



NetApp上の VMware Cloud Foundation

NetApp virtualization solutions

NetApp
August 24, 2025

目次

NetApp上の VMware Cloud Foundation	1
VMware Cloud Foundation とONTAPでハイブリッド クラウド エクスペリエンスを簡素化	1
はじめに	1
NetApp ONTAPの紹介	1
VMware Cloud Foundation の概要	1
VCF ドメイン	2
VCFによるストレージ	3
ONTAPがVCFに選ばれる理由	3
追加情報	4
まとめ	5
ドキュメントリソース	5
VMware Cloud Foundation とONTAP を使用した設計オプション	6
ストレージオプション	6
設計図	7
VMware Cloud Foundation とONTAPを使用してプライベート クラウド環境をセットアップする	11
新しいVCF 9インスタンスをデプロイする	11
既存のコンポーネントをVCF 9に統合	13
既存のVCF環境をVCF 9にアップグレードする	14
NetApp SnapMirrorとBlueXP DRaaSによる災害復旧の実装	14
開始	16
BlueXP disaster recovery構成	17
ソースサイトアレイと宛先サイトアレイ間のストレージレプリケーションの構成	17
VMware Disaster Recoveryの設定方法	18
BlueXP disaster recoveryは何を実現できるのでしょうか?	18
テストフェイルオーバー	23
クリーンアップフェイルオーバーテスト操作	25
計画的な移行とフェイルオーバー	26
フェイルバック	27
監視とダッシュボード	29
既存の vSphere クラスタを VCF に変換する	30
既存のデータストアを持つ vSphere 環境を VCF に変換する方法について学習します。	30
vCenter Server インスタンスを VCF 管理ドメイン (NFS データストア) に変換する	30
vCenter Server インスタンスを VCF 管理ドメイン (FC データストア) に変換する	44
VCFにプリンシパルストレージをプロビジョニングする	59
ONTAPを主要ストレージソリューションとしてVCF環境をプロビジョニングする	59
ONTAP上のFCベースのVMFSデータストアをVCF管理ドメインの主ストレージとして使用する	59
ONTAP上のNFSデータストアをVCF管理ドメインの主ストレージとして使用する	60
ONTAP上のFCベースのVMFSデータストアを	
VIワークロードドメインの主ストレージとして使用する	62

ONTAP上の NFS データストアを VI ワークロード ドメインの主ストレージとして使用する	64
補助ストレージでVCFを拡張	85
補助ストレージを使用して VCF 環境のストレージを拡張する方法について説明します。	85
ONTAP tools for VMware vSphereを使用して、管理ドメインの補助ストレージとして iSCSI データストアを追加します。	85
ONTAP tools for VMware vSphereを使用して、管理ドメインの補助ストレージとして FC ベースの VMFS データストアを追加します。	110
ONTAP tools for VMware vSphereを使用して、VI ワークロード ドメインに補助ストレージとしてvVols を追加します。	111
ONTAP tools for VMware vSphereを使用して、VI ワークロード ドメインに NFS とvVols を補助ストレージとして追加します。	139
VIワークロードドメインに補助ストレージとしてNVMe over TCPを追加する	164
FCベースのVMFSデータストアをVIワークロードドメインの補助ストレージとして追加する	188
SnapCenterでVCFを保護する	189
VMware vSphere 向けSnapCenterプラグインを使用して VCF ワークロード ドメインを保護する方法について学習します。	189
VMware vSphere 用のSnapCenterプラグインを使用して VCF ワークロード ドメインを保護する	190
VMware vSphere 用のSnapCenterプラグインを使用して VCF 管理ドメインとワークロード ドメインを保護する	225
NVMe over TCP ストレージと VMware vSphere 向けSnapCenterプラグインを使用して VCF ワークロード ドメインを保護します。	238
BlueXPでVMwareデータストアを保護する	245
BlueXP disaster recoveryを使用した VMware データストアの保護について学習します	245
VMware vSphere およびBlueXP backup and recoveryのSnapCenterプラグインを使用して、VMware の 3-2-1 データ保護を構成します。	245
BlueXP disaster recoveryを使用して VMFS データストアのディザスタリカバリを設定する	290
BlueXP disaster recoveryを使用して NFS データストアの災害復旧を設定する	309
vSphere Metro Storage Clusterでワークロードを保護する	330
ONTAP高可用性と VMware vSphere Metro Storage Cluster (vMSC) の統合について学習します。	330
MetroClusterを使用して VCF 管理ドメインのストレッチ クラスタを構成する	331
MetroClusterを使用して VI ワークロード ドメインのストレッチ クラスタを構成する	342
SnapMirror Active Syncを使用してVCF管理ドメインのストレッチクラスタを構成する	354
SnapMirror Active Syncを使用してVIワークロードドメインのストレッチクラスタを構成する	356
VMware vSphere からONTAPデータストアに VM を移行する	358
ネットワーク要件	359
VM移行シナリオ	361
VM テンプレートの移行シナリオ	386
ユースケース	393
参考資料	394
NFSストレージ向けの自律型ランサムウェア防御	394
Data Infrastructure Insightsでオンプレミス ストレージを監視する	404
Data Infrastructure Insightsサイトによるオンプレミスストレージの監視	404

ソリューション展開の概要	404
前提条件	405
ソリューションの展開	405
まとめ	422
追加情報	422

NetApp上の VMware Cloud Foundation

VMware Cloud Foundation とONTAPでハイブリッド クラウド エクスペリエンスを簡素化

NetApp ONTAP はVMware Cloud Foundation (VCF) と統合され、ブロック プロトコルとファイル プロトコルの両方をサポートする統合ストレージソリューションを提供します。この統合により、ハイブリッド クラウドの展開が簡素化され、データ管理とパフォーマンスが向上し、オンプレミスとクラウド環境全体で一貫したデータ サービスが確保されます。

はじめに

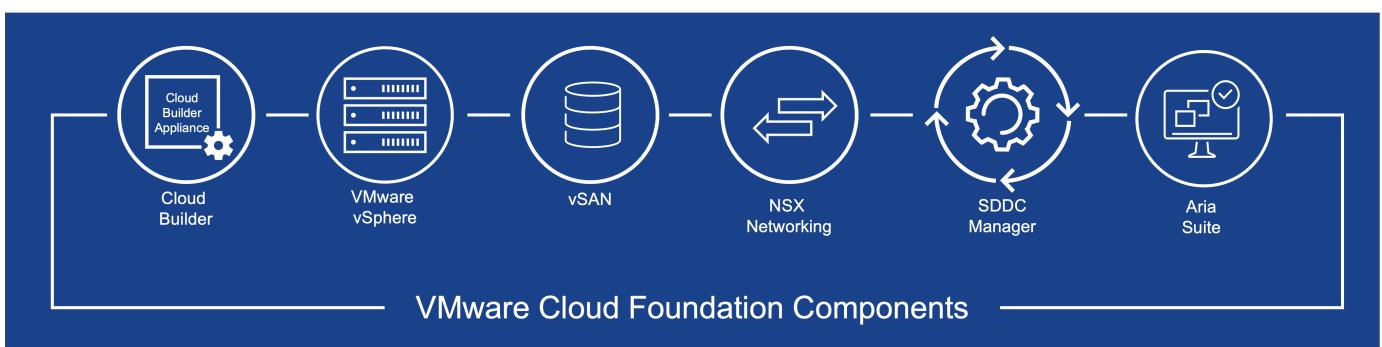
NetApp をVCF と併用すると、重複排除、圧縮、スナップショットなどの NetApp の高度な機能を通じて、データ管理とストレージ効率が向上します。この組み合わせにより、仮想化環境にシームレスな統合、高パフォーマンス、およびスケーラビリティが実現します。さらに、オンプレミスとクラウド インフラストラクチャ全体で一貫したデータ サービスと管理を可能にすることで、ハイブリッド クラウドの展開を簡素化します。

NetApp ONTAPの紹介

NetApp ONTAPは、幅広い製品ラインにわたって高度なストレージ機能を提供する包括的なデータ管理ソフトウェアです。ONTAPは、ソフトウェア定義ストレージとして、主要なクラウド プロバイダーによるファーストパーティ サービスとして、またNetApp ASA (All San Array)、AFF (All-flash FAS)、FAS (Fabric-Attached Storage) プラットフォームのストレージ OS として利用できます。ONTAPは、サイロを作成することなく、VMware 仮想化を含むさまざまなユース ケースで高パフォーマンスと低レイテンシを実現します。

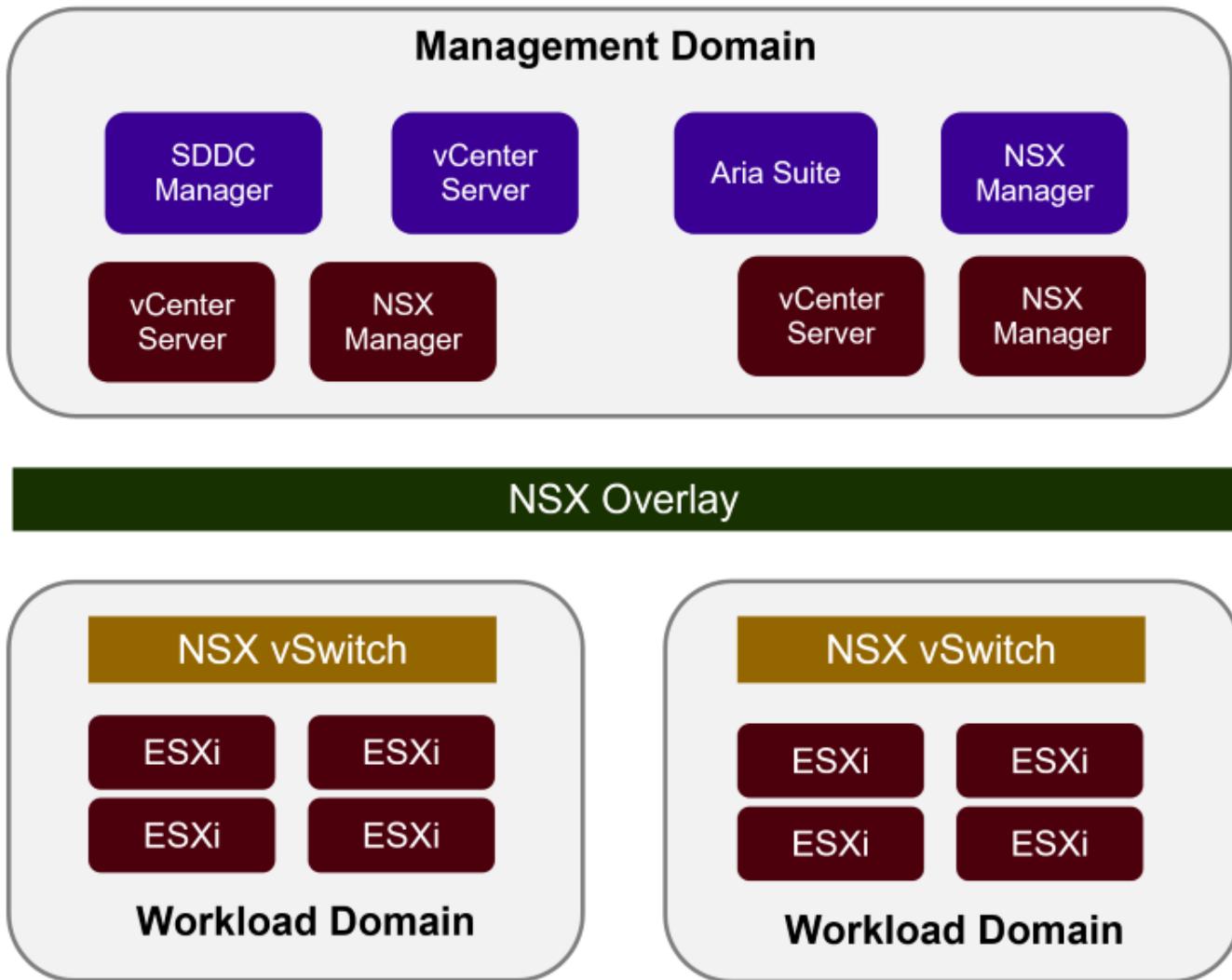
VMware Cloud Foundation の概要

VCFは、コンピューティング、ネットワーク、ストレージ オファリングを VMware 製品およびサードパーティ統合と統合し、ネイティブ Kubernetes と仮想マシンベースのワークロードの両方を容易にします。このソフトウェア プラットフォームには、VMware vSphere、NSX、Aria Suite Enterprise、Tanzu Kubernetes Grid、HCX Enterprise、SDDC Managerなどの主要コンポーネントと、vSAN 経由でホスト CPU コアにリンクされたストレージ容量が含まれています。NetApp ONTAPは、オンプレミスとパブリック クラウドの両方で、さまざまな VCF 導入モデルとシームレスに統合されます。



VCF ドメイン

ドメインは、VCF 内の基本的な構成要素であり、リソースを個別の独立したグループに編成することを可能にします。ドメインはインフラストラクチャをより効率的に整理し、リソースが効率的に利用されるようにするのに役立ちます。各ドメインは、独自のコンピューティング、ネットワーク、およびストレージ要素とともに展開されます。



VCF には主に 2 つのタイプのドメインがあります。

- ・ 管理ドメイン – 管理ドメインには、VCF 環境のコア機能を担当するコンポーネントが含まれます。コンポーネントは、リソースのプロビジョニング、監視、メンテナンスなどの重要なタスクを処理し、NetApp ONTAP Tools for VMware などのサードパーティ プラグインの統合が含まれます。管理ドメインは、ベスト プラクティスに従うために Cloud Builder Appliance を使用して展開することも、既存の vCenter 環境を VCF 管理ドメインに変換することもできます。
- ・ 仮想インフラストラクチャ ワークロード ドメイン – 仮想インフラストラクチャ ワークロード ドメインは、特定の運用ニーズ、ワークロード、または組織専用のリソース プールとして設計されています。ワークロード ドメインは SDDC マネージャーを介して簡単に展開され、一連の複雑なタスクを自動化するのに役立ちます。VCF 環境内に最大 24 個のワークロード ドメインをプロビジョニングでき、各ドメインはアプリケーション対応インフラストラクチャのユニットを表します。

VCFによるストレージ

ドメインの機能の中心となるのは、ドメインが消費するストレージです。VCFにはハイパーコンバージド ユースケース向けの CPU コアベースの vSAN 容量が含まれているだけでなく、幅広い外部ストレージソリューションもサポートしています。この柔軟性は、既存のストレージアレイに多額の投資を行っている企業や、vSAN がサポートできる範囲を超えたプロトコルをサポートする必要がある企業にとって非常に重要です。VMwareは、VCFで複数のストレージタイプをサポートしています。

VCFには主に2つのタイプのストレージがあります。

- ・**プリンシパルストレージ** – このストレージタイプは、ドメインの初期作成時に割り当てられます。管理ドメインの場合、このストレージには VCF 管理および運用コンポーネントが格納されます。ワークロード ドメインの場合、このストレージは、ドメインが展開されたワークロード、VM、またはコンテナーをサポートするように設計されています。
- ・**補足ストレージ** – 補足ストレージは、デプロイメント後に任意のワークロード ドメインに追加できます。このストレージタイプは、組織がストレージインフラストラクチャへの既存の投資を活用し、さまざまなストレージテクノロジーを統合して、パフォーマンス、スケーラビリティ、コスト効率を最適化するのに役立ちます。

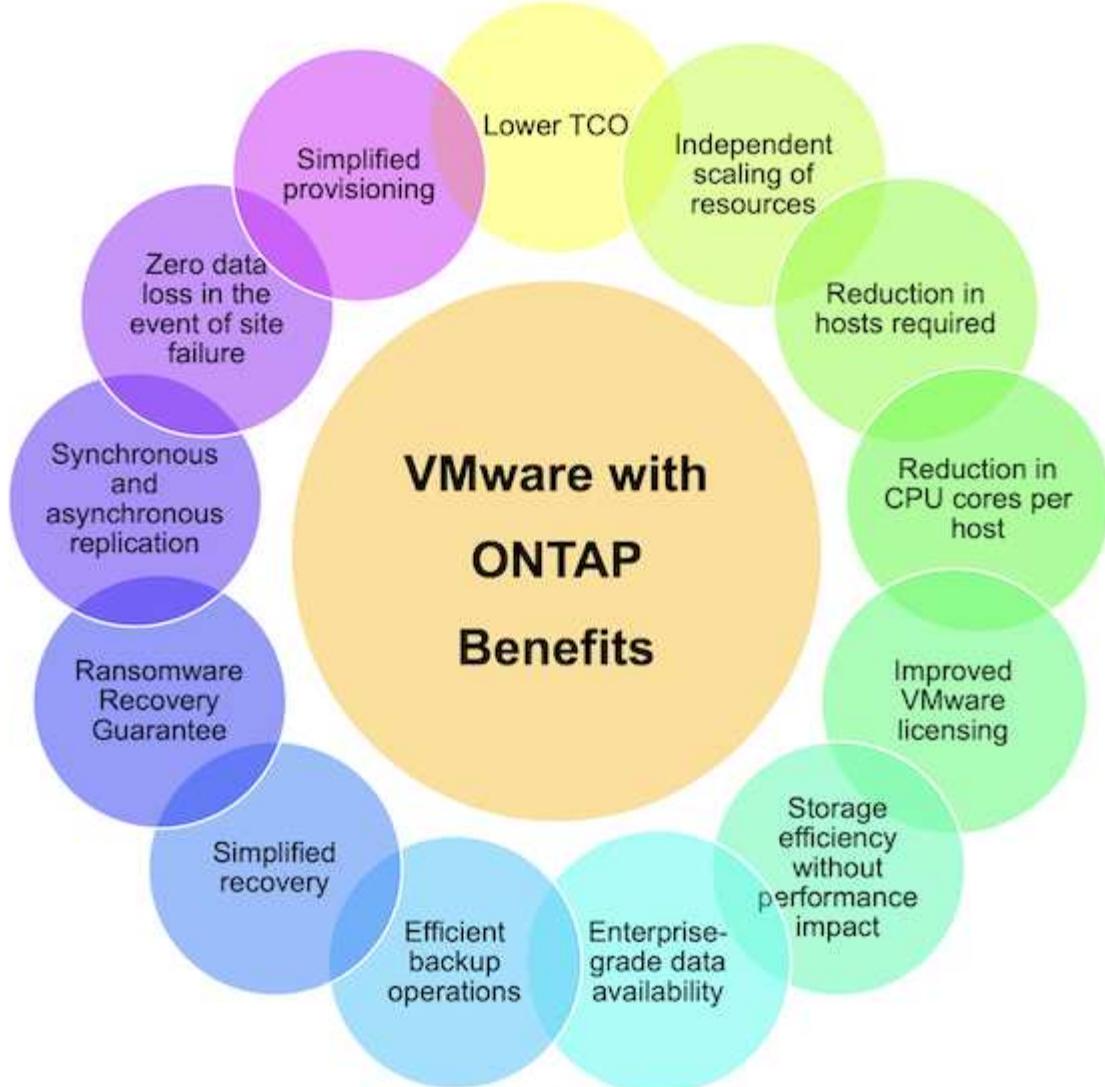
VCFストレージタイプをサポート

ドメインタイプ	プリンシパルストレージ	補助ストレージ
管理ドメイン	vSAN FC* NFS*	vVols (FC、iSCSI、または NFS) FC NFS iSCSI NVMe/TCP NVMe/FC NVMe/RDMA
仮想インフラストラクチャワークロードドメイン	vSAN vVols (FC、iSCSI、または NFS) FC NFS	vVols (FC、iSCSI、または NFS) FC NFS iSCSI NVMe/TCP NVMe/FC NVMe/RDMA

注: * 既存の vSphere 環境で VCF インポートツールを使用する場合、特定のプロトコルサポートが提供されます。

ONTAPがVCFに選ばれる理由

投資保護やマルチプロトコルサポートを含むユースケースに加えて、VCF ワークロード ドメイン内で外部共有ストレージを活用する理由は他にも多数あります。ワークロード ドメイン用にプロビジョニングされたストレージは、VMとコンテナをホストするためのリポジトリにすぎないと考えられるかもしれません。ただし、組織のニーズがライセンス容量の能力を超え、エンタープライズストレージが必要になることがよくあります。ONTAPによって提供され、VCF内のドメインに割り当てられるストレージは、導入が簡単で、将来を見据えた共有ストレージソリューションを提供します。



以下に挙げたVMware VCFにおけるONTAPの主なメリットの詳細については、以下を参照してください。["ONTAP for VMwareを選ぶ理由"](#)。

- ・初日から拡張まで柔軟に対応
- ・ストレージタスクをONTAPにオフロードする
- ・クラス最高のストレージ効率
- ・エンタープライズグレードのデータ可用性
- ・効率的なバックアップとリカバリ操作
- ・包括的な事業継続機能

追加情報

- ・"NetAppストレージ オプション"
- ・"vSphere Metro Storage Cluster (vMSC) のサポート"
- ・"ONTAP Tools for VMware vSphere"

- ・ "ONTAPを使用した VMware 自動化"
- ・ "NetApp SnapCenter"
- ・ "VMware と NetAppによるハイブリッド マルチクラウド"
- ・ "セキュリティとランサムウェア対策"
- ・ "VMwareワークロードをNetAppに簡単に移行"
- ・ "BlueXP災害復旧"
- ・ "データインフラストラクチャの洞察"
- ・ "VMデータコレクター"

まとめ

ONTAP は、すべてのワークロード要件に対応するプラットフォームを提供し、カスタマイズされたブロックストレージソリューションと統合されたサービスを提供することを通じて、信頼性とセキュリティに優れた方法で VM とアプリケーションの結果をより迅速に実現します。ONTAP には、データセンターの占有スペースを最小限に抑える高度なデータ削減および移動技術が組み込まれており、同時にエンタープライズ レベルの可用性を確保して重要なワークロードをオンライン状態に維持します。さらに、AWS、Azure、Google は、VMware-in-the-Cloud サービスの一部として、VMware クラウドベース クラスタ内での vSAN ストレージを強化するために、NetApp搭載の外部ストレージをサポートしています。全体的に、NetApp の優れた機能により、VMware Cloud Foundation の導入にとってより効果的な選択肢となります。

ドキュメントリソース

VMware Cloud Foundation 向けのNetAppサービスの詳細については、以下を参照してください。

VMware Cloud Foundation ドキュメント

- ・ "VMware Cloud Foundation ドキュメント"
- ・ NetAppを使用したVCFに関する4部構成のブログシリーズ*
- ・ "NetAppと VMware Cloud Foundation を簡単にするパート 1: はじめに"
- ・ "NetAppと VMware Cloud Foundation を簡単にするパート 2: VCF とONTAP の主要ストレージ"
- ・ "NetAppと VMware Cloud Foundation を簡単にするパート 3: VCF と Element のプリンシパル ストレージ"
- ・ "NetAppと VMware Cloud Foundation を簡単に - パート 4: VMware と補助ストレージ用のONTAPツール"

VMware Cloud Foundation とNetAppオールフラッシュ SAN アレイ

- ・ "NetApp ASAアレイを使用したVCFの紹介と技術概要"
- ・ "管理ドメインの主要ストレージとして FC 搭載ONTAP を使用する"
- ・ "VIワークロードドメインのプライマリストレージとしてFC搭載のONTAPを使用する"
- ・ "Ontap ツールを使用して、VCF 管理ドメインに iSCSI データストアを開きます。"
- ・ "Ontap ツールを使用して、VCF 管理ドメインに FC データストアを開きます。"
- ・ "Ontap ツールを使用して、VI ワークロード ドメインにvVols (iSCSI) データストアを開きます。"

- "VI ワークロード ドメインで使用するために NVMe over TCP データストアを構成する"
- "SnapCenter Plug-in for VMware vSphere を導入して使用し、VI ワークロード ドメイン内の VM を保護および復元します。"
- "SnapCenter Plug-in for VMware vSphere を導入して使用し、VI ワークロード ドメイン (NVMe/TCP データストア) 内の VM を保護および復元します。"

VMware Cloud Foundation と NetApp オールフラッシュ AFF アレイ

- "NetApp AFF アレイを搭載した VCF の紹介と技術概要"
- "管理ドメインの主要ストレージとして NFS を搭載した ONTAP を使用する"
- "VI ワークロード ドメインの主要ストレージとして NFS を搭載した ONTAP を使用する"
- "ONTAP ツールを使用して、VI ワークロード ドメインに vVols (NFS) データストアを展開します。"
- VMware Cloud Foundation 向け NetApp FlexPod ソリューション*
- "VMware Cloud Foundation による FlexPod ハイブリッド クラウドの拡張"
- "VMware Cloud Foundation のワークロード ドメインとしての FlexPod"
- "VMware Cloud Foundation のワークロード ドメインとしての FlexPod 設計ガイド"

VMware Cloud Foundation と ONTAP を使用した 設計オプション

VCF 9 を新規に開始することも、既存のデプロイメントを再利用して、VCF 9 と ONTAP を使用したプライベート クラウド環境を作成することもできます。VCF 9 の一般的な設計ブループリントと、NetApp 製品がどのように価値を高めるかについて学習します。

ストレージオプション

VMware Cloud Foundation with ONTAP は、さまざまなパフォーマンス、スケーラビリティ、可用性の要件を満たすために、さまざまなストレージ構成をサポートしています。次の表は、ご使用の環境で使用できる主なストレージ オプションと補足ストレージ オプションをまとめたものです。

製品ファミリー	FC 上の VMFS	NFSv3
ASA A シリーズおよび C シリーズ	はい	いいえ
AFF A シリーズおよび C シリーズ	はい	はい
FAS	はい	はい

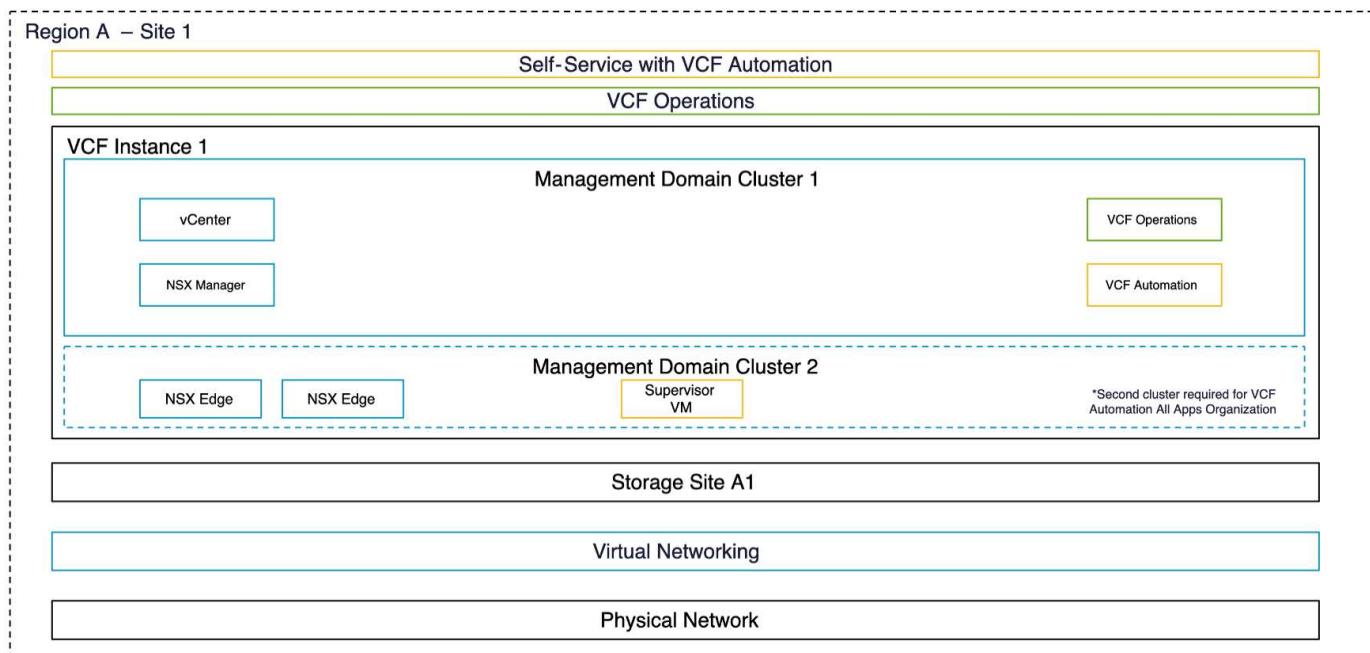
製品ファミリー	FC 上の VMFS	iSCSI 上の VMFS	NVMe-oF 上の VMFS	NFSv3	NFSv4.1
ASA A シリーズおよび C シリーズ	はい	はい	はい	いいえ	いいえ
AFF A シリーズおよび C シリーズ	はい	はい	はい	はい	はい
FAS	はい	はい	はい	はい	はい

設計図

次のブループリントは、さまざまなサイトおよびリソースのシナリオにおける VMware Cloud Foundation およびONTAPの一般的な展開モデルを示しています。

最小限の設置面積で単一のサイトにVCF艦隊を配備

この設計ブループリントは、最小限のリソースで单一の vSphere クラスタに管理コンポーネントとワークロード コンポーネントを展開するためのものです。 VMFS および NFSv3 プリンシパル データストアと、2 ノード構成によるシンプルな導入オプションをサポートします。 All Apps 組織モデルで VCF Automation を使用する予定の場合は、vSphere Supervisor ノードと NSX Edge ノードを展開するための 2 番目のクラスタが必要です。



リソースの消費を最小限に抑えるには、可能な場合は既存のONTAPツール インスタンスを使用します。利用できない場合は、Small プロファイルの單一ノードが適しています。 SnapCenter Plug-in for VMware vSphereは、ネイティブ スナップショットと別のONTAPストレージ アレイへのレプリケーションを使用して、仮想マシンとデータストアを保護します。



VCF を調査するためのリソースが不足している場合は、多くのクラウド プロバイダーが VCF をサービスとして提供しており、ONTAP はクラウド プロバイダーのファーストパーティ サービスとして利用できます。

このデザインの詳細については、["最小限の設置面積で単一のサイトにVCFフリートに関するBroadcomの技術文書を集約"](#)。

単一サイトでのVCF艦隊

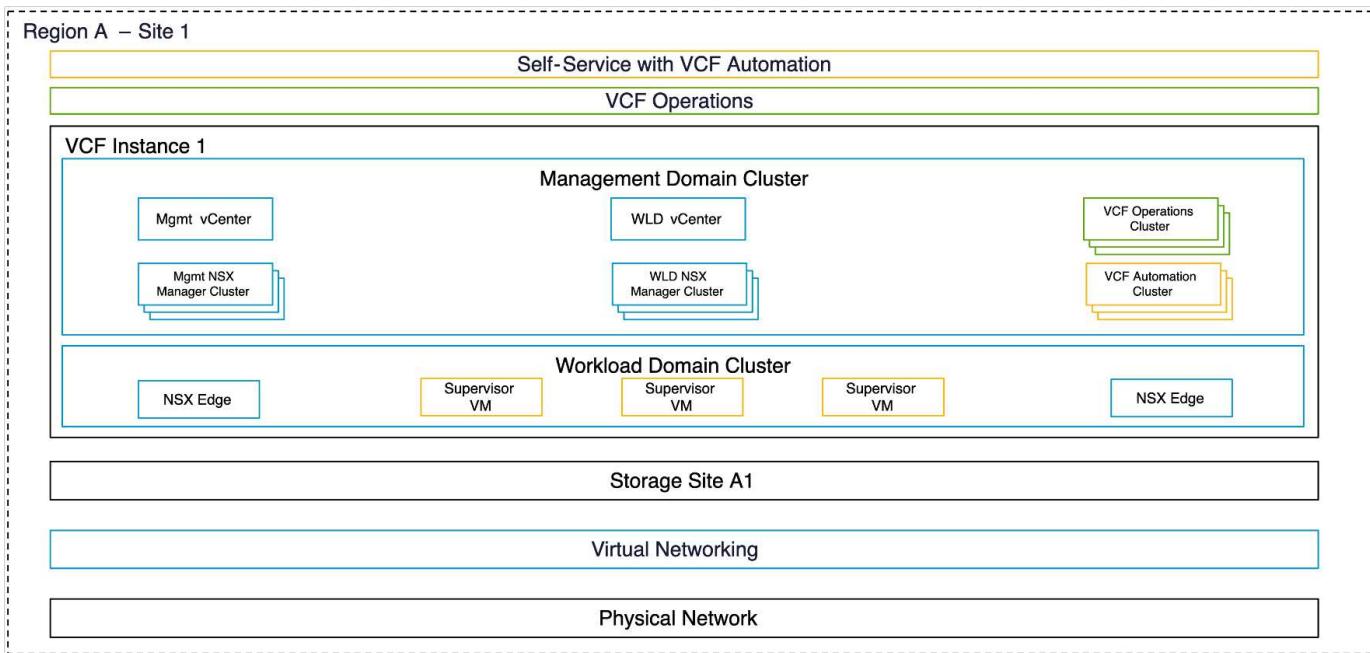
この設計ブループリントは、アプリケーションの高可用性に依存する単一のプライマリ データセンターを持つ顧客向けです。通常、単一の VCF 環境が含まれます。ブロック ワークロードにはASAを使用し、ファイル/統合ワークロードにはAFFを使用できます。

コンテンツ リポジトリは、VCF ドメイン間で VM テンプレートとコンテナ レジストリを共有します。 FlexGroupボリュームでホストされている場合、サブスクリプション データストアでFlexCache機能が利用で

きます。



FlexCacheデータストアでの VM のホスティングはサポートされていません。



HA モードのONTAPツールの単一インスタンスで、VCF フリート内のすべての vCenter を管理できます。参照["ONTAPツールの構成制限"](#)詳細については。ONTAPツールは、VCF SSO および VCF OPS スマート グループ化と統合され、同じ UI で複数の vCenter にアクセスできます。

ONTAPツールを使用した VCF 補足データストア

VM およびデータストアの保護のために、各 vCenter インスタンスにSnapCenterプラグインを展開する必要があります。

ストレージ ポリシー ベースの管理は、vSphere Supervisor とともに使用され、VKS の制御 VM をホストします。タグは VCF Ops で集中管理されます。NetApp Trident CSI は、ネイティブ アレイ機能を使用してアプリケーションのバックアップ保護を行うために VKS と併用されます。vSphere CSI を使用すると、永続ボリュームの詳細が VCF Automation に表示されます。

このブループリントの詳細については、["Broadcom の技術ドキュメントを单一サイトで VCF フリートに集約"](#)。

単一地域に複数の拠点を持つ VCF フリート

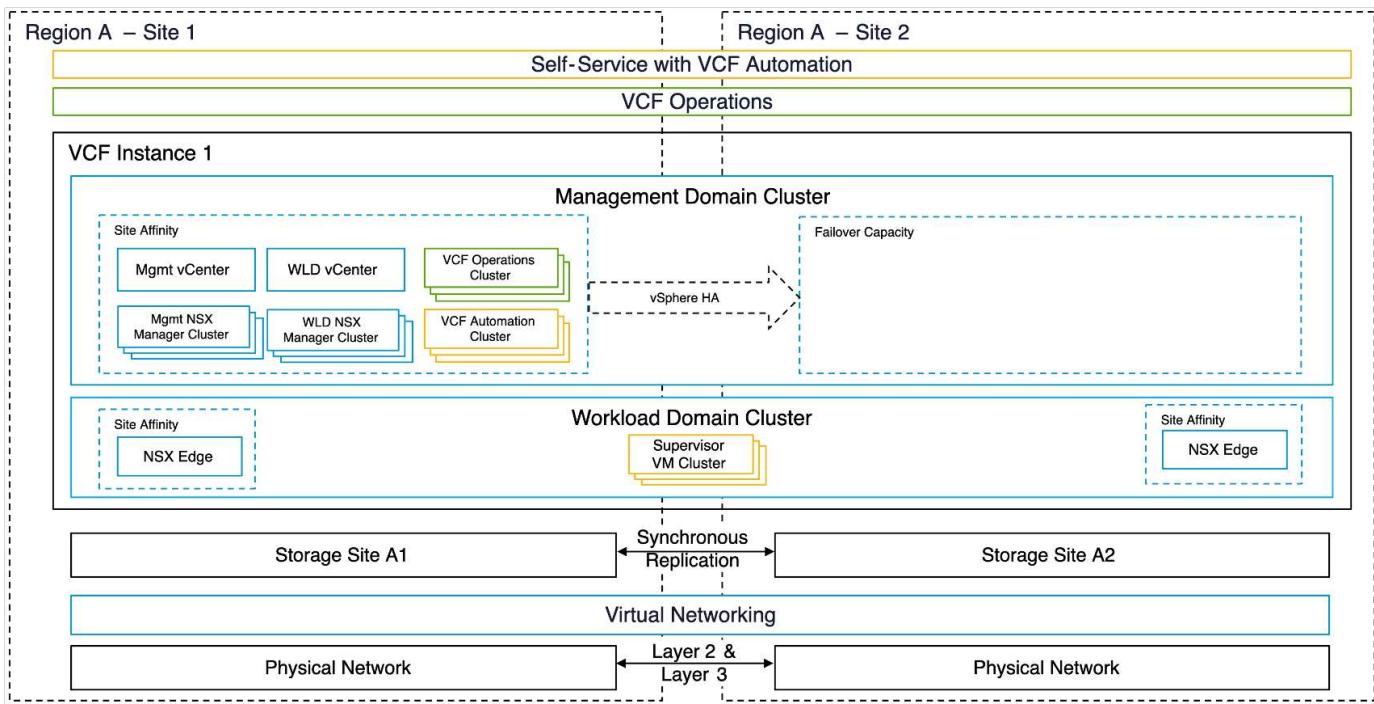
この設計は、ワークロードをさまざまな障害ドメインに分散することで、可用性の高いクラウドのようなサービスを提供する顧客向けです。

VMFS データストアの場合、SnapMirrorアクティブ同期は、vSphere Metro Storage Cluster で使用するためのアクティブ/アクティブストレージ ユニットを提供します。均一アクセス モードでは透過的なストレージフェイルオーバーが提供されますが、非均一アクセス モードでは障害ドメインの障害時に VM の再起動が必要になります。

NFS データストアの場合、vSphere Metro Storage Cluster を備えたONTAP MetroClusterにより高可用性が保証されます。メディエーターはスプリット ブレイン シナリオを回避し、BlueXPでホストできるようになります。

ました。

VM 配置ルールは、管理ドメイン コンポーネントの同じ障害ドメイン内の VM を制御します。



ONTAPツールは、 SnapMirrorアクティブ同期関係を設定するための UI を提供します。両方の障害ドメインのストレージシステムは、 ONTAPツールおよびSnapCenter Plug-in for VMware vSphereに登録する必要があります。

SnapMirrorおよびSnapMirror to Cloud 経由でBlueXP Backup and Recovery for VMs を使用して、3-2-1 バックアップ ポリシーを実装できます。3つの場所のいずれからでも復元を実行できます。

Trident Protect またはBlueXP Backup and Recovery for Kubernetes は、VKS クラスター アプリケーションを保護します。

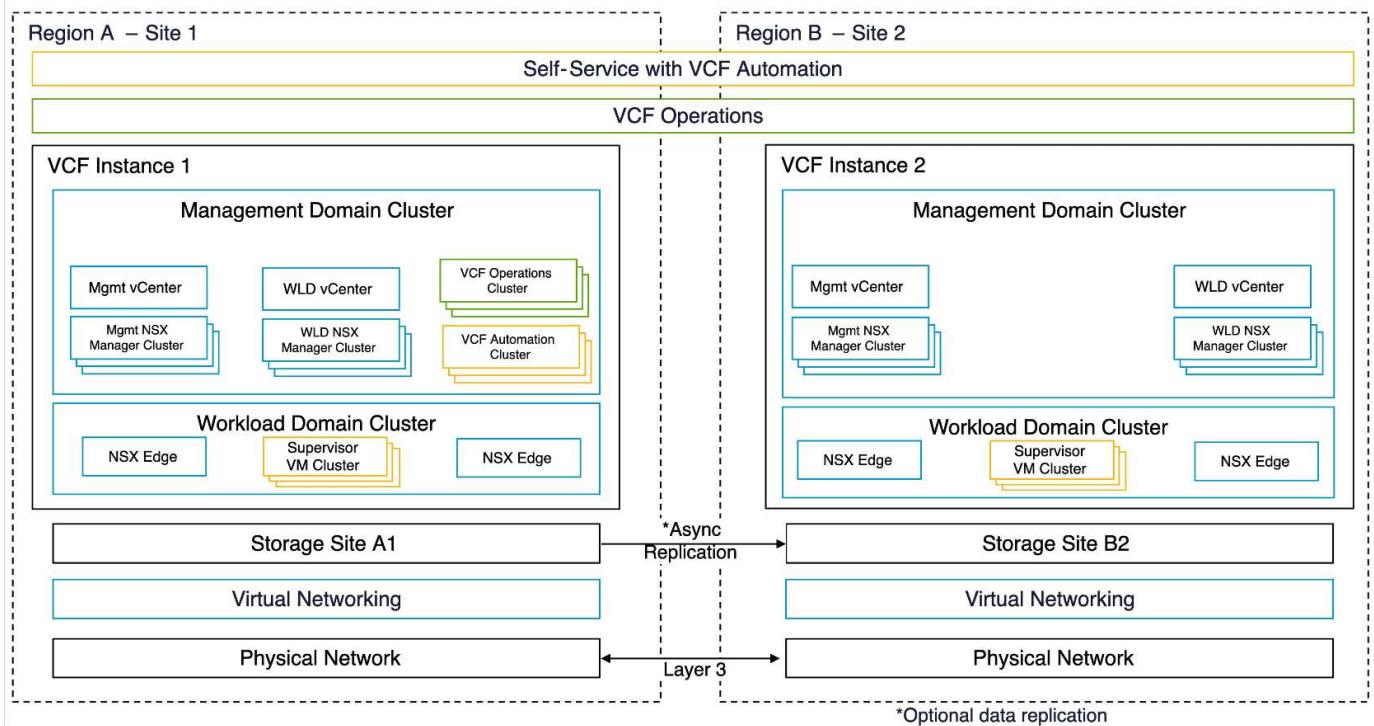
詳細については、"单一地域内の複数のサイトを持つ VCF フリートに関する Broadcom の技術ドキュメント"。

複数の地域にまたがる複数の拠点を持つ VCF フリート

この設計は、世界中に広がる顧客を対象としており、近接したサービスと災害復旧ソリューションを提供します。

VMware Live Site Recovery またはBlueXP Disaster Recovery as a Service を使用して、VM の災害復旧を管理できます。ONTAPツールは、ONTAPでストレージ操作を調整するための SRA(ストレージ レプリケーション アダプタ)を提供します。

製品ファミリー	SnapMirrorアクティブ同期	MetroCluster
ASA AシリーズおよびCシリーズ	はい	はい
AFF AシリーズおよびCシリーズ	はい	はい
FAS	いいえ	はい



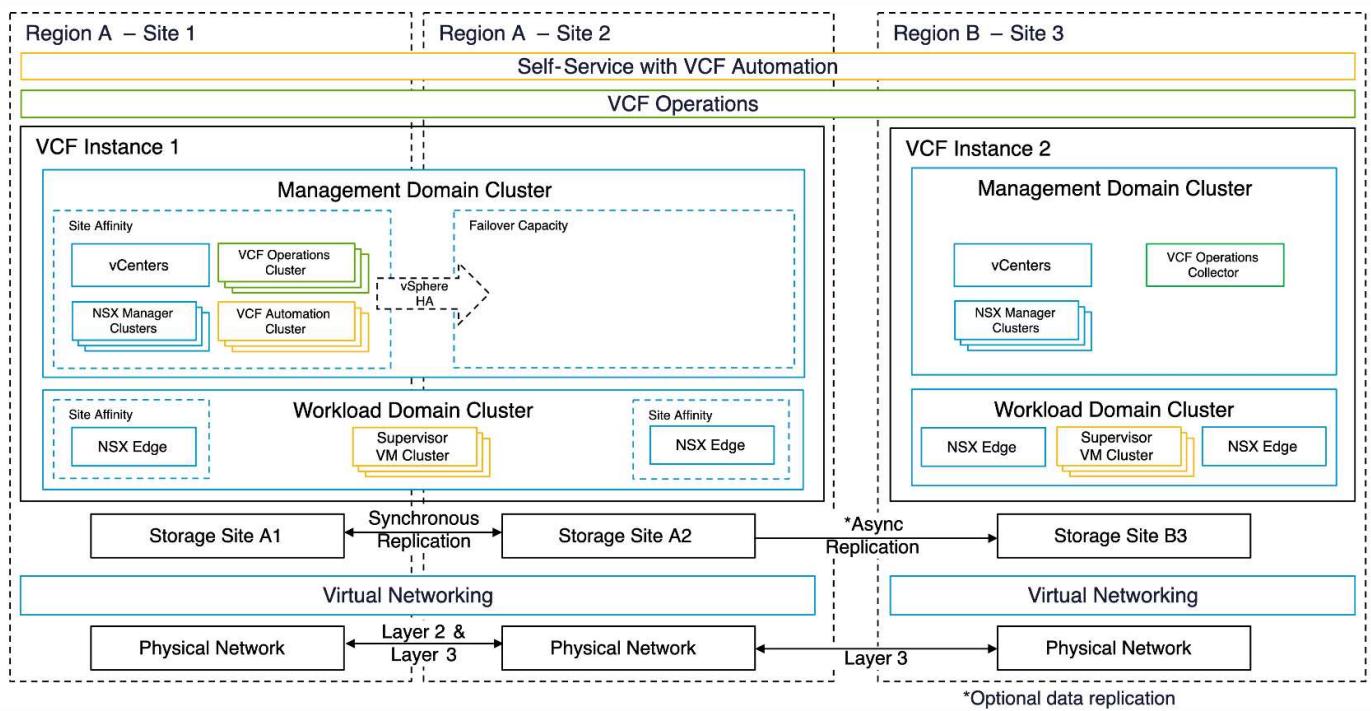
ONTAPツールは、データストアのレプリケーション設定用のUIを提供します。BlueXPは、ストレージアレイ間のレプリケーションにも使用できます。SnapCenter Plug-in for VMware vSphereは、スナップショットに既存のSnapMirror関係を利用します。

詳細については、["複数の地域にまたがる複数の拠点を持つVCFフリートに関するBroadcomの技術ドキュメント"](#)。

単一地域と追加地域に複数のサイトを持つVCFフリート

この設計は、VMとVKSアプリケーションの可用性と災害復旧の両方に対応します。

ASA、AFF、およびFASはこの設計オプションをサポートしています。



レプリケーション関係を設定するには、ONTAPツールまたはBlueXPを使用できます。

詳細については、"单一地域および追加地域に複数のサイトを持つ VCF フリートに関する Broadcom の技術ドキュメント"。

VMware Cloud Foundation とONTAPを使用してプライベートクラウド環境をセットアップする

ONTAPを使用して VMware Cloud Foundation 9 環境を展開、統合、またはアップグレードします。新しい VCF 9.0 環境をセットアップし、既存の vCenter インスタンスとONTAPデータストアを統合し、以前の VCF 展開をアップグレードする方法を学習します。

新しいVCF 9インスタンスをデプロイする

このワークフローを使用して、クリーンな VMware Cloud Foundation (VCF) 9.0 環境をデプロイします。展開後は、ワークロードを移行したり、アプリケーションのプロビジョニングを開始したり、インフラストラクチャ サービスを提供したりできます。

大まかな手順については、"ビルドジャーニー – 新しい VMware Cloud Foundation デプロイメントのインストール"。

手順

1. フォロー "Broadcom VCF 9 の導入手順"。
2. 展開準備手順で、プリンシパルストレージ オプションのタスクを完了します。

FC 上の VMFS

- すべての ESXi ホストの WWPN を収集します。走れる `esxcli storage san fc list` ESXi ホスト クライアントを使用するか、PowerCLI を使用します。
- ゾーニングを構成します。見る "[ONTAPシステムに推奨されるFCゾーニング構成](#)"。



物理アダプタの WWPN ではなく、SVM 論理インターフェイス (LIF) の WWPN を使用します。

- System Manager、ONTAP CLI、または API を使用して、LUN を作成し、WWPN によってホストにマップします。
- ESXi 上のストレージ アダプタを再スキャンし、VMFS データストアを作成します。

NFSv3

- 1台の ESXi ホストに VMkernel インターフェイスを作成します。
- 確実に "[SVMでNFSが有効になっています](#)" そして "[NFS経由のvStorageが有効になっています](#)"。
- ボリュームを作成し、ESXi ホストを許可するポリシーを使用してエクスポートします。
- 必要に応じて権限を調整します。
- ONTAP NFS VAAI VIB をデプロイし、vLCM イメージに含めます。例えば： esxcli software vib install -d /NetAppNasPlugin2.0.1.zip。 (NetAppサポートサイトから ZIP をダウンロードしてください。)
- VMkernel インターフェイスを作成したホストに NFS ボリュームをマウントします。例えば： esxcli storage nfs add -c 4 -H 192.168.122.210 -s /use1_m01_nfs01 -v use1-m01-c101-nfs01。



その `nConnect` セッション数はホストごとです。必要に応じて、展開後に他のホストを更新します。

- *VCF フリーの展開*フェーズの*展開の概要を確認し、次の手順を確認する*の最後に、次の操作を完了します。
 - ONTAP Toolsの導入
 - ["ONTAPツール10.xをダウンロード"](#) NetAppサポートサイトから。
 - ONTAPツール マネージャー、ノード、および内部通信に使用される仮想 IP の DNS レコードを作成します。
 - OVA を管理 vCenter Server にデプロイします。
 - ["管理ドメインvCenterを登録する"](#) ONTAPツール マネージャーを使用します。
 - ["ストレージバックエンドを追加する"](#) vSphere Client UI を使用します。
 - ["補足データストアを作成する"](#) (コンテンツ レジストリ用に 1 つ含めます)。
 - HA 展開を計画している場合は、コンテンツ レジストリを作成します。
 - ["HAを有効にする"](#) ONTAPツール マネージャーで。

- b. SnapCenter プラグインの導入
 - "SnapCenter Plug-in for VMware vSphere の導入"。
 - "ストレージバックエンドを追加する"。
 - "バックアップポリシーの作成"。
 - "リソース グループの作成"。
 - c. BlueXP コネクタをデプロイする
 - "コネクタなしで何ができるか確認する"。
 - "コネクタをデプロイする"。
 - d. バックアップとリカバリにはBlueXPを使用する
 - "VM ワークロードを保護する"。
 - "VKS ワークロードを保護する"。
2. VCF インスタンスに vCenter をワークロード ドメインとしてインポートした後、次の手順を実行します。
- a. ONTAPツールを登録する
 - "ワークロードドメインvCenterを登録する"ONTAPツール マネージャーを使用します。
 - "ストレージバックエンドを追加する"vSphere Client UI を使用します。
 - "補足データストアを作成する"。
 - b. SnapCenter Plug-in for VMware vSphere の導入
 - "SnapCenter Plug-in for VMware vSphere の導入"。
 - "ストレージバックエンドを追加する"。
 - "バックアップポリシーの作成"。
 - "リソース グループの作成"。
 - c. バックアップとリカバリにはBlueXPを使用する
 - "VM ワークロードを保護する"。
 - "VKS ワークロードを保護する"。

新しいワークロード ドメインを作成するときはいつでも、これらの手順を再利用できます。

既存のコンポーネントをVCF 9に統合

VCF フリートのいくつかのコンポーネントをすでに所有しており、それを再利用したい場合があります。vCenter インスタンスを再利用する場合、データストアはONTAPツールを使用して頻繁にプロビジョニングされ、VCF の主要ストレージとして機能します。

前提条件

- 既存の vCenter インスタンスが機能していることを確認します。
- ONTAPでプロビジョニングされたデータストアが利用可能であることを確認します。
- アクセスを確保する"Interoperability Matrix"。

手順

1. レビュー "[VCFに収束するためのサポートされているシナリオ](#)"。
2. ONTAPでプロビジョニングされたデータストアを主ストレージとして vCenter インスタンスに統合します。
3. サポートされているバージョンを確認するには、"[Interoperability Matrix](#)"。
4. アップグレード "[ONTAPツール](#)" 必要に応じて。
5. アップグレード "[VMware vSphere 用SnapCenterプラグイン](#)" 必要に応じて。

既存のVCF環境をVCF 9にアップグレードする

標準のアップグレード プロセスを使用して、以前の VCF デプロイメントをバージョン 9.0 にアップグレードします。その結果、管理ドメインとワークロード ドメインがアップグレードされたバージョン 9.0 を実行する VCF 環境が実現します。

前提条件

- 管理ドメインとワークロード ドメインをバックアップします。
- ONTAPツールとSnapCenterプラグインと VCF 9.0 の互換性を確認します。フォロー "[Interoperability Matrix](#)" に "[ONTAPツールのアップグレード](#)" そして "[VMware vSphere 用SnapCenterプラグイン](#)" VCF 9 でサポートされています。

手順

1. VCF 管理ドメインをアップグレードします。見る "[VCF管理ドメインをVCF 9にアップグレード](#)" 手順についてはこちらをご覧ください。
2. 任意の VCF 5.x ワークロード ドメインをアップグレードします。見る "[VCF 5.x ワークロード ドメインを VCF 9 にアップグレードする](#)" 手順についてはこちらをご覧ください。

NetApp SnapMirrorとBlueXP DRaaSによる災害復旧の実装

NetApp SnapMirrorとBlueXP DRaaSを使用したNFSデータストア向けVCF災害復旧ソリューション

運用サイトから災害復旧 (DR) サイトへのブロックレベルのレプリケーションは、サイトの停止やランサムウェア攻撃などのデータ破損イベントからワークロードを保護するための、回復力がありコスト効率に優れた戦略を提供します。 NetApp SnapMirrorレプリケーションにより、オンプレミスのONTAPシステムで実行されている VMware VCF 9 ワークロード ドメイン (NFS または VMFS データストアを使用) を、VMware も導入されている指定されたリカバリ データセンターにあるセカンダリONTAPシステムにレプリケートできるようになります。

このセクションでは、オンプレミスの VMware 仮想マシンの DR を確立するためのBlueXP Disaster Recovery as a Service (DRaaS) の構成について説明します。

セットアップには以下が含まれます:

- BlueXPアカウントを作成し、BlueXPコネクタを展開します。
- ONTAPアレイをBlueXPキャンバスに追加して、VMware vCenter とONTAPストレージ間の通信を容易にします。

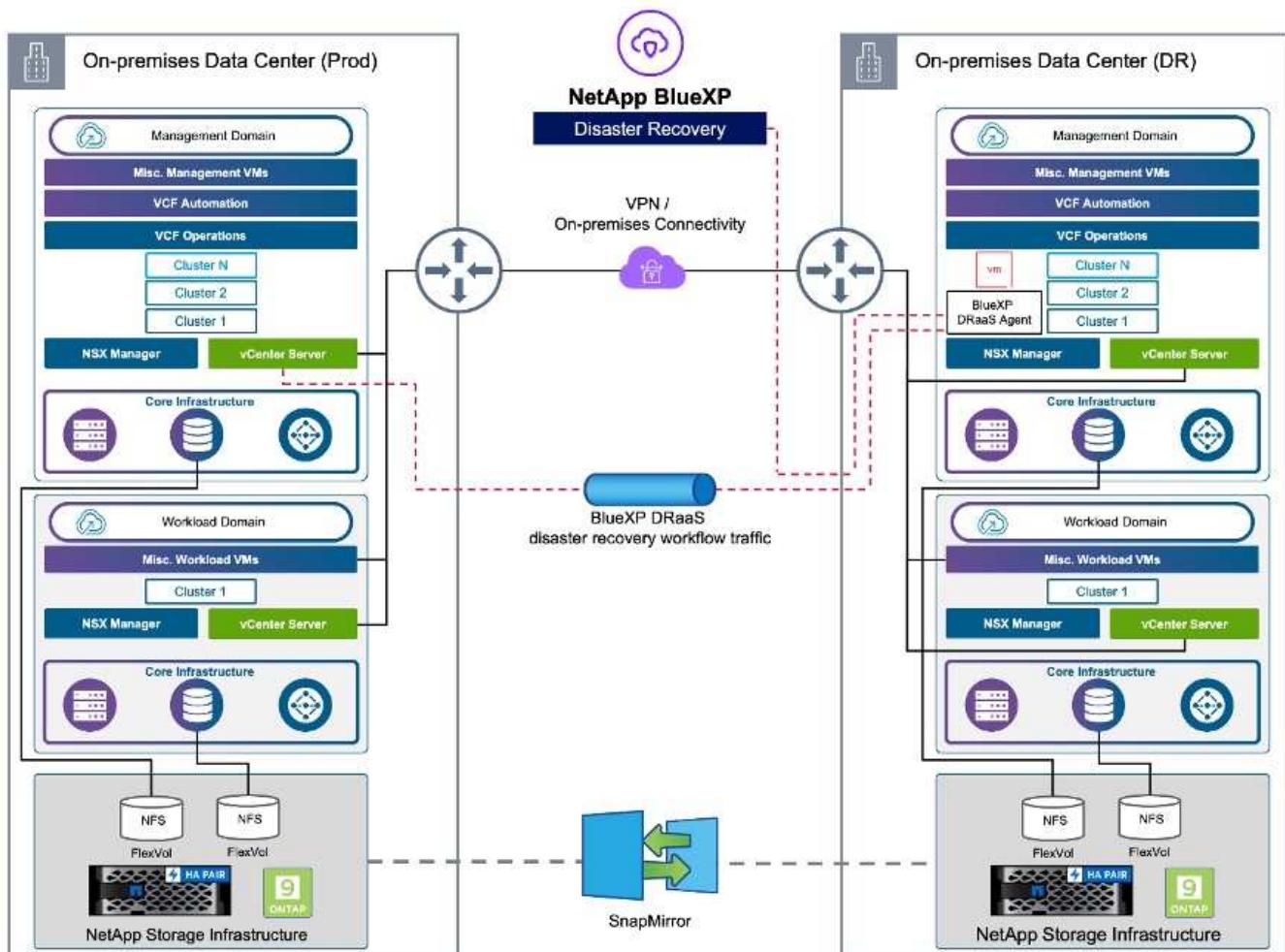
- ・ SnapMirrorを使用してサイト間のレプリケーションを構成します。
- ・ フェイルオーバーの準備を検証するためのリカバリ プランを設定およびテストします。

NetApp BlueXPコンソールに統合されたBlueXP disaster recoveryサービスにより、組織はオンプレミスのVMware vCenter およびONTAPストレージシステムをシームレスに検出できるようになります。検出されると、管理者はリソース グループを定義し、災害復旧計画を作成し、適切なリソースに関連付け、フェイルオーバーおよびフェールバック操作を開始またはテストできます。NetApp SnapMirror は、効率的なブロックレベルのレプリケーションを提供し、増分更新を通じて DR サイトが実稼働環境と同期された状態を維持できるようにします。これにより、最短 5 分でリカバリポイント目標 (RPO) を実現できます。

BlueXP DRaaS は、中断のない災害復旧テストもサポートします。ONTAP のFlexCloneテクノロジーを活用して、実稼働ワークロードに影響を与えることなく、最新の複製されたスナップショットから NFS データストアのスペース効率の高い一時コピーを作成します。テスト後、環境は簡単に解体でき、複製されたデータの整合性が維持されます。

実際のフェイルオーバーが発生した場合、BlueXP はリカバリ プロセスを調整し、ユーザーの介入を最小限に抑えて、指定された DR サイトで保護された仮想マシンを自動的に起動します。プライマリ サイトが復元されると、サービスはSnapMirror関係を元に戻し、すべての変更を元のサイトに複製して、スムーズで制御されたフェイルバックを可能にします。

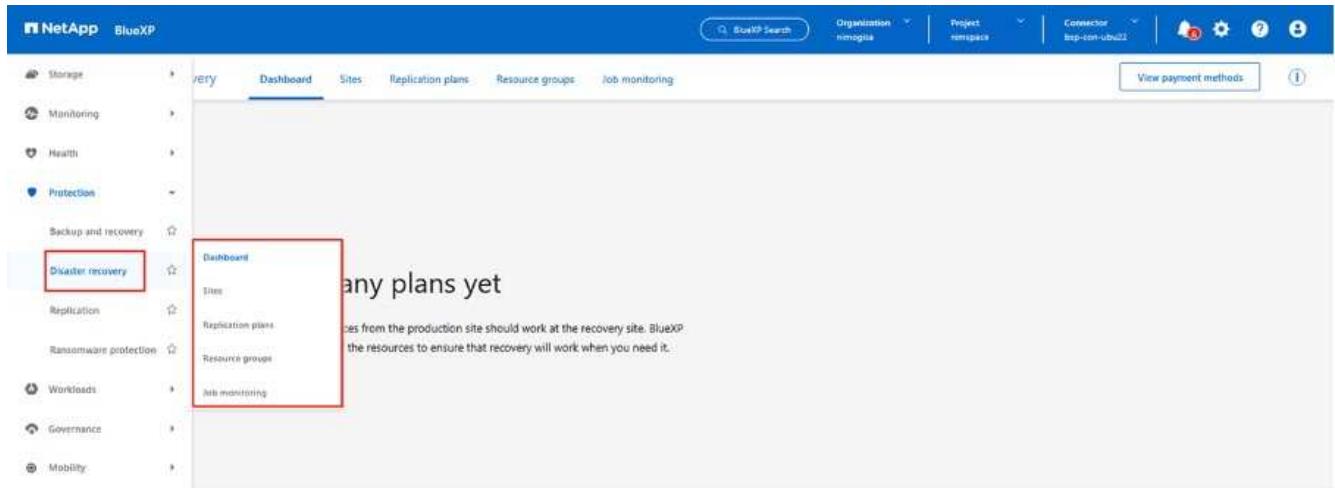
これらすべての機能は、従来の災害復旧ソリューションに比べて大幅に低いコストで提供されます。



開始

BlueXP disaster recoveryを開始するには、 BlueXPコンソールを使用してサービスにアクセスします。

1. BlueXPにログインします。
2. BlueXP の左側のナビゲーションから、[保護] > [災害復旧] を選択します。
3. BlueXP disaster recoveryダッシュボードが表示されます。



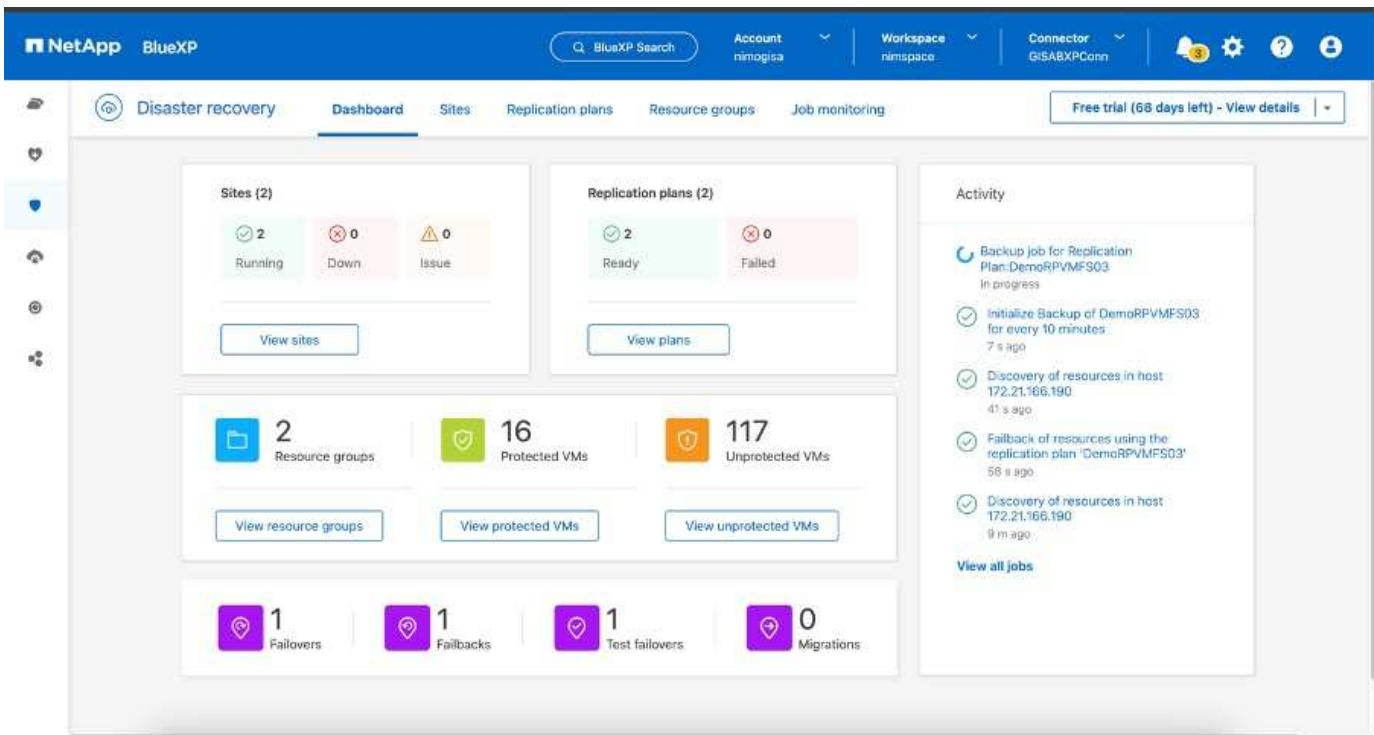
災害復旧計画を構成する前に、次の点を確認してください。"前提条件"満たされている:

- BlueXPコネクタはNetApp BlueXPに設定されます。
- BlueXPコネクタインスタンスは、ソースおよび宛先のワークロード ドメインの vCenter およびストレージ システムに接続できます。
- ストレージ NFS または VMFS データストアを提供するNetApp Data ONTAPクラスター。
- VMware 用の NFS または VMFS データストアをホストするオンプレミスのNetAppストレージ システムがBlueXPに追加されます。
- DNS 名を使用する場合は、DNS 解決を実施する必要があります。それ以外の場合は、vCenter の IP アドレスを使用します。
- SnapMirrorレプリケーションは、指定された NFS または VMFS ベースのデータストア ボリュームに対して構成されます。
- 環境にサポートされているバージョンの vCenter Server および ESXi サーバーがインストールされていることを確認します。

ソースサイトと宛先サイト間の接続が確立されたら、構成手順に進みます。これには数回のクリックと約 3 ~ 5 分かかります。

注: NetApp、BlueXPコネクタがネットワークを介してソース リソースおよび宛先リソースと通信できるように、宛先サイトまたは 3 番目のサイトにBlueXPコネクタを展開することを推奨しています。

このデモでは、ワークロード ドメインはONTAP NFS ストレージで構成されています。 VMFS ベースのデータストアの場合、ワークロードに関する手順は同じままです。



BlueXP disaster recovery構成

災害復旧の準備の最初のステップは、ソース vCenter とストレージ リソースを検出し、BlueXP disaster recoveryに追加することです。

BlueXPコンソールを開き、左側のナビゲーションから [保護] > [災害復旧] を選択します。[vCenter サーバーの検出]を選択するか、トップメニューを使用して、[サイト] > [追加] > [vCenter の追加]を選択します。

次のプラットフォームを追加します。

- ・ソースワークLOADドメインvCenter
- ・宛先ワークLOAD ドメイン vCenter。

vCenter が追加されると、自動検出がトリガーされます。

ソースサイトアレイと宛先サイトアレイ間のストレージレプリケーションの構成

SnapMirror は、NetApp環境でのデータ複製を提供します。NetApp Snapshot® テクノロジーに基づいて構築されたSnapMirrorレプリケーションは、前回の更新以降に変更または追加されたブロックのみを複製するため、非常に効率的です。SnapMirror は、NetApp OnCommand® System Manager またはONTAP CLI を使用して簡単に設定できます。BlueXP DRaaS は、クラスターと SVM ピアリングが事前に構成されている場合、SnapMirror関係も作成します。

プライマリストレージが完全に失われていない場合、SnapMirror はプライマリ サイトと DR サイトを再同期する効率的な手段を提供します。SnapMirror は2つのサイトを再同期し、SnapMirror関係を単純に反転するだけで、変更されたデータまたは新しいデータのみを DR サイトからプライマリ サイトに転送できます。つまり、BlueXP DRaaS のレプリケーション プランは、フェイルオーバー後にボリューム全体を再コピーすることなく、どちらの方向にも再同期できます。関係が逆方向に再同期される場合、スナップショット コピーの最後の正常な同期以降に書き込まれた新しいデータのみが宛先に送り返されます。



CLI または System Manager を介してボリュームにSnapMirror関係がすでに構成されている場合、BlueXP DRaaS はその関係を取得し、残りのワークフロー操作を続行します。

VMware Disaster Recoveryの設定方法

SnapMirrorレプリケーションを作成するプロセスは、どのアプリケーションでも同じです。このプロセスは手動でも自動でも実行できます。最も簡単な方法は、BlueXP DRaaS を活用することです。これは、次の 2つの条件が満たされている場合と同じことを自動化します。

- ・ソース クラスターと宛先クラスターにはピア関係があります。
- ・ソース SVM と宛先 SVM にはピア関係があります。

The screenshot shows the 'Add replication plan' wizard in the BlueXP interface. The 'Target datastore' section is highlighted with a red box. It contains the following configuration:

Working environment	SVM	Destination volume name
NTAP-328-N2	SVM_DR_Dstn	DRaaS_srcB_dest

Other visible fields include:

- Source datastore: DRaaS_srcB (OR_Src_NewDRaaS_srcB)
- Retention count for all datastores: 30
- Start taking backups and running retention from: 2025-08-14, 12:00 AM
- Take backups and run retention once every: 03 hours
- Preferred NFS LIF: Select preferred NFS LIF
- Export policy: Select export policy

BlueXP には、環境内のソースONTAPシステムを宛先にドラッグ アンド ドロップするだけで、残りのプロセスをガイドするウィザードを起動してSnapMirrorレプリケーションを構成する代替オプションも用意されています。

BlueXP disaster recoveryは何を実現できるのでしょうか？

ソース サイトと宛先サイトが追加されると、BlueXP disaster recoveryは自動的に詳細な検出を実行し、VM と関連メタデータを表示します。BlueXP disaster recoveryでは、VM で使用されるネットワークとポート グループも自動的に検出し、それらを入力します。

The screenshot shows the 'Sites' tab in the NetApp BlueXP interface. There are two entries: 'vcf9d' and 'vcf9e'. Each entry has a summary card with the following details:

- vcf9d:**
 - vCenter: vcf9d-vc01.siengmt.com
 - Status: Healthy
 - VMs: 8
 - Datastores: 3
 - Resource groups: 0
 - Connector: bxp-con-ubuntu22
- vcf9e:**
 - vCenter: vcf9e-vc01.siengmt.com
 - Status: Healthy
 - VMs: 5
 - Datastores: 2
 - Resource groups: 0
 - Connector: bxp-con-ubuntu22

サイトを追加したら、ドロップダウンからソースと宛先の vCenter プラットフォームを選択してレプリケーション プランを構成し、プランに含めるリソース グループ、アプリケーションの復元方法と電源オン方法のグループ化、およびクラスタとネットワークのマッピングを選択します。リカバリ プランを定義するには、[レプリケーション プラン] タブに移動し、[プランの追加] をクリックします。

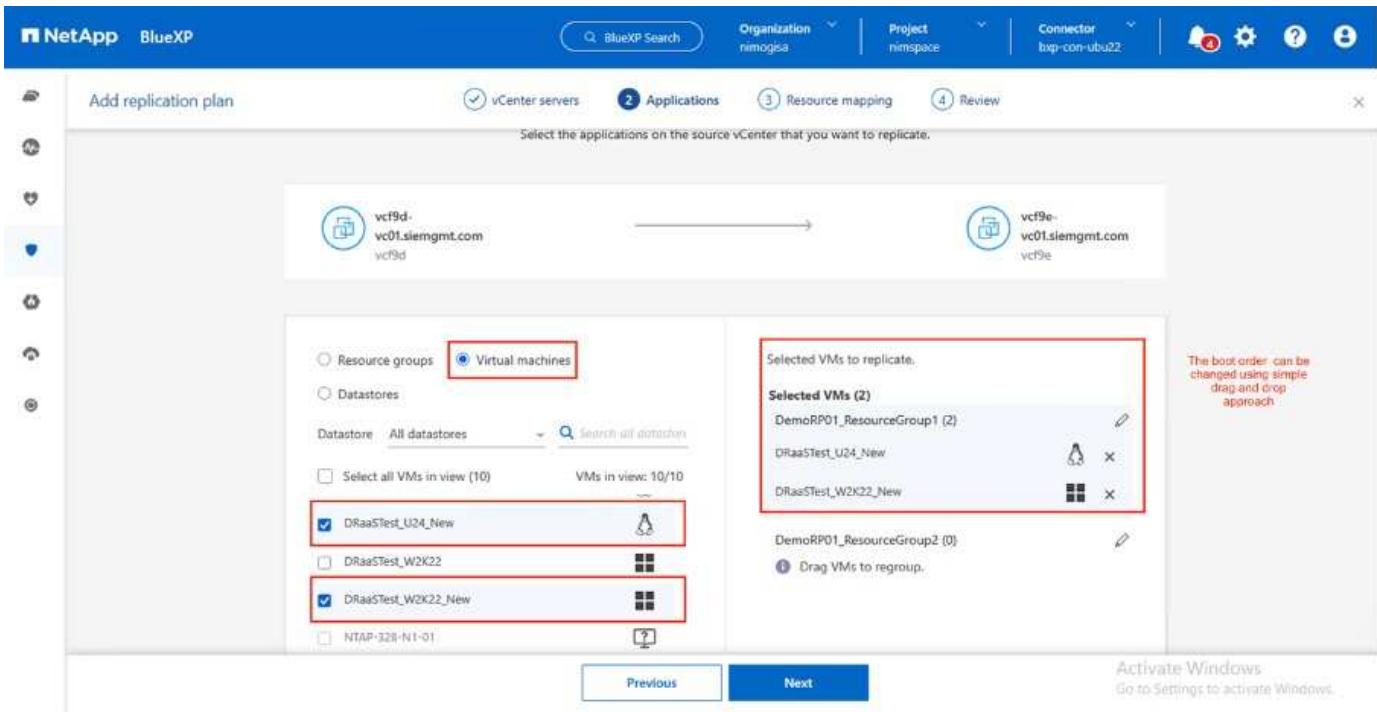
このステップでは、VM をリソース グループにグループ化できます。BlueXP disaster recovery リソース グループを使用すると、依存する VM のセットを、復旧時に実行できるブート順序とブート遅延を含む論理グループにグループ化できます。リソース グループは、リソース グループ タブを使用して作成することもできます。

まず、ソース vCenter を選択し、次に宛先 vCenter を選択します。

The screenshot shows the 'Add replication plan' wizard at step 1: vCenter servers. The interface includes the following elements:

- Replication plan name:** DemoRP01 (highlighted with a red box)
- Select a source vCenter where your data exists, to replicate to the selected target vCenter.**
- Source vCenter:** vcf9d-vc01.siengmt.com
- Target vCenter:** vcf9e-vc01.siengmt.com
- Buttons:** Cancel, Next
- Activation Message:** Activate Windows
Go to Settings to activate Windows.

次のステップは、既存のリソース グループを選択することです。リソース グループが作成されていない場合、ウィザードは、回復目標に基づいて必要な仮想マシンをグループ化します（基本的には機能リソース グループを作成します）。これは、アプリケーション仮想マシンを復元する操作シーケンスを定義するのにも役立ちます。



i リソース グループでは、ドラッグ アンド ドロップ機能を使用してブート順序を設定できます。これを使用すると、リカバリプロセス中に VM の電源がオンになる順序を簡単に変更できます。

レプリケーション プランを使用してリソース グループを作成したら、次の手順では、災害発生時に仮想マシンとアプリケーションを回復するためのブループリントまたはマッピングを選択します。このステップでは、ソース環境のリソースを宛先にどのようにマップするかを指定します。これには、コンピューティング リソース、仮想ネットワーク、IP カスタマイズ、事前スクリプトと事後スクリプト、ブート遅延、アプリケーションの一貫性などが含まれます。詳細については、["レプリケーション プランを作成する"](#)。前提条件で述べたように、SnapMirror レプリケーションは事前に構成することも、レプリケーション プランの作成時に指定された RPO と保持数を使用して DRaaS で構成することもできます。

注: デフォルトでは、テスト操作とフェイルオーバー操作の両方に同じマッピング パラメータが使用されます。テスト環境に異なるマッピングを設定するには、「フェイルオーバーとテスト マッピングに同じマッピングを使用する」チェックボックスをオフにした後、テスト マッピング オプションを選択します。リソース マッピングが完了したら、[次へ] をクリックします。

The screenshot shows the 'Resource mapping' step of the 'Add replication plan' wizard. It displays two vCenter servers: 'vcf9d-vc01.siengmt.com' (source) and 'vcf9e-vc01.siengmt.com' (target). Under 'Compute resources', 'Virtual networks', and 'Virtual machines', there are tabs for 'Failover mappings' and 'Test mappings'. Each tab has a checkbox labeled 'Mapped'. A red box highlights the 'Failover mappings' section for all three resource types. At the bottom, there are 'Previous' and 'Next' buttons.

完了したら、作成されたマッピングを確認し、「プランの追加」をクリックします。

The screenshot shows the 'Review' step of the 'Add replication plan' wizard. It displays the 'Plan details' and 'Failover mapping' tabs. Under 'Failover mapping', it shows the mapping between Source and Target for Datastores, Compute resource, and Virtual networks. A red box highlights the 'Failover mapping' tab. At the bottom, there are 'Previous' and 'Add plan' buttons.



異なるボリュームおよび SVM からの VM をレプリケーション プランに含めることができます。VM の配置 (同じボリューム上、同じ SVM 内の別のボリューム上、異なる SVM 上の別のボリューム上など) に応じて、BlueXP disaster recoveryでは整合性グループ スナップショットが作成されます。

The screenshot shows the NetApp BlueXP interface under the 'Disaster recovery' tab. A single replication plan, 'DemoRP01', is listed in the 'Replication plans' section. The plan is marked as 'Healthy' and 'Ready'. It is associated with a 'Protected site' (vcf9d) and a 'Resource group' (DemoRP01_ResourceGroup1). The 'Failover site' is also listed as vcf9e. The entire row for 'DemoRP01' is highlighted with a red border.

計画が作成されるとすぐに、一連の検証がトリガーされ、選択に応じてSnapMirrorレプリケーションとスケジュールが構成されます。

The screenshot shows the 'Job monitoring' section of the NetApp BlueXP interface. It displays a list of job activities for the 'DemoRP01' replication plan. The activities include creating the resource group, establishing a SnapMirror schedule, defining a policy for Volume ID 3ef8c1ae-791b-11f0-8f66-00a0b99a2c51, setting retention rules, and creating relationships between source and destination volumes. Most of these jobs are marked as 'Completed'. One job, 'Creating SnapMirror relationship for : DR_Src_NewDRaaS_SrcB->DR_Dstn_NewDRaaS_SrcB_dest', is shown as 'In Progress'. A tooltip for this job indicates it is 'Activating Windows'.

BlueXP DRaaS は次のワークフローで構成されています。

- ・ テストフェイルオーバー（定期的な自動シミュレーションを含む）
- ・ クリーンアップフェイルオーバーテスト
- ・ フェイルオーバー:
 - 計画的な移行（1回限りのフェイルオーバーのユースケースの拡張）
 - ディザスター・リカバリ
- ・ フェイルバック

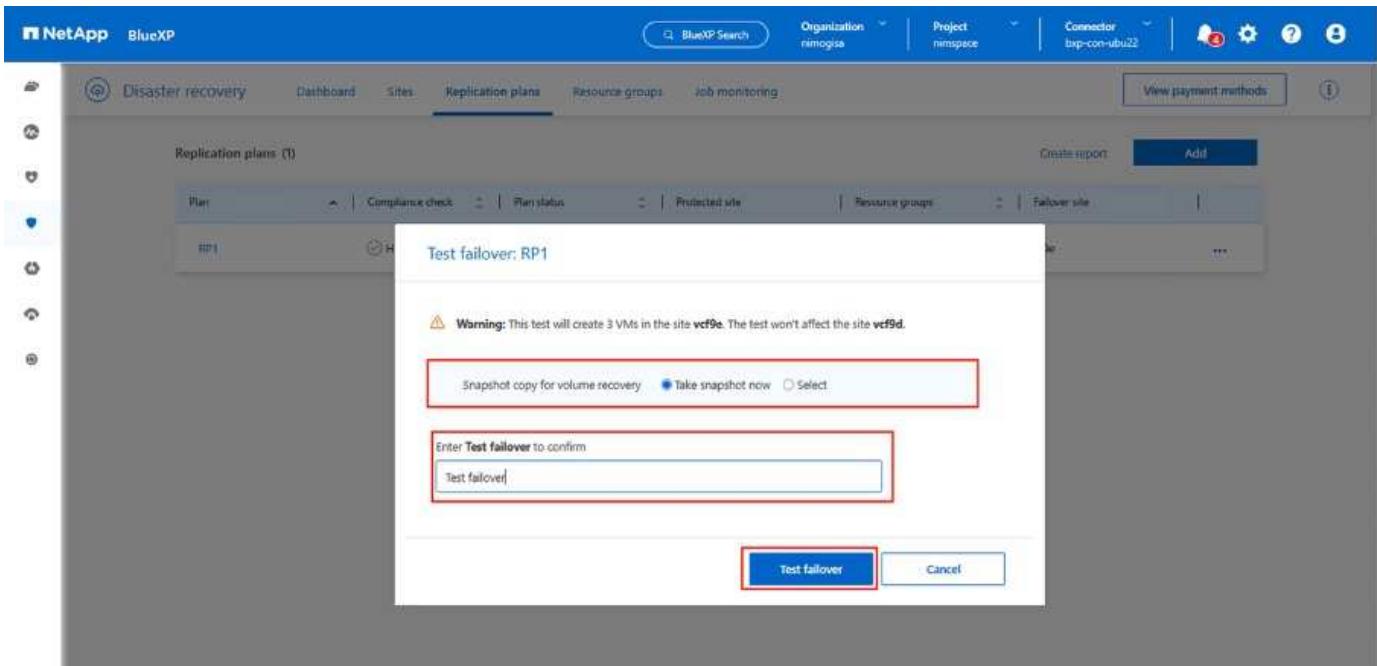
The screenshot shows the NetApp BlueXP web interface. In the top navigation bar, the 'Replication plans' tab is selected. Below it, a table lists a single replication plan: 'DemoRP01' with status 'Ready'. To the right of the table is a context menu with several options: 'View plan details', 'Run compliance check', 'Refresh resources', 'Protect resources', 'Test failover' (which is highlighted with a red box), 'Clean up failover test', 'Fail over', 'Fail back', 'Migrate', 'Edit schedules', 'Take snapshot now', and 'Disable'.

テストフェイルオーバー

BlueXP DRaaS のテスト フェイルオーバーは、VMware 管理者が実稼働環境を中断することなくリカバリ プランを完全に検証できるようにする運用手順です。

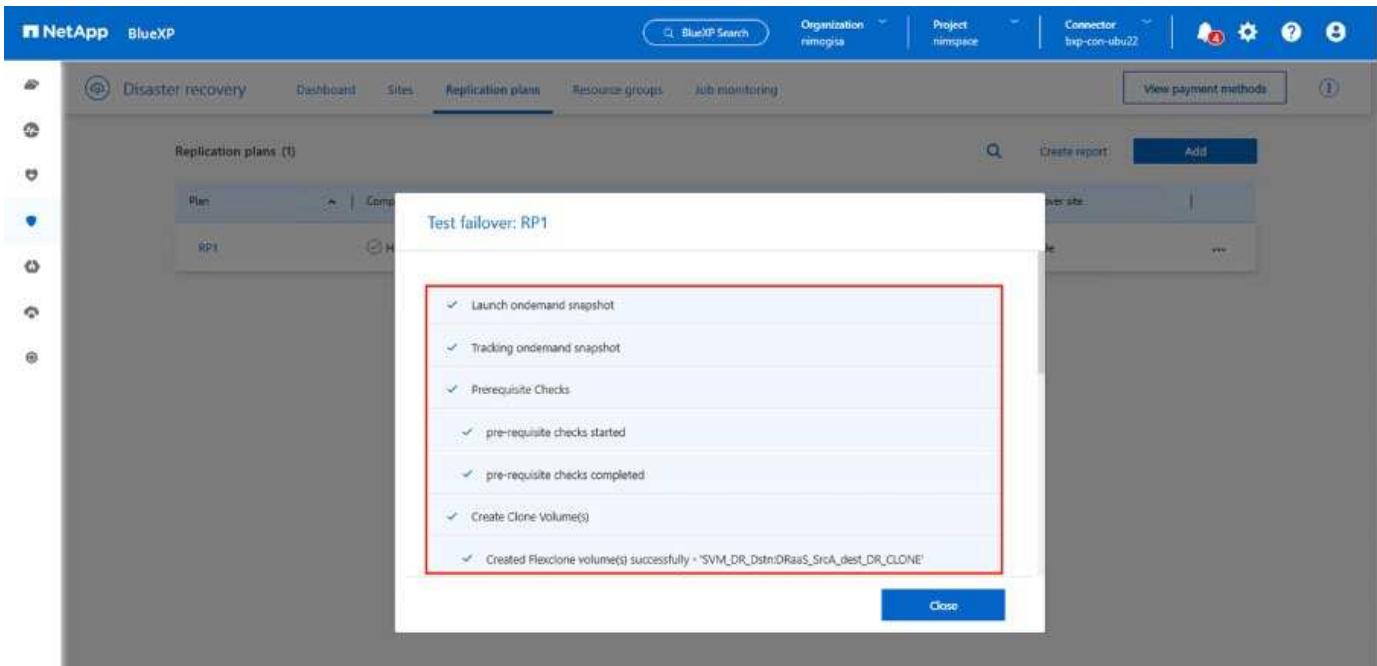
This screenshot is identical to the one above, showing the 'Replication plans' page with a single plan named 'RPT1'. The context menu is open over this plan, and the 'Test failover' option is highlighted with a red box.

BlueXP DRaaS には、テスト フェイルオーバー操作のオプション機能としてスナップショットを選択する機能が組み込まれています。この機能により、VMware 管理者は、環境で最近行われた変更が宛先サイトに複製され、テスト中に存在していることを確認できます。このような変更には、VM ゲスト オペレーティング システムへのパッチが含まれます。



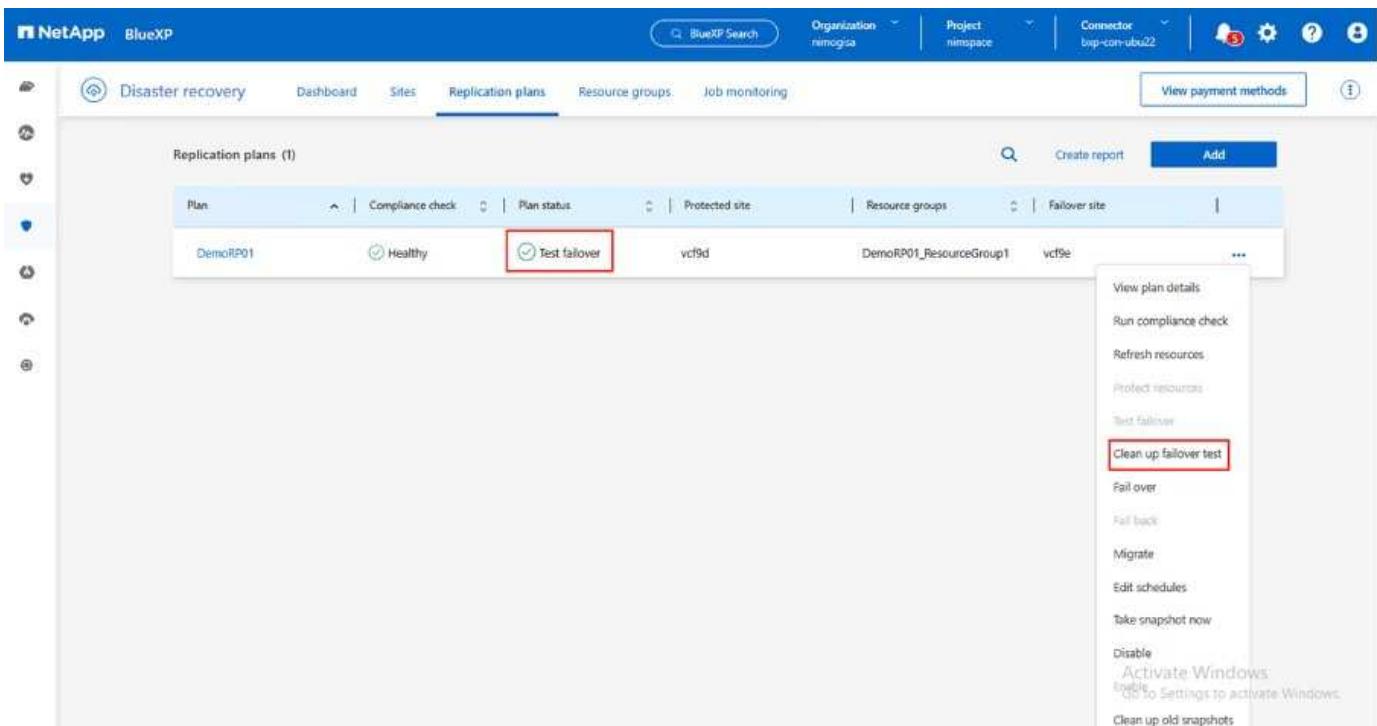
VMware 管理者がテスト フェイルオーバー操作を実行すると、BlueXP DRaaS は次のタスクを自動化します。

- SnapMirror関係をトリガーして、本番サイトで行われた最近の変更を宛先サイトのストレージに反映します。
- DR ストレージ アレイ上のFlexVolボリュームのNetApp FlexCloneボリュームを作成します。
- FlexCloneボリューム内のデータストアを DR サイトの ESXi ホストに接続します。
- マッピング中に指定されたテスト ネットワークに VM ネットワーク アダプターを接続します。
- DR サイトのネットワークの定義に従って、VM ゲスト オペレーティング システムのネットワーク設定を再構成します。
- レプリケーション プランに保存されているカスタム コマンドを実行します。
- レプリケーション プランで定義された順序で VM の電源をオンにします。



クリーンアップフェイルオーバーテスト操作

クリーンアップフェイルオーバーテスト操作は、レプリケーションプランテストが完了し、VMware管理者がクリーンアッププロンプトに応答した後に実行されます。

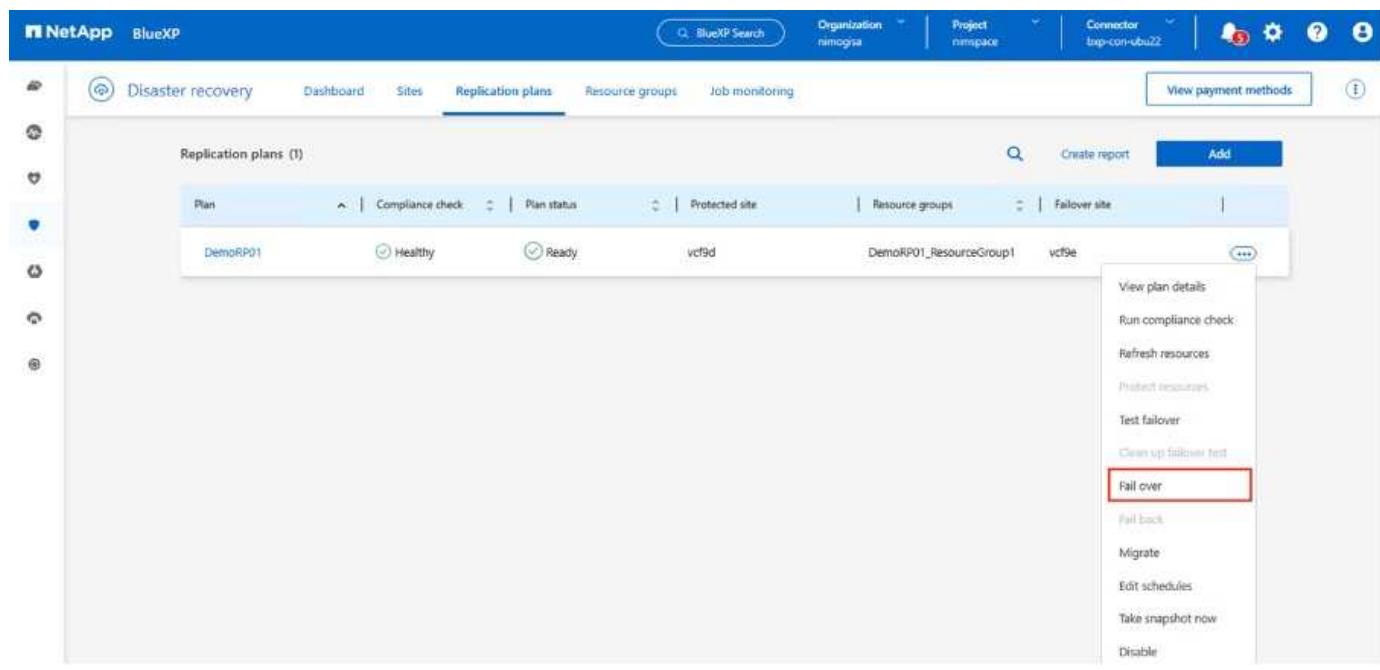


このアクションにより、仮想マシン(VM)とレプリケーションプランのステータスが準備完了状態にリセットされます。VMware管理者がリカバリ操作を実行すると、BlueXP DRaaSは次のプロセスを完了します。

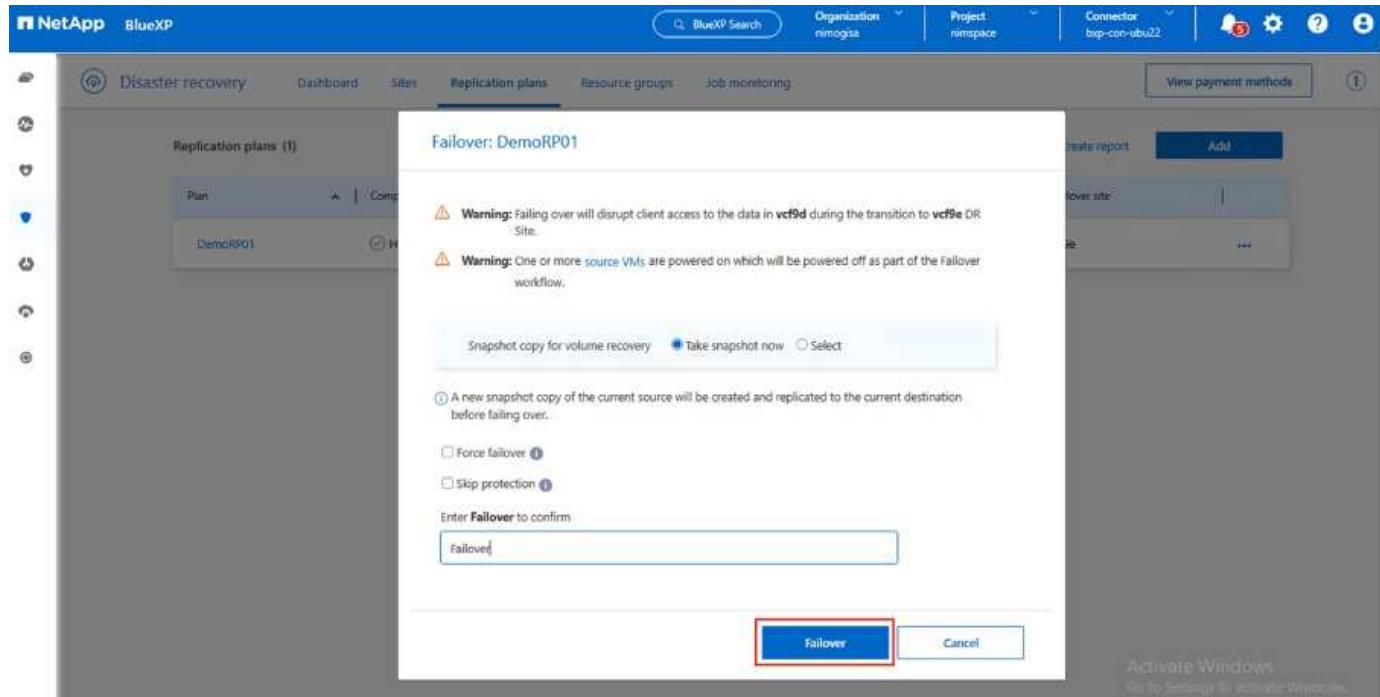
1. テストに使用されたFlexCloneコピー内の回復された各VMの電源をオフにします。
2. テスト中に回復されたVMを表示するために使用されたFlexCloneボリュームを削除します。

計画的な移行とフェイルオーバー

BlueXP DRaaS には、実際のフェイルオーバーを実行するための 2 つの方法(計画された移行とフェイルオーバー)があります。最初の方法である計画移行では、VM のシャットダウンとストレージ レプリケーションの同期をプロセスに組み込んで、VM を回復するか、効率的に移行先サイトに移動させます。計画された移行にはソース サイトへのアクセスが必要です。2 番目の方法であるフェールオーバーは、計画済み/計画外のフェールオーバーであり、完了できた最後のストレージ レプリケーション間隔から宛先サイトで VM が回復されます。ソリューションに設計された RPO に応じて、DR シナリオではある程度のデータ損失が予想されます。



The screenshot shows the BlueXP DRaaS web interface. In the top navigation bar, the 'Disaster recovery' tab is selected. Below it, the 'Replication plans' tab is active, showing a list of replication plans. One plan, 'DemoRP01', is listed with a status of 'Healthy' and 'Ready'. To the right of the plan list, a context menu is open, listing various actions: View plan details, Run compliance check, Refresh resources, Protect resources, Test failover, Clear up failover test, Fail over (this option is highlighted with a red box), Fall back, Migrate, Edit schedules, Take snapshot now, and Disable.

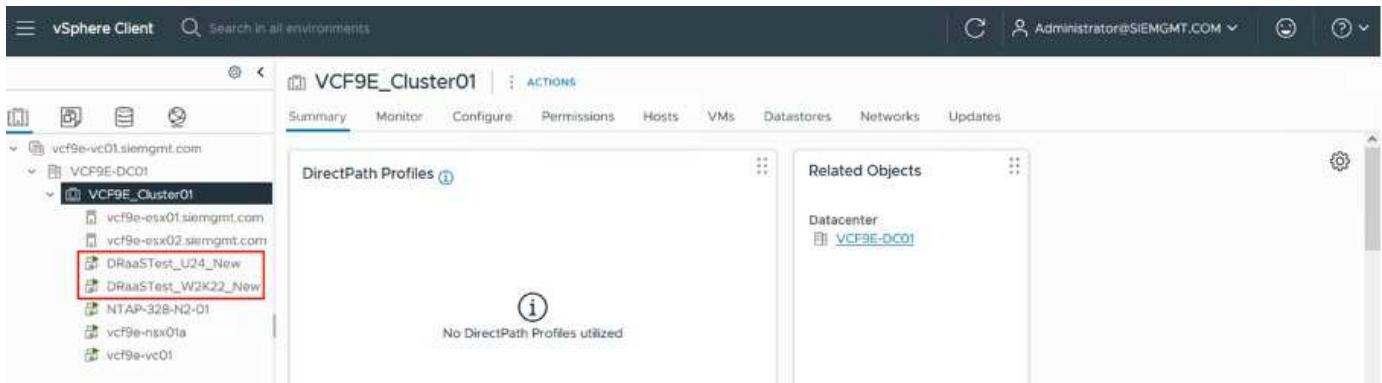


The screenshot shows the 'Failover: DemoRP01' dialog box. It contains two warning messages: 'Warning: Failing over will disrupt client access to the data in vcf9d during the transition to vcf9e DR Site.' and 'Warning: One or more source VMs are powered on which will be powered off as part of the Failover workflow.' Below the warnings, there are options for 'Snapshot copy for volume recovery': 'Take snapshot now' (radio button selected) and 'Select...'. There are also checkboxes for 'Force failover' and 'Skip protection'. At the bottom, there is a text input field labeled 'Enter Failover to confirm' containing the word 'Failover'. Two buttons are at the bottom: 'Failover' (highlighted with a red box) and 'Cancel'.

VMware 管理者がフェイルオーバー操作を実行すると、BlueXP DRaaS は次のタスクを自動化します。

- NetApp SnapMirror関係を解除してフェイルオーバーします。

- 複製されたデータストアを DR サイトの ESXi ホストに接続します。
- VM ネットワーク アダプターを適切な宛先サイト ネットワークに接続します。
- 宛先サイトのネットワークの定義に従って、VM ゲスト オペレーティング システムのネットワーク設定を再構成します。
- レプリケーション プランに保存されているカスタム コマンド (存在する場合) を実行します。
- レプリケーション プランで定義された順序で VM の電源をオンにします。



フェイルバック

フェイルバックは、回復後にソース サイトと宛先サイトの元の構成を復元するオプションの手順です。

The screenshot shows the NetApp BlueXP Disaster recovery interface. The 'Replication plans' tab is selected. A context menu is open over a plan named 'DemoRP01'. The menu options include: View plan details, Run compliance check, Refresh resources, Protect resources, Test failover, Clean up failover test, Fail over, Fail back (which is highlighted with a red box), Migrate, Edit schedules, Take snapshot now, Disable, Activate Windows (with a note to go to Settings to activate Windows), and Clean up old snapshots.

VMware 管理者は、サービスを元のソース サイトに復元する準備ができたら、フェイルバック手順を構成して実行できます。



BlueXP DRaaS は、レプリケーションの方向を反転する前に、すべての変更を元のソース仮想マシンにレプリケート (再同期) します。

このプロセスは、ターゲットへのフェールオーバーが完了した関係から開始され、次の手順が含まれます。

- 仮想マシンの電源をオフにして登録を解除すると、宛先サイトのボリュームがマウント解除されます。

vSphere Client | Search in all environments | Administrator@SIEMGMT.COM | vSphere Client

VCF9E_Cluster01 | ACTIONS

Summary Monitor Configure Permissions Hosts VMs Datastores Networks Updates

DirectPath Profiles | Related Objects

No DirectPath Profiles utilized

Datacenter
vCF9E_DC01

Recent Tasks

Task Name	Target	Status	Details
Remove datastore	DRaaS_SrcB	Completed	
Remove datastore	DRaaS_SrcB	Completed	
Unregister virtual machine	DRaaSTest_U24_New	Completed	
Unregister virtual machine	DRaaSTest_W2K2	Completed	
Power Off virtual machine	DRaaSTest_U24_New	Completed	
Power Off virtual machine	DRaaSTest_W2K2	Completed	

Initiator	Queued For	Start Time	Completion Time
SIEMGMT.COM\Administrator	7 ms	08/15/2025, 2:27:02 AM	08/15/2025, 2:27:03 AM
SIEMGMT.COM\Administrator	7 ms	08/15/2025, 2:27:01 AM	08/15/2025, 2:27:02 AM
SIEMGMT.COM\Administrator	4 ms	08/15/2025, 2:27:00 AM	08/15/2025, 2:27:01 AM
SIEMGMT.COM\Administrator	15 ms	08/15/2025, 2:27:00 AM	08/15/2025, 2:27:00 AM
SIEMGMT.COM\Administrator	26 ms	08/15/2025, 2:23:55 AM	08/15/2025, 2:23:56 AM
SIEMGMT.COM\Administrator	9 ms	08/15/2025, 2:23:55 AM	08/15/2025, 2:23:57 AM

- 元のソースのSnapMirror関係を解除して、読み取り/書き込み可能にします。
- レプリケーションを元に戻すには、SnapMirror関係を再同期します。
- ソースにボリュームをマウントし、ソース仮想マシンをパワーオンして登録します。

vSphere Client | Search in all environments | Administrator@SIEMGMT.COM | vSphere Client

DRaaSTest_U24_New | ACTIONS

Summary Monitor Configure Permissions Datastores Networks Snapshots Updates

Guest OS

Virtual Machine Details

ACTIONS

Power Status: Powered On
Guest OS: Ubuntu Linux (64-bit)
VMware Tools: Running, version:10362 (Current)
DNS Name (1): DRaaSTest-U24
IP Addresses (1): 10.193.170.56
Encryption: Not encrypted

Usage
Last updated: 8/15/25, 2:28 AM

CPU
1.323 GHz used

Memory
1.5 GB used

Storage
9.71 GB used

VIEW STATS

Recent Tasks

Task Name	Target	Status	Details
Power On virtual machine	DRaaSTest_W2K2	Completed	
Power On virtual machine	DRaaSTest_U24_New	Completed	

Initiator	Queued For	Start Time	Completion Time
SIEMGMT.COM\Administrator	6 ms	08/15/2025, 2:25:47 AM	08/15/2025, 2:25:47 AM
SIEMGMT.COM\Administrator	7 ms	08/15/2025, 2:25:47 AM	08/15/2025, 2:25:47 AM

BlueXP DRaaSへのアクセスと設定の詳細については、"BlueXP Disaster Recovery for VMwareについて学ぶ"

o

監視とダッシュボード

BlueXPまたはONTAP CLIから、適切なデータストアボリュームのレプリケーションのヘルスステータスを監視し、ジョブ監視を介してフェイルオーバーまたはテストフェイルオーバーのステータスを追跡できます。

The screenshot shows the BlueXP Job monitoring dashboard. At the top, there are six status indicators: Success (87), In progress (0), Queued (0), Canceled (0), Warning (0), and Failed (2). Below this is a circular gauge showing 89 jobs. A table lists five recent jobs:

ID	Status	Workload	Name	Start time	End time	Action
ae2db57a-b923-4220-86cc	Success	DRBackupRetention	Backup retention for plan DemoRP01	08/15/2025, 08:25:52 AM	08/15/2025, 08:25:53 AM	
00e9b796-b35a-4435-817t	Success	DRCleanupSecondaryBackups	Initialize DRcleanupSecondaryBackups of Clean...	08/15/2025, 08:25:13 AM	08/15/2025, 08:25:13 AM	
b5da76c8-ebd8-446d-998c	Success	Backup	Backup for replication plan 'DemoRP01'	08/15/2025, 08:24:58 AM	08/15/2025, 08:25:52 AM	
080910ff-778b-44c6-8081	Success	DRTestFailover	Test failover for replication plan 'DemoRP01'	08/15/2025, 08:24:57 AM	08/15/2025, 08:28:01 AM	Activate Windows
b8c32a38-201a-4dfa-9f0e-	Success	Compliance	Compliance check for replication plan 'DemoRP...	08/15/2025, 08:24:15 AM	08/15/2025, 08:24:19 AM	



ジョブが現在進行中またはキューに入っており、それを停止したい場合は、キャンセルするオプションがあります。

BlueXP disaster recoveryダッシュボードを使用すると、災害復旧サイトとレプリケーションプランの状態を確実に評価できます。これにより、管理者は正常なサイトやプラン、切断されたサイトやプラン、または機能低下したサイトやプランを迅速に特定できます。

The screenshot shows the BlueXP Disaster recovery dashboard. It displays the following information:

- Sites (2):** 2 Running, 0 Down, 0 Issue.
- Replication plans (1):** 1 Ready, 0 Failed.
- Activity (last 12 hours):** Backup reconciliation for plan DemoRP01 (3:1 ago), Discovery of resources in host v09d-vc01.siemgrt.com (in progress), Discovery of resources in host v09e-vc01.siemgrt.com (3:1 ago), Backup retention for plan DemoRP01 (4:m ago), Backup for replication plan DemoRP01 (4:m ago).
- Resource groups:** 1 Resource groups.
- Protected VMs:** 2 Protected VMs.
- Unprotected VMs:** 13 Unprotected VMs.
- Failovers:** 1 Failovers.
- Failbacks:** 1 Failbacks.
- Test failovers:** 0 Test failovers.
- Migrations:** 0 Migrations.

これにより、調整およびカスタマイズされた災害復旧計画を処理するための強力なソリューションが提供され

ます。フェイルオーバーは、計画されたフェイルオーバーとして実行することも、災害が発生して DR サイトをアクティブ化する決定が下されたときにボタンをクリックするだけでフェイルオーバーを実行することもできます。

既存の vSphere クラスタを VCF に変換する

既存のデータストアを持つ vSphere 環境を VCF に変換する方法について学習します。

ONTAP上で実行されている既存のデータストアを含む vSphere 環境を VMware Cloud Foundation (VCF) 環境に変換するには、現在のインフラストラクチャを最新のプライベート クラウド アーキテクチャに統合する必要があります。

このプロセスは、ONTAPストレージの柔軟性を活用して、シームレスなデータ アクセスと管理を実現します。VCF 管理ドメインが確立されると、管理者は追加の vSphere 環境を VCF エコシステムに効率的にインポートできます。この統合により、リソースの使用率が向上し、プライベート クラウドの管理が簡素化され、既存のワークロードの中断を最小限に抑えながらスムーズな移行が保証されます。

vCenter インスタンスの変換に関する技術的な詳細については、次のソリューションを参照してください。

- ・ "既存の vCenter インスタンスを VCF 管理ドメイン (NFS) に変換する"
- ・ "vCenterインスタンス (FCデータストア) をVCF管理ドメインに変換する"

vCenter Server インスタンスを VCF 管理ドメイン (NFS データストア) に変換する

NetApp ONTAP NFS データストアを含む既存の vSphere 8 クラスタを VMware Cloud Foundation (VCF) 管理ドメインに変換します。この手順には、NFS ストレージのプロビジョニング、VMware 用のONTAPツールの導入、VCF インポート ツールを使用してクラスターを変換し、VCF 内での管理の合理化とリソース使用率の最適化を行うことが含まれます。

はじめに

ONTAP上で実行されている既存の NFS データストアを使用してクラスターを変換するには、既存のインフラストラクチャを最新のプライベート クラウド アーキテクチャに統合する必要があります。このプロセスは、NFS ストレージの柔軟性を活用し、シームレスなデータ アクセスと管理を保証します。変換プロセスを通じて VCF 管理ドメインが確立されると、管理者は NFS データストアを使用するものも含め、追加の vSphere クラスターを VCF エコシステムに効率的にインポートできます。この統合により、リソースの使用率が向上するだけでなく、プライベート クラウド インフラストラクチャの管理が簡素化され、既存のワークロードの中断を最小限に抑えながらスムーズな移行が可能になります。

このソリューションでは、クラスタが VCF 管理ドメインに変換されたときに、vSphere 8 の NFS データストアがどのようにプリンシパル ストレージになるかを説明します。

シナリオの概要

このシナリオでは、次の大まかな手順について説明します。

- ・ ONTAP tools for VMware vSphereを導入します。

- ONTAPツールを使用して NFS データストアをプロビジョニングします。
- VCF インポート ツールを使用して、vSphere クラスターを検証します。
- vSphere クラスタに SDDC Manager をデプロイします。
- VCF 変換中に NSX を作成するための JSON ファイルを構成します。
- VCF インポート ツールを使用して、vSphere 8 クラスタを VCF 5.2 に変換します。

前提条件

このシナリオには、次のコンポーネントと構成が必要です。

- NFS トラフィックを許可するように構成されたストレージ仮想マシン (SVM) を備えたNetApp AFFストレージシステム。
- NFS トラフィックを伝送し、SVM に関連付けられた IP ネットワーク上に論理インターフェイス (LIF) が作成されています。
- 4 台の ESXi ホストと、クラスター上に共存する vCenter アプライアンスを備えた vSphere 8 クラスター。
- この目的のために確立された VLAN またはネットワーク セグメント上の vMotion および NFS ストレージ トラフィック用に構成された分散ポート グループ。
- VCF 変換に必要なソフトウェアをダウンロードします。

ONTAP tools for VMware vSphereは、 HA 構成または非 HA 構成のいずれにもインストールできます。ONTAPツールの前提条件の詳細については、以下を参照してください。["ONTAP tools for VMware vSphere の前提条件"](#)。

vSphere を VCF 5.2 に変換またはインポートする際にサポートされるストレージおよびその他の考慮事項については、以下を参照してください。["既存の vSphere 環境を VMware Cloud Foundation に変換またはインポートする前に考慮すべき事項"](#)。

必要なソフトウェアについては、["Broadcom サポートポータル"](#)。

ONTAPストレージシステムの構成については、["ONTAP 9ドキュメント"](#)中心。

VCFの設定方法については、以下を参照してください。["VMware Cloud Foundation ドキュメント"](#)。

展開手順

このソリューションでは、ONTAP tools for VMware vSphereを使用して NFS データストアをプロビジョニングする方法と、既存の vSphere 8 クラスタを VCF 管理ドメインに変換するプロセスについて説明します。

次の手順を実行します。

- ONTAP tools for VMware vSphereを導入します。
- ONTAPツールを使用して NFS データストアをプロビジョニングします。
- VCF インポート ツールを vCenter アプライアンスにコピーします。
- VCF インポート ツールを使用して、vCenter アプライアンスの事前チェックを実行します。
- vCenter クラスタに SDDC マネージャ VM をデプロイします。

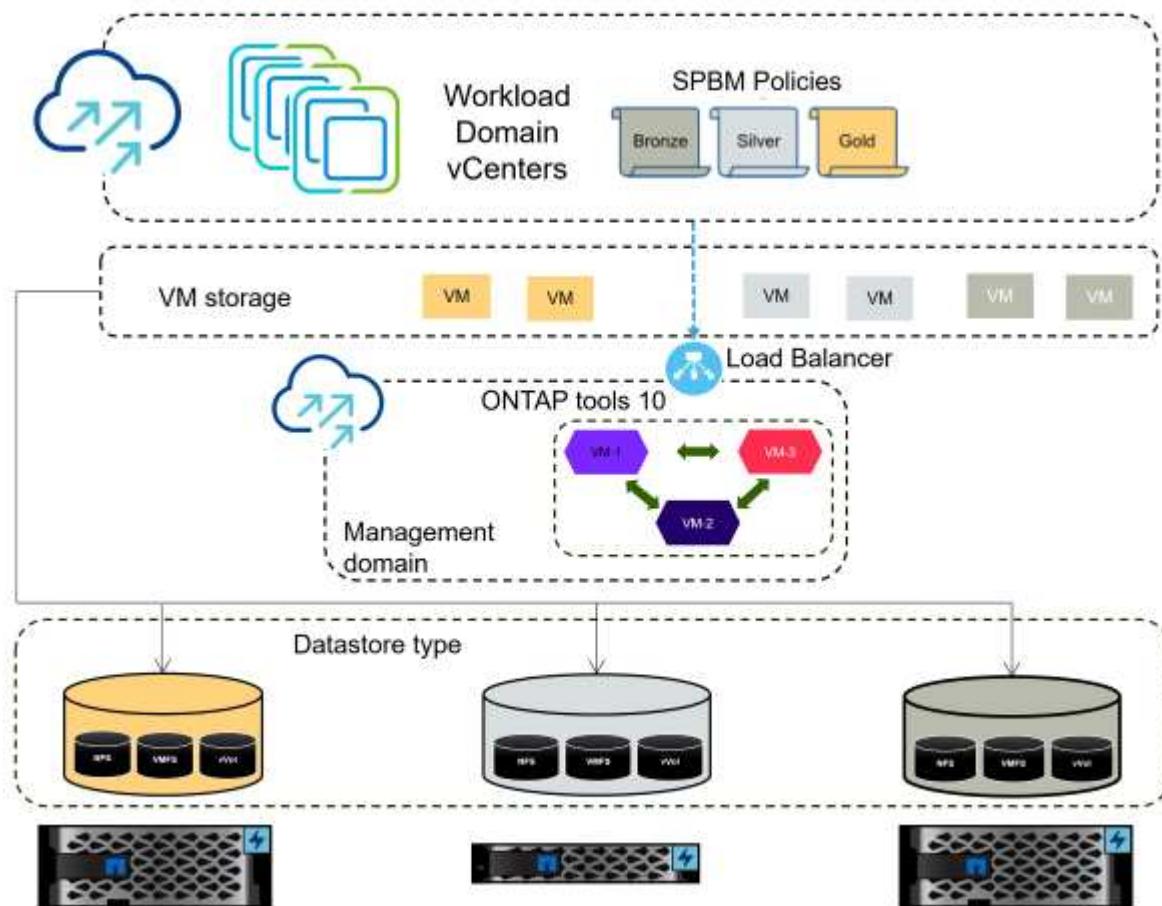
- 変換プロセス中に展開する NSX クラスタの JSON ファイルを作成します。
- 必要なソフトウェアを SDDC マネージャーにアップロードします。
- vSphere クラスターを SDDC マネージャー インベントリに変換します。

変換プロセスの概要については、以下を参照してください。 "[vSphere 環境を管理ドメインに変換するか、VMware Cloud Foundation で vSphere 環境を VI ワークロード ドメインとしてインポートする](#)"。

ONTAPツールを導入し、**NFSデータストア**をプロビジョニングする

ONTAPツール 10 のアーキテクチャは、ONTAPツール サービス、vSphere プラグイン、REST API を含むモジュール式のスケーラブルなフレームワークを活用して、VMware 環境とシームレスに統合し、効率的なストレージ管理、自動化、およびデータ保護を可能にするように設計されています。

ONTAP tools for VMware vSphereは、HA構成または非 HA 構成のいずれにもインストールできます。

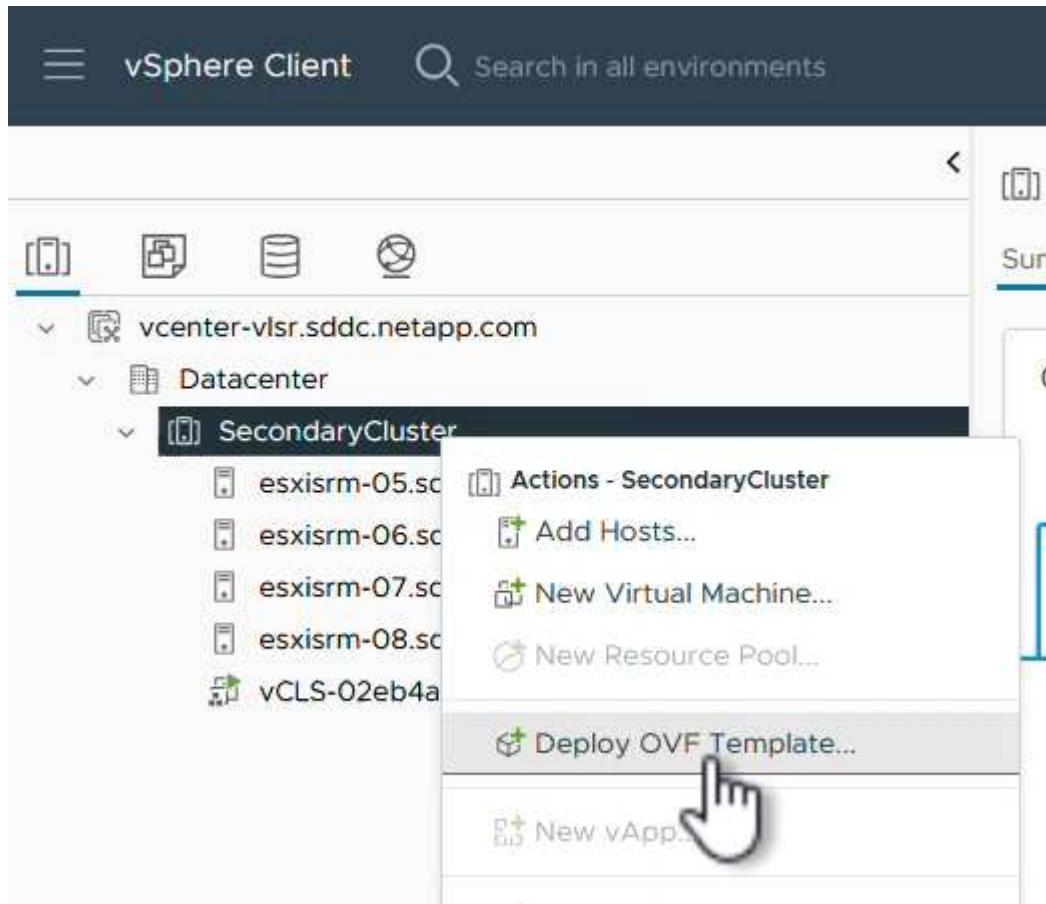


ONTAP tools for VMware vSphereを導入する

このステップでは、ONTAPツール 10 が非 HA 構成で導入されます。

HA構成および非HA構成の詳細な展開については、以下を参照してください。 "ONTAP tools for VMware vSphereを導入する"。

1. ONTAPツール10 OVAテンプレートを以下からダウンロードします。 "[NetAppサポートサイト](#)"。
2. vSphere クライアントで、クラスタを右クリックし、[OVF テンプレートのデプロイ] をクリックします。



3. *OVF テンプレートのデプロイ*で、次の手順を実行します。

- OVF テンプレートを選択します。
- 名前とフォルダを選択します。
- コンピューティング リソースを選択します。
- レビューの詳細。
- ライセンス契約に同意します。

4. テンプレートの構成ページで、ONTAPツールを HA 構成で展開するかどうかを含む展開タイプを選択します。続行するには、[次へ] をクリックします。

Deploy OVF Template

Configuration

Select a deployment configuration

	Description
<input checked="" type="radio"/> Easy deployment (S)	Deploy local provisioner Non-HA Small single node instance of ONTAP tools
<input type="radio"/> Easy deployment (M)	
<input type="radio"/> Advanced deployment (S)	
<input type="radio"/> Advanced deployment (M)	
<input type="radio"/> High-Availability deployment (S)	
<input type="radio"/> High-Availability deployment (M)	
<input type="radio"/> High-Availability deployment (L)	
<input type="radio"/> Recovery	

8 Items

CANCEL BACK NEXT

5. *ストレージの選択*ページで、VM をインストールするデータストアを選択し、*次へ*をクリックします。
6. ONTAPツール VM が通信するネットワークを選択します。続行するには、[次へ] をクリックします。
7. 「テンプレートのカスタマイズ」 ウィンドウで、必要な情報をすべて入力します。
 - アプリケーションのユーザー名とパスワード
 - プロキシ URL を含む ASUP (自動サポート) を有効にするかどうかを選択します。
 - 管理者のユーザー名とパスワード。
 - NTP サーバー。
 - メンテナンスのユーザー名とパスワード (コンソールで使用されるメイン アカウント)。
 - デプロイメント構成に必要な IP アドレスを指定します。
 - ノード構成のすべてのネットワーク情報を提供します。

Node Configuration		10 settings
HostName(*)	Specify the hostname for the VM otv10-primary	
IP Address(*)	Specify the IP address for the appliance 172.21.120.56	
IPv6 Address	Specify the IPv6 address on the deployed network only when you need dual stack.	
Prefix length	Specify the prefix length	
Netmask (Only for IPv4) (*)	Specify the subnet to use on the deployed network 255.255.255.0	
Gateway(*)	Specify the gateway on the deployed network 172.21.120.1	
Primary DNS(*)	Specify the primary DNS server's IP address 10.61.185.231	
Secondary DNS(*)	Specify the secondary DNS server's IP address 10.61.186.231	

CANCEL

BACK

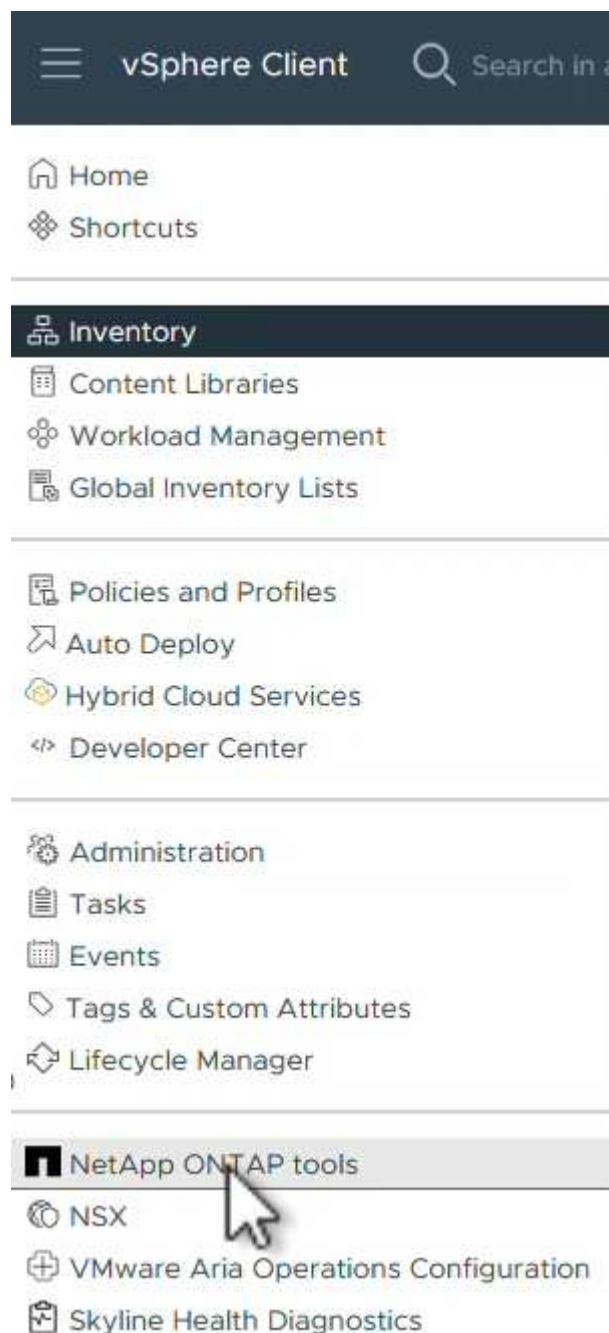
NEXT

8. 最後に、[次へ] をクリックして続行し、[完了] をクリックして展開を開始します。

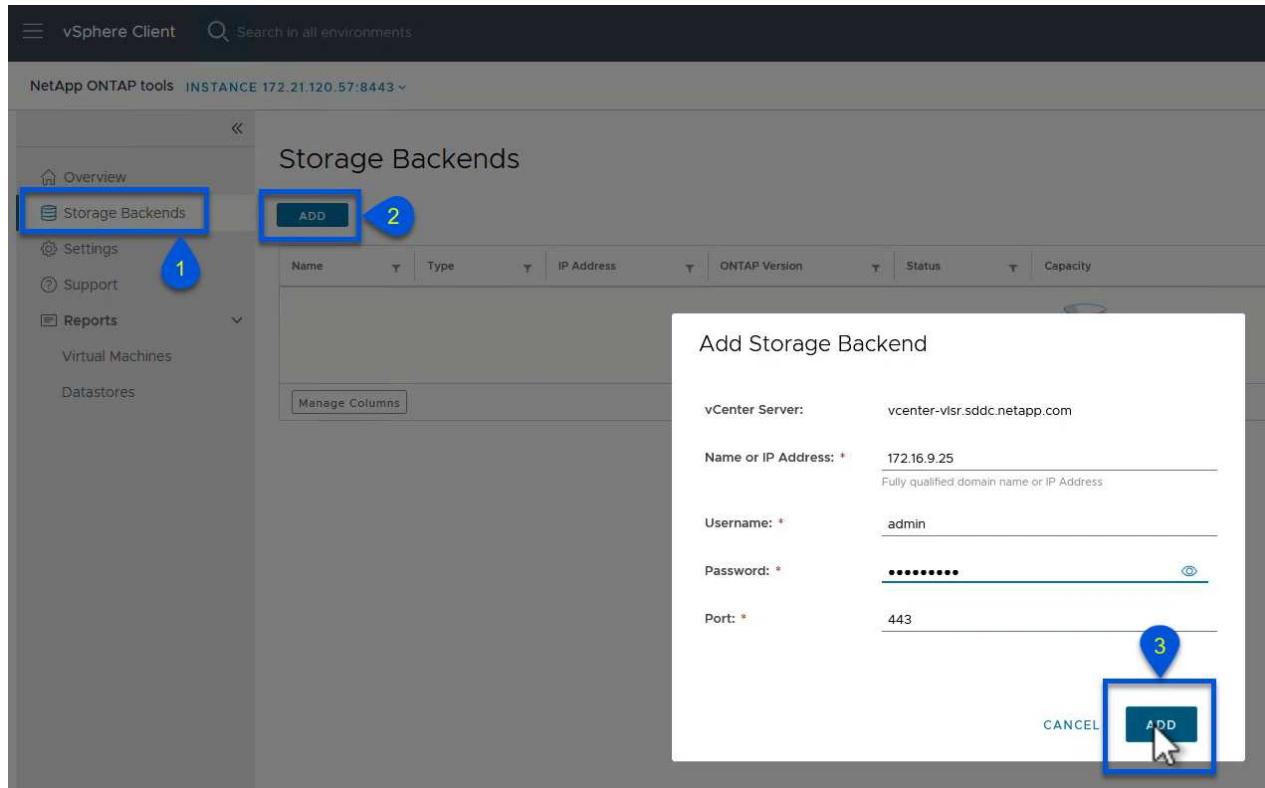
ONTAP Toolsの設定

ONTAPツール VM をインストールして電源を入れると、管理する vCenter サーバーやONTAPストレージシステムを追加するなど、いくつかの基本的な構成が必要になります。以下のドキュメントを参照してください。 "ONTAP tools for VMware vSphere" 詳細情報については。

1. 参照 "vCenterインスタンスを追加する" ONTAPツールを使用して管理されるように vCenter インスタンスを構成します。
2. ONTAPストレージシステムを追加するには、vSphere クライアントにログインし、左側のメインメニューに移動します。 * NetApp ONTAPツール* をクリックして、ユーザーインターフェイスを起動します。



- 左側のメニューのストレージ バックエンドに移動し、追加をクリックしてストレージ バックエンドの追加 ウィンドウにアクセスします。
- 管理するONTAPストレージ システムのIP アドレスと資格情報を入力します。*追加*をクリックして終了します。



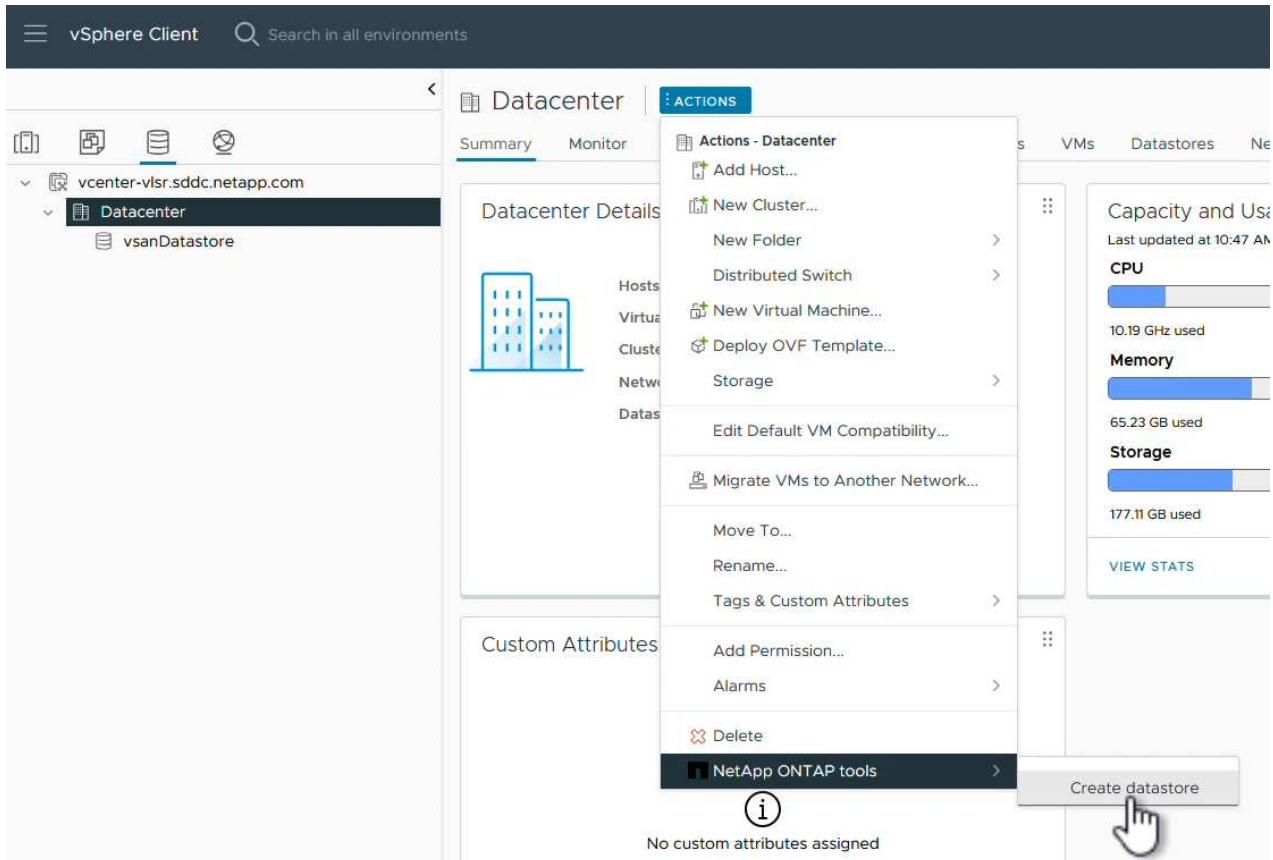
ここで、ストレージ バックエンドは、クラスター IP アドレスを使用して vSphere クライアント UI に追加されます。これにより、ストレージ システム内のすべての SVM を完全に管理できるようになります。あるいは、ONTAPツールマネージャを使用してストレージバックエンドを追加し、vCenterインスタンスに関連付けることもできます。
<https://loadBalanceIP:8443/virtualization/ui/>。この方法では、vSphere クライアント UI で SVM 資格情報のみを追加できるため、ストレージ アクセスをより細かく制御できます。



ONTAPツールを使用して NFS データストアをプロビジョニングする

ONTAPツールは、vSphere クライアント UI 全体に機能を統合します。このステップでは、ストレージ インベントリ ページから NFS データストアがプロビジョニングされます。

1. vSphere クライアントで、ストレージ インベントリに移動します。
2. アクション > NetApp ONTAPツール > データストアの作成 に移動します。



3. *データストアの作成* ウィザードで、作成するデータストアの種類を選択します。オプションは NFS または VMFS です。
4. 名前とプロトコル ページで、データストアの名前、サイズ、使用する NFS プロトコルを入力します。

Create Datastore

1 Type

2 Name and Protocol

3 Storage

4 Storage Attributes

5 Summary

Name and Protocol

Datastore name:

Size: TB
Minimum supported size is 1 GB.

