



クラスターを管理する AFX

NetApp
February 11, 2026

目次

クラスターを管理する	1
クラスタプロセスを監視する	1
AFXストレージシステムのダッシュボードを表示する	1
AFX ストレージ システムを最適化するための分析情報を表示します	1
AFX ストレージ システム クラスターのパフォーマンスを監視する	2
AFX ストレージ システムのイベントと監査ログを表示する	2
AFXストレージシステムのジョブを表示	3
ネットワークとセキュリティを管理する	4
AFXストレージシステムクラスタネットワークを管理する	4
AFXストレージシステムのイーサネットポートを管理する	6
AFXストレージシステム認証サービスの準備	7
AFX ストレージ システム クラスターのユーザーとロールを管理する	8
AFX ストレージ システム上の証明書を管理する	10
ストレージVMの管理	12
AFXストレージシステムのSVMを表示する	12
AFXストレージシステムSVMを作成する	12
AFXストレージシステムSVMを構成する	13
AFXストレージシステムSVMの移行	14
クラスターをサポートする	15
AFXストレージシステムクラスタのAutoSupportを管理する	15
AFX ストレージ システムのサポート ケースを送信して表示する	17
クラスターのアップグレードとメンテナンス	18
AFXストレージシステムクラスターを拡張する	18
AFXストレージシステム上のONTAPのアップグレード	21
AFXストレージシステムのファームウェアを更新する	21
ONTAP の復帰はAFX ストレージ システムではサポートされません	23
AFX ストレージ システム クラスターの追加管理	23
ライセンス	23
セキュリティ	24
関連情報	24

クラスターを管理する

クラスタプロセスを監視する

AFXストレージシステムのダッシュボードを表示する

System Manager にサインインして AFX ダッシュボードにアクセスし、クラスターのステータスを表示できます。これは、AFX 管理タスクを開始する前、または運用上の問題が疑われる場合に実行する最初のステップとして適しています。

開始する前に

次のものが必要になります:

- クラスタ管理LIFのIPアドレスまたはドメイン名
- 管理者アカウントの資格情報

手順

1. ブラウザとクラスタ管理 IP アドレスを使用して System Manager に接続します。

```
https://$FQDN_IPADDR/
```

例

```
https://10.61.25.33/
```

2. 管理者アカウントのユーザー名とパスワードを入力し、「**Sign in**」を選択します。
3. 左側のナビゲーション ペインで **ダッシュボード** を選択し、クラスターの 正常性 を含むページのタイルを確認します。
4. ナビゲーション ペインで、クラスター を選択し、次に **概要** を選択します。
5. クラスタ名、バージョン、ONTAPパーソナリティ、その他の詳細を確認します。
6. 概要ページの上部にある **Cabling** を選択すると、クラスターのハードウェアと接続が視覚的に表示されます。
7. ナビゲーション ペインで、イベントとジョブ を選択し、次に システム アラート を選択して、システムアラートを表示して確認します。

AFX ストレージ システムを最適化するための分析情報を表示します

ONTAP System Manager の *Insights* 機能を使用すると、NetApp のベスト プラクティスに沿った推奨構成更新を表示できます。これらの変更により、AFX クラスターのセキュリティとパフォーマンスを最適化できます。

たとえば、AFX では自律ランサムウェア保護 (ARP) 機能が利用可能であり、ランサムウェア対策保護を提供します。ARP が設定されていない場合、Insights から通知されます。

タスク概要

各分析情報はページ上で個別のタイルまたはカードとして表示され、実装するか無視するかを選択できます。特定のテクノロジーについて詳しく知るには、関連するドキュメント リンクを選択することもできます。

手順

1. システム マネージャーで、分析 を選択し、次に インサイト を選択します。
2. 利用可能な推奨事項を確認します。

次の手順

AFX 構成のベスト プラクティスを実装するには、推奨されるアクションのいずれかを実行します。

AFX ストレージ システム クラスターのパフォーマンスを監視する

AFX クラスターのパフォーマンスの概要を表示できます。

ストレージ容量

System Manager ダッシュボードには、クラスターのストレージ使用率の概要が表示されます。

手順

1. システム マネージャーのナビゲーション ペインで、ダッシュボード を選択します。
2. *容量*タイルを見つけて、使用可能および使用済みの物理ストレージを表示します。
3. 履歴データを表示するには、「履歴」を選択してActive IQにアクセスします。

クラスター パフォーマンス

System Manager は、AFX クラスターのパフォーマンスの詳細な概要を提供します。

手順

1. システム マネージャーで、[分析] を選択し、[パフォーマンス] を選択します。
2. レイテンシやスループットを含む、上部のクラスター パフォーマンスの概要を確認します。
3. *トップアクター*タブで、目的の SVM を選択し、必要に応じて*アクティビティ追跡を有効にする*をクリックします。
4. ボリューム パフォーマンス タブで、特定のボリュームのパフォーマンスの詳細を表示します。

関連情報

- ["追加のAFXクラスター管理"](#)

AFX ストレージ システムのイベントと監査ログを表示する

AFX によって生成されたイベントと監査ログ メッセージを確認して、内部処理を追跡し、潜在的な問題を診断できます。AFX システムは、この情報を他の関連データとともに転送し、追加の処理やアーカイブを行うように構成できます。

イベント

イベント メッセージは、システム アクティビティの貴重な記録を提供します。各イベントには、説明と一意の識別子、および推奨されるアクションが含まれます。

1. システム マネージャーで、イベントとジョブ を選択し、次に イベント を選択します。
2. 自動更新を有効にするなど、ページの上部にある推奨アクションを確認して対応します。
3. イベント ログ タブを選択して、メッセージのリストを表示します。
4. イベント メッセージを選択すると、シーケンス番号、説明、イベント、推奨アクションなどの詳細を確認できます。
5. 必要に応じて、「* Active IQ の提案*」タブを選択し、Active IQに登録して、クラスターの詳細なリスク情報を取得します。

