインに再割り当てしました。

VLANを作成します。

VLANは、ブロードキャストドメインにグループ化されたスイッチポートで構成されます。VLANを使用すると、IPネットワークインフラ内のセキュリティを強化し、問題を切り分け、使用可能なパスを制限できます。

開始する前に

ネットワークに配置されたスイッチは、IEEE 802.1Q規格に準拠しているか、ベンダー固有のVLANを実装している必要があります。

タスクの内容

- メンバーポートが含まれていないインターフェイスグループポートにVLANを作成することはできません。

- ポート上でVLANを初めて設定すると、ポートがダウンし、ネットワークが一時的に切断されることがあります。その後同じポートにVLANを追加しても、ポートの状態には影響しません。
- スイッチのネイティブVLANと同じ識別子のVLANをネットワークインターフェイス上に作成しないでください。たとえば、ネットワークインターフェイスe0bがネイティブVLAN 10上にある場合、そのインターフェイスにVLAN e0b-10を作成しないでください。

手順

1. System Managerで、*[ネットワーク]>[イーサネットポート]*を選択し、を選択します。+ VLAN
2. VLANのノードとブロードキャストドメインを選択します。
3. VLANのポートを選択します。

   クラスタLIFをホストしているポート、またはクラスタIPspaceに割り当てられているポートにVLANを接続することはできません。

4. VLAN IDを入力します。
5. [保存（ Save ）] を選択します。

結果

VLANを作成して、セキュリティを強化し、問題を切り分け、IPネットワークインフラストラクチャ内の使用可能なパスを制限します。

使用状況の監視と容量の拡張

ASA R2ストレージシステムでのクラスタとストレージユニットのパフォーマンスの監視

ONTAP System Managerを使用してクラスタの全体的なパフォーマンスと特定のストレージユニットのパフォーマンスを監視し、レイテンシ、IOPS、およびスループットが重要なビジネスアプリケーションにどのように影響しているかを判断します。パフォーマンスは、1時間から1年までのさまざまな期間にわたって監視できます。

たとえば、重要なアプリケーションで高レイテンシと低スループットが発生しているとします。過去5営業日のクラスタパフォーマンスを表示すると、同じ時間にパフォーマンスが低下していることがわかります。この情報を使用して、重要でないプロセスがバックグラウンドで実行され始めるときに、重要なアプリケーションがクラスタリソースを競合しているかどうかを判断します。その後、QoSポリシーを変更して、重要でないワークロードがシステムリソースに与える影響を制限し、重要なワークロードが最小スループットの目標を満たすようにすることができます。

クラスタのパフォーマンスの監視

クラスタのパフォーマンス指標を使用して、重要なアプリケーションのレイテンシを最小限に抑え、IOPSとスループットを最大化するためにワークロードを移行する必要があるかどうかを判断します。

手順

1. System Manager で、 * Dashboard * を選択します。
2. [パフォーマンス]*で、時間、日、週、月、または年単位で、クラスタのレイテンシ、IOPS、およびスループットを表示します。

3.  パフォーマンスデータをダウンロードする場合に選択します。

次の手順

クラスタのパフォーマンス指標を使用して、QoSポリシーの変更やアプリケーションワークロードのその他の調整が必要かどうかを分析し、クラスタ全体のパフォーマンスを最大化します。

ストレージユニットのパフォーマンスの監視

ストレージユニットのパフォーマンス指標を使用して、特定のアプリケーションがレイテンシ、IOPS、スループットに与える影響を判断します。

手順

1. System Managerで、*[ストレージ]*を選択します。
2. 監視するストレージユニットを選択し、*[概要]*を選択します。
3. [パフォーマンス]*で、時間、日、週、月、または年単位で、ストレージユニットのレイテンシ、IOPS、およびスループットを表示します。
4.  パフォーマンスデータをダウンロードする場合に選択します。

次の手順

レイテンシの低減とIOPSとスループットの最大化を実現するために、ストレージユニットに割り当てられたQoSポリシーを変更する必要があるかどうかを、ストレージユニットのパフォーマンス指標を使用して分析します。

