ASA r2のドキュメント

ASA r2

NetApp
September 26, 2024

目次

ASA r2のドキュメント

リリースノート

ASA R2システムのONTAP 9 .16.0の新機能

ASA R2システム向けのONTAP 9 .16.0の新機能について説明します。

プラットフォーム

更新	説明
新しいプラットフォーム	次の新しいNetApp ASA R2システムを使用できます。これらのプラットフォームは、ハードウェアとソフトウェアの統合ソリューションを提供し、SANのみのお客様のニーズに合わせてシンプルなエクスペリエンスを提供します。 • ASA A1K • ASA A70 • ASA A90

System Manager

更新	説明
"SANのみのお客様向けの合理的なサポート"	System Managerは合理化されており、SAN環境でサポートされていない機能が認識されなくなり、重要なSAN機能がサポートされるようになりました。

ストレージ管理

更新	説明
"シンプルなストレージ管理"	ASA R2システムでは、ストレージユニットとコンシステンシグループを使用してストレージ管理を簡易化します。 • ストレージユニット_を指定すると、SANホストでデータ処理に使用できるストレージスペースが確保されます。ストレージユニットとは、SCSIホストの場合はLUN、NVMeホストの場合はNVMeネームスペースを指します。 • コンシステンシグループ_は、1つのユニットとして管理されるストレージユニットの集まりです。

データセキュリティ

更新	説明
"オンボードキーマネージャとデュアルレイヤ暗号化"	ASA R2システムは、オンボードキーマネージャとデュアルレイヤ（ハードウェアとソフトウェア）暗号化をサポートしています。

開始する

ASA R2ストレージシステムの詳細

新しいNetApp ASA R2システム（ASA A1K、ASA A70、およびASA A90）は、ハードウェアとソフトウェアの統合ソリューションを提供し、SANのみのお客様のニーズに合わせてシンプルな操作性を実現します。

ASA R2システムは、単一のHAペア環境ですべてのSANプロトコル（iSCSI、FC、NVMe/FC、NVMe/TCP）をサポートします。SCSI（iSCSIおよびFC）プロトコルは、ホストとストレージの間のすべてのパスがアクティブ/最適化されるように、マルチパスに対称アクティブ/アクティブアーキテクチャを使用します。NVMeプロトコルでは、ホストとストレージ間の直接パスがサポートされます。

ASA R2システムでは、ONTAPソフトウェアとSystem Managerが合理化され、SAN環境でサポートされていない機能は削除されます。

ASA R2システムでは、ストレージユニットとコンシステンシグループを使用できます。

- ストレージユニット_を指定すると、SANホストでデータ処理に使用できるストレージスペースが確保されます。ストレージユニットとは、SCSIホストの場合はLUN、NVMeホストの場合はNVMeネームスペースを指します。
- コンシステンシグループ_は、1つのユニットとして管理されるストレージユニットの集まりです。

ASA R2システムは、ストレージユニットとコンシステンシグループを使用して、ストレージ管理とデータ保護を簡素化します。たとえば、10個のストレージユニットで構成されるデータベースが整合グループ内にあり、データベース全体をバックアップする必要があるとします。各ストレージユニットを個別にバックアップする代わりに、整合グループをバックアップすることでデータベース全体を保護できます。

盗難やランサムウェアなどの悪意のある攻撃からデータを保護するために、ASA R2システムはオンボードキーマネージャ、デュアルレイヤ暗号化、改ざん防止スナップショット、多要素認証、マルチ管理者検証をサポートしています。

ASA R2システムでは、現在のASA、AFF、またはFASシステムとのクラスタ混在はサポートされていません。

詳細情報

- ASA R2システムのサポートおよび制限の詳細については、を"NetApp Hardware Universe"参照してください。
- 詳細については、をご覧ください "新しいASA R2システムとASAシステムの比較"。
- の詳細については、を"NetApp ASA"参照してください。

ASA R2ストレージシステムのクイックスタート

ASA R2システムをセットアップして稼働させるには、ハードウェアコンポーネントを設置し、クラスタをセットアップし、ホストからストレージシステムへのデータアクセスをセットアップし、ストレージをプロビジョニングします。

1 ハードウェアの設置とセットアップ

"インストールとセットアップ"ASA R2システムを使用し、ONTAP環境にHAペアとして導入します。

2 クラスタのセットアップ

System Managerを使用すると、をすばやく簡単に実行"ONTAPクラスタをセットアップする"できます。

3 データアクセスのセットアップ

"ASA R2システムをSANクライアントに接続する"です。

4 ストレージのプロビジョニング

"ストレージのプロビジョニング"をクリックして、SANクライアントへのデータ提供を開始します。

次の手順

System Managerを使用して、でデータを保護できるようになりました"Snapshotの作成"。

ASA R2システムのインストール

ASA R2ストレージシステムのインストールとセットアップのワークフロー

ASA R2システムを設置して設定するには、ハードウェア要件を確認し、設置場所を準備し、ハードウェアコンポーネントを設置してケーブル接続し、システムの電源をオンにして、ONTAPクラスタをセットアップします。

1 **"ハードウェアの設置要件を確認する"**

ASA R2ストレージシステムを設置するためのハードウェア要件を確認します。

2 **"ASA R2ストレージシステムのインストールの準備"**

ASA R2システムを設置する準備をするには、設置場所の準備を整え、環境要件と電力要件を確認し、十分なラックスペースがあることを確認する必要があります。その後、機器を開梱して内容を納品書と比較し、ハードウェアを登録してサポートを利用できます。

3 **"ASA R2ストレージシステムのハードウェアの設置"**

ハードウェアを設置するには、ストレージシステムとシェルフ用のレールキットを設置し、ストレージシステムをキャビネットまたはTelcoラックに設置して固定します。次に、シェルフをレールにスライドさせます。最後に、ケーブル配線を整理するために、ケーブルマネジメントデバイスをストレージシステムの背面に取り付けます。

4 "ASA R2ストレージシステムのコントローラとストレージシェルフをケーブル接続"

ハードウェアをケーブル接続するには、まずストレージコントローラをネットワークに接続し、次にコントローラをストレージシェルフに接続します。

5 "ASA R2ストレージシステムの電源をオンにします。"

セットアップ時に各シェルフが一意に識別されるように、コントローラの電源をオンにする前に、各NS224シェルフの電源をオンにして一意のシェルフIDを割り当てます。

ASA R2ストレージシステムのインストール要件

ASA R2ストレージシステムとストレージシェルフに必要な機器と、持ち上げる際の注意事項を確認します。

設置に必要な機器

ASA R2ストレージシステムを設置するには、次の機器と工具が必要です。

- ストレージシステムを設定するためのWebブラウザへのアクセス
- 静電放電（ESD）ストラップ
- 懐中電灯
- USB /シリアル接続を備えたラップトップまたはコンソール
- NS224ストレージシェルフIDを設定するためのペーパークリップまたはボールペン
- No.2プラスドライバ

吊り上げ時の注意事項

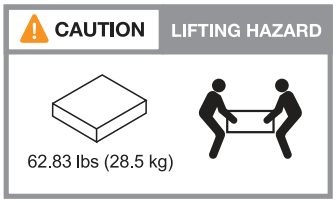
ASA R2ストレージシステムとNS224ストレージシェルフは重量があります。これらのアイテムを持ち上げたり移動したりするときは、注意してください。

ストレージシステムノオモミ

ASA R2ストレージシステムを移動または持ち上げるときは、必要な予防措置を講じてください。

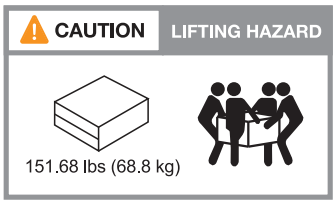
ASA A1K

ASA A1Kストレージシステムの重量は最大28.5 kg（62.83ポンド）です。システムを持ち上げるには、2人で作業するか、油圧リフトを使用します。



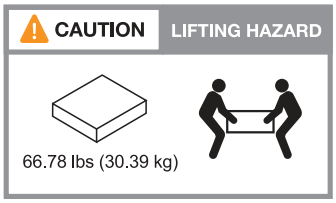
ASA A70および**ASA A90**

ASA A70ストレージ・システムまたはASA A90ストレージ・システムの重量は’最大68.8 kg（151.68ポンド）になることがありますシステムを持ち上げるには、4人で作業するか、油圧リフトを使用します。



収納シェルフの重量

NS224ストレージシェルフの重量は最大30.29kg（66.78ポンド）です。ストレージシェルフを持ち上げるには、2人で作業するか、油圧リフトを使用します。ストレージシェルフの重量がバランスを崩さないように、すべてのコンポーネント（前面と背面の両方）を保管してください。



関連情報

- "安全に関する情報と規制に関する通知"

次の手順

ハードウェア要件を確認したら、"ASA R2ストレージシステムの設置の準備"

ASA R2ストレージシステムのインストールの準備

ASA R2ストレージシステムを設置するための準備として、設置場所を準備し、開梱して内容を納品書と比較し、システムを登録してサポートを受けられるようにします。

ステップ1：サイトを準備する

ASA R2ストレージシステムを設置するには、設置場所および使用するキャビネットまたはラックが構成の仕様を満たしていることを確認してください。

手順

1. を使用して "NetApp Hardware Universe"、サイトがASA R2ストレージシステムの環境要件と電力要件を満たしていることを確認します。
2. 十分なラックスペースがあることを確認します。
   - 4U（ストレージシステムのHA構成）
   - NS224ストレージシェルフごとに2U
3. 必要なネットワークスイッチを取り付けます。

   インストール手順および互換性情報については、を参照してください "スイッチのドキュメント" "NetApp Hardware Universe" 。

手順2：箱を開封する

ASA R2ストレージシステムに使用するキャビネットやラックが必要な仕様を満たしていることを確認したら、すべての箱を開梱し、内容物を納品書の項目と比較します。

手順

1. すべての箱を慎重に開き、内容を整理された方法でレイアウトします。
2. 開梱した内容を、納品書のリストと比較します。

   梱包箱の側面にあるQRコードをスキャンすると、梱包リストを取得できます。

   次の項目は、ボックスに表示される内容の一部です。

   箱の中のすべてが納品書のリストと一致していることを確認してください。不一致がある場合は、それらをメモして、さらに対処してください。

* ハードウェア *	ケーブル	
• ベゼル • ケーブル マネジメント デバイス • ストレージシステム • 取扱説明書付きのレールキット（オプション） • ストレージシェルフ	• 管理イーサネットケーブル（RJ-45ケーブル） • ネットワークケーブル • 電源コード • ストレージケーブル（追加のストレージを注文した場合） • USB-Cシリアルポートケーブル	

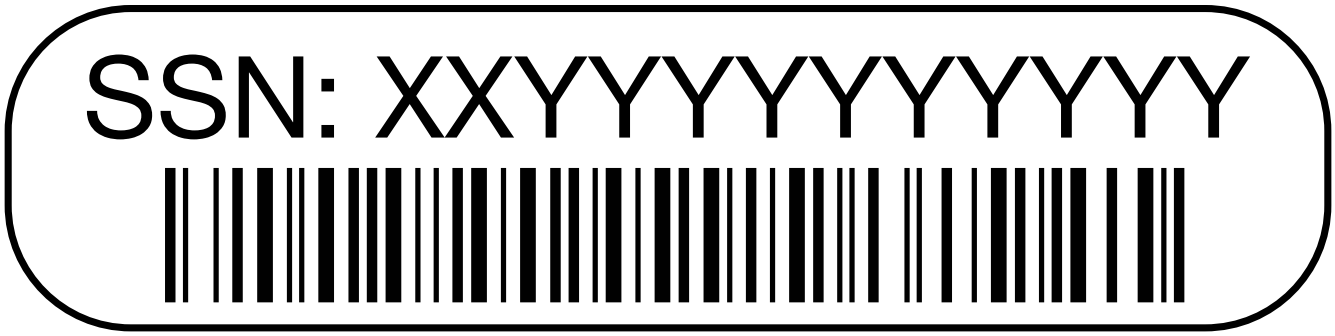
手順3：ストレージシステムを登録する

設置場所がASA R2ストレージシステムの仕様要件を満たしていることを確認し、注文したすべてのパーツが揃っていることを確認したら、システムを登録する必要があります。

手順

1. ストレージシステムのシリアル番号を確認します。

番号は、納品書、確認用Eメール、または開梱後にコントローラのシステム管理モジュールで確認できます。



2. に進みます "NetAppサポートサイト"。
3. ストレージシステムの登録が必要かどうかを判断します。

ユーザのタイプとアクセス方法	実行する手順
NetAppの既存のお客様	a. ユーザ名とパスワードを使用してサインインします。 b. [システム]>*[マイシステム]*を選択します。 c. 新しいシリアル番号が表示されていることを確認します。 d. そうでない場合は、NetAppの新規のお客様向けの手順に従います。
NetAppの新規のお客様	a. [今すぐ登録] をクリックしてアカウントを作成します。 b. Systems > Register Systems *を選択します。 c. ストレージシステムのシリアル番号と要求された詳細を入力します。 登録が承認されると、必要なソフトウェアをダウンロードできます。承認プロセスには最大 24 時間かかる場合があります。

次の手順

ASA R2ハードウェアの設置の準備が完了したら、次の作業"ASA R2ストレージシステムのハードウェアを設置します。"を行います。

ASA R2ストレージシステムのインストール

ASA R2ストレージシステムの設置準備が完了したら、システムのハードウェアを設置します。まず、レールキットを取り付けます。次に、ストレージシステムをキャビネットまたはTelcoラックに設置して固定します。

開始する前に

- レールキットに手順書が同梱されていることを確認します。
- ストレージシステムとストレージシェルフの重量に関連する安全上の問題に注意してください。

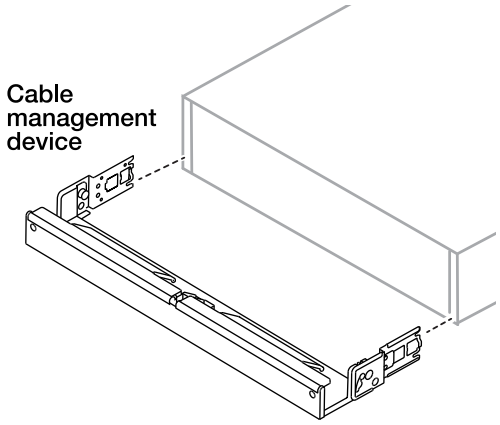
- ストレージ・システム内の通気は'ベゼルまたはエンド・キャップが取り付けられている前面から入り'ポートが取り付けられている背面から排出されます

手順

1. キットに付属の手順書に従って、ストレージシステムとストレージシェルフのレールキットを必要に応じて設置します。
2. キャビネットまたはTelcoラックにストレージシステムを設置して固定します。
   a. キャビネットまたはTelcoラックの中央にあるレールにストレージシステムを配置し、ストレージシステムを下から支えて所定の位置にスライドさせます。
   b. 付属の取り付けネジを使用して、ストレージシステムをキャビネットまたはTelcoラックに固定します。
3. ストレージシェルフを設置します。
   a. ストレージシェルフの背面をレールに合わせ、シェルフを下から支えてキャビネットまたはTelcoラックに挿入します。

      複数のストレージシェルフを設置する場合は、最初のストレージシェルフをコントローラの真上に配置します。2台目のストレージシェルフをコントローラの真下に置きます。ストレージシェルフを追加する場合は、このパターンを繰り返します。

   b. 付属の取り付けネジを使用して、ストレージシェルフをキャビネットまたはTelcoラックに固定します。
4. ケーブルマネジメントデバイスをストレージシステムの背面に接続します。



5. ベゼルをストレージシステムの前面に取り付けます。

次の手順

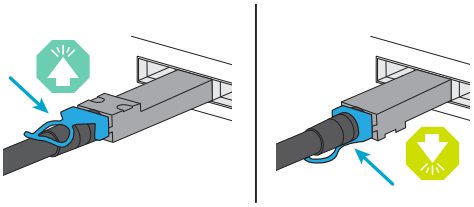
ASA R2システムのハードウェアの設置が完了したら、次の"ASA R2システムのコントローラとストレージシェルフをケーブル接続"手順を実行します。

ASA R2ストレージシステムのハードウェアのケーブル接続

ASA R2ストレージシステムのラックハードウェアを設置したら、コントローラにネットワークケーブルを接続し、コントローラとストレージシェルフの間をケーブルで接続します。

開始する前に

ケーブル配線図の図矢印を参照して、ケーブルコネクタのプルタブの向きが正しいかどうかを確認します。



- コネクタを挿入すると、カチッという音がして所定の位置に収まります。カチッという音がしない場合は、コネクタを取り外し、ケーブルヘッドを裏返してやり直してください。
- 光スイッチに接続する場合は、ポートにケーブル接続する前に、Small Form-factor Pluggable（SFP）トランシーバをコントローラポートに挿入します。

手順**1**：ストレージコントローラをネットワークに接続する

コントローラ同士、およびホストネットワークに直接接続します。

開始する前に

ストレージシステムをホストネットワークスイッチに接続する方法については、ネットワーク管理者にお問い合わせください。

タスクの内容

ここでは、一般的な設定について説明します。具体的なケーブル接続は、ご使用のストレージシステム用に注文したコンポーネントによって異なります。設定およびスロットプライオリティの詳細については、を参照してください "NetApp Hardware Universe"。

ASA A1K

ストレージコントローラを相互に接続してONTAPクラスタ接続を確立し、各コントローラのイーサネットポートをホストネットワークに接続します。

手順

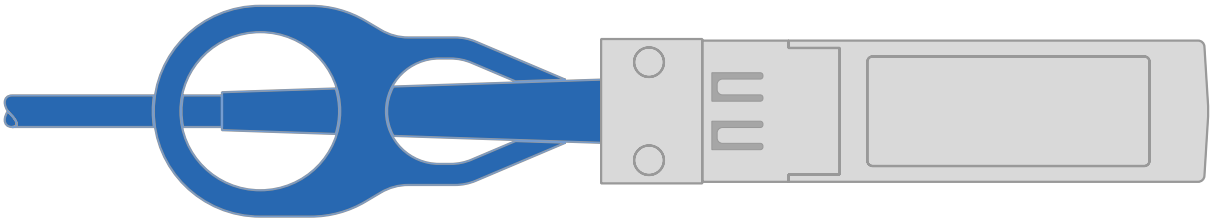
1. クラスタ/ HAインターコネクトケーブルを使用して、ポートe1aとe1a、ポートe7aとe7aを接続します。