Protocol:

Advanced Options

Datastore Cluster:

CANCEL BACK NEXT 



- ストレージページで、ONTAPストレージ プラットフォームとストレージ仮想マシン (SVM) を選択します。ここで、利用可能なカスタム エクスポート ポリシーを選択することもできます。続行するには、[次へ] をクリックします。

Create Datastore

1 Type

2 Name and Protocol

3 Storage

4 Storage Attributes

5 Summary

Storage

Platform: *

Storage VM: *
ntaphcli-a300e9u25 (172.16.9.25)

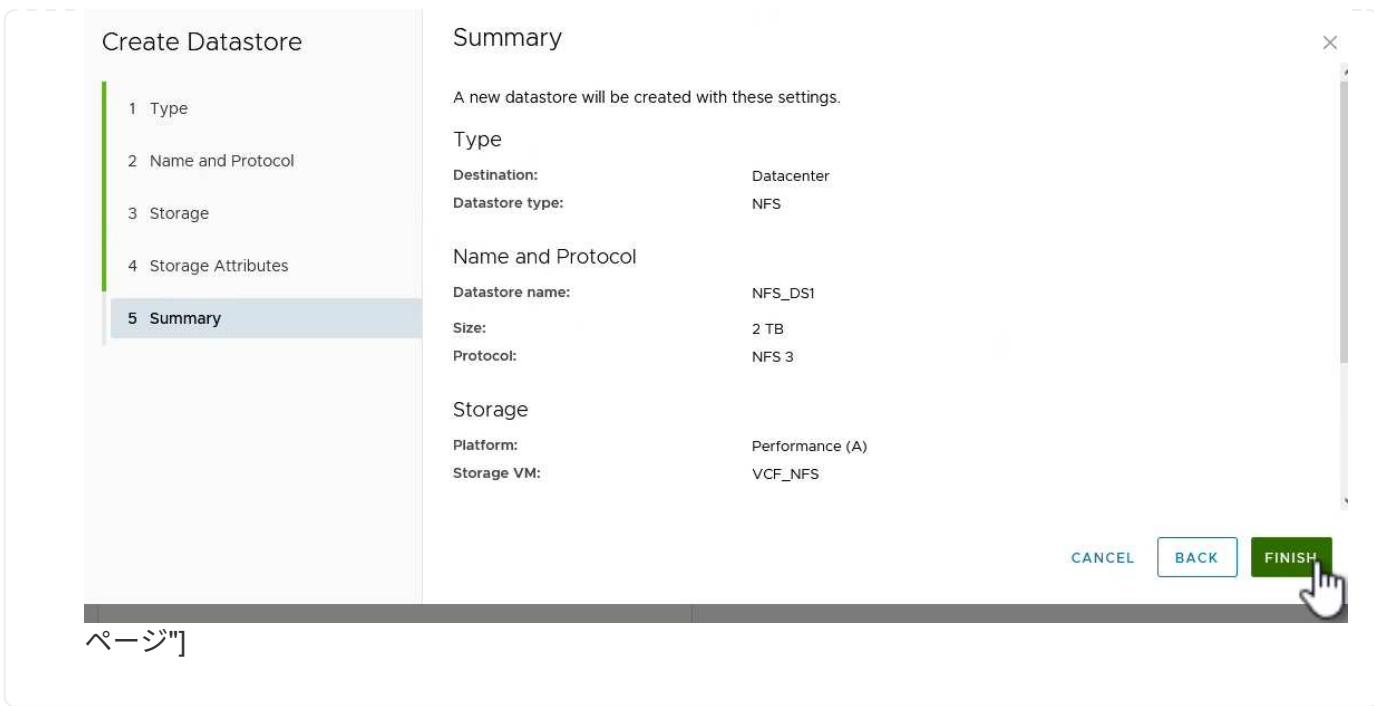
Advanced Options

Custom Export Policy:
Choose an existing policy or give a new name to the default policy.

CANCEL BACK NEXT 



- *ストレージ属性*ページで、使用するストレージ アグリゲートを選択します。続行するには、[次へ] をクリックします。
- *概要*ページで情報を確認し、*完了*をクリックしてプロビジョニング プロセスを開始します。ONTAPツールは、ONTAPストレージシステムにボリュームを作成し、それをクラスタ内のすべてのESXiホストにNFSデータストアとしてマウントします。



ページ"]

vSphere クラスタを VCF 5.2 に変換する

次のセクションでは、SDDC マネージャをデプロイし、vSphere 8 クラスタを VCF 5.2 管理ドメインに変換する手順について説明します。必要に応じて、詳細については VMware のドキュメントが参照されます。

VMware by Broadcom の VCF インポート ツールは、vCenter アプライアンスと SDDC マネージャの両方で使用されるユーティリティで、構成を検証し、vSphere および VCF 環境の変換およびインポート サービスを提供します。

```
https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vcf-5-2-and-earlier/5-2/map-for-administering-vcf-5-2/importing-existing-vsphere-environments-admin/vcf-import-tool-options-and-parameters-admin.html ["VCFインポートツールのオプションとパラメータ"]。
```

VCFインポートツールのコピーと抽出

VCF インポート ツールは、vCenter アプライアンスで使用され、vSphere クラスタが VCF 変換またはインポート プロセスに対して正常な状態にあることを検証します。

次の手順を実行します。

- 以下の手順に従ってください "VCFインポートツールをターゲットのvCenterアプライアンスにコピーします" VMware Docs を参照して、VCF インポート ツールを正しい場所にコピーします。
- 次のコマンドを使用してバンドルを抽出します。

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

vCenterアプライアンスを検証する

変換前に、VCF インポート ツールを使用して vCenter アプライアンスを検証します。

1. 次の手順に従ってください "変換前にターゲット vCenter で事前チェックを実行する" 検証を実行します。
2. 次の出力は、vCenter アプライアンスが事前チェックに合格したことを示しています。

```
root@localhost | /tmp/vcfimport/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter 172.21.166.57 --sso-user administrator@vsphere.local
[2024-10-23 19:03:23,609] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.0-24307788
Enter vCenter SSO password:
[2024-10-23 19:03:28,825] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2024-10-23 19:03:28,938] [INFO] vc_precheck: Connected to vCenter 172.21.166.57 in 0.11 seconds
[2024-10-23 19:03:28,939] [INFO] vc_precheck: Running pre-checks for vCenter 172.21.166.57...
[2024-10-23 19:03:28,939] [INFO] vc_precheck: [1/10] VM BOM version check... PASS
[2024-10-23 19:03:28,975] [INFO] vc_precheck: [2/10] vSAN stretched cluster check... PASS
[2024-10-23 19:03:28,999] [INFO] vc_precheck: [3/10] Supported storage available check... PASS
[2024-10-23 19:03:29,020] [INFO] vc_precheck: [4/10] vCenter VM location check... PASS
[2024-10-23 19:03:29,233] [INFO] vc_precheck: [5/10] VxRail registration check... PASS
[2024-10-23 19:03:29,414] [INFO] vc_precheck: [6/10] NSX-T registration check... PASS
[2024-10-23 19:03:29,437] [INFO] vc_precheck: [7/10] Standalone host check... PASS
[2024-10-23 19:03:31,870] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check... PASS
[2024-10-23 19:03:32,962] [INFO] vc_precheck: [9/10] ELM ring topology check... PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: [10/10] WCP import check... PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: All pre-checks passed!
[2024-10-23 19:03:33,383] [INFO] vc_precheck: Pre-Checks for vCenter 172.21.166.57 completed in 4.44 seconds
root@localhost | /tmp/vcfimport/vcf-brownfield-toolset ]#
```

SDDC マネージャーを展開する

SDDC マネージャーは、VCF 管理ドメインに変換される vSphere クラスター上に共存する必要があります。

展開を完了するには、VMware Docs の展開手順に従ってください。

参照 "ターゲット vCenter に SDDC Manager アプライアンスを展開する"。

詳細については、"委員会ホスト" VCF 管理ガイドを参照してください。

NSX 展開用の JSON ファイルを作成する

vSphere 環境を VMware Cloud Foundation にインポートまたは変換しながら NSX Manager をデプロイするには、NSX デプロイ仕様を作成します。NSX の展開には少なくとも 3 台のホストが必要です。



変換またはインポート操作で NSX Manager クラスタを展開する場合、NSX-VLAN ネットワークが利用されます。NSX-VLAN ネットワークの制限の詳細については、「既存の vSphere 環境を VMware Cloud Foundation に変換またはインポートする前の考慮事項」セクションを参照してください。NSX-VLAN ネットワークの制限については、以下を参照してください。["既存の vSphere 環境を VMware Cloud Foundation に変換またはインポートする前に考慮すべき事項"](#)。

以下は、NSX デプロイメント用の JSON ファイルの例です。

```
{  
    "license_key": "xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx",  
    "form_factor": "medium",  
    "admin_password": "NetApp!23456789",  
    "install_bundle_path": "/tmp/vcfimport/bundle-133764.zip",  
    "cluster_ip": "172.21.166.72",  
    "cluster_fqdn": "vcf-m02-nsx01.sddc.netapp.com",  
    "manager_specs": [  
        {  
            "fqdn": "vcf-m02-nsx01a.sddc.netapp.com",  
            "name": "vcf-m02-nsx01a",  
            "ip_address": "172.21.166.73",  
            "gateway": "172.21.166.1",  
            "subnet_mask": "255.255.255.0"  
        },  
        {  
            "fqdn": "vcf-m02-nsx01b.sddc.netapp.com",  
            "name": "vcf-m02-nsx01b",  
            "ip_address": "172.21.166.74",  
            "gateway": "172.21.166.1",  
            "subnet_mask": "255.255.255.0"  
        },  
        {  
            "fqdn": "vcf-m02-nsx01c.sddc.netapp.com",  
            "name": "vcf-m02-nsx01c",  
            "ip_address": "172.21.166.75",  
            "gateway": "172.21.166.1",  
            "subnet_mask": "255.255.255.0"  
        }]  
}
```

JSON ファイルを SDDC マネージャー上のディレクトリにコピーします。

SDDC マネージャーにソフトウェアをアップロードする

VCF インポート ツールと NSX デプロイメント バンドルを SDDC マネージャの /home/vcf/vcfimport ディレクトリにコピーします。

見る "[必要なソフトウェアを SDDC Manager アプライアンスにアップロードする](#)" 詳細な手順については、こちらをご覧ください。

vSphere クラスタを VCF 管理ドメインに変換する

変換プロセスを実行するには、VCF インポート ツールが使用されます。/home/vcf/vcf-import-package/vcf-brownfield-import-<version>/vcf-brownfield-toolset ディレクトリから次のコマンドを実行して、VCF インポート ツール関数のプリントアウトを確認します。

```
python3 vcf_brownfield.py --help
```

次のコマンドを実行して、vSphere クラスタを VCF 管理ドメインに変換し、NSX クラスタをデプロイします。

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user '<sso-user>' --domain-name '<wld-domain-name>' --nsx-deployment-spec-path '<nsx-deployment-json-spec-path>'
```

詳しい手順については、 "[vSphere 環境を SDDC Manager インベントリに変換またはインポートする](#)"。

VCFにライセンスを追加する

変換が完了したら、環境にライセンスを追加する必要があります。

1. SDDC Manager UI にログインします。
2. ナビゲーションペインで 管理 > ライセンス に移動します。
3. + ライセンス キー をクリックします。
4. ドロップダウンメニューから製品を選択します。
5. ライセンスキーを入力してください。
6. ライセンスの説明を入力します。
7. *[追加]*をクリックします。
8. ライセンスごとにこれらの手順を繰り返します。

ONTAP tools for VMware vSphere のビデオ デモ

[ONTAP tools for VMware vSphere を備えた NFS データストア](#)

vCenter Server インスタンスを VCF 管理ドメイン (FC データストア) に変換する

ONTAPファイバ チャネル データストアを使用する vSphere 8 クラスタを VMware Cloud Foundation 管理ドメインに変換します。この手順には、FC ストレージのプロビジョニング、VMware 用のONTAPツールの導入、VCF インポート ツールを使用した VCF 環境内のクラスターの移行と管理が含まれます。

はじめに

ONTAP上で実行されている既存のファイバ チャネル (FC) データストアを使用して vSphere 環境を変換するには、既存のインフラストラクチャを最新のプライベート クラウド アーキテクチャに統合する必要があります。このプロセスは、FC ストレージの堅牢性を活用し、シームレスなデータ アクセスと管理を保証します。変換プロセスを通じて VCF 管理ドメインが確立されると、管理者は FC データストアを使用する環境を含む追加の vSphere 環境を VCF エコシステムに効率的にインポートできます。この統合により、リソースの使用率が向上するだけでなく、プライベート クラウド インフラストラクチャの管理が簡素化され、既存のワークフローの中止を最小限に抑えながらスムーズな移行が可能になります。

このソリューションでは、クラスタが VCF 管理ドメインに変換されたときに、vSphere 8 の FC データストアがどのようにプリンシパル ストレージになるかを説明します。

シナリオの概要

このシナリオでは、次の大きな手順について説明します。

- ONTAP tools for VMware vSphereを導入します。
- ONTAPツールを使用して FC データストアをプロビジョニングします。
- VCF インポート ツールを使用して、vSphere クラスターを検証します。
- vSphere クラスタに SDDC Manager をデプロイします。
- VCF 変換中に NSX を作成するための JSON ファイルを構成します。
- VCF インポート ツールを使用して、vSphere 8 クラスタを VCF 5.2.1 に変換します。

前提条件

このシナリオには、次のコンポーネントと構成が必要です。

- ファイバ チャネル (FC) トラフィックを許可するように構成されたストレージ仮想マシン (SVM) を備えたNetApp ASA R2/ ASA/ AFFストレージシステム。
- FC トラフィックを伝送するために論理インターフェイス (LIF) が作成され、SVM に関連付けられています。
- FC トラフィックを伝送するように指定されたスイッチに FC ゾーニングが設定されています。
- 4 台の ESXi ホストと、クラスター上に共存する vCenter アプライアンスを備えた vSphere 8 クラスター。
- この目的のために確立された VLAN またはネットワーク セグメント上の vMotion 用に構成された分散ポート グループ。
- VCF 変換に必要なソフトウェアをダウンロードします。

ONTAP tools for VMware vSphereは、 HA 構成または非 HA 構成のいずれにもインストールできます。

ONTAPツールの前提条件の詳細については、以下を参照してください。 "[ONTAP tools for VMware vSphereの前提条件](#)"。

vSphere を VCF 5.2 に変換またはインポートする際にサポートされるストレージおよびその他の考慮事項については、以下を参照してください。 "[既存の vSphere 環境を VMware Cloud Foundation に変換またはインポートする前に考慮すべき事項](#)"。

必要なソフトウェアについては、 "[既存の vSphere 環境を変換またはインポートするためのソフトウェアをダウンロードする](#)"。

ONTAPストレージシステムの構成については、 "[ONTAP 9ドキュメント](#)" 中心。

VCFの設定方法については、以下を参照してください。 "[VMware Cloud Foundation 5.2 ドキュメント](#)"。

展開手順

このソリューションでは、ONTAP tools for VMware vSphereを使用して FC データストアをプロビジョニングする方法と、既存の vSphere 8 クラスタを VCF 管理ドメインに変換するプロセスについて説明します。

次の手順を実行します。

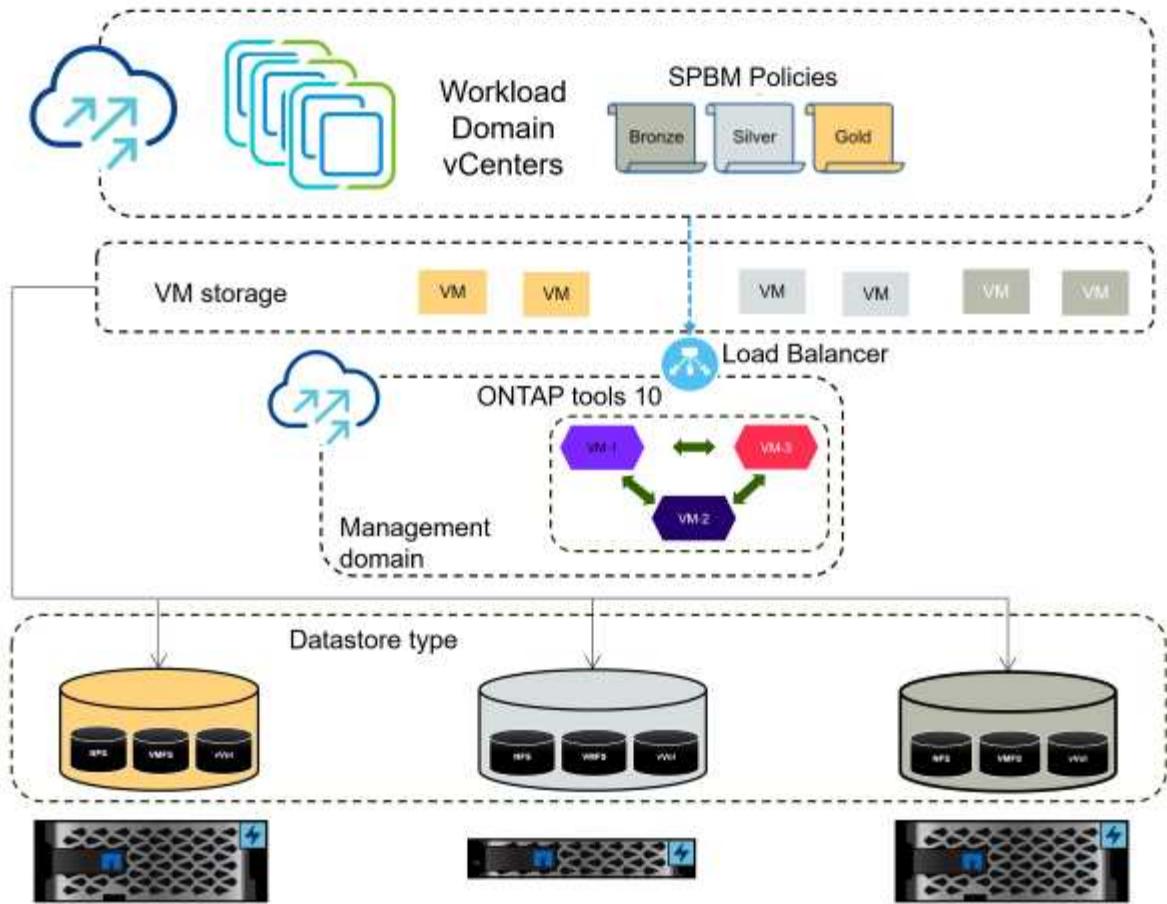
- ONTAP tools for VMware vSphereを導入します。
- ONTAPツールを使用して FC データストアをプロビジョニングします。
- VCF インポート ツールを vCenter アプライアンスにコピーします。
- VCF インポート ツールを使用して、vCenter アプライアンスの事前チェックを実行します。
- vCenter クラスタに SDDC マネージャ VM をデプロイします。
- 変換プロセス中に展開する NSX クラスタの JSON ファイルを作成します。
- 必要なソフトウェアを SDDC マネージャーにアップロードします。
- vSphere クラスターを SDDC マネージャー インベントリに変換します。

変換プロセスの概要については、以下を参照してください。 "[vSphere 環境を管理ドメインに変換するか、VMware Cloud Foundation で vSphere 環境を VI ワークロード ドメインとしてインポートする](#)"。

ONTAPツールを導入し、FCデータストアをプロビジョニングする

ONTAPツール 10 のアーキテクチャは、ONTAPツール サービス、vSphere プラグイン、REST API を含むモジュール式のスケーラブルなフレームワークを活用して、VMware 環境とシームレスに統合し、効率的なストレージ管理、自動化、およびデータ保護を可能にするように設計されています。

ONTAP tools for VMware vSphereは、 HA 構成または非 HA 構成のいずれにもインストールできます。

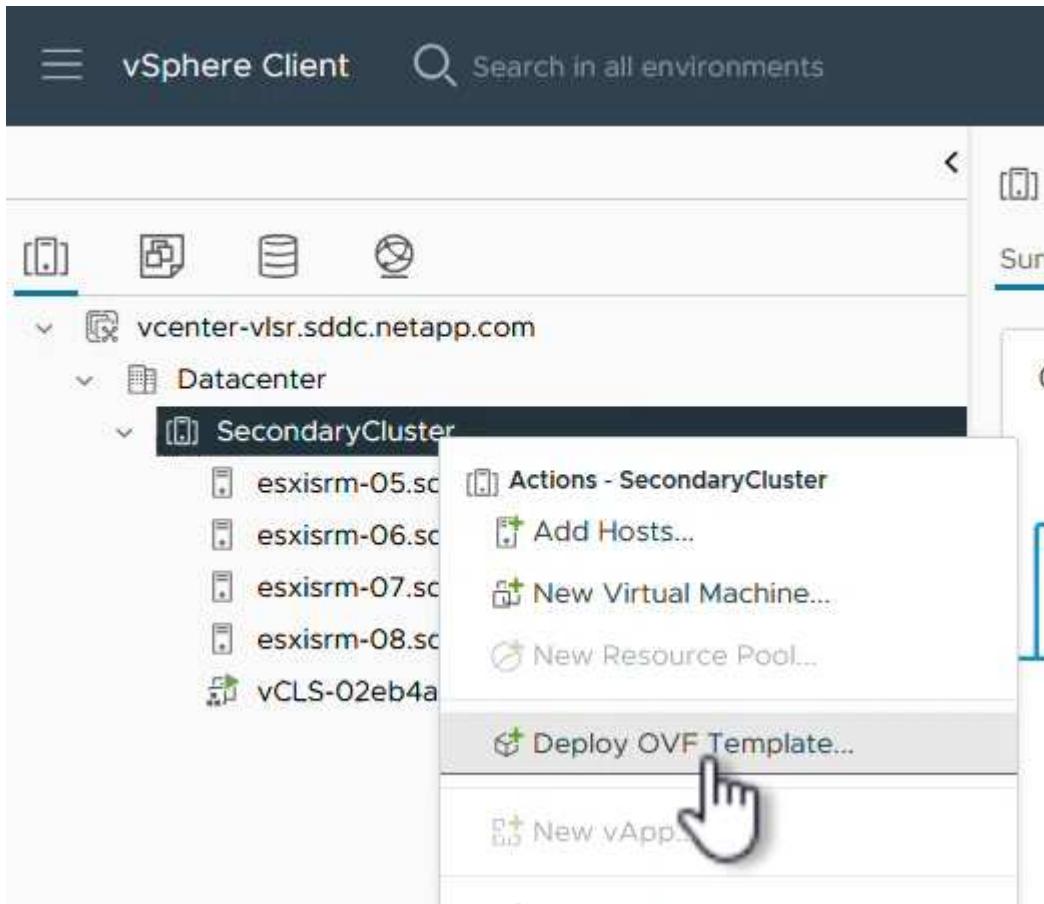


ONTAP tools for VMware vSphereを導入する

このステップでは、ONTAPツール 10 が非 HA 構成で導入されます。

HA構成および非HA構成の詳細な展開については、以下を参照してください。 "ONTAP tools for VMware vSphereを導入する"。

1. ONTAPツール10 OVAテンプレートを以下からダウンロードします。 "[NetAppサポートサイト](#)"。
2. vSphere クライアントで、クラスタを右クリックし、[OVF テンプレートのデプロイ] をクリックします。



3. *OVF テンプレートのデプロイ*で、次の手順を実行します。

- OVF テンプレートを選択します。
- 名前とフォルダを選択します。
- コンピューティング リソースを選択します。
- レビューの詳細。
- ライセンス契約に同意します。

4. テンプレートの構成ページで、ONTAPツールを HA 構成で展開するかどうかを含む展開タイプを選択します。続行するには、[次へ] をクリックします。

The screenshot shows the 'Deploy OVF Template' wizard with the following steps:

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Configuration** (highlighted)
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

The 'Configuration' step is currently active. A sub-menu titled 'Select a deployment configuration' is open, listing the following options:

	Description
<input checked="" type="radio"/> Easy deployment (S)	Deploy local provisioner Non-HA Small single node instance of ONTAP tools
<input type="radio"/> Easy deployment (M)	
<input type="radio"/> Advanced deployment (S)	
<input type="radio"/> Advanced deployment (M)	
<input type="radio"/> High-Availability deployment (S)	
<input type="radio"/> High-Availability deployment (M)	
<input type="radio"/> High-Availability deployment (L)	
<input type="radio"/> Recovery	

At the bottom right of the configuration window, there are buttons for 'CANCEL', 'BACK', and 'NEXT' (with a hand cursor icon).

5. *ストレージの選択*ページで、VM をインストールするデータストアを選択し、*次へ*をクリックします。
6. ONTAPツール VM が通信するネットワークを選択します。続行するには、[次へ] をクリックします。
7. 「テンプレートのカスタマイズ」 ウィンドウで、必要な情報をすべて入力します。
 - アプリケーションのユーザー名とパスワード
 - プロキシ URL を含む ASUP (自動サポート) を有効にするかどうかを選択します。
 - 管理者のユーザー名とパスワード。
 - NTP サーバー。
 - メンテナンスのユーザー名とパスワード (コンソールで使用されるメイン アカウント)。
 - デプロイメント構成に必要な IP アドレスを指定します。
 - ノード構成のすべてのネットワーク情報を提供します。

Node Configuration		10 settings
HostName(*)	Specify the hostname for the VM otv10-primary	
IP Address(*)	Specify the IP address for the appliance 172.21.120.56	
IPv6 Address	Specify the IPv6 address on the deployed network only when you need dual stack.	
Prefix length	Specify the prefix length	
Netmask (Only for IPv4) (*)	Specify the subnet to use on the deployed network 255.255.255.0	
Gateway(*)	Specify the gateway on the deployed network 172.21.120.1	
Primary DNS(*)	Specify the primary DNS server's IP address 10.61.185.231	
Secondary DNS(*)	Specify the secondary DNS server's IP address 10.61.186.231	

CANCEL

BACK

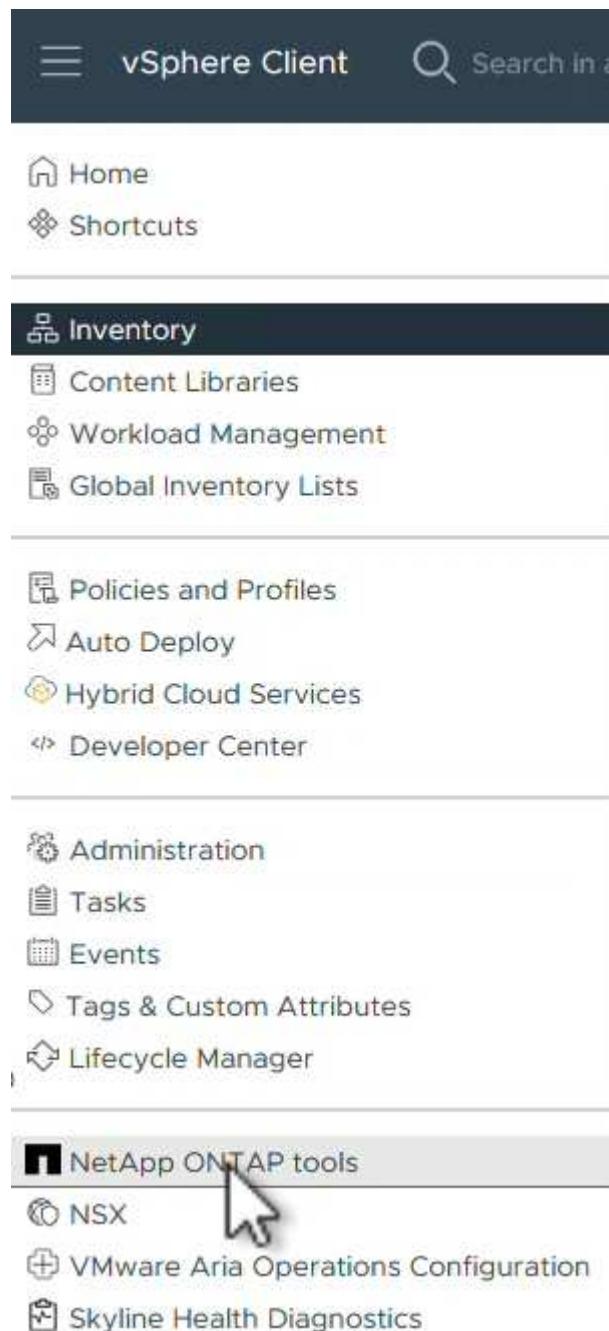
NEXT

8. 最後に、[次へ] をクリックして続行し、[完了] をクリックして展開を開始します。

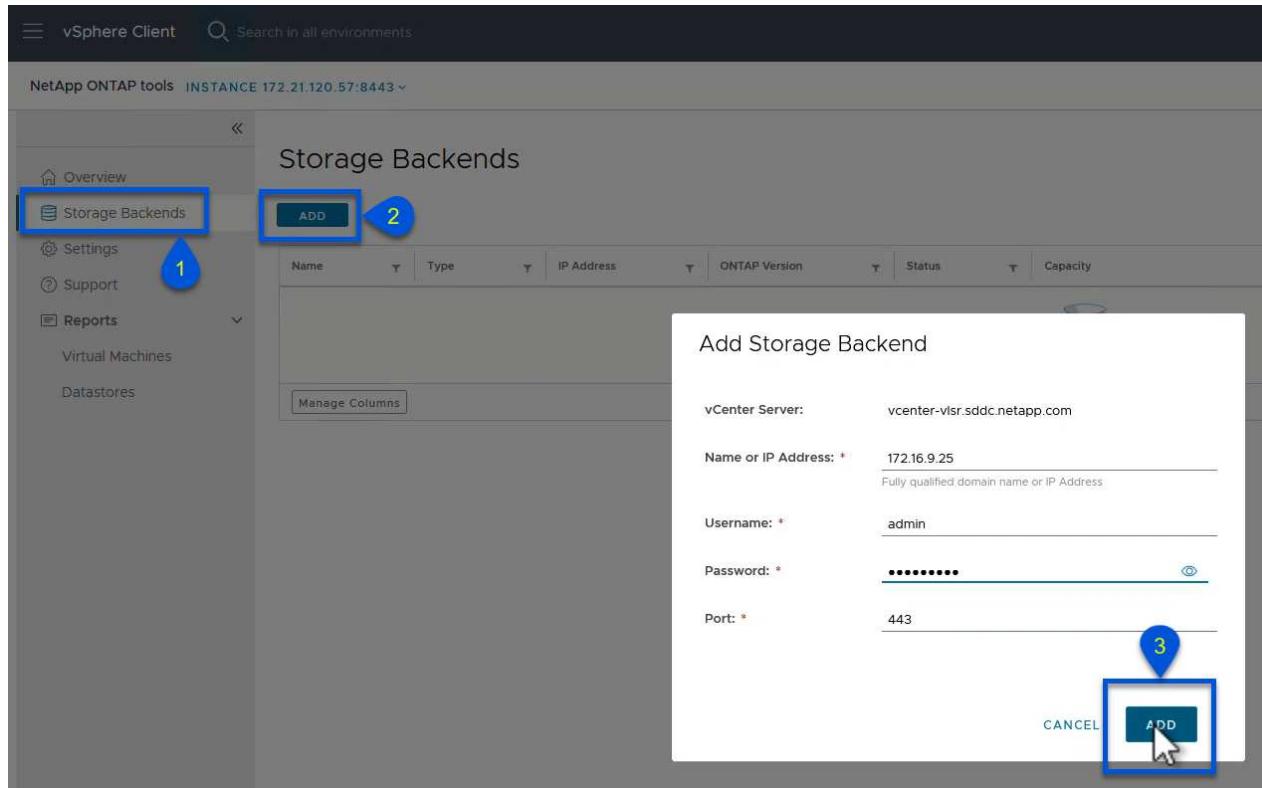
ONTAP Toolsの設定

ONTAPツール VM をインストールして電源を入れると、管理する vCenter サーバーやONTAPストレージシステムを追加するなど、いくつかの基本的な構成が必要になります。以下のドキュメントを参照してください。 "ONTAP tools for VMware vSphere" 詳細情報については。

1. 参照 "vCenterインスタンスを追加する" ONTAPツールを使用して管理されるように vCenter インスタンスを構成します。
2. ONTAPストレージシステムを追加するには、vSphere クライアントにログインし、左側のメインメニューに移動します。 * NetApp ONTAPツール* をクリックして、ユーザーインターフェイスを起動します。



- 左側のメニューのストレージ バックエンドに移動し、追加をクリックしてストレージ バックエンドの追加 ウィンドウにアクセスします。
- 管理するONTAPストレージ システムのIP アドレスと資格情報を入力します。*追加*をクリックして終了します。



ここで、ストレージ バックエンドは、クラスター IP アドレスを使用して vSphere クライアント UI に追加されます。これにより、ストレージ システム内のすべての SVM を完全に管理できるようになります。あるいは、ONTAPツールマネージャを使用してストレージバックエンドを追加し、vCenterインスタンスに関連付けることもできます。
<https://loadBalanceIP:8443/virtualization/ui/>。この方法では、vSphere クライアント UI で SVM 資格情報のみを追加できるため、ストレージ アクセスをより細かく制御できます。



ONTAPツールでFCデータストアをプロビジョニングする

ONTAPツールは、vSphere クライアント UI 全体に機能を統合します。この手順では、ホストのインベントリ ページから FC データストアがプロビジョニングされます。

1. vSphere クライアントで、ホスト (またはストレージ) インベントリに移動します。
2. アクション > NetApp ONTAPツール > データストアの作成 に移動します。

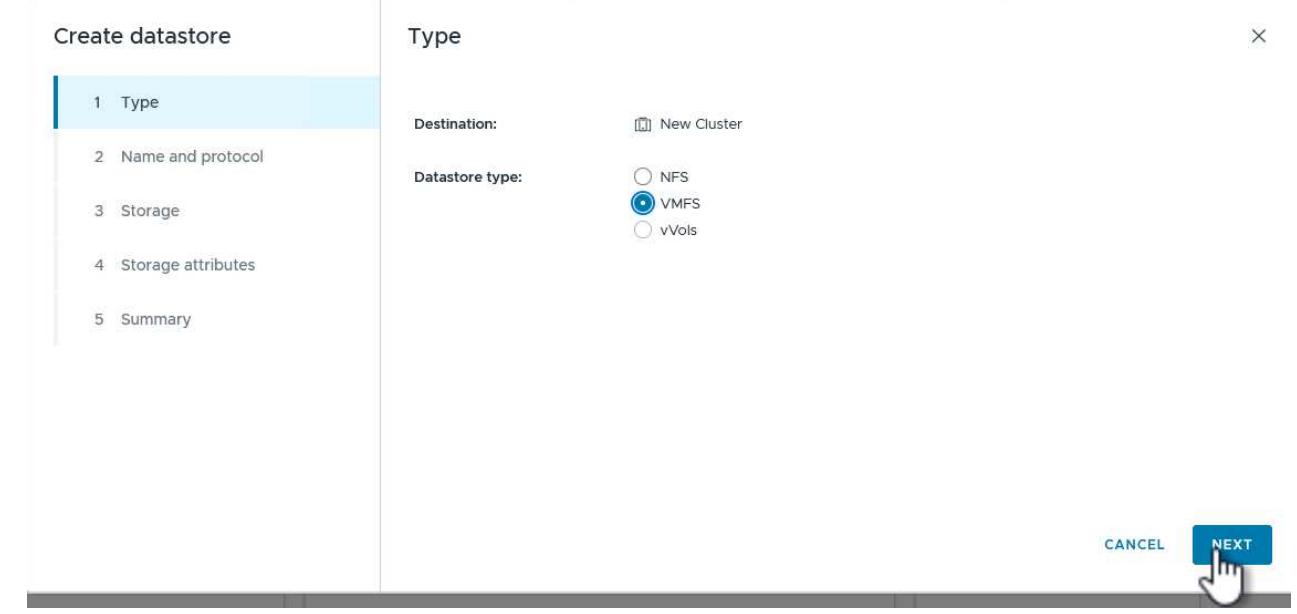
The screenshot shows the vSphere Client interface with the following details:

- Left Sidebar:** Shows a tree view of the vSphere environment, including a Datacenter named "vcfa-vcf.sddc.netapp.com" which contains several hosts.
- Middle Panel:** The "New Cluster" wizard is open, showing "Capacity and Usage" statistics for the selected hosts. It includes sections for CPU, Memory, and Storage usage.
- Right Panel:** The "Actions" menu is open under the "New Cluster" section. It lists various actions such as "Add Hosts...", "New Virtual Machine...", and "Deploy OVF Template...". A sub-menu for "NetApp ONTAP tools" is also visible.
- Bottom Panel:** The "Recent Tasks" table shows three completed tasks related to ONTAP tool discovery.

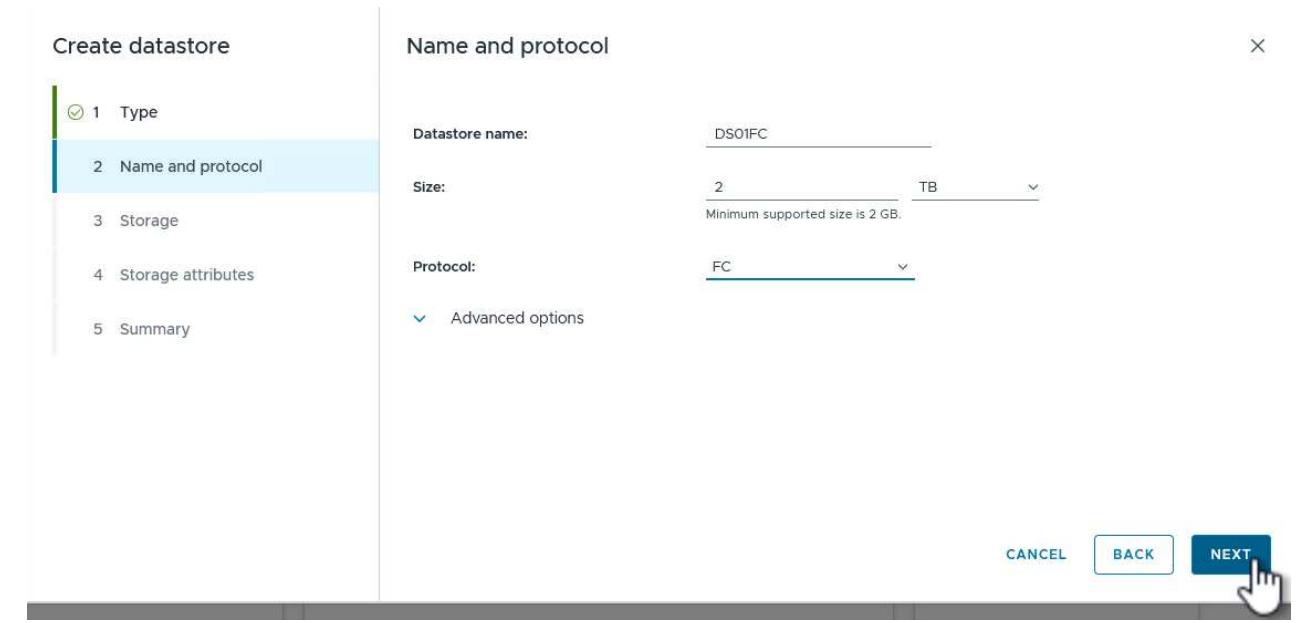
A hand cursor is hovering over the "Create Datastore" button in the "NetApp ONTAP tools" sub-menu.

Task Name	Target	Status	Details	Initiator	Queue For
ONTAP tools Discover hosts	vcsa-vcf.sddc.netapp.com	Completed	Discover hosts initiated with job id 137	VSphere	13 m
ONTAP tools Discover hosts	vcsa-vcf.sddc.netapp.com	Completed	Discover hosts initiated with job id 136	VSphere	13 m
ONTAP tools Discover	vcsa-vcf.sddc.netapp.com	Completed	Discover hosts initiated with job id 135	VSPHERE.LOCAL\Administrat	8 m

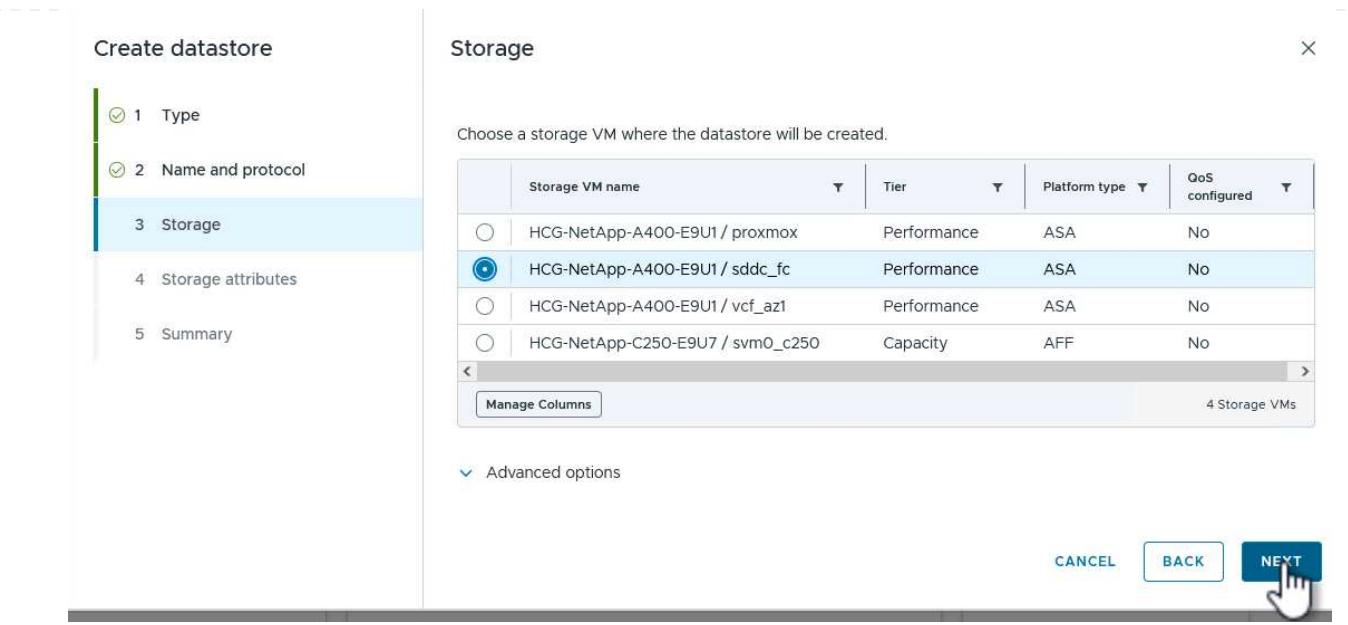
3. *データストアの作成*ウィザードで、作成するデータストアのタイプとして VMFS を選択します。



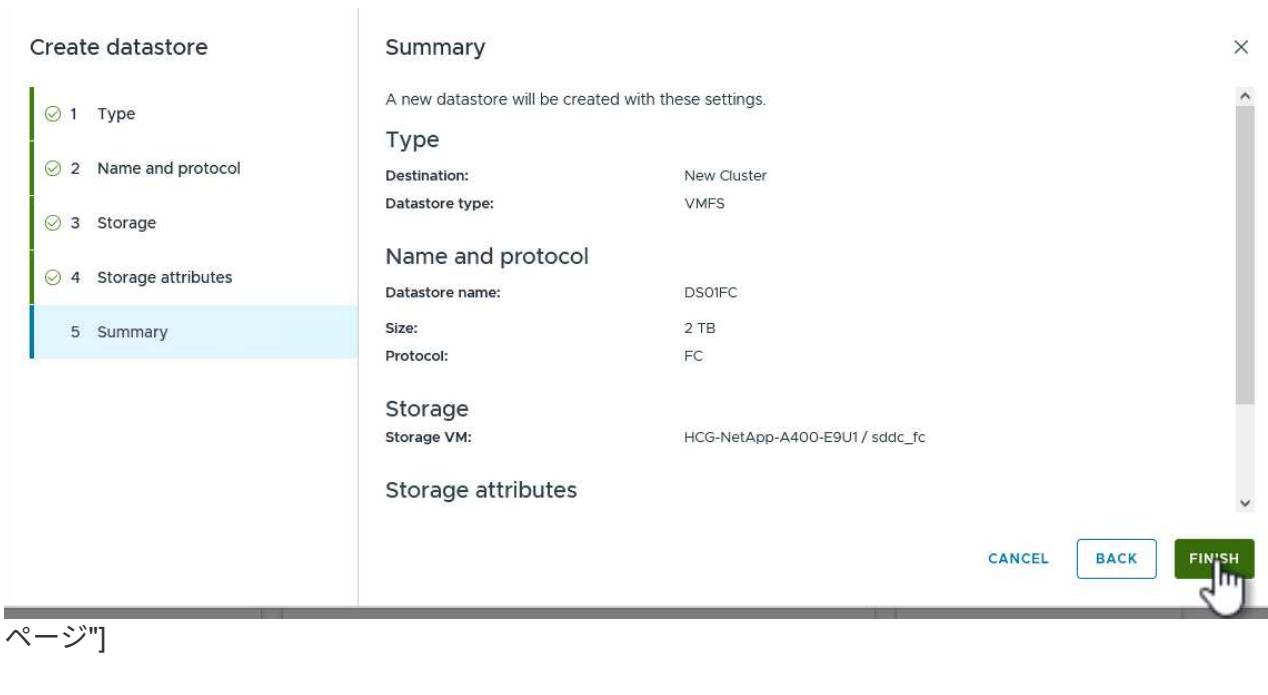
4. 名前とプロトコルページで、データストアの名前、サイズ、使用する FC プロトコルを入力します。



5. ストレージページで、ONTAPストレージ プラットフォームとストレージ仮想マシン (SVM) を選択します。ここで、利用可能なカスタム エクスポート ポリシーを選択することもできます。続行するには、[次へ] をクリックします。



6. *ストレージ属性*ページで、使用するストレージ アグリゲートを選択します。続行するには、[次へ] をクリックします。
7. *概要*ページで情報を確認し、*完了*をクリックしてプロビジョニング プロセスを開始します。ONTAPツールは、ONTAPストレージ システムにボリュームを作成し、それをクラスタ内のですべての ESXi ホストに FC データストアとしてマウントします。



vSphere 環境を VCF 5.2 に変換する

次のセクションでは、SDDC マネージャをデプロイし、vSphere 8 クラスタを VCF 5.2 管理ドメインに変換する手順について説明します。必要に応じて、詳細については VMware のドキュメントが参照されます。

VMware by Broadcom の VCF インポート ツールは、vCenter アプライアンスと SDDC マネージャの両方で

使用されるユーティリティで、構成を検証し、vSphere および VCF 環境の変換およびインポート サービスを提供します。

```
https://techdocs.broadcom.com/us/en/vmware-cis/vcf/vcf-5-2-and-earlier/5-2/map-for-administering-vcf-5-2/importing-existing-vsphere-environments-admin/vcf-import-tool-options-and-parameters-admin.html ["VCFインポートツールのオプションとパラメータ"] 。
```

VCFインポートツールのコピーと抽出

VCF インポート ツールは、vCenter アプライアンスで使用され、vSphere クラスタが VCF 変換またはインポート プロセスに対して正常な状態にあることを検証します。

次の手順を実行します。

1. 以下の手順に従ってください ["VCFインポートツールをターゲットのvCenterアプライアンスにコピーします"](#) VMware Docs を参照して、VCF インポート ツールを正しい場所にコピーします。
2. 次のコマンドを使用してバンドルを抽出します。

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

vCenterアプライアンスを検証する

変換前に、VCF インポート ツールを使用して vCenter アプライアンスを検証します。

1. 次の手順に従ってください ["変換前にターゲット vCenter で事前チェックを実行する"](#) 検証を実行します。
2. 次の出力は、vCenter アプライアンスが事前チェックに合格したことを示しています。

```
root@localhost [/tmp/vcfimport/vcf-brownfield-toolset]# python3 vcf_brownfield.py precheck --vcenter 172.21.166.57 --sso-user administrator@vsphere.local
[2024-10-23 19:03:23,609] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.0-24307788
Enter vCenter SSO password:
[2024-10-23 19:03:28,825] [INFO] vcf_brownfield: Starting VCF Brownfield precheck script version 1.0.0...
[2024-10-23 19:03:28,938] [INFO] vcf_precheck: Connected to vCenter 172.21.166.57 in 0.11 seconds
[2024-10-23 19:03:28,939] [INFO] vcf_precheck: Running pre-checks for vCenter 172.21.166.57...
[2024-10-23 19:03:28,939] [INFO] vcf_precheck: [1/10] VC BOM version check... PASS
[2024-10-23 19:03:28,975] [INFO] vcf_precheck: [2/10] vSAN stretched cluster check... PASS
[2024-10-23 19:03:28,999] [INFO] vcf_precheck: [3/10] Supported storage available check... PASS
[2024-10-23 19:03:29,020] [INFO] vcf_precheck: [4/10] vCenter VM location check... PASS
[2024-10-23 19:03:29,233] [INFO] vcf_precheck: [5/10] VxRail registration check... PASS
[2024-10-23 19:03:29,414] [INFO] vcf_precheck: [6/10] NSX-T registration check... PASS
[2024-10-23 19:03:29,437] [INFO] vcf_precheck: [7/10] Standalone host check... PASS
[2024-10-23 19:03:31,870] [INFO] vcf_precheck: [8/10] All cluster hosts connected to vDS check... PASS
[2024-10-23 19:03:32,962] [INFO] vcf_precheck: [9/10] ELM ring topology check... PASS
[2024-10-23 19:03:33,383] [INFO] vcf_precheck: [10/10] WCP import check... PASS
[2024-10-23 19:03:33,383] [INFO] vcf_precheck: All pre-checks passed!
[2024-10-23 19:03:33,383] [INFO] vcf_precheck: Pre-Checks for vCenter 172.21.166.57 completed in 4.44 seconds
root@localhost [/tmp/vcfimport/vcf-brownfield-toolset]#
```

SDDC マネージャーを展開する

SDDC マネージャーは、VCF 管理ドメインに変換される vSphere クラスター上に共存する必要があります。

展開を完了するには、VMware Docs の展開手順に従ってください。

参照 ["ターゲットvCenterにSDDC Managerアプライアンスを展開する"](#)。

詳細については、["委員会ホスト" VCF 管理ガイド](#)を参照してください。

NSX 展開用の JSON ファイルを作成する

vSphere 環境を VMware Cloud Foundation にインポートまたは変換しながら NSX Manager をデプロイするには、NSX デプロイ仕様を作成します。NSX の展開には少なくとも 3 台のホストが必要です。

詳細については、["既存の vSphere 環境を変換またはインポートするための NSX 展開仕様を生成する"](#)。



変換またはインポート操作で NSX Manager クラスタを展開する場合、NSX-VLAN ネットワークが利用されます。NSX-VLAN ネットワークの制限の詳細については、「既存の vSphere 環境を VMware Cloud Foundation に変換またはインポートする前の考慮事項」セクションを参照してください。NSX-VLAN ネットワークの制限については、以下を参照してください。["既存の vSphere 環境を VMware Cloud Foundation に変換またはインポートする前に考慮すべき事項"](#)。

以下は、NSX デプロイメント用の JSON ファイルの例です。

```
{  
    "license_key": "xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx",  
    "form_factor": "medium",  
    "admin_password": "*****",  
    "install_bundle_path": "/tmp/vcfimport/bundle-133764.zip",  
    "cluster_ip": "172.21.166.72",  
    "cluster_fqdn": "vcf-m02-nsx01.sddc.netapp.com",  
    "manager_specs": [  
        {  
            "fqdn": "vcf-m02-nsx01a.sddc.netapp.com",  
            "name": "vcf-m02-nsx01a",  
            "ip_address": "172.21.166.73",  
            "gateway": "172.21.166.1",  
            "subnet_mask": "255.255.255.0"  
        },  
        {  
            "fqdn": "vcf-m02-nsx01b.sddc.netapp.com",  
            "name": "vcf-m02-nsx01b",  
            "ip_address": "172.21.166.74",  
            "gateway": "172.21.166.1",  
            "subnet_mask": "255.255.255.0"  
        },  
        {  
            "fqdn": "vcf-m02-nsx01c.sddc.netapp.com",  
            "name": "vcf-m02-nsx01c",  
            "ip_address": "172.21.166.75",  
            "gateway": "172.21.166.1",  
            "subnet_mask": "255.255.255.0"  
        }]  
}
```

JSON ファイルを SDDC マネージャー上のディレクトリにコピーします。

SDDC マネージャーにソフトウェアをアップロードする

VCF インポート ツールと NSX デプロイメント バンドルを SDDC マネージャの /home/vcf/vcfimport ディレクトリにコピーします。

見る "[必要なソフトウェアを SDDC Manager アプライアンスにアップロードする](#)" 詳細な手順については、こちらをご覧ください。

vSphere クラスタを VCF 管理ドメインに変換する

変換プロセスを実行するには、VCF インポート ツールが使用されます。 /home/vcf/vcf-import-package/vcf-brownfield-import-<version>/vcf-brownfield-toolset ディレクトリから次のコマンドを実行して、VCF インポート ツール関数のプリントアウトを確認します。

```
python3 vcf_brownfield.py --help
```

次のコマンドを実行して、vSphere クラスタを VCF 管理ドメインに変換し、NSX クラスタをデプロイします。

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user '<sso-user>' --domain-name '<wld-domain-name>' --nsx-deployment-spec-path '<nsx-deployment-json-spec-path>'
```

詳しい手順については、 "[vSphere 環境を SDDC Manager インベントリに変換またはインポートする](#)"。

VCFにライセンスを追加する

変換が完了したら、環境にライセンスを追加する必要があります。

1. SDDC Manager UI にログインします。
2. ナビゲーションペインで 管理 > ライセンス に移動します。
3. + ライセンス キー をクリックします。
4. ドロップダウンメニューから製品を選択します。
5. ライセンスキーを入力してください。
6. ライセンスの説明を入力します。
7. *[追加]*をクリックします。
8. ライセンスごとにこれらの手順を繰り返します。

[ONTAP tools for VMware vSphere](#)のビデオ デモ

[ONTAP tools for VMware vSphere](#)を備えた NFS データストア

VCFにプリンシパルストレージをプロビジョニングする

ONTAPを主要ストレージソリューションとして**VCF**環境をプロビジョニングする

NetApp ONTAPストレージは、VMware Cloud Foundation (VCF) 管理および仮想インフラストラクチャ (VI) ワークロード ドメインに最適なプライマリストレージ ソリューションです。ONTAPは、高いパフォーマンス、拡張性、高度なデータ管理、シームレスな統合を実現し、運用効率とデータ保護を向上させます。

適切なドメインおよび適切なプロトコルで VCF 環境をプロビジョニングするための技術的な詳細については、次のソリューションを参照してください。

- "[FCによる管理ドメイン](#)"
- "[NFSを使用した管理ドメイン](#)"
- "[FC を使用した仮想インフラストラクチャ ワークロード ドメイン](#)"
- "[NFS を使用した仮想インフラストラクチャ ワークロード ドメイン](#)"

ONTAP上の**FC**ベースの**VMFS**データストアを**VCF**管理ドメインの主ストレージとして使用する

このユースケースでは、ONTAP上の既存の FC ベースの VMFS データストアを VMware Cloud Foundation (VCF) 管理ドメインのプライマリストレージとして使用する手順について説明します。この手順では、必要なコンポーネント、構成、および展開手順をまとめています。

はじめに

必要に応じて、VCF の SDDC マネージャーで実行する必要がある手順については外部ドキュメントを参照し、ストレージ構成部分に固有の手順を参照します。

既存のFCベースのvSphere環境をONTAPに変換する方法については、以下を参照してください。["vSphere 環境 \(FC データストア\) を VCF 管理ドメインに変換する"](#)。



VCF リリース 5.2 では、既存の vSphere 8 環境を VCF 管理ドメインに変換したり、VCF VI ワークロード ドメインとしてインポートしたりする機能が導入されました。このリリースより前は、VMware vSAN が VCF 管理ドメインの主要ストレージの唯一のオプションでした。



このソリューションは、NetApp ASA、AFF、FASなどの FC ストレージをサポートするONTAPプラットフォームに適用できます。

前提条件

このシナリオでは、次のコンポーネントと構成が使用されます。

- FC トラフィックを許可するように構成されたストレージ仮想マシン (SVM) を備えたNetAppストレージシステム。
- FC トラフィックを伝送し、SVM に関連付けられた FC ファブリック上に論理インターフェイス (LIF) が作成されています。
- ゾーニングは、ホスト HBA およびストレージ ターゲットの FC スイッチ上で単一のイニシエーター ターゲット ゾーニングを使用するように構成されています。

ONTAPストレージシステムの構成については、["ONTAP 9ドキュメント"](#)中心。

VCFの設定方法については、以下を参照してください。["VMware Cloud Foundation ドキュメント"](#)。

展開手順

管理ドメイン - デフォルトクラスタ

初期クラスター上の FC プリンシパル ストレージは、VCF ブラウンフィールド インポート ツールでのみサポートされます。 VCF が Cloud Builder ツール (リリース バージョン 5.2.x より前) を使用してデプロイされている場合は、vSAN のみがサポートされます。

既存のvSphere環境の使用に関する詳細については、["既存の vSphere 環境を管理ドメインに変換する"](#)詳細については。

管理ドメイン - 追加クラスター

管理ドメイン上の追加の vSphere クラスタは、次のオプションを使用して展開できます。

- vSphere 環境に追加のクラスターを用意し、VCF ブラウンフィールド インポート ツールを使用して vSphere 環境を管理ドメインに変換します。 ["ONTAP tools for VMware vSphere"](#) ["システムマネージャまたはONTAP API"](#) VMFS データストアを vSphere クラスタにデプロイするために使用できます。
- SDDC API を使用して追加のクラスターを展開します。 vSphere ホストには VMFS データストアが設定されている必要があります。 使用 ["システムマネージャまたはONTAP API"](#)LUN を vSphere ホストに展開します。
- SDDC Manager UI を使用して追加のクラスターを展開します。ただし、このオプションはバージョン 5.2.x までの VSAN データストアのみを作成します。

追加情報

ONTAPストレージシステムの構成については、["ONTAP 9ドキュメント"](#)中心。

VCFの設定方法については、以下を参照してください。["VMware Cloud Foundation ドキュメント"](#)。

ONTAP上のNFSデータストアをVCF管理ドメインの主ストレージとして使用する

このユースケースでは、ONTAP上の既存の NFS データストアを VMware Cloud Foundation (VCF) 管理ドメインのプライマリ ストレージとして使用する手順について説明します。この手順では、必要なコンポーネント、構成手順、および展開プロセスをま

とめています。

はじめに

必要に応じて、VCF の SDDC マネージャーで実行する必要がある手順については外部ドキュメントを参照し、ストレージ構成部分に固有の手順を参照します。

既存のNFSベースのvSphere環境をONTAPに変換する方法については、以下を参照してください。["vSphere 環境 \(NFS データストア\) を VCF 管理ドメインに変換する"](#)。

- i VCF リリース 5.2 では、既存の vSphere 8 環境を VCF 管理ドメインに変換したり、VCF VI ワークロード ドメインとしてインポートしたりする機能が導入されました。このリリースより前は、VMware vSAN が VCF 管理ドメインの主要ストレージの唯一のオプションでした。
- i このソリューションは、NetApp AFF や FAS などの NFS ストレージをサポートするONTAP プラットフォームに適用できます。

前提条件

このシナリオでは、次のコンポーネントと構成が使用されます。

- NFS トラフィックを許可するように構成されたストレージ仮想マシン (SVM) を備えたNetAppストレージシステム。
- NFS トラフィックを伝送し、SVM に関連付けられた IP ネットワーク上に論理インターフェイス (LIF) が作成されています。
- 4 台の ESXi ホストと、クラスター上に共存する vCenter アプライアンスを備えた vSphere 8 クラスター。
- この目的のために確立された VLAN またはネットワーク セグメント上の vMotion および NFS ストレージ トラフィック用に構成された分散ポート グループ。
- VCF 変換に必要なソフトウェアをダウンロードします。

ONTAPストレージシステムの構成については、["ONTAP 9ドキュメント"](#)中心。

VCFの設定方法については、以下を参照してください。["VMware Cloud Foundation ドキュメント"](#)。

展開手順

管理ドメイン - デフォルトクラスタ

初期クラスター上の NFS プリンシパル ストレージは、VCF ブラウンフィールド インポート ツールでのみサポートされます。VCF が Cloud Builder ツール (バージョン 5.2.x まで) を使用してデプロイされている場合、VSAN のみがサポートされます。

既存のvSphere環境の使用に関する詳細については、["既存の vSphere 環境を管理ドメインに変換する"](#)詳細について。

管理ドメイン - 追加クラスター

管理ドメイン上の追加の vSphere クラスターは、次のオプションを使用して展開できます。

- vSphere 環境に追加のクラスターを用意し、VCF ブラウンフィールド インポート ツールを使用して vSphere 環境を管理ドメインに変換します。 "[ONTAP tools for VMware vSphere](#)" "[システムマネージャまたはONTAP API](#)" NFS データストアを vSphere クラスタにデプロイするために使用できます。
- SDDC API を使用して追加のクラスターを展開します。 vSphere ホストには NFS データストアが設定されている必要があります。使用 "[システムマネージャまたはONTAP API](#)" LUN を vSphere ホストに展開します。
- SDDC Manager UI を使用して追加のクラスターを展開します。ただし、このオプションでは、リリース 5.2.x より前の vSAN データストアのみが作成されます。

追加情報

ONTAPストレージシステムの構成については、"[ONTAP 9ドキュメント](#)"中心。

VCFの設定方法については、以下を参照してください。"[VMware Cloud Foundation ドキュメント](#)"。

ONTAP上のFCベースのVMFSデータストアをVIワークロードドメインの主ストレージとして使用する

このユースケースでは、VMware Cloud Foundation (VCF) 仮想インフラストラクチャ (VI) ワークロード ドメインのプライマリストレージ ソリューションとして、ONTAP上にファイバーチャネル (FC) VMFS データストアをセットアップする手順について説明します。この手順では、必要なコンポーネント、構成手順、および展開プロセスをまとめています。

ファイバーチャネルの利点

高性能: FC は高速データ転送速度を提供するため、大量のデータへの高速かつ信頼性の高いアクセスを必要とするアプリケーションに最適です。

低レイテンシ: 非常に低いレイテンシ。これは、データベースや仮想化環境などのパフォーマンスが重視されるアプリケーションにとって非常に重要です。

信頼性: FC ネットワークは、冗長性やエラー訂正などの機能が組み込まれており、堅牢性と信頼性に優れています。

専用帯域幅: FC はストレージ トラフィックに専用の帯域幅を提供し、ネットワーク輻輳のリスクを軽減します。

NetAppストレージシステムでのファイバーチャネルの使用に関する詳細については、"[FCを使用したSANプロビジョニング](#)"。

シナリオの概要

このシナリオでは、次の大きな手順について説明します。

- FC トラフィック用の論理インターフェイス (LIF) を備えたストレージ仮想マシン (SVM) を作成します。
- 展開するホストの WWPN 情報を収集し、ONTAPストレージ システム上に対応するイニシエーター グループを作成します。
- ONTAPストレージ システムに FC ボリュームを作成します。

- ・イニシエーターグループをマップしてFCボリュームを作成する
- ・FCスイッチで単一のイニシエーター ターゲット ゾーニングを活用します。イニシエーターごとに1つのゾーンを作成します(単一イニシエーター ゾーン)。
 - 各ゾーンには、SVM のONTAP FC 論理インターフェイス (WWPN) であるターゲットを含めます。SVM ごとにノードごとに少なくとも2つの論理インターフェイスが必要です。物理ポートのWWPNを使用しないでください。
- ・SDDC Manager で vMotion トラフィック用のネットワーク プールを作成します。
- ・VI ワークロード ドメインで使用するためにVCF内のホストを委託します。
- ・FCデータストアをプリンシパル ストレージとして使用して、VCFにVI ワークロード ドメインを展開します。



このソリューションは、NetApp AFFやFASなどのNFSストレージをサポートするONTAPプラットフォームに適用できます。

前提条件

このシナリオでは、次のコンポーネントと構成が使用されます。

- ・FCスイッチに接続されたFCポートを備えたONTAP AFFまたはASAストレージシステム。
- ・FC lifsで作成されたSVM。
- ・FCスイッチに接続されたFC HBAを備えたvSphere。
- ・FCスイッチには単一のイニシエーター ターゲット ゾーニングが構成されています。



NetAppは、FC LUNにマルチパスを推奨しています。

展開手順

管理ドメイン - デフォルトクラスタ

初期クラスター上のFCプリンシパルストレージは、VCF ブラウンフィールドインポートツールでのみサポートされます。VCFがcloudbuilderツール(バージョン5.2.xまで)を使用して展開されている場合、VSANのみがサポートされます。参照する "[既存のvSphere環境を管理ドメインに変換する](#)" 詳細については。

管理ドメイン - 追加クラスター

管理ドメイン上の追加のvSphereクラスタは、次のオプションを使用して展開できます。^{*} vSphere環境に追加のクラスタを用意し、VCFブラウンフィールドインポートツールを使用してvSphere環境を管理ドメインに変換します。["ONTAP tools for VMware vSphere"](#)、["システムマネージャまたはONTAP API"](#) VMFSデータストアをvSphereクラスタにデプロイするために使用できます。^{*} SDDC APIを使用して追加のクラスターを展開します。vSphereホストにはVMFSデータストアが設定されている必要があります。使用["システムマネージャまたはONTAP API"](#)LUNをvSphereホストに展開します。^{*} SDDC Manager UIを使用して追加のクラスターを展開します。ただし、このオプションはバージョン5.2.xまでのVSANデータストアのみを作成します。

VI ワークロード ドメイン - デフォルトクラスタ

管理ドメインが起動したら、VI ワークロード ドメインを作成できます。

- SDDC マネージャー UI を使用します。vSphere ホストには VMFS データストアが設定されている必要があります。System Manager またはONTAP API を使用して、LUN を vSphere ホストに展開します。
- 既存の vSphere 環境を新しい VI ワークロード ドメインとしてインポートします。ONTAP tools for VMware vSphere、System Manager、またはONTAP API を使用して、VMFS データストアを vSphere クラスターに展開できます。

VI ワークロード ドメイン - 追加クラスター

VI ワークロードが起動して実行されると、次のオプションを使用して、FC LUN 上の VMFS を使用して追加のクラスターを展開できます。

- VCF ブラウンフィールド インポート ツールを使用してインポートされた vSphere 環境内の追加クラスター。ONTAP tools for VMware vSphere、System Manager、またはONTAP API を使用して、VMFS データストアを vSphere クラスターに展開できます。
- SDDC Manager UI または API を使用して追加のクラスターをデプロイします。vSphere ホストには VMFS データストアが設定されている必要があります。System Manager またはONTAP API を使用して、LUN を vSphere ホストに展開します。

追加情報

ONTAPストレージシステムの構成については、["ONTAP 9 ドキュメント"](#)中心。

VCFの設定方法については、以下を参照してください。["VMware Cloud Foundation ドキュメント"](#)。

ONTAP上の NFS データストアを VI ワークロード ドメインの主ストレージとして使用する

このユースケースでは、VMware Cloud Foundation (VCF) 仮想インフラストラクチャ (VI) ワークロード ドメインのプライマリ ストレージ ソリューションとしてONTAP上の NFS データストアを構成する手順について説明します。この手順では、必要なコンポーネント、構成手順、および展開プロセスをまとめています。

NFSの利点

シンプルさと使いやすさ: NFS はセットアップと管理が簡単なので、迅速かつ簡単なファイル共有を必要とする環境に最適です。

スケーラビリティ: ONTAP のアーキテクチャにより、NFS は効率的に拡張でき、インフラストラクチャに大きな変更を加えることなく増大するデータニーズに対応できます。

柔軟性: NFS は幅広いアプリケーションとワークロードをサポートしており、仮想化環境を含むさまざまなユースケースに幅広く対応できます。

詳細については、『vSphere 8 の NFS v3 リファレンス ガイド』を参照してください。

NetAppストレージシステムでのファイバーチャネルの使用に関する詳細については、["vSphere 8 向け NFS v3 リファレンス ガイド"](#)。

シナリオの概要

このシナリオでは、次の大まかな手順について説明します。

- NFS トライック用の論理インターフェース (LIF) を備えたストレージ仮想マシン (SVM) を作成する
- ONTAPストレージ仮想マシン (SVM) のネットワークを確認し、NFS トライックを伝送するための論理インターフェイス (LIF) が存在することを確認します。
- ESXi ホストが NFS ボリュームにアクセスできるようにするエクスポート ポリシーを作成します。
- ONTAPストレージ システムに NFS ボリュームを作成します。
- SDDC Manager で NFS および vMotion トライック用のネットワーク プールを作成します。
- VI ワークロード ドメインで使用するために VCF 内のホストを委託します。
- NFS データストアをプリンシパル ストレージとして使用して、VCF に VI ワークロード ドメインを展開します。
- VMware VAAI用のNetApp NFSプラグインをインストールする



このソリューションは、NetApp AFFやFASなどの NFS ストレージをサポートするONTAPプラットフォームに適用できます。

前提条件

このシナリオでは、次のコンポーネントと構成が使用されます。

- NFS トライックを許可するように構成されたストレージ仮想マシン (SVM) を備えたNetApp AFFストレージ システム。
- NFS トライックを伝送し、SVM に関連付けられた IP ネットワーク上に論理インターフェイス (LIF) が作成されています。
- VCF 管理ドメインの展開が完了し、SDDC マネージャー インターフェイスにアクセスできるようになりました。
- VCF 管理ネットワーク上で通信用に構成された 4 台の ESXi ホスト。
- この目的のために確立された VLAN またはネットワーク セグメント上の vMotion および NFS ストレージ トライック用に予約された IP アドレス。

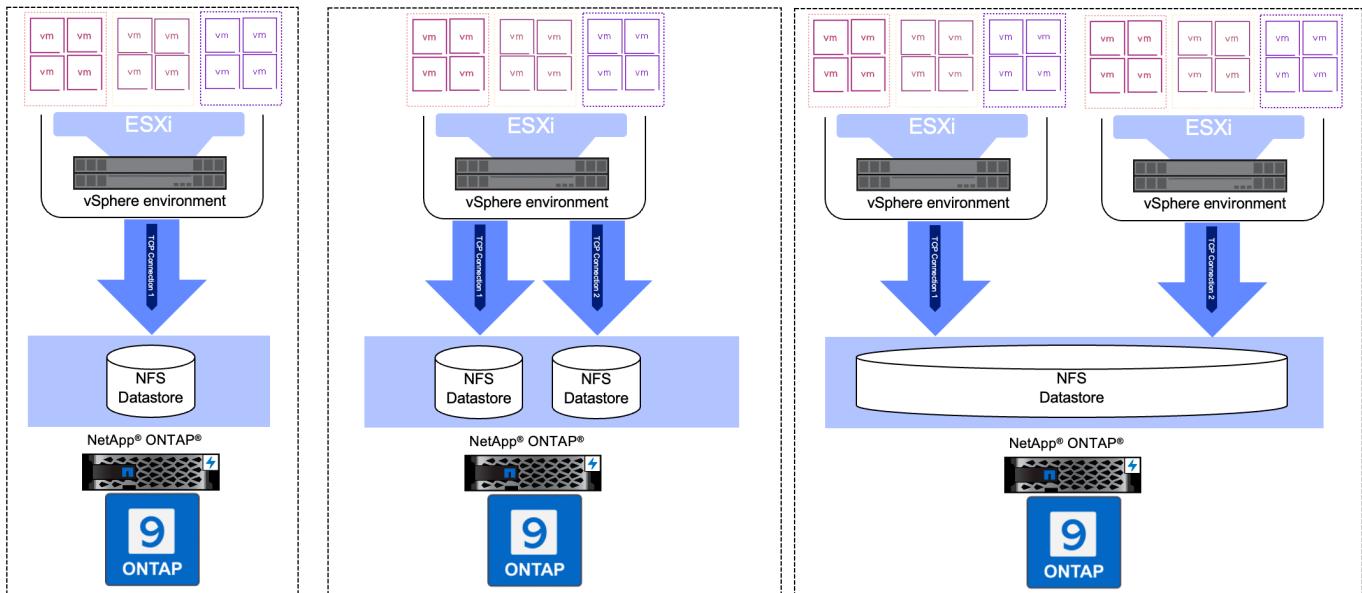


VI ワークロード ドメインを展開する場合、VCF は NFS サーバーへの接続を検証します。これは、NFS IP アドレスを使用して追加の vmkernel アダプタが追加される前に、ESXi ホスト上の管理アダプタを使用して実行されます。したがって、検証を続行できるようにするには、1) 管理ネットワークが NFS サーバーにルーティング可能であること、または 2) 管理ネットワークの LIF が NFS データストア ボリュームをホストしている SVM に追加されていることを確認する必要があります。

ONTAPストレージシステムの構成については、["ONTAP 9ドキュメント"](#)中心。

VCFの設定方法については、以下を参照してください。["VMware Cloud Foundation ドキュメント"](#)。

vSphereクラスタでNFSを使用する方法の詳細については、["vSphere 8 向け NFS v3 リファレンス ガイド"](#)。



展開手順

NFS データストアをプリンシパル ストレージとして VI ワークロード ドメインを展開するには、次の手順を実行します。

ONTAP SVMのネットワークを確認する

ONTAPストレージクラスタとVIワークロードドメイン間のNFSトラフィックを伝送するネットワークに必要な論理インターフェイスが確立されていることを確認します。

1. ONTAP System Manager から、左側のメニューの **Storage VMs** に移動し、NFS トラフィックに使用する SVM をクリックします。概要タブのネットワーク IP インターフェイス の下で、**NFS** の右側にある数字をクリックします。リストに必要な LIF IP アドレスがリストされていることを確認します。

The screenshot shows the ONTAP System Manager interface. On the left, the navigation menu is open, showing options like DASHBOARD, INSIGHTS, STORAGE, NETWORK, and EVENTS & JOBS. Under STORAGE, the 'Storage VMs' option is selected. In the main content area, the 'Storage VMs' page is displayed with a list of SVMs. One SVM, 'EHC_NFS', is selected and highlighted with a blue border. To the right of the SVM list, the 'NETWORK IP INTERFACES' section is visible, specifically the 'NFS' tab. This tab lists several IP addresses: 172.21.253.117, 172.21.253.118, 172.21.253.116, 172.21.253.112, 172.21.253.113, 172.21.118.163, and 172.21.118.164. The IP address '172.21.118.163' is also highlighted with a red box.

または、次のコマンドを使用して、ONTAP CLI から SVM に関連付けられている LIF を確認します。

```
network interface show -vserver <SVM_NAME>
```

1. ESXi ホストがONTAP NFS サーバと通信できることを確認します。SSH 経由で ESXi ホストにログインし、SVM LIF に ping を実行します。

```
vmkping <IP Address>
```



VI ワークロード ドメインを展開する場合、VCF は NFS サーバーへの接続を検証します。これは、NFS IP アドレスを使用して追加の vmkernel アダプタが追加される前に、ESXi ホスト上の管理アダプタを使用して実行されます。したがって、検証を続行できるようにするには、1) 管理ネットワークが NFS サーバーにルーティング可能であること、または 2) 管理ネットワークの LIF が NFS データストア ボリュームをホストしている SVM に追加されていることを確認する必要があります。

NFSボリュームを共有するためのエクスポートポリシーを作成する

ONTAP System Manager でエクスポート ポリシーを作成し、NFS ボリュームのアクセス制御を定義します。

1. ONTAP System Manager で、左側のメニューの **Storage VMs** をクリックし、リストから SVM を選択します。
2. *設定*タブで*エクスポート ポリシー*を見つけて、矢印をクリックしてアクセスします。

The screenshot shows the ONTAP System Manager interface. The left sidebar has a 'Storage VMs' section selected. The main area displays a list of Storage VMs with 'EHC_NFS' selected. A modal window titled 'Export Policies' is open over the list, showing a list of policies including 'default', '41 Rules', 'JetStream_NFS_v02', and 'JetStream_NFS_v03'. A hand cursor is hovering over the 'Add Rule' button in the bottom right corner of the modal.

3. 新しいエクスポート ポリシー ウィンドウでポリシーの名前を追加し、新しいルールの追加 ボタンをクリックし、+ 追加 ボタンをクリックして新しいルールの追加を開始します。

New export policy

NAME

WKLD_DM01

Copy rules from existing policy

STORAGE VM

svm0

EXPORT POLICY

default

RULES

No data

+ Add



Add New Rules

Save

Cancel

4. ルールに含める IP アドレス、IP アドレス範囲、またはネットワークを入力します。 **SMB/Cifs** および * FlexCache* ボックスのチェックを外し、以下のアクセス詳細を選択します。 ESXi ホストにアクセスするには、UNIX ボックスを選択するだけで十分です。

New Rule



CLIENT SPECIFICATION

172.21.166.0/24

ACCESS PROTOCOLS

- SMB/CIFS
- FlexCache
- NFS
- NFSv3
- NFSv4

ACCESS DETAILS

Type	Read-only Access	Read/Write Access	Superuser Access
All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All (As anonymous user) (i)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5p	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NTLM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel

Save



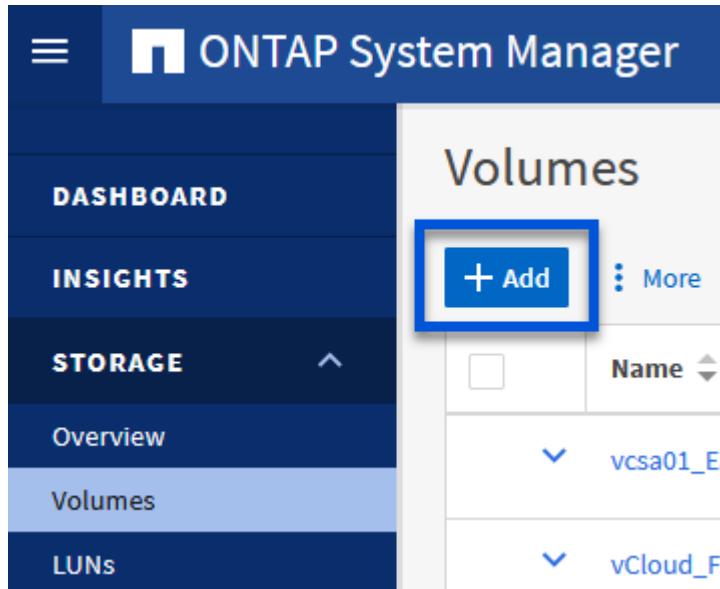
VI ワークロード ドメインを展開する場合、VCF は NFS サーバーへの接続を検証します。これは、NFS IP アドレスを使用して追加の vmkernel アダプタが追加される前に、ESXi ホスト上の管理アダプタを使用して実行されます。したがって、検証を続行するには、エクスポート ポリシーに VCF 管理ネットワークが含まれていることを確認する必要があります。

5. すべてのルールを入力したら、[保存] ボタンをクリックして新しいエクスポート ポリシーを保存します。
6. あるいは、ONTAP CLI でエクスポート ポリシーとルールを作成することもできます。ONTAP ドキュメントでエクスポート ポリシーを作成し、ルールを追加する手順を参照してください。
 - ONTAP CLIを使用して["エクスポート ポリシーの作成"](#)。
 - ONTAP CLIを使用して["エクスポート ポリシーへのルールの追加"](#)。

NFSボリュームを作成する

ワークロード ドメインのデプロイメントでデータストアとして使用する NFS ボリュームをONTAPストレージシステム上に作成します。

1. ONTAP System Manager から、左側のメニューの **Storage > Volumes** に移動し、**+Add** をクリックして新しいボリュームを作成します。



2. ボリュームの名前を追加し、必要な容量を入力して、ボリュームをホストするストレージ VM を選択します。続行するには、[その他のオプション] をクリックします。

Add Volume

X

NAME

CAPACITY



STORAGE VM



Export via NFS

[More Options](#)

[Cancel](#)

[Save](#)

- [アクセス許可] で、NFS サーバーと NFS トラフィックの両方の検証に使用される VCF 管理ネットワークまたは IP アドレスと NFS ネットワーク IP アドレスを含むエクスポート ポリシーを選択します。

Access Permissions

Export via NFS

GRANT ACCESS TO HOST

default



JetStream_NFS_v04

Clients : 0.0.0.0/0 | Access protocols : Any

NFSmountTest01

3 rules

NFSmountTestReno01

Clients : 0.0.0.0/0 | Access protocols : Any

PerfTestVols

Clients : 172.21.253.0/24 | Access protocols : NFSv3, NFSv4, NFS

TestEnv_VPN

Clients : 172.21.254.0/24 | Access protocols : Any

VCF_WKLD

2 rules

WKLD_DM01

2 rules

Wkld01_NFS

Clients : 172.21.252.205, 172.21.252.206, 172.21.252.207, 172.21.2

+



VI ワークロード ドメインを展開する場合、VCF は NFS サーバーへの接続を検証します。これは、NFS IP アドレスを使用して追加の vmkernel アダプタが追加される前に、ESXi ホスト上の管理アダプタを使用して実行されます。したがって、検証を続行できるようにするには、1) 管理ネットワークが NFS サーバーにルーティング可能であること、または 2) 管理ネットワークの LIF が NFS データストア ボリュームをホストしている SVM に追加されていることを確認する必要があります。

- あるいは、ONTAPボリュームはONTAP CLIで作成することもできます。詳細については、"lun create" ONTAPコマンドのドキュメントのコマンド。

SDDC マネージャーでネットワーク プールを作成する

ESXi ホストを VI ワークロード ドメインに展開するための準備として、ESXi ホストをコミッショニングする前に、SDDC マネージャでネットワーク プールを作成する必要があります。ネットワーク プールには、NFS サーバーとの通信に使用される VMkernel アダプタのネットワーク情報と IP アドレス範囲が含まれている必要があります。

1. SDDC Manager Web インターフェースから、左側のメニューの ネットワーク設定 に移動し、+ ネットワーク プールの作成 ボタンをクリックします。

The screenshot shows the 'Network Settings' page in the SDDC Manager. The left sidebar includes 'Dashboard', 'Solutions', 'Inventory' (selected), 'Workload Domains', 'Hosts', 'Lifecycle Management', and 'Administration'. The main area is titled 'Network Settings' with tabs for 'Network Pool' (selected), 'DNS Configuration', and 'NTP Configuration'. Below the tabs, there's a link 'View Network Pool details' and a prominent blue button labeled '+ CREATE NETWORK POOL' with a white hand cursor icon pointing at it. A table below the button has one visible row with the 'Network Pool Name' field containing 'vcf-m01-rp01'.

2. ネットワーク プールの名前を入力し、NFS のチェック ボックスをオンにして、すべてのネットワークの詳細を入力します。vMotion ネットワーク情報についてもこれを繰り返します。

The screenshot shows the 'Network Settings' section of the VMware Cloud Foundation interface. On the left, a sidebar lists various management categories like Dashboard, Solutions, Inventory, Workload Domains, Hosts, Lifecycle Management, Administration, and more. The 'Network Settings' category is currently selected. The main area is titled 'Create Network Pool' and displays configuration options for an 'NFS_NP01' pool. It includes tabs for 'Network Pool', 'DNS Configuration', and 'NTP Configuration'. Under 'Network Pool', the 'Network Type' is set to 'NFS' (selected) and 'vMotion' (selected). The 'NFS Network Information' section contains fields for VLAN ID (3974), MTU (9000), Network (172.21.18.0), Subnet Mask (255.255.255.0), and Default Gateway (172.21.18.1). The 'vMotion Network Information' section has similar fields with values 3423, 9000, 172.21.167.0, 255.255.255.0, and 172.21.167.1. Below these sections, there are 'Included IP Address Ranges' tables for both pools, each containing one range (172.21.18.145 to 172.21.18.148 for NFS, and 172.21.167.121 to 172.21.167.124 for vMotion). At the bottom are 'CANCEL' and 'SAVE' buttons.

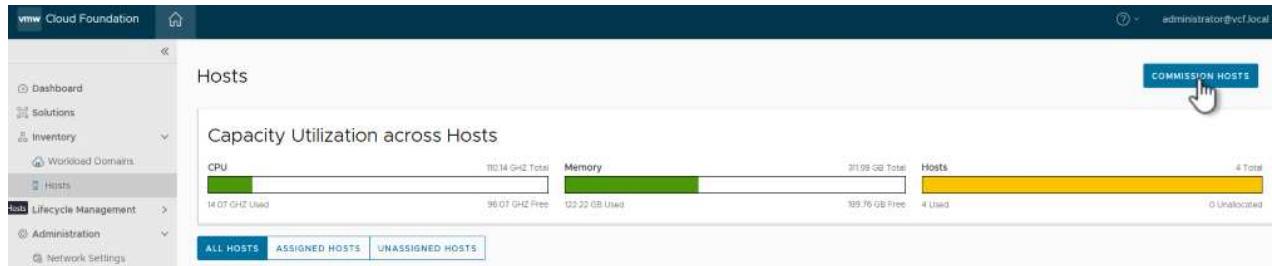
3. 保存ボタンをクリックして、ネットワーク プールの作成を完了します。

委員会ホスト

ESXi ホストをワークロード ドメインとして展開する前に、SDDC Manager インベントリに追加する必要があります。これには、必要な情報の提供、検証の通過、および試運転プロセスの開始が含まれます。

詳細については、["委員会ホスト" VCF 管理ガイド](#)を参照してください。

1. SDDC マネージャー インターフェースから、左側のメニューの ホスト に移動し、ホストのコミッション ボタンをクリックします。



2. 最初のページは前提条件のチェックリストです。すべての前提条件を再確認し、すべてのチェックボックスを選択して続行します。

Checklist

Commissioning a host adds it to the VMware Cloud Foundation inventory. The host you want to commission must meet the checklist criterion below.



Select All

- Host for vSAN/vSAN ESA workload domain should be vSAN/vSAN ESA compliant and certified per the VMware Hardware Compatibility Guide. BIOS, HBA, SSD, HDD, etc. must match the VMware Hardware Compatibility Guide.
- Host has a standard switch with two NIC ports with a minimum 10 Gbps speed.
- Host has the drivers and firmware versions specified in the VMware Compatibility Guide.
- Host has ESXi installed on it. The host must be preinstalled with supported versions (8.0.2-22380479)
- Host is configured with DNS server for forward and reverse lookup and FQDN.
- Hostname should be same as the FQDN.
- Management IP is configured to first NIC port.
- Ensure that the host has a standard switch and the default uplinks with 10Gb speed are configured starting with traditional numbering (e.g., vmnic0) and increasing sequentially.
- Host hardware health status is healthy without any errors.
- All disk partitions on HDD / SSD are deleted.
- Ensure required network pool is created and available before host commissioning.
- Ensure hosts to be used for VSAN workload domain are associated with VSAN enabled network pool.
- Ensure hosts to be used for NFS workload domain are associated with NFS enabled network pool.
- Ensure hosts to be used for VMFS on FC workload domain are associated with NFS or VMOTION only enabled network pool.
- Ensure hosts to be used for vVol FC workload domain are associated with NFS or VMOTION only enabled network pool.
- Ensure hosts to be used for vVol NFS workload domain are associated with NFS and VMOTION only enabled network pool.
- Ensure hosts to be used for vVol iSCSI workload domain are associated with iSCSI and VMOTION only enabled network pool.
- For hosts with a DPU device, enable SR-IOV in the BIOS and in the vSphere Client (if required by your DPU vendor).

CANCEL

PROCEED



3. ホストの追加と検証 ウィンドウで、ホスト **FQDN**、ストレージタイプ、ワークロード ドメインに使用する vMotion および NFS ストレージ IP アドレスを含む ネットワーク プール名、および ESXi ホストにアクセスするための資格情報を入力します。追加 をクリックして、検証するホストのグループにホストを追加します。

Commission Hosts

1 Host Addition and Validation

2 Review

Host Addition and Validation

Add Hosts

You can either choose to add host one at a time or download [JSON](#) template and perform bulk commission.

Add new Import

Host FQDN: vcf-wkld-esx02.sddc.netapp.com

Storage Type: vSAN NFS VMFS on FC vVol

Network Pool Name: NFS_NP01

User Name: root

Password: [REDACTED]

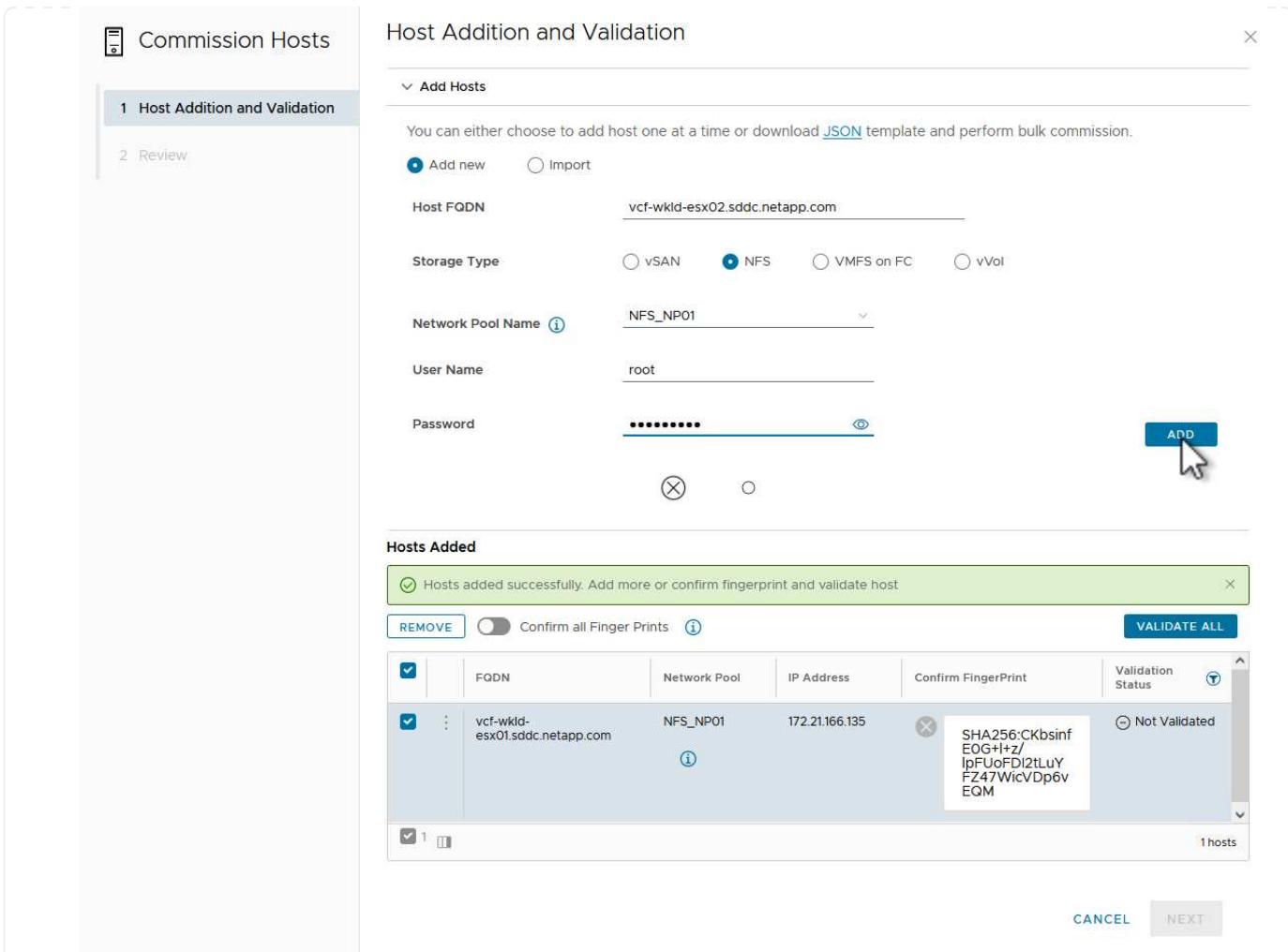
ADD

Hosts Added

Hosts added successfully. Add more or confirm fingerprint and validate host

<input checked="" type="checkbox"/>	FQDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
<input checked="" type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01	172.21.166.135	<input type="button" value="X"/> SHA256:CKbsinfEOG+Hz/lpFUoFDl2tLuYFZ47WicVDp6vEQM	<input checked="" type="radio"/> Not Validated

CANCEL NEXT



4. 検証するすべてのホストを追加したら、[すべて検証] ボタンをクリックして続行します。
5. すべてのホストが検証されたと仮定して、[次へ] をクリックして続行します。

Hosts Added

Host Validated Successfully.

[REMOVE](#)

Confirm all Finger Prints

[VALIDATE ALL](#)

<input checked="" type="checkbox"/>	FQDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
<input checked="" type="checkbox"/>	vcf-wkld-esx04.sddc.netapp.com	NFS_NP01	172.21.166.138	SHA256:9Kg+9nQaE4SQkOMsQPON/k5gZB9zyKN+6CBPmXsvLBc	Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx03.sddc.netapp.com	NFS_NP01	172.21.166.137	SHA256:nPX4/mei/2zmLJHfmPwbk6zhapoUxV2lOwZDPFHz+zo	Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx02.sddc.netapp.com	NFS_NP01	172.21.166.136	SHA256:AMhyR60OpTQ1YYq0DjhqVbj/M/GvrQaqUy7Ce+M4IWY	Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01	172.21.166.135	SHA256:CKbsinfEOG+l+z/lpFUoFDI2tLuYFZ47WicVDp6vEQM	Valid

[CANCEL](#)

[NEXT](#)



6. 委託するホストのリストを確認し、「委託」ボタンをクリックしてプロセスを開始します。 SDDC マネージャーのタスク ペインからコミッショニング プロセスを監視します。

Commission Hosts

1 Host Addition and Validation

2 Review

Review

Skip failed hosts during commissioning On

▼ Validated Host(s)

vcf-wkld-esx04.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.138 Storage Type: NFS
vcf-wkld-esx03.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.137 Storage Type: NFS
vcf-wkld-esx02.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.136 Storage Type: NFS
vcf-wkld-esx01.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.135 Storage Type: NFS

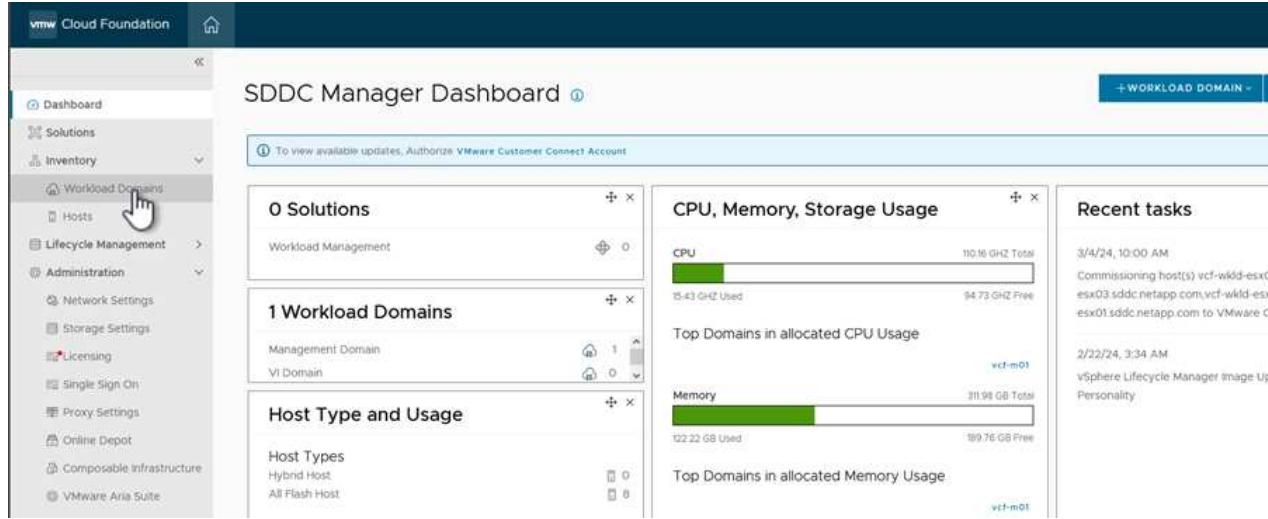
CANCEL BACK COMMISSION 

VIワークロードドメインのデプロイ

VI ワークロード ドメインの展開は、VCF Cloud Manager インターフェイスを使用して行われます。ここでは、ストレージ構成に関する手順のみを説明します。

VIワークロードドメインの展開手順については、以下を参照してください。["SDDC Manager UI を使用して VI ワークロード ドメインを展開する"](#)。

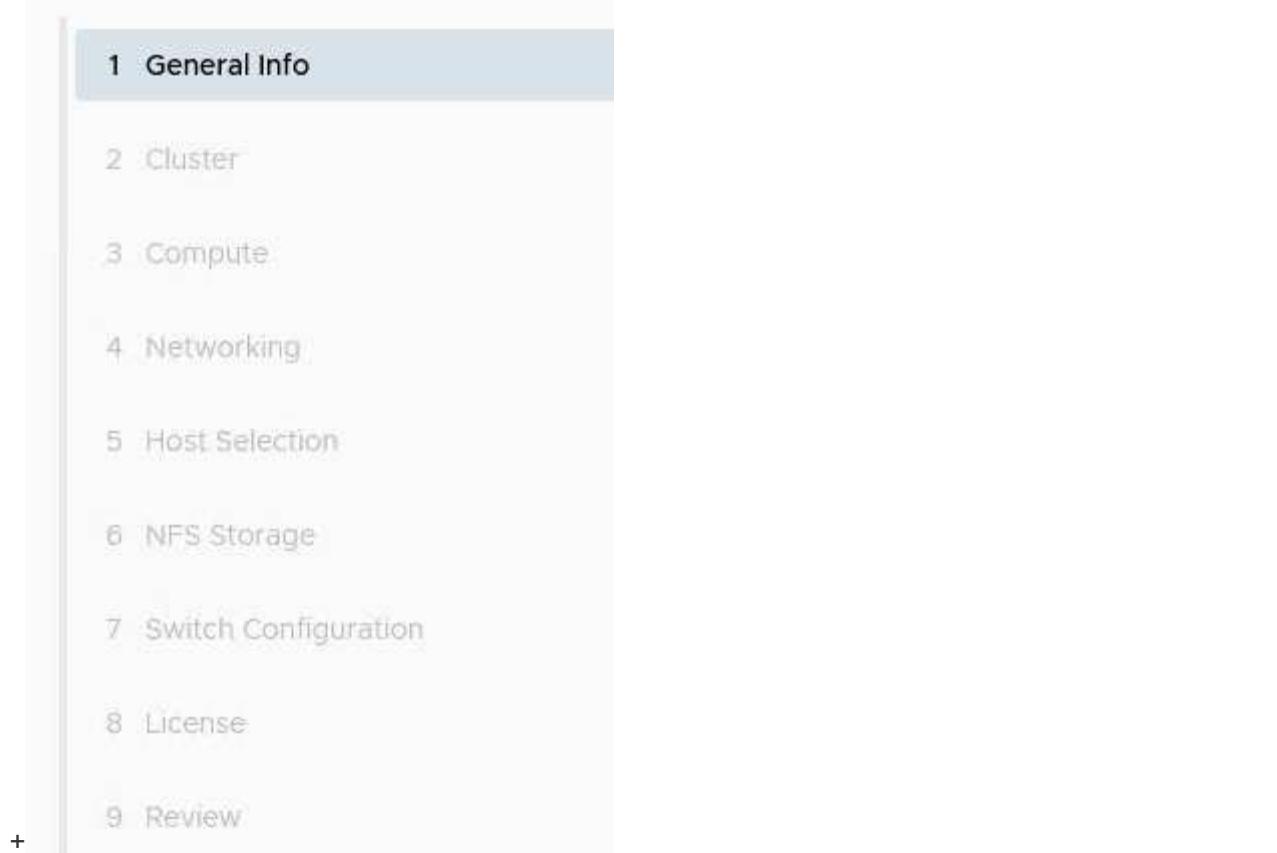
1. SDDC Manager ダッシュボードから、右上隅の + ワークロード ドメインをクリックして、新しいワークロード ドメインを作成します。



2. VI 構成ウィザードで、必要に応じて一般情報、クラスター、コンピューティング、ネットワーク、および ホスト選択 のセクションに入力します。

VI構成ウィザードに必要な情報を入力する方法については、以下を参照してください。["SDDC Manager UI を使用して VI ワークロード ドメインを展開する"](#)。

VI Configuration



1. NFS ストレージ セクションで、データストア名、NFS ボリュームのフォルダー マウント ポイント、およびONTAP NFS ストレージ VM LIF の IP アドレスを入力します。

The screenshot shows the 'VI Configuration' wizard with the '6 NFS Storage' step selected. On the right, the 'NFS Storage' configuration screen is shown with the following values:

NFS Share Details	
Datastore Name	VCF_WKLD_01
Folder	/VCF_WKLD_01
NFS Server IP Address	172.21.118.163

2. VI 構成ウィザードでスイッチ構成とライセンスの手順を完了し、[完了] をクリックしてワークロード ドメインの作成プロセスを開始します。

3. プロセスを監視し、プロセス中に発生する検証の問題を解決します。

VMware VAAI用のNetApp NFSプラグインをインストールする

NetApp NFS Plug-in for VMware VAAI は、ESXi ホストにインストールされた VMware 仮想ディスク ライブラリを統合し、より高速に完了する、より高性能なクローン作成操作を提供します。これは、VMware vSphere でONTAPストレージ システムを使用する場合に推奨される手順です。

VMware VAAI用のNetApp NFSプラグインを導入するための手順については、次のURLを参照してください。["VMware VAAI用のNetApp NFSプラグインをインストールする"](#)。

このソリューションのビデオデモ

[VCF ワークロード ドメインの主要ストレージとしての NFS データストア](#)

追加情報

ONTAPストレージシステムの構成については、["ONTAP 9ドキュメント"](#)を中心。

VCFの設定方法については、以下を参照してください。["VMware Cloud Foundation ドキュメント"](#)。

補助ストレージでVCFを拡張

補助ストレージを使用して VCF 環境のストレージを拡張する方法について説明します。

VMware Cloud Foundation (VCF) は、VCF 管理ドメインと仮想インフラストラクチャ (VI) ワークロード ドメインのストレージを拡張するための幅広い補足ストレージ オプションをサポートしています。

NetApp のONTAP Tools for VMware vSphere は、NetAppストレージを VCF 環境にシームレスに統合することで、この拡張のための効率的なソリューションを提供します。ONTAPツールはデータストアのセットアップと管理を簡素化し、管理者が vSphere Client から直接ストレージをプロビジョニングおよび管理できるようになります。スナップショット、クローニング、データ保護などのONTAPの高度な機能により、VCF 環境内のストレージ パフォーマンス、効率、スケーラビリティが向上します。

VCF 環境を拡張するための技術的な詳細については、次のソリューションを参照してください。

- "[iSCSIによる管理ドメイン](#)"
- "[FCによる管理ドメイン](#)"
- "[vVolsを使用した仮想インフラストラクチャ ワークロード ドメイン \(iSCSI\)](#)"
- "[vVolsを使用した仮想インフラストラクチャ ワークロード ドメイン \(NFS\)](#)"
- "[NVMe/TCPを使用した仮想インフラストラクチャ ワークロード ドメイン](#)"
- "[FCを使用した仮想インフラストラクチャ ワークロード ドメイン](#)"

ONTAP tools for VMware vSphereを使用して、管理ドメインの補助ストレージとして iSCSI データストアを追加します。

このユースケースでは、VMware Cloud Foundation (VCF) 管理ドメインの補助ストレージとして iSCSI データストアを追加する手順について説明します。この手順では、iSCSI 用の論理インターフェイス (LIF) を使用したストレージ仮想マシン (SVM) のセットアップ、ESXi ホストでの iSCSI ネットワークの構成、VMware vSphere 用のONTAPツールの導入、および VMFS データストアの作成についてまとめています。

iSCSIの利点

高性能: 高速で効率的なデータ転送速度と低遅延を実現する高性能を提供します。要求の厳しいエンタープライズ アプリケーションや仮想化環境に最適です。

管理の容易さ: 使い慣れた IP ベースのツールとプロトコルを使用して、ストレージ管理を簡素化します。

コスト効率が高い: 既存のイーサネット インフラストラクチャを活用することで、特殊なハードウェアの必要性が減り、組織は信頼性が高くスケーラブルなストレージ ソリューションを実現できます。

NetAppストレージシステムでiSCSIを使用する方法の詳細については、以下を参照してください。 "[iSCSIによる SAN プロビジョニング](#)"。

シナリオの概要

このシナリオでは、次の大まかな手順について説明します。

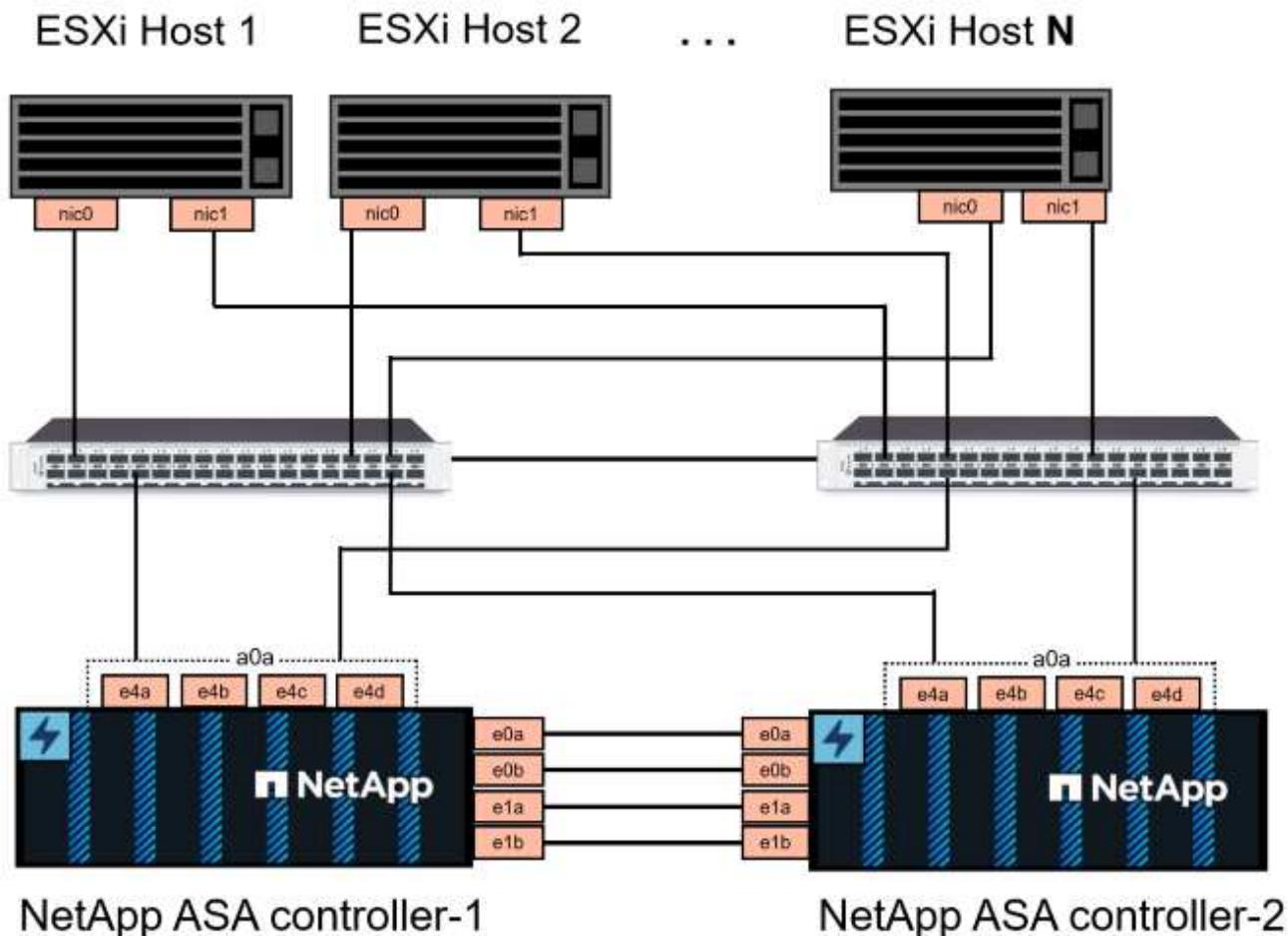
- iSCSI トラフィック用の論理インターフェイス (LIF) を備えたストレージ仮想マシン (SVM) を作成します。
- VCF 管理ドメイン上の iSCSI ネットワークの分散ポート グループを作成します。
- VCF 管理ドメインの ESXi ホスト上に iSCSI 用の vmkernel アダプタを作成します。
- VCF 管理ドメインにONTAPツールを導入します。
- VCF 管理ドメインに新しい VMFS データストアを作成します。

前提条件

このシナリオには、次のコンポーネントと構成が必要です。

- ストレージ トラフィック専用のイーサネット スイッチ上に物理データ ポートを備えたONTAP AFF またはASAストレージ システム。
- VCF 管理ドメインの展開が完了し、vSphere クライアントにアクセスできるようになりました。

NetApp は、iSCSI に対して完全に冗長化されたネットワーク設計を推奨しています。次の図は、ストレージ システム、スイッチ、ネットワーク アダプタ、およびホスト システムにフォールト トレランスを提供する冗長構成の例を示しています。 NetAppを参照してください "[SAN構成に関するリファレンス](#)" 追加情報については、こちらをご覧ください。



複数のパスにわたるマルチパスとフェイルオーバーのために、NetApp、iSCSI構成のすべてのSVMに対して、個別のイーサネットネットワーク内のストレージノードごとに少なくとも2つのLIFを用意することを推奨しています。

このドキュメントでは、新しいSVMを作成し、IPアドレス情報を指定してiSCSIトラフィック用の複数のLIFを作成するプロセスについて説明します。既存のSVMに新しいLIFを追加するには、["LIF（ネットワークインターフェイス）の作成"](#)。

VMwareでVMFS iSCSIデータストアを使用する方法の詳細については、以下を参照してください。["vSphere VMFS データストア - ONTAPを使用したiSCSIストレージバックエンド"](#)。



複数のVMkernelアダプタが同じIPネットワーク上に構成されている場合は、アダプタ間で負荷分散が行われるように、ESXiホストでソフトウェアiSCSIポートバイディングを使用することをお勧めします。KB記事を参照してください["ESX/ESXiでソフトウェアiSCSIポートバイディングを使用する際の考慮事項\(2038869\)"](#)。

展開手順

ONTAPツールを導入し、それを使用してVCF管理ドメインにVMFSデータストアを作成するには、次の手順を実行します。

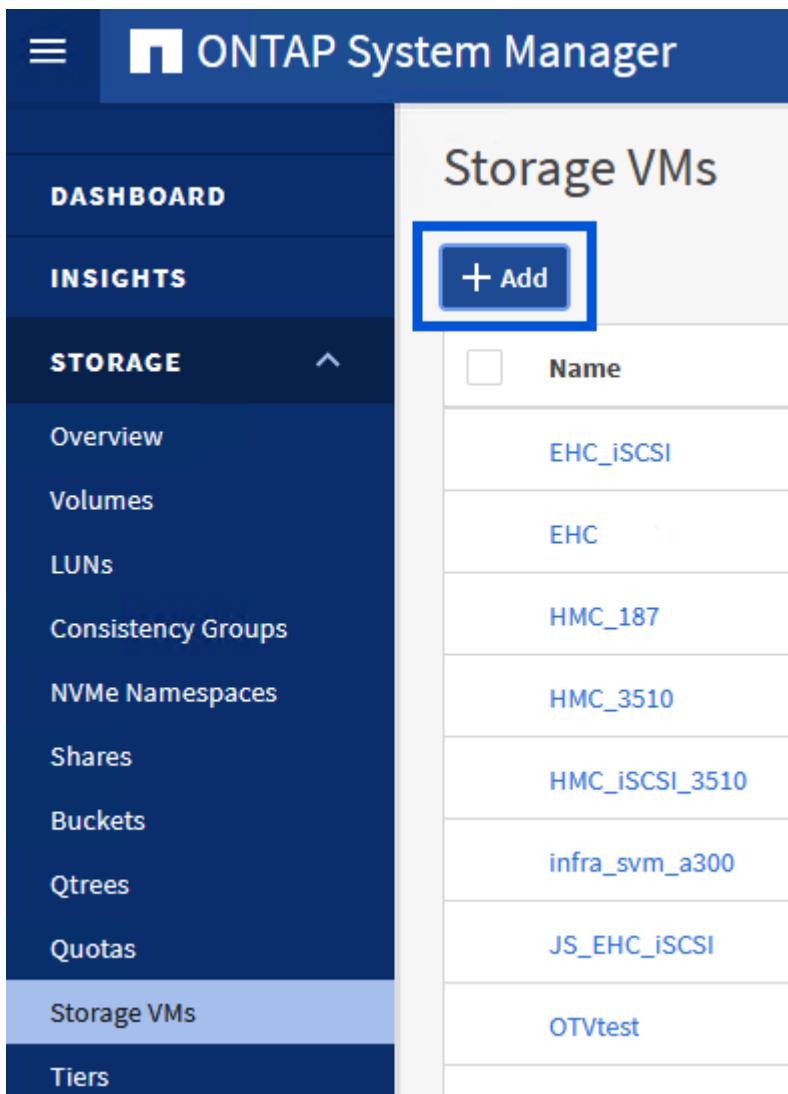
ONTAPストレージシステム上に**SVM**と**LIF**を作成する

次の手順はONTAP System Manager で実行されます。

ストレージVMとLIFを作成する

iSCSI トラフィック用の複数の LIF とともに SVM を作成するには、次の手順を実行します。

1. ONTAP System Manager から、左側のメニューの **Storage VMs** に移動し、**+ Add** をクリックして開始します。



2. ストレージ VM の追加 ウィザードで、SVM の名前を入力し、IP スペースを選択して、アクセスプロトコルの下にある iSCSI タブをクリックし、iSCSI を有効にする チェックボックスをオンにします。

Add Storage VM

X

STORAGE VM NAME

SVM_ISCSI

IPSPACE

Default

Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC NVMe

Enable iSCSI

3. ネットワーク インターフェイス セクションで、最初の LIF の IP アドレス、サブネット マスク、および ブロードキャスト ドメインとポートを入力します。後続の LIF については、チェックボックスを有効にして、残りのすべての LIF で共通の設定を使用するか、個別の設定を使用するかを選択できます。



複数のパスにわたるマルチパスとフェイルオーバーのために、NetApp、iSCSI 構成のすべての SVM に対して、個別のイーサネット ネットワーク内のストレージ ノードごとに少なくとも 2 つの LIF を用意することを推奨しています。

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS	SUBNET MASK	GATEWAY	BROADCAST DOMAIN AND PORT
172.21.118.179	24	Add optional gateway	NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS	PORT
172.21.119.179	a0a-3375

ntaphci-a300-02

IP ADDRESS	PORT
172.21.118.180	a0a-3374

IP ADDRESS	PORT
172.21.119.180	a0a-3375

- ストレージ VM 管理アカウント (マルチテナント環境の場合) を有効にするかどうかを選択し、[保存] をクリックして SVM を作成します。

Storage VM Administration

Manage administrator account

Save

Cancel

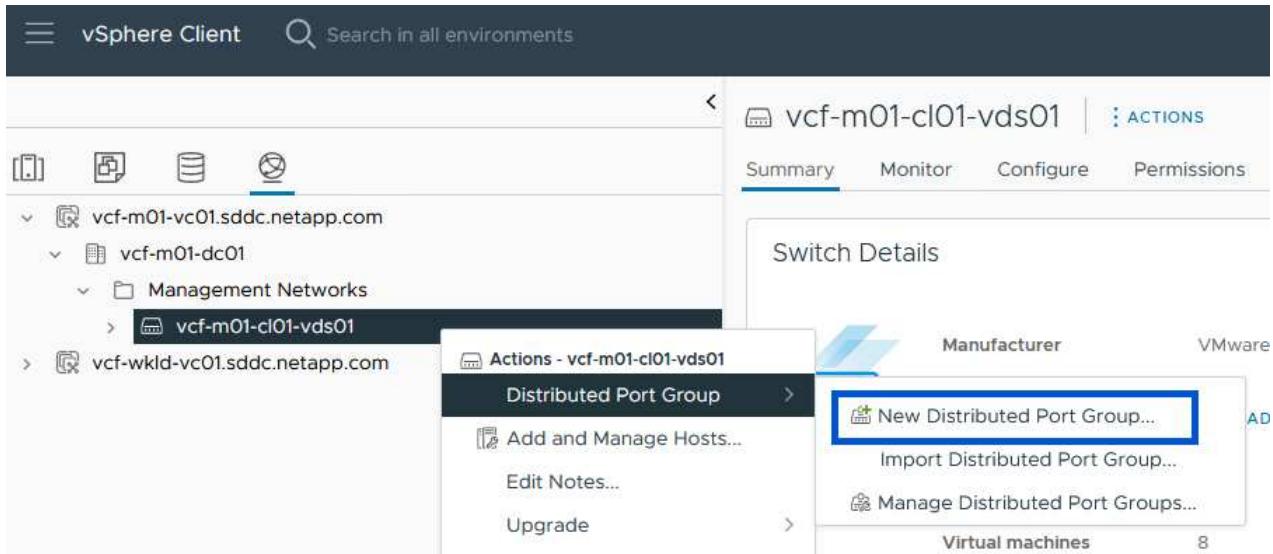
ESXiホストでiSCSIのネットワークを設定する

次の手順は、vSphere クライアントを使用して VCF 管理ドメイン クラスタで実行されます。

iSCSI トライフィック用の分散ポートグループを作成する

各 iSCSI ネットワークに新しい分散ポート グループを作成するには、次の手順を実行します。

1. 管理ドメイン クラスタの vSphere クライアントから、インベントリ > ネットワーク に移動します。既存の分散スイッチに移動し、*新しい分散ポート グループ...*を作成するアクションを選択します。



2. 新しい分散ポート グループ ウィザードで、新しいポート グループの名前を入力し、次へ をクリックして続行します。
3. *設定の構成*ページですべての設定を入力します。VLAN が使用されている場合は、正しい VLAN ID を必ず指定してください。続行するには、[次へ] をクリックします。

New Distributed Port Group

Configure settings

Set general properties of the new port group.