監査ログ


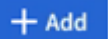
監査ログには、HTTP などのアクセス プロトコルの使用に基づくシステム アクティビティの記録が含まれます。

1. システム マネージャーで、イベントとジョブ を選択し、次に 監査ログ を選択します。
2. 追跡される操作を有効または無効にするには、[設定] を選択します。
3. オプションで*監査先の管理*を選択し、確認します。[\[通知の管理\]](#)詳細についてはこちらをご覧ください。

通知の管理

AFX では転送できる通知の種類がいくつかあります。

手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. *通知管理*に移動して選択.
3. AFX で使用される宛先を表示または構成するには、適切なアクションを選択します。たとえば、次のように構成します。
 - a. イベントの目的地: *イベントの目的地を表示*を選択します
 - b. 監査ログの保存先: *監査ログの保存先を表示*を選択します
4. 選択  必要に応じて、宛先情報を入力します。
5. *保存*を選択します。

関連情報

- ["ONTAPイベント、パフォーマンス、ヘルスモニタリング"](#)

AFXストレージシステムのジョブを表示

AFX には、構成と管理アクションに基づいてバックグラウンド ジョブを実行するための内部プラットフォームが含まれています。これらのジョブは、長時間実行される AFX コンポーネント、または管理タスクや REST API 要求に応じて実行される短時間のプロセスである可能性があります。必要に応じてジョブを表示および監視できます。

手順

1. システム マネージャーで、[イベントとジョブ] を選択し、[ジョブ] を選択します。
2. 必要に応じて、表示をカスタマイズしたり、求人情報を検索したりダウンロードしたりできます。

ネットワークとセキュリティを管理する

AFXストレージシステムクラスタネットワークを管理する

AFX ストレージ システムのネットワークを構成する必要があります。ネットワーク環境は、SVM のデータにアクセスするクライアントやクラスタ間通信など、いくつかのシナリオをサポートします。



ネットワーク リソースを作成することは重要な最初のステップです。必要に応じて、ネットワーク定義の編集や削除などの追加の管理アクションも実行する必要があります。

ブロードキャスト ドメインの作成

ブロードキャスト ドメインは、同じレイヤー 2 ネットワークの一部であるポートをグループ化することで、クラスタ ネットワークの管理を簡素化します。その後、ストレージ仮想マシン (SVM) に、データまたは管理トラフィック用のグループ内のポートを割り当てることができます。

クラスタのセットアップ中に、次のようないくつかのブロードキャスト ドメインが作成されます。

デフォルト

このブロードキャスト ドメインには、「デフォルト」 IP スペース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含まれます。

クラスタ

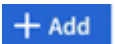
このブロードキャスト ドメインには、「クラスタ」 IP スペース内のポートが含まれます。これらのポートはクラスタ通信に使用され、クラスタ内のすべてのノードのすべてのクラスタ ポートが含まれます。

クラスタが初期化された後、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。

タスク概要

ブロードキャスト ドメインに定義されたポートの最大転送単位 (MTU) 値は、ブロードキャスト ドメインで設定された MTU 値に更新されます。

手順

1. システム マネージャーで、[ネットワーク] を選択し、[概要] を選択します。
2. *ブロードキャストドメイン*の下で、 **+ Add**。
3. ブロードキャスト ドメインの名前を入力するか、デフォルトを受け入れます。

どのブロードキャスト ドメイン名もIPspace内で固有でなければなりません。

4. 最大転送単位 (MTU) を指定します。

MTU は、ブロードキャスト ドメインで受け入れることができる最大のデータ パケットです。

5. 必要なポートを選択し、[保存] を選択します。

IPスペースを作成する

IPspace は、IP アドレスと関連するネットワーク構成の管理ドメインです。これらのスペースは、分離された管理とルーティングを通じて SVM をサポートするために使用できます。たとえば、クライアントが同じ IP アドレスとサブネット範囲から重複した IP アドレスを持っている場合に役立ちます。



サブネットを作成するには、IPspace が必要です。

手順

1. システム マネージャーで、[ネットワーク] を選択し、[概要] を選択します。
2. *IPspaces*の下で、 **+ Add**。
3. IPspace の名前を入力するか、デフォルトを受け入れます。

すべての IPspace 名はクラスター内で一意である必要があります。

4. *保存*を選択します。

次の手順

IPspace 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

サブネットワークまたはサブネットは、ネットワーク内の IP アドレス空間の論理的な分割を強制します。これにより、ネットワーク インターフェイス (LIF) の作成用に専用の IP アドレス 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、特定の IP アドレスとネットワーク マスクの組み合わせの代わりにサブネット名を使用できるため、LIF の作成が簡素化されます。

開始する前に

サブネットを定義するブロードキャスト ドメインと IPspace が必要です。また、次の点にも注意してください。

- すべてのサブネット名は、特定の IPspace 内で一意である必要があります。
- サブネットに使用される IP アドレス範囲は、他のサブネットの IP アドレスと重複することはできません。

手順

1. システム マネージャーで、[ネットワーク] を選択し、[概要] を選択します。
2. *サブネット*タブで、 **+ Add**。
3. サブネットの名前、IP アドレスの詳細、ブロードキャスト ドメインなどの構成の詳細を提供します。
4. *保存*を選択します。