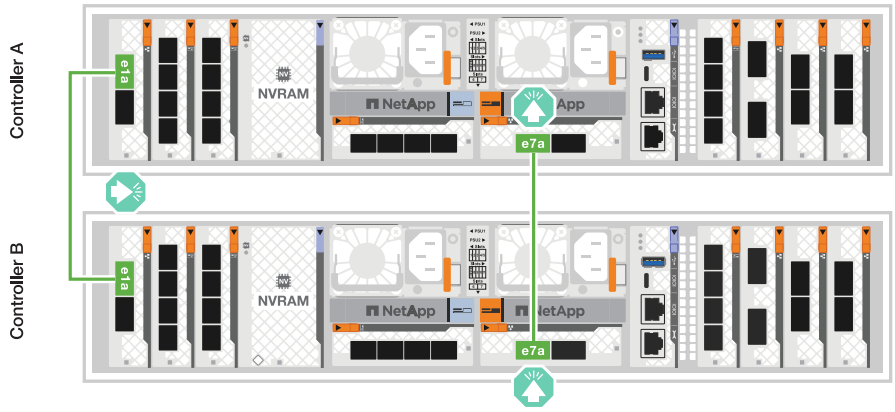
   クラスタインターコネクトトラフィックとHAトラフィックは、同じ物理ポートを共有します。

   a. コントローラAのポートe1aをコントローラBのポートe1aに接続します。

   b. コントローラAのポートe7aをコントローラBのポートe1aに接続します。

   クラスタ/ **HA**インターコネクトケーブル





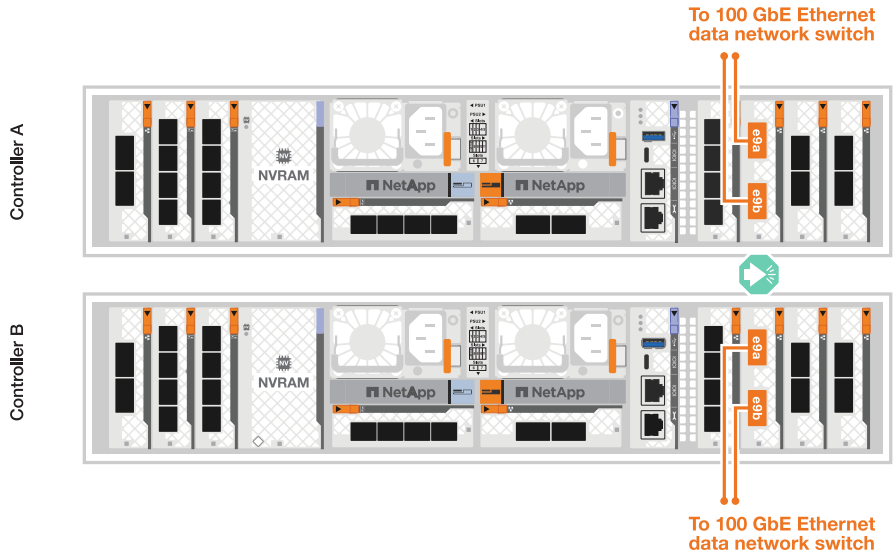
2. イーサネットモジュールポートをホストネットワークに接続します。

   次に、一般的なホストネットワークのケーブル接続例を示します。ご使用のシステム構成については、を参照してください "NetApp Hardware Universe" 。

   a. 図に示すように、ポートe9aとe9bをイーサネットデータネットワークスイッチに接続します。

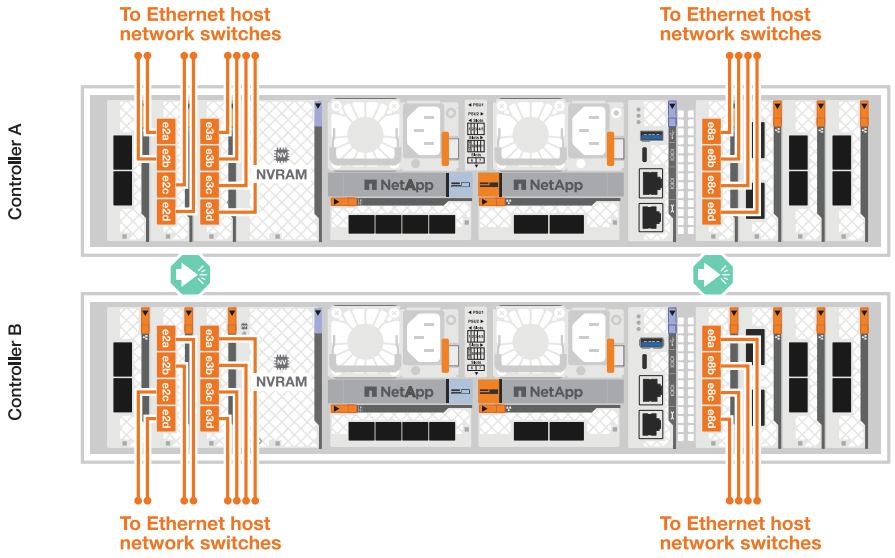
   クラスタトラフィックおよびHAトラフィックのシステムパフォーマンスを最大限に高めるために、ホストネットワーク接続にポートe1bおよびe7bを使用しないでください。パフォーマンスを最大化するには、別のホストカードを使用します。

   - 100GbEケーブル*



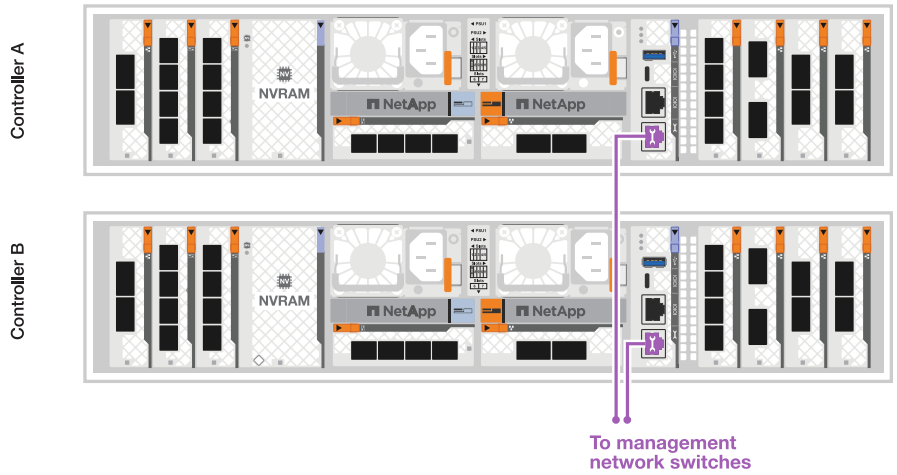
b. 10 / 25GbEホストネットワークスイッチを接続します。

- 10/25GbEホスト*



3. 1000BASE-T RJ-45ケーブルを使用して、コントローラ管理（レンチ）ポートを管理ネットワークスイッチに接続します。

◦ 1000BASE-T RJ-45ケーブル*



まだ電源コードを接続しないでください。

ASA A70および**ASA A90**

ストレージコントローラを相互に接続してONTAPクラスタ接続を確立し、各コントローラのイーサネットポートをホストネットワークに接続します。

手順

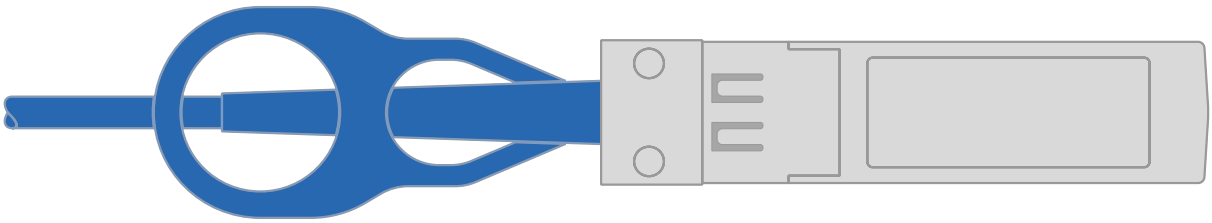
1. クラスタ/ HAインターコネクトケーブルを使用して、ポートe1aとe1aを接続し、ポートe7aとe7aを接続します。

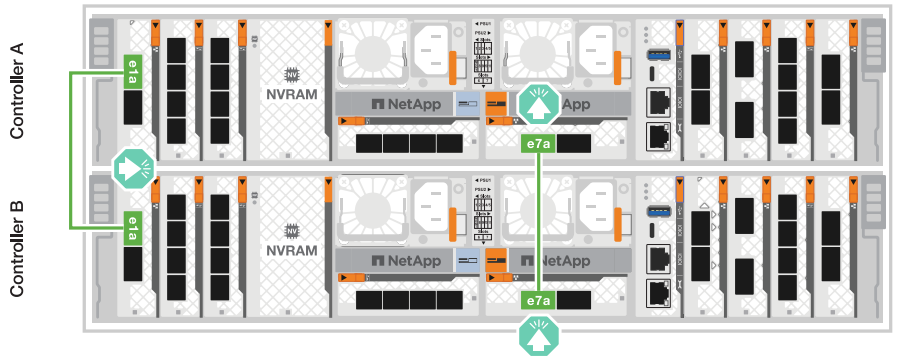
   クラスタインターコネクトトラフィックとHAトラフィックは、同じ物理ポートを共有します。

   a. コントローラAのポートe1aをコントローラBのポートe1aに接続します。

   b. コントローラAのポートe7aをコントローラBのポートe1aに接続します。

   クラスタ/ **HA**インターコネクトケーブル





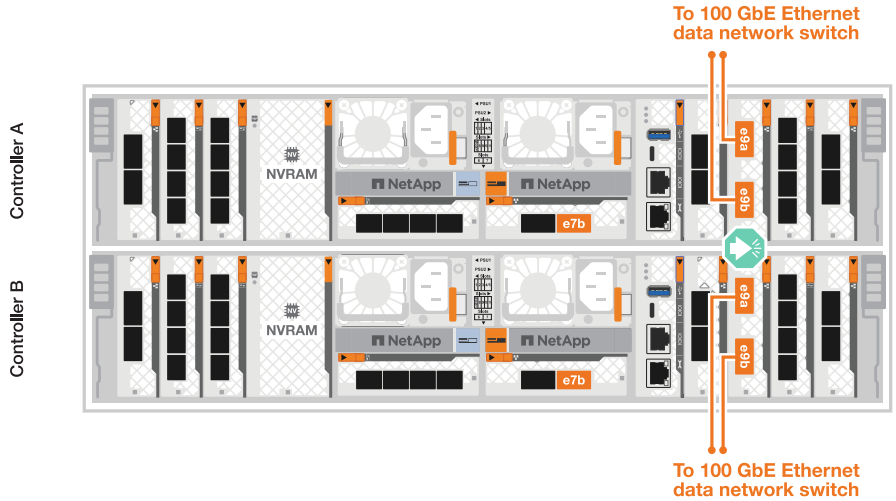
2. イーサネットモジュールポートをホストネットワークに接続します。

次に、一般的なホストネットワークのケーブル接続例を示します。ご使用のシステム構成については、を参照してください "NetApp Hardware Universe" 。

a. 図に示すように、ポートe9aとe9bをイーサネットデータネットワークスイッチに接続します。

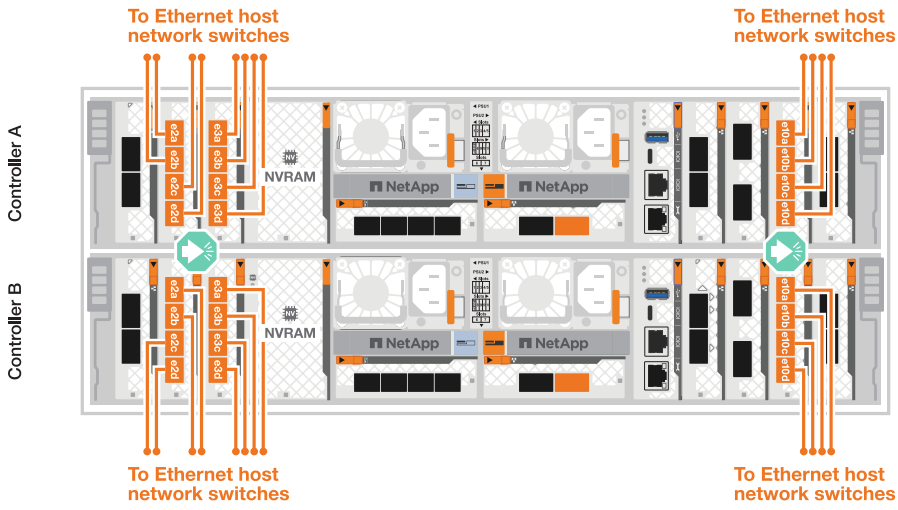
> クラスタトラフィックおよびHAトラフィックのシステムパフォーマンスを最大限に高めるために、ホストネットワーク接続にポートe1bおよびe7bを使用しないでください。パフォーマンスを最大化するには、別のホストカードを使用します。

- 100GbEケーブル*



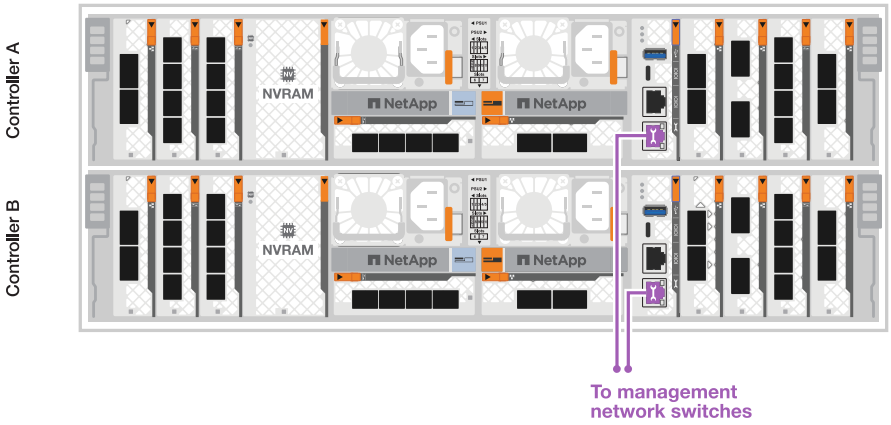
b. 10 / 25GbEホストネットワークスイッチを接続します。

- 4ポート、10/25GbEホスト*



3. 1000BASE-T RJ-45ケーブルを使用して、コントローラ管理（レンチ）ポートを管理ネットワークスイッチに接続します。

◦ 1000BASE-T RJ-45ケーブル*



まだ電源コードを接続しないでください。

手順**2**：ストレージコントローラをストレージシェルフに接続する

次のケーブル接続手順では、1台のシェルフと2台のシェルフにコントローラを接続する方法を示します。最大4台のシェルフをコントローラに直接接続できます。

ASA A1K

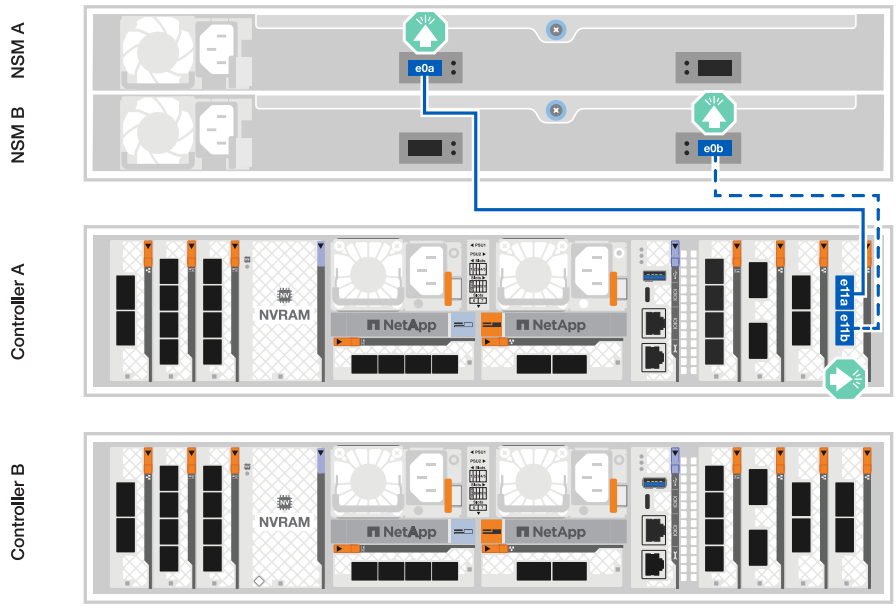
次のいずれかのケーブル接続オプションを、ご使用の環境に合わせて選択します。

オプション1：コントローラを1台のNS224ストレージシェルフに接続する

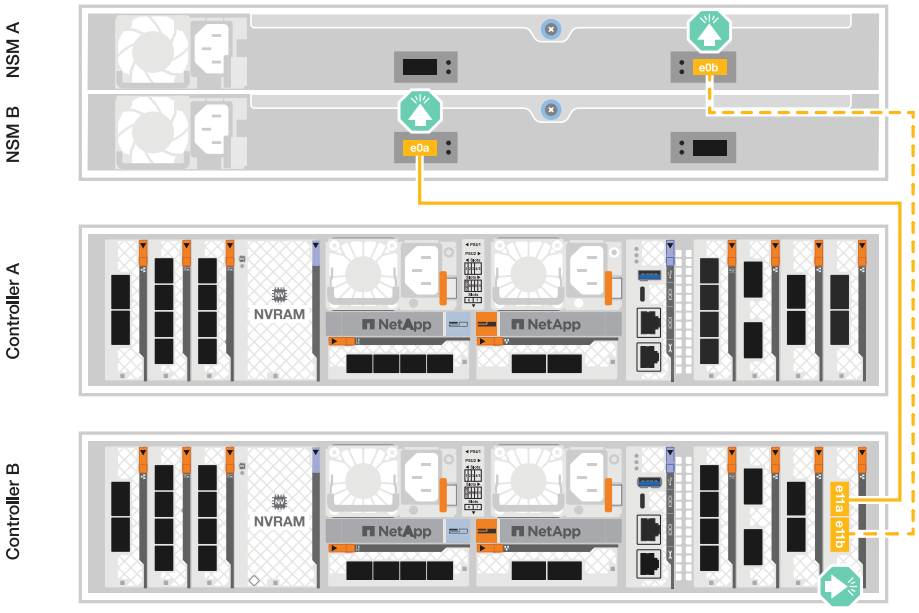
各コントローラをNS224シェルフのNSMモジュールに接続します。図は、各コントローラからのケーブル接続を示しています。コントローラAのケーブル接続は青、コントローラBのケーブル接続は黄色です。

