テクニカル レポート

ONTAPでのセキュアマルチテナンシー

概要と設計に関する考慮事項

NetApp
Dan Tulledge
2021年1月| TR-4160

概要

本レポートでは、NetApp® ONTAP®にStorage Virtual Machine（SVM）を使用したセキュアマルチテナンシーの実装について説明し、設計上の考慮事項とベストプラクティスを紹介します。

<<本レポートは機械翻訳による参考訳です。公式な内容はオリジナルである英語版をご確認ください。>>

目次

表一覧

図一覧

はじめに

モクテキトモクテキ

このテクニカルレポートでは、ONTAPを使用したセキュアマルチテナンシーの実装について説明します。一般的なStorage Virtual Machine（SVM）の導入シナリオについて説明し、SVMのベストプラクティスに関する推奨事項を提供します。本レポートはあくまでリファレンスガイドであり、製品ドキュメント、ONTAPテクニカルレポート、エンドツーエンドのONTAP運用に関する推奨事項に代わるものではありません。可能であれば、これらのドキュメントを参照します。

対象読者

本ドキュメントは、ONTAPのセキュアマルチテナンシーの概念、さまざまなSVMの導入シナリオ、およびベストプラクティスについて理解したいストレージアーキテクトおよびストレージ管理者を対象としています。本ドキュメントは、読者が『ONTAPの概念』に記載されているONTAPアーキテクチャに関する基本的な知識を持っていることを前提としています。

概要

セキュアマルチテナンシー（SMT）

セキュアマルチテナンシーとは何ですか？

従来、データをセキュアに格納したいと考えているストレージユーザは、1つ以上の物理ストレージアレイを購入して導入していました。アレイの物理サイズは、容量とスループットのニーズによって異なりますが、通常は、必要なデータとパフォーマンスを安全に分離するために、何らかの種類のアレイ全体が必要でした。

セキュア マルチテナンシーとは、複数の異なるテナント間で物理環境を共有する目的で、共有の物理ストレージ環境に設けられたセキュアな仮想パーティションを使用することです。たとえば、ストレージサービスプロバイダは、3つの異なる顧客それぞれがアレイのディスク容量とネットワークリソースの一部をプロビジョニングするようにストレージアレイを設定できます。セキュアなマルチテナント環境では、各顧客は、その顧客に明示的にプロビジョニングされたリソースにのみアクセスできます。お客様は、他のお客様のデータにアクセスすることも、他のお客様の存在や共通の物理アレイを共有していることを認識することもできません。セキュアなマルチテナント環境では、共有されているパフォーマンス機能の多くを単一のテナントが消費しないようにして、他のテナントに影響を与えないようにすることも必要です。

セキュアマルチテナンシーのメリット

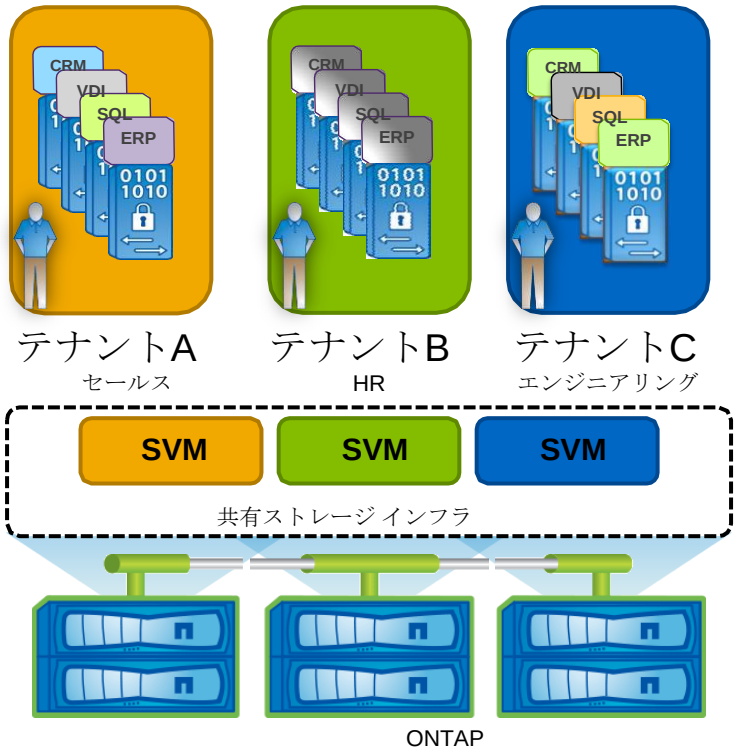
従来型のサイロ化したモデルは非効率的です。独立したワークロードごとに別々の物理ハードウェアスタックを導入すると、コストと時間がかかります。通常、サイロ化した環境でリソース使用率が低いと、リソースの無駄に直接つながります。一方、マルチテナント環境には次のようなメリットがあります。

- **コストの削減**：テナントごとに専用のセキュアな論理ストレージパーティションを割り当てると、スケールメリットが得られ、専用ハードウェアよりもコスト効率が高くなります。
- **導入時間の短縮：**論理パーティションは、別の物理アレイのラック、ケーブル接続、設置、構成に必要な時間のごくわずかな時間で作成できます。
- **リソース利用率の改善：**物理ハードウェアを共有することで、リソース利用率が向上し、ワークロードの変動を考慮して個々のワークロードをオーバープロビジョニングする必要がなくなります。
- **セキュアな分離：**セキュアマルチテナンシーにより、企業はテナントを共有リソースに統合しながら、明示的に割り当てられていないリソースにテナントがアクセスできないようにします。同じ物理ハードウェアを共有するテナントは独立して運用でき、単一のテナントがリソースを不当に消費することはありません。たとえば、本番環境と開発/テスト環境を同じシステムで実行でき、開発/テスト環境が本番環境のワークロードに影響を及ぼすリスクはありません。

ONTAPのSMT

ONTAPは、本質的にマルチテナントストレージオペレーティングシステムです。ONTAPは、すべてのデータアクセスがセキュアな仮想ストレージパーティションを介して行われるように設計されています。クラスタ全体のリソースを表す単一のパーティション、またはクラスタリソースの特定のサブセットを割り当てられた複数のパーティションを持つことができます。セキュアな仮想ストレージパーティションは、Storage Virtual Machine（SVM）と呼ばれます。

図1）SVM



Storage Virtual Machine SVM

の概要

ONTAPでデータへのアクセスに使用するセキュアな論理ストレージパーティションをSVMと呼びます。クラスタからのデータの提供には、少なくとも1つ、場合によっては複数のSVMが使用されます。SVMはクラスタの物理リソースを論理的なセットとして抽象化したものであり、データボリュームと論理ネットワークインターフェイス（LIF）は作成されてSVMに割り当てられ、SVMからアクセスできるクラスタ内の任意のノードに配置される場合があります。1つのSVMが複数のノード上のリソースを同時に所有する場合があり、それらのリソースはノード間で無停止で移動できます。たとえば、フレキシブルボリュームを新しいノードやアグリゲートに無停止で移動したり、データLIFを別の物理ネットワークポートに透過的に再割り当てしたりできます。この方法では、SVMはクラスタハードウェアを抽象化し、特定の物理ハードウェアに縛られることはありません。

SVMは、複数のデータプロトコルを同時にサポートできます。SVM内のボリュームを結合して単一のNASネームスペースを形成することで、SVMのすべてのを、単一の共有またはマウントポイントからNFSクライアントおよびCIFSクライアントにアクセスできるようになります。たとえば、UNIXとWindowsのファイルサービスライセンスが24ノードのクラスタで、1つのSVMが数千個のボリュームで構成され、いずれかのノードの1つのLIFからアクセスされるとします。SVMはブロックベースのプロトコルもサポートしており、iSCSI、FC、またはFCoEを使用してLUNを作成およびエクスポートできます。これらのいずれかまたはすべてのデータプロトコルが、特定のSVM内で使用するように設定されている可能性があります。

SVMはセキュアなエンティティであるため、SVMに割り当てられているリソースのみを認識し、他のSVMとそれぞれのリソースを認識することはありません。SVMは、それぞれ独自のセキュリティ ドメインを持つ独立したエンティティとして動作します。テナントは、委譲されたSVM管理アカウントを使用して、割り当てられたリソースを管理できます。各SVMは、Active Directory、LDAP、NISなどの一意の認証ゾーンに接続できます。

SVMは、同じ物理ハードウェアを共有する他のSVMから実質的に分離されます。

パフォーマンスの点では、QoSポリシーグループを使用して、最大IOPSとスループットレベルをSVMごとに設定できます。これにより、クラスタ管理者は、各SVMに割り当てられているパフォーマンス容量を数値化できます。

ONTAPは拡張性に優れているため、既存のクラスタにストレージコントローラとディスクを簡単に追加して、増大するニーズに合わせて容量とパフォーマンスを拡張できます。クラスタ内の仮想ストレージサーバは拡張性に優れているため、SVMも拡張性に優れています。新しいノードやアグリゲートがクラスタに追加されたときに、そのノードやアグリゲートを使用するようにSVMを無停止で設定できます。この方法では、ディスク、キャッシュ、およびネットワークの新しいリソースをSVMで利用できるようにして、新しいデータボリュームを作成したり、既存のワークロードをこれらの新しいリソースに移行したりして、パフォーマンスを分散させることができます。

また、この拡張性により、SVMの耐障害性も向上します。SVMは、特定のストレージコントローラのライフサイクルに縛られなくなります。撤去するハードウェアの交換のために新しいハードウェアが導入された場合は、SVMのリソースを古いコントローラから新しいコントローラに無停止で移動できます。この時点で、SVMをオンラインにしてデータを提供できる状態にしたまま、古いコントローラを撤去できます。

注： ONTAPの内部では、SVMはSVMとも呼ばれます。このドキュメントに記載されているコマンド例では `vserver`、コマンドを使用してSVMに関連する操作を実行します。

SVMのコンポーネント

LIF

SVMネットワークは、いずれもSVM内に作成されたLIFを介して行われます。LIFは論理構成要素として、LIFが配置されている物理ネットワークポートから抽象化されます。LIFについては、セクション3.2で詳しく説明します。

フレキシブル ボリューム

フレキシブルボリュームは、SVMの基本的なストレージユニットです。SVMにはルートボリュームが1つあり、1つ以上のデータボリュームを含めることができます。データボリュームは、クラスタ管理者からSVM用に委譲された任意のアグリゲート内に作成できます。SVMで使用されているデータプロトコルに応じて、ボリュームに、ブロックプロトコルで使用するLUN、NASプロトコルで使用するファイル、またはその両方を格納できます。NASプロトコルを使用してアクセスする場合は、ジャンクションと呼ばれるクライアントが認識できるディレクトリを作成して、ボリュームをSVMネームスペースに追加する必要があります。

ネームスペース

SVMにはそれぞれ独自のネームスペースがあり、そのSVMから共有されているすべてのNASデータにアクセスできます。このネームスペースは、SVMが物理的に配置されているノードやアグリゲートに関係なく、SVMにジャンクションされたすべてのボリュームへのマッピングとみなすことができます。ボリュームは、ネームスペースのルートまたはネームスペース階層の一部である他のボリュームの下でジャンクションできます。ネームスペースについてはセクション3で説明し、詳細については TR-4129：『Namespaces in Clustered Data ONTAP』を参照してください。