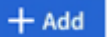
次の手順

新しいサブネットにより、ネットワーク インターフェイスの作成が簡素化されます。

ネットワークインターフェースを作成する

論理ネットワーク インターフェイス (LIF) は、IP アドレスと関連するネットワーク構成パラメータで構成されます。これは物理ポートまたは論理ポートに関連付けることができ、通常はクライアントが SVM によって提供されるデータにアクセスするために使用されます。LIF は障害発生時に回復力を提供し、ノード ポート間で移行できるため、通信が中断されることはありません。

手順

1. システム マネージャーで、[ネットワーク] を選択し、[概要] を選択します。
2. *ネットワークインターフェース*タブで、 **+ Add**。
3. インターフェイスの名前、インターフェイスの種類、許可されるプロトコル、IP アドレスの詳細などの構成の詳細を提供します。
4. *保存*を選択します。

関連情報

- ["AFXイーサネットポートを管理する"](#)
- ["ONTAPブロードキャストドメインについて学ぶ"](#)
- ["ONTAP IPspace構成について学ぶ"](#)
- ["ONTAPネットワークのサブネットについて学ぶ"](#)
- ["ネットワーク アーキテクチャ - 概要"](#)

AFXストレージシステムのイーサネットポートを管理する

AFX システムで使用されるポートは、ネットワーク接続と通信の基盤を提供します。ネットワークのレイヤー 2 構成をカスタマイズするには、いくつかのオプションがあります。

VLANの作成

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、セキュリティを強化し、潜在的な問題を分離し、IP ネットワーク インフラストラクチャ内で利用可能なパスを制限することができます。

開始する前に

ネットワーク上に配置されたスイッチが、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。

タスク概要

次の点に注意してください。

- メンバー ポートが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。
- VLANを初めてポートに設定したときに、ポートが停止してネットワーク接続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を追加するときは、この問題は発生しません。

- スwitch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に割り当てられている場合、そのインターフェイス上にVLAN e0b-10を作成しないでください。

手順

1. システム マネージャーで、ネットワーク を選択し、次に イーサネット ポート を選択します。
2. 選択 **+ VLAN**。
3. 必要なノード全体の ID、ブロードキャスト ドメイン、ポートなどの構成の詳細を指定します。

VLAN は、クラスタ LIF をホストするポート、またはクラスタ IPspace に割り当てられたポートには接続できません。

4. ***保存***を選択します。

結果

セキュリティを強化し、問題を分離し、IP ネットワーク インフラストラクチャ内で使用可能なパスを制限するために、VLAN を作成しました。

LAGの作成

リンク アグリゲート グループ (LAG) は、複数の物理ネットワーク接続を 1 つの論理接続に結合する技術です。これを使用すると、帯域幅を増やし、ノード間の冗長性を実現できます。

手順

1. システム マネージャーで、ネットワーク を選択し、次に イーサネット ポート を選択します。
2. ***リンク集約グループ***を選択します。
3. ノード、ブロードキャスト ドメイン、ポート、モード、負荷分散などの構成の詳細を提供します。
4. ***保存***を選択します。

関連情報

- ["AFX クラスタ ネットワークを管理する"](#)
- ["ONTAPネットワークポート構成について学ぶ"](#)
- ["物理ポートを組み合わせるONTAPインターフェースグループを作成する"](#)

AFXストレージシステム認証サービスの準備

AFX システムで使用される認証および承認サービスを、ユーザー アカウントとロールの定義に準備する必要があります。



LDAPの設定

認証情報を中央の場所で管理するように、Lightweight Directory Access Protocol (LDAP) サーバーを構成できます。

開始する前に

証明書署名要求を生成し、CA 署名付きサーバーデジタル証明書を追加する必要があります。

手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. 選択  **LDAP** の横にあります。
3. 選択  **Add** LDAP サーバーの名前または IP アドレスを入力します。
4. スキーマ、ベース DN、ポート、バインディングなどの必要な構成情報を提供します。
5. *保存*を選択します。


SAML 認証の設定

セキュリティアサーションマークアップ言語 (SAML) 認証を使用すると、LDAP などの他のプロトコルを使用するプロバイダーではなく、安全な ID プロバイダー (IdP) によってユーザーを認証できるようになります。

開始する前に

- リモート認証に使用する予定の ID プロバイダーを構成する必要があります。構成の詳細については、プロバイダーのドキュメントを参照してください。
- アイデンティティプロバイダーの URI が必要です。

手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. 選択  *セキュリティ* の下の *SAML 認証* の横にあります。
3. *SAML 認証を有効にする* を選択します。
4. **IdP 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。

確認画面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 メタデータを更新します。
6. システム マネージャーの確認ウィンドウに戻り、*ホスト URI またはメタデータを使用して IdP を構成しました* を選択します。
7. SAML ベースの認証を有効にするには、[ログアウト] を選択します。

IdP システムの認証画面が表示されます。

関連情報

- ["AFX クラスターのユーザーとロールを管理する"](#)
- ["リモート ONTAP ユーザーの SAML 認証を構成する"](#)
- ["認証とアクセス制御"](#)

AFX ストレージ システム クラスターのユーザーとロールを管理する

AFX で利用可能な認証および承認サービスに基づいて、ユーザー アカウントとロールを

定義できます。



各ONTAPユーザーには1つのロールを割り当てる必要があります。ロールには権限が含まれており、ユーザーが実行できるアクションを決定します。

アカウントロールを作成する

AFX クラスターがセットアップされ初期化されると、クラスター管理者とストレージ VM 管理者のロールが自動的に作成されます。追加のユーザー アカウント ロールを作成して、ロールに割り当てられたユーザーがクラスターで実行できる特定の機能を定義できます。

手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. *セキュリティ*セクションの*ユーザーとロール*の横にある ➔。
3. *役割*の下で選択 **+ Add**。
4. ロールの名前と属性を指定します。
5. *保存*を選択します。