手順

1. コントローラAで、次のポートを接続します。
   a. ポートe11aをNSM Aのポートe0aに接続します。
   b. ポートe11bをポートNSM Bのポートe0bに接続します。



2. コントローラBで、次のポートを接続します。
   a. ポートe11aをNSM Bのポートe0aに接続します。
   b. ポートe11bをNSM Aのポートe0bに接続します。

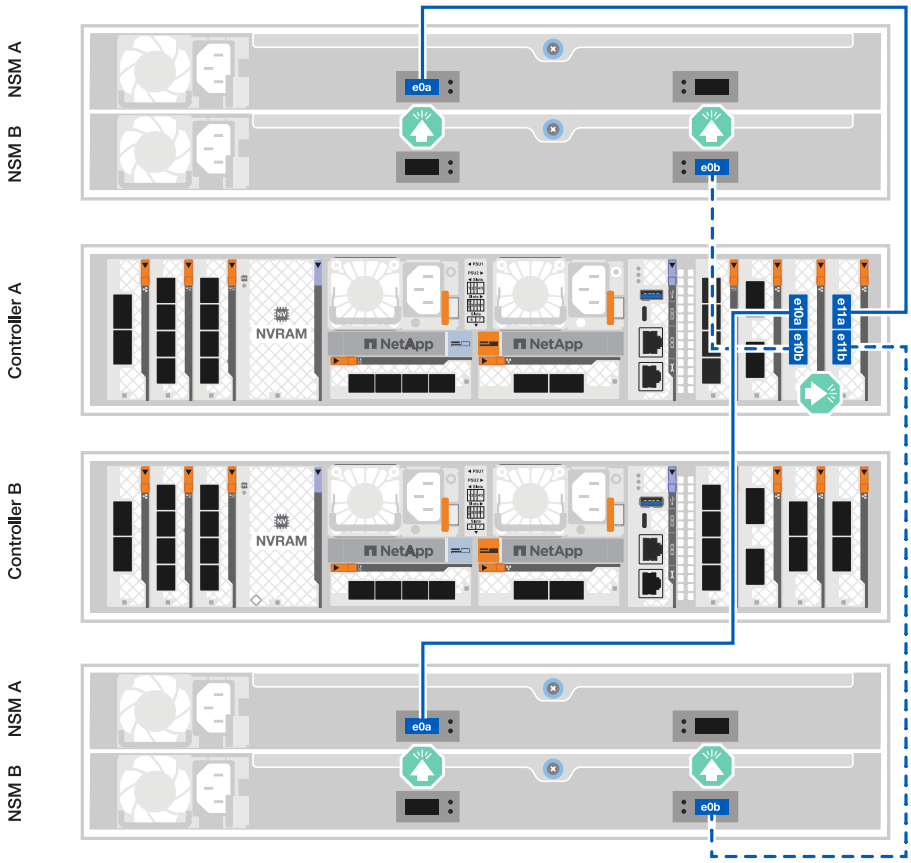

NSM A
NSM B
Controller A
Controller B
e0b
e0a
NVRAM
NetApp
NetApp
NVRAM
NetApp
NetApp
e1a
e1b

オプション2：コントローラを2台のNS224ストレージシェルフに接続する

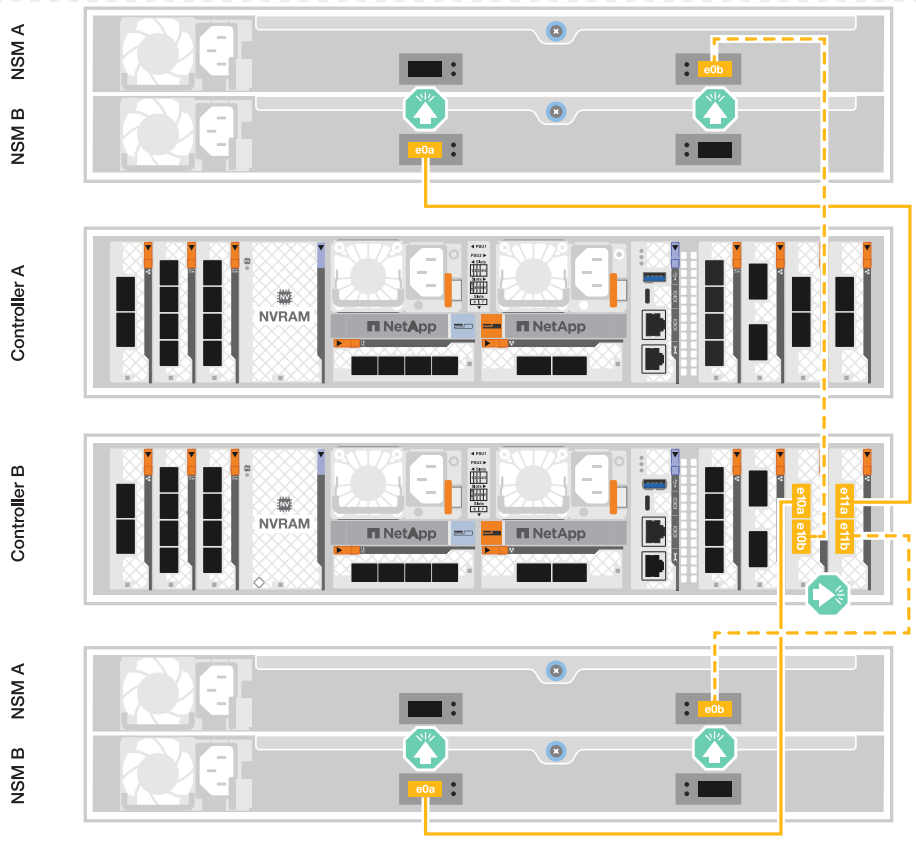
各コントローラを両方のNS224シェルフのNSMモジュールに接続します。図は、各コントローラからのケーブル接続を示しています。コントローラAのケーブル接続は青、コントローラBのケーブル接続は黄色です。

手順

1. コントローラAで、次のポートを接続します。
   a. ポートe11aをシェルフ1のNSM Aのポートe0aに接続します。
   b. ポートe11bをシェルフ2のNSM Bのポートe0bに接続します。
   c. ポートe10aをシェルフ2のNSM Aのポートe0aに接続します。
   d. ポートe10bをシェルフ1のNSM Aのポートe0bに接続します。



2. コントローラBで、次のポートを接続します。
   a. ポートe11aをシェルフ1のNSM Bのポートe0aに接続します。
   b. ポートe11bをシェルフ2のNSM Aのポートe0bに接続します。
   c. ポートe10aをシェルフ2のNSM Bのポートe0aに接続します。
   d. ポートe10bをシェルフ1のNSM Aのポートe0bに接続します。



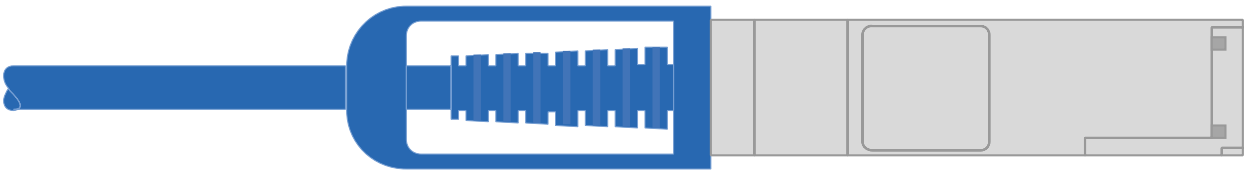
ASA A70および**ASA A90**

次のいずれかのケーブル接続オプションを、ご使用の環境に合わせて選択します。

オプション1：コントローラを1台のNS224ストレージシェルフに接続する

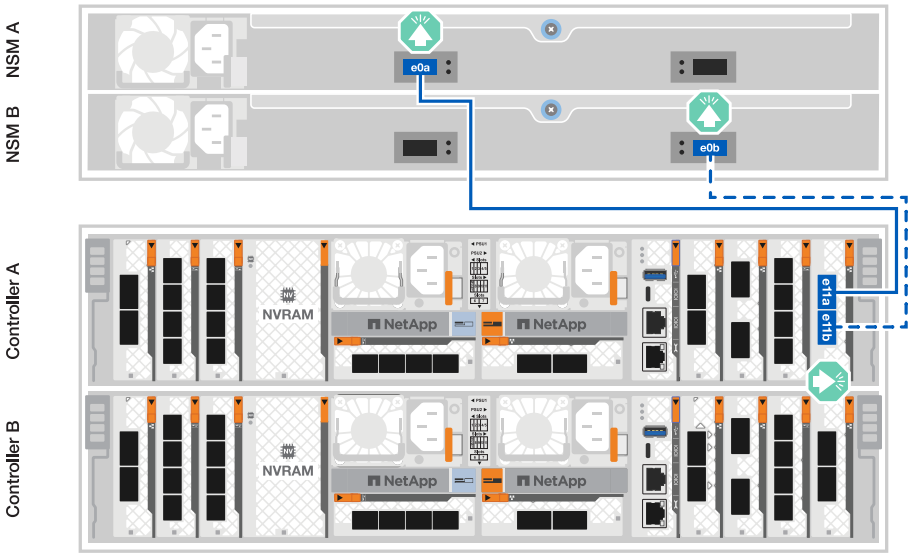
各コントローラをNS224シェルフのNSMモジュールに接続します。図は、各コントローラからのケーブル接続を示しています。コントローラAのケーブル接続は青、コントローラBのケーブル接続は黄色です。

- 100GbE QSFP28銅線ケーブル*

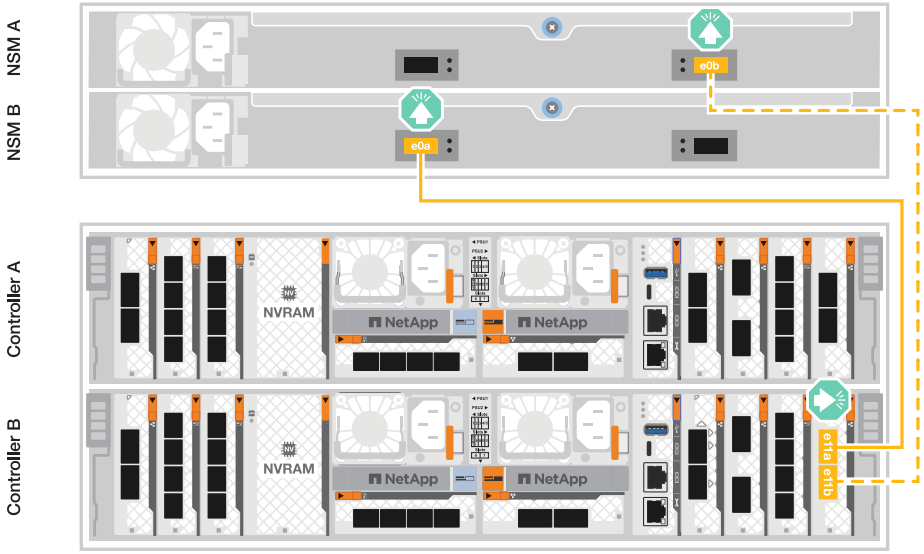


手順

1. コントローラAのポートe11aをNSM Aのポートe0aに接続します。
2. コントローラAのポートe11bをポートNSM Bのポートe0bに接続します。



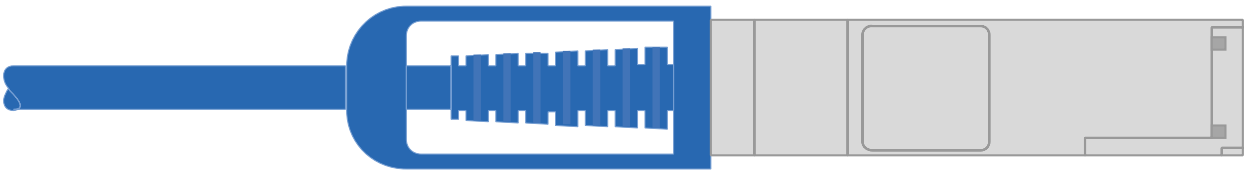
3. コントローラBのポートe11aをNSM Bのポートe0aに接続します。
4. コントローラBのポートe11bをNSM Aのポートe0bに接続します。


NSM A
NSM B
Controller A
Controller B
e0b
e0a
NVRAM
NetApp
NetApp
NVRAM
NetApp
NetApp
e11a
e11b

オプション**2**：コントローラを**2**台の**NS224**ストレージシェルフに接続する

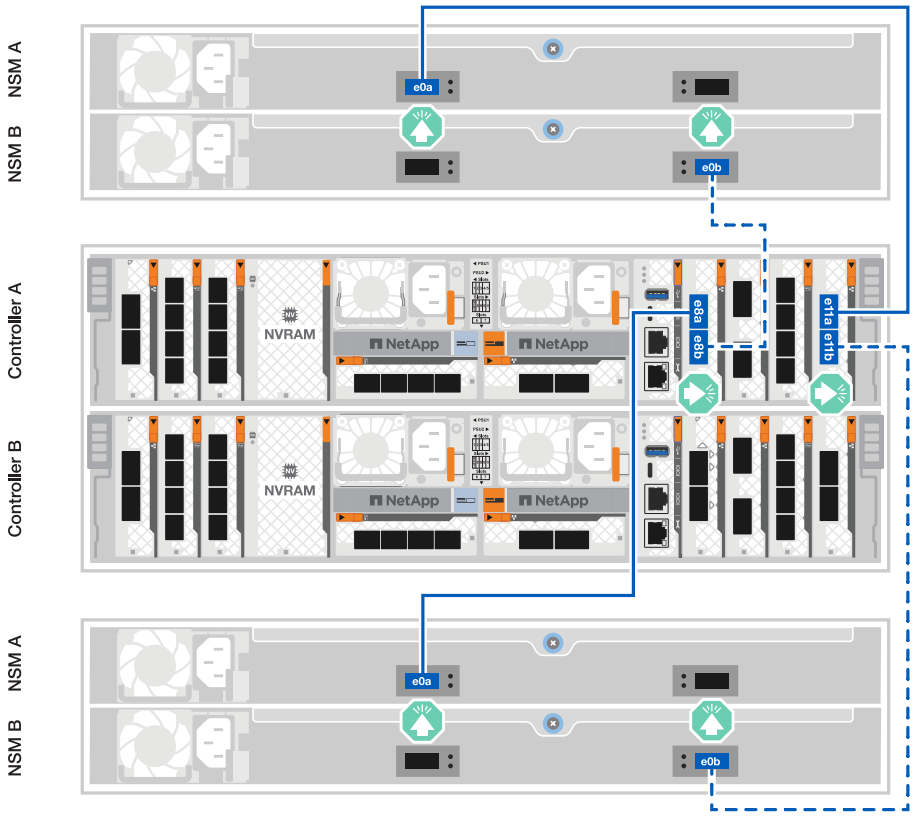
各コントローラを両方のNS224シェルフのNSMモジュールに接続します。図は、各コントローラからのケーブル接続を示しています。コントローラAのケーブル接続は青、コントローラBのケーブル接続は黄色です。

- 100GbE QSFP28銅線ケーブル*



手順

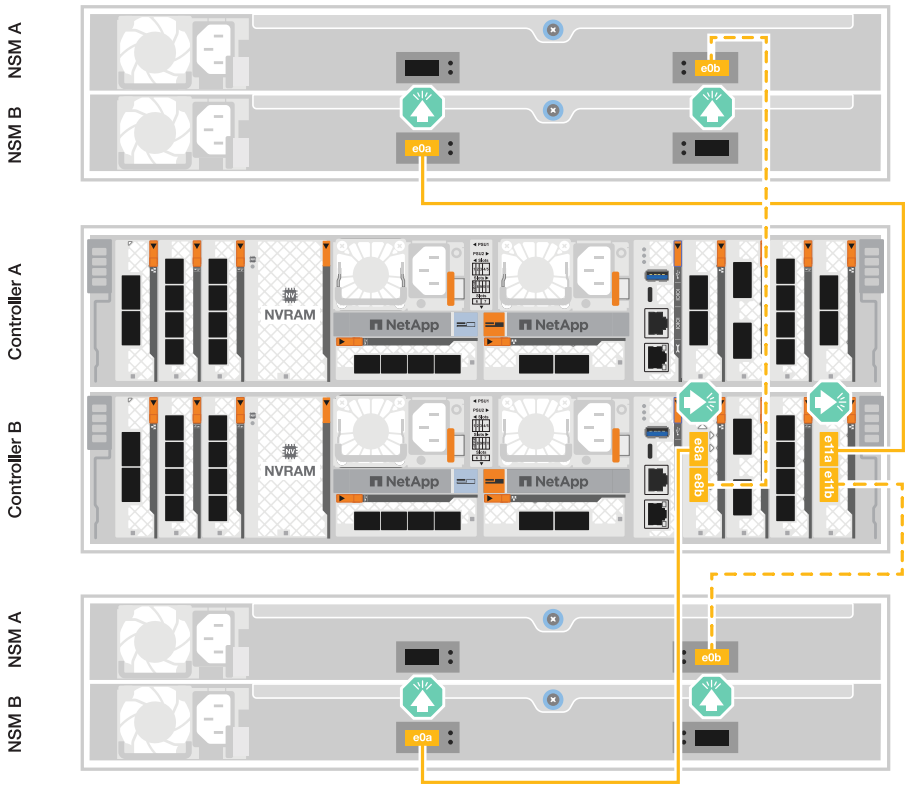
1. コントローラAで、次のポートを接続します。
   a. ポートe11aをシェルフ1、NSM Aのポートe0aに接続します。
   b. ポートe11bをシェルフ2、NSM Bのポートe0bに接続します。
   c. ポートe8aをシェルフ2、NSM Aのポートe0aに接続します。
   d. ポートe8bをシェルフ1、NSM Bのポートe0bに接続します。



2. コントローラBで、次のポートを接続します。
   a. ポートe11aをシェルフ1、NSM Bのポートe0aに接続します。
   b. ポートe11bをシェルフ2、NSM Aのポートe0bに接続します。

c. ポートe8aをシェルフ2、NSM Bのポートe0aに接続します。

d. ポートe8bをシェルフ1、NSM Aのポートe0bに接続します。



次の手順

ストレージコントローラをネットワークに接続し、コントローラをストレージシェルフに接続したら、次の作業を行い"ASA R2ストレージシステムの電源をオンにします。"ます。