NetApp ONTAP FlexGroupボリューム

FlexGroupボリュームは、複数のコンスティチュエント/メンバーボリュームで構成される単一のネームスペースです。ストレージ管理者が管理し、NetApp FlexVol® ボリュームのように機能します。FlexGroupボリューム内のファイルは、個々のメンバー ボリュームに割り当てられ、複数のボリュームやノードにまたがってストライピングされることはありません。1つのクラスタにFlexGroup Volumeを備えたSVMを複数配置でき、FlexVolを備えたSVMを含む同じクラスタにそれらのSVMを共存させることができます。FlexGroupボリュームの詳細については、TR-4037：『NetApp ONTAP FlexGroup Volumes』を参照してください。

SVMの設計に関する考慮事項

SVMのレイアウト

タンイチノSVMクラスタ

多くのクラスタでは、クラスタ内の使用可能なすべての物理リソースを使用する単一のSVMが最も論理的で柔軟性に優れたオプションになります。クラスタの使用可能なリソースをすべて消費する単一のテナントがある場合、このオプションは設定と保守が最も簡単なオプションです。ただし、インスタンスは多数あります。特にマルチテナント環境では、複数のSVMで構成されたクラスタを使用することを推奨します。これらのユースケースについては、次のセクションで説明します。最初に単一のSVMで構成されたクラスタでは、要件やニーズの変化に応じて追加のSVMを定義できます。

フクスウノSVMクラスタ

各クラスタにSVMを1つだけ配置することも可能ですが、複数のSVMが必要なシナリオやメリットがあるシナリオも多数あります。次のいずれかのシナリオでは、複数のSVMが作成される可能性があります。

ワークロードの分離

クラスタの個 々 のワークロード用にSVMを作成すると、格納するデータを直接担当するITグループにデータ管理を委譲できるというメリットがあります。アプリケーション所有者には、他のアプリケーションワークロードをホストするSVMの管理権限やクラスタ全体の管理権限は与えずに、特定のアプリケーションに属するデータセットを自律的に制御することができます。ワークロードが複数のSVMに分離されている場合は、QoSポリシーを適用して、SVM /ワークロードレベルでパフォーマンスを分離できます。データレプリケーションの要件が異なるワークロードでは、SVMを別 々 のSVMに分割することで、ワークロードを構成するボリュームとLUNを論理的にグループ化できます。

NASとSANの分離

SVMはONTAPと同様に、本質的にマルチプロトコルであり、NAS（CIFS、NFS）とSAN（iSCSI、FCP、FCoE）のワークロードに同時に対応できます。NASとSANのワークロードを別 々 のSVMで実行するという技術的な要件はありません。ただし、NASとSANのワークロードを別 々 のSVMに分離することが推奨される理由はいくつかあります。

多くの企業では、NASとSANの作業と責任が分担されています。専任のストレージ管理チームがある場合は、ストレージアレイやスイッチなどのストレージハードウェアをそのチームで管理するのが一般的です。また、通常は、LUNの作成とマスキング、およびLUNをホストに安全に割り当てるために必要なファイバチャネルゾーンの作成も担当します。このチームがONTAPクラスタの全体的な管理を担当する可能性が高くなります。ブロックデータサービスを提供するSVMも管理することは、チームのストレージ管理責任を論理的に拡張したものです。

一方、NASは、これらのストレージサービスを使用するサーバチームと緊密に連携する傾向があります。Windows環境では、サーバ管理者はCIFS共有の管理に強い関心を持っています。同様に、UNIX管理者はNFSエクスポートの管理に精通している傾向があります。

そのため、企業はNAS SVMを作成し、SAN SVMへの管理アクセスを許可することなく、それぞれのサーバ管理者に管理制御を委譲できます。

ファイルサーバ統合

複数のファイルサーバを単一のONTAPクラスタに統合する場合は、単一のSVMに簡単に移行できるものと、追加のSVMの作成が必要なものがあります。一般に、統合するファイルサーバが同じ認証サービスを共有し、同じセキュリティゾーンに属し、同じ管理チームによって管理され、共有名に解決できない重複がない場合は、1つのSVMで十分です。追加のSVMを作成しないと、ONTAPに移行するファイルサーバを物理的に統合しつつ、必要なセキュアな論理的分離を維持できます。一般的には、管理を合理化するために、認証とパフォーマンスの要件を満たしながら、技術的に可能な最小限のSVMにファイルサーバを統合することが推奨されます。

インフラサービスプロバイダ

SVMを使用すると、サービスプロバイダはストレージリソースをテナントにセキュアに割り当て、それらのリソースの管理を委譲できます。各テナントに専用の物理ハードウェアを割り当てたり、複数のテナントとそのデータを相互に公開したりする必要はありません。サービスプロバイダは、テナントSVMで使用できるクラスタリソースのタイプに基づいてサービス階層を作成できます。たとえば、SSDストレージ、NetApp Flash Cacheを搭載したハイパフォーマンスノード、ギガビットイーサネット（GbE）対10GbE対100GbEインターフェイスなどです。これらのリソースを使用するようにボリュームとLIFを無停止で再設定することで、サービスプロバイダはお客様の高可用性を維持できます。また、QoSを使用することで、プロバイダは各テナントに割り当てられるデータスループットを制御できます。QoSポリシーを設定すると、1つのテナントがノードのリソースを不当に消費することなく、クラスタの同じ物理ノードを複数のテナントで共有できます。

SVMの制限

ONTAPのデータにアクセスするには少なくとも1つのSVMが必要ですが、それ以上のSVMを作成して使用することも可能です。クラスタあたりのSVM数のベストプラクティスは、前述したアプリケーション環境やユースケース環境とともにいくつかの要因を考慮することで実現します。

- クラスタ内のノードの数
- ノードあたりのIP LIFとFCP LIFの最大数
- ポートあたりのIP LIF、iSCSI LIF、およびFCP LIFの最大数
- HAフェイルオーバーの発生時にパートナーLIFに対応できるポート容量を確保する
- SVM管理に専用の管理LIFを使用するか、データと管理を組み合わせたLIFを使用するか

ノードあたりのIP LIFの最大数、ノードあたりのFCP LIF数、ポートあたりのIP LIF数、ポートあたりのiSCSI LIF数、ポートあたりのFCP LIF数については、『NetApp Hardware Universe』を参照してください。

注： iSCSI LIFとは、iSCSIプロトコルが有効になっているIP LIFのことです。

注： ノードあたりのiSCSI LIFまたはFCP LIFの数を最大にするには、適切な数のポートが必要です。

NAS SVM

NAS SVMの場合、別々の管理LIFを使用するか、データLIFと組み合わせるかによって、作成可能なSVMの数が変わります。推奨される設定オプションは次のとおりです。

- **データLIFと管理LIFの組み合わせ：**この設定では、各SVMにアクティブなIP LIFが1つ必要です。このLIFは、データアクセスと管理アクセスの組み合わせに使用されます。
- **専用の管理LIF：**この構成では、各SVMに2つのIP LIF（アクティブな管理LIFとアクティブなデータLIF）が必要です。

注： HAペアでは、HAフェイルオーバーが可能になるように、各ノードのパートナーに十分な数のLIFがあることを確認する必要があります。たとえば、ノードあたりのIP LIFの最大数は256ですが、実際には128個のアクティブなLIFと128個のLIFがフェイルオーバー時にのみインスタンス化されることを意味します。

クラスタあたりのNAS SVMの最大数については、『NetApp Hardware Universe』を参照してください。

注： SVMには、最低限必要な数以上のLIFを追加することができます。これにより、クラスタごとに作成できるSVMの数が少なくなります。

SAN対応のSVM

SAN対応のSVMには、次の設定オプションが推奨されます。

- **専用のIP管理LIFを使用したFC / FCoEデータLIF。**この構成では、クラスタのノードごとに各SVMにFC / FCoE LIFが2つ必要です。管理用には、IP LIFを作成し、管理専用にする必要があります。
- **iSCSIデータLIFと専用のIP管理LIF**この構成では、クラスタのノードごとにSVMごとにiSCSI LIFが1つ必要です。このLIFは、iSCSIデータトラフィック専用に使用されます。冗長性を確保するために、複数の物理ポートを1つの仮想ポートにまとめたインターフェイスグループの上にLIFを作成することを推奨します。SVMごとの管理にはIP LIFも必要です。

クラスタあたりのSAN対応SVMの最大数については、『NetApp Hardware Universe』を参照してください。

注： SVMには、最低限必要な数以上のLIFを追加することができます。これにより、クラスタごとに作成できるSVMの数が少なくなります。

SANとNASが混在するSVM

クラスタには、NAS専用のSVMとSAN対応のSVMを混在させることができます。1つのクラスタに含めることができるSVMの正確な数は、作成するタイプによって異なります。クラスタ内に作成できるSVM数を正確に決定する主な要因は、クラスタノードでサポートされるLIFの数です。一般に、HAフェイルオーバーが可能な状態で、必要なデータLIFと管理LIFを作成できる容量がクラスタにあれば、SVMを作成できます。

テナントの階層化

SVMは、クラスタ内の使用可能なすべてのリソースを使用できますが、クラスタ管理者は、テナントがアクセスできるリソースとリソースのクラスを正確に制御することもできます。これにより、クラスタ管理者は、異なるビジネスユニット、ワークロード、または顧客に異なるクラスのリソースを割り当てる階層化戦略を実装できます。小規模なクラスタには階層の数が少ない可能性がありますが、複数のコントローラとディスクタイプを含む大規模なクラスタでは多数の階層をサポートできます。

SASアグリゲート、SATAアグリゲート、SSDアグリゲート、Flash Poolアグリゲートなど、さまざまなタイプのアグリゲートを作成できます。テナントボリュームは、初期作成時の要件に基づいて、適切なアグリゲートにプロビジョニングできます。これらのニーズや要件があとで変更された場合、クラスタ管理者はシステムを停止することなく、別の階層の別のアグリゲートにボリュームを再配置できます。

アグリゲートは、機能が異なるノードに配置することもできるため、階層の差別化につながる可能性があります。メモリやCPUの可能性が異なるノード間や、フラッシュベースキャッシュの容量が異なるノード間でワークロードを移動できます。

NASワークロードの場合は、機能が異なるインターフェイスに無停止でLIFを移行することもできます。たとえば、ネットワークアクセスは、帯域幅（GbE対10GbE対100GbE）または冗長性の程度（単一の物理ポートや複数の物理インターフェイスで構成されるインターフェイスグループなど）別に階層化できます。

パフォーマンスや容量の要件やサービスレベルアグリーメントに基づいて、システムを停止することなく、階層間でSVMリソースを移動できます。要件が変化するデータセットは、必要に応じて、ライフサイクル全体を通じて階層間で移動できます。たとえば、負荷の高いデータ処理用にハイパフォーマンス階層にボリュームを作成し、あとでアーカイブ用に対費用効果の高い階層に移動することができます。

注： `volume rehost` コマンドを使用して、ボリュームを別のSVMに再割り当てすることは可能です。

言語に関する考慮事項

各SVMには、SVMの作成時に言語設定が指定されます。この設定によって、SVM内のすべてのボリュームに格納されたデータに使用されるデフォルトの文字セットが決まります。このSVMの言語設定は、必要に応じてあとから変更できます。ただし、SVM内に作成されたボリュームの言語は変更できません。したがって、言語の選択を事前に計画し、正しく設定するように注意することが重要です。

SVMの言語を選択する際に考慮すべき非常に重要な要素の1つは、SnapMirrorデータ保護ミラーを使用してデータをレプリケートするかどうかです。SVM間でボリュームをレプリケートする場合は、ソースボリュームとデスティネーションボリュームの言語設定が同じである必要があります。ボリュームの言語設定が同じであれば、言語設定が異なるSVM間でレプリケートすることが可能です。技術的な要件に基づいて可能なかぎり適切な言語設定を選択し、すべてのSVMとボリュームでこの設定を標準化することを推奨します。