クラスターアカウントを作成する

クラスターまたは SVM の管理を実行するときに使用するクラスターレベルのアカウントを作成できます。

手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. *セキュリティ*セクションで、 ➔ *ユーザーとロール*の横。
3. 選択 **+ Add** *ユーザー*の下。
4. ユーザー名を入力し、ユーザーの役割を選択します。

役割はユーザーに適したものでなければなりません。たとえば、**admin** ロールは、クラスター上であらゆる範囲の構成タスクを実行できます。

5. ユーザーのログイン方法と認証方法を選択します。通常は「パスワード」になります。
6. ユーザーのパスワードを入力します。
7. *保存*を選択します。

結果

新しいアカウントが作成され、AFX クラスターで使えるようになります。

関連情報

- ["認証サービスの準備"](#)
- ["追加のAFX SVM管理"](#)



AFX ストレージ システム上の証明書を管理する

環境に応じて、AFX の管理の一環としてデジタル証明書を作成および管理する必要があります。実行できる関連タスクがいくつかあります。

証明書署名要求の生成

デジタル証明書の使用を開始するには、証明書署名要求 (CSR) を生成する必要があります。CSR は、証明機関 (CA) から署名付き証明書を要求するために使用されます。この一環として、ONTAP は公開キーと秘密キーのペアを作成し、公開キーを CSR に含めます。

手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. *セキュリティ*の下での*証明書*の横にある →
3. 選択 。
4. サブジェクトの共通名と国を指定します。オプションで組織と組織単位を指定します。
5. 証明書を定義するデフォルト値を変更するには、 [More options](#) 必要な更新を行います。
6. *生成*を選択します。


結果

公開鍵証明書を要求するために使用できる CSR を生成しました。

信頼できる証明機関を追加する

ONTAP は、トランスポート層セキュリティ (TLS) やその他のプロトコルで使用するための、信頼できるルート証明書のデフォルト セットを提供します。必要に応じて、信頼できる証明機関を追加できます。

手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. *セキュリティ*の下での*証明書*の横にある →。
3. *信頼された証明機関*タブを選択し、。
4. 名前、スコープ、共通名、タイプ、証明書の詳細などの構成情報を指定します。代わりに、[インポート] を選択して証明書をインポートすることもできます。
5. *追加*を選択します。

結果

信頼できる証明機関を AFX システムに追加しました。

信頼できる証明機関を更新または削除する

信頼できる証明機関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たくない場合は、削除する必要があります。

手順

1. *クラスター*を選択し、次に*設定*を選択します。

2. *セキュリティ*の下に*証明書*の横にある →。
3. *信頼された証明機関*タブを選択します。
4. 更新または削除する信頼証明機関を選択します。
5. 証明機関を更新または削除します。

証明機関を更新するには、次の手順を実行します。	証明機関を削除するには、次の手順を実行します。
a. 選択: 次に*更新*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. 選択: 次に、[削除]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

AFX システム上の既存の信頼された証明機関を更新または削除しました。

クライアント/サーバー証明書またはローカル証明機関を追加する

安全な Web サービスの有効化の一環として、クライアント/サーバー証明書またはローカル証明機関を追加できます。

手順

1. システム マネージャーで、[クラスター]を選択し、[設定]を選択します。
2. *セキュリティ*の下に*証明書*の横にある →。
3. 必要に応じて、*クライアント/サーバー証明書*または*ローカル証明機関*のいずれかを選択します。
4. 証明書情報を追加し、[保存]を選択します。

結果



新しいクライアント/サーバー証明書またはローカル認証局を AFX システムに追加しました。

クライアント/サーバー証明書またはローカル証明機関を更新または削除する

クライアント/サーバー証明書とローカル証明機関は毎年更新する必要があります。期限切れの証明書またはローカル証明機関を更新しない場合は、それらを削除する必要があります。

手順

1. *クラスター*を選択し、次に*設定*を選択します。
2. *セキュリティ*の下に*証明書*の横にある →。
3. 必要に応じて、*クライアント/サーバー証明書*または*ローカル証明機関*のいずれかを選択します。
4. 更新または削除する証明書を選択します。
5. 証明機関を更新または削除します。

証明機関を更新するには、次の手順を実行します。	証明機関を削除するには、次の手順を実行します。
a. 選択  次に*更新*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。	選択  次に、[削除] を選択します。

結果

AFX システム上の既存のクライアント/サーバー証明書またはローカル証明機関を更新または削除しました。

関連情報


- ["ONTAPでCA署名サーバ証明書を生成してインストールする"](#)
- ["System ManagerでONTAP証明書を管理する"](#)

ストレージVMの管理

AFXストレージシステムのSVMを表示する

AFX クラスターで定義されているデータ ストレージ VM を表示できます。各 SVM は、データを整理し、クライアント アクセスを提供するための分離された環境を提供します。

手順

1. システム マネージャーで、クラスター を選択し、次に ストレージ **VM** を選択します。
2. 希望するSVMにマウスを移動して選択  SVM の起動と停止を含む主要な管理オプションを表示します。
3. 必要に応じて特定の SVM を選択し、概要、設定、レプリケーション、ファイル システムなどの詳細を表示します。

関連情報

- ["AFXシステムSVMを構成する"](#)
- ["ストレージ仮想マシンを理解する"](#)

AFXストレージシステムSVMを作成する

SVM を作成すると、分離を実現し、セキュリティを強化できます。組織内のさまざまなグループやプロジェクトに対してこれを実行できます。

タスク概要

SVM を作成するときは、名前を指定し、クライアント アクセス用のプロトコルを少なくとも 1 つ設定する必要があります。クライアント プロトコルを選択すると、ネットワーク構成も求められます。SVM 構成は、作成後に必要に応じて変更できます。