1 Name and location

2 Configure settings

3 Ready to complete

Port binding: Static binding

Port allocation: Elastic ⓘ

Number of ports: 8

Network resource pool: (default) ⓘ

VLAN

VLAN type: VLAN

VLAN ID: 3374

Advanced

Customize default policies configuration

CANCEL BACK NEXT

The screenshot shows the 'Configure settings' step of a 'New Distributed Port Group' wizard. The 'Port allocation' dropdown is set to 'Elastic'. The 'VLAN ID' input field contains '3374'. The 'NEXT' button is highlighted with a mouse cursor icon.

- *完了準備完了*ページで変更を確認し、*完了*をクリックして新しい分散ポート グループを作成します。
- このプロセスを繰り返して、使用されている 2 番目の iSCSI ネットワークの分散ポート グループを作成し、正しい **VLAN ID** を入力したことを確認します。
- 両方のポート グループが作成されたら、最初のポート グループに移動し、[設定の編集...] アクションを選択します。

vSphere Client Search in all environments

vcf-m01-cl01-vds01-pg-iscsi-a ACTIONS

Summary Monitor Configure Permissions Ports

Distributed Port Group Details

Port binding	Static binding
Port allocation	Elastic
VLAN ID	3374
Distributed switch	vcf-m01-cl01-vds01
Network protocol profile	--
Network resource pool	--
Hosts	4

Actions - vcf-m01-cl01-vds01-pg-iscsi-a

- Edit Settings...
- Export Configuration...
- Restore Configuration...

7. 分散ポート グループ - 設定の編集 ページで、左側のメニューの チーミングとフェイルオーバー に移動し、 **uplink2** をクリックして未使用のアップリンクまで下に移動します。

Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-a

General Advanced VLAN Security Traffic shaping Teaming and failover Monitoring Miscellaneous

Load balancing Network failure detection Notify switches Fallback Failover order ⓘ

MOVE UP MOVE DOWN Active uplinks uplink1 Standby uplinks Unused uplinks uplink2

CANCEL OK

8. 2 番目の iSCSI ポート グループに対してこの手順を繰り返します。ただし、今回は **uplink1** を **Unused uplinks** まで下に移動します。

Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-b

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Network failure detection

Notify switches

Fallback

Route based on originating virtual port

Link status only

Yes

Yes

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks



uplink2

Standby uplinks

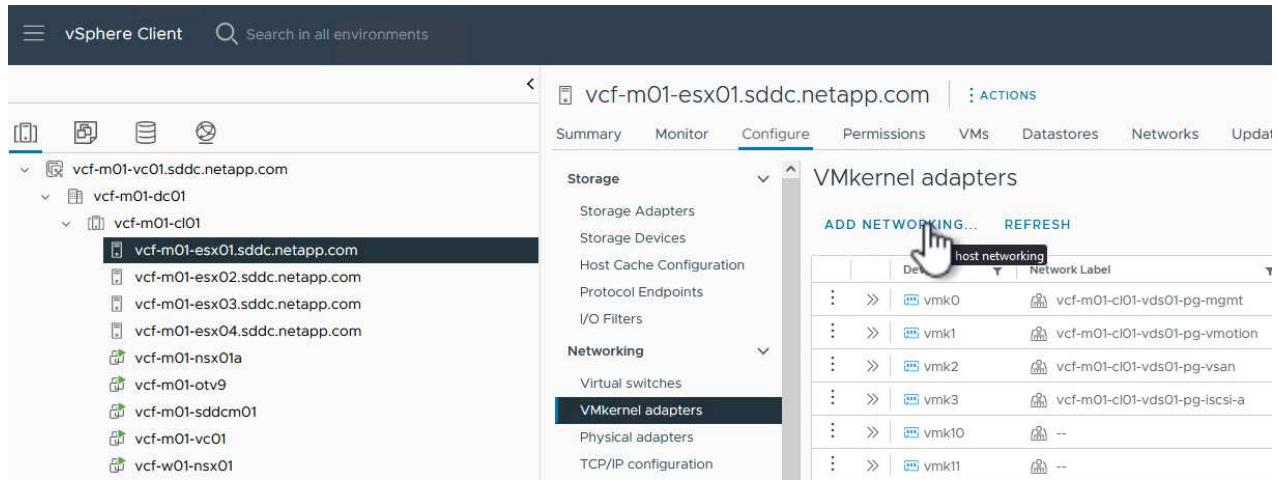
Unused uplinks

uplink1

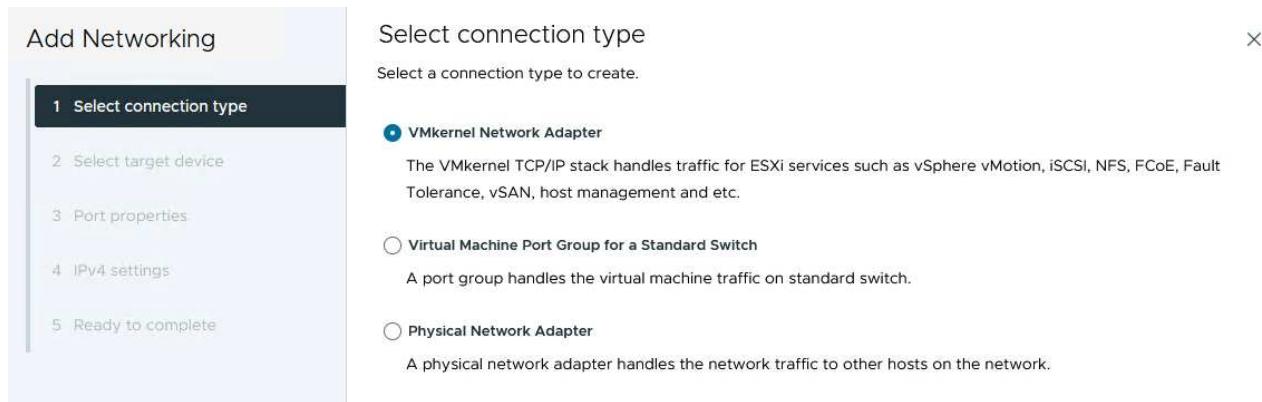
各ESXiホストにVMkernelアダプタを作成する

管理ドメイン内の各 ESXi ホストでこのプロセスを繰り返します。

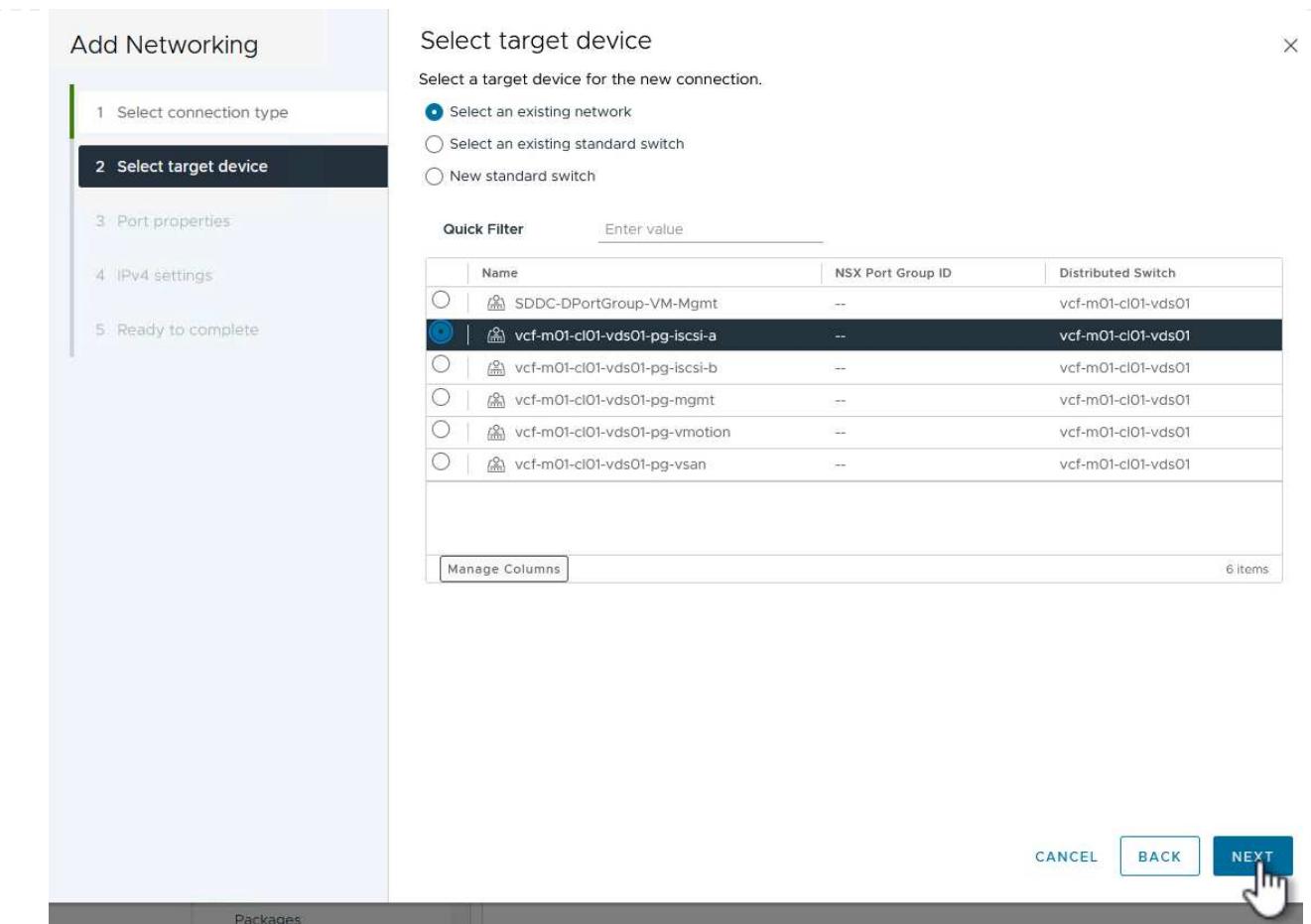
1. vSphere クライアントから、管理ドメイン インベントリ内の ESXi ホストの 1 つに移動します。 *構成*タブから*VMkernelアダプタ*を選択し、*ネットワークの追加...*をクリックして開始します。



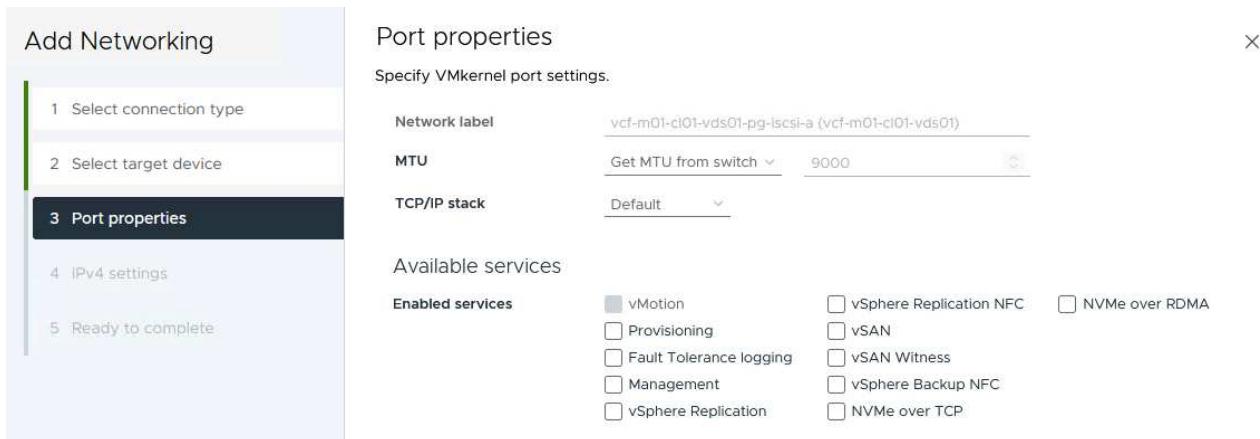
2. 接続タイプの選択 ウィンドウで **VMkernel** ネットワーク アダプタを選択し、次へをクリックして続行します。



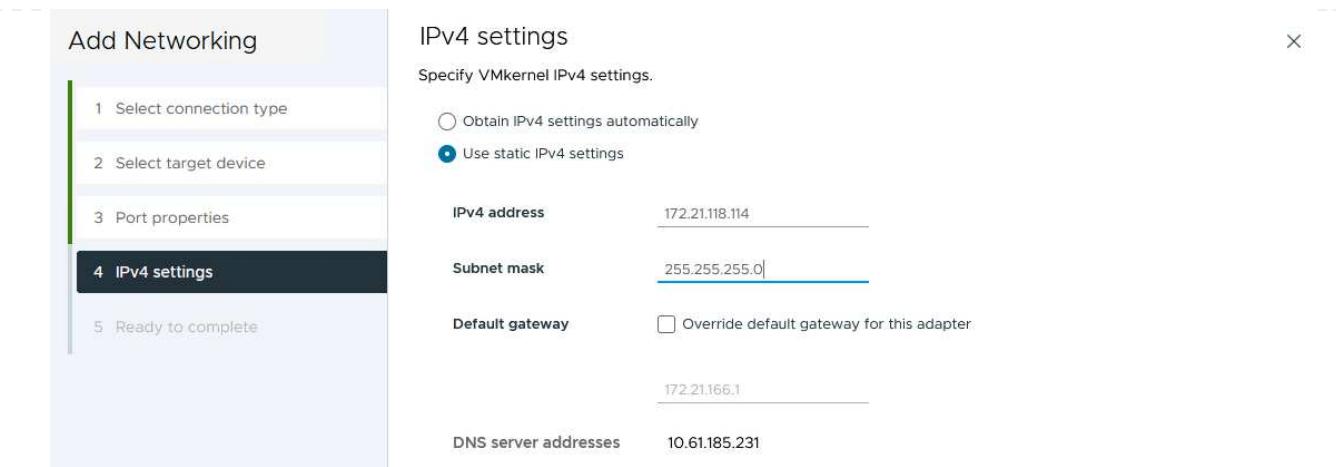
3. ターゲット デバイスの選択 ページで、以前に作成した iSCSI の分散ポート グループの 1 つを選択します。



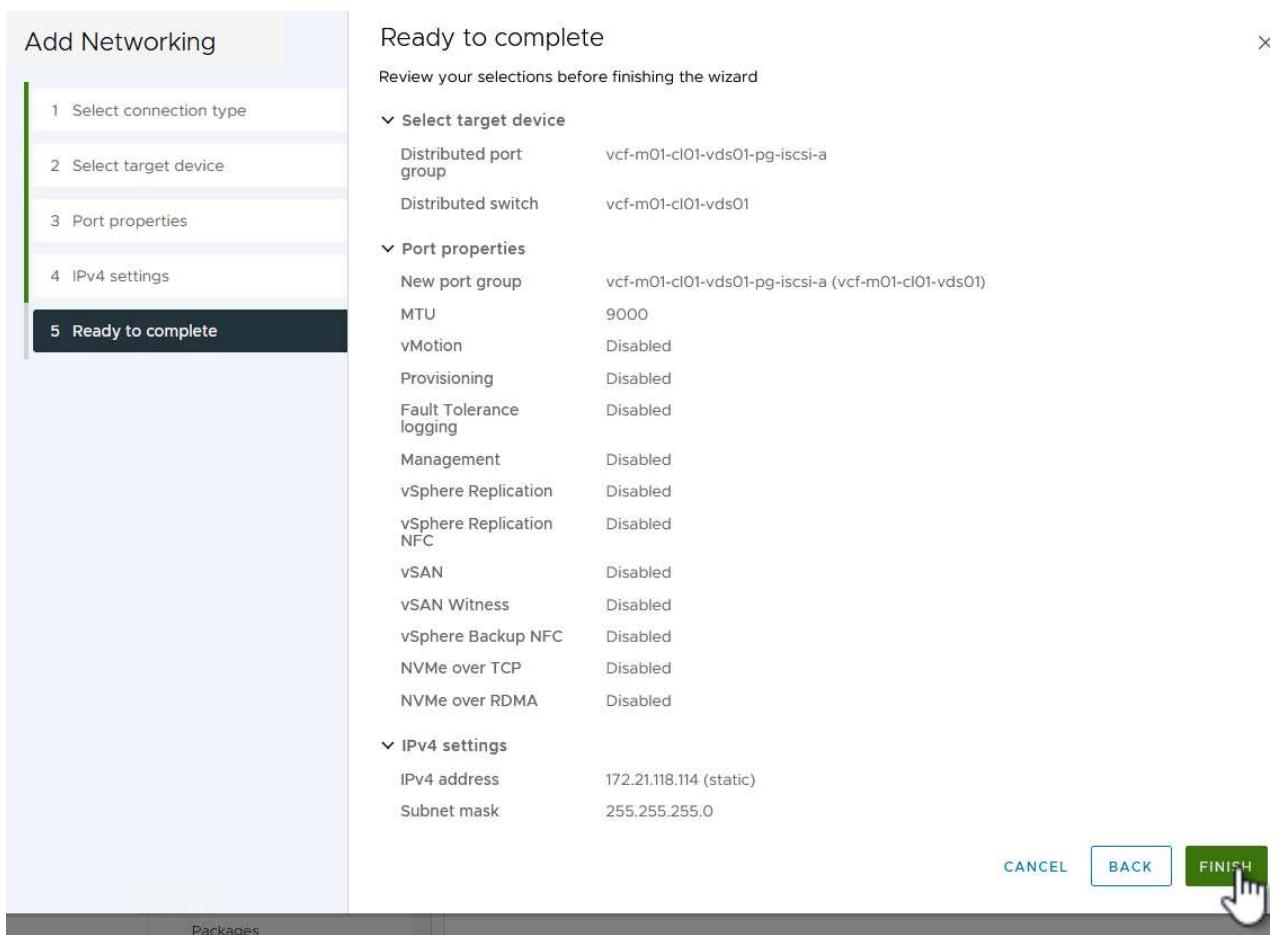
4. ポート プロパティ ページでデフォルトをそのままにして、次へ をクリックして続行します。



5. IPv4 設定 ページで、IP アドレス、サブネット マスク を入力し、新しいゲートウェイ IP アドレスを指定します (必要な場合のみ)。続行するには、[次へ] をクリックします。



6. *準備完了*ページで選択内容を確認し、*完了*をクリックして VMkernel アダプタを作成します。



7. このプロセスを繰り返して、2 番目の iSCSI ネットワーク用の VMkernel アダプタを作成します。

ONTAPツールを導入して使用し、ストレージを構成する

次の手順は、vSphere クライアントを使用して VCF 管理ドメイン クラスタ上で実行され、OTV の展

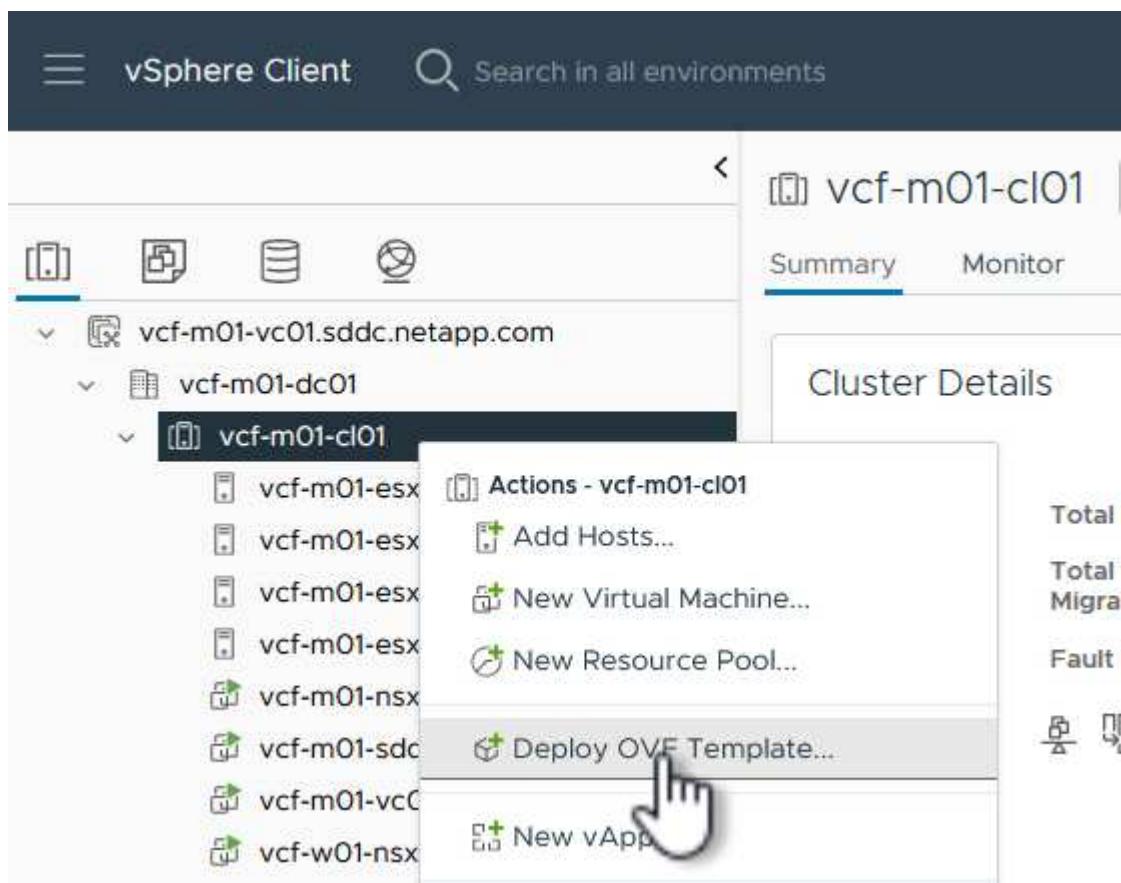
開、VMFS iSCSI データストアの作成、管理 VM の新しいデータストアへの移行が含まれます。

ONTAP tools for VMware vSphereを導入する

ONTAP tools for VMware vSphereは、VMアプライアンスとして導入され、ONTAPストレージを管理するための統合されたvCenter UIを提供します。

ONTAP tools for VMware vSphereをデプロイするには、次の手順を実行します。

1. ONTAPツールOVAイメージを以下から入手します。["NetApp サポート サイト"ローカルフォルダーにダウンロード](#)します。
2. VCF 管理ドメインの vCenter アプライアンスにログインします。
3. vCenter アプライアンス インターフェースから管理クラスタを右クリックし、[OVF テンプレートのデプロイ...]を選択します。



4. *OVF テンプレートのデプロイ*ウィザードで、*ローカル ファイル*ラジオ ボタンをクリックし、前の手順でダウンロードしたONTAPツール OVA ファイルを選択します。

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

Local file

UPLOAD FILES

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. ウィザードの手順 2～5 では、VM の名前とフォルダーを選択し、コンピューティング リソースを選択し、詳細を確認して、ライセンス契約に同意します。
6. 構成ファイルとディスク ファイルの保存場所として、VCF 管理ドメイン クラスタの vSAN データストアを選択します。

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format

As defined in the VM storage policy

VM Storage Policy

Datastore Default

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	Total
vcf-m01-cl01-ds-vsanc01	--	999.97 GB	7.17 TB	225.72 GB	7.17 TB
vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	25.75 GB
vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	25.75 GB
vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	25.75 GB
vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	25.75 GB

Manage Columns

Items per page 10 5 items

7. [ネットワークの選択] ページで、管理トラフィックに使用するネットワークを選択します。

X

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks**

Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	vcf-m01-cl01-vds01-pg-vsan

Manage Columns

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

vcf-m01-cl01-vds01-pg-vsan
SDDC-DPortGroup-VM-Mgmt
Browse ...

8. テンプレートのカスタマイズページで、必要な情報をすべて入力します。

- OTVへの管理アクセスに使用するパスワード。
- NTPサーバのIPアドレスを指定します。
- OTVメンテナンスアカウントのパスワード。
- OTVダービーDBパスワード。
- VMware Cloud Foundation (VCF)**を有効にするチェックボックスをオンにしないでください。補助ストレージを展開する場合、VCFモードは必要ありません。
- vCenterアプライアンスのFQDNまたはIPアドレスと、vCenterの資格情報を提供します。
- 必要なネットワークプロパティフィールドを指定します。

続行するには、[次へ]をクリックします。

Deploy OVF Template

1 Select an OVF template
 2 Select a name and folder
 3 Select a compute resource
 4 Review details
 5 License agreements
 6 Select storage
 7 Select networks
8 Customize template
 9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

1 2 properties have invalid values X

System Configuration		4 settings
Application User Password (*)	Password to assign to the administrator account. For security reasons, it is recommended to use a password that is eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.	
	Password	***** (i)
	Confirm Password	***** (i)
NTP Servers		A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. 172.21.166.1
Maintenance User Password (*)		Password to assign to maint user account.
	Password	***** (i)
	Confirm Password	***** (i)

Deploy OVF Template

1 Select an OVF template
 2 Select a name and folder
 3 Select a compute resource
 4 Review details
 5 License agreements
 6 Select storage
 7 Select networks
8 Customize template
 9 Ready to complete

Customize template

Configure vCenter or Enable VCF		5 settings
Enable VMware Cloud Foundation (VCF)	vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>	
vCenter Server Address (*)	Specify the IP address/hostname of an existing vCenter to register to. 172.21.166.140	
Port (*)	Specify the HTTPS port of an existing vCenter to register to. 443	
Username (*)	Specify the username of an existing vCenter to register to. administrator@vsphere.local	
Password (*)	Specify the password of an existing vCenter to register to.	
	Password	***** (i)
	Confirm Password	***** (i)
Network Properties		8 settings
Host Name	Specify the hostname for the appliance. (Leave blank if DHCP is desired) vcf-m01-otv9	
IP Address	Specify the IP address for the appliance. (Leave blank if DHCP is	

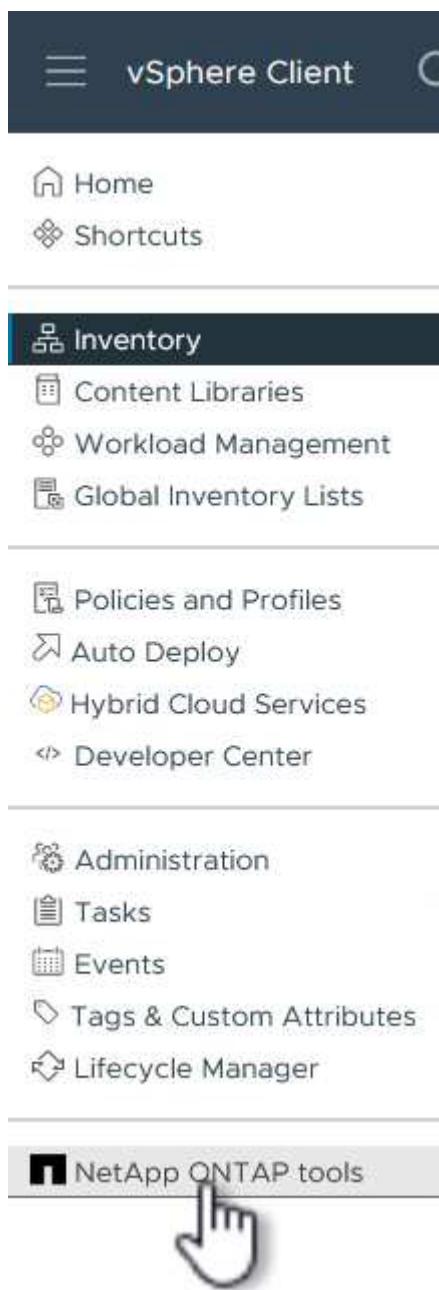
CANCEL BACK NEXT

9. [Ready to complete] ページですべての情報を確認し、[Finish] をクリックして OTV アプライアンスの展開を開始します。

OTVを使用して管理ドメインにVMFS iSCSIデータストアを構成する

OTVを使用して VMFS iSCSI データストアを管理ドメインの補助ストレージとして構成するには、次の手順を実行します。

1. vSphere クライアントでメイン メニューに移動し、* NetApp ONTAPツール* を選択します。



2. * ONTAPツール* に入ったら、[Getting Started] ページ (または Storage Systems) から [Add] をクリックして、新しいストレージシステムを追加します。

☰ vsphere Client Q Search in all environments

NetApp ONTAP tools INSTANCE 172.21.166.139:8443

Overview Storage Systems Storage capability profile Storage Mapping Settings Reports Datastore Report Virtual Machine Report vVols Datastore Report vVols Virtual Machine Report Log Integrity Report

ONTAP tools for VMware vSphere

Getting Started Traditional Dashboard vVols Dashboard

ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.

Add Storage System Provision Datastore

Add storage systems to ONTAP tools for VMware vSphere. Create traditional or vVols datastores.

What's new? September 4, 2023

- Qualified and supported with ONTAP 9.13.1
- Supports and interoperates with VMware vSphere 8.x releases
- Includes newer enhanced SCPs that efficiently map workloads to the newer All SAN Array platforms through policy based management

Next Steps

 [View Dashboard](#)

View and monitor the datastores in ONTAP tools for VMware vSphere.

 [Settings](#)

Configure administrative settings such as credentials, alarm thresholds.

Resources

- ONTAP tools for VMware vSphere Documentation Resources
- RBAC User Creator for Data ONTAP
- ONTAP tools for VMware vSphere REST API Documentation

3. ONTAPストレージ システムの IP アドレスと資格情報を入力し、[追加] をクリックします。

Add Storage System

(i) Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

vcf-m01-vc01.sddc.netapp.com

Name or IP address:

172.16.9.25

Username:

admin

Password:

Port:

443

[Advanced options >](#)

CANCEL

SAVE & ADD MORE

ADD



4. 「はい」をクリックしてクラスター証明書を承認し、ストレージシステムを追加します。

Add Storage System

i Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

vcf-m01-vc01.sddc.netapp.com

Authorize Cluster Certificate

Host 172.16.9.25 has identified itself with a self-signed certificate.

[Show certificate](#)

Do you want to trust this certificate?

NO

YES



CANCEL

SAVE & ADD MORE

ADD

管理VMをiSCSIデータストアに移行する

VCF 管理 VM を保護するためにONTAPストレージを使用することが望ましい場合は、vMotion を使用して VM を新しく作成された iSCSI データストアに移行できます。

VCF 管理 VM を iSCSI データストアに移行するには、次の手順を実行します。

1. vSphere Client から管理ドメイン クラスタに移動し、[VM] タブをクリックします。
2. iSCSI データストアに移行する VM を選択し、右クリックして [移行] を選択します。

The screenshot shows the vSphere Client interface. On the left, a tree view shows a cluster named 'vcf-m01-vc01.sddc.netapp.com' containing several datacenters (dc01, dc02) and hosts (host01, host02). In the center, the 'Virtual Machines' tab is selected. A context menu is open over a specific VM, with the 'Migrate...' option highlighted. The main pane displays a table of VMs with columns for Name, State, Status, Provisioned Space, Used Space, Host CPU, and Host Mem.

	Name	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
vcf-m01-nsx01a	Powered On	Normal	616.52 GB	97.88 GB	5 GHz	31.63 GB	
vcf-m01-nsx01b	Powered On	Normal	106.33 GB	19.33 GB	2.52 GHz	6.77 GB	
vcf-m01-nsx01c	Powered On	Normal	1.79 TB	237.82 GB	344 MHz	15.98 GB	
vcf-m01-nsx01d	Powered On	Normal	1.16 TB	143.81 GB	757 MHz	13.98 GB	
vcf-w01-nsx01	Powered On	Normal	600.35 GB	90.61 GB	7.99 GHz	48.11 GB	
vcf-w01-nsx02	Powered On	Normal	600.39 GB	94.6 GB	6.06 GHz	48.1 GB	
vcf-w01-nsx03	Powered On	Normal	600.45 GB	95.14 GB	7.16 GHz	48.14 GB	
vcf-wkld-vc01	Powered On	Normal	1.82 TB	126.69 GB	780 MHz	28.02 GB	

3. *仮想マシン - 移行*ウィザードで、移行タイプとして*ストレージのみの変更*を選択し、*次へ*をクリックして続行します。

The screenshot shows the 'Select a migration type' step of the migration wizard. It displays four options: 'Change compute resource only', 'Change storage only' (which is selected), 'Change both compute resource and storage', and 'Cross vCenter Server export'. A hand cursor is pointing at the 'Change storage only' option.

8 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only
Migrate the virtual machines to another host or cluster.

Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

4. *ストレージの選択*ページで、iSCSI データストアを選択し、*次へ*を選択して続行します。

8 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE CONFIGURE PER DISK

Select virtual disk format Same format as source

VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	T
mgmt_01_iscsi	--	3 TB	1.46 GB	3 TB	V
vcf-m01-cl01-ds-vsang01	--	999.97 GB	7.28 TB	52.38 GB	V

Manage Columns

Items per page: 10 2 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT



5. 選択内容を確認し、「完了」をクリックして移行を開始します。

6. 移転ステータスは、[最近のタスク] ペインから確認できます。

Recent Tasks			
Task Name	Target	Status	Details
Relocate virtual machine	vcf-w01-nsx03	38%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-wkld-vc01	42%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-otv9	36%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-nsx01a	49%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-w01-nsx02	47%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-sddcm01	39%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-w01-nsx01	42%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-vc01	44%	Migrating Virtual Machine active state

追加情報

ONTAPストレージシステムの構成については、["ONTAP 9ドキュメント"](#)中心。

VCFの設定方法については、以下を参照してください。["VMware Cloud Foundation ドキュメント"](#)。

このソリューションのビデオデモ

[VCF管理ドメインの補助ストレージとしてのiSCSIデータストア](#)

ONTAP tools for VMware vSphereを使用して、管理ドメインの補助ストレージとしてFCベースのVMFSデータストアを追加します。

このユースケースでは、ONTAP Tools for VMwareを使用して、ファイバチャネル(FC)経由のVMFSデータストアをVMware Cloud Foundation(VCF)管理ドメインの補助ストレージとして構成する手順について説明します。この手順では、VMware vSphere用のONTAPツールの導入、vCenterサーバーの登録、ストレージバックエンドの定義、およびFCデータストアのプロビジョニングについてまとめています。

ファイバチャネルの利点

高性能: FCは高速データ転送速度を提供するため、大量のデータへの高速かつ信頼性の高いアクセスを必要とするアプリケーションに最適です。

低レイテンシ: 非常に低いレイテンシ。これは、データベースや仮想化環境などのパフォーマンスが重視されるアプリケーションにとって非常に重要です。

信頼性: FCネットワークは、冗長性やエラー訂正などの機能が組み込まれており、堅牢性と信頼性に優れています。

専用帯域幅: FCはストレージトラフィックに専用の帯域幅を提供し、ネットワーク輻輳のリスクを軽減します。

NetAppストレージシステムでのファイバチャネルの使用に関する詳細については、["FCを使用したSANプロビジョニング"](#)。

シナリオの概要

VCF補足データストアは、vCenterを使用したDay-2運用の一部としてプロビジョニングされます。このシナリオでは、次の大きな手順について説明します。

- ・管理ドメインへのONTAPツールの導入
- ・VIワークロードvCenter ServerをONTAPツールに登録する
- ・VMware vSphereのONTAPツールプラグインでストレージバックエンドを定義する
- ・FCトランスポート上でVMFSをプロビジョニングする

前提条件

このシナリオには、次のコンポーネントと構成が必要です。

- FC スイッチに接続された FC ポートを備えたONTAPストレージシステム。
- FC lifs で作成された SVM。
- FC スイッチに接続された FC HBA を備えた vSphere。
- FC スイッチには単一のイニシエーター ターゲット ゾーニングが構成されています。



ONTAPシステム上の物理 FC ポートではなく、ゾーン構成で SVM FC 論理インターフェイスを使用します。

NetApp は、FC LUN にマルチパスを推奨しています。

ONTAPストレージシステムでのファイバチャネルの設定に関する詳細については、以下を参照してください。 "[SANストレージの管理](#)" ONTAP 9 のドキュメントを参照してください。

ONTAPストレージシステムでVMFSを使用する方法の詳細については、"[VMFS の導入ガイド](#)"。

管理ドメインの展開手順

ONTAPツールを導入し、それを使用して VCF 管理ドメインに VMFS データストアを作成するには、次の手順を実行します。

- "[管理ドメインにONTAPツールを導入する](#)"
- "[vSphere クライアントインターフェースを使用してストレージ バックエンドを定義する](#)"
- "[FC 上で VMFS をプロビジョニングする](#)"

追加情報

ONTAPストレージシステムの構成については、"[ONTAP 9ドキュメント](#)"中心。

VCFの設定方法については、以下を参照してください。"[VMware Cloud Foundation ドキュメント](#)"。

このソリューションのビデオデモ

[VCF管理ドメインの補助ストレージとしてのVMFS\(FC\)データストア](#)

ONTAP tools for VMware vSphereを使用して、VI ワークロード ドメインに補助ストレージとしてvVols を追加します。

このユースケースでは、VMware Cloud Foundation (VCF) 仮想インフラストラクチャ (VI) ワークロード ドメインの補助ストレージとして iSCSI を使用してvVolsデータストアを構成する手順について説明します。この手順では、iSCSI ネットワークの設定、VMware vSphere 用のONTAPツールの導入、およびvVolsデータストアのプロビジョニングの概要を説明します。

iSCSI は、vVolsデータストアのストレージ プロトコルとして使用されます。

iSCSIの利点

高性能: 高速で効率的なデータ転送速度と低遅延を実現する高性能を提供します。要求の厳しいエンタープライズ アプリケーションや仮想化環境に最適です。

管理の容易さ: 使い慣れた IP ベースのツールとプロトコルを使用して、ストレージ管理を簡素化します。

コスト効率が高い: 既存のイーサネット インフラストラクチャを活用することで、特殊なハードウェアの必要性が減り、組織は信頼性が高くスケーラブルなストレージ ソリューションを実現できます。

NetAppストレージシステムでiSCSIを使用する方法の詳細については、以下を参照してください。 "["iSCSIによる SAN プロビジョニング"](#)"。

シナリオの概要

このシナリオでは、次の大まかな手順について説明します。

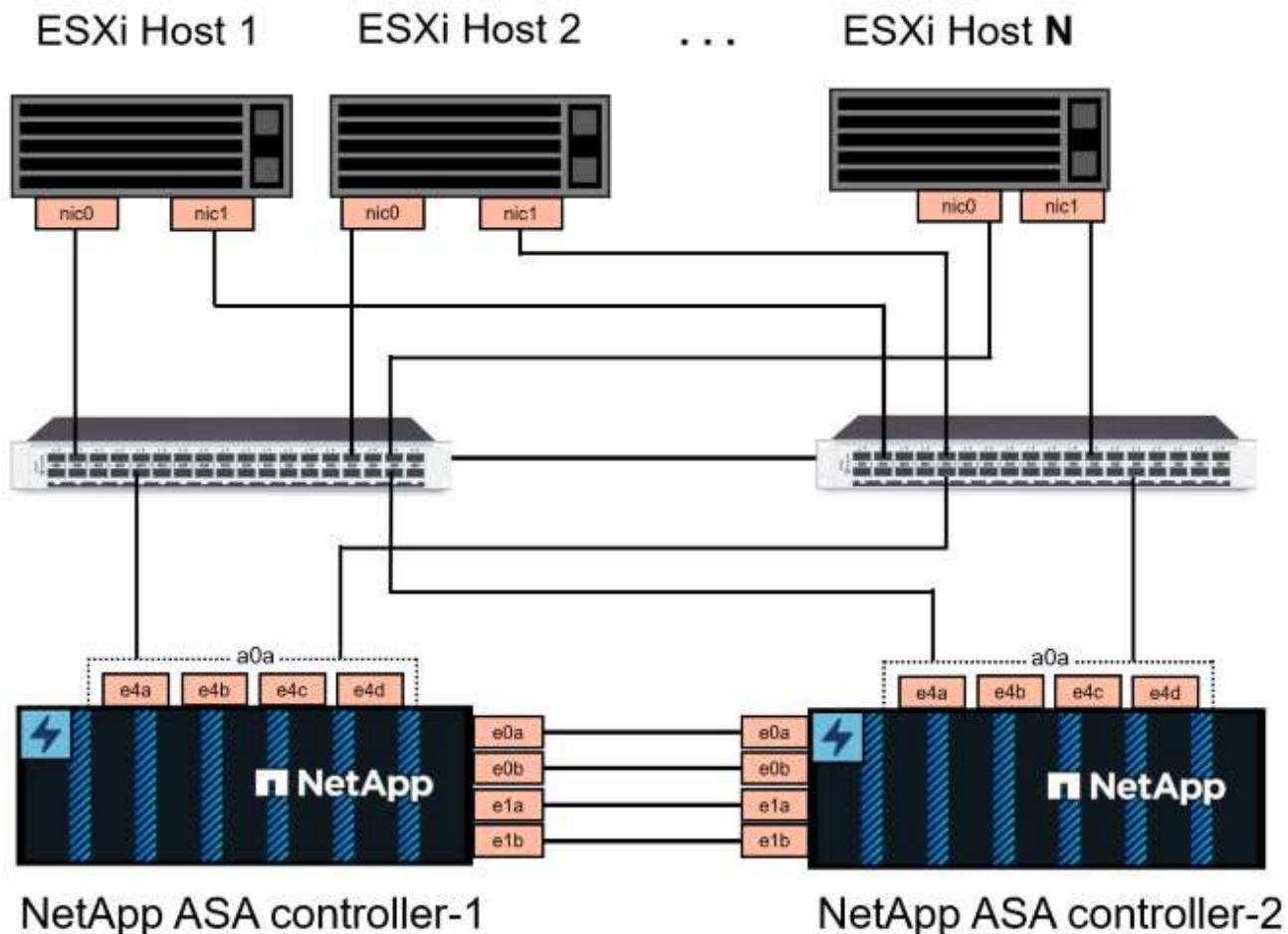
- iSCSI トラフィック用の論理インターフェイス (LIF) を備えたストレージ仮想マシン (SVM) を作成します。
- VI ワークロード ドメイン上の iSCSI ネットワーク用の分散ポート グループを作成します。
- VI ワークロード ドメインの ESXi ホスト上に iSCSI 用の vmkernel アダプタを作成します。
- VI ワークロード ドメインにONTAPツールを導入します。
- VI ワークロード ドメインに新しいvVolsデータストアを作成します。

前提条件

このシナリオには、次のコンポーネントと構成が必要です。

- ストレージ トラフィック専用のイーサネット スイッチ上に物理データ ポートを備えたONTAP AFF またはASAストレージ システム。
- VCF 管理ドメインの展開が完了し、vSphere クライアントにアクセスできるようになりました。
- VI ワークロード ドメインは以前にデプロイされています。

NetApp は、iSCSI に対して完全に冗長化されたネットワーク設計を推奨しています。次の図は、ストレージ システム、スイッチ、ネットワーク アダプタ、およびホスト システムにフォールト トレランスを提供する冗長構成の例を示しています。 NetAppを参照してください"["SAN構成に関するリファレンス"](#)追加情報については、こちらをご覧ください。



複数のパスにわたるマルチパスとフェイルオーバーのために、NetApp、iSCSI構成のすべてのSVMに対して、個別のイーサネットネットワーク内のストレージノードごとに少なくとも2つのLIFを用意することを推奨しています。

このドキュメントでは、新しいSVMを作成し、IPアドレス情報を指定してiSCSIトラフィック用の複数のLIFを作成するプロセスについて説明します。既存のSVMに新しいLIFを追加するには、["LIF（ネットワークインターフェイス）の作成"](#)。



複数のVMkernelアダプタが同じIPネットワーク上に構成されている場合は、アダプタ間で負荷分散が行われるように、ESXiホストでソフトウェアiSCSIポートバインディングを使用することをお勧めします。KB記事を参照してください["ESX/ESXiでソフトウェアiSCSIポートバインディングを使用する際の考慮事項\(2038869\)"](#)。

VMwareでVMFS iSCSIデータストアを使用する方法の詳細については、以下を参照してください。["vSphere VMFSデータストア - ONTAPを使用したiSCSIストレージバックエンド"](#)。

展開手順

ONTAPツールを導入し、それを使用してVCF管理ドメインにvVolsデータストアを作成するには、次の手順を実行します。

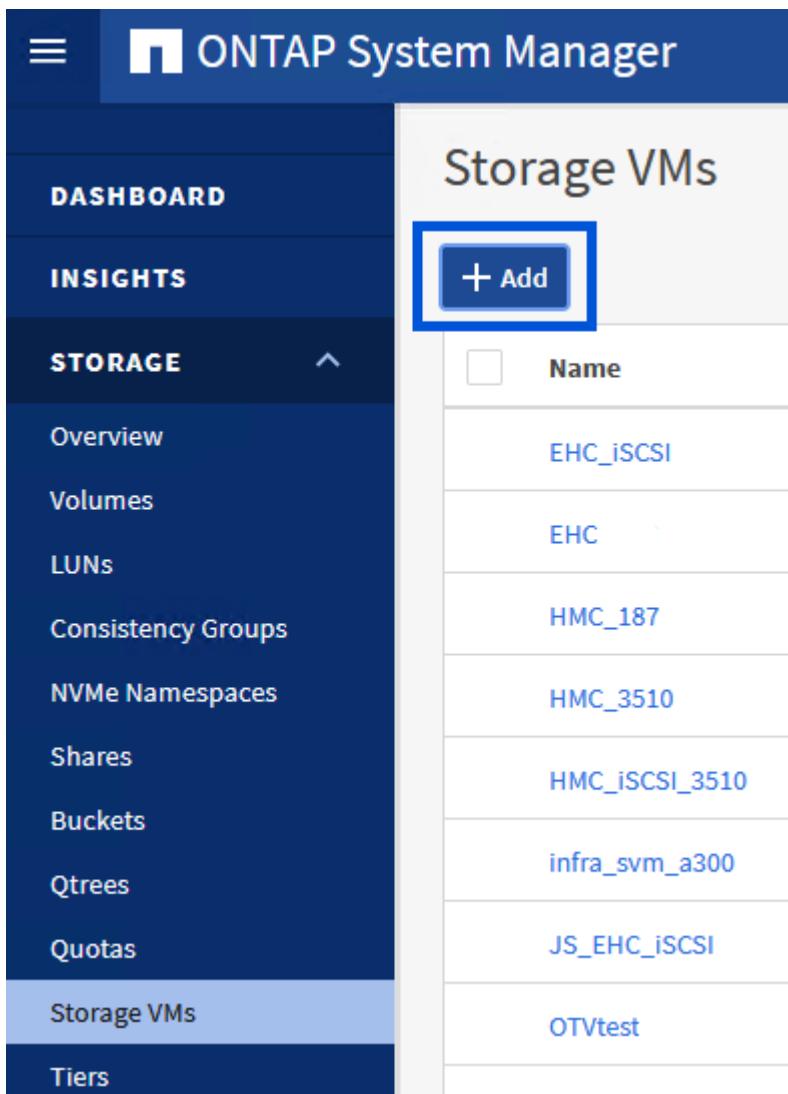
ONTAPストレージシステム上に**SVM**と**LIF**を作成する

次の手順はONTAP System Manager で実行されます。

ストレージVMとLIFを作成する

iSCSI トラフィック用の複数の LIF とともに SVM を作成するには、次の手順を実行します。

1. ONTAP System Manager から、左側のメニューの **Storage VMs** に移動し、**+ Add** をクリックして開始します。



2. ストレージ VM の追加 ウィザードで、SVM の名前を入力し、IP スペースを選択して、アクセスプロトコルの下にある iSCSI タブをクリックし、iSCSI を有効にする チェックボックスをオンにします。

Add Storage VM

X

STORAGE VM NAME

SVM_ISCSI

IPSPACE

Default

Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable iSCSI

3. ネットワーク インターフェイス セクションで、最初の LIF の IP アドレス、サブネット マスク、および ブロードキャスト ドメインとポートを入力します。後続の LIF については、チェックボックスを有効にして、残りのすべての LIF で共通の設定を使用するか、個別の設定を使用するかを選択できます。



複数のパスにわたるマルチパスとフェイルオーバーのために、NetApp、iSCSI 構成のすべての SVM に対して、個別のイーサネット ネットワーク内のストレージ ノードごとに少なくとも 2 つの LIF を用意することを推奨しています。

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS	SUBNET MASK	GATEWAY	BROADCAST DOMAIN AND PORT
172.21.118.179	24	Add optional gateway	NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS	PORT
172.21.119.179	a0a-3375

ntaphci-a300-02

IP ADDRESS	PORT
172.21.118.180	a0a-3374

IP ADDRESS	PORT
172.21.119.180	a0a-3375

- ストレージ VM 管理アカウント (マルチテナント環境の場合) を有効にするかどうかを選択し、[保存] をクリックして SVM を作成します。

Storage VM Administration

Manage administrator account

Save

Cancel

ESXiホストでiSCSIのネットワークを設定する

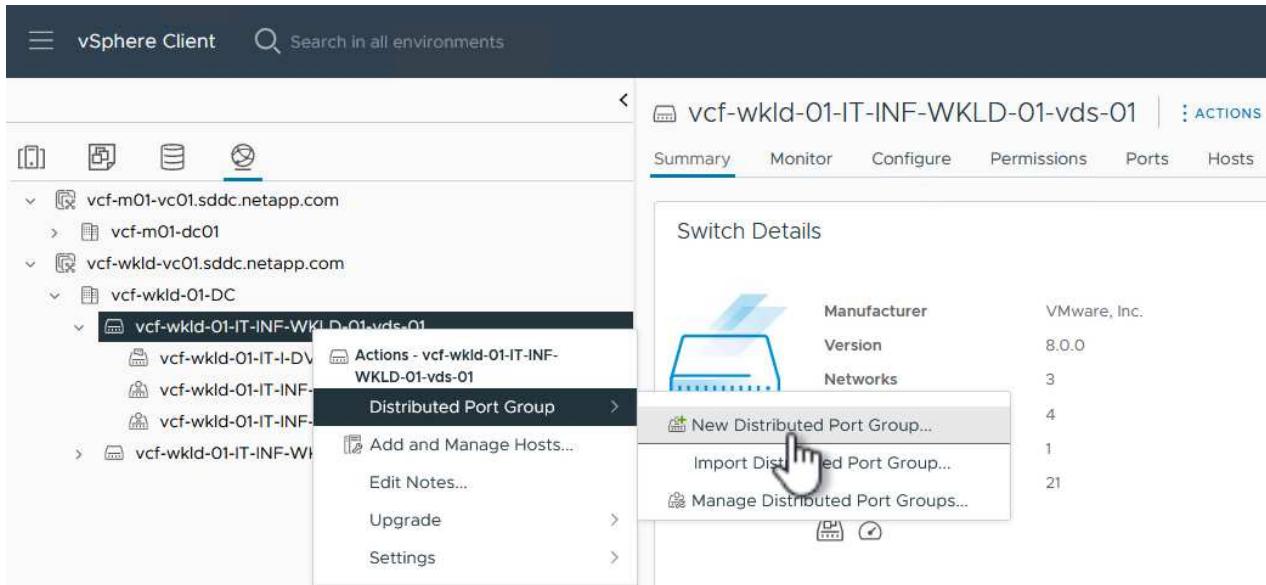
次の手順は、vSphere クライアントを使用して VI ワークロード ドメイン クラスタで実行されます。この場合、vCenter Single Sign-On が使用されているため、vSphere クライアントは管理ドメインとワークロード ド

メイン全体で共通になります。

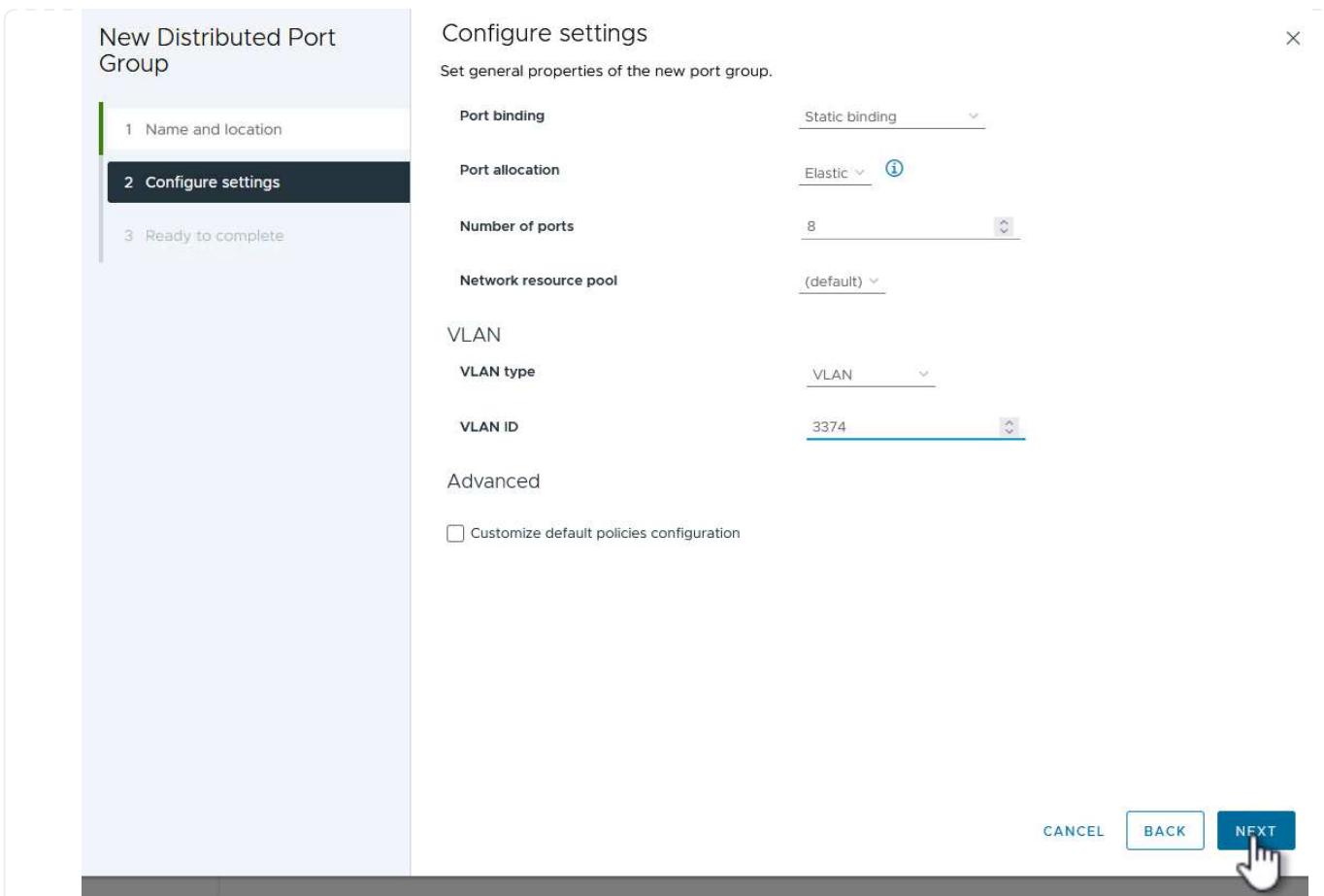
iSCSI トライフィック用の分散ポートグループを作成する

各 iSCSI ネットワークに新しい分散ポート グループを作成するには、次の手順を実行します。

1. vSphere クライアントから、ワークロード ドメインの インベントリ > ネットワーク に移動します。既存の分散スイッチに移動し、*新しい分散ポート グループ...*を作成するアクションを選択します。



2. 新しい分散ポート グループ ウィザードで、新しいポート グループの名前を入力し、次へ をクリックして続行します。
3. *設定の構成*ページですべての設定を入力します。VLAN が使用されている場合は、正しい VLAN ID を必ず指定してください。続行するには、[次へ] をクリックします。



- *完了準備完了*ページで変更を確認し、*完了*をクリックして新しい分散ポート グループを作成します。
- このプロセスを繰り返して、使用されている 2 番目の iSCSI ネットワークの分散ポート グループを作成し、正しい **VLAN ID** を入力したことを確認します。
- 両方のポート グループが作成されたら、最初のポート グループに移動し、[設定の編集...] アクションを選択します。

vSphere Client

Search in all environments

vcf-wkld-01-iscsi-a | ACTIONS

Summary		Monitor	Configure	Permissions	Ports	Hosts
Distributed Port Group Details <div style="display: flex; align-items: center;"> Port binding: Static binding Port allocation: Elastic VLAN ID: 3374 Distributed switch: vcf-wkld-01-IT-INF-WKLD-01-vds-01 Network protocol profile: -- </div>						

Actions - vcf-wkld-01-iscsi-a

Edit Settings... (with a hand cursor)

vcf-wkld-01-iscsi-a

vcf-wkld-01-i

vcf-wkld-01-i

vcf-wkld-01-i

vcf-wkld-01-i

7. 分散ポートグループ - 設定の編集 ページで、左側のメニューの チーミングとフェイルオーバー に移動し、 **uplink2** をクリックして 未使用のアップリンク まで下に移動します。

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-a

General Advanced VLAN Security Traffic shaping Teaming and failover Monitoring Miscellaneous

Load balancing Network failure detection Notify switches Fallback

Route based on originating virtual port
Link status only
Yes
Yes

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

CANCEL OK

8. 2 番目の iSCSI ポート グループに対してこの手順を繰り返します。ただし、今回は **uplink1** を **Unused uplinks** まで下に移動します。

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-b

General Advanced VLAN Security Traffic shaping Teaming and failover Monitoring Miscellaneous

Load balancing Network failure detection Notify switches Fallback

Route based on originating virtual port
Link status only
Yes
Yes

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink2

Standby uplinks

Unused uplinks

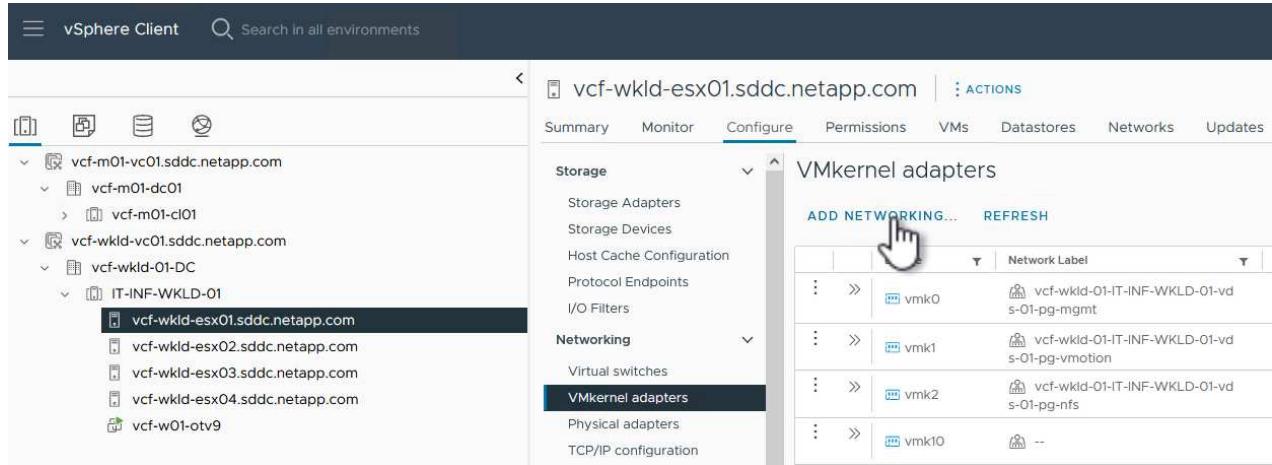
uplink1

CANCEL OK

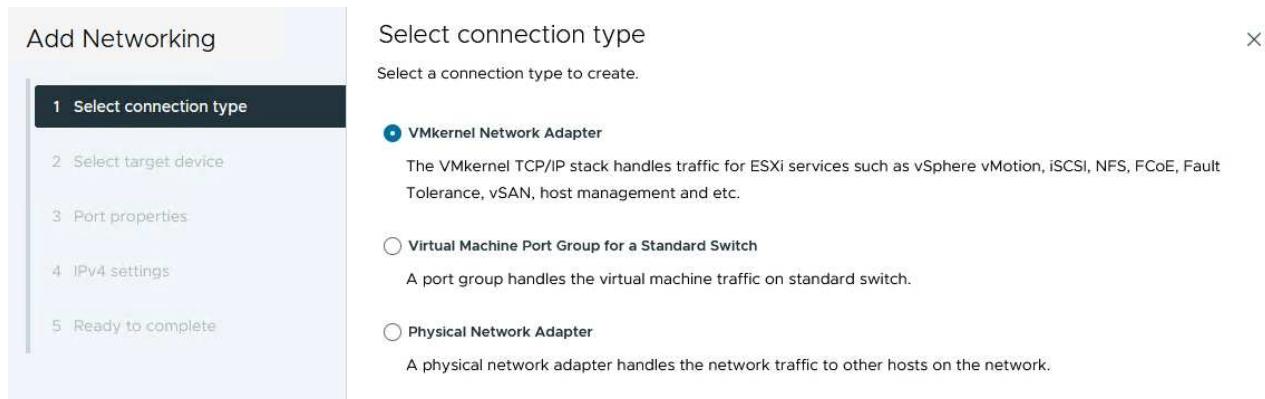
各ESXiホストにVMkernelアダプタを作成する

ワークロード ドメイン内の各 ESXi ホストでこのプロセスを繰り返します。

1. vSphere クライアントから、ワークロード ドメイン インベントリ内の ESXi ホストの 1 つに移動します。*構成*タブから*VMkernelアダプタ*を選択し、*ネットワークの追加...*をクリックして開始します。



2. 接続タイプの選択 ウィンドウで **VMkernel** ネットワーク アダプタを選択し、次へをクリックして続行します。



3. ターゲット デバイスの選択 ページで、以前に作成した iSCSI の分散ポート グループの 1 つを選択します。

Add Networking

Select a target device for the new connection.

Select an existing network
 Select an existing standard switch
 New standard switch

Name	NSX Port Group ID	Distributed Switch
vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Manage Columns

5 items

CANCEL BACK NEXT

4. ポートプロパティページでデフォルトをそのままにして、次へをクリックして続行します。

Add Networking

Specify VMkernel port settings.

Network label	vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	Get MTU from switch 9000
TCP/IP stack	Default

Available services

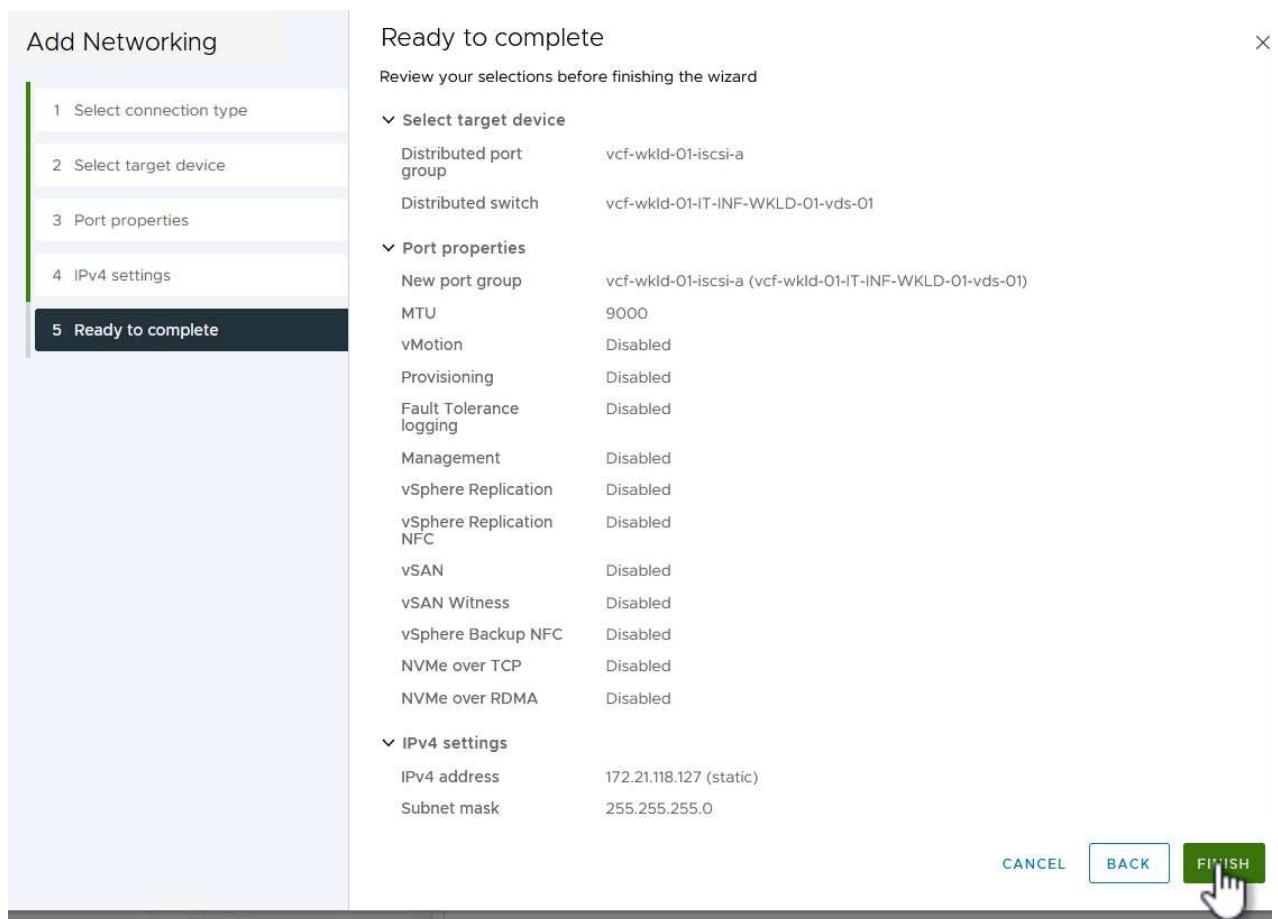
Enabled services	<input checked="" type="checkbox"/> vMotion <input type="checkbox"/> Provisioning <input type="checkbox"/> Fault Tolerance logging <input type="checkbox"/> Management <input type="checkbox"/> vSphere Replication	<input type="checkbox"/> vSphere Replication NFC <input type="checkbox"/> vSAN <input type="checkbox"/> vSAN Witness <input type="checkbox"/> vSphere Backup NFC <input type="checkbox"/> NVMe over TCP	<input type="checkbox"/> NVMe over RDMA
------------------	---	---	---

BACK NEXT

5. IPv4設定ページで、IPアドレス、サブネットマスクを入力し、新しいゲートウェイIPアドレスを指定します(必要な場合のみ)。続行するには、[次へ]をクリックします。



6. *準備完了*ページで選択内容を確認し、*完了*をクリックして VMkernel アダプタを作成します。



7. このプロセスを繰り返して、2 番目の iSCSI ネットワーク用の VMkernel アダプタを作成します。

ONTAPツールを導入して使用し、ストレージを構成する

次の手順は、vSphere クライアントを使用して VCF 管理ドメイン クラスタで実行され、ONTAPツールの導

入、vVols iSCSI データストアの作成、管理 VM の新しいデータストアへの移行が含まれます。

VI ワークロード ドメインの場合、ONTAPツールは VCF 管理クラスタにインストールされますが、VI ワークロード ドメインに関連付けられた vCenter に登録されます。

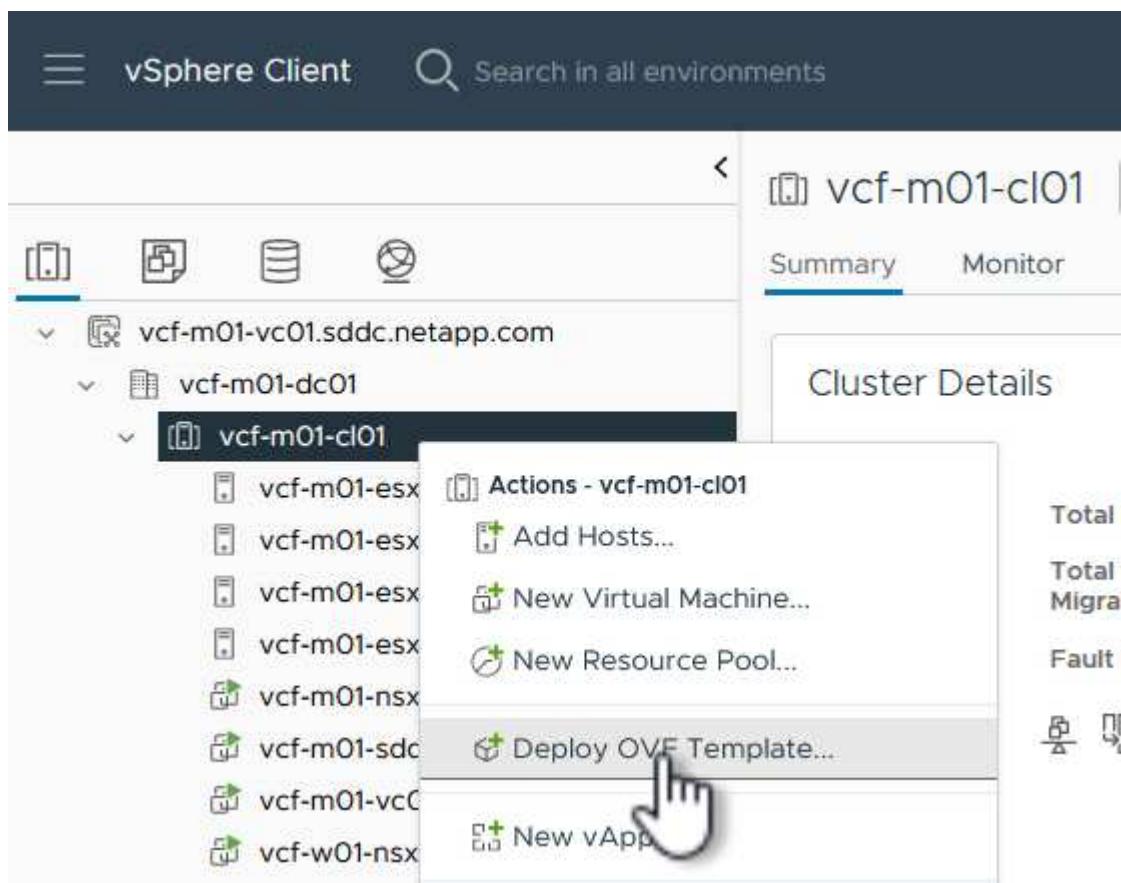
複数のvCenter環境でのONTAPツールの導入と使用に関する詳細については、以下を参照してください。["複数のvCenter Server環境でONTAP Toolsを登録するための要件"](#)。

ONTAP tools for VMware vSphereを導入する

ONTAP tools for VMware vSphereはVM アプライアンスとして導入され、ONTAPストレージを管理するための統合されたvCenter UIを提供します。

ONTAP tools for VMware vSphereをデプロイするには、次の手順を実行します。

1. ONTAPツールOVAイメージを以下から入手します。["NetApp サポート サイト"ローカルフォルダーにダウンロード](#)します。
2. VCF 管理ドメインの vCenter アプライアンスにログインします。
3. vCenter アプライアンス インターフェースから管理クラスタを右クリックし、[OVF テンプレートのデプロイ...]を選択します。



4. *OVF テンプレートのデプロイ*ウィザードで、*ローカル ファイル*ラジオ ボタンをクリックし、前の手順でダウンロードしたONTAPツール OVA ファイルを選択します。

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

Local file

UPLOAD FILES

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. ウィザードの手順 2～5 では、VM の名前とフォルダーを選択し、コンピューティング リソースを選択し、詳細を確認して、ライセンス契約に同意します。
6. 構成ファイルとディスク ファイルの保存場所として、VCF 管理ドメイン クラスタの vSAN データストアを選択します。

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format

As defined in the VM storage policy

VM Storage Policy

Datastore Default

Disable Storage DRS for this virtual machine

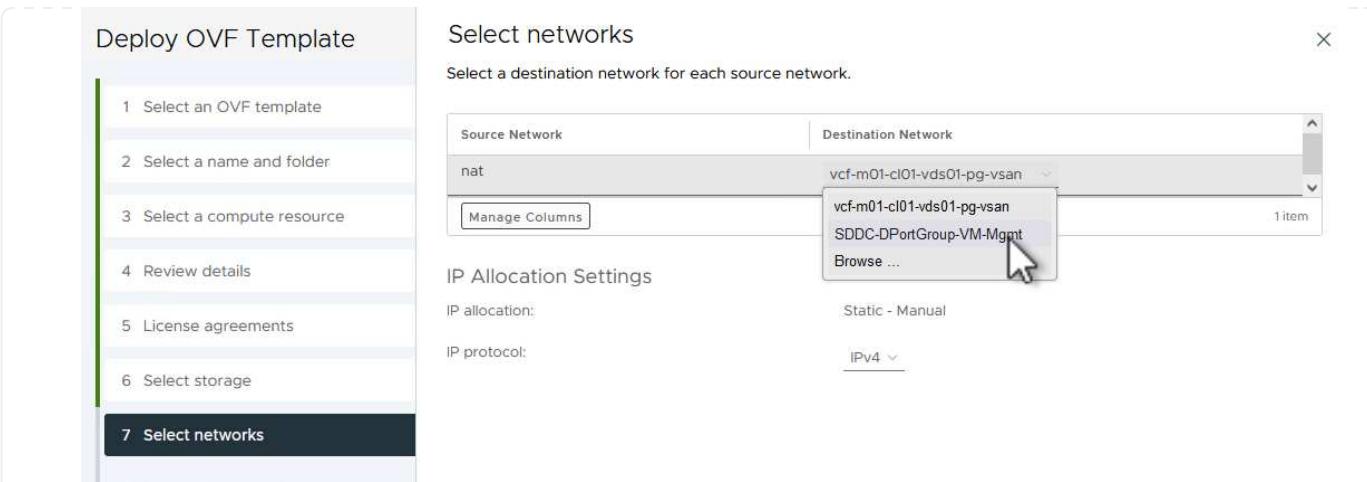
Name	Storage Compatibility	Capacity	Provisioned	Free	Total
<input checked="" type="radio"/> vcf-m01-cl01-ds-vsanc01	--	999.97 GB	7.17 TB	225.72 GB	v
<input type="radio"/> vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/> vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/> vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/> vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v

Manage Columns

Items per page 10 5 items

7. [ネットワークの選択] ページで、管理トラフィックに使用するネットワークを選択します。

X



8. テンプレートのカスタマイズページで、必要な情報をすべて入力します。

- ONTAPツールへの管理アクセスに使用するパスワード。
- NTPサーバのIPアドレスを指定します。
- ONTAPツールのメンテナンス アカウントのパスワード。
- ONTAP Tools Derby DB パスワード。
- **VMware Cloud Foundation (VCF)** を有効にする チェックボックスをオンにしないでください。
補助ストレージを展開する場合、VCF モードは必要ありません。
- VI ワークロード ドメイン の vCenter アプライアンスの FQDN または IP アドレス
- VI ワークロード ドメイン の vCenter アプライアンスの認証情報
- 必要なネットワーク プロパティ フィールドを指定します。

続行するには、[次へ] をクリックします。

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

1 2 properties have invalid values

System Configuration		4 settings
Application User Password (*)	Password to assign to the administrator account. For security reasons, it is recommended to use a password that is eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.	
	Password	*****
	Confirm Password	*****
NTP Servers		
A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used.		
172.21.166.1		
Maintenance User Password (*)		
Password to assign to maint user account.		
	Password	*****
	Confirm Password	*****

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Customize template

Configure vCenter or Enable VCF

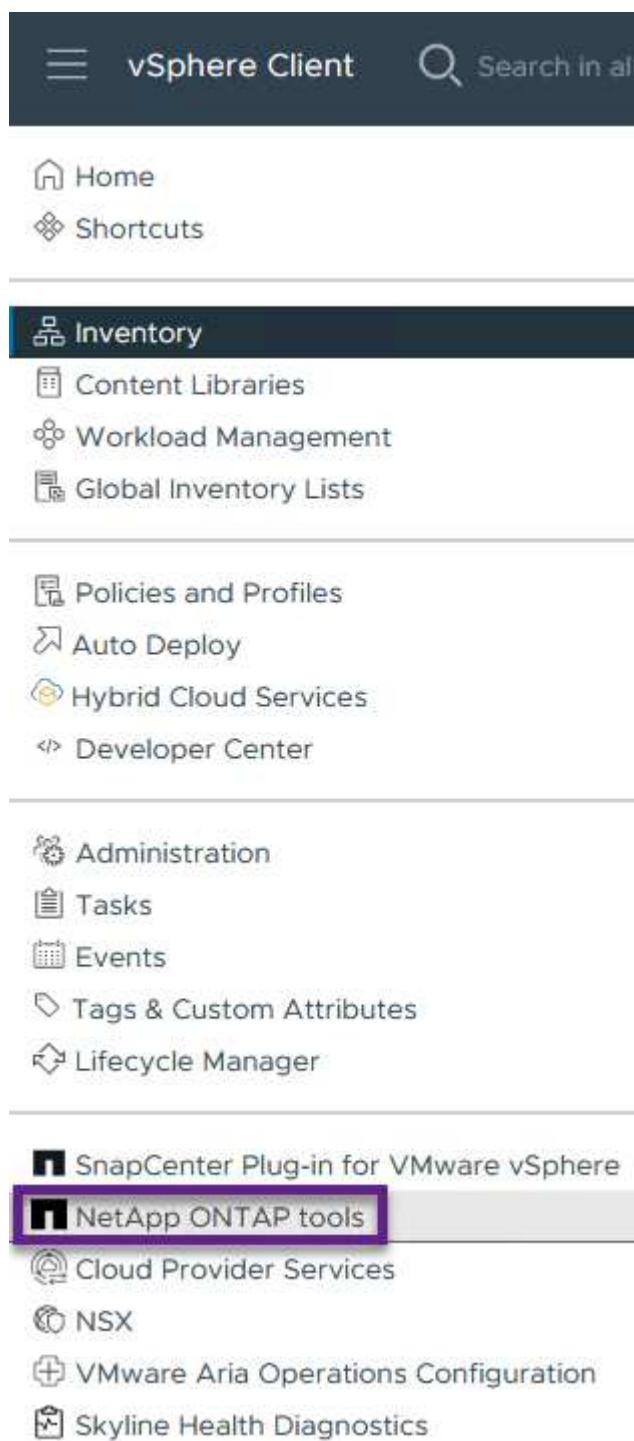
Enable VMware Cloud Foundation (VCF)		5 settings
Enable VMware Cloud Foundation (VCF)	vCenter server and user details are ignored when VCF is enabled.	
	<input type="checkbox"/>	
vCenter Server Address (*)	Specify the IP address/hostname of an existing vCenter to register to.	
	cf-wkld-vc01.sddc.netapp.com	
Port (*)	Specify the HTTPS port of an existing vCenter to register to.	
	443	
Username (*)	Specify the username of an existing vCenter to register to.	
	administrator@vsphere.local	
Password (*)	Specify the password of an existing vCenter to register to.	
	Password	*****
	Confirm Password	*****
Network Properties		
8 settings		
Host Name	Specify the hostname for the appliance. (Leave blank if DHCP is desired)	
	vcf-w01-otv9	
IP Address	Specify the IP address for the appliance. (Leave blank if DHCP is desired)	

CANCEL
BACK
NEXT

9. 「完了の準備」ページですべての情報を確認し、「完了」をクリックしてONTAP Tools アプライアンスの導入を開始します。

ONTAPツールにストレージ システムを追加します。

1. vSphere クライアントのメイン メニューから選択して、NetApp ONTAPツールにアクセスします。



2. ONTAPツール インターフェイスの **INSTANCE** ドロップダウン メニューから、管理対象のワークカード ドメインに関連付けられているONTAPツール インスタンスを選択します。

NetApp ONTAP tools INSTANCE 172.21.166.139:8443

Overview	Plugin Instance	Version	vCenter Server
Storage Systems	172.21.166.139:8443	9.13.0.36905	vcf-m01-vc01.sddc.netapp.com
Storage capability profile	172.21.166.149:8443	9.13.0.36905	vcf-wkld-vc01.sddc.netapp.com
Storage Mapping			
Settings			



3. ONTAPツールで、左側のメニューから ストレージ システム を選択し、追加 を押します。

Overview	Storage Systems
Storage Systems	ADD REDISCOVER ALL
Storage capability profile	

4. IP アドレス、ストレージ システムの資格情報、およびポート番号を入力します。検出プロセスを開始するには、[追加] をクリックします。



vVol には、SVM 認証情報ではなくONTAPクラスタ認証情報が必要です。詳細については、"ストレージシステムを追加する" ONTAPツールのドキュメント。

Add Storage System

i Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

vcf-m01-vc01.sddc.netapp.com ▾

Name or IP address:

172.16.9.25

Username:

admin

Password:

Port:

443

Advanced options ▾

ONTAP Cluster

Automatically fetch Manually upload

Certificate:

[CANCEL](#)

[SAVE & ADD MORE](#)

[ADD](#)

ONTAPツールでストレージ機能プロファイルを作成する

ストレージ機能プロファイルは、ストレージアレイまたはストレージシステムによって提供される機能を説明します。これらにはサービス品質の定義が含まれており、プロファイルで定義されたパラメータを満たすストレージシステムを選択するために使用されます。提供されているプロファイルの1つを使用することも、新しいプロファイルを作成することもできます。

ONTAPツールでストレージ機能プロファイルを作成するには、次の手順を実行します。

1. ONTAPツールで、左側のメニューからストレージ機能プロファイルを選択し、作成を押します。

The screenshot shows the vSphere Client interface. At the top, there is a search bar labeled "Search in all environments". Below it, the title "NetApp ONTAP tools INSTANCE 172.21.166.149:8443" is displayed. On the left, a sidebar menu has three items: "Overview", "Storage Systems", and "Storage capability profile", with "Storage capability profile" being the selected item. In the main content area, the title "Storage Capability Profiles" is shown above a "CREATE" button, which is highlighted with a blue border. To the right of the "CREATE" button is a "Name" input field.

2. *ストレージ機能プロファイルの作成* ウィザードで、プロファイルの名前と説明を入力し、*次へ*をクリックします。

The screenshot shows the "Create Storage Capability Profile" wizard. The left sidebar lists steps 1 through 6: 1 General, 2 Platform, 3 Protocol, 4 Performance, 5 Storage attributes, and 6 Summary. Step 1 General is currently selected and highlighted in grey. The main panel is titled "General" and contains the instruction "Specify a name and description for the storage capability profile." Below this, there are two fields: "Name:" with the value "Gold ASA iSCSI" entered, and "Description:" with an empty text area. At the bottom right of the panel are "CANCEL" and "NEXT" buttons.

3. プラットフォームタイプを選択し、ストレージシステムをオールフラッシュ SAN アレイに指定するには、**Asymmetric** を false に設定します。

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Platform

Platform: Performance

Asymmetric:

CANCEL BACK NEXT

This screenshot shows the 'Create Storage Capability Profile' wizard. The current step is '2 Platform'. On the right, there's a dropdown menu for 'Platform' with 'Performance' selected. Below it is a toggle switch for 'Asymmetric' which is turned on. At the bottom are standard navigation buttons: 'CANCEL', 'BACK', and 'NEXT'.

4. 次に、プロトコルを選択するか、すべての可能なプロトコルを許可するには「任意」を選択します。続行するには、[次へ] をクリックします。

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Protocol

Protocol: Any

Any
FCP
iSCSI
NVMe/FC

CANCEL BACK NEXT

This screenshot shows the 'Create Storage Capability Profile' wizard. The current step is '3 Protocol'. On the right, there's a dropdown menu for 'Protocol' with 'Any' selected. Below it is a list of protocol options: Any, FCP, iSCSI, and NVMe/FC. At the bottom are standard navigation buttons: 'CANCEL', 'BACK', and 'NEXT'.

5. パフォーマンス ページでは、許容される最小および最大の IOPS の形式でサービス品質を設定できます。

Create Storage Capability Profile

1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary

Performance

None ⓘ
 QoS policy group ⓘ

Min IOPS: _____

Max IOPS: 6000

Unlimited

CANCEL BACK NEXT

6. 必要に応じて、ストレージ効率、スペース予約、暗号化、階層化ポリシーを選択して、ストレージ属性ページを完了します。

Create Storage Capability Profile

1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary

Storage attributes

Deduplication: Yes ▾

Compression: Yes ▾

Space reserve: Thin ▾

Encryption: No ▾

Tiering policy (FabricPool): None ▾

CANCEL BACK NEXT

7. 最後に、概要を確認し、「完了」をクリックしてプロファイルを作成します。

Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary

Summary

Name:	ASA_Gold_iSCSI
Description:	N/A
Platform:	Performance
Asymmetric:	No
Protocol:	Any
Max IOPS:	6000 IOPS
Space reserve:	Thin
Deduplication:	Yes
Compression:	Yes
Encryption:	Yes
Tiering policy (FabricPool):	None

CANCEL

BACK

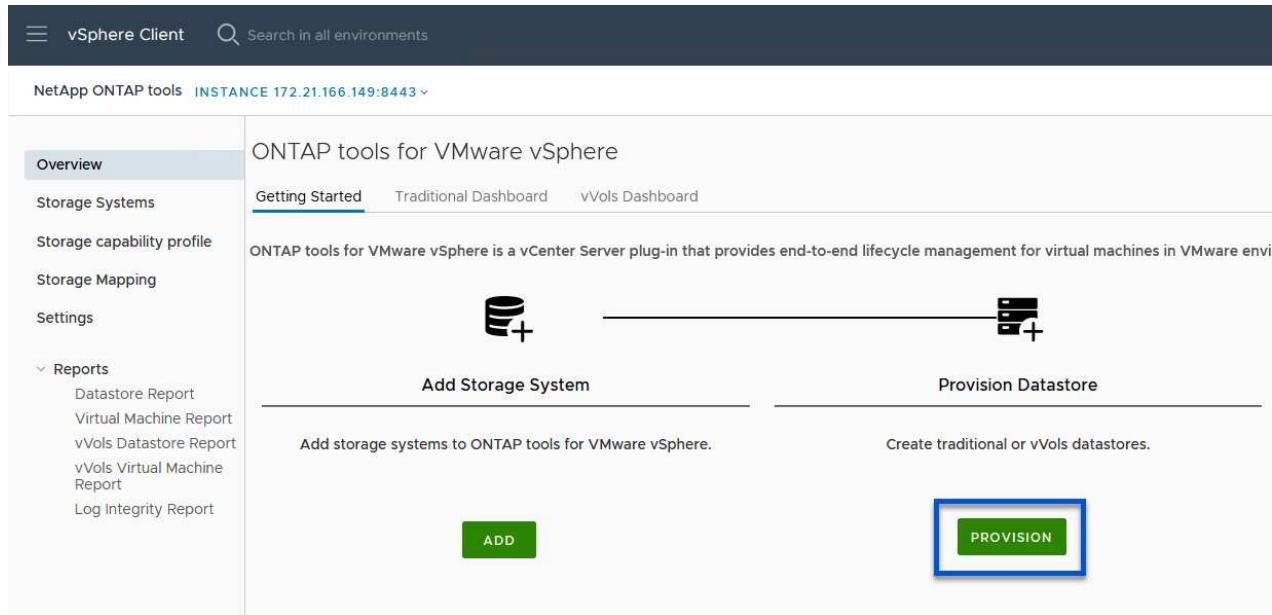
FINISH



ONTAPツールでvVolsデータストアを作成する

ONTAPツールでvVolsデータストアを作成するには、次の手順を実行します。

1. ONTAPツールで概要を選択し、開始タブからプロビジョニングをクリックしてウィザードを開始します。



vSphere Client Search in all environments

NetApp ONTAP tools INSTANCE 172.21.166.149:8443

Overview

Storage Systems

Storage capability profile

Storage Mapping

Settings

Reports

- Datastore Report
- Virtual Machine Report
- vVols Datastore Report
- vVols Virtual Machine Report
- Log Integrity Report

ONTAP tools for VMware vSphere

Getting Started Traditional Dashboard vVols Dashboard

ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware envi

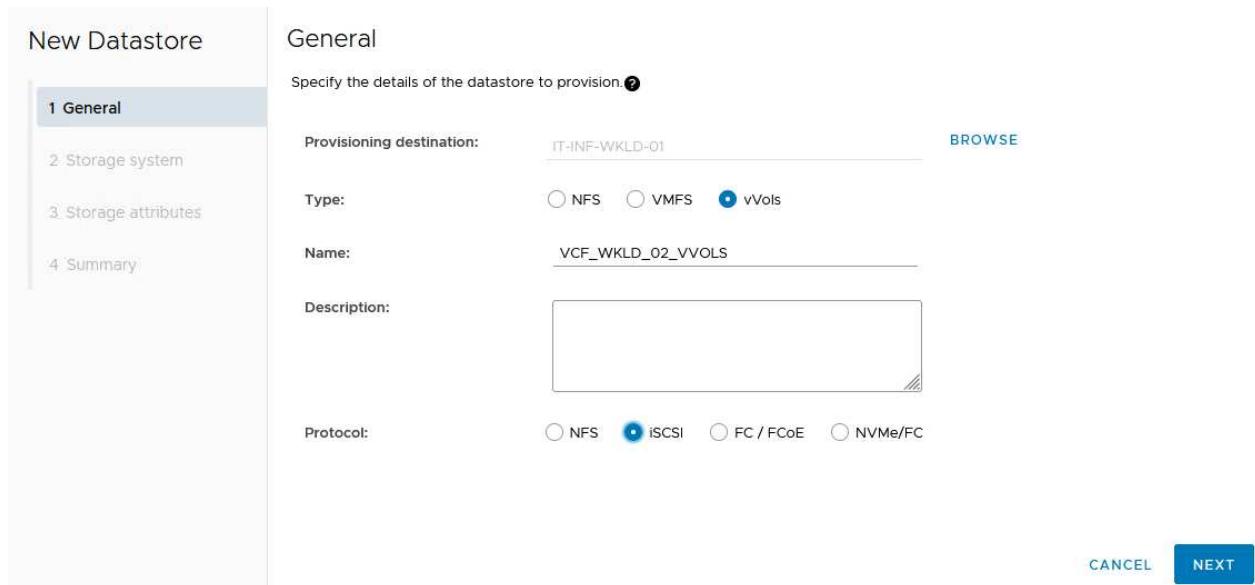
Add Storage System Provision Datastore

Add storage systems to ONTAP tools for VMware vSphere.

Create traditional or vVols datastores.

ADD PROVISION

2. 新しいデータストア ウィザードの全般ページで、vSphere データセンターまたはクラスターの宛先を選択します。データストアの種類として *vVols* を選択し、データストアの名前を入力して、プロトコルとして *iSCSI* を選択します。続行するには、[次へ] をクリックします。



New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

General

Specify the details of the datastore to provision. ?

Provisioning destination: IT-INF-WKLD-01 BROWSE

Type: NFS VMFS vVols

Name: VCF_WKLD_02_VVOLS

Description:

Protocol: NFS iSCSI FC / FCoE NVMe/FC

CANCEL NEXT

3. ストレージシステムページで、ストレージ機能プロファイル、ストレージシステム、および SVMを選択します。続行するには、[次へ] をクリックします。

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles:

- AFF_Encrypted_Min50_ASA_A
- FAS_Default
- FAS_Max20
- Custom profiles**
- ASA_Gold_iSCSI

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: VCF_iSCSI

CANCEL BACK NEXT

- ストレージ属性*ページで、データストアの新しいボリュームを作成することを選択し、作成するボリュームのストレージ属性を入力します。 *追加をクリックしてボリュームを作成し、次へをクリックして続行します。

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: Create new volumes Select volumes

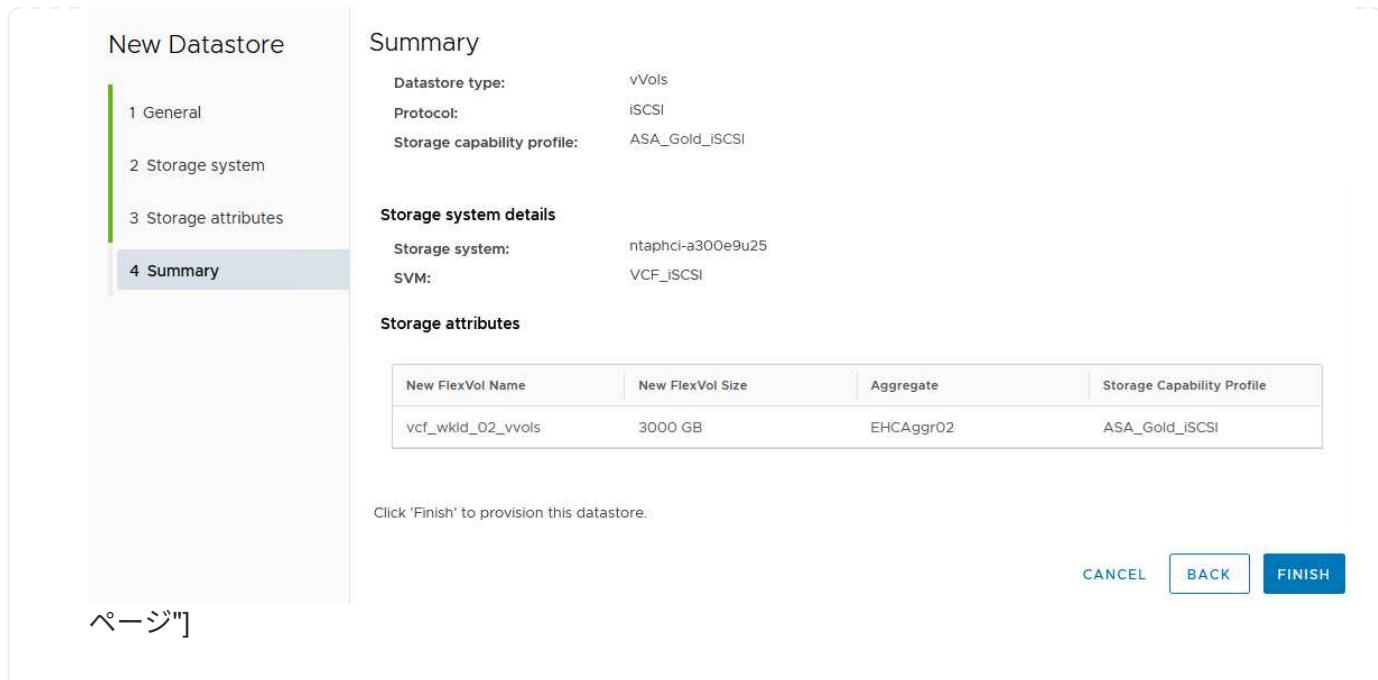
Create new volumes

Name	Size	Storage Capability Profile	Aggregate
 FlexVol volumes are not added.			
Name	Size(GB) ①	Storage capability profile	Aggregates
f_wkld_02_vvols	3000	ASA_Gold_iSCSI	EHCAggr02 - (27053.3 GB)

Space reserve: Thin

ADD CANCEL BACK NEXT

- 最後に、概要を確認し、「完了」をクリックして vVol データストアの作成プロセスを開始します。



ページ"]

追加情報

ONTAPストレージシステムの構成については、["ONTAP 9ドキュメント"](#)中心。

VCFの設定方法については、以下を参照してください。["VMware Cloud Foundation ドキュメント"](#)。

ONTAP tools for VMware vSphereを使用して、VI ワークロード ドメインに **NFS** と**vVols** を補助ストレージとして追加します。

このユースケースでは、ONTAP Tools for VMware を使用して、VMware Cloud Foundation (VCF) 仮想インフラストラクチャ (VI) ワークロード ドメインの補助ストレージとして NFS およびvVolsデータストアを追加する手順について説明します。この手順では、VMware vSphere 用のONTAPツールの導入、NFS 論理インターフェイスを使用したストレージ仮想マシン (SVM) の構成、NFS とvVols の両方のデータストアのプロビジョニングについてまとめています。

NFS は、vVolsデータストアのストレージプロトコルとして使用されます。

NFSの利点

シンプルさと使いやすさ: NFS はセットアップと管理が簡単なので、迅速かつ簡単なファイル共有を必要とする環境に最適です。

スケーラビリティ: ONTAP のアーキテクチャにより、NFS は効率的に拡張でき、インフラストラクチャに大きな変更を加えることなく増大するデータニーズに対応できます。

柔軟性: NFS は幅広いアプリケーションとワークロードをサポートしており、仮想化環境を含むさまざまなユースケースに幅広く対応できます。

詳細については、["vSphere 8 向け NFS v3 リファレンス ガイド"](#)。

シナリオの概要

このシナリオでは、次の大まかな手順について説明します。

- NFS トラフィック用の論理インターフェイス (LIF) を備えたストレージ仮想マシン (SVM) を作成します。
- VI ワークロード ドメイン上の NFS ネットワーク用の分散ポート グループを作成します。
- VI ワークロード ドメインの ESXi ホスト上に NFS 用の vmkernel アダプタを作成します。
- VI ワークロード ドメインにONTAPツールを導入します。
- VI ワークロード ドメインに新しい NFS データストアを作成します。
- VI ワークロード ドメインに新しいvVolsデータストアを作成します。

前提条件

このシナリオには、次のコンポーネントと構成が必要です。

- ストレージ トラフィック専用のイーサネット スイッチ上に物理データ ポートを備えたONTAP AFFまたはFASストレージシステム。
- VCF 管理ドメインの展開が完了し、vSphere クライアントにアクセスできるようになりました。
- VI ワークロード ドメインは以前にデプロイされています。

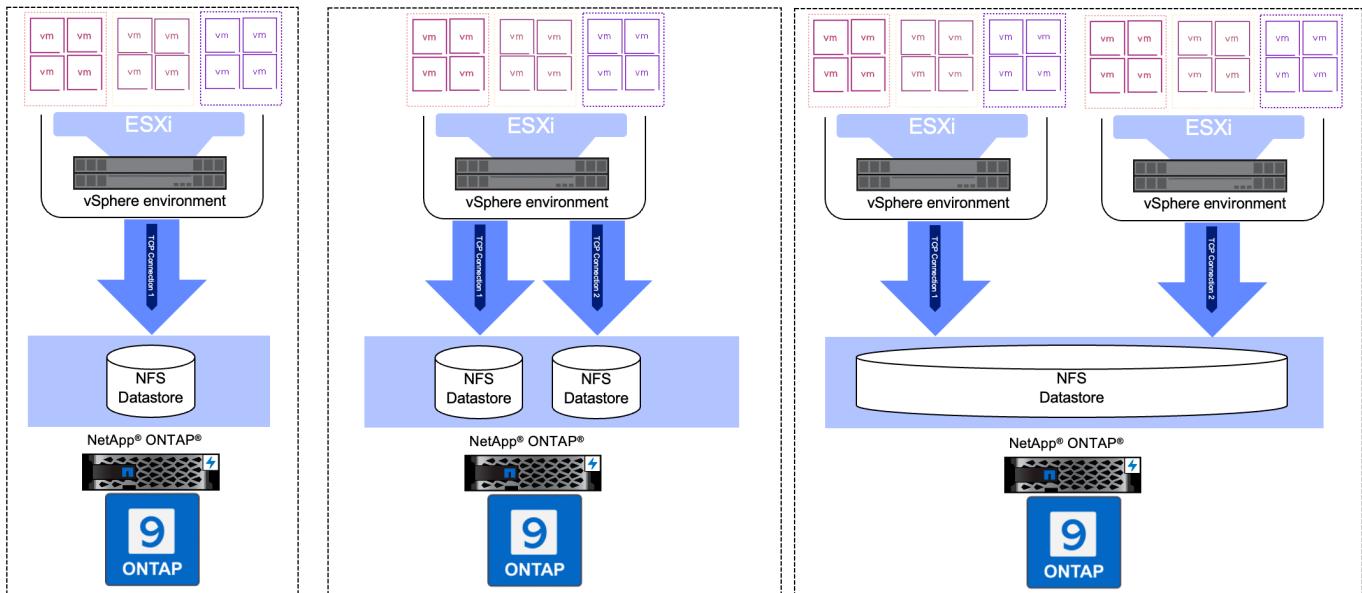
NetApp は、ストレージ システム、スイッチ、ネットワーク アダプタ、およびホスト システムにフォールト トレランスを提供する、NFS 用の冗長ネットワーク設計を推奨しています。アーキテクチャの要件に応じて、単一のサブネットまたは複数のサブネットで NFS を展開するのが一般的です。

参照 ["VMware vSphere で NFS を実行するためのベストプラクティス"](#)VMware vSphere に固有の詳細情報。

ONTAPをVMware vSphereで使用する場合のネットワークガイダンスについては、["ネットワーク構成 - NFS"](#) NetAppエンタープライズ アプリケーションドキュメントのセクション。

このドキュメントでは、新しい SVM を作成し、IP アドレス情報を指定して NFS トラフィック用の複数の LIF を作成するプロセスについて説明します。既存のSVMに新しいLIFを追加するには、["LIF \(ネットワークインターフェイス\) の作成"](#)。

vSphereクラスタでNFSを使用する方法の詳細については、["vSphere 8 向け NFS v3 リファレンス ガイド"](#)。



展開手順

ONTAPツールを導入し、それを使用してVCF管理ドメインにvVolsおよびNFSデータストアを作成するには、次の手順を実行します。

ONTAPストレージシステム上にSVMとLIFを作成する

次の手順はONTAP System Managerで実行されます。

ストレージVMとLIFを作成する

NFS トラフィック用の複数の LIF とともに SVM を作成するには、次の手順を実行します。

1. ONTAP System Manager から、左側のメニューの **Storage VMs** に移動し、**+ Add** をクリックして開始します。

The screenshot shows the ONTAP System Manager interface. The left sidebar has a 'Storage' section with various sub-options like Overview, Volumes, LUNs, etc., and 'Storage VMs' is currently selected. The main panel title is 'Storage VMs' and features a prominent blue button labeled '+ Add'. Below this button is a table with a header row containing a checkbox and the column title 'Name'. Eight entries are listed in the table: EHC_iSCSI, EHC, HMC_187, HMC_3510, HMC_iSCSI_3510, infra_svm_a300, JS_EHC_iSCSI, and OTVtest.

2. ストレージ VM の追加 ウィザードで、SVM の名前を入力し、IP スペースを選択して、アクセスプロトコルの下で **SMB/CIFS**、**NFS**、**S3** タブをクリックし、**NFS** を有効にする チェックボックスをオンにします。

Add Storage VM

X

STORAGE VM NAME

VCF_NFS

IPSPACE

Default



Access Protocol

SMB/CIFS, NFS, S3

iSCSI FC NVMe

Enable SMB/CIFS

Enable NFS

Allow NFS client access

⚠ Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

Enable S3

DEFAULT LANGUAGE [?](#)

c.utf_8



Ontap Tools for VMware vSphere を使用してデータストアの展開プロセスを自動化するため、ここで **NFS** クライアント アクセスを許可する ボタンをチェックする必要はありません。これには、ESXi ホストへのクライアント アクセスの提供が含まれます。

3. ネットワーク インターフェイス セクションで、最初の LIF の IP アドレス、サブネット マスク、および ブロードキャスト ドメインとポートを入力します。後続の LIF については、チェックボックスを有効にして、残りのすべての LIF で共通の設定を使用するか、個別の設定を使用するかを選択できます。

NETWORK INTERFACE
Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET

Without a subnet			
IP ADDRESS	SUBNET MASK	GATEWAY	BROADCAST DOMAIN AND PORT
172.21.118.119	24	Add optional gateway	NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

ntaphci-a300-02

SUBNET

Without a subnet		
IP ADDRESS	PORT	
172.21.118.120	a0a-3374	

4. ストレージ VM 管理アカウント (マルチテナント環境の場合) を有効にするかどうかを選択し、[保存] をクリックして SVM を作成します。

Storage VM Administration

Manage administrator account

Save

[Cancel](#)

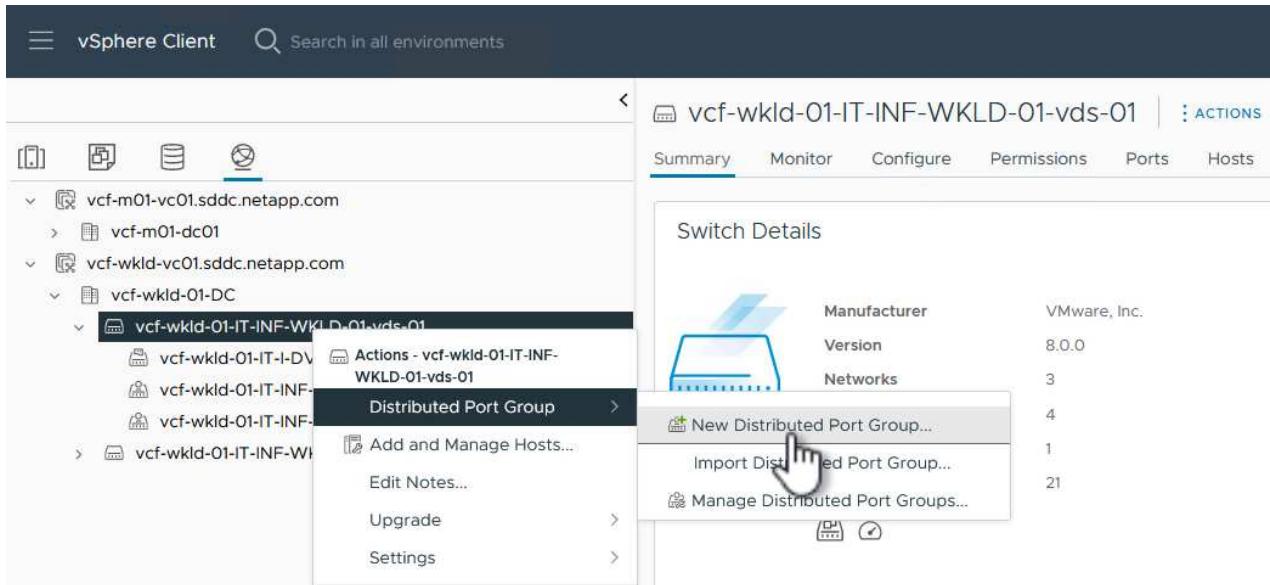
ESXiホスト上のNFSネットワークを設定する

次の手順は、vSphere クライアントを使用して VI ワークロード ドメイン クラスタで実行されます。この場合、vCenter Single Sign-On が使用されているため、vSphere クライアントは管理ドメインとワークロード ドメイン全体で共通になります。

NFS トラフィック用の分散ポートグループを作成する

NFS トラフィックを伝送するネットワークの新しい分散ポート グループを作成するには、次の手順を実行します。

1. vSphere クライアントから、ワークロード ドメインの インベントリ > ネットワーク に移動します。既存の分散スイッチに移動し、*新しい分散ポート グループ...*を作成するアクションを選択します。



2. 新しい分散ポート グループ ウィザードで、新しいポート グループの名前を入力し、次へ をクリックして続行します。
3. *設定の構成*ページですべての設定を入力します。 VLAN が使用されている場合は、正しい VLAN ID を必ず指定してください。 続行するには、[次へ] をクリックします。

New Distributed Port Group

1 Name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding: Static binding

Port allocation: Elastic (i)

Number of ports: 8

Network resource pool: (default)

VLAN

VLAN type: VLAN

VLAN ID: 3374

Advanced

Customize default policies configuration

CANCEL BACK NEXT 

vSphere Client Search in all environments

vcf-wkld-01-nfs | : ACTIONS

Summary Monitor Configure Peri

Distributed Port Group Details

Port binding
Port allocation
VLAN ID
Distributed switch
Network protocol profile
Network resource pool
Hosts
Virtual machines

Actions - vcf-wkld-01-nfs

Edit Settings... Export Configuration...

vcf-m01-vc01.sddc.netapp.com
vcf-wkld-vc01.sddc.netapp.com
vcf-wkld-01-DC
vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-iscsi-a
vcf-wkld-01-iscsi-b
vcf-wkld-01-IT-I-DVUplinks-10
vcf-wkld-01-IT-INF-WKLD-01-vds-01-...
vcf-wkld-01-IT-INF-WKLD-01-vds-01-...
vcf-wkld-01-nfs
vcf-wkld-01-nvm
vcf-wkld-01-nvm
vcf-wkld-01-IT-INF-

6. 分散ポートグループ - 設定の編集ページで、左側のメニューのチーミングとフェールオーバーに移動します。NFS トラフィックに使用するアップリンクのチーミングを有効にするには、アップリンクがアクティブ アップリンク領域にまとめられていることを確認します。使用されていないアップリンクを「未使用的アップリンク」に移動します。

Distributed Port Group - Edit Settings | vcf-wkld-01-nfs

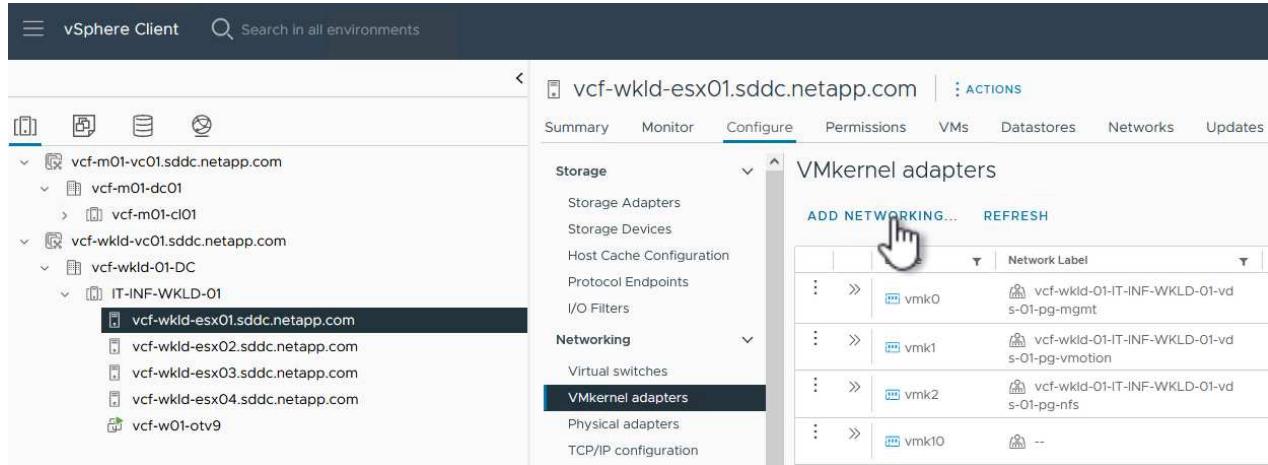
General	Load balancing	Route based on originating virtual port
Advanced	Network failure detection	Link status only
VLAN	Notify switches	Yes
Security	Failback	Yes
Traffic shaping		
Teaming and failover		
Monitoring	Failover order ⓘ	
Miscellaneous	MOVE UP MOVE DOWN	
Active uplinks		
<input type="checkbox"/> uplink2		
<input type="checkbox"/> uplink1		
Standby uplinks		
Unused uplinks		

7. クラスタ内の各 ESXi ホストに対してこのプロセスを繰り返します。

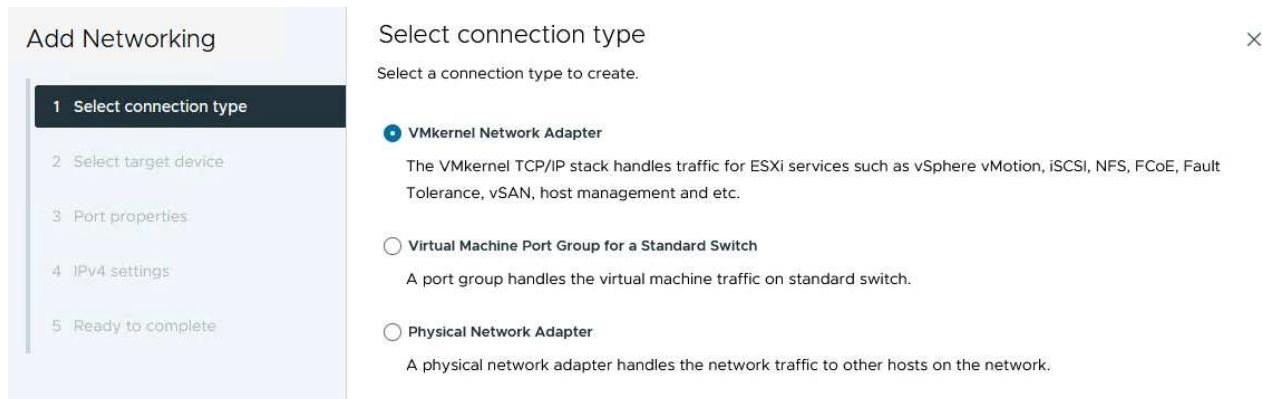
各ESXiホストにVMkernelアダプタを作成する

ワークロード ドメイン内の各 ESXi ホストでこのプロセスを繰り返します。

1. vSphere クライアントから、ワークロード ドメイン インベントリ内の ESXi ホストの 1 つに移動します。*構成*タブから*VMkernelアダプタ*を選択し、*ネットワークの追加...*をクリックして開始します。



2. 接続タイプの選択 ウィンドウで **VMkernel** ネットワーク アダプタを選択し、次へをクリックして続行します。



3. ターゲット デバイスの選択 ページで、以前に作成した NFS の分散ポート グループの 1 つを選択します。

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

Select an existing network
 Select an existing standard switch
 New standard switch

Quick Filter

Name	NSX Port Group ID	Distributed Switch
vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input checked="" type="radio"/> vcf-wkld-01-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

8 items

CANCEL BACK NEXT

4. ポート プロパティ ページでデフォルト (有効なサービスなし) を維持し、次へ をクリックして続行します。
5. **IPv4** 設定 ページで、IP アドレス、サブネット マスクを入力し、新しいゲートウェイ IP アドレスを指定します (必要な場合のみ)。続行するには、[次へ] をクリックします。

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically
 Use static IPv4 settings

IPv4 address

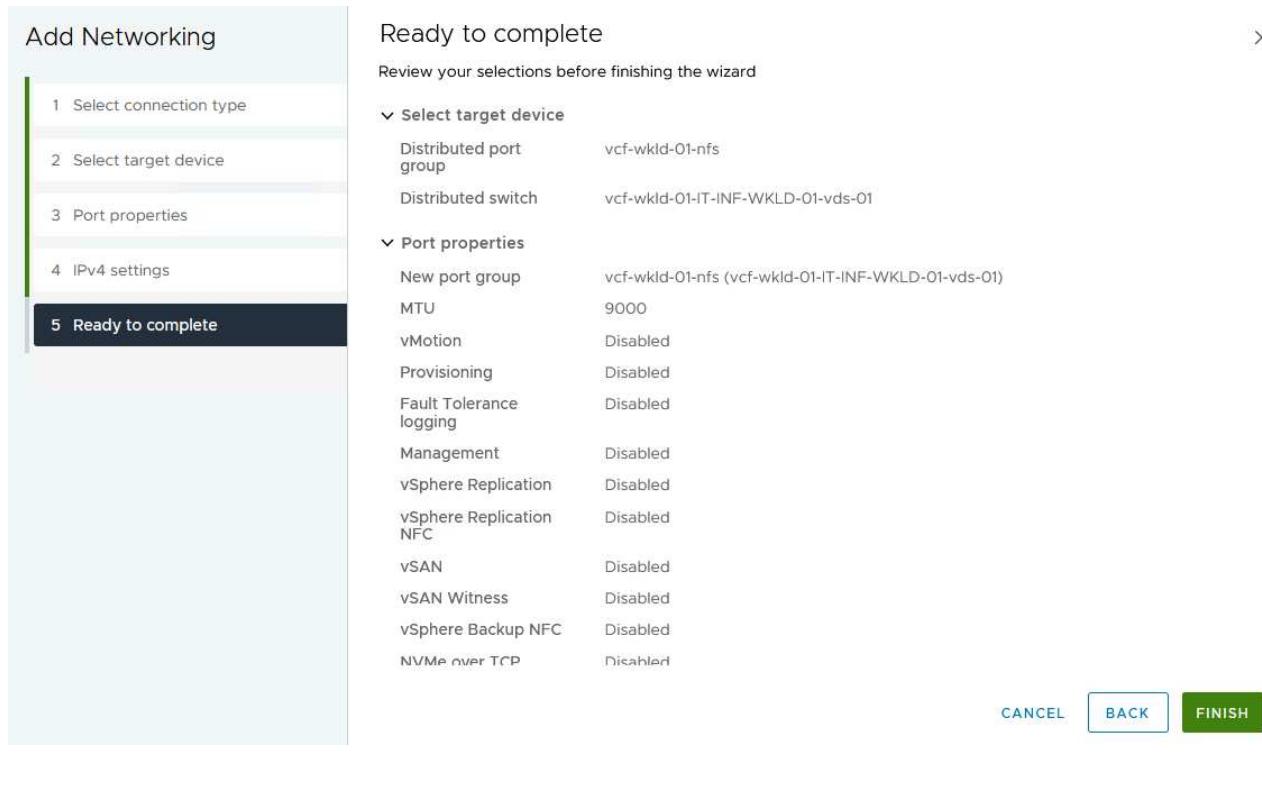
Subnet mask

Default gateway Override default gateway for this adapter

DNS server addresses

CANCEL BACK NEXT

6. *準備完了*ページで選択内容を確認し、*完了*をクリックして VMkernel アダプタを作成します。



ONTAPツールを導入して使用し、ストレージを構成する

次の手順は、vSphere クライアントを使用して VCF 管理ドメイン クラスタ上で実行され、OTV の展開、vVols NFS データストアの作成、管理 VM の新しいデータストアへの移行が含まれます。

VI ワークロード ドメインの場合、OTV は VCF 管理クラスタにインストールされますが、VI ワークロード ドメインに関連付けられた vCenter に登録されます。

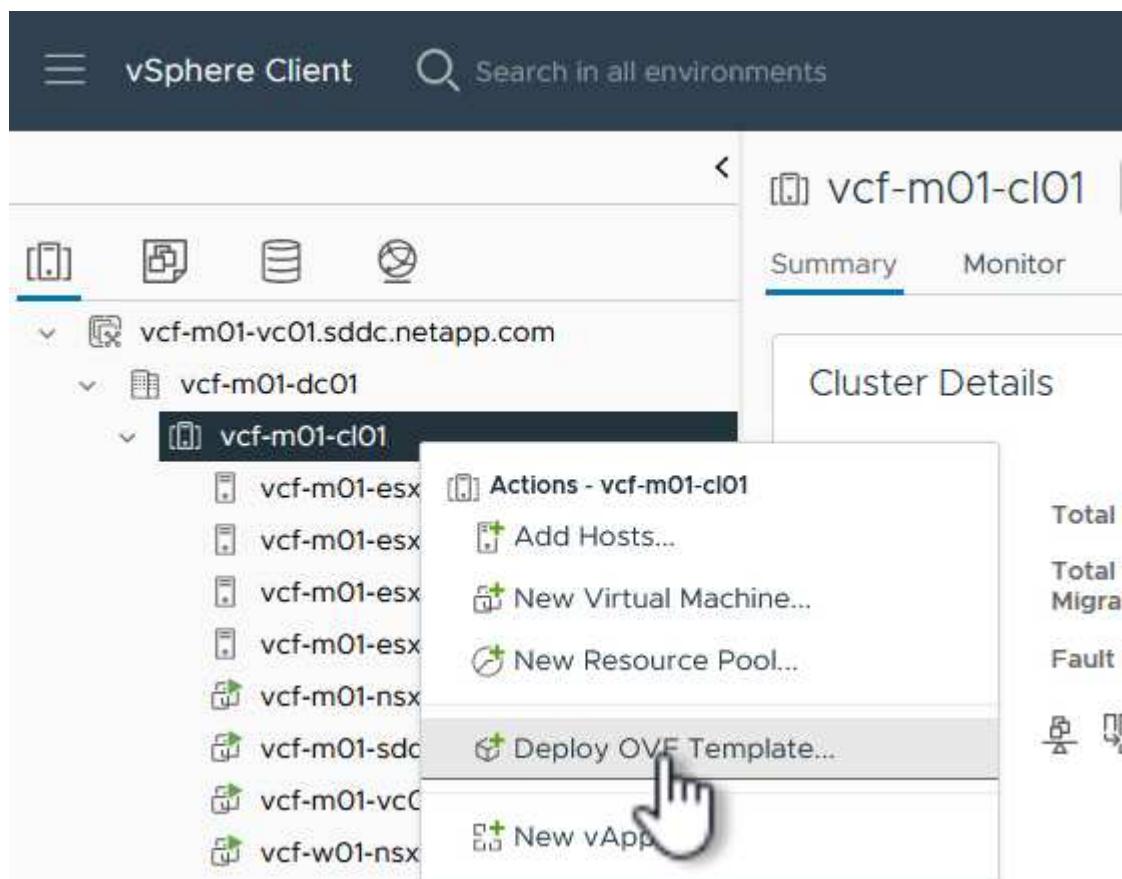
複数のvCenter環境でのONTAPツールの導入と使用に関する詳細については、以下を参照してください。["複数のvCenter Server環境でONTAP Toolsを登録するための要件"](#)。

ONTAP tools for VMware vSphereを導入する

ONTAP tools for VMware vSphereは、VMアプライアンスとして導入され、ONTAPストレージを管理するための統合されたvCenter UIを提供します。

ONTAP tools for VMware vSphereをデプロイするには、次の手順を実行します。

1. ONTAPツールOVAイメージを以下から入手します。["NetApp サポート サイト"ローカルフォルダーにダウンロード](#)します。
2. VCF 管理ドメインの vCenter アプライアンスにログインします。
3. vCenter アプライアンス インターフェースから管理クラスタを右クリックし、[OVF テンプレートのデプロイ...]を選択します。



4. *OVF テンプレートのデプロイ*ウィザードで、*ローカル ファイル*ラジオ ボタンをクリックし、前の手順でダウンロードしたONTAPツール OVA ファイルを選択します。

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

http | https://remoteserver-address/filetodeploy.ovf|.ova

Local file

UPLOAD FILES

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. ウィザードの手順 2～5 では、VM の名前とフォルダーを選択し、コンピューティング リソースを選択し、詳細を確認して、ライセンス契約に同意します。
6. 構成ファイルとディスク ファイルの保存場所として、VCF 管理ドメイン クラスタの vSAN データストアを選択します。

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format

As defined in the VM storage policy

VM Storage Policy

Datastore Default

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	Total
vcf-m01-cl01-ds-vsanc01	--	999.97 GB	7.17 TB	225.72 GB	999.97 GB
vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	25.75 GB
vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	25.75 GB
vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	25.75 GB
vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	25.75 GB

Manage Columns

Items per page 10 5 items

7. [ネットワークの選択] ページで、管理トラフィックに使用するネットワークを選択します。

X

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks**

Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	vcf-m01-cl01-vds01-pg-vsan

Manage Columns

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

vcf-m01-cl01-vds01-pg-vsan
SDDC-DPortGroup-VM-Mgmt
Browse ...