ASA R2ストレージシステムでのクラスタおよびストレージユニットの使用率の監視

ONTAP System Managerを使用してストレージ利用率を監視し、現在および将来のワークロードに対応するために必要なストレージ容量を確保します。

クラスタ利用率の監視

クラスタで消費されるストレージの量を定期的に監視し、必要に応じてスペースが不足する前にクラスタの容量を拡張できるようにします。

手順

1. System Manager で、 * Dashboard * を選択します。
2. [容量]*で、クラスタ上の使用済み物理スペースと使用可能なスペースを確認します。

   データ削減率は、Storage Efficiencyによって削減されるスペースの量を表します。

次の手順

クラスタのスペースが不足している場合や、クラスタに将来の需要を満たすための容量がない場合は、"新しいドライブを追加"ASA R2システムでストレージ容量を増やすことを計画する必要があります。

ストレージユニットの使用状況の監視

ビジネスニーズに基づいてストレージユニットのサイズをプロアクティブに拡張できるように、ストレージユ

ニットが消費するストレージの量を監視します。

手順

1. System Managerで、*[ストレージ]*を選択します。
2. 監視するストレージユニットを選択し、*[概要]*を選択します。
3. [ストレージ]*で、次の情報を確認します。
   - ストレージユニットのサイズ
   - 使用済みスペースの量
   - データ削減率

     データ削減率は、Storage Efficiencyによって削減されたスペースを表します。

   - Snapshot使用済み

     [Snapshot Used]は、Snapshotで使用されているストレージの量を表します。

次の手順

ストレージユニットの容量が上限に近づいている場合は"ストレージユニットの変更"、サイズを大きくする必要があります。

ASA R2ストレージシステムのストレージ容量を増やす

ノードまたはシェルフにドライブを追加して、ASA R2システムのストレージ容量を増やします。

NetApp Hardware Universeを使用して新しいドライブの設置を準備する

ノードまたはシェルフに新しいドライブを取り付ける前に、NetApp Hardware Universeを使用して、追加するドライブがASA R2プラットフォームでサポートされていることを確認し、新しいドライブ用の正しいスロットを特定します。ドライブを追加するための適切なスロットは、プラットフォームのモデルとONTAPのバージョンによって異なります。場合によっては、特定のスロットに順番にドライブを追加する必要があります。

手順

1. に移動します"NetApp Hardware Universe"。
2. [製品]*で、ハードウェア構成を選択します。
3. ASA R2プラットフォームを選択します。
4. ONTAPのバージョンを選択し、*[結果を表示]*を選択します。
5. 図の下にある* Click here to see alternative views *を選択し、設定に一致するビューを選択します。
6. 構成のビューを使用して、新しいドライブがサポートされていること、および取り付け用の正しいスロットを確認します。

結果

新しいドライブがサポートされていること、および取り付けに適したスロットがわかっていることを確認しておきます。

ASA R2に新しいドライブを取り付ける

1回の手順で少なくとも6本のドライブを追加する必要があります。ドライブを1本追加するとパフォーマンスが低下する可能性があります。

タスクの内容

この手順の手順は、ドライブごとに繰り返す必要があります。

手順

1. 自分自身を適切にアースします。
2. プラットフォームの前面からベゼルをそっと取り外します。
3. 新しいドライブを正しいスロットに挿入します。
   a. カムハンドルが開いた状態で、両手で新しいドライブを挿入します。
   b. ドライブが止まるまで押します。
   c. ドライブがミッドプレーンに完全に収まり、カチッという音がして固定されるまで、カムハンドルを閉じます。

      カムハンドルは、ドライブの前面に揃うようにゆっくりと閉じてください。
4. ドライブのアクティビティLED（緑）が点灯していることを確認します。
   - LEDが点灯している場合は、ドライブに電力が供給されています。
   - LEDが点滅している場合は、ドライブに電力が供給されており、I/Oが実行中です。ドライブファームウェアの更新中もLEDが点滅します。

     新しいドライブのファームウェアが最新バージョンでない場合は、自動的に更新されます（システムは停止されません）。
5. ノードにドライブの自動割り当てが設定されている場合は、新しいドライブがONTAPによってノードに自動的に割り当てられるまで待つことができます。ノードでドライブの自動割り当てが設定されていない場合、または必要に応じて、ドライブを手動で割り当てることができます。

   ノードに割り当てるまで新しいドライブは認識されません。

次の手順

新しいドライブが認識されたら、ドライブが追加され、所有権が正しく指定されていることを確認します。

ASA R2ストレージシステムのファームウェアの更新

ONTAPは、デフォルトで、ASA R2システム上のファームウェアとシステムファイルを自動的にダウンロードして更新します。推奨される更新がダウンロードされてインストールされる前に、ONTAP System Managerを使用して自動更新を無効にしたり、更新パラメータを編集したりして、操作が実行される前に利用可能な更新に関する通知を表示したりできます。