ASA R2ストレージシステムの電源をオンにします。

ASA R2ストレージシステムのラックハードウェアを設置し、コントローラとストレージシェルフのケーブルを接続したら、ストレージシェルフとコントローラの電源をオンにする必要があります。

手順1：シェルフの電源をオンにしてシェルフIDを割り当てる

NS224の各シェルフは一意のシェルフIDで識別されます。このIDにより、ストレージシステムの設定内でシェルフが区別されます。デフォルトでは、シェルフIDには「00」と「01」が割り当てられますが、ストレージシステム全体で一意になるように、これらのIDの調整が必要になる場合があります。

タスクの内容

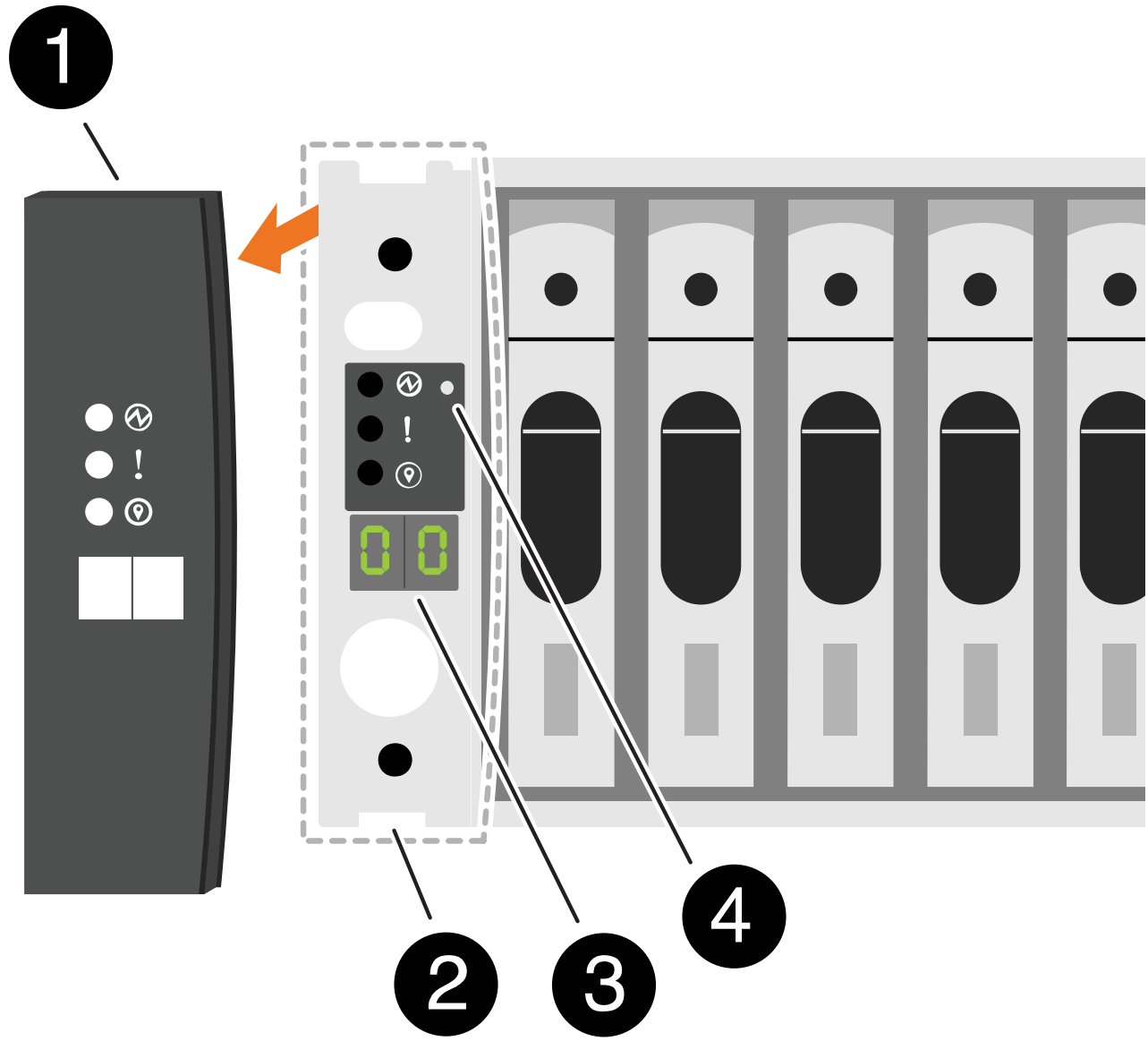
- 有効なシェルフIDは00~99です。
- シェルフIDを有効にするには、シェルフの電源を再投入する必要があります（両方の電源コードを取り外し、しばらく待ってから再度接続します）。

手順

1. シェルフの電源をオンにするには、まず電源コードをシェルフに接続し、電源コード固定クリップで所定の位置に固定してから、電源コードを別 々 の回路の電源に接続します。

   シェルフを電源に接続すると、シェルフの電源が自動的にオンになり、ブートします。

2. 前面プレートの後ろにあるシェルフIDボタンにアクセスするには、左側のエンドキャップを取り外します。



1	シェルフのエンドキャップ

	シェルフ前面プレート
	シェルフID番号
	シェルフIDボタン

3. シェルフIDの最初の番号を変更します。

   a. ペーパークリップまたは先端の細いボールペンのまっすぐになった端を小さな穴に差し込み、シェルフIDボタンを押します。

   b. デジタルディスプレイの1桁目の数字が点滅するまでシェルフIDボタンを押し続け、点滅したら放します。

      点滅するまでに最大15秒かかることがあります。これにより、シェルフIDのプログラミングモードがアクティブになります。

      IDの点滅に15秒以上かかる場合は、シェルフIDボタンをもう一度押し続け、最後まで押します。

   c. シェルフIDボタンを押して放し、目的の0~9の数字になるまで番号を進めます。

      プレスおよびリリースの所要時間は1秒程度です。

   1桁目の数字は点滅したままです。

4. シェルフIDの2番目の番号を変更します。

   a. デジタルディスプレイの2桁目の数字が点滅するまで、ボタンを押し続けます。

      点滅するまでに最大3秒かかることがあります。

   デジタルディスプレイの1桁目の数字の点滅が停止します。

a. シェルフIDボタンを押して放し、目的の0~9の数字になるまで番号を進めます。

   2桁目の数字は点滅し続けます。

5. 目的の番号をロックし、2桁目の番号の点滅が止まるまでシェルフIDボタンを押し続けてプログラミングモードを終了します。

   点滅が停止するまでに最大3秒かかることがあります。

   デジタルディスプレイの両方の数字が点滅し始め、約5秒後に黄色のLEDが点灯して、保留中のシェルフIDがまだ有効になっていないことを通知します。

6. シェルフIDを有効にするために、シェルフの電源を10秒以上再投入します。
   a. シェルフの両方の電源装置から電源コードを抜きます。
   b. 10 秒待ちます。
   c. 電源コードをシェルフの電源装置に再度接続して、電源を再投入します。

      電源コードを接続するとすぐに電源装置の電源がオンになります。電源装置の2色LEDが緑色に点灯します。

7. 左エンドキャップを取り付けます。

手順**2**：コントローラの電源をオンにする

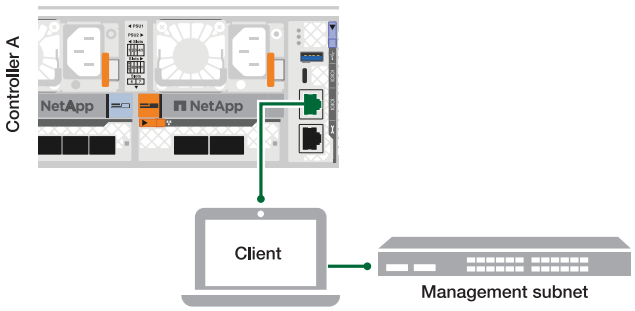
ストレージシェルフの電源をオンにして一意のIDを割り当てたら、ストレージコントローラの電源をオンにします。

手順

1. ラップトップをシリアルコンソールポートに接続します。これにより、コントローラの電源がオンになっているときのブートシーケンスを監視できます。
   a. ラップトップのシリアルコンソールポートを115、200ボー（N-8-1）に設定します。

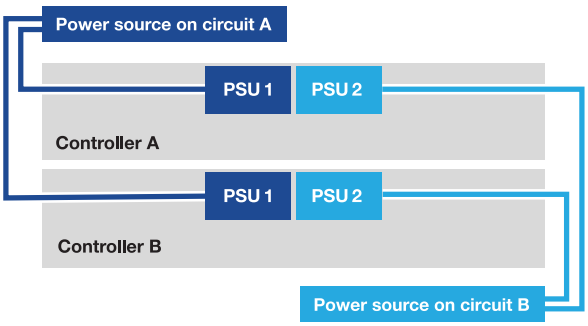
      シリアルコンソールポートの設定手順については、ラップトップのオンラインヘルプを参照してください。

   b. ストレージシステムに付属のコンソールケーブルを使用して、ラップトップにコンソールケーブルを接続し、コントローラのシリアルコンソールポートを接続します。
   c. ラップトップを管理サブネット上のスイッチに接続します。



d. 管理サブネット上のTCP/IPアドレスを使用して、ラップトップに割り当てます。

2. 電源コードをコントローラの電源装置に接続し、さらに別の回路の電源に接続します。



   - ストレージシステムがブートを開始します。初回のブートには最大 8 分かかる場合があります。
   - LEDが点滅し、ファンが起動します。これは、コントローラの電源がオンになっていることを示します。
   - ファンは最初に起動するときに非常にうるさい場合があります。起動時のファンの異音は正常。

3. 各電源装置の固定装置を使用して、電源ケーブルを固定します。

次の手順

ASA R2ストレージシステムの電源を入れたら、"ONTAP ASA R2クラスタのセットアップ"

ASA R2システムのセットアップ

ASA R2ストレージシステムでのONTAPクラスタのセットアップ

ONTAP System Managerの手順に従って、ONTAP ASA R2クラスタのセットアップワークフローをすばやく簡単に実行できます。

クラスタのセットアップ時に、デフォルトのデータStorage Virtual Machine（VM）が作成されます。必要に応じて、Domain Name System（DNS；ドメインネームシステム）を有効にしてホスト名を解決したり、Network Time Protocol（NTP；ネットワークタイムプロトコル）を使用して時刻を同期するようにクラスタを設定したり、保存データの暗号化を有効にしたりできます。

開始する前に

次の情報を収集します。

- クラスタ管理 IP アドレス

  クラスタ管理IPアドレスは、クラスタ管理インターフェイスの一意のIPv4アドレスです。クラスタ管理者は、管理Storage VMへのアクセスとクラスタの管理に使用します。このIPアドレスは、組織でIPアドレスを割り当てる管理者から取得できます。

- ネットワークサブネットマスク

  ONTAPでは、クラスタのセットアップ時に、ご使用の構成に適した一連のネットワークインターフェイスを推奨します。必要に応じて推奨構成を調整できます。

- ネットワークゲートウェイのIPアドレス

- パートナーノードのIPアドレス
- DNSドメイン名
- DNSネームサーバのIPアドレス
- NTPサーバのIPアドレス
- データサブネットマスク

手順

1. クラスタネットワークを検出
   a. ラップトップを管理スイッチに接続し、ネットワークコンピュータとデバイスにアクセスします。
   b. エクスプローラを開きます。
   c. を選択し、右クリックして[更新]*を選択します。
   d. いずれかのONTAPアイコンを選択し、画面に表示された証明書を受け入れます。

      System Manager が開きます。

2. [パスワード]*で、管理者アカウント用の強力なパスワードを作成します。

   パスワードは8文字以上で、アルファベットと数字をそれぞれ1文字以上含む必要があります。

3. 確認のためにパスワードを再入力し、*[続行]*を選択します。
4. [ネットワークアドレス]*で、ストレージシステム名を入力するか、デフォルトの名前をそのまま使用します。

   デフォルトのストレージシステム名を変更する場合は、新しい名前の1文字目はアルファベットで、44文字未満にする必要があります。名前にはピリオド（.）、ハイフン（-）、アンダースコア（_）を使用できます。

5. クラスタ管理IPアドレス、サブネットマスク、ゲートウェイIPアドレス、およびパートナーノードのIPアドレスを入力し、*[続行]*を選択します。
6. [ネットワークサービス]*で、*ホスト名の解決にドメインネームシステム（DNS）を使用する*と*時刻の同期を維持するためにネットワークタイムプロトコル（NTP）を使用する*のオプションを選択します。

   DNSを使用する場合は、DNSドメインとネームサーバを入力します。NTPを使用する場合は、NTPサーバを入力して*[続行]*を選択します。

7. [暗号化]*で、オンボードキーマネージャ（OKM）のパスフレーズを入力します。

   デフォルトでは、オンボードキーマネージャ（OKM）を使用した保存データの暗号化が選択されています。外部キー管理ツールを使用する場合は、選択内容を更新します。

   必要に応じて、クラスタのセットアップの完了後にクラスタで暗号化を設定できます。

8. [初期化]*を選択します。

   セットアップが完了すると、クラスタの管理IPアドレスにリダイレクトされます。

9. で、[プロトコルの設定]*を選択します。

IP（iSCSIおよびNVMe/TCP）を設定する手順	FCおよびNVMe/FCを設定する手順
a. を選択し、[IPインターフェイスの設定]*を選択します。 b. [サブネットの追加]*を選択します。 c. サブネットの名前を入力してから、サブネットのIPアドレスを入力します。 d. サブネットマスクを入力し、必要に応じてゲートウェイを入力して、*[追加]*を選択します。 e. 作成したサブネットを選択し、*[保存]*を選択します。 f. [保存（ Save ）] を選択します。	a. を選択し、[FCインターフェイスの設定]および/または[NVMe/FCインターフェイスの設定]*を選択します。 b. FCポート/ NVMe/FCポートを選択し、*[保存]*を選択します。

10. 必要に応じて、をダウンロードしてを実行し、"ActiveIQ Config Advisor"設定を確認します。

    ActiveIQ Config Advisorは、一般的な構成エラーをチェックするNetAppシステム向けのツールです。

次の手順

これで、"データアクセスのセットアップ"SANクライアントからASA R2システムに移行する準備が整いました。

SANホストからASA R2ストレージシステムへのデータアクセスを有効にする

データアクセスをセットアップするには、ONTAPでの適切な運用に欠かせないSANクライアントのパラメータと設定が正しく設定されていることを確認する必要があります。VMwareを使用している場合は、仮想マシンを移行する必要があります。

SANホストからのデータアクセスを設定する

SANホストからASA R2システムへのデータアクセスを設定するために必要な設定は、ホストのオペレーティングシステムとプロトコルによって異なります。最適なパフォーマンスと正常なフェイルオーバーを実現するには、正しい設定が重要です。

"VMware vSphere SCSIクライアント""VMware vSphere NVMeクライアント""その他のSANクライアント"ASA R2システムに接続するようにホストを適切に設定するには、ONTAP SANホストのマニュアルを参照してください。

VMware仮想マシンの移行

VMワークロードをASAストレージシステムからASA R2ストレージシステムに移行する必要がある場合はNetApp、を使用し"VMware vSphere vMotion"て、データのライブ移行を無停止で実行することを推奨します。

次の手順

これで、"ストレージのプロビジョニング"SANホストがストレージユニットに対してデータの読み取りと書き込みを実行できるようになります。

ONTAPを使用してデータを管理

ASA R2ストレージシステムのデモビデオ

ASA R2ストレージシステムでONTAP System Managerを使用して一般的なタスクをすばやく簡単に実行する方法を紹介する短いビデオをご覧ください。

ASA R2システムでSANプロトコルを設定する

"ビデオのトランスクリプト"

ASA R2システムでのSANストレージのプロビジョニング

"ビデオのトランスクリプト"

ASA R2システムからリモートクラスタにデータをレプリケート

"ビデオのトランスクリプト"

ストレージを管理

ASA R2システムでのONTAP SANストレージのプロビジョニング

ストレージをプロビジョニングするときに、SANホストがASA R2ストレージシステムに対してデータの読み取りと書き込みを実行できるようにします。ストレージをプロビジョニングするには、ONTAPシステムマネージャを使用して、ストレージユニットを作成し、ホストイニシエータを追加し、ホストをストレージユニットにマッピングします。また、読み取り/書き込み処理を有効にするために、ホストで手順を実行する必要があります。

ストレージユニットの作成

ASA R2システムでは、ストレージユニットによって、SANホストがデータ操作に使用できるストレージスペースが確保されます。ストレージユニットとは、SCSIホストの場合はLUN、NVMeホストの場合はNVMeネームスペースを指します。クラスタがSCSIホストをサポートするように設定されている場合は、LUNを作成するように求められます。NVMeホストをサポートするようにクラスタが設定されている場合は、NVMeネームスペースを作成するように求められます。ASA R2ストレージユニットの最大容量は128TBです。

"NetApp Hardware Universe"ASA R2システムの最新のストレージ制限については、を参照してください。

ホストイニシエータは、ストレージユニットの作成プロセスの一環としてストレージユニットに追加およびマッピングされます。また、"ホストイニシエータの追加""マッピング"ストレージユニットの作成後にそれらをストレージユニットに追加することもできます。

手順

1. System Managerで、*[ストレージ]*を選択し、を選択します + Add 。
2. 新しいストレージ・ユニットの名前を入力します

3. 作成する単位の数を入力します。

   複数のストレージ・ユニットを作成する場合'各ユニットは同じ容量'ホスト・オペレーティング・システム'ホスト・マッピングを使用して作成されます

4. ストレージユニットの容量を入力し、ホストオペレーティングシステムを選択します。
5. 自動選択された*ホストマッピング*を受け入れるか、マッピング先のストレージユニットに別のホストグループを選択してください。

   *ホスト・マッピング*は'新しいストレージ・ユニットのマッピング先となるホスト・グループを示します新しいストレージ・ユニット用に選択したホスト・タイプに対して既存のホスト・グループが存在する場合は'既存のホスト・グループがホスト・マッピング用に自動的に選択されますホストマッピング用に自動選択されたホストグループを受け入れることも、別のホストグループを選択することもできます。