8. テンプレートのカスタマイズページで、必要な情報をすべて入力します。

- OTVへの管理アクセスに使用するパスワード。
- NTPサーバのIPアドレスを指定します。
- OTVメンテナンスアカウントのパスワード。
- OTVダービーDBパスワード。
- VMware Cloud Foundation (VCF)**を有効にするチェックボックスをオンにしないでください。補助ストレージを展開する場合、VCFモードは必要ありません。
- VIワークロードドメインのvCenterアプライアンスのFQDNまたはIPアドレス
- VIワークロードドメインのvCenterアプライアンスの認証情報
- 必要なネットワークプロパティフィールドを指定します。

続行するには、[次へ]をクリックします。

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

1 2 properties have invalid values X

System Configuration		4 settings
Application User Password (*)	Password to assign to the administrator account. For security reasons, it is recommended to use a password that is eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.	
	Password	*****
	Confirm Password	*****
NTP Servers		
A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. 172.21.166.1		
Maintenance User Password (*)		
Password to assign to maint user account.		
	Password	*****
	Confirm Password	*****

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Customize template

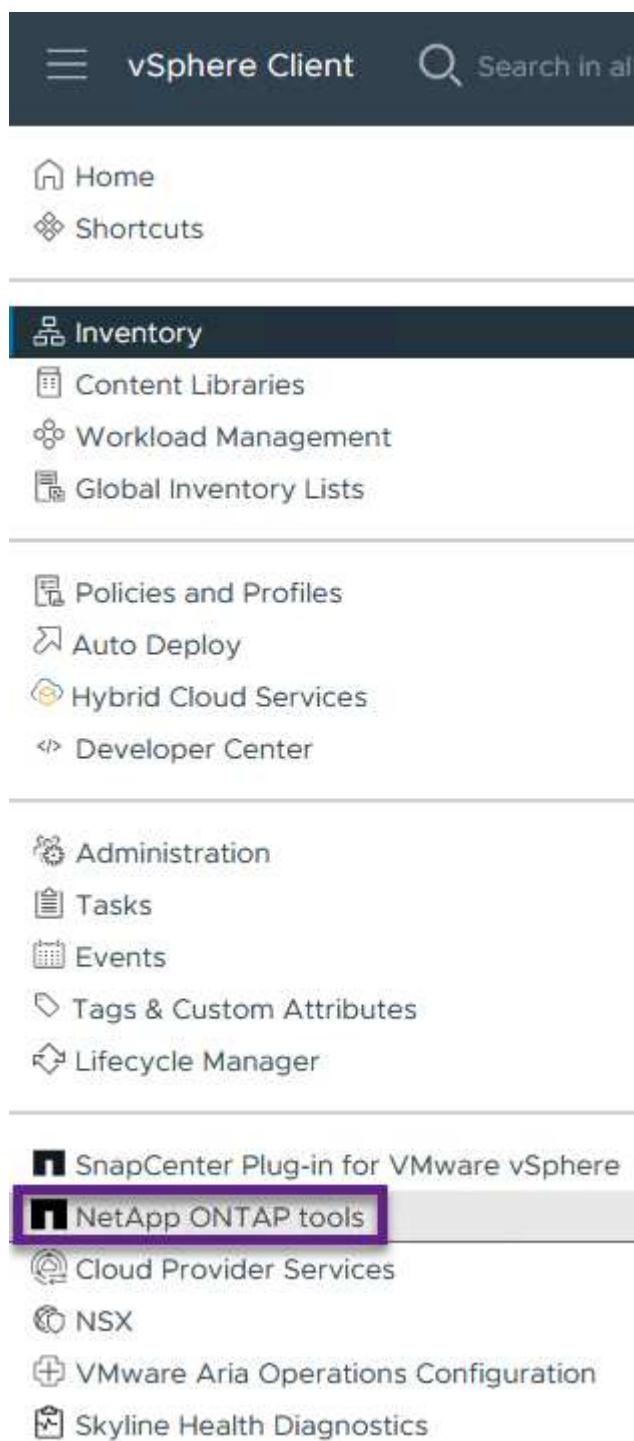
Configure vCenter or Enable VCF X

Configure vCenter or Enable VCF		5 settings
Enable VMware Cloud Foundation (VCF)	vCenter server and user details are ignored when VCF is enabled. □	
vCenter Server Address (*)	Specify the IP address/hostname of an existing vCenter to register to. cf-wkld-vc01.sddc.netapp.com	
Port (*)	Specify the HTTPS port of an existing vCenter to register to. 443	
Username (*)	Specify the username of an existing vCenter to register to. administrator@vsphere.local	
Password (*)	Specify the password of an existing vCenter to register to.	
	Password	*****
	Confirm Password	*****
Network Properties		
Host Name	Specify the hostname for the appliance. (Leave blank if DHCP is desired) vcf-w01-otv9	
IP Address	Specify the IP address for the appliance. (Leave blank if DHCP is desired)	

9. [Ready to complete] ページですべての情報を確認し、[Finish] をクリックして OTV アプライアンスの展開を開始します。

ONTAPツールにストレージ システムを追加します。

1. vSphere クライアントのメイン メニューから選択して、NetApp ONTAPツールにアクセスします。



2. ONTAPツール インターフェイスの **INSTANCE** ドロップダウン メニューから、管理対象のワークカード ドメインに関連付けられている OTV インスタンスを選択します。

	Plugin Instance	Version	vCenter Server
Storage Systems	172.21.166.139:8443	9.13.0.36905	vcf-m01-vc01.sddc.netapp.com
Storage capability profile	172.21.166.149:8443	9.13.0.36905	vcf-wkld-vc01.sddc.netapp.com
Storage Mapping			
Settings			

3. ONTAPツールで、左側のメニューから ストレージ システム を選択し、追加 を押します。

	Storage Systems
Overview	
Storage Systems	ADD
Storage capability profile	

4. IP アドレス、ストレージ システムの資格情報、およびポート番号を入力します。検出プロセスを開始するには、[追加] をクリックします。

Add Storage System

i Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

vcf-m01-vc01.sddc.netapp.com ▾

Name or IP address:

172.16.9.25

Username:

admin

Password:

Port:

443

Advanced options ▾

ONTAP Cluster

Automatically fetch Manually upload

Certificate:

[CANCEL](#)

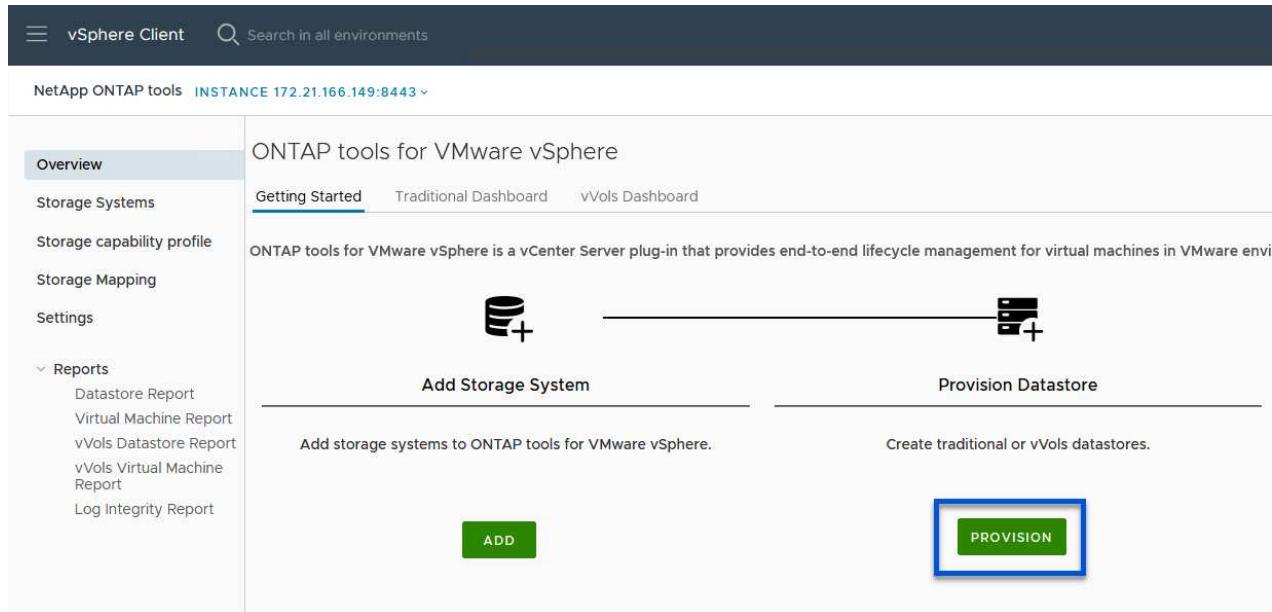
[SAVE & ADD MORE](#)

[ADD](#)

ONTAPツールでNFSデータストアを作成する

ONTAPツールを使用して NFS 上で実行されるONTAPデータストアを展開するには、次の手順を実行します。

1. ONTAPツールで 概要 を選択し、開始 タブから プロビジョニング をクリックしてウィザードを開始します。



2. 新しいデータストア ウィザードの 全般 ページで、vSphere データセンターまたはクラスターの宛先を選択します。データストアの種類として **NFS** を選択し、データストアの名前を入力して、プロトコルを選択します。FlexGroupボリュームを使用するかどうか、およびプロビジョニングにストレージ機能ファイルを使用するかどうかを選択します。続行するには、[次へ] をクリックします。

注意: データストア データをクラスター全体に分散 を選択すると、基盤となるボリュームがFlexGroupボリュームとして作成され、ストレージ機能プロファイルの使用ができなくなります。参照 "FlexGroupボリュームでサポートされる機能とサポートされない機能" FlexGroupボリュームの使用に関する詳細については、こちらをご覧ください。

New Datastore

General

Specify the details of the datastore to provision. ?

1 General 2 Storage system 3 Storage attributes 4 Summary

Provisioning destination:	vcf-wkld-01-DC	BROWSE
Type:	<input checked="" type="radio"/> NFS <input type="radio"/> VMFS <input type="radio"/> vVols	
Name:	VCF_WKLD_05_NFS	
Size:	2	TB
Protocol:	<input checked="" type="radio"/> NFS 3 <input type="radio"/> NFS 4.1	
<input type="checkbox"/> Distribute datastore data across the ONTAP cluster.		
<input checked="" type="checkbox"/> Use storage capability profile for provisioning		
Advanced options >		
		CANCEL NEXT

3. ストレージシステムページで、ストレージ機能プロファイル、ストレージシステム、および SVM を選択します。続行するには、[次へ] をクリックします。

New Datastore

Storage system

Specify the storage capability profiles and the storage system you want to use.

1 General 2 Storage system 3 Storage attributes 4 Summary

Storage capability profile:	Platinum_AFF_A
Storage system:	ntaphci-a300e9u25 (172.16.9.25)
Storage VM:	VCF_NFS

4. *ストレージ属性*ページで、使用するアグリゲートを選択し、*次へ*をクリックして続行します。

New Datastore

Storage attributes

Specify the storage details for provisioning the datastore.

1 General 2 Storage system 3 Storage attributes 4 Summary

Aggregate:	EHCAGgr02 - (25350.17 GB Free)
Volumes:	Automatically creates a new volume.
Advanced options >	

5. 最後に、*概要*を確認し、「完了」をクリックして NFS データストアの作成を開始します。

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Summary

General

vCenter server:	vcf-wkld-vc01.sddc.netapp.com
Provisioning destination:	vcf-wkld-01-DC
Datastore name:	VCF_WKLD_05_NFS
Datastore size:	2 TB
Datastore type:	NFS
Protocol:	NFS 3
Datastore cluster:	None
Storage capability profile:	Platinum_AFF_A

Storage system details

Storage system:	ntaphci-a300e9u25
SVM:	VCF_NFS

Storage attributes

Access control:	FHCAaar02
-----------------	-----------

CANCEL

BACK

FINISH

ONTAPツールでvVolsデータストアを作成する

ONTAPツールでvVolsデータストアを作成するには、次の手順を実行します。

1. ONTAPツールで概要を選択し、開始タブからプロビジョニングをクリックしてウィザードを開始します。

The screenshot shows the vSphere Client interface with the ONTAP tools for VMware vSphere plugin. The left sidebar has a 'Reports' section expanded, showing options like Datastore Report, Virtual Machine Report, vVols Datastore Report, vVols Virtual Machine Report, and Log Integrity Report. The main area displays the 'Getting Started' page for ONTAP tools, which includes sections for 'Add Storage System' and 'Provision Datastore'. The 'Provision Datastore' section contains a green 'ADD' button and a blue 'PROVISION' button, which is highlighted with a blue box.

2. 新しいデータストア ウィザードの全般ページで、vSphere データセンターまたはクラスターの宛先を選択します。データストアの種類として * vVols* を選択し、データストアの名前を入力して、プロトコルとして * NFS * を選択します。続行するには、[次へ] をクリックします。

The screenshot shows the 'General' step of the 'New Datastore' wizard. The left sidebar lists steps 1 through 4. Step 1, 'General', is selected. The main form fields are: 'Provisioning destination:' (vcf-wkld-01-DC), 'Type:' (radio button selected for 'vVols'), 'Name:' (VCF_WKLD_06_VVOLS_NFS), 'Description:' (empty text area), and 'Protocol:' (radio button selected for 'NFS'). At the bottom right are 'CANCEL' and 'NEXT' buttons, with 'NEXT' being highlighted.

3. ストレージシステムページで、ストレージ機能プロファイル、ストレージシステム、および SVMを選択します。続行するには、[次へ] をクリックします。

New Datastore

- 1 General
- 2 Storage system**
- 3 Storage attributes
- 4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profile:	Platinum_AFF_A
Storage system:	ntaphci-a300e9u25 (172.16.9.25)
Storage VM:	VCF_NFS

4. ストレージ属性*ページで、データストアの新しいボリュームを作成することを選択し、作成するボリュームのストレージ属性を入力します。*追加をクリックしてボリュームを作成し、次へをクリックして続行します。

Name	Size(GB) ①	Storage capability profile	Aggregates	Space reserve
vcf_wkld_06_vvols	2000	Platinum_AFF_A	EHCAGgr02 - (25404 GB)	Thin

ADD

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes**
- 4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: Create new volumes Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
vcf_wkld_06_vvols	2000 GB	Platinum_AFF_A	EHCAGgr02

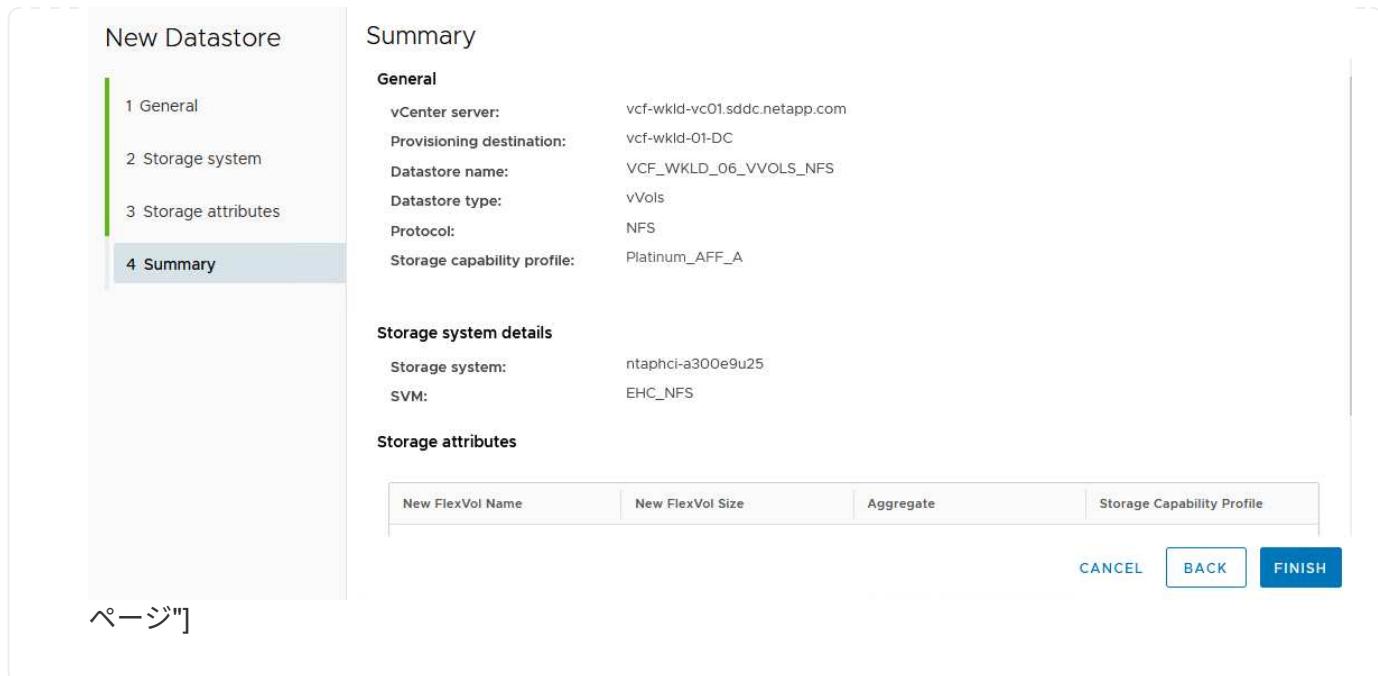
1 - 1 of 1 item

Name	Size(GB) ①	Storage capability profile	Aggregates	Space reserve
		Platinum_AFF_A	EHCAGgr02 - (25407.15 G)	Thin

Default storage capability profile: Platinum_AFF_A

CANCEL BACK NEXT

5. 最後に、*概要*を確認し、*完了*をクリックして vVol データストアの作成プロセスを開始します。



追加情報

ONTAPストレージシステムの構成については、["ONTAP 9ドキュメント"](#)中心。

VCFの設定方法については、以下を参照してください。["VMware Cloud Foundation ドキュメント"](#)。

VIワークロードドメインに補助ストレージとしてNVMe over TCPを追加する

このユースケースでは、ONTAP Tools for VMware を使用して、NVMe over TCP (NVMe/TCP) を VMware Cloud Foundation (VCF) 仮想インフラストラクチャ (VI) ワークロード ドメインの補助ストレージとして構成する手順について説明します。この手順では、NVMe/TCP 対応のストレージ仮想マシン (SVM) のセットアップ、NVMe 名前空間の作成、ESXi ホスト ネットワークの構成、および VMFS データストアの展開についてまとめています。

NVMe over TCPの利点

高性能: 低レイテンシと高データ転送速度で優れたパフォーマンスを実現します。これは、要求の厳しいアプリケーションや大規模なデータ操作にとって非常に重要です。

スケーラビリティ: スケーラブルな構成をサポートし、IT 管理者はデータ要件の増大に応じてインフラストラクチャをシームレスに拡張できます。

コスト効率が高い: 標準のイーサネット スイッチ上で実行され、TCP データグラム内にカプセル化されます。実装に特別な機器は必要ありません。

NVMeの利点の詳細については、以下を参照してください。["NVME とは何ですか?"](#)

シナリオの概要

このシナリオでは、次の大きな手順について説明します。

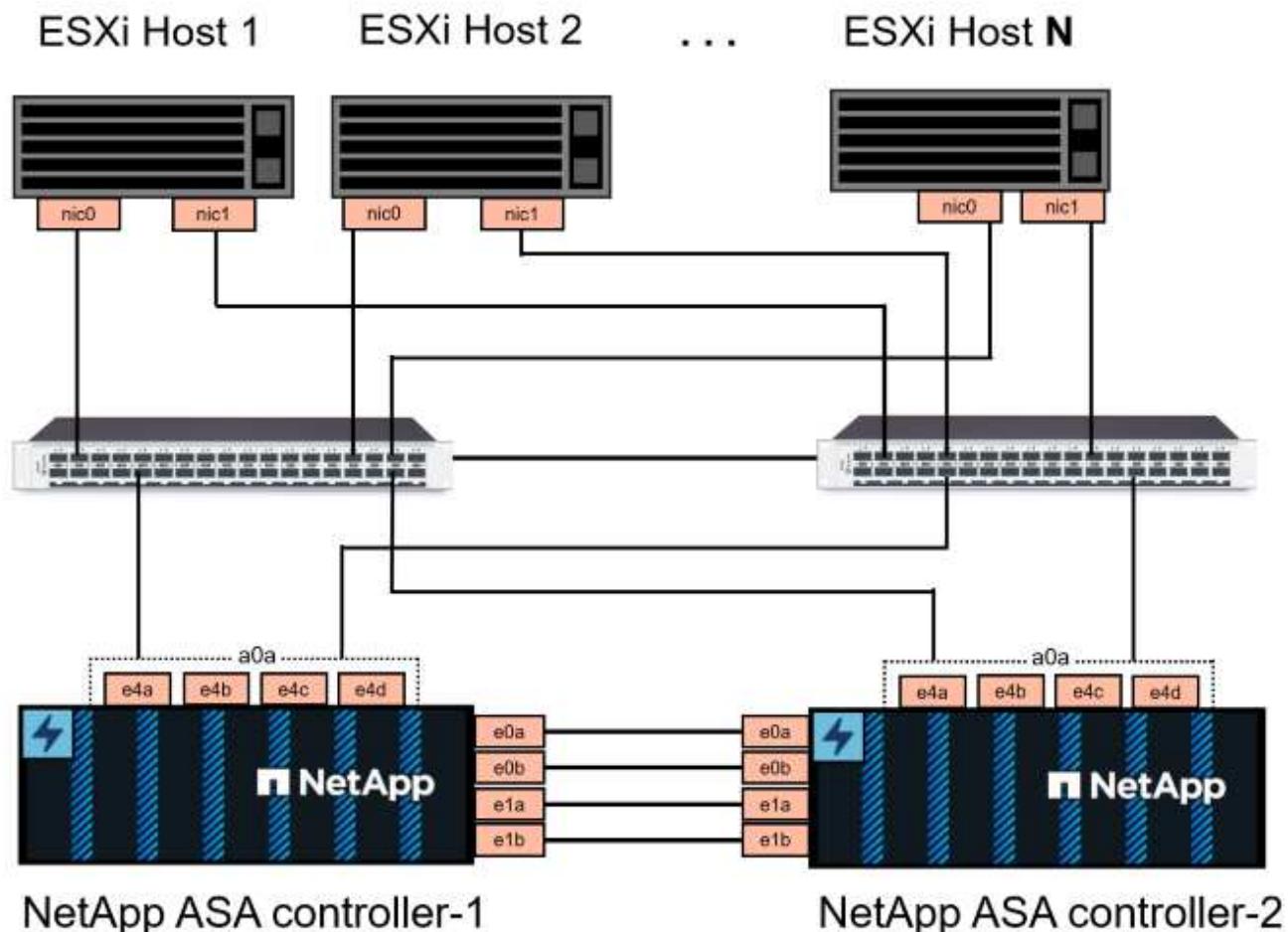
- NVMe/TCP トラフィック用の論理インターフェイス (LIF) を備えたストレージ仮想マシン (SVM) を作成します。
- VI ワークロード ドメイン上の iSCSI ネットワーク用の分散ポート グループを作成します。
- VI ワークロード ドメインの ESXi ホスト上に iSCSI 用の vmkernel アダプタを作成します。
- ESXi ホストに NVMe/TCP アダプターを追加します。
- NVMe/TCP データストアをデプロイします。

前提条件

このシナリオには、次のコンポーネントと構成が必要です。

- ストレージ トラフィック専用のイーサネット スイッチ上に物理データ ポートを備えたONTAP AFF またはASAストレージ システム。
- VCF 管理ドメインの展開が完了し、vSphere クライアントにアクセスできるようになりました。
- VI ワークロード ドメインは以前にデプロイされています。

NetApp は、NVMe/TCP に完全に冗長化されたネットワーク設計を推奨しています。次の図は、ストレージ システム、スイッチ、ネットワーク アダプタ、およびホスト システムにフォールト トレランスを提供する冗長構成の例を示しています。NetAppを参照してください["SAN構成に関するリファレンス"](#)追加情報については。



複数のパスにわたるマルチパスとフェイルオーバーのために、NetApp、NVMe/TCP 構成のすべての SVM に対して、個別のイーサネット ネットワーク内のストレージ ノードごとに少なくとも 2 つの LIF を用意することを推奨しています。

このドキュメントでは、新しい SVM を作成し、IP アドレス情報を指定して NVMe/TCP トラフィック用の複数の LIF を作成するプロセスについて説明します。既存の SVM に新しい LIF を追加するには、["LIF \(ネットワーク インターフェイス\) の作成"](#)。

ONTAPストレージシステムのNVMe設計に関する考慮事項の詳細については、以下を参照してください。["NVMeの構成、サポート、制限事項"](#)。

展開手順

NVMe/TCP を使用して VCF ワークロード ドメインに VMFS データストアを作成するには、次の手順を実行します。

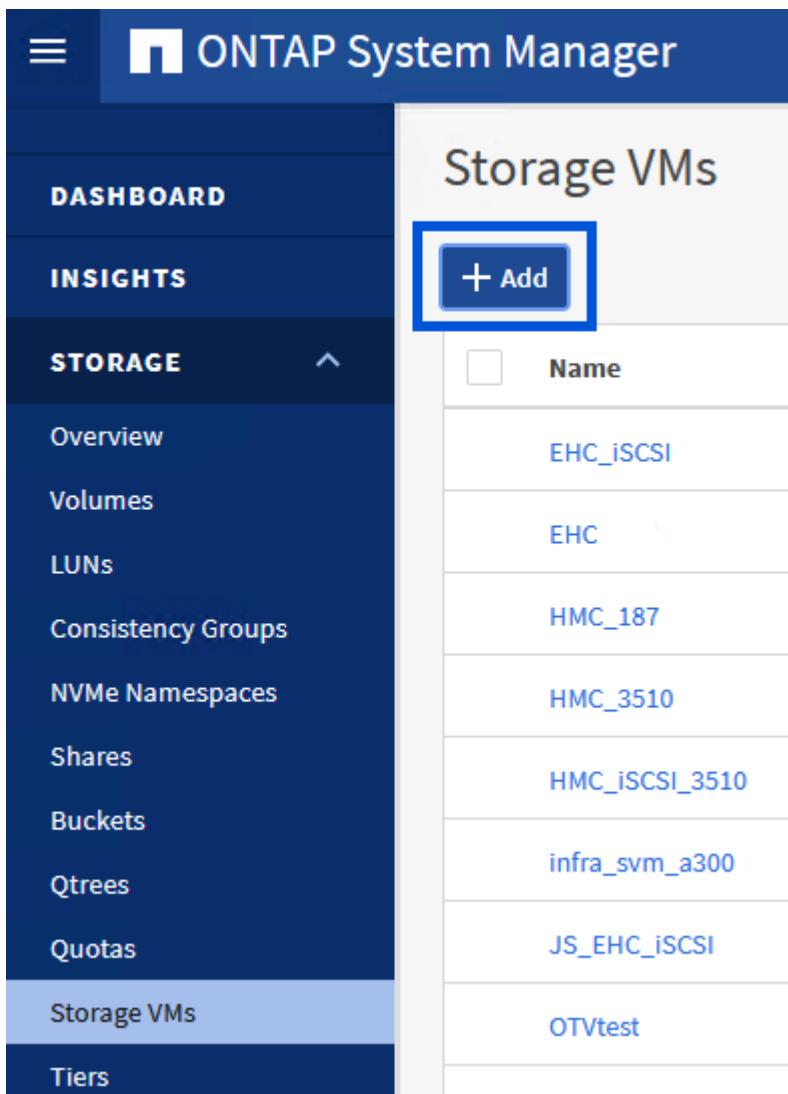
ONTAPストレージ システムに **SVM**、**LIF**、**NVMe** 名前空間を作成する

次の手順はONTAP System Manager で実行されます。

ストレージVMとLIFを作成する

NVMe/TCP トラフィック用の複数の LIF とともに SVM を作成するには、次の手順を実行します。

1. ONTAP System Manager から、左側のメニューの **Storage VMs** に移動し、**+ Add** をクリックして開始します。



2. ストレージ VM の追加 ウィザードで、SVM の名前を入力し、IP スペースを選択して、アクセスプロトコルの下にある NVMe タブをクリックし、NVMe/TCP を有効にするチェックボックスをオンにします。

Add Storage VM

X

STORAGE VM NAME

VCF_NVMe

IPSPACE

Default

Access Protocol

SMB/CIFS, NFS, S3 iSCSI FC

NVMe

Enable NVMe/FC

Enable NVMe/TCP

3. ネットワーク インターフェイス セクションで、最初の LIF の IP アドレス、サブネット マスク、および ブロードキャスト ドメインとポートを入力します。後続の LIF については、チェックボックスを有効にして、残りのすべての LIF で共通の設定を使用するか、個別の設定を使用するかを選択できます。



複数のパスにわたるマルチパスとフェイルオーバーのために、NetApp、NVMe/TCP 構成のすべての SVM に対して、個別のイーサネット ネットワーク内のストレージ ノードごとに少なくとも 2 つの LIF を用意することを推奨しています。

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS	SUBNET MASK	GATEWAY	BROADCAST DOMAIN AND PORT	
172.21.118.189	24	Add optional gateway	NFS_iSCSI	

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS	PORT
172.21.119.189	a0a-3375

ntaphci-a300-02

IP ADDRESS	PORT
172.21.118.190	a0a-3374

IP ADDRESS	PORT
172.21.119.190	a0a-3375

Storage VM Administration

Manage administrator account

Save

Cancel

4. ストレージ VM 管理アカウント (マルチテナント環境の場合) を有効にするかどうかを選択し、[保存] をクリックして SVM を作成します。

Storage VM Administration

Manage administrator account

Save

[Cancel](#)

NVMe名前空間を作成する

NVMe 名前空間は、iSCSI または FC の LUN に類似しています。vSphere Client から VMFS データストアを展開する前に、NVMe 名前空間を作成する必要があります。NVMe 名前空間を作成するには、まずクラスタ内の各 ESXi ホストから NVMe 修飾名 (NQN) を取得する必要があります。NQN は、ネームスペースのアクセス制御を提供するためにONTAPによって使用されます。

NVMe 名前空間を作成するには、次の手順を実行します。

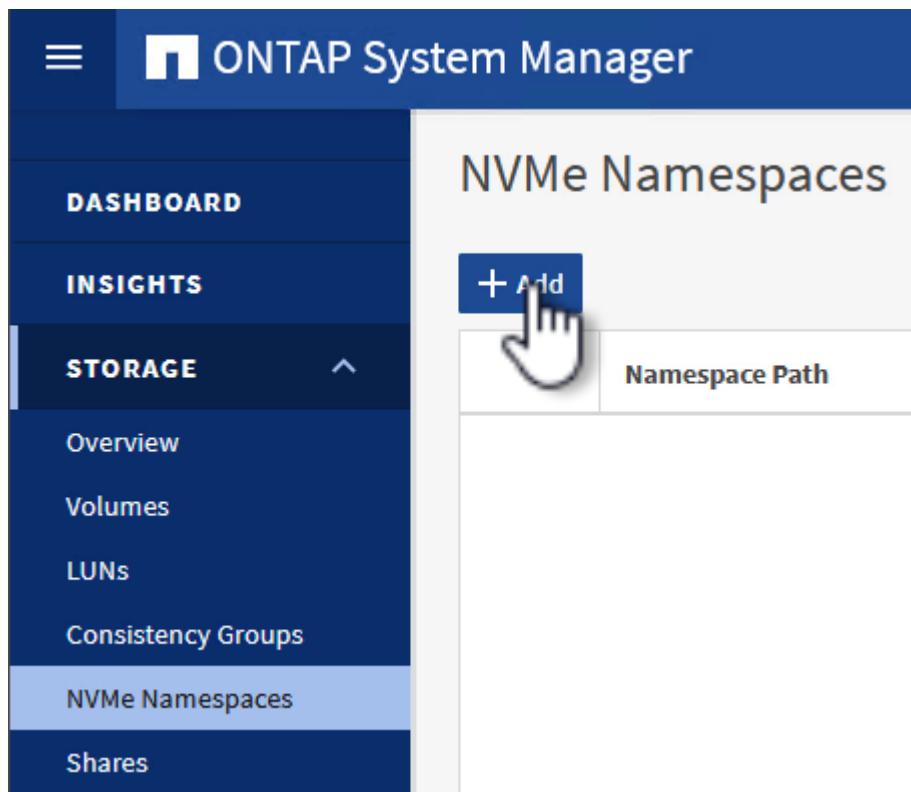
1. クラスター内の ESXi ホストとの SSH セッションを開き、その NQN を取得します。 CLI から次のコマンドを使用します。

```
esxcli nvme info get
```

次のような出力が表示されます。

```
Host NQN: nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-esx01
```

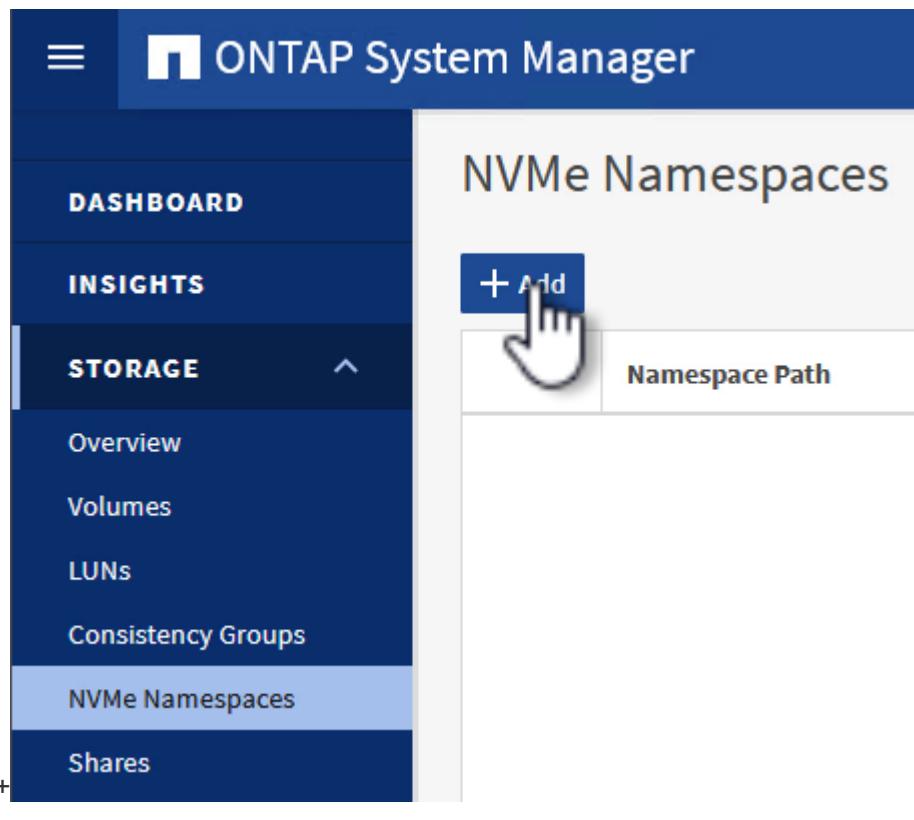
2. クラスタ内の各ESXiホストのNQNを記録します。
3. ONTAP System Manager から、左側のメニューの **NVMe Namespaces** に移動し、**+ Add** をクリックして開始します。



4. NVMe 名前空間の追加 ページで、名前のプレフィックス、作成する名前空間の数、名前空間のサイ

ズ、名前空間にアクセスするホスト オペレーティング システムを入力します。ホスト **NQN** セクションで、名前空間にアクセスする ESXi ホストから以前に収集された NQN のコンマ区切りリストを作成します。

スナップショット保護ポリシーなどの追加項目を構成するには、[その他のオプション] をクリックします。最後に、「保存」をクリックして NVMe 名前空間を作成します。



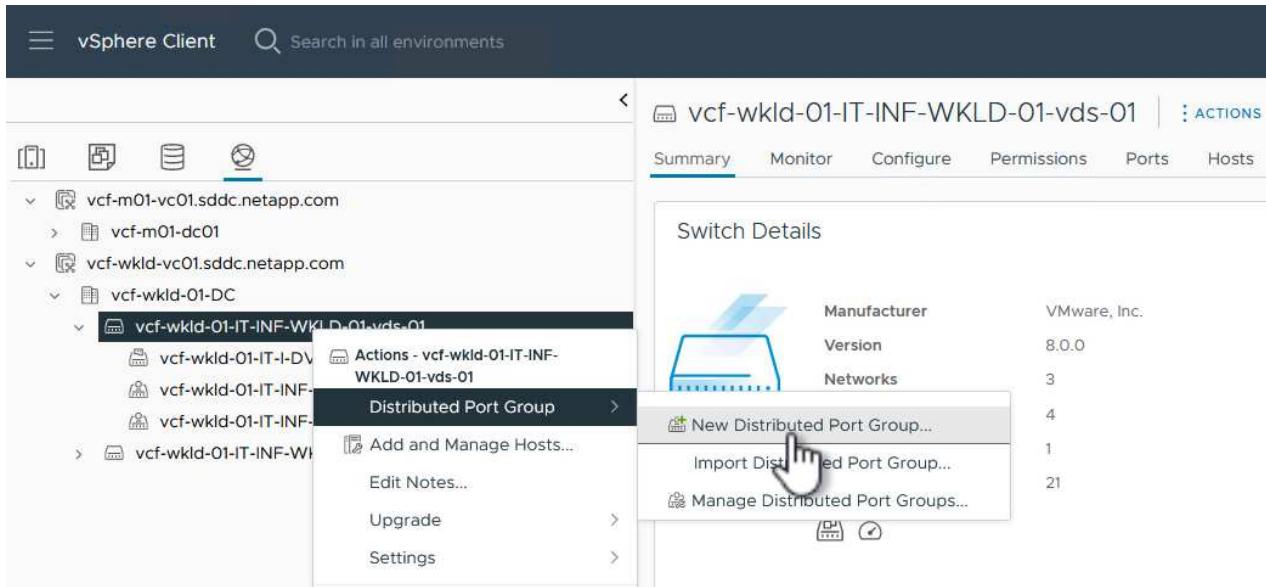
ESXiホストでネットワークとNVMeソフトウェアアダプタを設定する

次の手順は、vSphere クライアントを使用して VI ワークロード ドメイン クラスタで実行されます。この場合、vCenter Single Sign-On が使用されているため、vSphere クライアントは管理ドメインとワークロード ドメインの両方で共通になります。

NVMe/TCP トライック用の分散ポートグループを作成する

各 NVMe/TCP ネットワークに新しい分散ポート グループを作成するには、次の手順を実行します。

1. vSphere クライアントから、ワークロード ドメインの インベントリ > ネットワーク に移動します。既存の分散スイッチに移動し、*新しい分散ポート グループ...*を作成するアクションを選択します。



2. 新しい分散ポート グループ ウィザードで、新しいポート グループの名前を入力し、次へ をクリックして続行します。
3. *設定の構成*ページですべての設定を入力します。 VLAN が使用されている場合は、正しい VLAN ID を必ず指定してください。 続行するには、[次へ] をクリックします。

New Distributed Port Group

1 Name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding Static binding

Port allocation Elastic ⓘ

Number of ports 8

Network resource pool (default) ⓘ

VLAN

VLAN type VLAN

VLAN ID 3374

Advanced

Customize default policies configuration

CANCEL **BACK** **NEXT** 

4. *完了準備完了*ページで変更を確認し、*完了*をクリックして新しい分散ポート グループを作成します。
5. このプロセスを繰り返して、使用されている 2 番目の NVMe/TCP ネットワークの分散ポート グループを作成し、正しい **VLAN ID** を入力したことを確認します。
6. 両方のポート グループが作成されたら、最初のポート グループに移動し、[設定の編集...] アクションを選択します。

174

vSphere Client Search in all environments

vcf-wkld-01-nvme-a | : ACTIONS

Summary Monitor Configure Permissions

Distributed Port Group Details

	Port binding	Static
	Port allocation	Elastic
	VLAN ID	3374
	Distributed switch	VC WKLD
	Network protocol profile	--
	Network resource pool	--
	Hosts	4
	Virtual machines	0

Actions - vcf-wkld-01-nvme-a

- Ed Settings...
- Export Configuration...
- Restore Configuration...

7. 分散ポートグループ - 設定の編集ページで、左側のメニューのチーミングとフェイルオーバーに移動し、**uplink2**をクリックして未使用のアップリンクまで下に移動します。

Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-a

General Advanced VLAN Security Traffic shaping Teaming and failover Monitoring Miscellaneous

Load balancing Network failure detection Notify switches Fallback

Route based on originating virtual port

Link status only

Yes

Yes

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

8. 2番目のNVMe/TCPポートグループに対してこの手順を繰り返します。ただし、今回は**uplink1**を

Unused uplinks まで下に移動します。

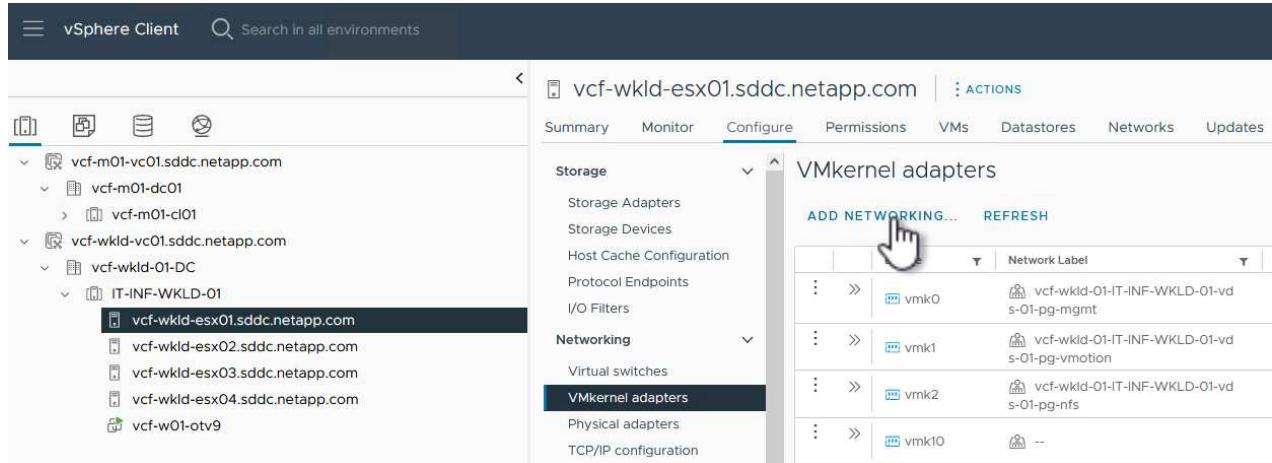
Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-b

General	Load balancing	Route based on originating virtual port
Advanced	Network failure detection	Link status only
VLAN	Notify switches	Yes
Security	Fallback	Yes
Traffic shaping		
Teaming and failover		
Monitoring	Failover order ⓘ	
Miscellaneous	MOVE UP MOVE DOWN	
	Active uplinks	
	<input type="checkbox"/> uplink2	
	Standby uplinks	
	Unused uplinks	
	<input type="checkbox"/> uplink1	

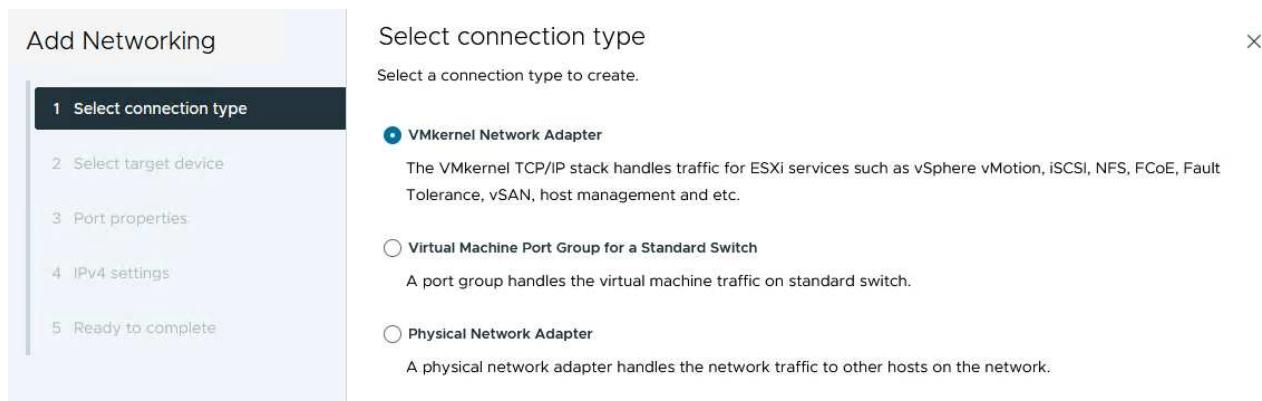
各ESXiホストにVMkernelアダプタを作成する

ワークロード ドメイン内の各 ESXi ホストでこのプロセスを繰り返します。

1. vSphere クライアントから、ワークロード ドメイン インベントリ内の ESXi ホストの 1 つに移動します。*構成*タブから*VMkernelアダプタ*を選択し、*ネットワークの追加...*をクリックして開始します。



2. 接続タイプの選択 ウィンドウで **VMkernel** ネットワーク アダプタを選択し、次へをクリックして続行します。



3. ターゲット デバイスの選択 ページで、以前に作成した iSCSI の分散ポート グループの 1 つを選択します。

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

Select an existing network

Select an existing standard switch

New standard switch

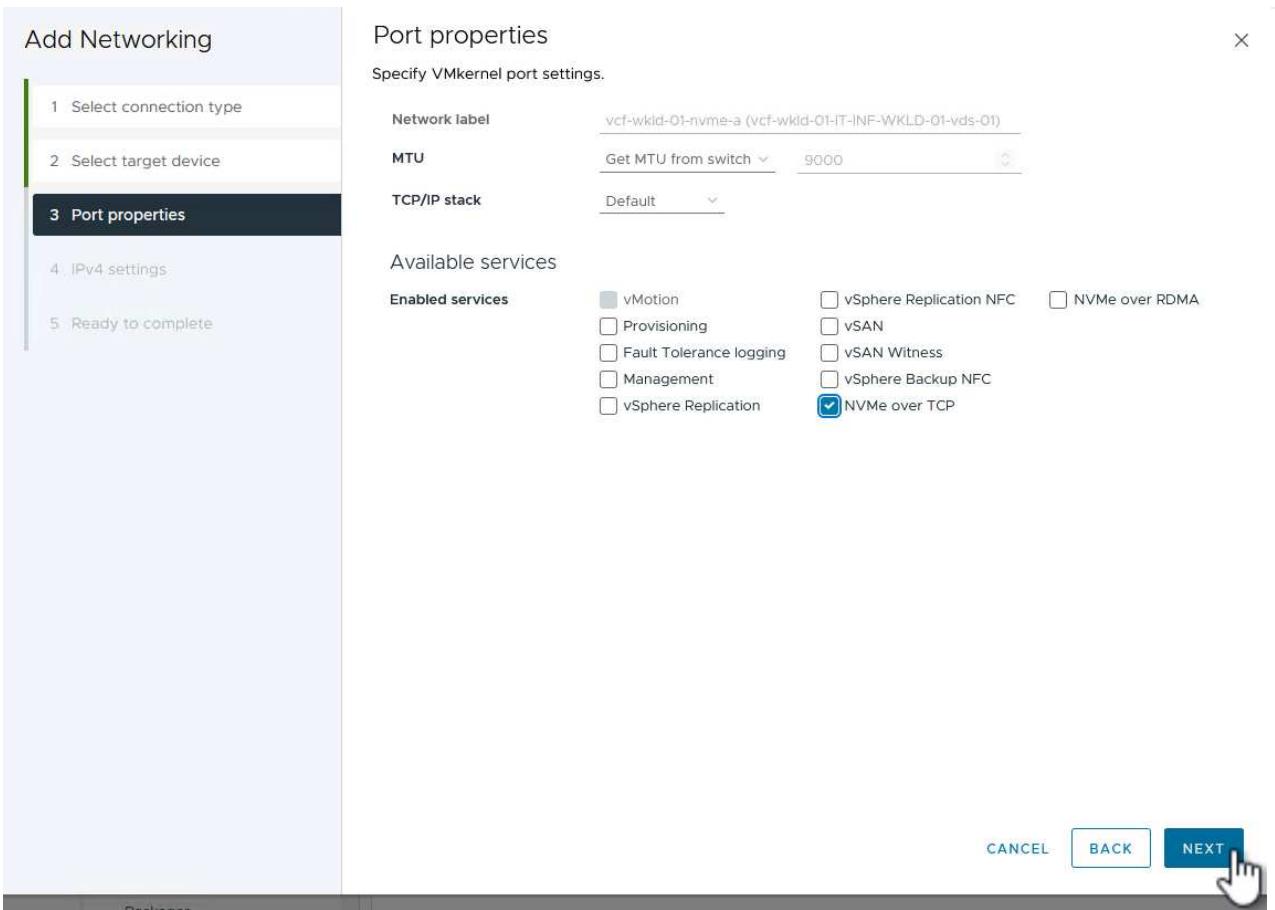
Quick Filter

Name	NSX Port Group ID	Distributed Switch
vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nmgt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

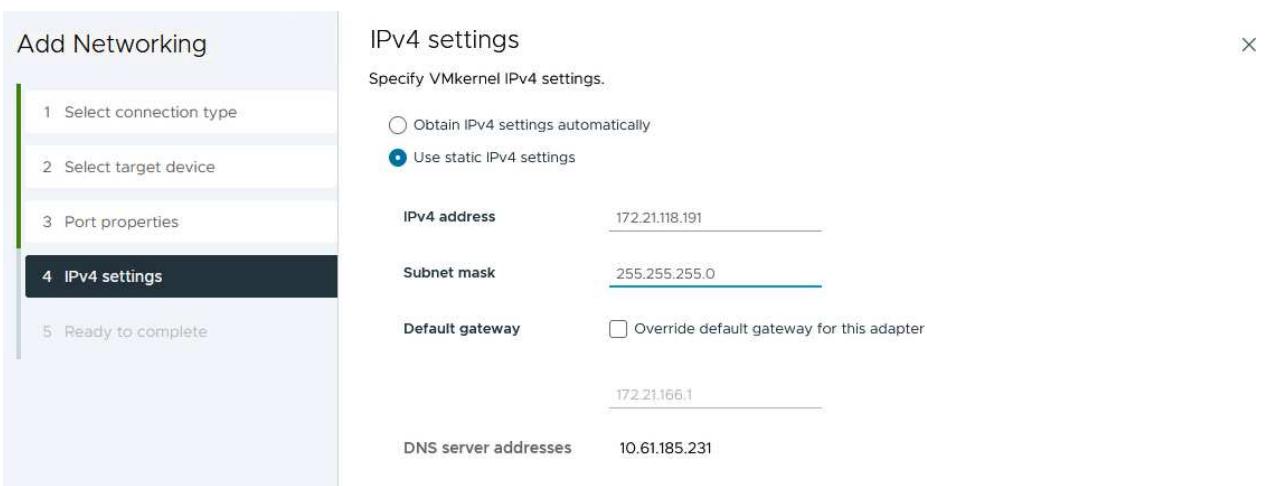
Manage Columns 7 items

CANCEL BACK NEXT 

4. ポート プロパティ ページで、**NVMe over TCP** のボックスをクリックし、次へをクリックして続行します。



5. **IPv4 設定** ページで、IP アドレス、サブネット マスクを入力し、新しいゲートウェイ IP アドレスを指定します(必要な場合のみ)。続行するには、[次へ] をクリックします。



6. *準備完了*ページで選択内容を確認し、*完了*をクリックして VMkernel アダプタを作成します。

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

✓ Select target device

Distributed port group	vcf-wkld-01-nvme-a
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

✓ Port properties

New port group	vcf-wkld-01-nvme-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Enabled
NVMe over RDMA	Disabled

✓ IPv4 settings

IPv4 address	172.21.118.191 (static)
Subnet mask	255.255.255.0

Packages

CANCEL BACK FINISH 

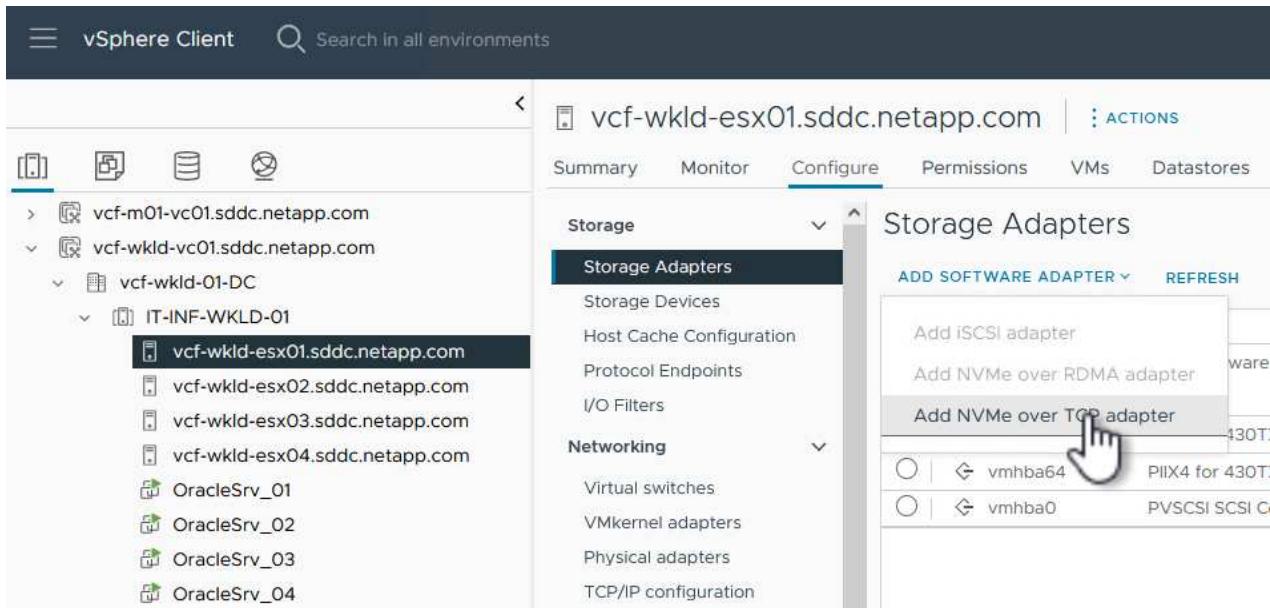
7. このプロセスを繰り返して、2番目の iSCSI ネットワーク用の VMkernel アダプタを作成します。

NVMe over TCPアダプタを追加する

ワークロード ドメイン クラスタ内での ESXi ホストには、ストレージ トラフィック専用の確立された NVMe/TCP ネットワークごとに NVMe over TCP ソフトウェア アダプタがインストールされている必要があります。

NVMe over TCP アダプターをインストールし、NVMe コントローラを検出するには、次の手順を実行します。

1. vSphere クライアントで、ワークロード ドメイン クラスタ内の ESXi ホストの 1 つに移動します。
*構成*タブからメニューの*ストレージ アダプタ*をクリックし、*ソフトウェア アダプタの追加*ドロップダウン メニューから*NVMe over TCP アダプタの追加*を選択します。



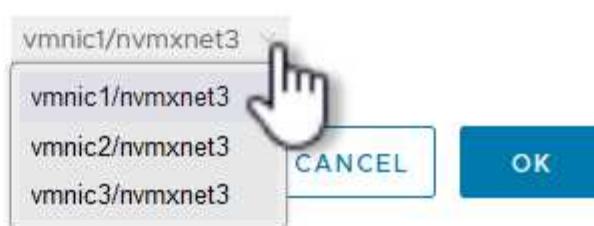
2. ソフトウェア NVMe over TCP アダプターの追加 ウィンドウで、物理ネットワーク アダプター ドロップダウン メニューにアクセスし、NVMe アダプターを有効にする正しい物理ネットワーク アダプターを選択します。

Add Software NVMe over TCP adapter

vcf-wkld-esx0
1.sddc.netapp.com

Enable software NVMe adapter on the selected physical network adapter.

Physical Network Adapter

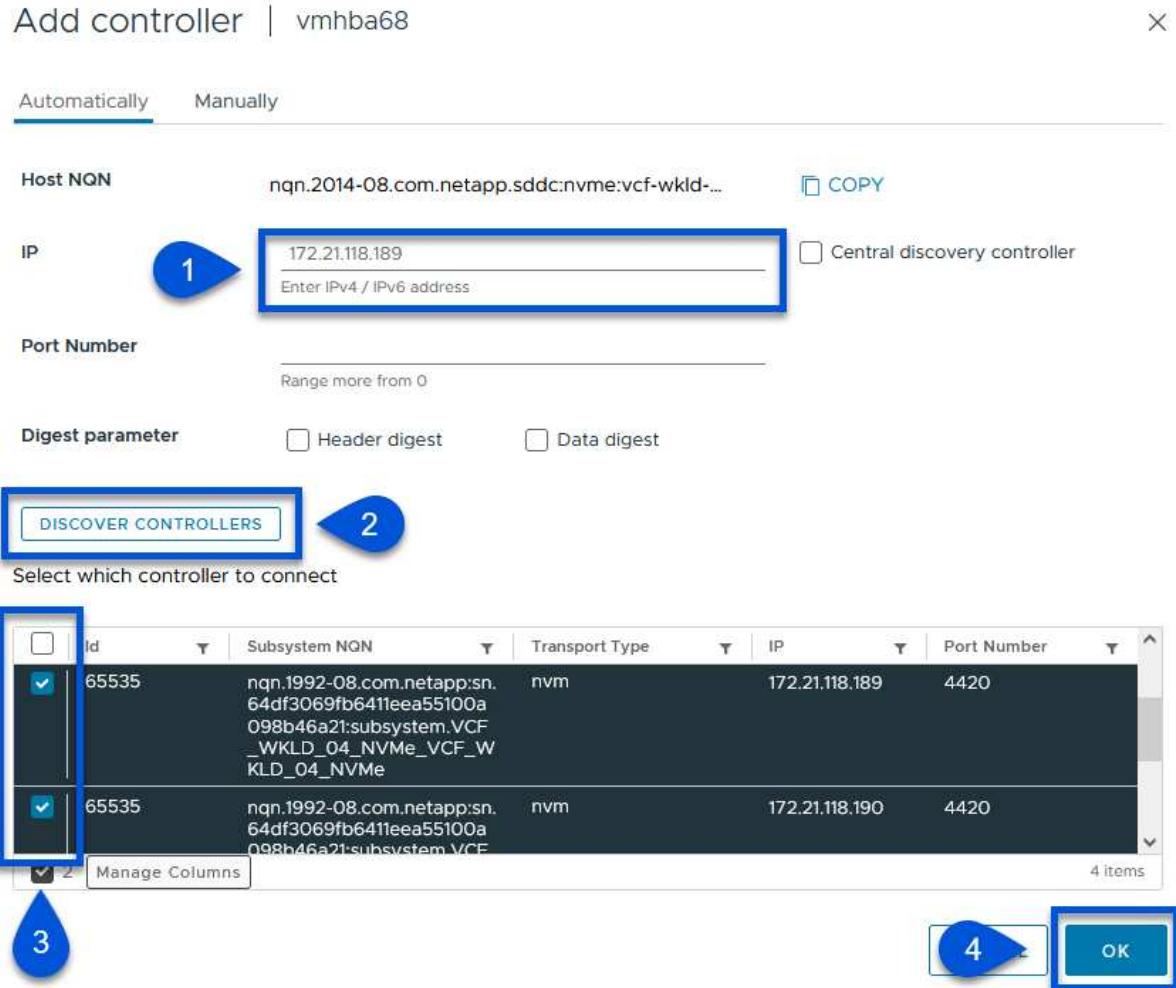


- NVMe over TCP トラフィックに割り当てられた 2 番目のネットワークに対してこのプロセスを繰り返し、正しい物理アダプターを割り当てます。
- 新しくインストールされた NVMe over TCP アダプターの 1 つを選択し、[コントローラー] タブで [コントローラーの追加*] を選択します。

- コントローラーの追加 ウィンドウで、自動 タブを選択し、次の手順を実行します。

- この NVMe over TCP アダプタに割り当てられた物理アダプタと同じネットワーク上の SVM 論理インターフェイスの 1 つに IP アドレスを入力します。
- *コントローラーの検出*ボタンをクリックします。

- 検出されたコントローラのリストから、この NVMe over TCP アダプタと一致するネットワークアドレスを持つ 2 つのコントローラのチェック ボックスをクリックします。
- 選択したコントローラーを追加するには、[OK] ボタンをクリックします。



6. 数秒後、NVMe 名前空間が [デバイス] タブに表示されます。

Storage Adapters

		Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
<input type="radio"/>	↳	vmhba65	iSCSI Software Adapter	iSCSI	Online	iscsi_vmk(iqn.1998-01.com.vmware:vcf-wkld-esx01.sddc.net/app.com:794177624:65)	4	2	8
<input type="radio"/>	↳	vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	1	1	1
<input type="radio"/>	↳	vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	0	0	0
<input type="radio"/>	↳	vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	3	3	3
<input checked="" type="radio"/>	↳	vmhba68	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	1	1	1
<input type="radio"/>	↳	vmhba69	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	0	0	0

6 items

[Properties](#) [Devices](#) [Paths](#) [Namespaces](#) [Controllers](#)

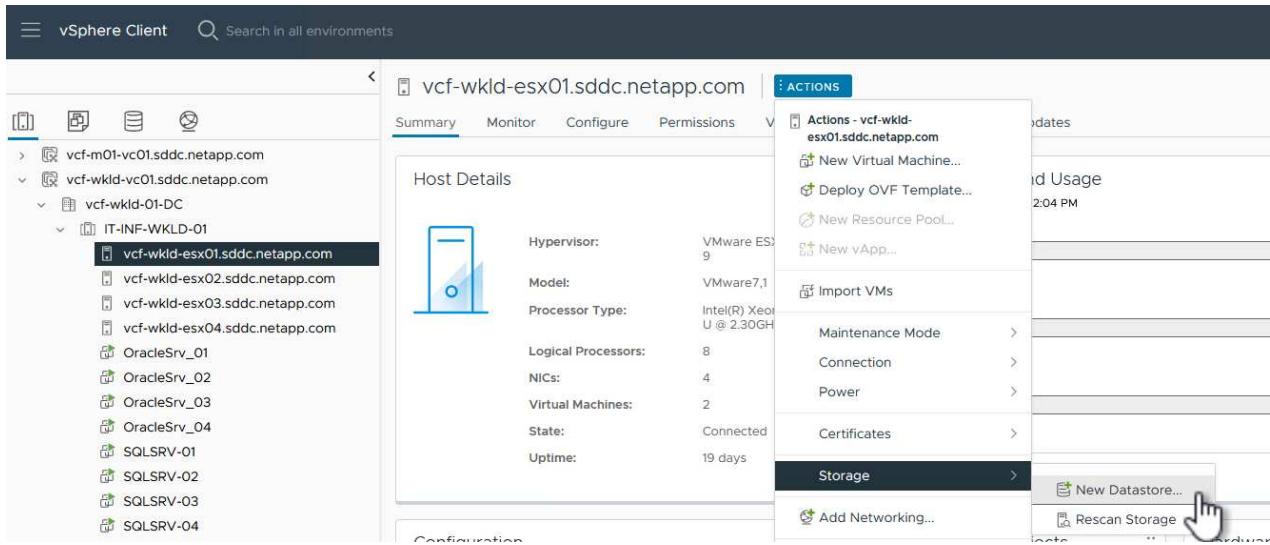
	Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type	Transport
<input type="checkbox"/>	NVMe TCP Disk (uuid:929a6a9045764784 9146e09d6e55b076)	0	disk	3.00 TB	Not Consumed	Attached	Supported	Flash	TCPTRANSPORT

7. この手順を繰り返して、NVMe/TCP トラフィック用に確立された 2 番目のネットワークの NVMe over TCP アダプターを作成します。

NVMe over TCPデータストアを展開する

NVMe 名前空間に VMFS データストアを作成するには、次の手順を実行します。

1. vSphere クライアントで、ワークロード ドメイン クラスタ内の ESXi ホストの 1 つに移動します。アクション メニューから ストレージ > 新しいデータストア... を選択します。



2. *新しいデータストア* ウィザードで、タイプとして*VMFS*を選択します。続行するには、[次へ] をクリックします。
3. *名前とデバイスの選択* ページで、データストアの名前を入力し、使用可能なデバイスのリストから NVMe 名前空間を選択します。

New Datastore

1 Type

2 Name and device selection

3 VMFS version

4 Partition configuration

5 Ready to complete

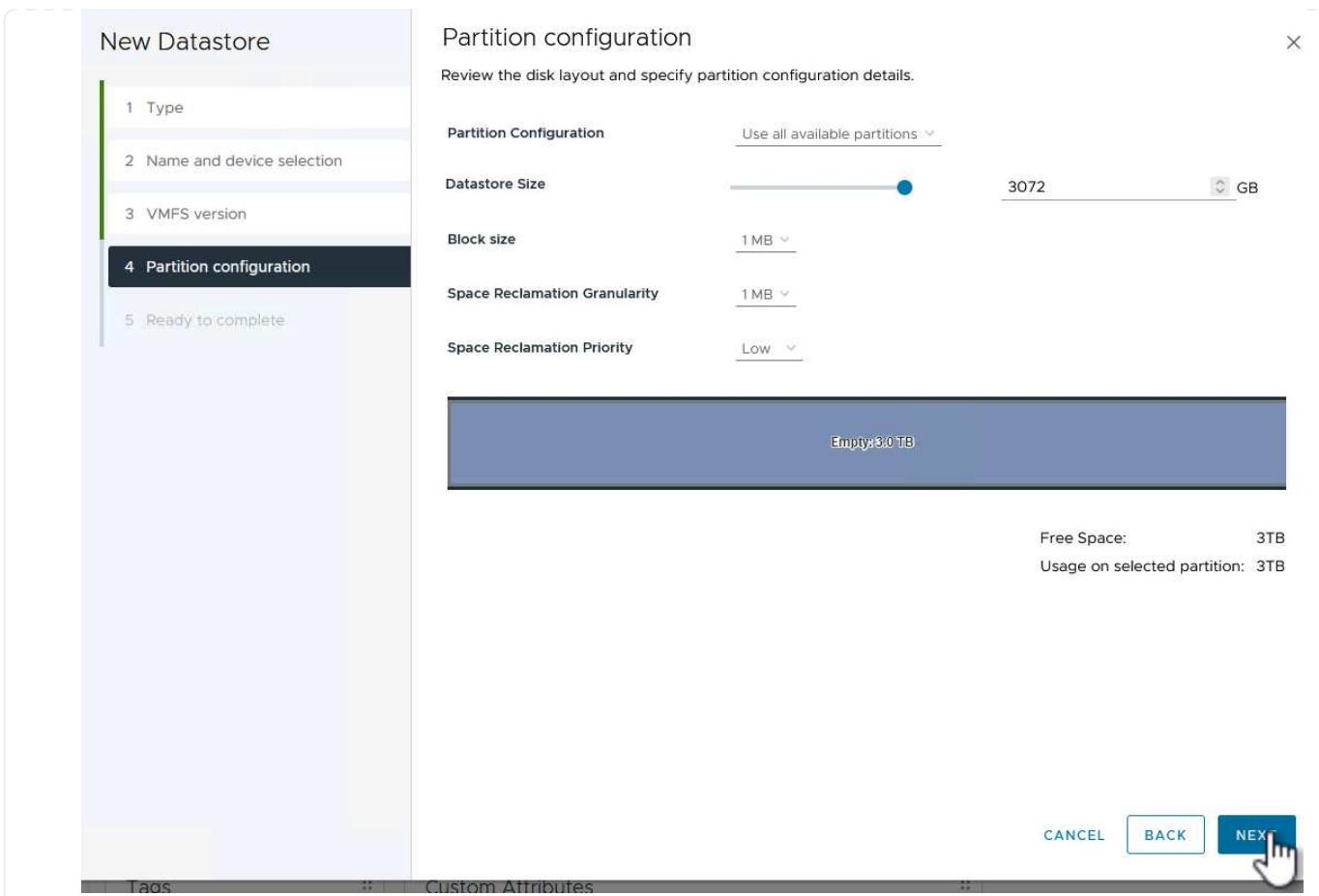
Name

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Cl V St
<input checked="" type="radio"/>	NVMe TCP Disk (uuid:929a6a90457647849146e09d6e55b076)	0	3.00 TB	Supported	Flash	512e	N
<input type="radio"/>	Local VMware Disk (naa.6000c29f83dcfce42d230340de66036)	0	4.00 GB	Not supported	Flash	512n	N
<input type="radio"/>	Local VMware Disk (naa.6000c291464644a835bc23d384813ac0)	0	75.00 GB	Not supported	Flash	512n	N

Manage Columns Export ▾ 3 items

CANCEL BACK **NEXT** 

Tags :: Custom Attributes ::



6. *完了準備完了*ページで概要を確認し、*完了*をクリックしてデータストアを作成します。
7. インベントリ内の新しいデータストアに移動し、[ホスト] タブをクリックします。正しく構成されている場合、クラスター内のすべての ESXi ホストがリストされ、新しいデータストアにアクセスできるようになります。

Name	State	Status	Cluster	Consumed CPU %	Consumed Memory %	HA State	Uptime
vcf-wkld-esx01.sddc.netapp.co	Connected	Normal	IT-INF-WKLD-0	15%	13%	Connected (Secondary)	19 days
vcf-wkld-esx02.sddc.netapp.co	Connected	Normal	IT-INF-WKLD-0	9%	15%	Running (Primary)	19 days
vcf-wkld-esx03.sddc.netapp.co	Connected	Normal	IT-INF-WKLD-0	9%	21%	Connected (Secondary)	19 days
vcf-wkld-esx04.sddc.netapp.co	Connected	Normal	IT-INF-WKLD-0	11%	4%	Connected (Secondary)	19 days

追加情報

ONTAPストレージシステムの構成については、["ONTAP 9ドキュメント"](#)中心。

VCFの設定方法については、以下を参照してください。["VMware Cloud Foundation ドキュメント"](#)。

FCベースのVMFSデータストアをVIワークロードドメインの補助ストレージとして追加する

このユースケースでは、VMware Cloud Foundation (VCF) 仮想インフラストラクチャ (VI) ワークロード ドメインの補助ストレージとしてファイバーチャネル (FC) を使用して VMFS データストアを構成する手順について説明します。この手順では、VMware vSphere 用のONTAPツールの導入、VI ワークロード vCenter サーバーの登録、ストレージ バックエンドの定義、および FC データストアのプロビジョニングについてまとめていきます。

ファイバーチャネルの利点

高性能: FC は高速データ転送速度を提供するため、大量のデータへの高速かつ信頼性の高いアクセスを必要とするアプリケーションに最適です。

低レイテンシ: 非常に低いレイテンシ。これは、データベースや仮想化環境などのパフォーマンスが重視されるアプリケーションにとって非常に重要です。

信頼性: FC ネットワークは、冗長性やエラー訂正などの機能が組み込まれており、堅牢性と信頼性に優れています。

専用帯域幅: FC はストレージ トラフィックに専用の帯域幅を提供し、ネットワーク輻輳のリスクを軽減します。

NetAppストレージシステムでのファイバーチャネルの使用に関する詳細については、["FCを使用したSANプロビジョニング"](#)。

シナリオの概要

VCF 補足データストアは、vCenter を使用した Day-2 運用の一部としてプロビジョニングされます。このシナリオでは、次の大まかな手順について説明します。

- ・ 管理ドメインへのONTAPツールの導入
- ・ VIワークロードvCenter ServerをONTAPツールに登録する
- ・ VMware vSphere のONTAPツール プラグインでストレージ バックエンドを定義する
- ・ FCトランスポート上でVMFSをプロビジョニングする

前提条件

このシナリオには、次のコンポーネントと構成が必要です。

- ・ FC スイッチに接続された FC ポートを備えたONTAP AFFまたはASAストレージ システム。
- ・ FC lifs で作成された SVM。
- ・ FC スイッチに接続された FC HBA を備えた vSphere。
- ・ FC スイッチには単一のイニシエーター ターゲット ゾーニングが構成されています。



ONTAPシステム上の物理 FC ポートではなく、ゾーン構成で SVM FC 論理インターフェイスを使用します。

NetApp は、FC LUN にマルチパスを推奨しています。

ONTAPストレージシステムでのファイバチャネルの設定に関する詳細については、以下を参照してください。 "[SANストレージの管理](#)" ONTAP 9 のドキュメントを参照してください。

ONTAPストレージシステムでVMFSを使用する方法の詳細については、"[VMFS の導入ガイド](#)"。

VIワークロードドメインのデプロイメント手順

ONTAPツールを導入し、それを使用して VCF VI ワークロード ドメインに VMFS データストアを作成するには、次の手順を実行します。

- "vCenterプラグインを有効にするには、VIワークロードvCenterを登録します。"
- "vSphere クライアントインターフェースを使用してストレージ バックエンドを定義する"
- "FC 上で VMFS をプロビジョニングする"

追加情報

ONTAPストレージシステムの構成については、"[ONTAP 9ドキュメント](#)"中心。

VCFの設定方法については、以下を参照してください。"[VMware Cloud Foundation ドキュメント](#)"。

このソリューションのビデオデモ

[VCF管理ドメインの補助ストレージとしてのVMFS\(FC\)データストア](#)

SnapCenterでVCFを保護する

VMware vSphere 向けSnapCenterプラグインを使用して **VCF** ワークロード ドメインを保護する方法について学習します。

SnapCenter Plug-in for VMware vSphereを使用して VMware Cloud Foundation (VCF) ワークロードを保護するために使用できるNetAppソリューションについて説明します。このプラグインは、バックアップとリカバリを簡素化し、アプリケーションの一貫性のあるバックアップを保証し、NetApp の効率化テクノロジーを使用してストレージを最適化します。

vSphere クライアントとのシームレスな統合を提供しながら、自動化されたワークフローとスケーラブルな操作をサポートします。 SnapMirrorレプリケーションによりオンプレミスまたはクラウドへのセカンダリ バックアップが提供され、仮想化環境で強力なデータ保護と運用効率が実現します。

詳細については、以下の解決策を参照してください。

- "[VCFワークロードドメインの保護](#)"

- ・ "VCFの複数のワークロードドメインを保護"
- ・ "NVMeでVCFワークロードドメインを保護する"
- ・ "SnapCenterプラグインとBlueXP backup and recoveryによる VMware の 3-2-1 データ保護"

VMware vSphere 用のSnapCenterプラグインを使用して VCF ワークロード ドメインを保護する

このユースケースでは、VMware vSphere 用のSnapCenterプラグインを使用して、VMware Cloud Foundation (VCF) ワークロード ドメイン内の VM とデータストアをバックアップおよび復元する手順について説明します。この手順では、VMware vSphere 用のSnapCenterプラグインの展開、ストレージシステムの追加、バックアップポリシーの作成、VM およびファイルの復元についてまとめています。

このソリューションでは、VMFS データストアのストレージ プロトコルとして **iSCSI** が使用されます。

シナリオの概要

このシナリオでは、次の大まかな手順について説明します。

- ・ VI ワークロード ドメインにSnapCenter Plug-in for VMware vSphereを展開します。
- ・ SCV にストレージ システムを追加します。
- ・ SCV でバックアップポリシーを作成します。
- ・ SCV にリソース グループを作成します。
- ・ SCV を使用して、データストアまたは特定の VM をバックアップします。
- ・ SCV を使用して、VM をクラスター内の別の場所に復元します。
- ・ SCV を使用してファイルを Windows ファイル システムに復元します。

前提条件

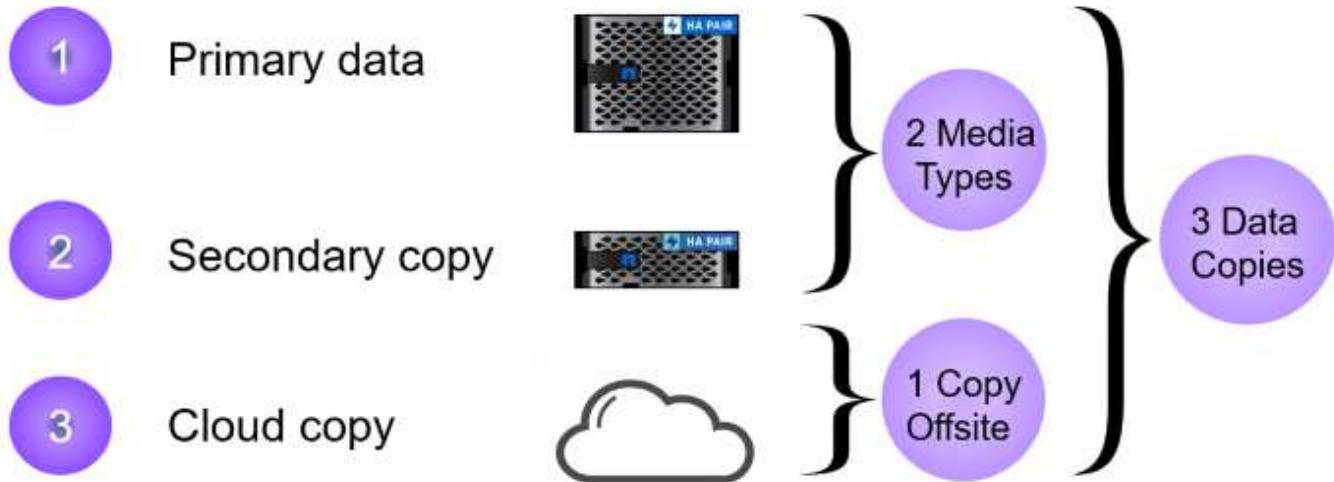
このシナリオには、次のコンポーネントと構成が必要です。

- ・ ワークロード ドメイン クラスタに割り当てられた iSCSI VMFS データストアを備えたONTAP ASAストレージ システム。
- ・ SnapMirrorを使用してセカンダリ バックアップを受信するように構成されたセカンダリONTAPストレージ システム。
- ・ VCF 管理ドメインの展開が完了し、vSphere クライアントにアクセスできるようになりました。
- ・ VI ワークロード ドメインは以前にデプロイされています。
- ・ 仮想マシンは、SCV が保護するように指定されているクラスター上に存在します。

iSCSI VMFSデータストアを補助ストレージとして構成する方法については、以下を参照してください。
"VMware 向けONTAPツールを使用した管理ドメインの補助ストレージとしての iSCSI" このドキュメントでは。 OTV を使用してデータストアを展開するプロセスは、管理ドメインとワークロード ドメインで同じです。



SCV で取得したバックアップをセカンダリーストレージに複製するだけでなく、VM 用のNetApp BlueXP backup and recoveryを使用して、3 大クラウド プロバイダーのいずれかのオブジェクトストレージにデータのオフサイト コピーを作成することもできます。詳細についてはソリューションを参照してください["SnapCenter プラグインとBlueXP backup and recoveryによる VMware の 3-2-1 データ保護"](#)。



展開手順

SnapCenter プラグインを展開し、それを使用してバックアップを作成し、VM とデータストアを復元するには、次の手順を実行します。

SCV を導入して使用し、VI ワークロード ドメイン内のデータを保護する

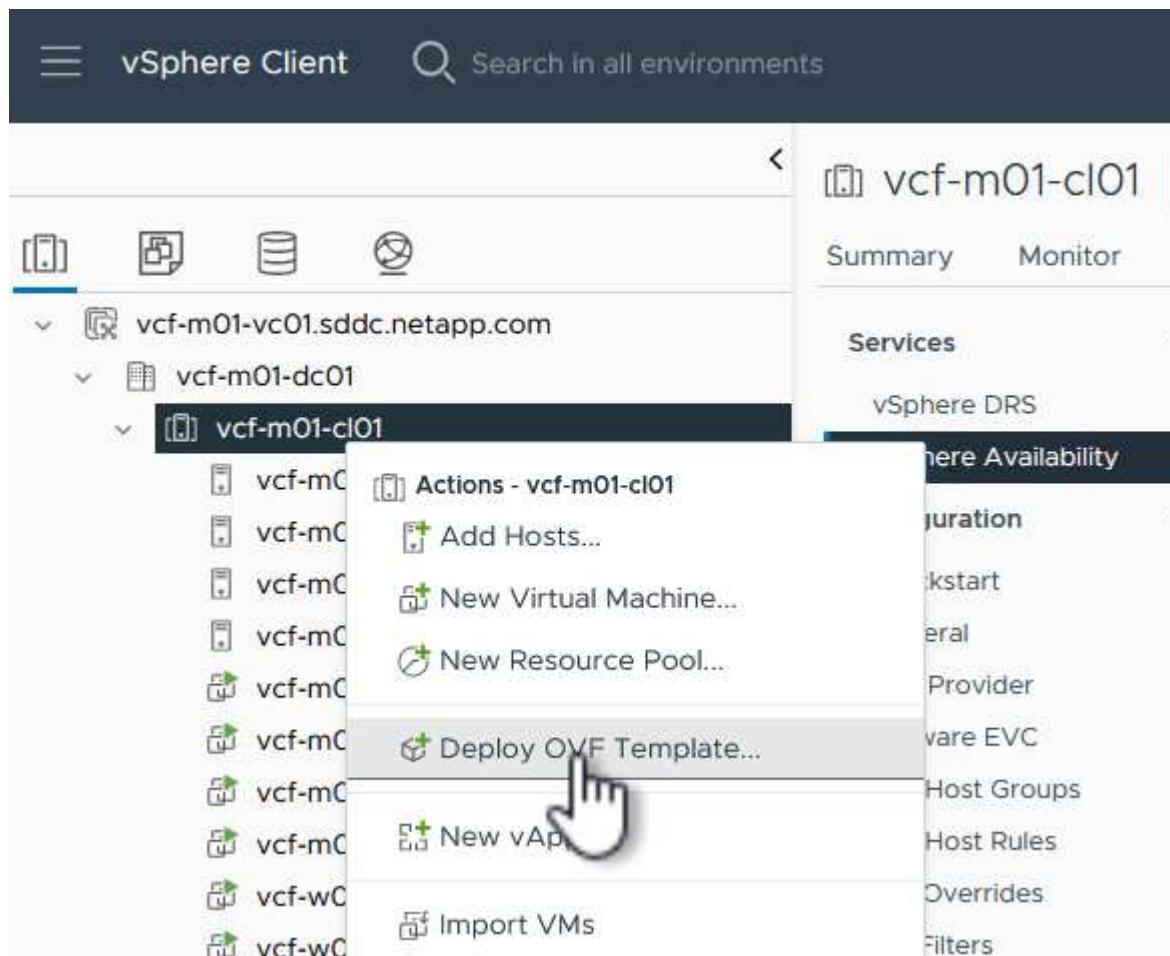
SCV を展開、構成、使用して VI ワークロード ドメイン内のデータを保護するには、次の手順を実行します。

SnapCenter Plug-in for VMware vSphereの導入

SnapCenterプラグインはVCF管理ドメインでホストされますが、VIワークロードドメインのvCenterに登録されます。各vCenterインスタンスには1つのSCVインスタンスが必要です。また、ワークロードドメインには、単一のvCenterインスタンスによって管理される複数のクラスターを含めることができますことに注意してください。

SCVをVIワークロードドメインにデプロイするには、vCenterクライアントから次の手順を実行します。

1. NetAppサポートサイトのダウンロードエリアからSCV展開用のOVAファイルをダウンロードします。[ここ](#)。
2. 管理ドメインvCenter Clientから、**OVFテンプレートのデプロイ...**を選択します。



3. **OVFテンプレートのデプロイ ウィザード**で、ローカルファイルラジオボタンをクリックし、以前にダウンロードしたOVFテンプレートをアップロードすることを選択します。続行するには、[次へ]をクリックします。

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template from remote URL or local file system
Enter a URL to download and install the OVF package from the internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL
<http://https://remoteserver-address/filetodeploy.ovf> .ova

Local file
scv-5.0P2-240310_1514.ova

UPLOAD FILES

- *名前とフォルダーの選択*ページで、SCV データ ブローカー VM の名前と管理ドメイン上のフォルダーを指定します。続行するには、[次へ] をクリックします。
- コンピューティング リソースの選択 ページで、VM をインストールする管理ドメイン クラスターまたはクラスター内の特定の ESXi ホストを選択します。
- *詳細の確認*ページで OVF テンプレートに関する情報を確認し、*ライセンス契約*ページでライセンス条項に同意します。
- *ストレージの選択*ページで、VM をインストールするデータストアを選択し、*仮想ディスク フォーマット*と*VM ストレージ ポリシー*を選択します。このソリューションでは、このドキュメントの別のセクションで以前に展開されたように、ONTAPストレージシステムにあるiSCSI VMFS データストアにVMがインストールされます。続行するには、[次へ] をクリックします。

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage**
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine (i)

Select virtual disk format Thin Provision

VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

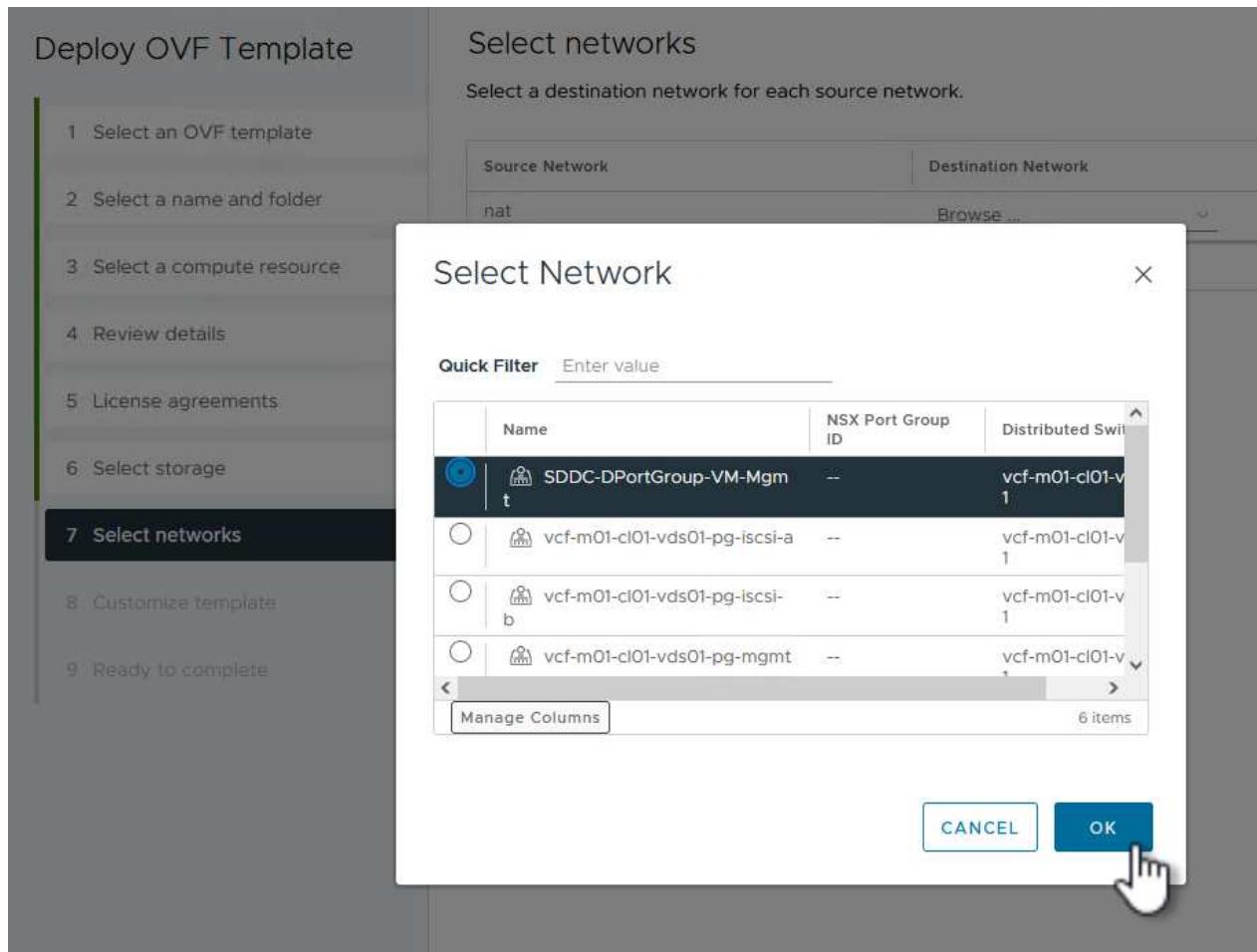
Name	Storage Compatibility	Capacity	Provisioned	Free
mgmt_01_iscsi	--	3 TB	3.71 TB	2.5 TB
vcf-m01-cl01-ds-vsan01	--	999.97 GB	49.16 GB	957.54 GB
vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB
vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB
vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB
vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB

Compatibility

Compatibility checks succeeded.

CANCEL **BACK** **NEXT**

8. ネットワークの選択ページで、ワークロード ドメイン vCenter アプライアンスおよびプライマリとセカンダリの両方のONTAPストレージシステムと通信できる管理ネットワークを選択します。



9. *テンプレートのカスタマイズ*ページで、デプロイメントに必要なすべての情報を入力します。

- ワーカロード ドメイン vCenter アプライアンスの FQDN または IP、および資格情報。
- SCV 管理アカウントの資格情報。
- SCV メンテナンス アカウントの資格情報。
- IPv4 ネットワーク プロパティの詳細 (IPv6 も使用できます)。
- 日付と時刻の設定。

続行するには、[次へ] をクリックします。

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

1. Register to existing vCenter		4 settings
1.1 vCenter Name(FQDN) or IP Address	cf-wkld-vc01.sddc.netapp.com	
1.2 vCenter username	administrator@vcf.local	
1.3 vCenter password	Password	***** (?)
	Confirm Password	***** (?)
1.4 vCenter port	443	
2. Create SCV Credentials		2 settings
2.1 Username	admin	
2.2 Password	Password	***** (?)
	Confirm Password	***** (?)
3. System Configuration		1 settings

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Customize template

4.2 Setup IPv4 Network Properties		6 settings
4.2.1 IPv4 Address	IP address for the appliance. (Leave blank if DHCP is desired) 172.21.166.148	
4.2.2 IPv4 Netmask	Subnet to use on the deployed network. (Leave blank if DHCP is desired) 255.255.255.0	
4.2.3 IPv4 Gateway	Gateway on the deployed network. (Leave blank if DHCP is desired) 172.21.166.1	
4.2.4 IPv4 Primary DNS	Primary DNS server's IP address. (Leave blank if DHCP is desired) 10.61.185.231	
4.2.5 IPv4 Secondary DNS	Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired) 10.61.186.231	
4.2.6 IPv4 Search Domains (optional)	Comma separated list of search domain names to use when resolving host names. (Leave blank if DHCP is desired) netapp.com,sddc.netapp.com	
4.3 Setup IPv6 Network Properties		6 settings
4.3.1 IPv6 Address	IP address for the appliance. (Leave blank if DHCP is desired)	
4.3.2 IPv6 PrefixLen	Prefix length to use on the deployed network. (Leave blank if DHCP is desired)	

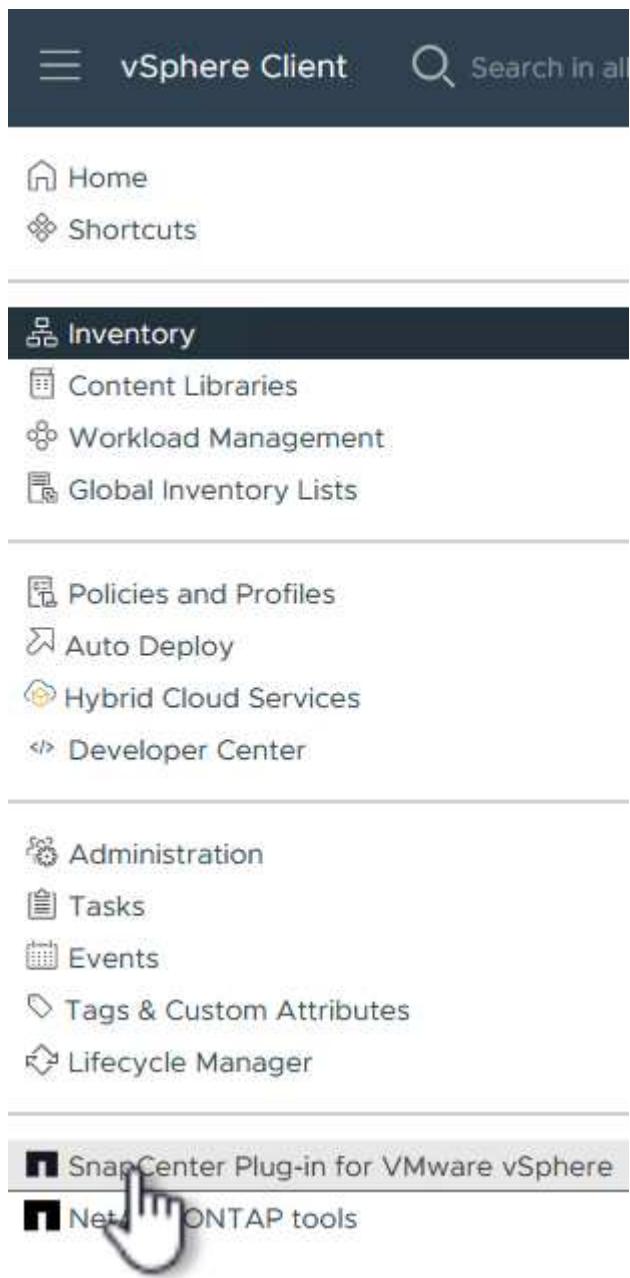


10. 最後に、「完了準備完了ページ」すべての設定を確認し、「完了」をクリックしてデプロイを開始します。

SCVにストレージシステムを追加する

SnapCenterプラグインをインストールしたら、次の手順を実行してストレージシステムをSCVに追加します。

1. SCVには、vSphere Clientのメインメニューからアクセスできます。



2. SCV UIインターフェイスの上部で、保護するvSphereクラスターに一致する正しいSCVインスタンスを選択します。

vSphere Client

Search in all environments

SnapCenter Plug-in for VMware vSphere INSTANCE 172.21.166.148:8080

Dashboard

Settings

3. 左側のメニューの「ストレージ システム」に移動し、「追加」をクリックして開始します。

vSphere Client

Search in all environments

SnapCenter Plug-in for VMware vSphere INSTANCE 172.21.166.148:8080

Storage Systems

Add Edit Delete Export

Name	Display Name
------	--------------

Dashboard

Settings

Resource Groups

Policies

Storage Systems

Guest File Restore

4. ストレージ システムの追加 フォームで、追加するONTAPストレージ システムの IP アドレスと資格情報を入力し、追加 をクリックしてアクションを完了します。

Add Storage System

×

Storage System	172.16.9.25
Authentication Method	<input checked="" type="radio"/> Credentials <input type="radio"/> Certificate
Username	admin
Password	*****
Protocol	HTTPS
Port	443
Timeout	60 Seconds
<input type="checkbox"/> Preferred IP	Preferred IP

Event Management System(EMS) & AutoSupport Setting

- Log Snapcenter server events to syslog
- Send AutoSupport Notification for failed operation to storage system

CANCEL

ADD



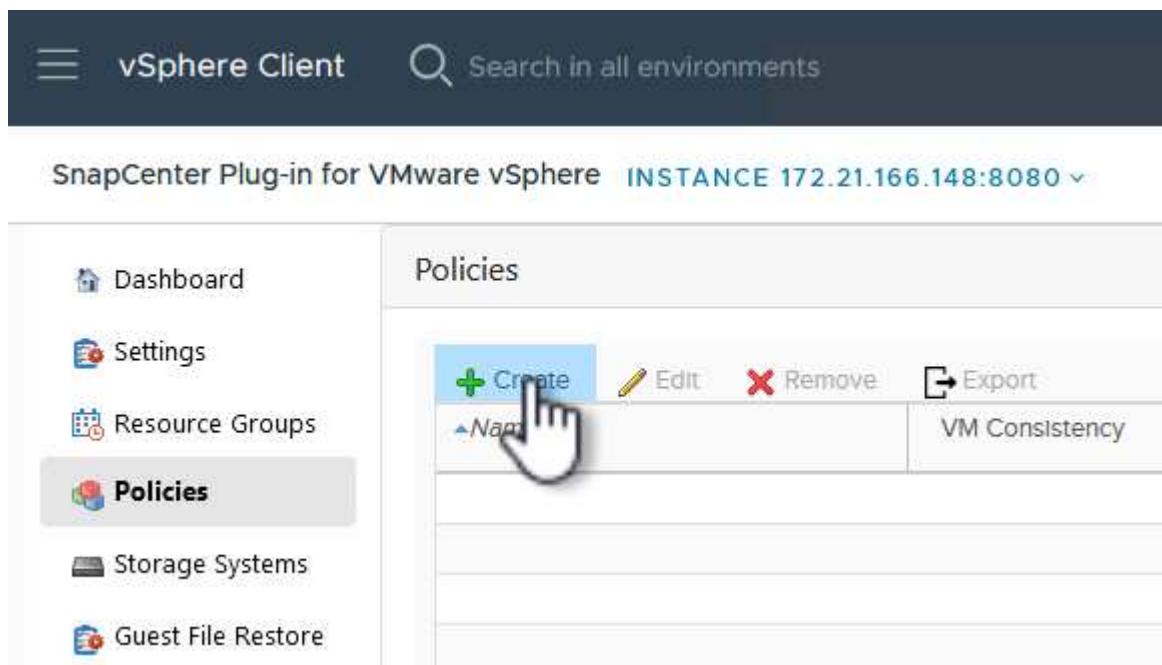
5. セカンダリ バックアップ ターゲットとして使用されるシステムを含む、管理する追加のストレージシステムに対してこの手順を繰り返します。

SCVでバックアップポリシーを構成する

SCVバックアップポリシーの作成の詳細については、以下を参照してください。["VMとデータストアのバックアップ ポリシーの作成"](#)。

新しいバックアップ ポリシーを作成するには、次の手順を実行します。

1. 左側のメニューから*ポリシー*を選択し、*作成*をクリックして開始します。



2. 新しいバックアップ ポリシー フォームで、ポリシーの名前と説明、バックアップを実行する頻度、およびバックアップを保持する期間を指定する保持期間を入力します。

ロック期間により、ONTAP SnapLock機能を使用して改ざん防止スナップショットを作成し、ロック期間を構成することができます。

*レプリケーション*の場合、ONTAPストレージボリュームの基礎となるSnapMirrorまたはSnapVault関係を更新する場合に選択します。



SnapMirrorとSnapVaultレプリケーションは、どちらもONTAP SnapMirrorテクノロジを使用してストレージボリュームをセカンダリストレージシステムに非同期的に複製し、保護とセキュリティを強化するという点で似ています。SnapMirror関係の場合、SCVバックアップポリシーで指定された保持スケジュールによって、プライマリボリュームとセカンダリボリュームの両方の保持が管理されます。SnapVault関係を使用すると、より長期の保持スケジュールや異なる保持スケジュールのために、セカンダリストレージシステムで個別の保持スケジュールを設定できます。この場合、スナップショットラベルはSCVバックアップポリシーとセカンダリボリュームに関連付けられたポリシーで指定され、独立した保持スケジュールを適用するボリュームを識別します。

追加の詳細オプションを選択し、「追加」をクリックしてポリシーを作成します。

New Backup Policy

X

Name	Daily_Snapmirror
Description	description
Frequency	Daily
Locking Period	<input type="checkbox"/> Enable Snapshot Locking <small>i</small>
Retention	Days to keep <input type="button" value="▼"/> 15 <input type="button" value="▲"/> <small>i</small>
Replication	<input checked="" type="checkbox"/> Update SnapMirror after backup <small>i</small> <input type="checkbox"/> Update SnapVault after backup <small>i</small>
	Snapshot label <input type="text"/>
Advanced <small>▼</small>	<input type="checkbox"/> VM consistency <small>i</small> <input type="checkbox"/> Include datastores with independent disks
Scripts <small>i</small>	<input type="text" value="Enter script path"/>

CANCEL

ADD



SCVでリソースグループを作成する

SCVリソースグループの作成の詳細については、以下を参照してください。["リソース グループの作成"](#)。

新しいリソース グループを作成するには、次の手順を実行します。

1. 左側のメニューから*リソース グループ*を選択し、*作成*をクリックして開始します。

The screenshot shows the vSphere Client interface. On the left, there is a sidebar with the following menu items: Dashboard, Settings, Resource Groups (which is currently selected and highlighted in red), Policies, Storage Systems, and Guest File Restore. The main pane is titled 'Resource Groups' and contains a table with columns for Name, Description, and Actions (Edit, Delete, Run Now). At the top of this table, there is a blue button labeled '+ Create' with a white plus sign, and a hand cursor is pointing directly at it. There are also other buttons for Edit, Delete, and Run Now.

2. *一般情報と通知*ページで、リソース グループの名前、通知設定、スナップショットの命名に関する追加オプションを指定します。
3. リソース ページで、リソース グループ内で保護するデータストアと VM を選択します。続行するには、[次へ] をクリックします。



特定の仮想マシンのみを選択した場合でも、データストア全体が常にバックアップされます。これは、ONTAP がデータストアをホストしているボリュームのスナップショットを取得するためです。ただし、バックアップ対象として特定の VM のみを選択すると、それらの VM のみに復元する機能が制限されることに注意してください。

Create Resource Group

1. General info & notification

Scope: Virtual Machines

2. Resource

Parent entity: VCF_WKLD_03_iSCSI

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Available entities

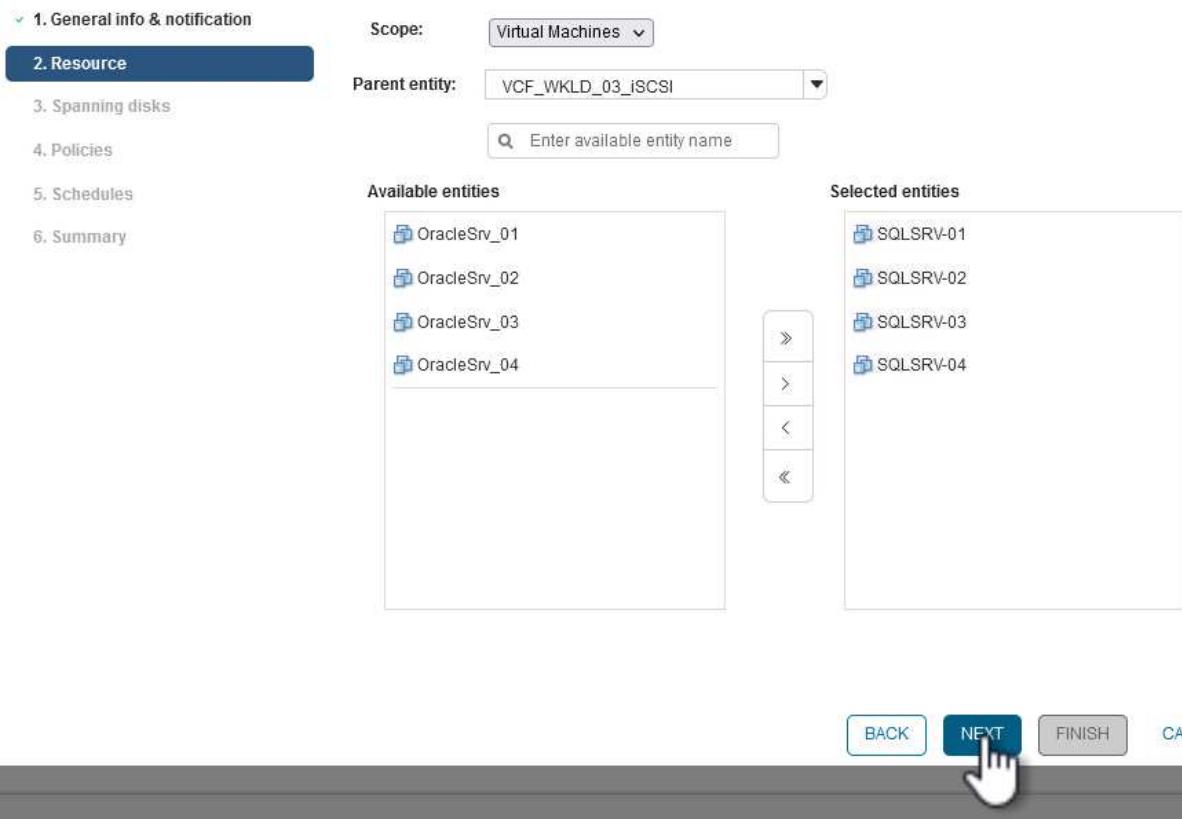
- OracleSrv_01
- OracleSrv_02
- OracleSrv_03
- OracleSrv_04

Selected entities

- SQLSRV-01
- SQLSRV-02
- SQLSRV-03
- SQLSRV-04

Enter available entity name

BACK NEXT FINISH CANCEL



4. スパニング ディスク ページで、複数のデータストアにまたがる VMDK を持つ VM を処理する方法のオプションを選択します。続行するには、[次へ] をクリックします。

Create Resource Group

- ✓ 1. General info & notification
 - Always exclude all spanning datastores
This means that only the datastores directly added to the resource group and the primary datastore of VMs directly added to the resource group will be backed up
 - ✓ 2. Resource
 - 3. Spanning disks**
 - 4. Policies
 - 5. Schedules
 - 6. Summary
- Always include all spanning datastores
All datastores spanned by all included VMs are included in this backup
- Manually select the spanning datastores to be included i
You will need to modify the list every time new VMs are added

There are no spanned entities in the selected virtual entities list.



5. ポリシー ページで、このリソース グループで使用される以前に作成したポリシーまたは複数のポリシーを選択します。続行するには、[次へ] をクリックします。

Create Resource Group

1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Create

<input type="checkbox"/>	Name	VM Consistent	Include independent di...	Schedule
<input checked="" type="checkbox"/>	Daily_Snapmirror	No	No	Daily
<input type="checkbox"/>				

BACK **NEXT** FINISH CANCEL

6. スケジュールページで、繰り返しと時刻を設定して、バックアップを実行するタイミングを確立します。続行するには、[次へ] をクリックします。

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource Daily_Snapmi... ▾ Type Daily

✓ 3. Spanning disks Every 1 Day(s)

✓ 4. Policies Starting 04/04/2024

5. Schedules At 04 45 PM

6. Summary

BACK **NEXT** FINISH CANCEL



7. 最後に*概要*を確認し、*完了*をクリックしてリソース グループを作成します。

Create Resource Group

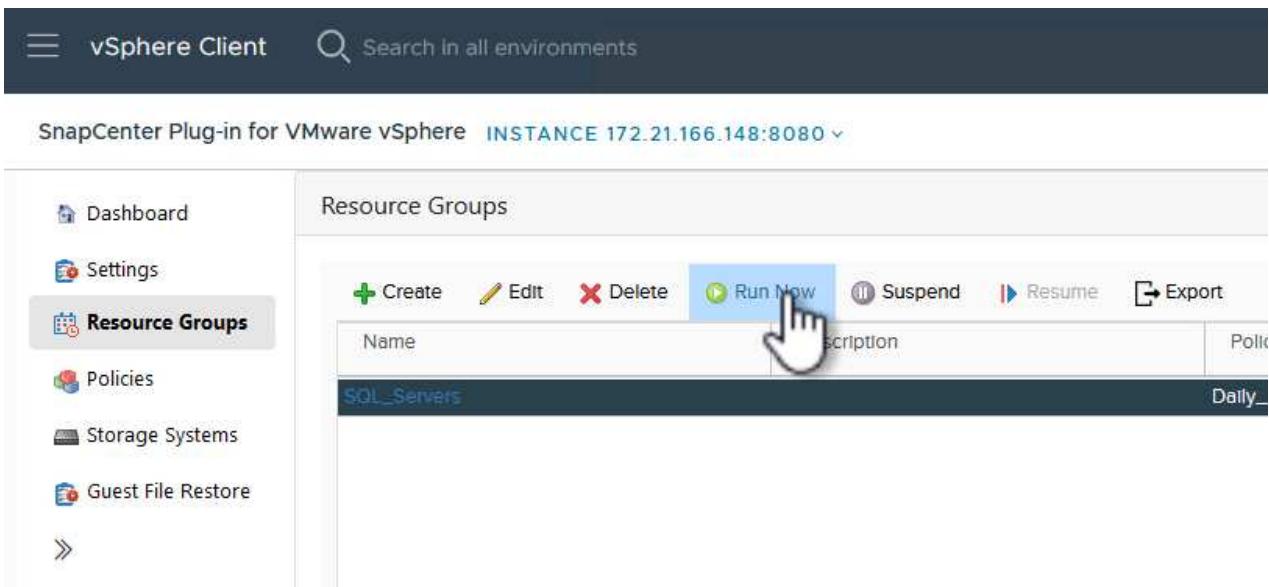
- ✓ 1. General info & notification
- ✓ 2. Resource
- ✓ 3. Spanning disks
- ✓ 4. Policies
- ✓ 5. Schedules
- 6. Summary**

Name	SQL_Servers		
Description			
Send email	Never		
Latest Snapshot name	None <small>?</small>		
Custom snapshot format	None <small>?</small>		
Entities	SQLSRV-01, SQLSRV-02, SQLSRV-03, SQLSRV-04		
Spanning	False		
Policies	Name	Frequency	Snapshot Locking Period
	Daily_Snapmir...	Daily	-

BACK NEXT **FINISH** CANCEL



8. リソース グループを作成したら、[今すぐ実行] ボタンをクリックして最初のバックアップを実行します。



vSphere Client Search in all environments

SnapCenter Plug-in for VMware vSphere INSTANCE 172.21.166.148:8080

Resource Groups	
Resource Groups	Run Now 
Create	Edit
Delete	Suspend
Resume	Export
Name	Description
SQL_Servers	Daily

9. ダッシュボードに移動し、最近のジョブアクティビティの下にあるジョブ ID の横にある番号をク

リックしてジョブモニターを開き、実行中のジョブの進行状況を表示します。

The screenshot shows the vSphere Client interface with the 'SnapCenter Plug-in for VMware vSphere' instance at '172.21.166.148:8080'. The left sidebar has 'Dashboard' selected. The main area is titled 'Dashboard' with tabs for 'Status', 'Job Monitor', 'Reports', and 'Getting Started'. Under 'RECENT JOB ACTIVITIES', there is a tooltip for a job named 'Backup Running SQL_Servers' with 'Job ID: 6' and '1 min ago'. The tooltip details the job's progress: 'Backup of Resource Group 'SQL_Servers' with Policy 'Daily_Snapmirror''. It lists several sub-tasks with green checkmarks: 'Retrieving Resource Group and Policy information', 'Discovering Resources', 'Validate Retention Settings', 'Quiescing Applications', 'Retrieving Metadata', 'Creating Snapshot copy', 'Unquiescing Applications', and 'Registering Backup'. Below the tasks, it says 'Running, Start Time: 04/04/2024 04:39:01 PM.' At the bottom of the tooltip are 'CLOSE' and 'DOWNLOAD JOB LOGS' buttons.

SCV を使用して VM、VMDK、およびファイルを復元する

SnapCenterプラグインを使用すると、プライマリ バックアップまたはセカンダリ バックアップから VM、VMDK、ファイル、フォルダーを復元できます。

VM は、元のホスト、同じ vCenter Server 内の代替ホスト、または同じ vCenter またはリンク モードの任意の vCenter によって管理される代替 ESXi ホストに復元できます。

vVol VM は元のホストに復元できます。

従来の VM の VMDK は、元のデータストアまたは代替データストアに復元できます。

vVol VM 内の VMDK は元のデータストアに復元できます。

ゲスト ファイル復元セッション内の個々のファイルとフォルダーを復元できます。このセッションでは、仮想ディスクのバックアップ コピーが添付され、選択したファイルまたはフォルダーが復元されます。

VM、VMDK、または個々のフォルダーを復元するには、次の手順を実行します。

SnapCenter プラグインを使用して VM を復元する

SCV を使用して VM を復元するには、次の手順を実行します。

1. vSphere クライアントで復元する VM に移動し、右クリックして * SnapCenter Plug-in for VMware vSphere* に移動します。サブメニューから*復元*を選択します。

vSphere Client Search in all environments

OracleSrv_04

Summary Monitor Configure Permissions

Guest OS

Actions - OracleSrv_04

- Power
- Guest OS
- Snapshots
- Open Remote Console

Migrate...

Clone

Fault Tolerance

VM Policies

Template

Compatibility

Export System Logs...

Edit Settings...

Move to folder...

Rename...

Edit Notes...

Tags & Custom Attributes

Add Permission...

Alarms

Remove from Inventory

Delete from Disk

vSAN

NetApp ONTAP tools

Create Resource Group

Add to Resource Group

Attach Virtual Disk(s)

Detach Virtual Disk(s)

Restore

File Restore

Recent Tasks

Task Name

Manage Columns Run

SnapCenter Plug-in for VMware vSphere

4 CPU(s), 22 MHz used

32 GB, 0 GB memory active

100 GB | Thin Provision ⓘ
VCF_WKLD_03_iSCSI

(of 2) vcf-wkld-01-IT-INF-WKLD-01-vc
(connected) | 00:50:56:83:02:f1

Disconnected ⓘ

ESXi 7.0 U2 and later (VM vers

Manage Columns Run

SnapCenter Plug-in for VMware vSphere



別の方法としては、インベントリ内のデータストアに移動し、[構成] タブで [SnapCenter Plug-in for VMware vSphere] > [バックアップ] に移動します。選択したバックアップから、復元する VM を選択します。

The screenshot shows the vSphere Client interface. On the left, the inventory tree displays several datastores under 'vcf-m01-vc01.sddc.netapp.com' and 'vcf-wkld-vc01.sddc.netapp.com'. A blue number '1' points to the 'vcf-wkld-vc01.sddc.netapp.com' node. A blue number '2' points to the 'VCF_WKLD_03_iSCSI' datastore. In the center, the 'Backups' tab is selected within the 'SnapCenter Plug-in for VMwa...' section. A blue number '3' points to the 'Backups' tab. The main pane shows a table of backup entries:

Name	Status	Locations	Snapshot Loc.	Created Time	Mounted	Policy	VMware Sn...
VCF_WKLD_iSCl_Destore_04-12-2024_12:50:01.0083	Completed	Primary & Secondary	-	4/12/2024 12:50:06 PM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCl_Destore_04-12-2024_15:50:01.0083	Completed	Primary & Secondary	-	4/12/2024 11:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCl_Destore_04-12-2024_10:50:01.0014	Completed	Primary & Secondary	-	4/12/2024 10:50:07 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCl_Destore_04-12-2024_09:50:01.0087	Completed	Primary & Secondary	-	4/12/2024 9:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCl_Destore_04-12-2024_07:50:01.0050	Completed	Primary & Secondary	-	4/12/2024 8:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCl_Destore_04-12-2024_07:50:01.0237	Completed	Primary & Secondary	-	4/12/2024 7:50:07 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCl_Destore_04-12-2024_06:50:01.0068	Completed	Primary & Secondary	-	4/12/2024 6:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCl_Destore_04-12-2024_05:50:01.0025	Completed	Primary & Secondary	-	4/12/2024 5:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCl_Destore_04-12-2024_04:50:01.0062	Completed	Primary & Secondary	-	4/12/2024 4:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCl_Destore_04-12-2024_03:50:01.0035	Completed	Primary & Secondary	-	4/12/2024 3:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCl_Destore_04-12-2024_02:50:01.0122	Completed	Primary & Secondary	-	4/12/2024 2:50:08 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCl_Destore_04-12-2024_01:50:01.0138	Completed	Primary & Secondary	-	4/12/2024 1:50:07 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCl_Destore_04-12-2024_00:50:01.0067	Completed	Primary & Secondary	-	4/12/2024 0:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCl_Destore_04-11-2024_23:50:01.0062	Completed	Primary & Secondary	-	4/11/2024 11:50:06 PM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCl_Destore_04-11-2024_22:50:01.0000	Completed	Primary & Secondary	-	4/11/2024 10:50:06 PM	No	Hourly_Snapmirror	No

2. *復元*ウィザードで、使用的するバックアップを選択します。続行するには、[次へ] をクリックします。

Restore

The screenshot shows the 'Select backup' step of the restore wizard. The left sidebar lists steps: 1. Select backup (highlighted), 2. Select scope, 3. Select location, 4. Summary. The main area has a search bar 'Search for Backups' and a table titled 'Available backups'.

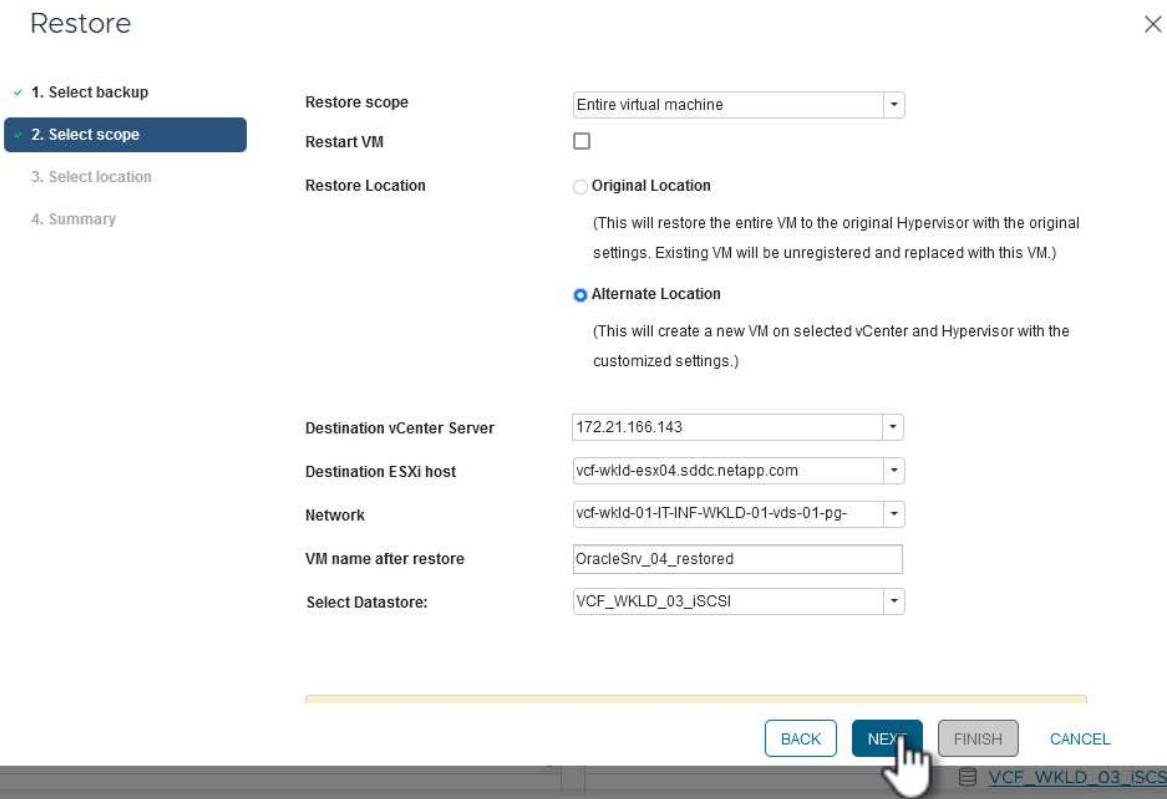
(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF_WKLD_jSCl_...	4/4/2024 4:50:0...	No	Hourly_Snapmirror	No
VCF_WKLD_jSCl_...	4/4/2024 4:45:1...	No	Hourly_Snapmirror	No

At the bottom, there are buttons: BACK, NEXT (highlighted with a cursor), FINISH, and CANCEL.

3. *範囲の選択*ページで、すべての必須フィールドに入力します。

- 復元範囲 - 仮想マシン全体を復元する場合に選択します。
- VM を再起動 - 復元後に VM を起動するかどうかを選択します。
- 復元場所 - 元の場所に復元するか、別の場所に復元するかを選択します。別の場所を選択するときは、各フィールドからオプションを選択します。
 - 宛先 vCenter Server - ローカル vCenter またはリンク モードの代替 vCenter
 - 宛先ESXiホスト
 - ネットワーク
 - 復元後のVM名
 - データストアを選択:



続行するには、[次へ] をクリックします。

- *場所の選択*ページで、プライマリまたはセカンダリのONTAPストレージ システムから VM を復元することを選択します。続行するには、[次へ] をクリックします。

Restore

✓ 1. Select backup

✓ 2. Select scope

3. Select location

4. Summary

Destination datastore	Locations
VCF_WKLD_03_iSCSI	(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI
	(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI
	(Secondary) svm_iscsi:VCF_WKLD_03_iSCSI_dest



- 最後に、*概要*を確認し、「完了」をクリックして復元ジョブを開始します。

Restore

✓ 1. Select backup

✓ 2. Select scope

✓ 3. Select location

4. Summary

Virtual machine to be restored	OracleSrv_04
Backup name	VCF_WKLD_iSCI_Datastore_04-04-2024_16.50.00.0940
Restart virtual machine	No
Restore Location	Alternate Location
Destination vCenter Server	172.21.166.143
ESXi host to be used to mount the backup	vcf-wkld-esx04.sddc.netapp.com
VM Network	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
Destination datastore	VCF_WKLD_03_iSCSI
VM name after restore	OracleSrv_04_restored



Change IP address of the newly created VM after restore operation to avoid IP conflict.

BACK

NEXT

FINISH

CANCEL

WF_WKLD_03

をクリックして復元ジョブを開始します"]

- 復元ジョブの進行状況は、vSphere Client の 最近のタスク ペインと SCV のジョブ モニターから監視できます。

vSphere Client Search in all environments

SnapCenter Plug-in for VMware vSphere INSTANCE 172.21.166.148:8080

RECENT JOB ACTIVITIES

- Restore Running [Job ID:18] VCF_WKLD_ISCI_Datastore_04-04-20... 1 min ago
- Backup Successful [Job ID:15] VCF_WKLD_ISCI_Datastore 8 min ago
- Backup Successful [Job ID:12] VCF_WKLD_ISCI_Datastore 13 min ago
- Backup Successful [Job ID:9] SQL_Servers 13 min ago
- Backup Successful [Job ID:6] SQL_Servers 19 min ago

CONFIGURATION

- 11 Virtual Machines
- 6 Datastores
- 14 SVMs
- 2 Resource Groups
- 2 Backup Policies

Job Details : 18

Restoring backup with name: VCF_WKLD_ISCI_Datastore_04-04-2024_16.50.00.0940

Preparing for Restore: Retrieving Backup metadata from Repository.

Pre Restore

Restore

Running, Start Time: 04/04/2024 04:58:24 PM.

CLOSE DOWNLOAD JOB LOGS

No data to display.