自動更新を有効にする

ストレージファームウェア、SP / BMCファームウェア、およびシステムファイルの推奨アップデートは、デフォルトで自動的にダウンロードされ、ASA R2システムにインストールされます。自動更新が無効になっている場合は、自動更新を有効にしてデフォルトの動作に戻すことができます。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. の横にあるを選択し、[有効化]*を選択します。
3. EULAを読んで同意します。
4. デフォルトのままにして、ファームウェアとシステムファイルを自動的に更新します。必要に応じて、通知を表示するか、推奨される更新を自動的に却下するかを選択します。
5. 更新の変更が現在および将来のすべての更新に適用されることを承認する場合に選択します。
6. [保存（ Save ）] を選択します。

結果

推奨されるアップデートは、選択したアップデートに基づいて、ASA R2システムに自動的にダウンロードされ、インストールされます。

自動更新を無効にする

推奨されるアップデートをインストール前に表示できるようにするには、自動アップデートを無効にします。自動更新を無効にした場合は、ファームウェアとシステムファイルの更新を手動で実行する必要があります。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. の横にあるを選択し、[無効化]*を選択します。

結果

自動更新は無効になっています。推奨される更新プログラムを定期的に確認し、手動インストールを実行するかどうかを決定する必要があります。

自動更新の表示

クラスタにダウンロードされ、自動インストールがスケジュールされているファームウェアおよびシステムファイルの更新のリストを表示します。また、以前に自動的にインストールされたアップデートも表示します。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. の横にあるを選択し、[すべての自動更新を表示]*を選択します。

自動更新の編集

ストレージファームウェア、SP / BMCファームウェア、およびシステムファイルの推奨される更新をクラスタに自動的にダウンロードしてインストールするか、推奨される更新を自動的に却下するかを選択できます。更新プログラムのインストールまたは却下を手動で制御する場合は、推奨される更新プログラムが利用可能に

なったときに通知を受け取るを選択します。その後、手動でインストールまたは却下を選択できます。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. の横にあるを選択し、[自動更新の編集]*を選択します。
3. 自動更新の選択を更新します。
4. [保存（ Save ）] を選択します。

結果

選択内容に基づいて自動更新が変更されます。

ファームウェアの手動更新

推奨される更新プログラムをダウンロードしてインストールする前に表示できる柔軟性が必要な場合は、自動更新を無効にしてファームウェアを手動で更新できます。

手順

1. ファームウェアアップデートファイルをサーバーまたはローカルクライアントにダウンロードします。
2. System Managerで、**[クラスタ]>[概要]***を選択し、[更新]*を選択します。
3. [Firmware update]*を選択し、を選択し + Update firmware ます。