   指定したオペレーティングシステムで実行されているホストのホストグループが存在しない場合は、ONTAPによって新しいホストグループが自動的に作成されます。

6. 次のいずれかを実行する場合は、*[その他のオプション]*を選択し、必要な手順を実行します。

オプション	手順
デフォルトのQoSポリシーを変更する ストレージユニットを作成するStorage Virtual Machine（VM）にデフォルトのQoSポリシーがまだ設定されていない場合、このオプションは使用できません。	a. で、[Quality of Service（QoS）]*の横にあるを選択します。 b. 既存の QoS ポリシーを選択してください。
新しいQoSポリシーを作成します。	a. で、[Quality of Service（QoS）]*の横にあるを選択します。 b. [新しいポリシーを定義する]*を選択します。 c. 新しいQoSポリシーの名前を入力します。 d. QoS制限、QoS保証、またはその両方を設定します。 i. 必要に応じて、* Limit *に、最大スループット制限、最大IOPS制限、またはその両方を入力します。 ストレージユニットに最大スループットとIOPSを設定すると、システムリソースへの影響が制限され、重要なワークロードのパフォーマンスが低下しないようになります。 ii. 必要に応じて、* Guarantee *に、最小スループット、最小IOPS、またはその両方を入力します。 ストレージユニットに最小スループットとIOPSを設定すると、競合するワークロードによる要求に関係なく、ストレージユニットは最小パフォーマンス目標を達成できます。 e. 「 * 追加」を選択します。

オプション	手順
新しいSCSIホストを追加します。	a. で、接続プロトコルとして[SCSI]*を選択します。 b. ホストオペレーティングシステムを選択します。 c. で[新しいホスト]*を選択します。 d. または[iSCSI]*を選択します。 e. 既存のホストイニシエータを選択するか、*イニシエータの追加*を選択して新しいホストイニシエータを追加します。 有効なFC WWPNの例は「01：02：03：04：0a：0b：0c：0d」です。有効なiSCSIイニシエータ名の例としては、「iqn.1995-08.com.example:string"」および「eui.0123456789abcdef」があります。
新しいSCSIホストグループを作成する	a. で、接続プロトコルとして[SCSI]*を選択します。 b. ホストオペレーティングシステムを選択します。 c. で[新しいホストグループ]*を選択します。 d. ホストグループの名前を入力し、グループに追加するホストを選択します。
新しいNVMeサブシステムを追加する	a. で、接続プロトコルとして[NVMe]*を選択します。 b. ホストオペレーティングシステムを選択します。 c. で[新しいNVMeサブシステム]*を選択します。 d. サブシステム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。 e. イニシエータの名前を入力します。 f. インバンド認証またはTransport Layer Security（TLS）を有効にする場合は、を選択し、オプションを選択します。 インバンド認証を使用すると、NVMeホストとASA R2システムの間でセキュアな双方向認証と一方向認証を確立できます。 TLSは、NVMe/TCPホストとASA R2システムの間でネットワーク経由で送信されるすべてのデータを暗号化します。 g. イニシエータをさらに追加する場合は、**[**イニシエータの追加**]** ホストNQNの形式は、<nqn.yyyy-mm>のあとに完全修飾ドメイン名を指定する必要があります。年は1970年以降である必要があります。合計最大長は223である必要があります。有効なNVMeイニシエータの例はnqn.2014-08.com.example:stringです。

7. 「 * 追加」を選択します。

次の手順

ストレージユニットが作成され、ホストにマッピングされます。これで、"スナップショットの作成"ASA R2システム上のデータを保護できます。

詳細情報

詳細については、をご覧ください "ASA R2システムでのStorage Virtual Machineの使用方法"。

ホストイニシエータの追加

ASA R2システムには、いつでも新しいホストイニシエータを追加できます。イニシエータは、ホストがストレージユニットにアクセスしてデータ処理を実行できるようにします。

開始する前に

ホストイニシエータの追加プロセス中にデスティネーションクラスタにホスト設定をレプリケートする場合は、クラスタがレプリケーション関係にある必要があります。必要に応じて、"レプリケーション関係を作成する"ホストを追加したあとに実行できます。

SCSIホストまたはNVMeホストのホストイニシエータを追加します。

SCSIホスト

手順

1. [ホスト]*を選択します。
2. [SCSI]*を選択し、を選択し + Add ます。
3. ホスト名を入力し、ホストオペレーティングシステムを選択して、ホストの説明を入力します。
4. ホスト設定をデスティネーションクラスタにレプリケートする場合は、*[ホスト設定をレプリケート]*を選択してから、デスティネーションクラスタを選択します。

   ホスト設定をレプリケートするには、クラスタがレプリケーション関係にある必要があります。

5. 新規または既存のホストを追加します。

新しいホストの追加	既存のホストを追加
a. [新しいホスト]*を選択します。 b. または[iSCSI]*を選択し、ホストイニシエータを選択します。 c. 必要に応じて、*ホストプロキシミティの設定*を選択します。 ホストのプロキシミティを設定すると、ONTAPがホストに最も近いコントローラを特定して、データパスの最適化とレイテンシの削減を実現できるようになります。これは、データをリモートサイトにレプリケートした場合にのみ該当します。Snapshotレプリケーションを設定していない場合は、このオプションを選択する必要はありません。 d. 新しいイニシエータを追加する必要がある場合は、*[イニシエータの追加]*を選択します。	a. [既存のホスト]*を選択します。 b. 追加するホストを選択します。 c. 「 * 追加」を選択します。

6. 「 * 追加」を選択します。

次の手順

ASA R2システムにSCSIホストが追加され、ホストをストレージユニットにマッピングする準備が整いました。

NVMeホスト

手順

1. [ホスト]*を選択します。
2. [NVMe]*を選択し、を選択し + Add ます。
3. NVMeサブシステムの名前を入力し、ホストオペレーティングシステムを選択して説明を入力します。
4. [Add initiator]*を選択します。

次の手順

NVMeホストがASA R2システムに追加され、ホストをストレージユニットにマッピングする準備が完了しました。

ホストグループの作成

ASA R2システムでは'_host group_は’ホストがストレージ・ユニットにアクセスできるようにするメカニズムですホストグループとは、SCSIホストのigroup、NVMeホストのNVMeサブシステムを指します。ホストは’所属するホスト・グループにマッピングされているストレージ・ユニットのみを認識できますホスト・グループがストレージ・ユニットにマッピングされると’グループのメンバーであるホストは’ストレージ・ユニットをマウント（ディレクトリとファイル構造を作成）することができます

ホストグループは、ストレージユニットの作成時に自動または手動で作成されます。必要に応じて、次の手順を使用して、ストレージユニットの作成前または作成後にホストグループを作成できます。

手順

1. System Managerで、*[ホスト]*を選択します。
2. ホストグループに追加するホストを選択します。

   最初のホストを選択すると、ホストグループに追加するオプションがホストのリストの上に表示されます。

3. [ホストグループに追加]*を選択します。
4. ホストを追加するホストグループを検索して選択します。

次の手順

これで’ホスト・グループが作成され’ストレージ・ユニットにマッピングできるようになりました

ストレージ・ユニットのホストへのマッピング

ASA R2ストレージユニットを作成し、ホストイニシエータを追加したら、データの提供を開始するために、ホストをストレージユニットにマッピングする必要があります。ストレージ・ユニットは’ストレージ・ユニット作成プロセスの一環としてホストにマッピングされますまた、既存のストレージユニットを新規または既存のホストにいつでもマッピングできます。

手順

1. [ストレージ]*を選択します。
2. マッピングするストレージ・ユニットの名前にカーソルを合わせます
3. を選択し、*[ホストにマッピング]*を選択します。
4. ストレージユニットにマッピングするホストを選択し、*[マップ]*を選択します。

次の手順

ストレージユニットがホストにマッピングされ、ホストでプロビジョニングプロセスを完了できる状態になります。

ホスト側の完全なプロビジョニング

ストレージユニットを作成し、ホストイニシエータを追加し、ストレージユニットをマッピングしたら、ASA R2システムでデータの読み取りと書き込みを行う前に、ホストで実行する必要があります。

手順

1. FCおよびFC / NVMeの場合は、FCスイッチをWWPNでゾーニングします。

   イニシエータごとに1つのゾーンを使用し、各ゾーンにすべてのターゲットポートを含めます。

2. 新しいストレージユニットを検出します。
3. ストレージ・ユニットとCREATE FILE SYSTEMを初期化します
4. ホストがストレージユニットのデータを読み取りおよび書き込みできることを確認します。

次の手順

プロビジョニングプロセスが完了し、データの提供を開始する準備ができました。これで、"スナップショットの作成"ASA R2システム上のデータを保護できます。

詳細情報

ホスト側の設定の詳細については"ONTAP SANホストのドキュメント"、使用しているホストのを参照してください。

ASA R2ストレージシステム上のデータのクローニング

データのクローニングでは、ONTAP System Managerを使用して、ASA R2システムにストレージユニットと整合グループのコピーが作成されます。このコピーは、アプリケーションの開発、テスト、バックアップ、データ移行、その他の管理機能に使用できます。

ストレージユニットのクローン

ストレージユニットのクローンを作成すると、クローンを作成したストレージユニットのポイントインタイムの書き込み可能なコピーである新しいストレージユニットがASA R2システムに作成されます。

手順

1. System Managerで、*[ストレージ]*を選択します。
2. クローニングするストレージユニットの名前にカーソルを合わせます。
3. を選択し、*[クローン]*を選択します。
4. クローンとして作成する新しいストレージ・ユニットのデフォルト名をそのまま使用するか、新しいストレージ・ユニットを入力します。
5. ホストオペレーティングシステムを選択します。

   デフォルトでは、クローン用に新しいSnapshotが作成されます。

6. 既存のSnapshotを使用する場合、新しいホストグループを作成する場合、または新しいホストを追加する場合は、*[その他のオプション]*を選択します。

オプション	手順
既存のSnapshotを使用する	a. で、[Use an existing snaphot]*を選択します。 b. クローンに使用するSnapshotを選択します。
新しいホストグループを作成する	a. で[新しいホストグループ]*を選択します。 b. 新しいホストグループの名前を入力し、グループに含めるホストイニシエータを選択します。
新しいホストを追加	a. で[新しいホスト]*を選択します。 b. 新しいホストの名前を入力し、* FC または iSCSI *を選択します。 c. 既存のイニシエータのリストからホストイニシエータを選択するか、*[追加]*を選択してホストに新しいイニシエータを追加します。

7. 「 * Clone * 」を選択します。

次の手順

クローンを作成したストレージ・ユニットと同じ新しいストレージ・ユニットが作成されましたこれで、必要に応じて新しいストレージユニットを使用する準備ができました。

クローン整合グループ

整合グループをクローニングすると、クローニングした整合グループと構造、ストレージユニット、データが同じ新しい整合グループが作成されます。アプリケーションのテストやデータの移行には、整合グループのクローンを使用します。たとえば、本番ワークロードを整合グループから移行する必要があるとします。整合グループをクローニングして本番環境のワークロードのコピーを作成すると、移行が完了するまでバックアップとして保持されます。

クローンは、クローニングする整合グループのSnapshotから作成されます。クローンに使用されるスナップショットは、デフォルトでクローニングプロセスが開始された時点で作成されます。既存のSnapshotを使用するようにデフォルトの動作を変更できます。

ストレージユニットのマッピングは、クローニングプロセスの一環としてコピーされます。Snapshotポリシーはクローニングプロセスではコピーされません。

クローンは、ASA R2システムにローカルに格納されている整合グループから作成することも、リモートの場所にレプリケートされた整合グループから作成することもできます。

ローカル**Snapshot**を使用したクローニング

手順

1. System Managerで、*[保護]>[整合グループ]*を選択します。
2. クローニングする整合グループにカーソルを合わせます。
3. を選択し、*[クローン]*を選択します。
4. クローン整合グループ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. ホストオペレーティングシステムを選択します。
6. ソース整合グループとクローンの関連付けを解除してディスクスペースを割り当てる場合は、*[クローンのスプリット]*を選択します。
7. 既存のSnapshotを使用する場合は、新しいホストグループを作成するか、クローン用に新しいホストを追加し、*[その他のオプション]*を選択します。

オプション	手順
既存のSnapshotを使用する	a. で、[既存のSnapshotを使用する]*を選択します。 b. クローンに使用するSnapshotを選択します。
新しいホストグループを作成する	a. で[新しいホストグループ]*を選択します。 b. 新しいホストグループの名前を入力し、グループに含めるホストイニシエータを選択します。
新しいホストを追加	a. で[新しいホスト]*を選択します。 b. 新しいホスト名を入力し、* FC または iSCSI *を選択します。 c. 既存のイニシエータのリストからホストイニシエータを選択するか、*[イニシエータの追加]*を選択してホストに新しいイニシエータを追加します。

8. 「 * Clone * 」を選択します。

リモート**Snapshot**を使用したクローニング

手順

1. System Managerで、*[保護]>[レプリケーション]*を選択します。
2. クローンを作成する*ソース*にカーソルを合わせます。
3. を選択し、*[クローン]*を選択します。
4. ソースクラスタとStorage VMを選択し、新しい整合グループ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. クローニングするSnapshotを選択し、*[クローン]*を選択します。

次の手順

リモートサイトから整合グループをクローニングしておきます。新しいコンシステンシグループは、ASA R2システム上で必要に応じてローカルで使用できます。

次の手順

データを保護するには、"スナップショットの作成"クローニングした整合グループを使用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ユニットの変更

ASA R2システムのパフォーマンスを最適化するには、容量の拡張、QoSポリシーの更新、ユニットにマッピングされているホストの変更など、ストレージユニットの変更が必要になる場合があります。たとえば、新しい重要なアプリケーションワークロードを既存のストレージユニットに追加した場合、新しいアプリケーションに必要なパフォーマンスレベルをサポートするために、ストレージユニットに適用されているサービス品質（QoS）ポリシーの変更が必要になることがあります。

容量の拡張

ストレージユニットの書き込み可能なスペースが不足した場合にデータアクセスが失われないように、ストレージユニットの容量がフルに達する前にサイズを拡張します。ストレージユニットの容量は、ONTAPで許可されている最大サイズである128TBに拡張できます。

ホストマッピングの変更

ワークロードの分散やシステムリソースの再設定を支援するために、ストレージユニットにマッピングされているホストを変更します。

QoS ポリシーの変更

サービス品質（QoS）ポリシーは、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ためのポリシーです。QoSポリシーを使用して、QoS throughput_limit_およびQoS throughput_guarante_を設定できます。

- QoSスループット制限

  QoS throughput_limit_は、ワークロードのスループットを最大IOPS、最大MBps、またはIOPSとMBpsに制限することで、ワークロードのシステムリソースへの影響を制限します。

- QoSスループット保証

  QoS throughput_guarantee _は、重要なワークロードのスループットが最小IOPS、MBps、またはIOPSとMBpsを下回らないようにすることで、競合するワークロードによる要求に関係なく、重要なワークロードが最小スループットを達成するようにします。

手順

1. System Managerで、*[ストレージ]*を選択します。
2. 編集するストレージユニットの名前にカーソルを合わせます。
3. を選択し、*[編集]*を選択します。
4. 必要に応じてストレージユニットのパラメータを更新し、容量の拡張、QoSポリシーの変更、ホストマッ

ピングの更新を行います。

次の手順

ストレージユニットのサイズを拡張した場合、ホストがサイズの変更を認識できるように、ホスト上のストレージユニットを再スキャンする必要があります。

ASA R2ストレージシステム上のストレージユニットの削除

ユニットに含まれるデータを維持する必要がなくなった場合は、ストレージユニットを削除します。不要になったストレージユニットを削除すると、他のホストアプリケーションに必要なスペースを解放できます。

開始する前に

削除するストレージユニットがレプリケーション関係にあるコンシステンシグループに含まれている場合は"コンシステンシ・グループからのストレージ・ユニットの削除"、削除する前にストレージユニットを削除する必要があります。

手順

1. System Managerで、*[ストレージ]*を選択します。
2. 削除するストレージユニットの名前にカーソルを合わせます。
3. を選択し、* Delete *を選択します。
4. 削除を元に戻せないことを承認します。
5. 「* 削除」を選択します。

次の手順

削除されたストレージユニットから解放されたスペースを、"サイズを大きくする"追加の容量が必要なストレージユニットに使用できます。

ASA R2ストレージの制限

最適なパフォーマンス、構成、サポートを実現するには、ASA R2ストレージの制限を確認しておく必要があります。

ASA R2システムは、次の機能をサポートしています。

クラスタあたりの最大ノード数	2
最大ストレージユニットサイズ	128TB

詳細情報

ASA R2ストレージの最新の制限の一覧については、を参照してください"NetApp Hardware Universe"。

データを保護

ASA R2ストレージシステム上のデータをバックアップするためのSnapshotの作成

ASA R2システムのデータをバックアップするには、スナップショットを作成する必要があります。ONTAPシステムマネージャを使用して、単一のストレージユニットのSnapshotを手動で作成したり、整合グループを作成して複数のストレージユニットのSnapshotを同時に自動でスケジュールしたりできます。

手順1：必要に応じて整合グループを作成

整合グループは、1つのユニットとして管理されるストレージユニットの集まりです。整合グループを作成して、複数のストレージユニットにまたがるアプリケーションワークロードのストレージ管理とデータ保護を簡易化します。たとえば、10個のストレージユニットで構成されるデータベースが整合グループ内にあり、データベース全体をバックアップする必要があるとします。各ストレージユニットをバックアップする代わりに、整合性グループにSnapshotデータ保護を追加するだけで、データベース全体をバックアップできます。

新しいストレージユニットを使用して整合グループを作成するか、既存のストレージユニットを使用して整合グループを作成します。

新しいストレージユニットを使用

手順

1. System Managerで、*[保護]>[整合グループ]*を選択します。
2. を選択し + Add 、*[Using new storage units]*を選択します。
3. 新しいストレージ・ユニットの名前'ユニット数'ユニットあたりの容量を入力します

   複数のユニットを作成する場合は、各ユニットが同じ容量とホストオペレーティングシステムで作成されます。各ユニットに異なる容量を割り当てるには、**[**その他のオプション**]***を選択し、[別の容量を追加する]*を選択します。

4. ホストオペレーティングシステムとホストマッピングを選択します。
5. 「 * 追加」を選択します。

次の手順

保護するストレージユニットを含む整合グループを作成しておきます。これで、スナップショットを作成する準備ができました。

既存のストレージユニットを使用

手順

1. System Managerで、*[保護]>[整合グループ]*を選択します。
2. を選択し + Add 、*[Using existing storage units]*を選択します。
3. 整合グループの名前を入力し、整合グループに含めるストレージユニットを検索して選択します。
4. 「 * 追加」を選択します。