Task Name	Target	Status	Details	Initiator	Queued For	Start Time
NetApp Mount Datastore	[vcf-wkld-esx04.sdd c.netapp.com]	35%	Mount operation completed successfully.	VCF.LOCAL\Administrator	6 ms	04/04/2024, 4:58:27 PM
NetApp Restore	[vcf-wkld-esx04.sdd c.netapp.com]	2%	Restore operation started.	VCF.LOCAL\Administrator	10 ms	04/04/2024, 4:58:27 PM

Recent Tasks Alarms

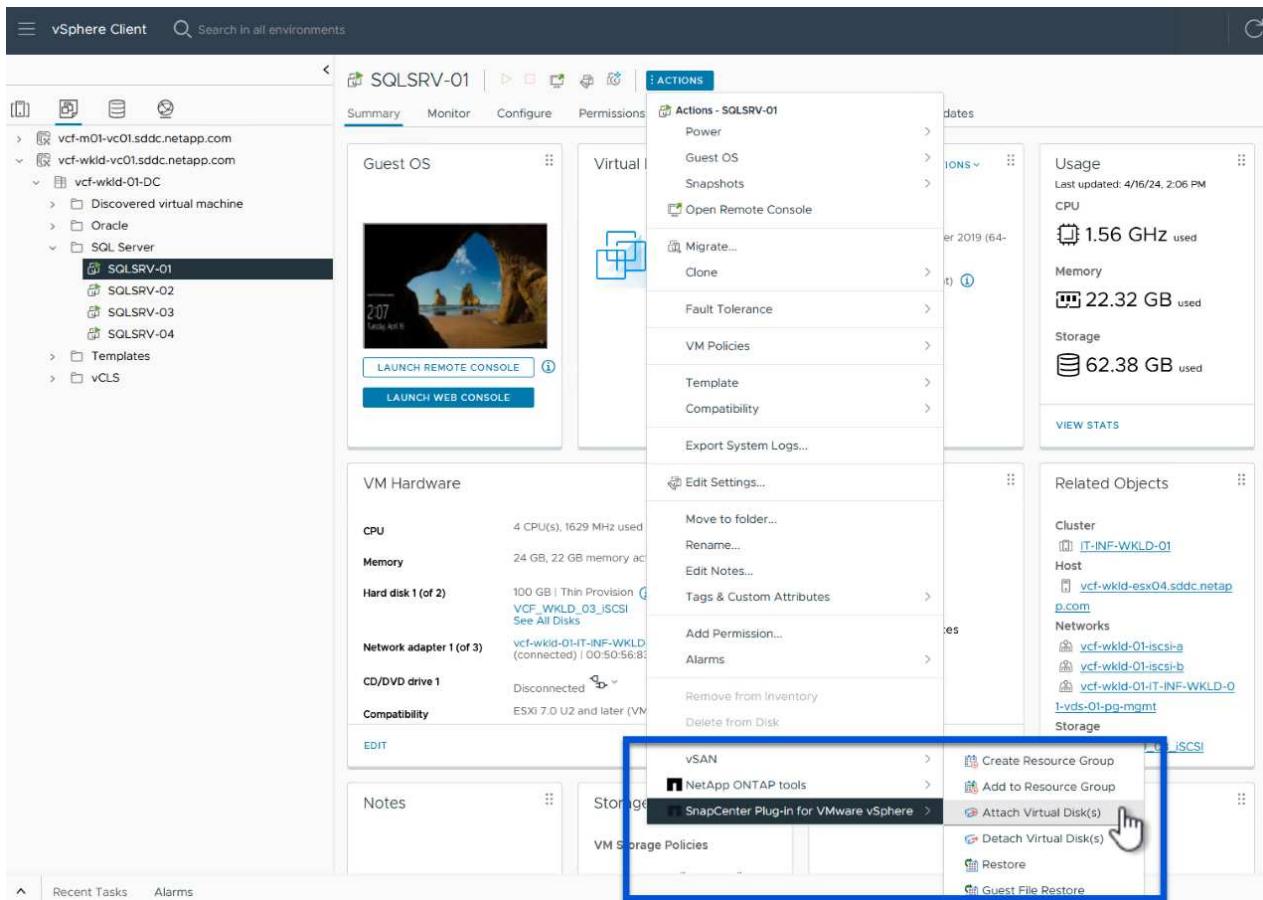
Manage Columns Running More Tasks

SnapCenterプラグインを使用してVMDKを復元する

ONTAPツールを使用すると、VMDKを元の場所に完全に復元したり、VMDKを新しいディスクとしてホストシステムに接続したりすることができます。このシナリオでは、ファイルシステムにアクセスするために、VMDKがWindowsホストに接続されます。

バックアップからVMDKをアタッチするには、次の手順を実行します。

1. vSphere ClientでVMに移動し、[アクション]メニューから[SnapCenter Plug-in for VMware vSphere] > [仮想ディスクの接続]を選択します。



2. *仮想ディスクの接続*ウィザードで、使用するバックアップインスタンスと接続する特定のVMDKを選択します。

Attach Virtual Disk(s)

X

[Click here to attach to alternate VM](#)

Backup

(This list shows primary backups. [1](#) Click here to modify the filter to display primary and secondary backups.)

Search for Backups

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0218	4/17/2024 9:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_08.50.01.0223	4/17/2024 8:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_07.50.01.0204	4/17/2024 7:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_06.50.01.0194	4/17/2024 6:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_05.50.01.0245	4/17/2024 5:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_04.50.01.0231	4/17/2024 4:50:01 AM	No	Hourly_Snapmirror	No

Select disks

<input type="checkbox"/> Virtual disk	Location
<input type="checkbox"/> [VCF_WKLD_03_ISCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.C
<input checked="" type="checkbox"/> [VCF_WKLD_03_ISCSI] SQLSRV-01/SQLSRV-01_1.v...	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.C



フィルター オプションを使用すると、バックアップを検索したり、プライマリストレージシステムとセカンダリストレージシステムの両方からのバックアップを表示したりできます。

Attach Virtual Disk(s)

X

[Click here to attach to alternate VM](#)

Backup

(This list shows primary backup

Search for Backups

Name
VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0218
VCF_WKLD_iSCSI_Datastore_04-17-2024_08.50.01.0223
VCF_WKLD_iSCSI_Datastore_04-17-2024_07.50.01.0204
VCF_WKLD_iSCSI_Datastore_04-17-2024_06.50.01.0194
VCF_WKLD_iSCSI_Datastore_04-17-2024_05.50.01.0245
VCF_WKLD_iSCSI_Datastore_04-17-2024_04.50.01.0231

Time range

From

To

Select disks

Virtual disk

[VCF_WKLD_03_ISCSI] SQLSRV-01/SQLSRV-01.vmdk

[VCF_WKLD_03_ISCSI] SQLSRV-01/SQLSRV-01_1.v...

Time range

From

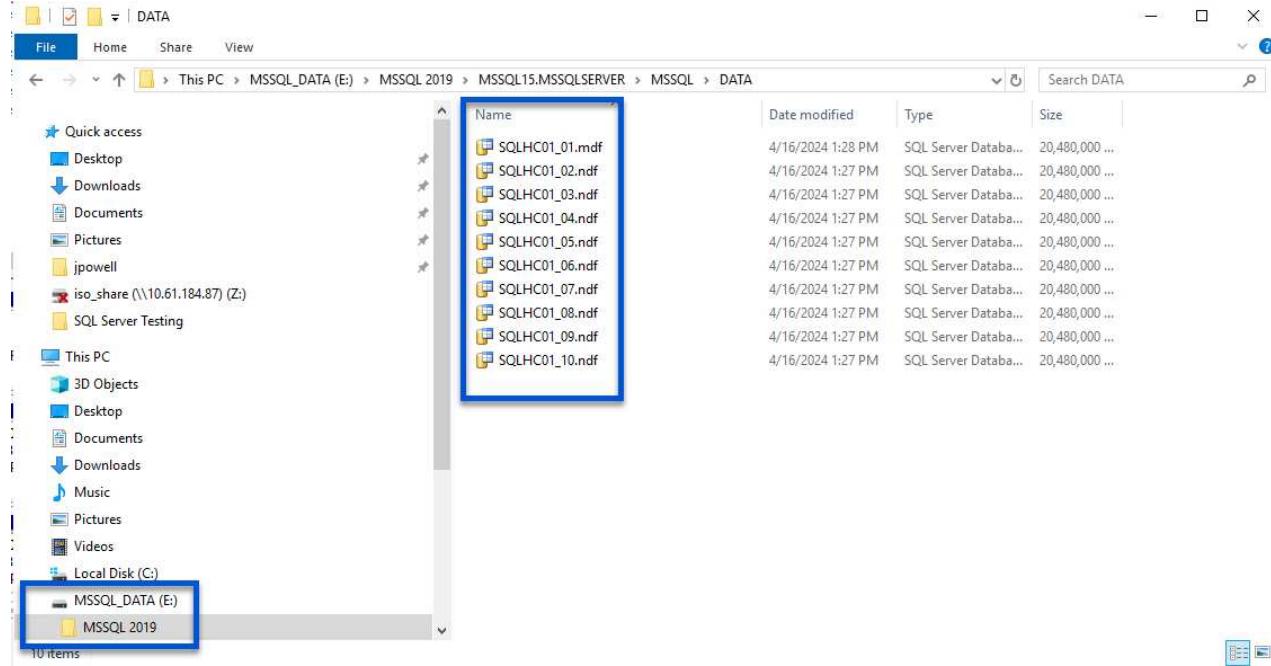
To

VMware snapshot

Mounted

Location

3. すべてのオプションを選択したら、[Attach] ボタンをクリックして復元プロセスを開始し、VMDK をホストに接続します。
4. アタッチ手順が完了すると、ホストシステムの OS からディスクにアクセスできるようになります。この場合、SCV は NTFS ファイルシステムを備えたディスクを Windows SQL Server の E: ドライブに接続し、ファイルシステム上の SQL データベース ファイルはファイル エクスプローラーからアクセスできるようになります。



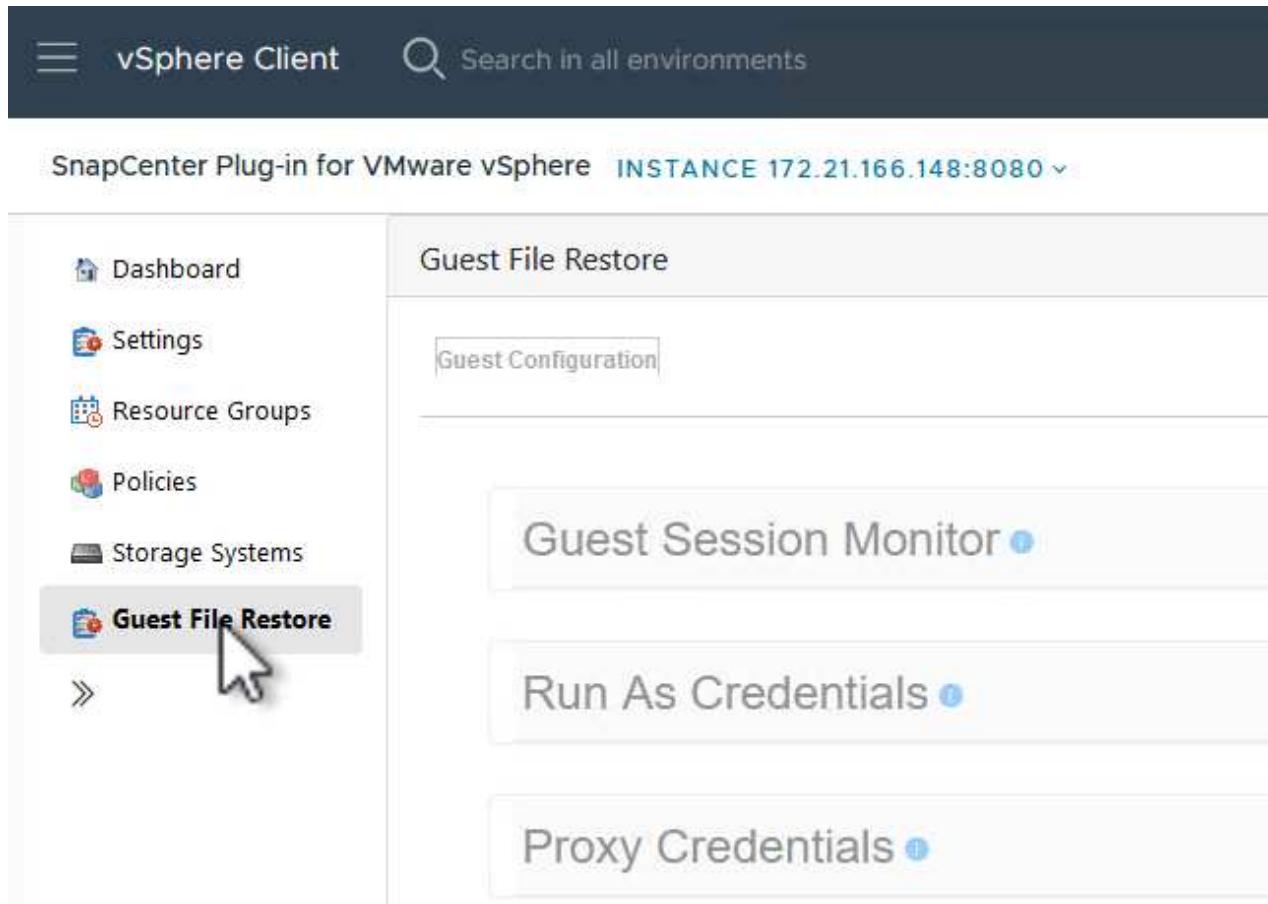
SnapCenter プラグインを使用したゲストファイルシステムの復元

ONTAPツールは、Windows Server OS 上の VMDK からのゲスト ファイル システムの復元機能を備えています。これは、SnapCenter プラグイン インターフェースから集中的に実行されます。

詳細については、"ゲスト ファイルとフォルダの復元" SCV ドキュメント サイト。

Windows システムのゲスト ファイル システムの復元を実行するには、次の手順を実行します。

- 最初のステップは、Windows ホスト システムへのアクセスを提供するための実行資格情報を作成することです。vSphere Client で CSV プラグイン インターフェイスに移動し、メイン メニューの ゲスト ファイル のリストア をクリックします。



- [実行資格情報] の下にある *+ アイコンをクリックして、[実行資格情報] ウィンドウを開きます。
- 資格情報レコードの名前、Windows システムの管理者のユーザー名とパスワードを入力し、[VM の選択] ボタンをクリックして、復元に使用するオプションの Proxy VM を選択しま

Run As Credentials

X

Run As Name	Administrator	
Username	administrator	
Password	*****	
Authentication Mode	Windows	
VM Name	<input type="text"/>	 Select VM
		
		 CANCEL  SAVE

す。

4. プロキシ VM ページで VM の名前を指定し、ESXi ホストまたは名前で検索して VM を見つけます。選択したら、[保存] をクリックします。

Proxy VM



VM Name

SQLSRV-01

Search by ESXi Host

ESXi Host

vcf-wkld-esx04.sddc.netapp.com

Virtual Machine

SQLSRV-01

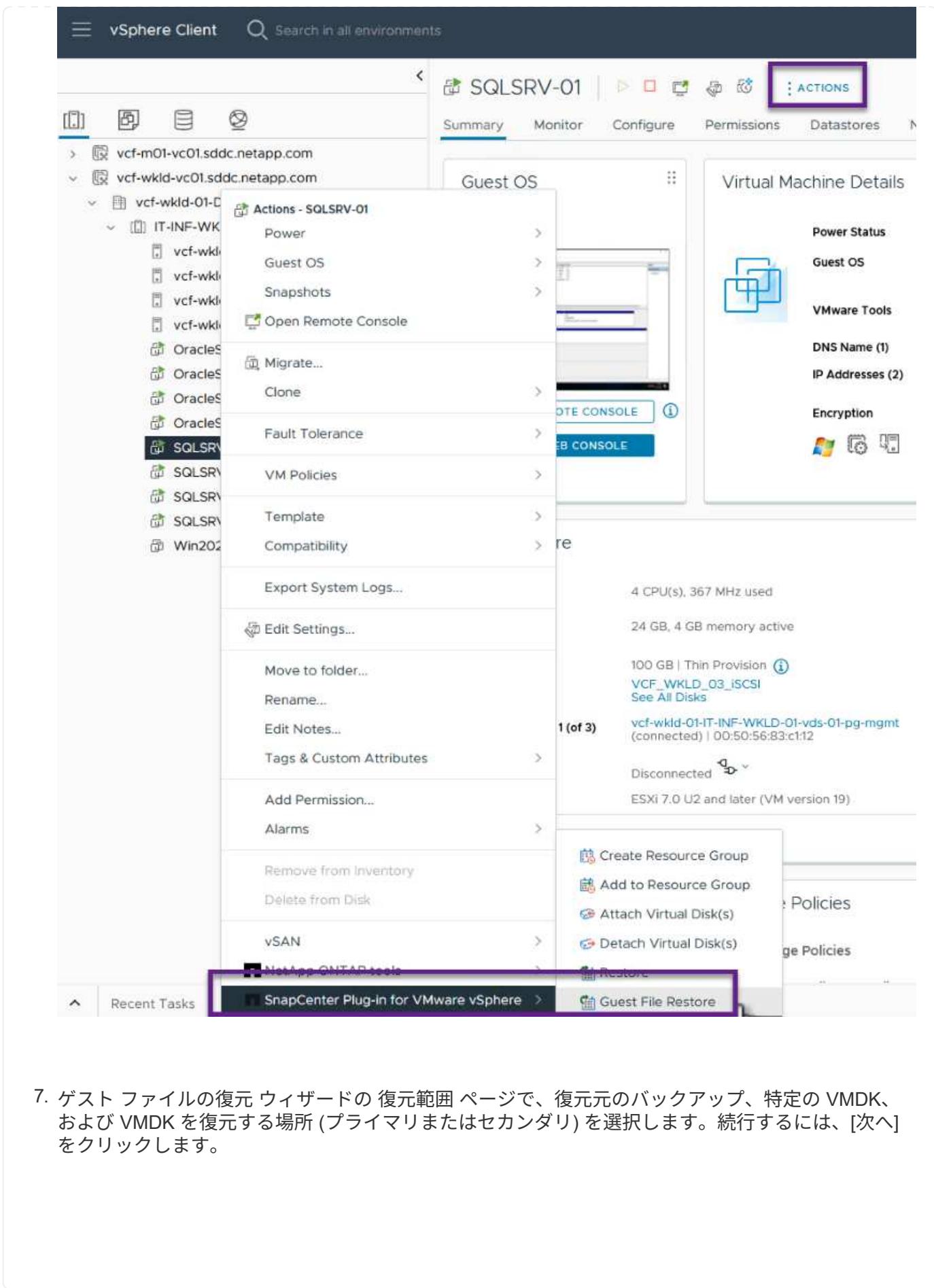
Search by Virtual Machine name

CANCEL

SAVE



5. Run As Credentials ウィンドウでもう一度 Save をクリックして、レコードの保存を完了します。
6. 次に、インベントリ内の VM に移動します。【アクション】メニューから、または VM を右クリックして、* [SnapCenter Plug-in for VMware vSphere] > [ゲスト ファイルのリストア]* を選択します。



Guest File Restore

X

1. Restore Scope

2. Guest Details

3. Summary

Backup Name	Start Time	End Time
SQL_Servers_04-16-2024_13.52.3...	4/16/2024 1:52:34 PM	4/16/2024 1:52:40 PM
VCF_WKLD_iSCSI_Datastore_04-1...	4/16/2024 1:50:01 PM	4/16/2024 1:50:08 PM

VMDK
[VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk
[VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.vmdk

Locations
Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:SQL_Servers_04-16-2024_13.52.34.0329
Secondary:svm_iscsi:VCF_WKLD_03_iSCSI_dest:SQL_Servers_04-16-2024_13.52.34.0329

BACK **NEXT** FINISH CANCEL



EDIT

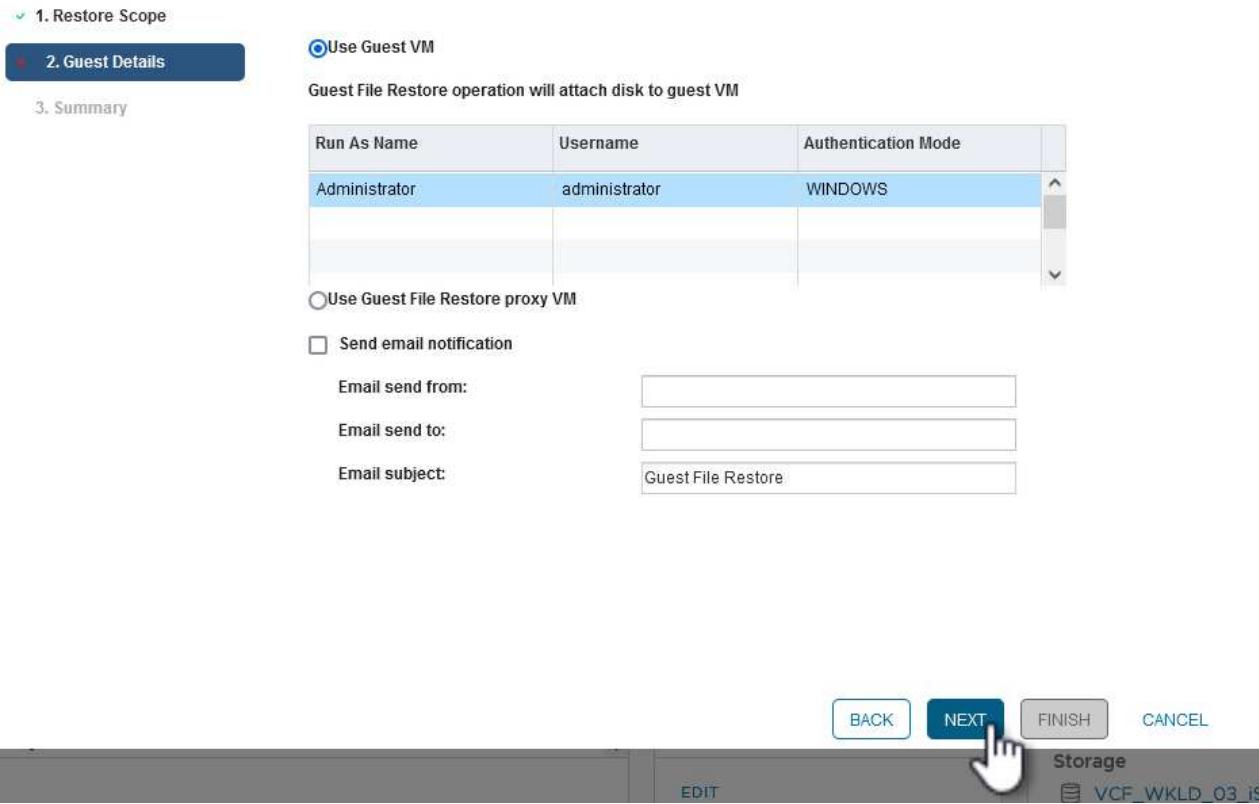
Storage

VCF_WKLD_03_iS...

8. ゲストの詳細*ページで、復元に*ゲスト VM を使用するか、ゲスト ファイル復元プロキシ VM を使用するかを選択します。また、必要に応じて、ここで電子メール通知設定を入力してください。続行するには、[次へ] をクリックします。

Guest File Restore

X



- 最後に、[概要] ページを確認し、[完了] をクリックしてゲストファイルシステムの復元セッションを開始します。
- SnapCenterプラグインインターフェイスに戻り、もう一度 ゲストファイルリストアに移動し、ゲストセッションモニターで実行中のセッションを表示します。続行するには、「ファイルの参照」の下のアイコンをクリックします。

Backup Name	Source VM	Disk Path	Guest Mount Path	Time To Expire	Browse Files
SQL_Servers_04-16-2024_13.52.34.0329	SQLSRV-01	/VCF_WKLD_03_iSCSI/sc-202404161419...	E:\	23h:58m	Browse Files

- ゲストファイルの参照 ウィザードで、復元するフォルダーまたはファイルと、復元先のファイルシステムの場所を選択します。最後に、「復元」をクリックして、「復元」プロセスを開始します。

Guest File Browse

X

Select File(s)/Folder(s) to Restore

Name		Size	
<input type="checkbox"/>	MSSQL15.MSSQLSERVER		
Selected 0 Files / 1 Directory			
Name	Path	Size	Delete
MSSQL 2019	E:\MSSQL 2019		

Select Restore Location

^

Select address family for UNC path:

IPv4

IPv6

Either Files to Restore or Restore Location is not selected!

CANCEL

RESTORE

Select Restore Location

Select address family for UNC path:

IPv4
 IPv6

Restore to path

Provide UNC path to the guest where files will be restored. eg: \\10.60.136.65\c\$

Run As Credentials while triggering the Guest File Restore workflow will be used to connect to the UNC path

If original file(s) exist:

Always overwrite
 Always skip

Disconnect Guest Session after successful restore

CANCEL RESTORE



12. リストアジョブは、vSphere Client のタスクペインから監視できます。

追加情報

VCFの設定方法については、以下を参照してください。 "[VMware Cloud Foundation ドキュメント](#)"。

ONTAPストレージシステムの構成については、 "[ONTAP 9 ドキュメント](#)" 中心。

SnapCenter Plug-in for VMware vSphereの使用については、 "[SnapCenter Plug-in for VMware vSphereのドキュメント](#)"。

VMware vSphere 用のSnapCenterプラグインを使用して VCF 管理ドメインとワークロード ドメインを保護する

SnapCenter Plug-in for VMware vSphereを使用して、複数の VCF ドメインを保護します。この手順には、各ドメインのプラグインの設定、バックアップポリシーの構成、および復元操作の実行が含まれます。

VMware Cloud Foundation (VCF) ワークロード ドメインを使用すると、組織はリソースを論理的に異なるドメインに分割して、さまざまなワークロードをグループ化し、セキュリティとフォールトトレランスを強化できます。

はじめに

ドメインは独立して拡張でき、特定のコンプライアンスに準拠し、マルチテナント機能を提供できます。VMware Cloud Foundation (VCF) のデータ保護は、管理ドメインとワークロード ドメイン全体のデータの可用性、整合性、および回復可能性を確保するための重要な要素です。NetApp SnapCenter Plug-in for VMware vSphere (SCV) は、NetApp のデータ保護機能を VMware 環境に統合する強力なツールです。NetAppストレージでホストされている VMware vSphere 仮想マシン (VM) のバックアップ、復元、クローン作成を簡素化します。

このドキュメントでは、SCV を使用して VCF の複数のドメインを保護するための展開手順について説明します。

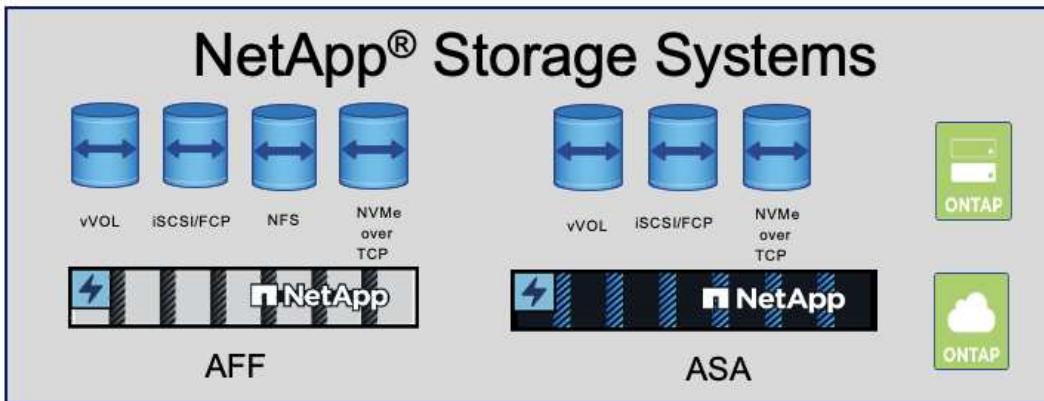
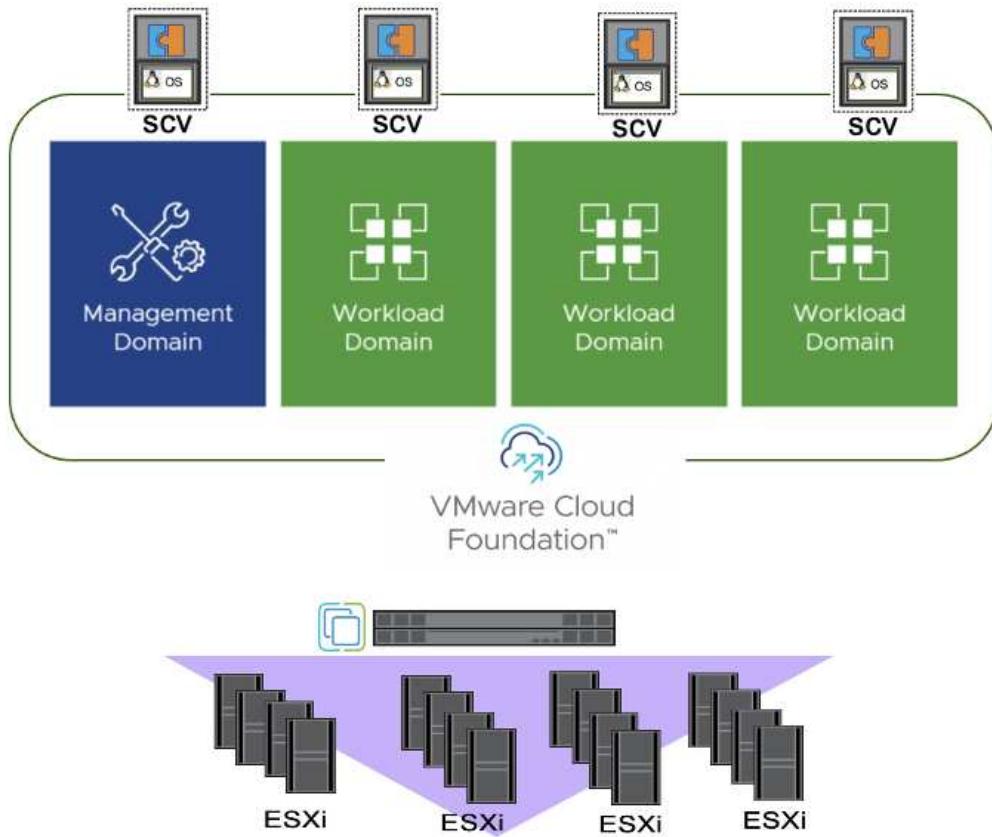
観客

VMware VCF ワークロード ドメインのデータ保護と災害復旧を保証するソリューション アーキテクトまたはストレージ管理者。

アーキテクチャの概要

SCV は、OVA ファイルを使用して Linux 仮想アプライアンスとして導入され、VM、データストア、ファイル、フォルダーに対して、高速でスペース効率が高く、クラッシュ整合性があり、VM 整合性のあるバックアップおよび復元操作を提供します。SCV はリモート プラグイン アーキテクチャを使用します。VCF 管理ドメイン vCenter に複数の SCV が展開されホストされていました。SCV と VCF ドメインは 1 対 1 の関係であるため、VCF 管理ドメインと各ワークロード ドメインには 1 つの SCV が必要です。

ONTAP FAS、AFF、または All SAN Array (ASA) プライマリ システム上にあり、ONTAP FAS、AFF、または ASA セカンダリ システムに複製されたデータ。SCV は SnapCenter Server と連携して、SnapCenter アプリケーション固有のプラグインの VMware 環境でのアプリケーションベースのバックアップおよび復元操作もサポートします。詳細については、["SnapCenter Plug-in for VMware vSphere のドキュメント。"](#)

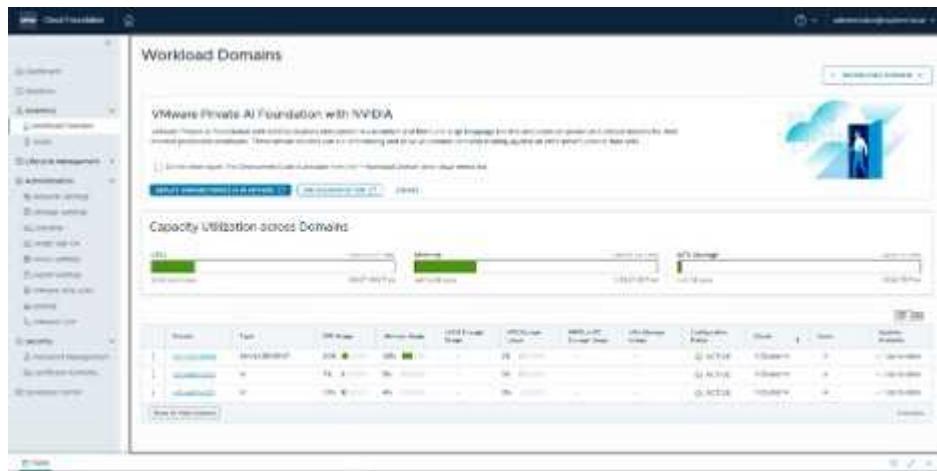


3-2-1 バックアップ ルールは、データのコピーを 3 つ作成し、それらを 2 種類の異なるメディアに保存し、1 つのコピーをオフサイトに保管するというデータ保護戦略です。BlueXP backup and recoveryは、オンプレミスとクラウド環境の両方にわたる幅広いバックアップおよびリカバリ操作に対して単一のコントロール プレーンを提供する、クラウド ベースのデータ管理ツールです。NetApp BlueXP backup and recoveryスイートの一部は、SCV(オンプレミス)と統合してデータのコピーをクラウド内のオブジェクトストレージに拡張する機能です。これにより、プライマリまたはセカンダリリストレージ バックアップから取得されたデータの 3 番目のコピーがオフサイトに作成されます。BlueXP backup and recoveryを使用すると、オンプレミスのこれら 2 つの場所のいずれかからデータのコピーを転送するストレージ ポリシーを簡単に設定できます。詳細については、["SnapCenter プラグインとBlueXP backup and recoveryによる VMware の 3-2-1 データ保護"](#)。

管理ドメインと複数のワークロードドメインを備えた VCF を展開する

VCF ワークロード ドメインは、SDDC Manager によってプロビジョニングされ、アプリケーションの準備が

整った、1つ以上のvSphere クラスターを持つESXi ホストのグループです。以下のVCF の例では、1つの管理ドメインと2つのワークロード ドメインがデプロイされています。NetAppストレージでVCFを導入する方法の詳細については、以下を参照してください。["NetApp VCF 導入ドキュメント。"](#)



SCV の展開、構成、および復元手順

ワークロード ドメインの数と管理ドメインに基づいて、複数のSCVを展開する必要があります。以下の例では、2つのワークロード ドメインと1つの管理ドメインがあり、3つのSCVがVCF管理ドメインvCenterにデプロイされています。

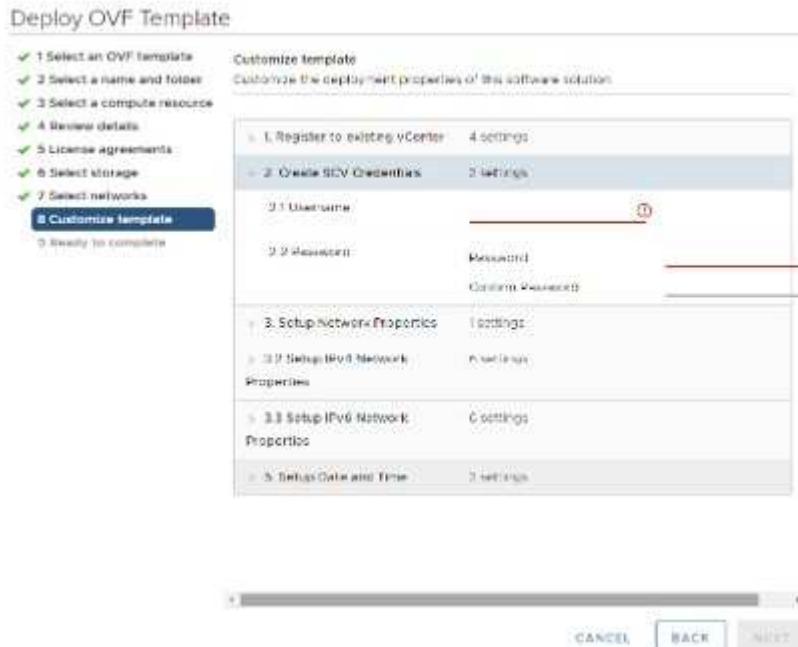


- vcf-m01-vc02.sddc.netapp.com
 - DataCenter
 - Cluster01
 - vcf-m01-esx01.sddc.netapp.com
 - vcf-m01-esx02.sddc.netapp.com
 - vcf-m01-esx03.sddc.netapp.com
 - vcf-m01-esx04.sddc.netapp.com
 - Cluster01-mgmt-001
 - vcf-m01-nsx01a
 - vcf-m01-nsx01b
 - vcf-m01-nsx01c
 - vcf-m01-sddc01
 - vcf-m01-vc02
 - vcf-m01wk-vc02
 - vcf-w01-nsx01
 - vcf-w01-nsx02
 - vcf-w01-nsx03
 - vcf-w02-nsx01
 - vcf-w02-nsx02
 - vcf-w02-nsx03
 - vct-wkld-vc01
 - vcf-mgmt-sc
 - vcf-wkld-sc01
 - vcf-wkld-sc02



管理ドメインと各ワークロードドメインにSCVを展開する

1. "Open Virtual Appliance (OVA) をダウンロードします。"
2. vSphere Clientで、vCenter Serverにログインします。[管理] > [証明書] > [証明書管理] に移動します。信頼されたルート証明書を追加し、各証明書を certs フォルダーにインストールします。証明書をインストールしたら、OVAを検証して導入できるようになります。
3. VCF ワークロード ドメイン vCenter にログインし、OVF テンプレートをデプロイして、VMware デ



プロイ ウィザードを起動します。

4. OVA の電源をオンにして SCV を起動し、[VMware ツールのインストール] をクリックします。
5. OVA コンソールのシステム構成メニューから MFA トークンを生成しま

```

System Configuration Menu:

  1 ) Reboot virtual machine
  2 ) Shut down virtual machine
  3 ) Change 'maint' user password
  4 ) Change time zone
  5 ) Change NTP server
  6 ) Enable SSH access
  7 ) Increase jail disk size (/jail)
  8 ) Upgrade
  9 ) Install VMware Tools
10 ) Generate MFA Token

  b ) Back
  x ) Exit

Enter your choice: 10

Generating MFA Token... Your MFA Token is : 435164
Press ENTER to continue...

```

す。

- 展開時に設定した管理者ユーザー名とパスワード、およびメンテナンス コンソールを使用して生成された MFA トークンを使用して、SCV 管理 GUI にログインします。
`https://<appliance-IP-address>:8080`管理 GUI にアクセスします。

Name (FQDN or IP)	Port
vcf-wkld-vc01.sddc.netapp.com	443

Username
administrator@vsphere.local

Password

Service	Status
Enabled	Enabled
Enabled	Connected

SCVの設定

VMをバックアップまたは復元するには、まずデータストアをホストするストレージ クラスターまたはVMを追加し、次に保持と頻度に関するバックアップ ポリシーを作成し、リソースを保護するためのリソース グループを設定します。

Getting Started with SnapCenter Plug-in for VMware vSphere



Add one or more storage systems that contain resources you want to protect.
Create one or more backup policies that manage the retention, frequency and other settings for resource group backups.
Create a container to add one or more resources that you want to protect with backup policies.

[Click here to configure](#)

[Click here to configure](#)

[Click here to configure](#)

1. vCenter Web クライアントにログインし、ツールバーのメニューをクリックして、SnapCenter Plug-in for VMware vSphereとストレージの追加を選択します。SCV プラグインの左側のナビゲータペインで、[ストレージ システム] をクリックし、[追加] オプションを選択します。[ストレージ システムの追加] ダイアログ ボックスで、基本的な SVM またはクラスタ情報に入力し、[追加] を選択します。NetAppストレージのIP アドレスを入力してログインします。
2. 新しいバックアップ ポリシーを作成するには、SCV プラグインの左側のナビゲータペインで [ポリシー] をクリックし、[新しいポリシー] を選択します。[新しいバックアップ ポリシー] ページで、ポリシー構成情報を入力し、[追加] をクリックします。

New Backup Policy

Name: wkld01

Description: description

Frequency: Daily

Locking Period: Enable Snapshot Locking i
1 Days

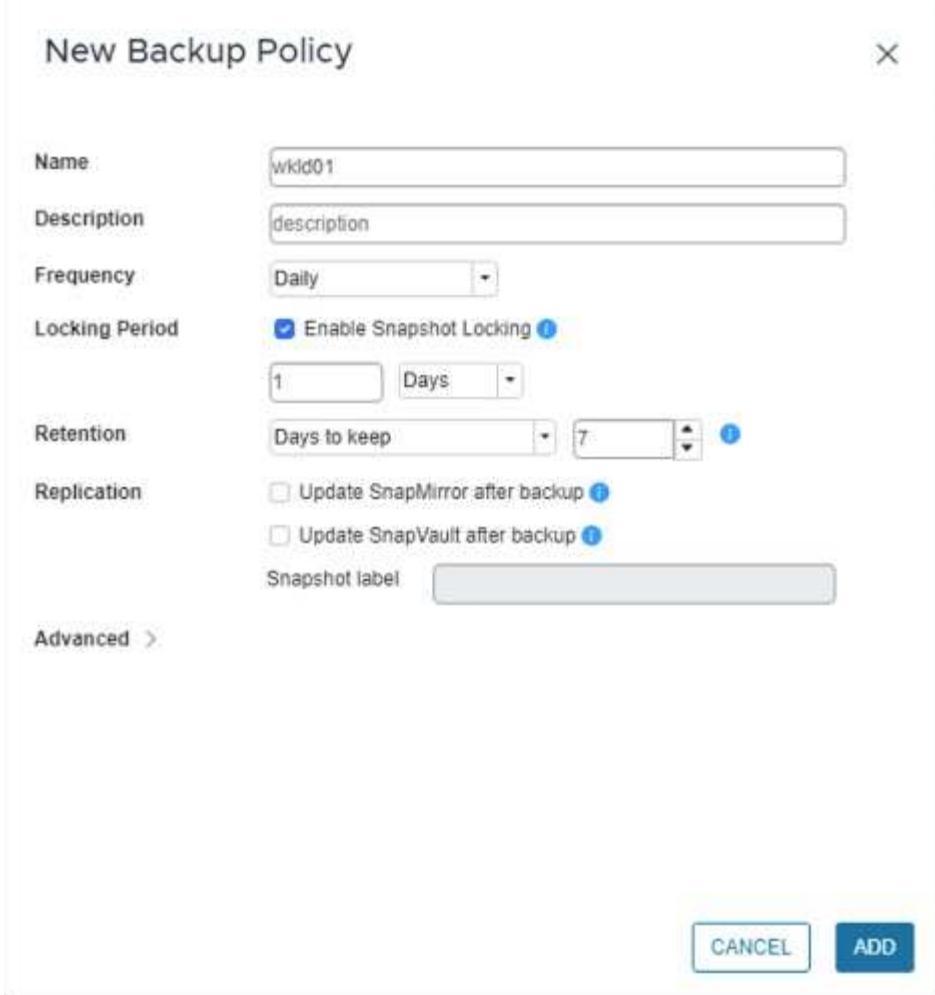
Retention: Days to keep: 7 i

Replication: Update SnapMirror after backup i
 Update SnapVault after backup i

Snapshot label:

Advanced >

CANCEL ADD



- SCV プラグインの左側のナビゲータペインで、[リソース グループ] をクリックし、[作成] を選択します。[Create Resource Group] ウィザードの各ページで必要な情報を入力し、リソース グループに含めるVMとデータストアを選択し、適用するバックアップ ポリシーを選択し、バックアップ スケジュールを指定します。

Create Resource Group

X

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

✓ 5. Schedules

✓ 6. Summary

Name	wkld01RG				
Description					
Send email	Never				
Latest Snapshot name	None <small>?</small>				
Custom snapshot format	None <small>?</small>				
Entities	wkld01				
Spanning	True				
Policies	Name	Frequency	Snapshot Locking Period		
	wkld01	Daily	1 Day		

BACK

NEXT

FINISH

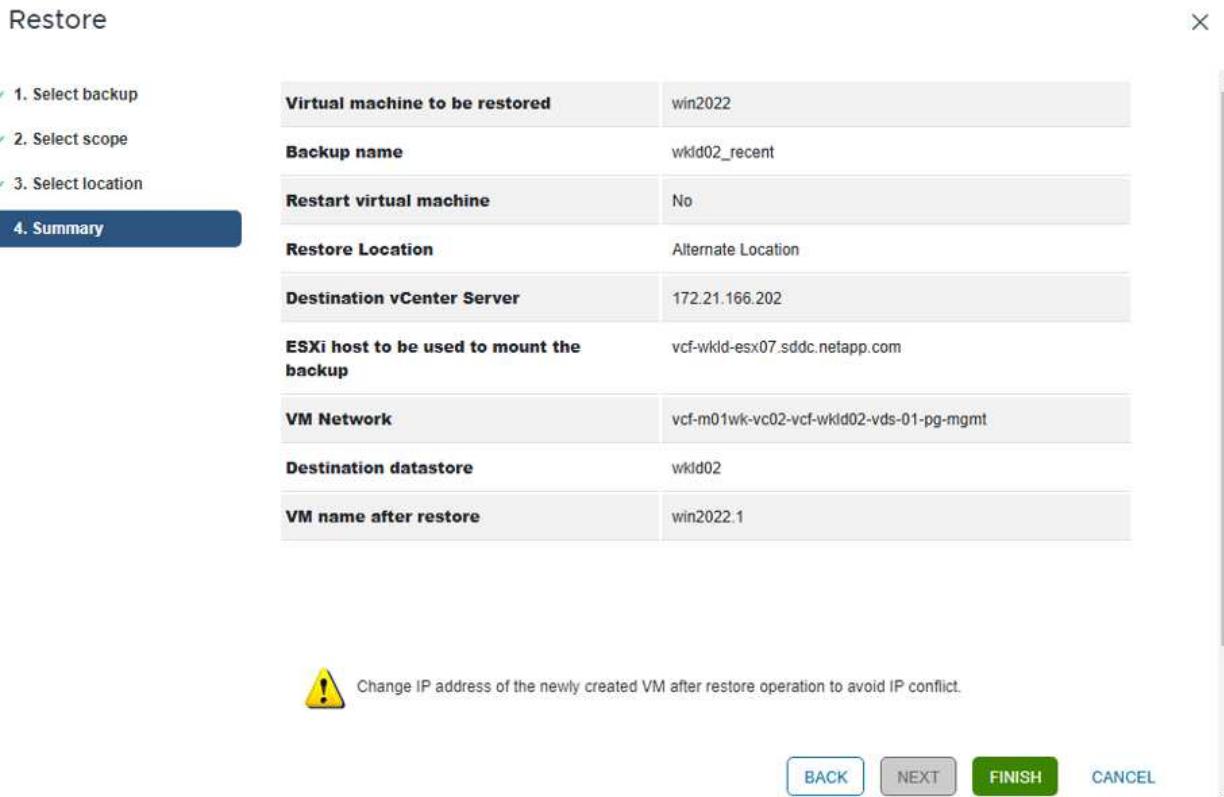
CANCEL

VMとファイルまたはフォルダのバックアップを復元する

バックアップから VM、VMDK、ファイル、フォルダーを復元できます。VM は、同じ vCenter Server 内の元のホストまたは代替ホスト、あるいは同じ vCenter によって管理される代替 ESXi ホストに復元できます。バックアップ内のファイルにアクセスする必要がある場合は、バックアップから従来のデータストアをマウントできます。バックアップは、バックアップが作成された ESXi ホストにも、同じタイプの VM およびホスト構成を使用する代替 ESXi ホストにもマウントできます。同じデータストアを 1 つのホストに複数回マウントできます。ゲストファイル復元セッションでは、仮想ディスクのバックアップコピーを接続してから、選択したファイルまたはフォルダを復元することで、個々のファイルやフォルダを復元することもできます。ファイルやフォルダも復元できます。

VM 復元手順

1. VMware vSphere クライアント GUI で、ツールバーの [メニュー] をクリックし、ドロップダウンリストから [VM とテンプレート] を選択し、VM を右クリックして、ドロップダウンリストから [SnapCenter Plug-in for VMware vSphere] を選択し、セカンダリ ドロップダウンリストから [復元] を選択してウィザードを起動します。
2. 復元ウィザードで、復元するバックアップ スナップショットを選択し、[復元範囲] フィールドで [仮想マシン全体] を選択し、復元場所を選択して、バックアップをマウントする宛先情報を入力します。[場所の選択] ページで、復元されたデータストアの場所を選択します。概要ページを確認し、「完了」をクリックします。



3. 画面下部の「最近のタスク」をクリックして、操作の進行状況を監視します。

データストアの復元手順

1. データストアを右クリックし、[SnapCenter Plug-in for VMware vSphere] > [マウント バックアップ] を選択します。

2. [データストアのマウント] ページで、バックアップとバックアップの場所(プライマリまたはセカンダリ)を選択し、[マウント]をクリックします。

Mount Datastore

ESXi host name vcf-wkld-esx05.sddc.netapp.com

Backup Search for Backups

(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
wkld02_recent	2/9/2025 8:00:01 PM	No	wkld02	Yes
RG-Datastore_02-09-202...	2/9/2025 6:56:01 PM	No	wkld02	Yes
wkld02_02-08-2025_20.0...	2/8/2025 8:00:01 PM	No	wkld02	Yes
RG-Datastore_02-08-202...	2/8/2025 6:56:01 PM	No	wkld02	Yes
wkld02_02-07-2025_20.0...	2/7/2025 8:00:01 PM	No	wkld02	Yes
RG-Datastore_02-07-202...	2/7/2025 6:56:01 PM	No	wkld02	Yes
wkld02_02-06-2025_20.0...	2/6/2025 8:00:01 PM	No	wkld02	Yes

Backup location

Backup type	Location
Primary	172.21.118.118:vcf_md_wkld02:wkld02_recent

CANCEL MOUNT

ファイルとフォルダの復元手順

1. ゲスト ファイルまたはフォルダーの復元操作のために仮想接続ディスクを使用する場合、復元する前に、接続先の VM に資格情報が設定されている必要があります。プラグインの下にあるSnapCenter Plug-in for VMware vSphereから、[ゲスト ファイルのリストアと実行資格情報] セクションを選択し、ユーザー資格情報を入力します。ユーザー名には「Administrator」と入力する必要があります。

2. vSphere クライアントから VM を右クリックし、[SnapCenter Plug-in for VMware vSphere] > [Guest File Restore] を選択します。[復元範囲] ページで、バックアップ名、VMDK 仮想ディスク、および場所 (プライマリまたはセカンダリ) を指定します。「サマリー」をクリックして確認します。

Backup Name	wkld02_recent
VMDK	[wkld02] New Virtual Machine/New Virtual Machine-000001.vmdk
Location	Primary: 172.21.118.118:vcf_md_wkld02_wkld02_recent

Warning: Attach operation will start when you click the Finish button. You can monitor the progress in the Recent Tasks tab and perform a restore operation from the Guest File Restore page listed under SnapCenter Plug-in for VMware vSphere.

BACK **NEXT** **FINISH** **CANCEL**

NetApp SnapCenter for VCP マルチドメインは、データ保護を集中化し、NetAppスナップショットを使用してバックアップに必要な時間とストレージ容量を効率的に削減し、強力なバックアップおよびレプリケーション機能によって大規模な VMware 環境をサポートし、VM 全体、特定の VMDK、または個々のファイルのきめ細かにカバリを可能にします。

SCV による **VCF** 複数ドメインの保護に関するビデオ デモ

[NetApp SCV で VMware VCF の複数ドメインを保護](#)

NVMe over TCP ストレージと **VMware vSphere** 向け**SnapCenter** プラグインを使用して **VCF** ワークロード ドメインを保護します。

SnapCenter Plug-in for VMware vSphere を使用して、NVMe で VCF ワークロード ドメインを保護します。この手順には、プラグインのセットアップ、最適なパフォーマンスを実現するための NVMe over TCP の構成、バックアップ、復元、またはクローン作成操作の実行が含まれます。

NVMe (Non-Volatile Memory Express) over TCP は、VMware Cloud Foundation ESXi サーバーと、All Flash FAS (AFF) や All SAN Array (ASA) などの NetApp ストレージ間の高速データ転送を可能にする最先端のネットワーク プロトコルです。

はじめに

NVMe over TCP を活用することで、要求の厳しいワークロードに対して低レイテンシと高スループットを実現します。 NVMe over TCP と NetApp SnapCenter Plug-in for VMware vSphere (SCV) の統合により、VMware 環境内での効率的なデータ管理、バックアップ、リストア、およびクローン作成操作の強化を実現する強力な組み合わせが実現します。

NVMe over TCP の利点

- ・ **高性能:** 低レイテンシと高いデータ転送速度で優れたパフォーマンスを実現します。これは、要求の厳しいアプリケーションや大規模なデータ操作にとって非常に重要です。
- ・ **スケーラビリティ:** スケーラブルな構成をサポートし、IT 管理者はデータ要件の増大に応じてインフラストラクチャをシームレスに拡張できます。
- ・ **効率:** バックアップと復元の操作が高速化され、ダウンタイムが短縮され、システム全体の可用性が向上します。

このドキュメントでは、最適なパフォーマンスを得るために NVMe over TCP を活用することに重点を置いて、VMware Cloud Foundation (VCF) 環境で SCV を展開および管理する手順について説明します。

観客

VMware VCF ワークロード ドメインのデータ保護と災害復旧を保証するソリューション アーキテクトまたはストレージ管理者。

アーキテクチャの概要

SCV は、VMware 環境内の VM、データストア、ファイル、フォルダーに対して、高速でスペース効率が高く、クラッシュ整合性と VM 整合性のあるバックアップと復元操作を容易にするように設計された強力なツールです。 SCV は、OVA ファイルを使用して Linux 仮想アプライアンスとして導入され、リモート プラグイン アーキテクチャを活用します。

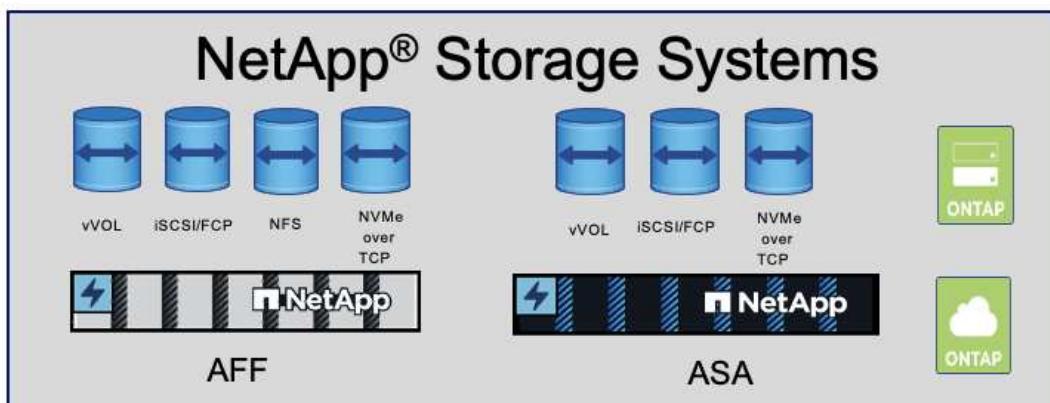
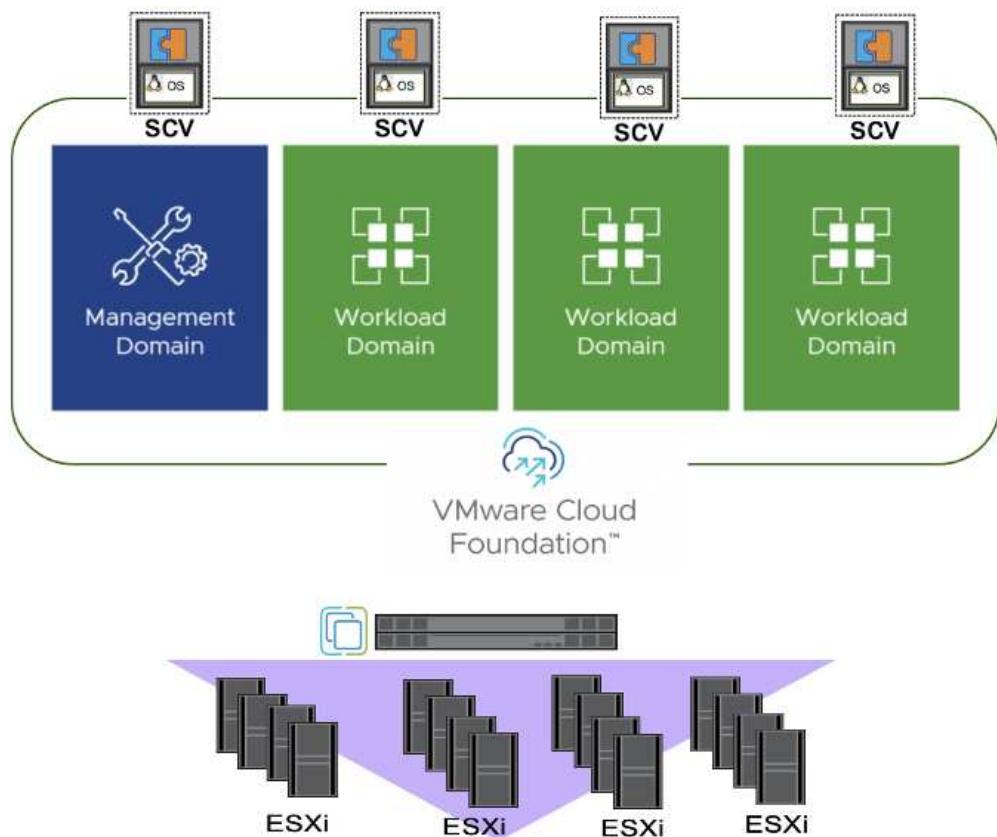
SCV 展開アーキテクチャ

- ・ **仮想アプライアンスの展開:** SCV は、OVA ファイルを使用して Linux 仮想アプライアンスとして展開され

ます。この展開方法により、合理的かつ効率的なセットアップ プロセスが保証されます。

- ・リモート プラグイン アーキテクチャ: SCV はリモート プラグイン アーキテクチャを使用して、複数のインスタンスを管理する際のスケーラビリティと柔軟性を実現します。
- ・1 対 1 の関係: 各 VCF ドメインには専用の SCV インスタンスが必要であり、分離された効率的なバックアップおよび復元操作を保証します。

ONTAP 9.10.1 以降のバージョンでは、NetApp AFF と ASA は NVMe over TCP をサポートします。AFF または ASA プライマリ システム上にあり、ONTAP AFF または ASA セカンダリ システムにレプリケートできるデータ。SCV は SnapCenter Server と連携して、SnapCenter アプリケーション固有のプラグインの VMware 環境でのアプリケーションベースのバックアップおよびリストア操作もサポートします。詳細については、["SnapCenter Plug-in for VMware vSphere のドキュメント"](#) そして ["SnapCenter でワーク LOAD を保護する"](#)



3-2-1 バックアップ ルールは、データのコピーを 3 つ作成し、それらを 2 種類の異なるメディアに保存し、1 つのコピーをオフサイトに保管するというデータ保護戦略です。BlueXP backup and recoveryは、オンプレミスとクラウド環境の両方にわたる幅広いバックアップおよびリカバリ操作に対して単一のコントロール プレーンを提供する、クラウド ベースのデータ管理ツールです。NetApp BlueXP backup and recoveryスイートの一部は、SCV(オンプレミス)と統合してデータのコピーをクラウド内のオブジェクトストレージに拡張する機能です。これにより、プライマリまたはセカンダリストレージ バックアップから取得されたデータの 3 番目のコピーがオフサイトに作成されます。BlueXP backup and recoveryを使用すると、オンプレミスのこれら 2 つの場所のいずれかからデータのコピーを転送するストレージ ポリシーを簡単に設定できます。詳細については、["SnapCenter プラグインとBlueXP backup and recoveryによる VMware の 3-2-1 データ保護"](#)。

NVMe 上の VCF 向け SCV の導入手順

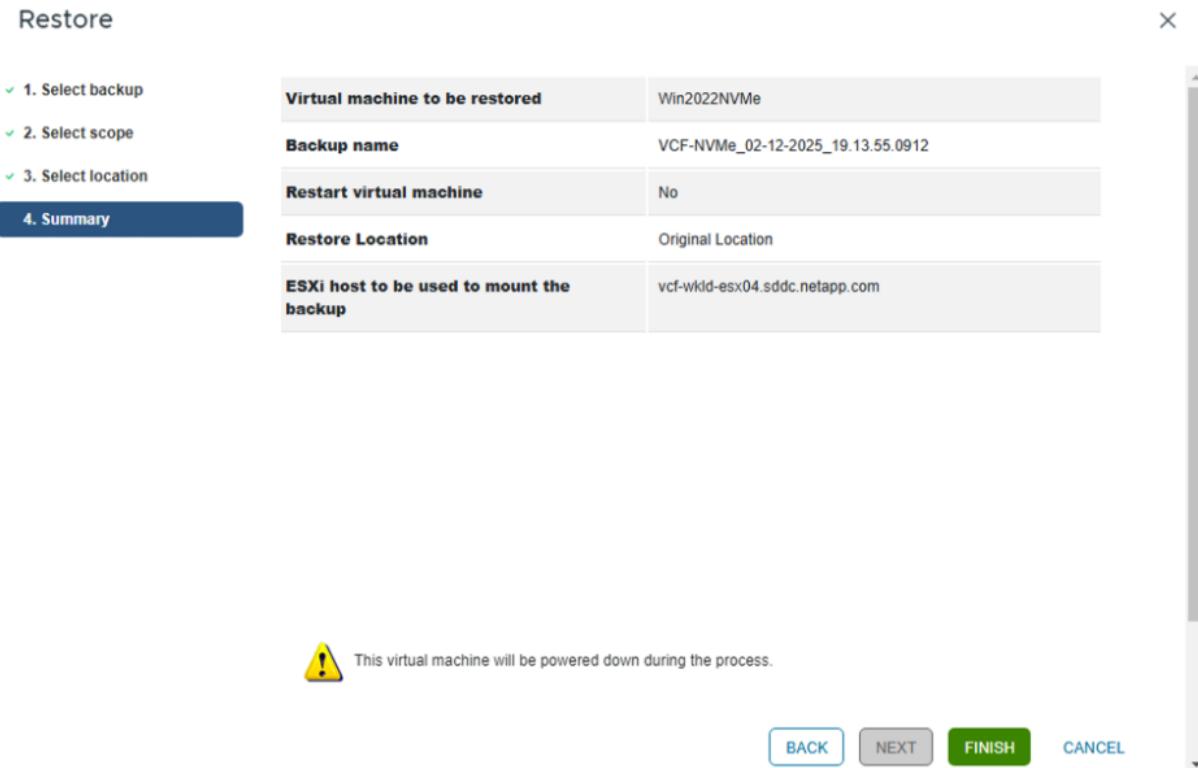
その["ONTAP tools for VMware vSphere"\(OTV\)](#)は、VMware 環境でNetAppストレージを管理するための強力かつ効率的なソリューションを提供します。OTVは、vCenter Serverと直接統合することで、ストレージ管理を簡素化し、データ保護を強化し、パフォーマンスを最適化します。オプションではありますが、OTVを導入すると、VMware 環境の管理機能と全体的な効率が大幅に向上します。

- ・ ["VCF ワークロード ドメイン用の NVMe/TCP ストレージを作成する"](#)
- ・ ["NetApp SnapCenter for VMware vSphere \(SCV\) を構成する"](#)

VM、データストア、仮想ディスク、ファイルまたはフォルダを復元する

SCV は、VMware 環境向けの包括的なバックアップおよび復元機能を提供します。VMFS 環境の場合、SCV はクローンおよびマウント操作を Storage VMotion と組み合わせて使用し、復元操作を実行します。これにより、データの効率的かつシームレスな復元が保証されます。詳細については["復元操作の実行方法。"](#)

- VM のリストア VM を同じ vCenter Server 内の元のホストにリストアするか、同じ vCenter Server によって管理されている別の ESXi ホストにリストアできます。
 - VM を右クリックし、ドロップダウン リストで [SnapCenter Plug-in for VMware vSphere] を選択し、2 番目のドロップダウン リストで [復元] を選択してウィザードを起動します。
 - 復元ウィザードで、復元するバックアップ スナップショットを選択し、[復元範囲] フィールドで [仮想マシン全体] を選択し、復元場所を選択して、バックアップをマウントする宛先情報を入力します。[場所の選択] ページで、復元されたデータストアの場所を選択します。概要ページを確認し、「完了」をクリックします。



- データストアをマウントする バックアップ内のファイルにアクセスする場合は、バックアップから従来のデータストアをマウントできます。バックアップは、バックアップが作成された ESXi ホストにも、同じタイプの VM およびホスト構成を使用する代替 ESXi ホストにもマウントできます。同じデータストアを 1 つのホストに複数回マウントできます。
 - データストアを右クリックし、[SnapCenter Plug-in for VMware vSphere] > [マウント バックアップ] を選択します。
 - [データストアのマウント] ページで、バックアップとバックアップの場所 (プライマリまたはセカンダリ) を選択し、[マウント] をクリックします。

Mount Datastore

X

ESXi host name vcf-wkld-esx03.sddc.netapp.com ▾

Backup

Search for Backups



(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF-NVMe_02-19-2025_...	2/19/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-18-2025_...	2/18/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-17-2025_...	2/17/2025 6:57:01 PM	Yes	wkld01	No
VCF-NVMe_02-16-2025_...	2/16/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-15-2025_...	2/15/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-14-2025_...	2/14/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-13-2025_...	2/13/2025 6:57:01 PM	No	wkld01	No

Backup location

Backup type	Location
Primary	VCF_NVMe:VCF_WKLD_DS:VCF-NVMe_02-19-2025_18.57.02.0052

CANCEL

MOUNT

- 仮想ディスクを接続する バックアップから 1 つ以上の VMDK を親 VM、同じ ESXi ホスト上の代替 VM、または同じ vCenter またはリンク モードの別の vCenter によって管理される代替 ESXi ホスト上の代替 VM に接続できます。
 - a. VM を右クリックし、SnapCenter Plug-in for VMware vSphere > 仮想ディスクの接続を選択します。
 - b. 「仮想ディスクの接続」 ウィンドウで、バックアップを選択し、接続する 1 つ以上のディスクと接続元の場所(プライマリまたはセカンダリ)を選択します。デフォルトでは、選択した仮想ディスクは親VMに接続されます。選択した仮想ディスクを同じ ESXi ホスト内の代替 VM に接続するには、[ここをクリックして代替 VM に接続する] を選択し、代替 VM を指定します。「添付」をクリックします。

Attach Virtual Disk(s) X

Click here to attach to alternate VM

Backup Search for Backups

(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF-NVMe_02-17-2025_18....	2/17/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-16-2025_18....	2/16/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-15-2025_18....	2/15/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-14-2025_18....	2/14/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-13-2025_18....	2/13/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-12-2025_19....	2/12/2025 7:13:55 PM	No	wkld01	No

Select disks

Virtual disk	Location
<input checked="" type="checkbox"/> [VCF_NVMe_DS] Win2022NVMe/Win2022NVMe.vmdk	Primary:VCF_NVMe:VCF_WKLD_DS:VCF-NVMe_02-17-2025_18.57.02.0697

- ファイルとフォルダの復元手順 個々のファイルとフォルダは、ゲストファイル復元セッションで復元できます。このセッションでは、仮想ディスクのバックアップ コピーを接続し、選択したファイルまたはフォルダを復元します。ファイルやフォルダも復元できます。詳細はチェック "SnapCenter のファイルとフォルダーの復元。"
- a. ゲストファイルまたはフォルダの復元操作のために仮想接続ディスクを使用する場合、復元する前に、接続先の VM に資格情報が設定されている必要があります。プラグインの下にあるSnapCenter Plug-in for VMware vSphereから、[ゲストファイルのリストアと実行資格情報] セクションを選択し、ユーザー資格情報を入力します。ユーザー名には「Administrator」と入力する必要があります。

b. vSphere クライアントから VM を右クリックし、[SnapCenter Plug-in for VMware vSphere] > [Guest File Restore] を選択します。[復元範囲] ページで、バックアップ名、VMDK 仮想ディスク、および場所 (プライマリまたはセカンダリ) を指定します。「サマリー」をクリックして確認します。

Guest File Restore

3. Summary

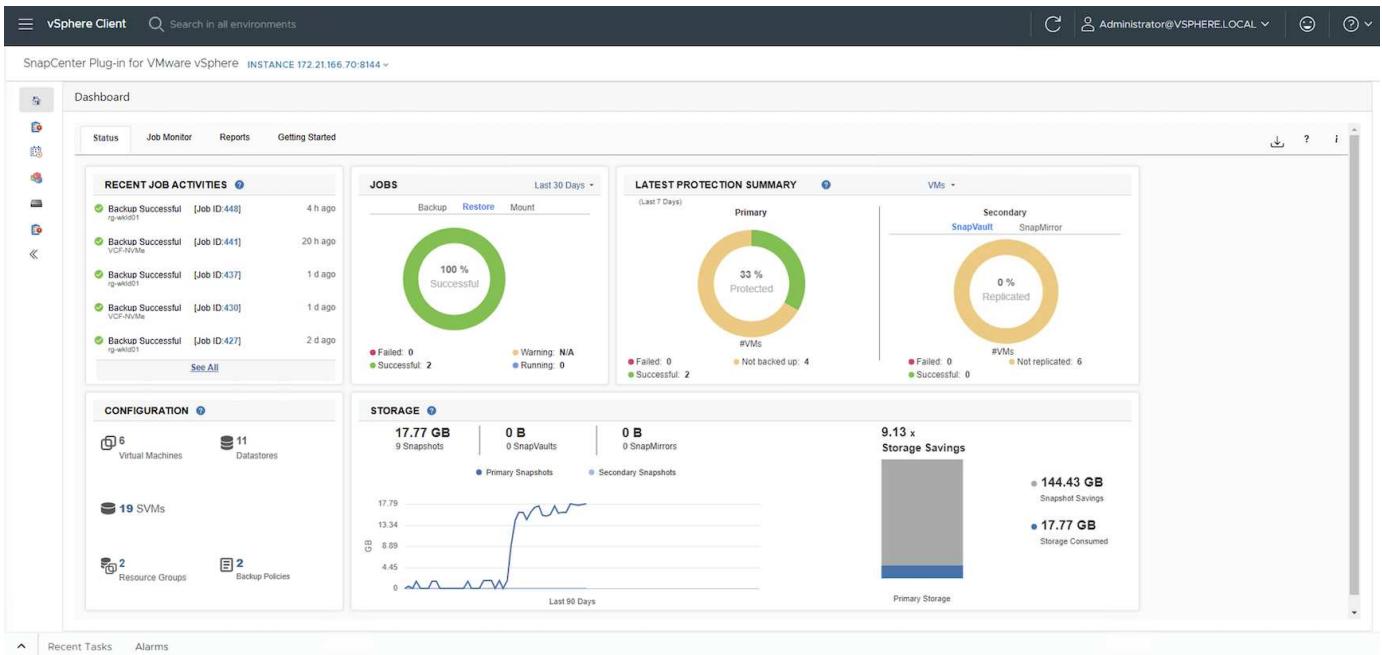
Backup Name	VCF-NVMe_03-02-2025_18.57.01.0662
VMDK	[VCF_NVMe_DS] Win2022NVMe/Win2022NVMe.vmdk
Location	Primary:VCF_NVMe:VCF_WKLD_DS:VCF-NVMe_03-02-2025_18.57.01.0662

! Attach operation will start when you click the Finish button. You can monitor the progress in the Recent Tasks tab and perform a restore operation from the Guest File Restore page listed under SnapCenter Plug-in for VMware vSphere.

BACK NEXT FINISH CANCEL

監視とレポート

SCV は、管理者がバックアップと復元操作を効率的に管理できるように、強力な監視およびレポート機能を提供します。ステータス情報の表示、ジョブの監視、ジョブログのダウンロード、レポートへのアクセスが可能です。詳細については、"VMware vSphere Monitor and Report 用のSnapCenterプラグイン。"



NVMe over TCP と NetApp SnapCenter Plug-in for VMware vSphere のパワーを活用することで、組織は VMware Cloud Foundation ワークロード ドメインに対して高性能なデータ保護とディザスタリカバリを実現できます。このアプローチにより、迅速で信頼性の高いバックアップおよび復元操作が保証され、ダウンタイムが最小限に抑えられ、重要なデータが保護されます。

BlueXPでVMwareデータストアを保護する

BlueXP disaster recoveryを使用した VMware データストアの保護について学習します

VMware 向けBlueXP disaster recoveryを使用した、NetApp のディザスタリカバリソリューションについて学習します。これにより、プライマリサイトから災害復旧サイトへのブロックレベルのレプリケーションを使用した、災害復旧のための堅牢なソリューションが提供されます。

BlueXP DRaaS は、ランサムウェア攻撃などのサイト障害やデータ整合性の問題からワークロードを保護するための効果的かつ経済的な方法です。さらに、NetApp BlueXP DRaaS は、管理されたクラウドベースの災害復旧ソリューションを提供することでこの戦略を強化し、災害発生時の迅速な復旧と最小限のダウンタイムを保証します。

技術的な詳細については、以下のソリューションを参照してください。

- "VMFS データストア向けBlueXP DRaaS を使用した DR"
- "NFS データストア向けBlueXP DRaaS を使用した DR"

VMware vSphere およびBlueXP backup and recoveryのSnapCenterプラグインを使用して、VMware の 3-2-1 データ保護を構成します。

VMware vSphere およびBlueXP backup and recoveryのSnapCenterプラグインを使用して、VMware 環境向けの 3-2-1 データ保護戦略を構成します。この手順には、プライマリおよびセカンダリONTAPクラスタ上の VM およびデータストアのバックアップの設

定、プラグインおよびBlueXPの設定、信頼性の高いリカバリのためのクラウドまたはオフサイトストレージへのデータレプリケーションの管理が含まれます。

3-2-1 バックアップ戦略は業界で認められたデータ保護方法であり、貴重なデータを保護するための包括的なアプローチを提供します。この戦略は信頼性が高く、予期しない災害が発生した場合でも、データのコピーが利用可能であることを保証します。

概要

この戦略は、次の3つの基本ルールで構成されます。

1. データのコピーを少なくとも3つ保存してください。これにより、1つのコピーが失われたり破損したりした場合でも、少なくとも2つのコピーが残っているので、それを頼りにすることができます。
2. 2つのバックアップコピーを異なるストレージメディアまたはデバイスに保存します。ストレージメディアを多様化することで、デバイス固有またはメディア固有の障害から保護することができます。1つのデバイスが破損したり、ある種類のメディアに障害が発生したりしても、他のバックアップコピーは影響を受けません。
3. 最後に、少なくとも1つのバックアップコピーがオフサイトにあることを確認します。オフサイトストレージは、オンサイトコピーが使用できなくなる可能性のある火災や洪水などの局所的な災害に対するファイルセーフとして機能します。

このソリューションドキュメントでは、SnapCenter Plug-in for VMware vSphere (SCV) を使用してオンプレミスの仮想マシンのプライマリバックアップとセカンダリバックアップを作成し、仮想マシン用のBlueXP backup and recoveryを使用してデータのコピーをクラウドストレージまたはStorageGRIDにバックアップする3-2-1バックアップソリューションについて説明します。

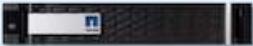
ユースケース

このソリューションは、次のユースケースに対応します。

- SnapCenter Plug-in for VMware vSphereを使用して、オンプレミスの仮想マシンとデータストアをバックアップおよび復元します。
- ONTAPクラスターでホストされ、仮想マシン用のBlueXP backup and recovery。

NetApp ONTAPデータストレージ

ONTAPは、SANプロトコルまたはNASプロトコルのどちらでアクセスする場合でも統合ストレージを提供する、NetAppの業界をリードするストレージソリューションです。3-2-1バックアップ戦略により、オンプレミスのデータが複数のメディアタイプで保護されることが保証され、NetAppは高速フラッシュから低コストのメディアに至るまでのプラットフォームを提供します。

FAS	AFF C-Series	AFF A-Series	ASA A-Series
			
Hybrid flash storage	Capacity all-flash storage	Performance all-flash storage	All-flash SAN storage
Unified (file, block, object)	Unified (file, block, object)	Unified (file, block, object)	Block optimized
Lowest price storage	Balanced price storage	Premium priced storage	Aggressively priced storage
Tier 2 @ 5-10ms latency Backup / Low-cost DR	Refresh of hybrid flash, Tier 1 @ 2-4ms latency Tier 2 workloads VMware datastores	Ideal for Tier 1 business-critical workloads with <1ms latency	Ideal for Tier 1 Block Six Nines Guaranteed

NetAppのハードウェアプラットフォームの詳細については、以下をご覧ください。 "[NetAppデータストレージ](#)"。

SnapCenter Plug-in for VMware vSphere

SnapCenter Plugin for VMware vSphere は、VMware vSphere と緊密に統合され、仮想マシンのバックアップとリストアの管理を容易にするデータ保護サービスです。このソリューションの一部として、 SnapMirror は、セカンダリONTAPストレージ クラスタ上に仮想マシン データの 2 番目の不变バックアップ コピーを作成するための高速で信頼性の高い方法を提供します。このアーキテクチャを導入すると、プライマリ バックアップの場所またはセカンダリ バックアップの場所から仮想マシンの復元操作を簡単に開始できるようになります。

SCV は、 OVA ファイルを使用して Linux 仮想アプライアンスとして展開されます。プラグインはリモート プラグインアーキテクチャを使用するようになりました。リモート プラグインは vCenter サーバーの外部で実行され、 SCV 仮想アプライアンス上でホストされます。

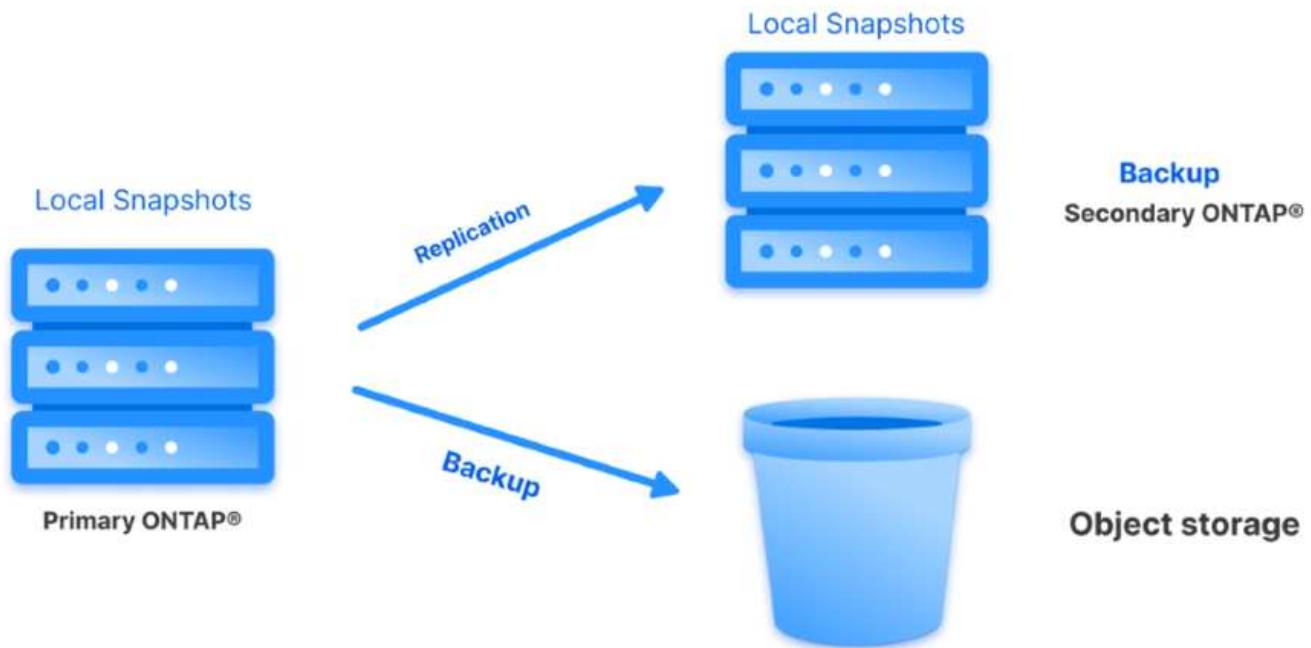
SCV の詳細については、 "[SnapCenter Plug-in for VMware vSphere のドキュメント](#)"。

仮想マシンのBlueXP backup and recovery

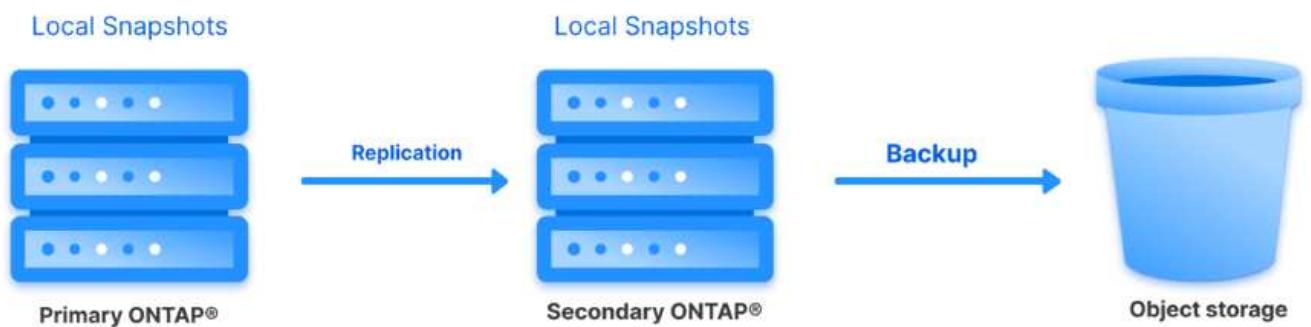
BlueXP backup and recovery は、オンプレミスとクラウド環境の両方にわたる幅広いバックアップおよびリカバリ操作に対して単一のコントロール プレーンを提供する、クラウドベースのデータ管理ツールです。 NetApp BlueXP backup and recovery スイートの一部である機能は、 VMware vSphere (オンプレミス) 用の SnapCenter プラグインと統合して、データのコピーをクラウド内のオブジェクトストレージに拡張します。これにより、プライマリまたはセカンダリストレージ バックアップから取得されたデータの 3 番目のコピーがオフサイトに作成されます。 BlueXP backup and recovery を使用すると、オンプレミスのこれら 2 つの場所のいずれかからデータのコピーを転送するストレージ ポリシーを簡単に設定できます。

BlueXP Backup and Recovery でソースとしてプライマリ バックアップとセカンダリ バックアップのいずれかを選択すると、次の 2 つのトポロジのいずれかが実装されます。

ファンアウト トポロジー – SnapCenter Plug-in for VMware vSphere によってバックアップが開始されると、 ローカル スナップショットが直ちに作成されます。次に、 SCV は最新のスナップショットをセカンダリONTAP クラスターに複製する SnapMirror 操作を開始します。 BlueXP Backup and Recovery では、 ポリシーによって、選択したクラウド プロバイダーのオブジェクトストレージに転送されるデータのスナップショット コピーのソースとしてプライマリONTAP クラスターが指定されます。



カスケード トポロジー SCV を使用してプライマリ データ コピーとセカンダリ データ コピーを作成する方法は、上記のファンアウト トポロジと同じです。ただし、今回は、オブジェクトストレージへのバックアップがセカンダリONTAPクラスターから実行されるように指定するポリシーがBlueXP Backup and Recovery に作成されます。



BlueXP backup and recoveryでは、オンプレミスのONTAPスナップショットのバックアップ コピーを AWS Glacier、Azure Blob、GCP アーカイブ ストレージに作成できます。



AWS Glacier and Deep Glacier Azure Blob Archive GCP Archive Storage

さらに、オブジェクトストレージのバックアップターゲットとしてNetApp StorageGRIDを使用することもできます。StorageGRIDの詳細については、["StorageGRIDランディングページ"](#)。

ソリューション展開の概要

このリストには、このソリューションを構成し、SCV およびBlueXP backup and recoveryからバックアップと復元操作を実行するために必要な高レベルの手順が示されています。

1. プライマリおよびセカンダリ データ コピーに使用するONTAPクラスタ間のSnapMirror関係を構成します。
2. VMware vSphere 用のSnapCenterプラグインを構成します。
 - a. ストレージシステムを追加する
 - b. バックアップポリシーの作成
 - c. リソース グループの作成
 - d. 最初のバックアップジョブを実行する
3. 仮想マシンのBlueXP backup and recoveryを構成する
 - a. 作業環境を追加する
 - b. SCVおよびvCenterアプライアンスの検出
 - c. バックアップポリシーの作成
 - d. バックアップを有効にする
4. SCVを使用してプライマリストレージとセカンダリストレージから仮想マシンを復元します。
5. BlueXPバックアップと復元を使用して、オブジェクトストレージから仮想マシンを復元します。

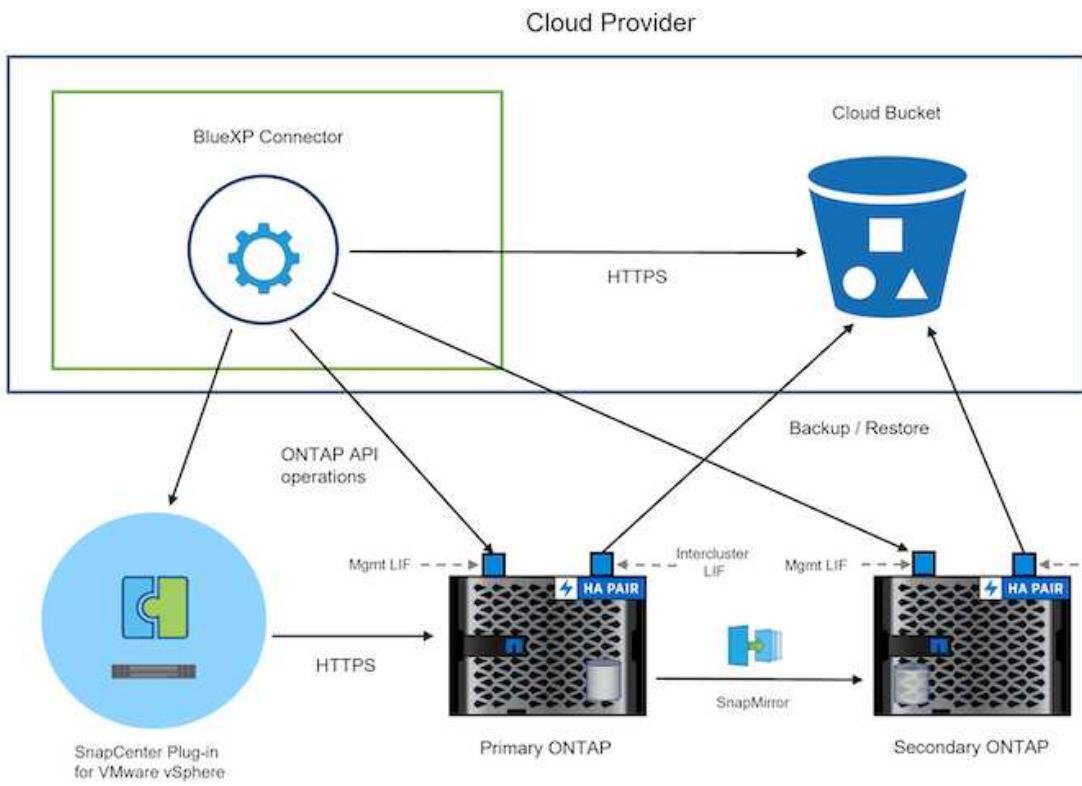
前提条件

このソリューションの目的は、VMware vSphere、VCF VI ワークロード ドメイン、または VCF 管理ドメインで実行されている仮想マシンのデータ保護を実証することです。このソリューションの仮想マシンは、NetApp ONTAPによって提供される NFS データストアでホストされます。このソリューションでは、次のコンポーネントが構成され、使用できる状態になっていることを前提としています。

1. VMware vSphere に接続された NFS または VMFS データストアを備えたONTAPストレージ クラスター。NFS と VMFS の両方のデータストアがサポートされています。このソリューションでは NFS データストアが利用されました。
2. NFS データストアに使用されるボリュームに対してSnapMirror関係が確立されたセカンダリONTAPストレージ クラスタ。
3. オブジェクトストレージ バックアップに使用されるクラウド プロバイダー用にBlueXPコネクタがインストールされています。
4. バックアップされる仮想マシンは、プライマリONTAPストレージ クラスタにある NFS データストア上にあります。
5. BlueXPコネクタとオンプレミスのONTAPストレージ クラスタ管理インターフェイス間のネットワーク接続。
6. BlueXPコネクタとオンプレミスの SCV アプライアンス VM 間、およびBlueXPコネクタと vCenter 間のネットワーク接続。
7. オンプレミスのONTAPクラスタ間 LIF とオブジェクトストレージ サービス間のネットワーク接続。
8. プライマリおよびセカンダリONTAPストレージ クラスタ上の管理 SVM 用に設定された DNS。詳細については、["ホスト名解決に使用するDNSの設定"](#)。

高レベルアーキテクチャ

このソリューションのテスト/検証は、最終的な展開環境と一致する場合も一致しない場合もあるラボで実行されました。



ソリューションの展開

このソリューションでは、オンプレミスデータセンターにある VMware vSphere クラスター内の Windows および Linux 仮想マシンのバックアップとリカバリを実行するために、SnapCenter Plug-in for VMware vSphere と BlueXP backup and recovery を利用するソリューションを展開および検証するための詳細な手順を示します。このセットアップの仮想マシンは、ONTAP A300 ストレージクラスタによってホストされる NFS データストアに保存されます。さらに、別のONTAP A300 ストレージクラスタは、SnapMirrorを使用して複製されたボリュームのセカンダリ デスティネーションとして機能します。さらに、Amazon Web Services と Azure Blob でホストされているオブジェクトストレージが、データの 3 番目のコピーのターゲットとして使用されました。

SCV によって管理されるバックアップのセカンダリ コピーの SnapMirror 関係の作成と、SCV と BlueXP backup and recovery の両方でのバックアップジョブの構成について説明します。

SnapCenter Plug-in for VMware vSphere の詳細については、["SnapCenter Plug-in for VMware vSphere のドキュメント"](#)。

BlueXP backup and recovery の詳細については、["BlueXP backup and recovery ドキュメント"](#)。

ONTAP クラスタ間の SnapMirror 関係を確立する

SnapCenter Plug-in for VMware vSphere は、ONTAP SnapMirror テクノロジを使用して、セカンダリ SnapMirror および/または SnapVault コピーのセカンダリ ONTAP クラスタへの転送を管理します。

SCV バックアップポリシーには、SnapMirror または SnapVault 関係を使用するオプションがあります。主な違いは、SnapMirror オプションを使用する場合、ポリシーでバックアップ用に構成された保持スケジュールがプライマリ ロケーションとセカンダリ ロケーションで同じになることです。SnapVault はアーカイブ用に設計されており、このオプションを使用すると、セカンダリ ONTAP ストレージクラスタ上のスナップショットコピーに対して SnapMirror 関係を使用して個別の保持スケジュールを確立できます。

SnapMirror関係の設定は、多くの手順が自動化されているBlueXPで実行することも、System ManagerとONTAP CLIを使用して実行することもできます。これらすべての方法について以下で説明します。

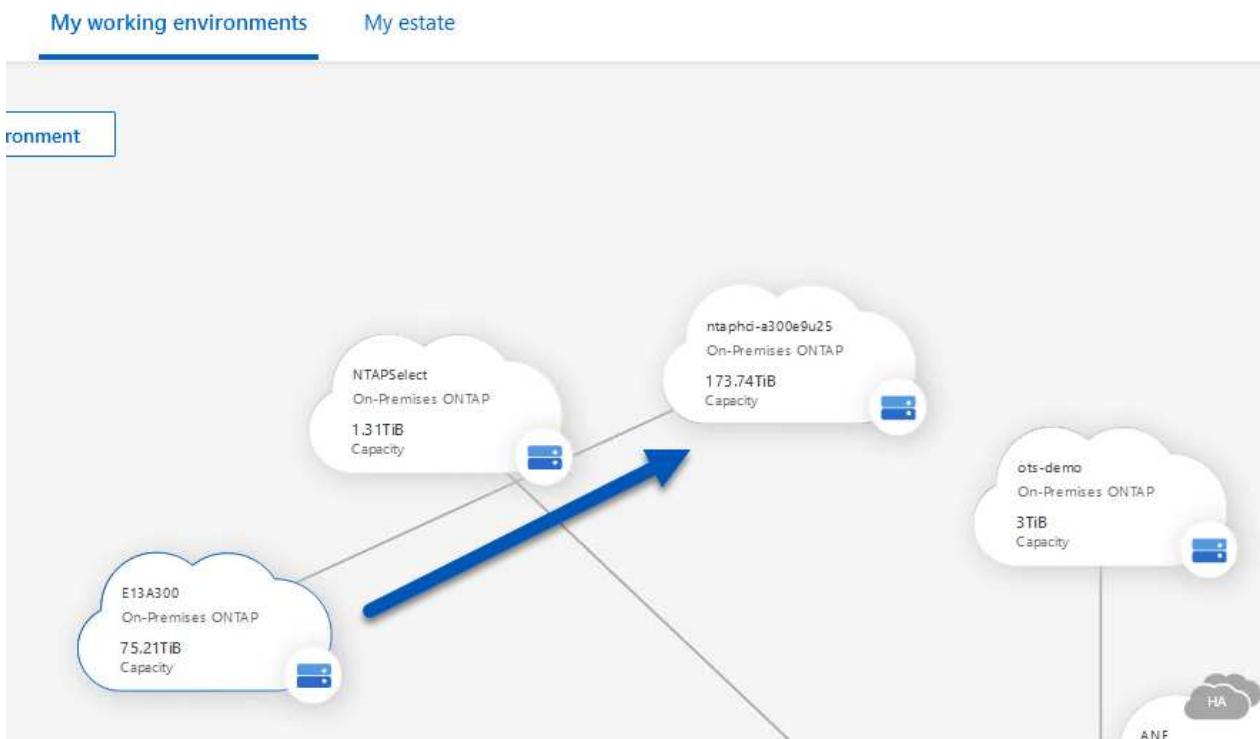
BlueXPとのSnapMirror関係を確立する

BlueXP Web コンソールから次の手順を完了する必要があります。

プライマリおよびセカンダリONTAPストレージシステムのレプリケーション設定

まず、BlueXP Web コンソールにログインし、Canvas に移動します。

1. ソース (プライマリ) ONTAPストレージシステムを、宛先 (セカンダリ) ONTAPストレージシステムにドラッグ アンド ドロップします。



2. 表示されるメニューから*レプリケーション*を選択します。



3. 宛先ピアリング設定ページで、ストレージシステム間の接続に使用する宛先クラスタ間 LIF を選択します。

Select the destination LIFs you would like to use for cluster peering setup.
 Replication requires an initial connection between the two working environments which is called a cluster peer relationship.
 For more information about LIF selections, see Cloud Manager documentation.

<input type="checkbox"/> CVO_InterCluster_B ntaphci-a300-02 : a0a-3510 172.21.254.212/24 up	<input type="checkbox"/> CVO_InterCluster_A ntaphci-a300-01 : a0a-3510 172.21.254.211/24 up	<input type="checkbox"/> zoneb-n1 ntaphci-a300-01 : a0a-3484 172.21.228.211/24 up	<input type="checkbox"/> zoneb-n2 ntaphci-a300-02 : a0a-3484 172.21.228.221/24 up	<input checked="" type="checkbox"/> intercluster_node_1 ntaphci-a300-01 : a0a-181 10.61.181.193/24 up	<input checked="" type="checkbox"/> intercluster_node_2 ntaphci-a300-01 : a0a-181 10.61.181.194/24 up
---	---	---	---	---	---

4. 宛先ボリューム名ページで、最初にソースボリュームを選択し、次に宛先ボリューム名を入力して、宛先SVMとアグリゲートを選択します。続行するには、[次へ]をクリックします。

Select the volume that you want to replicate

 E13A300 288 Volumes	 CDM01 INFO: Storage VM Name F502, Tiering Policy None, Volume Type RW CAPACITY: 206 GB Allocated, 53.72 MB Disk Used 	 Data INFO: Storage VM Name F502, Tiering Policy None, Volume Type RW CAPACITY: 512 GB Allocated, 0 GB Disk Used
 Demo INFO: Storage VM Name zonea, Tiering Policy None, Volume Type RW CAPACITY: 250 GB Allocated, 1.79 GB Disk Used	 Demo02_01 INFO: Storage VM Name Demo, Tiering Policy None, Volume Type RW CAPACITY: 500 GB Allocated, 34.75 MB Disk Used	

Destination Volume Name

Destination Volume Name

Demo_copy

Destination Storage VM

EHC_NFS

Destination Aggregate

EHCAGgr01

5. レプリケーションを実行するための最大転送速度を選択します。

Max Transfer Rate

You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.

Limited to: MB/s

Unlimited (recommended for DR only machines)

6. セカンダリ バックアップの保持スケジュールを決定するポリシーを選択します。このポリシーは事前に作成することも(以下の「スナップショット保持ポリシーの作成」手順の手動プロセスを参照)、必要に応じて事後に変更することもできます。

Replication Setup Replication Policy

↑ Previous Step Default Policies Additional Policies

CloudBackupService-1674046623282

Original Policy Name: CloudBackupService-1674046623282

Creates a SnapVault relationship which replicates Snapshot copies with the following labels to the destination volume:
hourly (12), daily (15), weekly (4)
(# of retained Snapshot copies in parenthesis)

[More info](#)

CloudBackupService-1674047424679

Custom Policy - No Comment

[More info](#)

CloudBackupService-1674047718637

Custom Policy - No Comment

[More info](#)

7. 最後に、すべての情報を確認し、「Go」ボタンをクリックしてレプリケーションのセットアッププロセスを開始します。

Replication Setup Review & Approve

↑ Previous Step

Source
Destination

E13A300

Demo

ntaphci-a300e9u25

Demo_copy

Review your selection and start the replication process

Source Volume Allocated Size:	250 GB	Destination Aggregate:	EHCAggr01
Source Volume Used Size:	1.79 GB	Destination Storage VM:	EHC_NFS
Source Thin Provisioning:	Yes	Max Transfer Rate:	100 MB/s
Destination Volume Allocated Size:	250 GB	SnapMirror Policy:	Mirror
Destination Thin Provisioning:	No	Replication Schedule:	One-time copy

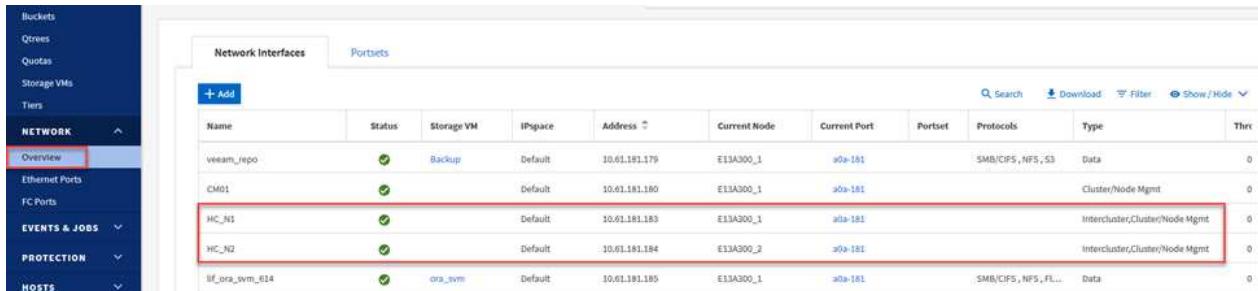
System ManagerとONTAP CLIを使用してSnapMirror関係を確立する

SnapMirror関係を確立するために必要なすべての手順は、System Manager またはONTAP CLI を使用して実行できます。次のセクションでは、両方の方法について詳細な情報を提供します。

送信元と宛先のクラスタ間論理インターフェースを記録する

ソースおよびデスティネーションのONTAPクラスタについては、System Manager または CLI からクラスタ間 LIF 情報を取得できます。

1. ONTAP System Manager で、[ネットワークの概要] ページに移動し、FSx がインストールされている AWS VPC と通信するように設定されているタイプ: クラスタ間の IP アドレスを取得します。



The screenshot shows the ONTAP System Manager interface under the 'NETWORK' section, specifically the 'Overview' tab. The 'Network Interfaces' table lists several network interfaces. Two specific entries, 'HC_N1' and 'HC_N2', are highlighted with red boxes. These entries represent intercluster interfaces. The table includes columns for Name, Status, Storage VM, IPspace, Address, Current Node, Current Port, Portset, Protocols, Type, and Thr.

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Portset	Protocols	Type	Thr
veeam_repo	✓	Backup	Default	10.61.181.179	E13A300_1	a0a-181		SMB/CIFS,NFS,S3	Data	0
CM01	✓		Default	10.61.181.180	E13A300_1	a0a-181			Cluster/Node Mgmt	0
HC_N1	✓		Default	10.61.181.183	E13A300_1	a0a-181			Intercluster,Cluster/Node Mgmt	0
HC_N2	✓		Default	10.61.181.184	E13A300_2	a0a-181			Intercluster,Cluster/Node Mgmt	0
lif_ora_tvm_614	✓	ora_svm	Default	10.61.181.185	E13A300_1	a0a-181		SMB/CIFS,NFS,FL...	Data	0

2. CLI を使用してクラスタ間 IP アドレスを取得するには、次のコマンドを実行します。

```
ONTAP-Dest::> network interface show -role intercluster
```

ONTAPクラスタ間のクラスタピアリングを確立する

ONTAPクラスタ間のクラスタピアリングを確立するには、開始側のONTAPクラスタで入力した一意のパスフレーズを、他のピアクラスタで確認する必要があります。

- 宛先ONTAPクラスタでピアリングを設定するには、`cluster peer create`指示。プロンプトが表示されたら、後でソースクラスターで作成プロセスを完了するために使用する一意のパスフレーズを入力します。

```
ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addrs  
source_intercluster_1, source_intercluster_2  
Enter the passphrase:  
Confirm the passphrase:
```

- ソースクラスタでは、ONTAP System ManagerまたはCLIを使用してクラスタピア関係を確立できます。ONTAP System Managerから、[Protection] > [Overview]に移動し、[Peer Cluster]を選択します。



DASHBOARD

STORAGE ^

Overview

Volumes

LUNs

Consistency Groups

NVMe Namespaces

Shares

Buckets

Qtrees

Quotas

Storage VMs

Tiers

NETWORK ^

Overview

Ethernet Ports

FC Ports

EVENTS & JOBS ^

PROTECTION ^

Overview

Relationships

HOSTS ^

Overview

< Intercluster Settings

Network Interfaces

IP ADDRESS

✓ 10.61.181.184

✓ 172.21.146.217

✓ 10.61.181.183

✓ 172.21.146.216

Cluster Peers

PEERED CLUSTER NAME

✓ Fsxlld0ae40e08acc0dea67

✓ OTS02

Peer Cluster

Generate Passphrase

Manage Cluster Peers

Mediator ?



Not configured.

Configure

Storage VM Peers



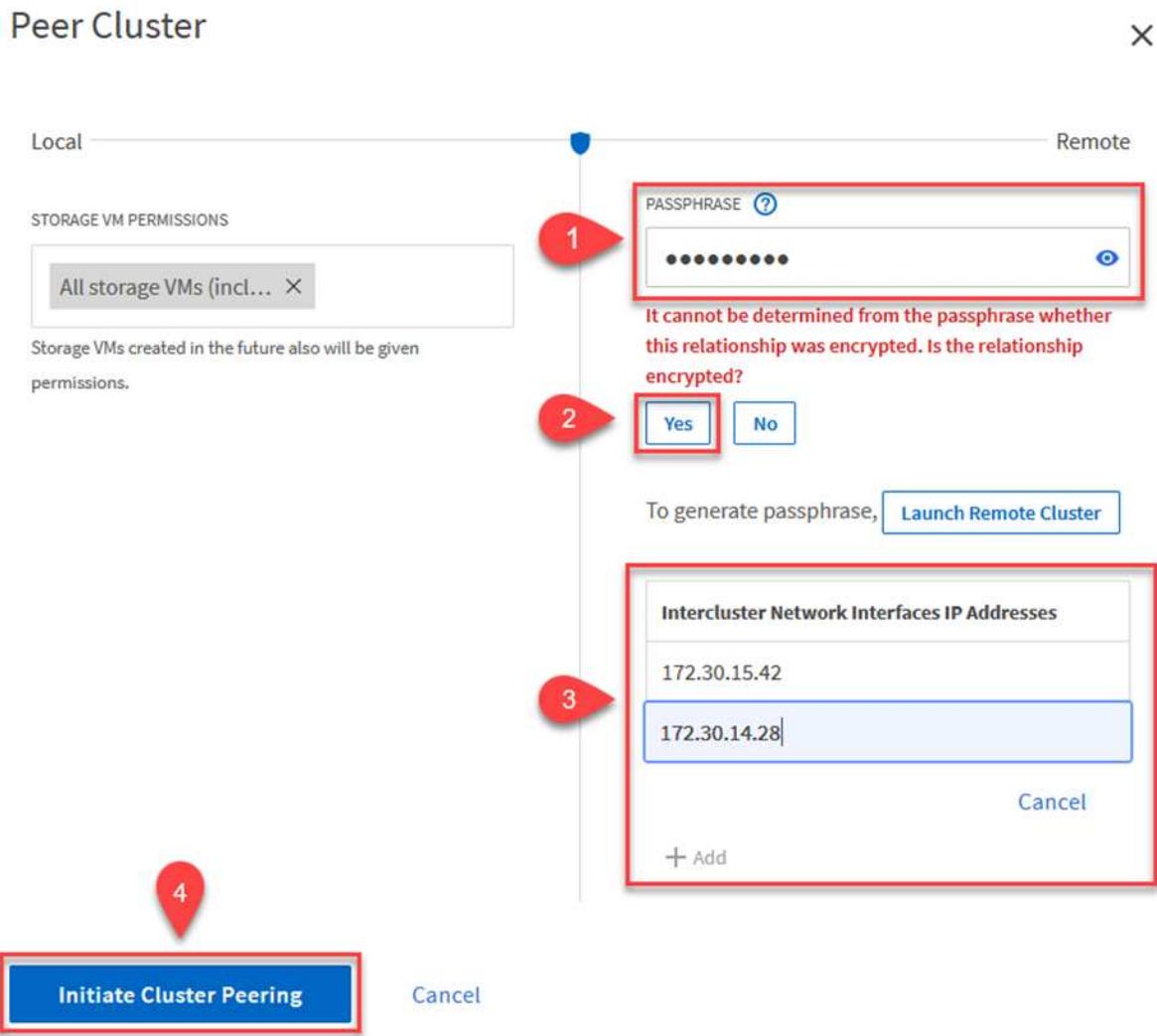
PEERED STORAGE VMS

✓ 3

3. [ピア クラスター] ダイアログ ボックスで、必要な情報を入力します。

- a. 宛先ONTAPクラスタでピア クラスタ関係を確立するために使用されたパスフレーズを入力します。

- b. 選択 'Yes' 暗号化された関係を確立します。
- c. 宛先ONTAPクラスタのクラスタ間 LIF IP アドレスを入力します。
- d. プロセスを終了するには、「クラスター ピアリングの開始」をクリックします。



4. 次のコマンドを使用して、宛先ONTAPクラスタからクラスタ ピア関係のステータスを確認します。

```
ONTAP-Dest::> cluster peer show
```

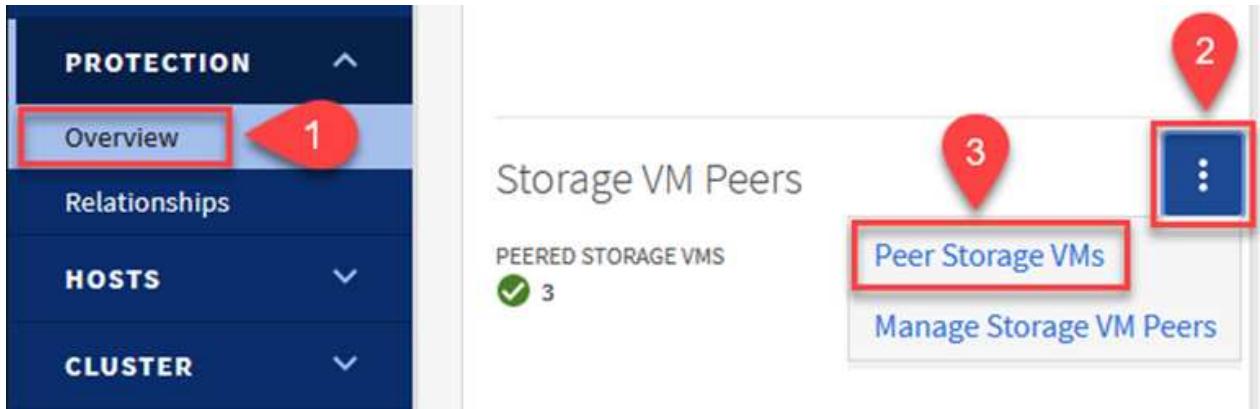
SVMピアリング関係を確立する

次の手順では、SnapMirror関係になるボリュームを含む宛先ストレージ仮想マシンとソースストレージ仮想マシン間のSVM関係を設定します。

1. 宛先ONTAPクラスタから、CLIから次のコマンドを使用してSVMピア関係を作成します。

```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver  
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. ソースONTAPクラスタから、ONTAP System ManagerまたはCLIのいずれかを使用してピアリング関係を受け入れます。
3. ONTAP System Managerから、[Protection] > [Overview]に移動し、[Storage VM Peers]の下の[Peer Storage VMs]を選択します。

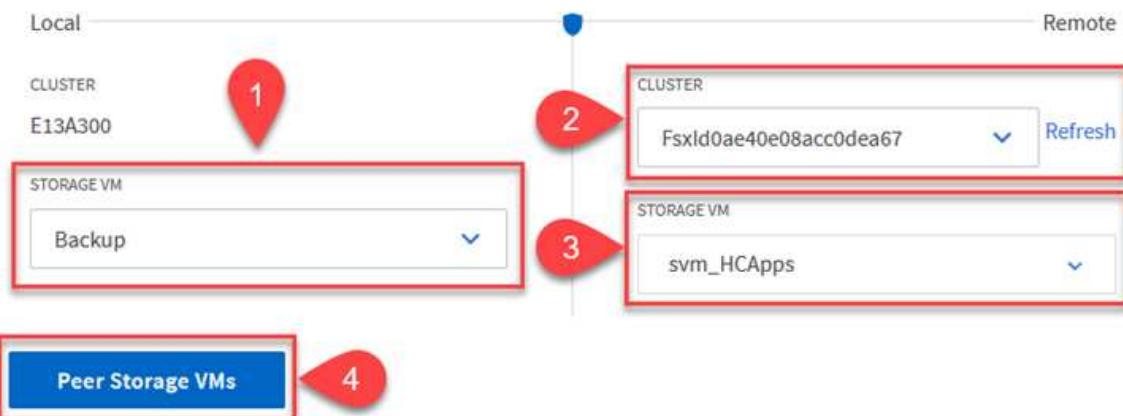


4. ピアストレージVMのダイアログボックスで、必須フィールドに入力します。

- ソースストレージVM
- 宛先クラスター
- 宛先ストレージVM

Peer Storage VMs

X



5. SVM ピアリング プロセスを完了するには、[ピア ストレージ VM] をクリックします。

スナップショット保持ポリシーを作成する

SnapCenter は、プライマリストレージシステム上にスナップショット コピーとして存在するバックアップの保持スケジュールを管理します。これは、SnapCenterでポリシーを作成するときに確立されます。SnapCenter は、セカンダリストレージシステムに保持されるバックアップの保持ポリシーを管理しません。これらのポリシーは、セカンダリ FSx クラスター上に作成され、ソース ボリュームと SnapMirror 関係にある宛先ボリュームに関連付けられた SnapMirror ポリシーを通じて個別に管理されます。

SnapCenter ポリシーを作成するときに、SnapCenter バックアップの作成時に生成される各スナップショットの SnapMirror ラベルに追加されるセカンダリ ポリシー ラベルを指定するオプションがあります。



セカンダリストレージでは、これらのラベルは、スナップショットの保持を強制する目的で、宛先ボリュームに関連付けられたポリシールールと照合されます。

次の例は、SQL Server データベースとログ ボリュームの毎日のバックアップに使用されるポリシーの一部として生成されたすべてのスナップショットに存在する SnapMirror ラベルを示しています。

Select secondary replication options

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Custom Label

sql-daily

Error retry count

3



SQL Server データベース用の SnapCenter ポリシーの作成の詳細については、["SnapCenter のドキュメント"](#)。

まず、保持するスナップショット コピーの数を指定するルールを含む SnapMirror ポリシーを作成する必要があります。

1. FSx クラスターに SnapMirror ポリシーを作成します。

```
ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. SnapCenter ポリシーで指定されたセカンダリ ポリシー ラベルと一致する SnapMirror ラベルを使用して、ポリシーにルールを追加します。

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

次のスクリプトは、ポリシーに追加できるルールの例を示しています。

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest  
-policy Async_SnapCenter_SQL -snapmirror-label sql-on-demand -keep 15
```



各SnapMirrorラベルと保持するスナップショットの数(保持期間)に対して追加のルールを作成します。

宛先ボリュームを作成する

ソースボリュームからのスナップショットコピーの受信者となる宛先ボリュームをONTAP上に作成するには、宛先ONTAPクラスターで次のコマンドを実行します。

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName  
-aggregate DestAggrName -size VolSize -type DP
```

ソースボリュームと宛先ボリューム間の**SnapMirror**関係を作成する

ソースボリュームと宛先ボリュームの間にSnapMirror関係を作成するには、宛先ONTAPクラスタで次のコマンドを実行します。

```
ONTAP-Dest::> snapmirror create -source-path  
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type  
XDP -policy PolicyName
```