ベスト プラクティス

特定のSVM言語を必須とする技術的要件がないかぎり、C.UTF-8（POSIX with UTF-8）言語を使用してSVM環境を標準化することを検討してください。

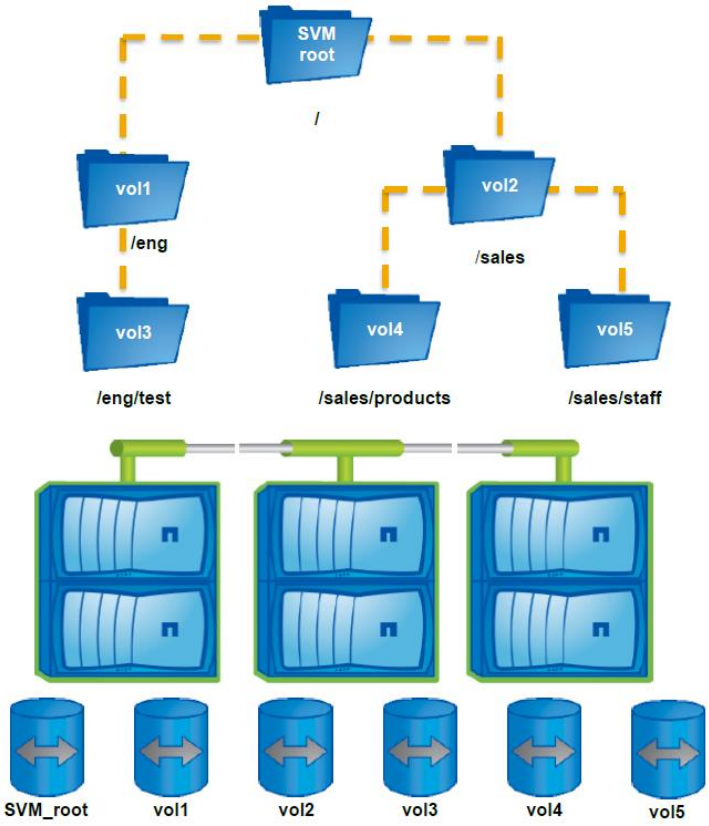
SVMネームスペースに関する考慮事項

ネームスペース

NASプロトコルの場合、SVMデータへのアクセスには、ネームスペースと呼ばれる単一の階層型ディレクトリ構造を使用します。各SVMには、クラスタ内の他のSVMのネームスペースとは分離されたネームスペースがあります。特定のSVM内に作成されたFlexVol®ボリュームは、そのSVMのネームスペースにのみマッピングできます。

ボリュームはジャンクションによってネームスペース階層にマッピングされます。各ボリュームには、一度に1つのジャンクションパスを設定できます。ジャンクションパスによって、ボリュームを配置するネームスペース内の場所が決まります。ボリュームのジャンクションパスがボリューム名に対応している必要はありませんが、対応していると、ネームスペース内で特定のボリュームがジャンクションされている場所がわかりやすくなります。ボリュームは、ネームスペースのルートまたはすでにジャンクションされている別のボリュームの下でジャンクションできます。図2にネームスペースの例を示します。

図2）SVMネームスペースにジャンクションされたボリューム



注： ネームスペースにジャンクションできるストレージオブジェクトはボリュームだけです。qtree、ボリュームサブディレクトリ、および個々のファイルはジャンクションできません。ボリュームは、別のボリュームから直接ジャンクションすることも、ユーザが作成したサブディレクトリやqtreeからジャンクションすることもできます。

エクスポート ポリシー

ネームスペース内の各ボリュームへのアクセスは、エクスポートポリシーの作成によって決まります。エクスポートポリシーによって、どのボリュームにどのホストからアクセスできるかが決まります。ボリュームに設定できるエクスポートポリシーは1つだけで、qtreeを含むボリューム内のすべてのデータを環境できます。ただし、同じエクスポートポリシーを複数のボリュームに適用できます。各エクスポートポリシーには、ホストまたはホストの範囲と、許可するアクセスのタイプを指定する複数のルールを含めることができます。

エクスポートポリシーの例は次のとおりです。

```
Vserver         Policy Name          Rule Index  Access Protocol  Client Match                RO Rule
--------------  -------------------  ----------  ---------------  --------------------------  ---------
vs1             vsphere              1           any              192.168.1.1                 any
vs1             vsphere              2           any              192.168.2.1                 any
vs1             vsphere              3           any              192.168.3.0/24              any
```

このエクスポートポリシーが割り当てられたボリュームは、最初の2つのルールで明示的に定義された2つのホスト、および3つ目のルールで定義されたサブネット全体にエクスポートされます。

エクスポートポリシーは常にボリュームレベルで作成されます。ONTAPにqtreeを配置することも可能ですが、qtreeを含むボリュームのエクスポートポリシーを作成することでqtreeのデータがエクスポートされます。qtreeは、そのqtreeを含むボリュームのエクスポートポリシーを継承します。FlexClone® ボリュームは、既存のFlexVolボリュームのスペース効率に優れたコピーであり、エクスポートポリシーが親FlexVolボリュームのエクスポートポリシーと一致している必要はありません。

ネームスペースとエクスポートポリシーの詳細については、『TR-4129：clusteredData ONTAPのネームスペース』

SVMネットワーク

ONTAPのネットワークオブジェクトのタイプ

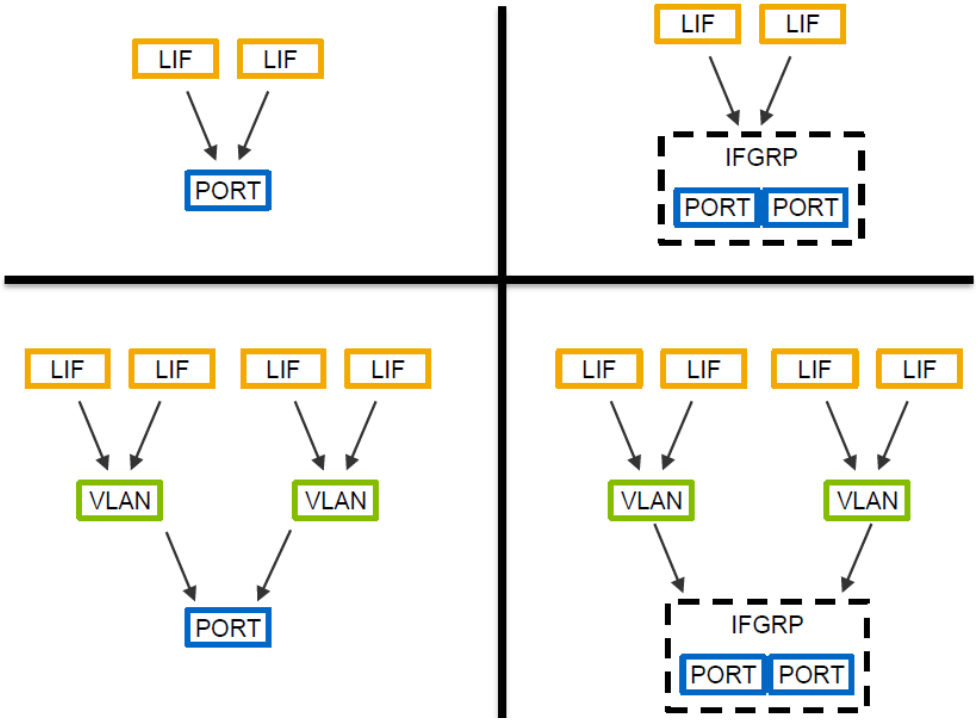
ONTAPには、物理、仮想、論理の3種類のネットワークオブジェクトがあります。

1つ目のタイプは、GbEポート、10GbEまたは100GbEポートなどの単純な物理ポートです。

2つ目のタイプは、インターフェイスグループや仮想LAN（VLAN）などの仮想ネットワークインターフェイスです。インターフェイスグループは、冗長性を確保するために、複数の物理ポートを1つの仮想インターフェイスに集約します。VLANインターフェイスは、単一の物理ポートまたはインターフェイスグループを複数の分離されたブロードキャストドメインに分割します。

最後に、LIFは抽象化として物理インターフェイスレイヤまたは仮想インターフェイスレイヤの上に作成されます。NASまたはiSCSIに対応するIPベースのLIFにはIPアドレスが割り当てられ、FCベースのLIFにはWWPNが割り当てられます。LIFは、SVMに直接割り当てられる唯一のインターフェイスタイプです。NASプロトコルに使用される管理LIFとデータLIFは移動可能で、システムを停止することなく、新しい物理ポート、インターフェイスグループ、またはVLANに再割り当てまたはフェイルオーバーできます。SANプロトコルで使用されるデータLIFは、同じ移動を必要とせず、新しい物理ポートに移行またはフェイルオーバーしません。これは、ONTAPのMPIOとALUAがホストトラフィックに最適なポートを自動的に選択するためです。ただし、SAN LIFを最初にオフラインにしてから、新しいホームポートに再割り当てすることは可能です。これにより、クラスタに新しいハードウェアを追加したり、既存のハードウェアを撤去したりできるようになります。SAN LIFをオフラインにしても、複数のSAN LIFを介してLUNが同時にエクスポートされるため、マッピングされたLUNにホストがアクセスできなくなり、LUNパスがホスト上のマルチパスI/Oソフトウェアによって管理されるわけではありません。

図3）ONTAPでのLIF構成のタイプ



LIF

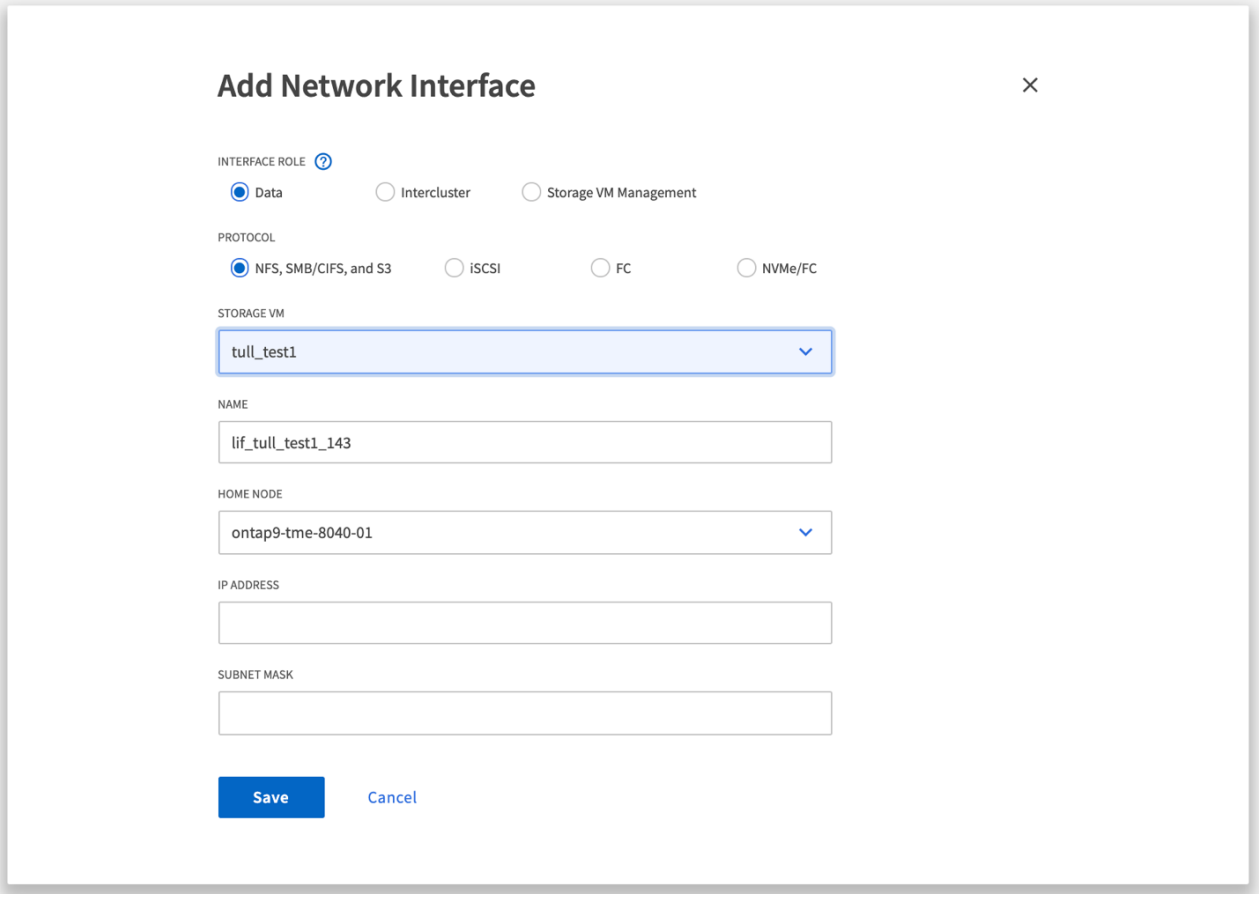
ONTAPにはいくつかの種類のLIFがあり、それぞれが目的別に使用されます。表4に、LIFタイプとその機能を示します。