開始する前に

次のものが必要になります:

- 最低4つのIPアドレス
- IPスペースの名前

手順

1. システム マネージャーで、クラスター を選択し、次に ストレージ **VM** を選択します。
2. 選択 **+ Add** 。
3. SVM の名前を指定します。
4. クライアント アクセスのプロトコルを選択し、必要に応じて構成の詳細を指定します。
5. IP アドレスとサブネット マスクを含む SVM のネットワーク インターフェイスを追加します。
6. ストレージ **VM** 管理 で、オプションとして次の操作を実行します。
 - a. 最大容量を有効にして値を選択する
 - b. SVMの管理者アカウントを管理する
7. *保存*を選択します。

関連情報

- ["AFXシステムSVMを構成する"](#)
- ["AFX システム クラスター ネットワークを管理する"](#)

AFXストレージシステム**SVM**を構成する

SVM を作成した後、要件とクライアントのニーズに基づいて構成を更新できます。

タスク概要

特定の SVM のランディング ページのタブに反映されているように、SVM 構成へのアクセス パスは 4 つあります。これらには次のものが含まれます。

• 概要

これにより、ネットワーク インターフェイスとサービス、プロトコル、ストレージ、保護に関連する現在の構成の詳細の概要をダッシュボードに簡単に表示できます。

• 設定

プロトコル、サービス、ポリシー、セキュリティなどの複数の領域に整理された SVM 構成全体にアクセスして更新できます。

• レプリケーション

このページには、SVM に定義されている現在のレプリケーション関係のリストが表示されます。

• ファイルシステム

SVMのアクティビティと分析を追跡できます

開始する前に

表示および更新する SVM を決定する必要があります。

手順

1. システム マネージャーで、クラスター を選択し、次に ストレージ **VM** を選択します。
2. 目的の SVM を選択し、[設定] タブを選択します。
3. ページ上の構成オプションを確認し、必要に応じて設定を選択して更新します。

AFXストレージシステムSVMの移行

SVM を 1 つのONTAPクラスタから別の ONTAP クラスタに移行できます。AFX を使用した SVM の移行は、Unified ONTAPの場合と同じように動作しますが、相互運用性に関する考慮事項と制限がいくつかあります。SVM 移行の実行の詳細については、Unified ONTAP のドキュメントを参照してください。

相互運用性の考慮事項

SVM の移行を計画して実行する前に、機能や制限などの相互運用性に関する考慮事項を認識しておく必要があります。

ユースケース

クラスタ管理者は、SVM をソース クラスタから宛先クラスタに再配置できます。これは、容量管理と負荷分散の一環として、または機器のアップグレードやデータ センターの統合を可能にするために実行できます。AFX ストレージ システムは Unified ONTAPからのインプレース アップグレードをサポートしていないため、SVM の移行は重要なユース ケースとなります。

アプリケーション ワークロードを、Unified ONTAPクラスターから AFX クラスターに中断なく移動できます。さらに、SVM は、AFX クラスターから Unified ONTAPクラスターへ、また AFX クラスター間での移行など、他の方法でも移行できます。

バージョンの相互運用性

次の表は、ソース クラスタと宛先クラスタのONTAPパーソナリティとリリースに基づいて許可される SVM 移行を示しています。

送受信方向	ソースバージョン	宛先バージョン
AFXに統合	9.15.1 - 9.17.1	9.17.1
AFXからUnifiedへ	9.17.1	9.17.1
AFXからAFXへ	9.17.1	9.17.1

事前確認

Unified ONTAPには、AFX でも実装されているいくつかの事前チェックが含まれています。さらに、AFX でサポートされていない機能にフラグを設定するための、次のようないくつかの新しい事前チェックが追加されました。

- FabricPool（複合アグリゲート上に存在するボリューム）
- シックプロビジョニングボリューム

ボリュームプロビジョニング

ボリュームは、AFX クラスターのストレージ可用性ゾーン (SAZ) 全体にわたって配置のバランスをとるようにプロビジョニングされます。

スペース保証

AFX はシックプロビジョニングをサポートしていません。移行対象の SVM 内のいずれかのボリュームがシック プロビジョニングされている場合、事前チェックを使用して移行を失敗させます。

暗号化

AFX システムはNetAppボリューム暗号化 (NVE) をサポートしますが、NetAppアグリゲート暗号化 (NAE) はサポートしません。このため、Unified ONTAPクラスタのすべての NAE ボリュームは、AFX に移行されると NVE ボリュームに変換されます。次の表は互換性と変換をまとめたものです。

ソース ボリューム	デスティネーション ボリューム
プレーンテキスト	プレーンテキスト
NVE	NVE
ナエ	NVE

追加の制限

SVM を移行する前に考慮する必要がある追加の制限があります。

MetroCluster

AFX ストレージ システムはNetApp MetroClusterをサポートしていません。これにより、SVM の移行時に制限が生じます。MetroCluster を使用するように設定されているAFFまたはFASシステム（または Unified ONTAPパーソナリティ）を実行している任意のNetAppシステム）との間で AFX SVM を移行することはできません。これらの移行シナリオはサポートされていませんが、AFX 事前チェックによって明示的にブロックされることもないため、試行しないように注意する必要があります。

関連情報

- ["ONTAP SVMデータモビリティ"](#)
- ["AFXストレージシステムをAFFおよびFASシステムと比較する"](#)
- ["AFX ストレージ システムに関する FAQ"](#)