SnapMirror関係を初期化する

SnapMirror関係を初期化します。このプロセスは、ソースボリュームから生成された新しいスナップショットを開始し、それを宛先ボリュームにコピーします。

ボリュームを作成するには、宛先のONTAPクラスターで次のコマンドを実行します。

```
ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

SnapCenter Plug-in for VMware vSphereを構成する

インストールが完了すると、vCenter Server Appliance 管理インターフェイスからSnapCenter Plug-in for VMware vSphereにアクセスできるようになります。SCVは、ESXiホストにマウントされ、WindowsおよびLinux VMを含むNFSデータストアのバックアップを管理します。

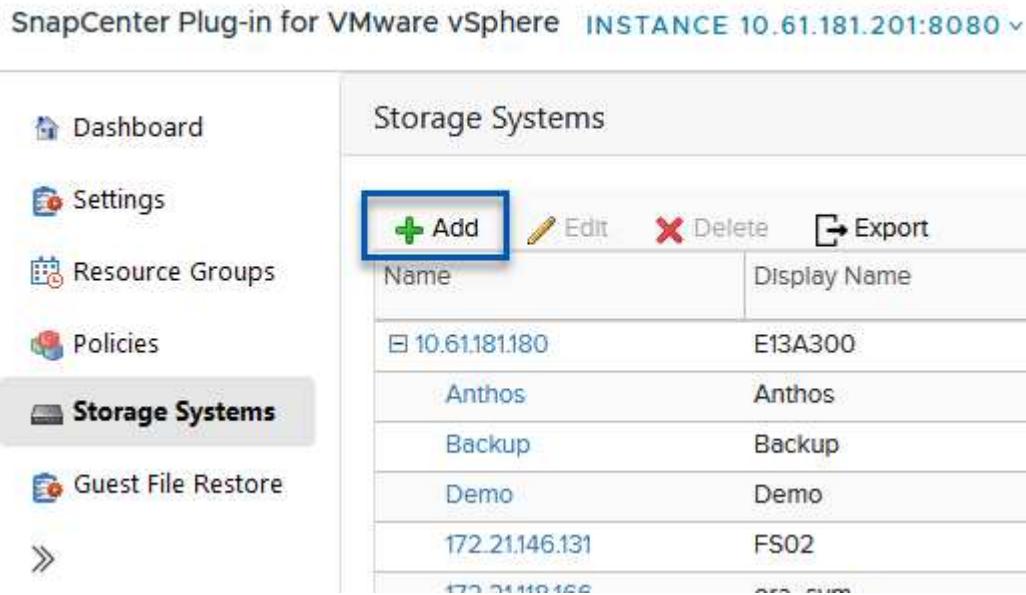
レビュー "データ保護のワークフロー" バックアップの構成手順の詳細については、SCV ドキュメントのセクションを参照してください。

仮想マシンとデータストアのバックアップを構成するには、プラグイン インターフェイスから次の手順を完了する必要があります。

Discovery ONTAPストレージシステム

プライマリ バックアップとセカンダリ バックアップの両方に使用されるONTAPストレージ クラスターを検出します。

1. SnapCenter Plug-in for VMware vSphereで、左側のメニューの ストレージ システム に移動し、追加ボタンをクリックします。



The screenshot shows the 'Storage Systems' page of the SnapCenter interface. On the left, a sidebar menu has 'Storage Systems' selected. At the top right, there are buttons for 'Add', 'Edit', 'Delete', and 'Export'. A table lists storage systems with columns for 'Name' and 'Display Name'. The first entry is '10.61.181.180' with 'E13A300' as the display name. Other entries include 'Anthos', 'Backup', 'Demo', and '172.21.146.131' with 'FS02' as the display name.

Name	Display Name
10.61.181.180	E13A300
Anthos	Anthos
Backup	Backup
Demo	Demo
172.21.146.131	FS02
172.21.146.130	FS01

2. プライマリONTAPストレージ システムの資格情報とプラットフォーム タイプを入力し、[追加] をクリックします。

Add Storage System

Storage System	10.61.185.145
Platform	All Flash FAS
Authentication Method	<input checked="" type="radio"/> Credentials <input type="radio"/> Certificate
Username	admin
Password	*****
Protocol	HTTPS
Port	443
Timeout	60 <input type="text"/> Seconds
<input type="checkbox"/> Preferred IP	Preferred IP

Event Management System(EMS) & AutoSupport Setting

- Log Snapcenter server events to syslog
- Send AutoSupport Notification for failed operation to storage system

3. セカンダリONTAPストレージ システムに対してこの手順を繰り返します。

SCVバックアップポリシーを作成する

ポリシーは、SCVによって管理されるバックアップの保持期間、頻度、およびレプリケーションオプションを指定します。

レビュー "VMとデータストアのバックアップポリシーの作成" 詳細については、ドキュメントのセクションを参照してください。

バックアップポリシーを作成するには、次の手順を実行します。

1. SnapCenter Plug-in for VMware vSphereで、左側のメニューの Policies に移動し、作成ボタンをクリックします。



The screenshot shows the 'Policies' screen of the SnapCenter Plug-in for VMware vSphere. On the left, there is a navigation menu with the following items: Dashboard, Settings, Resource Groups, Policies (which is selected and highlighted in grey), Storage Systems, and Guest File Restore. The main area is titled 'Policies' and contains a table with the following data:

Name	VM Co
Daily	No
FCD	No
Hourly	No
Monthly	No

A green 'Create' button is located at the top right of the table, and it is highlighted with a blue rectangular box.

2. ポリシーの名前、保持期間、頻度とレプリケーションのオプション、スナップショットラベルを指定します。

New Backup Policy

Name	Daily
Description	description
Retention	Days to keep 30
Frequency	Daily
Replication	<input type="checkbox"/> Update SnapMirror after backup <small>i</small> <input checked="" type="checkbox"/> Update SnapVault after backup <small>i</small>
	Snapshot label Daily
Advanced ▾	<input checked="" type="checkbox"/> VM consistency <small>i</small> <input type="checkbox"/> Include datastores with independent disks
	Scripts <small>i</small> Enter script path



SnapCenterプラグインでポリシーを作成すると、SnapMirrorとSnapVaultのオプションが表示されます。SnapMirrorを選択した場合、ポリシーで指定された保持スケジュールはプライマリスナップショットとセカンダリスナップショットの両方で同じになります。SnapVaultを選択した場合、セカンダリスナップショットの保持スケジュールは、SnapMirror関係で実装された別のスケジュールに基づいて決定されます。これは、セカンダリバックアップの保持期間を長くしたい場合に便利です。



スナップショットラベルは、セカンダリONTAPクラスタに複製されたSnapVaultコピーに対して特定の保持期間を設定したポリシーを適用するために使用できるため便利です。SCVをBlueXPバックアップおよびリストアで使用する場合、スナップショットラベルフィールドは空白にするか、BlueXPバックアップポリシーで指定されたラベルと一致する必要があります。

- 必要なポリシーごとにこの手順を繰り返します。たとえば、毎日、毎週、毎月のバックアップに個別のポリシーを設定します。

リソース グループの作成

リソース グループには、バックアップジョブに含めるデータストアと仮想マシン、および関連するポリシーとバックアップスケジュールが含まれます。

レビュー "リソース グループの作成" 詳細については、ドキュメントのセクションを参照してください。

リソース グループを作成するには、次の手順を実行します。

1. SnapCenter Plug-in for VMware vSphereで、左側のメニューの **リソース グループ** に移動し、作成ボタンをクリックします。

SnapCenter Plug-in for VMware vSphere INSTANCE 10.61.181.201:8080

The screenshot shows the 'Resource Groups' page. On the left, there is a sidebar with icons for Dashboard, Settings, Resource Groups (which is selected and highlighted in grey), Policies, Storage Systems, and Guest File Restore. On the right, there is a table titled 'Resource Groups' with columns for 'Name' and 'Desc'. The table contains four rows: 'SMBC', 'Oracle_Servers', 'Demo', and 'SQL_Servers_Weekly'. Above the table are four buttons: '+ Create' (highlighted with a blue box), 'Edit', 'Delete', and 'Run Now'.

Name	Desc
SMBC	
Oracle_Servers	
Demo	
SQL_Servers_Weekly	

2. リソース グループの作成ウィザードで、グループの名前と説明、および通知を受信するために必要な情報を入力します。「次へ」をクリックします
3. 次のページで、バックアップジョブに含めるデータストアと仮想マシンを選択し、[次へ] をクリックします。

Create Resource Group

✓ 1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope: Datastores

Datacenter: Datastores

Available entities: Demo, DemoDS, destination, esxi7-hc-01 Local, esxi7-hc-02 Local, esxi7-hc-03 Local

Selected entities: NFS_SCV, NFS_WKLD

特定の VM またはデータストア全体を選択するオプションがあります。どちらを選択した場合でも、バックアップは基礎となるボリュームのスナップショットを取得した結果であるため、ボリューム全体 (およびデータストア) がバックアップされます。ほとんどの場合、データストア全体を選択するのが最も簡単です。ただし、復元時に使用可能な VM のリストを制限する場合は、バックアップ対象として VM のサブセットのみを選択できます。

4. 複数のデータストアに存在する VMDK を持つ VM のデータストアをまたぐためのオプションを選択し、[次へ] をクリックします。

Create Resource Group

✓ 1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Always exclude all spanning datastores
This means that only the datastores directly added to the resource group and the primary datastore of VMs directly added to the resource group will be backed up

Always include all spanning datastores
All datastores spanned by all included VMs are included in this backup

Manually select the spanning datastores to be included
You will need to modify the list every time new VMs are added

There are no spanned entities in the selected virtual entities list.

BlueXP backup and recoveryでは、現在、複数のデータストアにまたがる VMDK を持つ VM のバックアップはサポートされていません。

5. 次のページで、リソース グループに関連付けるポリシーを選択し、[次へ] をクリックします。

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

4. Policies

5. Schedules

6. Summary

+ Create

Name	VM Consistent	Include independent di...	Schedule
<input checked="" type="checkbox"/> Daily	No	No	Daily
<input type="checkbox"/> FCD	No	Yes	On Demand Only
<input type="checkbox"/> Monthly	No	No	Monthly
<input type="checkbox"/> On Demand	No	No	On Demand Only
<input type="checkbox"/> Weekly	No	No	Weekly



BlueXP backup and recoveryを使用して SCV 管理スナップショットをオブジェクトストレージにバックアップする場合、各リソース グループは 1 つのポリシーにのみ関連付けることができます。

6. バックアップが実行される時刻を決定するスケジュールを選択します。*次へ*をクリックします。

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

5. Schedules

✓ 6. Summary

Daily

Type

Daily

Every

1

Day(s)

Starting

06/23/2023



At

07 00 PM

7. 最後に、概要ページを確認し、[完了] をクリックしてリソース グループの作成を完了します。

バックアップジョブを実行する

この最後のステップでは、バックアップジョブを実行し、その進行状況を監視します。BlueXP backup and recoveryからリソースを検出する前に、SCVで少なくとも1つのバックアップジョブが正常に完了している必要があります。

1. SnapCenter Plug-in for VMware vSphereで、左側のメニューの「リソース グループ」に移動します。
2. バックアップジョブを開始するには、目的のリソース グループを選択し、「今すぐ実行」ボタンをクリックします。

SnapCenter Plug-in for VMware vSphere INSTANCE 10.61.181.201:8080 ▾

The screenshot shows the 'Resource Groups' page of the SnapCenter interface. On the left, a sidebar menu includes 'Dashboard', 'Settings', 'Resource Groups' (which is selected and highlighted in grey), 'Policies', 'Storage Systems', 'Guest File Restore', and a 'More' section. The main area is titled 'Resource Groups' and contains a table with columns 'Name' and 'Description'. The table lists several groups: 'Win01', 'SMBC', 'Oracle_Servers', 'Demo', 'SQL_Servers_Daily' (which is highlighted with a blue background), and 'SQL_Servers_Weekly'. Above the table are buttons for 'Create', 'Edit', 'Delete', 'Run Now' (which is highlighted with a blue border), and 'Suspend'.

Name	Description
Win01	
SMBC	
Oracle_Servers	
Demo	
SQL_Servers_Daily	
SQL_Servers_Weekly	

3. バックアップジョブを監視するには、左側のメニューの「ダッシュボード」に移動します。最近のジョブアクティビティの下でジョブ ID 番号をクリックして、ジョブの進行状況を監視します。

- Validate Retention Settings
 - Quiescing Applications
 - Retrieving Metadata
 - Creating Snapshot copy
 - Unquiescing Applications
 - Registering Backup
 - Backup Retention
 - Clean Backup Cache
 - Send EMS Messages
 - (Job 2616) SnapVault Update
- Running, Start Time: 07/31/2023 07:24:40 PM.

[CLOSE](#)[DOWNLOAD JOB LOGS](#)

BlueXP backup and recoveryでオブジェクトストレージへのバックアップを構成する

BlueXPがデータインフラストラクチャを効果的に管理するには、事前にコネクタをインストールする必要があります。コネクタは、リソースの検出とデータ操作の管理に関するアクションを実行します。

BlueXPコネクタの詳細については、以下を参照してください。["コネクタについて学ぶ"](#) BlueXPドキュメント内。

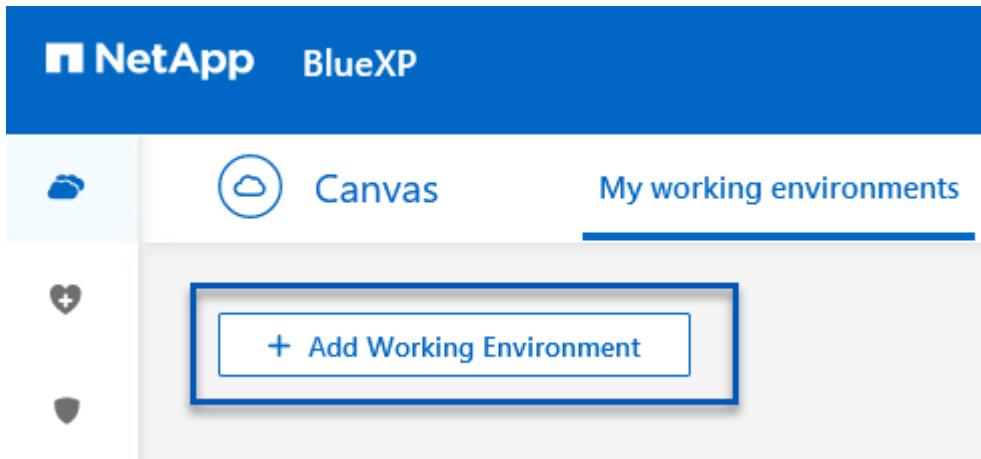
利用しているクラウドプロバイダーのコネクタがインストールされると、オブジェクトストレージのグラフィック表現がキャンバスから表示できるようになります。

SCVオンプレミスで管理されるデータをバックアップするようにBlueXP backup and recoveryを構成するには、次の手順を実行します。

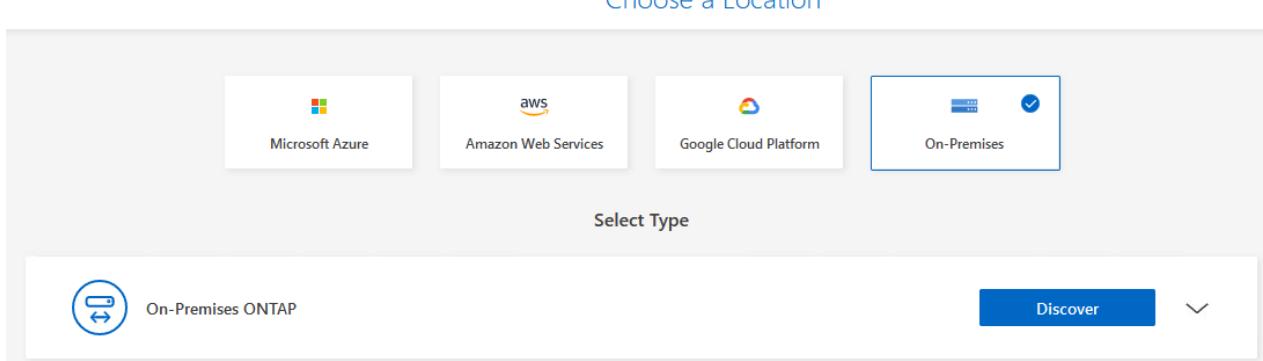
キャンバスに作業環境を追加する

最初のステップは、オンプレミスのONTAPストレージシステムをBlueXPに追加することです。

1. キャンバスから「作業環境の追加」を選択して開始します。



2. 場所の選択肢から「オンプレミス」を選択し、「検出」ボタンをクリックします。



3. ONTAPストレージシステムの資格情報を入力し、[検出]ボタンをクリックして作業環境を追加します。

ONTAP Cluster IP

10.61.181.180

User Name

admin

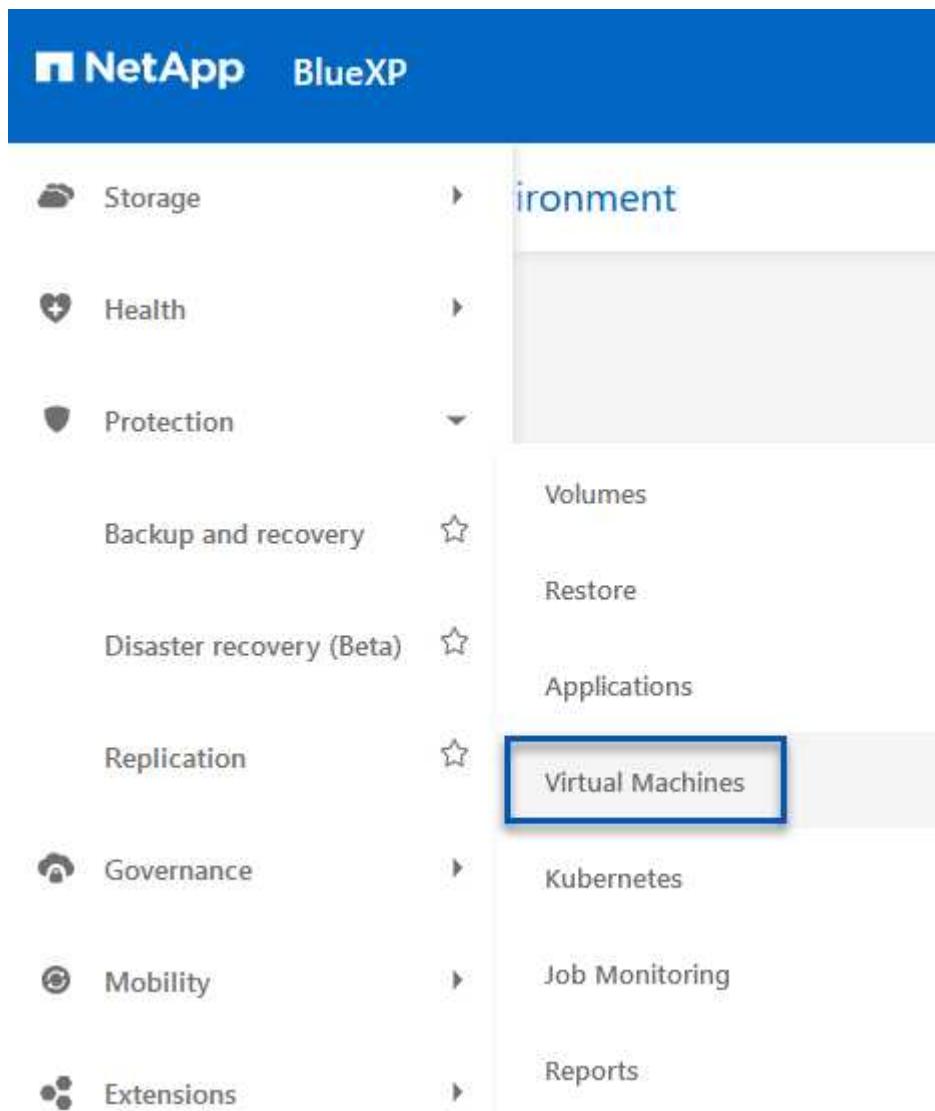
Password



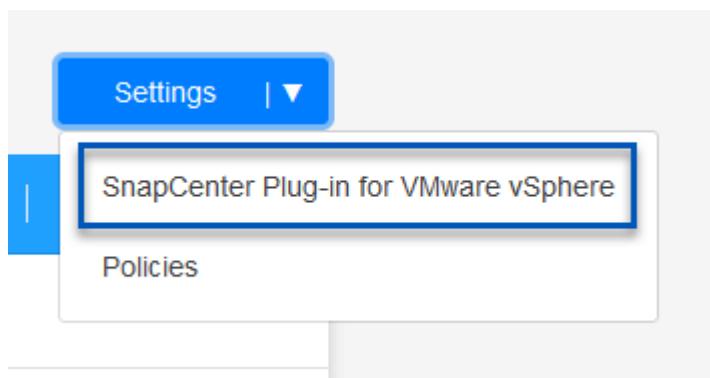
オンプレミスの SCV アプライアンスと vCenter の検出

オンプレミスのデータストアと仮想マシンのリソースを検出するには、SCV データ プローカーの情報と vCenter 管理アプライアンスの資格情報を追加します。

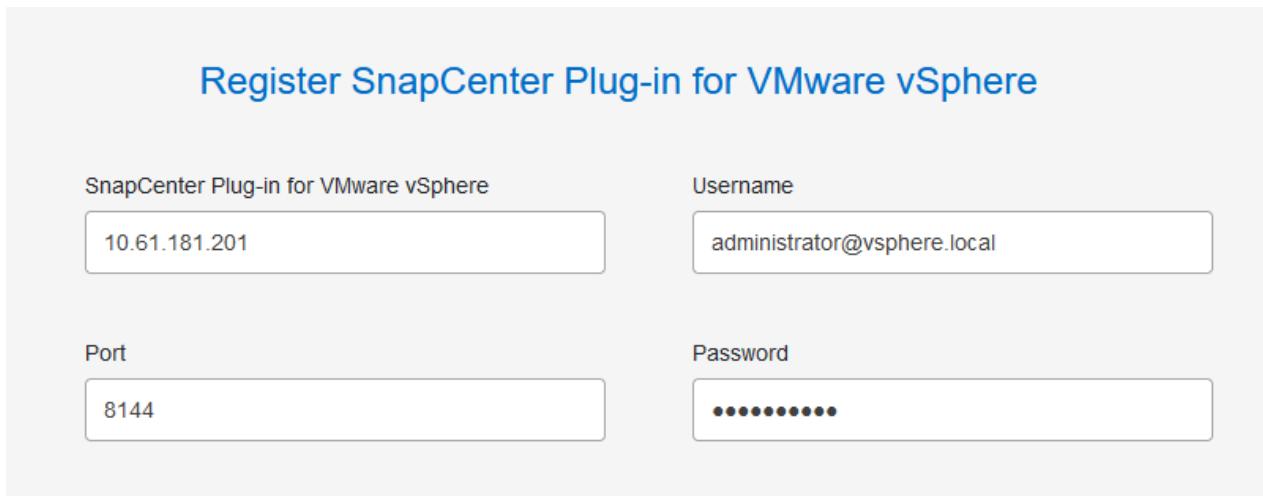
1. BlueXP の左側のメニューから *保護 > バックアップとリカバリ > 仮想マシン* を選択します。



2. 仮想マシンのメイン画面から [設定] ドロップダウン メニューにアクセスし、[SnapCenter Plug-in for VMware vSphere] を選択します。



3. 登録 ボタンをクリックし、SnapCenterプラグインアプライアンスのIPアドレスとポート番号、およびvCenter管理アプライアンスのユーザー名とパスワードを入力します。検出プロセスを開始するには、[登録] ボタンをクリックします。



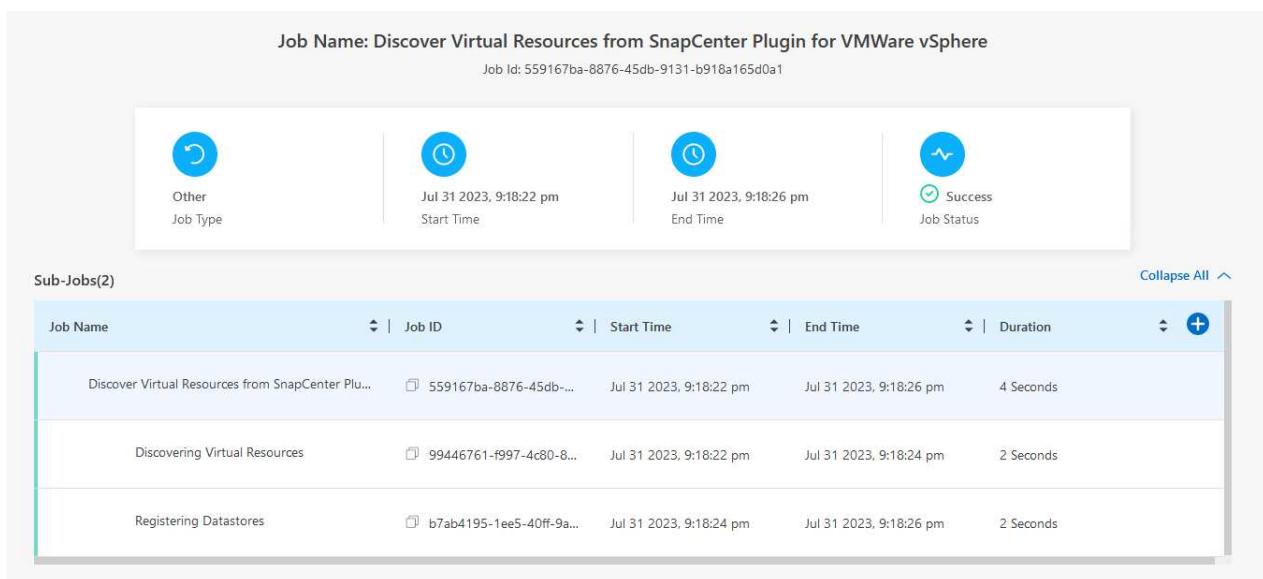
SnapCenter Plug-in for VMware vSphere

Username: administrator@vsphere.local

Port: 8144

Password: [REDACTED]

4. ジョブの進行状況は、「ジョブ監視」タブから監視できます。



Job Name: Discover Virtual Resources from SnapCenter Plugin for VMWare vSphere
Job Id: 559167ba-8876-45db-9131-b918a165d0a1

Job Name	Job ID	Start Time	End Time	Duration
Discover Virtual Resources from SnapCenter Plu...	559167ba-8876-45db-9131-b918a165d0a1	Jul 31 2023, 9:18:22 pm	Jul 31 2023, 9:18:26 pm	4 Seconds
Discovering Virtual Resources	99446761-f997-4c80-8...	Jul 31 2023, 9:18:22 pm	Jul 31 2023, 9:18:24 pm	2 Seconds
Registering Datastores	b7ab4195-1ee5-40ff-9a...	Jul 31 2023, 9:18:24 pm	Jul 31 2023, 9:18:26 pm	2 Seconds

5. 検出が完了すると、検出されたすべてのSCVアプライアンスのデータストアと仮想マシンを表示できるようになります。

4 Working Environments | 6 Datastores | 14 Virtual Machines

Datastore Protection: 4 Protected, 2 Unprotected

6 Datastores

Filter By +

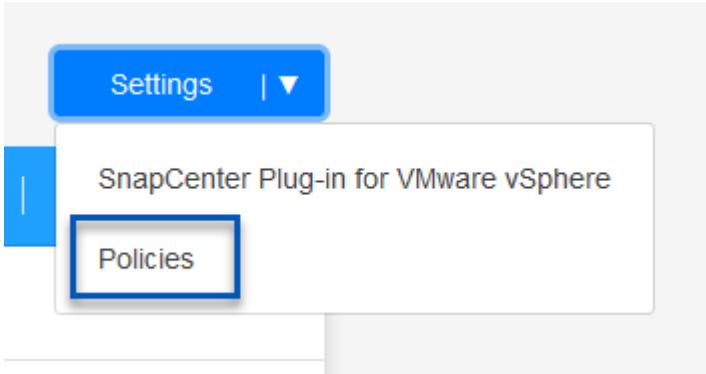
Datastore	Datastore Type	vCenter	Policy Name	Protection Status	Actions
NFS_SCV	NFS	vcsa7-hc.sddc.netapp.com		Unprotected	...
OTS_DS01	NFS	172.21.254.160	1 Year Daily LTR	Protected	...
SCV_WKLD	NFS	vcsa7-hc.sddc.netapp.com	1 Year Daily LTR	Protected	...
NFS_SQL	NFS	vcsa7-hc.sddc.netapp.com	1 Year Daily LTR	Protected	...
NFS_SQL2	NFS	vcsa7-hc.sddc.netapp.com	1 Year Daily LTR	Protected	...
SCV_DEMO	NFS	vcsa7-hc.sddc.netapp.com		Unprotected	...

BlueXPバックアップポリシーを作成する

仮想マシンのBlueXP backup and recoveryでは、保持期間、バックアップソース、アーカイブ ポリシーを指定するポリシーを作成します。

ポリシー作成の詳細については、以下を参照してください。 "データストアをバックアップするポリシーを作成する"。

1. BlueXP backup and recoveryのメイン ページで、[設定] ドロップダウン メニューにアクセスし、[ポリシー] を選択します。



2. ポリシーの作成 をクリックして、ハイブリッド バックアップのポリシーの作成 ウィンドウにアクセスします。
 - a. ポリシーの名前を追加する
 - b. 希望する保存期間を選択してください
 - c. バックアップをプライマリまたはセカンダリのオンプレミスONTAPストレージ システムから取得するかどうかを選択します。
 - d. オプションで、追加のコスト削減のために、どのくらいの期間後にバックアップがアーカイブ ストレージに階層化されるかを指定します。

Create Policy for Hybrid Backup

Policy Details	Policy Name <input type="text" value="12 week - daily backups"/>
Retention ⓘ <div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> <input checked="" type="radio"/> Daily </div> <div style="flex: 1;"> <input type="radio"/> Weekly </div> <div style="flex: 1;"> <input type="radio"/> Monthly </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="flex: 1;"> Backups to retain <input type="text" value="84"/> </div> <div style="flex: 1;"> SnapMirror Label <input type="text" value="Daily"/> </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="flex: 1;"> <input type="checkbox"/> Setup Retention Weekly </div> <div style="flex: 1;"> <input type="checkbox"/> Setup Retention Monthly </div> </div>	
Backup Source <div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> <input checked="" type="radio"/> Primary </div> <div style="flex: 1;"> <input type="radio"/> Secondary </div> </div>	
Archival Policy ⓘ <div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> <p>Backups reside in standard storage for frequently accessed data. Optionally, you can tier backups to archival storage for further cost optimization.</p> <p><input type="checkbox"/> Tier Backups to Archival</p> <p>Archival After (Days)</p> </div> <div style="flex: 1;"></div> </div>	
<input type="button" value="Cancel"/> <input style="background-color: #0072bc; color: white; border-radius: 5px; padding: 5px 10px; border: none; font-weight: bold; font-size: 1em; margin-left: 10px;" type="button" value="Create"/>	

ⓘ ここで入力したSnapMirrorラベルは、ポリシーを適用するバックアップを識別するために使用されます。ラベル名は、対応するオンプレミスの SCV ポリシーのラベル名と一致する必要があります。

3. *作成*をクリックしてポリシーの作成を完了します。

Amazon Web Services へのデータストアのバックアップ

最後のステップは、個々のデータストアと仮想マシンのデータ保護を有効にすることです。次の手順では、AWSへのバックアップをアクティブ化する方法を説明します。

詳細については、 "データストアを Amazon Web Services にバックアップする"。

1. BlueXP backup and recoveryのメイン ページから、バックアップするデータストアの設定ドロップダウンにアクセスし、[バックアップのアクティブ化] を選択します。

The screenshot shows a table titled '6 Datastores'. The columns are: Datastore, Datastore Type, vCenter, Policy Name, and Protection Status. The 'OTS_DS01' row has a 'Protected' status with a green checkmark. A context menu is open over this row, with the 'Activate Backup' option highlighted by a red box.

Datastore	Datastore Type	vCenter	Policy Name	Protection Status
NFS_SCV	NFS	vcsa7-hc.sddc.netapp.com		Unprotected
OTS_DS01	NFS	172.21.254.160	1 Year Daily LTR	Protected
SCV_WKLD	NFS	vcsa7-hc.sddc.netapp.com	1 Year Daily LTR	Protected

2. データ保護操作に使用するポリシーを割り当て、[次へ] をクリックします。

The screenshot shows a 'Assign Policy' step with five numbered steps at the top: 1 Assign Policy, 2 Add Working Environments, 3 Select Provider, 4 Configure Provider, and 5 Review. Below is a table titled '21 Policies' with columns: Policy Name, SnapMirror Label, Retention Count, Backup Source, and Archival Policy. The '5 Year Daily LTR' policy is selected, indicated by a checked checkbox.

Policy Name	SnapMirror Label	Retention Count	Backup Source	Archival Policy
<input type="radio"/> 5 Year Daily LTR	daily	daily : 1830	Primary	Not Active
<input checked="" type="radio"/> 5 Year Daily LTR	daily	daily : 1830	Primary	Not Active
<input type="radio"/> 7 Year Weekly LTR	weekly	weekly : 370	Primary	Not Active

3. 作業環境が以前に検出されている場合は、「作業環境の追加」ページに、チェックマークが付いたデータストアと作業環境が表示されます。作業環境が以前に検出されていない場合は、ここで追加できます。続行するには、[次へ] をクリックします。

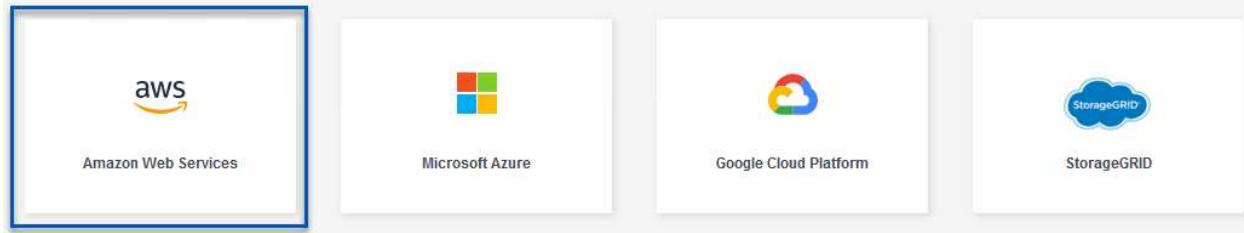
Add Working Environments

Provide ONTAP cluster (working environment) details that you want Cloud Manager to discover. Working environment details will appear for all volumes that reside on the same cluster. You will need to enter multiple working environments when volumes reside on different clusters.

SVM	Volume	Working Environment	
EHC_NFS	NFS_SCV	OnPremWorkingEnvironment-6MzE27u1	Edit

4. *プロバイダーの選択*ページでAWSをクリックし、*次へ*ボタンをクリックして続行します。

Select Provider



5. 使用する AWS アクセスキーとシークレットキー、リージョン、アーカイブ層など、AWS のプロバイダー固有の認証情報を入力します。また、オンプレミスのONTAPストレージシステムのONTAP IP スペースを選択します。*次へ*をクリックします。

Configure Provider

Cloud Manager needs the following details to connect with the cloud provider.

Provider Information		Location and Connectivity	
AWS Account		Region	US East (N. Virginia)
AWS Access Key	Enter AWS Access Key	IP space for Environment	OnPremWorkingEnvironment-6MzE27u1
	Required		Default
AWS Secret Key	Enter AWS Secret Key	Archival Tier	Glacier
	Required		

6. 最後に、バックアップジョブの詳細を確認し、[バックアップのアクティブ化] ボタンをクリックして、データストアのデータ保護を開始します。

Assign Policy

Add Working Environments

Select Provider

Configure Provider

5 Review

Review

Policy	5 Year Daily LTR
SVM	EHC_NFS
Volumes	NFS_SCV
Working Environment	OnPremWorkingEnvironment-6MzE27u1
Backup Source	Primary
Cloud Service Provider	AWS
AWS Account	[REDACTED]
AWS Access Key	[REDACTED]
Region	US East (N. Virginia)
IP space	Default
Tier Backups to Archival	No

Previous

Activate Backup



この時点ではデータ転送がすぐに開始されない場合があります。BlueXP backup and recoveryは、未処理のスナップショットを1時間ごとにスキャンし、それらをオブジェクトストレージに転送します。

データ損失の場合の仮想マシンの復元

データの安全を確保することは、包括的なデータ保護の1つの側面にすぎません。同様に重要なのは、データの損失やランサムウェア攻撃が発生した場合に、どこからでも迅速にデータを復元できる機能です。この機能は、シームレスなビジネス運用を維持し、リカバリポイント目標を達成するために不可欠です。

NetApp は、適応性に優れた 3-2-1 戦略を提供し、プライマリ、セカンダリ、およびオブジェクトストレージの場所で保持スケジュールをカスタマイズして制御できます。この戦略により、データ保護のアプローチを特定のニーズに合わせて柔軟にカスタマイズできるようになります。

このセクションでは、SnapCenter Plug-in for VMware vSphere と仮想マシンのBlueXP backup and recovery の両方からのデータ復元プロセスの概要を説明します。

SnapCenter Plug-in for VMware vSphere からの仮想マシンの復元

このソリューションでは、仮想マシンが元の場所と別の場所に復元されました。このソリューションでは、SCV のデータ復元機能のすべての側面がカバーされるわけではありません。SCV が提供するすべての詳細情報については、["バックアップからの VM のリストア" 製品ドキュメント](#)に記載されています。

SCVから仮想マシンを復元する

プライマリストレージまたはセカンダリストレージから仮想マシンを復元するには、次の手順を実行します。

1. vCenter クライアントから インベントリ > ストレージに移動し、復元する仮想マシンが含まれているデータストアをクリックします。
2. 構成タブから バックアップをクリックして、利用可能なバックアップのリストにアクセスします。

Name	Status	Locations	Start Time	End Time	Mounted	Policy	VMware Snapshot
scv_demo_daily_07-31-2023_19.24.36.0755	Completed	Primary & Secondary	7/30/2023 7:24:36 PM	7/30/2023 7:24:38 PM	No	Daily	No
scv_demo_daily_07-31-2023_09.38.00.08	Completed	Primary & Secondary	7/30/2023 9:38:00 AM	7/30/2023 9:38:02 AM	No	Daily	No
scv_demo_daily_07-30-2023_09.39.00.08	Completed	Primary & Secondary	7/30/2023 9:39:00 AM	7/30/2023 9:39:02 AM	No	Daily	No
scv_demo_daily_07-29-2023_09.39.00.08	Completed	Primary & Secondary	7/29/2023 9:39:00 AM	7/29/2023 9:39:02 AM	No	Daily	No
scv_demo_daily_07-28-2023_09.38.00.08	Completed	Primary & Secondary	7/28/2023 9:38:00 AM	7/28/2023 9:38:02 AM	No	Daily	No
scv_demo_daily_07-27-2023_09.37.28.08	Completed	Primary & Secondary	7/27/2023 9:37:28 AM	7/27/2023 9:37:30 AM	No	Daily	No
scv_demo_daily_07-27-2023_09.37.29.08	Completed	Primary & Secondary	7/27/2023 9:37:29 AM	7/27/2023 9:37:30 AM	No	Daily	No
scv_demo_daily_07-27-2023_09.38.00.08	Completed	Primary & Secondary	7/27/2023 9:38:00 AM	7/27/2023 9:38:02 AM	No	Daily	No
scv_demo_daily_07-27-2023_09.38.01.08	Completed	Primary & Secondary	7/27/2023 9:38:01 AM	7/27/2023 9:38:12 AM	No	Daily	No

3. バックアップをクリックして VM のリストにアクセスし、復元する VM を選択します。*復元*をクリックします。

Entity Name	Quiesced	UUID	Location
SQLSRV-07	No	5032d1f2-2591-7fb-46e3-8bd4a6b2fb4	[SCV_DEMO] SQLSRV-07/SQLSRV-07.vmx
scv_restore_test	Yes	50323c8e-04a3-5ac-a2df-a6bc0ced0419	[SCV_DEMO] scv_restore_test/scv_restore_test.vmx
SQLSRV-06	No	50327515-8cce-5942-0f85-350ad39bce42	[SCV_DEMO] SQLSRV-06/SQLSRV-06.vmx
SQLSRV-08	No	5032b2a9-e1af-c56a-6923-6dd0deeb6327	[SCV_DEMO] SQLSRV-08/SQLSRV-08.vmx
SQLSRV-05	No	50326625-dd29-af23-2fd5-fe04e0a57a69	[SCV_DEMO] SQLSRV-05/SQLSRV-05.vmx
SCV_DEMO	No	netfs://172.21.118.112//SCV_DEMO	SCV/vol/SCV_DEMO

4. 復元ウィザードから、仮想マシン全体を復元するか、特定の VMDK を復元するかを選択します。元の場所または別の場所にインストールすることを選択し、復元後の VM 名と宛先データストアを指定します。*次へ*をクリックします。

Restore

X

1. Select scope

2. Select location

3. Summary

Restore scope

Entire virtual machine

Restart VM



Restore Location

Original Location

(This will restore the entire VM to the original Hypervisor with the original settings. Existing VM will be unregistered and replaced with this VM.)

Alternate Location

(This will create a new VM on selected vCenter and Hypervisor with the customized settings.)

Destination vCenter Server

10.61.181.210

Destination ESXi host

esxi7-hc-04.sddc.netapp.com

Network

Management 181

VM name after restore

SQL_SRV_08_restored

Select Datastore:

NFS_SCV

BACK

NEXT

FINISH

CANCEL

5. プライマリまたはセカンダリのストレージ場所からバックアップすることを選択します。

Restore

X

1. Select scope

2. Select location

3. Summary

Destination datastore

SCV_DEMO

Locations

(Primary) SCV:SCV_DEMO

(Primary) SCV:SCV_DEMO

(Secondary) EHC_NFS:SCV_DEMO_dest

6. 最後に、バックアップジョブの概要を確認し、「完了」をクリックして復元プロセスを開始します。

BlueXP backup and recoveryから仮想マシンを復元する

仮想マシン用のBlueXP backup and recoveryを使用すると、仮想マシンを元の場所に復元できます。復元機能には、BlueXP Web コンソールからアクセスします。

詳細については、"クラウドから仮想マシンのデータを復元する"。

BlueXP backup and recoveryから仮想マシンを復元する

BlueXP backup and recoveryから仮想マシンを復元するには、次の手順を実行します。

1. 保護 > バックアップとリカバリ > 仮想マシンに移動し、仮想マシンをクリックして、復元可能な仮想マシンのリストを表示します。

The screenshot shows the BlueXP Backup and Recovery web interface. At the top, there's a navigation bar with tabs: Backup and recovery (selected), Volumes, Restore, Applications, Virtual Machines (highlighted with a blue underline), Kubernetes, Job Monitoring, and Reports. Below the navigation bar, there's a summary section with three items: 'Working Environments' (4), 'Datastores' (6), and 'Virtual Machines' (14, which is also enclosed in a blue rectangular box). The main area is currently empty, likely because the 'Virtual Machines' tab has just been selected.

2. 復元するVMの設定ドロップダウンメニューにアクセスし、

The screenshot shows the 'Virtual Machines' list view. At the top, it says '14 Virtual Machines'. There are filters for 'Filter By' and 'Settings'. The main table has columns: Virtual Machine, Datastore Type, vCenter, Policy Name, Protection Status, and Last Backup. Three rows are listed:

- SQLSRV-08: NFS, vCenter: vcsa7-hc.sddc.netap..., Protection Status: Unprotected
- SQLSRV-04: NFS, vCenter: vcsa7-hc.sddc.netap..., Policy Name: 1 Year Daily LTR, Protection Status: Protected, Last Backup: Jul 31, 2023, 7:2...
- OracleSrv_03: NFS, vCenter: vcsa7-hc.sddc.netap..., Protection Status: Unprotected

The 'Restore' button for the OracleSrv_03 row is highlighted with a blue box.

3. 復元するバックアップを選択し、「次へ」をクリックします。

The screenshot shows the 'Backups' list view. At the top, it says '17 Backups'. The table has columns: Backup Name and Backup Time. Three rows are listed:

- SQL_Servers_Daily_07-31-2023_19.23.39.0938 (selected with a checked checkbox)
- SQL_Servers_Daily_07-31-2023_16.40.00.0661
- SQL_Servers_Daily_07-30-2023_16.40.00.0690

The first backup row is highlighted with a blue box.

4. バックアップジョブの概要を確認し、[復元]をクリックして復元プロセスを開始します。

5. *ジョブ監視*タブから復元ジョブの進行状況を監視します。

The screenshot shows the NetApp SnapCenter interface with the following details:

- Job Name:** Restore 17 files from Cloud
- Job Id:** ec567065-dcf4-4174-b7ef-b27e6620fdbf
- Job Type:** Restore Files
- Restore Content:** NFS_SQL
- Content Files:** 17 Files
- Restore to:** NFS_SQL
- In Progress:** Job Status

Restore Content Configuration:

aws	ots-demo	NAS_VOLS	NFS_SQL	SQL_Servers_Daily_07-31-2023...
	Working Environment Name	SVM Name	Volume Name	Backup Name
				Jul 31 2023, 7:24:03 pm
				Backup Time

Restore from Configuration:

aws	AWS	us-east-1	982589175402	netapp-backup-d56250b0-24ad...
	Provider	Region	Account ID	Bucket/Container Name

まとめ

3-2-1 バックアップ戦略は、SnapCenter Plug-in for VMware vSphereと仮想マシン用のBlueXP backup and recoveryを使用して実装すると、データ保護のための堅牢で信頼性が高く、コスト効率に優れたソリューションを提供します。この戦略は、データの冗長性とアクセス性を保証するだけでなく、オンプレミスのONTAPストレージシステムとクラウドベースのオブジェクトストレージの両方から、任意の場所からデータを復元できる柔軟性も提供します。

このドキュメントで紹介するユースケースは、NetApp、VMware、および主要なクラウド プロバイダー間の統合を強調する実証済みのデータ保護テクノロジに重点を置いています。SnapCenter Plug-in for VMware vSphere は、VMware vSphere とのシームレスな統合を提供し、データ保護操作の効率的かつ集中的な管理を可能にします。この統合により、仮想マシンのバックアップおよびリカバリ プロセスが合理化され、VMware エコシステム内のスケジュール設定、監視、および柔軟な復元操作が容易になります。BlueXP backup and recoveryは、仮想マシン データの安全なエアギャップ バックアップをクラウド ベースのオブジェクトストレージに提供することで、3-2-1 の 1 つを実現します。直感的なインターフェースと論理的なワークフローにより、重要なデータを長期にわたってアーカイブするための安全なプラットフォームが提供されます。

追加情報

このソリューションで紹介されているテクノロジーの詳細については、次の追加情報を参照してください。

- ["SnapCenter Plug-in for VMware vSphereのドキュメント"](#)
- ["BlueXP ドキュメント"](#)

BlueXP disaster recoveryを使用して VMFS データストアのディザスタリカバリを設定する

このユースケースでは、VMware 仮想マシン ファイル システム (VMFS) データストアを使用して、オンプレミスの VMware VM にBlueXP disaster recoveryを使用してディザス

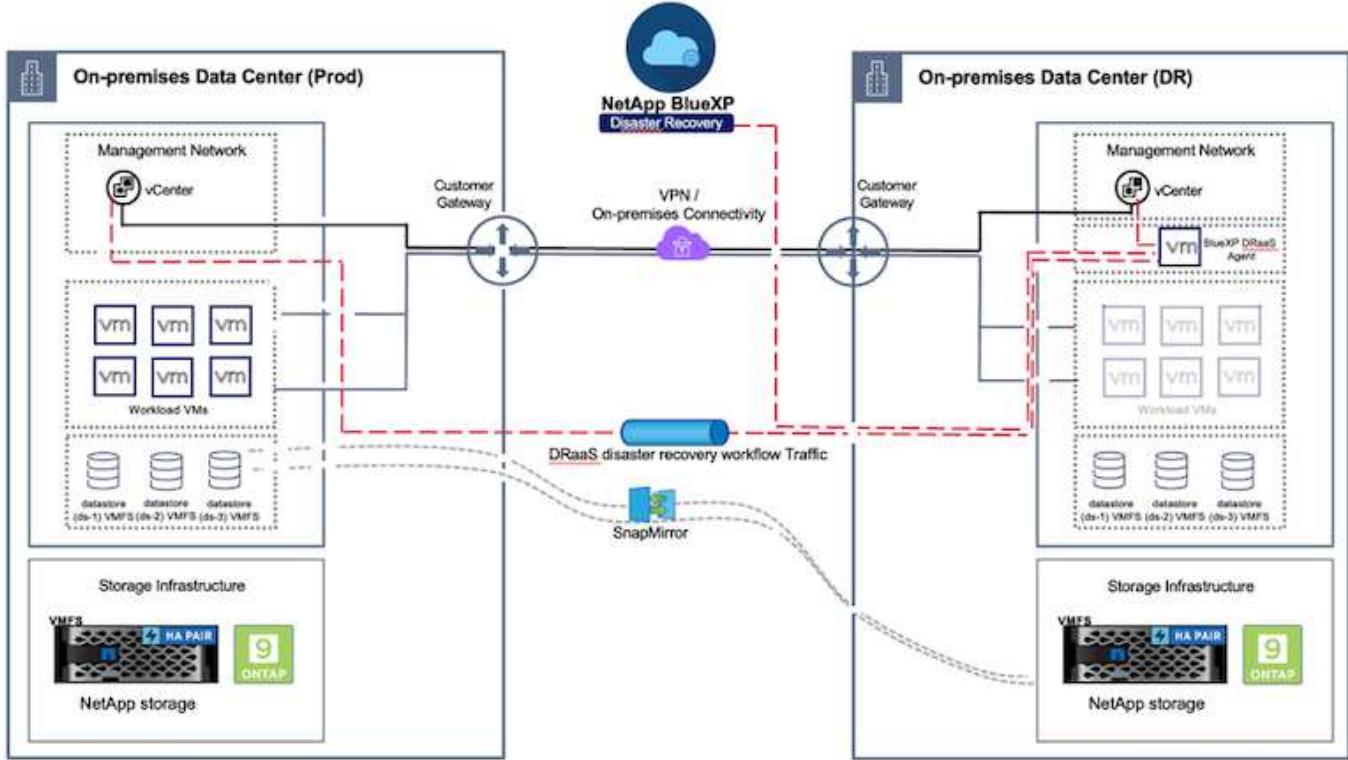
タリカバリを設定する手順について説明します。この手順には、BlueXPアカウントとコネクタの設定、ONTAPシステム間のSnapMirrorレプリケーションの確立、VMware vCenterとの統合、フェールオーバーとフェールバック操作の自動化が含まれます。

運用サイトから災害復旧サイトへのブロックレベルのレプリケーションを使用した災害復旧は、サイトの停止やランサムウェア攻撃などのデータ破損イベントからワークロードを保護する、回復力がありコスト効率に優れた方法です。NetApp SnapMirrorレプリケーションを使用すると、VMFSデータストアを使用してオンプレミスのONTAPシステムで実行されているVMwareワークロードを、VMwareが存在する指定されたリカバリデータセンター内の別のONTAPストレージシステムに複製できます。

はじめに

このドキュメントのセクションでは、オンプレミスのVMware VMの災害復旧を別の指定サイトに設定するためのBlueXP DRaaSの構成について説明します。このセットアップの一部として、BlueXPアカウント、BlueXPコネクタ、VMware vCenterからONTAPストレージへの通信を可能にするために必要なONTAPアレイがBlueXPワークスペース内に追加されます。さらに、このドキュメントでは、サイト間のレプリケーションを構成する方法と、リカバリプランを設定およびテストする方法についても詳しく説明します。最後のセクションでは、サイト全体のフェールオーバーを実行する手順と、プライマリサイトが回復されオンラインで購入されたときにフェールバックする方法について説明します。

NetApp BlueXPコンソールに統合されているBlueXP disaster recoveryサービスを使用すると、顧客はオンプレミスのVMware vCenterとONTAPストレージを検出し、リソースグループを作成し、ディザスタリカバリプランを作成してリソースグループに関連付け、フェイルオーバーとフェイルバックをテストまたは実行できます。SnapMirrorは、ストレージレベルのブロックレプリケーションを提供し、2つのサイトを増分変更で最新の状態に保ち、RPOを最大5分に抑えます。また、本番環境や複製されたデータストアに影響を与えることなく、定期的な訓練としてDR手順をシミュレートすることもできます。BlueXP disaster recoveryは、ONTAPのFlexCloneテクノロジーを活用して、DRサイトで最後に複製されたスナップショットからVMFSデータストアのスペース効率の高いコピーを作成します。DRテストが完了すると、顧客はテスト環境を削除するだけで済み、実際の複製された本番リソースには影響しません。実際のフェイルオーバー(計画的または計画外)が必要な場合、数回クリックするだけで、BlueXP disaster recoveryサービスが、指定された災害復旧サイトで保護された仮想マシンを自動的に起動するために必要なすべての手順を調整します。このサービスは、必要に応じて、プライマリサイトへのSnapMirror関係を逆転させ、フェイルバック操作のためにセカンダリサイトからプライマリサイトへの変更を複製します。これらすべては、他によく知られている代替手段に比べて、ほんのわずかなコストで実現できます。



開始

BlueXP disaster recoveryを開始するには、BlueXPコンソールを使用してサービスにアクセスします。

1. BlueXPにログインします。
2. BlueXPの左側のナビゲーションから、[保護] > [災害復旧] を選択します。
3. BlueXP disaster recoveryダッシュボードが表示されます。

Category	Value
Protected VMs	21
Unprotected VMs	117
Replication plans	1 Ready, 2 Failed
Activity	Recent backup jobs (e.g., DemoRP004, RPVMFS03, RPVMFS01)

災害復旧計画を構成する前に、次の前提条件が満たされていることを確認してください。

- BlueXPコネクタはNetApp BlueXPに設定されます。コネクタはAWS VPCにデプロイする必要があります。
- BlueXPコネクタインスタンスは、ソースおよびターゲットのvCenterおよびストレージシステムに接続できます。
- VMware用のVMFSデータストアをホストするオンプレミスのNetAppストレージシステムがBlueXPに追加されます。
- DNS名を使用する場合は、DNS解決を実施する必要があります。それ以外の場合は、vCenterのIPアドレスを使用します。
- 指定されたVMFSベースのデータストアボリュームに対してSnapMirrorレプリケーションが構成されます。

ソースサイトと宛先サイト間の接続が確立されたら、構成手順に進みます。これには約3~5分かかります。



NetApp、実際の障害や自然災害の発生時にBlueXPコネクタがネットワークを介してソースリソースおよび宛先リソースと通信できるように、災害復旧サイトまたは第3のサイトにBlueXPコネクタを導入することを推奨しています。



このドキュメントの執筆時点では、オンプレミスからオンプレミスへのVMFSデータストアのサポートはテクノロジー プレビュー段階です。この機能は、FCおよびiSCSIプロトコルベースのVMFSデータストアの両方でサポートされます。

BlueXP disaster recovery構成

災害復旧の準備の最初のステップは、オンプレミスのvCenterとストレージリソースを検出し、BlueXP disaster recoveryに追加することです。



ONTAPストレージシステムがキャンバス内の作業環境に追加されていることを確認します。BlueXPコンソールを開き、左側のナビゲーションから 保護 > 災害復旧 を選択します。vCenterサーバーの検出を選択するか、トップメニューを使用して サイト > 追加 > vCenter の追加 を選択します。

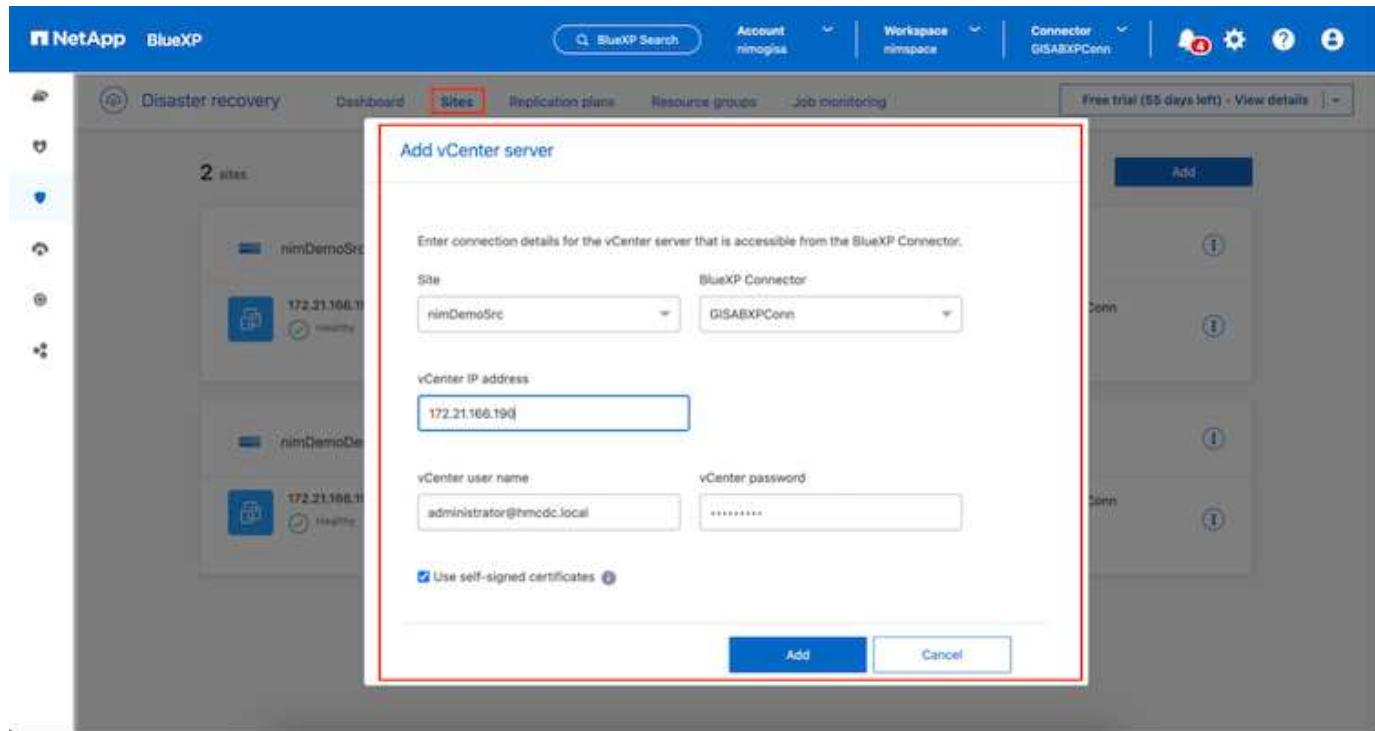
The screenshot shows the NetApp BlueXP interface with the 'Sites' tab selected. A modal dialog box is open, titled 'Add site'. It contains fields for 'Site' (set to 'nimDemoSrc') and 'Location' (set to 'On-prem'). The 'Add' and 'Cancel' buttons are at the bottom. The entire dialog box is highlighted with a red border.

次のプラットフォームを追加します。

- ・ソース。オンプレミスのvCenter。

The screenshot shows the NetApp BlueXP interface with the 'Sites' tab selected. A modal dialog box is open, titled 'Add vCenter server'. It contains fields for 'Site' (set to 'nimDemoSrc'), 'BlueXP Connector' (set to 'GISABXPConn'), 'vCenter IP address' (set to '172.21.166.155'), 'vCenter user name' (set to 'administrator@hmcdc.local'), and 'vCenter password' (set to '*****'). A checkbox for 'Use self-signed certificates' is checked. The 'Add' and 'Cancel' buttons are at the bottom. The 'vCenter IP address', 'vCenter user name', and 'vCenter password' fields are highlighted with a red border.

- 行き先。VMC SDDC vCenter。



vCenter が追加されると、自動検出がトリガーされます。

ソースサイトと宛先サイト間のストレージレプリケーションの構成

SnapMirror はONTAPスナップショットを利用して、ある場所から別の場所へのデータの転送を管理します。最初に、ソースボリュームのスナップショットに基づく完全なコピーが宛先にコピーされ、ベースライン同期が実行されます。ソースでデータの変更が発生すると、新しいスナップショットが作成され、ベースラインスナップショットと比較されます。変更されたと判明したブロックは宛先に複製され、新しいスナップショットが現在のベースライン、つまり最新の共通スナップショットになります。これにより、プロセスを繰り返し、増分更新を宛先に送信できるようになります。

SnapMirror関係が確立されると、宛先ボリュームはオンライン読み取り専用状態になり、引き続きアクセス可能になります。SnapMirror は、ファイルやその他の論理レベルではなく、ストレージの物理ブロックで動作します。つまり、複製先ボリュームは、スナップショット、ボリューム設定などを含め、複製元ボリュームと同一のレプリカになります。データ圧縮やデータ重複排除などのONTAPスペース効率機能が複製元ボリュームで使用されている場合、複製されたボリュームではこれらの最適化が保持されます。

SnapMirror関係を解除すると、宛先ボリュームが書き込み可能になり、通常はSnapMirrorを使用して DR 環境にデータを同期しているときにフェイルオーバーを実行するために使用されます。SnapMirror は非常に洗練されており、フェイルオーバー サイトで変更されたデータをプライマリシステムに効率的に再同期し、プライマリシステムが後でオンラインに戻ったときに、元のSnapMirror関係を再確立することができます。

VMware Disaster Recoveryの設定方法

SnapMirrorレプリケーションを作成するプロセスは、どのアプリケーションでも同じです。このプロセスは手動でも自動でも実行できます。最も簡単な方法は、BlueXPを利用して、環境内のソースONTAPシステムを宛先にドラッグ アンド ドロップするだけでSnapMirrorレプリケーションを構成し、残りのプロセスをガイドするウィザードを起動することです。

The screenshot shows the NetApp BlueXP interface. On the left, there's a sidebar with icons for Canvas, My working environments (which is selected), and My estate. The main area displays a diagram of a cloud-to-cloud replication setup. A central cloud icon labeled "Replication" is connected to two other clouds: "NTAP915_Src" (On-Premises ONTAP) and "Amazon S3". The "NTAP915_Src" cloud has a tooltip with options: "Enable this service" (Volume caching, Replication, Copy & sync), "NTAP915_Tgt" (On-Premises ONTAP, 9.39TB Capacity), and "Amazon S3" (0 buckets). On the right, a detailed view of the "NTAP915_Src" cluster shows its services: Backup and recovery (On), Copy & sync (Off), Tiering (On), Classification (Off), Edge caching (Unselected), and Replication (On, 1 destination target). A blue button at the bottom right says "Enter Working Environment".

BlueXP DRaaS では、次の 2 つの条件が満たされている場合、同じことを自動化することもできます。

- ・ソース クラスターと宛先クラスターにはピア関係があります。
- ・ソース SVM と宛先 SVM にはピア関係があります。

The screenshot shows the "Add replication plan" wizard, step 5: "Resource mapping". It lists "Source cluster" (vVCSA8-Cluster01) and "Target cluster" (wVDD4-Cluster01). Under "Virtual networks", "Virtual machines", and "Datastores", the "Mapped" status is checked. In the "Datastores" section, a red box highlights the "RPO for all datastores in minutes" field (set to 30) and the "Retention count for all datastores" field (set to 30). Below these fields, it shows "Required Source datastore" (Src_NFS_DG01 (svm_NFS-Src_NFS_Vol01)) and "Target datastore" (Src_NFS_DG01 (svm_nim_nfsv3/Src_NFS_DG01_ce)). Transfer schedule(RPO) is also listed. At the bottom, there are "Previous" and "Next" buttons.



CLI 経由でボリュームにSnapMirror関係がすでに設定されている場合、BlueXP DRaaS はその関係を取得し、残りのワークフロー操作を続行します。



上記の方法以外にも、SnapMirrorレプリケーションはONTAP CLI または System Manager 経由で作成することもできます。SnapMirrorを使用してデータを同期するために使用されるアプローチに関係なく、BlueXP DRaaS は、シームレスで効率的な災害復旧操作のワークフローを調整します。

BlueXP disaster recoveryは何を実現できるのでしょうか？

ソースサイトと宛先サイトが追加されると、BlueXP disaster recoveryは自動的に詳細な検出を実行し、VMと関連メタデータを表示します。BlueXP disaster recoveryでは、VMで使用されるネットワークとポートグループも自動的に検出し、それらを入力します。

The screenshot shows the BlueXP Disaster Recovery interface. At the top, there are navigation tabs: Disaster recovery, Dashboard, **Sites**, Replication plans, Resource groups, and Job monitoring. A red box highlights the 'Sites' tab. Below the tabs, it says '2 sites'. There are two entries: 'nimDemoSrc' and 'nimDemoDest'. Each entry has a summary card with the following details:

Site	IP Address	Status	VMs	Datastores	Resource groups	Connector
nimDemoSrc	172.21.166.155	Healthy	72	13	1	GISABXPConn
nimDemoDest	172.21.166.190	Healthy	61	3	0	GISABXPConn

サイトを追加した後、VMをリソースグループにグループ化できます。BlueXP disaster recoveryリソースグループを使用すると、依存するVMのセットを、復旧時に実行できるブート順序とブート遅延を含む論理グループにグループ化できます。リソースグループの作成を開始するには、[リソースグループ]に移動し、[新しいリソースグループの作成]をクリックします。

2 resource groups

Resource group	Source site	Source vCenter
DemoRG01	nimDemoSrc	172.21.166.155
DemoRGVMFS03	nimDemoSrc	172.21.166.155

Added the resource group.



レプリケーション プランの作成時にリソース グループを作成することもできます。

VM のブート順序は、リソース グループの作成中に、簡単なドラッグ アンド ドロップ メカニズムを使用して定義または変更できます。

Add resource group

Name: DemoRGVMFS03 vCenter: 172.21.166.155

Select virtual machines:

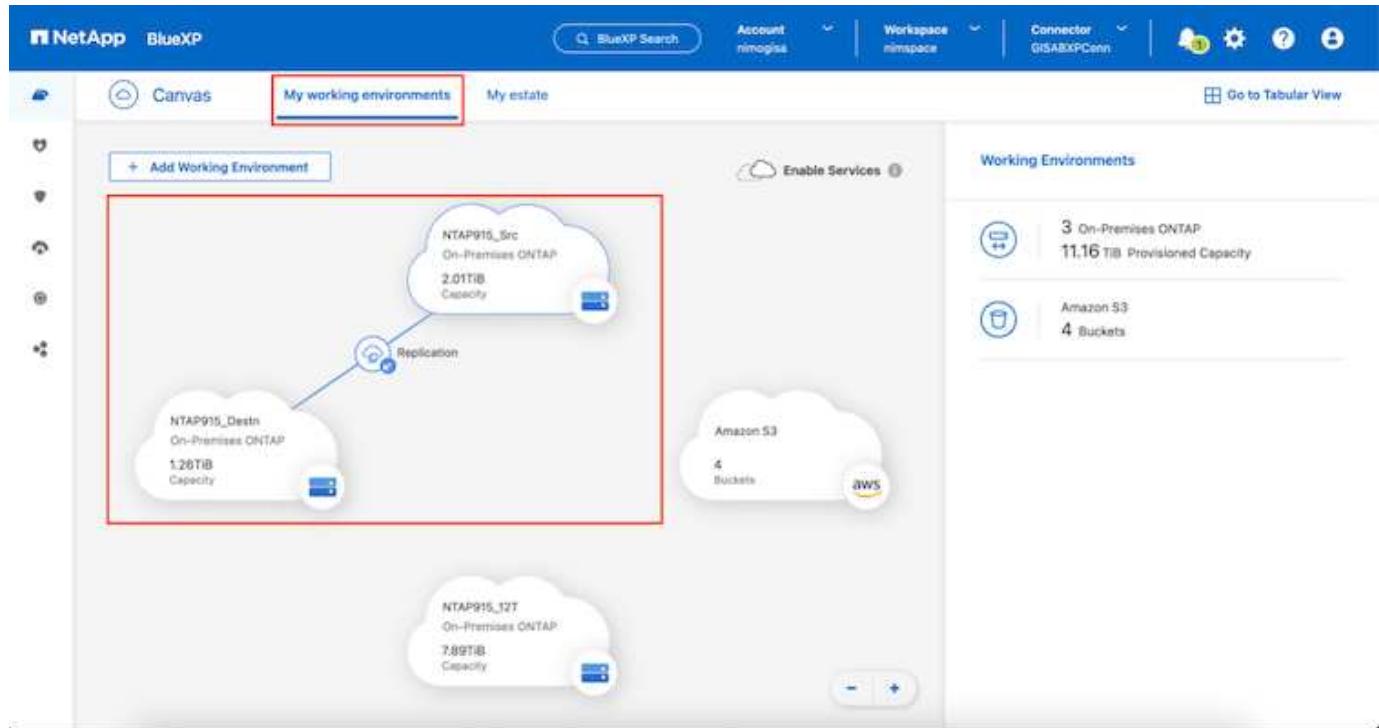
Selected VMs (5)

- iSCSI_DemoVM01
- iSCSI_DemoVM03
- iSCSI_DemoVM02
- iSCSI_DemoVM04
- iSCSI_DemoVM05

Use drag and drop here to modify the boot order

Add Cancel

リソース グループを作成したら、次のステップは、災害発生時に仮想マシンとアプリケーションを復旧するための実行ブループリントまたは計画を作成することです。前提条件で述べたように、SnapMirrorレプリケーションは事前に構成することも、レプリケーション プランの作成時に指定されたRPOと保持数を使用してDRaaSで構成することもできます。

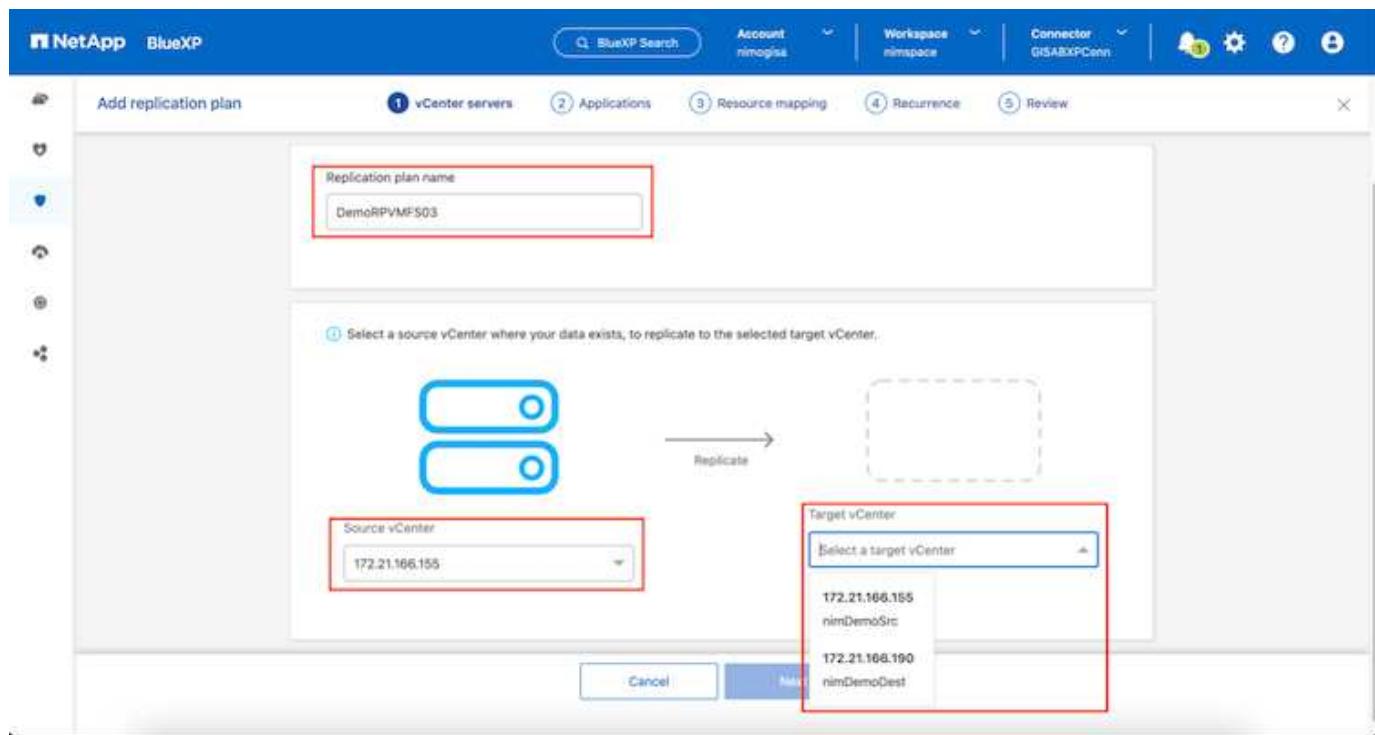


The screenshot shows the 'Replication' tab selected in the top navigation bar. The dashboard displays metrics: 6 Volume Relationships, 495.27 GiB Replicated Capacity, 0 Currently Transferring, 6 Healthy, and 0 Failed. Below this is a table titled 'Volume Relationships (6)'.

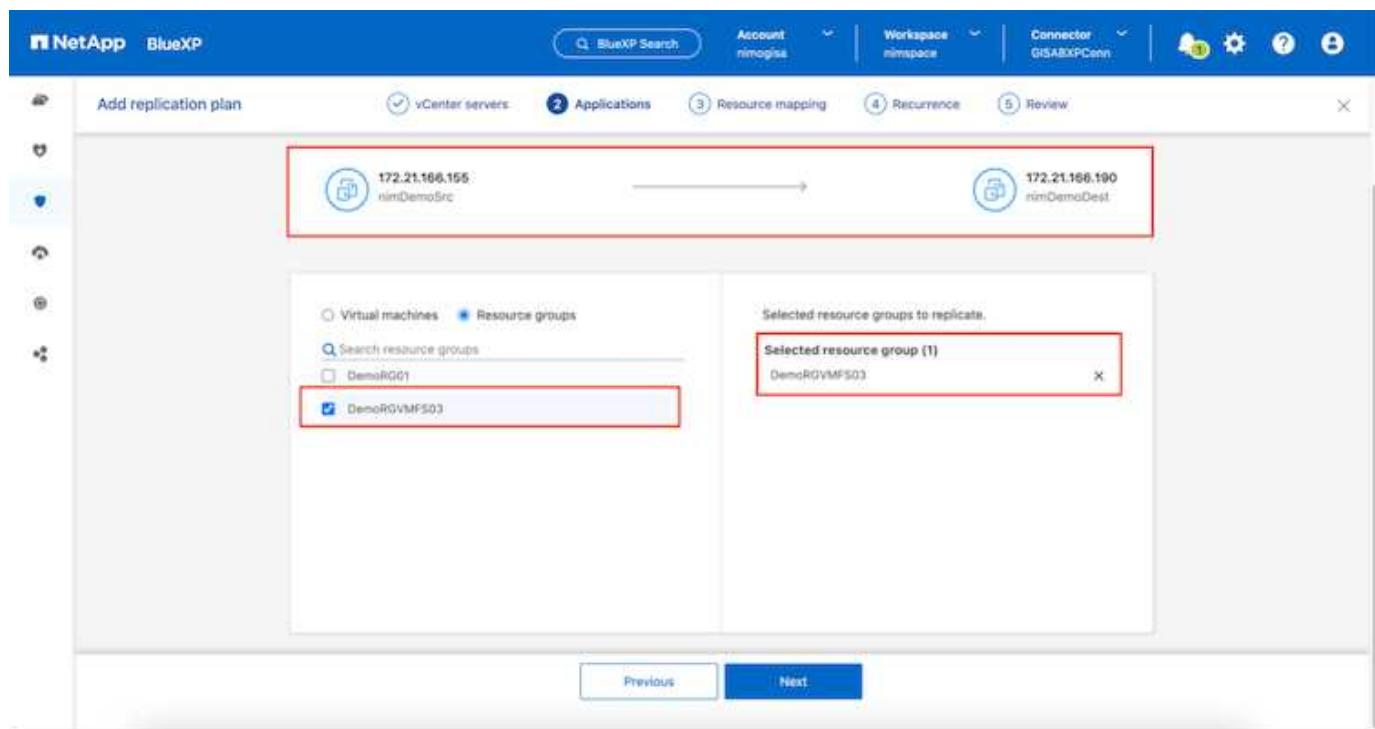
Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful
✓	DRaaS5_src NTAP915_Src	DRaaS5_src_copy NTAP915_Destn	5 seconds	idle	snapmirrored	Jul 15, 2024, 8:05:05 28.41 MiB
✓	Src_NFS_DS03 NTAP915_Src	Src_NFS_DS03_CP NTAP915_Destn	13 seconds	idle	snapmirrored	Jul 15, 2024, 8:07:13 183.41 MiB
✓	Src_NFS_DS04 NTAP915_Src	Src_NFS_DS04_CP NTAP915_Destn	6 seconds	idle	snapmirrored	Jul 15, 2024, 8:05:06 183.38 MiB
✓	Src_NFS_Vol01 NTAP915_Src	Src_NFS_DS01_cp NTAP915_Destn	14 seconds	idle	snapmirrored	Jul 15, 2024, 8:43:22 546.23 MiB
✓	Src_iSCSI_DS01 NTAP915_Src	Src_iSCSI_DS01_cp NTAP915_Destn	20 seconds	idle	snapmirrored	Jul 12, 2024, 4:24:34 22.35 MiB
✓	Src_iSCSI_DS03 NTAP915_Src	Src_iSCSI_DS03_CP NTAP915_Destn	6 seconds	idle	snapmirrored	Jul 15, 2024, 8:05:06 254.89 MiB

ドロップダウンからソースと宛先の vCenter プラットフォームを選択してレプリケーション プランを構成し、プランに含めるリソース グループ、アプリケーションの復元方法と電源オン方法のグループ化、およびクラスタとネットワークのマッピングを選択します。リカバリ プランを定義するには、[レプリケーション プラン] タブに移動し、[プランの追加] をクリックします。

まず、ソース vCenter を選択し、次に宛先 vCenter を選択します。



次のステップは、既存のリソース グループを選択することです。リソース グループが作成されていない場合、ウィザードは、回復目標に基づいて必要な仮想マシンをグループ化します（基本的には機能リソース グループを作成します）。これは、アプリケーション仮想マシンを復元する操作シーケンスを定義するのにも役立ちます。



リソース グループでは、ドラッグ アンド ドロップ機能を使用してブート順序を設定できます。これを使用すると、リカバリプロセス中に VM の電源がオンになる順序を簡単に変更できます。



リソース グループ内の各仮想マシンは、順序に基づいて順番に起動されます。2つのリソース グループが並行して開始されます。

以下のスクリーンショットは、リソース グループが事前に作成されていない場合に、組織の要件に基づいて仮想マシンまたは特定のデータストアをフィルターするオプションを示しています。

Add replication plan

1 eCenter servers 2 Applications 3 Resource mapping 4 Recurrence 5 Review

Applications

Select the applications on the source vCenter that you want to replicate.

172.21.188.155
nimDemoSrc

172.21.188.190
nimDemoDest

Replicate

Virtual machines Resource groups

Datastore: All datastores Search All Datastores

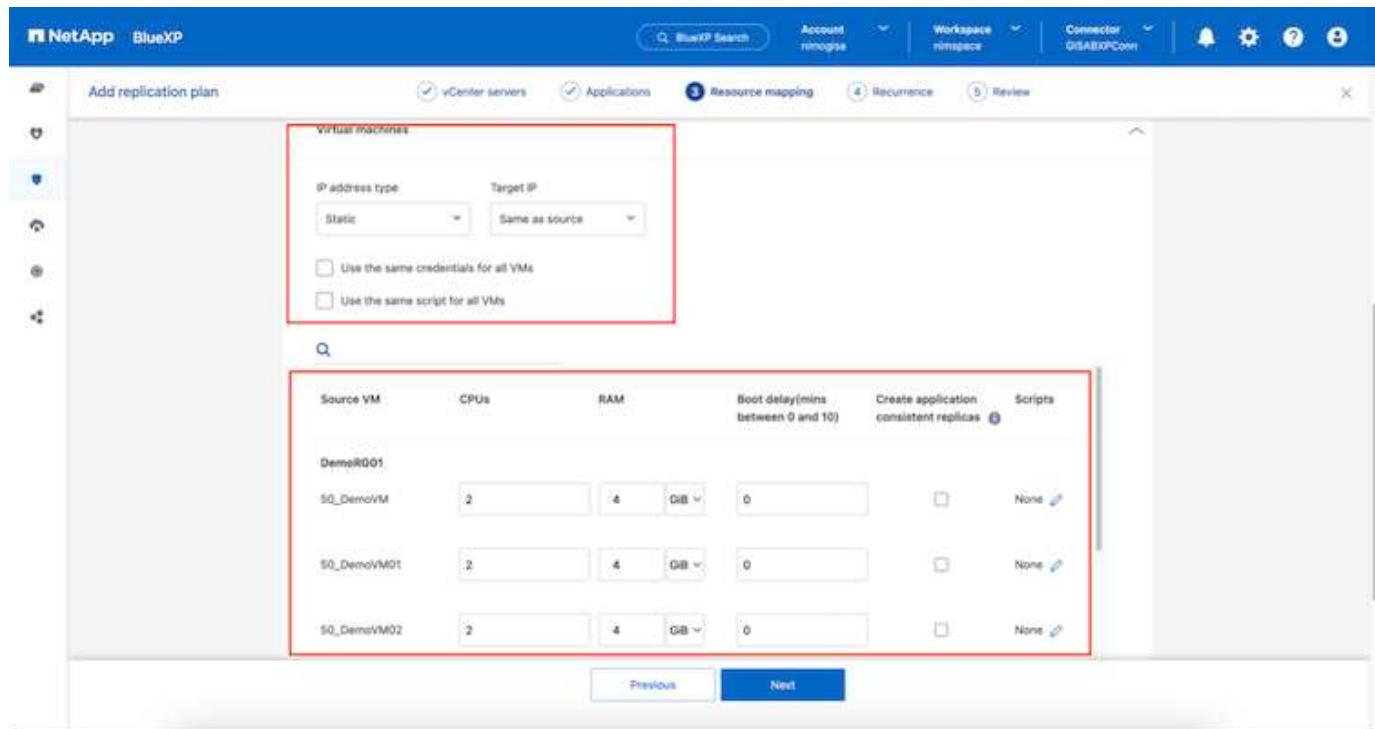
UbuntuVM01
Win2K19VM01
SCVSDP1VM01
vOTY34Z2Node
SO_DemoVM01

Selected VMs (0)

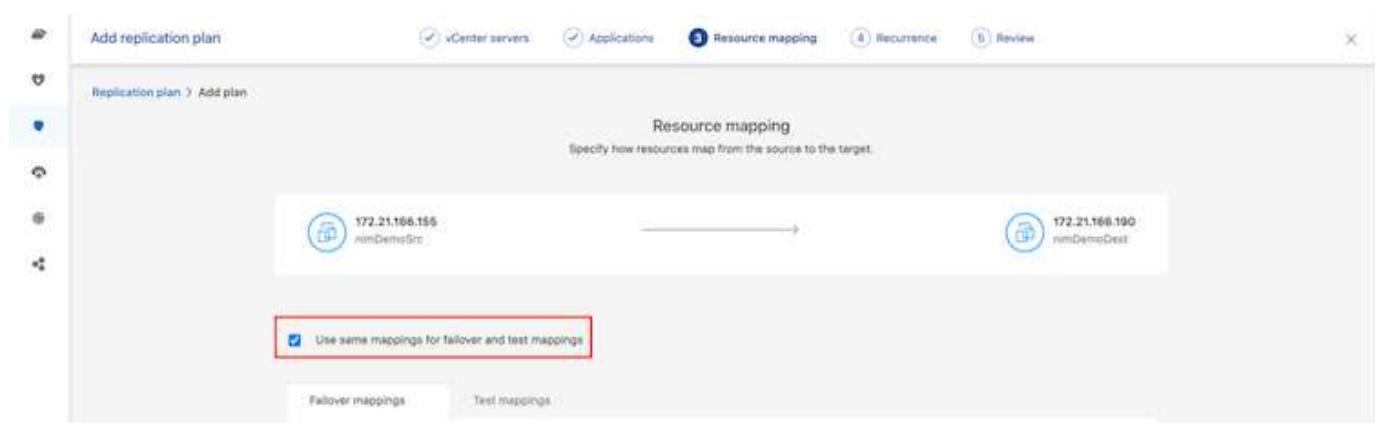
ResourceGroup1
Select VMs to replicate.

Previous Next

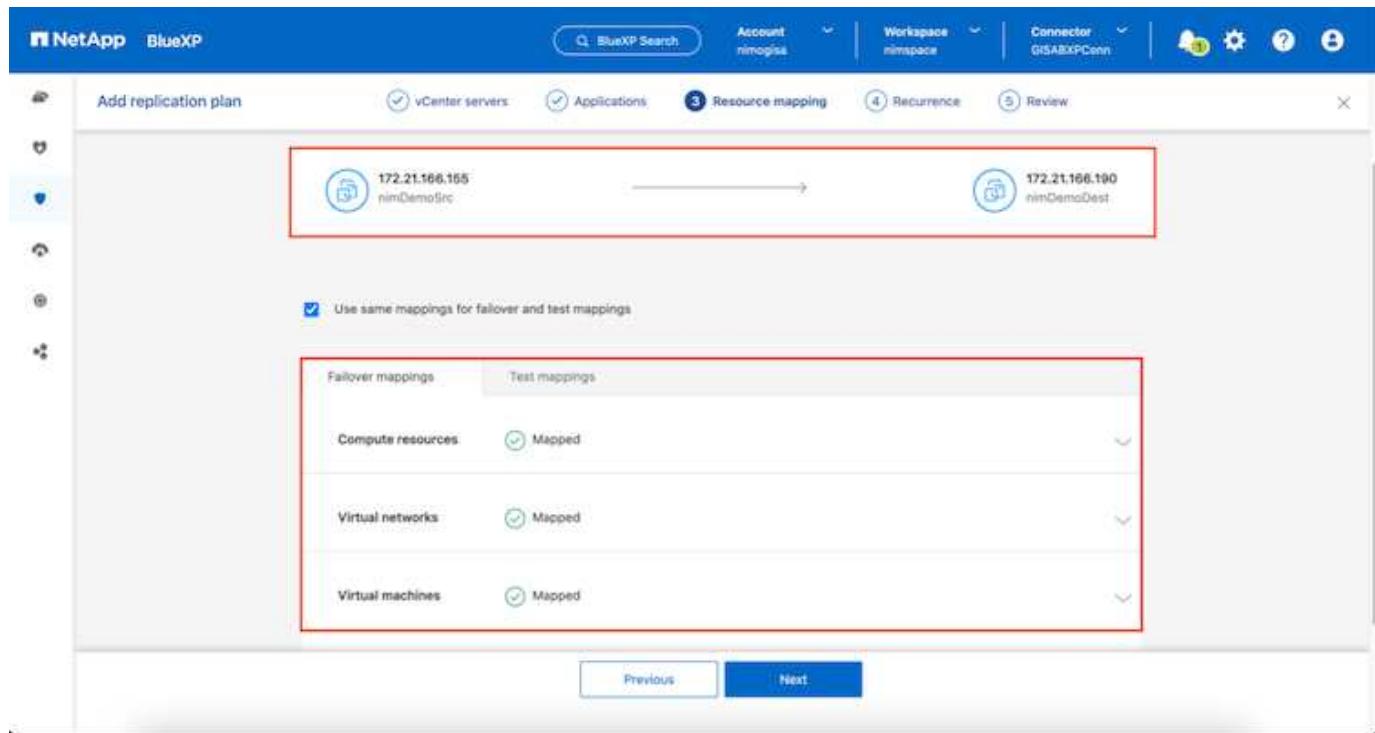
リソース グループを選択したら、フェールオーバー マッピングを作成します。このステップでは、ソース環境のリソースを宛先にどのようにマップするかを指定します。これには、コンピューティング リソース、仮想ネットワークが含まれます。IP カスタマイズ、事前スクリプトと事後スクリプト、ブート遅延、アプリケーションの一貫性など。詳細については、["レプリケーションプランを作成する"](#)。



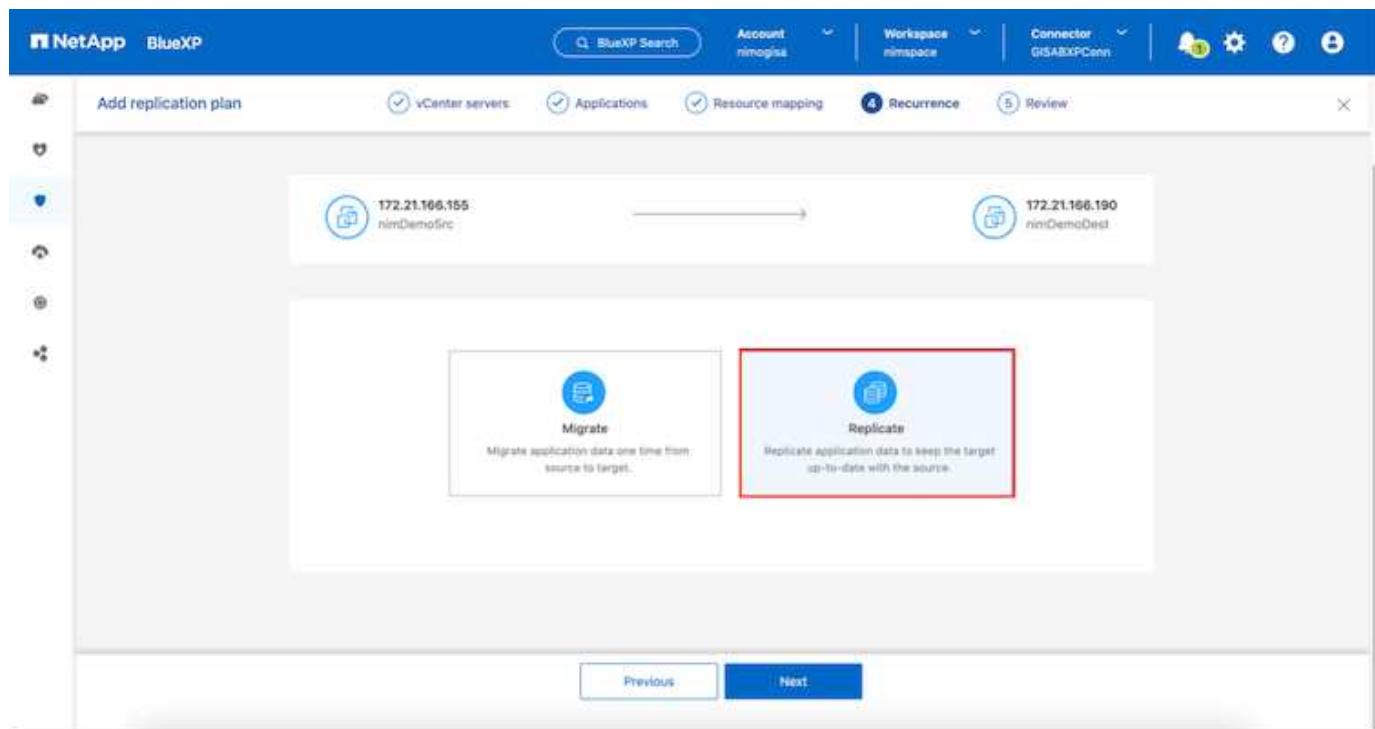
デフォルトでは、テスト操作とフェイルオーバー操作の両方に同じマッピング パラメータが使用されます。テスト環境に異なるマッピングを適用するには、以下に示すようにチェックボックスをオフにした後、テスト マッピング オプションを選択します。



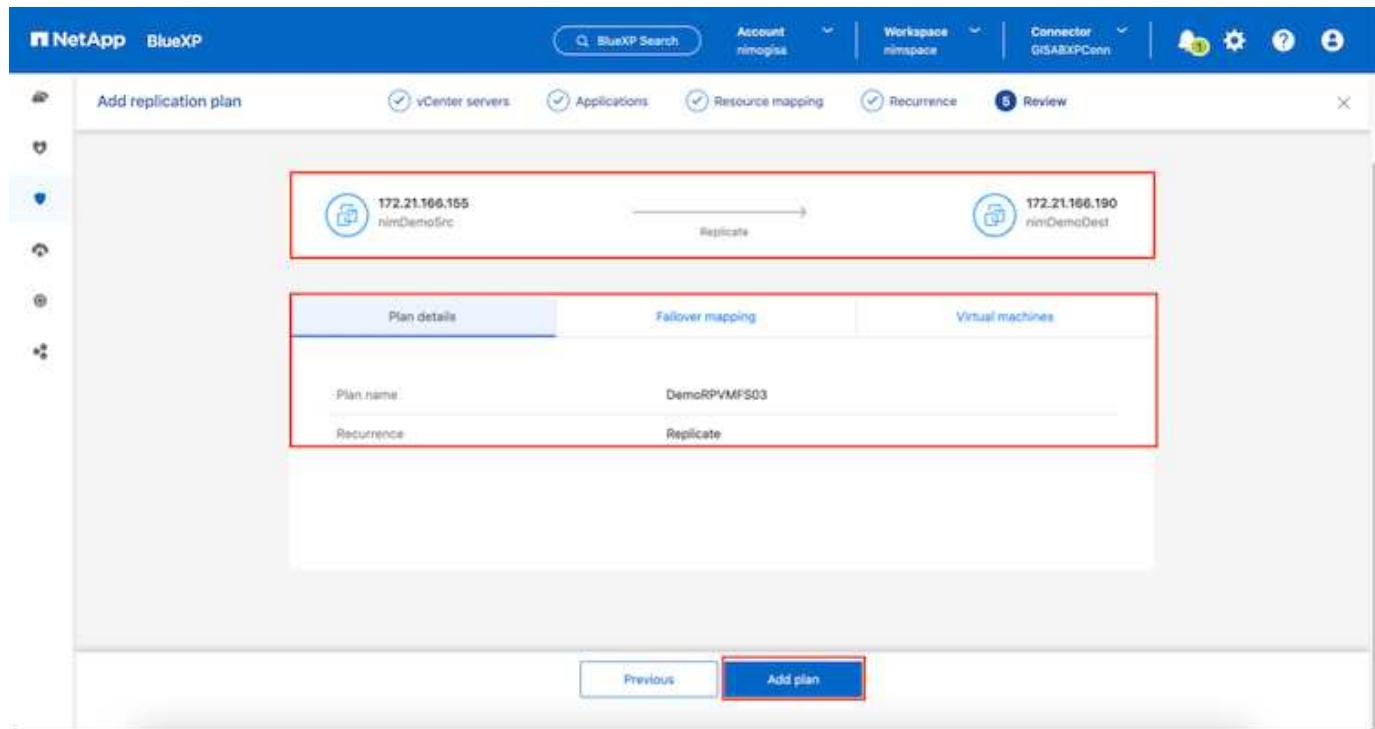
リソース マッピングが完了したら、[次へ] をクリックします。



繰り返しタイプを選択します。簡単に言えば、「移行」（フェイルオーバーを使用した1回限りの移行）または定期的な連続レプリケーションオプションを選択します。このチュートリアルでは、「複製」オプションが選択されています。



完了したら、作成されたマッピングを確認し、「プランの追加」をクリックします。



The screenshot shows the 'Replication plans' page in the NetApp BlueXP interface. The 'Replication plans' tab is selected. There are two plans listed: 'DemoRPVMS03' and 'RPNFS001'. Both plans are marked as 'Healthy' and 'Ready'. The table columns include Plan, Compliance check, Plan status, Protected site, Resource group, Recurrence, Failover site, and an ellipsis column. A search bar and an 'Add' button are located at the top right of the table area.

レプリケーション プランが作成されると、フェールオーバー オプション、テスト フェールオーバー オプション、または移行オプションを選択して、要件に応じてフェールオーバーを実行できます。BlueXP disaster recoveryでは、レプリケーション プロセスが 30 分ごとに計画に従って実行されることが保証されます。フェイルオーバーおよびテストフェイルオーバーのオプションでは、最新のSnapMirror Snapshot コピーを使用することも、ポイントインタイム Snapshot コピーから特定の Snapshot コピーを選択することもできます (SnapMirrorの保持ポリシーに従って)。ランサムウェアなどの破損イベントが発生し、最新のレプリカがすでに侵害されたり暗号化されたりしている場合、ポイントインタイム オプションは非常に役立ちます。BlueXP disaster recoveryでは、利用可能なすべての復旧ポイントが表示されます。

The screenshot shows the Disaster recovery section of the NetApp BlueXP interface. A modal window titled "Failover: DemoRPVMS03" is open. Inside, there are two warning messages: "Warning: Falling over will disrupt client access to the data in nimDemoSrc during the transition to nimDemoDest DR Site." and "Warning: All VMs are powered on." Below these are options for "Snapshot copy for volume recovery" with radio buttons for "Take snapshot now" and "Select". A third warning message states: "Warning: The corresponding volume will be restored with the selected snapshot copy. All the changes made after this snapshot copy was created will be lost." At the bottom of the modal, there is a "Snoozed" button and a "Force failover" checkbox.

レプリケーション プランで指定された構成でフェイルオーバーまたはテスト フェイルオーバーをトリガーするには、[フェイルオーバー] または [フェイルオーバーのテスト] をクリックします。

The screenshot shows the Disaster recovery section with the "Replication plans" tab selected. Two plans are listed: "DemoRPVMS03" and "RPNFS001". The "DemoRPVMS03" plan is highlighted with a red box. A context menu is open for this plan, listing the following options: "View plan details", "Run compliance check", "Test failover" (highlighted with a red box), "Clean up follower test", "Fail over" (highlighted with a red box), "Fail back", "Edit schedules", "Take snapshot now", "Disable", "Enable", and "Delete".

フェイルオーバーまたはテストフェイルオーバー操作中に何が起こりますか？

テスト フェイルオーバー操作中に、BlueXP disaster recoveryは、最新の Snapshot コピーまたは宛先ボリュームの選択されたスナップショットを使用して、宛先ONTAPストレージ システムにFlexCloneボリュームを作成します。

（i） テスト フェイルオーバー操作では、宛先のONTAPストレージ システムにクローン ボリュームが作成されます。

（i） テスト リカバリ操作を実行しても、SnapMirrorレプリケーションには影響しません。

The screenshot shows the NetApp BlueXP interface with the 'Disaster recovery' tab selected. A modal window titled 'Test failover: DemoRPVMFS03' displays a list of tasks:

- ✓ DR Test Failover Update Mirror.
- ✓ SnapMirror relationship for volume :svm_iSCSI:Src_iSCSI_D503
- ✓ Destination volume 'Src_iSCSI_D503_CP' size is less than source volume 'Src_iSCSI_D503' size
- ✓ SnapMirror relationship is healthy for volume :svm_iSCSI:Src_iSCSI_D503
- ✓ Destination storage environment found for volume :svm_iSCSI:Src_iSCSI_D503
- ✓ Take snapshot now option is not selected, primary backup & snapmirror update not performed.

A blue button at the bottom right of the modal says 'Run in background'.

プロセス中、BlueXP disaster recoveryは元のターゲット ボリュームをマップしません。代わりに、選択したスナップショットから新しいFlexCloneボリュームが作成され、FlexCloneボリュームをサポートする一時データストアがESXiホストにマップされます。

The screenshot shows the vSphere Client interface with the vCenter 'wklld04-vc01.hmc当地域' selected. The 'Summary' tab is active. The 'vCenter Details' section shows:

- Version: 8.0.2
- Build: 22385739
- Last Updated: May 20, 2024, 3:21 AM
- Last File-Based Backup: Not scheduled
- Clusters: 1
- Hosts: 2
- Virtual Machines: 6

The 'Capacity and Usage' section shows:

Category	Used	Total
CPU	72.12 GHz used	73.44 GHz capacity
Memory	485.84 GB used	485.84 GB free
Storage	51.99 GB used	3.91 TB free
Network	4 TB used	4 TB capacity

At the bottom, the 'Recent Tasks' table lists:

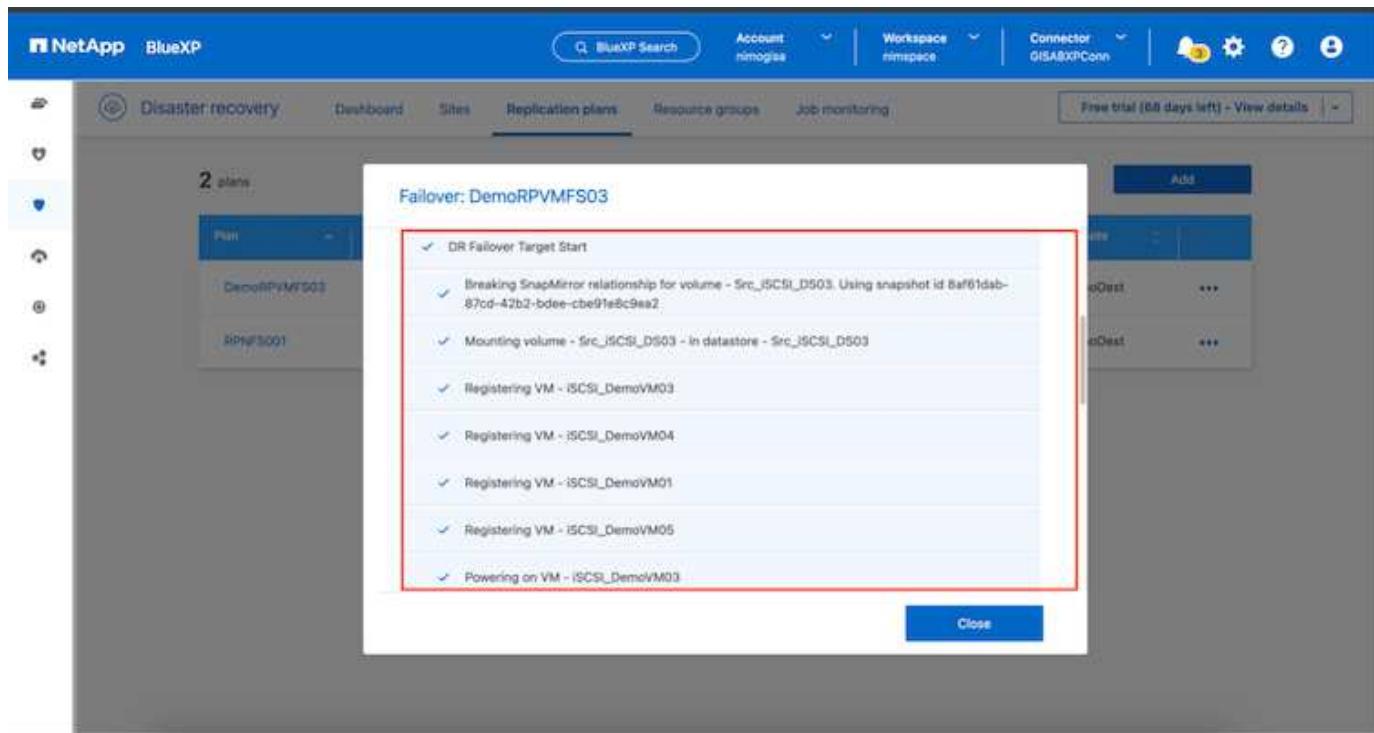
Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time
Rescan VMFS	wklld04-esx01.hmc当地域	Completed		HMCDC.LOCAL/Administrator	2 ms	07/30/2024, 3:22:47 AM	07/30/2024, 3:22:47 AM
Rescan all HBAs	wklld04-esx01.hmc当地域	Completed		HMCDC.LOCAL/Administrator	3 ms	07/30/2024, 3:22:47 AM	07/30/2024, 3:22:47 AM

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time
Register virtual machine	wkld04-DC01	20%	Registering Virtual Machine on destination host	System	20 ms	07/30/2024, 3:23:43 AM	
Register virtual machine	wkld04-DC01	20%	Registering Virtual Machine on destination host	System	17 ms	07/30/2024, 3:23:43 AM	

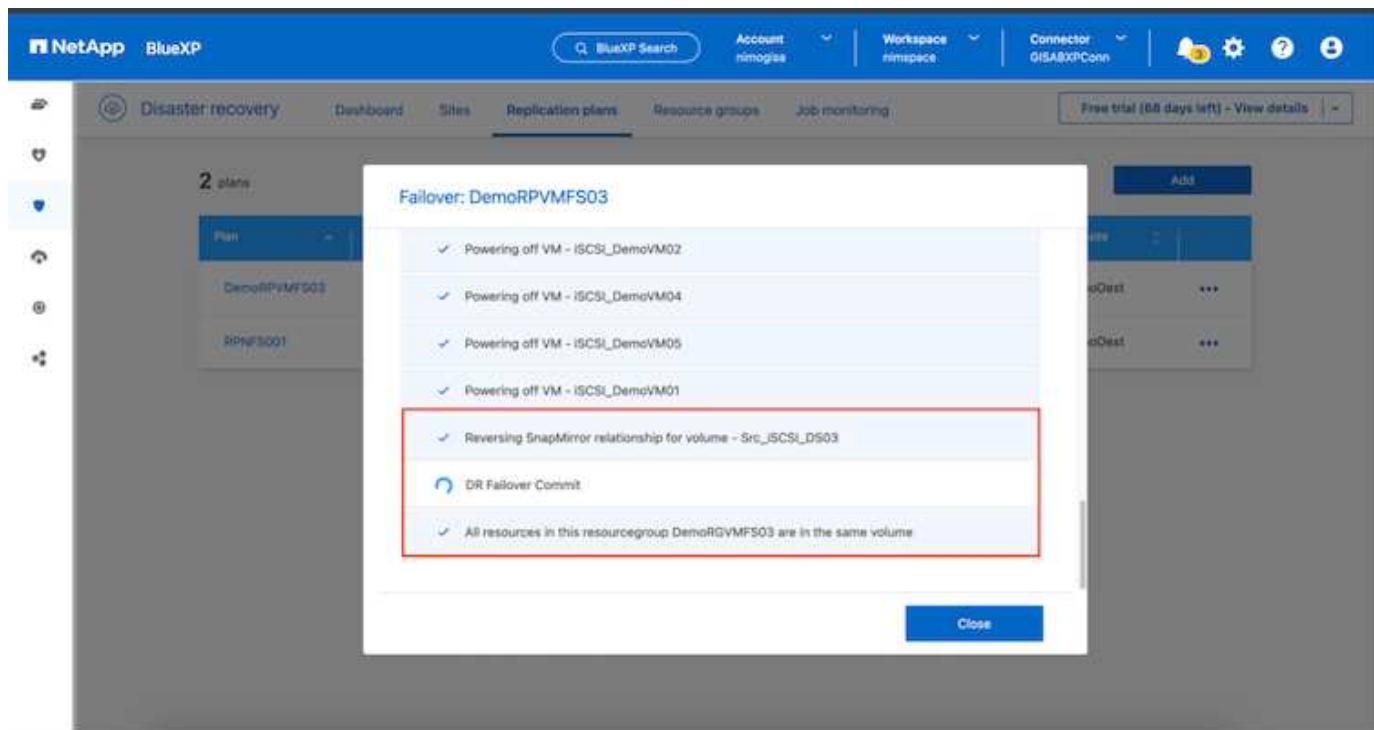
テスト フェイルオーバー操作が完了すると、「クリーンアップ フェイルオーバー テスト」を使用してクリーンアップ操作をトリガーできます。この操作中、BlueXP disaster recoveryは、操作で使用されたFlexClone ボリュームを破棄します。

実際の災害が発生した場合、BlueXP disaster recoveryは次の手順を実行します。

1. サイト間のSnapMirror関係を解除します。
2. 再署名後に VMFS データストア ボリュームをマウントし、すぐに使用できるようにします。
3. VMを登録する
4. VMの電源をオンにする



プライマリ サイトが起動すると、BlueXP disaster recoveryによってSnapMirrorの逆再同期が有効になり、フェイルバックが有効になります。これもボタンをクリックするだけで実行できます。



移行オプションを選択した場合は、計画されたフェイルオーバー イベントと見なされます。この場合、ソース サイトの仮想マシンをシャットダウンする追加の手順がトリガーされます。残りの手順はフェイルオーバー イベントと同じままです。

BlueXPまたはONTAP CLI から、適切なデータストア ボリュームのレプリケーションのヘルス ステータスを監視し、ジョブ監視を介してフェイルオーバーまたはテスト フェイルオーバーのステータスを追跡できます。

The screenshot shows the NetApp BlueXP Disaster recovery interface. At the top, there are navigation links for Disaster recovery, Dashboard, Sites, Replication plans, Resource groups, and Job monitoring. The Job monitoring section is currently selected. It displays a summary of job status: 0 Jobs (Success), 0 In progress, 0 Queued, 0 Warning, and 0 Failed. Below this, a table lists 11102 jobs, all of which are marked as Success. The table columns include ID, Status, Workload, Name, Start time, End time, and three dots for more options.

ID	Status	Workload	Name	Start time	End time	...
2983d7f3-7eb0-475d	Success	Discovery	Discovery of resources in host 172.21.166...	07/30/2024, 11:52:...	07/30/2024, 11:52:...	...
f7ea7c0c-90d8-49b2	Success	DRFallback	Fallback of resources using the replication...	07/30/2024, 11:49:...	07/30/2024, 11:52:...	...
471f5cf2-1e97-48ca	Success	Discovery	Discovery of resources in host 172.21.166...	07/30/2024, 11:43:...	07/30/2024, 11:44:...	...

これにより、調整およびカスタマイズされた災害復旧計画を処理するための強力なソリューションが提供されます。フェイルオーバーは、計画されたフェイルオーバーとして実行することも、災害が発生して DR サイトをアクティブ化する決定が下されたときにボタンをクリックするだけでフェイルオーバーを実行することもできます。

このプロセスについて詳しく知りたい場合は、詳細なウォークスルービデオをご覧いただくか、["ソリューションシミュレータ"](#)。

BlueXP disaster recoveryを使用して NFS データストアの災害復旧を設定する

このユースケースでは、NFS データストアを使用するオンプレミスの VMware VM に対してBlueXP disaster recoveryを使用してディザスター リカバリを設定する手順について説明します。この手順には、BlueXPアカウントとコネクタの設定、VMware vCenter とONTAPストレージ間の通信を可能にするためのONTAPアレイの追加、サイト間のレプリケーションの構成、リカバリ プランの作成とテストが含まれます。

運用サイトから災害復旧サイトへのブロックレベルのレプリケーションを通じて災害復旧を実装することは、サイトの停止やランサムウェア攻撃などのデータ破損イベントからワークロードを保護するための、回復力がありコスト効率に優れた方法です。NetApp SnapMirrorレプリケーションを使用すると、NFS データストアを備えたオンプレミスのONTAPシステムで実行されている VMware ワークロードを、VMware も導入されている指定されたリカバリ データセンターにある別のONTAPストレージシステムに複製できます。

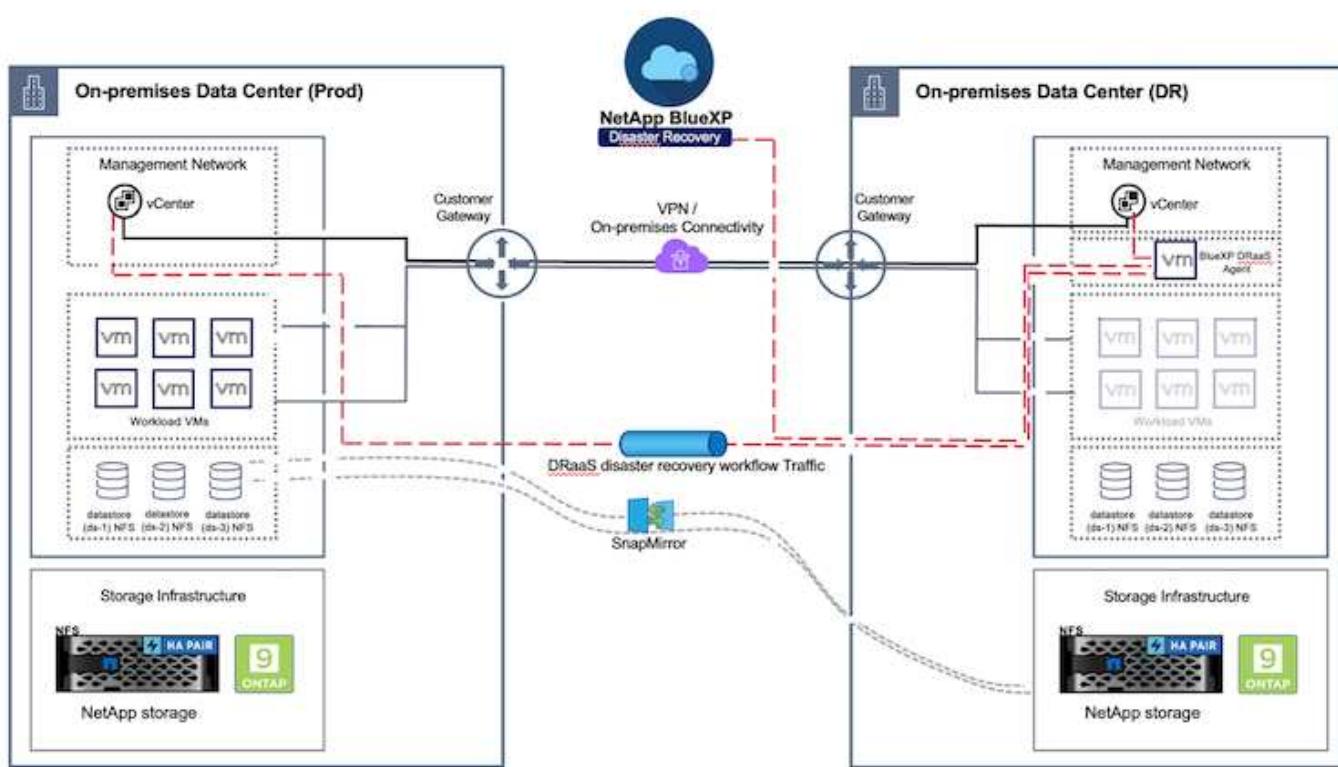
はじめに

このドキュメントのセクションでは、オンプレミスの VMware VM の災害復旧を別の指定サイトに設定するためのBlueXP DRaaS の構成について説明します。このセットアップの一部として、BlueXPアカウント、BlueXPコネクタ、VMware vCenter からONTAPストレージへの通信を可能にするために必要なONTAPアレイがBlueXPワークスペース内に追加されます。さらに、このドキュメントでは、サイト間のレプリケーションを構成する方法と、リカバリ プランを設定およびテストする方法についても詳しく説明します。最後のセクションでは、サイト全体のフェールオーバーを実行する手順と、プライマリ サイトが回復されオンラインで

購入されたときにフェールバックする方法について説明します。

NetApp BlueXPコンソールに統合されたBlueXP disaster recoveryサービスを利用することで、企業はオンプレミスのVMware vCenterとONTAPストレージを簡単に検出できます。組織は、リソースグループを作成し、災害復旧計画を作成し、それをリソースグループに関連付け、フェールオーバーとフェールバックをテストまたは実行できます。SnapMirrorは、ストレージレベルのブロックレプリケーションを提供して、2つのサイトを増分変更で最新の状態に保ち、最大5分のリカバリポイント目標(RPO)を実現します。さらに、本番環境に影響を与えることなく、追加のストレージコストが発生したりすることなく、災害復旧手順をシミュレートできます。

BlueXP disaster recoveryは、ONTAPのFlexCloneテクノロジーを活用して、ディザスター・リカバリ・サイトで最後に複製されたスナップショットからNFSデータストアのスペース効率の高いコピーを作成します。災害復旧テストを完了すると、実際の複製された本番リソースに影響を与えることなく、テスト環境を簡単に削除できます。実際のフェイルオーバーが発生した場合、BlueXP disaster recoveryサービスは、数回クリックするだけで、指定された災害復旧サイトで保護された仮想マシンを自動的に起動するために必要なすべての手順を調整します。このサービスは、必要に応じて、プライマリ・サイトとのSnapMirror関係を逆転させ、フェイルバック操作のためにセカンダリ・サイトからプライマリ・サイトへの変更を複製します。これらすべての機能は、他のよく知られた代替手段に比べて、ほんのわずかなコストで提供されます。



開始

BlueXP disaster recoveryを開始するには、BlueXPコンソールを使用してサービスにアクセスします。

1. BlueXPにログインします。
2. BlueXPの左側のナビゲーションから、[保護] > [災害復旧] を選択します。
3. BlueXP disaster recoveryダッシュボードが表示されます。

災害復旧計画を構成する前に、次の前提条件が満たされていることを確認してください。

- BlueXPコネクタはNetApp BlueXPに設定されます。
- BlueXPコネクタインスタンスは、ソースおよびターゲットのvCenterおよびストレージシステムに接続できます。
- ストレージNFSデータストアを提供するNetApp Data ONTAPクラスター。
- VMware用のNFSデータストアをホストするオンプレミスのNetAppストレージシステムがBlueXPに追加されます。
- DNS名を使用する場合は、DNS解決を実施する必要があります。それ以外の場合は、vCenterのIPアドレスを使用します。
- 指定されたNFSベースのデータストアボリュームに対してSnapMirrorレプリケーションが構成されます。
- 環境にサポートされているバージョンのvCenter ServerおよびESXiサーバーがインストールされていることを確認します。

ソースサイトと宛先サイト間の接続が確立されたら、構成手順に進みます。これには数回のクリックと約3～5分かかります。



NetApp、BlueXPコネクタがネットワークを介してソースリソースおよび宛先リソースと通信できるように、宛先サイトまたは3番目のサイトにBlueXPコネクタを展開することを推奨しています。

The screenshot shows the NetApp BlueXP Disaster recovery dashboard. It includes sections for Sites (2), Replication plans (2), Resource groups (2), and various metrics like Protected VMs (16) and Unprotected VMs (117). The Activity section lists recent events such as backup jobs and resource discoveries.

BlueXP disaster recovery構成

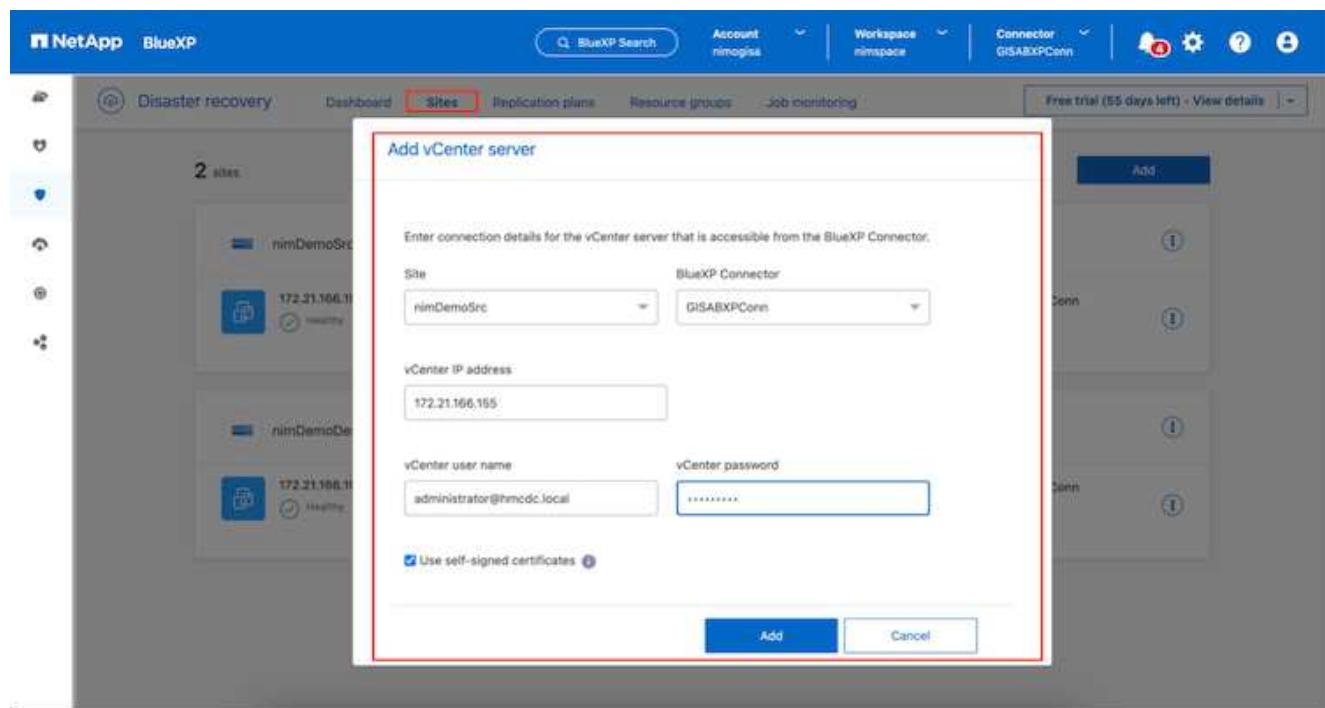
災害復旧の準備の最初のステップは、オンプレミスの vCenter とストレージ リソースを検出し、BlueXP disaster recoveryに追加することです。

BlueXPコンソールを開き、左側のナビゲーションから 保護 > 災害復旧 を選択します。vCenter サーバーの検出を選択するか、トップメニューを使用して サイト > 追加 > vCenter の追加を選択します。

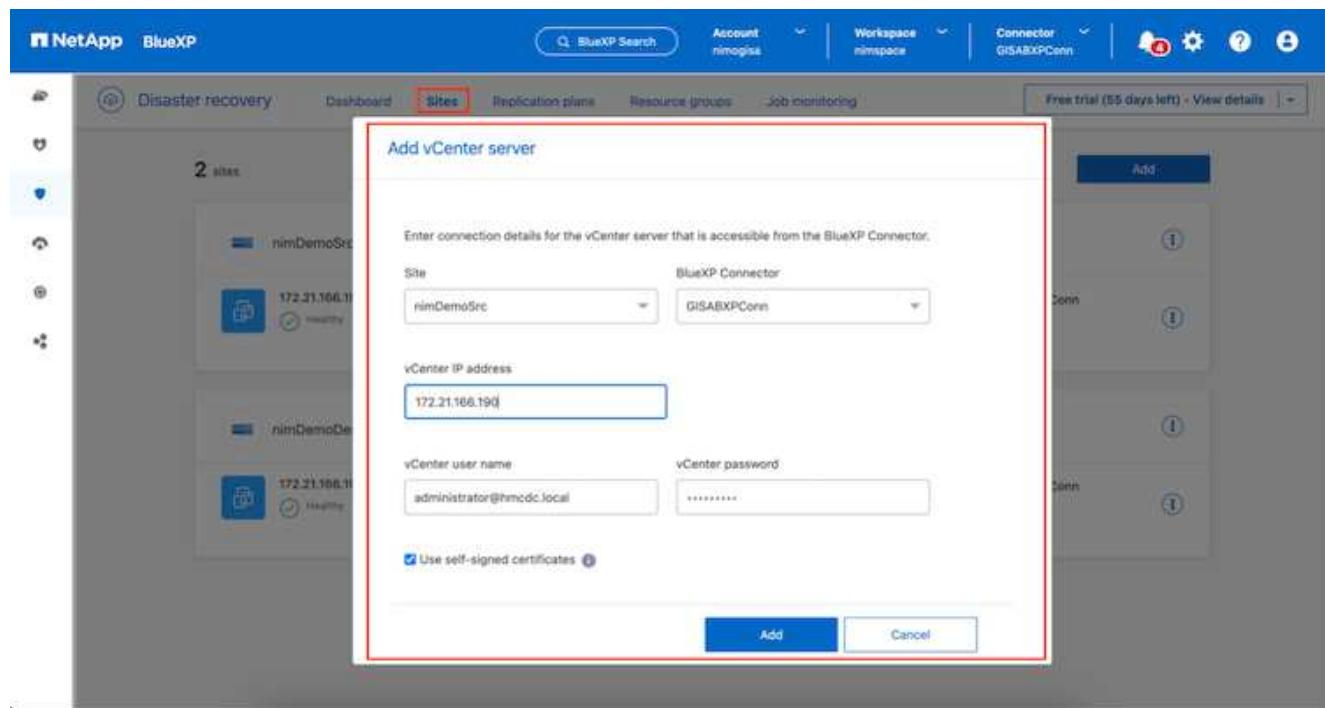
The screenshot shows the 'Add site' dialog box. It has fields for 'Site' (DemoSrv) and 'Location' (On-prem). The 'Location' field is highlighted with a red border.

次のプラットフォームを追加します。

- ・ソース。オンプレミスの vCenter。



- ・行き先。VMC SDDC vCenter。



vCenter が追加されると、自動検出がトリガーされます。

ソースサイトアレイと宛先サイトアレイ間のストレージレプリケーションの構成

SnapMirror は、NetApp環境でのデータ複製を提供します。NetApp Snapshot テクノロジーに基づいて構築されたSnapMirrorレプリケーションは、前回の更新以降に変更または追加されたブロックのみを複製するため、

非常に効率的です。SnapMirror は、NetApp OnCommand System ManagerまたはONTAP CLI を使用して簡単に設定できます。BlueXP DRaaS は、クラスターと SVM ピアリングが事前に構成されている場合、SnapMirror関係も作成します。

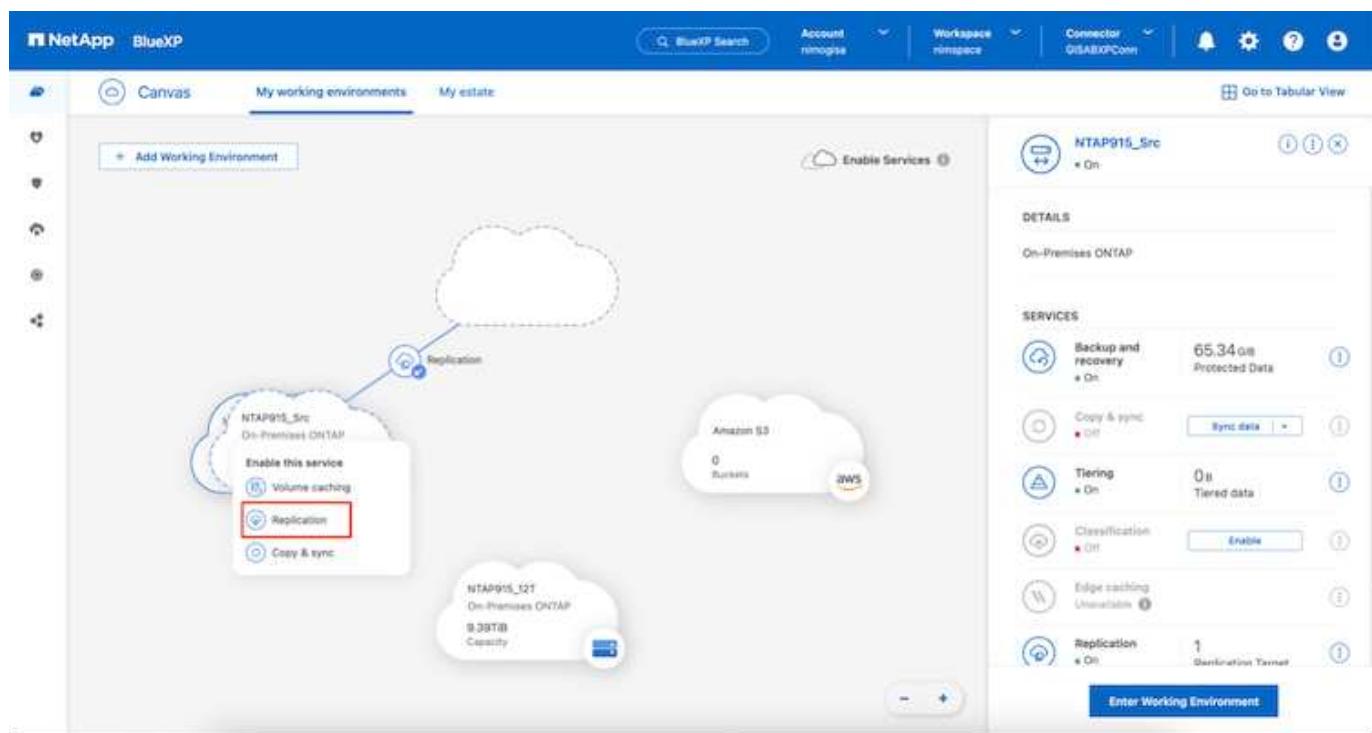
プライマリストレージが完全に失われていない場合、SnapMirror はプライマリ サイトと DR サイトを再同期する効率的な手段を提供します。SnapMirror は2つのサイトを再同期し、SnapMirror関係を単純に反転するだけで、変更されたデータまたは新しいデータのみを DR サイトからプライマリ サイトに転送できます。つまり、BlueXP DRaaS のレプリケーションプランは、フェイルオーバー後にボリューム全体を再コピーすることなく、どちらの方向にも再同期できます。関係が逆方向に再同期される場合、スナップショット コピーの最後の正常な同期以降に書き込まれた新しいデータのみが宛先に送り返されます。



CLI または System Manager を介してボリュームにSnapMirror関係がすでに構成されている場合、BlueXP DRaaS はその関係を取得し、残りのワークフロー操作を続行します。

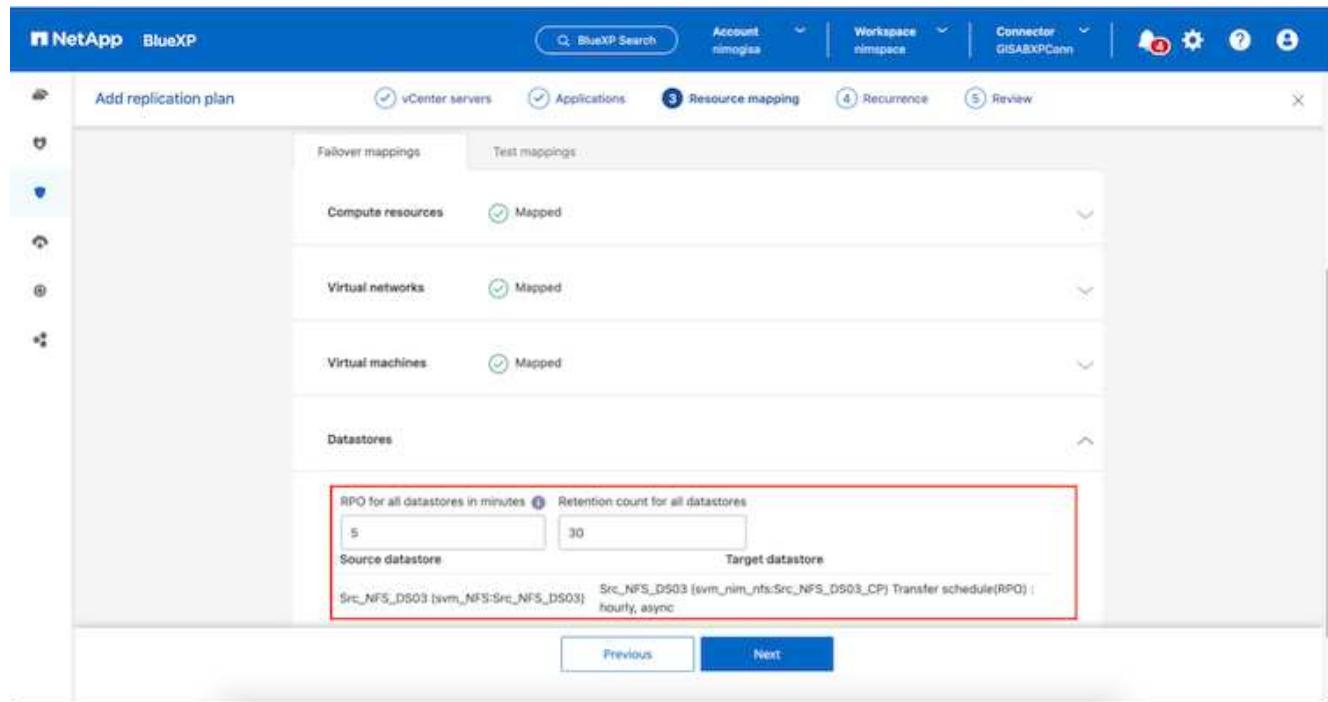
VMware Disaster Recoveryの設定方法

SnapMirrorレプリケーションを作成するプロセスは、どのアプリケーションでも同じです。このプロセスは手動でも自動でも実行できます。最も簡単な方法は、BlueXPを利用して、環境内のソースONTAPシステムを宛先にドラッグ アンド ドロップするだけでSnapMirrorレプリケーションを構成し、残りのプロセスをガイドするウィザードを起動することです。



BlueXP DRaaS では、次の 2 つの条件が満たされている場合、同じことを自動化することもできます。

- ・ソース クラスターと宛先クラスターにはピア関係があります。
- ・ソース SVM と宛先 SVM にはピア関係があります。



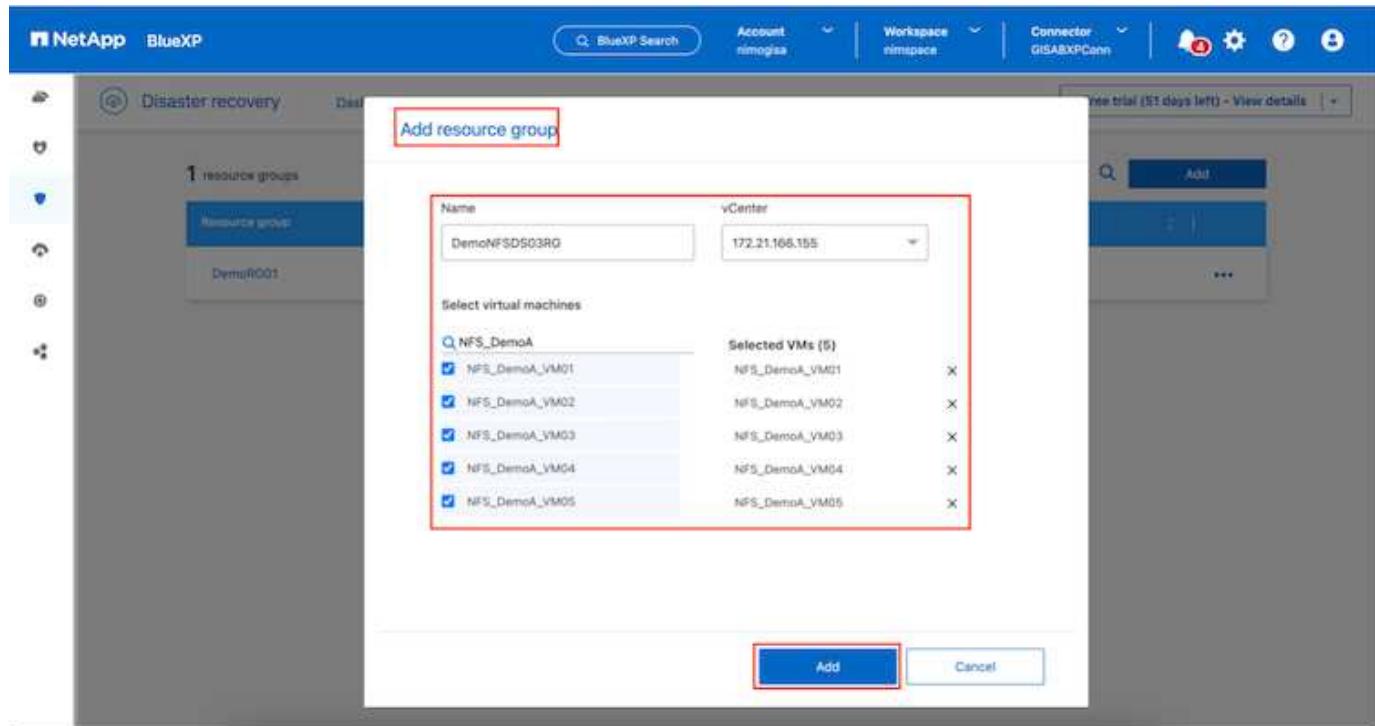
CLI 経由でボリュームにSnapMirror関係がすでに設定されている場合、BlueXP DRaaS はその関係を取得し、残りのワークフロー操作を続行します。

BlueXP disaster recoveryは何を実現できるのでしょうか？

ソース サイトと宛先サイトが追加されると、BlueXP disaster recoveryは自動的に詳細な検出を実行し、VM と関連メタデータを表示します。BlueXP disaster recoveryでは、VM で使用されるネットワークとポートグループも自動的に検出し、それらを入力します。

Site	IP Address	Status	VMs	Datastores	Resource groups	Connector
nimDemoSrc	172.21.166.155	Healthy	72	13	1	GISABXPConn
nimDemoDest	172.21.166.190	Healthy	61	3	0	GISABXPConn

サイトを追加した後、VM をリソース グループにグループ化できます。BlueXP disaster recovery リソース グループを使用すると、依存する VM のセットを、復旧時に実行できるブート順序とブート遅延を含む論理グループにグループ化できます。リソース グループの作成を開始するには、[リソース グループ] に移動し、[新しいリソース グループの作成] をクリックします。

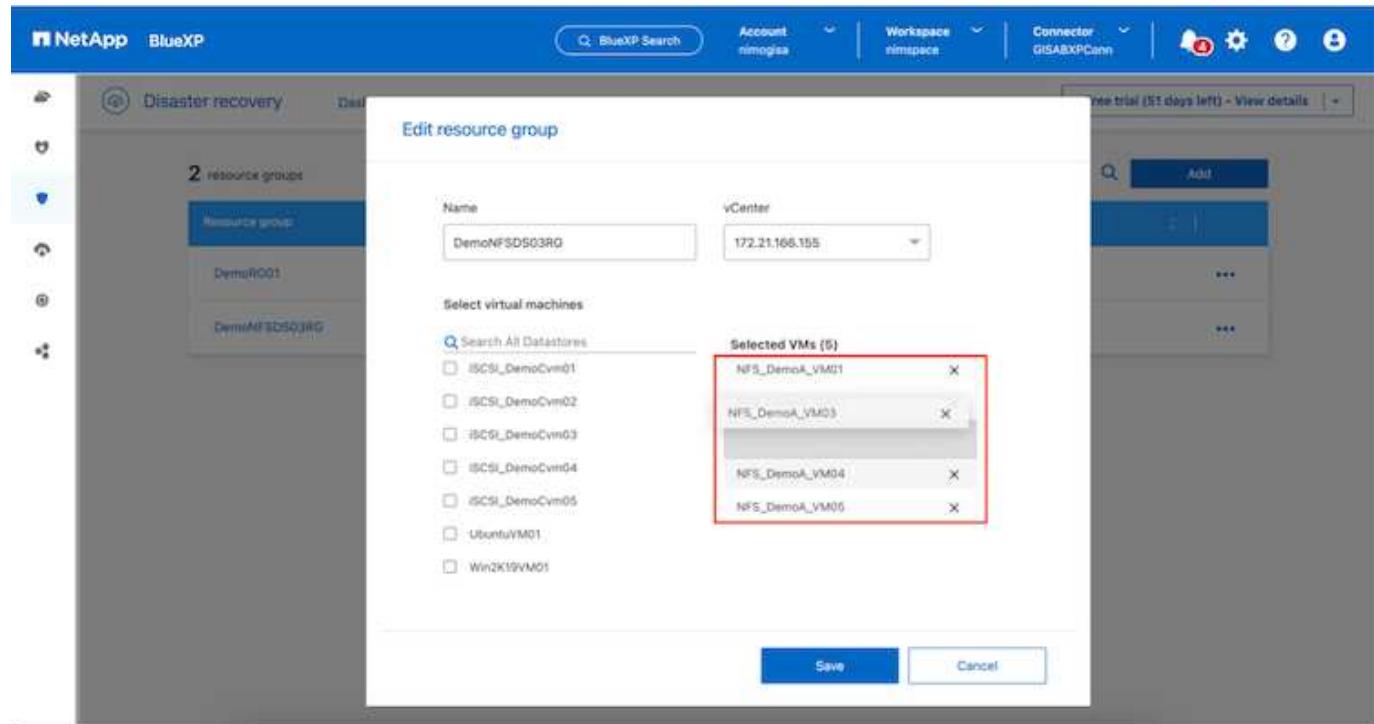


Resource group	Source site	Source vCenter
DemoRG01	nimDemoSrc	172.21.166.155
DemoNFS03RG	nimDemoSrc	172.21.166.155

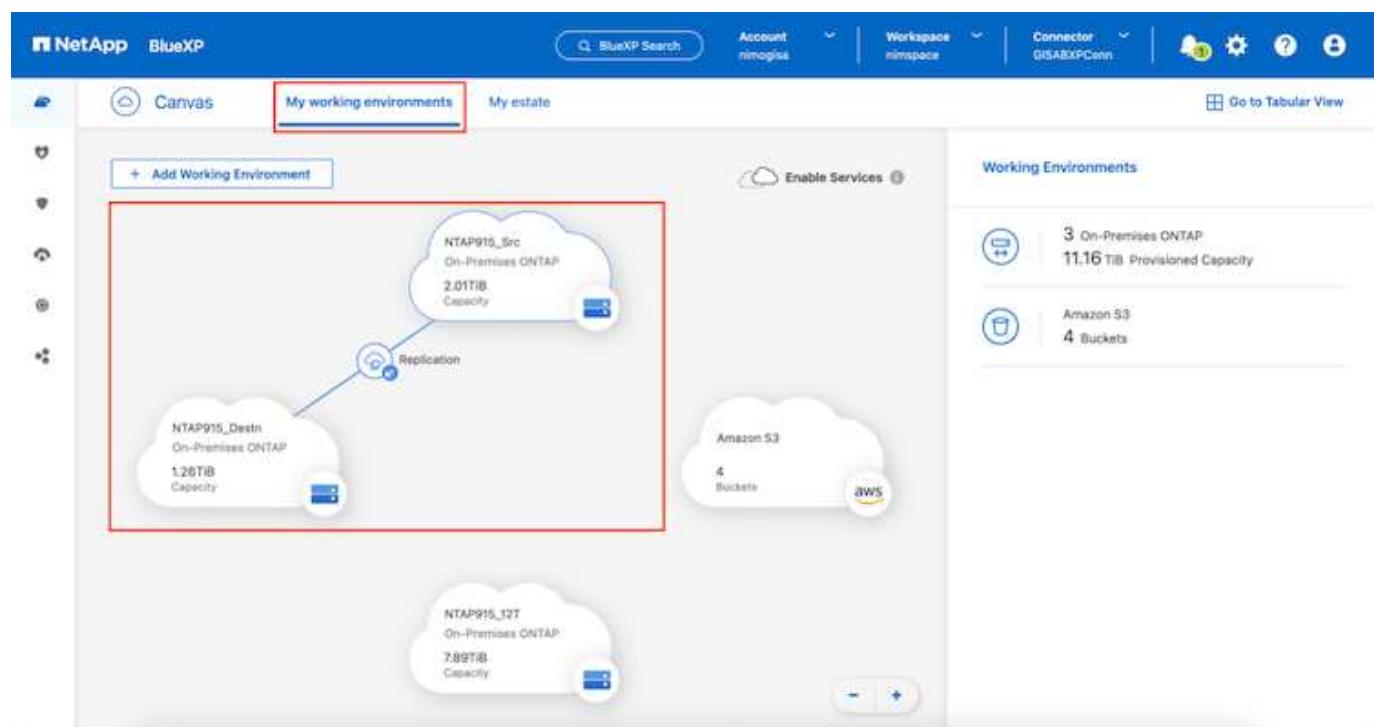


レプリケーション プランの作成時にリソース グループを作成することもできます。

VM のブート順序は、リソース グループの作成中に、簡単なドラッグ アンド ドロップ メカニズムを使用して定義または変更できます。



リソース グループを作成したら、次のステップは、災害発生時に仮想マシンとアプリケーションを復旧するための実行ブループリントまたは計画を作成することです。前提条件で述べたように、SnapMirrorレプリケーションは事前に構成することも、レプリケーション プランの作成時に指定された RPO と保持数を使用して DRaaS で構成することもできます。



Volume Relationships (8)

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
Green	NTAP915_Src	NTAP915_Destn	24.5 MB	idle	snapmirrored	Aug 5, 2024, 6:16:38 386.63 MB
Green	Demo_TPS_DS01 NTAP915_Src	Demo_TPS_DS01_Copy NTAP915_Destn	13 seconds	idle	snapmirrored	Aug 5, 2024, 6:16:38 386.63 MB
Green	Src_25G_Vol01 NTAP915_Src	Src_25G_Vol01_Copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12:13:29 79.23 MB
Green	Src_NFS_DS03 NTAP915_Src	Src_NFS_DS03_COPY NTAP915_Destn	12 seconds	idle	snapmirrored	Aug 16, 2024, 12:13:24.84 MB
Green	Src_NFS_DS04 NTAP915_Src	Src_NFS_DS04_COPY NTAP915_Destn	3 seconds	idle	snapmirrored	Aug 16, 2024, 12:13:47.38 MB
Green	Src_iSCSI_DS04 NTAP915_Src	Src_iSCSI_DS04_copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12:13:108.87 MB
Green	nimbra NTAP915_Src	nimbra_dest NTAP915_Destn	2 seconds	idle	snapmirrored	Aug 16, 2024, 12:13:3.48 KB

ドロップダウンからソースと宛先の vCenter プラットフォームを選択してレプリケーション プランを構成し、プランに含めるリソース グループ、アプリケーションの復元方法と電源オン方法のグループ化、およびクラスタとネットワークのマッピングを選択します。リカバリ プランを定義するには、[レプリケーション プラン] タブに移動し、[プランの追加] をクリックします。

まず、ソース vCenter を選択し、次に宛先 vCenter を選択します。

Add replication plan

1 vCenter servers 2 Applications 3 Resource mapping 4 Recurrence 5 Review

Replication plan name
DemoNFSDS03RP

Select a source vCenter where your data exists, to replicate to the selected target vCenter.

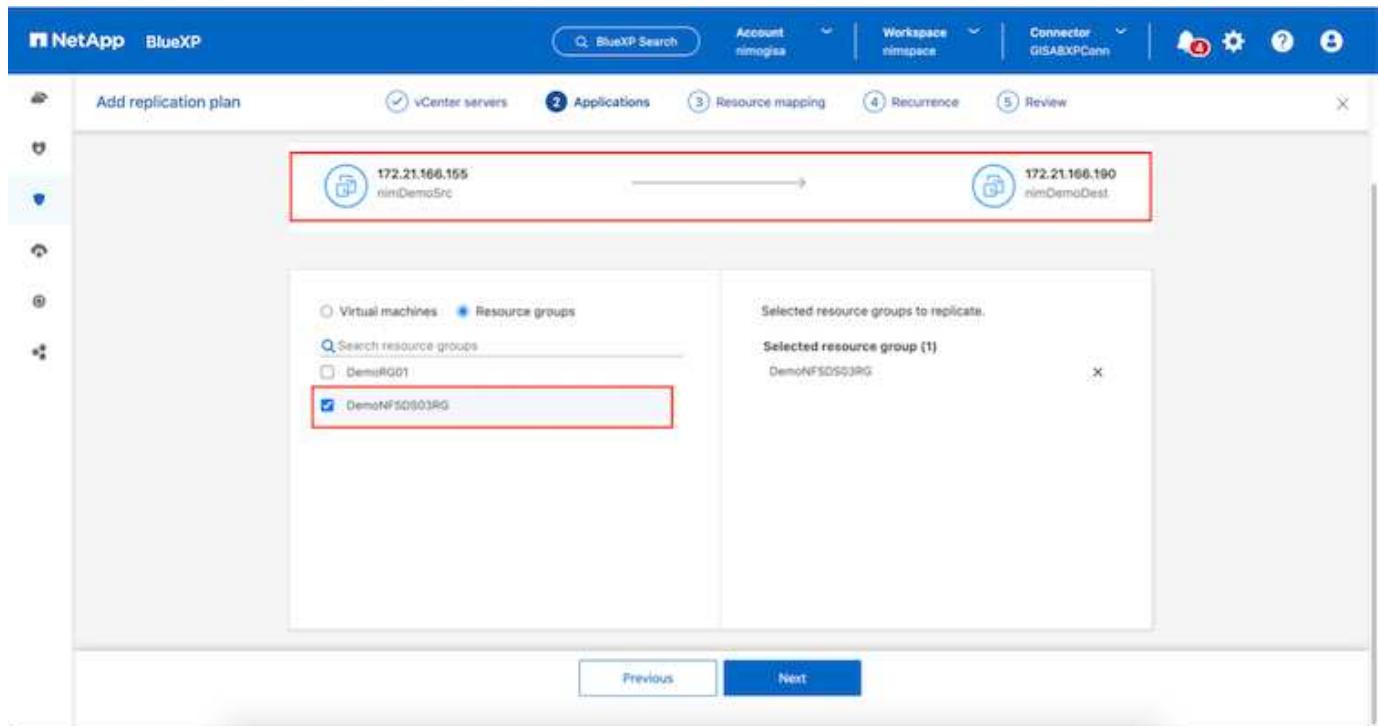
Source vCenter: 172.21.166.155

Target vCenter: 172.21.166.190

Next

次のステップは、既存のリソース グループを選択することです。リソース グループが作成されていない場合、ウィザードは、回復目標に基づいて必要な仮想マシンをグループ化します（基本的には機能リソース グループを作成します）。これは、アプリケーション仮想マシンを復元する操作シーケンスを定義するのにも役立

ちます。

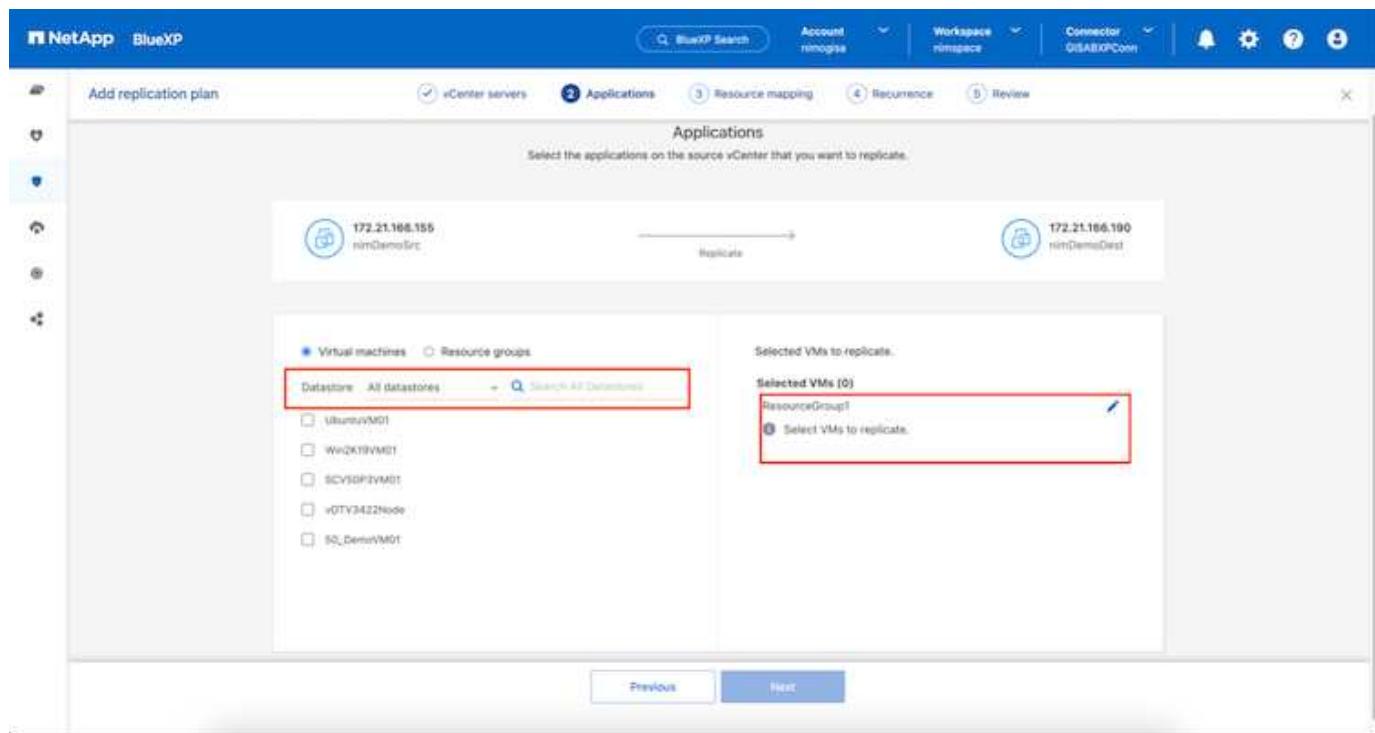


リソース グループでは、ドラッグ アンド ドロップ機能を使用してブート順序を設定できます。これを使用すると、リカバリプロセス中に VM の電源がオンになる順序を簡単に変更できます。

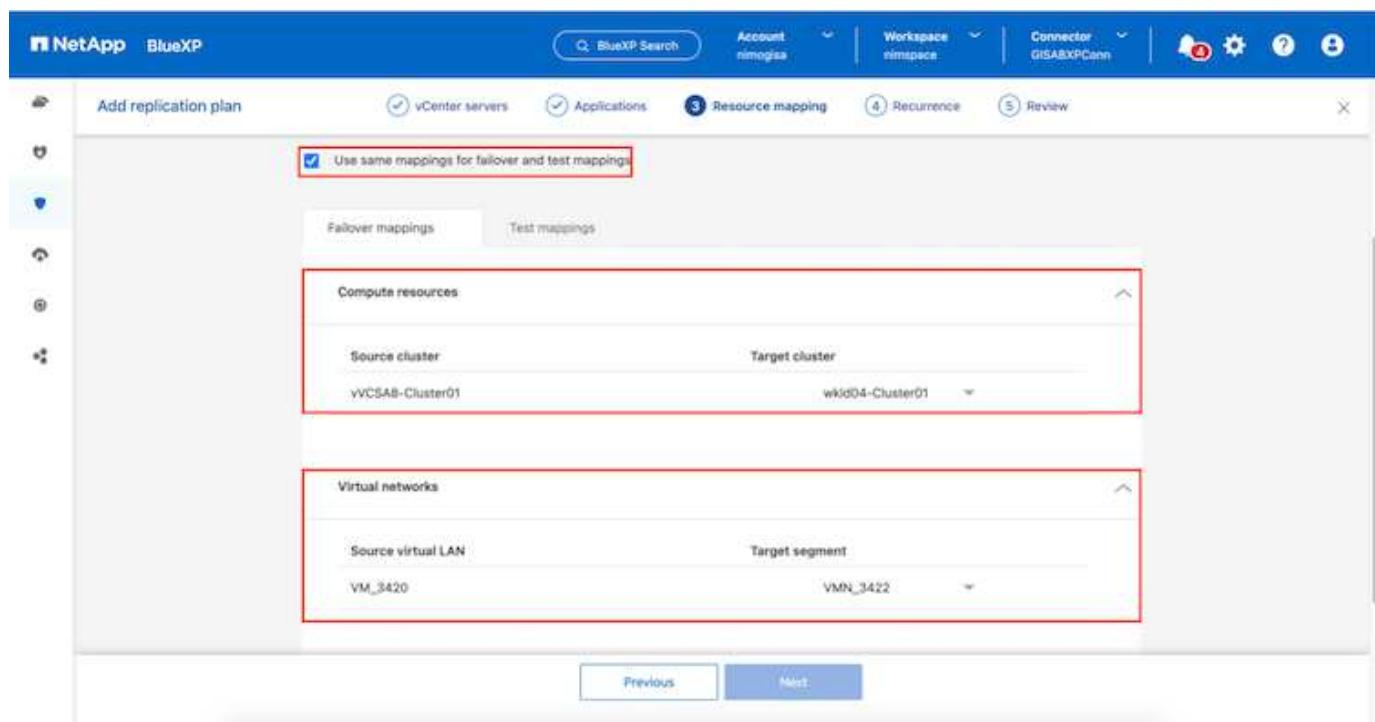


リソース グループ内の各仮想マシンは、順序に基づいて順番に起動されます。2 つのリソース グループが並行して開始されます。

以下のスクリーンショットは、リソース グループが事前に作成されていない場合に、組織の要件に基づいて仮想マシンまたは特定のデータストアをフィルターするオプションを示しています。



リソース グループを選択したら、フェールオーバー マッピングを作成します。このステップでは、ソース環境のリソースを宛先にどのようにマップするかを指定します。これには、コンピューティング リソース、仮想ネットワークが含まれます。IP カスタマイズ、事前スクリプトと事後スクリプト、ブート遅延、アプリケーションの一貫性など。詳細については、"レプリケーションプランを作成する"。



デフォルトでは、テスト操作とフェイルオーバー操作の両方に同じマッピング パラメータが使用されます。テスト環境に異なるマッピングを設定するには、以下に示すようにチェックボックスをオフにした後、テスト マッピング オプションを選択します。

Add replication plan

vCenter servers Applications Resource mapping Recurrence Review

Virtual machines

IP address type Target IP

Static Same as source

Use the same credentials for all VMs

Use the same script for all VMs

Source VM CPUs RAM Boot delay(mins between 0 and 10) Create application consistent replicas

DemoNFSDS03RG

NFS_DemoA_VM01	2	4	GB	0	<input type="checkbox"/>
NFS_DemoA_VM02	2	4	GB	0	<input type="checkbox"/>

Previous Next

リソース マッピングが完了したら、[次へ] をクリックします。

Add replication plan

vCenter servers Applications Resource mapping Recurrence Review

172.21.166.165 nimDemoSrc → 172.21.166.190 nimDemoDest

Use same mappings for failover and test mappings

Failover mappings Test mappings

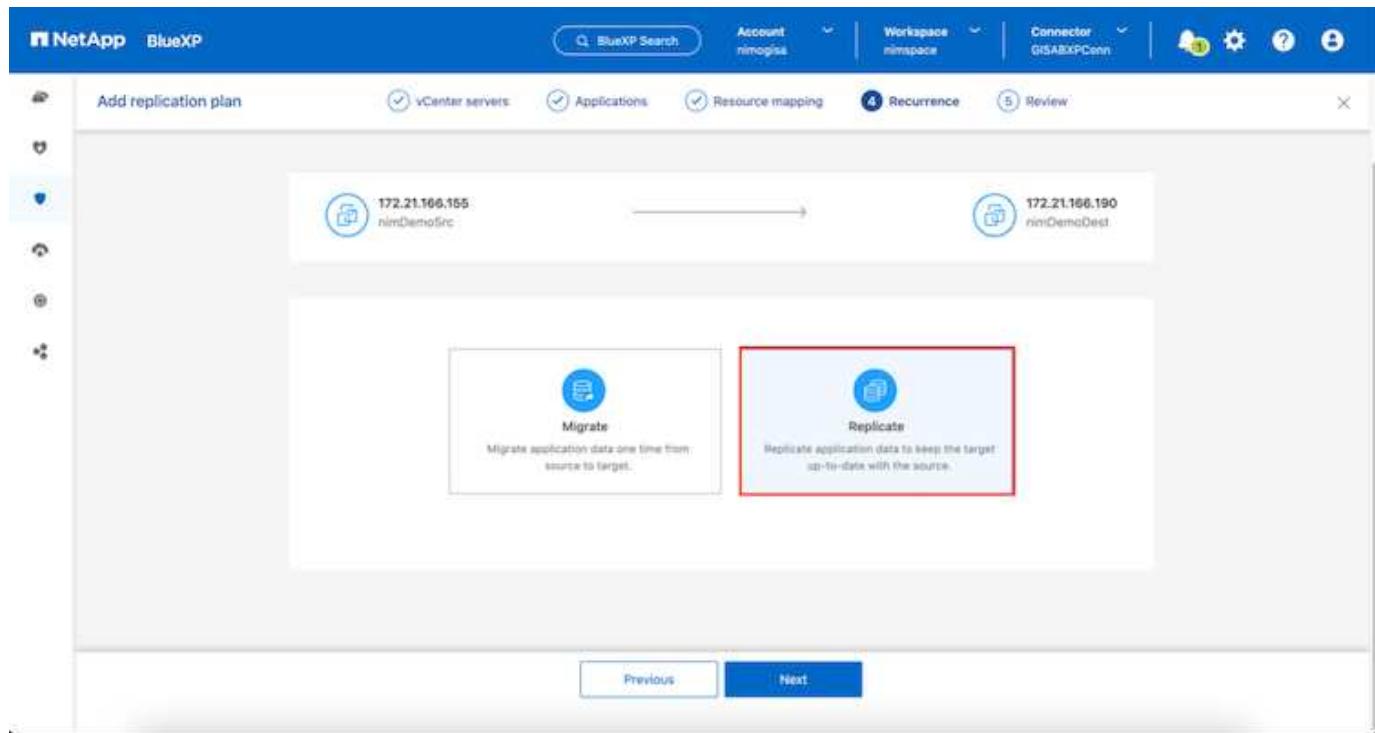
Compute resources Mapped

Virtual networks Mapped

Virtual machines Mapped

Previous Next

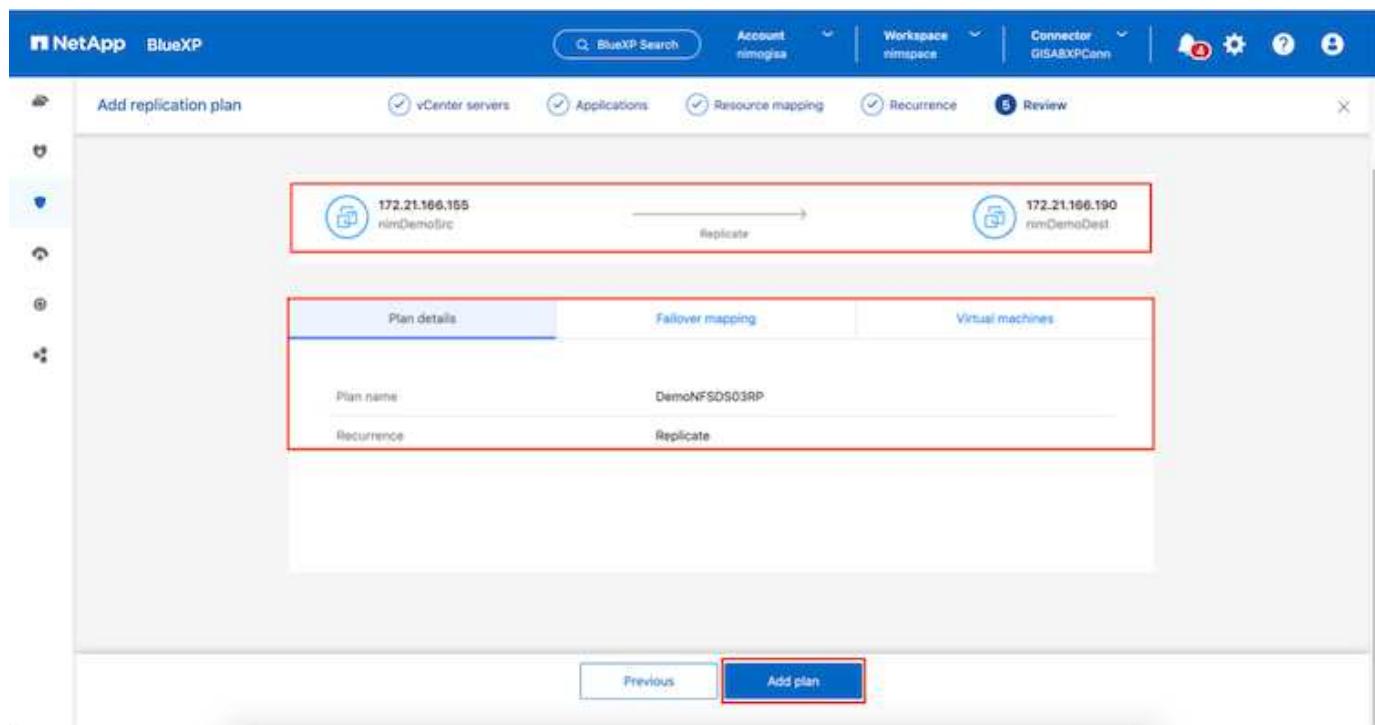
繰り返しタイプを選択します。簡単に言えば、「移行」（フェイルオーバーを使用した1回限りの移行）または定期的な連続レプリケーション オプションを選択します。このチュートリアルでは、「複製」オプションが選択されています。



完了したら、作成されたマッピングを確認し、「プランの追加」をクリックします。



異なるボリュームおよび SVM からの VM をレプリケーション プランに含めることができます。VM の配置 (同じボリューム上、同じ SVM 内の別のボリューム上、異なる SVM 上の別のボリューム上など) に応じて、BlueXP disaster recoveryでは整合性グループ スナップショットが作成されます。



The screenshot shows the NetApp BlueXP web interface. At the top, there are navigation tabs: Disaster recovery, Dashboard, Sites, Replication plans (which is highlighted with a red box), Resource groups, and Job monitoring. To the right of these are account information (Account: nimogisa, Workspace: nimspace), connector details (Connector: GSA8XPCann), and user profile icons. A banner at the top right indicates a 'Free trial (51 days left) - View details'. On the left, there's a vertical sidebar with various icons. The main content area shows a table titled '1 plans'. The table has columns: Plan, Compliance check, Plan status, Protected site, Resource groups, Recurrence, and Failover site. The single row in the table is highlighted with a red box. The 'Plan' column shows 'DemoNFS503RP', 'Compliance check' shows 'Healthy' with a green checkmark, 'Plan status' shows 'Ready' with a green checkmark, 'Protected site' is 'nimDemoSrc', 'Resource groups' is 'DemoNFS503RG', 'Recurrence' is 'Replicate', and 'Failover site' is 'nimDemoDest'. There's also a '...' button at the end of the row.

BlueXP DRaaS は次のワークフローで構成されています。

- ・ テストフェイルオーバー（定期的な自動シミュレーションを含む）
- ・ クリーンアップフェイルオーバーテスト
- ・ フェイルオーバー
- ・ フェイルバック

テストフェイルオーバー

BlueXP DRaaS のテスト フェイルオーバーは、VMware 管理者が実稼働環境を中断することなくリカバリ プランを完全に検証できるようにする運用手順です。

The screenshot shows the NetApp BlueXP web interface. At the top, there's a navigation bar with tabs for Disaster recovery, Dashboard, Sites, Replication plans (which is currently selected and highlighted with a red box), Resource groups, and Job monitoring. Below the navigation is a search bar and user account information. The main content area displays a table of replication plans. One plan, 'DemoNFSDS03RP', is selected and shown in more detail. To the right of this plan, a context menu is open, listing options like View plan details, Run compliance check, Test failover (which is also highlighted with a red box), Clean up failover test, Fail over, Fail back, Edit schedules, Take snapshot now, Disable, Enable, and Delete.

BlueXP DRaaS には、テスト フェイルオーバー操作のオプション機能としてスナップショットを選択する機能が組み込まれています。この機能により、VMware 管理者は、環境で最近行われた変更が宛先サイトに複製され、テスト中に存在していることを確認できます。このような変更には、VMゲストオペレーティングシステムへのパッチが含まれます。

This screenshot shows a 'Test failover' dialog box overlaid on the BlueXP interface. The dialog title is 'Test failover: DemoNFSDS03RP'. It contains several warning messages: one about creating VMs in the destination site and another about restoring a volume with a selected snapshot copy. Below these are sections for 'Snapshot copy for volume recovery' (with radio buttons for 'Take snapshot now' and 'Select') and a list of available snapshots. A specific snapshot, 'DemoNFSDS03RP_DemoNFSDS03RG_B-16-202', is selected and highlighted with a red box. At the bottom of the dialog, there's an input field for 'Enter Test failover to confirm' and two buttons: 'Test failover' (highlighted with a red box) and 'Cancel'.

VMware 管理者がテスト フェイルオーバー操作を実行すると、BlueXP DRaaS は次のタスクを自動化します。

- SnapMirror関係をトリガーして、本番サイトで行われた最近の変更を宛先サイトのストレージに反映します。

- DR ストレージ アレイ上のFlexVolボリュームのNetApp FlexCloneボリュームを作成します。
- FlexCloneボリューム内の NFS データストアを DR サイトの ESXi ホストに接続します。
- マッピング中に指定されたテスト ネットワークに VM ネットワーク アダプターを接続します。
- DR サイトのネットワークの定義に従って、VM ゲスト オペレーティング システムのネットワーク設定を再構成します。
- レプリケーション プランに保存されているカスタム コマンドを実行します。
- レプリケーション プランで定義された順序で VM の電源をオンにします。

The screenshot shows the vSphere Client interface. In the top navigation bar, it says "vSphere Client" and "Administrator@HMCDC.LOCAL". Below the navigation bar, there's a search bar and several icons.

The main area displays a storage resource named "Src_NFS_DS03". A red box highlights this resource. To its left is a tree view showing other storage resources like "wkld04-vc01hmc当地" and "wkld04-DC01".

On the right side of the "Src_NFS_DS03" card, there are two sections: "Details" and "Capacity and Usage". The "Details" section shows the following information:

Type	NFS 3
Hosts	2
Virtual machines	5
VM templates	
Server	172.21.66.166
Folder	/Src_NFS_DS03_TEST
Location	/s://vmfs/volumes/b0c8c2d-1e687494/

The "Capacity and Usage" section shows:

Storage	7122 GB free
26.78 GB Used	100 GB capacity

Below the storage details, there are "VIEW STATS" and "REFRESH" buttons.

At the bottom of the screen, there's a "Recent Tasks" section with a table showing completed tasks:

Task Name	Target	Status	Details	Initiator	Outstanding For	Start Time	Completion Time
Reconfigure virtual machine	NFS_DemoA_VM02	Completed		HMCDC.LOCAL/Administrator	3 ms	08/16/2024, 6:53:59 AM	08/16/2024, 6:53:59 AM
Register virtual machine	wkld04-DC01	Completed		System	6 ms	08/16/2024, 6:53:58 AM	08/16/2024, 6:53:59 AM
Register virtual machine	wkld04-DC01	Completed		System	2 ms	08/16/2024, 6:53:58 AM	08/16/2024, 6:53:59 AM
Register virtual machine	wkld04-DC01	Completed	Registering Virtual Machine on destination host	System	2 ms	08/16/2024, 6:53:58 AM	08/16/2024, 6:54:00 AM

A red box highlights the last task in the list.

クリーンアップフェイルオーバーテスト操作

クリーンアップ フェイルオーバー テスト操作は、レプリケーション プラン テストが完了し、VMware 管理者がクリーンアップ プロンプトに応答した後に実行されます。

The screenshot shows the NetApp BlueXP web interface. At the top, there's a navigation bar with tabs for Disaster recovery, Dashboard, Sites, Replication plans (which is selected), Resource groups, and Job monitoring. On the far right, there are account and workspace dropdowns, a connector status, and various icons. Below the navigation, a search bar and a 'Free trial (51 days left) - View details' button are visible. The main content area shows a table with one row under the heading '1 plans'. The table columns include Plan, Compliance check, Plan status, Protected site, Resource groups, Recurrence, and Failover site. The first row has values: DemoNFS03RP, Healthy, Test failover (highlighted with a red box), nimDemoSrc, DemoNFS03RG, Replicate, and nimDemoDest. To the right of the table is a context menu with options like View plan details, Run compliance check, Test failover, Clean up failover test (highlighted with a red box), Fail over, Fail back, Edit schedules, Take snapshot now, Disable, Enable, and Delete.

このアクションにより、仮想マシン (VM) とレプリケーション プランのステータスが準備完了状態にリセットされます。

VMware 管理者がリカバリ操作を実行すると、BlueXP DRaaS は次のプロセスを完了します。

1. テストに使用されたFlexCloneコピー内の回復された各 VM の電源をオフにします。
2. テスト中に回復された VM を表示するために使用されたFlexCloneボリュームを削除します。

計画的な移行とフェイルオーバー

BlueXP DRaaS には、実際のフェイルオーバーを実行するための 2 つの方法 (計画された移行とフェイルオーバー) があります。最初の方法である計画移行では、VM のシャットダウンとストレージ レプリケーションの同期をプロセスに組み込んで、VM を回復するか、効率的に移行先サイトに移動させます。計画された移行にはソース サイトへのアクセスが必要です。2 番目の方針であるフェールオーバーは、計画済み/計画外のフェールオーバーであり、完了できた最後のストレージ レプリケーション間隔から宛先サイトで VM が回復されます。ソリューションに設計された RPO に応じて、DR シナリオではある程度のデータ損失が予想されます。

The screenshot shows the NetApp BlueXP web interface. At the top, there are navigation tabs: Disaster recovery, Dashboard, Sites, Replication plans (which is the active tab), Resource groups, and Job monitoring. A search bar says 'BlueXP Search'. On the right, there are account and workspace dropdowns, a connector status, and user icons. Below the tabs, it says '1 plans'. The main area shows a table with columns: Plan, Compliance check, Plan status, Protected site, Resource groups, Recurrence, and Failover site. One row is selected, showing 'DemoNFS03RP' as the plan name, 'Healthy' as the status, 'nimDemoSrc' as the protected site, 'DemoNFS03RG' as the resource group, 'Replicate' as the recurrence, and 'nimDemoDest' as the failover site. A context menu is open for this row, listing options: View plan details, Run compliance check, Test failover, Clean up failover test, Fail over (which is highlighted with a red box), End backup, Edit schedules, Take snapshot now, Disable, Enable, and Delete.

VMware 管理者がフェイルオーバー操作を実行すると、BlueXP DRaaS は次のタスクを自動化します。

- NetApp SnapMirror関係を解除してフェイルオーバーします。
- 複製された NFS データストアを DR サイトの ESXi ホストに接続します。
- VM ネットワーク アダプターを適切な宛先サイト ネットワークに接続します。
- 宛先サイトのネットワークの定義に従って、VM ゲスト オペレーティング システムのネットワーク設定を再構成します。
- レプリケーション プランに保存されているカスタム コマンド (存在する場合) を実行します。
- レプリケーション プランで定義された順序で VM の電源をオンにします。

Src_NFS_DS03

Task Name	Target	Status	Details	Initiator	Quoted Elap.	Start Time	Completion Time
Power On virtual machine	NPS_DemoA_VM02	Completed	Powering on the new Virtual Machine	HMCDC.LOCAL\Administrator	4 ms	05/16/2024, 7:04:07 A.M.	05/16/2024, 7:04:12 A.M.
Power On virtual machine	NPS_DemoB_VM02	Completed	Powering on the new Virtual Machine	HMCDC.LOCAL\Administrator	3 ms	05/16/2024, 7:04:07 A.M.	05/16/2024, 7:04:12 A.M.
Power On virtual machine	NPS_DemoC_VM02	Completed	Powering on the new Virtual Machine	HMCDC.LOCAL\Administrator	3 ms	05/16/2024, 7:04:06 A.M.	05/16/2024, 7:04:07 A.M.
Power On virtual machine	NPS_DemoD_VM02	Completed	Powering on the new Virtual Machine	HMCDC.LOCAL\Administrator	2 ms	05/16/2024, 7:04:06 A.M.	05/16/2024, 7:04:06 A.M.

フェイルバック

フェイルバックは、回復後にソース サイトと宛先サイトの元の構成を復元するオプションの手順です。

Disaster recovery

1 plans

DemoNFS03RP

Healthy

Failed over

nimDemoSrc

DemoNFS03RG

Replicate

nimDemoDest

Add

View plan details

Run compliance check

Test failover

Clean up failover test

Fail over

Fail back

Edit schedules

Take snapshot now

Disable

Enable

Delete

VMware 管理者は、サービスを元のソース サイトに復元する準備ができたら、フェイルバック手順を構成して実行できます。

注意: BlueXP DRaaS は、レプリケーションの方向を反転する前に、すべての変更を元のソース仮想マシンにレプリケート(再同期)します。このプロセスは、ターゲットへのフェールオーバーが完了した関係から開始

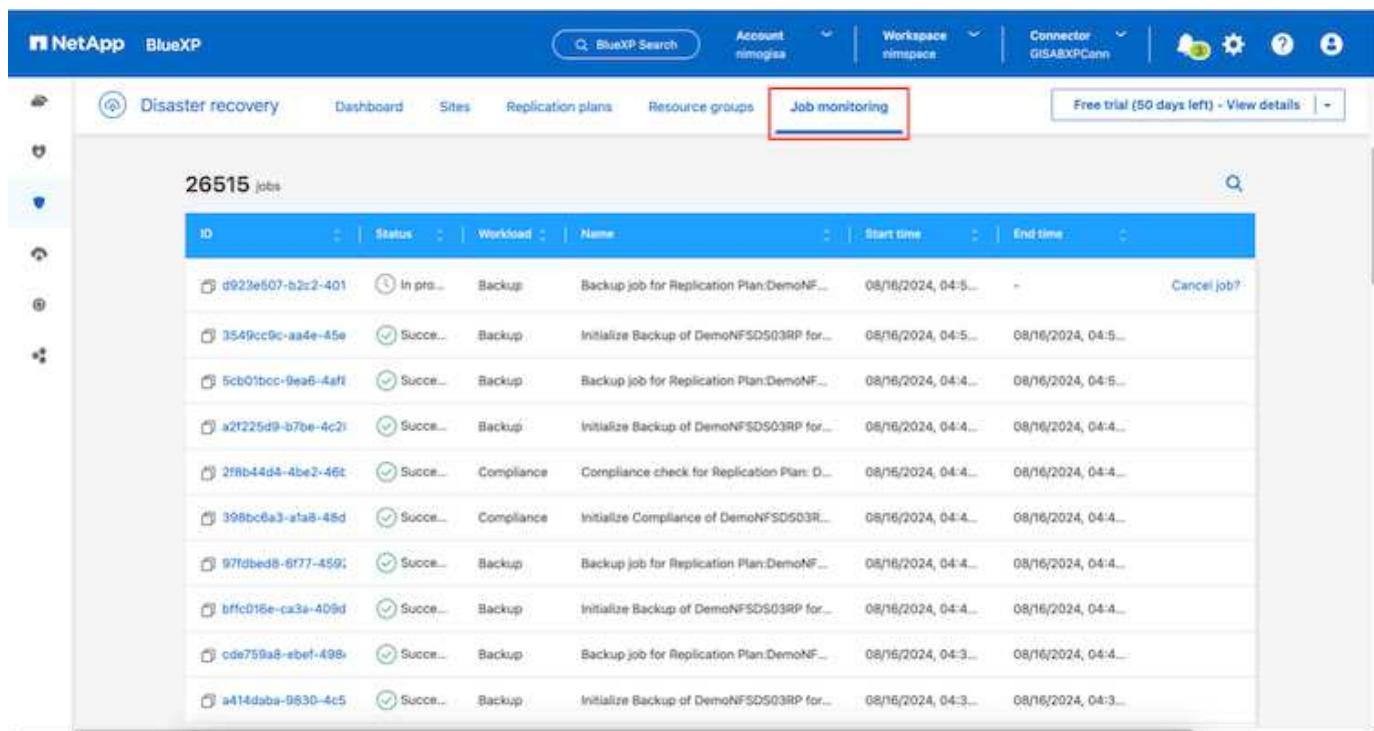
され、次の手順が含まれます。

- 仮想マシンの電源をオフにして登録を解除すると、宛先サイトのボリュームがマウント解除されます。
- 元のソースのSnapMirror関係を解除して、読み取り/書き込み可能にします。
- レプリケーションを元に戻すには、SnapMirror関係を再同期します。
- ソースにボリュームをマウントし、ソース仮想マシンをパワーオンして登録します。

BlueXP DRaaSへのアクセスと設定の詳細については、["BlueXP Disaster Recovery for VMwareについて学ぶ"](#)。

監視とダッシュボード

BlueXPまたはONTAP CLIから、適切なデータストアボリュームのレプリケーションのヘルスステータスを監視し、ジョブ監視を介してフェイルオーバーまたはテストフェイルオーバーのステータスを追跡できます。



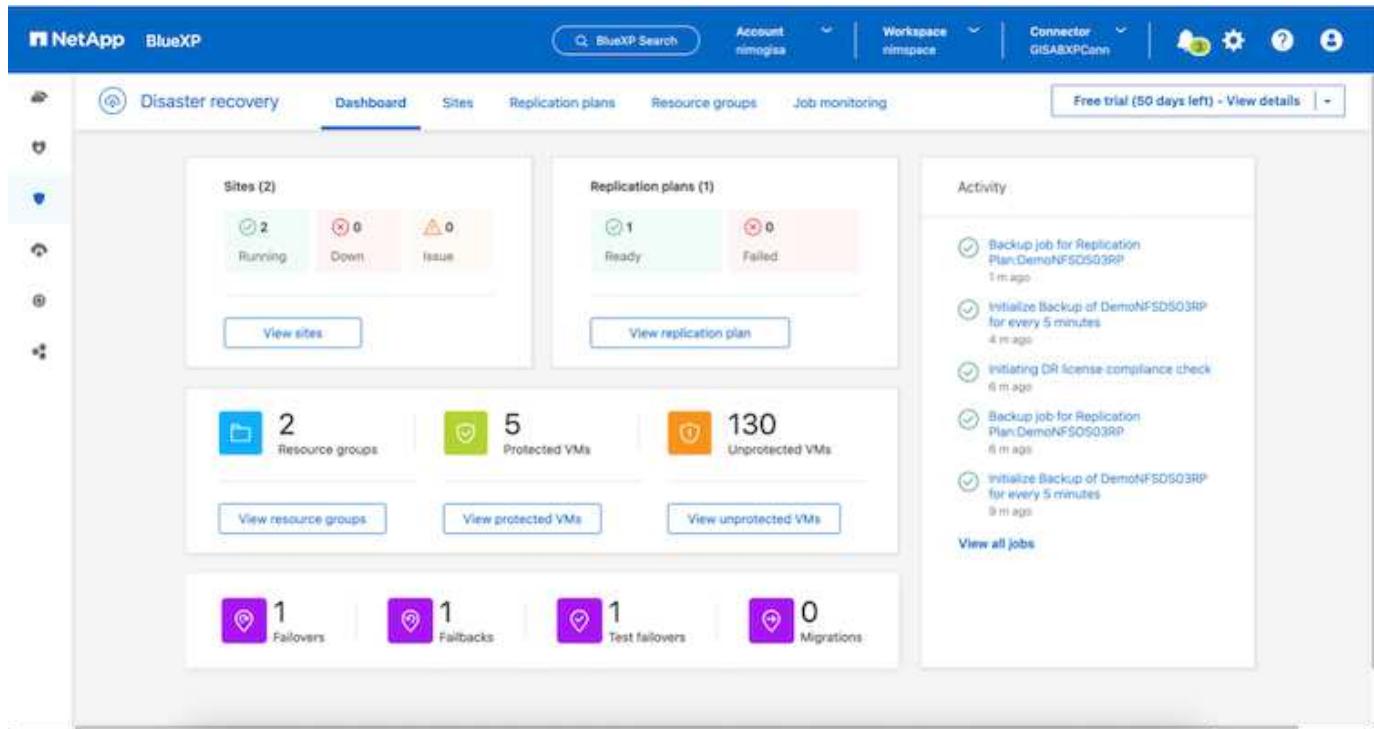
The screenshot shows the BlueXP Disaster recovery dashboard. At the top, there are navigation tabs: Disaster recovery (which is selected), Dashboard, Sites, Replication plans, Resource groups, and Job monitoring (which is highlighted with a red box). Below the tabs, a search bar and account/workspace information are displayed. The main area is titled "26515 jobs" and contains a table with columns: ID, Status, Workload, Name, Start time, End time, and Cancel job?.

ID	Status	Workload	Name	Start time	End time	Cancel job?
d923e507-b2c2-401	In pro...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:5...	-	Cancel job?
3549cc9c-aa4e-45e	Succes...	Backup	Initialize Backup of DemoNFS03RP for...	08/16/2024, 04:5...	08/16/2024, 04:5...	
5cb01bcc-9ea6-4aff	Succes...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:5...	
a2f225d9-b70e-4c2	Succes...	Backup	Initialize Backup of DemoNFS03RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
2ff8b44d4-4be2-46t	Succes...	Compliance	Compliance check for Replication Plan: D...	08/16/2024, 04:4...	08/16/2024, 04:4...	
398bc6a3-ata8-48d	Succes...	Compliance	Initialize Compliance of DemoNFS03RP...	08/16/2024, 04:4...	08/16/2024, 04:4...	
97fdbed8-6777-459	Succes...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:4...	
bffcd16e-ca3a-409d	Succes...	Backup	Initialize Backup of DemoNFS03RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
cde759a8-ebef-498	Succes...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:3...	08/16/2024, 04:4...	
a414daba-9830-4c5	Succes...	Backup	Initialize Backup of DemoNFS03RP for...	08/16/2024, 04:3...	08/16/2024, 04:3...	



ジョブが現在進行中またはキューに入っており、それを停止したい場合は、キャンセルするオプションがあります。

BlueXP disaster recoveryダッシュボードを使用すると、災害復旧サイトとレプリケーションプランの状態を確実に評価できます。これにより、管理者は正常なサイトやプラン、切断されたサイトやプラン、または機能低下したサイトやプランを迅速に特定できます。



これにより、調整およびカスタマイズされた災害復旧計画を処理するための強力なソリューションが提供されます。フェイルオーバーは、計画されたフェイルオーバーとして実行することも、災害が発生して DR サイトをアクティブ化する決定が下されたときにボタンをクリックするだけでフェイルオーバーを実行することもできます。

このプロセスについて詳しく知りたい場合は、詳細なウォークスルービデオをご覧いただくか、["ソリューションシミュレータ"](#)。

vSphere Metro Storage Clusterでワークロードを保護する

ONTAP高可用性と VMware vSphere Metro Storage Cluster (vMSC) の統合について学習します。

NetApp ONTAP の高可用性を VMware vSphere Metro Storage Cluster (vMSC) と統合するために使用できるNetAppソリューションについて学習します。これにより、VMware Cloud Foundation (VCF) 管理および VI ワークロード ドメインに堅牢なソリューションが提供されます。

この組み合わせにより、地理的に分散したサイト間での継続的なデータ可用性、シームレスなフェイルオーバー、災害復旧が保証され、重要なワークロードの回復力と運用の継続性が向上します。SnapMirrorアクティブシンクにより、サイト全体の障害が発生してもビジネスサービスの運用が継続され、セカンダリ コピーを使用してアプリケーションが透過的にフェイルオーバーできるようになります。SnapMirrorアクティブ同期でフェイルオーバーをトリガーするために、手動操作やカスタム スクリプトは必要ありません。

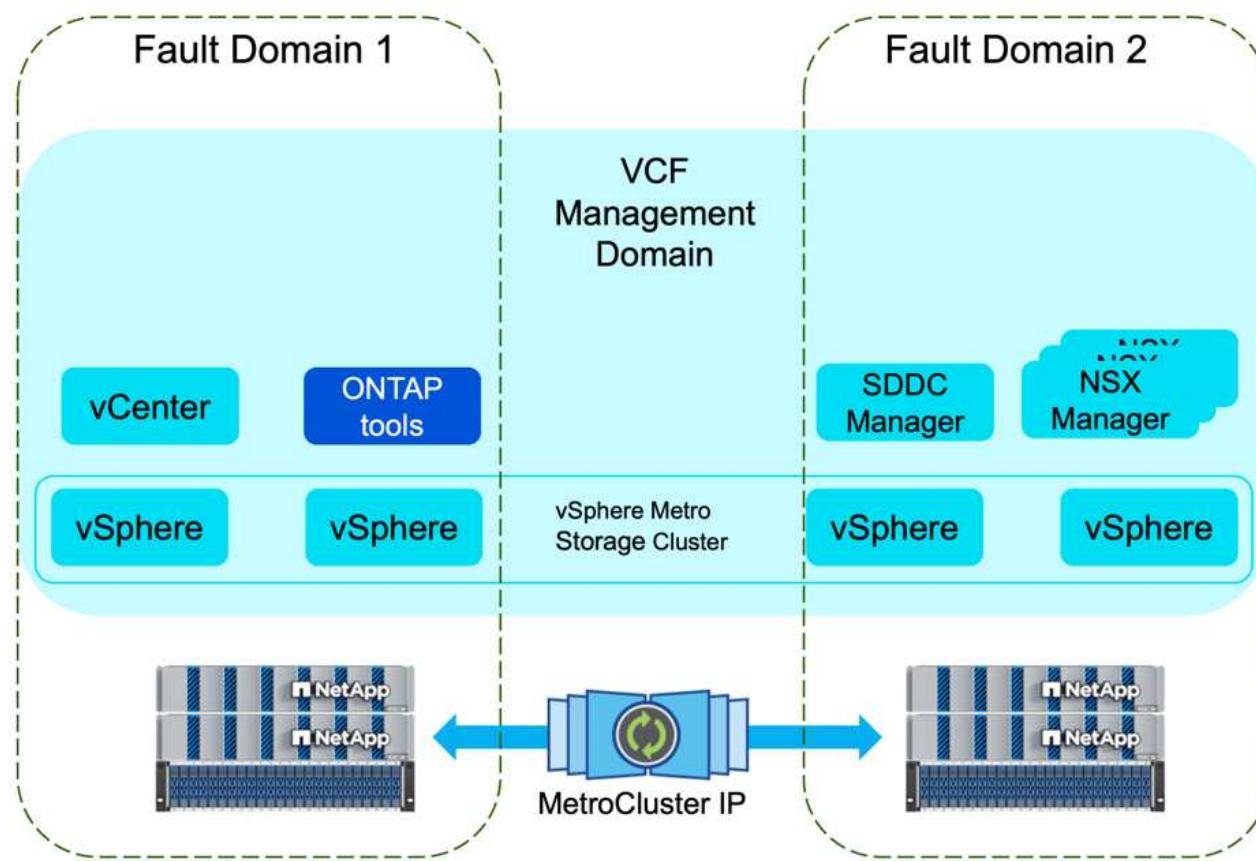
詳細については、以下の解決策を参照してください。

- ["SnapMirror Active Sync を使用した管理ドメインのストレッチ クラスタ"](#)
- ["MetroClusterを使用した管理ドメインのストレッチ クラスタ"](#)

- ・ "SnapMirror Active Sync を使用した VI ワークロード ドメインのストレッチ クラスタ"
- ・ "MetroClusterを使用した VI ワークロード ドメインのストレッチ クラスタ"

MetroClusterを使用して VCF 管理ドメインのストレッチ クラスタを構成する

このユースケースでは、プライマリ データストアとして NFS を使用したONTAP MetroClusterを使用して、VMware Cloud Foundation (VCF) 管理ドメインのストレッチ クラスタを構成する手順について説明します。この手順には、vSphere ホストと vCenter Server のデプロイ、NFS データストアのプロビジョニング、VCF インポート ツールを使用したクラスタの検証、NSX 設定の構成、環境の VCF 管理ドメインへの変換が含まれます。



はじめに

このソリューションでは、ONTAP MetroClusterを使用して、NFS をプリンシパル データストアとしてストレッチ VCF 管理ドメインを実装する方法を説明します。

シナリオの概要

このシナリオでは、次の大きな手順について説明します。

- ・ vSphere ホストと vCenter サーバーをデプロイします。

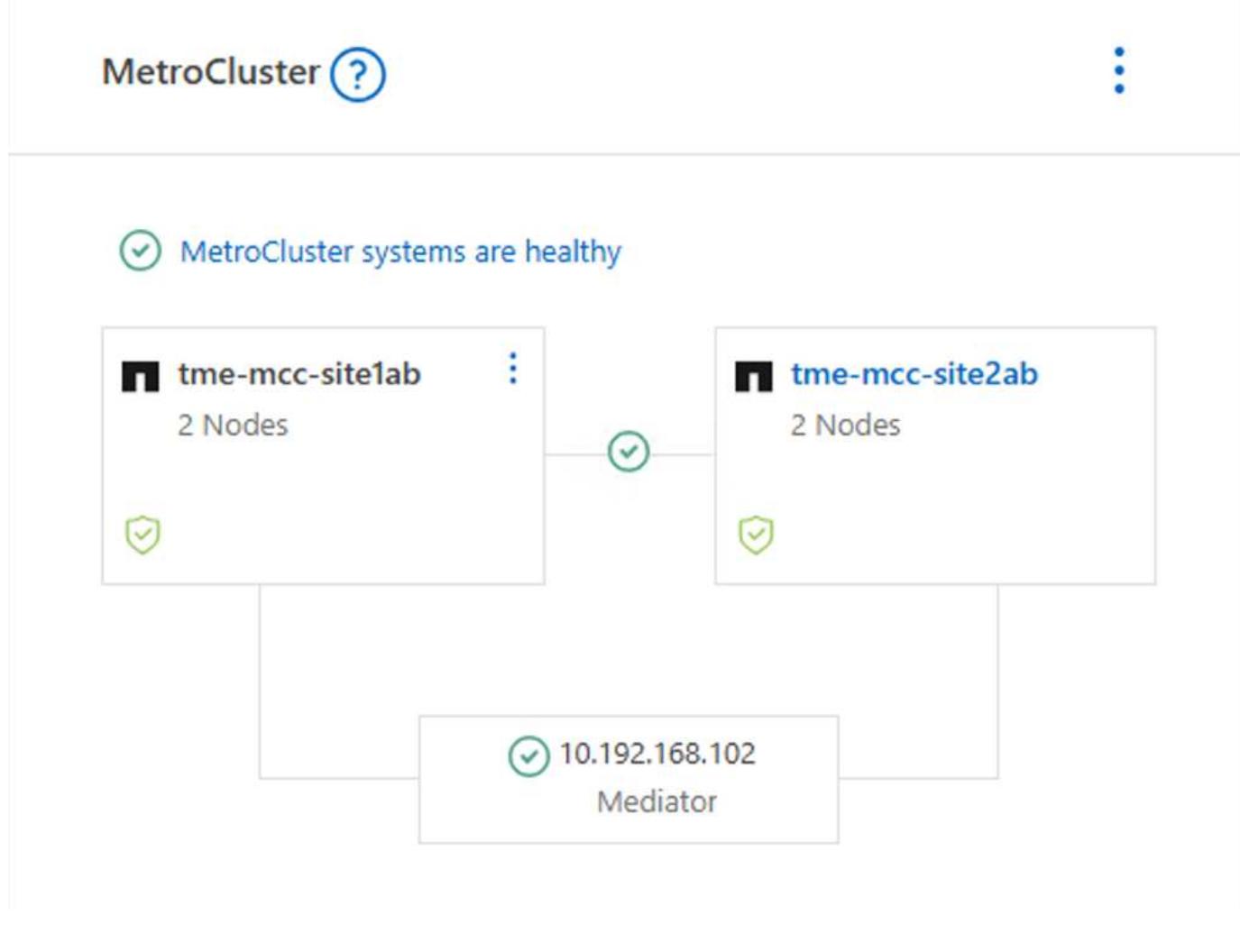
- NFS データストアを vSphere ホストにプロビジョニングします。
- vSphere クラスタに SDDC Manager をデプロイします。
- VCF インポート ツールを使用して、vSphere クラスターを検証します。
- VCF 変換中に NSX を作成するための JSON ファイルを構成します。
- VCF インポート ツールを使用して、vSphere 8 環境を VCF 管理ドメインに変換します。

前提条件

このシナリオには、次のコンポーネントと構成が必要です。

- サポートされているONTAP MetroCluster構成
- NFS トラフィックを許可するように構成されたストレージ仮想マシン (SVM)。
- NFS トラフィックを伝送し、SVM に関連付けられた IP ネットワーク上に論理インターフェイス (LIF) が作成されています。
- ネットワーク スイッチに接続された 4 台の ESXi ホストを備えた vSphere 8 クラスター。
- VCF 変換に必要なソフトウェアをダウンロードします。

以下は、 MetroCluster構成を示す System Manager のサンプル スクリーンショットです。



両方の障害ドメインからの SVM ネットワーク インターフェイスは次のとおりです。

Name	Status	Storage VM	IPspace	Address	Current node
<input type="text"/> Q		<input type="text"/> ch-svm	<input type="text"/>	<input type="text"/>	<input type="text"/>
lif_ch-svm-mcc02_8775	!	ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a
lif_ch-svm-mcc01_3118	✓	ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a
lif_ch-svm-mcc02_9778	!	ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b
lif_ch-svm-mcc01_6783	✓	ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b

Name	Status	Storage VM	IPspace	Address	Current node
<input type="text"/> Q		<input type="text"/> ch-svm	<input type="text"/>	<input type="text"/>	<input type="text"/>
lif_ch-svm-mcc01_3118	!	ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a
lif_ch-svm-mcc02_8775	✓	ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a
lif_ch-svm-mcc01_6783	!	ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b
lif_ch-svm-mcc02_9778	✓	ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b

[注意] SVM はMetroCluster内の障害ドメインの 1 つでアクティブになります。

Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
ch-svm-mcc01	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	<input type="radio"/>
ch-svm-mcc02-mc	Stopped	Sync_destination		Default	n/a	<input type="radio"/>

Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
ch-svm-mcc01-mc	Stopped	Sync_destination		Default	n/a	<input type="radio"/>
ch-svm-mcc02	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	<input type="radio"/>

参照する "MetroClusterを使用した vMSC"。

vSphere を VCF 5.2 に変換またはインポートする際にサポートされるストレージおよびその他の考慮事項については、以下を参照してください。 "既存の vSphere 環境を VMware Cloud Foundation に変換またはインポートする前に考慮すべき事項"。

VCF管理ドメインに変換するvSphereクラスタを作成する前に、 "vSphere クラスタにおける NSX の考慮事項"。

必要なソフトウェアについては、 "既存の vSphere 環境を変換またはインポートするためのソフトウェアをダウンロードする"。

ONTAPストレージシステムの構成については、 "ONTAP 9ドキュメント" 中心。

VCFの設定方法については、以下を参照してください。 "VMware Cloud Foundation ドキュメント"。

展開手順

NFSを主データストアとしてVCFストレッチ管理ドメインを展開するには、

次の手順を実行します。

- vSphere ホストと vCenter をデプロイします。
- vSphere クラスターを作成します。
- NFS データストアをプロビジョニングします。
- VCF インポート ツールを vCenter アプライアンスにコピーします。
- VCF インポート ツールを使用して、vCenter アプライアンスの事前チェックを実行します。
- vCenter クラスタに SDDC マネージャ VM をデプロイします。
- 変換プロセス中に展開する NSX クラスタの JSON ファイルを作成します。
- 必要なソフトウェアを SDDC マネージャにアップロードします。
- vSphere クラスタを VCF 管理ドメインに変換します。

変換プロセスの概要については、以下を参照してください。 "vSphere 環境を管理ドメインに変換するか、 VMware Cloud Foundation で vSphere 環境を VI ワークロード ドメインとしてインポートする"。

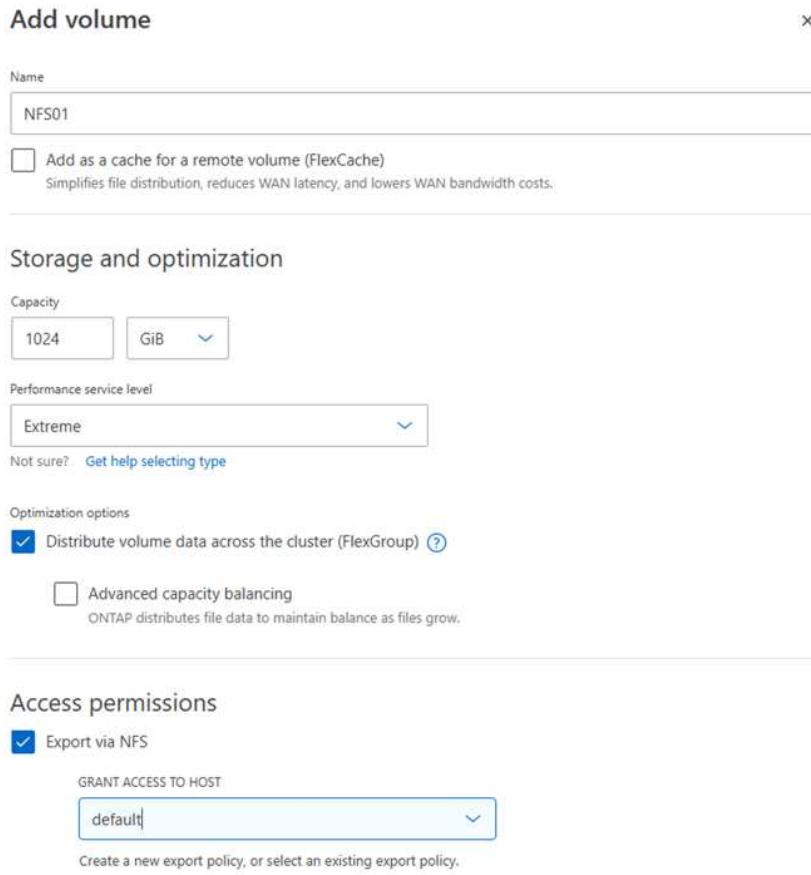
vSphereホストとvCenterを展開する

Broadcom サポート ポータルからダウンロードした ISO を使用してホストに vSphere を展開するか、 vSphere ホストの既存の展開オプションを使用します。

NFS データストアをホスト VM にマウントする

この手順では、NFS ボリュームを作成し、それをデータストアとしてマウントして VM をホストします。

1. System Manager を使用してボリュームを作成し、vSphere ホストの IP サブネットを含むエクスポート ポリシーに接続します。



2. vSphere ホストに SSH で接続し、NFS データストアをマウントします。