表1）LIFのタイプ

LIFの種類	機能	最小要件	最大許可数
ノード管理	特定のノード、SNMP、NTP、およびASUP™のシステムメンテナンスに使用	ノードあたり1	ポートおよびサブネットあたり1
クラスタ管理	クラスタ全体の管理インターフェイス	クラスタあたり1	N/A
クラスタ	クラスタ内のトラフィックに使用	ノードあたり2	ノードあたり2
データ	SVMに関連し、データプロトコルおよびプロトコルサービス（NIS、LDAP、Active Directory、WINS、DNS）に使用	SVMあたり1	HA構成ではノードあたり128 非HAではノードあたり256
クラスタ間	クラスタピアやSnapMirrorトラフィックのセットアップなど、クラスタ間通信に使用	クラスタ ピアが有効な場合はノードあたり1	N/A

図4に示すように、データLIFはデータプロトコルアクセス、SVM管理アクセス、またはその両方に使用できます。

図4）ONTAP System ManagerのLIF作成オプション



SVMリソースの配置

ONTAPのSVMの主な特長の1つは、それぞれが単一のコントローラやHAペアにバインドされていない、クラスタ上に存在する論理エンティティであることです。そのため、SVMには、クラスタ内の任意のノードのリソースと複数のノードのリソースを同時に含めることができます。これにより、管理者は非常に高い柔軟性を手に入れることができます。たとえば、SVMのデータボリュームを単一のアグリゲートに配置したり、複数のノード上の複数のアグリゲートに分散したりできます。ONTAPのデータ移動機能を使用すると、新しいアグリゲートが別のノードにあっても、システムを停止することなくこれらのボリュームを別のアグリゲートに再配置できます。同様に、データLIFは論理的なものであり、新しい物理ポート、VLAN、またはインターフェイスグループに無停止で移動できます。これらのポートは理論的にはクラスタの任意のノードに配置できますが、適切な物理ネットワークに接続された物理ポートにLIFを移動するように注意する必要があります。NASクライアントは、任意のノード上のSVMのデータLIFを使用して共有やエクスポートに接続し、ボリュームが含まれているノードやアグリゲートに関係なく、SVMのすべてのデータボリュームにアクセスできます。これにより、クラスタに新しいリソースを導入したり、クラスタからリソースを撤去したり、ワークロードと容量をクラスタ全体に分散したりする、物理レベルでこれまでにない柔軟性が実現します。

SAN LIFに関する考慮事項

NASデータアクセスに使用されるLIFとは異なり、iSCSI、FCP、またはFCoEのアクセスに使用されるLIFは、割り当てられたホーム物理ポートから移行されません。また、iSCSIに使用されるLIFは、NFSやCIFSなどの他のプロトコルには使用できないため、iSCSI専用にする必要があります。そのため、通常は適切なタイプのSAN LIFがクラスタの各ノードに作成されます。

ホストではマルチパスI/Oドライバを使用し、Asymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）を使用してLUNアクセスに使用する最適なLIFを決定することが想定されます。

LUNあたりのパス数に上限があるホストオペレーティングシステムでは、多数のノードで構成される大規模なクラスタや、ノードあたりの使用可能なパス数が多い小規模なクラスタでは、これが課題になる可能性があります。ホストで使用できるパスの数を減らすには、ポートセットの使用を検討してください。ポートセットでは、ノードあたりの使用可能なパスの数、またはLUNを使用できるノードの数を制限できます。

ONTAPでのSANのベストプラクティスの詳細については、TR-4080：『Best Practices for Modern SAN』を参照してください。

ベスト プラクティス

iSCSIプロトコルを使用するSVMの場合は、データプロトコルにアクセスしないSVM管理専用のLIFを作成し、適切に設定されたフェイルオーバーグループにそのLIFを配置することを検討してください。iSCSIのデータLIFは移行されないため、この構成によって管理インターフェイスの高可用性が促進されます。

テナントのネットワーク分離

マルチテナンシーの重要な側面は、テナント間でセキュアに分離できるようにネットワークトラフィックを保護することです。エンタープライズ環境では共通のIPネットワークを共有する方が望ましい場合もありますが、共有インフラ環境内の個々のテナントで使用するSVMは、IPネットワークを共有しないように分離したままにしてください。どちらの目的も、ルーティンググループを使用することで達成できます。

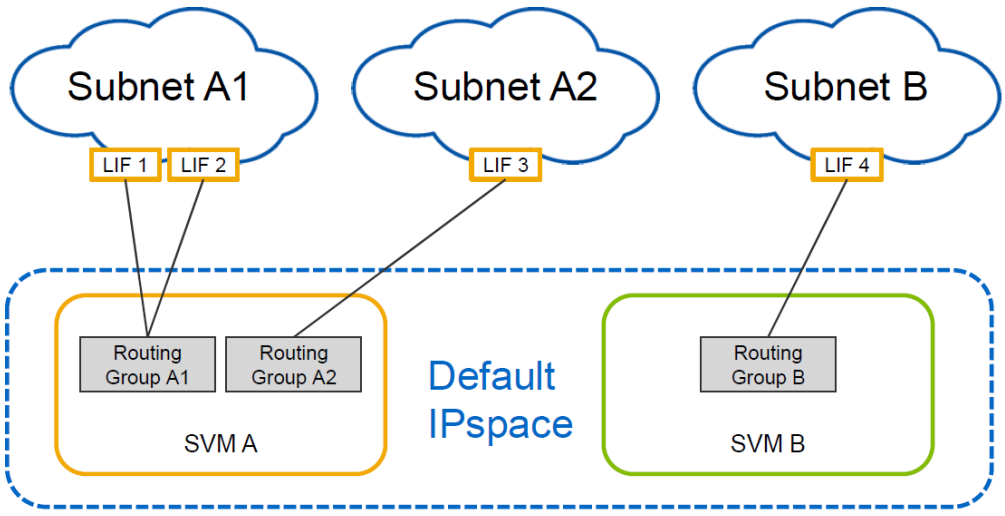
ルーティング グループ

ルーティンググループは、SVMに属するLIFのアウトバウンドネットワークトラフィックを制御するためにSVMで使用されます。各ルーティンググループは、個別のルーティングテーブルです。1つのSVMに複数のルーティンググループを設定することは可能ですが、SVM間でルーティンググループが共有されることはありません。SVMに属する各LIFは、1つのルーティンググループにのみ関連付けられます。同じSVMの複数のLIFは共通のルーティンググループを共有でき、同じIPサブネット上に配置する必要があります。ルーティンググループは、分離されたセキュアなトラフィック転送と、SVMを対象としたネットワークの管理と制御を実現します。

単一のIPネットワーク

企業の一般的な導入シナリオは、ワークロード、部門、または管理レベルでマルチテナンシーを提供することです。この使用例では、単一の企業全体のIPネットワークが展開されます。ここでは、特定のSVMに限定されたルーティンググループを使用して、パケット転送とネットワーク管理に必要な制御と分離を行うことができます。

図5）単一の企業全体のIPネットワーク

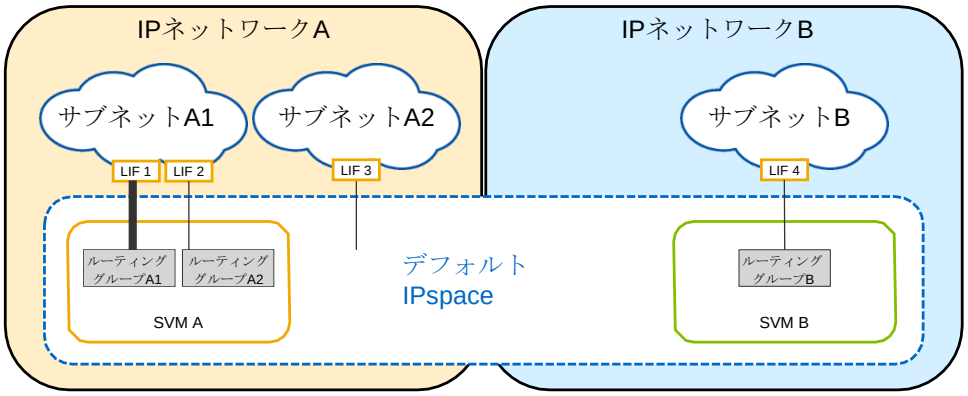


複数のIPネットワーク

セキュアなマルチテナントネットワーク構成のもう1つのユースケースは、テナントごとに一意のIPアドレス範囲を持つ分離されたIPネットワークを必要とする企業やサービスプロバイダです。たとえば、本番環境とは別のネットワークにテスト/開発用SVMを配置している企業や、DMZにデータをホストしている企業などです。この例では、各SVMは1つ以上のサブネットで構成される独自のIPネットワークに限定されます。クラスタの物理リソースをセキュアに拡張し、多数のセキュアなSVMを作成できるようにするために、SVM LIFをVLANインターフェイスの上に作成します。各ルーティンググループは個別のルーティングテーブルを表すため、トラフィックはSVM間でルーティングされません。

注： ここに示すサブネットは、別のVLANなど、異なるネットワークに完全に接続されている可能性があります。同じSVMに複数のLIFを使用して、複数のVLANに接続することができます。

図6）同一企業内の複数の非オーバーラップIPネットワーク



IPspaceを使用すると、複数のIPネットワークが必要で、テナント間で同一のIPアドレス範囲を再利用する構成が容易になります。

管理ネットワーク制御

事前定義されたSVM管理ロールを使用して委譲されたSVM管理者は、クラスタ管理者が使用できるネットワークコマンドの一部にしかアクセスできません。別の物理インターフェイスまたはVLANにLIFを移動できるのは、クラスタ管理者だけです。SVM管理者がLIFを無効なポートに誤って再割り当てすることがないため、これはSVM管理者にとって本質的に安全です。クラスタ管理者ロールを作成してクラスタを管理することもできますが、LIFを直接移動したり、LIFのフェイルオーバーグループやルーティンググループを変更したりすることは制限されます。このようなカスタムロールの例を次に示します。

```
cluster::> security login role show -role NoNetworkAccess
  (security login role show)
           Role          Command/                                        Access
Vserver    Name          Directory                                Query  Level
---------- ------------- ---------- ---------------------------------------- -----------
cluster NoNetworkAccess
                         DEFAULT                                           all
cluster NoNetworkAccess
                         network interface failover-groups                 none
cluster NoNetworkAccess
                         network interface migrate                         none
cluster NoNetworkAccess
                         network interface migrate-all                     none
cluster NoNetworkAccess
                         network routing-groups                            none
```