クラスターをサポートする

AFXストレージシステムクラスタのAutoSupportを管理する

AutoSupport は、AFX ストレージ システムの健全性をプロアクティブに監視するために使用できるNetAppテクノロジーです。NetAppテクニカル サポート、社内のサポート組織、またはサポート パートナーにメッセージを自動的に送信できます。

AFX クラスターをセットアップすると、AutoSupportがデフォルトで有効になり、メッセージがNetAppテクニカル サポートに送信されます。社内のサポート組織にメッセージを送信するには、クラスターを適切に構成し、有効な電子メール ホストを提供する必要があります。AFX はアクティブになってから 24 時間後

にAutoSupportメッセージの送信を開始します。




AutoSupport を管理するには、クラスタ管理者アカウントを使用して System Manager にサインインする必要があります。

AutoSupportの接続性をテストする

クラスタをセットアップした後、AutoSupport の接続をテストして、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できることを確認する必要があります。



手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. * AutoSupport*の横にある選択  次に*接続をテスト*します。
3. AutoSupportメッセージの件名を入力し、*テストAutoSupportメッセージを送信*を選択します。

AutoSupportの受信者を追加する

オプションで、AutoSupportメッセージを受信する電子メール アドレスのリストに社内サポート組織のメンバーを追加できます。

手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. * AutoSupport*の横にある選択  そして*その他のオプション*をクリックします。
3. *メール*の横にある  その後 **+ Add**。
4. 受信者のメール アドレスを入力します。受信者のカテゴリとして以下を選択します。
 - あなたのパートナーのための*パートナー*
 - 一般 社内サポート組織のメンバー向け
5. *保存*を選択します。


結果

追加した電子メール 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

AFX システムに問題が発生した場合は、AutoSupportデータを手動で送信する必要があります。これにより、問題を特定して解決するまでの時間が大幅に短縮されます。

手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. * AutoSupport*の横にある選択  そして*生成して送信*します。
3. AutoSupportメッセージの件名を入力します。
4. *送信*を選択します。


結果

AutoSupportデータはテクニカル サポートに送信されます。

サポートケースの生成を抑制する

AFX システムでアップグレードまたはメンテナンスを実行している場合は、アップグレードまたはメンテナンスが完了するまでAutoSupportサポート ケースの生成を抑制することをお勧めします。

手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. * AutoSupport*の横にある選択  次に、*サポート ケースの生成を抑制*します。
3. サポート ケースの生成を抑制する時間数と、ケースを生成しないノードを指定します。
4. *送信*を選択します。


結果

指定した時間中はAutoSupportケースは生成されません。指定され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を完了した場合は、サポート ケースの生成を直ちに再開する必要があります。

サポートケース生成を再開する

アップグレードまたはメンテナンス期間中にサポート ケースの生成を抑制した場合は、アップグレードまたはメンテナンスが完了したらすぐにサポート ケースの生成を再開する必要があります。

手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. * AutoSupport*の横にある選択  その後、*サポート ケースの生成を再開*します。
3. AutoSupportケース生成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

AutoSupportケースは、必要に応じて AFX システムに対して自動生成されます。

関連情報

- ["ONTAP AutoSupportについて学ぶ"](#)
- ["ONTAP AutoSupportを使用するための準備"](#)

AFX ストレージ システムのサポート ケースを送信して表示する

サポートが必要な問題がある場合は、ONTAP System Manager 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 System Manager を使用して、進行中または終了したケースを表示することもできます。

開始する前に

あなたはそうする必要があります["Active IQに登録済み"](#)AFX ストレージ システムのサポート ケースを表示します。

手順

1. 新しいサポート ケースを作成して送信するには、System Manager で次の項目を選択します。
 - a. クラスター、そして*サポート*
 - b. * NetAppサポートへ移動*
2. 以前に送信したケースを表示するには、システム マネージャーで次の項目を選択します。
 - a. クラスター、そして*サポート*
 - b. 私のケースを見る

関連情報

- ["ONTAP System Manager を使用してサポートケースを表示および送信する"](#)

クラスターのアップグレードとメンテナンス

AFXストレージシステムクラスターを拡張する

ストレージ容量とは独立して、AFX クラスターのコンピューティング容量を拡張できます。拡張は中断なく実行され、ボリュームがノード間で再バランス調整されるため、パフォーマンスが直線的に向上します。この機能は、AFX システム ユーザーの継続的なニーズに合わせて調整する際に大きなメリットとなります。

クラスターの拡張の準備

AFX クラスターを拡張する前に、基本的な要件とトラブルシューティングの一般的なアプローチを理解しておく必要があります。

要件

クラスター管理者アカウントの認証情報が必要であり、SSH を使用してONTAP CLI に接続できる必要があります。クラスターを拡張する場合は、偶数個のノードを追加し、リリースに基づいて AFX システムのサイズ制限に従う必要があります。

トラブルシューティング

クラスターの拡張を実行する際には、知っておくべき概念とトラブルシューティングのシナリオがいくつかあります。

自動ボリューム再調整

自動トポロジ管理 (ATM) は、割り当ての不均衡を検出し、クラスター ノード間でボリュームのバランスを再調整する内部 AFX システム コンポーネントです。これは、データをコピーするのではなく、メタデータの更新を使用してボリュームを再配置するために、Zero Copy Volume Move (ZCVM) テクノロジーに依存しています。ZCVM は、AFX ストレージ システムで使用するデフォルトのボリューム移動テクノロジーです。

考えられるトラブルシューティングのシナリオ

AFX クラスターの拡張に関連するボリュームの移動中に調査する必要があるシナリオがいくつかあります。

ATMによって取引量は移動されていない

これは、クラスターがすでにバランスが取れている場合、または移動するのに適したボリュームがない場合に発生する可能性があります。

ATM をいつ、どのように稼働させるべきかについての混乱

ボリュームが予想どおりに速く配布されないように見える場合があります。ATM は 5 分ごとにハードウェア イベントを検出して応答しようとしています。最悪の場合、最後のリバランス操作が完了してから 40 分後にリバランス操作が開始されます。