```
[root@SiteA-vs01:~] esxcli storage nfs add -c 4 -H 10.192.164.225 -s /NFS01 -v NFS01
[root@SiteA-vs01:~] esxcli storage nfs list
Volume Name Host Share Vmknic Accessible Mounted Connections Read-Only isPE Hardware Acceleration
----- 
NFS01 10.192.164.225 /NFS01 None true true 4 false false Not Supported
[root@SiteA-vs01:~]
```

3. 追加のデータストアが必要な場合は上記の手順を繰り返し、ハードウェア アクセラレーションがサポートされていることを確認します。

```
[root@MCCA01:~] esxcli storage nfs list
Volume Name Host Share Vmknic Accessible Mounted Connections Read-Only isPE Hardware Acceleration
----- 
NFS02 10.192.164.230 /NFS02 None true true 4 false false Supported
NFS01 10.192.164.225 /NFS01 None true true 4 false false Supported
[root@MCCA01:~]
```

NFS データストアに vCenter をデプロイします。 vCenter アプライアンスで SSH と Bash シェルが有効になっていることを確認します。

vSphere クラスタを作成する

1. vSphere Web クライアントにログインし、NFS VAAI が展開されているホストの 1 つを追加して、データセンターと vSphere クラスターを作成します。クラスター内のすべてのホストを単一のイメージ オプションで管理することを選択しました。[ヒント] クラスター レベルで構成を管理を選択しないでください。詳細については、"vSphere クラスタにおける NSX の考慮事項"。ONTAP MetroClusterを使用したvMSCのベストプラクティスについては、"vMSC 設計および実装ガイドライン"
2. 他の vSphere ホストをクラスタに追加します。
3. 分散スイッチを作成し、ポート グループを追加します。
4. "標準の vSwitch から分散スイッチにネットワークを移行します。"

vSphere 環境を VCF 管理ドメインに変換する

次のセクションでは、SDDC マネージャをデプロイし、vSphere 8 クラスタを VCF 5.2 管理ドメインに変換する手順について説明します。必要に応じて、詳細については VMware のドキュメントが参照されます。

VMware by Broadcom の VCF インポート ツールは、vCenter アプライアンスと SDDC マネージャの両方で使用されるユーティリティで、構成を検証し、vSphere および VCF 環境の変換およびインポート サービスを提供します。

```
https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/vcf-admin/GUID-44CFCB85-C001-41B2-BBB4-E71928B8D955.html ["VCFインポートツールのオプションとパラメータ"]。
```

VCFインポートツールのコピーと抽出

VCF インポート ツールは、vCenter アプライアンスで使用され、vSphere クラスタが VCF 変換またはインポート プロセスに対して正常な状態にあることを検証します。

次の手順を実行します。

1. 次の手順に従ってください "VCFインポートツールをターゲットのvCenterアプライアンスにコピーします" VMware Docs を参照して、VCF インポート ツールを正しい場所にコピーします。
2. 次のコマンドを使用してバンドルを抽出します。

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

vCenterアプライアンスを検証する

変換前に、VCF インポート ツールを使用して vCenter アプライアンスを検証します。

1. 次の手順に従ってください "変換前にターゲット vCenter で事前チェックを実行する" 検証を実行します。
2. 次の出力は、vCenter アプライアンスが事前チェックに合格したことを示しています。

```
[root@mcc-vc01 ~] ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter mcc-vc01.sddc.netapp.com --sso-user administrator@vsphere.local
[2025-03-20 23:02:02,518] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.2-24494579
[2025-03-20 23:02:02,521] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
[2025-03-20 23:02:02,521] [INFO] vcf_brownfield: Connected to vCenter mcc-vc01.sddc.netapp.com in 0.12 seconds
[2025-03-20 23:02:06,089] [INFO] vc_precheck: Running pre-checks for vCenter mcc-vc01.sddc.netapp.com...
[2025-03-20 23:02:06,091] [INFO] vc_precheck: VC BOM version check... PASS
[2025-03-20 23:02:06,135] [INFO] vc_precheck: [2/10] vSAN stretched cluster check... PASS
[2025-03-20 23:02:06,156] [INFO] vc_precheck: [3/10] Supported storage available check... PASS
[2025-03-20 23:02:06,170] [INFO] vc_precheck: [4/10] vCenter VM location check... PASS
[2025-03-20 23:02:06,424] [INFO] vc_precheck: [5/10] VxRail registration check... PASS
[2025-03-20 23:02:06,614] [INFO] vc_precheck: [6/10] NSX-T registration check... PASS
[2025-03-20 23:02:06,638] [INFO] vc_precheck: [7/10] Standalone host check... PASS
[2025-03-20 23:02:06,824] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check... PASS
[2025-03-20 23:02:10,245] [INFO] vc_precheck: [9/10] vCenter vMotion topology check... PASS
[2025-03-20 23:02:10,791] [INFO] vc_precheck: [10/10] WCP license check... PASS
[2025-03-20 23:02:10,880] [INFO] vc_precheck: All pre-checks passed!
[2025-03-20 23:02:10,881] [INFO] vc_precheck: Pre-checks for vCenter mcc-vc01.sddc.netapp.com completed in 4.79 seconds
[root@mcc-vc01 ~] ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]#
```

SDDC マネージャーを展開する

SDDC マネージャーは、VCF 管理ドメインに変換される vSphere クラスター上に共存する必要があります。

展開を完了するには、VMware Docs の展開手順に従ってください。

The screenshot shows the vSphere Client interface. On the left, the navigation bar displays the SDDC structure: `mcc-vc01.sddc.netapp.com` > `RTP` > `vMSC`. The `vMSC` node is selected and highlighted in blue. On the right, the main pane is titled `vMSC` and shows the `Summary` tab selected. The `Cluster Details` section displays the following information:

Total Processors:	32
Total vMotion Migrations:	4

参照 "ターゲットvCenterにSDDC Managerアプライアンスを展開する"。

NSX 展開用の JSON ファイルを作成する

vSphere 環境を VMware Cloud Foundation にインポートまたは変換しながら NSX Manager をデプロイするには、NSX デプロイ仕様を作成します。NSX の展開には少なくとも 3 台のホストが必要です。



変換またはインポート操作で NSX Manager クラスタをデプロイする場合、NSX VLAN でバックアップされたセグメントが使用されます。NSX-VLAN でバックアップされたセグメントの制限の詳細については、「既存の vSphere 環境を VMware Cloud Foundation に変換またはインポートする前の考慮事項」セクションを参照してください。NSX-VLAN ネットワークの制限については、以下を参照してください。["既存の vSphere 環境を VMware Cloud Foundation に変換またはインポートする前に考慮すべき事項"](#)。

以下は、NSX デプロイメント用の JSON ファイルの例です。

```
{  
    "deploy_without_license_keys": true,  
    "form_factor": "small",  
    "admin_password": "*****",  
    "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-  
133764.zip",  
    "cluster_ip": "10.61.185.114",  
    "cluster_fqdn": "mcc-nsx.sddc.netapp.com",  
    "manager_specs": [  
        {  
            "fqdn": "mcc-nsxa.sddc.netapp.com",  
            "name": "mcc-nsxa",  
            "ip_address": "10.61.185.111",  
            "gateway": "10.61.185.1",  
            "subnet_mask": "255.255.255.0"  
        },  
        {  
            "fqdn": "mcc-nsxb.sddc.netapp.com",  
            "name": "mcc-nsxb",  
            "ip_address": "10.61.185.112",  
            "gateway": "10.61.185.1",  
            "subnet_mask": "255.255.255.0"  
        },  
        {  
            "fqdn": "mcc-nsxc.sddc.netapp.com",  
            "name": "mcc-nsxc",  
            "ip_address": "10.61.185.113",  
            "gateway": "10.61.185.1",  
            "subnet_mask": "255.255.255.0"  
        }]  
}
```

JSON ファイルを SDDC マネージャーの vcf ユーザーのホーム フォルダーにコピーします。

SDDC マネージャーにソフトウェアをアップロードする

VCF インポート ツールを vcf ユーザーのホーム フォルダにコピーし、NSX デプロイメント バンドルを SDDC マネージャの /nfs/vmware/vcf/nfs-mount/bundle/ フォルダにコピーします。

見る "必要なソフトウェアを SDDC Manager アプライアンスにアップロードする" 詳細な手順については、こちらをご覧ください。

変換前のvCenterの詳細チェック

管理ドメインの変換操作または VI ワークロード ドメインのインポート操作を実行する前に、既存の vSphere 環境の構成が変換またはインポートに対してサポートされていることを確認するために詳細なチェックを実行する必要があります。。ユーザー vcf として SDDC Manager アプライアンスに SSH 接続します。。VCF インポート ツールをコピーしたディレクトリに移動します。。次のコマンドを実行して、vSphere環境が変換できることを確認します。

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user  
'<sso-user>' --sso-password '*****' --local-admin-password  
'*****' --accept-trust
```

vSphere クラスタを VCF 管理ドメインに変換する

変換プロセスを実行するには、VCF インポート ツールが使用されます。

次のコマンドを実行して、vSphere クラスタを VCF 管理ドメインに変換し、NSX クラスタをデプロイします。

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user '' --sso-password '*****' --vcenter-root-password '*****' --local-admin-password '*****' --backup-password '*****' --domain-name '<Mgmt-domain-name>' --accept-trust --nsx-deployment-spec-path /home/vcf/nsx.json
```

vSphere ホスト上で複数のデータストアが使用可能な場合、デフォルトで NSX VM がデプロイされるプライマリ データストアとして考慮する必要があるデータストアを指定するよう要求されます。

```
[2025-03-24 19:29:00,394] [INFO] vcenter_connection: Connecting to mcc-vc01.sddc.netapp.com as administrator@vsphere.local
[2025-03-24 19:29:00,583] [INFO] discover_domain: =====
[2025-03-24 19:29:00,586] [INFO] discover_domain: Starting inventory payload generation for vCenter: mcc-vc01.sddc.netapp.com, as domain of type: MANAGEMENT
[2025-03-24 19:29:00,586] [INFO] discover_domain: [1/5] Starting discovery of PSC and vCenter configuration data from vCenter: mcc-vc01.sddc.netapp.com
[2025-03-24 19:29:00,596] [INFO] discover_domain: [1/5] Completed discovery of PSC and vCenter configuration data from vCenter: mcc-vc01.sddc.netapp.com in 0.01s
[2025-03-24 19:29:00,596] [INFO] discover_domain: =====
[2025-03-24 19:29:00,596] [INFO] discover_domain: [2/5] Starting discovery of clusters in vCenter: mcc-vc01.sddc.netapp.com
[2025-03-24 19:29:00,613] [INFO] discover_domain: >>>> [1/1] Starting discovery of cluster: vMSC
Please select a primary datastore for cluster vMSC:
() NFS01
1) NFS02
2) NFS02
Choose a number: 1
[2025-03-24 19:29:25,192] [INFO] discover_domain: >>>> [1/1] Discovered cluster: vMSC in 24.58s
[2025-03-24 19:29:25,193] [INFO] discover_domain: [2/5] Completed discovery of 1 clusters in vCenter: mcc-vc01.sddc.netapp.com in 24.6s
```

詳しい手順については、 "VCF変換手順"。

NSX VM は vCenter にデプロイされます。

The screenshot shows the vSphere Client interface. On the left, the navigation tree displays a hierarchy: Datacenter > mcc-vc01.sddc.netapp.com > RTP > vMSC. The vMSC node is selected and highlighted in blue. On the right, the main pane is titled 'vMSC' and shows the 'Summary' tab selected. A large section titled 'Cluster Details' provides information about the cluster, including 'Total Processors: 32' and 'Total vMotion Migrations: 5'. Below this, there are icons for hosts, VMs, and datastores.

SDDC マネージャーには、指定された名前で作成された管理ドメインと、データストアとしての NFS が表示されます。

The screenshot shows the 'Workload Domains' section of the SDDC Manager. At the top, there are three horizontal progress bars: CPU (73.44 GHz Total, 5.88 GHz Used), Memory (511.98 GB Total, 470.5 GB Free, 41.48 GB Used), and NFS Storage (3 TB Total, 1.7 TB Used). Below these are two tables. The first table shows domain-level metrics like CPU Usage, Memory Usage, vSAN Storage Usage, and NFS Storage Usage. The second table lists hosts within a cluster, showing their status (ACTIVE), number of hosts (4), and update availability (Up-to-date). A 'Show Or Hide Columns' button is also present.

クラスターを検査すると、NFS データストアの情報が提供されます。

The screenshot shows the 'vMSC' interface under the 'Inventory' section. It displays 'Resource Usage' (CPU: 24.61 GHz, Memory: 89.68 GB) and 'Storage' (NFS: Used 1.73 TB / 3 TB (Free 1.27 TB)). On the right, there is a 'Tags' section where 'vft_imported (VCF Imported Cluster)' is listed. The left sidebar includes links for Dashboard, Solutions, and various management sections like Lifecycle Management, Administration, and Security.

VCFにライセンスを追加する

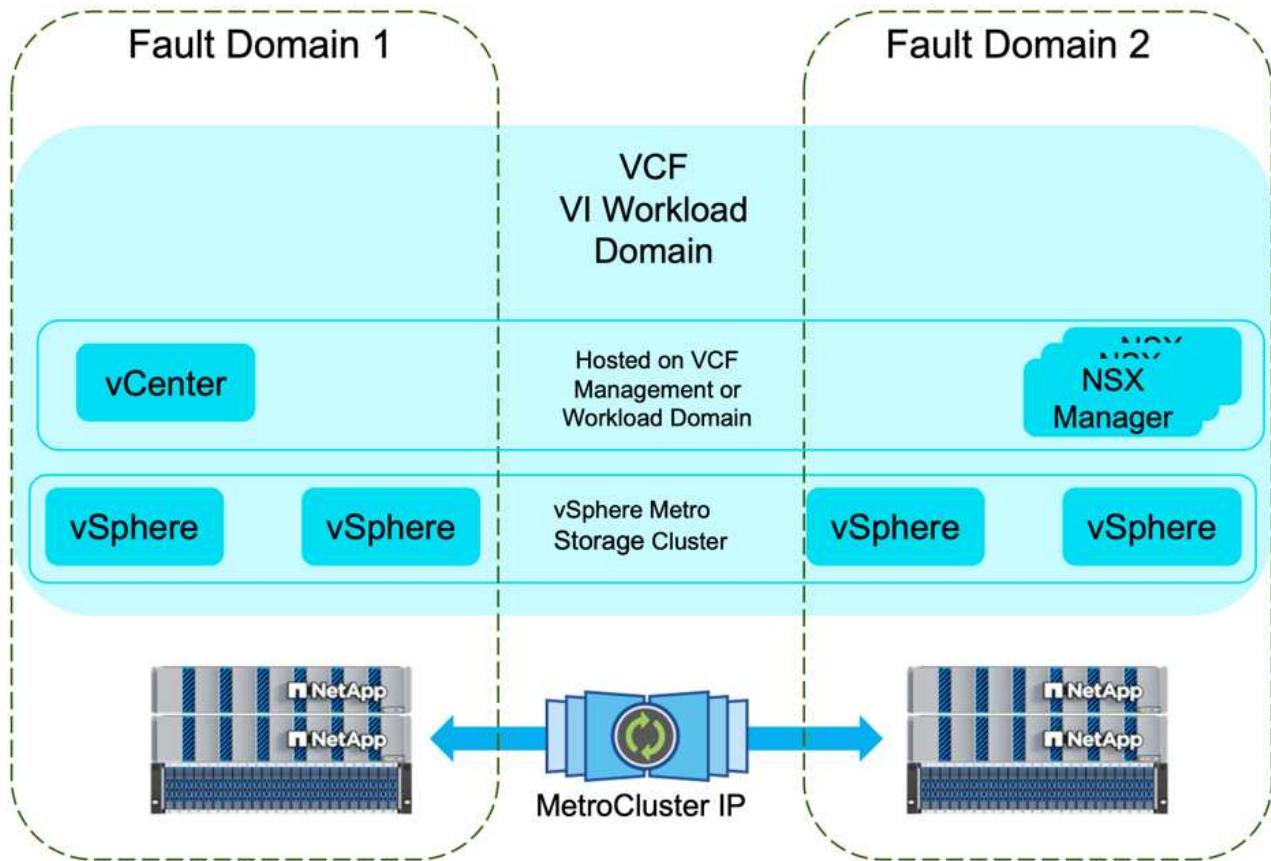
変換が完了したら、環境にライセンスを追加する必要があります。

1. SDDC Manager UI にログインします。
2. ナビゲーションペインで 管理 > ライセンス に移動します。
3. + ライセンス キー をクリックします。
4. ドロップダウンメニューから製品を選択します。
5. ライセンスキーを入力してください。
6. ライセンスの説明を入力します。
7. *[追加]*をクリックします。
8. ライセンスごとにこれらの手順を繰り返します。

MetroClusterを使用して VI ワークロード ドメインのストレッチ クラスタを構成する

このユースケースでは、ONTAP MetroClusterを使用して、NFS をプリンシパル データストアとして拡張 VCF VI ワークロード ドメインを構成する手順について説明します。この手順には、vSphere ホストと vCenter Server のデプロイ、NFS データストアのプロビジョニング、vSphere クラスタの検証、VCF 変換中の NSX の構成、および既存の VCF 管理ドメインへの vSphere 環境のインポートが含まれます。

VCF 上のワークロードは、vSphere Metro Storage Cluster (vMSC) によって保護されます。FC または IP 展開のいずれかを備えたONTAP MetroCluster は、通常、VMFS および NFS データストアのフォールト トランクスを提供するために使用されます。



はじめに

このソリューションでは、ONTAP MetroClusterを使用して、NFSをプリンシパル データストアとしてステッチされたVCF VI ワークロード ドメインを実装する方法を説明します。VI ワークロード ドメインは、SDDC Managerを使用して展開するか、既存のvSphere環境をVI ワークロード ドメインとしてインポートすることができます。

シナリオの概要

このシナリオでは、次の大まかな手順について説明します。

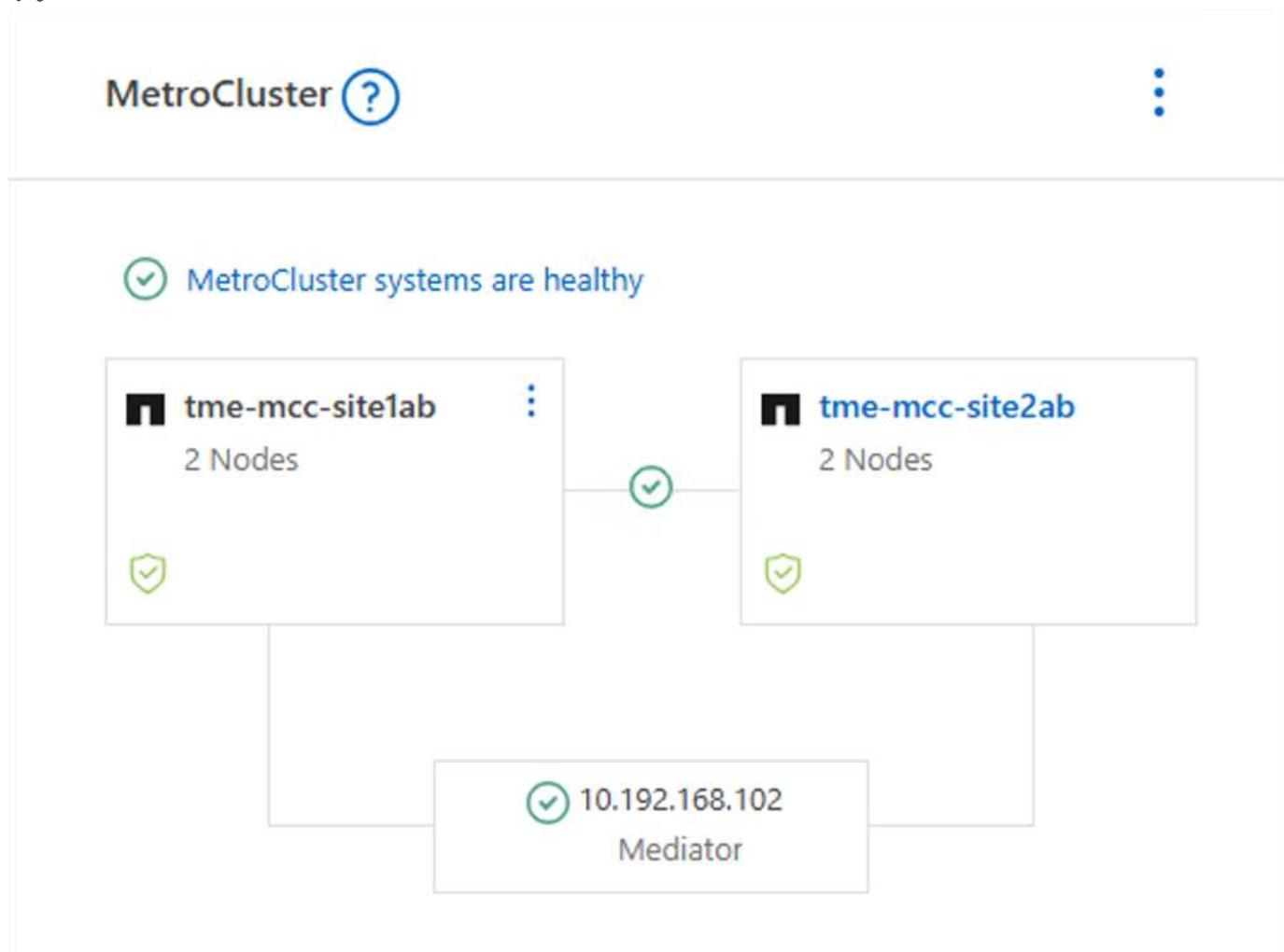
- vSphereホストとvCenterサーバーをデプロイします。
- NFSデータストアをvSphereホストにプロビジョニングします。
- VCFインポートツールを使用して、vSphereクラスターを検証します。
- VCF変換中にNSXを作成するためのJSONファイルを構成します。
- VCFインポートツールを使用して、vSphere8環境をVCF VI ワークロード ドメインとして既存のVCF管理ドメインにインポートします。

前提条件

このシナリオには、次のコンポーネントと構成が必要です。

- ・サポートされているONTAP MetroCluster構成
- ・NFS トラフィックを許可するように構成されたストレージ仮想マシン (SVM)。
- ・NFS トラフィックを伝送し、SVM に関連付けられた IP ネットワーク上に論理インターフェイス (LIF) が作成されています。
- ・ネットワーク スイッチに接続された 4 台の ESXi ホストを備えた vSphere 8 クラスター。
- ・VCF 変換に必要なソフトウェアをダウンロードします。

以下は、MetroCluster構成を示す System Manager のサンプルスクリーンショットです。



両方の障害ドメインからの SVM ネットワークインターフェイスは次のとおりです。

Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node	↑
<input type="text"/>	<input type="button"/>	<input type="text"/> ch-svm	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
lif_ch-svm-mcc02_8775	!	ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a	
lif_ch-svm-mcc01_3118	✓	ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a	
lif_ch-svm-mcc02_9778	!	ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b	
lif_ch-svm-mcc01_6783	✓	ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b	

Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node	↑
<input type="text"/>	<input type="button"/>	<input type="text"/> ch-svm	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
lif_ch-svm-mcc01_3118	!	ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a	
lif_ch-svm-mcc02_8775	✓	ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a	
lif_ch-svm-mcc01_6783	!	ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b	
lif_ch-svm-mcc02_9778	✓	ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b	

[注意] SVM はMetroCluster内の障害ドメインの 1 つでアクティブになります。

NetApp ONTAP System Manager | tme-mcc-site1a

Storage VMs

+ Add

Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
ch-svm-mcc01	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	!
ch-svm-mcc02-mc	Stopped	Sync_destination		Default	n/a	!

NetApp ONTAP System Manager | tme-mcc-site2a

Storage VMs

+ Add

Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
ch-svm-mcc01-mc	Stopped	Sync_destination		Default	n/a	!
ch-svm-mcc02	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	!

参照する "MetroClusterを使用したvMSC"。

vSphere を VCF 5.2 に変換またはインポートする際にサポートされるストレージおよびその他の考慮事項については、以下を参照してください。 "[既存の vSphere 環境を VMware Cloud Foundation に変換またはインポートする前に考慮すべき事項](#)"。

VCF管理ドメインに変換するvSphereクラスタを作成する前に、 "[vSphere クラスタにおける NSX の考慮事項](#)"

必要なソフトウェアについては、 "[既存の vSphere 環境を変換またはインポートするためのソフトウェアをダウンロードする](#)"。

ONTAPストレージシステムの構成については、 "[ONTAP 9ドキュメント](#)" 中心。

VCFの設定方法については、以下を参照してください。 "[VMware Cloud Foundation ドキュメント](#)"。

展開手順

NFSを主データストアとしてVCFストレッチ管理ドメインを展開するには、

次の手順を実行します。

- vSphere ホストと vCenter をデプロイします。
- vSphere クラスターを作成します。
- NFS データストアをプロビジョニングします。
- VCF インポート ツールを vCenter アプライアンスにコピーします。
- VCF インポート ツールを使用して、vCenter アプライアンスの事前チェックを実行します。
- インポート プロセス中にデプロイする NSX クラスタの JSON ファイルを作成します。
- 必要なソフトウェアを SDDC マネージャーにアップロードします。
- vSphere クラスタを VCF VI ワークロード ドメインに変換します。

変換プロセスの概要については、以下を参照してください。 "[vSphere 環境を管理ドメインに変換するか、VMware Cloud Foundation で vSphere 環境を VI ワークロード ドメインとしてインポートする](#)"。

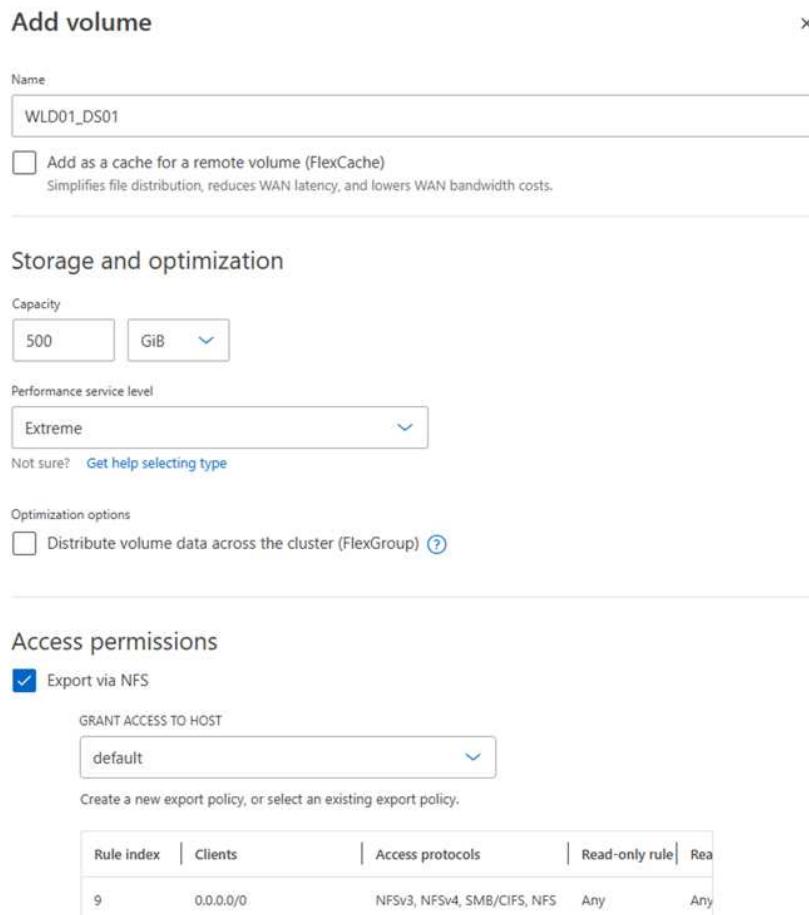
vSphereホストとvCenterを展開する

Broadcom サポート ポータルからダウンロードした ISO を使用してホストに vSphere を展開するか、vSphere ホストの既存の展開オプションを使用します。

NFS データストアをホスト VM にマウントする

この手順では、NFS ボリュームを作成し、それをデータストアとしてマウントして VM をホストします。

1. System Manager を使用してボリュームを作成し、vSphere ホストの IP サブネットを含むエクスポート ポリシーに接続します。



2. vSphere ホストに SSH で接続し、NFS データストアをマウントします。

```
esxcli storage nfs add -c 4 -H 10.192.164.225 -s /WLD01_DS01 -v DS01  
esxcli storage nfs add -c 4 -H 10.192.164.230 -s /WLD01_DS02 -v DS02  
esxcli storage nfs list
```

NFS データストアに vCenter をデプロイします。 vCenter アプライアンスで SSH と Bash シェルが有効になっていることを確認します。

The screenshot shows the vSphere Client interface. On the left, there's a navigation bar with icons for hosts, datastores, and clusters. Below it is a tree view of hosts under 'RTP' (Resource Pool Tree), including 'mcc-vc02.sddc.netapp.com' and its children 'sitea-vs01.sddc.netapp.com', 'sitea-vs02.sddc.netapp.com', 'siteb-vs01.sddc.netapp.com', and 'siteb-vs02.sddc.netapp.com'. The 'siteb-vs02.sddc.netapp.com' node is selected and highlighted in dark blue. To the right, the main pane displays 'Host Details' for 'siteb-vs02.sddc.netapp.com'. The hypervisor is listed as 'VMware ESXi, 8.0.3, 24280767'. Other details include Model: Intel(R) Xeon(R) Gold 5120 C PU @ 2.20GHz, Logical Processors: 12, NICs: 2, Virtual Machines: 1, State: Connected, and Uptime: 19 hours.

vSphere クラスタを作成する

1. vSphere Web クライアントにログインし、NFS VAAI が展開されているホストの 1 つを追加して、データセンターと vSphere クラスターを作成します。クラスター内のすべてのホストを単一のイメージ オプションで管理することを選択しました。[ヒント] クラスター レベルで構成を管理を選択しないでください。詳細については、"[vSphere クラスタにおける NSX の考慮事項](#)"。ONTAP MetroClusterを使用したvMSCのベストプラクティスについては、"[vMSC 設計および実装ガイドライン](#)"
2. 他の vSphere ホストをクラスタに追加します。
3. 分散スイッチを作成し、ポート グループを追加します。
4. "[標準の vSwitch から分散スイッチにネットワークを移行します。](#)"

vSphere 環境を VCF VI ワークロード ドメインに変換する

次のセクションでは、SDDC マネージャをデプロイし、vSphere 8 クラスタを VCF 5.2 管理ドメインに変換する手順について説明します。必要に応じて、詳細については VMware のドキュメントが参照されます。

VMware by Broadcom の VCF インポート ツールは、vCenter アプライアンスと SDDC マネージャの両方で使用されるユーティリティで、構成を検証し、vSphere および VCF 環境の変換およびインポート サービスを提供します。

<https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/vcf-admin/GUID-44CBCB85-C001-41B2-BBB4-E71928B8D955.html> ["VCFインポートツールのオプションとパラメータ"] 。

VCFインポートツールのコピーと抽出

VCF インポート ツールは、vCenter アプライアンスで使用され、vSphere クラスタが VCF 変換またはインポート プロセスに対して正常な状態にあることを検証します。

次の手順を実行します。

1. 次の手順に従ってください ["VCFインポートツールをターゲットのvCenterアプライアンスにコピーします"](#) VMware Docs を参照して、VCF インポート ツールを正しい場所にコピーします。
2. 次のコマンドを使用してバンドルを抽出します。

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

vCenterアプライアンスを検証する

VI ワークロード ドメインとしてインポートする前に、VCF インポート ツールを使用して vCenter アプライアンスを検証します。

1. 次の手順に従ってください ["変換前にターゲット vCenter で事前チェックを実行する"](#) 検証を実行します。

NSX 展開用の JSON ファイルを作成する

vSphere 環境を VMware Cloud Foundation にインポートまたは変換しながら NSX Manager をデプロイするには、NSX デプロイ仕様を作成します。NSX の展開には少なくとも 3 台のホストが必要です。



変換またはインポート操作で NSX Manager クラスタをデプロイする場合、NSX VLAN でバックアップされたセグメントが使用されます。NSX-VLAN でバックアップされたセグメントの制限の詳細については、「既存の vSphere 環境を VMware Cloud Foundation に変換またはインポートする前の考慮事項」セクションを参照してください。NSX-VLAN ネットワークの制限については、以下を参照してください。["既存の vSphere 環境を VMware Cloud Foundation に変換またはインポートする前に考慮すべき事項"](#)。

以下は、NSX デプロイメント用の JSON ファイルの例です。

```
{  
    "deploy_without_license_keys": true,  
    "form_factor": "small",  
    "admin_password": "*****",  
    "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-  
133764.zip",  
    "cluster_ip": "10.61.185.105",  
    "cluster_fqdn": "mcc-wld01-nsx.sddc.netapp.com",  
    "manager_specs": [  
        {  
            "fqdn": "mcc-wld01-nsxa.sddc.netapp.com",  
            "name": "mcc-wld01-nsxa",  
            "ip_address": "10.61.185.106",  
            "gateway": "10.61.185.1",  
            "subnet_mask": "255.255.255.0"  
        },  
        {  
            "fqdn": "mcc-wld01-nsxb.sddc.netapp.com",  
            "name": "mcc-wld01-nsxb",  
            "ip_address": "10.61.185.107",  
            "gateway": "10.61.185.1",  
            "subnet_mask": "255.255.255.0"  
        },  
        {  
            "fqdn": "mcc-wld01-nsxc.sddc.netapp.com",  
            "name": "mcc-wld01-nsxc",  
            "ip_address": "10.61.185.108",  
            "gateway": "10.61.185.1",  
            "subnet_mask": "255.255.255.0"  
        }]  
}
```

JSON ファイルを SDDC マネージャーの vcf ユーザーのホーム フォルダーにコピーします。

SDDC マネージャーにソフトウェアをアップロードする

VCF インポート ツールを vcf ユーザーのホーム フォルダにコピーし、NSX デプロイメント バンドルを SDDC マネージャの /nfs/vmware/vcf/nfs-mount/bundle/ フォルダにコピーします。

見る "必要なソフトウェアを SDDC Manager アプライアンスにアップロードする" 詳細な手順については、こちらをご覧ください。

変換前のvCenterの詳細チェック

管理ドメインの変換操作または VI ワークロード ドメインのインポート操作を実行する前に、既存の vSphere 環境の構成が変換またはインポートに対してサポートされていることを確認するために詳細なチェックを実行する必要があります。。ユーザー vcf として SDDC Manager アプライアンスに SSH 接続します。。VCF インポート ツールをコピーしたディレクトリに移動します。。次のコマンドを実行して、vSphere環境が変換できることを確認します。

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user '' --sso-password '*****' --local-admin-password '*****' --accept-trust
```

```
[root@vc01 ~]# cd vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset/
[vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset]$ python3 vcf_brownfield.py check
[2025-03-23 17:40:44,979] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.2-24494579
[2025-03-23 17:40:44,980] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
usage: vcf_brownfield_check [-h] vcenter VCENTER_IPADDRESS --sso-user SSO_USER --sso-password SSO_PASSWORD [-l local-admin-password LOCAL_ADMIN_PASSWORD] [-s skip-nsx-deployment-checks] [-a accept-trust]
vcf_brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset$ python3 vcf_brownfield.py check --vcenter mcc-vc02.sddc.netapp.com --sso-user administrator@vsphere.local --sso-password '*****' --local-admin-password '*****' --accept-trust
[2025-03-23 17:41:46,001] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.2-24494579
[2025-03-23 17:41:46,001] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
[2025-03-23 17:41:46,080] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:46,081] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:46,081] [INFO] request_helper: Response status from retrieving domain: 200
[2025-03-23 17:41:46,081] [INFO] sddc_manager_helper: Generating SDDC Manager controller token
[2025-03-23 17:41:47,015] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:47,016] [INFO] sddc_manager_helper: Retrieving SDDC Manager controller info
[2025-03-23 17:41:47,016] [INFO] sddc_manager_helper: Using cached SDDC Manager token header
[2025-03-23 17:41:47,511] [INFO] request_helper: Response status from SDDC Manager controller info retrieval: 200
[2025-03-23 17:41:47,511] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:47,504] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:47,595] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:47,661] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:47,661] [INFO] request_helper: Response status from retrieving domain: 200
[2025-03-23 17:41:47,661] [INFO] sddc_manager_helper: Generating SDDC Manager controller token
[2025-03-23 17:41:48,114] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:48,115] [INFO] sddc_manager_helper: Retrieving SDDC Manager trusted certificates
[2025-03-23 17:41:48,115] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:48,115] [INFO] request_helper: Response status from retrieving domain: 200
[2025-03-23 17:41:48,112] [INFO] request_helper: Response status from retrieving trusted certificates: 200
[2025-03-23 17:41:48,418] [INFO] trust_vc01: Retrieved server: mcc-vc02.sddc.netapp.com thumbprint (SHA256): 94:F3:C7:05:DF:FF:E6:C9:6B:86:50:92:3C:B7:7D:15:85:68:38:A1:FD:27:2B:56:60:85:FA:D5:82:AE:3C:46
[2025-03-23 17:41:48,419] [WARNING] trust_vc01: Auto accept trust is turned ON.
[2025-03-23 17:41:48,419] [INFO] vcenter_rest_api_helper: Generating session to vcenter: mcc-vc02.sddc.netapp.com
[2025-03-23 17:41:48,419] [INFO] vcenter_rest_api_helper: Response status from retrieving authentication: 201
[2025-03-23 17:41:48,553] [INFO] vcenter_rest_api_helper: Retrieving trusted root CA chain ID's of vcenter: mcc-vc02.sddc.netapp.com
[2025-03-23 17:41:48,685] [INFO] request_helper: Response status from vcenter trusted root CA chain ID's retrieval: 200
[2025-03-23 17:41:50,086] [INFO] vcenter_rest_api_helper: Retrieving trusted root CA chain with id: 9CA840D66A8C841D51ADACE988EB7F85CAA087F of vcenter: mcc-vc02.sddc.netapp.com
[2025-03-23 17:41:50,086] [INFO] request_helper: Response status from retrieving trusted root CA chain retrieval: 200
[2025-03-23 17:41:50,074] [INFO] sddc_manager_helper: Retrieving SDDC Manager trusted certificates
[2025-03-23 17:41:50,074] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:50,940] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:50,976] [INFO] request_helper: Response status from retrieving trusted certificates: 200
[2025-03-23 17:41:50,985] [INFO] sddc_manager_certificate_utils: Adding new trusted certificate for alias: 9ca840d66a8c841d51adace988eb7f85c4a9b7f with thumbprint: DA:6F:94:90:09:83:66:66:C7:CD:60:49:EC:98:2E:03:EA:AB:57:ED:8B:EC:03:5C:31:09:40:46:40:48:14:FF
[2025-03-23 17:41:50,985] [INFO] sddc_manager_certificate_utils: Adding new trusted certificate for alias: 9ca840d66a8c841d51adace988eb7f85c4a9b7f with thumbprint: 94:F3:C7:05:DF:FF:E6:C9:6B:86:50:92:3C:B7:7D:15:85:68:3B:1A:FD:27:2B:56:60:85:FA:D5:82:AE:3C:46
[2025-03-23 17:41:50,985] [INFO] sddc_manager_helper: Importing trusted certificates to SDDC Manager trust store
[2025-03-23 17:41:50,985] [INFO] request_helper: Response status from certificates import: 200
[2025-03-23 17:41:50,988] [INFO] request_helper: Randomly sleep from certificates refresh: 200
```

vSphere クラスタを VCF VI ワークロード ドメインに変換する

変換プロセスを実行するには、VCF インポート ツールが使用されます。

次のコマンドを実行して、vSphere クラスタを VCF 管理ドメインに変換し、NSX クラスタをデプロイします。

```
python3 vcf_brownfield.py import --vcenter '<vcenter-fqdn>' --sso-user '<sso-user>' --sso-password '*****' --vcenter-root-password '*****' --local-admin-password '*****' --backup-password '*****' --domain-name '<Mgmt-domain-name>' --accept-trust --nsx-deployment-spec-path /home/vcf/nsx.json
```

vSphere ホスト上で複数のデータストアが使用可能な場合でも、どのデータストアをプライマリ データストアとして考慮する必要があるかを指定する必要はありません。

詳しい手順については、["VCF変換手順"](#)。

NSX VM は vCenter にデプロイされます。

The screenshot shows the vSphere Client interface. In the left sidebar, under the 'Datastores' section, there is a tree view. A node labeled 'mcc-vc02.sddc.netapp.com' has a child node 'RTP' expanded, showing several hosts: 'sitea-vs01.sddc.netapp.com', 'sitea-vs02.sddc.netapp.com', 'siteb-vs01.sddc.netapp.com', and 'siteb-vs02.sddc.netapp.com'. The 'siteb-vs02.sddc.netapp.com' node is selected and highlighted with a dark blue background. In the main content area, the title bar shows 'siteb-vs02.sddc.netapp.com' and the 'Actions' menu. Below the title bar, there are tabs for 'Summary', 'Monitor', 'Configure', 'Permissions', 'VMs', and 'Datastores'. The 'Summary' tab is selected. On the right, a 'Host Details' card displays the following information:

Hypervisor:	VMware ESXi, 8.0.3, 24280767
Model:	
Processor Type:	Intel(R) Xeon(R) Gold 5120 C PU @ 2.20GHz
Logical Processors:	12
NICs:	2
Virtual Machines:	2
State:	Connected
Uptime:	20 hours

SDDC マネージャーには、指定された名前と NFS をデータストアとして作成された VI ワークロード ドメインが表示されます。

Workload Domains

Capacity Utilization across Domains

	CPU	Memory	NFS Storage
Total	177.84 GHz Total 35.67 GHz Used	1,023.97 GB Total 184.45 GB Used	3.98 TB Total 1.76 TB Used
Free	138.17 GHz Free	905.52 GB Free	2.22 TB Free

Domain Type CPU Usage Memory Usage vSAN Storage Usage NFS Storage Usage VMFS on FC Storage Usage vVol Storage Usage Configuration Status Cluster Hosts Updates Available

MCC-Mg_	MANAGED	36% (13.16 GHz)	18% (28.69 GB)	- (58%)	- (2%)	- (2%)	ACTIVE	1 Cluster	4	✓ Up-to-date
WLD01	VMWARE	13% (4.64 GHz)	6% (1.82 GB)	- (2%)	- (1%)	- (1%)	ACTIVE	1 Cluster	4	✓ Up-to-date

Show Or Hide Column

2 domains

クラスターを検査すると、NFS データストアの情報が提供されます。

BACK TO WLD01

Stretch Cluster

ACTIONS Managed by Image

ACTIVE

Summary Network Hosts

Resource Usage

CPU	13.16 GHz used of 104.4 GHz (91.24 GHz free)	Memory	28.69 GB used of 511.99 GB (483.3 GB free)
-----	---	--------	---

Tags

- vft_IMPORTED_VCF Imported Cluster

ASSIGN

Storage

NFS

Datastore Name:	D503
Server:	10.192.164.230
Folder:	/WLD01_D503

Datastore Name:	D501
Server:	10.192.164.225
Folder:	/WLD01_D501

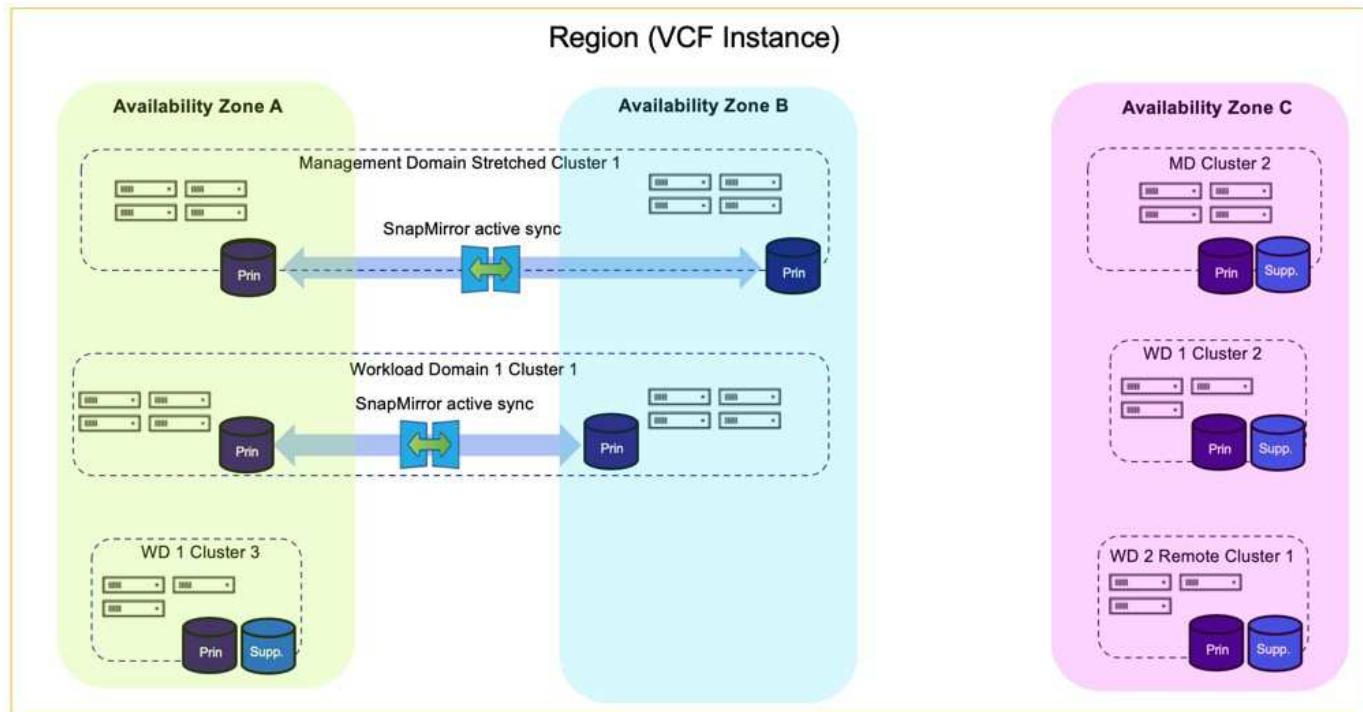
VCFにライセンスを追加する

変換が完了したら、環境にライセンスを追加する必要があります。

1. SDDC Manager UI にログインします。
2. ナビゲーションペインで 管理 > ライセンス に移動します。
3. + ライセンス キー をクリックします。
4. ドロップダウンメニューから製品を選択します。
5. ライセンスキーを入力してください。
6. ライセンスの説明を入力します。
7. *[追加]*をクリックします。
8. ライセンスごとにこれらの手順を繰り返します。

SnapMirror Active Syncを使用してVCF管理ドメインのストレッチクラスタを構成する

このユースケースでは、ONTAP tools for VMware vSphereを使用して、VCF 管理ドメインのストレッチ クラスタを構成する手順について説明します。この手順には、vSphere ホストと vCenter Server の展開、ONTAPツールのインストール、SnapMirror Active Sync によるデータストアの保護、保護されたデータストアへの VM の移行、および補足ストレージの構成が含まれます。

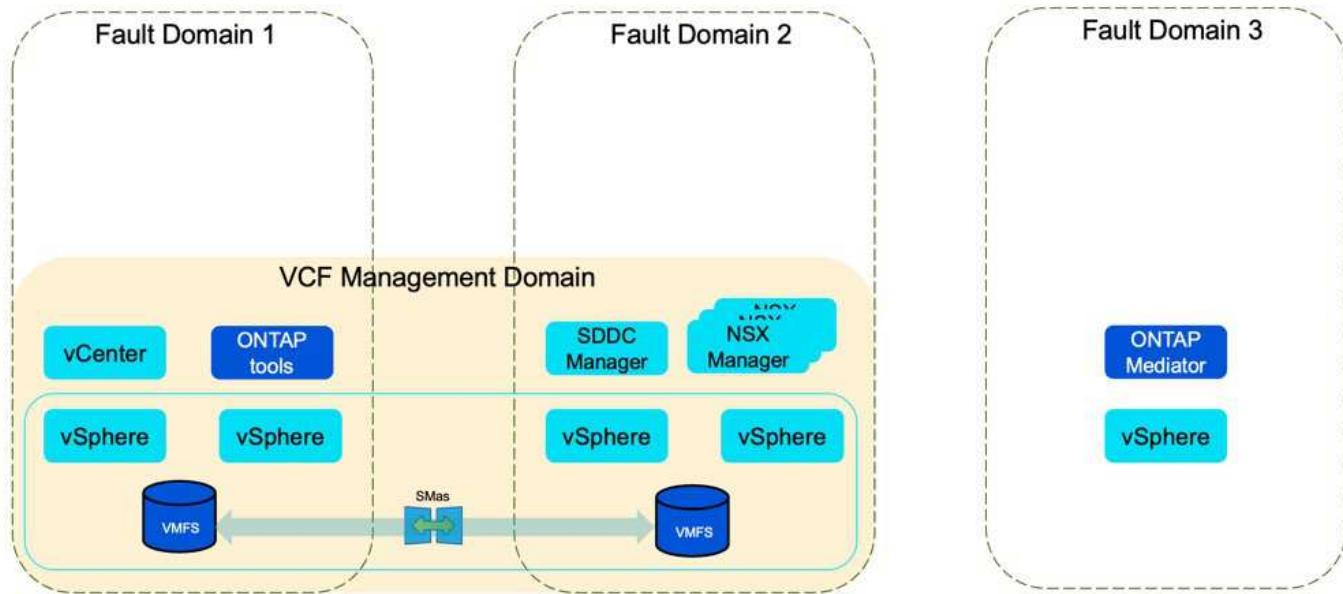


シナリオの概要

ストレッチ クラスター ソリューションは、デフォルトのクラスター、または VCF 管理ドメインまたはワークロード ドメイン内の追加のクラスターに実装できます。FC 上の VMFS は、プリンシパル データストアと

補助データストアの両方でサポートされます。iSCSI 上の VMFS は、補足データストアでのみサポートされます。SnapMirrorアクティブ同期を使用した NVMe-oF 上の VMFS のサポートについては、IMTを参照してください。

VMFS with FC



管理ドメイン上の主ストレージ

VCF 5.2 以降では、VCF インポート ツールを使用して、VSAN なしで管理ドメインを展開できます。VCFインポートツールの変換オプションを使用すると、["既存のvCenterの展開を管理ドメインに導入する"](#)。vCenter 内のすべてのクラスターは管理ドメインの一部になります。

1. vSphereホストを展開する
2. ローカル データストアに vCenter Server を展開します (vCenter は管理ドメインに変換される vSphere ホスト上に共存する必要があります)
3. ONTAP tools for VMware vSphereを導入する
4. VMware vSphere 用SnapCenterプラグインの導入 (オプション)
5. データストアを作成する (FCゾーン構成が設定されている必要があります)
6. vSphere クラスタを保護する
7. VMを新しく作成したデータストアに移行する



クラスタが拡張または縮小されるたびに、クラスタのONTAPツールでホスト クラスタ関係を更新し、ソースまたはターゲットに加えられた変更を示す必要があります。

管理ドメイン上の補助ストレージ

管理ドメインが起動して実行されると、ONTAPツールを使用して追加のデータストアを作成し、整合性グループの拡張をトリガーできます。



vSphere クラスタが保護されている場合、クラスタ内のすべてのデータストアが保護されます。

VCF 環境が Cloud Builder ツールを使用して展開されている場合、iSCSI を使用して補足ストレージを作成するには、ONTAPツールを展開して iSCSI データストアを作成し、vSphere クラスターを保護します。



クラスタが拡張または縮小されるたびに、クラスタのONTAPツールでホスト クラスタ関係を更新し、ソースまたはターゲットに加えられた変更を示す必要があります。

追加情報

ONTAPストレージシステムの構成については、["ONTAP 9ドキュメント"](#)中心。

VCFの設定方法については、以下を参照してください。["VMware Cloud Foundation 5.2 ドキュメント"](#)。

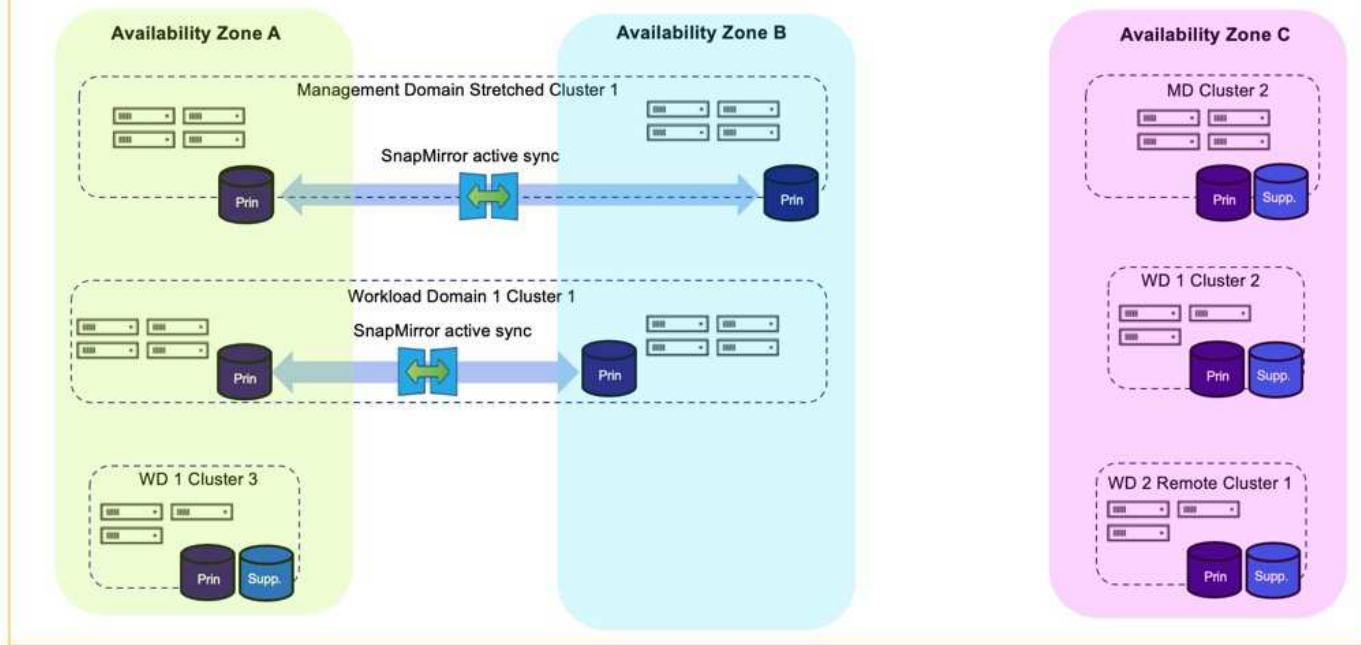
このソリューションのビデオデモ

[ONTAPツールを使用した VCF 用ストレッチ クラスタ](#)

SnapMirror Active Syncを使用してVIワークロードドメインのストレッチクラスタを構成する

このユースケースでは、ONTAP tools for VMware vSphereを使用してSnapMirror Active Sync を使用し、仮想インフラストラクチャ (VI) ワークロード ドメインのストレッチ クラスターを構成する手順について説明します。この手順には、ファイバ チャネル上の VMFS を使用した VCF ワークロード ドメインの作成、ONTAPツールを使用した vCenter の登録、ストレージ システムの登録、および vSphere クラスタの保護が含まれます。

Region (VCF Instance)



シナリオの概要

VCF ワークロード ドメイン上のデータストアは、SnapMirrorアクティブ シンクを使用して保護し、ストレッチ クラスタ ソリューションを提供できます。保護は vSphere クラスタ レベルで有効になり、クラスタ内のすべてのONTAPブロック データストアが保護されます。

ワークロード ドメイン上のプリンシパルストレージ

ワークロード ドメインは、VCF インポート ツールを使用してインポートするか、SDDC マネージャーを使用してデプロイすることで作成できます。SDDC マネージャーを使用して展開すると、既存の環境をインポートするよりも多くのネットワーク オプションが提供されます。

1. FC上のVMFSでワークロード ドメインを作成する
2. "ワークロード ドメイン vCenter をONTAPツール マネージャーに登録して、vCenter プラグインを展開します。"
3. "ONTAPツールにストレージシステムを登録する"
4. "vSphere クラスタを保護する"



クラスタが拡張または縮小されるたびに、クラスタのONTAPツールでホスト クラスタ関係を更新し、ソースまたはターゲットに加えられた変更を示す必要があります。

ワークロードドメインの補助ストレージ

ワークロード ドメインが起動して実行されると、ONTAPツールを使用して追加のデータストアを作成し、整合性グループの拡張をトリガーできます。



vSphere クラスタが保護されている場合、クラスタ内のすべてのデータストアが保護されます。

追加情報

ONTAPストレージシステムの構成については、["ONTAP 9ドキュメント"](#)中心。

VCFの設定方法については、以下を参照してください。["VMware Cloud Foundation ドキュメント"](#)。

このソリューションのビデオデモ

[ONTAPツールを使用した VCF 用ストレッチ クラスタ](#)

VMware vSphere からONTAPデータストアに VM を移行する

VMware vSphere 環境では、仮想マシンをNetApp ONTAP対応データストアに移行することで大きなメリットが得られます。vSAN やサードパーティのストレージシステムから移行する場合でも、既存のインフラストラクチャをアップグレードする場合でも、さまざまな vMotion シナリオと移行戦略を検討して、VM をONTAPデータストアにシームレスに移行します。これにより、ONTAP のエンタープライズ クラスのストレージ機能を活用しながら、ビジネスの継続性が確保されます。

Broadcom の VMware vSphere は、仮想マシンをホストするための VMFS、NFS、および vVol データストアをサポートしています。顧客は、ハイパーコンバージド インフラストラクチャまたは集中型共有ストレージシステムを使用してこれらのデータストアを作成することができます。

お客様は、ONTAPベースのストレージシステムでホスティングすることで、スペース効率の高い仮想マシンのスナップショットやクローン、データセンターやクラウド全体でさまざまな導入モデルを選択できる柔軟性、監視およびアラート ツールによる運用効率、VM データを検査するためのセキュリティ、ガバナンス、オプションのコンプライアンス ツールなどが得られることに価値を見出しています。

ONTAPデータストアでホストされている VM は、SnapCenter Plugin for VMware vSphere (SCV) を使用して保護できます。SCV はストレージ ベースのスナップショットを作成し、リモートONTAPストレージシステムに複製します。復元はプライマリ ストレージ システムまたはセカンダリ ストレージ システムから実行できます。

お客様は、Cloud Insights または Aria Operations、あるいはその両方の組み合わせ、あるいはONTAP API を使用してトラブルシューティング、パフォーマンス監視、レポート、アラート通知機能を実行するその他のサードパーティ ツールを柔軟に選択できます。

お客様は、ONTAP Tools vCenter Plug-in またはその API を使用してデータストアを簡単にプロビジョニングでき、電源がオンの状態でも VM をONTAPデータストアに移行できます。



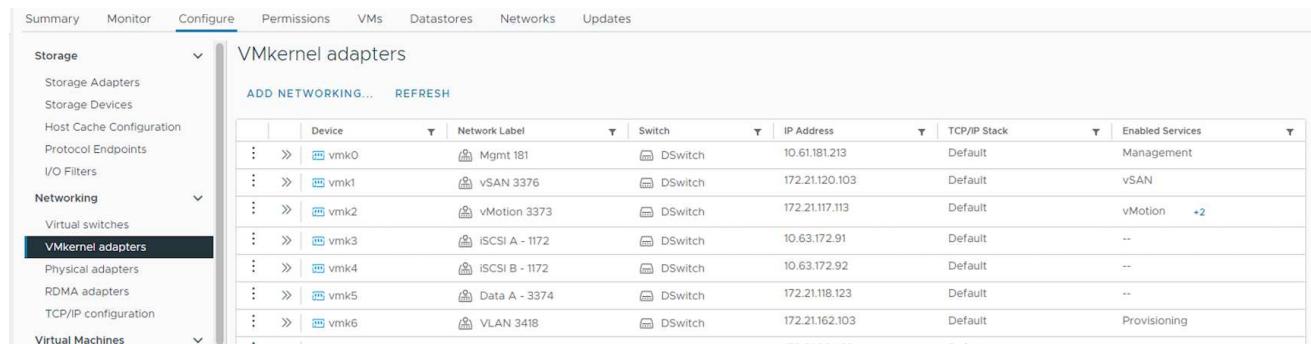
Aria Automation、Tanzu (またはその他の Kubernetes フレーバー) などの外部管理ツールでデプロイされる一部の VM は通常、VM ストレージ ポリシーに依存します。同じ VM ストレージ ポリシー内のデータストア間で移行する場合、アプリケーションへの影響は少なくなります。アプリケーション所有者に確認して、これらの VM を新しいデータストアに適切に移行してください。vSphere 8が導入されました ["遅延に敏感なアプリケーション向けの vSphere vMotion 通知"](#) vMotion 用にアプリケーションを準備します。

ネットワーク要件

vMotion による VM 移行

接続性、フォールトトレランス、およびパフォーマンスの向上を実現するために、ONTAPデータストアにはデュアルストレージネットワークがすでに導入されているものと想定されています。

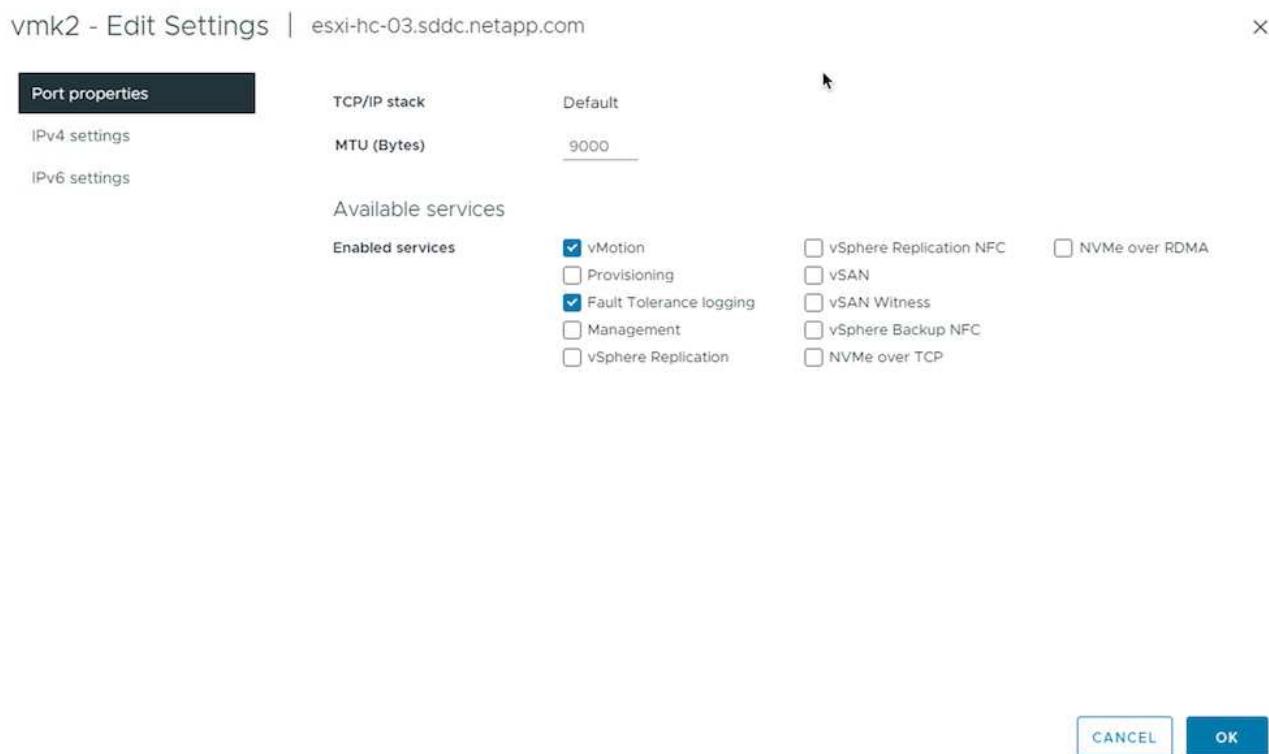
vSphere ホスト間での VM の移行も、vSphere ホストの VMKernel インターフェイスによって処理されます。ホットマイグレーション(VM の電源がオン)の場合、vMotion 対応サービスを備えた VMKernel インターフェイスが使用され、コールドマイグレーション(VM の電源がオフ)の場合、プロビジョニングサービスが有効な VMKernel インターフェイスがデータの移動に使用されます。有効なインターフェースが見つからない場合は、管理インターフェースを使用してデータを移動しますが、これは特定のユースケースでは望ましくない可能性があります。



The screenshot shows the vSphere Web Client interface under the 'Configure' tab. In the left sidebar, 'Networking' is selected, and 'VMkernel adapters' is highlighted. The main pane displays a table titled 'VMkernel adapters' with columns: Device, Network Label, Switch, IP Address, TCP/IP Stack, and Enabled Services. The table lists seven entries: vmk0, vmk1, vmk2, vmk3, vmk4, vmk5, and vmk6. vmk2 is selected, indicated by a blue border around its row.