役割については、次のセクションで詳しく説明します。

ネットワークのベストプラクティスの詳細については、TR-4847：『Best Practices for Clustered Data ONTAPNetwork Configurations』を参照してください。

SVMのセキュリティ

ユーザとロール

管理ユーザ

ONTAPにはデフォルトの管理ユーザアカウントがあり、カスタマイズされた一連の権限を持つユーザを作成するための強力な手段もあります。デフォルトのクラスタ管理者は admin ユーザです。クラスタ管理者は、クラスタ全体とそのすべてのリソースを管理できます。SVMの場合、デフォルトの管理者は vsadmin ユーザです。vsadmin ユーザはSVMごとに作成されますが、SVMの管理を委譲するには明示的に有効にする必要があります。SVM管理者は、担当するSVMのみを管理できます。

ユーザロール

ONTAPのロールは、特定のコマンドディレクトリ、コマンドサブディレクトリ、またはコマンドに対してユーザに付与するアクセスのタイプを指定する一連のアクセス制御ルールです。

ONTAPには、クラスタとSVMの両方のコンテキスト用に事前定義されたロールがあります。

表2）デフォルトのクラスタユーザロール

ロール	Access Level（アクセス レベル）	機能
admin	すべて	すべて
readonly	読み取り専用	read-only
なし	なし	なし

表3）SVMユーザのデフォルトロール

ロール	デフォルトの機能
vsadmin	• 自分のユーザアカウントのローカルパスワードと公開鍵を管理します。 • ボリューム、クォータ、qtree、Snapshot™ コピー、FlexCache® ファイル、ファイルの管理 • NetApp SnapLock® の処理を実行（privileged deleteを除く） • LUNを管理します。 • データ保護ミラーを管理します。 • プロトコルの設定 • サービスの設定 • ジョブの監視 • ネットワーク接続とネットワーク インターフェイスの監視 • SVMの健全性の監視
vsadmin-volume	• 自分のユーザアカウントのローカルパスワードと公開鍵を管理します。 • ボリューム、クォータ、qtree、Snapshotコピー、FlexCacheファイル、ファイルの管理 • LUNを管理します。 • プロトコルの設定 • サービスの設定 • ネットワークインターフェイスの監視 • SVMの健全性の監視

ロール	デフォルトの機能
vsadmin-protocol	• 自分のユーザアカウントのローカルパスワードと公開鍵を管理します。 • プロトコルの設定 • サービスの設定 • LUNを管理します。 • ネットワークインターフェイスの監視 • SVMの健全性の監視
vsadmin-backup	• 自分のユーザアカウントのローカルパスワードと公開鍵を管理します。 • NDMP処理を管理します。 • リストアしたボリュームの作成（読み取り/書き込み） • NetApp SnapMirror® 関係とSnapshotコピーを管理します。 • ボリュームとネットワーク情報の表示
vsadmin-snaplock	• 自分のユーザアカウントのローカルパスワードと公開鍵を管理します。 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshotコピー、およびファイルを管理します。 • privileged deleteなどのSnapLock処理の実行 • プロトコルの設定 • サービスの設定 • ジョブの監視 • ネットワーク接続とネットワーク インターフェイスの監視
vsadmin-readonly	• 自分のユーザアカウントのローカルパスワードと公開鍵を管理します。 • SVMの健全性の監視 • ネットワーク インターフェイスの監視 • ボリュームとLUNの表示 • サービスとプロトコルの表示

カスタムユーザとカスタムロール

デフォルトのユーザとロールに加えて、追加のクラスタユーザとSVMユーザを作成したり、ユーザがアクセスできるコマンドを指定するカスタムロールを定義したりすることができます。

表7）ロールベースアクセス制御（RBAC）の定義

仕様	アクセス	説明
ディレクトリ/サブディレクトリ	すべて	ディレクトリ、およびディレクトリに含まれるすべてのサブディレクトリとコマンドへのアクセスを許可します。
	読み取り専用	ディレクトリおよびサブディレクトリへの読み取り専用アクセスを許可します。
	なし	ディレクトリ、およびそのディレクトリに含まれるすべてのサブディレクトリとコマンドへのアクセスを拒否します。
コマンド	すべて	コマンドの実行を許可します。

仕様	アクセス	説明
	なし	コマンドの実行を拒否します。

ロールは、一般的なものから特定のものまで階層的に定義されます。特定のコマンドまたはサブディレクトリに対して定義されたルールは、親ディレクトリに対して定義されたルールよりも優先されます。

CLIを使用したユーザの作成

新しいユーザを作成するには、 `security login create` コマンドを使用します。次の例では、ONTAPクラスタ上にローカルにユーザを作成し、セキュアシェル（SSH）を使用してパスワードを使用してログインしています。ドメインまたはLDAPユーザを指定したり、パスワードの代わりに公開鍵の使用を指定したりすることもできます。

```
cluster::> security login create -username newuser -application ssh -authmethod password -role
customrole -vserver vs1

Please enter a password for user 'newuser':
Please enter it again:

cluster::> security login show -vserver vs1 -username newuser

Vserver: vs1
                            Authentication                  Acct
UserName         Application Method         Role Name        Locked
---------------------- -------------- ------------------- ---------------------- --------
newuser          ssh         password       customrole       no
```

CLIを使用したロールの作成

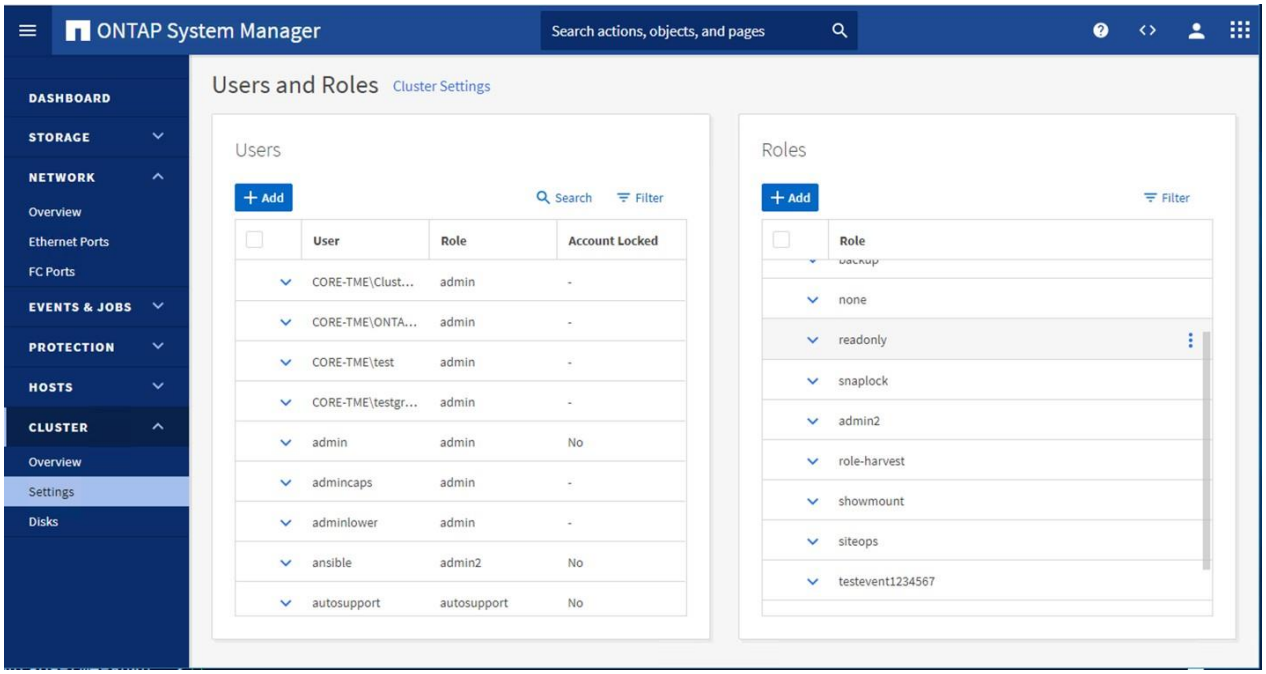
ロールは、CLIで `security login role create` コマンドを使用して作成します。ロールは一度に1つのルールを作成します。次の一連のコマンドを実行すると、前述のネットワーク管理のセクションで説明したカスタムロールが作成されます。

```
role create -vserver cluster -role NoNetworkAccess -cmddirname "network interface failover-
groups" -access none

role create -vserver cluster -role NoNetworkAccess -cmddirname "network interface migrate" -
access none

role create -vserver cluster -role NoNetworkAccess -cmddirname "network interface migrate-all" -
access none

role create -vserver cluster -role NoNetworkAccess -cmddirname "network routing-groups" -access
none

role modify -vserver cluster -role NoNetworkAccess -cmddirname DEFAULT -access all
```