CLI コマンドを使用します。

クラスター拡張操作を監視するために使用できるコマンドがいくつかあります。

- `volume move show`
- `volume move show -instance`

必要に応じて、NetApp サポートに連絡して追加のサポートを受ける必要があります。

ノードを追加してクラスターを拡張する

この手順では、既存のクラスターにノードのペアを追加する方法について説明します。この手順は、他のデプロイメント環境にも適応できます。ONTAP CLI と System Manager 管理インターフェ이스の両方を使用する必要があります。

手順

1. ONTAP CLI に接続し、高度な権限レベルを設定します。

```
afx> set advanced
```

2. 現在のノードのボリュームの場所を表示します。ノードあたりのボリュームの数に注意してください。

```
afx> vol show -fields node,size,constituent-count -is-constituent true -node *
```

3. クラスター相互接続 IP アドレスを表示し、後の手順で使用するために保存します。

```
afx> net int show -role cluster
```

4. クラスターに追加する各ノードのサービス プロセッサにログインします。
5. プロンプトから「**system console**」と入力して、ノードのコンソールにアクセスします。
6. ノードを起動してブート メニュー プロンプトを表示します。

```
LOADER> boot_ontap menu
```

メニューが読み込まれない場合は、**Ctrl+C** キーを押してブート メニューにアクセスします。

7. 必要に応じてメニューからブート オプションの 1 つを選択します。プロンプトが表示されたら、「**yes**」と入力して続行します。

ここから LOADER に戻された場合は、LOADER プロンプトで **boot_ontap** と入力します。

8. クラスタ セットアップ ウィザードを使用して、ノード管理 LIF、サブネット、およびゲートウェイを構成します。

この構成は、System Manager によってクラスタに追加するノードを検出するために使用されます。ポート、IP アドレス、ネットマスク、デフォルト ゲートウェイなどの値をプロンプトに従って入力します。

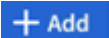
9. CLI にアクセスするには、**CTL+C** を押します。
10. クラスタ相互接続アドレスを変更して、ネットワーク内でルーティングできるようにします。環境に適した構成を使用します。

```
afx> net int show -role cluster
```

```
afx> net int modify -vserver Cluster -lif clus1 -address 192.168.100.201
```

```
afx> net int modify -vserver Cluster -lif clus2 -address 192.168.100.202
```

この手順は、他のインターフェイスがONTAPによって自動的に作成される 169.254.xx アドレスを使用しない場合にのみ必要です。

11. 他の AFX ノード コントローラーでも上記の手順を繰り返します。
12. クラスタ管理 IP アドレスを使用してシステム マネージャにアクセスします。
13. システム マネージャで、クラスター を選択し、次に 概要 を選択し、ノード タブを選択します。
14. 「このクラスターの一部ではありません」セクションを見つけて選択してください  **+ Add** 。
- クラスタ相互接続 IP アドレスが変更される前にノードが検出された場合は、ウィンドウを終了して戻ってノードを再度検出する必要があります。
- オプションとして、System Managerの代わりにCLIを使用してノードを追加することもできます。コマンドを参照してください。 `cluster add-node` 。
15. ノードの追加 メニューで構成の詳細を指定します。管理 IP アドレスは手動で追加することも、サブネットを使用して追加することもできます。
16. ONTAP CLI に接続して、ノード追加操作のステータスを監視します。

```
afx> add-node-status
```

17. 操作が完了したら、すべてのノードにわたってボリュームの配置を確認します。適切なノード名を使用して、各ノードに対してコマンドを 1 回発行します。

```
afx> set advanced
```

```
afx> vol show -fields node,size,constituent-count -is-constituent true -node  
NODE_NAME
```

結果

- クラスタに新しいノードを追加しても中断はありません。
- ボリュームの移動は自動的に行われるはずです。
- パフォーマンスは直線的に増加します。

関連情報

- ["AFX システムの管理を準備する"](#)
- ["ONTAP AFX ストレージ システムに関する FAQ"](#)
- ["NetAppサポート サイト"](#)

AFXストレージシステム上のONTAPのアップグレード

AFX システムでONTAPソフトウェアをアップグレードすると、コストの削減、重要なワークロードの高速化、セキュリティの強化、組織で利用可能なデータ保護の範囲の拡大に役立つ新しいONTAP機能と強化された ONTAP 機能を活用できます。



AFXストレージシステムはサポートしていません ["ONTAPのリバート"](#) 操作。

AFX ストレージ システムのONTAPソフトウェア アップグレードは、他のONTAPシステムのアップグレードと同じプロセスに従います。Active IQ Digital Advisor (Digital Advisorとも呼ばれます) の有効なSupportEdge契約をお持ちの場合は、["アップグレードアドバイザーでアップグレードを準備する"](#)。Upgrade Advisorから提供されるインテリジェンスを活用すれば、クラスタを評価し、使用している構成に固有のアップグレード計画を作成して、不確実性とリスクを最小限に抑えることができます。Active IQ Digital Advisorの有効なSupportEdge契約をお持ちでない場合は、["アップグレードアドバイザーなしでアップグレードを準備する"](#)。

アップグレードの準備ができれば、以下の方法でアップグレードを実行することをお勧めします。["システムマネージャからの自動無停止アップグレード \(ANDU\) "](#)。ANDUでは、ONTAPのハイアベイラビリティ (HA) フェイルオーバー テクノLOGYを利用して、アップグレード中もクラスタからデータが提供されます。