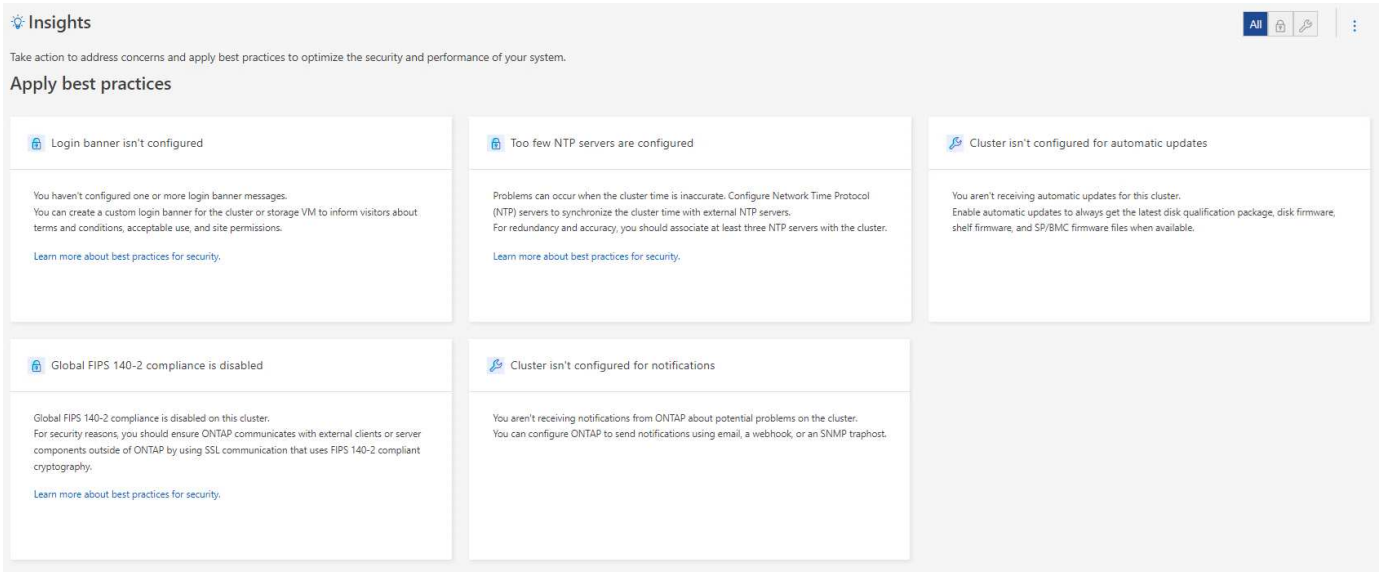
結果

ファームウェアが更新されました。

ASA R2ストレージシステムの分析情報でクラスタのセキュリティとパフォーマンスを最適化

ONTAP System Managerのview_insights_inを使用して、クラスタのセキュリティとパフォーマンスを最適化するためにASA R2システムに実装できるベストプラクティスと設定変更を特定します。

たとえば、クラスタ用にNetwork Time Protocol（NTP；ネットワークタイムプロトコル）サーバが設定されているとします。ただし、クラスタ時間管理を最適化するために必要なNTPサーバの数が推奨される数を下回っていることがわかりません。クラスタ時間が不正確な場合に発生する問題を回避するために、設定されているNTPサーバが少なすぎることが通知され、この問題の詳細を確認するか、修正するか、または却下するかを選択できます。



手順

1. System Managerで、*[Insights]*を選択します。
2. 推奨事項を確認

次のステップ

ベストプラクティスを実装し、クラスタのセキュリティとパフォーマンスを最適化するために必要な操作を実行します。

ASA R2ストレージシステムでのクラスタイベントとジョブの表示

ONTAPシステムマネージャを使用して、システムで発生したエラーやアラートのリストと推奨される対処方法を確認します。システム監査ログと、アクティブ、完了、または失敗したジョブのリストを表示することもできます。

手順

1. System Managerで、*[イベントとジョブ]*を選択します。
2. クラスタのイベントとジョブを表示します。

表示する項目	操作
クラスタイベント	を選択し、[イベントログ]*を選択します。
Active IQの推奨事項	「イベント」*を選択し、「Active IQ suggestions」*を選択します。
システムアラート	a. [システムアラート]*を選択します。 b. 対処するシステムアラートを選択します。 c. アラートを承認または抑制します。

表示する項目	操作
クラスタジョブ	[ジョブ]*を選択します。
監査ログ	[監査ログ]*を選択します。

クラスタイベントと監査ログに関するEメール通知を送信する

クラスタイベントまたは監査ログエントリが発生したときに特定のEメールアドレスに通知を送信するようにシステムを設定します。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. [通知管理]*の横にあるを選択します。
3. イベントの送信先を設定するには、**[**イベントの送信先の表示**]***を選択し、[イベントの送信先]を選択します。監査ログのデスティネーションを設定するには、[監査デスティネーションの表示]を選択し、[監査ログのデスティネーション]*を選択します。
4. を選択します + Add 。
5. 保存先の情報を入力し、*[追加]*を選択します。

結果

追加したEメールアドレスに、クラスタイベントと監査ログに関する指定したEメール通知が送信されるようになります。

ノードの管理

ASA R2ストレージシステムでノードをリブートする

メンテナンス、トラブルシューティング、ソフトウェアの更新、またはその他の管理上の理由で、ノードのリブートが必要になることがあります。ノードがリブートされると、HAパートナーが自動的にテイクオーバーを実行します。リブートされたノードがオンラインに戻ったあとに、パートナーノードで自動ギブバックが実行されます。