ONTAP System Managerでのユーザとロールの作成

ONTAPシステムマネージャでカスタムロールを作成および編集するには、[クラスタ]->[設定]->[ユーザとロール]に移動します。

図7）ONTAPシステムマネージャのユーザとロール



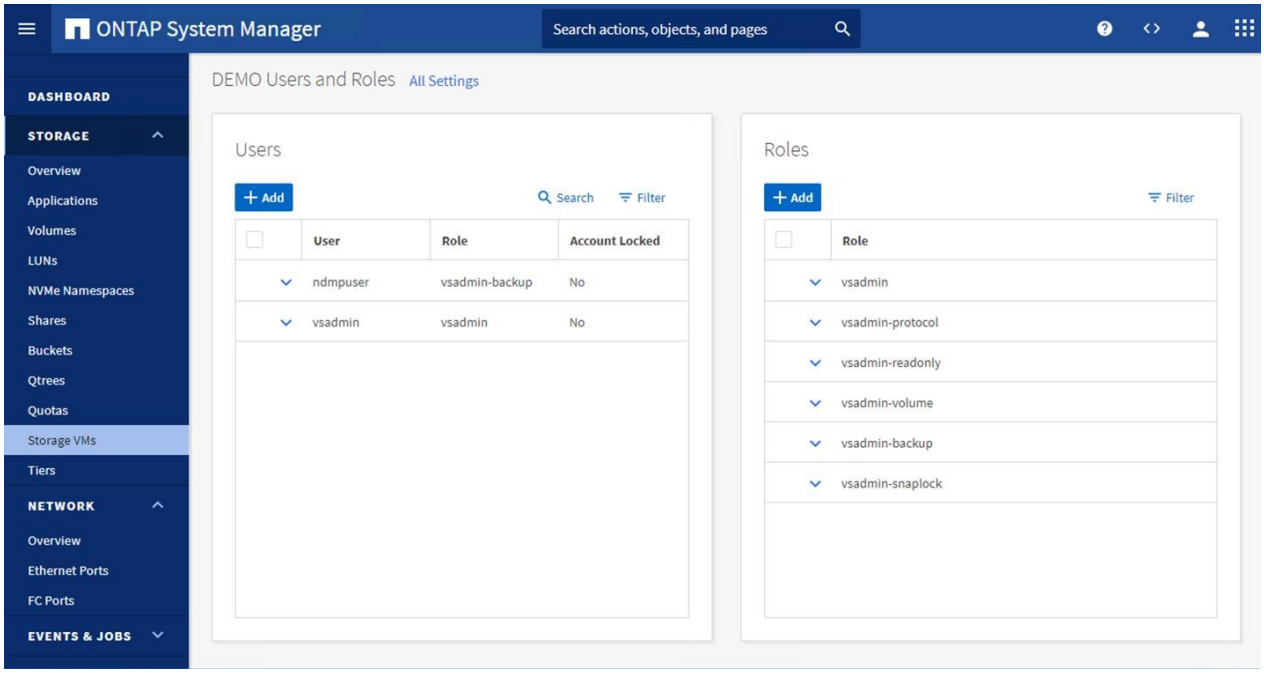
SVM管理者の委譲

クラスタレベルでの管理権限を持つユーザに加えて、各SVMに対して、その特定のSVMに対してのみ管理権限を持つアカウントを有効にすることができます。各SVMには、 `vsadmin` デフォルトで作成されたアカウントがありますが、明示的に有効にする必要があります。`vsadmin` アカウントを有効にするには、パスワードを割り当ててからアカウントのロックを解除します。

```
cluster::> security login password -username vsadmin -vserver vs1

Enter a new password:
Enter it again:

cluster::> security login unlock -username vsadmin -vserver vs1

cluster::> security login show -username vsadmin -vserver vs1

Vserver: vs1
                                Authentication                  Acct
UserName        Application     Method          Role Name       Locked
--------------- --------------- --------------- --------------- ------
vsadmin         ontapi          password        vsadmin         no
vsadmin         ssh             password        vsadmin         no
2 entries were displayed.
```

System ManagerからSVM管理者を有効にすることもできます。[Storage]、[Storage VM]<SVM name>、[Storage]、[Settings]、[Users and Roles]の順に選択します。

図8）SVM管理の委譲



アグリゲートの委譲

SVM管理者に管理アクセスを委譲する場合は、SVMが新しいフレキシブルボリュームのプロビジョニングに使用できるアグリゲートも委譲することが重要です。クラスタ管理者は、クラスタ内の任意のアグリゲートを使用して、SVM用の新しいボリュームを作成したり、既存のフレキシブルボリュームを再配置したりできます。ただし、SVM管理者は、そのSVMに委譲されたアグリゲートにのみ新しいボリュームを作成できます。委譲されたアグリゲートは `aggr_list`、SVMのオプションに表示されます。

CLIでは `vserver modify` 、クラスタ管理者はコマンドを使用してアグリゲートを委譲できます。

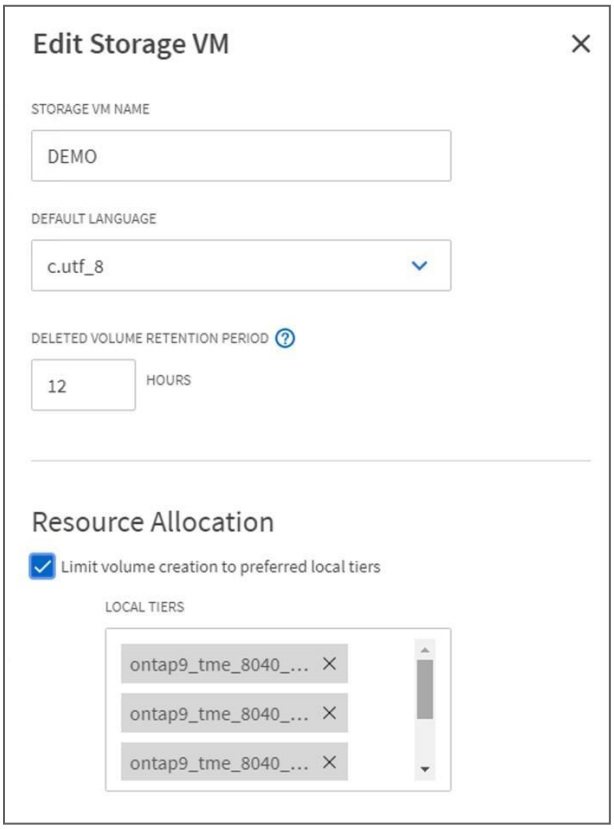
```
cluster::> vserver modify -vserver vs1 -aggr-list aggr_data1,aggr_data2
```

svm showコマンドを使用すると、割り当てられているアグリゲートを確認できます。

```
cluster::> vserver show -vserver vs1 -fields aggr-list
vserver aggr-list
---------- ----------------------------
Vs1     aggr_data1,aggr_data2
```

System Managerからアグリゲートを委譲することもできます。[Storage]<SVM name>、[Storage VMs]、[Storage VMs]、[Overview]、[Edit]の順に選択します。

図9）ボリューム作成時のアグリゲートの委譲



注：System Manager 9.8では、アグリゲートはローカル階層と呼ばれます。

ファイアウォールルール

ONTAPには、システムで使用可能な管理サービスプロトコルへのアクセスを制限する機能が含まれています。システム定義のファイアウォールポリシーが多数用意されており、 `system services firewall policy` コマンドディレクトリを使用してカスタムポリシーを作成できます。

次の例は、システム定義の `mgmt` ポリシーに適用されているファイアウォールルールを表示します。

```
system services firewall policy show -policy mgmt -vserver demo
Vserver Policy       Service    Allowed
-------------------- ---------- ----------------------------------------------------
demo
        mgmt
                     dns        0.0.0.0/0, ::/0
                     http       0.0.0.0/0, ::/0
                     https      0.0.0.0/0, ::/0
                     ndmp       0.0.0.0/0, ::/0
                     ndmps      0.0.0.0/0, ::/0
                     ntp        0.0.0.0/0, ::/0
                     portmap    0.0.0.0/0
                     snmp       0.0.0.0/0, ::/0
                     ssh        0.0.0.0/0, ::/0
```

`mgmt` ポリシーをベースとしてカスタムファイアウォールポリシーを作成するには `ystem services firewall policy clone`、コマンドを使用してポリシーをクローニングします。

```
system services firewall policy clone -policy mgmt -destination-policy mgmt-custom -vserver demo
-destination-vserver demo2
```

新しくクローニングしたファイアウォールポリシーをカスタマイズするには、system services firewall policy modifyコマンドを使用します。

たとえば、192.168.1.0/24サブネットからのみSSHアクセスを許可するには、次のコマンドを使用します。

```
system services firewall policy modify -policy mgmt-custom -service ssh -allow-list
192.168.1.0/24 -vserver demo2
system services firewall policy show mgmt-custom
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------------
demo2
        mgmt-custom
                     dns        0.0.0.0/0, ::/0
                     http       0.0.0.0/0, ::/0
                     https      0.0.0.0/0, ::/0
                     ndmp       0.0.0.0/0, ::/0
                     ndmps      0.0.0.0/0, ::/0
                     ntp        0.0.0.0/0, ::/0
                     portmap    0.0.0.0/0
                     snmp       0.0.0.0/0, ::/0
                     ssh        192.168.1.0/24
9 entries were displayed.
```

ファイアウォールポリシーをLIFに割り当てるには `-firewall-policy`、目的のLIFの属性を変更します。

```
cluster::> network interface modify -vserver vs1 -lif vs1_mgmt -firewall-policy mgmt-custom

cluster::> network interface show -vserver vs1 -lif vs1_mgmt

                    Vserver Name: vs1
          Logical Interface Name: vs1_mgmt
               (Deprecated)-Role: data
                   Data Protocol: nfs
                 Network Address: 192.168.1.1
                         Netmask: 255.255.255.0
            Bits in the Netmask: 24
                       Home Node: cluster-01
                       Home Port: e0a
                    Current Node: cluster-01
                    Current Port: e0a
              Operational Status: up
                 Extended Status: -
                      Numeric ID: 1025
                         Is Home: true
           Administrative Status: up
                 Failover Policy: nextavail
                 Firewall Policy: mgmt-custom
                     Auto Revert: false
   Fully Qualified DNS Zone Name: none
         DNS Query Listen Enable: false
             Failover Group Name: system-defined
                        FCP WWPN: -
                  Address family: ipv4
                         Comment: -
```

NetApp Volume Encryption（NVE）用のSVMを対象とした外部KMIPサーバ

ONTAP 9.6以降では、SVMスコープを使用して、クラスタ内の指定したSVMに対して外部キー管理を設定できます。この方法は、各テナントが異なるSVM（または一連のSVM）を使用してデータを提供するマルチテナント環境に最適です。特定のテナントのSVM管理者だけが、そのテナントのキーにアクセスできます。SVMを対象とした外部キー管理ツールは、クラスタを対象とした外部キー管理ツールと共存できます。オンボード キー管理はクラスタ スコープで設定でき、外部キー管理はSVMスコープで設定できます。`security key-manager key migrate` コマンドを使用すると、クラスタスコープのオンボードキー管理からSVMスコープの外部キー管理ツールにキーを移行できます。

NVE用のSVMを対象とした外部KMIPサーバの設定の詳細については、NetApp暗号化パワーガイドを参照してください。

SVMのパフォーマンスの監視と分離

ストレエシQoSノシヨウ

ONTAPにはストレージQuality of Service（QoS；サービス品質）機能が搭載されています。クラスタ管理者は、さまざまなストレージオブジェクトに対して最大スループットしきい値を設定してシステムパフォーマンスを管理できます。ストレージQoSポリシーをストレージオブジェクトに割り当てることで、オブジェクトが想定よりも多くのクラスタリソースを消費しないようにすることができます。

ストレージオブジェクト

次のストレージオブジェクトにストレージQoSポリシーを適用できます。

- SVM
- FlexVol
- LUN
- ファイル

ここでは、ストレージQoSポリシーをSVMレイヤで適用する方法について説明します。

ポリシーグループ

ポリシーグループは、特定のSVMのスループット制限を定義するために使用されます。スループット制限が設定されていないポリシーグループを作成して割り当てることもできます。これにより、制限を適用せずにSVMのスループットを監視できます。クラスタごとに最大12、000個のポリシーグループを作成でき、それらのグループには最大40、000個のストレージオブジェクトを割り当てることができます。

ポリシーグループは `qos policy-group create`、コマンドを使用して作成します。既存のグループは、`qos policy-group modify` コマンドを使用して変更できます。スループット制限は、IOPSまたはMB/秒を指標として定義できます。

```
cluster::> qos policy-group create -policy-group pg2 -vserver vs2 -max-throughput 1000iops

cluster::> qos policy-group modify -policy-group pg1 -max-throughput 1000MB/S
```

ポリシーグループは `qos policy-group show` 、コマンドを使用して表示できます。

```
cluster::> qos policy-group show
Name              Vserver     Class         Wklds Throughput    Is Shared
----------------- ----------- ------------- ----- ------------- ----------
pg1               vs1         user-defined 0     0-1000MB/S. true
pg2               vs2         user-defined -     0-1000IOPS. true
2 entries were displayed.
```

SVMへのストレージQoSポリシーグループの割り当て

ポリシーグループを定義したら `-qos-policy-group` 、SVMの属性を変更することでそのポリシーグループをSVMに割り当てることができます。

SVMごとに、1つのQoSポリシーグループに割り当てることができるストレージオブジェクトのタイプは1つだけです。SVM全体がポリシーグループに追加された場合、特定のボリュームやLUNをポリシーグループに追加することはできません。