次の手順

保護するストレージユニットを含む整合グループを作成しておきます。これで、スナップショットを作成する準備ができました。

手順2：Snapshotを作成する

Snapshotは、データのローカルの読み取り専用コピーであり、ストレージユニットを特定の時点にリストアするために使用できます。

スナップショットは、オンデマンドで作成することも、に基づいて定期的に自動的に作成することもできます"Snapshotポリシーとスケジュール"。Snapshotポリシーとスケジュールは、Snapshotを作成するタイミング、保持するコピーの数、Snapshotに名前を付ける方法、およびSnapshotにレプリケーション用のラベルを付ける方法を指定します。たとえば、毎日午前12時10分にSnapshotを1つ作成し、最新の2つのコピーを保持して「daily」（タイムスタンプが付加された）という名前を付け、レプリケーション用に「daily」というラベルを付けるとします。

Snapshotのタイプ

単一のストレージユニットまたは整合性グループのオンデマンドSnapshotを作成できます。複数のストレージユニットを含む整合グループの自動スナップショットを作成できます。単一のストレージユニットの自動スナップショットは作成できません。

- オンデマンドのスナップショット

  ストレージユニットのオンデマンドスナップショットはいつでも作成できます。オンデマンドSnapshotで保護するために、ストレージユニットが整合性グループのメンバーである必要はありません。整合性グループのメンバーであるストレージユニットのオンデマンドSnapshotを作成した場合、整合性グループ内の他のストレージユニットはオンデマンドSnapshotに含まれません。整合性グループのオンデマンドSnapshotを作成すると、整合性グループ内のすべてのストレージユニットがSnapshotに含まれます。

- Snapshotの自動作成

  自動Snapshotは、Snapshotポリシーを使用して作成されます。Snapshotの自動作成用にストレージユニットにSnapshotポリシーを適用するには、そのストレージユニットが整合グループのメンバーである必要があります。Snapshotポリシーを整合性グループに適用すると、整合性グループ内のすべてのストレージユニットが自動Snapshotで保護されます。

整合性グループまたはストレージユニットのSnapshotを作成します。

整合性グループの**Snapshot**

手順

1. System Managerで、*[保護]>[整合グループ]*を選択します。
2. 保護する整合グループの名前にカーソルを合わせます。
3. を選択し、* Protect *を選択します。
4. オンデマンドで即座にSnapshotを作成する場合は、**[**ローカル保護**]***で[今すぐSnapshotを追加]*を選択します。

   ローカル保護では、ストレージユニットを含むクラスタにSnapshotが作成されます。

   a. Snapshot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、必要に応じてSnapMirrorラベルを入力します。

      SnapMirrorラベルはリモートデスティネーションで使用されます。

5. Snapshotポリシーを使用して自動Snapshotを作成する場合は、*[Snapshotのスケジュール設定]*を選択します。

   a. Snapshot ポリシーを選択します。

      デフォルトのSnapshotポリシーをそのまま使用するか、既存のポリシーを選択するか、新しいポリシーを作成します。

オプション	手順
既存のSnapshotポリシーを選択します	デフォルトポリシーの横にあるを選択し、使用する既存のポリシーを選択します。
新しいSnapshotポリシーを作成します。	i. を選択し Add 、Snapshotポリシーのパラメータを入力します。 ii. [ポリシーの追加]*を選択します。

6. Snapshotをリモートクラスタにレプリケートする場合は、**[**リモート保護**]***で[リモートクラスタにレプリケート]*を選択します。

   a. ソースクラスタとStorage VMを選択し、レプリケーションポリシーを選択します。

      デフォルトでは、レプリケーションの最初のデータ転送がすぐに開始されます。

7. [保存（ Save ）] を選択します。

ストレージユニットのスナップショット

手順

1. System Managerで、*[ストレージ]*を選択します。
2. 保護するストレージユニットの名前にカーソルを合わせます。
3. を選択し、* Protect を選択します。オンデマンドで即座に**Snapshot**を作成する場合は、[ローカル保護]で[今すぐSnapshotを追加]*を選択します。

ローカル保護では、ストレージユニットを含むクラスタにSnapshotが作成されます。

4. Snapshot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、必要に応じてSnapMirrorラベルを入力します。

   SnapMirrorラベルはリモートデスティネーションで使用されます。

5. Snapshotポリシーを使用して自動Snapshotを作成する場合は、*[Snapshotのスケジュール設定]*を選択します。

   a. Snapshot ポリシーを選択します。

      デフォルトのSnapshotポリシーをそのまま使用するか、既存のポリシーを選択するか、新しいポリシーを作成します。

オプション	手順
既存のSnapshotポリシーを選択します	デフォルトポリシーの横にあるを選択し、使用する既存のポリシーを選択します。
新しいSnapshotポリシーを作成します。	i. を選択し Add 、Snapshotポリシーのパラメータを入力します。 ii. [ポリシーの追加]*を選択します。

6. Snapshotをリモートクラスタにレプリケートする場合は、**[**リモート保護**]***で[リモートクラスタにレプリケート]*を選択します。

   a. ソースクラスタとStorage VMを選択し、レプリケーションポリシーを選択します。

      デフォルトでは、レプリケーションの最初のデータ転送がすぐに開始されます。

7. [保存（ Save ）] を選択します。

次の手順

Snapshotでデータを保護したので"Snapshotレプリケーションのセットアップ"、バックアップとディザスタリカバリのために、地理的に離れた場所に整合グループをコピーする必要があります。

ASA R2ストレージシステムからリモートクラスタにSnapshotをレプリケート

Snapshotレプリケーションは、ASA R2システム上の整合グループを地理的に離れた場所にコピーするプロセスです。最初のレプリケーションの後、コンシステンシグループへの変更は、レプリケーションポリシーに基づいてリモートロケーションにコピーされます。レプリケートされた整合グループは、ディザスタリカバリまたはデータ移行に使用できます。

ASA R2ストレージシステムから別のASA R2ストレージシステムへのSnapshotレプリケーションのみがサポートされます。ASA R2システムから現在のASA、AFF、またはFASシステムにSnapshotをレプリケートすることはできません。

Snapshotレプリケーションを設定するには、ASA R2システムとリモートサイトの間にレプリケーション関係

を確立する必要があります。レプリケーション関係はレプリケーションポリシーによって管理されます。すべてのSnapshotをレプリケートするデフォルトポリシーは、クラスタのセットアップ時に作成されます。デフォルトのポリシーを使用することも、必要に応じて新しいポリシーを作成することもできます。

手順**1**：クラスタピア関係を作成する

データをリモートクラスタにレプリケートして保護するには、ローカルクラスタとリモートクラスタの間にクラスタピア関係を作成する必要があります。

手順

1. ローカルクラスタで、System Managerで*[クラスタ]>[設定]*を選択します。
2. の横にある[クラスタ間設定]でを選択し、[クラスタピアの追加]*を選択します。
3. [Lauch remote cluster]*を選択します。これにより、リモートクラスタでの認証に使用するパスフレーズが生成されます。
4. リモートクラスタのパスフレーズが生成されたら、ローカルクラスタの*[パスフレーズ]*に貼り付けます。
5. を選択 Add し、クラスタ間ネットワークインターフェイスのIPアドレスを入力します。
6. [クラスタピアリングの開始]*を選択します。

次の手順

ローカルASA R2クラスタとリモートクラスタのピア関係を設定しておきます。レプリケーション関係を作成できるようになりました。

手順**2**：必要に応じて、レプリケーションポリシーを作成します。

Snapshotレプリケーションポリシーは、ASA R2クラスタで実行される更新をリモートサイトにレプリケートするタイミングを定義します。

手順

1. System Managerで、**[保護]>[**ポリシー**]***を選択し、[レプリケーションポリシー]*を選択します。
2. を選択します Add 。
3. レプリケーションポリシー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てから、説明を入力します。
4. [ポリシーの範囲]*を選択します。

   レプリケーションポリシーをクラスタ全体に適用する場合は、**[**クラスタ**]***を選択します。レプリケーションポリシーを特定の**Storage VM**のストレージユニットにのみ適用する場合は、[Storage VM]*を選択します。

5. [ポリシータイプ]*を選択します。

オプション	手順
ソースに書き込まれたデータをリモートサイトにコピーします。	a. [非同期]*を選択します。 b. [ソースからSnapshotを転送]*で、デフォルトの転送スケジュールをそのまま使用するか、別の転送スケジュールを選択します。 c. すべてのスナップショットを転送するか、転送するスナップショットを決定するルールを作成する場合に選択します。 d. 必要に応じて、ネットワーク圧縮を有効にします。
ソースサイトとリモートサイトに同時にデータを書き込みます。	a. [同期]*を選択します。

6. [保存（ Save ）] を選択します。

次の手順

これでレプリケーションポリシーが作成され、ASA R2システムとリモートサイトの間にレプリケーション関係を作成できるようになりました。

詳細情報

詳細については、をご覧ください "クライアントアクセスヨウノStorage VM"。

手順**3**：レプリケーション関係を作成する

Snapshotレプリケーション関係により、ASA R2システムとリモートサイトの間に接続が確立され、リモートクラスタに整合グループをレプリケートできるようになります。レプリケートされた整合グループは、ディザスタリカバリまたはデータ移行に使用できます。

ランサムウェア攻撃から保護するために、レプリケーション関係を設定するときに、デスティネーションSnapshotをロックするように選択できます。ロックされたSnapshotは、誤ってまたは悪意を持って削除することはできません。ロックされたSnapshotを使用して、ランサムウェア攻撃によってストレージユニットが侵害された場合にデータをリカバリできます。

開始する前に

デスティネーションSnapshotをロックする場合は、"Snapshotコンプライアンスクロックを初期化する"レプリケーション関係を作成する前にロックする必要があります。

ロックされたデスティネーションSnapshotを使用するかどうかに関係なく、レプリケーション関係を作成します。

ロックされた**Snapshot**あり

手順

1. System Managerで、*[保護]>[整合グループ]*を選択します。
2. 整合グループを選択します。
3. を選択し、* Protect *を選択します。
4. で、[リモートクラスタにレプリケート]*を選択します。
5. [レプリケーションポリシー]*を選択します。

   _vault_replicationポリシーを選択する必要があります。
6. [デスティネーションの設定]*を選択します。
7. [デスティネーションSnapshotをロックして削除を防止する]*を選択します。
8. 最大および最小のデータ保持期間を入力します。
9. データ転送の開始を遅らせるには、*[すぐに転送を開始する]*の選択を解除します。

   デフォルトでは、最初のデータ転送がすぐに開始されます。
10. 必要に応じて、デフォルトの転送スケジュールを上書きするには、*デスティネーション設定*を選択し、*転送スケジュールを上書き*を選択します。

    転送スケジュールがサポートされるまでに30分以上かかる必要があります。
11. [保存（ Save ）] を選択します。

ロックされた**Snapshot**なし

手順

1. System Managerで、*[保護]>[レプリケーション]*を選択します。
2. ローカルデスティネーションまたはローカルソースとのレプリケーション関係を作成する場合に選択します。

オプション	手順
ローカル保存先	a. [ローカルデスティネーション]*を選択し、を選択します Replicate 。 b. ソース整合性グループを検索して選択します。 _source_consistencyグループは、レプリケートするローカルクラスタ上の整合グループです。

オプション	手順
ローカルソース	a. [Local sources]*を選択し、を選択します Replicate。 b. ソース整合性グループを検索して選択します。 _source_consistencyグループは、レプリケートするローカルクラスタ上の整合グループです。 c. [レプリケーションのデスティネーション]*で、レプリケート先のクラスタを選択し、Storage VMを選択します。

3. レプリケーションポリシーを選択します。
4. データ転送の開始を遅らせるには、*送信先設定*を選択し、*すぐに転送を開始*の選択を解除します。

   デフォルトでは、最初のデータ転送がすぐに開始されます。

5. 必要に応じて、デフォルトの転送スケジュールを上書きするには、*デスティネーション設定*を選択し、*転送スケジュールを上書き*を選択します。

   転送スケジュールがサポートされるまでに30分以上かかる必要があります。

6. [保存（ Save ）] を選択します。

次の手順

レプリケーションポリシーと関係を作成したので、レプリケーションポリシーの定義に従って最初のデータ転送が開始されます。必要に応じて、レプリケーションフェイルオーバーをテストして、ASA R2システムがオフラインになった場合にフェイルオーバーが正常に実行されることを確認できます。

手順**4**：レプリケーションのフェイルオーバーをテストする

必要に応じて、ソースクラスタがオフラインの場合に、リモートクラスタ上のレプリケートされたストレージユニットからデータを正常に提供できることを検証します。

手順

1. System Managerで、*[保護]>[レプリケーション]*を選択します。
2. テストするレプリケーション関係にカーソルを合わせ、を選択します。
3. [Test failover]*を選択します。
4. フェイルオーバー情報を入力し、*[Test failover]*を選択します。

次の手順

ディザスタリカバリのためにスナップショットレプリケーションを使用してデータを保護したので、"保存データを暗号化"ASA R2システム内のディスクの転用、返却、置き忘れ、盗難に際してデータが読み取られないようにする必要があります。

ASA R2ストレージシステム上のKubernetesアプリケーションを保護

Astra Control Centerを使用してKubernetesアプリケーションを保護します。Astra Control Centerを使用すると、Kubernetesクラスタ間でアプリケーションとデータを移行したり、NetApp SnapMirrorテクノロジを使用してリモートシステムにアプリケーションをレプリケートしたり、ステージング環境から本番環境にアプリケーションをクローニングしたりできます。

詳細情報

"Astra Controlを使用したKubernetesアプリケーションの保護の詳細"です。

ASA R2ストレージシステム上のデータのリストア

Snapshotによって保護されているコンシステンシグループまたはストレージユニット内のデータが失われたり破損したりした場合は、データをリストアできます。

整合グループのリストア

整合グループをリストアすると、整合グループ内のすべてのストレージユニットのデータがSnapshotのデータに置き換えられます。Snapshotの作成後にストレージユニットに加えられた変更はリストアされません。

整合性グループは、ローカルまたはリモートのSnapshotからリストアできます。

ローカル**Snapshot**からのリストア

手順

1. System Managerで、*[保護]>[整合グループ]*を選択します。
2. リストアする必要のあるデータを含む整合グループをダブルクリックします。

   整合グループの詳細ページが開きます。

3. [Snapshots]*を選択します。
4. リストアするSnapshotを選択し、を選択します。
5. **[**この**Snapshot**から整合性グループをリストアする**]***を選択し、[リストア]*を選択します。

リモート**Snapshot**からのリストア

手順

1. System Managerで、*[保護]>[レプリケーション]*を選択します。
2. [ローカルデスティネーション]*を選択します。
3. リストアする*ソース*を選択し、を選択します。
4. [* Restore] を選択します。
5. データのリストア先となるクラスタ、Storage VM、および整合グループを選択します。
6. リストア元のSnapshotを選択します。
7. プロンプトが表示されたら、「restore」と入力し、* Restore *を選択します。

結果

整合性グループは、リストアに使用したSnapshotのポイントインタイムにリストアされます。

ストレージユニットのリストア

ストレージ・ユニットをリストアすると'ストレージ・ユニット内のすべてのデータがスナップショットのデータに置き換えられますスナップショットの作成後にストレージユニットに加えられた変更はリストアされません。

手順

1. System Managerで、*[ストレージ]*を選択します。
2. リストアする必要のあるデータが格納されているストレージ・ユニットをダブルクリックします。

   ストレージユニットの詳細ページが開きます。

3. [Snapshots]*を選択します。
4. リストアするSnapshotを選択します。
5. を選択し、*[リストア]*を選択します。
6. を選択し、[リストア]*を選択します。

結果

ストレージユニットは、リストアに使用されたスナップショットのポイントインタイムにリストアされます。

ASA R2ストレージシステム上のONTAP整合性グループを管理します。

整合グループは、1つのユニットとして管理されるストレージユニットの集まりです。ストレージ管理を簡易化するために、整合グループを使用します。たとえば、10個のストレージユニットで構成されるデータベースが整合グループ内にあり、データベース全体をバックアップする必要があるとします。各ストレージユニットをバックアップする代わりに、整合性グループにSnapshotデータ保護を追加するだけで、データベース全体をバックアップできます。ストレージユニットを個別にではなくコンシステンシグループとしてバックアップすると、すべてのユニットの整合性のあるバックアップが提供されます。ユニットを個別にバックアップすると、不整合が発生する可能性があります。

整合性グループへのSnapshotデータ保護の追加

整合性グループにSnapshotデータ保護を追加すると、事前定義されたスケジュールに基づいて、整合性グループのローカルSnapshotが一定の間隔で作成されます。

"データのリストア"失われたスナップショットまたは破損したスナップショットをに使用できます。

手順

1. System Managerで、*[保護]>[整合グループ]*を選択します。
2. 保護する整合グループにカーソルを合わせます。
3. を選択し⋮、*[編集]*を選択します。
4. で、[Snapshotのスケジュール設定]*を選択します。
5. Snapshot ポリシーを選択します。

   デフォルトのSnapshotポリシーをそのまま使用するか、既存のポリシーを選択するか、新しいポリシーを作成します。

オプション	手順
既存のSnapshotポリシーを選択します	⌄デフォルトポリシーの横にあるを選択し、使用する既存のポリシーを選択します。

オプション	手順
新しいSnapshotポリシーを作成します。	a. を選択し Add 、新しいポリシー名を入力します。 b. ポリシーのスコープを選択します。 c. [スケジュール]*でを選択します Add 。 d. [スケジュール名]*に表示される名前を選択します。 次に、を選択します 。 e. ポリシースケジュールを選択します。 f. [Maximum snapshots]*で、整合グループで保持するSnapshotの最大数を入力します。 g. 必要に応じて、* SnapMirror label *の下にSnapMirrorラベルを入力します。 h. [保存（ Save ）] を選択します。

6. 「 * 編集 * 」を選択します。

次のステップ

Snapshotでデータを保護できるようになったので、"Snapshotレプリケーションのセットアップ"バックアップとディザスタリカバリのために、地理的に離れた場所に整合グループをコピーする必要があります。