関連情報

- ["ONTAPアップグレードについて学ぶ"](#)。

AFXストレージシステムのファームウェアを更新する

ONTAP は、デフォルトで AFX ストレージ 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。推奨される更新プログラムをダウンロードしてインストールする前に確認したい場合は、自動更新を無効にすることができます。更新パラメータを編集して、アクションを実行する前に利用可能な更新の通知を表示することもできます。

自動更新の有効化

AFX クラスターの自動更新を有効にすると、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 ファイルの推奨更新がデフォルトで自動的にダウンロードされ、インストールされます。

手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. *ソフトウェア更新*の下で*有効*を選択します。
3. EULA をお読みください。

4. 推奨される更新の「通知を表示」のデフォルトを受け入れます。オプションで、推奨される更新を自動的に更新するか、自動的に閉じるかを選択します。
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確認する場合に選択します。
6. *保存*を選択します。

結果

推奨される更新は、更新の選択に基づいて、ONTAP AFX 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

推奨される更新プログラムがインストールされる前に表示する柔軟性が必要な場合は、自動更新を無効にします。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. システム マネージャーで、クラスター > 設定 を選択します。
2. *ソフトウェア更新*の下で*無効*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判断する必要があります。

自動更新を表示

クラスター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 ファイルの更新の一覧を表示します。以前に自動的にインストールされた更新プログラムも表示します。

手順

1. システム マネージャーで、クラスター > 設定 を選択します。
2. *ソフトウェアアップデート*の横にある → をクリックし、[すべての自動更新を表示] を選択します。

自動更新を編集する

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 ファイルの推奨更新を自動的にダウンロードしてクラスターにインストールするか、推奨更新を自動的に破棄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破棄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するように選択し、その後、手動でインストールまたは破棄を選択できます。

手順

1. システム マネージャーで、クラスター > 設定 を選択します。
2. ソフトウェアアップデート*の横にある → 次に、[*その他のすべての更新プログラム]を選択します。
3. 自動更新の選択を更新します。
4. *保存*を選択します。

結果

自動更新は選択内容に基づいて変更されます。

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す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. ファームウェア更新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. システム マネージャーで、クラスター > 概要 を選択し、その他のすべての更新 を選択します。
3. *手動更新*の下で、*ファームウェア ファイルの追加*を選択し、*サーバーからダウンロード*または*ローカル クライアントからアップロード*を選択します。
4. ファームウェア更新ファイルをインストールします。

結果

ファームウェアが更新されました。

ONTAP の復帰は AFX ストレージ システムではサポートされません

ONTAP クラスターを元に戻すとは、すべてのノードを以前のメジャー ONTAP リリースに移動するプロセスです。

NetApp AFX ストレージ システムは ONTAP の復帰をサポートしていません。AFX を使用して元に戻す操作を試みると、クラスターが不安定になり、データが失われる可能性があります。AFX システムでは元に戻す操作を試みないでください。

AFX ストレージ システム クラスターの追加管理

一般的な AFX クラスター管理に加えて、環境に応じて実行する必要がある他のタスクがある場合があります。追加タスクのほとんどは System Manager を使用して実行できますが、場合によっては CLI を使用する必要があることもあります。



ここで説明する ONTAP の機能と管理は、AFX ストレージ システムと、Unified ONTAP を実行する AFF または FAS システムに共通です。関連する Unified ONTAP ドキュメントへのリンクが必要に応じて含まれています。

ライセンス

AFX システムは、Unified ONTAP AFF および FAS システムと同様の方法でライセンスされます。AFX クラスターには、サポートされているプロトコルのほとんどの機能がデフォルトで含まれています。


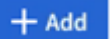
ONTAP ライセンス管理

ONTAP ライセンスは、1 つ以上のソフトウェア権限の記録です。すべてのライセンスは、NetApp ライセンス ファイル (NLF) を使用して定義および提供されます。参照 ["ONTAP ライセンスの概要"](#) 詳細についてはこちらをご覧ください。

AFXシステムにライセンスをインストールする

ライセンス ファイルをインストールして、AFX ストレージ システムの必要に応じて追加機能をアクティブ化できます。

手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. *ライセンス*の横にある .
3. 利用可能なONTAP機能を表示するには、[機能] タブを選択します。
4. オプションでライセンスをインストールするには、[インストール済みライセンス] タブを選択します。
5. 選択 .
6. ローカル ライセンス ファイルを選択し、[追加] を選択します。

セキュリティ

AFX 展開で構成および使用できるオプションのセキュリティ機能がいくつかあります。

ONTAPのセキュリティとデータ暗号化

AFX ストレージ システムのセキュリティとプライバシーを保護することが重要です。言い及ぶ "[セキュリティとデータ暗号化](#)"


ONTAP認証とアクセス制御

AFX ストレージ システムには、認証およびアクセス制御サービスを構成するためのいくつかのオプションが用意されています。参照 "[認証とアクセス制御](#)" 詳細についてはこちらをご覧ください。

AFX システムで OAuth 2.0 を管理する

OAuth 2.0 は、署名されたアクセス トークンを使用し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る業界標準の認証フレームワークです。

手順

1. システム マネージャーで、[クラスター] を選択し、[設定] を選択します。
2. *セキュリティ*セクションで、*OAuth 2.0認証*の横にある .
3. OAuth.2.0を有効にする
4. *構成の追加*を選択し、構成の詳細を入力します。
5. *保存*を選択します。

関連情報

- "[AFX ストレージ システムに関する FAQ](#)"
- "[ONTAP OAuth 2.0導入の概要](#)"
- "[AFX SVMの追加管理](#)"

著作権に関する情報

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

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

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

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

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

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

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

商標に関する情報

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