ベスト プラクティス

クラスタ管理者は、ストレージQoSポリシーの使用方法をSVMレベルで標準化することで、テナントごとにスループットの上限を適用できるようになります。SVM管理者はボリュームとLUNを作成できますが、ストレージQoSポリシーの作成や割り当てはできないため、 SVMにポリシーを割り当てることで、クラスタ管理者は、特定のSVM内の各ストレージオブジェクトを最初に割り当てたあとで確実にストレージQoSポリシーの対象にすることができます。

次の例は、SVMレベルでQoSポリシーを適用する例を示しています。

```
cluster::> vserver modify -vserver vs1 -qos-policy-group pg1

cluster::> vserver show -vserver vs1 -fields qos-policy-group
vserver qos-policy-group
------- ----------------
vs1     pg1
```

QoSを使用したSVMのパフォーマンスの監視

ストレージオブジェクトがQoSポリシーグループに割り当てられている場合は、QoSワークロードが定義されます。QoSは `qos statistics`、コマンドと各種オプション（ワークロードの特性、レイテンシ、ディスク利用率、CPU利用率など）を使用して、ワークロードのパフォーマンスに関する詳細な情報を大量に提供します。詳細については、このドキュメントでは説明しません。詳細については、ONTAP QoS統計情報のドキュメントを参照してください。

データ保護

ONTAPは、同じクラスタ内またはピアクラスタにデータをレプリケートする手段を提供します。負荷共有ミラーとデータ保護ミラーの両方がサポートされます。ピアリングとミラーリングの詳細については、TR-4015：『SnapMirror Configuration and Best Practices Guide for ONTAP 9』を参照してください。

クラスタとSVMのピアリング

負荷共有とデータ保護のためにクラスタ内ボリュームミラーを作成することができます。ソースクラスタとデスティネーションクラスタの両方に特別なクラスタ間LIFが設定されていて、それらのクラスタがピア関係で接続されている場合は、クラスタ間ミラーを作成することもできます。2つのクラスタ間のレプリケーショントラフィックは、クラスタ間LIFを介して発生します。

ONTAPには、クラスタピアリングに加えてSVMピアリングの概念が含まれています。ピアクラスタ間のクラスタ内ミラーリングとクラスタ間ミラーリングの両方で、ソースボリュームとデスティネーションボリュームを含むSVMもピア関係にある必要があります。これにより、データ保護ミラーの制御をより細かく制御できるようになり、データ保護ミラーの制御をSVM管理者に委譲するための基盤が提供されます。

注： SVMのピア関係を設定できるのは、SVMが同じクラスタ内にある場合、またはSVMを含むクラスタのピア関係も設定されている場合のみです。

SVMピアは `vserver peer`、コマンドを使用して作成および表示できます。次の例は、同じクラスタの2つのSVM間にSVMピア関係を設定します。

```
cluster::> vserver peer create -vserver vs1 -peer-vserver vs2 -applications snapmirror

Info: 'vserver peer create' command is successful.

cluster::> vserver peer show-all
            Peer        Peer                                    Peering         Remote
Vserver     Vserver     State       Peer Cluster                Applications    Vserver
----------- ----------- ----------- --------------------------- --------------- -----------
vs1         vs2         peered      cluster                     snapmirror      vs2
vs2         vs1         peered      cluster                     snapmirror      vs1
2 entries were displayed.
```

ピア関係を設定する2つのSVMは同じクラスタ内にあるため、peer createコマンドの実行後に対処する必要はありません。ただし、ピア関係を設定するSVMがクラスタピア関係が確立された別々のクラスタにある場合、リモートクラスタのクラスタ管理者がピア関係を承認するまで、SVMピア関係は保留状態になります。

```
cluster2::> vserver peer show

            Peer        Peer
Vserver     Vserver     State
----------- ----------- ------------
vs1         vs3         pending
```

リモートクラスタ管理者は、SVMピア要求を承認するために `vserver peer accept` コマンドを問題する必要があります。

```
cluster2::> vserver peer accept -vserver vs1 -peervserver vs3
```

固有のSVMの命名要件

2つのSVMをピアリングするには、それらの名前がソースクラスタとデスティネーションクラスタの両方で一意である必要があります。たとえば、cluster1のvs1というSVMがcluster2のSVM vs2とピア関係にある場合、cluster1にvs2というSVMを作成することはできず、cluster2にvs1というSVMを作成することもできません。

ベスト プラクティス

ピア関係にあるクラスタ間でSVM名が一意になるような命名規則を採用します。そのためには、各SVMに完全修飾ドメイン名を使用して名前を付ける方法があります。

言語に関する考慮事項

ボリュームには、ボリュームが含まれているSVMとは異なる言語を使用できます。ボリュームの作成時に言語を指定しなかった場合、デフォルトでは、そのボリュームを含むSVMの言語が継承されます。ボリュームの作成時に別の言語を指定することもできます。SVMの言語は変更できますが、ボリュームの言語は変更できません。言語タイプが異なるSVM間でSnapMirrorコピーを実行することは可能ですが、ソースボリュームとデスティネーションボリュームは同じ言語でなければなりません。

ONTAP 8.2のSVMのデフォルトの言語はC.UTF-8です。この設定では、国に固有でないニュートラルなエンコードが提供されます。技術的な要件によって異なる言語エンコーディングの使用が規定されている場合を除き、C.UTF-8の使用を検討してください。

UTF-8エンコーディングは可変長です。UTF-8のバイトに特定のビットが存在するかどうかは、エンコードされた文字を構成するバイト数を示します。したがって、[language]で特定の特殊文字を使用すると、[language].UTF-8解析が使用されている場合に原因エラーが発生します。

次の見極めの質問を使用して、SVMの言語エンコーディングに最適なオプションを判断してください。

- 古いCIFSクライアント（Windows®95/95/ME）はありますか？「はい」の場合は、SVMの言語エンコーディングを[language]クライアントロケールに一致させます。
- UTF-8を使用していないNFSv2/3クライアントはありますか。「はい」の場合は、SVMの言語エンコーディングを[language]クライアントロケールに一致させます。
- Windows 95/98/ME以降のすべてのCIFSクライアントと、すべてのNFSクライアントでUTF-8ロケールが使用されているか。その場合は、SVMの言語エンコードをC.UTF-8に設定します。一部のクライアントがUTF-8を使用していない場合は、SVMの言語エンコードを[language]クライアントロケールに設定します。

表7に、SVMの言語の指定方法を示します。en_USは各例で使用されていますが、適切なクライアントロケールで置き換えることができます。

表4）SVMの言語に関する推奨事項

クライアント プロトコル	クライアントのエンコードの種類	SVMの言語に関する推奨事項
CIFS（Windows 95/98/ME）	ISO 8859-1	[language]を使用します。例：「en_US」

クライアント プロトコル	クライアントのエンコードの種類	SVMの言語に関する推奨事項
CIFS（Windows NT®3.1以降）	UCS-2	• すべてのクライアントがUTF-8を使用する場合は、C.UTF-8を使用します。 UTF-8を使用しないクライアントがある場合は、[language]を使用します。例：「en_US」
NFSv2 / 3	Non-UTF-8クライアントロケール	[language]を使用します。例：「en_US」
NFSv2 / 3	UTF-8クライアントロケール	C.UTF-8を使用します。
NFSv4	UTF-8	C.UTF-8を使用します。
FCまたはiSCSI	N/A	C.UTF-8を推奨。C/POSIXも許容される。

Unicode以外のクライアント言語エンコーディングが混在した環境では、SVMの言語エンコーディングが最も優先度の高いクライアント言語エンコーディングと一致している必要があります。

クライアントごとに同じファイルアクセスプロトコル（NFSv3など）を使用し、言語エンコードが異なる場合は、文字が正しく表示されないことがあります。クライアントに複数のクライアントロケールが混在している場合も同様です。

SVMの言語設定を選択する際は、次のベストプラクティスも考慮する必要があります。

- CIFSクライアントとNFSクライアントの両方を使用する環境の場合は、NFSクライアントの言語エンコーディングを一致させます。
- 「スマートクォート」や通貨記号など、ASCII以外の文字をファイル名に使用しないでください(たとえば、ユーロの場合は€、英国ポンドの場合は£)。
- UTF-8言語エンコーディングは、UTF-8以外のエンコーディングよりも優先されます。ただし、これが推奨されない状況があります。たとえば、NFSクライアントでUTF-8以外のエンコーディングを使用している場合は、SVMの言語も同じ非UTF-8エンコーディングに設定する必要があります。
- CIFSとNFSの間でファイルを共有する場合は、NFS文字セットに含まれるとの両方に有効な文字のみを使用してください。
- NFSv3からNFSv4に移行する場合は、SVMの言語がNFSv3クライアントの言語と同じである必要があります。
- SVM内のボリュームをSnapMirrorデスティネーションにする場合は、SnapMirrorソースとなるボリュームと同じ言語を選択します。

負荷共有ミラー

負荷共有（LS）ミラーは特殊なSnapMirrorです。CIFSまたはNFSv3を使用してアクセスするボリュームのパフォーマンスと可用性を向上できます。LSミラーを使用して、読み取り専用データセットの読み取りを複数のノードに分散できます。SVMルートボリュームの複数のインスタンスを作成する場合は、LSミラーを使用してSVMのネームスペースの可用性を高めることもできます。

クラスタの各ノードにSVMルートボリュームのLSミラーを作成すると、プライマリボリュームが使用できなくなった場合に使用できる冗長コピーが複数作成されます。ルートボリュームが一時的に使用できなくなっても、ボリュームへの読み取りアクセスはLSミラー経由で提供され、ネームスペースは引き続き使用できます。ルートボリュームが完全に使用できなくなった場合は、ミラーの1つを昇格して書き込みアクセスを可能にすることができます。

このレベルの可用性を達成するためには、いくつかのトレードオフを行う必要があります。SVMルートボリュームはSVMネームスペースルートの場所であるため、ルートでネームスペースにジャンクションされた新しいボリュームは、LSミラーセットが更新されるまで表示されません。required（`snapmirror update-ls-set`）コマンドはSVMレベルでは使用できないため、この更新はクラスタ管理者のみが実行できます。クラスタ管理者は、これらの更新を定期的に実行するようにスケジュールを設定できます。SVM管理者は、ミ

ラーセットが更新されたあとにのみネームスペースの更新が表示されることに注意してください。クラスタのクレデンシャルで処理し、ネームスペースを更新する自動化されたワークフローも、LSミラーセットを更新する必要があります。

ベスト プラクティス

耐障害性とネームスペースの可用性を高めるために、SVMルートボリューム用の負荷共有ミラーセットを作成することを検討してください。

データ保護ミラー

ONTAPでは、SnapMirrorデータ保護ミラーを作成することで、同じクラスタまたは別のクラスタ上のSVM間でボリュームを非同期でミラーリングできます。これらのデータ保護ミラーは、ローカルのバックアップコピーを維持するため、またはリモートでレプリケートされたコピーを提供するために使用され、ディザスタリカバリやビジネス継続性に使用できます。

SnapVaultによるバックアップ

NetApp SnapVault® 機能を使用すると、ソースボリュームとデスティネーションボリューム間でSnapshotを非対称に保持できます。ローカルのSnapshotコピーは短期的なバックアップとリカバリ用に保持し、SnapVaultコピーは長期的なアーカイブストレージ用に保持できます。

管理ツール CLI

カンリツールCLI

ONTAPコマンドラインインターフェイスは、クラスタ管理者とSVM管理者が使用できます。クラスタ管理者は、クラスタコンテキストでCLIにアクセスするために、SSHを使用してクラスタ管理LIFに接続できます。このコンテキストから、クラスタ全体およびクラスタ上の各SVMに関連する項目を管理者が管理できます。