整合性グループからの**Snapshot**データ保護の削除

整合性グループからSnapshotデータ保護を解除すると、整合性グループ内のすべてのストレージユニットのSnapshotが無効になります。

手順

1. System Managerで、*[保護]>[整合グループ]*を選択します。
2. 保護を停止する整合グループにカーソルを合わせます。
3. を選択し、*[編集]*を選択します。
4. [Local protection]*で、[Schedule snapshots]の選択を解除します。
5. 「 * 編集 * 」を選択します。

結果

整合グループ内のどのストレージユニットに対してもSnapshotは作成されません。

整合グループへのストレージユニットの追加

コンシステンシグループにストレージユニットを追加して、コンシステンシグループが管理するストレージの容量を拡張します。

既存のストレージユニットを整合グループに追加することも、新しいストレージユニットを作成して整合グループに追加することもできます。

既存のストレージユニットの追加

手順

1. System Managerで、*[保護]>[整合グループ]*を選択します。
2. 展開する整合グループにカーソルを合わせます。
3. を選択し、* Expand *を選択します。
4. [既存のストレージユニットを使用する]*を選択します。
5. 整合グループに追加するストレージユニットを選択し、*[拡張]*を選択します。

新しいストレージユニットの追加

手順

1. System Managerで、*[保護]>[整合グループ]*を選択します。
2. 展開する整合グループにカーソルを合わせます。
3. を選択し、* Expand *を選択します。
4. [新しいストレージユニットを使用する]*を選択します。
5. 作成する単位数と単位あたりの容量を入力します。

   この1つのユニットを複数作成すると、各ユニットは同じ容量とホストオペレーティングシステムで作成されます。ユニットごとに異なる容量を割り当てるには、*[Add a different capacity]*を選択して、ユニットごとに異なる容量を割り当てます。

6. [Expand]*を選択します。

次の手順

新しいストレージユニットを作成したら"ホストイニシエータの追加"、とを実行し"新しく作成したストレージ・ユニットをホストにマッピングします"ます。ホストイニシエータを追加すると、ホストはストレージユニットにアクセスしてデータ処理を実行できるようになります。ストレージ・ユニットをホストにマッピングすると'ストレージ・ユニットは'マッピング先のホストへのデータの提供を開始できます

次の手順

コンシステンシグループの既存のスナップショットには、新しく追加したストレージユニットは含まれません。"すぐにSnapshotを作成する"次のスケジュールされたSnapshotが自動的に作成されるまで、新たに追加したストレージユニットを保護するには、整合性グループに属している必要があります。

コンシステンシ・グループからのストレージ・ユニットの削除

ストレージユニットを削除する場合、ストレージユニットを別の整合グループの一部として管理する場合、またはストレージユニットに含まれるデータを保護する必要がなくなった場合は、ストレージユニットを整合グループから削除する必要があります。ストレージユニットを整合グループから削除すると、ストレージユニットと整合グループ間の関係は解除されますが、ストレージユニットは削除されません。

手順

1. System Managerで、*[保護]>[整合グループ]*を選択します。
2. ストレージユニットを削除するコンシステンシグループをダブルクリックします。

3. セクションの[ストレージユニット]で、削除するストレージユニットを選択し、[整合グループから削除]*を選択します。

結果

ストレージユニットはコンシステンシグループのメンバーではなくなりました。

次のステップ

ストレージユニットのデータ保護を継続する必要がある場合は、別のコンシステンシグループにストレージユニットを追加します。

整合グループを削除する

整合グループのメンバーを1つのユニットとして管理する必要がなくなった場合は、整合グループを削除できます。整合グループを削除すると、そのグループに含まれていたストレージユニットはクラスタ上でアクティブなままになります。

開始する前に

削除する整合グループがレプリケーション関係にある場合は、整合グループを削除する前に関係を解除する必要があります。以前のレプリケーションコンシステンシグループを削除すると、コンシステンシグループに含まれていたストレージユニットはクラスタでアクティブなままになり、それらのレプリケートコピーはリモートクラスタに残ります。

手順

1. System Managerで、*[保護]>[整合グループ]*を選択します。
2. 削除する整合グループにカーソルを合わせます。
3. を選択し、* Delete *を選択します。
4. 警告を受け入れ、*[削除]*を選択します。

次の手順

整合グループを削除すると、その整合グループに含まれていたストレージユニットはSnapshotによって保護されなくなります。これらのストレージユニットをデータ損失から保護するために、別の整合グループに追加することを検討してください。

ASA R2ストレージシステムのONTAPデータ保護ポリシーとスケジュールを管理します。

Snapshotポリシーを使用して、整合性グループ内のデータを自動スケジュールで保護します。Snapshotポリシー内のポリシースケジュールを使用して、Snapshotを作成する頻度を決定します。

新しい保護ポリシースケジュールを作成する

保護ポリシースケジュールは、Snapshotポリシーを実行する頻度を定義します。日数、時間数、または分数に基づいて一定の間隔で実行するスケジュールを作成できます。たとえば、1時間ごとに実行するスケジュールや、1日に1回のみ実行するスケジュールを作成できます。特定の曜日または月の特定の時間に実行するスケジュールを作成することもできます。たとえば、毎月20日の午前12時15分に実行するスケジュールを作成できます。

さまざまな保護ポリシースケジュールを定義することで、アプリケーションごとにSnapshotの作成頻度を柔

軟に増減できます。これにより、重要なワークロードの保護レベルが向上し、重要度の低いワークロードに必要な保護レベルよりもデータ損失のリスクが軽減されます。

手順

1. [保護]>[ポリシー]を選択し、[スケジュール]*を選択します。
2. を選択します + Add 。
3. スケジュールの名前を入力し、スケジュールパラメータを選択します。
4. [保存（ Save ）] を選択します。

次の手順

新しいポリシースケジュールを作成したので、ポリシー内で新しく作成したスケジュールを使用して、スナップショットを作成するタイミングを定義できます。

Snapshot ポリシーを作成します

スナップショットポリシーは、スナップショットを作成する頻度、許可されるスナップショットの最大数、およびスナップショットを保持する期間を定義します。

手順

1. System Managerで、**[保護]>[**ポリシー**]***を選択し、[Snapshotポリシー]*を選択します。
2. を選択します + Add 。
3. Snapshotポリシーの名前を入力します。
4. [クラスタ]*を選択して、ポリシーをクラスタ全体に適用します。[Storage VM]*を選択して、ポリシーを個々 のStorage VMに適用します。
5. [スケジュールの追加]*を選択し、Snapshotポリシーのスケジュールを入力します。
6. [ポリシーの追加]*を選択します。

次の手順

これでSnapshotポリシーを作成したので、整合性グループに適用できます。Snapshotポリシーで設定したパラメータに基づいて、整合性グループのSnapshotが作成されます。

整合性グループへの**Snapshot**ポリシーの適用

Snapshotポリシーを整合性グループに適用して、整合性グループのSnapshotを自動的に作成、保持、およびラベル付けします。

手順

1. System Managerで、**[保護]>[**ポリシー**]***を選択し、[Snapshotポリシー]*を選択します。
2. 適用するSnapshotポリシーの名前にカーソルを合わせます。
3. を選択し⋮、*適用*を選択します。
4. Snapshotポリシーを適用する整合性グループを選択し、*[適用]*を選択します。

次の手順

Snapshotでデータを保護したので"レプリケーション関係を設定する"、バックアップとディザスタリカバリのために、地理的に離れた場所に整合グループをコピーする必要があります。

Snapshotポリシーを編集、削除、または無効にする

Snapshotポリシーを編集して、ポリシー名、Snapshotの最大数、またはSnapMirrorラベルを変更します。ポリシーとそれに関連付けられているバックアップデータをクラスタから削除するには、ポリシーを削除してください。ポリシーで指定されたSnapshotの作成または転送を一時的に停止するには、ポリシーを無効にします。

手順

1. System Managerで、**[保護]>[ポリシー]***を選択し、[Snapshotポリシー]*を選択します。
2. 編集するSnapshotポリシーの名前にカーソルを合わせます。
3. を選択し、編集、削除、または*無効*を選択します。

結果

Snapshotポリシーを変更、削除、または無効にしておきます。

レプリケーションポリシーを編集します。

レプリケーションポリシーを編集して、ポリシーの説明、転送スケジュール、およびルールを変更します。また、ポリシーを編集してネットワーク圧縮を有効または無効にすることもできます。

手順

1. System Managerで、*[保護]>[ポリシー]*を選択します。
2. [レプリケーションポリシー]*を選択します。
3. 編集するレプリケーションポリシーにカーソルを合わせ、を選択します。
4. 「 * 編集 * 」を選択します。
5. ポリシーを更新し、*[保存]*を選択します。

結果

レプリケーションポリシーを変更しておきます。

データセキュリティ

ASA R2ストレージシステム上の保存データの暗号化

保存データを暗号化すると、ストレージメディアの転用、返却、置き忘れ、盗難に際してデータを読み取ることができません。ONTAP System Managerを使用してデータをハードウェアレベルとソフトウェアレベルで暗号化し、デュアルレイヤ保護を実現できます。

NetAppストレージ暗号化（NSE）は、自己暗号化ドライブ（SED）を使用したハードウェア暗号化をサポートしています。SEDはデータを書き込み時に暗号化します。各SEDには一意の暗号化キーが含まれています。SEDに保存されている暗号化されたデータは、SEDの暗号化キーなしでは読み取ることができません。SEDから読み取るノードは、SEDの暗号化キーにアクセスするために認証される必要があります。ノードの認証では、キー管理ツールから認証キーを取得し、その認証キーをSEDに提供します。認証キーが有効な場合、SEDはノードに格納されたデータにアクセスするための暗号化キーをノードに付与します。

ASA R2のオンボードキーマネージャまたは外部キーマネージャを使用して、ノードに認証キーを提供しま

す。

NSEに加えて、ソフトウェア暗号化を有効にしてデータのセキュリティを強化することもできます。

手順

1. System Managerで、*[クラスタ]>[設定]*を選択します。
2. セクションの[暗号化]で、[設定]*を選択します。
3. キー管理ツールを設定します。

オプション	手順
オンボードキーマネージャの設定	a. [オンボードキーマネージャ]*を選択してキーサーバを追加します。 b. パスフレーズを入力します。
外部キー管理ツールを設定する	a. [外部キーマネージャ]*を選択してキーサーバを追加します。 b. + Add キーサーバを追加する場合に選択します。 c. KMIPサーバCA証明書を追加します。 d. KMIPクライアント証明書を追加します。

4. [デュアルレイヤ暗号化]*を選択して、ソフトウェア暗号化を有効にします。
5. [保存（ Save ）] を選択します。

次の手順

保存データの暗号化が完了したので、NVMe/TCPプロトコルを使用している場合は"ネットワーク経由で送信されるすべてのデータを暗号化"、NVMe/TCPホストとASA R2システムの間でデータを暗号化できます。

ASA R2ストレージシステムに対するランサムウェア攻撃からデータを保護

ランサムウェア攻撃に対する保護を強化するには、Snapshotをリモートクラスタにレプリケートし、デスティネーションSnapshotをロックして改ざんを防止します。ロックされたSnapshotは、誤ってまたは悪意を持って削除することはできません。ロックされたSnapshotを使用して、ランサムウェア攻撃によってストレージユニットが侵害された場合にデータをリカバリできます。

SnapLock Complianceクロックの初期化

改ざん防止Snapshotを作成する前に、ローカルクラスタとデスティネーションクラスタでSnapLock Complianceクロックを初期化する必要があります。

手順

1. [*Cluster] > [Overview] を選択します。
2. セクションで、[Initialize SnapLock Compliance Clock]*を選択します。

3. [初期化]*を選択します。
4. コンプライアンスクロックが初期化されていることを確認します。
   a. [*Cluster] > [Overview] を選択します。
   b. セクションでを選択し、 SnapLock Compliance Clock *を選択します。

次の手順

ローカルクラスタとデスティネーションクラスタでSnapLock Complianceクロックを初期化したら、を実行できます"ロックされたSnapshotを使用してレプリケーション関係を作成する"。

ASA R2ストレージシステム上のセキュアなNVMe接続

NVMeプロトコルを使用している場合は、インバンド認証を設定してデータセキュリティを強化できます。インバンド認証を使用すると、NVMeホストとASA R2システムの間でセキュアな双方向認証と一方向認証を確立できます。インバンド認証はすべてのNVMeホストで使用できます。NVMe/TCPプロトコルを使用している場合は、NVMe/TCPホストとASA R2システムの間でネットワーク経由で送信されるすべてのデータを暗号化するようにトランスポートレイヤセキュリティ（TLS）を設定することで、データセキュリティをさらに強化できます。

手順

1. を選択し、[NVMe]*を選択します。
2. を選択します + Add 。
3. ホスト名を入力し、ホストオペレーティングシステムを選択します。
4. ホストの説明を入力し、ホストに接続するStorage VMを選択します。
5. ホスト名の横にあるを選択します。
6. [インバンド認証]*を選択します。
7. NVMe/TCPプロトコルを使用している場合は、*[Transport Layer Security（TLS）が必要]*を選択します。
8. 「 * 追加」を選択します。

結果

インバンド認証やTLSによって、データのセキュリティが強化されます。

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。

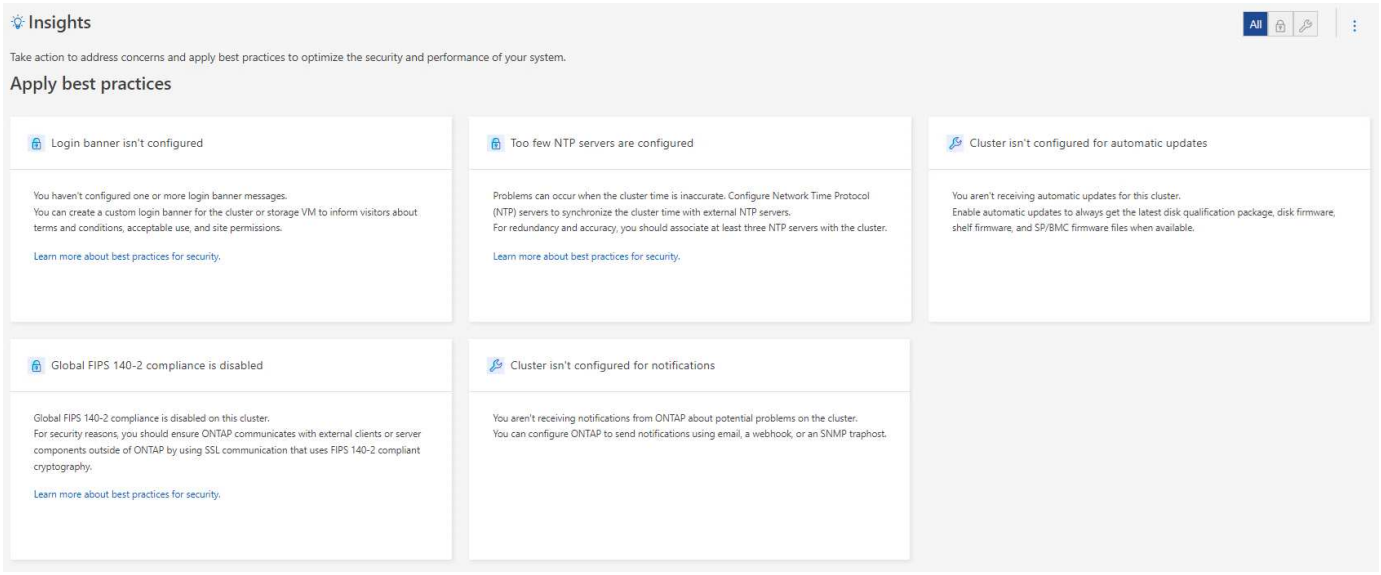
結果

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。

ASA R2ストレージシステムの保守

https://docs.netapp.com/us-en/ontap-systems/asa-r2-landing-maintain/index.html["ASA R2のドキュメントの管理"^]ASA R2システムコンポーネントのメンテナンス手順については、を参照してください。

詳細

ASA R2 for ONTAPパワーユーザ

ASA R2システムを他のONTAPシステムと比較する

ASA R2システムは、オールフラッシュプラットフォーム上に構築されたSAN専用環境向けに、ハードウェアとソフトウェアの統合ソリューションを提供します。ASA R2システムのストレージレイヤ、サポートされるプロトコル、ONTAPパーソナリティの実装において、他のONTAPシステム（ASA、AFF、FAS）とは異なります。

ASA R2システムでは、ONTAPソフトウェアが合理化され、SAN関連以外の機能の可視性と可用性を制限しながら、重要なSAN機能をサポートします。たとえば、ASA R2システムで実行されているSystem Managerには、NASクライアントのホームディレクトリを作成するオプションは表示されません。この合理化されたバージョンのONTAPは、_ASA R2 personality_として識別されます。他のすべてのONTAPシステム（ASA、AFF、FAS）で実行されているONTAPは、_Unified ONTAP personality_として識別されます。ONTAPのパーソナリティの違いについては、ONTAPコマンドリファレンス（マニュアルページ）、REST API仕様、およびEMSメッセージ（該当する場合）を参照してください。

ONTAPストレージのパーソナリティは、System ManagerまたはONTAP CLIを使用して確認できます。

- System Managerのメニューで、*[クラスタ]>[概要]*を選択します。
- CLIから、次のように入力します。 `san config show`

ONTAPストレージシステムのパーソナリティは変更できません。

Unified ONTAPパーソナリティを実行するONTAPシステムのストレージレイヤでは、ストレージのベースユニットとしてアグリゲートが使用されます。アグリゲートは、ストレージシステムで使用可能な特定のディスクセットを所有します。アグリゲートは、自身が所有するディスクのスペースをLUNおよびネームスペース用のボリュームに割り当てます。Unified ONTAPユーザは、コマンドラインインターフェイス（CLI）を使用して、アグリゲート、ボリューム、LUN、ネームスペースを作成および変更できます。

ASA R2システムのストレージレイヤでは、アグリゲートではなくストレージアベイラビリティゾーンを使用します。ストレージアベイラビリティゾーンは、ストレージシステム内の使用可能なすべてのディスクにアクセスできる共通のストレージプールです。ストレージアベイラビリティゾーンは、ASA R2 HAペアの両方のノードから認識できます。ストレージユニット（LUNまたはNVMeネームスペースに基づく）を作成すると、そのストレージユニットを格納するStorage Virtual Machine（VM）を含むボリュームがONTAPのストレージアベイラビリティゾーンに自動的に作成されます。この自動化されたシンプルなストレージ管理アプローチにより、ASA R2システムでは、特定のSystem Managerオプション、ONTAPコマンド、およびREST APIエンドポイントを使用できないか、または使用方法が制限されています。たとえば、ボリュームの作成と管理はASA R2システムで自動化されているため、*[ボリューム]*メニューはSystem Managerに表示されず、 `volume create`コマンドはサポートされません。