手順

1. System Managerで、*[クラスタ]>[概要]*を選択します。
2. リブートするノードの横にあるを選択し、*[リブート]*を選択します。
3. ノードをリブートする理由を入力して、*[リブート]*を選択します。

   リブートに入力した理由は、システム監査ログに記録されます。

次の手順

ノードのリブート中は、データサービスが中断されないように、ノードのHAパートナーによってテイクオーバーが実行されます。リブートが完了すると、HAパートナーがギブバックを実行します。

ASA R2ストレージシステムでノードの名前を変更する

ONTAPシステムマネージャを使用して、ASA R2システム上のノードの名前を変更できます。組織の命名規則やその他の管理上の理由で、ノードの名前を変更しなければならない場合があります。

手順

1. System Managerで、*[クラスタ]>[概要]*を選択します。
2. 名前を変更するノードの横にあるを選択し、*[名前の変更]*を選択します。
3. ノードの新しい名前を入力し、*[名前の変更]*を選択します。

結果

新しい名前がノードに適用されます。

ASA R2ストレージシステムでのユーザアカウントとロールの管理

System Managerを使用して、Active Directoryドメインコントローラアクセス、LDAPおよびSAML認証をユーザアカウントに設定します。ユーザアカウントロールを作成して、そのロールに割り当てられたユーザがクラスタで実行できる特定の機能を定義します。

Active Directoryドメインコントローラアクセスの設定

Active Directory（AD）ドメインコントローラからクラスタまたはStorage VMへのアクセスを設定し、ADアカウントからのアクセスを有効にできるようにします。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. セクションの[Active Directory]で、[設定]*を選択します。

次の手順

これで、ASA R2システムでADアカウントアクセスを有効にできます。

LDAPの設定

認証用のユーザ情報を一元的に管理するように、Lightweight Directory Access Protocol（LDAP）サーバを設定します。

開始する前に

証明書署名要求を生成し、CA署名済みサーバデジタル証明書を追加しておく必要があります。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. セクションで、[LDAP]*の横にあるを選択します。

3. 必要なLDAPサーバとバインド情報を入力し、*[保存]*を選択します。

次の手順

ユーザ情報と認証にLDAPを使用できるようになりました。

SAML認証の設定

Security Assertion Markup Language（SAML）認証を使用すると、Active DirectoryやLDAPなどの直接接続のサービスプロバイダではなく、セキュアなアイデンティティプロバイダ（IdP）でユーザを認証できます。

開始する前に

- リモート認証に使用するIdPを設定しておく必要があります。

  設定については、IdPのドキュメントを参照してください。

- IdPのURIが必要です。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. で、 SAML認証*の横にあるを選択します。
3. [SAML認証を有効にする]*を選択します。
4. IdPのURLとホストシステムのIPアドレスを入力し、*[保存]*を選択します。

   確認ウィンドウにメタデータ情報が表示され、クリップボードに自動的にコピーされます。

5. 指定したIdPシステムに移動し、クリップボードからメタデータをコピーしてシステムのメタデータを更新します。
6. System Managerの確認ウィンドウに戻り、*[ホストのURIまたはメタデータでIdPを設定しました]*を選択します。
7. SAMLベースの認証を有効にする場合は、*[ログアウト]*を選択します。

   IdPシステムに認証画面が表示されます。

次の手順

ユーザアカウントにSAML認証を使用できるようになりました。

ユーザアカウントロールの作成

クラスタ管理者とStorage VM管理者のロールは、クラスタの初期化時に自動的に作成されます。追加のユーザアカウントロールを作成して、そのロールに割り当てられたユーザがクラスタで実行できる特定の機能を定義します。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. セクションで、[ユーザとロール]*の横にあるを選択します。
3. [ロール]*で、を選択します + Add 。

4. ロール属性を選択します。

   複数の属性を追加するには、を選択します + Add 。

5. [保存（ Save ）] を選択します。

結果

新しいユーザアカウントが作成され、ASA R2システムで使用できるようになります。

管理者アカウントの作成

管理者ユーザアカウントを作成して、アカウントユーザがアカウントに割り当てられたロールに基づいてクラスタに対して特定の操作を実行できるようにします。アカウントのセキュリティを強化するには、アカウントの作成時に多要素認証（MFA）を設定します。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. セクションで、[ユーザとロール]*の横にあるを選択します →。
3. [ユーザ]*で、を選択します + Add 。
4. ユーザ名を入力し、ユーザに割り当てるロールを選択します。
5. ユーザのログイン方法と認証方法を選択します。
6. MFAを有効にするには、を選択し + Add 、セカンダリログイン方法と認証方法を選択します。
7. ユーザのパスワードを入力します。
8. [保存（ Save ）] を選択します。