SVM管理者は、SSHを使用して、SVMコンテキストのCLIに直接接続できます。このコンテキストから、アクセスが委譲されているSVMに直接関連する項目を管理できます。SVM管理者は、データプロトコルとサービス、ボリューム、LUN、qtreeなどのストレージオブジェクト、ボリュームのSnapshotコピーを管理し、SVMの全体的な健常性を監視できます。

CLIにログインしたクラスタ管理者は `vserver context` 、コマンドを使用してSVMコンテキストに切り替えることができます。

現在のところ、SVM管理者が使用できる対話型の管理ツールはコマンドラインインターフェイスだけです。

注： ONTAPでは、最大250の同時SSHセッションがあります。

NetApp Manageability SDK

ONTAPには、NetApp Manageability SDKを通じて利用できる豊富なAPIセットが含まれています。SDKには、C、C++、Java®、Perl、C#、 VB.NET、Windows PowerShell™、Python、およびRubyです。これらのAPIを使用して、ONTAP管理を既存のオーケストレーションツールと統合したり、カスタムの管理ポータルを作成したりできます。

ONTAP PowerShellツールキット

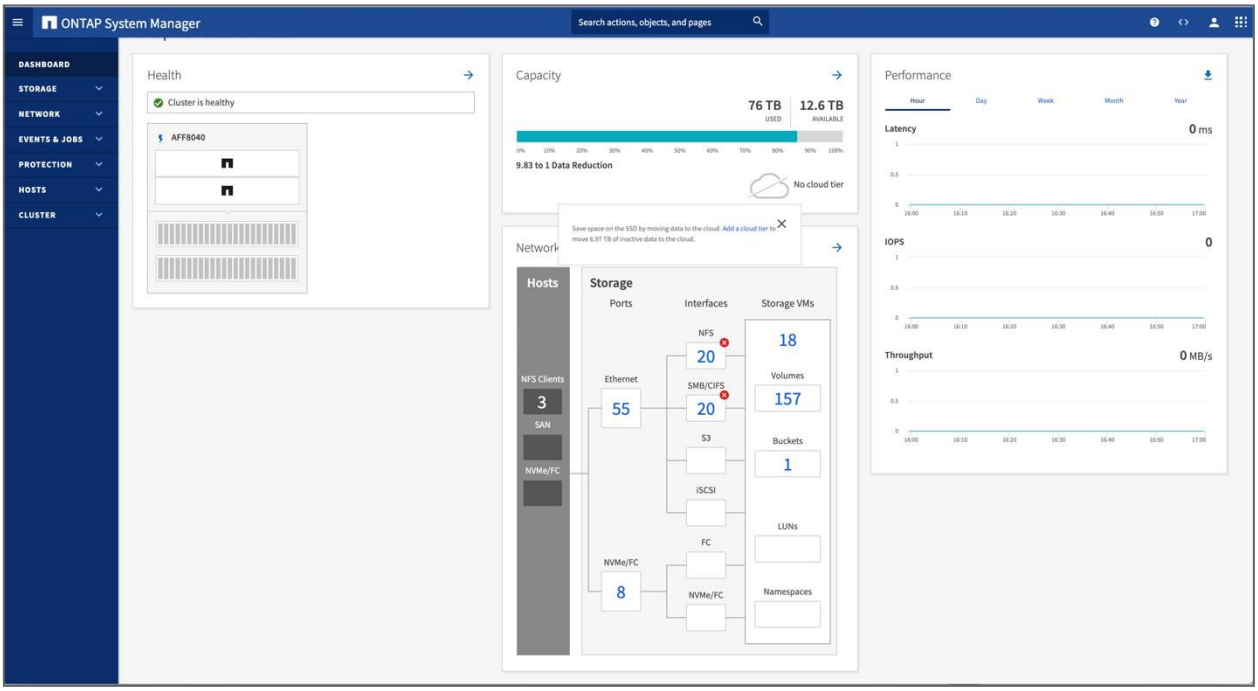
Windows PowerShellを使用した管理と自動化を希望されるお客様には、NetAppにはONTAPで使用できる強力なコマンドレットセットが用意されています。NetAppコミュニティポータルから利用できるONTAP PowerShell Toolkitは、クラスタとSVMを同様に管理するための強力で用途の広い手段です。詳細については、「Data ONTAP PowerShell Toolkitを最大限に活用する」を参照してください。

ONTAP System Manager

NetApp ONTAPシステムマネージャは、グラフィカルなWebベースの管理ツールです。ストレージシステムとストレージオブジェクトをGUIベースで管理できます。データプロトコルの設定、ストレージオブジェクトのプロビジョニング、SVMの作成と管理などが可能です。

注： System Managerへのログインは、クラスタ管理者のみが使用できます。

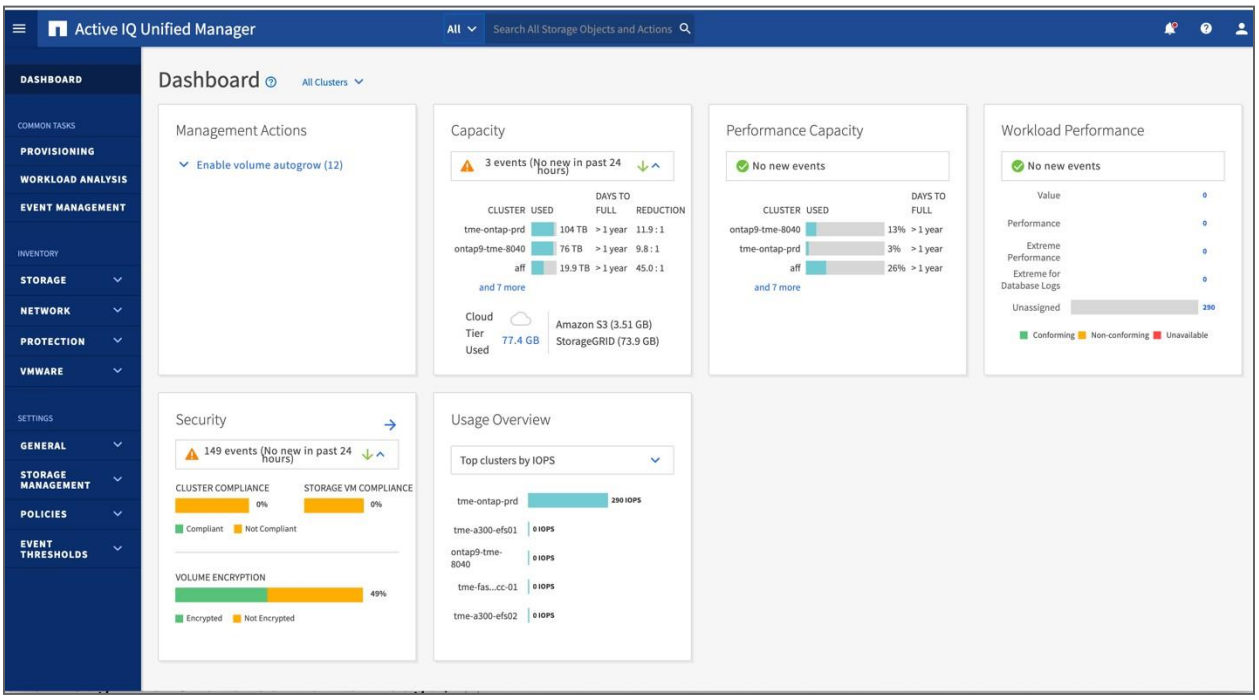
図10）ONTAPシステムマネージャ



Active IQ Unified Manager

Active IQ Unified Managerは、複数の環境の複数のクラスタを管理するための一元化されたインターフェイスです。大規模なストレージインフラを監視、アラート、レポートする機能が含まれています。Active IQ Unified Managerの詳細については、NetAppのドキュメントサイトを参照してください。

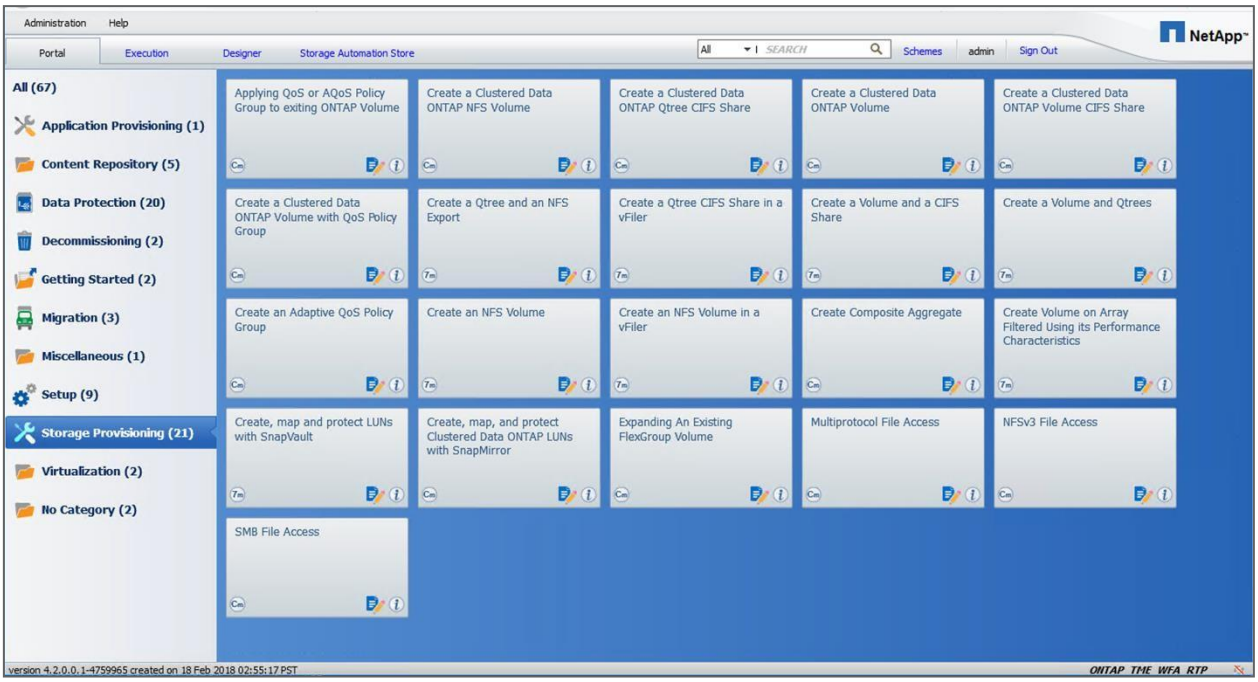
図11）Active IQ Unified Manager



OnCommand Workflow Automation

OnCommand Workflow Automation（OnCommand WFA）は、ストレージ自動化のための強力なツールです。OnCommand WFAを使用すると、ストレージ管理者は、カスタムワークフローを作成、テスト、公開して、さまざまなストレージ機能やタスクを実行できます。OnCommand WFAの詳細については、OnCommand Workflow Automationドキュメントリソースページを参照してください。

図12）OnCommand Workflow Automationポータル



詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントやWebサイトを参照してください。

- ONTAP 9ドキュメント センター
  http://docs.netapp.com/ontap-9/index.jsp

バージョン履歴

バージョン	日付	ドキュメント バージョン履歴
バージョン1.0	2013年7月	ONTAP 9より前のリリース
バージョン1.1	2020年12月	ONTAP 9用に更新
バージョン1.2	2021年1月	IPspaceの更新

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4160-0121-JP

NetApp