	Device	Network Label	Switch	IP Address	TCP/IP Stack	Enabled Services
⋮	vmk0	Mgmt 181	DSwitch	10.61.181.213	Default	Management
⋮	vmk1	vSAN 3376	DSwitch	172.21.120.103	Default	vSAN
⋮	vmk2	vMotion 3373	DSwitch	172.21.17.113	Default	vMotion +2
⋮	vmk3	iSCSI A - 1172	DSwitch	10.63.172.91	Default	--
⋮	vmk4	iSCSI B - 1172	DSwitch	10.63.172.92	Default	--
⋮	vmk5	Data A - 3374	DSwitch	172.21.18.123	Default	--
⋮	vmk6	VLAN 3418	DSwitch	172.21.162.103	Default	Provisioning

VMKernel インターフェイスを編集するときに、必要なサービスを有効にするオプションがここにあります。



The screenshot shows the 'Edit Settings' dialog for the vmk2 port. The 'Port properties' tab is selected. Under 'TCP/IP stack', 'Default' is chosen. Under 'MTU (Bytes)', '9000' is entered. In the 'Available services' section, several checkboxes are available:

Enabled services	Options
vMotion	<input checked="" type="checkbox"/>
Provisioning	<input type="checkbox"/>
Fault Tolerance logging	<input checked="" type="checkbox"/>
Management	<input type="checkbox"/>
vSphere Replication	<input type="checkbox"/>
vSphere Replication NFC	<input type="checkbox"/>
vSAN	<input type="checkbox"/>
vSAN Witness	<input type="checkbox"/>
vSphere Backup NFC	<input type="checkbox"/>
NVMe over TCP	<input type="checkbox"/>
NVMe over RDMA	<input type="checkbox"/>

At the bottom right of the dialog are 'CANCEL' and 'OK' buttons.



vMotion および Provisioning VMkernel インターフェイスで使用されるポートグループに、少なくとも 2 つの高速アクティブ アップリンク NIC が使用可能であることを確認します。

VM移行シナリオ

vMotion は、電源状態に関係なく VM を移行するためによく使用されます。特定のシナリオに関する追加の考慮事項と移行手順については、以下を参照してください。



理解する "[vSphere vMotion の VM の条件と制限](#)" VM 移行オプションに進む前に。

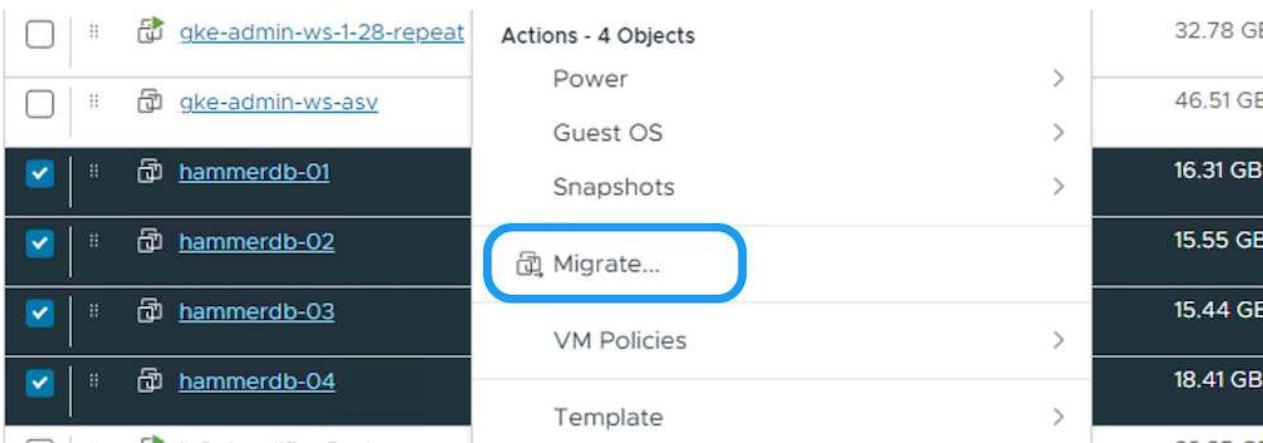
特定の vSphere データストアからの VM の移行

UI を使用して VM を新しいデータストアに移行するには、以下の手順に従います。

1. vSphere Web Client で、ストレージ インベントリからデータストアを選択し、VM タブをクリックします。



2. 移行する必要がある VM を選択し、右クリックして [移行] オプションを選択します。



3. ストレージのみを変更するオプションを選択し、「次へ」をクリックします。

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only
Migrate the virtual machines to another host or cluster.

Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL **NEXT**

4. 必要な VM ストレージ ポリシーを選択し、互換性のあるデータストアを選択します。[Next]をクリックします。

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE **CONFIGURE PER DISK**

Select virtual disk format: Thin Provision

VM Storage Policy: NetApp Storage

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free
ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB
DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB
destination	Incompatible	250 GB	31.8 MB	249.97 GB
DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB
E13A400_ISCSI	Incompatible	2 TB	858.66 GB	1.85 TB

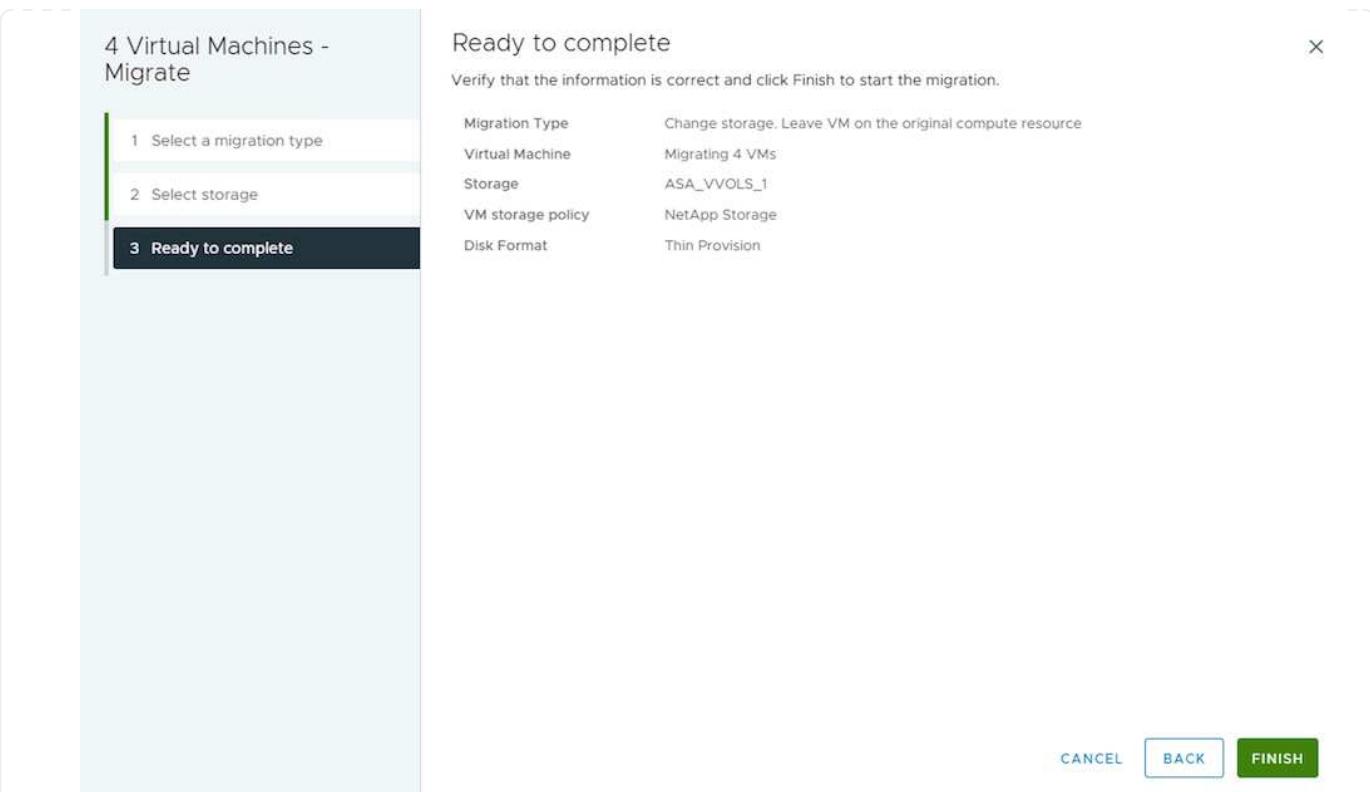
Manage Columns Items per page: 5 1 - 5 of 14 items < < 1 / 3 > >

Compatibility

✓ Compatibility checks succeeded.

CANCEL **BACK** **NEXT**

5. 確認して「完了」をクリックします。



PowerCLI を使用して VM を移行するためのサンプル スクリプトを次に示します。

```

#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific datastore
$vm = Get-DataStore 'vSanDatastore' | Get-VM Har*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration

```

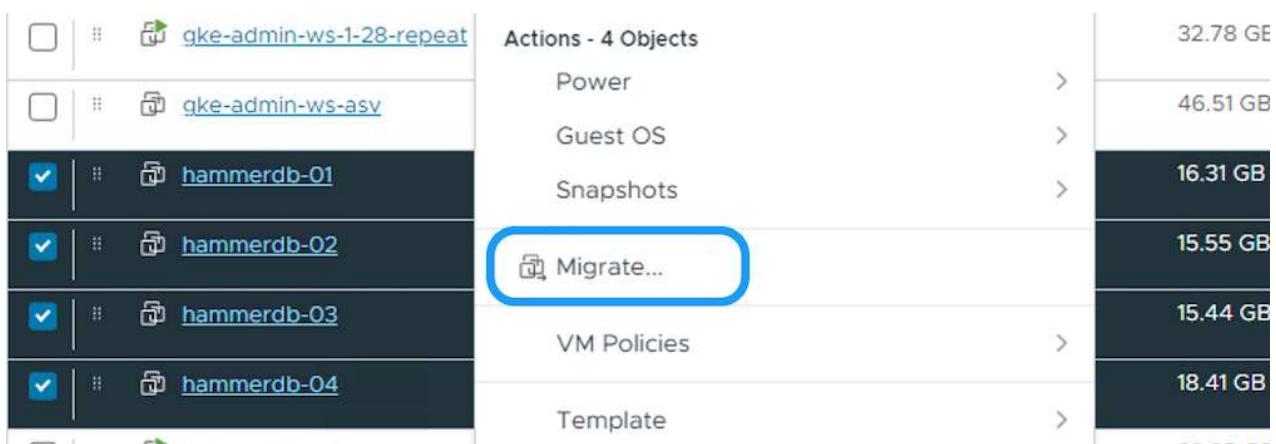
同じ vSphere クラスタ内の VM の移行

UI を使用して VM を新しいデータストアに移行するには、以下の手順に従います。

1. vSphere Web Client で、ホストおよびクラスタ インベントリからクラスタを選択し、VM タブをクリックします。



2. 移行する必要がある VM を選択し、右クリックして [移行] オプションを選択します。



3. ストレージのみを変更するオプションを選択し、「次へ」をクリックします。

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only

Migrate the virtual machines to another host or cluster.

Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

- 必要な VM ストレージ ポリシーを選択し、互換性のあるデータストアを選択します。[Next]をクリックします。

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE

CONFIGURE PER DISK

Select virtual disk format

Thin Provision

VM Storage Policy

NetApp Storage

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free
ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB
DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB
destination	Incompatible	250 GB	31.8 MB	249.97 GB
DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB
E13A400_ISCSI	Incompatible	2 TB	858.66 GB	1.85 TB

Compatibility

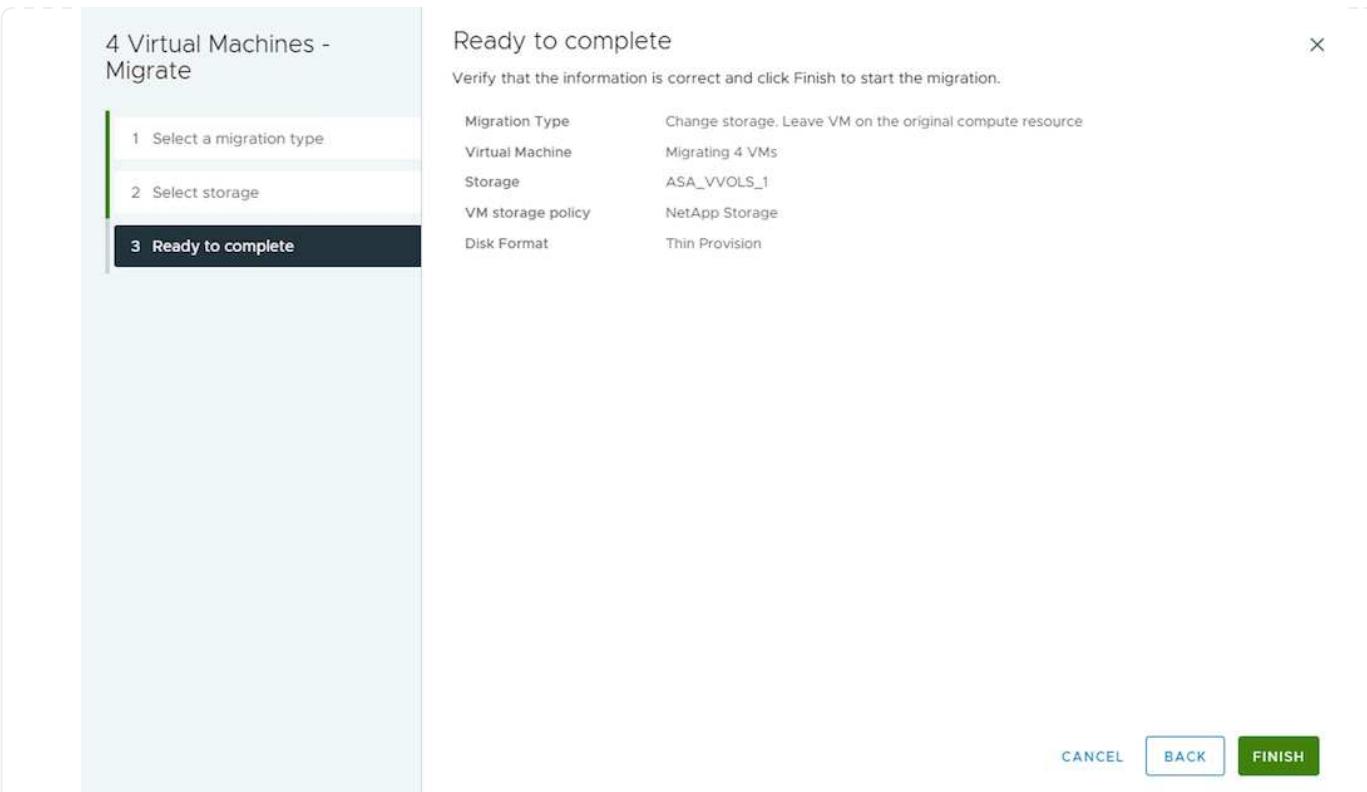
✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

- 確認して「完了」をクリックします。



PowerCLI を使用して VM を移行するためのサンプル スクリプトを次に示します。

```

#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-c101' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration

```



データストア クラスターが完全に自動化されたストレージ DRS (Dynamic Resource Scheduling) で使用されており、両方の (ソースとターゲット) データストアが同じタイプ (VMFS/NFS/vVol) である場合は、両方のデータストアを同じストレージ クラスターに保持し、ソースでメンテナンス モードを有効にして、ソース データストアから VM を移行します。エクスペリエンスは、コンピューティング ホストがメンテナンスのために処理される方法と同様になります。

複数の vSphere クラスタ間での VM の移行



参照する "CPU 互換性と vSphere Enhanced vMotion 互換性" ソース ホストとターゲット ホストの CPU ファミリまたはモデルが異なる場合。

UI を使用して VM を新しいデータストアに移行するには、以下の手順に従います。

1. vSphere Web Client で、ホストおよびクラスタ インベントリからクラスタを選択し、VM タブをクリックします。

The screenshot shows the vSphere Client interface. The top navigation bar has tabs for Summary, Monitor, Configure, Permissions, Hosts, VMs, Datastores, Networks, and Updates. The 'VMs' tab is currently selected. Below the navigation bar, there is a search bar labeled 'Search in all environments'. The main content area displays a tree view of hosts and clusters. Under the 'vcf-m01-vc01.sddc.netapp.com' cluster, there are two datacenters: 'vcf-m01-dc01' and 'vcf-m01-cl01'. The 'vcf-m01-cl01' node is expanded, showing several virtual machines. One specific VM, 'vcf-m01-cl01', is highlighted with a dark blue background.

2. 移行する必要がある VM を選択し、右クリックして [移行] オプションを選択します。

The screenshot shows the 'Actions - 4 Objects' menu open over a list of selected VMs. The selected VMs are 'hammerdb-01', 'hammerdb-02', 'hammerdb-03', and 'hammerdb-04'. The 'Migrate...' option is highlighted with a blue rounded rectangle. To the right of the menu, there is a vertical list of storage resources with their capacities: '32.78 GB', '46.51 GB', '16.31 GB', '15.55 GB', '15.44 GB', and '18.41 GB'. The 'hammerdb-01' VM is currently assigned to the '16.31 GB' storage resource.

3. コンピューティングリソースとストレージを変更するオプションを選択し、[次へ] をクリックします。

4 Virtual Machines - Migrate

1 Select a migration type

- 2 Select a compute resource
- 3 Select storage
- 4 Select networks
- 5 Select vMotion priority
- 6 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

- Change compute resource only
Migrate the virtual machines to another host or cluster.
- Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. 移行する適切なクラスターに移動して選択します。

4 Virtual Machines - Migrate

1 Select a migration type

- 2 Select a compute resource
- 3 Select storage
- 4 Select networks
- 5 Select vMotion priority
- 6 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

- vcf-m01-vc01.sddc.netapp.com
 - vcf-m01-dc01
- vcf-wkld-vc01.sddc.netapp.com
 - vcf-wkld-01-DC
 - IT-INF-WKLD-01

Compatibility

- ✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. 必要な VM ストレージ ポリシーを選択し、互換性のあるデータストアを選択します。[Next]をクリックします。

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select folder

5 Select networks

6 Select vMotion priority

7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE CONFIGURE PER DISK

Select virtual disk format Thin Provision

VM Storage Policy NFS

Name	Storage Compatibility	Capacity	Provisioned	Free
VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB
VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB
VCF_WKLD_03_ISCSI	Incompatible	3 TB	858.61 GB	2.85 TB
vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
vcf-wkld-esx03-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB

Manage Columns

Items per page: 10 7 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

6. ターゲット VM を配置する VM フォルダーを選択します。

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select folder

5 Select networks

6 Select vMotion priority

7 Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

- vcf-wkld-01-DC
- Discovered virtual machine**
- vCLS

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

7. ターゲット ポート グループを選択します。

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder
- 5 Select networks**
- 6 Select vMotion priority
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.
Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
SDDC-DPortGroup-VM-Mgmt	4 VMs / 4 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-0

ADVANCED >>

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. 確認して「完了」をクリックします。

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select storage
- 3 Ready to complete**

Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL BACK FINISH

PowerCLI を使用して VM を移行するためのサンプル スクリプトを次に示します。

```

#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-c101' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to another cluster and Datastore specified by Policy
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)

#When Portgroup is specific to each cluster, replace the above command
with
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy) -PortGroup
(Get-VirtualPortGroup 'VLAN 101')

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration

```

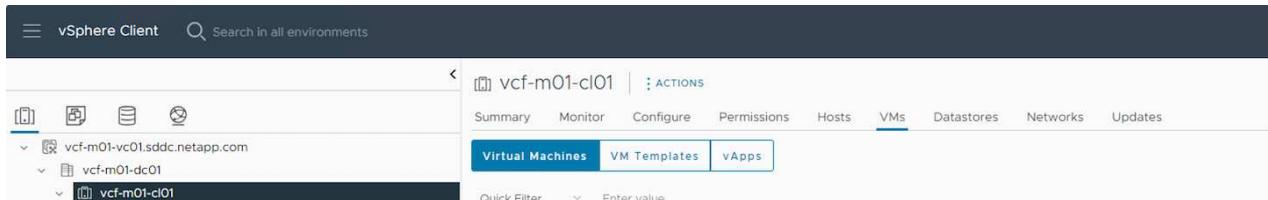
同じ SSO ドメイン内の vCenter サーバー間での VM の移行

以下の手順に従って、同じ vSphere Client UI にリストされている新しい vCenter サーバーに VM を移行します。

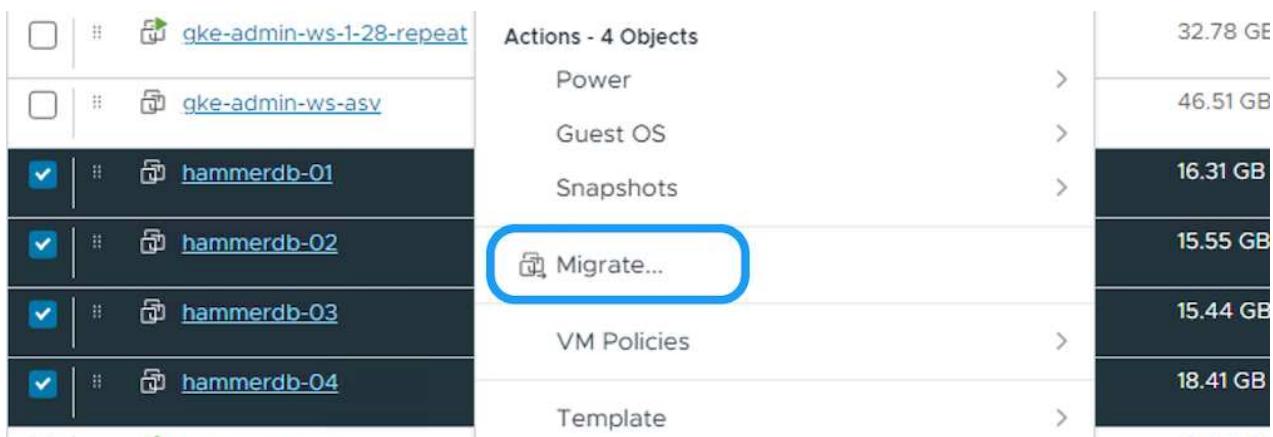


ソースおよびターゲットのvCenterバージョンなどの追加要件については、以下を確認してください。 "vCenter Server インスタンス間の vMotion の要件に関する vSphere ドキュメント"

1. vSphere Web Client で、ホストおよびクラスタインベントリからクラスタを選択し、VM タブをクリックします。



2. 移行する必要がある VM を選択し、右クリックして [移行] オプションを選択します。



3. コンピューティングリソースとストレージを変更するオプションを選択し、[次へ] をクリックします。

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only
Migrate the virtual machines to another host or cluster.

Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL NEXT

4. ターゲット vCenter サーバーでターゲット クラスタを選択します。

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

v vcf-m01-vc01.sddc.netapp.com
 > vcf-m01-dc01

v vcf-wkld-vc01.sddc.netapp.com
 > vcf-wkld-01-DC
 > IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

5. 必要な VM ストレージ ポリシーを選択し、互換性のあるデータストアを選択します。[Next]をクリックします。

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select folder

5 Select networks

6 Select vMotion priority

7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE CONFIGURE PER DISK

Select virtual disk format Thin Provision

VM Storage Policy NFS

Name	Storage Compatibility	Capacity	Provisioned	Free
VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB
VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB
VCF_WKLD_03_ISCSI	Incompatible	3 TB	858.61 GB	2.85 TB
vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
vcf-wkld-esx03-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB

Manage Columns

Items per page: 10 7 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

6. ターゲット VM を配置する VM フォルダーを選択します。

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select folder

5 Select networks

6 Select vMotion priority

7 Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

- vcf-wkld-01-DC
- Discovered virtual machine**
- vCLS

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

7. ターゲット ポート グループを選択します。

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder
- 5 Select networks**
- 6 Select vMotion priority
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.
Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
SDDC-DPortGroup-VM-Mgmt	4 VMs / 4 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-0

ADVANCED >>

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. 移行オプションを確認し、「完了」をクリックします。

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select storage
- 3 Ready to complete**

Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL BACK FINISH

PowerCLI を使用して VM を移行するためのサンプル スクリプトを次に示します。

```

#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' -server $sourcevc | Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration

```

異なる SSO ドメイン内の vCenter サーバー間での VM の移行



このシナリオでは、vCenter サーバー間に通信が存在することを前提としています。それ以外の場合は、以下にリストされているデータセンター間の場所のシナリオを確認してください。前提条件については、["高度な Cross vCenter vMotion に関する vSphere ドキュメント"](#)

UI を使用して VM を別の vCenter サーバーに移行するには、以下の手順に従います。

1. vSphere Web Client で、ソース vCenter サーバーを選択し、[VM] タブをクリックします。

The screenshot shows the vSphere Web Client interface. The top navigation bar has tabs for Summary, Monitor, Configure, Permissions, Datacenters, Hosts & Clusters, VMs (which is highlighted in blue), Datastores, Networks, Linked vCenter Server Systems, Extensions, and Updates. Below the navigation bar, there's a search bar and a user profile icon. The main content area shows a tree view of datacenters: 'vcsa-hc.sddc.netapp.com' (selected) > 'Datacenter' > 'HMC Cluster'. At the bottom, there are 'Quick Filter' and 'Enter value' fields.

2. 移行する必要がある VM を選択し、右クリックして [移行] オプションを選択します。

The screenshot shows the vSphere Web Client interface with multiple VMs selected on the left (hammerdb-01, hammerdb-02, hammerdb-03, hammerdb-04). A context menu is open over them, titled 'Actions - 4 Objects'. The menu items are: Power, Guest OS, Snapshots, Migrate..., VM Policies, and Template. The 'Migrate...' option is highlighted with a blue oval. To the right of the menu, there's a table showing memory usage: 32.78 GE, 46.51 GB, 16.31 GB, 15.55 GB, 15.44 GB, and 18.41 GB.

3. オプション「Cross vCenter Server エクスポート」を選択し、「次へ」をクリックします。

4 Virtual Machines - Migrate

1 Select a migration type

- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

- Change compute resource only
Migrate the virtual machines to another host or cluster.
- Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.
 Keep VMs on the source vCenter Server (performs a VM clone operation).

CANCEL NEXT



VM はターゲットの vCenter サーバーからインポートすることもできます。その手順については、"高度な Cross vCenter vMotion を使用して仮想マシンをインポートまたはクローンする"

4. vCenter 資格情報の詳細を入力し、「ログイン」をクリックします。

Migrate | SQLSRV-05

1 Select a migration type

2 Select a target vCenter Server

- 3 Select a compute resource
- 4 Select storage
- 5 Select networks
- 6 Ready to complete

Select a target vCenter Server

Export Virtual Machines to the selected target vCenter Server.

SAVED VCENTER SERVERS **NEW VCENTER SERVER**

vCenter Server address: vcf-wkld-vc01.sddc.netapp.com
vCenter Server FQDN or IP address

Username: administrator@vcf.local
example@domain.local

Password: Password

Save vCenter Server address

LOGIN

CANCEL BACK NEXT

5. vCenter ServerのSSL証明書のサムプリントを確認して承認します。

Security Alert

X

Unable to verify the authenticity of the external vCenter Server.

The SHA1 thumbprint of the vCenter Server certificate is:



17:42:0C:EB:82:1E:A9:86:F1:E0:70:93:AD:EB:8C:0F:27:41:F1:30

Connect anyway?

Click Yes if you trust the vCenter Server.

Click No to cancel connecting to the vCenter Server.

NO

YES

6. ターゲット vCenter を展開し、ターゲット コンピューティング クラスターを選択します。

Migrate | SQLSRV-05

1 Select a migration type

2 Select a target vCenter Server

3 Select a compute resource

4 Select storage

5 Select networks

6 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

VM ORIGIN ⓘ

vcf-wkld-vc01.sddc.netapp.com

vcf-wkld-01-DC

IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

7. VMストレージポリシーに基づいてターゲットデータストアを選択します。

Migrate | SQLSRV-05

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE CONFIGURE PER DISK

Select virtual disk format Thin Provision

VM Storage Policy NFS

Name	Storage Compatibility	Capacity	Provisioned	Free	Total
VCF_WKLD_01	Compatible	5 TB	5.93 GB	5 TB	N/A
VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	24 MB	2.93 TB	N/A
VCF_WKLD_03_JSCSI	Incompatible	3 TB	1.35 TB	2.59 TB	N/A
vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	N/A
vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	N/A

Manage Columns Items per page 10 7 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. ターゲットVMフォルダーを選択します。

Migrate | SQLSRV-05

Select folder

Select the destination virtual machine folder for the virtual machine migration.

>Select location for the virtual machine migration.

vcf-wkld-01-DC

- Discovered virtual machine
- Oracle
- SQL Server**
- vCLS

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

9. 各ネットワークインターフェイスカードマッピングのVMポートグループを選択します。

Migrate | SQLSRV-05

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select folder
- 6 Select networks**
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.

VM ORIGIN ⓘ

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
» Mgmt 181	1 VMs / 1 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-01-p
» Data A - 3374	1 VMs / 1 Network adapters	vcf-wkld-01-iscsi-a
» Data B - 3375	1 VMs / 1 Network adapters	vcf-wkld-01-iscsi-b

3 items

ADVANCED >

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

10. 確認して「完了」をクリックすると、vCenter サーバー間で vMotion が開始されます。

Migrate | SQLSRV-05

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select folder
- 6 Select networks
- 7 Ready to complete**

Ready to complete

Verify that the information is correct and click Finish to start the migration.

VM ORIGIN ⓘ

Migration Type	Change compute resource and storage
Virtual Machine	SQLSRV-05
vCenter	vcf-wkld-vc01.sddc.netapp.com
Folder	SQL Server
Cluster	IT-INF-WKLD-01
Networks	Virtual network adapters from 3 networks will be reassigned to new destination networks
Storage	VCF_WKLD_01
VM storage policy	NFS
Disk Format	Thin Provision

CANCEL BACK FINISH

PowerCLI を使用して VM を移行するためのサンプル スクリプトを次に示します。

```

#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'Source Cluster' -server $sourcevc | Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration

```

データセンター間のVMの移行

- NSX フェデレーションまたはその他のオプションを使用してレイヤー 2 トラフィックがデータセンター全体に拡張される場合は、vCenter サーバー間で VM を移行する手順に従います。
- HCXはさまざまな "移行の種類" ダウンタイムなしで VM を移動するための、データセンター間のレプリケーション アシスト vMotion が含まれます。
- "Site Recovery Manager (SRM)" 通常は災害復旧を目的としており、ストレージアレイベースのレプリケーションを利用した計画的な移行にもよく使用されます。
- 繙続的データ保護 (CDP) 製品では、"vSphere API for IO (VAIO)" データを傍受し、そのコピーをリモート ロケーションに送信して、RPO がほぼゼロのソリューションを実現します。
- バックアップおよびリカバリ製品も利用できます。しかし、多くの場合、RTO が長くなります。
- "BlueXP災害復旧サービス (DRaaS)"ストレージアレイベースのレプリケーションを利用し、特定のタスクを自動化してターゲットサイトで VM を回復します。

ハイブリッドクラウド環境でのVMの移行

- ・ "ハイブリッドリンクモードを構成する"そして、以下の手順に従ってください"同じ SSO ドメイン内の vCenter サーバー間での VM の移行"
- ・ HCXはさまざまな "移行の種類"電源がオンの状態で VM を移動する、データセンター間のレプリケーションアシスト vMotion など。
 - "TR 4942: VMware HCX を使用してワーカーロードを FSx ONTAP データストアに移行する"
 - "TR-4940: VMware HCX を使用してワーカーロードを Azure NetApp Files データストアに移行する - クイックスタート ガイド"
 - "VMware HCX を使用して Google Cloud VMware Engine 上の Google Cloud Google Cloud NetApp Volumes データストアにワーカーロードを移行する - クイックスタート ガイド"
- ・ "BlueXP 災害復旧サービス (DRaaS)"ストレージアレイベースのレプリケーションを利用し、特定のタスクを自動化してターゲットサイトで VM を回復します。
- ・ サポートされている継続的データ保護 (CDP) 製品では、"vSphere API for IO (VAIO)"データを傍受し、そのコピーをリモート ロケーションに送信して、RPO がほぼゼロのソリューションを実現します。



ソース VM がブロック vVol データストアに存在する場合、SnapMirrorを使用して、サポートされている他のクラウドプロバイダーのAmazon FSx ONTAPまたはCloud Volumes ONTAP (CVO) に複製し、クラウドネイティブ VM で iSCSI ボリュームとして使用できます。

VM テンプレートの移行シナリオ

VM テンプレートは、vCenter Server またはコンテンツ ライブラリによって管理できます。VM テンプレート、OVF および OVA テンプレート、その他の種類のファイルの配布は、ローカル コンテンツ ライブラリに公開することによって処理され、リモート コンテンツ ライブラリはそれをサブスクライブできます。

- ・ vCenter インベントリに保存されている VM テンプレートは VM に変換でき、VM 移行オプションを使用できます。
- ・ OVF および OVA テンプレート、コンテンツ ライブラリに保存されている他の種類のファイルは、他のコンテンツ ライブラリに複製できます。
- ・ コンテンツ ライブラリ VM テンプレートは任意のデータストアでホストでき、新しいコンテンツ ライブラリに追加する必要があります。

データストアでホストされている VM テンプレートの移行

1. vSphere Web Client で、VM およびテンプレート フォルダー ビューの VM テンプレートを右クリックし、VM に変換するオプションを選択します。

The screenshot shows the vSphere Client interface. On the left, there's a navigation sidebar with categories like RTP, SQL Server, Tanzu, and Templates. Under Templates, several items are listed: ESXi-8.0-U1a, vdbench template, win10-template (which is selected and highlighted in blue), win2019 template, and win2022-template. The main pane displays 'VM Template Details' for 'win10-template'. It shows the Guest OS as Microsoft Windows, VMware Tools as 'Not running, version:123i', and other details like DNS Name (1) as DESKTOP-HGNBVPL. A context menu is open over the template, with the 'Convert to Virtual Machine...' option highlighted by a blue oval. Other options in the menu include New VM from This Template..., Clone to Template..., Clone to Library..., Move to folder..., Rename..., Edit Notes..., Tags & Custom Attributes, Add Permission..., Alarms, Remove from Inventory, Delete from Disk, vSAN, and NetApp ONTAP tools.

2. VM として変換されたら、VM 移行オプションに従います。

コンテンツライブラリアイテムの複製

1. vSphere Web Clientでコンテンツライブラリを選択します



vSphere Client



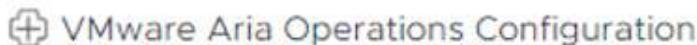
Search in all en



Home



Content Libraries



- 複製したいアイテムがあるコンテンツライブラリを選択します
- アイテムを右クリックし、「アイテムの複製」をクリックします。

vSphere Client

CL01

ACTIONS

Summary Templates Other Types Subscriptions

Quick Filter Enter value.

Name	Guest OS	Stored Locally	Security Compliant	Size	Last Modified Date	Last Sync Date	Content Library	UUID	Content Version	Description
NetApp ONTAP-9.12.1.5	Yes	Yes	16.97 MB	04/03/2024, 5:08:57 PM			CL01	urn:vmedia:com.vmware.content.library.item-9e40-e203-414f-642-sec9-fbeec94e36-3190-4650-8239-45f7-86ad-2fffc3f1461d8	2	

Edit Notes...
Rename...
Tags >
Delete



アクションメニューを使用する場合は、アクションを実行するための正しいターゲット オブジェクトがリストされていることを確認してください。

- 対象のコンテンツライブラリを選択し、[OK] をクリックします。

Clone Library Item | NetApp ONTAP-9.12.1.5

Name NetApp ONTAP-9.12.1.5

Notes

Select a content library where to clone the library item.

Name	Notes	Creation Date
CL01		9/26/2023, 5:02:03 PM
CL02		4/1/2024, 12:37:51 PM

CANCEL OK

- アイテムがターゲット コンテンツライブラリで使用可能であることを確認します。



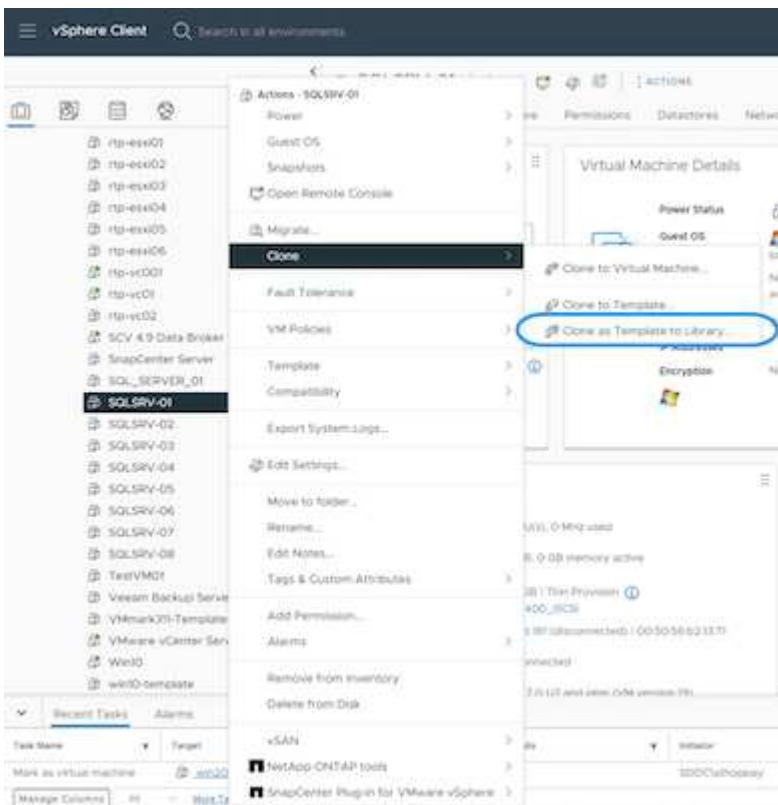
以下は、コンテンツ ライブラリ CL01 から CL02 にコンテンツ ライブラリ項目をコピーするサンプル PowerCLI スクリプトです。

```
#Authenticate to vCenter Server(s)
$sourcevc = Connect-VIServer -server 'vcenter01.domain' -force
$targetvc = Connect-VIServer -server 'vcenter02.domain' -force

#Copy content library items from source vCenter content library CL01 to
target vCenter content library CL02.
Get-ContentLibraryItem -ContentLibrary (Get-ContentLibrary 'CL01' -Server
$sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-
ContentLibraryItem -ContentLibrary (Get-ContentLibrary 'CL02' -Server
$targetvc)
```

コンテンツライブラリにテンプレートとしてVMを追加する

1. vSphere Web ClientでVMを選択し、右クリックしてライブラリのテンプレートとしてクローンを選択します。



VM テンプレートをライブラリにクローンするように選択した場合、VM テンプレートとしてではなく、OVF および OVA テンプレートとしてのみ保存できます。

2. テンプレートタイプがVMテンプレートとして選択されていることを確認し、ウィザードの回答に従って操作を完了します。

SQLSRV-01 - Clone Virtual Machine To Template

1 Basic information

Template type: VM Template

Name: SQLSRV-01

Notes:

Select a folder for the template

- vcsa-hc.sddc.netapp.com
- Datacenter

CANCEL NEXT



コンテンツライブラリのVMテンプレートの詳細については、"vSphere VM 管理ガイド"

ユースケース

サードパーティのストレージシステム (vSAN を含む) からONTAPデータストアへの移行。

- ONTAPデータストアがプロビジョニングされている場所に基づいて、上記のVM移行オプションを選択します。

vSphere の以前のバージョンから最新バージョンへの移行。

- インプレース アップグレードが不可能な場合は、新しい環境を立ち上げて上記の移行オプションを使用できます。



クロス vCenter 移行オプションでは、ソースでエクスポート オプションが使用できない場合はターゲットからインポートします。その手順については、"高度な Cross vCenter vMotion を使用して仮想マシンをインポートまたはクローンする"

VCF ワークロード ドメインへの移行。

- 各 vSphere クラスタからターゲット ワークロード ドメインに VM を移行します。



ソース vCenter 上の他のクラスタにある既存の VM とのネットワーク通信を許可するには、ソース vCenter vSphere ホストをトランスポート ゾーンに追加して NSX セグメントを拡張するか、エッジで L2 ブリッジを使用して VLAN での L2 通信を許可します。NSX のドキュメントを確認する "["ブリッジ用のエッジVMを構成する"](#)"

参考資料

- ["vSphere 仮想マシンの移行"](#)
- ["vSphere vMotion を使用した仮想マシンの移行"](#)
- ["NSX フェデレーションにおける Tier-0 ゲートウェイ構成"](#)
- ["HCX 4.8 ユーザーガイド"](#)
- ["VMware Live Recovery ドキュメント"](#)
- ["VMware 向けBlueXP disaster recovery"](#)

NFSストレージ向けの自律型ランサムウェア防御

ランサムウェアができるだけ早く検出することは、その拡散を防ぎ、コストのかかるダウンタイムを回避するために重要です。効果的なランサムウェア検出戦略には、ESXi ホストおよびゲスト VM レベルで複数の層の保護を組み込む必要があります。ランサムウェア攻撃に対する包括的な防御を実現するために複数のセキュリティ対策が実装されていますが、ONTAP を使用すると、全体的な防御アプローチにさらに多くの保護層を追加できます。いくつかの機能を挙げると、スナップショット、自律ランサムウェア保護、改ざん防止スナップショットなどがあります。

上記の機能が VMware と連携して、ランサムウェアからデータを保護し、回復する方法を見てみましょう。vSphere とゲスト VM を攻撃から保護するには、セグメント化、エンドポイントでの EDR/XDR/SIEM の利用、セキュリティ アップデートのインストール、適切な強化ガイドラインの遵守など、いくつかの対策を講じることが不可欠です。データストアに存在する各仮想マシンは、標準のオペレーティング システムもホストします。多層ランサムウェア保護戦略の重要な要素である、エンタープライズ サーバー マルウェア対策製品スイートがインストールされ、定期的に更新されていることを確認します。これに加えて、データストアに電力を供給する NFS ボリューム上で Autonomous Ransomware Protection (ARP) を有効にします。ARP は、ボリューム ワークロード アクティビティとデータ エントロピーを調べる組み込みオンボックス ML を活用して、ランサムウェアを自動的に検出します。ARP は、ONTAP の組み込み管理インターフェイスまたはシステム マネージャを通じて設定でき、ボリュームごとに有効化されます。

The screenshot shows the ONTAP System Manager interface. On the left, there's a navigation sidebar with sections like DASHBOARD, INSIGHTS, STORAGE (Overview, Volumes, LUNs, NVMe namespaces, Consistency groups, Shares, QoS, Quotas, Storage VMs, Tiers), NETWORK, EVENTS & JOBS, PROTECTION, HOSTS, and CLUSTER. The main area is titled 'Volumes' and shows a list of volumes with their names: 'Src_NFS_Vol01', 'NFSARDemo02', 'NFSDD502ARP', 'nimpra', 'SQLDatavol', 'Src_25G_Vol01', 'Src_iSCSI_D05', 'Src_iSCSI_D502', 'Src_iSCSI_D504', and 'Src_NFS_Vol01' again at the bottom. Below the list, there's a 'Security' tab selected, showing sub-options: Overview, Snapshot copies, SnapMirror, Back up to cloud, Security (selected), File system, and Quota Reports. Under the Security tab, there's a section titled 'Anti-ransomware' with a status switch labeled 'Disabled'. A tooltip says: 'Enable anti-ransomware if you're running applications on this NFS volume.' At the bottom right of the main area, there's a link to 'Activate Windows'.

i 現在テクニカル プレビュー段階にある新しいNetApp ARP/AIでは、学習モードは必要ありません。代わりに、AIを活用したランサムウェア検出機能により、すぐにアクティブ モードに移行できます。

i ONTAP Oneでは、これらすべての機能セットが完全に無料です。ライセンスの障壁を気にすることなく、NetAppの強力なデータ保護、セキュリティ、およびONTAPが提供するすべての機能にアクセスできます。

アクティブ モードになると、ランサムウェアである可能性のある異常なボリューム アクティビティの検索を開始します。異常なアクティビティが検出されると、自動スナップショット コピーが直ちに作成され、ファイル感染にできるだけ近い復元ポイントが提供されます。ARPは、暗号化されたボリュームに新しい拡張子が追加されたり、ファイルの拡張子が変更されたりしたときに、VMの外部にある NFS ボリューム上の VM 固有のファイル拡張子の変更を検出できます。

ONTAP System Manager

DASHBOARD

INSIGHTS

STORAGE

- Overview
- Volumes
- LUNs
- NVMe namespaces
- Consistency groups
- Shares
- Quotas
- Storage VMs
- Tiers

NETWORK

EVENTS & JOBS

PROTECTION

HOSTS

CLUSTER

Volumes

+ Add Delete Protect More

Src_NFS_DS04 All Volumes

Overview Snapshot copies SnapMirror Back up to cloud Security File system Quota Reports

Anti-ransomware

Enabled in active mode

Pause anti-ransomware Event severity settings

Volume's workload characteristics

Learned statistics LARGEST PERCENT OF HIGH ENTROPY DATA

Surge statistics LARGEST PERCENT OF HIGH ENTROPY DATA

Configure workload characteristics

HIGHEST RATE OF FILE CREATION 16 files/minute HIGHEST RATE OF FILE CREATION

ランサムウェア攻撃が仮想マシン(VM)をターゲットとし、VM外部に変更を加えずにVM内部のファイルを変更する場合、たとえば.txt、.docx、.mp4ファイルなどのファイルタイプの場合、VMのデフォルトのエントロピーが低いと、Advanced Ransomware Protection(ARP)は依然として脅威を検出します。このシナリオではARPが保護スナップショットを作成しますが、VM外部のファイル拡張子が改ざんされていないため、脅威アラートは生成されません。このようなシナリオでは、防御の初期層で異常が特定されますが、ARPはエントロピーに基づいてスナップショットを作成するのに役立ちます。

詳細については、「ARPと仮想マシン」セクションを参照してください。["ARPの使用例と考慮事項"](#)。

ランサムウェア攻撃は、ファイルからバックアップデータに移行し、ファイルの暗号化を開始する前にバックアップやスナップショットのリカバリポイントを削除しようとすることで、これらをターゲットとするケースが増えています。しかし、ONTAPでは、プライマリシステムまたはセカンダリシステムに改ざん防止スナップショットを作成することでこれを防ぐことができます。["NetAppスナップショットコピーのロック"](#)。

vSphere Client

Search in all environments

Administrator@HMDCI.LOCAL

Snapshot Center Plugin for VMware vSphere INSTANCE 172.21.164.1

Policies

Create Edit Remove

Name: Po_NFSDS04

Description: description

Frequency: Daily

Locking Period: Enable Snapshot Locking

Retention: Days to keep: 7

Replication: Update SnapMirror after backup

Update SnapVault after backup

Snapshot label: Daily

Warning for ONTAP 9.12.1 and below version

Snapshot	Filter	Retention Period
Yes	No	1 Day
No	10 days	10 days
Yes	7 days	7 days
Yes	7 days	7 days

Recent Tasks

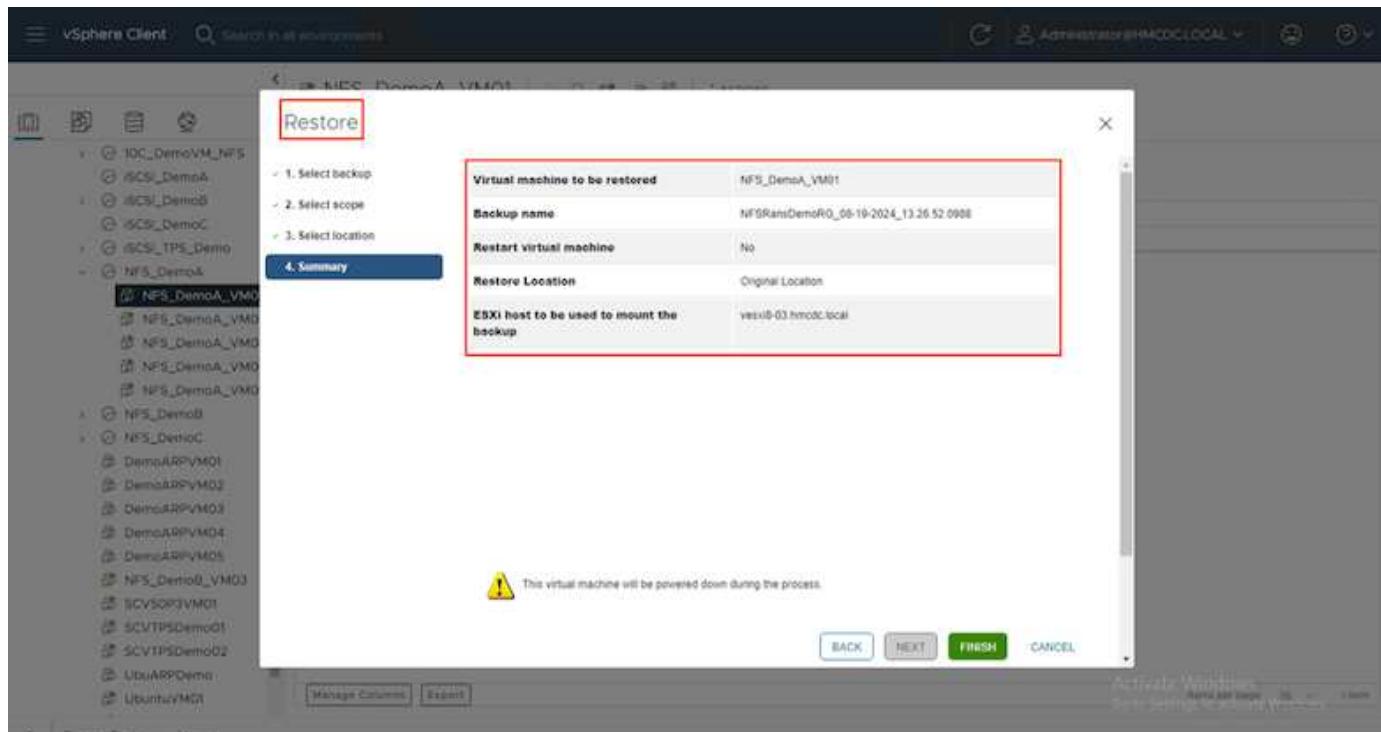
Remove snapshots: /dev/NFS-Demo_VMDK

Revert snapshots: /dev/NFS-Demo_VMDK

Register virtual machine: /dev/VMWARE-0000

CANCEL UPDATE

これらのスナップショット コピーは、ランサムウェア攻撃者や不正な管理者によって削除または変更できないため、攻撃後でも利用できます。データストアまたは特定の仮想マシンが影響を受ける場合、SnapCenter は数秒で仮想マシンのデータを回復し、組織のダウンタイムを最小限に抑えることができます。



上記は、ONTAPストレージが既存の技術にレイヤーを追加し、環境の将来性を強化する方法を示しています。

詳細については、以下のガイダンスをご覧ください。["ランサムウェアに対するNetAppソリューション"](#)。

これらすべてをSIEMツールと調整して統合する必要がある場合は、BlueXP ransomware protectionなどのオフタップサービスを使用できます。ランサムウェアからデータを保護するように設計されたサービスです。このサービスは、Oracle、MySQL、VMデータストア、オンプレミスのNFSストレージ上のファイル共有などのアプリケーションベースのワークロードを保護します。

この例では、NFSデータストア「Src_NFS_DS04」はBlueXP ransomware protectionを使用して保護されています。

NetApp BlueXP

Ransomware protection Dashboard Protection Alerts Recovery Reports Free trial (55 days left) - view details ▾

Workloads (10)

Workload	Type	Connector	Importance	Protection st...	Detection sta...	Detection pol...	Snapshot an...	Backup destina...	Action
Src_nfs_ds02	VM datastore	G1SABXPConn	Critical	Protected	Learning mode	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	<button>Edit protection</button>
Braas_src_test_3130	VM file share	G1SABXPConn	Standard	At risk	None	None	None	n/a	<button>Protect</button>
Nfsd02arp_804	VM file share	G1SABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	<button>Edit protection</button>
Oreas_src_7027	VM file share	G1SABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	<button>Protect</button>
Src_nfs_vol1_7948	VM file share	G1SABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	<button>Protect</button>
Src_nfs_ds03	VM datastore	G1SABXPConn	Standard	At risk	None	None	SnapCenter for VMw...	netapp-backup-add...	<button>Protect</button>
Src_nfs_ds04	VM datastore	G1SABXPConn	Standard	Protected	Active	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	<button>Edit protection</button>
Src_nfs_ds04	File share	G1SABXPConn	Critical	Protected	Active	rps-policy-primary	BlueXP backup and ...	netapp-backup-ba3...	<button>Edit protection</button>
Testvol_1787	File share	G1SABXPConn	Standard	Protected	Learning mode	rps-policy-primary	None	netapp-backup-ba3...	<button>Edit protection</button>
Nfsardemo02_1419	File share	G1SABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	<button>Edit protection</button>

NetApp BlueXP

Ransomware protection Dashboard Protection Alerts Reports

Protected Protection health Edit protection

0 Alerts

Not marked for recovery Recovery

Protection

VM datastore Storage

These policies managed by SnapCenter for VMware will not be modified by applying a detection policy to this workload.

Pol_NFSDS04 Snapshot policy

1 Year Daily LTR Backup policy

Location: urn:scv:scvmUI:Resou...
vCenter server: vvcasl-01.hmcidc.local
Connector: G1SABXPConn

Cluster id: add38d26-348c-11ef-8...
Working Env name: NTAP915_Src
Storage VM name: svm_NFS
Volume name: Src_NFS_DS04
Used size: 29 GiB

BlueXP ransomware protectionの設定の詳細については、以下を参照してください。["BlueXP ransomware protectionを設定する"](#)そして["BlueXP ransomware protection設定を構成する"](#)。

例を挙げてこれを詳しく説明してみましょう。このチュートリアルでは、データストア「Src_NFS_DS04」が影響を受けます。

VM Disk files under Ransomware Attack and VM affected

Name	Size	Modified	Type	Path
SO_Demo8/VMscoreBoard	8 KB	08/05/2024, 1:02:39 AM	File	[Src_NFS_DS04] NFS_Demo8_VM01/ScoreBoard
SO_DMH/VM.scoreboard	8 KB	08/09/2024, 9:57:11 AM	File	[Src_NFS_DS04] NFS_Demo8_VM01/VM/DMH
NFS_Demo8_VM01-0024d79/vmem	4,194,304 KB	07/31/2024, 5:59:48 AM	File	[Src_NFS_DS04] NFS_Demo8_VM01/VMDK/vmem
NFS_Demo8_VM01-0024d79/vmog	0.09 KB	08/05/2024, 1:02:39 AM	File	[Src_NFS_DS04] NFS_Demo8_VM01/VM/VM01-0024d79/vmog
NFS_Demo8_VM01-akuu.xml	0.01 KB	08/05/2024, 1:02:46 AM	File	[Src_NFS_DS04] NFS_Demo8_VM01/VM/akuu.xml
NFS_Demo8_VM01-vmem	0.48 KB	07/12/2024, 9:02:56 AM	Non-volatile Memory File	[Src_NFS_DS04] NFS_Demo8_VM01/VM/VM01-vmem
NFS_Demo8_VM01.vmd	0.04 KB	08/09/2024, 9:08:46 AM	File	[Src_NFS_DS04] NFS_Demo8_VM01/VM/VM01.vmd
NFS_Demo8_VM01.vmem	3.4 KB	08/09/2024, 9:08:46 AM	Virtual Machine	[Src_NFS_DS04] NFS_Demo8_VM01/VMDK/vmem
NFS_Demo8_VM01.vmdk	0.48 KB	08/05/2024, 1:02:39 AM	File	[Src_NFS_DS04] NFS_Demo8_VM01/VMDK/vmdk
NFS_Demo8_VM01.vmxnfs	0.07 KB	08/09/2024, 9:31:22 AM	File	[Src_NFS_DS04] NFS_Demo8_VM01/VFS/VM01.vmxnfs
NFS_Demo8_VM01-3-ctx.vmxnfs	940.54 KB	08/09/2024, 9:31:22 AM	File	[Src_NFS_DS04] NFS_Demo8_VM01/VFS/VM01-3-ctx.vmxnfs
NFS_Demo8_VM01-3-fatal.vmxnfs	10,485.380 KB	08/09/2024, 9:31:22 AM	File	[Src_NFS_DS04] NFS_Demo8_VM01/VFS/VM01-3-fatal.vmxnfs
NFS_Demo8_VM01-3.vmxnfs	0.64 KB	08/09/2024, 9:31:22 AM	File	[Src_NFS_DS04] NFS_Demo8_VM01/VFS/VM01-3.vmxnfs

ARP は検出するとすぐにボリュームのスナップショットをトリガーしました。

NetApp Snapshot triggered during suspected abnormal activity

Name	Snapshot copy creation time	Snapshot restore size
snapmirror.42ad5432-3537-11ef-bd57-00a0b8f6d346_21 59491296 2024-08-09_160500	Aug/9/2024 9:05 AM	50.5 GiB
Anti_ransomware_backup.2024-08-09_1326	Aug/9/2024 6:26 AM	44.5 GiB
RG_NFSDS04_08-09-2024_08.08.16.0981	Aug/9/2024 5:08 AM	27.8 GiB
RG_NFSDS04_08-09-2024_07.54.48.0205	Aug/9/2024 4:55 AM	27.7 GiB
	Aug/9/2024 3:27 AM	27.6 GiB
RG_NFSDS04_08-09-2024_06.27.18.0190	Aug/9/2024 3:27 AM	27.6 GiB
RG_NFSDS04_08-09-2024_05.00.28.0747	Aug/9/2024 2:00 AM	27.7 GiB

The screenshot shows the ONTAP System Manager dashboard. A prominent blue banner at the top right reads "ARP detects abnormal activity on the Volume". Below the banner, the "SRC_NFS_DS04" volume is selected. The "Security" tab is active. A section titled "Anti-ransomware" shows a status of "Enabled in active mode" with a toggle switch. It displays a warning message: "Abnormal volume activity detected on 09 Aug 2024 5:53 AM" and lists "10 files" as suspected ransomware files. A button labeled "View suspected file type" is present. To the right, there are links to "Pause anti-ransomware" and "Event severity settings". The left sidebar includes sections for DASHBOARD, INSIGHTS, STORAGE (Overview, Volumes, LUNs, NVMe namespaces, Consistency groups, Shares, Qtree, Quotas, Storage VMs, Tiers), NETWORK, EVENTS & JOBS, PROTECTION, HOSTS, and CLUSTER.

フォレンジック分析が完了すると、SnapCenterまたはBlueXP ransomware protectionを使用して、復元を迅速かつシームレスに実行できます。SnapCenterを使用して、影響を受ける仮想マシンに移動し、復元する適切なスナップショットを選択します。

The screenshot shows the vSphere Client interface. A blue banner at the top right says "Select the VM to be restored within the backup". On the left, the inventory tree shows various hosts and datastores, including "NFS_DemoB_VM01". The main pane shows the "Backups" tab for "NFS_DemoB_VM01". It displays a table of entities included in the backup, with one row highlighted. The table columns are: Entity Name, Guaranteed, UUID, and Location. The highlighted row is "NFS_DemoB_VM01" with a UUID of "50125ad9-70c4-218e-82db-a40d14932ba0". The location is listed as "[Src_NFS_DS04] NFS_DemoB_VM01 NFS_DemoB_VM01.vmx". The bottom right corner of the interface has a watermark "Activate Windows".

このセクションでは、BlueXP ransomware protectionが、VM ファイルが暗号化されたランサムウェアインシデントからの回復をどのように調整するかについて説明します。



VM がSnapCenterによって管理されている場合、BlueXP ransomware protectionはVM 整合性プロセスを使用して VM を以前の状態に復元します。

1. BlueXP ransomware protectionにアクセスすると、BlueXP ransomware protectionダッシュボードにアラートが表示されます。
2. アラートをクリックすると、生成されたアラートの特定のボリューム上のインシデントを確認できます。

The screenshot shows the 'Protection View specific to the NFS Volume' for the workload 'Src_NFS_DS04'. The top navigation bar includes 'NetApp BlueXP', 'Ransomware protection', 'Dashboard', 'Protection' (selected), 'Alerts', 'Recovery', and 'Reports'. The main area displays the following information:

- Protection:** Standard Importance, Protected.
- Alerts:** 1 alert, View alerts.
- Storage:** Cluster id: add38d26-348c-11ef-8..., Working Env name: NTAP915_src, Storage VM name: svm_NFS, Volume name: Src_NFS_DS04, Used size: 29 GiB.

Below these sections, there are two dropdown menus under 'Protection':

- Pol_NFS0504 Snapshot policy
- 1 Year Daily LTR Backup policy

3. 「復元が必要」を選択して、ランサムウェア インシデントを復旧準備完了としてマークします（インシデントが中和された後）。

The screenshot shows the 'Alerts' view for the alert 'alert2198'. The top navigation bar includes 'NetApp BlueXP', 'Ransomware protection', 'Dashboard', 'Protection', 'Alerts' (selected), and 'Recovery'. The main area displays the following information:

- Alert Details:** Workload: Src_NFS_DS04, Location: urn:scv:scvmlj:Resou..., Type: VM datastore, Connector: G1SABXPConn.
- Incident Summary:** 1 Potential attack, First detected: 4 hours ago, Impacted data: 29 GiB, Impacted files: 10.
- Incident Table:** A table titled 'incident (1) | All selected' showing one row for 'Inc1820' with details: Incident ID: Inc1820, Volume: Src_NFS_DS04, SVM: svm_NFS, Working environment: NTAP915_src, Type: Potential attack, Status: New, First detected: 4 hours ago, Evidence: 1 new extensions detected, Automated responses: 2 Snapshot copies.



インシデントが誤検知であることが判明した場合、アラートは無視できます。

4. [リカバリ] タブに移動し、[リカバリ] ページのワークロード情報を確認して、「復元が必要」状態のデータストアボリュームを選択し、[復元] を選択します。

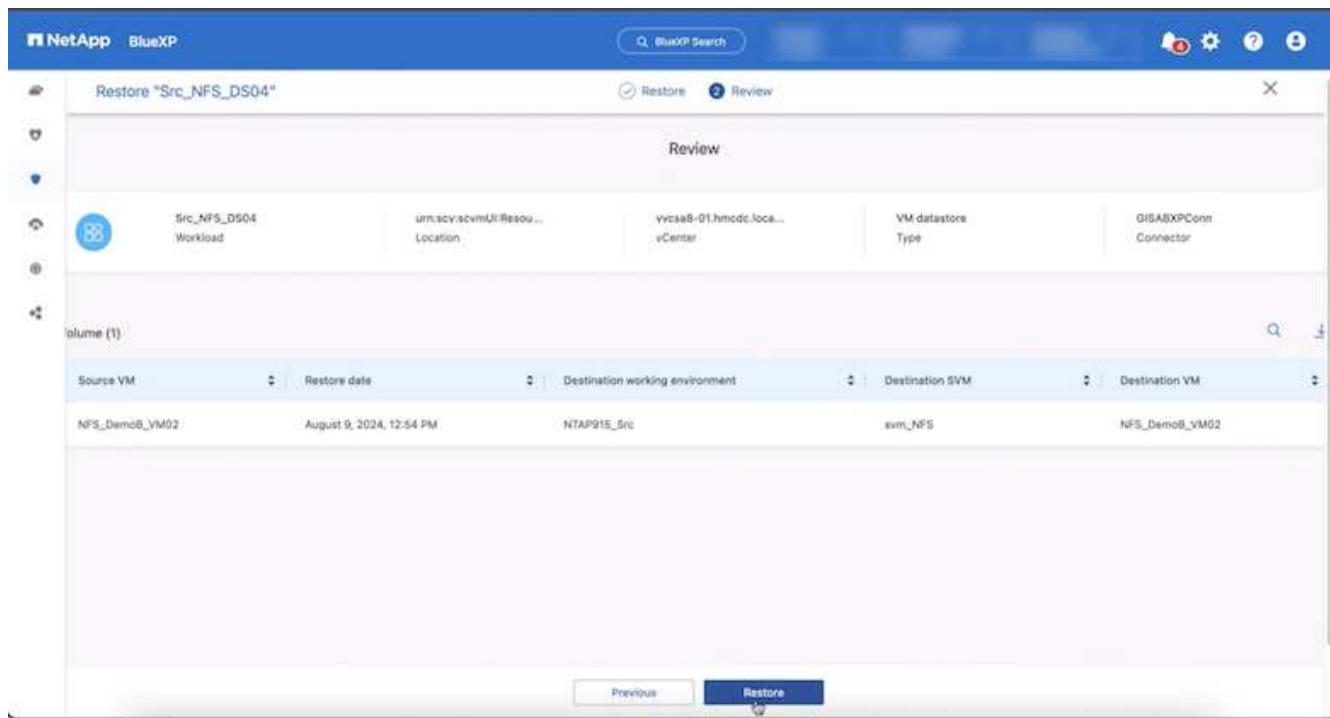
The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'NetApp BlueXP', 'BlueXP Search', and various icons. The main area is titled 'Ransomware protection' and displays three status boxes: 'Restore needed' (2 Data), 'In progress' (0 Data), and 'Restored' (0 Data). Below this is a table titled 'Workloads (2)'. The columns include Workload, Location, Type, Connector, Snapshot and backup, Recovery status, Progress, Importance, Total data, and Action. The first workload, 'Nfsds02arrj_004', is listed with 'Restore needed' status and a 'Restore' button. The second workload, 'Src_nfs_ds04', is also listed with 'Restore needed' status and a 'Restore' button.

5. この場合、復元範囲は「VM ごと」です（SnapCenter for VMs の場合、復元範囲は「VM ごと」です）。

The screenshot shows the 'Restore "Src_NFS_DS04"' dialog. At the top, there are 'Restore' and 'Review' buttons. A blue header bar says 'Select "Restore Point" and VM needed to be restored'. The main area has tabs for 'Restore scope' (selected) and 'VM-consistent'. Under 'Source', it says 'First attack reported August 9, 2024, 1:53 PM'. The 'Restore points (6)' table lists six restore points:

Restore point	Type	Date
RG_NFSDS04_08-09-2024_06.08.16.0981	snapshot	August 9, 2024, 1:08 PM
RG_NFSDS04_08-09-2024_07.54.48.0206	snapshot	August 9, 2024, 12:54 PM
RG_NFSDS04_08-09-2024_06.27.18.0190	snapshot	August 9, 2024, 11:27 AM
RG_NFSDS04_08-09-2024_05.00.28.0747	snapshot	August 9, 2024, 10:00 AM

6. データの復元に使用する復元ポイントを選択し、「宛先」を選択して「復元」をクリックします。



7. 上部のメニューから [回復] を選択し、[回復] ページでワーク LOAD を確認します。ここで、操作のステータスがさまざまな状態を遷移します。復元が完了すると、VM ファイルは以下のように復元されます。

Name	Type	Size	Last Modified
NFS_DemoB_VM02.vmdk	File	8.794.304 KB	07/02/2024, 07:53:48 AM
NFS_DemoB_VM02-00000001.vmdk	File	0.01 KB	07/02/2024, 07:46:43 AM
NFS_DemoB_VM02-00000002.vmdk	File	0.01 KB	06/19/2024, 10:30:47 AM
NFS_DemoB_VM02-00000003.vmdk	File	0.01 KB	06/19/2024, 12:23:45 PM
NFS_DemoB_VM02.vmsd	File	8.794.304 KB	07/02/2024, 07:53:48 AM
NFS_DemoB_VM02.vmxnfo.xml	File	0.01 KB	06/19/2024, 10:30:33 PM
NFS_DemoB_VM02.vmxnfo	Virtual Machine	3.4 KB	06/19/2024, 10:30:33 PM
NFS_DemoB_VM02.vmxnfo	File	0.4 KB	06/19/2024, 10:30:30 AM
NFS_DemoB_VM02.vmxnfo	File	0.02 KB	06/19/2024, 10:30:10 AM
NFS_DemoB_VM02.vmxnfo	File	6.635 KB	06/19/2024, 10:30:51 PM
NFS_DemoB_VM02_2.vmdk	Virtual Disk	5.397.860 KB	06/19/2024, 10:30:52 PM
vmware.log	VM Log File	13.336 KB	07/02/2024, 07:46:43 AM
vmware-2.vmdk	Virtual Disk	107.9 KB	06/19/2024, 07:37:47 AM
vmware-3.vmdk	Virtual Disk	107.9 KB	06/19/2024, 07:47:31 PM



リカバリは、アプリケーションに応じてSnapCenter for VMware またはSnapCenterプラグインから実行できます。

NetAppソリューションは、可視性、検出、修復のためのさまざまな効果的なツールを提供し、ランサムウェアを早期に発見して拡散を防ぎ、必要に応じて迅速に回復してコストのかかるダウンタイムを回避するのに役立ちます。可視化と検出のためのサードパーティ ソリューションやパートナー ソリューションと同様に、従

来の階層型防御ソリューションは依然として普及しています。効果的な修復は、あらゆる脅威への対応において依然として重要です。

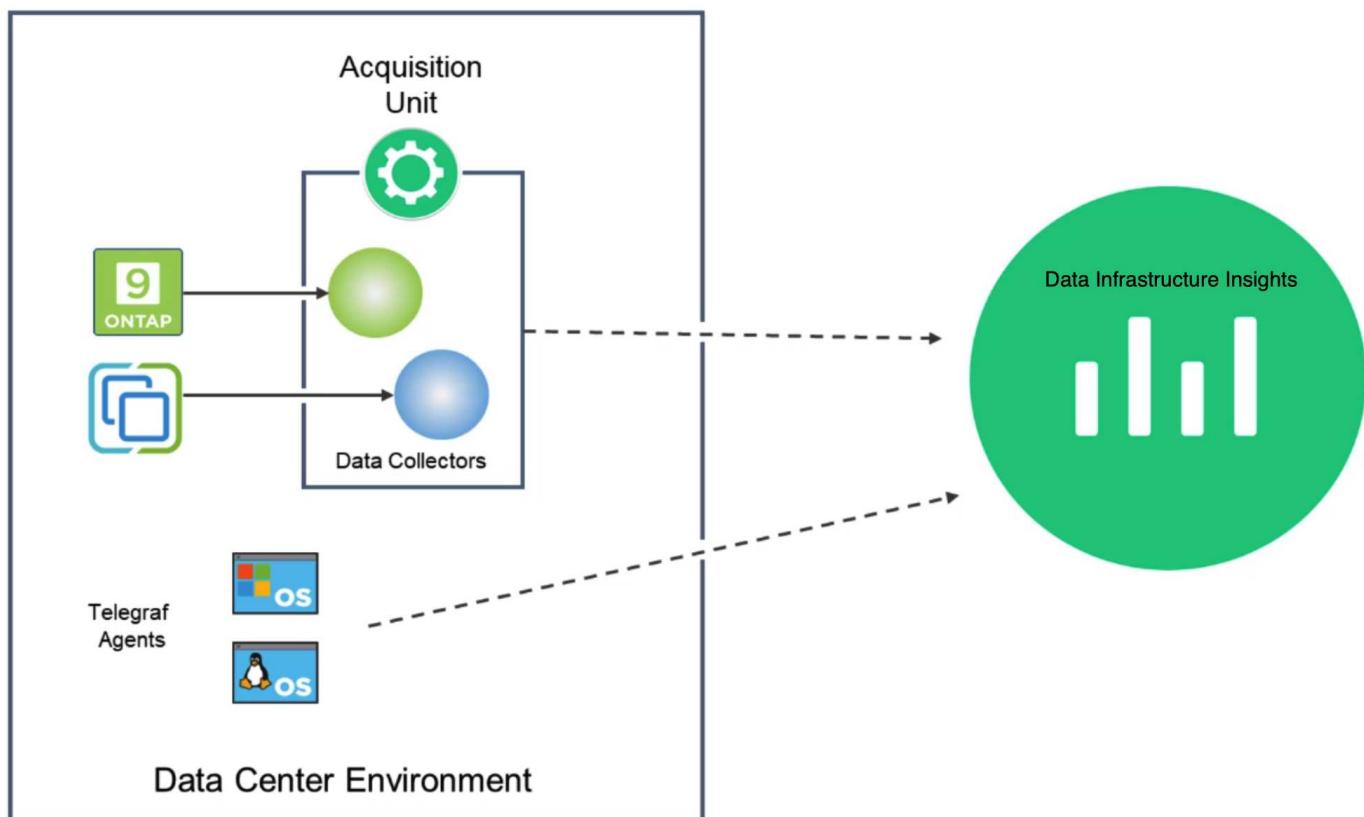
Data Infrastructure Insightsでオンプレミスストレージを監視する

NetApp Data Infrastructure Insights (旧称Cloud Insights) は、オンプレミスとクラウドの両方における IT インフラストラクチャのパフォーマンス、健全性、コストを監視および分析するために設計されたクラウドベースのプラットフォームです。データコレクターを展開し、パフォーマンス メトリックを分析し、ダッシュボードを使用して問題を特定し、リソースを最適化する方法を学習します。

Data Infrastructure Insightsサイトによるオンプレミスストレージの監視

Data Infrastructure Insights は、VMware vSphere や NetApp ONTAPストレージシステムなどの資産のデータコレクターがセットアップされた Acquisition Unit ソフトウェアを通じて動作します。これらのコレクターはデータを収集し、それをData Infrastructure Insightsに送信します。次に、プラットフォームはさまざまなダッシュボード、ウィジェット、メトリック クエリを活用して、ユーザーが解釈しやすいようにデータを整理し、洞察に富んだ分析を作成します。

Data Infrastructure Insightsのアーキテクチャ図:



ソリューション展開の概要

このソリューションでは、Data Infrastructure Insightsを使用してオンプレミスの VMware vSphere およ

びONTAPストレージシステムを監視する方法を紹介します。

このリストには、このソリューションでカバーされている大まかな手順が示されています。

1. vSphere クラスターのデータコレクターを構成します。
2. ONTAPストレージシステム用にデータコレクターを構成します。
3. 注釈ルールを使用してアセットにタグを付けます。
4. 資産を調査して相関させます。
5. Top VM Latency ダッシュボードを使用して、ノイズの多い近隣VMを分離します。
6. VMのサイズを適正化する機会を特定します。
7. クエリを使用してメトリックを分離および並べ替えます。

前提条件

このソリューションでは、次のコンポーネントを使用します。

1. ONTAP 9.13 を搭載したNetApp All-Flash SAN アレイ A400。
2. VMware vSphere 8.0 クラスター。
3. NetApp BlueXPアカウント。
4. データ収集用の資産へのネットワーク接続を備えたローカルVMにインストールされたNetApp Data Infrastructure Insights Acquisition Unit ソフトウェア。

ソリューションの展開

データコレクターを構成する

VMware vSphere およびONTAPストレージシステムのデータコレクターを構成するには、次の手順を実行します。

ONTAPストレージシステムのデータコレクターを追加する

1. Data Infrastructure Insightsにログインしたら、**Observability > Collectors > Data Collectors** に移動し、ボタンを押して新しいData Collectorをインストールします。

The screenshot shows the 'Data Collectors (84)' page in NetApp Cloud Insights. The left sidebar has 'Observability' selected. The top navigation bar includes a search icon, settings, help, and a refresh icon. The main area shows a table with columns: Name ↑, Status, Type, Acquisition Unit, and IP. A blue box highlights the '+ Data Collector' button in the top right corner of the table header.

2. ここから * ONTAP* を検索し、* ONTAP Data Management Software* をクリックします。

The screenshot shows a search interface with a search bar containing 'ontap'. Below it, four options are listed: 'FSx for NetApp ONTAP', 'Cloud Volumes ONTAP', 'ONTAP Data Management Software' (which is highlighted with a blue box and has a cursor over it), and 'ONTAP Select'.

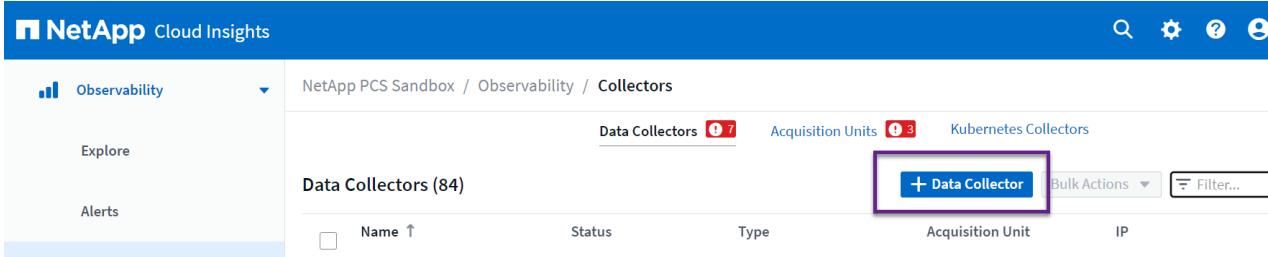
3. *コレクターの設定*ページで、コレクターの名前を入力し、正しい*取得ユニット*を指定して、ONTAPストレージシステムの資格情報を入力します。*保存して続行*をクリックし、ページの下部にある*セットアップの完了*をクリックして設定を完了します。

The screenshot shows the 'Configure Collector' step of the setup process. It includes:

- A progress bar at the top with three steps: 'Select a Data Collector' (done), 'Configure Data Collector' (in progress), and 'Complete Setup' (not yet started).
- A 'NetApp ONTAP Data Management Software' logo.
- A title 'Configure Collector'.
- A section 'Add credentials and required settings' with fields:
 - Name: ntaphci-a300e9u25
 - Acquisition Unit: bxp-au01
 - NetApp Management IP Address: 10.61.185.145
 - User Name: admin
 - Password: (redacted)
- Buttons: 'Save and Continue' (highlighted with a blue box and a cursor), 'Test Connection', and 'Advanced Configuration'.

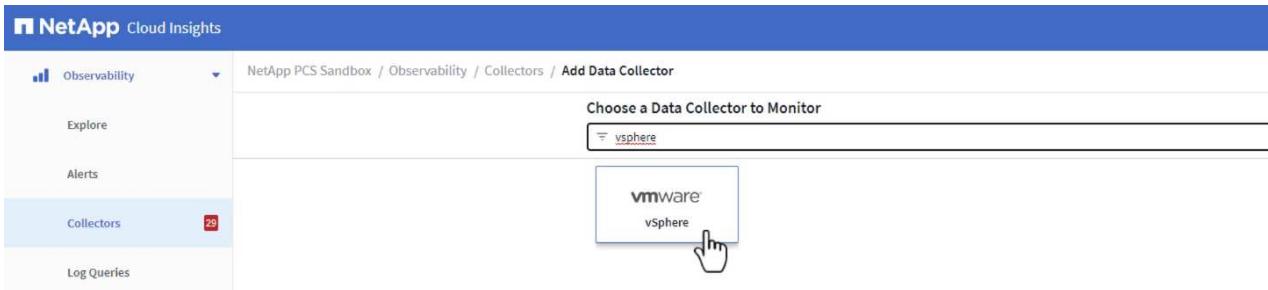
VMware vSphere クラスタのデータコレクタを追加する

- もう一度、**Observability > Collectors > Data Collectors** に移動し、ボタンを押して新しい Data Collector をインストールします。



The screenshot shows the 'Data Collectors (84)' page in NetApp Cloud Insights. The left sidebar has 'Observability' selected. The top navigation bar includes a search icon, settings, help, and a refresh icon. The main header is 'NetApp PCS Sandbox / Observability / Collectors'. Below the header, there are tabs for 'Data Collectors' (with 7 notifications), 'Acquisition Units' (with 3 notifications), and 'Kubernetes Collectors'. A large blue button labeled '+ Data Collector' is highlighted with a red box. Below it are filter and bulk action options.

- ここから vSphere を検索し、**VMware vSphere** をクリックします。



The screenshot shows the 'Add Data Collector' page. The left sidebar has 'Collectors' selected, with a red notification badge showing 29. The top navigation bar is identical to the previous screenshot. The main area has a heading 'Choose a Data Collector to Monitor' and a search bar with 'vsphere' typed in. Below the search bar, a list item 'VMware vSphere' is shown with a cursor pointing at it.

- *コレクターの構成*ページで、コレクターの名前を入力し、正しい*取得ユニット*を指定して、vCenter サーバーの資格情報を入力します。 *保存して続行*をクリックし、ページの下部にある*セットアップの完了*をクリックして設定を完了します。

Configure Collector

Add credentials and required settings Need Help?

Name Acquisition Unit

Virtual Center IP Address User Name

Password

Complete Setup **Test Connection**

Advanced Configuration

Collecting:

- Inventory
- VM Performance

Inventory Poll Interval (min) Communication Port

Filter VMs by Choose 'Exclude' or 'Include' to Specify a List

Filter Device List (Comma Separated Values For Filtering By ESX_HOST, CLUSTER, and DATACENTER Only)

Performance Poll Interval (sec)

Collect basic performance metrics only

Complete Setup **Test Connection**

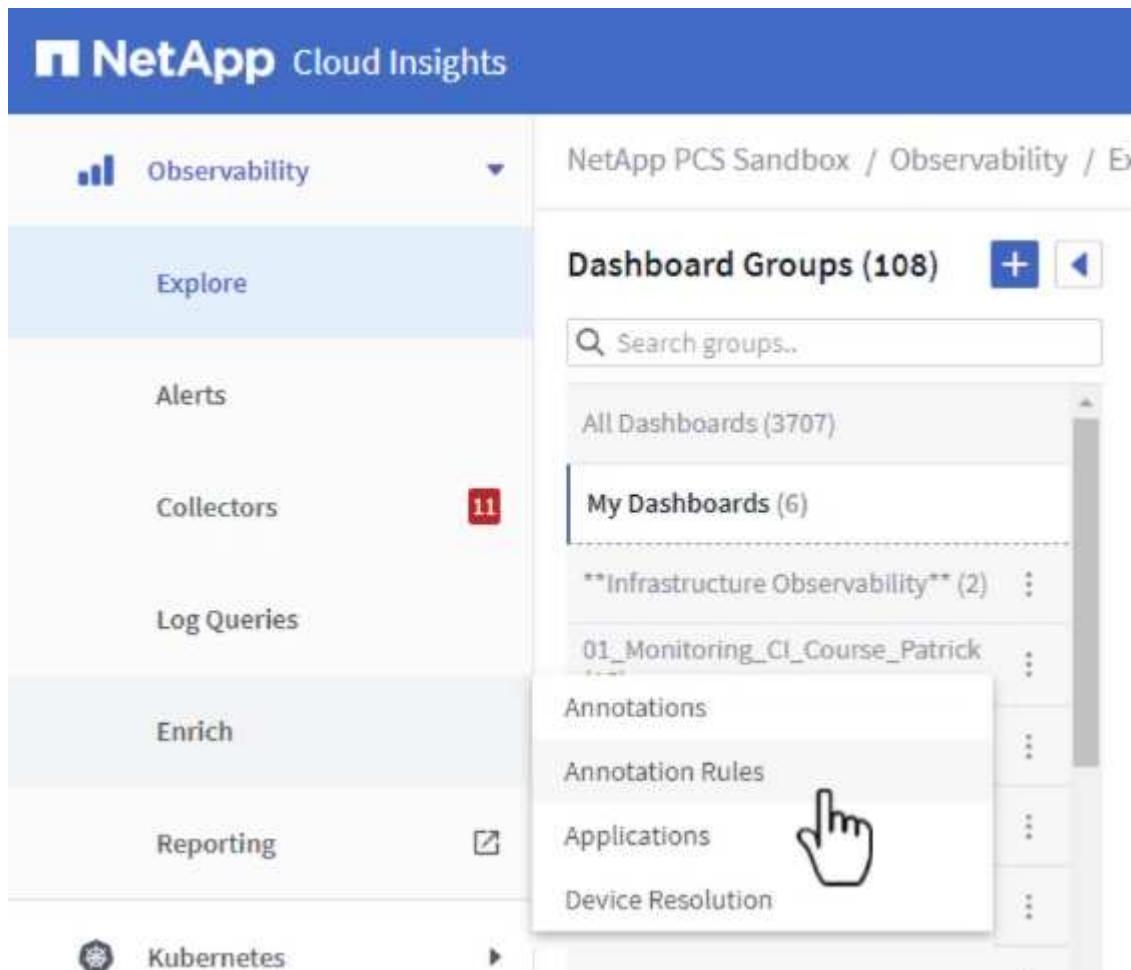
アセットに注釈を追加する

注釈は、アセットにタグを付け、Cloud Insightsで利用できるさまざまなビューやメトリック クエリでフィルタリングしたり識別したりできるようにするための便利な方法です。

このセクションでは、*データセンター*でフィルタリングするための注釈が仮想マシン アセットに追加されます。

注釈ルールを使用してアセットにタグを付ける

- 左側のメニューで、**Observability > Enrich > Annotation Rules** に移動し、右上の **+ Rule** ボタンをクリックして新しいルールを追加します。



- [ルールの追加] ダイアログ ボックスで、ルールの名前を入力し、ルールが適用されるクエリ、影響を受ける注釈フィールド、および入力される値を検索します。

Add Rule

Name
Add tags to Solutions Engineering VMs

Query
Solutions Engineering VMs

Annotation
DataCenter

Value
Solutions Engineering

Cancel **Save** 

3. 最後に、「注釈ルール」ページの右上隅にある「すべてのルールを実行」をクリックしてルールを実行し、アセットに注釈を適用します。

NetApp PCS Sandbox / Observability / Enrich / Annotation Rules

Annotation rules (217) + Rule  Filter...

Name	Resource Type	Query	Annotation	Value
Annotate Tier 1 Storage Pools	Storage Pool	Find Storage Pools (no aggr0) for Tier...	Tier	Tier 1
Annotate Tier 2 Storage Pools	Storage Pool	Find Storage Pools (no aggr0) for Tier...	Tier	Tier 2

Rules running... Run All Rules 

資産の調査と相関関係の分析

Cloud Insights は、ストレージシステムと vSphere クラスター上で一緒に実行されている資産に関する論理的な結論を導き出します。

このセクションでは、ダッシュボードを使用して資産を相関させる方法を説明します。

ストレージパフォーマンスダッシュボードから資産を相關させる

1. 左側のメニューで、**Observability > Explore > All Dashboards** に移動します。

The screenshot shows the NetApp Cloud Insights interface. The top navigation bar has 'NetApp Cloud Insights' and a 'Cloud Icons' logo. Below it, a blue header bar contains the 'Observability' icon and the word 'Observability'. A dropdown menu is open over the 'Explore' button, which is highlighted in light blue. The dropdown menu lists several options: 'Home Dashboard', 'All Dashboards' (with a hand cursor icon pointing at it), '+ New Dashboard', 'Metric Queries', and 'Infrastructure Insights' (with a 'NEW' badge). The 'Collectors' button is also visible with a red badge showing the number '17'. The background shows a blurred view of other dashboard components.

2. + ギャラリーからボタンをクリックすると、インポート可能な既製のダッシュボードのリストが表示されます。

The screenshot shows the 'Dashboards' page in NetApp Cloud Insights. The top navigation bar is identical to the previous screenshot. The left sidebar shows 'Explore' selected. The main area displays 'Dashboard Groups (108)' and 'All Dashboards (3,708)'. A search bar labeled 'Search groups...' is present. On the right, there is a table listing dashboards, with columns for 'Name', 'Owner', and 'Actions'. Two buttons are visible: '+ From Gallery' and '+ Dashboard'. A hand cursor icon points to the '+ From Gallery' button. The table lists two items: '# Internal Volumes by IOPS Range [do not set as Home Page!]' owned by 'Workneh Hilina' and '# Internal Volumes by IOPS Range' owned by 'Simon Wu'.

3. リストからFlexVolパフォーマンスのダッシュボードを選択し、ページの下部にあるダッシュボードの追加ボタンをクリックします。

- ONTAP FAS/AFF - Cluster Capacity
- ONTAP FAS/AFF - Efficiency
- ONTAP FAS/AFF - FlexVol Performance
- ONTAP FAS/AFF - Node Operational/Optimal Points
- ONTAP FAS/AFF - PrePost Capacity Efficiencies
- Storage Admin - Which nodes are in high demand?
- Storage Admin - Which pools are in high demand?
- StorageGRID - Capacity Summary
- StorageGRID - ILM Performance Monitoring
- StorageGRID - MetaData Usage
- StorageGRID - S3 Performance Monitoring
- VMware Admin - ESX Hosts Overview
- VMware Admin - Overview
- VMware Admin - VM Performance
- VMware Admin - Where are opportunities to right size?
- VMware Admin - Where can I potentially reclaim waste?
- VMware Admin - Where do I have VM Latency?

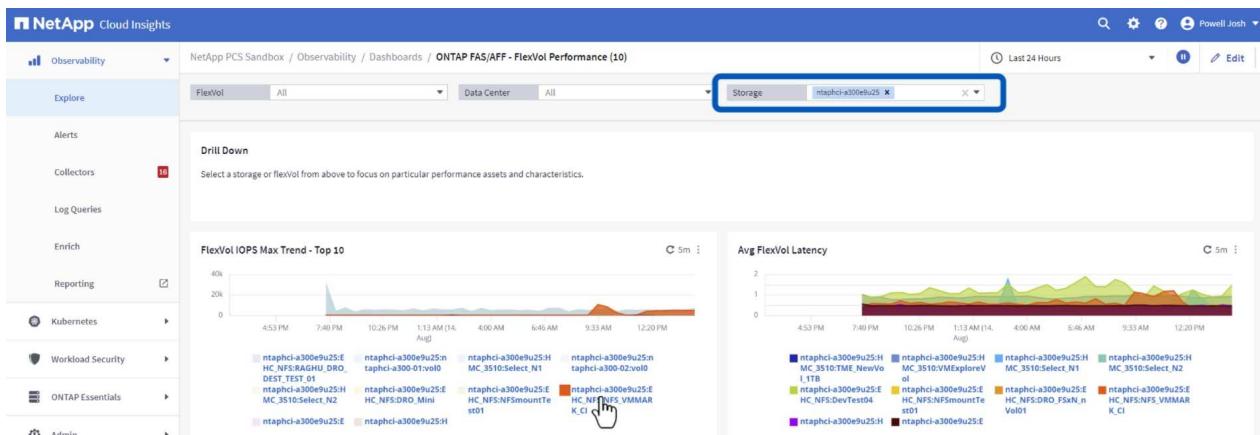
Additional Dashboards (13)

These dashboards require additional data collectors to be installed. [Add More](#)

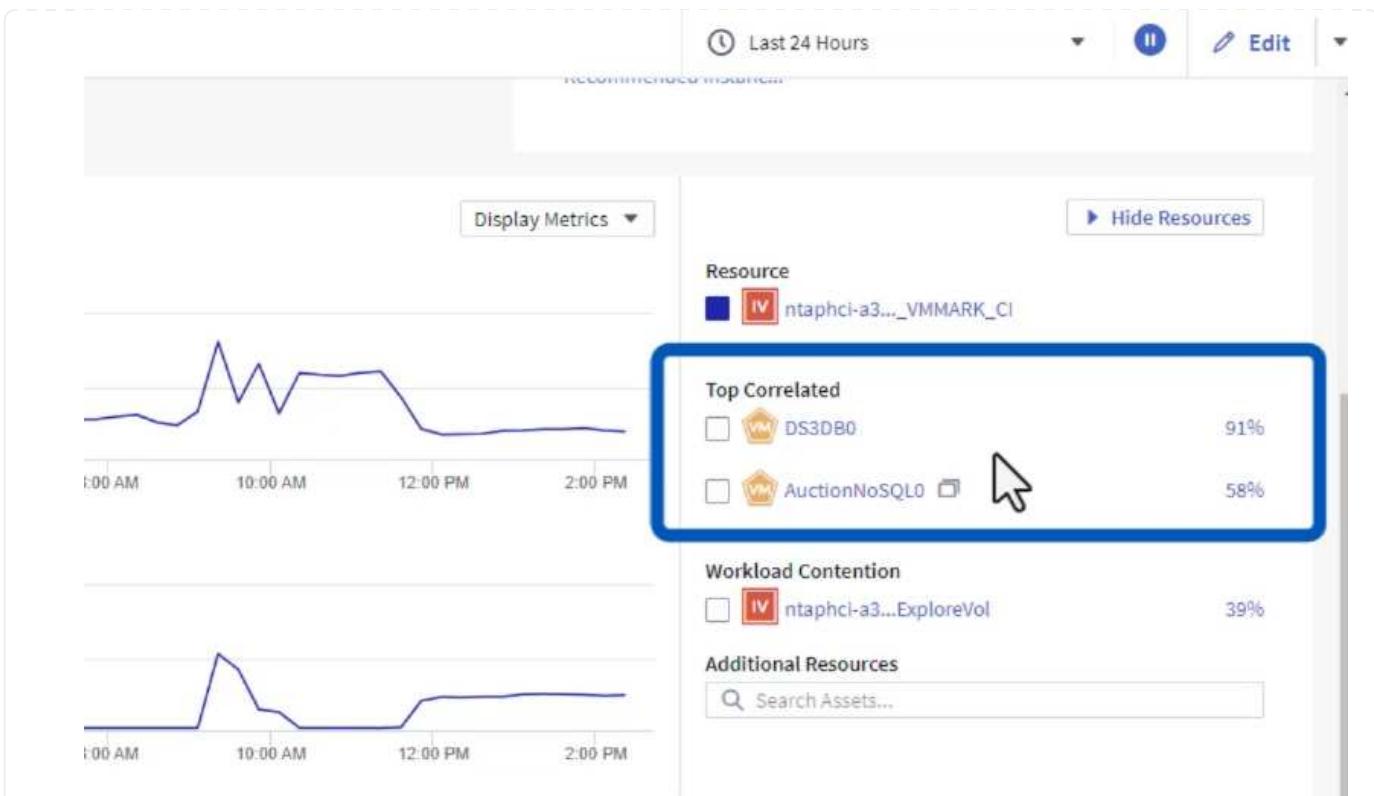
[Add Dashboards](#)

[Go Back](#)

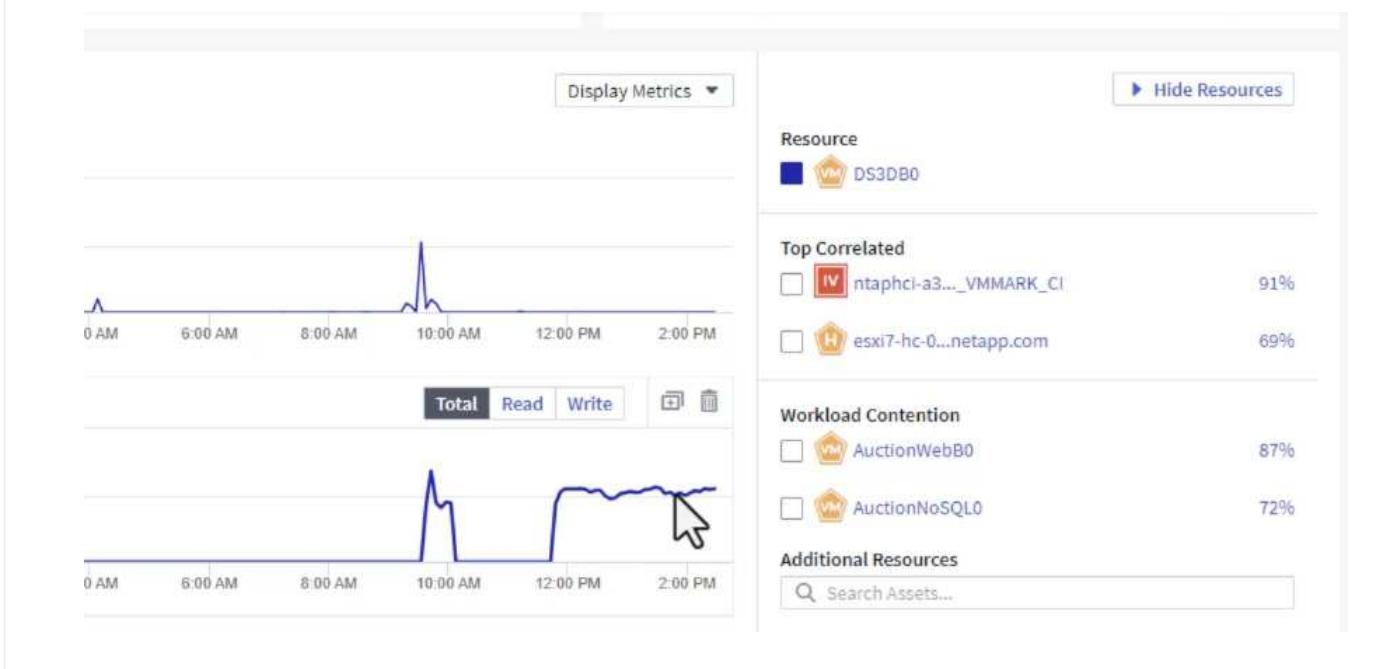
- インポートしたら、ダッシュボードを開きます。ここから、詳細なパフォーマンス データを含むさまざまなウィジェットを表示できます。フィルターを追加して単一のストレージ システムを表示し、ストレージ ボリュームを選択して詳細を表示します。



- このビューでは、このストレージ ボリュームに関連するさまざまなメトリックと、ボリューム上で実行されている最も使用率が高く相関関係にある仮想マシンを確認できます。



6. 使用率が最も高い VM をクリックすると、その VM のメトリックが詳細に表示され、潜在的な問題が表示されます。



Cloud Insightsを使用して、騒がしい隣人を特定する

Cloud Insights には、同じストレージ ボリューム上で実行されている他の VM に悪影響を与えていたりするピア VM を簡単に分離できるダッシュボードが備わっています。

トップ VM レイテンシ ダッシュボードを使用して、ノイズの多い近隣 VM を分離します。

- この例では、ギャラリーにある VMware Admin - Where do I have VM Latency? というダッシュボードにアクセスします。

The screenshot shows the 'Dashboards' section of the NetApp PCS Sandbox interface. On the left, there's a sidebar with 'Dashboard Groups (108)' and a search bar. The main area is titled 'My Dashboards (6)' and lists six dashboards, each with a title, owner, and a small preview icon. The sixth dashboard, 'VMware Admin - Where do I have VM Latency? (9)', is highlighted with a blue selection bar and a hand cursor icon pointing at it.

- 次に、前の手順で作成した Data Center アノテーションでフィルタリングして、アセットのサブセットを表示します。

The screenshot shows the 'VMware Admin - Where do I have VM Latency? (9)' dashboard. At the top, there's a filter bar with several dropdowns and buttons. One of the dropdowns is labeled 'Annotations' and has 'Data Center' selected, indicated by a purple selection bar and a hand cursor icon pointing at it. Other options in the dropdown include 'Solutions Engineering' and 'All'.

- このダッシュボードには、平均レイテンシによる上位 10 個の VM のリストが表示されます。ここから、対象の VM をクリックして詳細を確認します。

VM Count With Latency Concern

C 5m

Avg Latency (all VMs)

C 5m

50

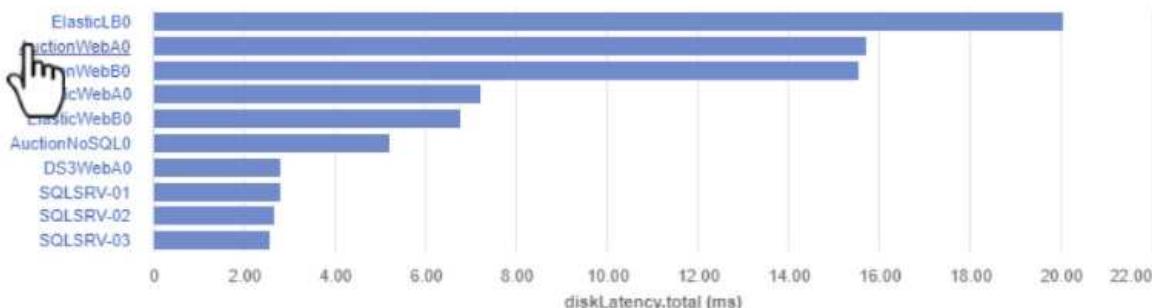
VM's

1.55 ms

diskLatency.total

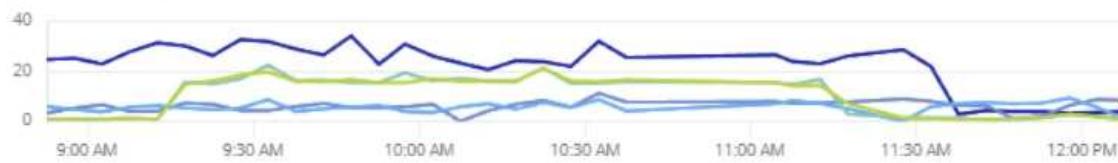
Avg VM Latency - Top 10

C 5m

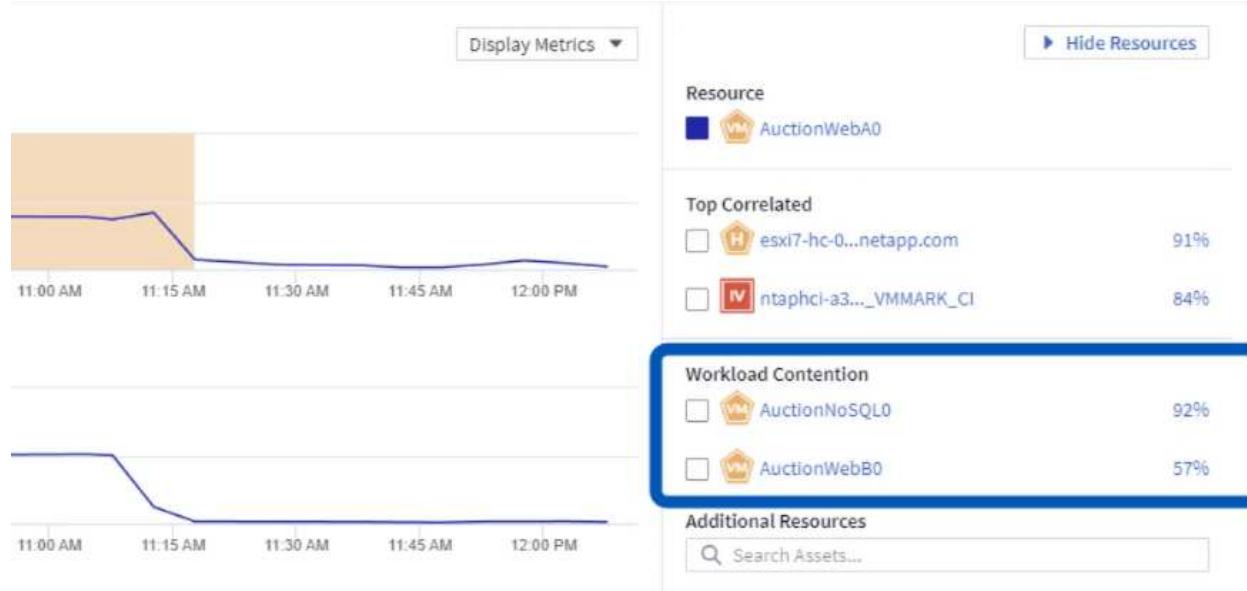


Top 5 Avg VM Latency Trend

C 30s



4. ワークロードの競合を引き起こす可能性のある VM がリストされ、利用可能になります。これらの VM のパフォーマンス メトリックを詳しく調べて、潜在的な問題を調査します。



Cloud Insightsで過剰利用されているリソースと利用されていないリソースを表示する

VM リソースを実際のワークロード要件に一致させることで、リソース使用率を最適化し、インフラストラクチャとクラウド サービスのコストを削減できます。 Cloud Insights のデータはカスタマイズ可能で、過剰に使用されている VM や十分に使用されていない VM を簡単に表示できます。

VM を適切なサイズにする機会を特定する

- この例では、ギャラリーにある **VMware Admin - 適切なサイズにする機会はどこにありますか？** というダッシュボードにアクセスします。

My Dashboards (6)



Name ↑

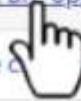
All SAN Array Status (2)

Cloud Volumes ONTAP - FlexVol Performance (6)

ONTAP - Volume Workload Performance (Frontend) (7)



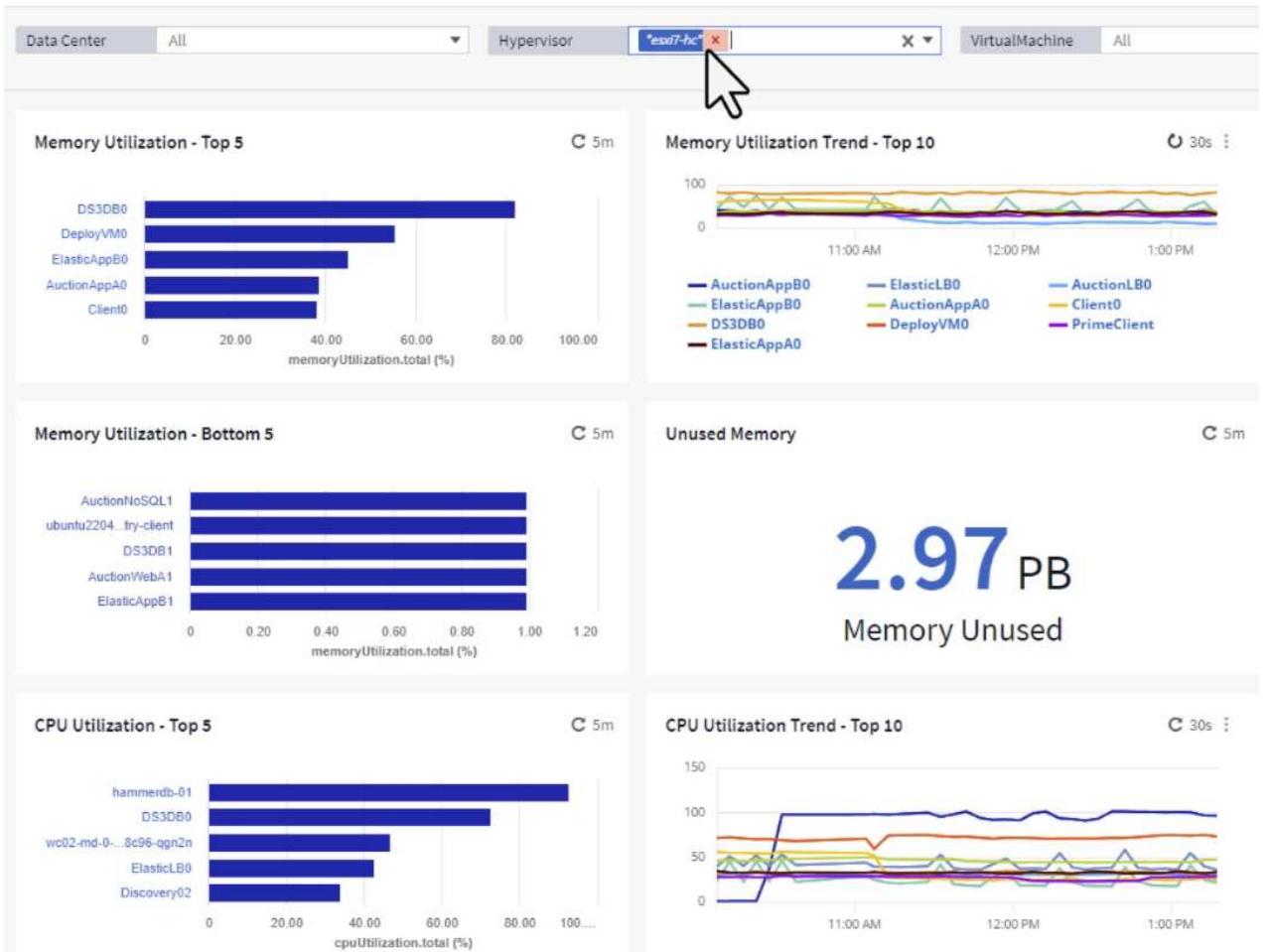
[VMware Admin - Where are opportunities to right size? \(37\)](#)



[VMware Admin - Where can I potentially reclaim waste? \(11\)](#)

[VMware Admin - Where do I have VM Latency? \(9\)](#)

- まず、クラスター内のすべての ESXi ホストでフィルタリングします。次に、メモリと CPU 使用率による上位および下位の VM のランキングを確認できます。



3. テーブルを使用すると、並べ替えが可能になり、選択したデータの列に基づいて詳細が提供されます。

Memory Usage

C 5m :

121 items found

Virtual Machine	memory (MiB)	memoryUt...
DS3DB0	768.0	81.64
DeployVM0	92.0	55.06
ElasticAppB0	92.0	44.91
AuctionAppA0	336.0	38.42
Client0	480.0	37.98
AuctionAppB0	336.0	37.83
ElasticAppA0	92.0	35.63
ElasticLB0	96.0	35.13
user-cluster1-8872k-78c65dd794...	92.0	32.47
PrimeClient	48.0	30.30

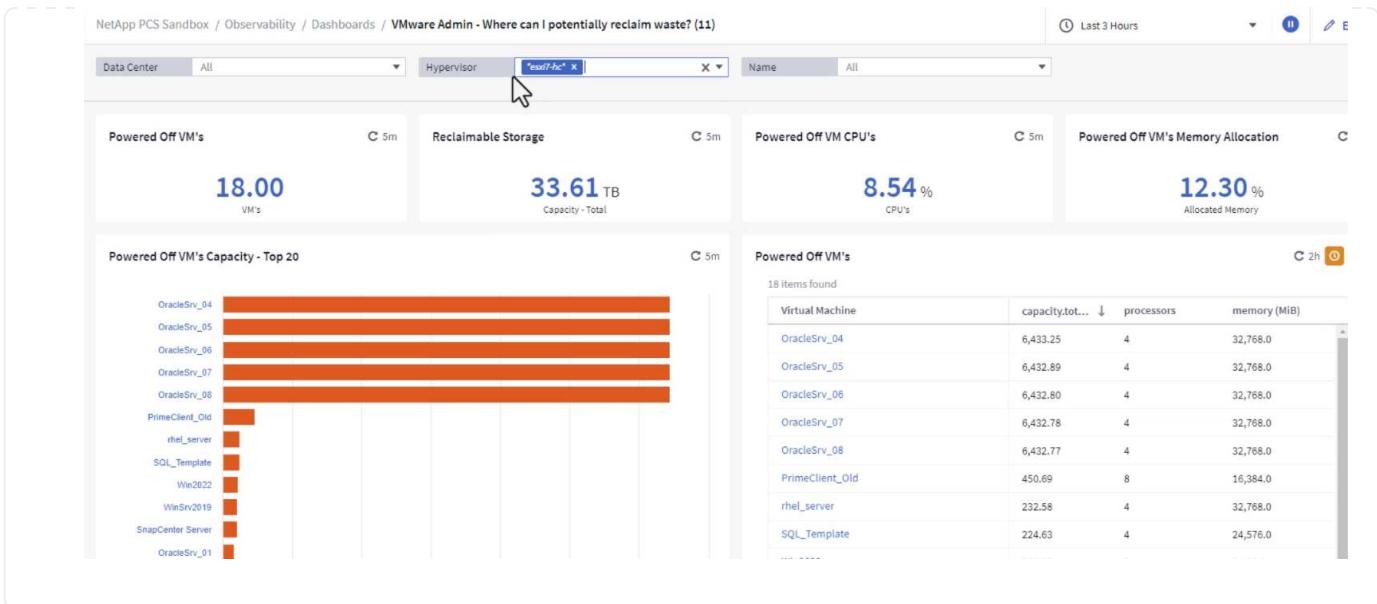
CPU Utilization

C 5m :

121 items found

Virtual Machine	name
hammerdb-01	hammerdb-01
DS3DB0	DS3DB0
wc02-md-0-xwdgb-8cf48c96-qgn...	wc02-md-0-xwdgb-8cf48c96-qg...
ElasticLB0	ElasticLB0

- VMware Admin - 無駄を潜在的に回収できる場所はどこ? という別のダッシュボードには、電源がオフになっている VM が容量使用量によって並べ替えられて表示されます。

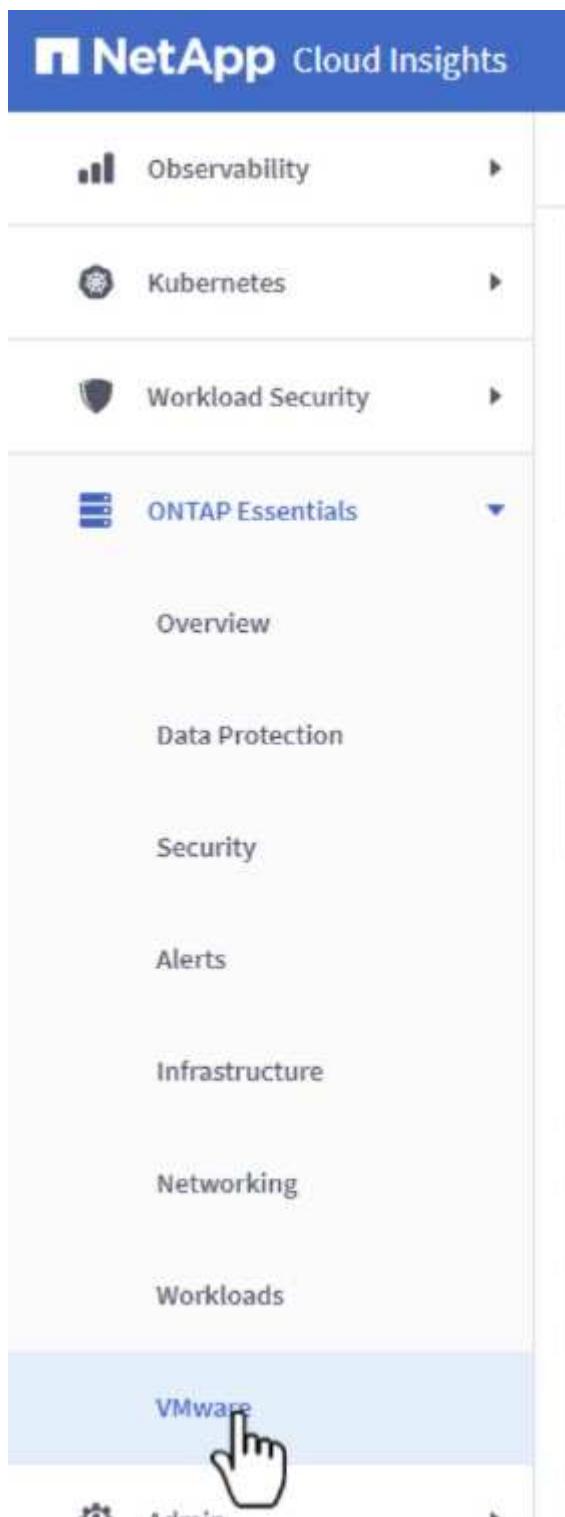


クエリを使用してメトリックを分離および並べ替える

Cloud Insightsによって収集されるデータの量は非常に包括的です。メトリック クエリは、大量のデータを便利な方法で並べ替え、整理するための強力な手段を提供します。

ONTAP Essentials で詳細な VMware クエリを表示する

1. 包括的な VMware メトリック クエリにアクセスするには、* ONTAP Essentials > VMware* に移動します。



2. このビューでは、上部にデータをフィルタリングおよびグループ化するための複数のオプションが表示されます。すべてのデータ列はカスタマイズ可能で、追加の列も簡単に追加できます。

VirtualMachine | All Virtual Machines

Filter by Attribute: storageResources.storage.vendor: NetApp | host.os: "vmware"

Filter by Metric: +

Group By: Virtual Machine

Formatting: Show Expanded Details | Conditional Formatting | Background Color | Show In Range as green

281 items found

Virtual Machine	name	powerState	capacity.used (GiB)	capacity.total (GiB)	capacityRatio.us...	diskIops.total (IO/s)	diskLatency.total...	diskThroughput....
01rfk8sprodclient	01rfk8sprodclient	On	49.38	69.86	70.68	1.21	8.13	0.01
02rfk8sprodserver	02rfk8sprodserver	On	63.64	74.06	85.93	22.80	4.13	0.11
03rfk8sprodmaster01	03rfk8sprodmaster01	On	65.13	77.21	84.36	26.64	5.64	0.20
04rfk8sprodmaster02	04rfk8sprodmaster02	On	63.89	76.27	83.77	26.82	5.14	0.16
05rfk8sprodmaster03	05rfk8sprodmaster03	On	63.77	75.58	84.38	28.23	4.63	0.17
AIQUM 9.11 (vApp)	AIQUM 9.11 (vApp)	On	152.00	152.00	100.00	23.24	0.19	0.41
AIQUM 9.12 (Linux)	AIQUM 9.12 (Linux)	On	55.28	100.00	55.28	0.01	11.83	0.00
AN-JumpHost01	AN-JumpHost01	On	90.00	90.00	100.00	1.39	0.19	0.01
AuctionAppA0	AuctionAppA0	On	9.38	16.00	58.62	1.21	0.44	0.12
AuctionAppA1	AuctionAppA1	On	6.44	16.00	40.26	0.00	3.00	0.00

まとめ

このソリューションは、NetApp Cloud Insightsの使用を開始する方法と、この可観測性ソリューションが提供できる強力な機能の一部を紹介する入門書として設計されました。製品には何百ものダッシュボードとメトリック クエリが組み込まれているため、すぐに使い始めることができます。Cloud Insightsのフル バージョンは 30 日間の試用版として提供されており、基本バージョンはNetApp の顧客に無料で提供されます。

追加情報

このソリューションで紹介されているテクノロジーの詳細については、次の追加情報を参照してください。

- ["NetApp BlueXPとData Infrastructure Insightsのランディング ページ"](#)
- ["NetApp Data Infrastructure Insights ドキュメント"](#)

著作権に関する情報

Copyright © 2025 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隨時、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 5225.227-19（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権を有し、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権については、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。