結果

新しい管理者アカウントが作成され、ASA R2クラスタで使用できるようになります。

ASA R2ストレージシステムでセキュリティ証明書を管理します。

デジタルセキュリティ証明書を使用して、リモートサーバのIDを確認します。

Online Certificate Status Protocol （ OCSP ）は、 SSL 接続と Transport Layer Security （ TLS ）接続を使用して、 ONTAP サービスからのデジタル証明書要求のステータスを検証します。

証明書署名要求を生成する

証明書署名要求（CSR）を生成して、パブリック証明書の生成に使用できる秘密鍵を作成します。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. で、[証明書]*の横にあるを選択し →、を選択します + Generate CSR 。
3. サブジェクトの共通名を入力し、国名を選択します。

4. GSRのデフォルトを変更する場合は、拡張キー使用法を選択するか、サブジェクトの別名を追加します。More options次に、を選択し、必要な更新を行います。
5. [*Generate （生成）] を選択します

結果

パブリック証明書の生成に使用できるCSRを生成しておきます。

信頼された認証局を追加します。

ONTAPには、Transport Layer Security（TLS）を使用するアプリケーション用の信頼されたルート証明書のデフォルトセットが用意されています。必要に応じて、信頼された認証局を追加できます。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. で、[証明書]*の横にあるを選択します。
3. [信頼された認証局]*を選択します。
4. 証明書の詳細を入力またはインポートして、を選択しますAdd。

結果

新しい信頼された認証局をASA R2システムに追加しておきます。

信頼された認証局を更新または削除する

信頼された認証局は毎年更新する必要があります。期限切れの証明書を更新しない場合は、削除する必要があります。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. で、[証明書]*の横にあるを選択します。
3. [信頼された認証局]*を選択します。
4. 更新または削除する信頼できる認証局を選択します。
5. 認証局を更新または削除します。

認証局を更新する手順	認証局を削除する手順
a. を選択し、*[Renew]*を選択します。 b. 証明書情報を入力またはインポートし、*更新*を選択します。	a. を選択し、* Delete *を選択します。 b. 削除することを確認し、*[削除]*を選択します。

結果

ASA R2システム上の既存の信頼された認証局を更新または削除しておきます。

クライアント/サーバ証明書またはローカル認証局を追加する

セキュアなWebサービスを有効にするには、クライアント/サーバ証明書またはローカル認証局を追加します。

手順

1. System Managerで、* Cluster > Settings *の順に選択します。
2. で、[証明書]*の横にあるを選択します→。
3. または[ローカル認証局]*を選択します。
4. 証明書情報を追加して、を選択します + Add 。

結果

ASA R2システムに新しいクライアント/サーバ証明書または地方自治体を追加しておきます。

クライアント/サーバ証明書またはローカル認証局の更新または削除

クライアント/サーバ証明書とローカル認証局は、毎年更新する必要があります。期限切れの証明書やローカル認証局を更新しない場合は、削除する必要があります。

手順

1. [* Cluster]>[Settings]（設定）*を選択します。
2. [セキュリティ]*で、[証明書]の横にあるを選択します→。
3. または[ローカル認証局]*を選択します。
4. 更新または削除する証明書を選択します。
5. 認証局を更新または削除します。

認証局を更新する手順	認証局を削除する手順
a. を選択し⋮、*[Renew]*を選択します。 b. 証明書情報を入力またはインポートし、*更新*を選択します。	を選択し⋮、* Delete *を選択します。

結果

ASA R2システム上の既存のクライアント/サーバ証明書またはローカル認証局を更新または削除した。

ASA R2ストレージシステムのホスト接続の確認

ホストデータの処理に問題がある場合は、ONTAPシステムマネージャを使用して、ホストからASA R2ストレージシステムへの接続がアクティブであることを確認できます。

手順

1. System Managerで、*[ホスト]*を選択します。

   ホスト接続ステータスは、ホストグループの名前の横に次のように表示されます。

- **ok**:すべてのイニシエータが両方のノードに接続されていることを示します。
- 一部接続済み：一部のイニシエータが両方のノードに接続されていないことを示します。
- 接続なし：イニシエータが接続されていないことを示します。

次の手順

接続の問題を修正するために、ホストを更新します。ONTAPは15分ごとに接続ステータスを再確認します。