ASA R2ストレージは、次の点で他のONTAPストレージシステムと比較されます。

	ASA r2	ASA	AFF	FAS
• ONTAPパーソナリティ*	ASA r2	ASA	統合	統合
• SANプロトコルのサポート*	はい	はい	はい	はい
• NASプロトコルのサポート*	いいえ	いいえ	はい	はい
ストレージ・レイヤーのサポート	ストレエシアベイラビリティソオン	アグリゲート	アグリゲート	アグリゲート

次のASAプラットフォームは、ASA R2システムに分類されます。

- ASA A1K
- ASA A70
- ASA A90

詳細情報

- 詳細については、をご覧ください "ONTAPハードウェアシステム"。
- のASAおよびASA R2システムの構成の完全なサポートと制限事項を参照してください"NetApp Hardware Universe"。
- の詳細については、を"NetApp ASA"参照してください。

ASA R2システムの相違点のまとめ

ASA R2システムと、ONTAP CLI（コマンドラインインターフェイス）およびREST APIに関連するFAS、AFF、およびASAシステムの主な違いを次に示します。

プロトコルサービスを使用したデフォルトの**SVM**作成

新しいクラスタには、SANプロトコルが有効になったデフォルトのデータSVMが自動的に含まれます。IPデータLIFは、iSCSIプロトコルとNVMe/TCPプロトコルをサポートし、 `default-data-blocks`デフォルトでサービスポリシーを使用します。

自動ボリューム作成

ストレージユニット（LUNまたはネームスペース）を作成すると、ストレージのアベイラビリティゾーンからボリュームが自動的に作成されます。これにより、シンプルで共通のネームスペースが実現します。ストレージユニットを削除すると、関連付けられているボリュームも自動的に削除されます。

シンプロビジョニングとシックプロビジョニングに対する変更

のストレージユニットは、常にASA R2ストレージシステム上でシンプロビジョニングされます。シックプロビジョニングはサポートされません。

ASA R2ストレージシステムのONTAPソフトウェアのサポートおよび制限事項

ASA R2システムはSANソリューションを幅広くサポートしていますが、一部のONTAPソフトウェア機能はサポートされていません。

ASA R2システムでは、次の機能はサポートされません。

- iSCSI LIFフェイルオーバー
- FabricPool
- LUNシックプロビジョニング
- MetroCluster
- オブジェクトプロトコル
- ONTAP S3 SnapMirrorとS3 API
- SnapMirrorからクラウドへ
- SnapMirrorからASA R2以外のシステムへ
- 選択的LUNマップ（SLM）

ASA R2システムは、次の機能をサポートしています。

- SnapLock
- デュアルレイヤ暗号化

詳細情報

- "NetApp Hardware Universe"ASA R2ハードウェアのサポートおよび制限事項の詳細については、を参照してください。
- "Snapshotをロックする方法"ASA R2システム。
- "デュアルレイヤ暗号化の適用方法"ASA R2システム上のデータに接続します。

ASA R2ストレージシステムのONTAP CLIサポート

ASA R2システムでは、ストレージシステムで使用可能な特定のディスクセットを所有する従来のアグリゲートの代わりに、_ストレージ可用性ゾーン_を使用します。ストレージアベイラビリティゾーンは、ストレージシステム内の使用可能なすべてのディスクにアクセスできる共通のストレージプールです。ストレージアベイラビリティゾーンは、ASA R2 HAペアの両方のノードから認識できます。ストレージユニット（LUNまたはNVMeネームスペース）を作成すると、ストレージユニットを格納するStorage Virtual Machine（VM）を含むボリュームがONTAPによってストレージアベイラビリティゾーン

に自動的に作成されます。

このようにシンプルなストレージ管理アプローチが採用 `storage aggregate`されているため、ASA R2システムではコマンドはサポートされていません。一部の `lun`volume`コマンドとパラメータのサポートも制限されています。

次のコマンドおよびコマンドセットは、R2上のASAではサポートされていません。

サポートされない**<code> LUN </code>**コマンド

- `lun copy`
- `lun geometry`
- `lun import`
- `lun mapping add-reportng-nodes`
- `lun mapping-remove-reporting-nodes`
- `lun maxsize`
- `lun move`
- `lun move-in-volume`

  このコマンドは、lun rename / vserver nvme namespace renameに置き換えられました。

- `lun transition`

サポートされない**<code> Volume </code>**のコマンドとパラメータ

- `volume autosize`
- `volume create`
- `volume delete`
- `volume expand`
- `volume modify`

  このコマンドは、次のパラメータと組み合わせて使用する場合は使用できません。

  - `-anti-ransomware-state`
  - `-autosize`
  - `-autosize-mode`
  - `-autosize-shrik-threshold-percent`
  - `-autosize-reset`
  - `-group`
  - `-is-cloud-write-enabled`
  - `-is-space-enforcement-logical`
  - `-max-autosize`
  - `-min-autosize`
  - `-offline`
  - `-online`
  - `-percent-snapshot-space`
  - `-qos*`
  - `-size`
  - `-snapshot-policy`
  - `-space-guarantee`
  - `-space-mgmt-try-first`
  - `-state`
  - `-tiering-policy`
  - `-tiering-minimum-cooling-days`
  - `-user`
  - `-unix-permisions`
  - `-vserver-dr-protection`
- `volume make-vsroot`
- `volume mount`

- volume move
- volume offline
- volume rehost
- volume rename
- volume restrict
- volume transition-prepare-to-downgrade
- volume unmount

サポートされない**<code> volume clone </code>**コマンド

- volume clone create
- volume clone split

サポートされない**<code> Volume SnapLock </code>**コマンド

- volume snaplock modify

サポートされない**<code> volume snapshot </code>**コマンド

- volume snapshot
- volume snapshot autodelete modify
- volume snapshot policy modify

サポートされない**<code> Volume </code>**コマンドセット

- `volume activity-tracking`
- `volume analytics`
- `volume conversion`
- `volume file`
- `volume flexcache`
- `volume flexgroup`
- `volume inode-upgrade`
- `volume object-store`
- `volume qtree`
- `volume quota`
- `volume reallocation`
- `volume rebalance`
- `volume recovery-queue`
- `volume schedule-style`

サポートされない**<code> storage </code>**コマンド

- `storage failover show-takeover`
- `storage failover show-giveback`
- `storage aggregate relocation`
- `storage disk assign`
- `storage disk partition`
- `storage disk reassign`

詳細情報

"ONTAPコマンド リファレンス"サポートされるコマンドの一覧については、を参照してください。

CLIを使用したONTAP ASA R2クラスタのセットアップ

お勧め"System Managerを使用してONTAP ASA R2クラスタをセットアップする"ます。System Managerには、クラスタの運用を迅速かつ簡単に開始できるガイド付きワークフローが用意されています。ただし、ONTAPコマンドを使い慣れている場合は、クラスタのセットアップにONTAPのコマンドラインインターフェイス（CLI）を使用することもできます。CLIを使用したクラスタセットアップには、System Managerを使用したクラスタセットアップに比べて追加のオプションや利点はありません。

クラスタのセットアップ時に、デフォルトのデータStorage Virtual Machine（VM）が作成され、初期ストレージユニットが作成され、データLIFが自動的に検出されます。必要に応じて、Domain Name System（DNS；ドメインネームシステム）を有効にしてホスト名を解決したり、Network Time Protocol（NTS；ネットワー

クタイムプロトコル）を使用して時刻を同期するようにクラスタを設定したり、保存データの暗号化を有効にしたりできます。

開始する前に

次の情報を収集します。

- クラスタ管理 IP アドレス

  クラスタ管理IPアドレスは、クラスタ管理インターフェイスの一意のIPv4アドレスです。クラスタ管理者は、管理Storage VMへのアクセスとクラスタの管理に使用します。このIPアドレスは、組織でIPアドレスを割り当てる管理者から取得できます。

- ネットワークサブネットマスク

  ONTAPでは、クラスタのセットアップ時に、ご使用の構成に適した一連のネットワークインターフェイスを推奨します。必要に応じて推奨構成を調整できます。

- ネットワークゲートウェイのIPアドレス
- パートナーノードのIPアドレス
- DNSドメイン名
- DNSネームサーバのIPアドレス
- NTPサーバのIPアドレス
- データサブネットマスク

手順

1. HAペアの両方のノードの電源をオンにします。
2. ローカルネットワークで検出されたノードを表示します。

   ```
   system node show-discovered -is-in-cluster false
   ```

3. クラスタセットアップウィザードを開始します。

   ```
   cluster setup
   ```

4. AutoSupportステートメントを確認します。
5. ノード管理インターフェイスのポート、IPアドレス、ネットマスク、およびデフォルトゲートウェイの値を入力します。
6. コマンドラインインターフェイスを使用してセットアップを続行する場合は* Enter を押し、新しいクラスタを作成する場合は create *と入力します。
7. システムのデフォルトを受け入れるか、独自の値を入力します。
8. 1つ目のノードでのセットアップが完了したら、クラスタにログインします。
9. クラスタがアクティブで、第1ノードが正常であることを確認します。

```
system node show-discovered
```

10. クラスタに2つ目のノードを追加します。

```
cluster add-node -cluster-ip <partner_node_ip_address>
```

11. 必要に応じて、クラスタ全体のシステム時間を同期します。

対称認証を使用しない同期	`cluster time-service ntp server create -server <server_name>`
対称認証と同期	`cluster time-service ntp server create -server <server_ip_address> -key-id <key_id>`

a. クラスタがNTPサーバに関連付けられていることを確認します。

```
Cluster time-service ntp show
```

12. 必要に応じて、をダウンロードしてを実行し、"ActiveIQ Config Advisor"設定を確認します。

次の手順

これで、"データアクセスのセットアップ"SANクライアントからシステムに接続する準備が整いました。

ASA R2のREST APIサポート

ASA R2 REST APIは、Unified ONTAPパーソナリティで提供されるREST APIに基づいており、ASA R2パーソナリティの固有の特性と機能に合わせていくつかの変更が加えられています。

APIの変更の種類

ASA R2システムREST APIと、FAS、AFF、およびASAシステムで使用できるUnified ONTAP REST APIには、いくつかの違いがあります。変更の種類を理解することで、オンラインのAPIリファレンスドキュメントをより有効に活用できます。

Unified ONTAPでサポートされない新しいASA R2エンドポイント

ASA R2 REST APIには、Unified ONTAPでは使用できないエンドポイントがいくつか追加されています。

たとえば、ASA R2システムのREST APIには、新しいブロックボリュームエンドポイントが追加されています。ブロックボリュームエンドポイントは、LUNネームスペースオブジェクトとNVMeネームスペースオブジェクトの両方にアクセスし、リソースをまとめて表示できるようにします。これはREST APIでのみ使用できます。

別の例として、* storage-units *エンドポイントは、LUNおよびNVMeネームスペースの集計ビューを提供します。いくつかのエンドポイントがあり、それらはすべてベースまたは派生元 `/api/storage/storage-units`です。 `/api/storage/luns`およびも確認する必要があります `/api/storage/namespaces。

一部のエンドポイントで使用される**HTTP**メソッドの制限

ASA R2で使用できるいくつかのエンドポイントには、Unified ONTAPと比較して使用できるHTTPメソッドが制限されています。たとえば `/api/protocols/nvme/services`、ASA R2システムでエンドポイントを使用する場合、POSTとDELETEは実行できません。

エンドポイントと**HTTP**メソッドのプロパティの変更

一部のASA R2システムエンドポイントとメソッドの組み合わせでは、Unified ONTAP Personalityで使用可能な定義済みプロパティの一部がサポートされていません。たとえば、エンドポイントでPATCHを使用する場合、 `/api/storage/volumes/{uuid}`ASA R2では次のようないくつかのプロパティがサポートされません。

- `autosize.maximum`
- `autosize.minimum`
- `autosize.mode`

内部処理の変更

ASA R2での特定のREST API要求の処理方法にいくつかの変更があります。たとえば、エンドポイントの削除要求 `/api/storage/luns/{uuid}`は非同期で処理されます。

OAuth 2.0によるセキュリティの強化

OAuth 2.0は業界標準の認可フレームワークです。署名されたアクセストークンに基づいて、保護されたリソースへのアクセスを制限および制御するために使用されます。ASA R2システムリソースを保護するために、System Managerを使用してOAuth 2.0を設定できます。

System ManagerでOAuth 2.0をセットアップすると、REST APIクライアントによるアクセスを制御できます。まず、認可サーバーからアクセストークンを取得する必要があります。RESTクライアントは、認証要求ヘッダーを使用して、そのトークンをベアラトークンとしてASA R2クラスタに渡します。詳細については、を参照してください "OAuth 2.0を使用した認証と許可" 。

Swagger UIから**ASA R2 API**のリファレンスドキュメントにアクセス

REST APIのリファレンスドキュメントには、ASA R2システムのSwagger UIからアクセスできます。

タスクの内容

ASA R2のリファレンスドキュメントページにアクセスして、REST APIの詳細を確認してください。その一環として、文字列* Platform Specifications *を検索して、ASA R2システムでのAPI呼び出しとプロパティのサポートに関する詳細を確認できます。

開始する前に

次の情報が必要です。

- ASA R2システムのクラスタ管理LIFのIPアドレスまたはホスト名
- REST APIにアクセスする権限を持つアカウントのユーザ名とパスワード

手順

1. ブラウザにURLを入力し、* Enter *：+を押します。
   `https://<ip_address>/docs/api`
2. 管理者アカウントを使用してサインインします。

   ASA R2 APIドキュメントページが表示され、主要なリソースカテゴリ別に分類されたAPI呼び出しが表示されます。

3. ASA R2システムのみに該当するAPI呼び出しの例を確認するには、* SAN カテゴリまで下にスクロールし、[GET /storage/storage-units]*をクリックします。

ヘルプを表示します

ASA R2ストレージシステム上のAutoSupportを管理します。

AutoSupportは、システムヘルスをプロアクティブに監視し、NetApp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するメカニズムです。

テクニカルサポートへのAutoSupportメッセージは、クラスタのセットアップ時にデフォルトで有効になります。メッセージを社内のサポート部門に送信するには、正しい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。ONTAPは、有効になってから24時間後にAutoSupportメッセージの送信を開始します。

開始する前に

AutoSupportを管理するには、クラスタ管理者である必要があります。

AutoSupport接続のテスト

クラスタのセットアップが完了したら、AutoSupport接続をテストして、テクニカルサポートがAutoSupportによって生成されたメッセージを受信することを確認する必要があります。

手順

1. System Managerで、*[クラスタ]>[設定]*を選択します。
2. AutoSupport の横にある*を選択し、 Test connectivity *を選択します。
3. AutoSupportメッセージの件名を入力し、* Send test AutoSupport message *を選択します。

次の手順

は、テクニカルサポートがASA R2システムからAutoSupportメッセージを受信できること、および問題が発生した場合のサポートに必要なデータを提供できることを確認しています。

AutoSupport受信者の追加

社内のサポート部門のメンバーを、AutoSupportメッセージを受信するEメールアドレスのリストに追加します。

手順

1. System Managerで、*[クラスタ]>[設定]*を選択します。
2. AutoSupport の横にある*を選択し、 More options *を選択します。
3. [Eメール]*の横にあるを選択し、を選択します Add 。
4. 受信者のEメールアドレスを入力し、次に受信者カテゴリを入力します。

   パートナーの場合は、受信者カテゴリとして*パートナー*を選択します。社内のサポート組織のメンバーには、*[全般]*を選択します。

5. 保存を選択します。

次の手順

追加したメールアドレスには、特定の受信者カテゴリの新しいAutoSupportメッセージが送信されます。

AutoSupportデータの送信

ASA R2システムで問題が発生した場合、AutoSupportデータを使用すると、問題の特定と解決にかかる時間が大幅に短縮されます。

手順

1. System Managerで、*[クラスタ]>[設定]*を選択します。
2. AutoSupport の横にある*を選択し、 Generate and send *を選択します。
3. AutoSupportメッセージの件名を入力し、*送信*を選択します。

次の手順

AutoSupportデータがテクニカルサポートに送信されます。

サポートケースの生成を抑制

ASA R2システムでアップグレードまたはメンテナンスを実行する場合は、アップグレードまたはメンテナンスが完了するまでAutoSupportでサポートケースが生成されないようにすることができます。

手順

1. System Managerで、*[クラスタ]>[設定]*を選択します。
2. AutoSupport の横にある*を選択し、 Suppress support case generation *を選択します。
3. サポートケースが生成されないようにする時間数を指定してから、ケースを生成しないノードを選択してください。
4. 「*送信」を選択します。

次の手順

指定した時間内はAutoSupportケースは生成されません。指定した時間が経過する前にアップグレードまたはメンテナンスが完了した場合は、サポートケースの生成をただちに再開する必要があります。

サポートケースの生成を再開

アップグレードまたはメンテナンス期間中にサポートケースが生成されないようにした場合は、アップグレードまたはメンテナンスの完了後すぐにサポートケースの生成を再開する必要があります。

手順

1. System Managerで、*[クラスタ]>[設定]*を選択します。
2. AutoSupport の横にある*を選択し、 Resume support case generation *を選択します。
3. 生成されたAutoSupportケースを再開するノードを選択します。
4. 「*送信」を選択します。

結果

ASA R2システムのAutoSupportケースは、必要に応じて自動生成されます。

ASA R2ストレージシステムのサポートケースの送信と確認

サポートが必要な問題が発生した場合は、ONTAPシステムマネージャを使用してテクニカルサポートにケースを送信できます。ONTAPシステムマネージャを使用して、完了したケースや進行中のケースを確認することもできます。

"Active IQに登録済み"ASA R2システムのサポートケースを表示する必要があります。

手順

1. サポートケースを送信するには、System Managerで*[クラスタ]>[サポート]を選択し、[Go to NetApp Support]*を選択します。
2. 以前に送信されたケースを表示するには、System Managerで*[クラスタ]>[サポート]を選択し、[ケースを表示]*を選択します。

法的通知

法的通知では、著作権に関する声明、商標、特許などにアクセスできます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp、NetAppのロゴ、およびNetAppの商標ページに記載されているマークは、NetApp、Inc.の商標です。その他の会社名および製品名は、それを所有する各社の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

NetAppが所有する特許の最新リストは、次のサイトで参照できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。